Accès, routage et sécurisation pour les réseaux sans fil : une nouvelle approche

Marc Gilg

IRIMAS UNIVERSITÉ HAUTE-ALSACE
Institut de Recherche en Informatique, Mathématiques, Automatique et Signal

université de Haute-Alsace

habilitation à diriger les recherches

*S*pécialité : Informatique

Présenté par :

Marc GILG

Accès, routage et sécurisation pour les réseaux sans fil : une nouvelle approche

---

Soutenue le 26/11/2018 devant le jury composé de :

Président	Ye-Qiong SONG	Prof, Université de Lorraine
Rapporteurs	Mourad GUEROUI	Prof, Université de Versailles
	Hervé GUYENNET	Prof, Université de Franche-Comté
	Ahmed SERHROUCHNI	Prof, Telecom-ParisTech
Garant	Pascal LORENZ	Prof, Université de Haute-Alsace

Remerciements

Je remercie mes parents pour leur soutien pendant toutes ces années.

Je remercie le professeur Pascal Lorenz qui m'a accuelli dans son équipe et m'a encouragé à me présenter à l'Habilitation à Diriger les Recherches.

Je remercie les différents membres de l'équipe Réseaux et Télécommunications de Colmar et du laboratoire IRIMAS, ainsi que les doctorants, sans qui ce travail n'aurait pas pu être fait.

Je remercie Jean et Nicole Perrin qui ont relu ce mémoire et qui m'ont aidé à le structurer.

Je remercie les rapporteurs le Professeur Mourad GUEROUI de l'Université de Versailles, le Professeur Hervé GUYENNET, de l'Université de Franche-Comté, et le Professeur Ahmed SERHROUCHNI de l'école Telecom-ParisTech, qui ont accepté d'évaluer ce travail et qui sont membres du jury.

Je remercie le Professeur Ye-Qiong SONG d'avoir présidé le jury.

Table des matières

Table des figures

Chapitre 1

Introduction Générale

1.1 Introduction

Ce mémoire est présenté pour obtenir l'Habilitation à Diriger les Recherches en Informatique. L'activité de recherche a été faite, depuis 2006, dans l'équipe Réseaux et Télécommunications, sous la direction du Professeur Pascal Lorenz, du laboratoire IRIMAS de l'Université de Haute-Alsace. Les travaux présentés se focalisent sur **la partie accès et routage pour les réseaux sans fils**, notamment Ad-Hoc et réseaux de capteurs. Ne sont donc *pas présents les travaux de recherches en Mathématiques que j'ai présentés lors de ma Thèse en Algèbre, ni les travaux faits récemment sur la thématique des bâtiments intelligents*, bien que cette dernière thématique soit présente dans les sujets proposés pour une recherche future.

Venant d'un cursus en Mathématique pure, j'ai travaillé après ma thèse en tant qu'Ingénieur de Recherche au Centre de Ressources Informatiques de l'Université de Haute-Alsace, sous la direction de monsieur Romuald Greisner. Cette transition m'a permis d'acquérir une connaissance opérationnelle des réseaux et de leur exploitation. Mais **ma recherche a été influencée par mon passé de mathématicien**, ce qui m'a permis d'avoir une approche originale sur la thématique de la qualité de service dans les réseaux sans fils.

1.2 Contexte

Les réseaux sans fils se répartissent en deux familles : les réseaux d'infrastructures et les réseaux Ad-Hoc. Les réseaux d'infrastructures sont le plus utilisés et sont composés d'équipements mobiles, qui se connectent à une borne pour obtenir, par exemple, une connectivité internet. Ce type de réseaux n'est pas étudié dans ce mémoire.

Les réseaux Ad-Hoc sont composés de mobiles qui établissent des communications point à point entre eux. **Ces réseaux sont soumis à plusieurs contraintes** :

— *Des contraintes physiques* dues à la limitation des ressources d'un noeud. Les ressources peuvent être des ressources de calcul, de mémoire, ou des ressources énergétiques
— *Des contraintes liées à l'utilisation d'un lien radio.* Parmi ces contraintes on trouve l'impossibilité d'utiliser une même fréquence par plusieurs mobiles à la fois, ou des problèmes d'interférences entre plusieurs émetteurs. Ces contraintes sont prises en compte dans les méthodes d'accès et l'ordonnancement des transmissions
— *Des contraintes liées à la topologie du réseau.* Si la communication directe entre deux noeuds est triviale, pour des noeuds éloignés, c'est plus complexe. Une des solutions est d'utiliser

des noeuds intermédiaires pour acheminer les communications. Ici se pose la question de la construction d'un chemin entre la source et la destination, et de la maintenance de ce lien en cas de mobilité des noeuds.
— *Des contraintes applicatives* : contraintes du temps réel, du temps d'acheminement, du volume de données, de la sécurité des échanges

Certaines de ces contraintes sont primordiales pour certains types de réseaux Ad-Hoc. Par exemple, pour les réseaux de capteurs sans fils, la contrainte des *ressources énergétiques* doit être prise en compte. Un capteur étant alimenté par batterie, sa durée de vie dépend donc de sa consommation énergétique.

1.3 Axe de recherche

Si l'ensemble des contributions présentés dans ce mémoire concerne les réseaux Ad-Hoc et les réseaux de capteurs sans fils, l'approche que j'ai utilisée est inhabituelle. L'ensemble des solutions que nous proposons est **fortement influencée par mon passé de mathématicien**. Nous sortons du cadre classique : problématiques, algorithmes, protocoles et validation par simulations **pour avoir une approche plus théorique des problématiques de qualité de service**.

Ainsi, des outils comme **la théorie des graphes, le traitement d'images ou les déformations** sont utilisés pour proposer des solutions originales. L'axe de recherche que nous proposons ici est de trouver de nouvelles approches venant de différentes thématiques pour apporter un aspect théorique aux problèmes d'accès, de routage et de sécurisation des réseaux Ad-Hoc.

Nous proposons aussi de *poursuivre ces travaux en incluant de nouvelles méthodes provenant des recherches sur l'intelligence artificielle, l'apprentissage profond et la fouille de données.*

1.4 Contributions

Une première problématique étudiée est **la congestion**, ainsi que **l'équité d'accès** des réseaux Ad-Hoc. La notion de **clique**, provenant de la théorie des graphes, a permis de construire un algorithme d'accès [GL04] limitant la congestion des réseaux Ad-Hoc.

Ces travaux ont été poursuivis avec un étudiant, Monsieur Abderrahim MAKLHOUF, qui a soutenu sa Thèse le 20 juillet 2009. Dans son travail, une approche théorique est menée à l'aide d'un **index d'équité**, qui permet de mesurer si un réseau est équitable ou non. Nous avons évalué cet index de manière théorique pour des réseaux constitués de **réseaux en étoile**. Il a été **démontré que l'équité n'est pas possible pour des réseaux autres que les réseaux consitués d'une seule étoile** [GLM08, MGL09, GML09]. Malgré cette limitation théorique, des algorithmes d'accès ont été proposés pour atteindre un index d'équité maximale.

Avec un autre étudiant en Thèse, Monsieur Yaser YOUSEF, nous nous sommes penché sur des Réseaux Ad-Hoc particuliers : les réseaux de capteurs sans fils. La thèse a été soutenue le 8 Juillet 2010. Dans cette configuration, les noeuds sont des capteurs alimentés avec des batteries. Cette limitation énergétique implique un coût pour la transmission et la réception de paquets. Le choix de la route devient crucial et peut écourter la durée de vie de certain capteurs. Pour construire des routes respectueuses de la consommation d'énergie, nous avons utilisé **une image en niveau de gris pour modéliser le réseau et sa répartition énergétique**. Cette approche innovante a permis la construction de **protocoles de routage utilisant des algorithmes de traitement d'images** [GYL09, YGL10b, YGL10a]. Suite à ces travaux, une approche utilisant les déformations de routes a été proposée pour créer des protocoles de routage [Gil17].

Avec le Doctorant Amir Abdelkader ALOUIZ, arrivé en 2017, nous nous sommes intéressés à

un algorithme de routage réactif : AOMDV. Ce protocole est une modification du protocole AODV et permet de construire à la demande une table de routage avec plusieurs chemins. Nous avons fait évoluer ce protocole en introduisant **un algorithme qui permet de tenir compte de la consommation d'énergie le long d'un chemin** [AHLG18].

Finalement, avec le doctorant Kamel SADDIKI, coencadré depuis 2017, nous nous sommes intéressés au protocole de routage proactif OLSR. Ce protocole utilise des noeuds particulier MPR pour transmettre les informations sur la topologie du réseau et pour acheminer le trafic. Ce protocole est vulnérable, car un noeud malveillant peut se faire désigner comme un noeud MPR. Nous avons proposé **une métrique pour détecter la déclaration de liens fictifs et un protocole utilisant cette détection pour limiter l'action malveillante** [LGSH17]. Une deuxième publication a été acceptée, qui prend en compte *une attaque coordonnée* de noeuds malveillants [SBHLG18].

1.5 Plan

Après cette introduction, je décris mon parcours professionnel et universitaire. Mes activités de recherche sont présentées, notamment mes **coencadrements de thèses**, mes **publications**, ainsi que mes activités de **relectures**. Puis mes activités d'**enseignements** et mes engagements **administratifs** terminent ce chapitre.

Après cette présentation, mes travaux de recherche dans le domaine des réseaux sans fils sont détaillés. Les travaux sont présentés dans **un ordre chronologique**, mais **cet ordre correspond aussi au positionnement dans la couche OSI**. Tout d'abord les contributions sur la *couche d'accès* sont données : limitation de la congestion des réseaux Ad-Hoc et équité d'accès forment les chapitres 3 et 4. Le chapitre 5 présente une *évolution vers la couche réseau* en s'intéressant au routage. Le réseau évolue aussi et devient *réseau de capteurs*. Ce chapitre présente une approche originale en utilisant une **analogie réseaux/images**. Les chapitres 6 et 7 sont des études plus classiques sur les **protocoles de routage** pour les réseaux sans fils. Le chapitre 6 présente une amélioration d'un **algorithme de routage réactif** AOMDV, et le chapitre 7 une amélioration de la **sécurité** d'un **algorithme proactif** OLSR. Le Chapitre 8 donnera un résumé et des projets futurs. Finalement, une conclusion présentera mon projet en tant qu'≪Habilité≫.

Chapitre 2

Curriculum vitae

2.1 État civil

Marc GILG
Né le 3 Juillet 1970 à Colmar
Maître de Conférence depuis 2006
Hors Classe au contingent national depuis le 1er Septembre 2018

2.1.1 Adresse professionnelle

Département Réseaux & Télécommunications
Institut Universitaire Technologique
34 rue du Grillenbreit
BP 50568
68 008 COLMAR Cedex
Tel : 03 89 20 23 68
courriel : marc.gilg@uha.fr

2.1.2 Laboratoire d'affectation

Groupe de Recherche en Télécommunications de Colmar (GRTC)
Laboratoire IRIMAS
EA 2332
IUT de Colmar

2.1.3 Parcours Universitaire

- 1988 Baccalauréat C, lycée St André Colmar
- 1988-1989 Math Sup, Lycée Albert Schweitzer, Mulhouse
- 1989-1990 Math Spé M, Lycée Albert Schweitzer, Mulhouse
- 1990-1991 DEUG2 Science, Université de Haute-Alsace, Colmar, mention Assez-Bien
- 1991-1992 Licence de Mathématiques, Université de Haute-Alsace, Mulhouse, mention Assez-Bien

— 1992-1993 **Maîtrise** de Mathématique, Université de Haute-Alsace, Mulhouse, mention Bien Maîtrise (faite dans le cadre **ERASMUS**) à L'**Université d'Edimbourg**, Ecosse, Grande Bretagne
— 1993-1994 Diplôme d'Etude Approfondie en Mathématiques, Université de Haute-Alsace Mulhouse et Université Louis Pasteur Strasbourg, mention Très Bien.
— 1995-1996 Service National en Coopération, Enseignant en mathématique au Lycée Moderne, Odienne, Côte d'Ivoire
— 1996-2000 Etudiant en Doctorat de Mathématique.
Thèse soutenue le 19 Mail 2000 ayant comme titre : **Super-Algébres de Lie Nilpotentes** devant le jury :
M. Goze (Président), Yu. Khakimdjanov (Directeur) M. Bordemann (rapporteur), J. R. Gomez (rapporteur), A. Medina (rapporteur), A. Makhlouf, Mention Très Honorable.

2.1.4 Parcours Professionnel

J'ai exercé les activités suivantes avant ma titularisation dans l'éducation nationale :
— Du 01/09/96 au 31/08/98, Enseignant Vacataire et Tuteur, Université de Haute-Alsace
— Du 01/09/98 au 31/08/99, Attaché Temporaire d'Education de Recherche (ATER), Université de Haute-Alsace
— DU 13/06/00 au 26/06/00, Technicien Informatique Vacataire, Université de Haute-Alsace
— Du 23/08/00 au 22/11/00, Technicien Informatique, Infoservice, Colmar
— Du 23/11/00 au 31/08/01, Ingénieur de Recherche Contractuel, Université de Haute-Alsace
— Du 01/09/01 au 31/08/02, Ingénieur de Recherche Stagiaire, Université Louis Pasteur, IUT de Schiltigheim
— Du 01/09/02 au 31/08/06, Ingénieur de Recherche Titulaire, Université de Haute-Alsace.

2.1.5 Réseaux Sociaux

ORCID : https ://orcid.org/0000-0003-4322-4947
PUBLONS : https ://publons.com/a/1359726/

2.2 Carrière

Après l'obtention de mon **doctorat de mathématiques le 19 Mai 2000, spécialité algèbre**, j'ai rejoint le Centre de Ressource Informatique de l'Université de Haute-Alsace en tant qu'Ingénieur de Recherche (IGR). J'ai réussi le **Concours d'IGR** et j'ai occupé ce poste jusqu'en 2006. Pendant cette période, j'ai effectué des tâches d'Administrateur Système Linux et réseaux. J'étais aussi Responsable de la Sécurité des Systèmes d'Information Adjoint (RSSIa). Parallèlement à cette activité administrative, j'ai commencé une **activité de recherche sur les réseaux Ad-Hoc** dans le Groupe de Recherche en Télécommunication de Colmar. Cela m'a permis d'être **requalifié en section 27 (Informatique)** ; précédemment j'étais qualifié en section 25 (mathématique).

J'ai réussi le **concours de Maître de Conférence en Informatique** en 2006. Depuis cette date je suis affecté à l'IUT de Colmar au Département Réseaux et Télécommunications. Parallèlement à cette activité, j'ai gardé des **tâches administratives en rapport avec mon ancien poste d'ingénieur**.

J'ai été **chargé de mission pour la migration du système téléphonique** de l'Université vers la téléphonie sur IP en 2006. Je suis **membre de la Commission Paritaire d'Établissement (CPE)** en tant que représentant de l'établissement pour le corps ITARF. Depuis 2007 je suis **RSSI titulaire** de l'Université. Le Président de l'Université m'a aussi nommé au poste de **Fonction-**

naire de Sécurité et de Défense (FSD) de l'Université de Haute-Alsace. De 2012 à 2015 j'ai été **Chef de Département** Réseaux et Télécommunication et de 2012 à 2016 **élu à la Commission de Recherche et au Conseil Académique** de l'Université de Haute-Alsace.

Ce parcours un peu atypique m'a permis de **découvrir différentes facettes de l'Université**. J'ai changé de discipline, passant des Mathématiques pures à l'Ingénierie et l'Informatique. Cette **double compétence me permet d'aborder les problématiques réseaux avec un regard formel**, apportant une **nouvelle approche**. Ceci c'est notamment illustré par l'encadrement de **deux thèses soutenues**, et par la rédaction d'un chapitre de livre en 2017. Actuellement, je **coencadre 6 thèses** en collaboration avec l'Algérie, sur les thématiques de la sécurité des réseaux utilisant le protocole de routage OLSR, sur les bâtiments intelligents et la domotique, ainsi que sur la sécurité des réseaux véhiculaires.

Au niveau enseignement, mon expérience d'Ingénieur de Recherche en réseaux (ITRF BAP E) est mise à profit dans le domaine des réseaux et télécommunications. Mes cours couvrent les niveaux DUT, 1ère et 2ème année, Licence professionnelle et Master première et deuxième année. Ces cours peuvent être regroupés en **trois thématiques** : Système Linux, virtualisation et nuages, Routage et IOS Cisco, Sécurité des Systèmes d'Information. Lors de mon mandat de Chef de Département en Réseaux et Télécommunications de l'IUT de Colmar, j'ai assuré la gestion du Département.

Au niveau national, je suis **vice-président pour la région Grand-EST de l'association CybertEdu**. Cette association, créée par l'Agence Nationale de la Sécurité des Systèmes d'Informations (ANSSI) a pour but d'introduire les notions de sécurité dans l'ensemble des formations dans le domaine du numérique en France. Dans ce cadre j'ai **organisé un colloque** pour les collègues du Grand-Est le 19 Juin 2018 à Colmar, portant sur *le chiffrement et la sécurité des logiciels embarqués*.

Suite à mon emploi d'Ingénieur de Recherche, j'ai conservé des tâches administratives au niveau de l'établissement. Je suis **Responsable de la Sécurité des Systèmes d'Information** Titulaire depuis 2007. En prolongement de cette mission, la Présidente de l'Université m'a nommé **Fonctionnaire Sécurité Défense** (FSD) de l'établissement. Depuis 2018, je suis **Auditeur** auprès de l'**Institut des Hautes Études de la Défense Nationale (IHEDN)**.

2.3 Activités de recherche

2.3.1 Présentation des thématiques de recherche

Congestion des réseaux

A partir de 2005 j'ai réalisé des travaux portant sur les réseaux Ad-Hoc. On y a notamment étudié **la congestion des réseaux et l'optimisation de la bande passante**. Les travaux que nous avons réalisés s'appuient sur la Théorie des Graphes, en particulier celle des cliques maximales, pour apporter une solution à la congestion tout en essayant de préserver la bande passante. Deux algorithmes d'accès ont été développés. Ces algorithmes ont été présentés lors de deux Conférences internationales avec comités de lectures [GL04, GL05]

Equité d'accès

A la suite de cette recherche, nous nous sommes intéressés à l'**équité d'accès dans les réseaux Ad-Hoc**. Nous avons formalisé un index d'équité pour mesurer la disparité d'émission des nœuds dans les réseaux Ad-Hoc. De manière théorique, cet index a été calculé pour des réseaux de type

étoile et double-étoile. Il a été *démontré que l'équité parfaite ne peut pas être obtenue dans un réseau double-étoile*. Finalement un *algorithme d'accès* a été donné. Ces travaux ont fait l'objet d'une **Thèse en 2009**, que j'ai co-encadrée et de **deux communications** dans des Conférences internationales avec Comité de Lecture en 2008, dont une a reçu un prix **Best paper Award** [GLM08, MGL09] et a fait l'objet d'un article dans un journal international en 2009 [GML09].

Réseaux de capteurs

Suite à ces travaux, j'ai **élargi mon champ de recherche aux réseaux de capteurs**. Ces réseaux sont des réseaux Ad-Hoc particuliers dont les nœuds ont une alimentation sur batterie, avec une capacité limitée. Le but de nos travaux a été de *trouver des protocoles de routage prenant en compte cette capacité énergétique, pour construire des routes optimisant la durée de vie du réseau.*

Une approche originale, utilisant une représentation des réseaux par des **images en niveaux de gris**, a permis la construction de *protocoles de routage utilisant des algorithmes de traitements d'image.*

Une **Thèse a été soutenue suite à ces travaux en 2010**. **Deux communications** ont été faites dans des Conférences internationales avec Comité de Lectures en 2010 et 2011, [GYL09, YGL10b] ainsi qu'**une publication d'article dans un journal international** [YGL10a].

Finalement l'ensemble de ces travaux a été présenté dans un **chapitre** d'un ouvrage collectif en 2017 [Gil17].

De 2012 à 2016 j'ai été Chef de Département d'IUT. Pendant cette période il y a eu inévitablement une baisse de mon activité de recherche.

Réseaux domotiques

Depuis 2015, je co-encadre une Thèse algérienne dans le domaine des **bâtiments intelligents**. Le but de cette Thèse est, en écoutant le trafic d'un réseau domotique, type KNX, de *découvrir des scénarios pour automatiser certaines tâches.* Cette thèse fait appel à la **Théorie des Croyances**. **Un article a été accepté dans un journal international** [CGLL18].

Sécurité des réseaux

Depuis 2017, je co-encadre 3 Thèses algériennes portant sur **la sécurisation du protocole de routage OLSR**. Ces thèses s'intéressent à différents aspects d'attaques des réseaux OLSR, effectués par des nœuds malveillants. **Une publication a été réalisée dans un journal international en 2017** [LGSH17], et une autre a été acceptée pour une conférence en 2018 [SBHLG18].

Depuis 2017, je co-encadre une Thèse algérienne sur la **Sécurité des Réseaux Véhiculaires**. Dans cette thèse nous *adaptons le protocole d'anonymat I2P au réseau des VANET* et nous nous intéressons à l'**échange des clés et la construction de tunnels**.

Coopération internationalle

Je participe activement au **groupe EUCOR** : EUCOR regroupe cinq Universités du Rhin Supérieur. Le cluster « Upper Rhine Cluster for sustainability research (URCforSR) », et particulièrement l'axe 2 : « Sustainable Buldings », inclut des aspects domotiques et de bâtiments

intelligents, un axe de recherche que je souhaite développer. L'internet des objets est aussi une composante qui interagit avec ces réseaux domotiques. Il y a donc des protocoles à dévellopper.

2.3.2 Encadrement de thèses

Accompagner les Doctorants

Fonctions Pédagogiques

J'ai accompagné **8 Doctorants** venant de pays différents : un Marocain, un Syrien et six Algériens. Le financement de leur thèse est fait par leur pays d'origine. Cela implique que **leur sujet est imposé** en fonction des priorités d'application définies en amont. Bien que je n'aie pas contribué au sujet, je dois m'y **adapter** et j'ai **orienté leur sujet par rapport à mes thématiques** de recherche.

En effet, les étudiants viennent en majorité après **une ou deux années de recherche déjà réalisées**.

De fait, leur travail a été *essentiellement bibliographique* sans réellement réussir à innover. Mon rôle consiste à **développer avec eux une problématique concrète** susceptible de déboucher sur des applications.

Une fois la problématique définie et que l'étudiant a trouvé les premiers résultats par simulation, **je l'amène à enrichir le travail par une étude théorique et une modélisation mathématique** liée à la thématique de l'étudiant.

Une fois par semaine, je réunis tous les thésards présents pour **une scéance de travail collectif** où chacun présente ses travaux réalisés pendant la semaine. Il s'agit en fait d'un séminaire de recherche dans le sens où, sous ma direction, les doctorants structurent le travail qu'ils ont réalisé (outils, bibliographies, démonstrations, simulations), et où ils peuvent mutualiser les compétences mises en œuvre. C'est le moment privilégié où je peux estimer l'avancé du groupe, et pour mes propres travaux de recherche, envisager de nouvelles pistes de méthodologie et d'applications.

L'intérêt théorique de ses travaux peut paraître relativement limité. Néanmoins, il correspond à une attente très forte de doctorants qui sans cet approfondissement théorique et méthodologique, n'aurai pas pu faire aboutir leur recherche. Cette fonction est donc pleinement celle de l'enseignant chercheur que je suis.

C'est par ailleurs le sens même du contrat entre l'Université et l'Etat qui finance les doctorants.

Recherche

En termes d'avancement de mes propres travaux, c'est plutôt un frein par rapport à la recherche fondamentale que je souhaiterais mener, mais dans le même temps cette contrainte d'applications pratiques à trouver est créative puisqu'elle m'oblige, comme un ingénieur, à produire des protocoles innovants au cas par cas, et ensuite de les reformuler dans un ensemble plus général. C'est ainsi que la réflexion engagée lors des séminaires contribue à un champ plus vaste de réflexions, qui recouvre également l'ensemble des fonctions que j'assure comme responsable de la sécurité des systèmes d'information, me permet d'avoir une vision réaliste et constructive et d'alimenter à mon tour les recherches internationales sur ces sujets.

Ainsi que je l'ai annoncé plus haut dans mon exposé, cela correspond à un approfondissement des réseaux Ad-Hoc aux réseaux de capteurs, aux réseaux domotiques, à la sécurisation des protocoles, et finalement à l'intelligence artificielle. C'est à ce dernier domaine, l'intelligence artificielle, que je souhaiterais me consacrer actuellement.

Abderrahim MAKHLOUF "Etude des mécanismes de l'équité de la qualité de service dans les réseaux Ad Hoc"

Quotité : 50%
Co-encadrant : Pascal Lorenz
Thèse soutenue le 20 juillet 2009

Cette Thèse s'intéresse à l'équité dans les réseaux Ad-Hoc. La notion d'équité est très intuitive. Il existe plusieurs définitions : équité du nombre de paquets transmis, équité de la durée d'utilisation du réseau, d'utilisation de la bande passante, etc ... Le point de départ de la Thèse est la définition mathématique de l'index d'équité pour une ressource donnée selon K. Jain, Dah-Ming W. Chiu et William R. Hawe. *La thèse essaye de déterminer théoriquement cet index pour un réseau Ad-Hoc.* La démarche consiste à *approcher un réseau quelconque par un ensemble de réseaux en étoile.* Le premier résultat de la Thèse est la démonstration d'une condition nécessaire et suffisante pour qu'un réseau étoile soit équitable. Pour un réseau double-étoile (formé de deux étoiles avec une connexion entre eux) il est démontré qu'on ne peut pas avoir un comportement équitable, sauf si l'une des deux étoiles est réduite à un seul nœud. C'est à dire qu'on est en présence d'un réseau étoile. Ce deuxième résultat montre *la difficulté d'établir l'équité dans un réseau Ad-Hoc.* Finalement, l'étude théorique donne un majorant pour l'index d'équité d'un réseau double étoile. Dans la suite de la Thèse, des *algorithmes d'accès sont donnés pour approcher cet index d'équité maximal.* Des simulations avec NS2 illustrent ces algorithmes.

Ces travaux on donnés lieu à **deux communications** dans des Conférences internationales avec Comité de Lecture en 2008, dont une a reçu un prix **Best paper Award** [GLM08, MGL09] et on fait l'objet d'**un article dans un journal international** en 2009 [GML09].

Yaser YOUSEF "Routage pour la gestion de l'énergie dans les réseaux de capteurs sans fil"

Quotité : 50%
Co-encadrant : Pascal Lorenz
Thèse soutenue le 8 juillet 2010

Les réseaux de capteurs sans fils sont des réseaux Ad-Hoc particuliers. Les capteurs sont supposés être alimentés par une source d'énergie de capacité finie. *La consommation d'énergie est cruciale pour la durée de vie du capteur.* Le principal poste de consommation énergétique est la communication sans fil. La Thèse propose **une méthode originale** pour créer un routage qui tienne compte de cette contrainte énergétique. Cette nouvelle approche consiste à faire une analogie entre un réseau de capteur et **une image en niveaux de gris** pour utiliser des outils de traitement d'image afin de créer des algorithmes de routage. L'analogie consiste à former une image où un pixel représente un capteur, et sa luminosité le niveau d'énergie contenue dans sa batterie. Le routage des informations dans le réseau de capteurs se traduit dans l'image en niveaux de gris par des chemins passant par les pixels les plus lumineux. Ces chemins sont construits à partir de filtres de convolutions (filtre moyen, filtre gradient, filtre Gaussien) et de détection de contours (filtre de Sobel). Des *algorithmes de routage y sont proposés, utilisant ces différents filtres.*

Deux communications ont été faites dans des Conférences internationales avec Comité de Lectures en 2010 et 2011, [GYL09, YGL10b] ainsi qu'**une publication d'article dans un journal international** [YGL10a].

