République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Cheikh Larbi Tbessi Tébessa
Faculté des Sciences de l'Ingénieur
Département Informatique & Mathématique

MEMOIRE

Présenté en vue de l'obtention du titre de
Magistère en Informatique
Option : Intelligence Artificielle

Routage et Conservation d'Energie dans les Réseaux Mobiles Ad hoc utilisant OLSR

Présenté par : M^r^ Nabil GHANEM.

Dirigé par : MC. GHOUALMI Nacira.

Soutenu le 10/01/2010

Devant le Jury composé de:

Président : P^r^. Benmohammed Mohammed	Professeur	Université de Constantine
Rapporteur : D^r^. Ghoualmi-Zine Nacira	Maître de conférences	Université d'Annaba
Examinateurs :		
D^r^ Meslati Djamel	Maître de conférences	Université d'Annaba
D^r^ Farah Nadir	Maître de conférences	Université d' Annaba

A ma famille...

Remerciements

Si ce mémoire a pu voir le jour, c'est certainement grâce au soutien et l'aide de plusieurs personnes qui m'ont permis d'accomplir ce travail dans des conditions idéales. Je profite de cet espace pour les remercier tous :

Je remercie tout particulièrement M^{me} Nacira GHOUALMI pour avoir accepté de diriger ce mémoire, pour ses précieux conseils, et pour la confiance qu'elle m'a accordée.

Mes très vifs remerciements vont au Professeur BENMOHAMMED Mohammed pour m'avoir fait honneur et avoir accepté la position du Président du jury.

Je suis très heureux et c'est un honneur pour moi que D^{r} MESLATI Djamel et D^{r} FARAH Nadir aient accepté de faire partie du jury. Qu'ils trouvent ici l'expression de toute ma profonde gratitude.

Je remercie chaleureusement mon ami d'enfance, ami de toujours Ridha MOUICI pour son aide très précieuse.

Enfin, à tous les membres de ma famille pour leur soutien indéfectible, leur encouragement, leur disponibilité et leur compréhension.

Résumé

L'informatique mobile exige beaucoup de traitements. Mises à part les activités de communication, la consommation d'énergie est l'un des problèmes les plus critiques pour les dispositifs mobiles à pile. Notamment, dans les réseaux ad hoc où chaque nœud est responsable de la transmission des paquets de données des nœuds voisins, une précaution particulière doit être prise non seulement pour minimiser la consommation d'énergie de tous les nœuds pertinents mais également pour équilibrer les niveaux individuels des piles. Un déséquilibre dans l'utilisation de l'énergie peut provoquer un échec sur l'un des nœuds surchargés et conduire au partitionnement et à la réduction de la durée de vie du réseau. Dans ce mémoire, nous présentons d'abord l'algorithme du routage OLSR (*Optimized Link State Routing*) standard. Ensuite, nous intégrons à OLSR le critère de consommation d'énergie en tant que critère de QoS. Dans cet objectif, nous apportons une amélioration au niveau de l'heuristique du choix des nœuds relais multipoints MPR (*Multipoint Relays*) car elle représente le point fort du routage OLSR. Trois algorithmes sont proposés pour le processus de sélection des MPR selon la contrainte d'énergie.

Mots clés : Réseaux mobiles ad hoc, performance des réseaux ad hoc, consommation d'énergie, routage par état de lien, communication sans fil.

الملخصّ :

إن المعلوماتيّة النّقالة تتطلّب عدّة أنشطة. بغض النظر عن عمليات الإتّصال ، يعتبر استهلاك الطّاقة من المشاكل الأكثر حساسية بالنّسبة للأجهزة الجوّالة ذات كومة على وجه الخصوص في الشّبكات الخاصة حيث كل نقطة هي مسؤولة على إرسال بيانات النّقط المجاورة.

حذر خاص يجب القيام به ليس فقط من أجل تخفيض استهلاك طاقة النقط المعنية و لكن أيضا العمل على تحقيق توازن المستوى الفردي للكوم . أي خلل في استعمال الطّاقة يمكن يؤدّي إلى فشل إحدى النّقط ذات حمولة الزّائدة، الفصل في الشبكة و الإنقاص في مدّة حياتها .

في هذا البحث نقدم أولا، منهج OLSR (Optimized Link State Routing) العام، بعد ذلك نضيف إلى OLSR معيار استهلاك الطّاقة كمعيار لجودة الخدمة (QOS).

في هذا الصّدد، نقدم تحسين في مستوى الاختيار التّجريبي لنقاط الوصل المتعدّدة النّقط MPR لأنها تمثل نقطة مركز قوة منهج OLSR. لذلك نطرح 3 قواعد في عملية اختيار نقاط الوصل MPR حسب قيد الطّاقة.

الكلمات الرّيسية : الشبكات الخاصة النّقالة ، فعالية الشبكة الخاصة ، استهلاك الطّاقة، منهج على أساس حالة الرابطة، الإتصال اللاّسلكي.

Abstract

Mobile computer science requires much processing. Beside the communication activities, the energy consumption is one of the most critical problems for the mobile devices with battery. Especially, in ad hoc networks where every node is responsible to transmit data packets for the neighbor nodes, a particular wariness must be not only taken to minimize the energy consumption of all appropriate nodes but also to balance the batteries individual levels. An Unbalance in the energy usage can procure a failure on one of the overloaded nodes and lead to the partitioning and to the decreasing the network lifetime.

In this report paper, we introduce first the standard OLSR routing algorithm (Optimized Link State Routing). Then, we insert into OLSR the energy consumption criteria as QoS criteria.

In this object, we bring an improvement at multipoint relays (MPR) nodes selection heuristic because it represents the strong point of the OLSR routing.

Three algorithms are suggested for the MPR selection process according to the energy constraint.

Keywords : Mobiles ad hoc networks, ad hoc networks performance, energy consumption, link state routing, wireless communication.

Table des figures

Liste des tableaux

Table des matières

Introduction

1. Motivations

Le domaine des réseaux ad-hoc suscite de plus en plus d'intérêt depuis ces dernières années. La particularité de ce type de réseau est qu'il n'a besoin d'aucune installation fixe à l'inverse d'autres types de réseaux. Donc, il est facile et rapide à déployer. De plus, les différents composants de ce réseau sont libres de se mouvoir mais, en même temps, ceci résulte en une topologie dynamique susceptible de changer d'une façon imprévisible.

L'activité du groupe MANET [1] (*Mobile Ad-hoc Networks*) de l'IETF (*Internet Engineering Task Force*) montre que le développement de ces réseaux sans fil et sans infrastructure est en plein essor. Les industriels imaginent déjà toutes sortes d'applications. Militaires bien sûr pour la création de réseaux tactiques mobiles, mais aussi civiles pour les interventions d'urgence, les communications avec les automobiles, la reconfiguration de réseaux sans câblage dans les entreprises ou bien la création de réseaux temporaires autour d'événement. Sans conteste, les atouts majeurs de cette nouvelle génération de réseaux mobiles sont la flexibilité et leur faible coût.

Dans les réseaux ad hoc mobiles, des nœuds indépendants coopèrent les uns avec les autres pour implémenter les fonctionnalités du réseau, tel que le routage des paquets. Étant donné que les nœuds composant le réseau ad hoc sont autonomes et libres de se mouvoir à leur gré, la conception d'un protocole de routage résistant au facteur de mobilité devient une tâche complexe à élaborer.

Un des grands challenges pour ce type de réseaux réside dans l'autonomie restreinte des stations mobiles le constituant. Effectivement, cette autonomie est fournie par de simple batteries, et donc représente une ressource finie et rare. Chaque paquet envoyé ou reçu, de même que chaque utilisation du terminal mobile profite de cette ressource. Et comme l'amélioration du confort, et de l'ensemble des fonctionnalités offertes aux utilisateurs est de plus en plus appréciable, réduire la consommation d'énergie au minimum est un défi important dans les réseaux mobiles. Cet objectif devient davantage considérable pour les réseaux ad hoc, où les stations ont de surcroît la fonction de

routage. En effet, relayer des paquets au nom d'autres nœuds, consomme l'énergie propre au nœud.

2. Contributions

Nous avons constaté que la totalité des protocoles de routage actuels OLSR[1], AODV[2], DSR[3], FSR[4], …, proposés au sein du groupe MANET de l'IETF, utilisent la même métrique (nombre de sauts ou temps de transmission minimum). Constatant, également, que le choix du protocole de routage influe réellement sur la consommation d'énergie dans les réseaux ad hoc, nous proposons de nouveaux protocoles de routage utilisant des métriques basées sur l'énergie. Ces métriques vont permettre de rallonger la durée de vie des batteries, et par conséquent la durée de vie du réseau ad hoc (survivabilité du réseau).

Ces nouveaux protocoles permettent ainsi, d'assurer que la connectivité du réseau soit maintenue aussi longtemps que possible, tout en évitant de le partitionner en sous-réseau disjoints. Les protocoles que nous avons développé E_OLSR1, E_OLSR2 et E_OLSR3 sont des protocoles proactifs et sont basés sur l'un des plus importants protocoles de routage actuels : OLSR.

E_OLSR1 conserve le même principe du chois des MPR dans E_OLSR1, néanmoins il utilise la métrique énergétique dans le cas ou plusieurs candidats MRP lui sont présentés.

En revanche le processus de sélection des MPR dans E_OLSR2 est basé sur la sélection intrinsèque énergétique. Le facteur énergie est un paramètre prioritaire dans le routage d'E_OLSR2.

E_OLSR3 une approche hybride d'E_OLSR1 et d'E_OLSR2, est basée également sur un processus de sélection des MPR selon la consommation d'énergie. Une contrainte de seuil d'énergie résiduelle est intégrée à l'heuristique de choix des MPR. Le protocole E_OLSR3 favorise la route dont la durée de vie est maximum, et par conséquent la route qui ne contient pas de nœuds dont la durée de vie est faible. En effet ceci permet de distribuer d'une manière équitable la surcharge du routage dans le réseau.

L'ordre quasi-linéaire de ce document correspond à une volonté d'amener le lecteur à mieux comprendre les différentes caractéristiques de chacune des solutions proposées. Ce document est organisé comme suit :

[1] Optimized Link State Routing
[2] Ad hoc On Demand Vector
[3] Dynamic Service Routing
[4] Fisheye State Routing

Le prochain chapitre de ce mémoire présente une vision d'ensemble sur les réseaux ad hoc. Nous y détaillons les principaux algorithmes de routage ad hoc existants. Ces notions sont nécessaires pour la compréhension des chapitres suivants du document.

Le deuxième chapitre présente en détail le protocole de routage OLSR. Ce protocole se distingue par sa technique de diffusion optimisée appelée relais multipoint.

Le chapitre 3 est un état de l’art des techniques de conservation d’énergie dans les réseaux ad hoc. Nous arborons quelques propositions parmi les plus intéressantes, permettant de réduire cette consommation pour chacune des couches du modèle OSI. Nous mettons l'accent sur la couche réseau (routage) et comparons, par un ensemble de simulations, l'impact du routage sur la consommation d’énergie.

Dans le dernier chapitre, nous présentons de nouveaux protocoles proactifs E_OLSR1, E_OLSR2 et E_OLSR3 permettant d'assurer la survivabilité du réseau, en réduisant autant que possible, la consommation des batteries dans les nœuds. Les procédures de recherche de route y sont décrites pour chaque protocole et sont comparés à celles utilisées dans OLSR. Un ensemble de simulation a été réalisé pour comparer leurs performances.

Enfin, une synthèse globale reprenant l'ensemble du travail effectué pendant ce mémoire, conclut ce document.

CHAPITRE

1 Routage dans les Réseaux sans fil ad hoc

1. Introduction

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 [2] (*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 (cf. 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 [1] (*Mobile Ad-hoc Networks*).

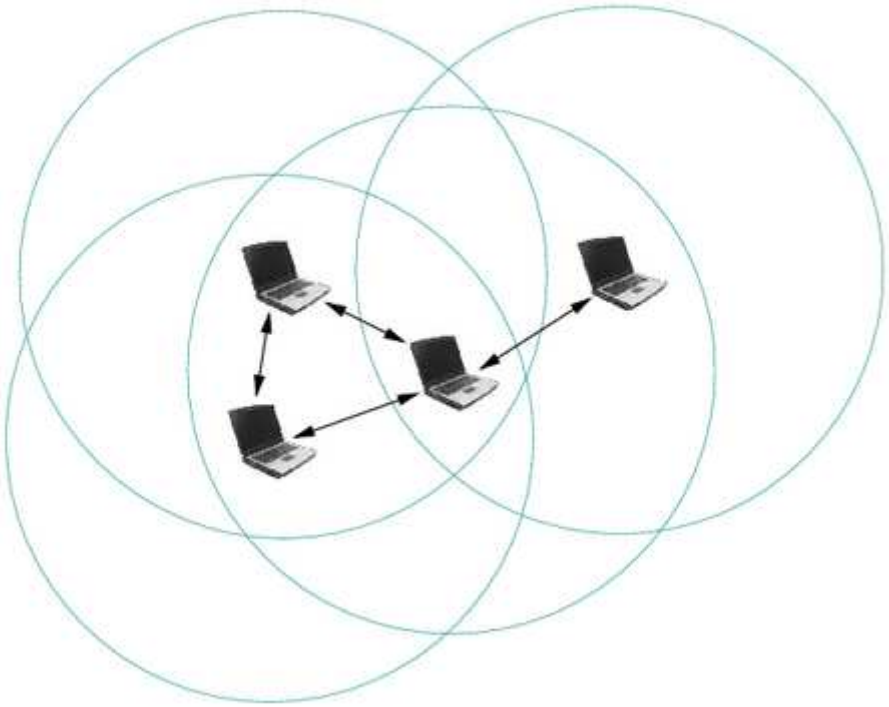


FIG. 1.1 – Exemple de réseau sans fil

Mais des problèmes existent, de la couche matérielle jusqu'à la couche application [3]. 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 de routage totalement distribués, dans le but d'obtenir un comportement global cohérent malgré le caractère plus ou moins indépendant de chaque nœud.

2. Définition des réseaux sans fil ad hoc

Les réseaux ad hoc sont caractérisés par un ensemble de stations, pouvant être mobiles, interconnectées et communiquent entre elles via une interface radio (uni ou bidirectionnelle). Ce type de réseau ne nécessite aucune infrastructure préexistante et aucune administration centralisée formant ainsi un réseau temporaire. Ceci résulte en une topologie changeante dans le temps d'une manière imprévisible. D'autre part, la portée des transmissions radio étant limitée, le relayage est rendu obligatoire, et il faut donc que les nœuds formant ce réseau ad hoc coopèrent pour retransmettre les messages

d'une source vers une destination. Les chemins utilisés et les nœuds traversés sont déterminés par un protocole de routage dédié.

Pour que le réseau fonctionne, il faut que chaque nœud soit volontaire pour relayer le trafic des autres participants. Néanmoins, des stratégies peuvent être mises en œuvre et adoptées qui peuvent aller jusqu'à chercher à ne pas épuiser les batteries de certains plutôt que d'autres.

L'énergie n'est qu'un exemple des paramètres possibles; d'autres plus importants concernent l'existence et la fiabilité d'une route, ainsi que la charge du trafic des nœuds traversés.

3. Les applications cibles

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

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

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

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

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

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

- Réseaux en mouvement : informatique embarquée et véhicules communicants.

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

4. Avantages

Les avantages de cette technologie sont nombreux du fait qu'il n'y a pas besoin d'infrastructure préexistante :

- Les réseaux ad hoc peuvent être déployés dans un environnement quelconque ;
- Le coût d'exploitation du réseau est nul : aucune infrastructure n'est à mettre en place initialement et surtout aucun entretien n'est à prévoir ;
- Le déploiement d'un réseau ad hoc est : (i) simple et ne nécessite aucun pré-requis puisqu'il suffit de disposer d'un certain nombre de terminaux dans un espace pour créer un réseau ad hoc, et (ii) rapide puisqu'il est immédiatement fonctionnel dès lors que les terminaux sont présents ;
- La souplesse d'utilisation est importante puisque les seuls éléments pouvant tombés en panne sont les terminaux eux mêmes. Autrement dit, il n'y a pas de panne "pénalisante" de manière globale (une station qui sert au routage peut être remplacée par une autre si elle tombe en panne).

5. Inconvénients

Même si les perspectives pour les réseaux ad hoc sont prometteuses, plusieurs contraintes restent encore à traiter :

- La connectivité limite les possibilités de communication. Ainsi, deux stations ne sont joignables que s'il existe un ensemble de stations pouvant assumer la fonction de routeur afin de faire suivre les paquets de données échangées entre les deux stations. Dans l'architecture filaire, les possibilités de communication sont prévisibles avant sa mise en place et les bornes d'accès d'une architecture cellulaire telle que GSM ou UMTS permettent de manière similaire de connaître avec exactitude les zones de couverture. Ce n'est plus le cas avec les réseaux ad hoc où une communication n'est possible que si la collaboration entre stations est suffisante pour lier l'émetteur au récepteur ;
- Les liens entre les stations ne sont pas isolés les uns des autres et polluent le voisinage, par diffusion, lors de chaque émission/réception de données. Par conséquent, tout paquet de diffusion émis vers une station en cours de communication (que le paquet lui soit destiné ou pas) va altérer la communication de cette station. La diffusion est un facteur qui alourdit aussi d'autres paramètres tels que la bande passante et la consommation de batterie ;

- La sécurité dans les réseaux ad hoc est difficile à contrôler, notamment parce que sur l'interface air l'écoute clandestine est très simple à réaliser ;

- L'absence de centralisation rend les stations toutes semblables ; il devient alors difficile d'adopter des politiques de gestion globale du réseau. En effet, mettre en place un système de facturation est techniquement délicat, et offrir des qualités de service (QoS) différentes aux utilisateurs est aussi difficilement contrôlable dans ce contexte ;

- L'absence totale d'administration centralisée rend complexe et coûteuse l'utilisation des techniques de multiplexage des communications utilisées dans les réseaux avec point d'accès (FDMA, TDMA, etc.). En effet, pour utiliser ce type de mécanismes, il faut d'une part, concevoir un protocole distribué permettant aux nœuds de se partager les fréquences, les codes ou les unités de temps. D'autre part, la mobilité des nœuds d'un tel réseau provoque des changements fréquents de topologie. Le routage étant aussi distribué, les routeurs sont les mobiles et un transfert de données peut aisément être interrompu par le départ d'un nœud de la route utilisée.

- Enfin, la faible autonomie des batteries constitue un frein à une utilisation longue du terminal et à la mise en place de nouveaux services. C'est une contrainte qui existe certes dans les réseaux de type GSM ou UMTS, mais qui est plus forte dans les réseaux ad hoc, puisque les ressources énergétiques sont mises en commun même pour les besoins du routage. Nous nous intéressons dans ce mémoire, plus spécialement, à ce dernier point. Nous proposons, dans le Chapitre 4, des solutions permettant de mieux gérer cette consommation des batteries.

6. IEEE 802.11 en mode ad hoc

La norme *IEEE 802.11* (*ISO/IEC 8802-11*) est un standard international décrivant les caractéristiques d'un réseau local sans fil (*WLAN*). Le nom **WiFi** (contraction de *Wireless Fidelity*, parfois notée *Wi-Fi*) correspond initialement au nom donnée à la certification délivrée par la WECA (*Wireless Ethernet Compatibility Alliance*), l'organisme chargé de maintenir l'interopérabilité entre les matériels répondant à la norme 802.11. Par abus de langage (et pour des raisons de marketing) le nom de la norme se confond aujourd'hui avec le nom de la certification. Ainsi un réseau Wifi ou ASFI (*Accès Sans Fil à Internet*) est en réalité un réseau répondant à la norme 802.11.

La norme 802.11 permet de créer des réseaux locaux sans fil à haut débit pour peu que la station à connecter ne soit pas trop distante d'une autre station.

Dans sa première version définie en 1997, les transmissions infrarouges étaient envisagées, les versions les plus récentes du standard telles que IEEE 802.11b pour un débit partagé de 11Mbps, IEEE 802.11g avec un débit de 22Mbps ou encore IEEE 802.11a pour un débit de 56 Mbps sur la base desquelles sont construites l'essentiel des cartes d'interface commercialisées, s'adressent principalement à des transmissions radio fréquences.

Initialement le standard IEEE 802.11 permet l'utilisation de trois différentes technologies pour la couche physique :

- FHSS: Frequency Hoping Spread Spectrum.
- DSSS: Direct Sequence Spread Spectrum.
- IR : Infra Red.

Deux autres couches physiques ont été rajoutées par la suite par 802.11b (1999) pour permettre les hauts débits. La première est une couche DSSS modifiée afin d'améliorer le débit jusqu' à 5,5 et 11 Mbps, initialement à 1 et 2 Mbps. La deuxième est OFDM (Orthogonal Frequency Division Multiplex) pour les débits jusqu' à 54 Mbps. Les produits conformes au standard IEEE.802.11b se voient attribuées le logo Wi-Fi (Wireless Fidelity). Ces produits utilisent la couche physique DSSS dans la bande de fréquence 2.4 GHz.