Karima CHEMOUN, suivie depuis 2015

Quotité : 50%
Co-encadrant : Pascal Lorenz
La Thèse sera soutenue fin 2018

Le but de cette Thèse est d'**analyser les trames d'un réseau domotique** (KNX par exemple) pour y découvrir des scénarios qui peuvent être automatisés. Après la modélisation du problème, il s'est avéré que la recherche de séquences fréquentes est un problème de fouille de données bien connu. Une **nouvelle approche de type probabiliste**, inspiré de la *Théorie des Croyances* a été faite. Cette approche a été présentée dans un article qui a été accepté dans un journal international avec Comité de Lecture [CGLL18].

Kamel SADDIKI, suivi depuis 2017

Quotité : 50%
Co-encadrant : Pascal Lorenz
La Thèse sera soutenue fin 2018

Cette thèse s'intéresse aux **attaques du protocole OLSR**, qui est un protocole de routage pour les réseaux sans fils. Le protocole proactif OLSR se base sur des nœuds privilégiés, les relais multipoints (MPR). Ces nœuds ont la fonction de collecter localement les informations sur l'état des liens, afin d'obtenir une vision de la topologie du réseau. **Le protocole est attaqué par la méthode du trou noir**, dans laquelle un nœud malveillant essaie de devenir relais multipoint pour diffuser de fausses informations de topologie, dans le but de modifier le routage du réseau.

Une solution proposée pour contrer cette attaque a été de **définir une métrique servant à détecter les nœuds malveillants**. Cette solution a donné lieu a une **publication dans un journal international** avec comité de lecture [LGSH17]. Une **deuxième publication** a été acceptée, portant sur une attaque coordonnée de deux noeuds [SBHLG18].

Amir Abdelkader AOUIZ, suivi depuis 2017

Quotité : 50%
Co-encadrant : Pascal Lorenz

Le protocole de routage AODV permet de trouver un chemin entre une source et une destination dans un réseau sans fils. Malheureusement, ce protocole réactif ne conserve qu'une route. Il existe un protocole modifié AOMDV qui conserve plusieurs routes dans la table de routage. Nous avons modifié ce protocole pour en faire un **protocole prenant en compte la variation d'energie** sur un chemin. Le but étant d'augmenter la durée de vie d'un réseau de capteurs. Ce nouveau protocole a été **publié dans un journal** [AHLG18].

Diab TAYED, suivi depuis 2017

Quotité : 50%
Co-encadrant : Pascal Lorenz

Cette Thèse est réalisée dans le **domaine de la sécurisation des réseaux véhiculaires**. On y propose d'adapter le réseau d'anonymat I2P au réseau véhiculaire. Le protocole I2P utilise un principe point à point, pour construire des tunnels entre une source et une destination. Le choix des nœuds intermédiaires est crucial pour **garantir l'anonymat de la communication**. L'efficacité de la communication dépend aussi de la localisation de ces nœuds, ce qui est en contradiction avec l'anonymat. Le fait d'être un réseau véhiculaire apporte des contraintes supplémentaires pour ces nœuds. Un premier protocole portant sur la distribution de clés de chiffrement dans un réseau véhiculaire a été **soumis à publication** dans un journal : Tayeb Diab, Marc Gilg, Pascal Lorenz, *A secure communication model using lightweight Diffie-Hellman method in vehicular Ad-Hoc networks*, International Jounal of Security and Networks.

Hichem Sid Ahmed BELKHIRA, suivi depuis 2017

Quotité : 50%
Co-encadrant : Pascal Lorenz

Cette Thèse a pour but d'introduire des **notions de sélection basées sur la capacité énergétique des nœuds** pour l'élection des nœuds MPR du protocole de routage OLSR.

Amine BOUDOUAIA, suivi depuis 2018

Quotité : 50%
Co-encadrant : Pascal Lorenz

Le but de cette Thèse est de créer un **algorithme de gestion de clés de chiffrement pour les grappes** de noeuds d'un réseau Ad-Hoc.

Conclusion

Parmi les 8 Doctorants que j'ai co-encadré, deux (Abderrahim MAKHLOUF et Yaser YOUSEF) ont **soutenus leur Thèse**, deux (Karima CHEMOUN et Kamel SADDIKI) sont en cours de rédaction de leur mémoire et **devront soutenir fin 2018**. Amir AOUIZ, Diab TAYEB et Hichem BELKHIRA sont en *cours de rédaction pour des publications* qui devront être soumis fin 2018. La prochaine section présente la liste des publications réalisées.

2.3.3 Publications

Types de Publication	Nombres
Articles dans des revues internationales	7
Livres ou chapitres de livres	1
Articles dans des conférences internationales	13
Articles dans des conférences nationales	1
Rapports de recherche, papiers soumis etc.	1

Chapitre de livre

— Marc GILG, *Chapitre 2-Representation of Networks of Wireless Sensors with a Grayscale Image : Application to Routing*, Building Wireless Sensor Networks, Editeur : Smain Femmam, Elsvier, pp. 31-63, 2017, ISBN 978-1-78548-274-8

Journal International

1. M. Gilg, A. Makhlouf, P. Lorenz,*Fairness index in single and double star Network*, International Journal On Advances in sytems and Measurements, Vol 2, No1 , pp. 109-118,2009.
2. Y. Yousef, M. Gilg, P. Lorenz, *Using Convolution Filters for Energy Efficient Routing Algorithm in Sensor Networks*, International Journal On Advances in Intelligent Systems, vol 3, no 1&2, 2010, ISSN : 1942-2679
3. Kamel Saddiki, Sofiane Boukli-Hacene, Pascal Lorenz, Marc GILG, *Black Hole attack detection and ignoring in OLSR protocol*, Int. J. of Trust Management in Computing and Communications, Vol 4. N.1, pp. 75-93, 2017
4. J. Caldeira, J. Rodrigues, J. Moutinha, M. Gilg, P. Lorenz, *Core-Body Temperature Acquisition Tools for Long-term Monitoring and Analysis*, International Journal on Advances if Life Sciences, vol. 2, no. 3 & 4, 2010, pages 209-218
5. J. Caldeira, J. Rodrigues, M. Gilg, P. Lorenz, *Performance Assessment of a New Intra-Mobility Solution for Healthcare Wireless Sensor Networks*, International Journal of Ad-Hoc and Ubiquitous Computing, Inderscience Publishers, vol. 15, No. 1/2/3, 2014, pages 215-226
6. Amir Adbelkader AOUIZ, Sofiane BOUKLI HACENE, Pascal LORENZ, Marc GILG, *Network life time maximization of the AOMDV protocol using nodes energy variation*, Network Protocols and Algorithms, vol. 10 N. 2, pages 73-94, 2018
7. Karima Chemoun, Marc GILG, Mourad Laghrouche, and Pascal Lorenz, *Evidence theory-based framework for improving automation in home automation system*, International Journal of Communication systems, Wiley, pages 1-22, 2018

Conférences internationales avec Comité de Lecture et sélection sur article long

1. M. Gilg, P. Lorenz, *An Adjustable Scheduling Algorithm in Wireless Ad Hoc Networks*, 3rd European Conference on Universal Multiservice Networks, Porto, Portugal, LNCS 3262, pp 216-226, October 25-27, 2004
2. M. Gilg and P. Lorenz, *A Totally Distributed and Adjustable Scheduling Algorithm in Wireless Ad-Hoc Networks*, International Conference on Networking and Services, ICNS'2005, Papeete, Tahiti, French Polynesia, October 23-28, 2005
3. M. Gilg, J. M. Kelif, P. Lorenz, *Power allocation problem in homogeneous and perturbated homogeneous CDMA networks*, IEEE International Conference on Communications, ICC'08, Beijing, pp. 343-348, May 19-23, 2008
4. M. Gilg, A. Makhlouf, P. Lorenz,*Fairness in a Static Wireless Network*, International Conference on Services and Networks Communications, ICNS'08, Sliema, Malta, pp. 17-22, October 25-30, 2008

5. A. Makhlouf, M. Gilg, P. Lorenz, *Fairness in Double Star Ad Hoc Network*, The fifth International Conference on Networking and Services, ICNS'09, Valencia, Spain, pp. 107-111, 20-25 April, 2009
6. M. Gilg, Y. Yousef, P. Lorenz, *Using Image Processing Algorithms for Energy Efficient Routing Algorithm in Sensor Networks*, International Conference on Adaptive and Self-adaptive Systems and Applications, ADAPTIVE'09, Athens, Greece, pp. 132-136, 2009
7. M. Popescu, P. Lorenz, M. Gilg, J.M. Nicod *Event Management Ontology : Mechanisme for Semantic-Driven Diagnosis*, Sixth International Conference on Networking and Services, ICNS'10, Cancun, Mexico, March 7-13, 2010
8. Y. Yousef, M. Gilg, P. Lorenz, *Using Matrix convolutions and Clustering for Energy Efficient Routing Algorithm in Sensor Networks*, Sixth Advanced International Conference on Telecommunications, AICT'10, Barcelona, Spain. pp. 275-279, May 9-15, 2010
9. P. Lorenz, M. Gilg, J.J.P.C. Rodrigues, *Modelization of Temporal Mechanisms for Sensors Networks*, 6th International Mobile Multimedia Communications Conference, MobiMedia'10, 6-8 September 2010, Lisbon, Portugal, pages 1-15
10. M. Popescu, P. Lorenz, M. Gilg, J.M. Nicod, *Temporal Aspects in Diagnosis Validation*, Fourth International Conference on Advances in Semantic Processing, SEMAPRO'10, October 25-30, 2010, Florence, Italy, pages 43-48
11. J. Lloret, M. Gilg, M. Garcia, and P. Lorenz, *A group-based protocol for improving energy distribution in smart grids*, IEEE International Conference on Communications (ICC), pp. 1-6, June 2011
12. M. Gilg, P. Lorenz, and J. Rodrigues, *Location-aided routing using image representation for wireless sensor networks*, IEEE International Conference on Communications (ICC), pages 1-5, June 1011
13. Kamel Saddiki, Soufiane Boukli-Hacene, Pascal Lorenz and Marc GILG, *Trust neighbours-based to mitigate the cooperative black hole attack in OLSR protocol*, SSCC-2018, Bangalore, India

2.3.4 Service à destination de la communauté

J'ai participé à plusieurs **Comités** et **organisations de conférences** et j'ai **relu** plusieurs **articles** pour des journaux. L'ensemble de ces activités est recensé dans la liste ci-dessous :

Éditeur

J'ai participé à la sélection des articles pour la Conférence : *Fourth International Conference on Digital Telecommunications*, ICDT'09, 20-25 Juillet 2009 Colmar.

Comité de programme

J'ai participé au **Comité de programme** et à la **relecture d'articles** (2 à 3 articles par conférence) des conférences suivantes :

— International Conference on Networking and Services, (ICNS '06), 16-19 Juillet 2006, *Silicon Valley, USA*
— International Conference on Networking and Services, (ICNS'07), 19-25 Juin 2007, *Athens, Grèce*
— International Conference on Networking and Services, (ICNS'08), 26-31 Octobre 2008, *Sliema, Malte*
— International Conference on Networking and Services, (ICNS'09), 20-25 Avril 2009, *Valencia, Espagne*

— Fourth International Conference on Digital Telecommunications, (ICDT'09), 20-25 Juillet 2009, *Colmar, France*
— Communications QoS, Reliability and Performance Modeling Symposium, (ICC'07), 24-27 Juin 2007, *Glasgow, Scotland*
— International Conference on Systems and Networks Communications, (ICSNC'09), 20-25 Septembre 2009, *Porto, Portugal*
— 7th Annual Conference on Communication Networks and Services Research, (CNSR'09), 11-13 Mai 2009, Moncton, *New Brunswick, Canada*
— The Third International Conference on Communication Theory, Reliability, and Quality of Service, 2010, *Glyfada, Grèce*
— Conference on Communication Networks and Services Research, (CNSR'10), May 11- 14, 2010, *Montreal, Canada*
— The Second International Conference on Adaptive and Self-adaptive Systems and Applications (ADAPTIVE 2010), November 21-26, 2010 - *Lisbon, Portugal*

Relectures pour des journaux

J'ai relu 2 articles pour chacun des journaux ci-dessous :
— Security and Communication Networks, 2008, (Wiley)
— Journal of Network and Computer Applications, 2009, (Elsevier)
— *International Journal of Communication Systems (IJCS)*, (Wiley), **19** relectures depuis 2011
— The Computer Journal (COMPJ), (Oxford Journals) Sensors, 2009, (MDPI Publishing)
— Multimedia System Journal, 2010, ACM/Springer
— Journal of Medical Systems, 2010, (Springer)
— IEEE Transactions on Emerging Topics in Computing, 2018
— International Journal of Distributed Sensor Networks, 2018, (Sage)
— Transactions on Emerging Topics in Computing, 2018, (IEEE)

Session Chair

J'ai été **Session Chair** pour les conférences suivantes :
— International Conference on Networking and Services, (ICNS'08), 26-31 Octobre 2008, *Sliema, Malte*
— IEEE International Conference on Communications, (ICC'08), 19-23 Mai 2008, *Pékin, Chine*
— International Conference on Networking and Services, (ICNS'09), 20-25 Avril 2009, Valencia, Espagne
— International Conference on Adaptive and Self-adaptive Systems and Applications, (ADAPTIVE'09), 15-20 Novembre 2009, *Athens, Grèce*
— Fourth International Conference on Digital Telecommunications (ICDT'09) 20-25 Juillet 2009, *Colmar, France*
— The Sixth Advanced International Conference on Telecommunications (AICT 2010) 9-15 Mai 2010, *Barcelone, Espagne*

2.4 Activités d'enseignements en informatique

2.4.1 Présentation de l'activité d'enseignement

Mon **enseignement** est essentiellement donné à l'*IUT de Colmar*, au Département Réseaux et Télécommunications, mais une petite partie est aussi réalisée à *Mulhouse en Master*. Le volume horaire prévisionnel pour 2018 est de 309h eq TD.

Je fais chaque année des **suivis de Projets Tuteurés, de Stages et d'apprentis** en **DUT** et **Licences professionnelles**. En 2018 j'ai suivi un Projet Tuteuré en Master 2 Informatique Mobile Répartie.

Mon enseignement se concentre sur trois thématiques :
— réseau et routage
— système Linux et virtualisation
— cybersécurité
Depuis 2018, j'ai donné des **TD de Mathématiques** en DUT 1ère année.

Mes enseignements sont mis à disposition sur la plateforme MOODLE. Certaines évaluations se font à partir de QCM utilisant le logiciel Auto-Multiple Choice. Chaque année **un nouveau cours** est proposé en **fonction de l'évolution technologique** (Virtualisation XEN en 2014, puce cryptographique TPM en 2015, stockage de données distribué avec Ceph en 2016, Token cryptographique en 2017, sécurité du développement et débordement de pile en 2018). En 2014 **j'ai présenté une conférence avec un article long au Workshop RT de la Réunion**. Cet article est le résumé d'un TP de 32h qui amène l'étudiant à *créer un réseau d'entreprise sous Linux* avec tous les services : DHCP, DNS, LDAP, messagerie, serveur de fichier, serveur d'applications.

J'étais correspondant C2I de la composante IUT de Colmar pendant 4 ans. Durant cette période j'ai organisé l'épreuve sur papier dans les différents amphithéâtres de l'IUT.

Dans le **cadre d'ERASMUS**, j'ai effectué deux séjours au Portugal. J'y ai fait **plusieurs cours sur les réseaux domotiques** au **niveau Master**.

Je suis vice-président Grand Est de l'Association CyberEdu, qui a pour but d'**introduire des notions de *cybersécurité* dans les enseignements en informatique**. Cette Association a été créée par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). J'organise dans ce cadre des **Colloques pour les enseignants du supérieur** de la région et je participe à la labellisation des enseignements.

2.4.2 Direction, animation, montage de formations

J'ai été élu au poste de **Chef de Département Réseaux et Télécommunications** à l'IUT de Colmar. J'ai assuré la direction du département du **1er Novembre 2012 au 1 décembre 2016**. Pendant cette période j'ai géré le budget du département et le recrutement des étudiants de DUT en formation initiale. J'ai été l'initiateur de la **création d'un parcours trinational avec l'Allemagne et la Suisse** qui s'est réalisé par l'élargissement de la licence ICS du département GEII de l'IUT de Mulhouse aux étudiants du département Réseaux et Télécommunications.

En Juin 2014 j'ai organisé l'**Assemblée des Chefs de Département** Réseaux et Télécommunications à l'IUT de Colmar. Cette Assemblée a réuni 93 enseignants des départements Réseaux et Télécommunication de France.

Par la fonction de Chef de Département, j'ai été amené à participer au **projet pédagogique WANRT** créé par l'Assemblée des Chefs de Département Réseaux et Télécommunications. La WANRT s'*appuie sur des Projets Tuteurés pour mettre en place une infrastructure réseaux entre différents départements RT de France*, pour supporter différents jeux.

Dans un but de **promotion du département**, des **Lycéens sont invité** à venir jouer sur cette infrastructure. J'ai notamment encadré un groupe de Projet Tuteuré qui avait la gestion du jeu *Global Offensive* au niveau national. Ce projet nécessite la *coordination de 15 départements R&T* à travers la France.

J'ai aussi contribué au rayonnement du Département en prenant l'*initiative de réunir plus de **900 anciens étudiants*** lors d'un **repas pour les 20 ans** de la création du Département.

2.4.3 Diffusion, rayonnement, activités internationales

Au *3ème Workshop Pédagogique Réseaux et Télécoms*, en 2014 à la Réunion, j'ai publié un *article de 6 pages* sur l'ensemble de mon cours Linux de Licence professionnelle ASUR s'intitulant « **Une infrastructure de serveurs d'entreprise sur une plateforme Xen** »

Par le programme d'échange **Erasmus**, j'ai été invité deux fois par l'Université de Beria Interior à Covilhã *au Portugal*, pour une durée d'une semaine chaque fois. Lors de ces déplacements, j'ai donné un *cours sur les réseaux de capteurs et la domotique* au **niveau Master**.

Liste des enseignements en informatique

J'assure les enseignements suivants :

- **En DUT Réseaux et Télécom 1ère année : Module Virtualisation, 50 étudiants, 38,5h TP**
  - Administration des Systèmes Linux
  - Virtualisation sous Linux avec KVM, Xen
  - Interface Virtmanager
  - Introduction à Openstack
- **En DUT Réseaux et Télécom 1ème année : Module Mathématique, 10 étudiants, 38,5h TP**
  - Polynômes
  - Tracer de courbes
  - Résolution d'équations
- **En DUT Réseaux et Télécom 2ème année : Module Sécurité, 30 étudiants, 7h CM, 17,5h TD, 34h TP**
  - La sécurité des systèmes d'informations
  - Les pare-feu avec IPtables
  - Algorithmes de cryptage et de hachages
  - Infrastructure de Gestion de Clés
  - Le protocole SSL
  - Les VPN et IPSEC
- **Licence professionnelle ISVD, Protocoles Voix sur IP, 10h TD**
  - La convergence
  - les protocoles SIP H323 MGCP et IAX2
- **Licence professionnelle ASUR, 4h TD, 16h TP**
  - Stockage distribué avec Ceph
- **Licence Professionnelle ASUR : Administration Linux, 6h TD, 32h TP**
  - Virtualisation avec Xen
  - Gestion DNS et DHCP
  - Annuaire OpenLDAP et authentification
  - Serveur de fichiers NFS
  - Serveur de terminaux X-window
- **Licence Professionnelle ASUR : Virtualisation, 2h TD, 8h TP**
  - Virtualisation avec Xen
  - Virtualisation LXC
  - Nuage Openstack

— **Licence Professionnelle ASUR et ISVD : Sécurité, 6h CM, 1h TP, 20h TP**
  — La sécurité des systèmes d'informations
  — Algorithmes de cryptage et de hachage
  — Infrastructure de Gestion de Clés
  — Le protocole SSL
  — Les VPN OpenVPN et IPSEC

— **Master ISC 1ère année, Sécurité, 40 étudiants, 6h CM, 8h TD**
  — Les Pare-feu
  — Iptables
  — ACL Cisco
  — Algorithmes de cryptage et de hachages
  — Infrastructure de Gestion de Clés
  — Le protocole SSL

— **Master ISC 1ère année, Routage Dynamique, 40 étudiants, 6h CM, 2h TD, 6h TP**
  — Protocole RIP
  — Protocole OSPF

— **Master IMR 2ère année, Sécurité des dévelloppement, 20 étudiants, 6h CM, 8h TD**
  — Débordement de pile sous Linux

2.5 Activités administratives

2.5.1 Présentation générale des responsabilités

L'implication administrative au niveau de l'établissement s'inscrit dans le prolongement de ma fonction d'**Ingénieur de Recherche**, que j'ai occupée jusqu'en 2006. Comme Ingénieur de Recherche j'ai en effet acquis la **connaissance précise** du fonctionnement d'un service administratif de l'Universitré y compris la **gestion du personnels, du budjet**, et **des marchés publiques**.

Cette expérience d'Ingénieur de Recherche m'a également été très utile pendant mon mandat de Directeur de Département. J'ai souhaité m'investir également dans les autres aspects à caractère administratif mais également porteur de l'**importance Humain** et du **rayonnement de l'Université de Haute-Alsace** en tant qu'**élu**.

Ainsi j'ai porté plusieurs responsabilités :

— En 2006-2007 j'étais Chargé de Mission pour la transition de la téléphonie de l'établissement vers la technologie IP. Pour cette mission j'ai travaillé avec un bureau d'étude et validé les différentes phases de la migration en défendant les intérêts de l'Université.
— Depuis 2007 j'exerce la fonction de **Responsable de la Sécurité des Systèmes d'Information (RSSI)**.
— Depuis 2008, j'exerce la fonction de **Fonctionnaire de Sécurité et de Défense (FSD)** de l'Université,
— De Novembre 2012 à Décembre 2015 j'ai été **Directeur du Département** d'IUT Réseaux et Télécommunications de l'IUT de Colmar.
— De 2012 à 2016, j'ai été élu à la **commission de recherche et au Conseil Académique restreint**.
— Je suis membre suppléant de la **Commission Paritaire de l'Etablissement (CPE)** nommé par le chef d'établissement.
— Je suis membre du **groupe de réflexion EUCOR** sur les Universités du Rhin Supérieur.

2.5.2 Responsable de la sécurité des systèmes d'information de l'Université depuis 2007

Quand j'ai été ingénieur de recherche au Centre de Ressources Informatiques de l'Université de Haute-Alsace, j'ai occupé la fonction de Responsable de la Sécurité des Systèmes d'Information Adjoint (RSSIa). En devenant Maître de Conférence, je suis devenu titulaire suite au départ à la retraite de l'ancien RSSI.

En tant que **RSSI**, je suis **rattaché à la Présidence de l'Université** pour toutes les questions de sécurité de l'information. J'ai un rôle de conseil auprès de la gouvernance de l'établissement, ainsi je **contribue à la réunion des Vice-Présidents et des Chargés de Mission** qui se tient toute les deux semaines présidée par la Présidente de notre Université.

Je suis en relation avec le Haut-Fonctionnaire de Sécurité et de Défense du ministère de l'enseignement supérieur et de la recherche. J'assure un **rôle de contrôle** auprès des services informatiques et un **rôle de formateur** auprès des utilisateurs, ainsi que la mise en œuvre de la Politique de Sécurité des Systèmes d'Information de l'État (PSSIE) en adaptant les directives ministérielles à l'établissement, qui comportent 197 indicateurs.

J'ai pris l'initiative d'organiser une **réunion mensuelle avec les ingénieurs** de la Direction du Numérique.

Avec le développement du numérique et de ses menaces, cette fonction prend de plus en plus d'importance.

2.5.3 Fonctionnaire de Sécurité et de Défense de l'Université

Je suis **Fonctionnaire de Sécurité et de défense** de l'Université de Haute-Alsace. En relation avec le Haut-Fonctionnaire de Défense et de Sécurité (HFDS) du ministère de l'enseignement supérieur et de la recherche, je suis chargé d'assurer la protection de l'établissement dans le cadre de la protection des intérêts fondamentaux de la nation. Cela regroupe la *protection du patrimoine scientifique et technique*, la *protection du secret de la défense nationale*, la *protection et la sécurité publique*.

Depuis les attentats de 2015 cette fonction est devenue essentielle. Je participe au **groupe de travail Gestion de Crise de l'établissement**. La Protection du Patrimoine Scientifique et Technique (PPST) prend aussi de l'ampleur. La partie visible en est **la mise en place des Zones à Régime Restrictif (ZRR)**. Dans ce cadre je conseille les directeurs de laboratoires et je traite les incidents relatifs à la sécurité.

J'effectue le **traitement des dossiers d'habilitation**. J'ai été volontaire pour intégrer **deux groupes de travail auprès du HFDS**.

— Le premier groupe est constitué d'universités et d'organismes de recherche (CNRS, INRIA, INRA, ...). *Ce groupe propose des solutions* au ministère pour *améliorer la gestion des ZRR*.
— Le deuxième groupe de travail, composé de FDS et de RSSI, a été crée dans le but de *faire une note sur la gestion des ressources informatiques dans les ZRR*. Une note a été publiée en 2014 sur les Informations à Régime Restrictif (IRR).

Depuis 2018, je suis **auditeur auprès de l'IHEDN** (Institut des Haute-Etudes de la Défense Nationales).

2.5.4 Chef de Département Réseaux et Télécommunication de Novembre 2012 à Décembre 2015

J'ai été élu chef de département Réseaux et Télécommunications à l'IUT de Colmar. J'avais **un rôle d'animation du département** et j'ai géré le **budget** du département et le **recrutement** des étudiants. J'ai été l'initiateur de la création d'un **parcours trinational** avec l'Allemagne et la Suisse en élargissant la Licence ICS du département GEII de l'IUT de Mulhouse aux étudiants du département Réseaux et Télécommunications. J'ai organisé l'Assemblée des Chefs de Département à l'IUT de Colmar en Juin 2014. Cette Assemblée a **réuni 93 enseignants des départements Réseaux et Télécommunications** de France.

2.5.5 Membre de la commission de Recherche et du Conseil Académique de l'Université de 2012 à 2016

Élu à la Commission de Recherche et au Conseil Académique Restreint de l'Université de Haute-Alsace, j'ai examiné les **dossiers de titularisations** de Maîtres de Conférence, pour le passage à la hors classe, ainsi que plusieurs dossier de **demande de subvention des laboratoires**. Nous avions un rôle de conseil pour la politique scientifique de l'établissement.

2.5.6 Membre de la Commission Paritaire d'Etablissement

Je suis nommé membre suppléant de la Commission Paritaire d'établissement par le Président de l'Université. Dans cette commission nous examinons les **changements de grade** et **les avancements des agents ITARF** de l'établissement.

2.5.7 Membre du groupe de réflexion Eucor

L'université de Haute-Alsace fait partie du *Groupement européen de coopération territoriale (GECT) Eucor* qui regroupe cinq Universités du Rhin Supérieur : Freiburg (Allemagne), Karlsruher Institut für Technologie (Allemagne), Bâle (Suisse), l'Université de Strasbourg et l'Université de Haute-Alsace. Je suis **membre actif de ce groupe de réflexion** qui a pour mission de proposer des actions à mener dans ce cadre, parmi lesquelles des actions de financement pour des projets de recherche incluant plusieurs Universités du Rhin Supérieur.