La couche MAC (Médium Access Control) du standard IEEE 802.11 utilise la technique CSMA/CA [5] (Carrier Sensé Multiple Access/Collision Avoidance) comme technique d'accès au canal. En plus le standard définit un mécanisme supplémentaire RTS/CTS (Request To Send/Clear To Send) pour éviter les collisions et le problème des nœuds cachés. Un nœud A voulant émettre des données vers un nœud B envoie un message RTS indiquant la durée de transmission du paquet. Le nœud B répond alors par un message CTS à A, ce dernier est assuré que le canal est libre, et peut commencer son émission de données. Les voisins (de A et B) recevant ces types paquets (RTS/CTS) vont arrêter leurs tentatives d'accès au canal pendant la durée indiquée.

La portée radio varie selon la fréquence et la technique de modulation utilisée ainsi que l'environnement, intérieur ou extérieur et les obstacles présents. Elle atteint quelques centaines de mètres en air libre.

Nous ne détaillerons pas les différentes classes de modulations de la couche physique ni les différentes méthodes d'accès à la couche MAC, puisque notre analyse ultérieure porte uniquement sur la couche réseau.

Précisons qu'en mode ad hoc sans station de base, le IEEE 802.11 ne spécifie pas de routage, il permet uniquement la communication directe entre deux machines qui s'entendent.

Il est possible d'utiliser n'importe quel protocole de niveau 3 du modèle OSI sur un réseau sans fil 802.11 au même titre que sur un réseau Ethernet.

7. Routage dans les réseaux ad hoc

Le groupe MANET se concentre sur les protocoles de routage dans les réseaux mobiles ad hoc, et se propose de standardiser des protocoles de routage au niveau IP. Les protocoles de routage doivent être totalement distribués, c'est-à-dire qu'aucune entité centrale ne doit tout commander; en plus, les protocoles doivent réagir aux changements imprévisibles et rapides du réseau sans fil. Les nœuds composant le réseau ad hoc sont autonomes et libres de se mouvoir à leur gré ; En effet, l'avantage de développer des protocoles MANET par rapport aux autres types de routage est de s'abstraire de la couche physique utilisée par le nœud. De cette façon on peut former un seul réseau logique qui peut être composé de plusieurs sous réseaux utilisant différents types de couches physiques.

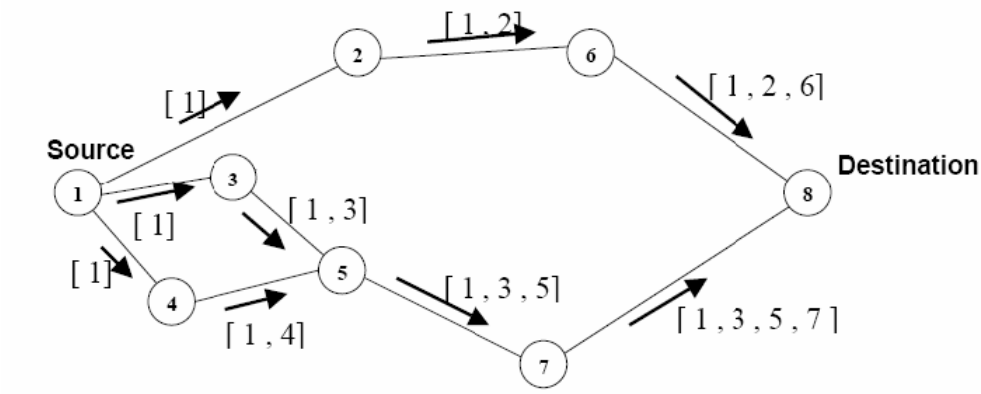
Globalement, on distingue deux familles de protocoles de routage ad hoc : les protocoles de routage dits "proactifs", qui anticipent la demande d'acheminement de paquets et les protocoles de routage "réactifs" qui réagissent à la demande. Entre ces deux familles, une autre approche commence à émerger, il s'agit des protocoles dits "hybrides" qui s'inspirent à la fois des protocoles proactifs et des protocoles réactifs. La liste des protocoles de routage qui suit est loin d'être exhaustive ; il en existe bien d'autre mais cette sélection couvre les protocoles les plus classiques et les plus étudiés. Nous donnons, ci-après, une vue globale de ces protocoles et de leurs caractéristiques essentielles.

7.1 Les protocoles réactifs

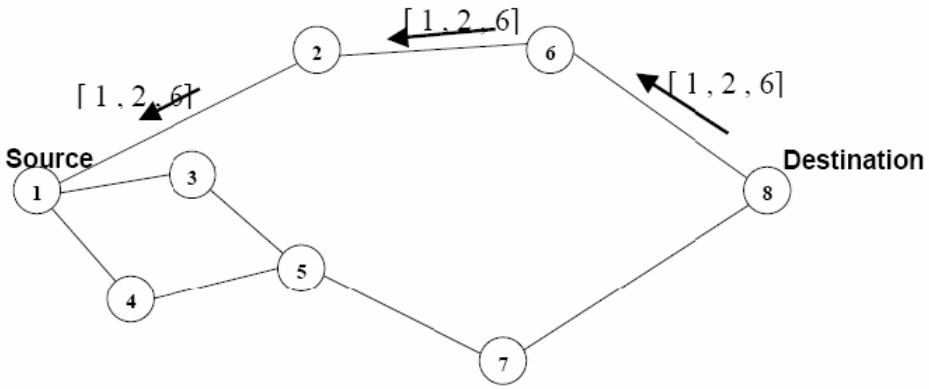
Les protocoles de routage appartenant à cette catégorie, créent et maintiennent les routes selon les besoins. Lorsque le réseau a besoin d'une route, une procédure de découverte globale de routes est lancée, et cela dans le but d'obtenir une information. Le routage à la demande induit une lenteur à cause de la recherche des chemins, ce qui peut dégrader les performances des applications interactives (exemple les applications des bases de données distribuées). En outre, il est impossible de connaître au préalable la qualité du chemin (en termes de bande passante, délais,… etc.). Une telle connaissance est importante dans les applications multimédias. Dans ce qui suit, nous allons décrire les protocoles les plus importants de cette classe : DSR et AODV.

7.1.1 Dynamic Source Routing (DSR)

Le protocole de routage à source dynamique [6], est basé sur l'utilisation de la technique "routage source". Dans cette technique : la source des données détermine la séquence complète des nœuds aux travers desquels, les paquets de données seront envoyés.



(a) Construction de l'enregistrement de route



(b) le renvoi du chemin

FIG. 1.2 – Principe du routage DSR [38]

Un site initiateur de l'opération de *découverte de routes*, diffuse un paquet requête de route *RREQ (Route Request).* Si l'opération de découverte est une réussite, l'initiateur reçoit un paquet réponse de route *RREP (Route Reply)* qui liste la séquence des nœuds permettant à la destination d'être atteinte. Le paquet requête de route *RREQ* contient donc un champ enregistrement de route, dans lequel sera accumulée la séquence des nœuds visités durant la propagation de la requête dans le réseau, comme le montre la figure 1.2.

Afin d'assurer la validité des chemins utilisés, DSR exécute une procédure de *maintenance de routes* quand un nœud détecte un problème fatal de transmission. A l'aide de sa couche de liaison, un message erreur de route *RERR* (*Route Error*) est envoyé à l'émetteur à l'origine du paquet. Le message d'erreur contient l'adresse du nœud qui a détecté l'erreur et celle du nœud qui le suit dans le chemin. Lors de la réception du paquet erreur de route *RERR* par l'hôte source, le nœud concerné par l'erreur est supprimé du chemin sauvegardé, et tous les chemins qui contiennent ce nœud sont tronqués à ce point là. Par la suite, une nouvelle opération de découverte de routes vers la destination, est initiée par l'émetteur.

7.1.2 Ad hoc On-Demand Distance Vector (AODV)

Le protocole AODV [7] [8] représente essentiellement une amélioration de l'algorithme DSDV discuté plus bas, dans le contexte proactif. Le protocole AODV, réduit le nombre de diffusions de messages, et cela en créant les routes lors du besoin, contrairement à DSDV, qui maintient la totalité des routes.

AODV utilise les principes des numéros de séquences afin de maintenir la consistance des informations de routage.
A cause de la mobilité des nœuds dans les réseaux ad hoc, les routes changent fréquemment ce qui fait que les routes maintenues par certains nœuds, deviennent invalides. Les numéros de séquence permettent d'utiliser les routes les plus récentes.

De la même manière que dans DSR, AODV utilise une requête de route *RREQ* dans le but de créer un chemin vers une certaine destination. Cependant, AODV maintient les chemins d'une façon distribuée en gardant une table de routage, au niveau de chaque nœud de transit appartenant au chemin cherché.
Un nœud envoie une requête de route *RREQ* dans le cas où il aurait besoin de connaître une route vers une certaine destination et qu'une telle route ne soit pas disponible. Cela peut arriver si la destination n'est pas connue au préalable, si le chemin existant vers la destination a dépassé sa durée de vie, ou s'il est devenu défaillant. Le champ numéro de séquence destination du paquet *RREQ*, contient la dernière valeur connue du numéro de séquence, associée au nœud destination. Cette valeur est recopiée de la table de routage. Si le numéro de séquence n'est pas connu, la valeur nulle sera prise par défaut. Le numéro de séquence source du paquet *RREQ* contient la valeur du numéro de séquence du nœud source.

Afin de maintenir des routes consistantes, une transmission périodique du message "HELLO" est effectuée. Si trois messages "HELLO" ne sont pas reçus consécutivement à partir d'un nœud voisin, le lien en question est considéré défaillant.

Le protocole AODV ne présente pas de boucle de routage, en outre il évite le problème « comptage à l'infini » (*counting to infinity*) de Bellman-Ford ce qui offre une convergence rapide quand la topologie du réseau ad hoc change.

7.2 Les protocoles proactifs

Les protocoles de routage proactifs pour les réseaux mobiles ad hoc, sont basés sur le même principe des protocoles de routage utilisés dans les réseaux filaires. Les deux principales méthodes utilisées sont la méthode "état de lien" (*Link State*) et la méthode "vecteur de distance" (*Distance Vector*). Ces deux méthodes exigent une mise à jour périodique des données de routage qui doit être diffusée par les différents nœuds de routage du réseau. Donc, les nœuds proactifs tentent de maintenir et conserver une vue exacte à chaque instant, de chacun des autres nœuds du réseau. L'intérêt majeur pour les couches supérieures du modèle OSI, est qu'elles n'ont plus à attendre que les routes se construisent, car elles sont déjà présentes dans les tables de routages. Nous allons décrire dans ce qui suit, les protocoles les plus importants de cette classe LSR, OLSR et DSDV.

7.2.1 Le protocole LSR

Dans le protocole LSR (Link State Routing) [9], chaque station diffuse périodiquement à ses voisines l'état de ses liens. Ceux-ci diffusent à leur tour, et de proche en proche, de manière récursive les informations qui leurs parviennent, jusqu'à les faire converger pour qu'elles soient connues de toutes les stations. De cette manière, chaque station va pouvoir constituer ainsi sa propre table de routage, qui va être utilisée lorsque la station souhaitera joindre un destinataire : une simple recherche dans la table suffira pour localiser le récepteur. Ce protocole illustre parfaitement le concept de routage proactif, et cumule les défauts inhérents à cette technologie (une diffusion parfois excessive des données de routage, et un gaspillage de la bande passante). En faible mobilité, ce protocole fournit de bons résultats, mais qui s'affaiblissent progressivement quand la mobilité des stations augmente.

7.2.2 Optimized Link State Routing (OLSR)

Comme son nom l'indique, OLSR [10] [11], est un protocole à état de lien (LSR) optimisé. OLSR offre des routes optimales en termes de nombre de sauts dans le réseau. Dans un protocole à état de lien chaque nœud déclare ses liens directs avec ses voisins à tout le réseau. Dans le cas d'OLSR, les nœuds ne déclarent qu'une sous partie de leur voisinage. L'ensemble des voisins déclarés est choisi de façon à pouvoir atteindre tout le voisinage à deux sauts. Cet ensemble s'appelle l'ensemble des relais multipoint.

Les relais multipoint sont utilises dans le but de minimiser le trafic du à la diffusion des messages de contrôle dans le réseau. De plus, les routes sont construites à base des relais multipoint.

Pour maintenir à jour toutes les informations nécessaires au choix des relais multipoint et le calcul de la table de routage, les nœuds OLSR ont besoin de s'échanger des informations périodiquement. Pour s'informer du proche voisinage, les nœuds OLSR envoient, des messages de HELLO contenant leur liste de voisins. Ces messages permettent a chacun de choisir son ensemble de relais multipoint constitue d'un sous-ensemble de voisins. Le deuxième type de message primordial à OLSR s'appelle, le message TC. Par ce message les sous-ensembles de voisinage sont déclarés périodiquement dans le réseau, en utilisant ces mêmes relais multipoint. Ces informations offrent, une carte de réseau contenant tous les nœuds et un ensemble partiel des liens, mais suffisant pour la construction de la table de routage.

La table de routage est construite au niveau de tous les nœuds et le routage des données s'effectue saut par saut sans l'intervention d'OLSR dont son rôle s'arrête à la mise à jour de la table de routage de la pile IP. OLSR sera décrit, plus en détail ultérieurement dans un chapitre propre.

7.2.3 Le protocole DSDV

Le protocole DSDV (Dynamic destination-Sequenced Distance Vector) [12] se base sur l'algorithme distribué de Bellman-Ford (DBF), qui utilise les vecteurs de distance. Chaque station maintient une table de routage contenant toutes les destinations qu'elle peut atteindre et le coût (en nombre de saut) pour atteindre la destination, ainsi qu'un numéro de séquence lié à chaque destination dont le but est d'éviter la formation de boucle de routage. Cette table est constituée par l'intégration des données de mise à jour émises par chaque station. Ces mises à jour s'effectuent en fonction du temps ou bien en fonction d'événements liés à une modification de la topologie du réseau (lien rompu, nouvelle station, etc.). Elles se font soit de manière incrémentale (les seules données qui ont changé par rapport à la dernière mise à jour), soit intégralement (la table toute entière), ceci selon l'importance des modifications constatées.

Un paquet de mise à jour contient le nouveau numéro de séquence incrémenté, du nœud émetteur. Et pour chaque nouvelle route il contient : l'adresse de la destination, le nombre de nœuds (ou de sauts) séparant le nœud de la destination et le numéro de séquence (des données reçues de la destination) tel qu'il a été estampillé par la destination.

Cependant dans ce protocole, une unité mobile doit attendre jusqu'à ce qu'elle reçoive la prochaine mise à jour initiée par la destination, afin de mettre à jour l'entrée associée à cette destination, dans la table de distance. Ce qui fait que le temps d’exécution de

DSDV est élevé. DSDV utilise une mise à jour périodique basée sur les événements, ce qui cause un contrôle excessif dans la communication.

7.3 Les protocoles hybrides

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

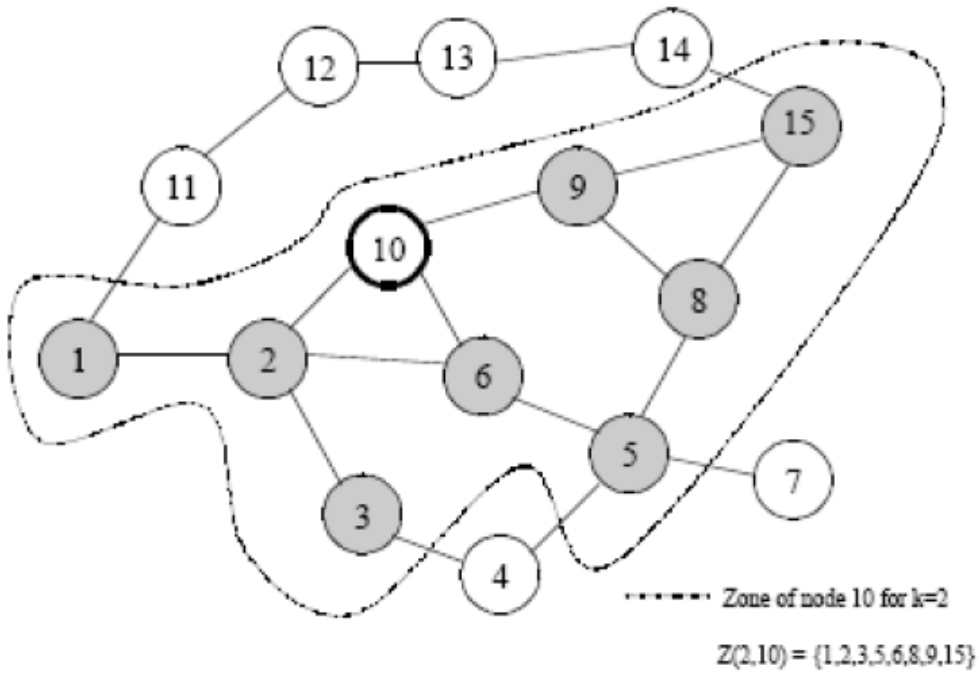


FIG. 1.3 – Exemple de zone IARP dans ZRP [37]

7.3.1 Zone Routing Protocol (ZRP)

Le protocole ZRP [13] est un exemple de protocole hybride, à mi-chemin entre les deux familles de protocoles (proactif et réactif). Ce protocole 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*). ZRP définit deux zones de routage :

- **IARP** (**IntrAzone Routing Protocol)** : Dans cette zone, chaque nœud définit une distance d en nombre de sauts pour laquelle il choisit de maintenir l'ensemble des tables de routage en s'aidant d'un protocole de routage proactif. Chacun des nœuds du réseau peut choisir une distance *d* différente afin d'estimer et de choisir son entourage proche, en fonction de la densité de son voisinage ou d'une métrique adaptée (vitesse de transmission, qualité du lien, etc.) (cf. figure 1.3).

- **IERP (IntErzone Routing Protocol)** : Lorsqu'un nœud doit communiquer, ou relayer, un message à un autre nœud qui n'est pas dans sa zone de routage (i.e. absent de sa table de routage) il envoie à chacun de ses voisins de bordure (i.e. distance = *d*) une requête de recherche de route vers cette destination. Si l'un de ces nœuds de bordure possède le nœud recherché dans sa table de routage (i.e. obtenu avec le protocole IARP), il répond au nœud émetteur qu'il peut servir de passerelle vers le nœud destinataire. Les autres nœuds de bordure qui ne connaissent pas ce nœud destinataire, émettent à leur tour une requête de découverte de route vers leurs propres nœuds de bordure et ainsi de suite.

La complexité de cet algorithme ne lui a pas permis pour le moment de bénéficier d'un déploiement important. Cette tentative pour cumuler les qualités des deux approches se place en intermédiaire plus qu’une solution, parce qu’elle est moins efficace que les algorithmes de routage de base, en forte mobilité ou avec beaucoup de stations.

7.4 Difficile comparaison entre les protocoles réactifs et proactifs

La comparaison des capacités théoriques entre les protocoles de routage proactifs et réactifs est difficile. On peut récapituler ici quelques points forts de chacune des familles avec leur utilisation dans des réseaux particuliers. De plus les nouvelles normes d'accès au médium radio, pourront peut-être radicalement changer les évolutions futures de ces deux familles.

Economie d'énergie et de bande passante : Dans les cas des réseaux à faible mobilité, on semble devoir privilégier les protocoles de routages réactifs dans le but de limiter l'utilisation de la bande passante et donc d'économiser l'énergie. En effet, émettre des

messages Hello pour une grande période de temps, semble être une perte d'énergie alors que les routes sont prévues pour évoluer très lentement ou par palier.

Rapidité d'établissement des routes - statiques & mobiles : Les protocoles proactifs maintiennent les routes pour toutes les destinations du réseau. Au moment où le nœud a besoin d'une route, elle est déjà présente dans sa table de routage. De plus ce mécanisme est effectué régulièrement à expiration de temporisateurs. Cela implique que la charge du trafic de contrôle est indépendante de la mobilité et du trafic de données au sein du réseau [14]. Les protocoles réactifs détectent et réparent plus rapidement les changements de topologie lorsqu'ils interviennent dans des réseaux ad hoc fortement mobiles. Les protocoles proactifs, comptant sur les mécanismes de mises à jour par temporisateurs, peuvent être plus lents à établir de nouvelles routes [15].

Simplicité des implémentations : Les protocoles réactifs doivent s'interfacer de manière forte avec la pile TCP/IP du système d'exploitation sous-jacent. En effet, ils doivent intercepter chacun des paquets de données que les couches supérieures du modèle OSI émettent. Dans le cas d'AODV, il s'agit seulement du premier paquet qui est mis en attente jusqu'à la construction d'une entrée dans la table de routage, pour ensuite relâcher le paquet au système d'exploitation, qui va se charger de router proprement dit les données. Dans le cas de DSR, chaque paquet qui transite doit être modifié pour ajouter ou retirer la succession de nœuds à emprunter. Comme pour AODV, le premier paquet est mis en attente le temps pour le démon DSR de découvrir la route. La famille des protocoles proactifs construit simplement des routes régulièrement et n'a pas à intercepter les paquets qui transitent. Ce deuxième modèle semble donc plus simple à implémenter et paraît donc moins susceptible de rencontrer des bogues.

Performances générales : DSR semble être le protocole réactif le plus expérimenté par simulation [16] et le plus prometteur dès que les mécanismes d'ACK au niveau 2 seront court-circuités. D'une manière générale, les protocoles réactifs (AODV, DSR) sont basés sur l'inondation. Ils n'offrent pas la garantie d'une route optimale. En revanche les protocoles proactifs sont basés sur la connaissance ou l'exploration topologique du réseau. Grâce aux messages HELLO, la route optimale est garantie.

8. Conclusion

Les principaux défis à relever dans les réseaux ad hoc sont fondamentalement liés au problème de routage. Nous avons vu, dans la section 7 de ce chapitre, que plusieurs protocoles de routage ont été conçus. Cependant, très vraisemblablement, le protocole de routage optimal dans toutes les situations n'existe pas. En effet, les études de performance de ces algorithmes montrent que leurs performances sont souvent moyennes. Les meilleurs résultats n'étant atteignables que dans certaines situations bien précises. Afin de choisir le meilleur protocole de routage le plus approprié, il convient

de définir les conditions d'utilisation (mobilité, nombre de stations, QoS, etc.) souhaitées, et de choisir ensuite l'algorithme qui satisfera au mieux ces conditions. La priorité principale étant de garder les terminaux mobiles en marche.

Il ne faut cependant pas perdre de vue que même si l'aspect du routage reste fondamental, d'autre problématiques, doivent être résolues avant qu'on puisse espérer voir les réseaux ad hoc remplir le rôle pour lesquels ils ont été conçus : on pense à l'auto configuration des nœuds déployés, au routage multicast ainsi qu'a la sécurité de fonctionnement, mais aussi à un système de métrique qui puissent intégrer des informations de niveau inférieur comme la puissance ou la consommation d'énergie, le débit et le taux d'erreur des liaisons radio sous-jacentes.

CHAPITRE 2

Le protocole OLSR et les relais multipoint

1. Introduction

OLSR (Optimized Link State Routing) est une pure optimisation des protocoles filaire de type OSPF en vue de leur utilisation dans des réseaux sans fil mobiles et multi-sauts. Le protocole OLSR est proposé au groupe de standardisation MANET de l'IETF. Le protocole OLSR appartient à la famille des protocoles à état de liens. Le concept principal d'optimisation dans OLSR est le relais multipoint, MultiPoint Relay, ou MPR. L'idée des MPR est de minimiser l'inondation de paquets de contrôle en réduisant le nombre de retransmissions dans une même région du réseau. Chaque nœud du réseau sélectionne un sous-ensemble de ses voisins qui va avoir la tâche de retransmettre ses propres paquets de contrôle. C'est ce sous-ensemble qu'on appelle MPR du nœud.

OLSR appartient à la famille des protocoles proactifs. Afin de maintenir la connaissance de topologie, les nœuds OLSR s'échangent des paquets de contrôles périodiquement. La détection du voisinage se fait à l'aide de paquets de HELLO. La dissémination des informations de topologie quant à elle se fait par la diffusion des paquets TC (*Topology Control*) en utilisant la diffusion optimisée avec les relais multipoint. Les messages TC contiennent une liste de liens du voisinage du nœud qui génère le paquet. Ceci permet aux autres nœuds d'avoir une connaissance partielle de la topologie, mais qui est suffisante pour construire et router les paquets de n'importe quelle source vers n'importe quelle destination présente dans le réseau, et ce, sur un plus court chemin.

2. Optimized Link State Routing (OLSR)

Le protocole OLSR est composé essentiellement de deux entités complémentaires :

- **La découverte du voisinage** : chaque nœud procède à la découverte de ses voisins directs et ses voisins à deux sauts. Chaque nœud doit aussi désigner ses relais multipoint.

- **La gestion de topologie** : cette deuxième entité, s'occupe de l'apprentissage de la topologie globale du réseau. Cet apprentissage se fait par l'analyse des paquets de contrôle contenant des informations sur la topologie locale à deux sauts. Il s'agit d'une connaissance totale de tous les nœuds présents dans le réseau et une connaissance partielle des liens entre ces derniers.

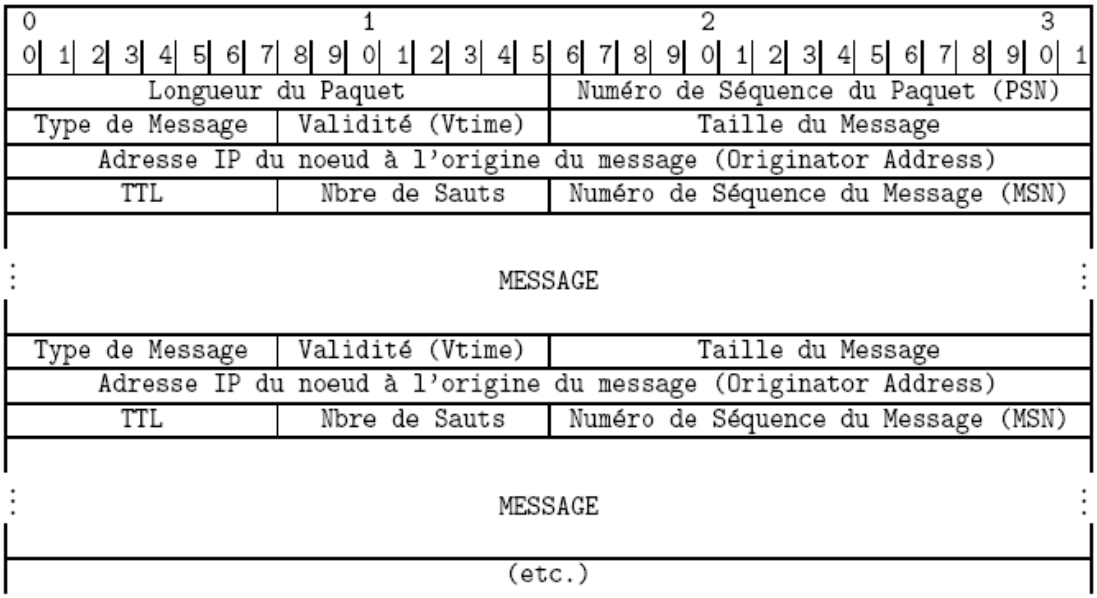


FIG. 2.1 – Format du paquet OLSR [10]

Ces informations collectées sont largement suffisantes pour calculer et router les paquets de données vers toutes les destinations présentes dans le réseau à un instant donné. Les nœuds du réseau s'échangent des messages de contrôle encapsulés dans un paquet OLSR (cf. figure 2.1) en utilisant le protocole de transport UDP sur le port 698. Ce format de paquet est commun à chaque message et constitue une enveloppe pour leur acheminement. Un même paquet peut transporter plusieurs messages, de même type ou de type différent. OLSR utilise quatre types de messages : HELLO, TC, MID et HNA. Les messages HELLO sont utilisés pour la détection de voisinage. Les messages *TC* servent à diffuser les informations de topologie dans tout le réseau. Les messages MID permettent de publier la liste des interfaces de chaque nœud. Quant aux messages HNA, ils sont utilisés pour déclarer les sous-réseaux et hôtes (hors MANET) joignables par un nœud jouant le rôle de passerelle.

2.1 Découverte de voisinage

OLSR est un pur protocole de niveau 3. Comme tous les protocoles de routage ad hoc sans fil classiques, il a été conçu pour fonctionner indépendamment de la couche liaison sous-jacente. Même s'il peut, dans ses mécanismes d'optimisation optionnels, obtenir des informations directement de l'interface radio, il spécifie un mécanisme de détection de voisinage et de qualité des liens au niveau 3. Pour détecter les changements de topologie locale, un nœud OLSR émet périodiquement (*Hello_Interval*) des messages *Hello*. Ces messages sont encapsulés dans un paquet OLSR et utilise le même en-tête que tout message de contrôle OLSR (cf. figure 2.1). Ce message contient l'adresse du nœud émetteur ainsi que celles de ses voisins et les types de liens et de voisinage qui les associent (symétrique, asymétrique, perdu, inconnu, voisin symétrique, MPR, etc.) (cf. figure 2.2).

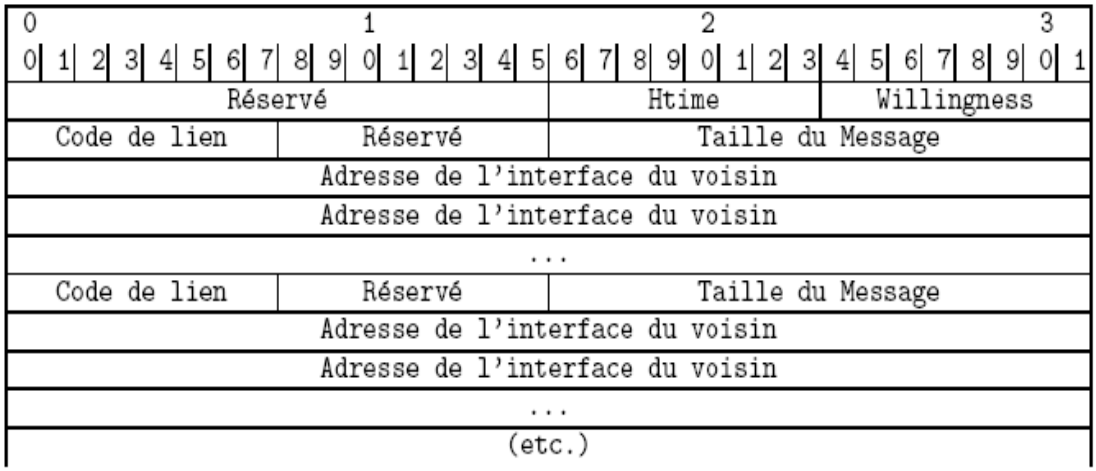


FIG. 2.2 – Format du message Hello OLSR [10]

Pour découvrir de possibles MPR qui vont optimiser l'inondation, chaque nœud doit découvrir les voisins avec lesquels il est en contact direct symétrique. Les incertitudes introduites par la propagation radio font qu'un lien peut être unidirectionnel (i.e. asymétrique). Chaque lien doit donc être vérifié dans les deux sens. Ainsi la figure 2.3 montre un échange de messages Hello entre deux nœuds afin d'établir cette symétrie :

1. A envoie un message Hello vide avec sa seule adresse. B reçoit ce message Hello et enregistre A comme voisin asymétrique, car il ne trouve pas sa propre adresse dans ce message,
2. B, après l'expiration du temporisateur *Hello_Interval* émet à son tour un message Hello qui déclare le nœud A comme lien asymétrique. Quand A reçoit le message il y découvre sa propre adresse : il enregistre B comme voisin symétrique.

3. A envoie un nouveau message Hello qui intègre B en sa qualité de voisin symétrique.
4. B à la réception de ce message modifie l'enregistrement pour A dans sa table de liens en le déclarant symétrique et réémet un message Hello qui annonce ce nouvel état de lien.

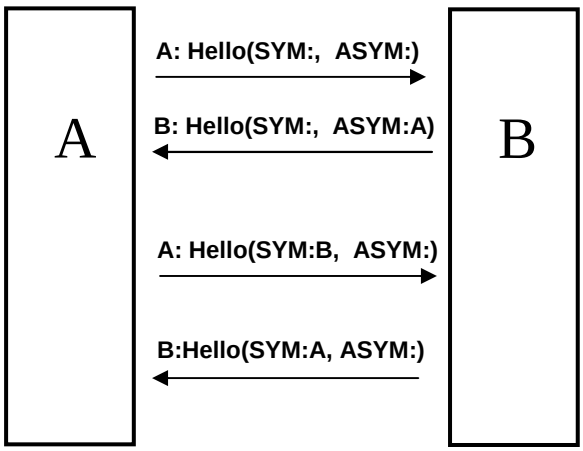


FIG. 2.3 Détection de voisinage avec l'échange des messages Hello

L_LOCAL_IFACE_ADDR	adresse de l'interface du nœud
L_NEIGHBOR_IFACE_ADDR	adresse de l'interface du voisin
L_SYM_TIME	date au-delà de laquelle le lien ne sera plus considéré symétrique
L_ASYM_TIME	date au-delà de laquelle le lien ne sera plus considéré asymétrique
L_TIME	date à laquelle le lien expire et l'enregistrement est supprimé de la table

FIG. 2.4 – Table des Liens (Link Set)

Ces états de liens sont stockés dans une table qui décrit les paires interfaces locales/interfaces distantes (i.e. les interfaces des voisins, cf. figure 2.4). En effet OLSR peut fonctionner sur des nœuds qui possèdent plusieurs interfaces radio et ainsi connecter plusieurs domaines de réseau ou plusieurs types de technologie (i.e. WiFi<=>Bluetooth<=>WiMax<=>Ethernet<=>...), ou offrir de la redondance dans les tables de routage.

N_NEIGHBOR_MAIN_ADDR	adresse principale du voisin
N_STATUS	spécifie si le voisin est symétrique ou asymétrique

FIG. 2.5 – Table de Voisinage (Neighbor Set)

N_NEIGHBOR_MAIN_ADDR. . . . . .adresse principale d'un voisin symétrique N_2HOP_ADDR. . . . . .adresse d'un voisin symétrique du nœud ci dessus N_TIME . . . . . date à laquelle le lien expire et l'enregistrement est supprimé de la table

FIG. 2.6 – Table de voisinage à deux sauts (2-Hop Neighbor Set)

M_MAIN_ADDR. . . . . adresse principale du MPR

FIG. 2.7 – Table des MPR (MPR Set)

MS_MAIN_ADDR. . . . . adresse principale du sélecteur MPR MS_TIME. . . . . date à laquelle l'entrée doit être supprimée

FIG. 2.8 – Table des sélecteurs de MPR (MPR Selector Set)

Ces messages de contrôle Hello sont envoyés en diffusion (broadcast) sont reçus puis traités par chacun des voisins à un saut. Ils ne sont pas relayés au-delà. Ils permettent ainsi à chaque nœud de connaître ses voisins à deux sauts, c'est-à-dire les nœuds joignables exclusivement au moyen d'un voisin symétrique : tous les voisins symétriques de l'émetteur du message Hello qui ne sont pas eux-mêmes déjà enregistrés dans la table des voisins à un saut de celui qui reçoit le message Hello, sont des voisins à deux sauts, strictement. Ainsi le nœud peut mettre à jour sa table de voisinage à un saut (cf. figure 2.5), pour ensuite rediffuser un message Hello avec ses propres informations mises à jour. Puis il enregistre les couples d'adresses "voisin symétrique - voisin symétrique du voisin" dans sa table de voisinage à deux sauts (cf. figure 2.6).

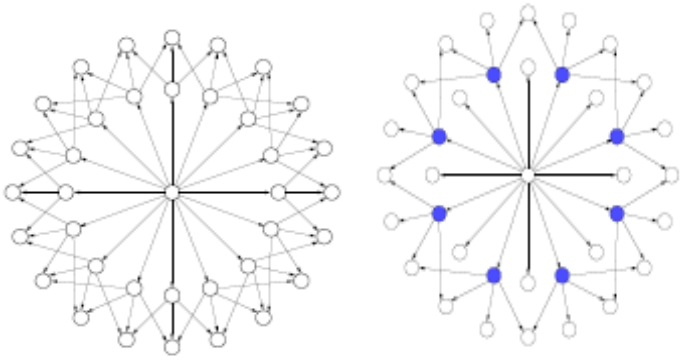
Une fois en possession de ces deux tables (i.e. table de voisinage à un saut et table de voisinage à deux sauts), chaque nœud peut calculer et optimiser le nombre de ses MPR qu'il va utiliser pour diffuser ses éventuels autres types de messages de contrôle (messages TC, MID, etc.) à destination de chacun des nœuds du réseau.

Une fois enregistrés dans une troisième table, la table des MPR (cf. figure 2.7), les prochains messages Hello indiquent cet état de fait. Le nœud qui découvre dans le message Hello que l'émetteur l'a déclaré et sélectionné comme MPR, enregistre alors l'émetteur dans une quatrième table : la table de ses MPR Selectors (cf. figure 2.8).

Ces informations sont considérées valides pendant une certaine période (*NEIGHB_HOLD_TIME*) au bout desquelles, si elles n'ont pas été rafraîchies afin de rester valides, sont effacées des quatre tables.

2.2 La technique des relais multipoint

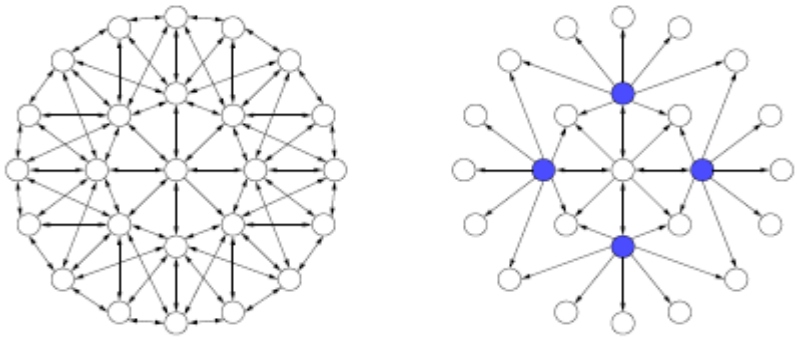
Les MPR d'un nœud constituent le plus petit sous-ensemble de voisins symétriques qui permet de couvrir une surface radio comme celle illustrée dans la figure 2.9 (a), au sens de la couverture à un saut à partir de ses voisins. Dans la figure 2.9 (b) les huit nœuds colorés suffisent pour couvrir cette même zone que celle couverte par ses seize voisins réunis à partir du nœud central dans figure 2.9 (a). C'est ce sous-ensemble qu'on appelle relais multipoint d'un nœud. Un message relayé par les MPR est ainsi reçu par tous les voisins à deux sauts. Autrement dit, l'ensemble des MPR d'un nœud est constitué du nombre minimal de voisins à un saut qui permet de joindre tous les voisins à deux sauts.



(a) Inondation d'un paquet dans un réseau.

(b) Couverture des voisins à deux sauts par les MPR.

FIG. 2.9 Couverture des voisins à deux sauts



(a) Inondation d'un paquet dans un réseau sans fil multi-sauts. Chaque flèche indique toutes les transmissions/ retransmissions

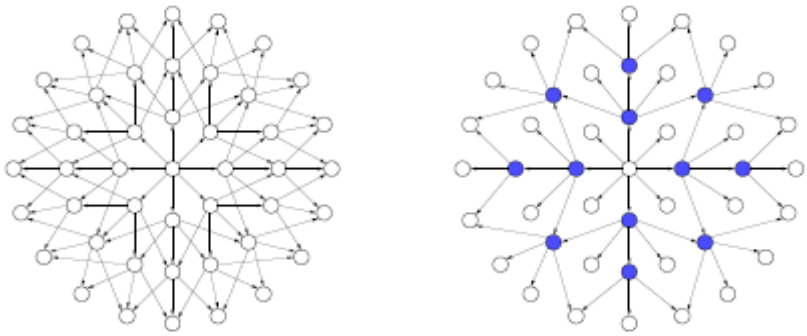
(b) Inondation d'un paquet Avec les MPR. Les flèches indiquent toutes les transmissions/ retransmissions

FIG. 2.10 – Inondation d'un paquet dans un réseau de 25 nœuds sans MPR(a) et avec MPR(b)

Historiquement le routeur d'un réseau filaire adopte un principe radical : un paquet en diffusion n'est jamais retransmis sur l'interface par laquelle il est reçu [17]. Dans un environnement sans fil, en général, la même antenne est utilisée pour la réception et l'émission : il n'y a alors pas d'autre possibilité que de recevoir et de réémettre en utilisant la même antenne et donc de réémettre sur la même interface les paquets à rediffuser. Ainsi chaque émetteur va recevoir autant de copies qu'il existe de voisins symétriques qui vont relayer et réémettre à leur tour son paquet. La figure 2.10(a) page précédente montre une inondation simple, dans un réseau sans fil. On observe que l'émission d'un seul paquet entraîne une multitude de réceptions par l'émetteur du paquet dupliqué par ses voisins : une émission par le nœud central pour huit émissions, de son propre paquet dupliqué par ses voisins directs.

L'un des rôles des MPR est aussi de limiter ce nombre de recopies et de traitements par l'émetteur, consommateurs d'énergie, même s'il ignore ses propres paquets, et de bande passante. Dans la figure 2.10(b) le nœud central ne reçoit plus que 4 copies de son propre message.