Chapitre 3

Congestion dans les réseaux Ad-Hoc

3.1 Introduction

Cette première partie est consacrée à l'étude de la congestion dans les réseaux Ad-Hoc et présente les travaux réalisés en 2004 et 2005.

Les réseaux sans fil utilisent des interfaces radio comme support de communication. Il existe plusieurs protocoles pour diffuser des données sur ce type de média. Les protocoles sans fil les plus connus sont ceux utilisés dans les réseaux Wifi de type 802.11b/g. Dans l'étude qui suit, nous utilisons cette famille de protocoles. Ce choix a une conséquence non négligeable sur l'utilisation des canaux de communication. De ce fait, une station ne peut recevoir qu'un paquet de données à la fois, sinon il en résulte une collision. Ce phénomène peut être illustré par un groupe de trois personnages. Deux personnes s'adressent en même temps à un même individu. Celui-ci recevra deux informations et cela est inaudible pour lui. Pour résoudre ce problème dans la vie courante on utilise des règles de politesse qui stipulent que chaque personne s'exprime à son tour. Dans les réseaux 802.11b/g, le principe est le même, et la règle de politesse qu'on utilise est le protocole d'accès au réseau CSMA/CA. Ce protocole à pour but d'éviter les collisions. Mais ce protocole a ses limites : si une station a beaucoup d'interlocuteurs, il est extrêmement difficile d'éviter les collisions sans pour autant maintenir un débit satisfaisant. Si par exemple nous avons un grand nombre de personnes s'adressant à un même individu, et si pour éviter les collisions, nous autorisons chaque personne à prononcer un mot à tour de rôle, il faudra un temps conséquent pour que chaque personne puisse dire sa phrase. Il y donc un phénomène de congestion du trafic qui se produit. Et c'est justement ce phénomène qui va focaliser notre étude dans ce chapitre.

Les phénomènes de congestion dans les réseaux Ad-Hoc sont un thème de recherche largement étudié et ils restent toujours d'actualité. Encore récemment, un article [10] nous propose un mécanisme de contrôle de congestion pour les réseaux Ad-Hoc. De tels mécanismes peuvent agir à différent nivaux : protocoles d'accès, routage, etc ... L'article [4] nous présente quelques uns de ces protocoles.

Certaines publications [72] proposent la multiplication des interfaces radio pour limiter les collisions. La modification des protocoles d'accès à la couche radio reste aussi une alternative intéressante [61, 54, 52, 73, 100, 36].

De nos jours, des protocoles multicouches (niveaux accès et routages) apportent encore plus d'efficacité [85, 97, 95, 77]. Des développements théoriques sont venus soutenir ce type d'études [19, 40, 98].

La bande passante est aussi un critère qui fut largement étudier [64, 93, 67, 49].

Les travaux que nous avons réalisé s'appuient sur la théorie des graphes, en particulier celle des cliques maximales pour apporter une solution à la congestion tout en essayant de préserver la bande passante. Les cliques maximales ont déjà servi de base pour un algorithme d'accès dans [84]. Nous avons poursuivi dans cette voie et nous avons proposé deux algorithmes d'accès qui ont été présentés lors de conférences internationales [GL04, GL05].

Le chapitre se divisera en plusieurs sections : nous commencerons par une présentation des réseaux Ad-Hoc, de leur fonctionnement et de leurs contraintes. La deuxième section donnera un cadre théorique à notre étude en introduisant plusieurs définitions, notamment celui du graphe de contention et des cliques maximales. La troisième section présentera les algorithmes que nous avons proposés ainsi que les simulations qui ont été faites. La dernière section conclura ce chapitre.

3.2 Les réseaux Ad-Hoc

3.2.1 Présentation des réseaux Ad-Hoc

Les réseaux Ad-Hoc sont une famille de réseaux sans fils. Dans ce type de réseau, les stations ou noeuds, établissent des liens de communication directement entre elles sans passer par une infrastructure telle que des points d'accès. La figure 3.1 illustre un tel réseau :

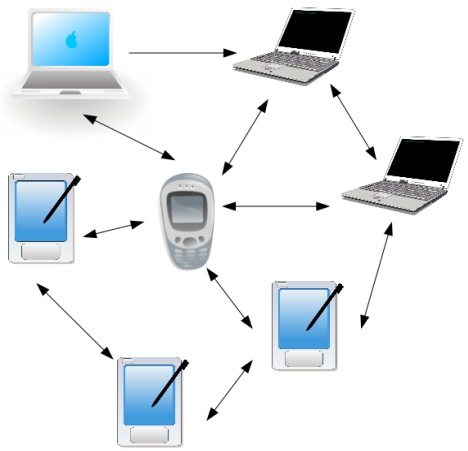

FIGURE 3.1 – Réseau Ad-Hoc

De tels réseaux sont souvent utilisés dans des environnements où il n'y a pas d'infrastructure fixe, par exemple un champ de bataille, une zone sinistrée par un tremblement de terre, etc ...

Les réseaux Ad-Hoc ont des spécifications particulières :
- *une topologie dynamique* : les noeuds sont mobiles, donc la topologie évolue
- *un besoin d'auto-configuration* : il est souhaitable que le noeuds ne nécessite pas d'administrateur pour s'adapter aux modifications de topologie.
- *l'utilisation d'algorithmes de routage spécifiques* : les noeuds acheminent l'information en la relayant. Il faut donc pouvoir établir des chemins entre les stations du réseau.
- *l'utilisation d'interfaces radio* de type Wifi implique le fonctionnement unidirectionnel des liens : communication half duplex.

— *une bande passante limitée* par l'utilisation d'interfaces Wifi et la nécessité de partage des ressources radio.

Nous utilisons le protocole 802.11 (Wifi) pour la transmission des données. Ce protocole utilise les mécanismes d'accès CSMA/CA.

3.2.2 La couche d'accès CSMA/CA

Le protocole d'accès CSMA/CA a pour but de réguler l'accès radio et d'éviter les collisions. Pour cela, il met en place plusieurs règles :

— Avant de communiquer, la source doit préciser le temps nécessaire d'occupation du canal.
— Chaque participant doit émettre uniquement si le délai de la source précédente a expiré.
— Pour savoir si un message a été reçu, un accusé de réception confirme la bonne réception à un participant.
— Si deux sources émettent à la fois, l'absence d'accusé de réception indique une collision
— Un participant attend un délai aléatoire pour émettre.

Les règles du protocole CSMA

Ces règles se traduisent par plusieurs mécanismes :

— Détection de porteuse
Il y a deux façons de faire : l'écoute de la porteuse et la vérification des réservations en cours via le NAV (network allocation vector).
— DCF (distributed coordination function)
Cette fonction décale aléatoirement la phase d'émission après que le médium est disponible (Intervale DIFS). Ceci diminue le risque de collision.
— La trame d'accusé de réception
Un accusé de réception est envoyé après une réception en respectant un cours intervalle de temporisation SIFS.

Ces différentes phases se résument dans la figure 3.2 :

FIGURE 3.2 – Trame CSMA

Le problème du noeud caché et les trames RTS/CTS

Supposons que nous avons 3 noeuds : 1 noeud central avec 2 noeuds voisin. On suppose que les voisins n'ont pas de communication directe. Ceci est représenté dans la figure 3.3 :

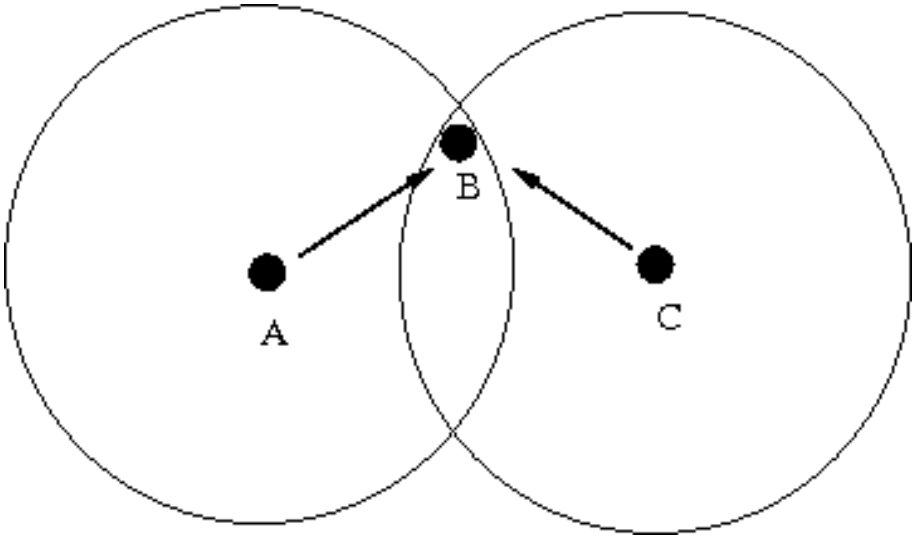

FIGURE 3.3 – Problème du noeud caché

Dans la figure 3.3, les noeuds A et C transmettent un message à B. Or A n'est pas dans le rayon de communication de C. De ce fait, si C émet un paquet, A ne peut pas le détecter. A peut donc envoyer un paquet à B au même moment que C. Il se produit donc une collision en B.

Pour éviter cela, un noeud souhaitant émettre, par exemple C, réserve une fenêtre temporelle en envoyant un message RTS (request to send) à B. B répond par un message CTS (clear to send) signifiant que la voie est libre. A étant dans le rayon de communication de B, il reçoit le message CTS et est informé de l'intention d'émission de C. Cela résout le problème du noeud caché car tout les participants sont informés de l'occupation du canal de communication.

Limitation de la méthode CSMA/CA

Le protocole d'accès CSMA/CA évite les collisions en mettant en place un mécanisme de réservation de fenêtre temporelle dans laquelle peut se faire la transmission des données. Un tel mécanisme n'est pas adapté à un grand nombre de noeuds. Effectivement, si un noeud a un grand nombre de voisins, il sera difficile pour lui de trouver un intervalle de temps libre pour transmettre. De plus, pendant cet intervalle, tous ses voisins à un et deux sauts ne pourront pas émettre. Il en résulte une diminution de la capacité du réseau à acheminer un volume important d'informations.

C'est ce problème que nous étudions ici et que nous allons formaliser.

3.3 Le graphe de contention

Dans la section précédente, nous avons vu que le protocole d'accès CSMA/CA utilise un mécanisme de réservation pour éviter les collisions. Ainsi, un noeud réservant un intervalle temporel par les trames RTS/CTS pour transmettre bloquera toutes tentatives d'émissions pour ses voisins à un et deux sauts. Dans cette section, nous allons formaliser cela par le graphe de contention. Nous donnons aussi quelques définitions et propriétés sur la bande passante d'un réseau Ad-Hoc issues de [GL04] et [84].

3.3.1 Définitions fondamentales

Graphe de contention

Définition 1 (Graphe topologique)**.** Un graphe topologique d'un réseau est un graphe non orienté $G = (S, A)$ où les sommets S représentent les noeuds du réseau et les arrêtes A les flux entre les noeuds.

La figure 3.4 représente un graphe topologique d'un réseau :

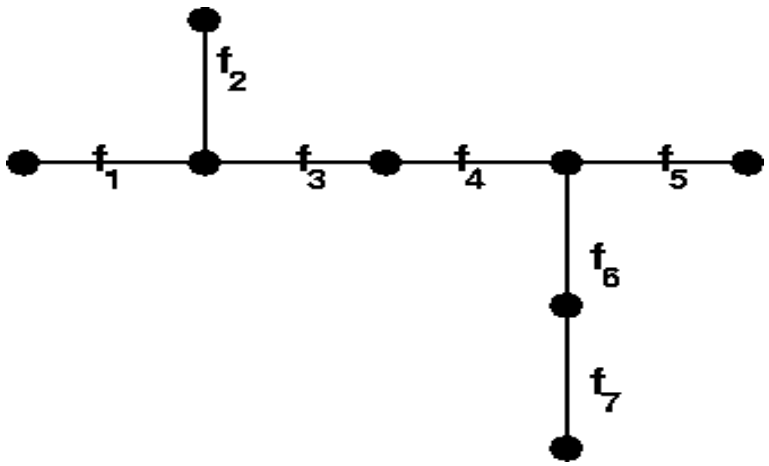

FIGURE 3.4 – Graphe topologique d'un réseau

Dans un tel graphe, si le réseau fonctionne avec le protocole d'accès CSMA/CA, les flux adjacents et leurs voisins sont générateurs de collisions. De tels flux sont appelés **contondant**. Ceci permet de définir une relation entre des flux et le graphe de contention :

Définition 2 (Relation de contention)**.** Deux flux sont contondant s'ils sont distant d'au plus 2 noeuds dans le graphe de topologie.

Définition 3 (Graphe de contention)**.** Un graphe de contention de flux est le un graphe non-orienté $G' = (S', A')$ où l'ensemble des sommets S' est formé des flux et les arrêtes A' représentent la relation de contention entre deux flux.

La figure 3.5 représente le graphe de contention du réseau de la figure 3.4 :

Dans un graphe de contention, deux flux adjacents sont générateurs de collisions. Nous pouvons formuler la remarque suivante :

Remarque. Pour un réseau de type CSMA/CA, deux flux adjacents dans le graphe de contention sont générateur de collisions et donc ne peuvent exister au même moment.

Nous pouvons nous posez la question suivante : si un flux existe, quels sont les flux du graphe de contention qui ne peuvent exister au même moment ? La réponse est : ce sont les flux qui forment une clique maximale.

Clique maximale

Définition 4 (Clique maximale)**.** Un sous-graphe maximal complet d'un graphe G est appelé une clique maximale.

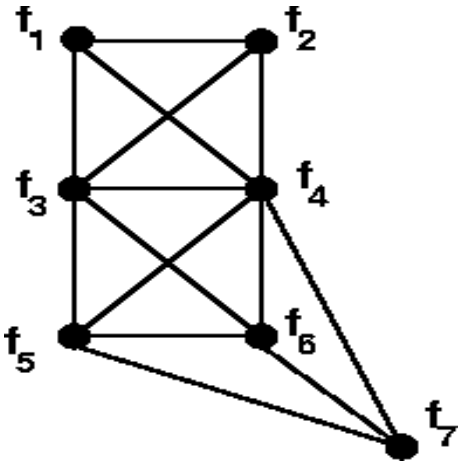

FIGURE 3.5 – Graphe de contention

Dans le graphe de contention de la figure 3.5, les cliques maximales sont : $C_1 = \{f_1, f_2, f_3, f_4\}$, $C_2 = \{f_3, f_4, f_5, f_6\}$ et $C_3 = \{f_4, f_5, f_6, f_7\}$.

Définition 5 (Nombre maximal de cliques)**.** Le nombre maximal des cliques d'un flux f est le nombre de cliques maximales qui contient f. Si ce nombre vaut 1 alors f est un flux de clique simple, sinon il est dit de cliques multiples.

Une telle contrainte sur l'existence des flux à une incidence non négligeable sur la quantité d'informations que peut acheminer un réseau au cours du temps.

La bande passante

Définition 6 (Débit moyen)**.** Le débit moyen d'un réseau est le rapport du nombre de paquets transmis par le temps nécessaire.

$$Tps = \frac{\text{nombre de paquets transmis}}{\text{temps de transmission}}$$

Définition 7 (Débit moyen d'un flux)**.** Le débit moyen d'un flux est la limite de la division du nombre de paquets transmis par le temps nécessaire.

$$Tps(f_j) = \lim_{T \to +\infty} \frac{\text{nombre de paquets transmis par } f_i \text{ pendant le temps } T}{T}$$

Remarque. Comme un flux ne peut transmettre au plus un paquet par unité de temps, on a :

$$0 \leq Tps(f_i) \leq 1$$

Pour chaque clique, un seul flux peut exister au même instant. Dans un réseau, le nombre maximal de flux qui peuvent exister au même moment est le nombre de cliques indépendants. Ce nombre maximise le débit moyen. Nous avons donc :

Lemme 3.3.1 (Débit maximal)**.** *Le débit maximal Tps_{max}, sans autres contraintes sur le réseau CSMA/CA, est donné par le nombre maximal de flux indépendants dans le graphe de contention.*

Dans ce contexte, seuls les flux participants à un ensemble de flux indépendants sont susceptibles d'émettre. Il existe donc des flux qui n'émettent jamais. Nous pouvons ajouter une contrainte pour que chaque flux émet sensiblement le même nombre de paquets, c'est la contrainte d'équité.

Lemme 3.3.2 (Débit en cas d'équité)**.** *Le débit maximal avec une contrainte d'équité,* TPS_{fair} *est donnée par :*

$$Tps_{fair} = \frac{\sum_i W_i}{X_w(G)}$$

où $X_w(G)$ *est le nombre chromatique du graphe de contention* G *et* W_i *le poids du flux* f_i*.*

Démonstration. En coloriant successivement les flux du graphe de contention, nous obtenons, en un délai minimal, un ordre pour que tous les flux émettent. □

3.4 Algorithme d'accès utilisant des cliques

L'algorithme que nous présentons ici a été publié dans [GL04]. Il utilise la notion de cliques évoquée précédemment pour donner le contrôle sur le débit moyen Tps du réseau. Ce débit moyen est contrôlé à l'aide d'une variable $TpsW$ qui définit une cible pour ce débit. Cette valeur est bornée par les valeurs limites Tps_{fair} et Tps_{max} tel que :

$$Tps_{fair} \leq TpsW \leq Tps_{max}$$

L'algorithme suppose que chaque noeud connaît pour chacun de ses flux leur nombre maximal de cliques. Le principe de l'algorithme est de favoriser les flux avec un nombre maximal de cliques faible.

3.4.1 Description de l'algorithme

Initialisation

On suppose que chaque noeud connaît pour chaque flux son nombre maximal de cliques. La détermination de ce nombre peut se faire par une reconnaissance de la topologie du réseau utilisant l'inondation de paquets de contrôles et l'utilisation de l'algorithme de Bierstone [12] pour le calcul des cliques.

L'algorithme utilise un coefficient de refus e_i qui est initialisé au nombre maximal de cliques pour le flux f_i. La fréquence d'existence d'un flux sera inversement proportionnelle à la valeur de e_i. Le coefficient de refus augmentera à chaque activation du flux.

Chaque noeud a un tableau d'acquittement a_k pour chacun de ses flux f_k qui est initialisé. Le réseau procède à la nomination d'un noeud comme maître du réseau. Ce noeud permettra la synchronisation des émissions. Une fois le maître choisi, il envoie un message Master Ready à tout le réseau.

Traitement des messages du maître pas les noeuds

Chaque noeud effectue les opérations suivantes pour chaque flux f_j :

— Réception d'un message *Master Ready* :
Si $P_j = Vrai$ alors des données sont envoyées par le flux f_j et le noeud procède au calcul de permission pour le flux f_j. Sinon, le noeud fait un calcul de permission pour le flux f_j sans envoyer de paquets.

— Réception d'un message *Master Init* :
les valeurs e_j sont initialisées au nombre maximal de cliques des flux f_j et les calculs de permissions sont faits.

— Réception des valeurs P_k et e_k des flux voisins f_k :
envoie d'un accusé de réception *Ack*

— Réception d'un message *Ack* du flux f_k :
Le noeud met la valeur $a_k = 1$ et s'il a reçu un accusé de réception de tous les flux alors :
  — il recherche le flux f_k, voisins de f_j, dans le graphe de contention, f_j compris, avec $P_k = vrai$ et le nombre de paquets émis le plus bas.
  — parmi les flux trouvés, il sélectionne le flux f_h avec le plus petit indice h
  — Si $h \neq j$ alors $P_j = faux$ et $e_j = e_j - 1$
  — Le noeud envoie un message *Ready*, pour le flux f_j, au maître.

Calcul de permission

Pour chaque flux f_j, il faut calculer sont droit à l'émission. Cela se fait par l'algorithme suivant :
— La variable P_j est initialisée à faux.
— Si les paramètres P_k, e_k des voisins sont inconnus alors on les demande.
— Si pour tous les flux voisins on a $P_k = faux$ et $e_j \leq e_k$ alors on met $P_j = Vrai$, $e_j = e_j + 1$ et on initialise les coefficients a_k à 0 pour les voisins f_k et les paramètres P_j, e_j sont envoyés aux voisins, sinon, on envoie le message *Ready* avec les valeurs P_j, e_j au maître.
— Le noeud se met en attente pour des nouveaux messages.
Ce droit à l'émission favorise les flux avec un coefficient de refus e_k minimal. On sélectionne donc par un critère topologique le flux qui est le moins gênant dans le réseau tout en corrigeant cette sélection à chaque émission.

Traitement des messages par le maître

Si le noeud maître reçoit le message *Ready* pour tous les flux, il calcule :

$$Tps = \frac{\text{nombre de permissions à vrai} - \text{nombre de faux}}{\text{temps courant}} \tag{3.1}$$

Si $Tps < TpsW$ alors il envoie un message *Master Init* vers tous les noeuds, sinon il leur envoie le message *Master Ready*.

Dans cette dernière partie de l'algorithme, le maître évalue la bande passante Tps et la compare à la consigne $TpsW$. Si la valeur courante de la bande passante est inférieure à la consigne, le maître réinitialise les coefficients de refus.

3.4.2 Etude théorique de l'algorithme

Nous allons démontrer la convergence de la bande passante du réseau vers la valeur de consigne lors de l'execution de l'algorithme précédent. Pour cela, nous définissons une suite de sous-graphes du graphe de contention.

Définition 8. Soit $K_n(E_n, V_n), n \in \mathbb{N}$ une suite de sous graphe du graphe de contention G définie par :

$$K_n = \left\{ C_f, \text{une clique de } G \setminus \bigcup_{i=1}^{n-1} K_i / \exists f \in E_n \text{ avec } e_f = min \left\{ e_{\tilde{f}}, \tilde{f} \in G \setminus \bigcup_{i=1}^{n-1} K_i \right\} \right\}$$

Remarque. K_n est la réunion des cliques contenant un flux f qui a un coefficient de refus e_f minimal dans G privée des sous-graphes K_1 à K_{n-1}. Ainsi K_1 regroupe les cliques de G qui contiennent un flux avec un coefficient de refus minimal, en particulier la clique contenant f_1 de coefficient de refus $e_1 = min\{e_f, f \in E\}$.

Le théorème suivant montre que pour un ensemble de flux en état de transmettre ayant un coefficient de refus identique, nous pouvons trouver un sous-graphe K_n tel que cet ensemble de flux y est indépendant et maximal.

Théorème 3.4.1. *Soit $f_1, \dots f_p$ un ensemble de flux en transmission d'un graphe de contention G avec e_f comme coefficient de refus. Alors il existe $n \in \mathbb{N}$ tel que $f_1, \dots f_p$ est un ensemble de flux indépendants maximals dans K_n.*

Démonstration. La démonstration se fait par récurrence.

Soit $f_1^1, f_2^1, \dots, f_{q_1}^1, f_1^2, \dots, f_{q_2}^2, \dots$ des flux en transmission de G tel que f_i^j a un coefficient de refus e_j. On suppose que $e_1 < e_2 < e_3 < \dots < e_n$.

Par le choix de l'algorithme, f_i^1 a le coefficient de refus e_1 minimal de sa clique $C_{f_1^1}$. Nous avons $C_{f_1^1} \subset K_1$ par la définition de K_1, qui n'est pas vide selon la remarque précédente.

Comme $f_1^1, \dots f_{q_1}^1$ sont en transmission, ils forment un ensemble de flux indépendant de K_1. Supposons que cet ensemble n'est pas maximal, alors il existe un flux f_1 de coefficient de refus e_1 qui n'appartient pas à E_1. Comme f_1 est en transmission, il a le coefficient de refus minimal de sa clique C_{f1} et donc $f_1 \in E_1$. Il y a une contradiction. L'ensemble $f_1^1, \dots f_{q_1}^1$ est donc maximal dans K_1.

Par récurrence, on suppose que $f_1^r \dots f_{q_r}^r$ est un ensemble indépendant maximal de K_r pour $r < n$.

Montrons que $f_1^n \dots f_{q_n}^n$ de coefficient de refus e_n est un ensemble indépendant maximal de K_n. Selon l'algorithme, chaque flux en transmission f_i^n a un coefficient de refus minimal pour sa clique $C_{f_i^n}$. Nous devons montrer que $C_{f_i^n} \subset K_n$ pour $1 \leq i \leq q_n$. Supposons que $f_i^n \notin E_n$ pour une valeur de i fixé alors il existe $r < n$, tel que $f_i^n \in E_r$, car $K_n \subset G \setminus K_1 \cup K_2 \cup \dots K_{n-1}$. f_i^n a un voisin dans sa clique f_i^r avec un coefficient $e_r < e_n$. Ceci est en contradiction avec le fait que f_i^n est en transmission.

L'ensemble de flux $f_1^n \dots f_{q_n}^n$ est donc indépendant et maximal dans K_n. Et donc par récurrence, ceci est vrai pour $n \in \mathbb{N}$. □

Le corollaire suivant donne une condition sur le coefficient de refus des flux en transmission pour avoir un débit maximal.

Corollaire 3.4.2. *Si $\forall f \in E$, le coefficient de refus e_f est égale au nombre de cliques maximales de f alors on a :*

$$Tps_n = Tps_{max}$$

Démonstration. Soit $f_1^1, f_2^1, \dots, f_{q_1}^1, f_1^2, \dots, f_{q_2}^2, \dots$ des flux en transmission de G tel que f_i^j a un coefficient de refus de e_j. On suppose que $e_1 < e_2 < e_3 < \dots < e_n$.

Soit $F_p = \{f_1^p, \dots, f_{q_p}^p\}$ l'ensemble indépendant maximal de K_p donné par le théorème 3.4.1.

Montrons que $F = \cup_p F_p$ est un ensemble indépendant maximal du graphe de contention G. Comme tous les flux sont en transmission, il est indépendant. Montrons qu'il est maximal.

On a $K_1 = \{C_f \subset G, \exists f \in E / e_f = min\{e_g, g \in E\}\}$. K_1 est l'ensemble des cliques de G contenant un flux avec un coefficient de refus minimal. On a, par hypothèse, que e_f est égale au nombre de cliques maximales de f. Comme les flux sont en transmission, l'algorithme a sélectionné les flux avec un coefficient de refus minimal. Donc F_1 est l'ensemble des flux indépendants de K_1 ayant un nombre de cliques maximales le plus petit dans G.

Pour chaque ensemble F_p, nous sélectionnons ainsi un nombre maximal de flux indépendant. Finalement, nous construisons un ensemble maximal de flux indépendants de G. C'est le plus grand ensemble de flux qui peut être en transmission simultanée. On a donc un débit maximal Tps_{max}.

□

A l'aide du corollaire précédent, nous pouvons établir une condition pour que la bande passante Tps de notre réseau converge vers la valeur Tps_{max}.

Théorème 3.4.3. *Si $TpsW \geq Tps_{max}$ alors on a :*

$$\lim_{n \to +\infty} Tps_n = Tps_{max}$$

Démonstration. Si $TpsW \geq Tps_{max}$ alors on a $Tps_n \leq TpsW$ pour tout n. Les coefficients de refus e_i seront toujours réinitialisés par notre algorithme à la valeur de clique maximale du flux f_i.

En utilisant le corollaire 3.4.2 on en déduit que $Tps_n = Tps_{max}$. □

Grâce au théorème 3.4.1 nous pouvons aussi donner une condition pour que la bande passante du réseau Tps_n converge vers la bande passante en fonctionnement équitable Tps_{fair}. Pour cela, nous allons établir préalablement un lemme.