Le nombre de retransmissions nécessaires pour une inondation simple d'un réseau est n-1, ou n est le nombre de nœuds du réseau. En limitant le nombre de nœuds voisins qui vont prendre en charge la diffusion des paquets de contrôle, le nombre de retransmissions va diminuer : les MPR optimisent l'arbre de diffusion. Ainsi dans le cas de la figure 2.11(a), 24 réémissions sont nécessaires pour diffuser un message aux nœuds extérieurs (à trois sauts du nœud central). Dans le cas la figure 2.11(b) la réémission par les 12 nœuds élus MPR du réseau est suffisante pour obtenir le même résultat.



(a) Diffusion à 3 sauts par inondation simple

(b) Diffusion à 3 sauts par inondation avec MPR

FIG. 2.11 – Diffusion par inondation sans MPR(a) et avec MPR(b)

Pour diffuser un message dans tout le réseau, chaque nœud désigne ses voisins relais multipoint qui joueront le rôle de premiers répéteurs du nœud central. Récursivement et en répétant ce processus, le message diffusé atteint la totalité des nœuds. [18] démontre que la connaissance de deux niveaux de voisinage permet la diffusion des messages dans tout le réseau.

La particularité de cette technique est qu'elle fonctionne d'une manière totalement indépendante et distribuée ; chaque nœud calcule ses relais multipoint en se basant sur la connaissance de son voisinage à deux sauts. Le nœud doit informer ses voisins de leur nouveau rôle. Dans un environnement mobile avec une topologie changeante d'une manière imprévisible, l'ensemble des relais multipoint doit être recalculé à chaque fois qu'on détecte une modification dans le voisinage à deux sauts. C'est pour cette raison que le statut de relais multipoint est conditionné par le voisinage pour une durée limitée.

Heuristique de choix des relais multipoint

La connaissance des voisins du second niveau d'un nœud permet de procéder à l'élection de ses nœuds multipoint relais. Notons que, cette opération d'élection est faite au niveau de tous les nœuds du réseau. Son but est de trouver un ensemble de nœuds voisins qui couvrent tous les nœuds du second niveau.

Exemple de déroulement de l'algorithme de sélection

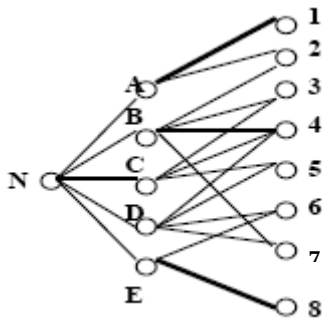


FIG. 2.12 – Sélection des voisins possédant un seul lien avec un nœud du second niveau

Prenons un exemple pour mieux illustrer le principe de cet algorithme (le même que précédemment). On se propose de chercher l'ensemble de relais multipoint du nœud N (cf. figure 2.12).

La première étape consiste à trouver les nœuds du premier niveau possédant des liens uniques avec un nœud du second niveau. Ces nœuds feront partie nécessairement de l'ensemble de relais multipoint *M* afin que les voisins à deux sauts soient totalement couverts. Selon l'exemple que l'on a pris, A et E sont dans ce cas (couvrant 1 et 8). On les insère dans *M*, et on élimine tous les nœuds du second niveau couverts par A et E (cf. figure 2.12) : les nœuds 1, 2 ainsi que 6 et 8.

La deuxième étape est une boucle : à chaque itération, on cherche le nœud du premier niveau qui couvre le maximum de nœuds du second niveau. On l'ajoute dans l'ensemble *M* et élimine ses nœuds du second niveau. La boucle prend fin naturellement lorsqu'il n'y a plus de nœuds du second niveau (N2={}). La figure 2.13 illustre les différentes étapes du déroulement de cet algorithme.

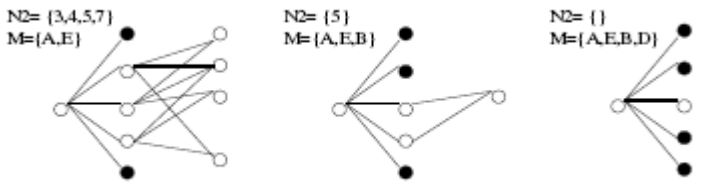


FIG. 2.13 – Illustration de l'algorithme de choix des relais multipoint

Plus formellement l'algorithme de sélection des relais multipoint se présente comme suit :

On désigne par *N(x)* l'ensemble des voisins directs de *x*, par *N2(x)* l'ensemble des voisins du second niveau, et *MPR(x)* étant l'ensemble des relais multipoint de *x*.

1. Commencer par un ensemble de relais multipoint vide *MPR(x)* = {}.

2. Choisir les nœuds de l'ensemble des voisins *N(x)* qui sont les seuls ayant un lien avec un voisin du second niveau. Ajouter ces nœuds sélectionnés de *N(x)* à l'ensemble *MPR(x)*, et éliminer tous les nœuds du second niveau couverts par ces derniers de l'ensemble *N2(x)*.
3. Tant que *N2*(x) ≠{} refaire
   (a) Calculer le degré de chaque nœud dans *N(x)*. Le degré pour un nœud est le nombre des voisins du second niveau couverts par celui-ci présent dans *N2(x)*.
   (b) Ajouter le nœud de *N(x)*, ayant le degré maximal à l'ensemble des relais multipoint *MPR(x)*, et enlever tous les nœuds du second niveau couverts par celui ci de *N2(x)*.

2.3 Construction de la topologie

Dans cette section, nous décrivons le contenu des informations de contrôle et comment elles sont utilisées pour construire les routes.

La détection de voisinage permet à chaque nœud de communiquer avec ses voisins directs et de choisir ses relais multipoint qui lui permettent de disséminer ses informations de contrôle dans le réseau. Si un nœud possède plusieurs interfaces, alors, il doit envoyer ces informations de contrôle sur toutes ses interfaces. Les routes sont construites eu utilisant les relais multipoint et les liens directs avec les voisins.

2.3.1 Table des liens topologiques

Les mécanismes de détection des liens et de voisinage, ont permis de créer les tables nécessaires à l'échange par diffusion des messages d'informations de topologie TC (*Topology Control*, cf. figure 2.14). Ces messages vont permettre de créer des tables de liens topologiques (cf. figure 2.15), dernière étape avant la création de la table de routage.

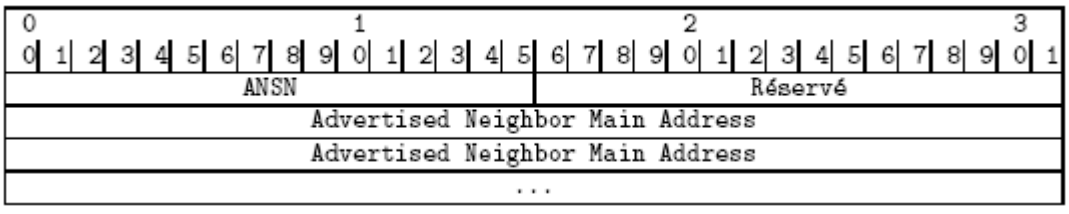


FIG. 2.14 – Format du message TC [10]

Le nœud qui a été élu MPR annonce chacune des entrées de sa table des MPR Selector (cf. figure 2.8) dans autant de champs *ADVERTISED_NEIGHBOR_MAIN_ADDRESS*

que nécessaires du message TC. A chaque modification de cette table, le nœud construit un nouveau message TC en incrémentant le numéro de séquence associé à sa topologie courante (i.e. le champ *ANSN*). Ainsi chaque nœud du réseau pourra choisir en fonction du numéro de séquence déjà en sa possession de supprimer les entrées concernant l'émetteur du message TC de sa table de topologie et de les recréer avec les nouvelles valeurs transportées dans le message.

Un nœud qui n'est pas MPR n'émet pas de message TC. Mais s'il advient que sa table des MPR Selector, à cause d'une rupture de lien, se vide avant l'expiration du délai de 15 secondes (*TOP_HOLD_TIME*), le nœud émet un message TC vide pour prévenir le réseau afin que toutes les entrées de couple *T_LAST_ADDR*, *T SEQ* soit supprimées dans sa table de topologie.

T_DEST_ADDR	adresse principale annoncée du voisin
T_LAST_ADDR	adresse de l'initiateur (Originator Address)
T_SEQ	Numéro de séquence associé à l'originator ANSN
T_TIME	date à laquelle l'entrée expire et doit être supprimée de la table

FIG. 2.15 – Table des liens topologiques (TC Set)

Ainsi chaque nœud connaît maintenant toute destination du réseau. Sa table de topologie contient tous les MPR Selector annoncés par tous les MPR du réseau :

T_DEST_ADDR est un nœud du réseau

T_LAST_ADDR est le dernier saut pour joindre ce nœud (le MPR)

Le nœud peut maintenant lancer un calcul de plus court chemin vers chacune de ces entrées, en s'appuyant sur toutes les autres tables à sa disposition.

2.3.2 Table des Associations d'Interfaces

Un nœud qui utiliserait plusieurs interfaces pour se connecter d'une part à un réseau IP Wifi et de l'autre à un réseau IP Bluetooth, ou WiMax, par exemple, pourrait choisir de router les données entre ces deux réseaux de technologie radio différentes. Or le concept de voisin, et donc de MPR, dans OLSR appelle un seul identifiant. Chaque nœud du réseau doit pouvoir établir une correspondance entre ce concept de voisinage, à un seul identifiant, et chacune des interfaces physiques qui peuvent être présentes sur le nœud mobile. Ces interfaces doivent pouvoir être adressées par chacun des nœuds du réseau. C'est le rôle des messages MID (cf. figure 2.16) et de la table d'association des interfaces (*MID Set*) ou Interface Association Set (cf. figure 2.17).

Un nœud qui ne posséderait qu'une seule interface n'aurait pas à fournir cette correspondance : l'adresse de son interface est utilisée comme identifiant de voisinage. Ce nœud ne génère donc pas de message MID. Un nœud possédant plusieurs interfaces doit faire un choix et sélectionner une de ses interfaces comme identifiant permanent dans le réseau OLSR. Cet identifiant est appelé adresse principale, et c'est cette adresse que porteront chacun des messages issus de ce nœud dans le champ *ORIGINATOR_ADDRESS* de chacun des messages de contrôle émis par le nœud. Pour faire connaitre ses autres interfaces, le nœud génère donc un message MID (*Multiple Interface Definition*) dans lequel il inscrit ses interfaces secondaires dans les champs *OLSR_ INTERFACE_ADDRESS* et comme pour les futurs messages de contrôle, le champ *ORINATOR_ADDRESS* de ce message MID initial est fixé avec la valeur de l'adresse principale choisie.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    OLSR Interface Address                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    OLSR Interface Address                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                              ...                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

FIG. 2.16 – Format du message MID [10]

Cette association doit être connue de chacun des nœuds du réseau. Les messages MID, émis régulièrement toutes les 5 secondes (*MID_Interval*), sont donc relayés de manière optimisée par les MPR. Le nœud choisit une période de validité pour ces informations et fixe ainsi le champ *VTIME* à la valeur de 15 secondes (*MID_HOLD_TIME*), durée pendant laquelle tous les nœuds du réseau devront conserver ces correspondances dans leur table d'association des interfaces.

A la réception d'un message MID chaque nœud du réseau intègre alors les renseignements contenus dans ces messages MID dans sa table d'association des interfaces, en associant *l'Originator_Address* du message et chacune des entrées *OLSR_INTERFACE_ADDRESS* trouvées dans le message MID.

I_IFACE_ADDR . . . . adresse de l'interface auxiliaire/secondaire
I_MAIN_ADDR . . . . adresse principale de l'initiateur (Originator Address)
I_TIME . . . . date à laquelle l'entrée expire et doit être supprimée de la table

FIG. 2.17 – Table d'association des interfaces (MID Set)

Cette table permet à un nœud de faire la correspondance entre l'adresse principale d'un nœud qui l'identifie comme voisin, concept central d'OLSR qui transite dans

chacun des messages de contrôle de topologie, et les adresses physiques du nœud qui seront au final inscrites dans chacune des tables de routage du réseau. Nous retrouverons cette table au moment de calculer les routes.

2.3.3 Table des réseaux extérieurs

Un nœud peut servir de passerelle vers un réseau filaire comme un LAN ou l'Internet. L'interface qui mène à ce réseau externe ne participe pas au réseau OLSR et, pour être connue des nœuds du réseau, elle doit être annoncée d'une manière similaire à la diffusion de la topologie. Il s'agit alors propager dans le réseau OLSR une information de réseau traditionnelle : l'adresse IP du réseau, son masque et sa passerelle. Le message HNA (*Host and Network Association*, cf. figure 2.18) permet d'apporter ces informations à chacun des nœuds. Ce message peut transporter aussi des adresses de machine unique, par exemple pour annoncer un serveur SMTP ou DNS. A l'inverse, pour qu'une machine extérieure au réseau OLSR puisse adresser une machine à l'intérieur du réseau OLSR, il faut mettre en place des mécanismes de translation d'adresse, car les adresses des réseaux ad hoc sont en général de classe privée, ou déclarer officiellement la passerelle qui émet les messages HNA comme routeur vers un réseau particulier. Dans ce dernier cas, les informations sont directement accessibles à partir des tables de topologie ou des tables de routage.

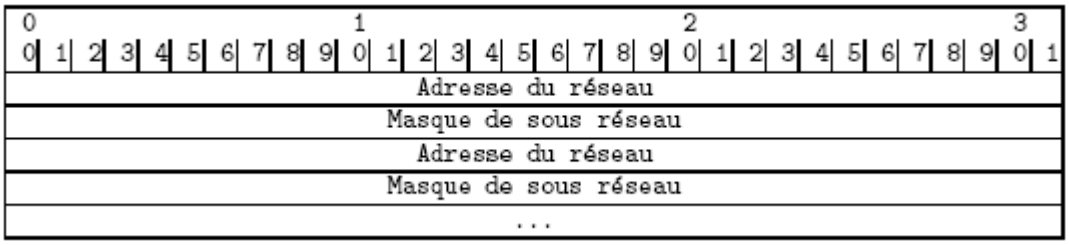


FIG. 2.18 – Format du message HNA [10]

Chaque nœud enregistre ces messages dans une table des réseaux extérieurs (cf. figure 2.19). Le champ *A_GATEWAY_ADDR* est fixé avec la valeur du champ *Originator Address* classique du message, et les champs *A_NETWORK_ADDR* et *A_NETMASK*, avec les valeurs trouvées dans le message. Le champ *A_TIME* est fixé avec la valeur de 15 secondes (*HNA_HOLD_TIME*), trouvé dans le champ *VTIME* de l'en-tête du message.

A_GATEWAY_ADDR	adresse de la passerelle
A_NETWORK_ADDR	adresse du réseau externe
A_NETMASK	masque du sous réseau
A_TIME	date à laquelle l'entrée expire et doit être supprimée de la table

FIG. 2.19 – Table des réseaux extérieurs (HNA Set)

Le principe du message HNA ressemble à celui du message TC : l'émetteur du message (i.e. L'ORIGINATOR ADDRESS) annonce la possibilité de joindre une cible par son intermédiaire. La différence vient de la possibilité d'invalider rapidement des liens dans le cas du message TC grâce au numéro de séquence (ANSN). Dans le cas du HNA, une route vers l'extérieur qui aura été rompue, disparaitra à expiration du délai A_TIME.

2.4 Routage

OLSR n'achemine que des messages de contrôle. C'est au système d'exploitation sous-jacent de prendre en charge le routage effectif des paquets de données. Le routage se fait conformément aux spécifications du RFC3626. OLSR se contente d'ajouter et de tenir à jour les tables de routage pour le réseau dont il a la charge.

OLSR calcule sa table de routage à chaque disparition ou addition d'une entrée d'une de ces tables :

- La table des liens
- La table de voisinage à un saut
- La table de voisinage à deux sauts
- La table de topologie
- La table des interfaces multiples

Par opposition, le recalcul de la table de routage n'entraîne pas de modifications dans ces tables intermédiaires.

R_DEST_ADDR. . . . . adresse de destination
R_NEXT_ADDR . . . . . adresse du prochain saut à utiliser
R_DIST. . . . . estimation de la distance à la destination
R_IFACE_ADDR . . . . . interface à utiliser

FIG. 2.20 – Informations de routage OLSR

Chaque entrée dans la table correspond à un tuple de quatre éléments (*R_DEST_ADDR*, *R_NEXT_ADDR*, *R_DIST*, *R_IFACE_ADDR*) (cf. figure 2.20). La table de routage possède le format suivant:

1.	**R_Dest_Addr**	**R_Next_Addr**	**R_Dist**	**R_Iface_Addr**
2.	**R_Dest_Addr**	**R_Next_Addr**	**R_Dist**	**R_Iface_Addr**
3.	**…**	**…**	**…**	**…**

FIG. 2.21 – Table de routage OLSR finale

Principe de calcul de la table de routage

La table de roulage est mise à jour à chaque fois qu'on détecte un changement dans la base de voisinage ou de la topologie. Plus précisément, quand on détecte l'apparition ou bien la disparition d'un nœud dans le voisinage, ou la disparition ou l'apparition d'un tuple dans la base de topologie. Cette mise à jour n'entraine aucune génération de message dans le réseau ; il s'agit d'un simple recalcul local.

Le calcul de la table de routage se fait conformément à la procédure suivante :

1. Détruire toutes les entrées ultérieures de la table.
2. On insère dans la table tous les voisins directs qui sont les voisins symétriques à un saut. Ces informations sont extraites de la base de voisinage. Pour chaque entrée on ajoute : *R_DEST_ADDR* correspondant a l'adresse principale du voisin *N_NEIGHBOR_MAIN_ADDR* dans la base de voisinage. *R_NEXT_ADDR* correspondant à l'interface voisine *L_NEIGHBOR_IFACE_ADDR*, et *R_IFACE_ADDR* correspondant à *L_LOCAL_IFACE_ADDR*. *R_DIST* est naturellement initialisé à 1.
3. Ensuite, on insère les destinations à plus de un saut (h=1). La procédure suivante est exécutée pour chaque valeur de h, en commençant par h=1 et en incrémentant h par 1, à chaque itération. Cette boucle s'arrête lorsqu'il n'y a plus de nouvelles entrées dans la table de routage.

    - Pour chaque tuple dans la base d'informations de topologie, si *T_DEST_ADDR* ne correspond à aucun *R_DEST_ADDR* des entrées de la table de routage, et *T_LAST_ADDR*, correspond à l'un des *R_DEST_ADDR* avec un *R_DIST* égale à h, alors, on insère une nouvelle entrée dans la table de routage tel que :

        - *R_DEST_ADDR* égale à *T_DEST_ADDR*.
        - *R_NEXT_ADDR* égale au *R_NEXT_ADDR* de l'entrée dont le *R_DEST_ADDR* est égale à *T_LAST_ADDR*.
        - *R_DIST* égale à h+1.

Par la suite, la table de routage est complétée par l'ensemble des associations des interfaces en ajoutant des entrées pour : toutes les interfaces non présentes dans la table de roulage mais dont l'adresse principale associée y figure déjà. Finalement, on termine l'insertion des routes vers l'ensemble des associations des réseaux et les hôtes rattachés. Bien évidement, l'adresse du next hop et 1a distance sont les mêmes que celle de l'adresse principale qui permet de joindre ces interfaces et sous-réseaux.

3. Conclusion

Grâce aux MPR, le protocole OLSR permet de restreindre le nombre de retransmissions dans le mécanisme d'inondation. Les MPR sont les seuls à générer des messages de contrôle, et les messages qu'ils génèrent n'incluent que les liens aux nœuds qui les ont sélectionnés comme MPR. Les éléments de base de topologie ainsi diffusés à chacun des nœuds du réseau pour construire une vision globale du réseau vont permettre de construire des routes optimales dont l'ensemble des nœuds intermédiaires ne seront pas forcément que des MPR.

L'utilisation des MPR lors de l'inondation de l'information, constitue une grande optimisation apportée par OLSR par rapport aux algorithmes à état des liens classiques. Ce concept va permettre à OLSR de pousser encore plus loin les optimisations dans les mécanismes de construction et de diffusion de la topologie du réseau ad hoc.

Le format du paquet de contrôle d'OLSR permet d'ajouter des fonctionnalités comme la prise en charge des périodes de sommeil, le multicast, les économies d'énergie. Cette modularité en fait un protocole particulièrement adaptable pour tester de nouvelles idées afin de déployer des réseaux ad hoc.

CHAPITRE

3

Consommation d'énergie dans les réseaux ad hoc

1. Motivations

L'objectif pour un réseau ad hoc est que les terminaux mobiles soient utilisés au maximum n'importe où et n'importe quand "any-where and anytime". Cependant, l'une des grandes limitations de cet objectif concerne le support énergétique. En effet, la principale contrainte dans les communications sans fil est la durée de vie limitée des terminaux mobiles dont le support énergétique représente souvent une batterie dont la capacité est limitée.

Nous donnons, ci-dessous, quelques exemples des principaux facteurs affectant la consommation de batteries dans un réseau sans fil :

- *la transmission radio* : la consommation la plus importante est due à la transmission radio. Il convient de noter qu'une émission est davantage coûteuse qu'une réception et que comparativement, une veille est la moins coûteuse ;

- *gestion du terminal* : une autre utilisation des batteries est due à l'alimentation des ressources propres au terminal, qu'il s'agit de CPU, de disque dur, des mémoires, d'affichage, etc. ;

- *fonctionnalités* des protocoles permettant d'assurer la liaison entre les stations pendant une communication : nous citons, par exemple, les protocoles de contrôle de collision, de congestion, de routage;

- *les applications* : les applications qui commencent à émerger pour les réseaux ad hoc consomment également les ressources de la batterie et plus spécialement les applications utilisant des calculs pour la compression ou le cryptage de données, par exemple.

Plusieurs études ont montré que les plus grands facteurs consommant la batterie d'un ordinateur portable sont le microprocessor (CPU), l'écran à cristaux liquides (LCD), le disque dur, le lecteur de CDROM, le lecteur de disquette, le système d'E/S, et la carte réseau sans fil [19]. La conservation d’énergie a donc, été pendant longtemps traitée au niveau de la couche physique. Cependant, nous pouvons remarquer, dans la liste énumérée ci-dessus, qu'il existe d'autres facteurs, en dehors de la couche physique, pouvant affecter la consommation d’énergie des batteries. Ainsi, la conception de nouveaux protocoles de communication réseaux devrait aider à réduire cette consommation. La section 2 donne un aperçu de ce qui se fait dans ce domaine. Nous nous concentrons, dans la section 3, sur la couche réseau et nous allons prouver l'impact du choix du protocole de routage sur la consommation d’énergie dans les réseaux ad hoc.

2. Protocoles minimisant la consommation des batteries

Chacune des couches du modèle OSI a fait l'objet de propositions pour réduire la consommation des batteries selon différentes approches [20]. Notons que le problème de consommation d’énergie ne peut être traité séparément dans une des couches protocolaires. Nous allons exposer ici quelques propositions parmi les plus intéressantes concernant ces différentes couches.

2.1 Couche Physique

Dans le passé, les recherches sur la consommation d’énergie se sont concentrées sur la couche physique étant donné que la consommation d’énergie dans un ordinateur portable était considérée comme origine directe du matériel utilisé. Ces travaux concernent l'augmentation de la capacité de la batterie, une fréquence d'horloge variable pour le CPU, l'utilisation des mémoires flash, etc. Notons qu'à la différence d'autres domaines de l'informatique, la technologie de batterie n'a pas subi un avancement significatif au cours des 30 dernières années.

2.2 Sous-couche MAC

La couche MAC (Médium Access Control) évoquée plus haut dans le chapitre 1 est une sous-couche de la couche liaison de données. Cette couche fait l'interface avec la couche physique et comprend des protocoles définissant la manière d'allouer les canaux radios partagés entre l'ensemble des nœuds mobiles. L'objectif de la couche MAC consiste à éliminer, autant que possible, les collisions puisque les collisions provoquent des retransmissions, et les retransmissions mènent à une consommation inutile d’énergie. Notons que, dans un réseau sans fil, les retransmissions ne peuvent pas être complètement évitées à cause du taux d'erreurs très élevés et de la mobilité des nœuds.

Il existe plusieurs protocoles MAC : IEEE 802.11 [4], EC-MAC [21] et PAMAS [22]. Nous choisissons de présenter le protocole PAMAS parce que c'est un protocole conçu spécialement dans le but de réduire la consommation d’énergie dans les réseaux ad hoc.

2.2.1 Le protocole PAMAS

Le protocole PAMAS (Power Aware Multi-Access Protocol with Signalling) [22], est un protocole à accès multiples au médium radio basé sur le protocole MACA (Multiple Access Collision Avoidance) [23] permettant de palier aux problèmes de station cachée.

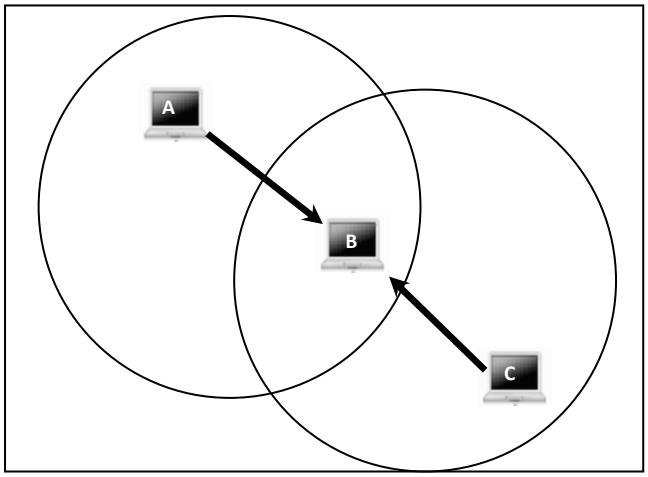


FIG. 3.1 – Problème du terminal caché

PAMAS rajoute par rapport à MACA, l'utilisation de deux canaux distincts, l'un utilisé pour la signalisation, transportant donc les messages de contrôle RTS/CTS (Request ToSend/Clear To Send) ; l'autre utilisé pour le transport des données.

Ainsi, toute station ne peut perturber que le canal de signalisation, n'affectant pas le transport des données. Bien sûr, les messages RTS peuvent toujours être soumis aux problèmes de collision mais leur taille est relativement courte et, de manière générale, la perte subie en demandant une réémission ultérieure d'un tel paquet est nettement inférieure à celle subie pour la réémission d'un paquet de données.

Par ailleurs, le principal apport de PAMAS est la conservation des batteries des nœuds. Ceci est réalisé grâce à une optimisation de la couche MAC, en permettant à

toutes les stations d'éteindre leur interface radio afin de réduire leur consommation d'énergie, à chaque fois que leur interface radio n'est pas utilisable. En effet, le protocole se base sur le constat qu'une station ne peut recevoir de message tant qu'elle écoute une autre communication, et ne peut pas émettre non plus si l'une de ses voisines est en train de recevoir des messages (pour causes d'interférences). Toute station pourra éteindre son interface radio (s'endormir) au cas où :

- elle ne veut pas émettre et au moins un voisin est en train d'émettre vers une autre station ;
- elle veut émettre et au moins un voisin est en train de recevoir ;
- elle veut émettre mais tous ces voisins sont déjà en train d'émettre.

Pour déterminer la durée pendant laquelle la station peut rester éteinte, il faut que le paquet RTS indique la longueur du message de façon à ce que le paquet CTS le diffuse au voisinage, qui en est ainsi avertie. Un problème se pose cependant lorsque les stations se réveillent et trouvent le canal occupé, ignorant la durée de cette nouvelle communication et surtout augmentant la probabilité de collision des messages RTS. Une solution à ce problème est apportée en utilisant un algorithme de backoff. Ainsi, une station, avant toute émission, se voit affecté un quota de temps (différent pour chaque station) au bout duquel elle est autorisée à émettre son paquet de requête RTS. La station dont le délai, avant d'émettre, est le plus court va donc pouvoir contacter sa cible, qui lui répondra par diffusion que le canal est occupé. Cette réponse va être entendue de tous les voisins directs de la cible qui seront ainsi avertis du message et par conséquent, abandonneront le processus d'émission de leur paquet RTS. Ce mécanisme va donc permettre de disperser dans le temps les messages RTS pour réduire les possibilités de collisions des stations qui se réveillent en utilisant PAMAS. PAMAS est donc un bon protocole réduisant les collisions, et minimisant la consommation des batteries. En outre, son intégration aux protocoles de routage classique est assez aisée.

2.3 Sous-couche LLC

Dans ce paragraphe, nous nous intéressons aux fonctionnalités de contrôle d'erreur de la sous-couche de la couche liaison de données: LLC (Logical Link Control). Les deux techniques les plus utilisées pour le contrôle d'erreur, dans un environnement filaire, sont ARQ (Automatic Repeat Request) et FEC (Forward Error Correction). Ces méthodes consomment beaucoup d'énergie en raison des retransmissions et de la surcharge nécessaires pour la correction d'erreurs. Utiliser ce genre de protocoles, dans un environnement sans fil, nécessite une grande adaptation vu le taux d'erreur qui est

plus élevé (bruit, évanouissement du signal, mobilité, etc.). Quelques travaux récents ont proposé des algorithmes d'adaptation de ces méthodes de contrôle d'erreurs permettant également de réduire la consommation d’énergie [24] [25].

Dans [24] par exemple, les auteurs proposent d'incorporer un protocole de sondage (probing) permettant de ralentir la transmission des données dès lors que l'état du canal est dégradé. Ainsi, le protocole ARQ est utilisé normalement jusqu'à ce que l'émetteur détecte une erreur sur les données ou sur le canal de contrôle qui est due au non réception d'acquittement (ACK). A cet instant, le protocole passe en mode sondage dans lequel un paquet de sondage (probe) est envoyé chaque t slots. Le paquet de sondage contient seulement un en-tête avec peu ou pas de charge utile et consomme donc peu d'énergie. Ce mode est adopté jusqu'à ce qu'un acquittement ACK soit correctement reçu. Le protocole alors revient en mode normale et continue la transmission des données à partir du point auquel il a été interrompu.

2.4 Couche réseau

Les protocoles de couche réseau composent la plus grande classe de protocoles d'économie d'énergie. Ils diffèrent selon le type du trafic :

- Trafic en unicast
- Trafic de diffusion

2.4.1 Trafic de diffusion

La diffusion est une importante opération dans les réseaux et plus spécialement dans les réseaux ad hoc en raison de la mobilité des nœuds. Dans ces réseaux, les diffusions chargent considérablement le réseau en plus d'accroître les collisions, qui entraînent ensuite des rediffusions. C'est une source de consommation des batteries qui peut vite être importante. Des solutions à ce problème ont été suggérées, en utilisant différentes stratégies possibles [26]:

- *des considérations probabilistes* : la première fois qu'un message est reçu il est diffusé avec une probabilité *p*, en considérant qu'une absence de diffusion peut être compensée par les voisins, si la valeur de *p* est bien adaptée ;
- *des considérations de comptage* : ne pas diffuser un paquet s'il a déjà été diffusé. Cette solution est simple et évite les redondances mais elle n'est pas toujours efficace ;

- *ou encore des considérations de proximité* : ne pas diffuser un paquet, s'il vient d'une station proche d'une distance d, puisqu'une diffusion aura environ la même portée. Ces solutions sont approximatives, mais les simulations en ont montré l'intérêt.

2.4.2 Trafic unicast

La principale métrique utilisée dans les protocoles de routage ad hoc traditionnels est le nombre minimum de sauts. Cependant, cette métrique a un effet négatif sur la consommation d’énergie de certains nœuds. Par exemple, dans la figure 3.2, le trafic allant du nœud A au nœud D va toujours passer par le nœud E, ce qui va provoquer la consommation de toute la batterie de ce dernier. Et si tel est le cas, le nœud F devient injoignable et le réseau devient partitionné. L'utilisation d'un algorithme de routage qui tient compte de la métrique énergétique va, au contraire, utiliser une autre route que celle passant par le nœud E (par exemple, la route passant par les nœuds B et C).

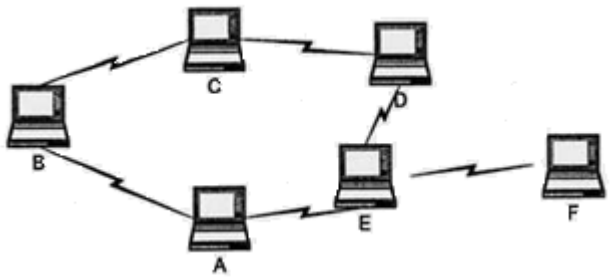


FIG. 3.2 – Topologie d'un réseau ad hoc

Les protocoles de routage spécifiquement développés pour réduire la consommation des batteries ne fournissent pas de nouveaux algorithmes de routage mais proposent des améliorations à ceux déjà existants. L'idée fondamentale de ces protocoles est de router les paquets en fonction de la minimisation d'un critère relatif à la consommation des batteries, et qui peut être de deux types :

- Coût des liens
- Coût des batteries sur les nœuds

2.4.2.1 Coût des liens

Cette métrique mesure la puissance nécessaire par bit pour transmettre un paquet de la source à la destination. Les auteurs [27] [28] se basant sur cette métrique, fournissent un algorithme MTPR (*Minimum Total Transmission Power Routing*). Ils considèrent que la puissance dépend de la taille des paquets et de la distance *d* qui sépare deux nœuds voisins. L'objectif est de déterminer le chemin le plus court en termes de consommation d'énergie. Ainsi, les chemins avec plus de sauts ayant des portées de transmission courtes sont favorisés pour le routage; ceux avec moins de sauts mais ayant des portées de transmission plus longues sont délaissés.

Cette métrique minimise de manière globale la consommation d'énergie dans le réseau cependant, ceci s'effectue au détriment de la capacité restante de la batterie des nœuds participants dans le processus de routage. Plus précisément, le problème peut être défini par les équations mathématiques suivantes :

$$\begin{gathered} min \sum_{i=0}^{d-1} E[n_i, n_{i+1}] \\ E[n_i, n_{i+1}] \propto (packet\_size, distance) \end{gathered} \quad (1)$$

où:

- n_i : nœud au chemin du routage,
- n_0 : nœud source,
- n_d : nœud destination,
- $E[n_i, n_{i+1}]$: énergie consommée pour la transmission d'un bit sur le lien $[n_i, n_{i+1}]$.

2.4.2.2 Coût des batteries sur les nœuds

Cette métrique évalue la quantité d'énergie présente sur les nœuds [27], [28], [29]. Contrairement à la métrique du coût du lien, celle-ci est plus précise pour décrire individuellement la durée de vie de chaque nœud. L'objectif est de déterminer un chemin constitué des nœuds de plus forte capacité énergétique, (c.à.d. les nœuds de plus faible coût). Ainsi, les équations mathématiques peuvent être de la forme :

$$max \sum_{i=0}^{d} c_i(t) = min \sum_{i=0}^{d} \frac{1}{c_i(t)} \qquad (2)$$
$$\frac{1}{c_i(t)} > \gamma$$

où:

- $c_i(t)$: la capacité restante de la batterie du nœud n_i en fonction du temps,
- $1/c_i(t)$: le coût de la batterie du nœud n_i en fonction du temps,
- $c_0(t)$: la capacité restante de la batterie du nœud source en fonction du temps,
- $c_d(t)$: la capacité restante de la batterie du nœud destination en fonction du temps,
- γ : seuil fixé.

Se basant sur cette métrique, les auteurs [27] [28] ont proposé deux protocoles de routage max-min. Le premier protocole se nomme MMBCR, il considère le nœud le plus faible en matière d'énergie restante de la batterie sur un chemin possible est le nœud déterminant. Ainsi, la route choisie est celle dont le nœud le plus fiable (nœud crucial) a la puissance restante maximale parmi les nœuds cruciaux enclavés dans les chemins possibles en direction de la même destination. En considérant uniquement la somme des valeurs de la fonction coût de la batterie $f_i(t) = 1/c_i(t)$, le système MMBCR détermine le coût d'une route à l'aide de la fonction suivante :

$$P(r_j) = \max_{\forall\, n_i \in r_j} f_i(t)$$

Ainsi, la route optimale est déterminée comme suite :

$$R(r_o) = \min_{r_j \in r*} P(r_j)$$

Le deuxième protocole de routage max-min CMMBCR est une approche hybride en considérant à la fois l'énergie restante de la batterie des nœuds et la consommation totale d'énergie sur l'itinéraire en entier. Les chemins sélectionnés sont ceux dont tous les nœuds ont une capacité restante de batterie supérieure à un seuil γ. L'itinéraire retenu parmi la sélection est celui dont l'énergie de transmission est minimale. Ainsi, si tous les chemins ont des nœuds avec une capacité de batterie inférieure au seuil γ,

l'itinéraire qui inclut des nœuds avec la capacité la plus inférieure devra être évité afin de prolonger la durée de vie de ces nœuds. La capacité de la batterie d'une route r_j à l'instant t est définie comme suivant :

$$R_j(t) = \min_{\forall\, n_i \in r_j} c_i(t)$$

Soit deux nœuds n_a et n_b. Ce protocoles considère deux ensembles Q et A, où Q est l'ensemble de tous les itinéraires possibles entre deux nœuds n_a et n_b à l'instant t et A l'ensemble de tous les itinéraires possibles entre deux nœuds quelconque (toutes les paires possible du réseau) qui vérifient la condition $Rj(t) \geq \gamma$ (γ étant un seuil fixe) à l'instant t.

Le choix d'un itinéraire entre [n_a, n_b] fonctionne comme suite :

$$\begin{cases} si\ A \cap Q \neq \emptyset & alors\ choisir\ un\ itinéraire\ en\ appliquant\ l'énergie\ minimale\ (1) \\ sinon & choisir\ un\ itinéraire\ en\ appliquant\ MMBCR\ (2) \end{cases}$$

2.5 Couche Transport

La couche transport fournit un service de transport de données de bout en bout. Le protocole de transport le plus généralement utilisé pour les réseaux fixes, où les liens physiques sont assez fiables, est le protocole TCP (Transmission Control Protocol). Cependant, en raison des propriétés du lien sans fil, les performances de TCP se dégradent significativement. TCP fait appel à un grand nombre de retransmissions et à des mesures de contrôle de congestion lors d'erreur sur le lien sans fil ou de pertes dues aux handoff. Cependant, et comme indiqué auparavant, les retransmissions consomment inutilement l'énergie des batteries.

Des propositions de protocoles telles que Reno et New Reno [30], ont été faites dans l'unique but de concevoir des protocoles de transport dans un environnement sans fil. Bien que ces protocoles aient mené, ou non, à une plus grande efficacité énergétique, ils n'ont pas directement étudié l'idée de réduire la consommation d'énergie au niveau de la couche transport.

2.6 Couche Application

L'efficacité énergétique dans la couche application est devenue un important domaine pour les industriels ainsi que pour les chercheurs. En industrie, des API ont été développées [31] afin d'aider les réalisateurs de logiciel à créer des programmes qui sont moins consommateurs d'énergie. En recherche, les auteurs de [32] proposent une technique de transmission de vidéo encodée permettant de réduire la consommation des

batteries. L'idée fondamentale de ce travail consiste à diminuer le nombre de bits transmis sur le lien sans fil afin de réduire la consommation d’énergie tout en préservant une qualité visuelle acceptable de la vidéo.

3. Impact du routage sur la consommation d’énergie

Dans cette section, nous nous positionnons au niveau 3 (couche réseau) du modèle OSI. L'objectif est d'observer l'impact du protocole de routage sur la consommation d’énergie dans les réseaux ad hoc. Ainsi, nous cherchons à comparer quatre importants protocoles de routage ad hoc présentés dans le chapitre 1 : DSDV, OLSR, AODV et DSR. Nous évoquerons tout d'abord, les éléments importants inhérents aux algorithmes de routage étudiés qui peuvent influencer la consommation d’énergie. Ceci nous servira ensuite, comme base pour présenter nos résultats de simulation et pour les analyser.

3.1 Caractéristiques énergétiques des protocoles de routage

La section suivante discute de certaines caractéristiques des protocoles étudiés qui pourraient affecter la consommation d’énergie. En effet, quelques différences significatives, du point de vue consommation d’énergie, entre le comportement proactif et réactif des algorithmes de routage étudiés sont listées ci-après :

- *la bande passante est différemment sollicitée* : le fait qu'il s'agisse d'un protocole de routage proactif ou réactif se traduit, en terme de consommation, par le fait que, dans le cas proactif on doit consommer de l’énergie pour mettre à jour périodiquement la table de routage, et dans le cas réactif, on doit consommer de l'énergie uniquement pour découvrir une route au cas où communication doit être établie. Dans les algorithmes de routage proactifs, les diffusions permanentes de paquets de contrôle ne seront probablement jamais utilisées ultérieurement. Clairement, les mécanismes réactifs ont un net avantage sur ce point (mais probablement pas en ce qui concerne les délais de routage),

- *la gestion de la mobilité* : un autre avantage des protocoles de type réactif concerne la gestion des scénarios de mobilité. Effectivement, dans le cas d'un protocole proactif, plus le nombre de nœuds en mouvement est nombreux, plus les mises à jour nécessaires à réparer les tables de routage sont nombreuses. Ces mises à jour gaspillent inutilement les batteries ;

- *Réduction des diffusions* : avec OLSR, seules les stations multipoints MPR peuvent assumer la fonction de routeur, ce qui minimise les diffusions, et par conséquent la consommation d’énergie.