Lemme 3.4.4. *Supposons qu'a l'instant n_0 tous les coefficients de refus e_i aient la même valeur $e_i = c_{n_0}$, $\forall i \in \mathbb{N}^*$, alors il existe un temps $n_1 \geq n_0$ tel que :*

$$Tps_{n_1} = Tps_{fair} \text{ et } e_i = c_{n_0} + 1 = c_{n_1}$$

Démonstration. A l'instant n_0, on a par hypothèse que tous les coefficients e_i ont la même valeur. Selon le théorème 3.4.1, l'ensemble des flux en transmission F_{n_0} est un ensemble maximal indépendant de K_{n_0}. A l'instant $n_0 + 1$, les flux en émission $f_1^{n_0}, \dots f_{q_{n_0}}^{n_0}$ ont comme coefficient de refus $e_i = c_{n_0} + 1$. Les autres flux, quant à eux, ont toujours un coefficient de refus égale à c_{n_0}. Les prochains flux en transmission auront donc un coefficient de refus égale à c_{n_0}. Ce sera un ensemble indépendant maximal de $G \setminus F_{n_0}$.

Par récurrence, on montre que

$$F_{n_0+p} \subset G \setminus F_{n_0} \cup F_{n_0+1} \cup \dots \cup F_{n_0+p-1}$$

Comme l'ensemble G est fini, il existe $n_1 \geq n_0$ tel que

$$G \setminus F_{n_0} \cup F_{n_0+1} \cup \dots \cup F_{n_1-1} = \emptyset$$

A cet instant, tous les flux ont transmis un paquet et ils ont comme coefficient de refus $c_{n_1} = c_{n_0} + 1$. □

Le prochain théorème nous montre que la bande passante de notre algorithme Tps_n converge vers Tps_{fair} si la valeur de la consigne $TpsW$ est petite.

Théorème 3.4.5. *Soit Tps_{min} la valeur minimum que peut atteindre la bande passante du réseau Tps_n obtenu par notre algorithme.*

Si $TpsW < Tps_{min}$ alors on a :

$$\lim_{n \to +\infty} Tps_n = Tps_{fair}$$

Démonstration. Comme on a $TpsW < Tps_{min}$ la bande passante du réseau Tps_n sera toujours supérieur à la consigne $TpsW$. Les coefficients de refus e_i ne sont donc jamais réinitialisés. A chaque instant, on choisit les valeurs minimum des coefficients de refus pour choisir les flux en émission. A chaque transmission, les coefficients de refus sont augmentés de 1. Il existe par conséquent un instant n_0 où tous les coefficients de refus sont égales à c_0.

Nous pouvons alors appliquer le lemme 3.4.4 : il existe un instant n_1 où $Tps_{n_1} = Tps_{fair}$ et $e_i = c_0 + 1$.

Nous pouvons établir facilement par récurrence que $\forall k \in \mathbb{N}^*$ on a :

$$Tps_{n_0 + k.n_1} = Tps_{fair}$$

Soit $p \in \mathbb{N}^*$ tel que $p \leq n_1$, on a alors :

$$Tps_{n_0 + k.n_1 + p} = \frac{T_{n_0 + k.n_1} + T_p}{n_0 + k.n_1 + p}$$

où $T_{n_0 + k.n_1}$ représente le nombre de paquets émis jusqu'à l'instant $n_0 + k.n_1$ et T_p le nombre de paquets émis pendant la durée p. Comme T_p est une valeur finie, on a :

$$\lim_{p \to +\infty} Tps_{n_0 + k.n_1 + p} = Tps_{fair}$$

Ceci prouve que :

$$\lim_{n \to +\infty} Tps_n = Tps_{fair}$$

□

Nous avons étudié les cas où $TpsW \geq Tps_{max}$ et $TpsW < Tps_{min}$. Nous allons maintenant étudier le cas où $Tps_{fair} \leq TpsW \leq Tps_{max}$. Le théorème suivant montre que la bande passante du réseau Tps_n tend vers la consigne $TpsW$:

Théorème 3.4.6. *Soit $TpsW$ la valeur de consigne tel que*

$$Tps_{fair} \leq TpsW \leq Tps_{max}$$

alors on a :

$$\lim_{n \to +\infty} Tps_n = TpsW$$

Le théorème 3.4.6 montre que nous contrôlons la bande passante du réseau si la valeur souhaitée se trouve dans l'intervalle $[Tps_{fair}, Tps_{max}]$.

Démonstration. Au commencement, tous les coefficients de refus sont initialisés à la valeur de clique maximale. Utilisant le corollaire 3.4.2 on a $Tps_n = Tps_{max}$.

Puis à chaque émission les coefficients de refus les plus faibles augmentent. Il arrive un moment n_0 où ils sont tous égaux. Selon le lemme 3.4.4 il existe un temps n_1 tel que $Tps_n = Tps_{fair}$.

Comme on a $TpsW \geq Tps_{fair}$, il existe un instant n_2 tel que $Tps_{n_2} \leq TpsW$. A cet instant, les coefficients de refus sont réinitialisés à la valeur de clique maximale.

Montrons qu'il existe $k \in \mathbb{N}$ tel que $Tps_{k+n_2} \geq TpsW$. Supposons que ce ne soit pas le cas, alors $\forall n \geq n_2$ on a $Tps_n \leq TpsW$. Dans ce cas, les coefficients de refus sont constamment réinitialisés à la valeur de clique maximale. On a alors $Tps_n = Tps_{max} \geq TpsW$. Ceci est une contradiction.

Ceci montre que Tps_n est en oscillation autour de la valeur de consigne $TpsW$.

Soit $\overline{Tps_n}$ la suite extraite qui contient les maximaux locaux de Tps_n et $\underline{Tps_n}$ la suite extraite qui contient les minimaux locaux de Tps_n tel que $\overline{Tps_n}$ et $\underline{Tps_n}$ soient deux extremum consécutifs. Alors on a selon la définition de Tps_n :

$$\lim_{n \to +\infty} \underline{Tps_n} = \lim_{n \to +\infty} \overline{Tps_n} = TpsW$$

Ceci montre que

$$\lim_{n \to +\infty} Tps_n = TpsW$$

□

Nous illustrons notre algorithme par des simulations.

3.4.3 Simulations

Environnement de Simulations

Les simulations que nous présentons ici utilisent le langage C et la bibliothèque OpenMPI. OpenMPI définit des fonctions de communications interprocessus pour le calcul parallèle. Nous utilisons ces communications pour simuler les communications inter-noeuds. Nous utilisons ces simulations avec différentes valeurs de $TpsW$ pour illustrer le comportement de notre algorithme.

Le graphe de contention du réseau est celui donné dans la figure 3.5. Pour ce réseau, nous avons $Tps_{fair} = 1.75$ et $Tps_{max} = 2$.

Simulation avec $TpsW = 1.8$

Nous avons $Tps_{fair} \leq TpsW \leq Tps_{max}$. La convergence de la bande passante Tps_n doit se faire vers $TpsW$. La figure 3.6 montre l'évolution de Tps_n au court du temps.

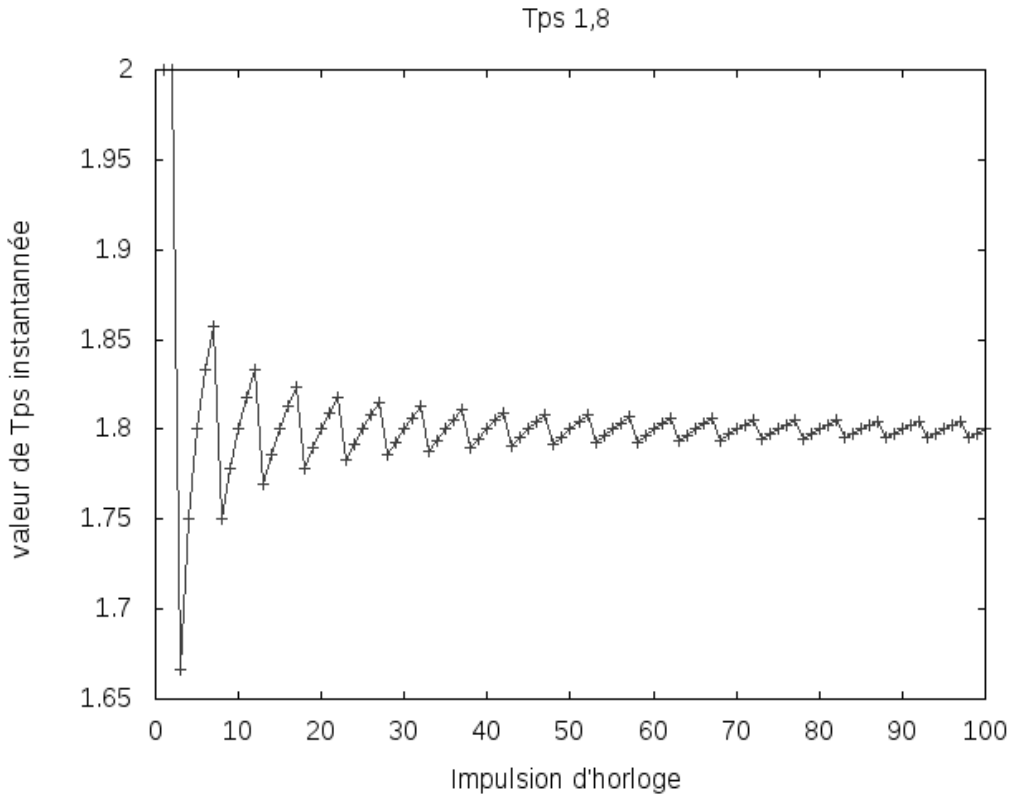

FIGURE 3.6 – Tps_n pour $TpsW = 1.8$

Nous remarquons l'oscillation et la convergence de Tps_n vers $TpsW$.

La figure 3.7 montre le nombre de paquets émis par chaque noeud en fonction du temps.

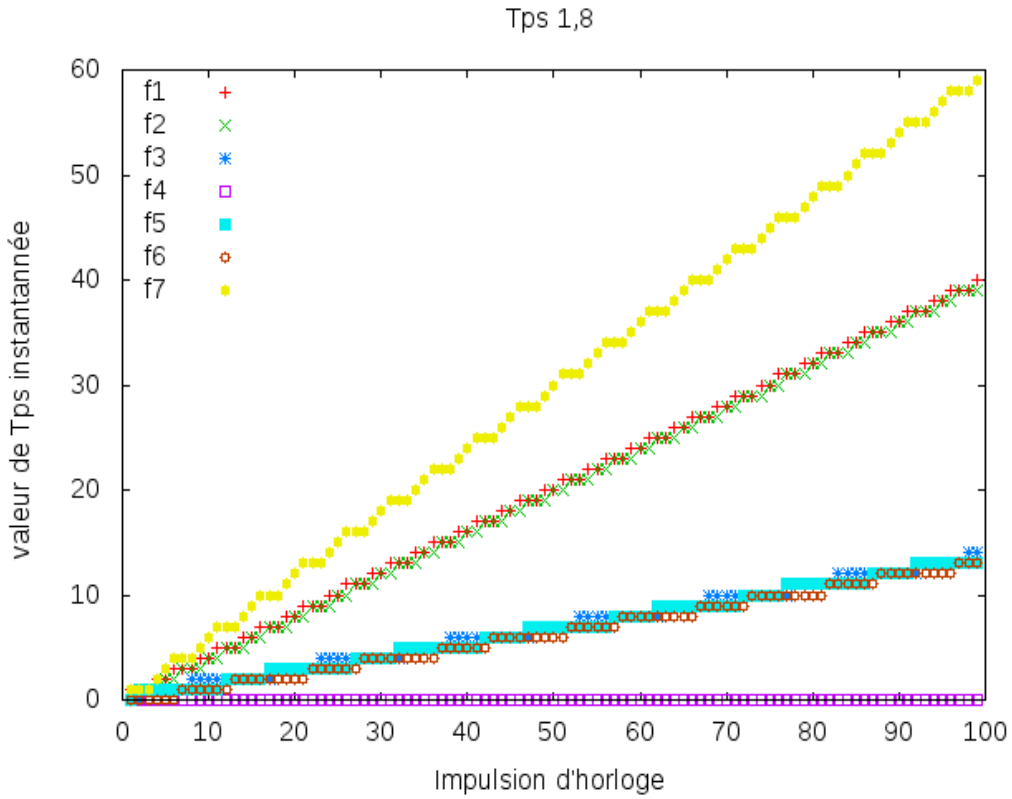

FIGURE 3.7 – Nombre de paquets émis pour $TpsW = 1.8$

Nous remarquons que le comportement du réseau n'est pas équitable et qu'il c'est formé quatre groupes de noeuds $\{f_7\}, \{f_1, f_2\}, \{f_3, f_5, f_6\}, \{f_4\}$. Dans chaque groupe, les noeuds ont un comportement équitable entre eux. Ceci est dû à une position topologiquement équivalente dans le réseau.

Simulation avec $TpsW = 1.5$

Nous avons $TpsW < Tps_{min}$, la convergence doit se faire vers Tps_{fair}.

La figure 3.8 montre l'évolution de Tps_n au court du temps.

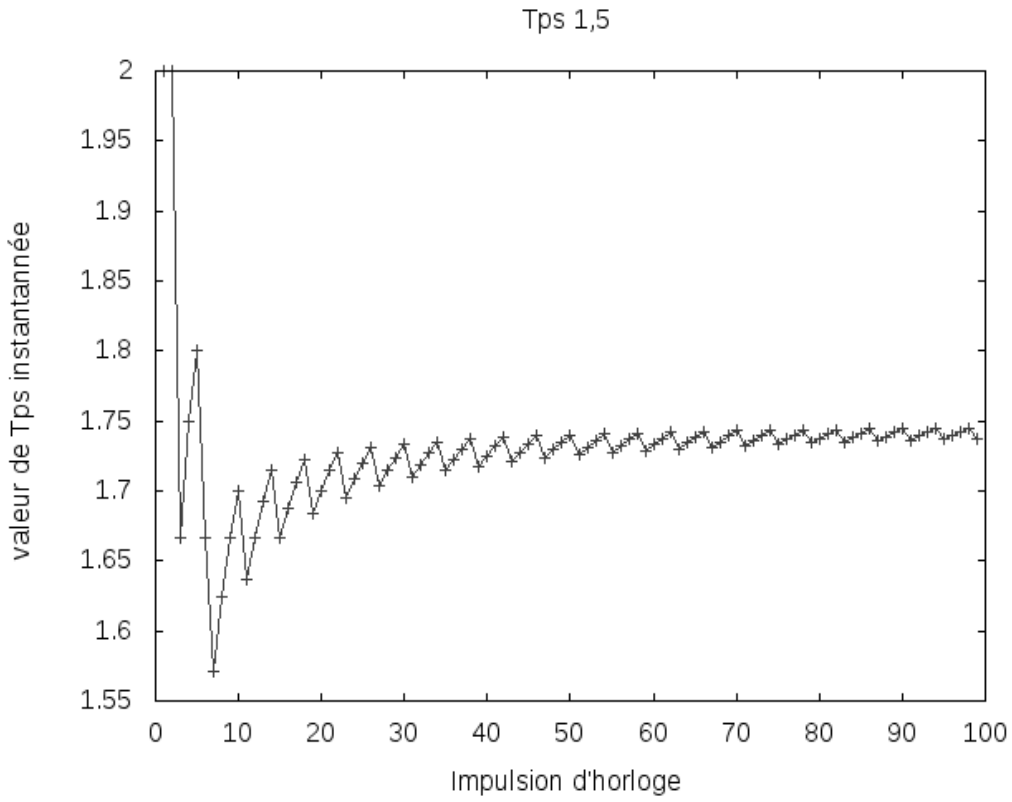

FIGURE 3.8 – Tps_n pour $TpsW = 1.5$

Nous remarquons l'oscillation et la convergence de Tps_n vers Tps_{fair}.

La figure 3.9 montre le nombre de paquets émis par chaque noeud en fonction du temps.

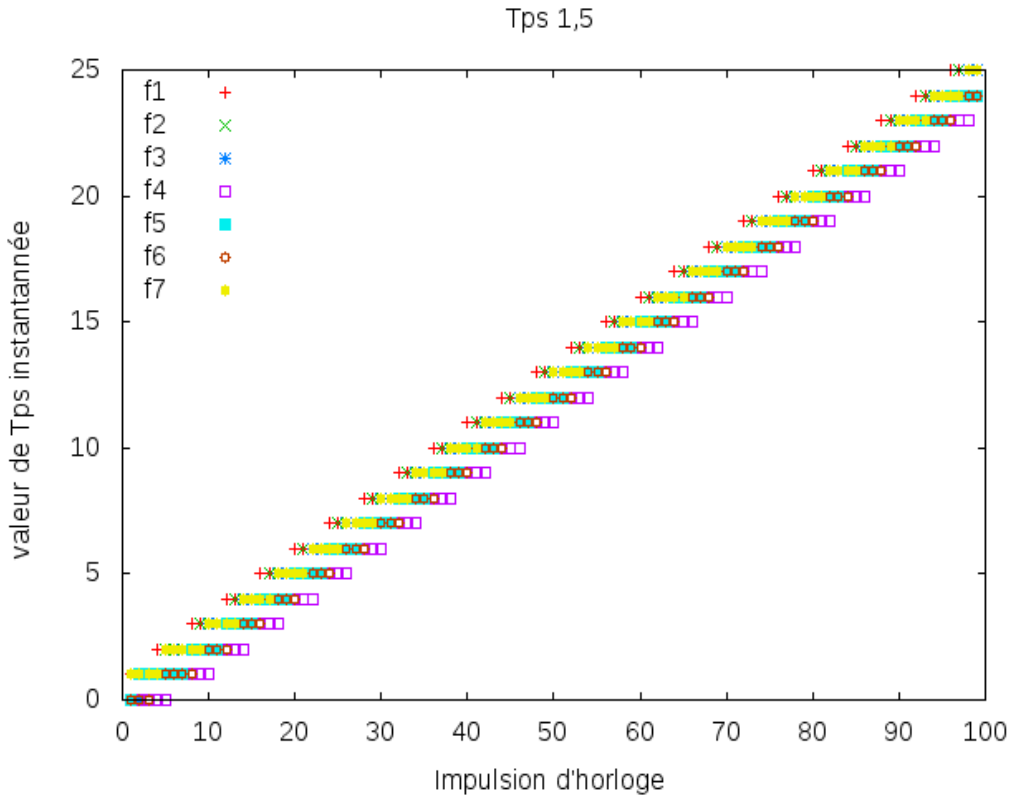

FIGURE 3.9 – Nombre de paquets émis pour $TpsW = 1.5$

La figure 3.9 confirme le comportement équitable du réseau.

Simulation avec $TpsW = 2$

Nous avons $TpsW = Tps_{max}$, la convergence doit se faire vers Tps_{max}.

La figure 3.10 montre l'évolution de Tps_n au court du temps.

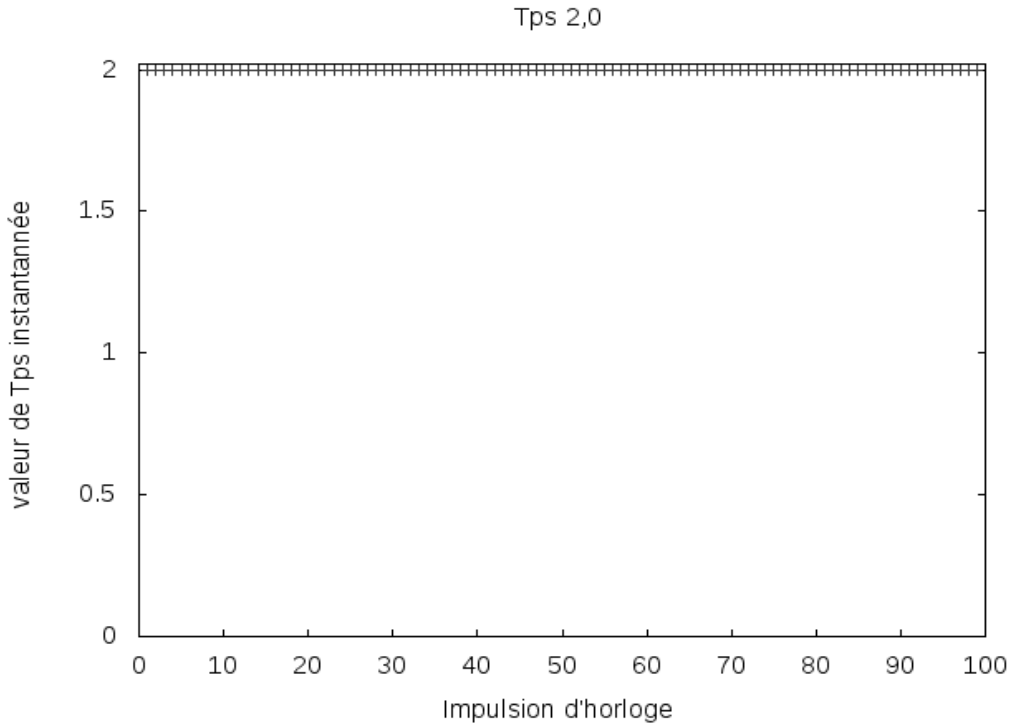

FIGURE 3.10 – Tps_n pour $TpsW = 2$

Nous remarquons qu'il n'y a pas d'oscillations et la convergence de Tps_n vers Tps_{max}.

La figure 3.11 montre le nombre de paquets émis par chaque noeud en fonction du temps.

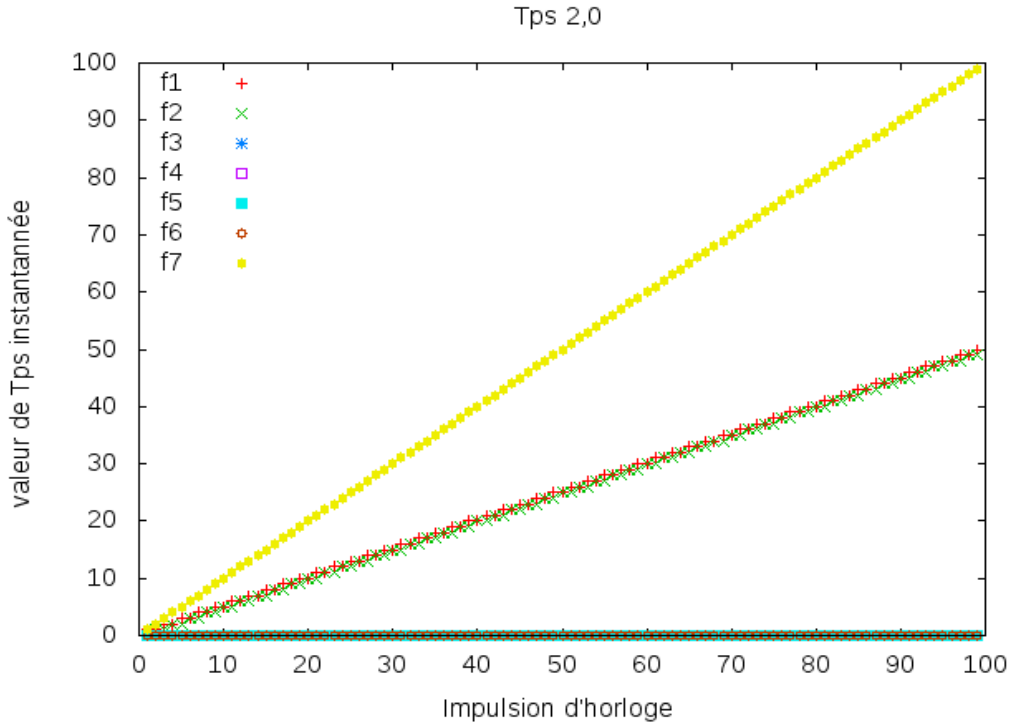

FIGURE 3.11 – Nombre de paquets émis pour $TpsW = 2$

La figure 3.11 montre toujours 3 groupes de noeuds : le premier est en émission constante, ce sont des noeuds relativement indépendants. Un deuxième groupe, où les émissions se font en alternance dans le groupe, et un troisième groupe qui n'émet jamais. La encore la position du flux dans le graphe de contention est déterminante.

3.4.4 Conclusion de l'algorithme d'accès utilisant les cliques

Ce premier algorithme que nous présentons ici permet de contrôler dans une certaine mesure la bande passante du réseau. L'étude théorique a établi cette convergence. Cet algorithme est basé sur la topologie du graphe de contention du réseau. Les simulations ont confirmées les résultats obtenus de manière théorique, mais elles ont surtout mis en évidence que la position des flux dans le graphe de contention est déterminante. Il semble que nous pouvons établir des comportements similaires en fonction une position topologiquement équivalente. Le comportement équitable ou non a aussi été mis en évidence.

Une des faiblesses de notre algorithme est le recours à un noeud maître qui centralise et organise l'émission des paquets. Ceci est contre la philosophie des réseaux Ad-Hoc et pénalise la mobilité des noeuds. Nous proposons un autre algorithme qui sera totalement distribué pour contrer cette faiblesse.

3.5 Algorithme distribué pour le contrôle de la bande passante

3.5.1 Introduction

L'algorithme précédent se base sur le fait qu'un flux appartenant à un grand nombre de cliques maximales gène un grand nombre de noeuds s'il est en émission. La connaissance du nombre maximal de cliques nécessite une connaissance globale du réseau. Ceci est un obstacle pour les topologies changeantes, comme celles des réseaux mobiles.

L'algorithme que nous avons proposé dans [GL05] utilise le degré de chaque flux dans le graphe de contention comme régulateur. Effectivement, un flux avec un degré important dans le graphe de contention sera très perturbateur et empêchera un grand nombre de flux voisin d'exister. De plus, cette information étant locale, il suffit qu'un flux connaisse ses voisins pour déterminer son degré.

L'algorithme que nous présentons ici favorisera les flux avec un degré faible. Si deux flux adjacents ont le même degré, on choisira celui qui a émis le plus petit nombre de paquets. Si cela ne donne pas l'unicité, on choisira de plus celui avec l'adresse Mac la plus petite. Dans cette configuration, c'est un ensemble maximal indépendant de flux qui emmétra et la bande passante du réseau sera Tps_{max}.

Pour corriger cela, nous augmenterons formellement le degré d'un flux après chaque émission. Comme le degré le plus faible est choisi, il y aura un moment où tous les degré seront égaux. A ce moment, nous sommes dans une configuration équitable et la convergence de la bande passante du réseau se fera vers Tps_{fair}.

Pour obtenir des états intermédiaires, nous utilisons un paramètre r qui représente le seuil temporel entre deux activations consécutives d'un flux. Si $r \leq 0$ alors le flux sera activé sans contrainte et le réseau convergera vers un état équitable. Si r est infini, alors le degré reste constant et la bande passante convergera vers Tps_{max}.

3.5.2 Algorithme distribué

Initialisation

Au début, chaque noeud initialise les valeurs suivantes pour chaque flux f_i dont il est la source :
— e_i le degré du flux f_i.
— a_i = Faux, a_i est un booléen qui certifie qu'un noeud a acquitté le message pour le flux f_i.
— rn_i = Faux, rn_i est un booléen qui informe que le flux f_i est près à être activé.
— P_i = Faux, P_i est un booléen qui permet ou pas l'activation du flux f_i.
— $PP_i = 0$ le nombre d'activations du flux f_i.
— $time = 0$ l'heure courant, ici initialisé à 0
— $lastime = 0$ le moment de la dernière transmission
— r le paramètre de contrôle initialisé par l'administrateur
— deg_i le degré du flux f_i dans le graphe de contention.
— $elocal_i = deg_i$ une variable locale pour le degré.
Après l'initialisation, le noeud fait le calcul de permission et se met en attente d'un message.