Ces éléments précédents peuvent être résumés avec le tableau suivant :

	DSDV	OLSR	AODV	DSR
Routes maintenue dans	table de routage	table de routage	table de routage	cache de route
Découverte de route nécessaire	Non	Non	Oui	Oui
Mise à jour périodique nécessaire	Oui	Oui	Non	Non
Mise à jour auprès de	Tous des voisins	Seulement aux MPR	Pas de mise à jour	Pas de mise à jour
Utilise des messages ''Hello''	Oui	Oui	Oui (aux voisins actifs seulement)	Non
Chemin inséré dans l'en-tête du paquet	Non	Non	Non	Oui
Utilise des temporisateurs de source	Non	Non	Oui	Non
Multiple routes disponibles	Non	Non	Non	Oui

TAB. 3.1 – Comparaison des caractéristiques des quatre protocoles de routage

Ainsi, chaque approche a ses propres avantages et inconvénients que nous allons pouvoir évaluer via des simulations. Ces simulations permettront de comprendre, plus précisément, leur mode de fonctionnement relatif à l'utilisation de l'énergie.

3.2 Etude comparative des protocoles de routage

L'étude de performances de ces quatre protocoles de routage (DSDV, OLSR, DSR et AODV) a été réalisée grâce au simulateur NS-2 [33] développé par le groupe de recherche VINT de l'université de Berkeley. Le groupe de recherche Monarch de l'université de Carnegie Mellon- CMU a étendu le simulateur NS-2 pour inclure des scénarios de mobilité. La majorité des protocoles de routage ad hoc y sont implémentés. Les nouvelles versions de cette extension incluent, également, des modèles d'énergie pour les nœuds mobiles, et que nous avons utilisé pour cette étude. La couche MAC implémente l'interface IEEE 802.11 utilisant la fonction DCF (Distributed Coordination Function) comme méthode d'accès. La carte d'interface réseau utilise les valeurs spécifiées pour les cartes WaveLan de Lucent [34], et qui sont détaillés dans le prochain chapitre.

Nous avons considéré un scénario de base en le faisant varier par la suite. Dans le scénario de base, nous définissons le réseau ad hoc comme une surface de (600x600) m2, avec 20 nœuds aléatoirement dispersés sur cette surface. Les nœuds se déplacent

pendant une durée de 1000 seconds, avec une vitesse maximum de 2m/s et un temps de pause de 35 secondes. Ils communiquent ensemble en générant chaque seconde 4 paquets CBR de 512 octets.

La consommation d'énergie est principalement due à la transmission/réception des paquets de données et des paquets de contrôle. Enfin, nous avons apporté des modifications au scénario de base pour voir comment ceux-ci peuvent influencer la consommation. Trois paramètres ont été considérés : la vitesse des nœuds, le nombre de nœuds et la quantité du trafic.

3.2.1 Résultats de simulation

La consommation d'énergie pour ces protocoles de routage en fonction de la vitesse des nœuds est présentée dans la figure 3.3. Ces résultats indiquent que les protocoles réactifs tels que DSR et AODV consomment moins d'énergie que les protocoles proactifs. En effet, les protocoles réactifs ne consomment presque rien lorsqu'il n'y a aucun trafic dans le réseau, tandis que les protocoles proactifs consomment constamment de l'énergie par les calculs de routes, même si aucun paquet ne sera envoyé. Les protocoles réactifs sont donc moins sensibles au déplacement des nœuds. En outre, la mise en place de nouveaux relais multipoint lorsque la topologie du réseau change, rend OLSR un peu plus consommateur que DSDV.

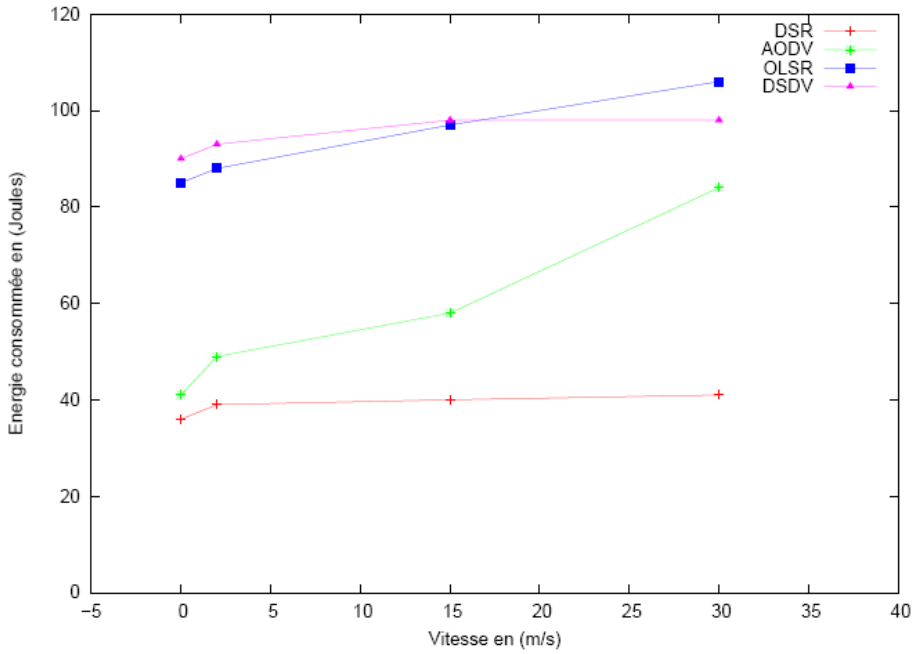


FIG. 3.3 – Consommation d'énergie en fonction de la vitesse des nœuds

Dans la figure 3.4, on peut constater que les protocoles réactifs surpassent, encore une fois, les protocoles proactifs lorsque le nombre de nœuds augmente. En fait, plus le nombre de nœuds est grand, plus les protocoles proactifs souffrent de leur mise à jour. Nous remarquons qu'AODV est moins stable que DSR. Nous remarquons également que si OLSR consomme beaucoup, DSDV consomme encore davantage et de manière irrégulière. En effet, OLSR réduit le nombre de diffusions aux seuls nœuds multipoints MPR. Mais globalement, les protocoles proactifs posent dans ce cas (un grand réseau avec beaucoup de nœud) un problème de passage à l'échelle (scalabilité).

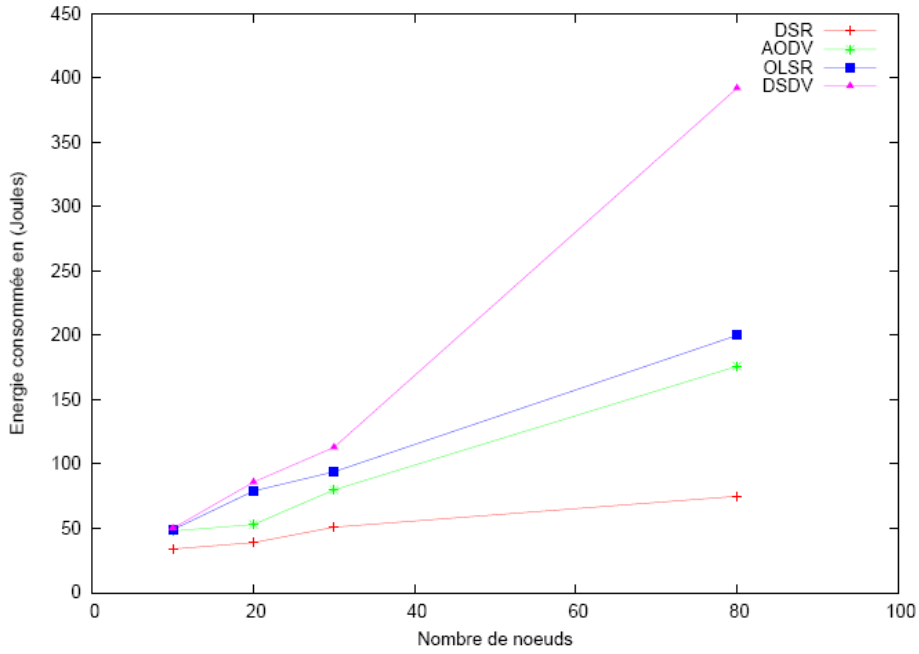
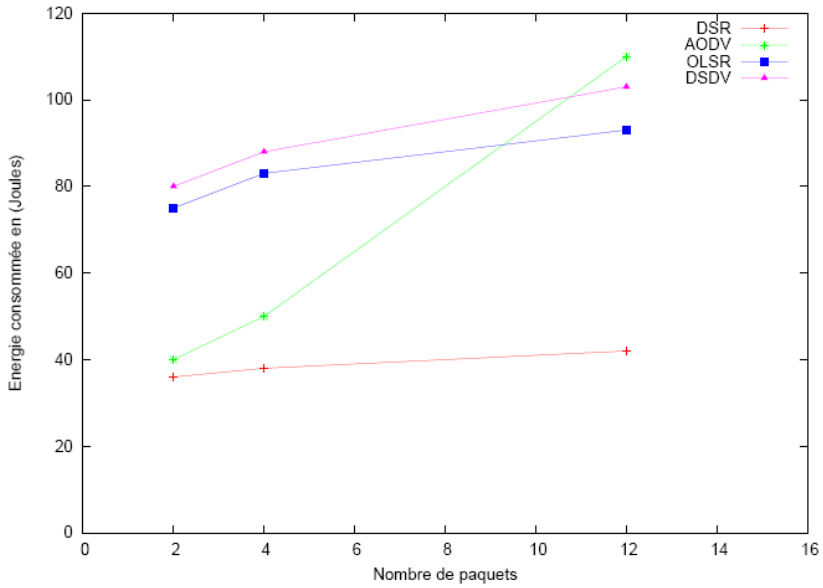


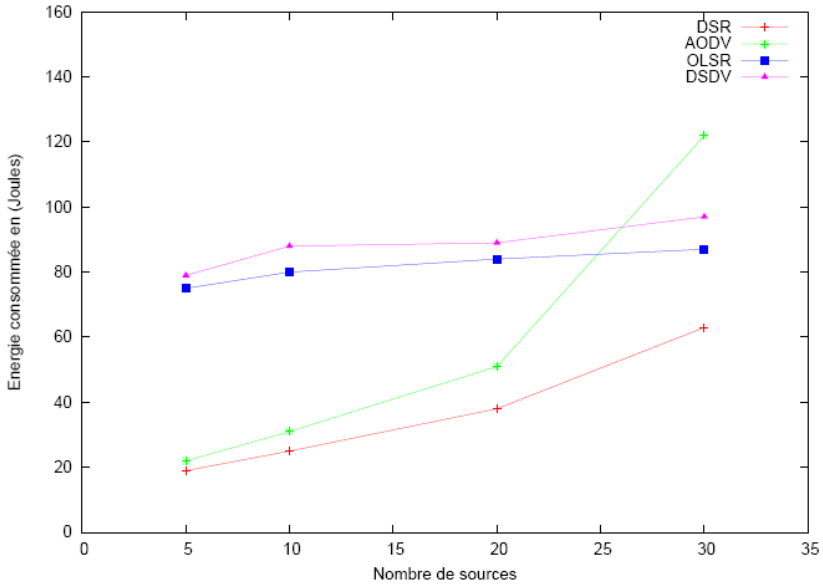
FIG. 3.4 – Consommation d'énergie en fonction du nombre de nœuds

Finalement, la figure 3.5(a) et la figure 3.5(b) montrent un comportement similaire des protocoles de routage, puisque les paramètres que l'on fait varier concernent le trafic et que les résultats obtenus sont semblables. À mesure que le trafic augmente, DSDV et OLSR voient leur énergie décroître de manière régulière, avec un net avantage pour OLSR. Ils rentabilisent en quelque sorte le travail de leur mise en place de la table de routage puisque les découvertes de routes ont déjà été faites de manière globale. En revanche, DSR même s'il est plutôt stable quand le nombre de paquets croit, il réagit mal lorsque le nombre de sources augmente. Cela est du au fait que dans le premier cas, les chemins sont les mêmes et seul le nombre de paquets varie ; alors que dans le second cas, de nouvelles découvertes de routes sont à initier pour établir la communication entre la source et la destination. À une plus grande échelle, le même problème apparaît

avec AODV, puisque AODV montre aussi ses faiblesses lorsque le trafic augmente et de manière encore plus importante qu'avec DSR. En fait, AODV est contraint pour deux de ses caractéristiques, les messages HELLO, périodiquement envoyés aux voisins actifs dans les communications, ainsi que les ré-découvertes de route forcées par un temporisateur qui permet de purger les entrées de la table.



(a)



(b)

FIG. 3.5 – Consommation d'énergie en fonction du (a) nombre paquets (b) nombre de sources

4. Conclusion

Dans ce chapitre, nous avons pu s'en assurer, grâce à un ensemble de résultats expérimentaux, que le choix du protocole de routage influe réellement sur le taux de consommation d’énergie dans 1es réseaux ad hoc.

Par ailleurs, nous remarquons que ces protocoles (DSR, AODV, OLSR et DSDV) ainsi que tous les autres protocoles normalisés dans le groupe MANET de l'IETF, s'intéressent à découvrir uniquement le plus court chemin lors du processus de découverte de route. Cependant une métrique de routage basée sur la consommation d’énergie peut s'avérer plus efficace. D’autant plus, que cette métrique n'est pas forcément un frein à la rapidité du processus de transmission. Par exemple, une station qui assure une forte connectivité peut engendrer un délai de transmission plus long que celui prévu initialement. Ceci est dû au fait que sa position en fait une cible de routage idéale, pouvant amener à une situation de congestion sur ces liens.

Autrement dit, le plus court chemin n'est probablement pas le critère le plus efficace, puisqu'un service de même qualité peut être apporté par d'autres critères. Nous proposons, dans la dernière partie de ce mémoire, des extensions de l'un des plus importants protocoles de routage actuels qui est OLSR. Ces extensions prennent en compte une métrique basée sur la consommation d’énergie lors de la sélection des MPR, permettant ainsi d'augmenter la durée de vie du réseau ; c'est probablement le facteur principal pour pouvoir communiquer.

CHAPITRE

4 Protocoles minimisant la consommation d’énergie

1. Motivations

Nous avons présenté dans le chapitre précédent quelques solutions existantes, permettant de réduire la consommation des batteries dans les réseaux ad hoc. Nous avons principalement mis le point sur les protocoles en rapport avec la couche 3 (routage) du modèle OSI, et avons démontré que la consommation d’énergie devrait être une question cruciale lors de la conception d'un algorithme de routage.

De ce fait, le principe majeur sur lequel se base notre réflexion est l'équité. En effet, certaines situations géographiques (centre du réseau) sont relativement sollicitées ; tout comme un certain nombre de personnes qui sont des consommateurs gourmands, alors que d'autres sont des consommateurs moyens ou faibles. L'objectif consiste à ce que ces derniers (consommateurs moyens ou faibles) ne soient pas trop défavorisés lors de la sélection de route, tout en permettant aux premiers (consommateurs gourmands) d'exploiter pleinement leurs batteries. Autrement dit, l'objectif est de réduire tant que possible le problème de la station cible, dans lequel un terminal n'aura pas servi à son utilisateur, mais uniquement en tant que routeur, pour les besoins des autres utilisateurs.

Dans ce chapitre, nous allons présenter de nouveaux protocoles de routage ad hoc, dont la métrique de routage est basée sur la consommation d’énergie, précisément sur l’énergie résiduelle des nœuds. Ces nouveaux protocoles ont pour principaux objectifs de garantir que la connectivité du réseau soit maintenue aussi longtemps que possible, et que le niveau d'énergie du réseau entier soit du même ordre. Nous avons regroupé ces deux objectifs en un seul terme, qui est "survivabilité" d'un réseau ad hoc. Les protocoles que nous avons développés E_OLSR1, E_OLSR2 et E_OLSR3 garantissent cette survivabilité. Ce sont des protocoles proactifs et, comme l'indiquent leurs noms, ils sont basés sur l'un des plus importants protocoles de routage actuels qui est OLSR (ce dernier est détaillé dans le Chapitre 2).

2. Changement de Critère de Sélection des MPR

OLSR est un protocole de routage best-effort, il offre des routes optimales en termes de nombre de sauts dans le réseau. La technique de sélection des MPR permet au nœud de choisir le voisin qui couvre le plus grand nombre des voisins de second niveau, cette stratégie minimise l'inondation du réseau. Cependant, avec un tel mécanisme nous n'obtiendrons pas le meilleur chemin en terme énergétique. Pour intégrer l'énergie comme métrique au niveau du choix des MPR, on propose trois améliorations d'OLSR. Dans cette partie, nous allons essayer de présenter leur principe.

Le choix des MPR est essentiel dans la détermination de la route optimale en énergie dans le réseau, En se basant sur cette idée, nous proposons trois algorithmes de sélection des MPR.

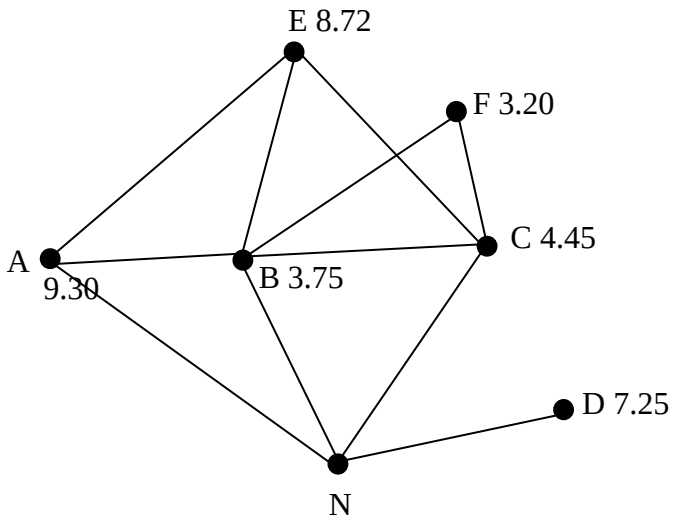


FIG. 4.1 – Exemple de réseau pour illustrer la sélection des MPR

2.1 E_OLSR1

Dans E_OLSR1, la sélection des MPR se fait pratiquement de la même manière que dans OLSR standard. Cependant, s'il y a plusieurs voisins à un saut qui couvrent le même nombre de voisins du second niveau, le nœud avec la meilleure capacité restante (E_r) l'emporte, étant ainsi élu nœud MPR par le nœud local N.

En utilisant les mêmes conventions que précédemment (utilisées dans le chapitre 2), l'algorithme de sélection des relais multipoints peut être formalisé comme suite :

On désigne par *N(x)* l'ensemble des voisins directs de x, par *N2(x)* l'ensemble des voisins du second niveau, et MPR(x) l'ensemble des relais multipoint de x.

1. Commencer par un ensemble de relais multipoint vide *MPR(x)* = {}.
2. Choisir les nœuds de l'ensemble des voisins *N(x)* qui sont les seuls à avoir un lien avec un voisin du second niveau. Ajouter ces nœuds sélectionnés de *N(x)* à l'ensemble *MPR(x)*, et éliminer tous les nœuds du second niveau couvert par ces derniers de l'ensemble *N2(x)*.
3. Tant que *N2(x)* ≠ {} faire
   (a) Calculer le degré de chaque nœud dans *N(x)*. Le degré pour un nœud est le nombre des voisins du second niveau couvert par celui-ci présent dans *N2(x)*. S'il y a une égalité, celui avec la plus grande énergie résiduelle est choisi
   (b) Ajouter le nœud de *N(x)*, ayant le degré maximal à l'ensemble des relais multipoint *MPR(x)*, et enlever tous les nœuds du second niveau couvert par celui ci de *N2(x)*.

Supposons que chaque nœud dans, le réseau de la figure 4.1 connaît son niveau d'énergie. Le nœud N choisirait avec E_OLSR1 les MPR suivants:

Noeud_local	Voisin à 1 saut	Voisin à 2 sauts	MPR
N	A, B, C, D	E, F	C

TAB. 4.1 – Sélection des MPR dans E_OLSR1

Entre B et C, c'est le nœud C qui est retenu comme MPR puisqu'il possède la meilleure énergie résiduelle.

2.2 E_OLSR2

Contrairement à OLSR standard et E_OLSR1, cette extension favorise la métrique énergétique dans la sélection des relais multipoints. E_OLSR2 opte pour la capacité restante de la batterie comme critère principal dans le processus de choix des MPR. Ainsi E_OLSR2 choisira à chaque itération le voisin ayant une capacité restante d'énergie maximale jusqu' à ce que tous les voisins du second niveau soient couverts. S'il s'agit d'une égalité parfaite, cet algorithme pourra s'appuyer sur d'autres paramètres de sélection. Au deuxième niveau de sélection, le nombre maximal de voisins du second niveau couverts par ces nœuds directs égaux sera déterminant.