Calcul de permission

Chaque noeud détermine pour chaque flux f_i, dont il est la source, la permission d'activation comme suite :

— P_i = Faux, pas d'activation à priori
— Si pour tous flux f_k voisin de f_i dans le graphe de contention on a P_k = Faux et $e_i \leq e_k$ alors P_i = Vrai. Dans ce cas, il faut :
  — mettre $a_k = 0$
  — mettre rn_k = Faux
  — envoyer les *Nouvelles valeurs* P_j, e_j à chaque voisin f_k (à chaque noeud source de f_k) sinon, on envoie les valeurs P_j, e_j à chaque voisin, y compris à la destination du flux f_j.

Traitement du message *Nouvelles valeurs* P_k, e_k

Si un noeud reçoit le message *Nouvelles valeurs* P_k, e_k du flux f_k pour le flux f_i alors il fait les opérations suivantes :
— Il met à jour les valeurs P_k, e_k pour le flux f_i.
— Il renvoie un message d'acquittement à destination du flux f_k.
— Il se met en attente de nouveaux messages

Traitement du message *Valeurs* P_k, e_k

Si un noeud reçoit le message *Valeurs* P_k, e_k du flux f_k pour le flux f_i alors il fait les opérations suivantes :
— Il met à jour les valeurs P_k, e_k pour le flux f_i.
— Il change la valeur rn_k = Vrai
— Si pour tous les flux voisins f_k, y compris f_i la valeur rn_k est vrai alors :
  — Si P_i = Vrai alors on incrémente PP_i, on sauvegarde le temps courant $lastime = time$, et f_i émet un paquet.
  — Pour tous les voisins f_k, y compris f_i, on met rn_k et P_k à Faux.
  — On incrémente l'horloge $time = time + 1$.
  — Si $time - lastime > r$ alors on met $elocal_i = -1$ sinon (si $elocal_i = -1$ alors $elocal_i = deg_i$)
  — Faire $e_i = elocal_i$
  — Faire un calcul de permission pour f_i
— Attendre un nouveau message.

Traitement du message d'acquittement de f_k

Si un noeud reçoit un acquittement du flux f_k pour f_i alors :
— Il met à jour les valeurs P_k, e_k
— Il met a_k = Vrai
— S'il a reçus tous les acquittements de tous les voisins f_k de f_i et si P_i = vrai, il vérifie si PP_i est minimal par rapport aux compteurs PP_k des flux voisin. Si ce n'est pas le cas, alors P_i = Faux.
— Il envoie le message *Valeur* P_i, e_i aux voisins, y compris f_i.
— Il attend un nouveau message

Réception d'un paquet par le flux f_k

Si un noeud reçoit un paquet par le flux f_k, alors :
— Il augmente le compteur PP_k.
— Il attend un nouveau message

3.5.3 Etude des coefficients e_i de l'algorithme distribué

L'algorithme précédent se base sur la valeur e_i des différents flux pour décider de leur activation. C'est le flux, avec la valeur e_i la plus petite par rapport à ses voisins, qui sera en mesure d'émettre. En regardant l'algorithme, nous pouvons formuler la remarque suivante :

Remarque. Soit T_i l'instant de la dernière activation du flux f_i. La valeur du coefficient e_i sera à l'instant T :
- $e_i = -1$ si $T - T_i > r$
- $e_i = deg(f_i)$ sinon

En accord avec la remarque précédente nous pouvons partitionner l'ensemble des flux à l'instant T en deux sous-ensembles :

$$NF_T = \{f_i \text{ tel que } e_i = -1\}$$
$$DF_T = \{f_i \text{ tel que } e_i = deg(f_i)\}$$

L'algorithme permet l'activation du flux f_i si pour tous ses voisins f_k on a $e_i \leq e_k$, $\forall f_k \in N(f_i)$, les voisins de f_i. Cela permet d'établir le lemme suivant :

Lemme 3.5.1. *Soit f_i un flux activé à l'instant T, alors :*
- *Si $N(f_i) \cap NF_T \neq \emptyset$ alors $f_i \in NF_T$*
- *Si $N(f_i) \cap NF_T = \emptyset$ alors $e_i = deg(f_i) \leq deg(f_k)$ pour $f_k \in N(f_i)$*

Démonstration. Soit f_i un flux activé tel que $N(f_i) \cap NF_T \neq \emptyset$. Alors f_i a un voisin f_k tel que $e_k = -1$. Comme f_i est activé on a $e_i \leq e_k = -1$. Ce implique que $e_i = -1$ et $f_i \in NF_T$.

Soit f_i un flux activé tel que $N(f_i) \cap NF_T = \emptyset$. Alors pour tous les voisins f_k de f_i ont $e_k = deg(f_k)$. Le flux f_i est activé, on a donc $e_i \leq e_k$ et par conséquent $deg(f_i) \leq deg(f_k)$. □

Le lemme suivant montre qu'a un instant donné, pour le flux f_i nous avons $e_i = -1$. Ceci garantie que le flux f_i sera activé au cours du temps.

Lemme 3.5.2. *Soit f_i un flux activé tel que $N(f_i) \cap NF_T = \emptyset$ à l'instant T. Alors il existe un instant T_0 tel que $0 \leq T_0 \leq r$ et :*

$$N(f_i) \cap NF_{T+j} = \emptyset \text{ pour } 0 \leq j \leq T_0$$
$$N(f_i) \cap NF_{T+T_0+1} \neq \emptyset$$

Démonstration. Soir f_i un flux activé tel que $N(f_i) \cap NF_T = \emptyset$ à l'instant T. Utilisant le lemme 3.5.1 on a $e_i = deg(f_i) \leq e_k = deg(f_k)$ pour tous les flux voisins f_k de f_i. A l'instant $T+1$ on a $T + 1 - T_i \leq r$ car $r > 0$ et f_i a été activé à l'instant T. Ceci implique qu'à l'instant $T+1$ on a toujours $e_i = deg(f_i)$.

Si tous les flux voisins f_k de f_i ont leur moment de dernière émission T_k tel que $T + 1 - T_k \leq r$ alors on a $e_k = deg(f_k)$ et $N(f_i) \cap NF_{T+1} = \emptyset$. Le flux f_i reste activé.

S'il existe un voisin f_k tel que $T+1-T_k > r$ alors on a $e_k = -1$. Ceci implique $N(f_i) \cap NF_{T+1} \neq \emptyset$. On a alors $T_0 = 0$.

Par récurrence, on montre que si $N(f_i) \cap NF_{T+1} = \emptyset$, le flux f_i reste activé et les flux voisins f_k ne sont pas activés jusqu'à $T - 1$. Ceci implique que $T_k \leq T - 1$ et $T + r - T_k > r$. Nous avons alors que $e_k = -1$ et $N(f_i) \cap NF_{T+r} \neq \emptyset$. Ceci prouve l'existence de T_0 tel que $0 \leq T_0 < r$. □

Le théorème suivant montre que pour $r = 1$, chaque flux tend vers le même nombre d'activations.

Théorème 3.5.3. *Si $r = 1$, on a pour chaque flux f_i, $1 \leq i \leq N$:*

$$Tps(f_i) = \frac{Tps}{N}$$

Où $N \in \mathbb{N}^*$ est le nombre total de flux possibles dans le réseau.

Démonstration. Selon le lemme 3.5.2, si $r = 1$ on a $T_0 = 0$. On en déduit alors que pour un flux activé f_i à l'instant T on a

$$N(f_i) \cap NF_{T+1} = \emptyset$$

Ceci implique que pour $T > 1$ les flux en transmission f_i ont leur coefficient $e_i = -1$. Le comportement d'un tel réseau est le même qu'un réseau où tous les coefficients $e_k = -1, \forall k$ sont constants. A chaque instant T, ce sont les flux les moins souvent activés qui transmettent.

Soit $P_k(T)$ le nombre de paquets transmis par le flux f_k à l'instant T. La différence de paquets transmit entre deux flux peut être au plus de N, le nombre total de flux. Pour chaque flux f_i et f_k on a :

$$P_i(T) - N \leq P_k(T) \leq P_i(T) + N$$

En sommant sur k et divisant par T, on obtient :

$$N\frac{P_i(T)}{T} - \frac{N^2}{T} \leq \frac{\sum_{k=1}^{N} P_k(T)}{T} \leq N\frac{P_i(T)}{T} + \frac{N^2}{T}$$

Si T tend vers l'infini, on a :

$$N \times Tps(f_i) \leq Tps \leq N \times Tps(f_i)$$

On en déduit que $Tps(f_i) = \frac{Tps}{N}$. □

On en déduit le corollaire suivant :

Corollaire 3.5.4. *Si $r = 1$, le meilleur débit pour un flux f_i est :*

$$Tps(f_i) = \frac{Tps_{fair}}{N}$$

Nous allons illustrer notre algorithme par des simulations.

3.5.4 Simulation de l'algorithme distribué

Environnement de simulations

Pour cette simulation nous utilisons la bibliothèque de programmation parallèle OpenMPI. Les simulations sont faites pour une durée de 100 impulsions d'horloge. Nous utilisons un réseau constitué de 16 noeuds reliés par 15 flux selon la figure 3.12.

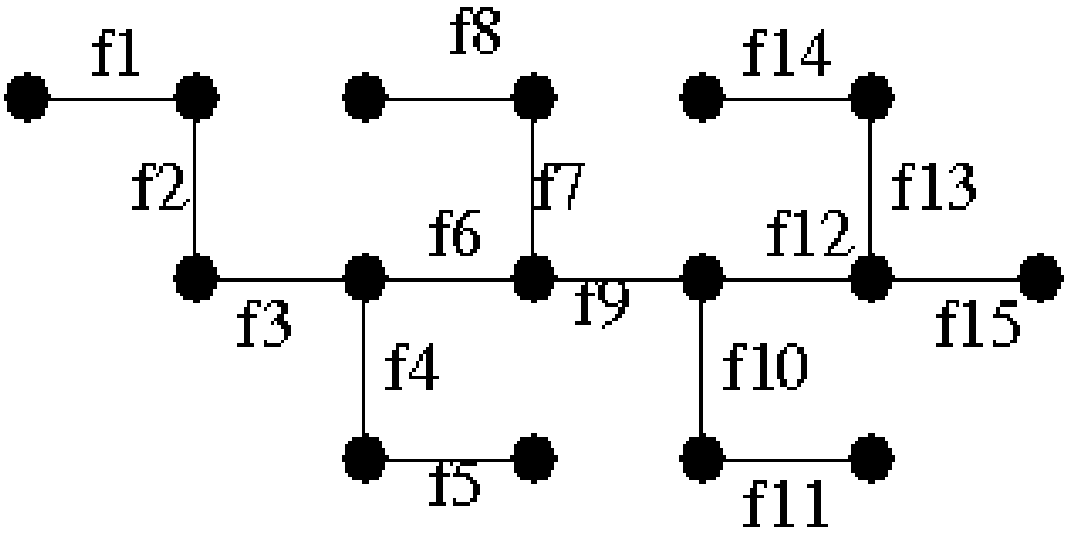

FIGURE 3.12 – Topologie du réseau Ad-Hoc à 16 noeuds

Le graphe de contention de ce graphe est donné dans la figure 3.13.

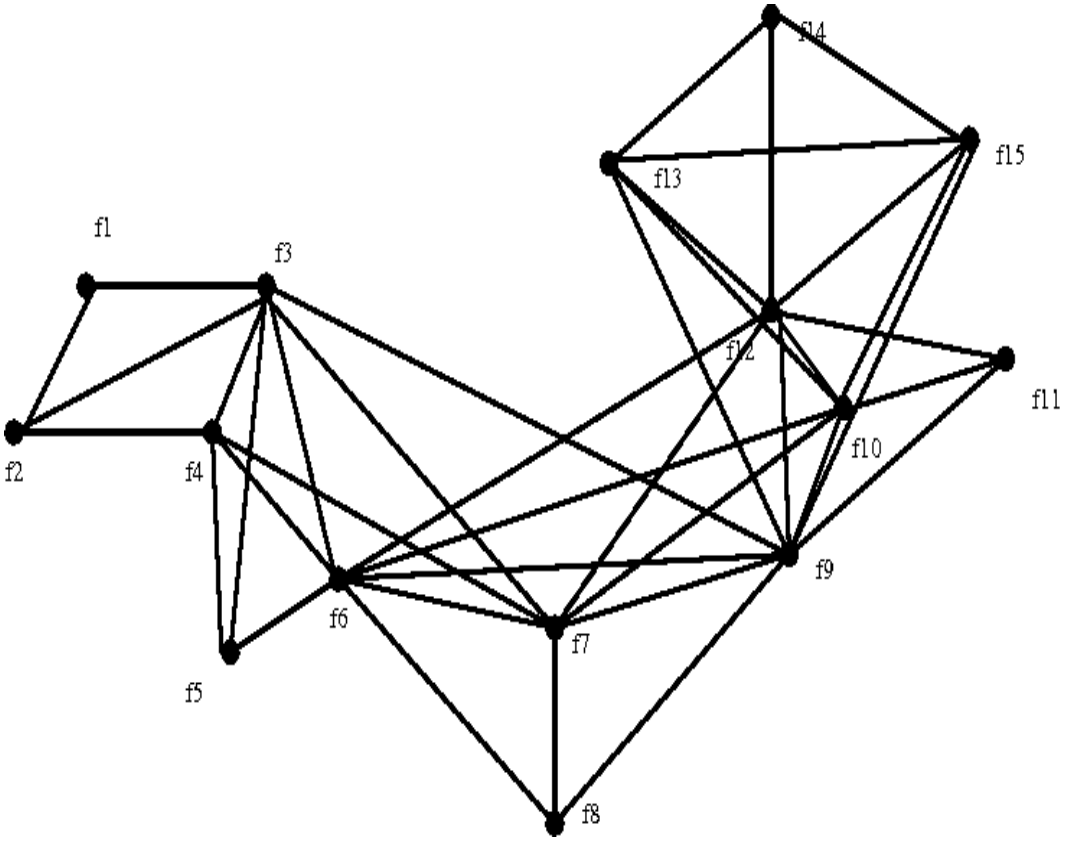

FIGURE 3.13 – Graphe de contention du réseau Ad-Hoc à 16 noeuds

Dans ce réseau, nous avons $Tps_{max} = 5$.

Débit instantané

Nous traçons le débit du réseau en fonction de r après 100 impulsions d'horloge :

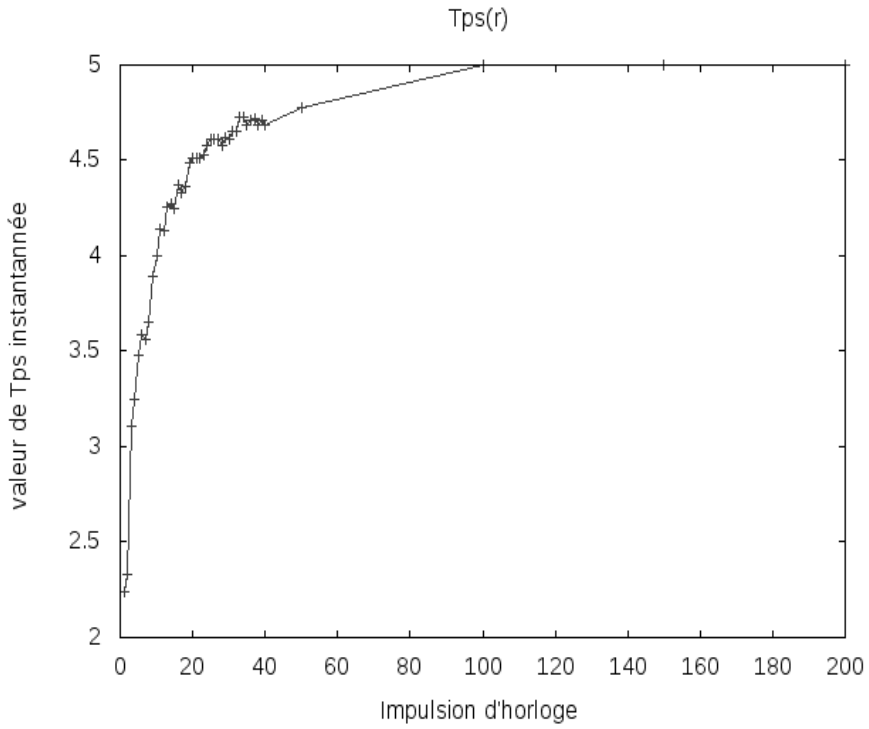

FIGURE 3.14 – Valeur de Tps en fonction de r

Dans la figure 3.14, nous remarquons que Tps augmente avec r de manière exponentielle. La valeur minimum pour Tps est obtenue avec $r = 1$ et vaut 2.25, ce qui est inférieur à Tps_{fair}. Cette valeur est dû au fait que pour $r = 1$ tous les flux susceptibles d'être activés ne le sont pas. Ceci est dû à la méthode anticollision de l'algorithme qui est trop limitative.

La valeur maximale pour Tps est $Tps_{max} = 5$, cette valeur est obtenue pour $r > 100$.

Nombre minimum et maximum de paquets transmis

La figure suivante montre le nombre minimum de paquets transmis en fonction de r pour un flux :

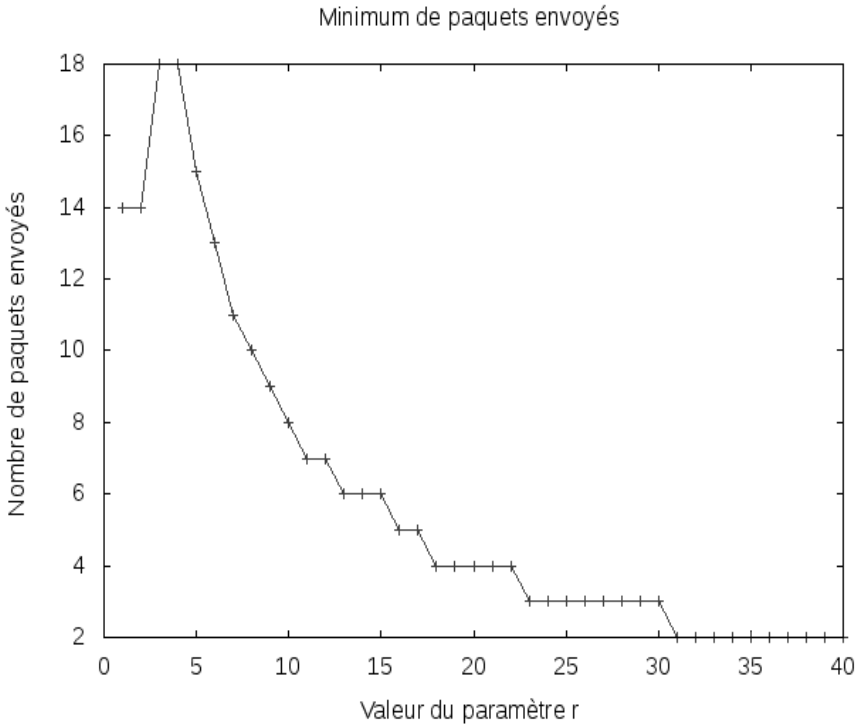

FIGURE 3.15 – Nombre de paquets minimum transmis en fonction de r pour un flux

Nous remarquons que dans la figure 3.15, le nombre de paquets décroît pour $r > 3$. Pour $r = 1$, nous avons 14 paquets transmis, ce qui est cohérent avec le théorème 3.5.3 :

$$Tps(f_i) = \frac{2.25}{15} = 0.15$$

Le graphique suivant montre le nombre maximum de paquets transmis par un flux en fonction de r :

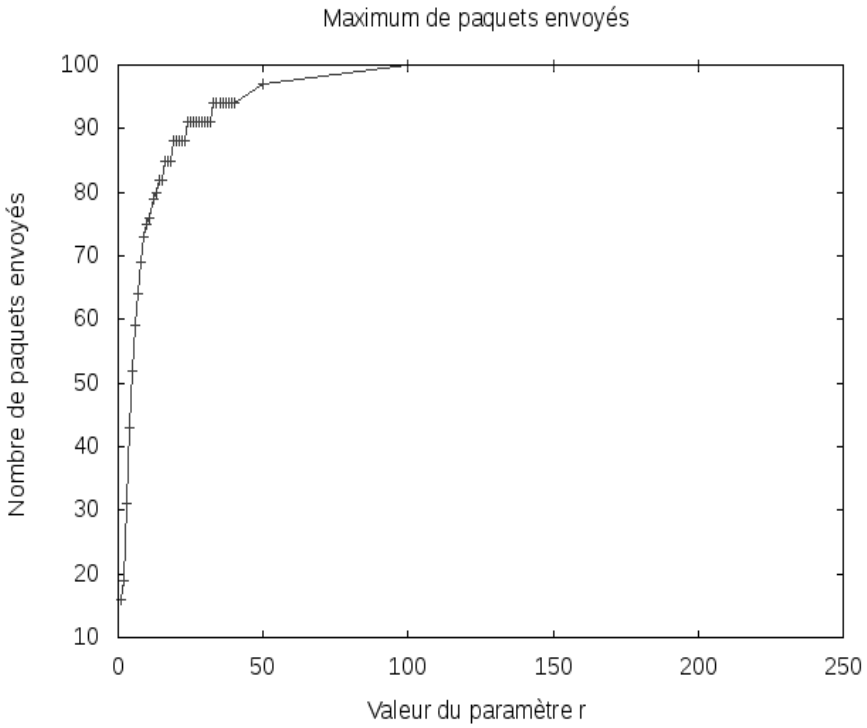

FIGURE 3.16 – Nombre de paquets maximum transmis en fonction de r pour un flux

La figure 3.16 montre que pour $r > 3$, le nombre maximal de paquets émis par un flux est croissant. On a 16 paquets émis pour $r = 1$, ce qui est cohérent avec le théorème 3.5.3.

Paquets envoyés en fonction du temps

Nous allons nous intéresser aux nombres de paquets transmis par chaque flux pour les valeurs de $r = 1, 5, 30$. Les graphes illustreront la capacité d'envoyer des paquets en fonction de la position des flux dans le graphe de contention.

La prochaine figure montre le nombre de paquets émis par flux pour $r = 1$:

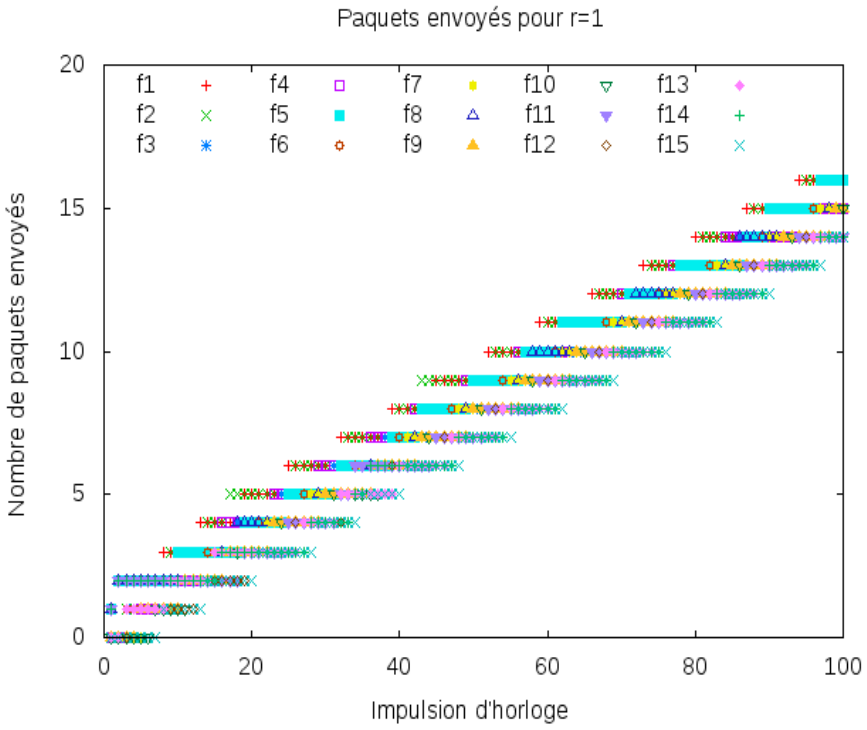

FIGURE 3.17 – Nombre de paquets transmis par un flux pour $r = 1$

Nous remarque que le comportement du réseau est équitable, car chaque flux a sensiblement le même nombre de paquets émis en fonction du temps.

La prochaine figure montre le nombre de paquets émis par flux pour $r = 5$:

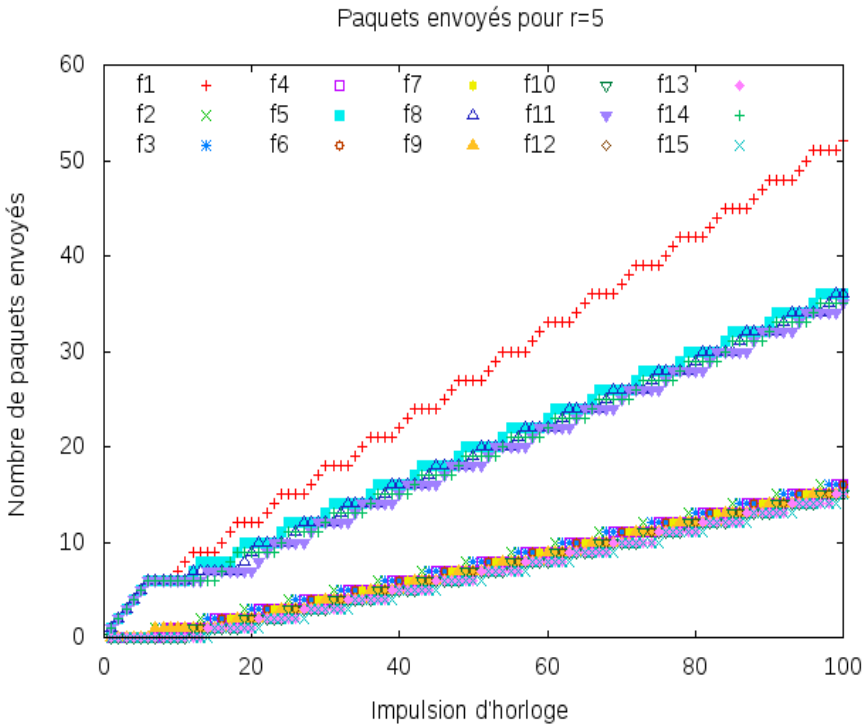

FIGURE 3.18 – Nombre de paquets transmis par un flux pour $r = 5$

Dans la figure 3.18, nous remarquons que le flux f_1, qui a le degré le plus petit, émet un grand nombre de paquets : 56 pour une durée de 100 impulsions d'horloge. Les flux f_5, f_8, f_{11} et f_{14} qui ont un degré de 3 émettent 36 paquets. Le flux f_3 a aussi un degré de 3, mais il entre en concurrence avec f_1. Il n'émet donc que 16 paquets, comme les autres flux du réseau.

Ceci montre clairement que le débit est déterminé par la situation topologique des flux dans le graphe de contention.

La prochaine figure montre le nombre de paquets émis par flux pour $r = 30$:

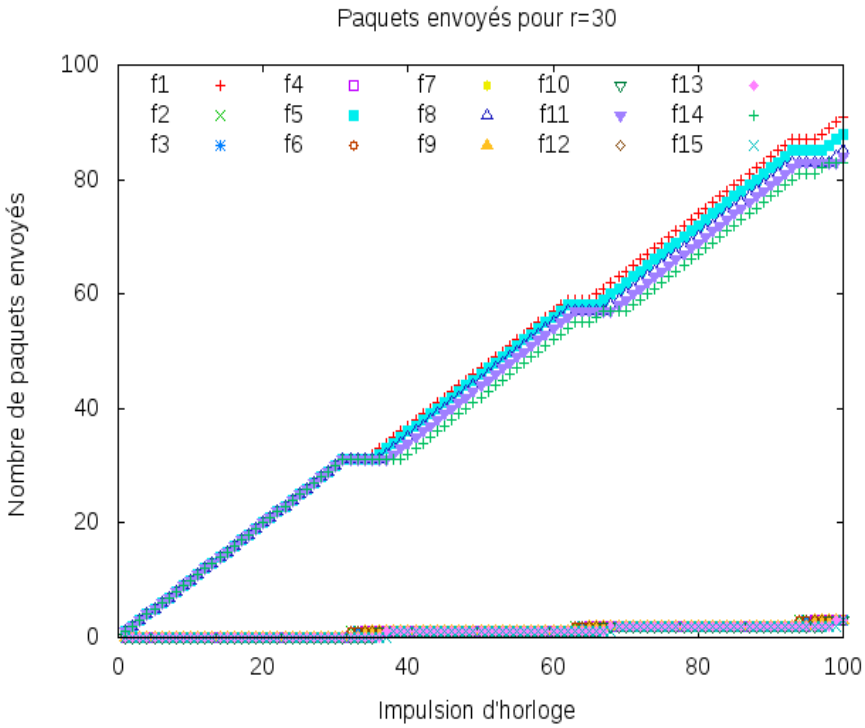

FIGURE 3.19 – Nombre de paquets transmis par un flux pour $r = 30$

Nous remarquons que dans la figure 3.19, les flux f_1, f_5, f_8, f_{11} et f_{14} émettent le plus de paquets. Ces flux forment un ensemble maximal indépendant de flux dans le graphe de contention. Il y a donc convergence de Tps vers Tps_{max}.

3.6 Conclusion

Dans ce chapitre, nous avons étudié la bande passant dans les réseaux Ad-Hoc. Nous avons présenté la problématique des collisions dans ces réseaux. Il en résulte la nécessité de gérer l'accès au réseau pour garantir une certaine bande passante. Pour cela, nous nous sommes intéressé aux flux qui transportent les paquets. La relation d'équivalence d'être contondant pour deux flux permet de créer le graphe de contention.

Dans le graphe de contention, deux flux voisins ne peuvent être activés à la fois sous peine de générer une collision. La notion de clique maximale permet d'identifier pour un flux donné, les flux qui sont contondant à celui-ci.

Nous nous sommes basé sur cette propriété pour élaborer deux algorithmes d'accès utilisant cette notion de graphe de contention. En faisant l'étude théorique de ces algorithmes et des simulations, nous avons mis en évidence que l'importance de la position topologique des flux dans le graphe de contention est primordiale pour leur activation ou non. Ainsi, des flux topologiquements équivalents sont activés par groupe de même degré de contention pour gérer la bande passante du réseau.

Nous avons aussi remarqué qu'un comportement équitable du réseau apparaît dans certains cas, et ceci au détriment de la bande passante maximale. Dans le chapitre suivant, nous allons nous intéresser à cette équité et le rapport qu'elle a avec la topologie du réseau Ad-Hoc.

Chapitre 4

L'équité dans les réseaux Ad-Hoc

4.1 Introduction

Dans le chapitre précédent, nous avons étudié la congestion dans les réseaux Ad-Hoc. Nous avons proposé plusieurs algorithmes pour contrôler le débit dans les réseaux Ad-Hoc. Au vu des simulations, ces algorithmes dans certaines conditions aboutissent à un comportement équitable du réseau. Nous avons aussi mis en évidence que la position des noeuds dans les réseaux Ad-Hoc est cruciale et que des positions topologiquements équivalentes donnent lieu à un même comportement.

Dans ce chapitre, nous allons approfondir l'étude sur le comportement équitable des réseaux Ad-Hoc. Comme nous l'avons vu au chapitre précédent, le comportement équitable d'un réseau Ad-Hoc est souvent contradictoire avec la recherche du débit maximal. De nombreuses études ont été réalisées sur l'équité des réseaux Ad-Hoc. Ces études agissent sur différents mécanismes pour parvenir à un comportement équitable.

Un premier levier possible pour obtenir l'équité est la modification de la couche MAC. Cette couche est responsable de l'envoi des paquets via le lien physique. Le protocole CSMA/CA utilisé au niveau MAC dans les réseaux Ad-Hoc conduit à l'inéquité, ce phénomène a été largement étudié dans [27]. Dans l'article [32], l'auteur propose la modification de la couche MAC pour résoudre le problème de l'équité entre flux et pour maximiser le débit du réseau. Le protocole DQMAN, proposé dans [7], se base sur un compromis entre une relation hiérarchique, dynamique et spontanée, entre des noeuds maîtres et esclaves. Le protocole PRAS-CP, présenté dans [6] régule la transmission des paquets au niveau MAC pour rechercher l'équité. Le protocole CSMA/CA définit une fenêtre de contention pour éviter la collision des paquets. Dans [75], l'auteur propose le protocole SBA qui modifie les fenêtres de contention standard pour améliorer l'équité et l'efficacité du réseau. Les articles [23], [62], [76] et [68] explorent la même voie avec les protocoles AEFT et NUM. Le protocole "Channel Mac", proposé dans [11], utilise un mécanisme distribué pour améliorer le débit ou l'équité. En wifi, le protocole 802.11e permet une gestion de la qualité de service. L'article [94] s'intéresse aux performances des protocoles 802.11e, EY-NPMA et DWOP par rapport à l'équité. La qualité de service, dont l'équité, est aussi étudiée dans [30] et [3]. Le contrôle de la congestion implique une gestion avancé de la disponibilité des liens. Cette gestion a une influence non négligeable sur l'équité comme le montre l'article [78]. Cette optimisation de l'utilisation de la bande passante se retrouve dans le protocole OCSMA proposé dans [17]. D'autres articles proposent la modification de la couche MAC pour la recherche de l'équité pour d'autres types de réseaux comme ceux basés sur le mécanisme d'accès TDMA [65], ou plus généralement [28] et [16]. Le réordonnancement de l'envoi des paquets par la couche MAC est proposé dans [101].

La modification de la couche MAC est l'un des moyens pour obtenir un comportement équitable. Plus précisément, c'est la régulation de l'envoi des paquets qui permet d'obtenir l'équité. L'article

[21] formalise ce problème par un problème d'optimisation. Une approche probabiliste a permis d'élaborer le protocole PCRQ décrit dans [31]. L'article [87] propose aussi une approche probabiliste. Dans [63] l'équité est obtenue en adoptant un ordonnancement de l'envoi des paquets en fonction des chemins. Le problème plus complexe de l'équité des réseaux MIMO est étudié dans [45]. Le protocole FQ-EDCA proposé dans [2] optimise la qualité de service dans le but d'établir un ordonnancement équitable de la transmission de paquets. L'algorithme DOS décrit dans [103] implémente un mécanisme distribué pour l'envoi de paquets. L'algorithme STFQ de [18] utilise la même philosophie en s'appuyant sur les noeuds voisins. L'auteur de [88] propose de réglementer l'envoi de paquets en utilisant différentes régions. L'ordonnancement de l'envoi des paquets pour la recherche de l'équité est donc l'un des moyens privilégiés. Le protocole CHOKeW, décrit dans [96], régule la transmission de paquets pour obtenir une équité spécifique aux flux TCP.

L'équité est souvent orienté équité de la transmission de paquets dans les réseaux Ad-Hoc. Elle peut aussi s'exprimer différemment en fonction du protocole de transport utilisé. Par exemple TCP introduit des contraintes particulières liées à la validation des transmissions. L'équité à ce niveau se heurte au phénomène de congestion particulier à TCP. L'article [86] propose comme solution le protocole TCP Adaptive RTO pour améliorer l'équité des transmissions TCP. Une modification du protocole TCP, Transport Protocol for Ad-Hoc (TPA), décrit dans [9] permet aussi d'améliorer l'équité. Le routage, se situant au niveau 3 du modèle OSI, est aussi un levier sur lequel on peut agir pour améliorer l'équité dans un réseau. L'auteur de [83] propose plusieurs stratégies de routage pour maximiser le débit et l'équité d'un réseau Ad-Hoc. L'article [37] se contente d'améliorer l'équité des flux TCP en s'appuyant uniquement sur le routage. L'agrégation des flux au niveau routage proposé dans [53] est aussi une voie possible. Cette agrégation de flux devient cruciale si le protocole TCP est utilisé. Effectivement, l'article [81] montre l'importance de réduire les flux de contrôle TCP en mutualisant les transferts pour améliorer le débit et l'équité d'un réseau Ad-Hoc. La spécificité des réseaux multicast demande aussi la modification du routage pour obtenir une utilisation équitable des réseaux Ad-Hoc. L'article [70] propose une telle modification en utilisant des informations de positionnement des noeuds.

La recherche de l'équité peut conduire à des approches plus originales. Certains articles [43], [14] et [34] proposent d'utiliser la théorie des jeux pour parvenir à l'équité. D'autres [24] et [25] développement un protocole coopérative pour être équitable. Une approche probabiliste du problème est donnée dans [57]. On peut aussi parvenir à des algorithmes complexes de type cross-layer [39]. Nous pouvons aussi avoir des notions d'équité dans des domaines les plus divers comme le commerce électronique [91], la répartition d'énergie [55] ou la sécurité [92].

L'équité est ainsi un vaste champ de recherche. Mais de quelle équité parle-t-on ? Les articles précédents se focalisent sur l'équité dans les réseaux Ad-Hoc. Mais plusieurs équités sont données : équité sur l'émission de paquets, équité des flux TCP, etc .... Dans notre travail, nous avons besoin de formaliser cette équité. Une définition mathématique de l'équité a été proposée par R. K. Jain, D. W. Chui et W. R. Hawe dans [74]. Ce travail a été le point de départ de la thèse de A. Makhlouf que j'ai encadré, et à donner lieu à deux communications dans des conférences internationales [GLM08], [MGL09] et une publication dans un journal [GML09].

Dans ce chapitre, nous introduisons l'équité par le formaliste mathématique donné dans [74]. Ensuite, nous chercherons à évaluer l'index d'équité pour un réseau Ad-Hoc. Pour cela nous tenterons d'approcher ces réseaux par une topologie particulière : les réseaux étoiles et des combinaisons de ces réseaux. Nous établirons la condition pour qu'un réseau étoile soit équitable. Nous montrerons aussi que pour les réseaux double-étoile, l'équité n'est pas possible. Nous exposerons ensuite plusieurs protocoles pour améliorer l'index d'équité d'un réseau. Des simulations viendront terminer ce chapitre.

4.2 Index d'équité

4.2.1 La notion d'équité

L'équité est souvent une notion intuitive. Dans un réseau Ad-Hoc, chaque noeud est susceptible d'émettre ou de recevoir des paquets. Regardant un tel réseau, comment dire si son fonctionnement est équitable ? Est-il équitable si chaque noeud accède pendant la même durée aux ressources du réseau ? Ou bien, le réseau est équitable si chaque noeud transmet la même quantité de paquets ? Dans ce cas, faut-il comptabiliser les paquets de contrôle, ou uniquement l'information "utile" ? Si nous nous plaçons au niveau d'un noeud, si celui-ci ne reçoit jamais de paquets, cela lui donnera un sentiment d'injustice. Faut-il donc évaluer l'équité en fonction des paquets reçus ? Nous pouvons constater que la notion d'équité peut avoir un sens très différent.

Un autre problème que nous pouvons soulever est de savoir comment quantifier l'équité. Dans un réseau, si 80% des noeuds émettent le même nombre de paquets, nous voulons dire que ce réseau est plus équitable qu'un réseau ou seulement 10% des noeuds émettent le même nombre de paquets. L'article [74] tente de répondre à ces questions en introduisant l'index d'équité.

4.2.2 Propriété de l'index d'équité

Nous voulons évaluer l'équité d'un système distribué pour une population donnée. Dans notre cas, il s'agit de l'allocation de certaines ressources pour un réseau comportant un certain nombre de noeuds. Nous souhaitons évaluer l'équité pour l'accès à ces ressources dans le réseau. Pour cela nous définissons l'index d'équité ayant comme propriétés :

- *d'être indépendant vis à vis la taille de la population :* l'index devra s'applique quel que soit le nombre de noeuds, fini ou infini.
- *d'être indépendant vis à vis de la métrique et de l'échelle :* l'index d'équité s'applique pour une ressource donnée. Cet index ne devra pas dépendre de l'unité de mesure appliquée à cette ressource.
- *être dans l'intervalle* $[0, 1]$ *:* nous voulons un index qui peut s'exprimer comme un pourcentage.
- *être une fonction continue :* nous voulons qu'une variation sur l'allocation d'une ressource implique une variation de l'index d'équité.

4.2.3 Définition de l'index d'équité

L'index d'équité est une fonction qui dépend des ressources x dont on veut mesurer l'équité pour une population donnée.

Définition 9 (Index d'équité)**.** Dans un système distribué, chaque entité i se voit attribuer une ressource x_i. L'**index d'équité** $f(x)$ est la fonction :

$$f(x) = \frac{\left(\sum_{i=1}^{n} x_i\right)^2}{n \sum_{i=1}^{n} x_i^2} \quad x_i \geq 0$$

où n représente le nombre total d'entités.

Remarque. L'index d'équité est proche de notre intuition. Supposons que les ressources allouées x_i soient toutes identiques, on a alors $f(x) = 1$.

Si par contre une seule entité se voit attribuer une ressource x_1, on a alors :

$$f(x) = \frac{x_1^2}{nx_1^2} = \frac{1}{n}$$

On a alors $\lim_{n \to +\infty} f(x) = 0$, l'inégalité augmente et l'index devient nul si le nombre d'entités augmente.

Les exemples suivants montrent que l'index d'équité mesure bien le manque d'égalité d'un système de ressources distribuées.

Example. Supposons que nous avons un système distribué composé d'une population de 100 personnes et que nous voulons répartir 20 euros entre ces personnes. Nous pouvons :

- donner 0,2 euros à chaque personne : c'est une répartition équitable et l'index d'équité vaut 1.
- donner 2 euros à 10 personnes : l'index d'équité vaut alors $0,1$, soit 10%.
- donner 1 euros à 20 personnes : l'index d'équité vaut alors $0,2$, soit 20%.

Définition 10 (Index de discrémination)**.** L'**index de discrimination** est l'index qui mesure l'inégalité d'un réseau. Il est donné par la formule :

$$f_d(x) = 1 - f(x)$$

C'est le complémentaire à 1 de l'index d'équité.

L'index d'équité permet de mesurer le niveau d'équité d'un système distribué. Nous allons l'appliquer aux réseaux Ad-Hoc. Ici le système est composé des noeuds du réseau. Pour chaque noeud, nous choisissons d'utiliser le **nombre de paquets émis ou reçus comme mesure de la ressource** que nous étudions. Ainsi un réseau équitable sera un réseau où tous les noeuds ont un taux d'émission similaire. Ceci correspond à la notion d'équité donnée au chapitre 3.

4.2.4 L'équité pour les simulations de l'algorithme distribué

Nous pouvons d'ailleurs tracer l'index d'équité des simulations du chapitre 3. Par exemple,la figure 3.17 qui représente les paquets envoyés en fonction du temps permet de tracer l'index d'équité :

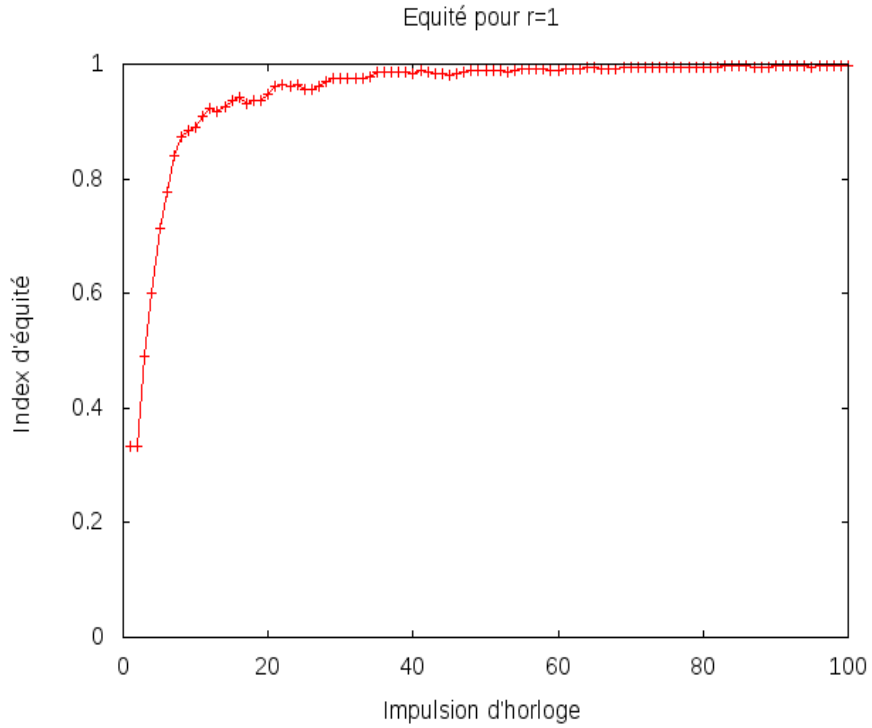

FIGURE 4.1 – Index d'équité pour $r = 1$

Nous remarquons que pour $r = 1$ nous avons un comportement équitable du réseau. Ce qui était signalé dans le chapitre 3. L'index d'équité est cohérent avec l'intuition que nous avons sur la notion d'équité. Regardons comment évolue cette équité en changeant le paramètre r.

Pour $r = 5$ nous avons la figure 4.2.

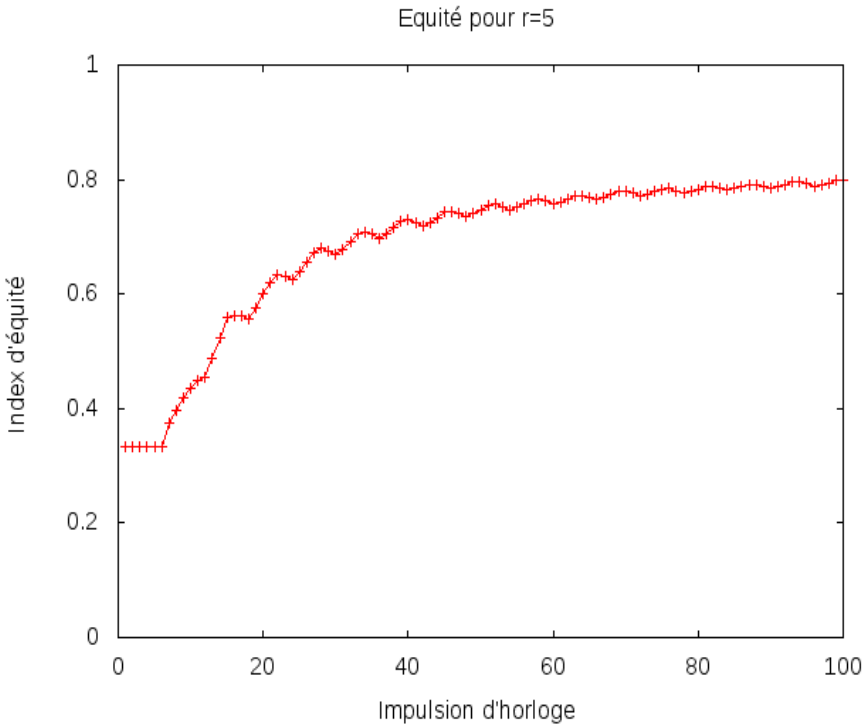

FIGURE 4.2 – Index d'équité pour $r = 5$

L'index d'équité est plus faible, environ $0,8$. Ce qui montre que les flux ont des débits différents. La figure 3.18 montre 3 groupes de flux. Le plus important comporte 10 flux sur 15. Il y a donc $\frac{10}{15} \approx 0,66\%$ de flux qui sont équitables entre eux. Ce qui est proche de la valeur $0,75$.

Pour $r = 30$ on a un index d'équité qui varie selon la figure 4.3.

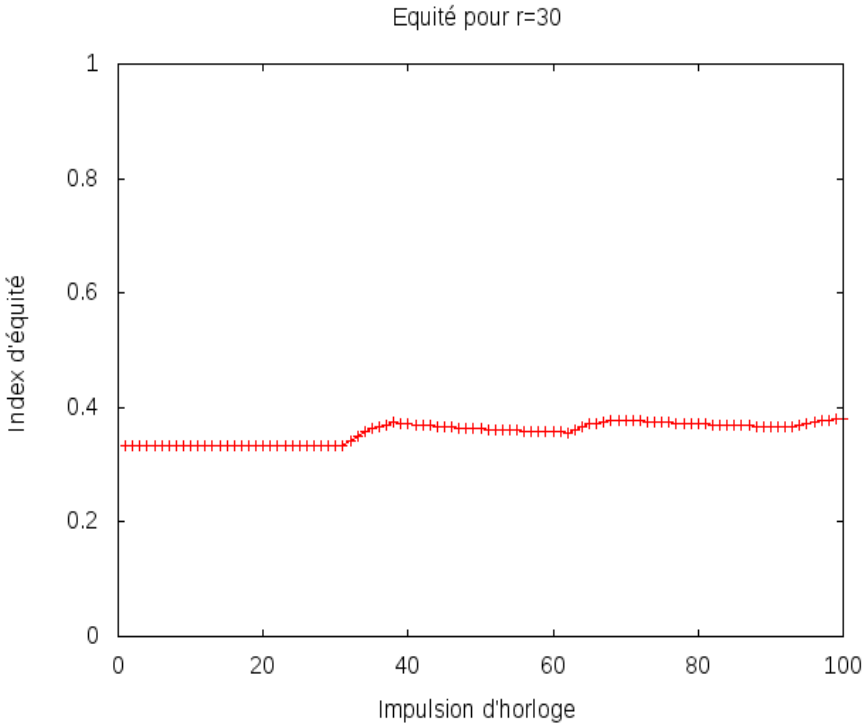

FIGURE 4.3 – Index d'équité pour $r = 30$

Nous remarquons que l'index d'équité est stable à $0,37$ ce qui est plutôt mauvais. En regardant la figure 3.19, nous remarquons qu'il y a 5 flux qui émettent régulièrement des paquets. On a donc $\frac{5}{15} \approx 0,33\%$ de flux en émissions, ce qui est proche de $0,37$.

Ces quelques exemples montrent que l'index d'équité correspond bien à la notion intuitive qu'on a de l'équité. L'index permet aussi de mesurer l'importance du comportement équitable ou non. Mais ici, on a évalué l'index d'équité à partir de simulations. Mais qu'en est-il pour un réseau quelconque ? Peut-on donner l'index maximal possible ? Pour essayer de répondre à ces questions, nous proposons de faire une étude théorique sur des topologies particulières.

4.3 L'équité dans les topologies réseaux en étoile

4.3.1 L'index d'équité pour un réseau Ad-Hoc

Évaluer l'index d'équité pour un réseau Ad-Hoc est un problème complexe. Pour avoir une estimation de l'index, nous proposons d'approcher un réseau Ad-Hoc quelconque par une suite de réseaux en étoiles qui seront reliés entre eux. Cela simplifiera le problème et permettra de donner, dans une certaine mesure, une condition pour avoir un fonctionnement équitable du réseau, c'est à dire avec un index d'équité de 1. Étudions dans un premier temps l'équité d'un réseau étoile.

4.3.2 Réseaux étoiles

Le réseau **étoile** est constitué d'un noeud central qui communique avec n voisins. C'est le réseau le plus élémentaire. La figure 4.4 montre ce type de réseau.

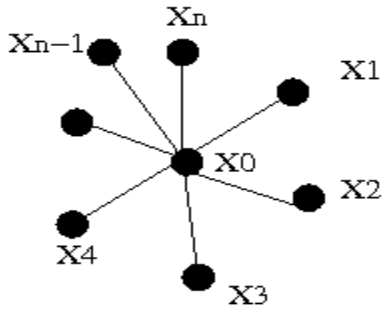

FIGURE 4.4 – Réseau étoile

Définition 11 (Réseau étoile)**.** Un réseau étoile SN_n est composé de $n+1$ noeuds $\{X_1, X_1 \ldots, X_n\}$ tel que les noeuds $\{X_1, \ldots, X_n\}$ sont voisins de X_0 et tel qu'il n'existe pas de connexion entre les noeuds X_i, X_j pour $i, j > 0$.

Calculons l'index d'équité pour ce réseau. Ici la ressource considérée est le nombre de paquets reçus par unité de temps, ce qui représente le taux de réception. Le réseau sera dit équitable si chaque noeud à le même taux de réception.

Nous supposons que :
— x_i représente le taux de réception d'un noeud,
— $r_{j,i}$ représente le taux de réception des paquets provenant du noeud X_i reçu par le noeud X_j,
— D_i représente le nombre de voisins (degré) du noeud X_i,
— S_j représente le taux de transmission du noeud X_j.

Le taux de réception x_i du noeud X_i est la somme des taux de réception des paquets reçus par chaque voisin de X_i. On a donc avec les notations précédentes :

$$x_i = \sum_{j=1}^{D_i} r_{i,j}$$

Nous supposons qu'il n'y a pas de perte de paquets. Dans un réseau étoile, le taux de réception des paquets provenant par X_i reçu par X_0 correspond au taux de transmission de X_i soit S_i. On a donc $r_{0,i} = S_i$ et :

$$x_0 = \sum_{j=1}^{n} S_j$$

Si le noeud central X_0 émet un paquet, tous les voisins reçoivent ce paquet et X_0 est la seule source possible pour les noeuds $X_i,\ i \geq 1$, on a donc $r_{i,0} = S_0,\ i \geq 1$.

Nous pouvons en déduire le lemme suivant :

Lemme 4.3.1. *Soit SN_n un réseau étoile. Soit S_i le taux de transmission du noeud X_i, alors le réseau SN_n est équitable si et seulement si :*

$$S_0 - \sum_{i=1}^{n} S_i = 0 \tag{4.1}$$

Démonstration. L'index d'équité du réseau étoile SN_n est donné par la formule :

$$f(x) = \frac{\left(\sum_{i=0}^{n} x_i\right)^2}{(n+1)\sum_{i=0}^{n} x_i^2}$$

ce qui implique

$$\begin{aligned} f(x) &= \frac{\left(\sum_{j=1}^{n} S_j + \sum_{i=1}^{n} S_0\right)^2}{(n+1)\left(\sum_{j=1}^{n} S_j\right)^2 \sum_{i=1}^{n} S_0^2} \\ &= \frac{\left(\sum_{j=1}^{n} S_j + nS_0\right)^2}{n(n+1)\left(\sum_{j=1}^{n} S_j\right)^2 S_0^2} \end{aligned}$$

Si le réseau est équitable, nous avons $f(x) = 1$. Ce qui implique :

$$\left(\sum_{j=1}^{n} S_j + nS_0\right)^2 = n(n+1)\left(\sum_{j=1}^{n} S_j\right)^2 S_0^2$$

En développant et simplifiant on obtient la condition :

$$S_0 - \sum_{i=1}^{n} S_i = 0$$

□

Remarque. Pour un réseau étoile équitable, le nombre de paquets émis par le noeud central est égale à la somme des paquets émis par les noeuds périphériques. Ceci correspond bien à l'équité en réception car un paquet émis par le noeud central est reçu n fois, une fois par chaque noeud périphérique. Par contre si un noeud périphérique envoie un paquet, celui-ci n'est reçu que par le noeud central. Dans ce cas, chaque paquet émis n'est comptabilisé qu'une fois.

Nous avons une condition pour avoir l'équité dans un réseau étoile. Essayons de généraliser cette relation pour un réseau comportant une suite de réseaux en étoile.