Formellement l'algorithme de sélection des MPR se résume comme suit :

1. Commencer par un ensemble de relais multipoint vide *MPR(x)* = {}.
2. Choisir les nœuds de l'ensemble des voisins *N(x)* qui sont les seuls à avoir un lien avec un voisin du second niveau. Ajouter ces nœuds sélectionnés de *N(x)* à l'ensemble *MPR(x)*, et éliminer tous les nœuds du second niveau couvert par ces derniers de l'ensemble *N2(x)*.
3. Tant que *N2(x)* ≠ {} faire
   (a) Calculer le degré de chaque nœud dans *N(x)*. Le degré pour un nœud est la capacité restante de la batterie. S'il y a une égalité, celui qui couvre le plus grand nombre des voisins du second niveau est choisi comme un MPR.
   (b) Ajouter le nœud de *N(x)*, ayant le degré maximal à l'ensemble des relais multipoint *MPR(x)*, et enlever tous les nœuds du second niveau couvert par celui ci de *N2(x)*.

En appliquant cet algorithme au réseau de la figure 4.1 les MPR du nœud N seraient :

Noeud_local	Voisin à 1 saut	Voisin à 2 sauts	MPR
N	A, B, C, D	E, F	A,C

TAB. 4.2 – Sélection des MPR dans E_OLSR2

Parmi les voisins directs du nœud N, c'est les nœuds A, B et C qui ont une connexion avec les voisins à deux sauts du nœud local. Le voisin A est considéré comme le meilleur en terme énergétique. Ainsi, A sera choisi comme premier MPR de N pour couvrir le nœud E du second niveau.

D'une manière identique, C est choisi comme le prochain MPR pour permettre de couvrir F, ainsi tous les voisins à deux sauts sont couverts et l'algorithme prend fin.

2.4 E_OLSR3

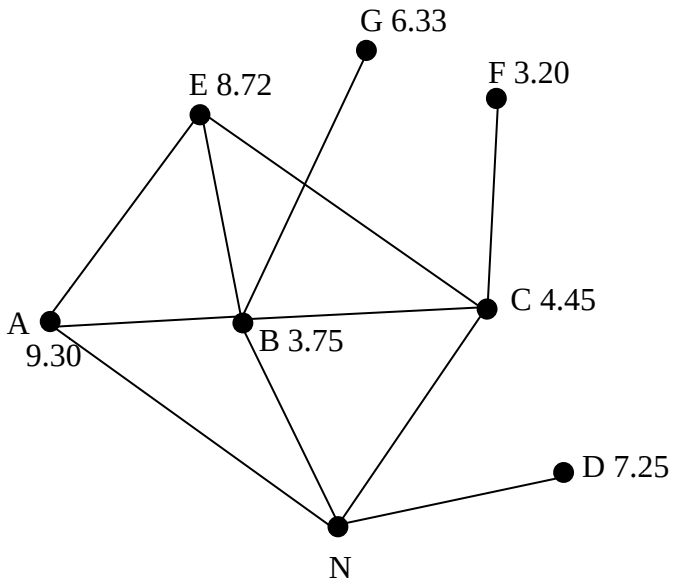


FIG. 4.2 – Exemple de réseau pour illustrer la sélection des MPR dans E_OLSR3

E_OLSR3 est une approche hybride combinant à la fois E_OLSR1 et E_OLSR2, appliquant un seuil d'énergie restante de la batterie au niveau des nœuds ($Th_r = \gamma$). Cette notion de seuil permettra au nœud d'accepter où de refuser le rôle de MPR et d'assumer la fonction de routage de données selon le principe de la technique des relais multipoints. L'idée de base est de commencer par appliquer E_OLSR1 pour les nœuds forts en énergie ($E_r \geq \gamma$). S'il s'avère que les nœuds du second niveau ne sont pas encore tous couverts alors qu'il reste seulement des voisins directs avec une capacité $E_r < \gamma$, alors E_OLSR3 basculera vers l'application d'E_OLSR2.

Ainsi, l'algorithme de choix des MPR dans E_OLSR3 est une boucle. A chaque itération, il cherche un nœud du premier niveau qui remplie la condition à la fois de couvrir le maximum de voisins du second niveau et de posséder un seuil de puissance suffisant. La boucle s'arrêtera naturellement lorsque tous les nœuds du second niveau seront couverts où bien lorsqu'il ne restera plus que des MPR ayant une énergie insuffisante. Dans ce cas, la suite de l'algorithme utilisera E_OLSR2.

Formellement l'algorithme de sélection des MPR se résume comme suit :

1. On désigne par $N1_g(x)$ l'ensemble des voisins directs de x dont l'énergie restante $E_r \geq \gamma$ et $N1_f(x)$ l'ensemble des voisins directs de x dont l'énergie restante $E_r < \gamma$.
2. Commencer par un ensemble de relais multipoint vide $MPR(x) = \{\}$.
3. Choisir les nœuds de l'ensemble des voisins $N(x)$ qui sont les seuls à avoir un lien avec un voisin du second niveau. Ajouter ces nœuds sélectionnés de $N(x)$ à l'ensemble $MPR(x)$, et éliminer tous les nœuds du second niveau couvert par ces derniers de l'ensemble $N2(x)$.
4. Tant que $N2(x) \neq \{\}$ faire

   Tant que $N1_g(x) \neq \{\}$ refaire

   (a) Calculer le degré de chaque nœud dans $N1_g(x)$. Le degré pour un nœud est le nombre des voisins du second niveau couvert par celui-ci présent dans $N2(x)$. S'il y a une égalité, celui avec la plus grande énergie résiduelle est choisi

   (b) Ajouter le nœud de $N1_g(x)$, ayant le degré maximal à l'ensemble des relais multipoint $MPR(x)$, et enlever tous les nœuds du second niveau couvert par celui-ci de $N2(x)$.

   Fin tant que

   Tant que $N1_g(x) = \{\}$ et $N2(x) \neq \{\}$ refaire

   (a) Calculer le degré de chaque nœud dans $N1_f(x)$. Le degré pour un nœud est la capacité restante de la batterie. S'il y a une égalité, celui qui couvre le plus grand nombre des voisins du second niveau est choisi comme un MPR.

   (b) Ajouter le nœud de $N1_f(x)$, ayant le degré maximal à l'ensemble des relais multipoint $MPR(x)$, et enlever tous les nœuds du second niveau couvert par celui-ci de $N2(x)$.

   Fin tant que

Pour illustrer le principe d'E_OLSR3, nous allons examiner le réseau de la figure 4.2. Le choix des MPR du nœud local N selon un seuil fixé à 4 joules serait comme suit:

Noeud_local	Voisin à 1 saut	Voisin à 2 sauts	MPR
N	A, B, C, D	E, F, G	B, C

TAB. 4.3 – Sélection des MPR dans E_OLSR3, seuil 4 joules

Entre les nœuds A, B et C, les voisins directs qui ont une connexion avec les nœuds du second niveau du nœud local N, seuls A et C sont au-dessus du seuil fixé à 4 joules. Dans un premier temps, les nœuds A et C seront les candidats prioritaires dans le processus de choix des MPR. Le nœud B ne sera pris en considération que si les nœuds A ou/et C ne parviennent

pas à couvrir tout le voisinage à deux sauts. D'abord en appliquant E_OLSR1, le nœud C sera choisi comme nœud MPR puisqu'il a 2 voisins (les nœuds F et E) à deux sauts par rapport au nœud local N tandis que A en a seulement 1 (le nœud E). Etant donné qu'il reste le nœud G à atteindre, E_OLSR3 serait contraint à basculer vers l'application du principe d'E_OLSR2. Bien que le nœud B soit en dessous du seuil fixé, il sera inclut dans l'ensemble des MPR et tout le voisinage du deuxième niveau est désormais couvert.

3. Simulation

L'étude de performances des différents algorithmes présentés dans ce chapitre ont été réalisées grâce à l'environnement de simulation NS-2 (Network Simulateur) [33]. Le choix de NS-2 pour la simulation vient de l'importance de la communauté d'utilisateurs, assurant que ce simulateur propose une modélisation relativement réaliste des phénomènes physiques et une implémentation fiable des protocoles inclus dans la distribution. Si NS est un outil largement utilisé dans la communauté scientifique, il souffre d'une documentation peu claire. Il est souvent nécessaire de reporter directement au code source du simulateur pour résoudre un problème particulier.

NS-2 intègre, dans sa version actuelle, quelques protocoles de routage pour les réseaux ad-hoc comme AODV, TORA, DSR, DSDV et bien sûr OLSR. NS-2 implémente une couche MAC et physique IEEE 802.11 qui inclut un modèle de propagation radio, des interfaces radio, et utilise le modèle CSMA comme méthode d'accès au médium. Le modèle radio prend en compte les collisions, les délais de propagation et l'atténuation du signal. La bande passante totale considérée est de 2Mbps et la portée radio de chaque nœud est de 250 mètres.

Nous simulons un réseau ad hoc composé de 36 nœuds (stations sans fil) placés au hasard (la distribution la plus proche de la réalité) dans une région de (800x800) m^2. Des connexions aléatoires sont établies entre les différents nœuds. Ces connexions sont du type CBR à 4 paquets/seconde et la taille des paquets est de 1024 octets. La capacité initiale de la batterie de chaque nœud est fixée à 10 unités. Cette énergie initiale est réduite au fur et à mesure par la transmission et la réception de données. Quand elle atteint le niveau zéro, le nœud correspondant ne peut plus participer à la communication et est considéré comme 'décédé' ou 'mort'. Pour chacun des nœuds, la consommation d'énergie est mesurée à la couche radio au cours de la simulation. Nous considérons le cas simple où la puissance de transmission est fixe. Dans ce cas-là, chaque paquet transmis ou relayé consomme une quantité fixe d'énergie.

Selon les spécifications des cartes de Lucent utilisant la norme IEEE 802.11 [34] la puissance de transmission varie entre 0.045 Watts en mode sommeil et 1.25-1.50 Watts en mode réception/transmission, respectivement. Pour obtenir l'énergie consommée instantanée, la puissance d'émission est multipliée par le temps de transmission. Par exemple, la transmission d'un paquet de données de 1024 octets consomme $6.14 * 10^{-3}$ Joules (1.50 Watts * 1024 * 8 bits / 2000000 bps). Nous faisons les deux hypothèses suivantes :

- Nous supposons que le temps nécessaire pour la réception de données est semblable au temps nécessaire pour la transmission de données dans chacun des nœuds intermédiaires. Le problème est qu'un nœud doit toujours pouvoir être à l'écoute d'un éventuel émetteur qui chercherait à le contacter, et que cette écoute est coûteuse en terme d'énergie. Cette écoute reste souvent inutilisée, et est donc purement 'parasite'. Elle peut toujours être réduite par des protocoles tels que PAMAS [22], présenté dans le chapitre précédent. Les normes de réseaux sans fil telles que l'IEEE 802.11 [35] et Bluetooth fournissent aussi un mécanisme pour que chaque nœud puisse savoir quand se réveiller et recevoir des paquets, et dormir le reste du temps. Sans cette supposition, la consommation d'énergie est dominée par une réception ou écoute abusive, et les algorithmes proposés deviennent moins avantageux ;

- En second lieu, la consommation d'énergie pendant la mise en veille a été ignorée. Puisqu'un nœud peut rester en veille pendant longtemps, une idée pour conserver l'énergie est de mettre le nœud en mode sommeil quand il est en mode veille.

La principale métrique de performances dans cette étude est la durée de vie du réseau ; c'est ce que nous avons appelé la survivabilité. Cette métrique peut être définie de différentes manières :

1- temps nécessaire pour le décès de K nœuds dans le réseau ;

2- temps nécessaire pour le décès d'un premier nœud dans le réseau ;

3- temps nécessaire pour le décès de tous les nœuds dans le réseau.

Les deux premières définitions ont été adoptées pour notre étude. La durée de vie du réseau pour les algorithmes proposés est comparée pour différents scénarios. Cette comparaison est souvent faite par rapport à OLSR puisque ces algorithmes y sont dérivés.

Nous avons testé les deux cas où : (i) les nœuds sont fixes et donc ont une mobilité nulle, et (ii) les nœuds sont mobiles et se déplacent sur la surface de simulation avec différentes vitesses de déplacement.

3.1 Nœuds fixes

La Figure 4.3 montre les moments auxquels un certain nombre de nœuds décèdent à cause de l'épuisement de leurs batteries, dans le cas où tous les nœuds du réseau ad hoc sont fixes. Nous choisissons la valeur du nombre de premiers nœuds décédés (K) entre 1 et 7 pendant un temps de simulation de 8000 secondes. Nous constatons que pour OLSR, le premier nœud meurt environ 1929 secondes plus tôt que dans E_OLSR1, 2714 secondes plus tôt que dans E_OLSR2, 3329 secondes plus tôt que dans E_OLSR3. Pareil, que pour 4 nœuds, ceux-ci

décèdent environ 857 secondes plus tôt que dans E_OLSR1, 1143 secondes plus tôt que dans E_OLSR2, et 1848 plus tôt que dans E_OLSR3.

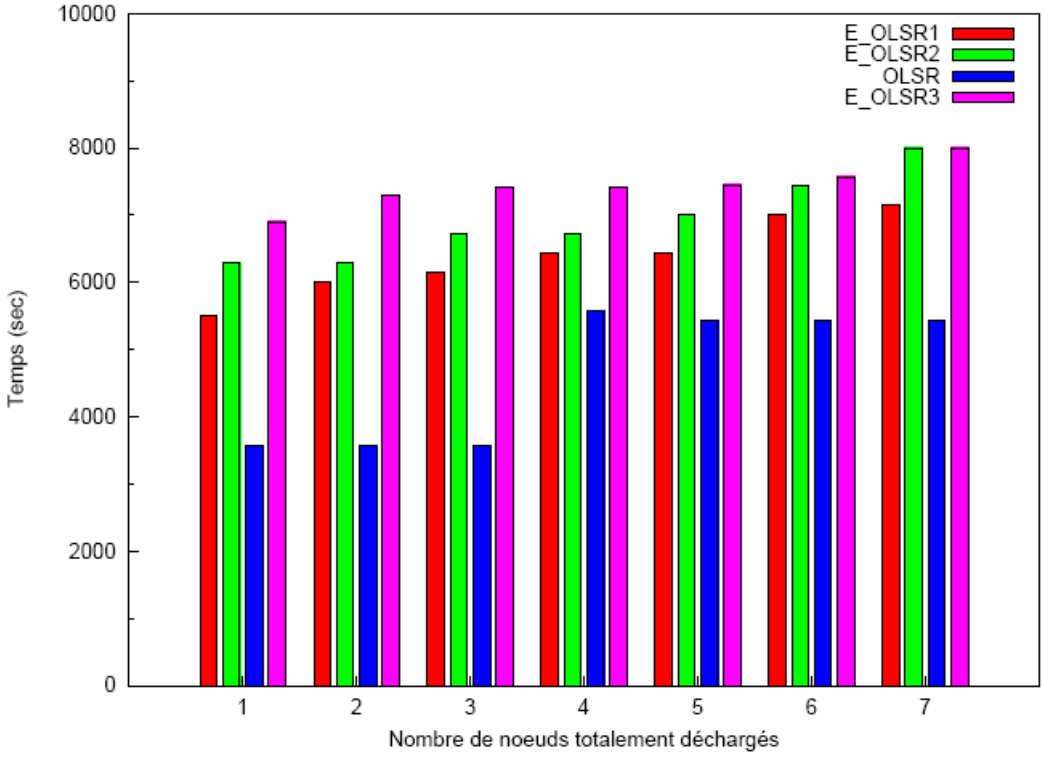


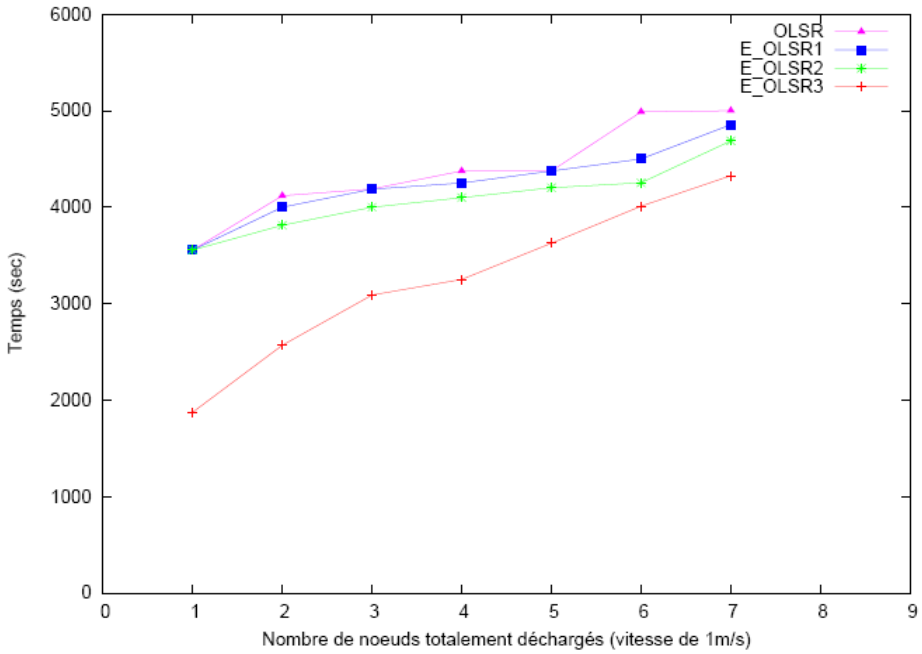
FIG. 4.3 – Le nombre de nœuds morts/temps

Nous remarquons qu'E_OLSR3 donne de meilleures performances qu'E_OLSR2. En effet, E_OLSR3 prend en compte non seulement la capacité résiduelle de la batterie mais sous condition qu'elle soit d'une quantité minimale suffisante. Or, l'algorithme E_OLSR2 utilise également comme coût la capacité résiduelle de la batterie mais sans la notion de seuil. Effectivement, cette différence au niveau de la fonction coût permet à E_OLSR3 d'avoir une prévision sur le temps de vie restant pour le nœud. Ceci peut être un bon indicateur sur le trafic passant par le nœud. Si un nœud est faible en énergie (en dessous du seuil fixé), ceci implique que ce nœud est sollicité et que le routage à travers ce même nœud peut conduire à la partition du réseau. Dans le cas ou les voisins à deux sauts ne sont pas encore couverts et que les voisins candidats MPR sont en dessous du seuil fixé, E_OLSR3 tente également de tirer profit du routage du chemin le plus court. En occurrence, E_OLSR3 minimise le nombre de nœuds impactés par le routage ce qui lui permet de creuser l'écart en matière de réduction d'énergie.

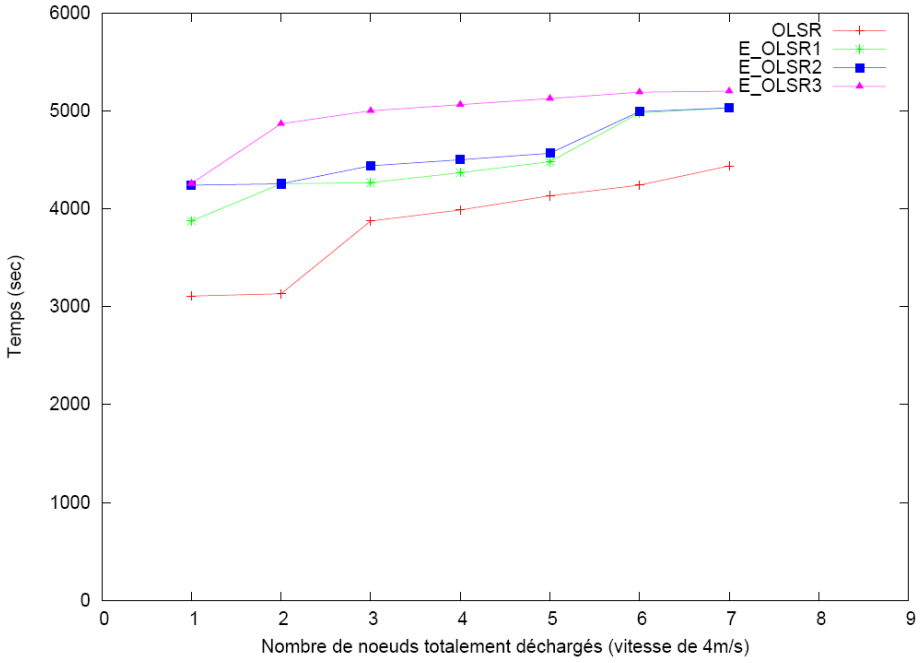
3.2 Nœuds mobiles

L'effet de la mobilité est présenté par la Figure 4.4. Nous avons comparé les performances des trois algorithmes E_OLSR1, E_OLSR2 et E_OLSR3 par rapport à OLSR. Comme nous pouvons le constater, nos algorithmes sont toujours meilleurs par rapport à OLSR en termes de nombre de nœuds décédés.