4.3.3 Réseau double-étoile

Un réseau double-étoile est constitué de deux étoiles qui ont une arrête commune. La figure 4.5 montre un réseau double-étoile.

Définition 12 (Réseau double-étoile)**.** Un réseau Ad-Hoc $SN_{n,m}$ de $n+m+1$ noeuds $\{X_0, \ldots, X_n, X_m, \ldots X_{n+m}\}$ est un réseau double-étoile si :
- Si $\{X_1, \ldots, X_n\}$ sont voisins de X_0
- Si $\{X_{n+1}, \ldots, X_{n+m}\}$ sont voisins de X_n
- S'il n'y a pas d'autres connexions dans le réseau.

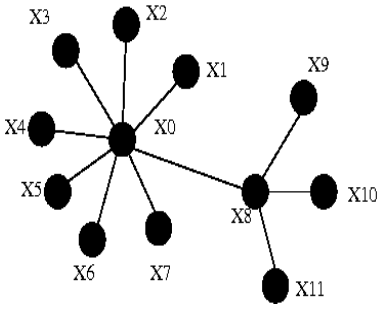

FIGURE 4.5 – Réseau double-étoile

La ressource que nous étudions est le taux de réception x_i. En supposons qu'il n'y a pas de perte, nous pouvons lier le taux de transmissions S_i du noeud X_i au taux de réception x_i :

$$\begin{aligned} x_0 &= \sum_{i=1}^{n} S_i \\ x_i &= S_0, \quad 1 \leq i \leq n-1 \\ x_n &= S_0 + \sum_{j=n+1}^{n+m} S_j \\ x_j &= S_n, \quad n+1 \leq i \leq n+m \end{aligned}$$

Donc on a :

$$f(x) = \frac{\left(\sum_{i=1}^{n} S_i + (n-1)S_0 + S_0 + \sum_{j=n+1}^{n+m} S_j + mS_n\right)^2}{(n+m+1)\left(\left(\sum_{i=1}^{n} S_i\right)^2 + (n-1)S_0^2 + \left(S_0 + \sum_{j=n+1}^{n+m} S_j\right)^2 + mS_n^2\right)}$$

Supposons que le réseau est équitable. On a alors $f(x) = 1$ et nous établissons le lemme suivant :

Lemme 4.3.2. *Un réseau double-étoile $SN_{n,m}$ est équitable si et seulement si :*

$$n(a - X - Y)^2 + m(a + Y)^2 + m(n-1)a^2 = 0 \tag{4.2}$$

où :
- $a = S_0 - S_n$
- $X = \sum_{i=1}^{n-1} S_i$
- $Y = \sum_{i=n+1}^{n+m} S_i$

Démonstration. Si $f(x) = 1$ on a :

$$\left(\sum_{i=1}^{n+m} S_i\right)^2 + n^2 S_0^2 + m^2 S_n^2 + 2nS_0\left(\sum_{i=1}^{n+m} S_i\right) + 2mS_n\left(\sum_{i=1}^{n+m} S_i\right) + 2nmS_0S_n -$$
$$(n+m+1)\left(\left(\sum_{i=1}^{n} S_i\right)^2 + nS_0^2 + \left(\sum_{j=n+1}^{n+m} S_j\right)^2 + 2S_0\left(\sum_{j=n+1}^{n+m} S_j\right) + mS_n^2\right) = 0$$

En simplifiant, on obtient :

$$2(n+1)\left(\sum_{i=1}^{n} S_i - S_0\right)\left(\sum_{i=n+1}^{n+m} S_i\right) - m\left(\sum_{i=1}^{n-1} S_i\right)^2$$
$$-n\left(S_0 - \sum_{i=1}^{n+m} S_i\right)^2$$
$$-m\left(S_0 - S_n + \sum_{i=n+1}^{n+m} S_i\right)^2 - m(n-1)(S_0 - S_n)^2 = 0$$

Posons alors :

$$u = \sum_{i=1}^{n-1} S_i$$
$$v = \sum_{i=n+1}^{n+m} S_i$$

On obtient alors :

$$\left(u - \frac{1}{n+m}v\right)^2 + \left(\frac{(n+m-1)(n+m+1)}{(n+m)^2}\right)v^2 - \frac{2n(S_0 - S_n)}{n+m}\left(u - \frac{1}{n+m}v\right)$$
$$+ \frac{(2m(n+m+1)(S_0 - S_n)}{(n+m)^2}v + \frac{n(m+1)(S_0 - S_n)^2}{n+m} = 0$$

Posons :

$$X = u - \frac{1}{n+m}v$$
$$Y = v$$

En simplifiant on obtient la relation du lemme. □

Remarque. Dans l'équation 4.2 tous les termes sont positifs. Donc pour annuler la somme, il faut que chaque terme soit nul.

Nous allons discuter de l'existence des solutions suivant les valeurs de n et m.

Cas où $n \neq 0, m = 0$

L'équation 4.2 devient :

$$n(a - X)^2 = 0$$

Cela implique $a = X$. Nous obtenons la même condition que pour un réseau étoile.

Cas $n = 0, m \neq 0$

Si $n = 0$ et $m \neq 0$ la relation 4.2 devient :

$$(a + Y)^2 - a^2 = 0$$

Cela implique $Y = 0$ ou $Y = -2a$. Y est positif, donc $Y = 0$. Aucun paquet n'est alors transmis, car $Y = 0$ et $n = 0$ implique que toutes les transmissions sont nulles.

Cas où $n = 1, m \neq 0$

Si $n = 1$ alors $X = 0$ et l'équation 4.2 devient :

$$(a - Y)^2 + m(a + Y)^2 = 0$$

Comme $m \neq 0$ on a nécessairement :

$$\begin{cases} a - Y = 0 \\ a + Y = 0 \end{cases}$$

Ceci implique $a = 0$ et $Y = 0$. Dans ce cas X_0 et X_1 sont en transmission avec $S_1 = S_0$. On est réduit à un réseau en étoile avec deux participants.

Cas où $n = 1, m \neq 0$

Si $n = 1$ on a $X = 0$ et l'équation 4.2 devient :

$$(a - Y)^2 = 0$$

Donc $Y = a$, ce qui correspond à un réseau étoile SN_{m+1} centré en X_n.

Cas où $n \neq 0, n \neq 1, m \neq 0$

Dans ce cas, aucun des coefficients de l'équation 4.2 est nul. Il faut donc que :

$$\begin{cases} a - X - Y = 0 \\ a + Y = 0 \\ a = 0 \end{cases}$$

Ceci implique que $a = 0, Y = 0, X = 0$. Il n'y a pas de transmission de paquets.

Nous pouvons à l'aide de ces résultats établir le théorème suivant :

Théorème 4.3.3. *Dans un réseau double-étoile, l'équité est obtenue dans les conditions suivantes :*

- *Si* $m = 0, n > 0$, *avec* $S_0 = \sum_{i=1}^{n} S_i$, *il s'agit d'un réseau étoile* SN_n
- *si* $m > 0, n = 1$ *avec* $S_1 = \sum_{i=2}^{m+1}$, *il s'agit d'un réseau étoile* SN_{m+1}
- *si on est dans un autre cas : il n'y a pas de transmissions*

Remarque. Le théorème 4.3.3 montre qu'un réseau double-étoile équitable se dégénère en un réseau étoile. Il n'existe donc pas de réseau double-étoile non dégénéré équitable.

La condition d'équité est obtenue sur $f(x) = 1$. Nous avons vu que cela n'est pas possible pour un réseau double-étoile. Mais nous pouvons essayer de donner un majorant pour l'index d'équité en posant $f(x) = \alpha$.

Si $f(x) = \alpha$ on a :

$$\left(\sum_{i=1}^{n+m} S_i\right)^2 + n^2 S_0^2 + m^2 S_n^2 + 2nS_0 \left(\sum_{i=1}^{n+m} S_i\right) + 2mS_n \left(\sum_{i=1}^{n+m} S_i\right) + 2nmS_0 S_n -$$
$$\alpha(n + m + 1)\left(\left(\sum_{i=1}^{n} S_i\right)^2 + nS_0^2 + \left(\sum_{j=n+1}^{n+m} S_j\right)^2 + 2S_0 \left(\sum_{j=n+1}^{n+m} S_j\right) + mS_n^2\right) = 0$$

Ceci implique que :

$$2\sum_{i=1}^{n-1}S_i\sum_{i=n+1}^{n+m}S_i+(1-\alpha(n+m+1))\left(\sum_{i=1}^{n-1}S_i\right)^2+(1-\alpha(n+m+1))\left(\sum_{j=n+1}^{n+m}S_j\right)^2+$$
$$2(nS_0+(m+1-\alpha(n+m+1))S_n)\sum_{i=1}^{n-1}S_i+2\left((m+1)S_n+(n-\alpha(n+m+1))S_0\right)\sum_{j=n+1}^{n+m}S_j+$$
$$2n(m+1)S_0S_n+n\left(n-\alpha(n+m+1)\right)S_0^2+(m+1)\left(1+m-\alpha(n+m+1)\right)S_n^2=0$$

Cas où $1-\alpha(n+m+1)=0$

On suppose que $1-\alpha(n+m+1)=0$ et on pose :

$$\begin{cases}X=\displaystyle\sum_{i=1}^{n-1}S_i\\ Y=\displaystyle\sum_{j=n+1}^{n+m}S_j\end{cases}$$

On a alors :

$$(X+(m+1)S_n+(n-1)S_0)(Y+nS_0+mS_n)-m(n-1)S_0S_n$$
$$-\frac{n\,(n-1)}{2}S_0^2-\frac{(m+1)m}{2}S_n^2=0$$

La solution est une hyperbole dans les variables S_0 et S_n.

Cas où $1-\alpha(n+m+1)\neq 0$

Si $1-\alpha(n+m+1)\neq 0$ on a :

$$2\sum_{i=1}^{n-1}S_i\sum_{i=n+1}^{n+m}S_i+(1-\alpha(n+m+1))\left(\sum_{i=1}^{n-1}S_i\right)^2+(1-\alpha(n+m+1))\left(\sum_{j=n+1}^{n+m}S_j\right)^2+$$
$$2(nS_0+(m+1-\alpha(n+m+1))S_n)\sum_{i=1}^{n-1}S_i+2\left((m+1)S_n+(n-\alpha(n+m+1))S_0\right)\sum_{j=n+1}^{n+m}S_j+$$
$$2n(m+1)S_0S_n+n\left(n-\alpha(n+m+1)\right)S_0^2+(m+1)\left(1+m-\alpha(n+m+1)\right)S_n^2=0$$

On pose :

$$\begin{cases}\displaystyle\sum_{i=1}^{n-1}S_i=X+Y\\ \displaystyle\sum_{j=n+1}^{n+m}S_j=X-Y\end{cases}$$

$$
\begin{aligned}
2(X+Y)(X-Y) + (1-\alpha(n+m+1))\,(X+Y)^2 + (1-\alpha(n+m+1))\,(X-Y)^2 + \\
2(nS_0 + (m+1-\alpha(n+m+1))S_n)(X+Y) + \\
2\,((m+1)S_n + (n-\alpha(n+m+1))S_0)\,(X-Y) + \\
2n(m+1)S_0S_n + n\,(n-\alpha(n+m+1))\,S_0^2 + (m+1)\,(1+m-\alpha(n+m+1))\,S_n^2 = 0
\end{aligned}
$$

$$
\begin{aligned}
&2\,(2-\alpha(n+m+1))\left(X + \frac{((2n-\alpha(n+m+1))S_0 + (2(m+1)-\alpha(n+m+1))S_n)}{2(2-\alpha(n+m+1))}\right)^2 \\
&- 2\alpha(n+m+1)\left(Y - \frac{(\alpha(n+m+1)S_0 - \alpha(n+m+1)S_n)}{\alpha 2(n+m+1)}\right)^2 + \\
&\left(\frac{(2n-\alpha(n+m+1))(2(m+1)-\alpha(n+m+1))}{\alpha(n+m+1)-2} + 2n(m+1) - \alpha(n+m+1)\right) S_0S_n + \\
&+ \left(\frac{(2n-\alpha(n+m+1))^2}{2(\alpha(n+m+1)-2)} + n\,(n-\alpha(n+m+1)) + \frac{\alpha(n+m+1)}{2}\right) S_0^2 + \\
&+ \left(\frac{2((m+1)-\alpha(n+m+1))^2}{\alpha(n+m+1)-2} + (m+1)\,(1+m-\alpha(n+m+1)) + \frac{\alpha(n+m+1)}{2}\right) S_n^2 = 0
\end{aligned}
$$

La dernière équation permet d'établir le lemme suivant :

Lemme 4.3.4. *Un réseau double-étoile $SN_{n,m}$ avec $1-\alpha(n+m+1) \neq 0$ a comme index d'équité α s'il vérifie l'équation :*

$$
2(2-\alpha(n+m+1)))U^2 - 2\alpha(n+m+1)V^2 + \mathcal{Q}(S_0, S_n) = 0 \tag{4.3}
$$

où

$$
\begin{aligned}
U &= \sum_{i=1}^{n-1} S_i + \frac{(2n-\alpha(n+m+1))S_0}{2(2-\alpha(n+m+1))} + \frac{(2(m+1)-\alpha(n+m+1))S_n}{2(2-\alpha(n+m+1))} \\
V &= \sum_{i=n+1}^{n+m} S_i - \frac{\alpha(n+m+1)S_0 - \alpha(n+m+1)S_n}{2\alpha(n+m+1)} \\
\mathcal{Q}(S_0, S_n) &= AS_0^2 + 2BS_0S_n + CS_n^2
\end{aligned}
$$

Où $\mathcal{Q}$ est la forme quadratique avec :

$$
\begin{aligned}
A &= -\frac{(n-1)(n+m+1)\alpha((n+m+1)\alpha - n - 1)}{(n+m+1)\alpha - 2} \\
B &= \frac{m(n-1)(n+m+1)\alpha}{\alpha(n+m+1)-2} \\
C &= -\frac{(n+m+1)^2\alpha^2(2m-3) - 2(n+m+1)\alpha(m^2-2)}{2(\alpha(n+m+1)-2)}
\end{aligned}
$$

L'équation 4.3 est une forme quadratique en U et V. Nous devons étudier l'existence de solutions pour cette équation. L'index d'équité α est toujours positif. Le coefficient de V^2 est donc négatif. Le coefficient de U^2 dépend de $2-\alpha(n+m+1)$. On a donc :

Corollaire 4.3.5. *Pour un réseau double-étoile $SN_{n,m}$, l'existence de l'index d'équité $\alpha \neq \frac{1}{n+m+1}$ est possible si l'équation 4.3 est satisfaite.*

- *Si on a $\alpha < \frac{2}{n+m+1}$ alors il existe des solutions*
- *Si on a $\alpha > \frac{2}{n+m+1}$ et $\mathcal{Q}(S_0, S_n) \leq 0$ alors il n'existe pas de solutions autre que $(U, V) = (0, 0)$.*

Démonstration. Si on a $\frac{2}{n+m+1} > \alpha$ alors les coefficients de U^2 et V^2 sont de signes opposés.

Si on a $\alpha > \frac{2}{n+m+1}$ et $\mathcal{Q}(S_0, S_n) \leq 0$ alors tous les membres de l'équation 4.3 sont négatifs. La seule solution possible est donc $(U, V) = (0, 0)$ et $\mathcal{Q}(S_0, S_n) = 0$. □

Le corollaire 4.3.5 montre l'importance du signe de la forme quadratique $\mathcal{Q}(S_0, S_n)$ si $\alpha > \frac{2}{n+m+1}$. Nous allons donc étudier ce signe. Cherchons quand la forme quadratique $\mathcal{Q}(S_0, S_n)$ peut être positive avec $\alpha > \frac{2}{n+m+1}$.

Si $\alpha > \frac{2}{n+m+1}$, alors les dénominateurs des coefficients de $\mathcal{Q}$, à savoir A, B et C sont positif. Nous nous intéressons donc aux numérateurs.

Nous avons que :
— le signe de A est de celui de $n + 1 - \alpha(n + m + 1)$
— le signe de B est positif car $n > 1$
— le signe de C est de celui de $2(m^2 - 2) - (2m - 3)(n + m + 1)\alpha$
Nous en déduisons que A est positif si et seulement si :

$$\alpha \leq \frac{n+1}{n+m+1}$$

et que C est positif si et seulement si :

$$\alpha \leq \frac{2(m^2-2)}{(2m-3)(n+m+1)}$$

Or nous avons $\alpha > \frac{2}{n+m+1}$, ce qui donne pour C :

$$\frac{2}{n+m+1} < \alpha \leq \frac{2(m^2-2)}{(2m-3)(n+m+1)}$$

Ceci implique que $\frac{m^2-2}{2m-3} > 1$. Ceci est vérifié, car en simplifiant on obtient $(m-1)^2 > 0$.

Nous pouvons établir le lemme suivant :

Lemme 4.3.6. *Supposons que* $1 < n \leq m$ *et que*

$$\frac{2}{n+m+1} < \alpha \leq \frac{n+1}{n+m+1}$$

alors la forme quadratique $\mathcal{Q}(S_0, S_n)$ *est positive.*

Démonstration. Comme on a $\alpha \leq \frac{n+1}{n+m+1}$, A est positif et comme $1 < n$, B est positif. Montrons que C est positif. Cela revient à montrer que :

$$\frac{n+1}{n+m+1} \leq \frac{2(m^2-2)}{(2m-3)(n+m+1)}$$

Nous avons $1 < n \leq m$ donc $n + 1 \leq m + 1$ et $m + 1 \leq \frac{2(m^2-2)}{2m-3}$. Finalement on a :

$$\frac{n+1}{n+m+1} \leq \frac{m+1}{n+m+1} \leq \frac{2(m^2-2)}{(2m-3)(n+m+1)}$$

C est donc positif, ainsi que la forme quadratique. □

Le corollaire 4.3.5 et le lemme 4.3.6 permettent d'établir le théorème suivant :

Théorème 4.3.7. *Soit un réseau double-étoile $SN_{n,m}$ tel que $1 < n \leq m$ alors il est possible d'obtenir un index d'équité α tel que*

$$\alpha \leq \frac{n+1}{n+m+1}$$

Démonstration. Le corollaire 4.3.5 montre l'existence de solutions si $\alpha < \frac{2}{n+m+1}$ et si $\alpha \geq \frac{2}{n+m+1}$ avec $\mathcal{Q}(S_0, S_n) \geq 0$. Le lemme 4.3.6 montre justement que la forme quadratique est positif si $\alpha \leq \frac{n+1}{n+m+1}$. □

Par dualité, nous pouvons établir le corollaire suivant :

Corollaire 4.3.8. *Soit α l'index d'équité d'un réseau double-étoile $SN_{n,m}$, α existe*

— *si $1 < n \leq m$ et*

$$\alpha \leq \frac{n+1}{n+m+1}$$

— *si $1 < m \leq n$ et*

$$\alpha \leq \frac{m+2}{n+m+1}$$

Démonstration. En posant $Y_0 = X_n, Y_1 = X_{n+1}, \ldots Y_{p-1} = X_{n+m}$ et $Y_p = X_0, Y_{p+1} = X_1, \ldots Y_{p+q} = X_{n-1}$ on obtient un réseau double-étoile $SN_{p,q}$ avec $p = m + 1$ et $q = n - 1$. □

4.3.4 Conclusion

Nous avons étudié dans cette section l'index d'équité pour le taux de réception dans les réseaux Ad-Hoc en étoile et en double-étoiles. Une relation nécessaire et suffisante pour obtenir l'équité dans les réseaux étoile a été établit. Nous avons aussi prouvé que l'équité n'est pas possible dans un réseau double-étoile. Par contre, l'étude théorique a permis d'établir des majorants pour l'index d'équité. Vu la complexité pour obtenir des résultats sur l'index d'équité dans les réseaux double-étoile, nous n'avons pas généralisé cette méthode. Nous proposons maintenant d'utiliser ces résultats pour développer des algorithmes qui ont pour objectif d'améliorer l'équité de réception dans les réseaux Ad-Hoc.

4.4 Algorithmes pour l'équité dans les réseaux Ad-Hoc

4.4.1 Algorithme pour les réseaux étoiles

Pour un réseau étoile SN_n, l'équité est satisfaite si et seulement si l'équation 4.1 est vérifiée. L'algorithme que nous proposons ici essaye de satisfaire cette équation. Pour cela, il va ajuster le taux de transmission du noeud central S_0 pour que son débit soit égal au taux de réception des paquets reçus par ses voisins. Voici les étapes de l'algorithme effectuées par le noeud Y_i :

1. Initialiser le paramètre s avec la valeur donnée par l'administrateur.
2. Calculer la somme A_i des paquets reçus en provenance des noeuds voisins.
3. Comparer la somme A_i avec son taux de transmission S_i
4. Si $S_i - A_i > s$ alors on diminue son taux de transmission S_i. Si S_i est négatif, alors $S_i = 0$.
5. Si $S_i - A_i < s$ alors on augmente son taux de transmission S_i si cela est possible.
6. Si $S_i = 0$ pour un certain temps choisi par l'administrateur, on augmente S_i.
7. Aller à l'étape 2.

Le paramètre s permet de contrôler la sensibilité de l'algorithme. Une valeur proche de zéro implique une grande exigence sur l'équité. Le taux de transmission S_i risque de varier constamment. Une valeur plus large de s est moins exigeante sur l'équité mais permet de garantir un taux d'émission plus stable.

Simulation de l'algorithme pour les réseaux étoiles

La simulation est faite avec le logiciel Ns2. Le protocole de routage DSDV est utilisé. Chaque noeud génère un trafique FTP. Nous comptabilisons les paquets TCP reçus.

Simulation avec un réseau étoile SN_6

Dans cette simulation, le noeud centrale X_0 établit une connexion FTP avec chaque voisin X_i, avec $i \geq 1$. Et chaque X_i, pour $i \geq 1$ établit une connexion FTP avec X_0.

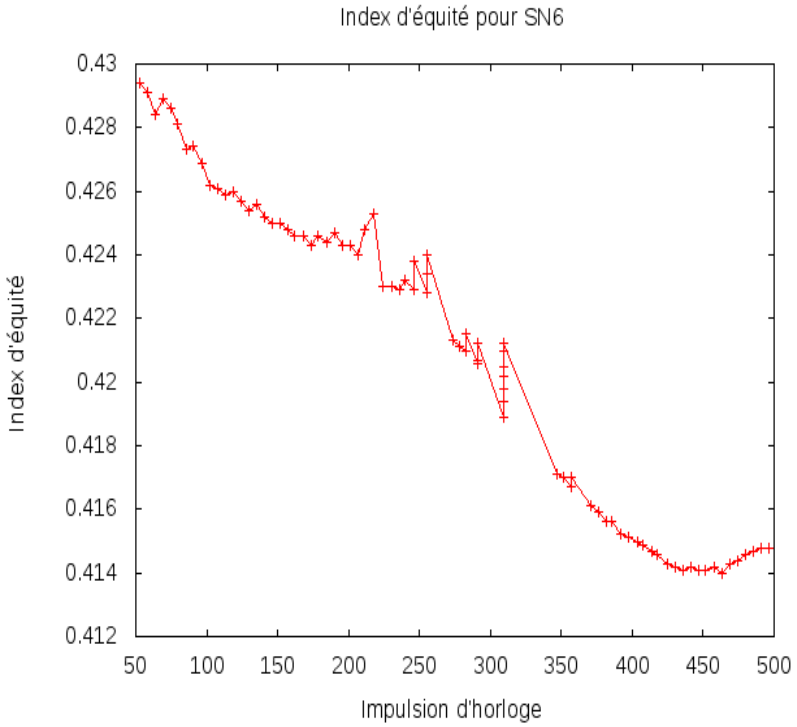

FIGURE 4.6 – Index d'équité pour SN_6, protocole standard

La figure 4.6 montre que pour un réseau étoile SN_6 fonctionnant avec un protocole Wifi Standard, l'index d'équité diminue légèrement. Nous pouvons aussi tracer la différence de l'équation 4.1.

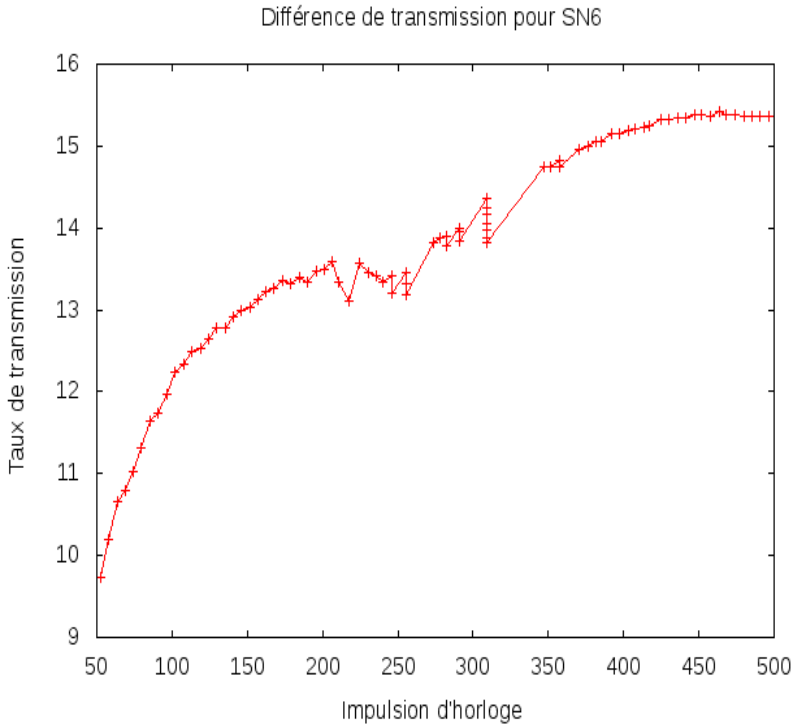

FIGURE 4.7 – Différence de transmissions pour SN_6, protocole standard

Nous remarquons dans la figure 4.7 que la différence de l'équation 4.1 augmente et ce jusqu'à une valeur de 15,5 paquets par impulsion d'horloge. Ceci est cohérent avec la baisse de l'index d'équité. Appliquons maintenant notre algorithme. Nous posons $s = 500$ et $S_i = 1Mb/s$. Le débit réduit sera de $0,5Mb/s$.

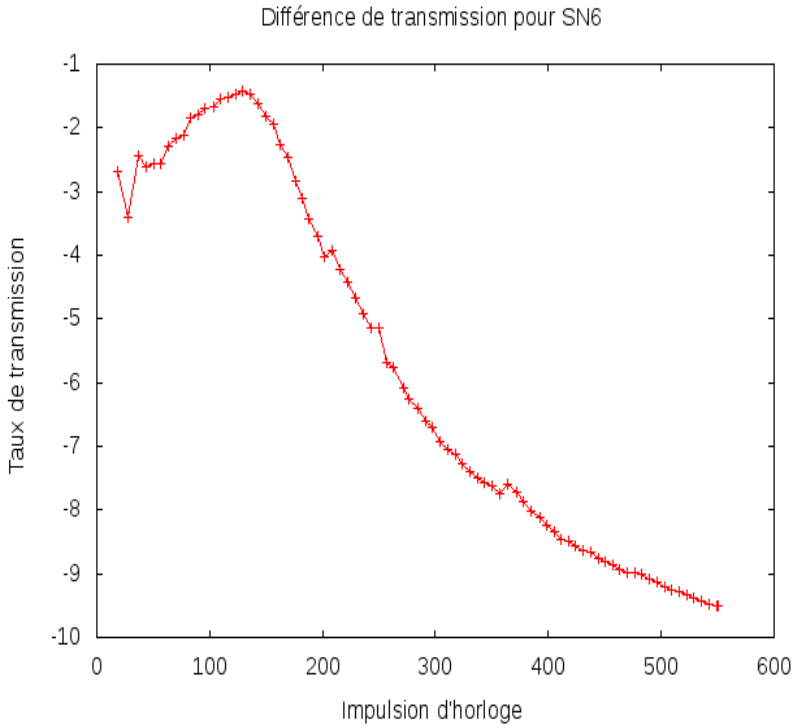

FIGURE 4.8 – Différence de transmissions pour SN_6, protocole modifié

Dans la figure 4.8 nous remarquons que la valeur de la différence des taux de transmission se stabilise vers -10 paquets par impulsion d'horloge. Ce qui en valeur absolue est inférieur aux 15,5 obtenu précédemment. Il y a donc une amélioration, ce qui se traduit par un index d'équité qui passe sur une courte période de 0,41 à 0,43.