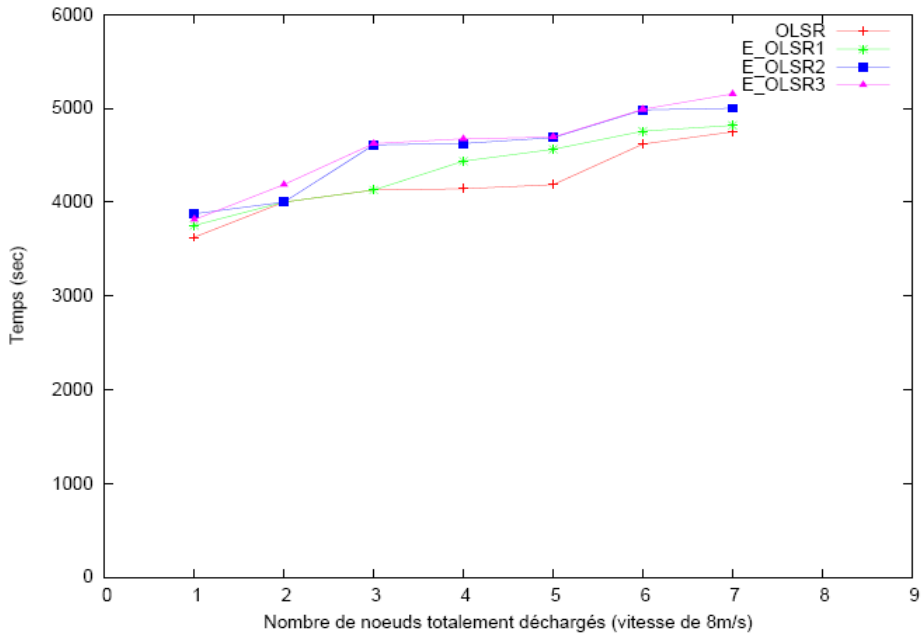
Nous constatons que pour OLSR, et pour une vitesse des nœuds égale à 4 mètres/seconde par exemple, le premier nœud meurt environ 766 secondes plus tôt que dans E_OLSR1, 1132 secondes plus tôt que dans E_OLSR2, et 1150 secondes plus tôt que dans E_OLSR3. Cette diminution de performances, par rapport au cas où les nœuds sont fixes, est tout à fait légitime. A mesure que la vitesse de déplacement des nœuds augmente, le taux de consommation d’énergie dans le réseau augmente aussi. Ceci est normal puisqu'une vitesse de déplacement plus élevée implique plus de découvertes de route, et par conséquent une consommation d'énergie plus élevée dans le réseau. En outre, à mesure que la mobilité des nœuds augmente, la différence entre OLSR et nos algorithmes devient moins importante.



(a)



(b)



(c)

FIG. 4.4 – Nombre de nœuds morts avec une vitesse (a) de 1m/s (b) 4m/s (c) 8m/s.

Afin de trouver la meilleure route disponible, les algorithmes que nous avons proposés ont besoin, lors du processus de recherche de route, de propager davantage de paquets de contrôle dans le réseau. Pour mesurer cette surcharge de signalisation, nous avons calculé le rapport entre la quantité de paquets de contrôle (en octets) et la quantité de paquets données (en octets) transmis dans le réseau pendant un temps de simulation de 6000 secondes. Nous pouvons voir, dans la Figure 4.5, les valeurs de la surcharge en fonction de la vitesse de déplacement des nœuds dans le réseau. La différence entre OLSR et nos algorithmes E_OLSR1, E_OLSR2 et E_OLSR3 croît avec la vitesse des nœuds. Ceci est dû au fait qu'en plus des mécanismes introduits dans nos algorithmes pour la sélection des MPR, s'ajoute le fait que les routes ne deviennent plus valides avec des vitesses de déplacement plus grandes.

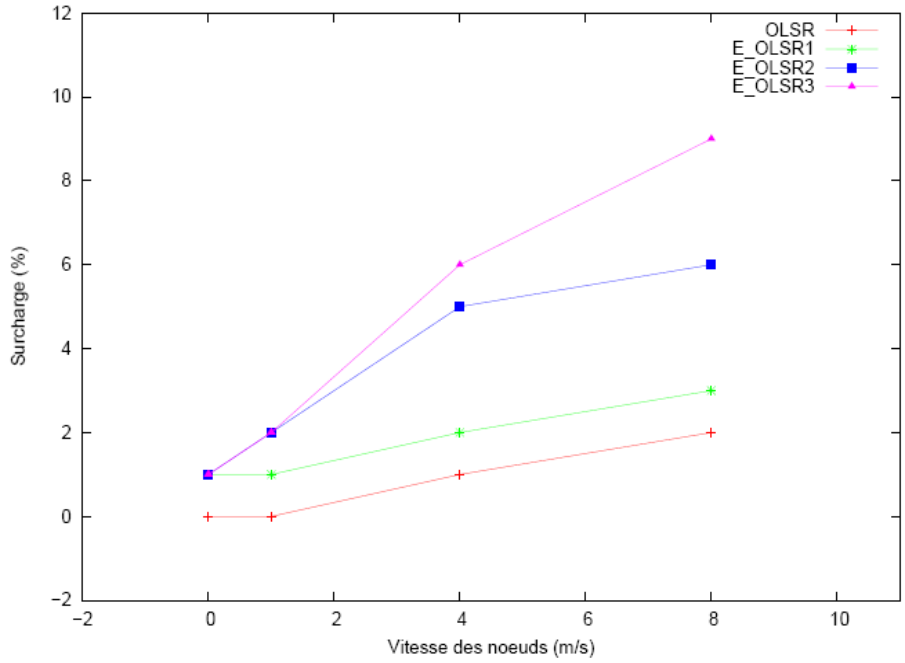


FIG. 4.5 – Surcharge de signalisation en fonction de la vitesse des nœuds

4. Conclusion

Dans ce chapitre, nous proposons trois algorithmes de routage basés sur le protocole OLSR. Les algorithmes proposés ont pour but de rallonger la vie des batteries de chaque nœud, et par conséquent la survivabilité d'un réseau ad hoc. Il est à noter que les protocoles de routage actuels normalisés à l'IETF, tels que OLSR, ne s'intéressent pas à l'impact du routage sur la

consommation d’énergie dans le réseau. Ils s'intéressent, en revanche, à trouver le plus court chemin en terme de nombres de sauts.

Nous avons comparé en terme de performance énergétique le protocole OLSR avec les trois heuristiques proposées. Dans OLSR standard les nœuds meurent plus vite que dans nos approches proposées. Bien qu’E_OLSR1 utilise pratiquement le même algorithme de sélection des MPR qu’OLSR standard, il accomplit une meilleure performance. E_OLSR1 peut ne pas trouver le plus court chemin mais le chemin le plus optimal au sens énergétique.

L’algorithme E_OLSR2 offre les meilleures routes possibles d’un point de vue énergétique au détriment de la notion traditionnelle du chemin le plus court liée au délai de transmission de bout en bout.

E_OLSR3 heuristique hybride tente de trouver un compromis entre la notion du chemin le plus court et le chemin optimal en puissance. Cette approche est basée sur la métrique de l’énergie restante des nœuds, une métrique plus précise pour décrire la durée de vie des nœuds. E_OLSR3 se distingue d’E_OLSR2 par l’application d’un seuil qui lui permet de mieux contrôler et surtout de bien équilibrer la consommation d’énergie à travers le réseau.

Les résultats de simulations prouvent bien que les mécanismes, rajoutés au protocole de routage OLSR, améliorent considérablement ses performances en terme de survivabilité du réseau. Ces mécanismes réalisent ceci avec des surcharges minimums, et sans avoir à affecter d'autres couches protocolaires. Ces heuristiques sont simples et faciles à intégrer dans le protocole de routage OLSR.

Conclusion et perspectives

1. Conclusion

Les réseaux ad hoc sont des architectures un peu particulières de réseaux locaux sans fil, basées sur des technologies comme le Wi-Fi qui permet de se connecter à Internet à haut débit dans un rayon de quelques centaines de mètres autour d'une borne radio (Station de Base - BS), elle même connectée au réseau filaire. Mais, alors que chaque utilisateur d'un réseau Wi-Fi se connecte via une borne radio, dans un réseau ad hoc, les terminaux (ordinateurs ou téléphones mobiles, etc.) peuvent aussi communiquer entre eux, sans intermédiaire, donc sans infrastructure. Ils peuvent même servir de relais les uns aux autres. C'est une sorte "d'architecture molle", évolutive et automatique. À la clef: souplesse et autonomie, puisque le réseau évolue en fonction des accès et des utilisateurs du moment. Il peut même être totalement indépendant de toute infrastructure. En outre, la portée du signal est démultipliée par le nombre d'utilisateurs, et les débits peuvent être préservés, alors qu'ils sont obligatoirement partagés avec une borne radio Wi-Fi.

Ces réseaux reposent avant tout sur les développements logiciels de nouveaux protocoles de routage "intelligents", qui prennent en compte les spécificités de ces réseaux (mobilité des terminaux, capacité limitée des batteries, etc.). Effectivement, en raison de la capacité limitée des batteries des terminaux, la consommation d'énergie devrait être un critère fondamental lors de la conception de tels algorithmes de routage. Nous avons démontré, grâce à un ensemble d'expériences, que le routage utilisé est l'un des principaux facteurs agissant sur le taux de consommation d'énergie dans ces réseaux. Il est à noter que les protocoles de routage actuels, normalisés dans le groupe MANET de l'IETF, ne prennent pas en compte la métrique consommation d'énergie pendant le processus de découverte de route. Ils s'intéressent, en revanche, à découvrir le plus court chemin. La métrique consommation d'énergie, peut s'avérer plus efficace. D'autant que cette nouvelle métrique n'est pas forcément un frein à la rapidité du processus de routage. Autrement dit, une métrique basée sur la consommation d'énergie permettrait d'augmenter la durée de vie du réseau ; c'est probablement le facteur principal pour pouvoir communiquer.

Dans ce mémoire, nous nous sommes intéressés à ces réseaux et, en particulier, à la manière d'étendre les protocoles de routage actuels en prenant comme objectif de rallonger la durée de vie des batteries, et par conséquent la survivabilité du réseau. Pour ce faire, nous avons proposé trois nouveaux algorithmes de routage E_OLSR1, E_OLSR2 et E_OLSR3 basés sur l'un des plus importants protocoles de routage actuels qui est OLSR. Ce dernier, ne considère pas la contrainte de l'énergie pour optimiser le routage, mais cherche plutôt, le chemin le plus court en terme de sauts.

Ces solutions prennent en compte une métrique basée sur la consommation d'énergie lors de la détection des MPR. Ces extensions 'énergétiques' d'OLSR, sont des solutions simples, et l'ensemble des résultats de simulations démontre clairement, qu'elles améliorent considérablement ses performances en améliorant la survivabilité du réseau. Elles réalisent cet objectif avec des surcharges minimes, et sans avoir à affecter les autres couches protocolaires. Ces algorithmes équilibrent la consommation d'énergie sur la totalité du réseau.

Si le simulateur NS-2 utilisé pour obtenir les résultats de ce document est reconnu dans la communauté scientifique comme étant proche du monde réel, beaucoup de simplifications y sont faites. Certains phénomènes, comme la propagation des ondes radio sont mal compris ou difficiles à modéliser. Par exemple, NS ne permet pas de modéliser la présence d'obstacles tels que des murs dans l'environnement [36]. C'est pourquoi il sera nécessaire d'effectuer les mêmes tests sur une implémentation réelle d'OLSR.

2. Perspectives

Le monde des réseaux ad hoc sans fil est encore en phase de gestation. Plusieurs domaines et axes de recherches intéressants liés à ce type de réseau restent à explorer et auxquels il faudra trouver des réponses adéquates. Ci-dessous quelques axes de recherche à explorer :

- Les protocoles de routage ad hoc sans fil, et en particulier OLSR sont conçus pour des réseaux locaux, mais, il est très intéressant de regarder le routage pour des réseaux encore plus grands.

- Réfléchir à introduire d'autres mécanismes de qualité de service en fonction du routage entre les différents utilisateurs et suivant les contraintes de chacun.

- Une deuxième voie de recherche très liée à la première, serait, l'étude du routage fiable et les applications multimédia (comme la vidéoconférence par exemple) qui demandent souvent une certaine qualité de service. On aura besoin aussi d'introduire des mécanismes de contrôle d'admission, afin, de garantir un bon service.

- Un autre axe de recherche serait d'étudier la sécurité dans les réseaux ad hoc sans fil qui sont très fragiles et vulnérables aux attaques. Des mécanismes d'authentification et de cryptage doivent être mis en œuvre pour se protéger contre les attaques visant à

- espionner le réseau ou bien perturber son fonctionnement en diffusant de fausses informations par exemple. L'intégrité du réseau doit être assurée en renforçant la sécurité.

Bibliographie

[1] Internet Engineering Task Force (IETF), Mobile Ad-hoc Networks (MANET), http://www.ietf.org/html.charters/manet-charter.html

[2] M. Rahnema, "Overview of the gsm system and protocol architecture", *IEEE Communications Magazine*, vol.31, no.4, pp. 92–100, April 1993.

[3] Z.J. Haas and S. Tabrizi. "On some challenges and design choices in ad-hoc communications", In *IEEE MILCOM'98*, pp. 18-21, October 1998.

[4] IEEE 802.11, 1999 Edition (ISO/IEC 8802-11: 1999) IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements - Part 11 : Wireless LAN Medium, Access Control (MAC) and Physical Layer (PHY) Specifications.

[5] IEEE Computer Society LAN MAN Standards Committee, Wireless LAN Medium Access Control (MAC) and Physical Layer (phy) specifications, *IEEE Std. 802.11-1197*.

[6] D.B. Johnson, Y. Hu, D.A. Maltz, "The Dynamic Source Routing protocol (DSR) for Mobile Ad hoc Networks, *IETF Intenet Draft*, http://www.ietf.org./rfc4728.txt, February 2009.

[7] C. Perkins and E. Belding-Royer and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing", *IETF Intenet Draft*, http://www.ietf.org/rfc/rfc3561.txt, July 2003.

[8] C. Perkins and E. Royer "Ad-hoc On-Demand Distance Vector Routing", *Proc. Second Annual IEEE Workshop on Mobile Computing Systems and Applications*, pp. 90–100, February 1999.

[9] C. Huitema, "Routing in the Internet", *Prentice Hall*, April 1995.

[10] T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol (OLSR)", *IETF Intenet Draft*, http://www.ietf.org/rfc/rfc3626.txt, October 2003.

[11] A. QUAYUM T, A. Laouit and L. Viennot "Multipoint relaying technique for flooding broadcast messages in mobile wireless networks", *Proc. HICSS'02*, January 2002.

[12] C. E. Perkins et P. Bhagwat, "Highly dynamic Destination-Sequenced Distance-Vector routing for mobile computers", *Proc. ACM SIGCOMM'94*, pp. 234-244, October 1994.

[13] Z.J. Haas and M.R. Pearlman "The performance of query control schemes for the zone routing protocol", *Proc. ACM SIGCOMM'98*, vol. 28, no.4, pp. 167-177, October, 1998.

[14] T. Clausen, P. Jacquet and L. Viennot, "Comparative study of routing protocols for mobile ad-hoc networks", *Proc. of The First Annual Mediterranean Ad Hoc Networking Workshop*, September 2002.

[15] S. Papanastasiou, L. M. Mackenzie, M. Ould-Khaoua and Vassilis Charissis, "On the interaction of TCP and routing protocols in MANETs", *Proc. IEEE Computer Society AICT-ICIW'06*, pp. 62, February 2006.

[16] Wolfgang Kiess and Martin Mauve, "A Survey on Real-World Implementations of Mobile Ad-Hoc Networks", *Elsevier's Ad Hoc Networks*, vol.5, no.3, pp. 324-339, April 2007.

[17] J.C. Mogul, "Broadcasting Internet datagrams in the presence of subnets", *RFC 922*, October 1984.

[18] P. Jacquet, P. Minet, P. Mühlethaler and N. Rivierre, "Increasing reliability in cable-free radio LANs - Low level forwarding in HIPERLAN", *Wireless Personal Communication*, vol.4, no.1, pp. 51-63, January 1997.

[19] M. Stemm and R.H. Katz, "Measuring and reducing energy consumption of network interfaces in hand-held devices", *IEICE Transactions on Fundamentals of Electronics, Communications, and Computer Science*, vol.E80-B, no.8, pp. 1125-1131, 1997.

[20] C.E. Jones, K.M. Sivalingam, P. Agrawal and J. C. Chen, "A survey of energy efficient network Protocols for wireless Networks", *in Wireless Networks*, vol. 7, no. 4, pp. 343-358, July 2001.

[21] K.M. Sivalingam, J.C. Chen, P. Agrawal and M. Sivastava, "Design and analysis of lower-power access protocols for wireless and mobile ATM networks", *ACM/Blatzer Wierless Networks* vol.6, no.1, pp. 73-87, February 2000.

[22] S. Singh and C.S. Raghavendra, "PAMAS - power aware multi-access protocol with signalling for ad hoc networks", *ACM Computer Communication Review*,vol.28, no.3, pp. 5-26, July 1998.

[23] P. Kam, "MACA - a New Channel Access Method for Packet Radio", *Proc. ARRL/CRRL Amateur Radio 9th Computer Networking Conference*, pp. 134-140, September 1990.

[24] M. Zorzi and R.R. Rao, "Error control and energy consumption in communications for nomadic computing", *IEEE Transactions on Computers*, vol.46, no.3, pp. 279-289, March 1997.

[25] P. Lettieri, C. Fragouli and M.B. Srivastava, "Low power error control for wireless links", *Proc. of 3rd Annual ACM/IEEE MOBICOM'97*, pp. 139–150, September 1997.

[26] S. Ni, Y. Tseng, Y. Chen et J. Chen, "The broadcast storm problem in a mobile ad hoc network", *Proc. of the Fifth Annual ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM'99)*, pp. 151-162, August 1999.

[27] D. Kim, J. Park, C.K Toh and Y. Choi "Power-aware route maintenance protocol for mobile ad hoc networks", *Proc. IEEE International Conference on Telecommunications (ICT)*, vol.1, pp. 501-506, March 2003.

[28] D. Kim, J.J. Garcia-Luna-Aceves, K. Obraczka, J-C. Cano, and P. Manzoni, "Performance Analysis of Power-Aware Route Selection Protocols in Mobile Ad Hoc Networks", *Proc. IEEE Networks 2002*, pp. 26-29, August 2002.

[29] M. Maleki, K. Dantu and M. Pedram, "Power-aware source routing protocol for mobile ad hoc networks", *Proceedings of ISLPED'02*, pp. 72-75, August 2002.

[30] M. Zorzi and R.R. Rao, "Energy efficiency of TCP in a local wireless environment", *Mobile Networks and Applications*, vol.6, no.3, p. 265-278, June 2001.

[31] Intel Corporation, Microsoft Corporation, Phoenix Technologies Ltd., Toshiba Corporation, "Advanced Configuration and Power Interface", Source Internet : http://www.acpi.info/spec30a.htm, December 2005.

[32] P. Agrawal, J.C. Chen, S. Kishore, P. Ramanathan and K.M. Siva-lingam, "Battery power sensitive video processing in wireless networking", *Proc. of IEEE* PIMRC'98, September 1998.

[33] The Network Simulator ns-2, http://www.isi.edu/nsnam/ns/

[34] A. Kamerman and L. Monteban, "WaveLAN-II: A High-Performance Wireless LAN for the Unlicensed Band", *Bell Labs Technical Journal*, vol.2, no.3, pp. 118-133, Summer 1997.

[35] H. WOESNER, J-P. EBERT, M. SCHLAGER and A. WOLISZ, "Power-Saving Mechanisms in Emerging Standards for Wireless LANs: The MAC Level Perspective", *IEEE Personal Communications*, vol.5, no.3, pp. 40-48, June 1998.

[36] C. CHAUDET "Influence des interférences sur les problèmes de réservation de bande passante dans les réseaux ad-hoc", *Rapport de DEA*, ENS, Juin 2001.

[37] C. ELORRIETA, "Protocoles de routage pour l'interconnnexion des réseaux ad-hoc et UMTS", *Rapport de Licence*, ULB, Juin 2007.

[38] T. LEMLOUMA, "Le Routage dans les réseaux Mobiles ad-hoc", Rapport de Master, USTHB, Septembre 2000.

Publication

[1] N. GHANEM, N.GHOUALMI, "Routage et Conservation d'Energie dans les Réseaux Mobiles Ad hoc utilisant OLSR", *ICSIP'09*, 02-03 Mai 2009.

[2] N. GHANEM, N.GHOUALMI, "Routage et Conservation d'Energie dans les Réseaux Mobiles Ad hoc utilisant OLSR", *CNTA'09*, 23-24 Mai 2009.