Simulation avec un réseau non étoilé

L'algorithme inspiré des réseaux étoiles peut aussi s'appliquer à n'importe quel réseau. Dans ce cas, quel est le bénéfice pour l'index d'équité ? Nous allons appliquer l'algorithme pour les réseaux étoile au réseau de la figure 3.5.

La figure 4.9 représente l'index d'équité pour ce réseau en fonction du temps pour l'algorithme standard de Ns2.

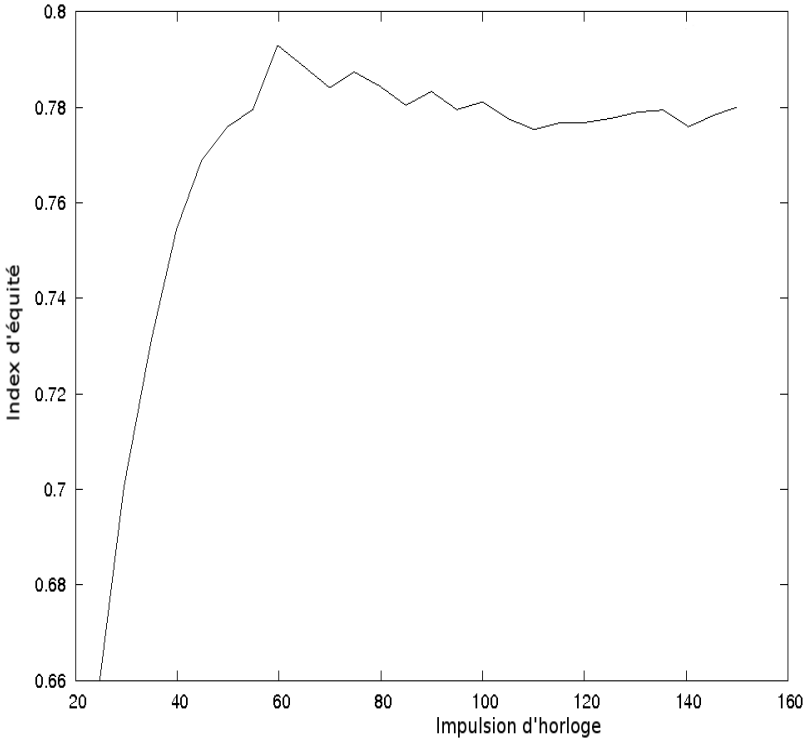

FIGURE 4.9 – Index d'équité pour un réseau non étoile, protocole standard

La figure 4.10 représente l'index d'équité pour ce réseau en fonction du temps pour l'algorithme standard de Ns2.

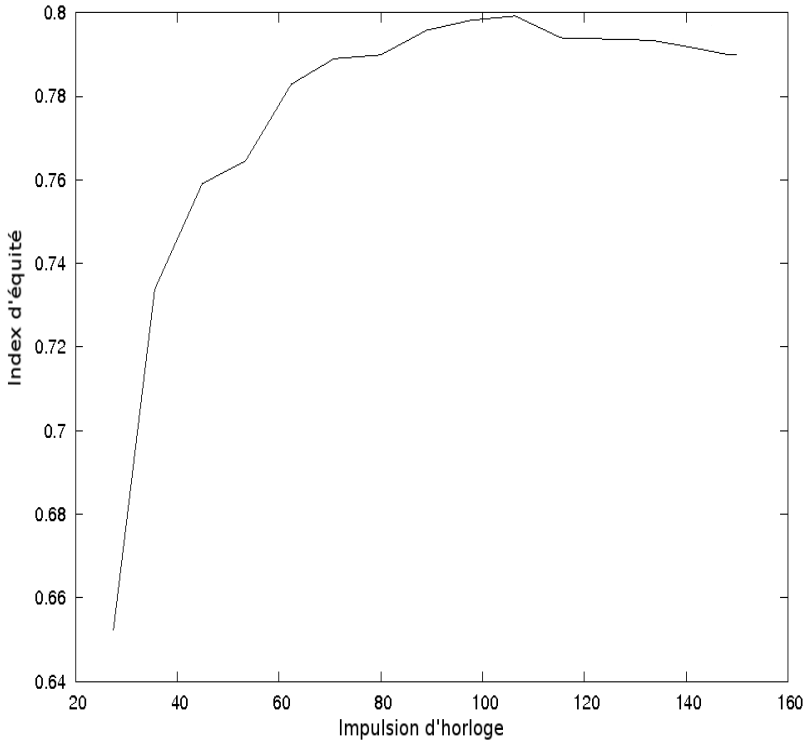

FIGURE 4.10 – Index d'équité pour un réseau non étoile, protocole modifié

Nous remarquons qu'il y a une légère amélioration pour l'index d'équité dû à notre algorithme. Cela est du au fait que dans le réseau 3.5, le flux f_4 a un rôle central comme dans un réseau étoile. Par cet exemple, nous avons montré que le fait de développer un algorithme d'équité pour les réseaux étoiles permet, dans certains cas, d'être étendu aux réseaux Ad-Hoc en général.

4.4.2 Simulation pour les réseaux double-étoile

Un réseau double-étoile est équitable si la relation 4.2 est vérifiée. Si le réseau double-étoile n'est pas équitable, alors l'équation 4.2 n'est pas nulle. Pour approcher l'équité, nous proposons d'agir sur le taux de transmission des noeuds centraux X_0 et X_n pour minimiser la valeur de l'équation 4.2. Le fait d'agir sur le taux de transmission des noeuds centraux X_0 et X_n modifie la valeur de a dans l'équation 4.2. La figure 4.11 montre la variation de l'index d'équité d'un réseau double-étoile $SN_{8,3}$ en fonction des taux de transmission des noeuds centraux X_0 et X_n.

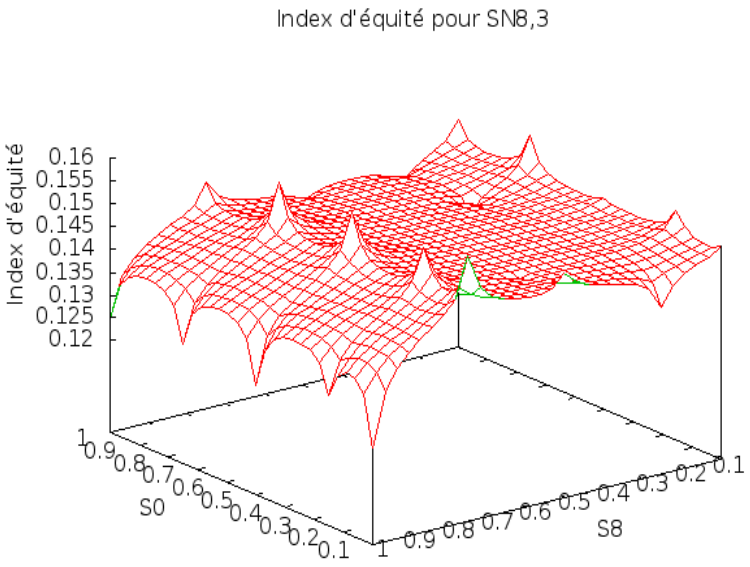

FIGURE 4.11 – Index d'équité pour un réseau double étoile $SN_{8,3}$

Nous remarquons que la valeur d'index maximal est obtenue pour $S_0 = 0,25$, $S_8 = 0,75$. L'index d'équité vaut alors $0,1596$. Le corollaire 4.3.8 nous donne pour $S_{8,3}$ un index d'équité inférieur à $\frac{5}{13} \approx 0,38$. Par contre, la valeur obtenue est relativement faible. L'ajustement des taux de transmission des noeuds centraux semble insuffisant pour obtenir un comportement équitable.

4.5 Conclusion

Dans ce chapitre, nous avons étudié le comportement équitable d'un réseau Ad-Hoc. La notion d'équité est souvent intuitive. Pour les besoins de cette étude, c'est la définition de K. Jain, Dah-Ming W. Chiu et William R. Hawe qui a été utilisée. Cette définition introduit l'index d'équité qui permet de quantifier le comportement équitable d'un réseau. L'évaluation de cet index étant difficile pour un réseau Ad-Hoc quelconque, nous introduisons dans un premier temps la topologie en étoile. Pour cette topologie, une condition nécessaire et suffisant est donnée pour que ce réseau soit équitable. Cette condition a permis de proposer un algorithme d'accès pour obtenir un comportement équitable. Nous avons essayé de généraliser cette méthode. Les réseaux double-étoile se composent d'une réunion de deux réseaux en étoile. Nous avons démontré qu'un tel réseau ne peut pas avoir un comportement équitable, sauf s'il se dégénère en un réseau étoile. Par contre, un calcul a permis de donner un majorant pour l'index d'équité. Une simulation a montrée qu'en ajustant le taux de transmission des noeuds centraux, l'équité a été améliorée, mais cela reste insuffisant.

Ce chapitre a mis en évidence la relation entre la topologie du réseau et les limites de son comportement équitable. Dans la suite de notre mémoire, nous allons nous intéresser à une famille de réseaux Ad-Hoc particulier : les réseaux de capteurs sans fil. Ces réseaux ont des contraintes supplémentaires par rapport aux réseaux Ad-Hoc, ce qui permet d'axer notre étude sur des points plus spécifiques comme la consommation d'énergie dans le réseau.

Chapitre 5

Représentation de réseaux de capteurs sans fil avec une image en niveau de gris : Application au routage.

5.1 Introduction

Dans les chapitres précédents, l'étude portait sur les réseaux Ad-Hoc. Nous y avons étudié la congestion et l'équité dans ces réseaux. Dans ce chapitre nous nous focalisons sur une sous classe des réseaux Ad-Hoc : les réseaux de capteurs sans fil.

Les réseaux de capteurs sans fil sont soumis à des contraintes supplémentaires par rapport à un réseaux Ad-Hoc. Ces contraintes sont dû au fonctionnement du capteur lui-même ou aux types d'applications utilisant ces capteurs. Les capteurs sans fil sont parfois utilisés pour couvrir une zone hostile. De ce fait, les opérations de maintenances sont difficiles, voire impossible à effectuer. L'approvisionnement en énergie pour le fonctionnement du capteur est souvent limité à la seule batterie d'origine. Ainsi la durée de vie du capteur est liée à l'emport d'énergie initiale et la gestion de cette ressource. Cette contrainte énergétique est à la source d'un axe de recherche très actif [99].

Un capteur se compose de plusieurs points de consommation d'énergie. L'acquisition des données, leur traitement, leur conditionnement pour la transmission et la communication sont différentes actions consommatrices en énergie. Parmi elles, la communication est la plus importante et c'est sur elle que se focalise notre étude.

De multiples stratégies ont été développées pour maîtriser l'énergie utilisée pour la communication des capteurs. Ces stratégies s'appliquent à tous les niveaux de la communication : accès à la couche physique ou MAC, acheminement des paquets ou routage, mais aussi en optimisant les données à transmettre.

Au niveau de la couche MAC, de l'énergie est gaspillée pour la réémission de paquets lors de collisions, pour le traitement de paquets de contrôle qui ne contiennent pas d'informations applicatives, ou bien encore de traitement de paquets dont le noeud n'est pas destinataire. Les différents protocoles spécifiques au réseau de capteurs ont essayé de répondre à ces problématiques. Le protocole S-MAC [8], par exemple, utilise une synchronisation entre capteurs pour pouvoir cycliquement les désactiver. D'autres protocoles utilise le même principe de désactivation des capteurs pour conserver l'énergie [1]. Ces protocoles sont de plus dynamiques et s'adaptent à certaines conditions, de

trafiques [5]. Le protocole PC-MAC [38] essaye de minimiser la consommation d'énergie en limitant les collisions.

La partie routage a aussi été largement explorée. A ce niveau c'est la façon d'acheminer les paquets qui vont être un moyen d'économiser l'énergie. Les algorithmes de routage sont aussi affectés par la spécificité matériel des capteurs : limitation en stockage pour la table de routage et en puissance de calcul pour déterminer les routes. Ces protocoles de routage essayent de profiter de certaines caractéristiques des réseaux de capteurs sans fil, notamment de la haute densité géographique. La recherche est très active dans ce domaine et a produit de nombreux protocoles. Ces protocoles peuvent être classé selon leur méthode de fonctionnement [33]. Il y a ceux basé sur des critères géographiques, ceux orienté données et ceux utilisant une topologie hiérarchique ou à liens multiples. Dans les algorithmes géographiques on peut citer GKAR [90] qui est un protocole de type K-anycast. Certain algorithmes comme EASPRP [26] recherche le chemin le plus court avec des contraintes énergétiques. Le protocole de routage EERT [59] permet la qualité de service tout en utilisant des contrainte énergétiques. Un autre protocole de routage temps réel est REFER [51] basé sur les graphes de Kautz. Certains algorithmes de routage peuvent être combinés pour éviter des lieux pauvres en capteurs [69].

La mobilité des capteurs peut aussi être pris en compte comme dans [29] qui propose un algorithme hybride pour le routage et la mobilité. Un autre protocole GAROUTE [79] utilise un algorithme génétique pour traiter des capteurs mobiles et les regrouper par grappes. Les grappes sont des amas de capteurs avec en générale un capteur centralisateur pour effectuer un traitement locale de l'information et de l'agrégation de données dans le but de réduire les communications [102, 66, 82]. Le protocole LEACH [80, 20, 35] est le premier protocole utilisant la notion de grappe pour répartir la charge sur tout le réseau. Ce protocole a été modifié dans [89] pour réduire le temps d'acheminement et les interférences. Le protocole EEDR [42] se focalise sur le relayage de données dans un but d'économie d'énergie.

Il y a d'autres méthodes qui ont été utilisées pour limiter la consommation d'énergie et rallonger la durée de vie d'un réseau de capteurs sans fil. Dans [41], on utilise des critères de couverture pour optimiser l'utilisation des capteurs. Des simulations basées sur la méthode SCC (Sponsored Coverage Calculation) [104] explorent aussi cette voie. Limiter l'échange de données est aussi un facteur d'économie d'énergie comme le montre le protocole SEPSen [48], qui propose un traitement des données pendant leur acheminement. La répartition du trafic et la gestion de ressources proposée dans [56] essaye d'optimiser la consommation d'énergie. Ces différentes techniques ont fait l'objet de simulations. Différents simulateurs pour les réseaux de capteurs ont été comparés dans [50].

Dans ce chapitre, une méthode innovante basée sur une analogie d'un réseau et d'une image en niveau de gris sera présenté. C'est dans la thèse de Y. Yousef, que j'ai coencadré, que cette analogie a été faite pour la première fois. Cette thèse a donné lieu à deux conférences internationales avec comité de lecture et sélection sur article long [GYL09, YGL10b] et une publication dans un journal international [YGL10a]. L'analogie consiste à représenter la répartition géographique d'une valeur, l'énergie par exemple, par une image en niveau de gris, où un pixel représente la localisation du capteur, et l'intensité du pixel la valeur pour ce capteur. Cette analogie sera utilisé pour développer de nouveaux protocoles de routage en appliquant des algorithmes de traitement d'image. Des simulations viendront illustrer cette méthode.

5.2 Analogie par l'image

5.2.1 Les images en niveau de gris.

Une image en informatique est représenté par un ensemble de points, appeler pixel, qui se positionne à des coordonnées entières. Chaque pixel apparaît par une luminosité plus ou moins intense. L'ensemble de ces pixels juxtaposés crée une image en niveau de gris tel que le faisait les

téléviseurs noir et blanc à une certaine époque 5.1.

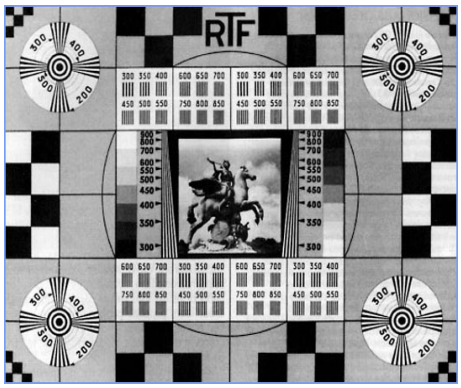

FIGURE 5.1 – Image en niveaux de gris

Sur une telle image, nous pouvons reconnaître des formes, des objets, personnages ... Pour un ordinateur, l'exploitation d'une telle image est plus difficile, mais des algorithmes ont été développés, par exemple pour la reconnaissance de contours, de caractères, etc... Dans cette configuration, un pixel ne se situant pas au bord de l'image à 8 pixels voisins qui l'entourent.

La luminosité, ou niveau de gris, est représentée par une valeur prise dans un certain intervalle. Plus que l'image est nuancée, plus cet intervalle est important. En informatique, le traitement se fait sur des valeurs binaires (O ou 1). Une image en niveau de gris codée sur 8 bits permet 2^8 niveaux de gris possibles, soit une intensité allant de 0 à 255. Par convention la valeur 0 représente l'absence de luminosité, donc le noir et la valeur 255 le blanc.

5.2.2 Construction de l'image pour un réseau

Nous pouvons utiliser une image en niveau de gris pour représenter la répartition géographique d'une valeur. Un réseau de capteurs sans fil est constitué de capteurs qui communiquent entre eux. Chaque capteur à différentes valeurs comme par exemple le nombre de paquets reçus ou émis, la puissance de son signal, ou encore l'énergie disponible dans sa batterie. Chacune de ces valeurs est un nombre réel. En choisissant une échelle adéquate, ces valeurs peuvent être discrétisées et représentées par un entier positif. Supposons que les valeurs entières se situent entre 0 et 255. On obtient alors une représentation de cette valeurs sur 8 bits, et cette valeurs va être interprétée comme une valeur de luminosité.

Chaque capteur est donc pourvu d'une valeur de luminosité. Supposons que ces capteurs sont disposés sur plan. En munissant ce plan d'un repère euclidien, un capteur est positionné à des coordonnées (x, y) qu'on peut supposer entière. Finalement, en assimilant chaque capteur à un pixel on obtient une image en niveau de gris 5.2.

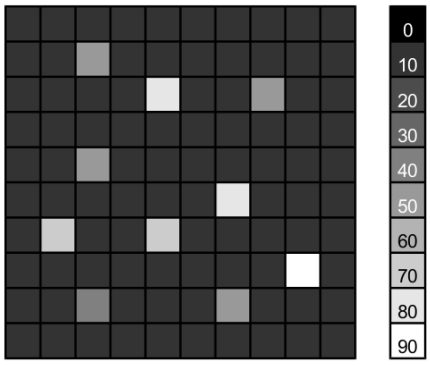

FIGURE 5.2 – Réseaux de 10 capteurs en niveaux de gris

Dans l'image 5.2, les capteurs qui sont dans le rayon de communication ne sont pas forcément voisins sur l'image. Ceci peut être gênant si on souhaite appliquer des algorithmes de traitement d'image, comme un filtre de convolution par exemple. Pour remédier à ce problème, 8 voisins "virtuels" sont créés représentant une valeur de luminosité moyenne autour du capteur central.

5.2.3 Création de voisins virtuels

Dans une image, un pixel a généralement 8 voisins. Or dans l'image précédente, il se peut qu'un pixel n'a aucun voisin, alors que le capteur qu'il représente à plusieurs voisins au sens d'être dans le rayon de communication. Ceci peut être gênant dans certains cas, notamment pour l'application de filtres de convolution, si la notion de voisin, au sens réseau, doit être conservée.

L'idée de l'image en niveau de gris est de représenter la répartition géographique d'une valeur dans un réseau. Pour un capteur donné, ce qui est important c'est sa vision de cette valeur par rapport à ses voisins. Comme un pixel a 8 voisins, un capteur va avoir 8 voisins virtuels qui sont créés comme suite :

— Le capteur considère tous les capteurs voisins dans son rayon de communication.
— L'environnement du capteur est subdivisé en 8 secteurs.
— Une luminosité est calculée pour chaque secteur en faisant la moyenne des luminosités des capteurs qu'il contient.
— Les 8 secteurs avec leur luminosité forment les 8 voisins virtuels du capteur.

La figure 5.3 montre les 8 secteurs autour d'un capteur.

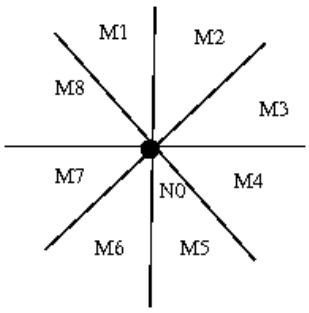

FIGURE 5.3 – Les 8 secteurs du capteur N_0

A l'aide des valeurs de luminosité $M_1, \ldots, M_8$ de ces huit voisins virtuels une image locale du

capteur peut être donnée sous forme de matrice :

$$Mv = \begin{pmatrix} M_8 & M_1 & M_2 \\ M_7 & N_0 & M_3 \\ M_6 & M_5 & M_4 \end{pmatrix} \tag{5.1}$$

La matrice (5.1) peut être utilisée comme entrée pour des algorithmes de traitements d'image, notamment les filtres de convolution.

5.3 Algorithmes de traitement d'image

5.3.1 Les filtres de convolution

En traitement d'image, il existe plusieurs techniques. L'une d'elle appelée filtres de convolution consiste à remplacer la luminosité d'un pixel par une valeur calculée à l'aide des luminosités des 8 pixels voisins. Ces filtres peuvent être de plusieurs types, il y a par exemple les filtres de convolution, filtre gaussien [15] ou filtrede sobel [47, 22, 46, 13].

Une image peut être vu comme une matrice I où la valeur $I(x, y)$ correspond à la luminosité du pixel aux coordonnées (x, y). A cette matrice nous appliquons une autre matrice K, appelée le noyau, en utilisant un produit de convolution. Le noyau K est la caractéristique du filtre de convolution, il peut être de taille 3×3 ou 5×5.

Le produit de convolution entre les matrices I et K consiste à calculer une nouvelle valeur pour le pixel $I(x, y)$. Cette valeur est obtenue en multipliant $I(x, y)$ par $k(2, 2)$ et les voisins de $I(x, y)$ par les valeurs de K correspondantes et en faisant la somme.

On note le produit de convolution $*$:

$$I * K = \begin{pmatrix} I(1,1) & I(1,2) & \dots & I(1,n) \\ \vdots & & I(x,y) & \vdots \\ I(m,1) & I(m,2) & \dots & I(m,n) \end{pmatrix} * \begin{pmatrix} K(1,1) & K(1,2) & K(1,3) \\ K(2,1) & K(2,2) & K(2,3) \\ K(3,1) & K(3,2) & K(3,3) \end{pmatrix}$$

et on a alors pour une matrice K 3×3 :

$$I * K_{x,y} = \sum_{i=-1}^{1} \sum_{j=-1}^{1} I(x+i, y+j) * K(2+i, 2+j) \tag{5.2}$$

Le noyau K détermine l'action du filtre sur l'image. Dans la suite différent types de filtres de convolution sont présentés.

5.3.2 Le filtre moyen

Le filtre moyen est un filtre de convolution qui remplace la luminosité d'un pixel par la moyenne des luminosités de lui-même et de ses pixels voisins. Il utilise le noyau suivant :

$$K = \begin{pmatrix} \frac{1}{9} & \frac{1}{9} & \frac{1}{9} \\ \frac{1}{9} & \frac{1}{9} & \frac{1}{9} \\ \frac{1}{9} & \frac{1}{9} & \frac{1}{9} \end{pmatrix}$$

La figure 5.4 montre comment le filtre moyen agit sur une photo.

FIGURE 5.4 – Action du filtre moyen

5.3.3 Le filtre gradient

Un gradient représente la variation d'une valeur dans une direction donnée. Ici le filtre gradient permet pour chaque pixel de donner la variation de luminosité dans la direction X ou Y selon le type de noyau utilisé. Voici les noyaux K pour les différentes directions :

$$\frac{\partial I}{\partial x} = \begin{pmatrix} 0 & 1 & -1 \\ 0 & 1 & -1 \\ 0 & 1 & -1 \end{pmatrix} \tag{5.3}$$

$$\frac{\partial I}{\partial(-x)} = \begin{pmatrix} -1 & 1 & 0 \\ -1 & 1 & 0 \\ -1 & 1 & 0 \end{pmatrix} \tag{5.4}$$

$$\frac{\partial I}{\partial(-y)} = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \\ -1 & -1 & -1 \end{pmatrix} \tag{5.5}$$

$$\frac{\partial I}{\partial y} = \begin{pmatrix} -1 & -1 & -1 \\ 1 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix} \tag{5.6}$$

Les figures 5.5 et 5.6 montre une image filtrée dans les directions X et Y avec un filtre normalisé.

FIGURE 5.5 – Action du filtre gradient X

FIGURE 5.6 – Action du filtre gradient Y

5.3.4 Le filtre Gaussien

Le filtre Gaussien utilise un noyau créé à partir de la fonction gaussienne :

$$G(x,y) = \frac{1}{2\pi\sigma^2} \exp^{\frac{x^2+y^2}{2\sigma^2}}$$

Ce filtre crée une moyenne pondéré en favorisant les pixels centraux par rapport à la périphérie. Le paramètre σ contrôle l'importance donnée aux valeurs du centre.

La figure 5.7 montre l'action du filtre Gaussien.

FIGURE 5.7 – Action du filtre Gaussien avec $\sigma = 0.04$

5.3.5 Le filtre de Sobel

Le filtre de Sobel est utilisé dans la détection de contour. Il utilise deux noyaux gradient G_x et G_y. Le filtre de Sobel donne à chaque pixel une luminosité moyenne $\sqrt{G_x^2 + G_y^2}$. Les noyaux G_x et G_y sont donnés par :

$$G_x = \begin{pmatrix} -1 & -2 & -1 \\ 0 & 0 & 0 \\ 1 & 2 & 1 \end{pmatrix} \tag{5.7}$$

$$G_y = \begin{pmatrix} -1 & 0 & 1 \\ -2 & 0 & 2 \\ -1 & 0 & 1 \end{pmatrix} \tag{5.8}$$

Les figures 5.8 et 5.9 montrent l'action des filtres gradient G_x et G_y.

FIGURE 5.8 – Action du filtre gradient G_X

De ces deux gradients, le filtre de Sobel retrouve les contours de l'image initial 5.10. Les intensités de gris ont été inversées pour plus de lisibilité.

FIGURE 5.9 – Action du filtre gradient G_Y

FIGURE 5.10 – Action du filtre Sobel (intensité inverse)

Il existe d'autres filtres de convolution comme le filtre gaussien, le masque flou etc ... Mais ces filtres n'ont pas été exploités dans ce mémoire.

5.3.6 Détection de contours par les modèles déformables

La détection de contour est une notion intéressante dans notre analogie pour détecter la frontière entre des régions riches en énergie et des régions pauvres en énergie. Le filtre de Sobel, décrit dans la section 5.3.5 est l'une des méthodes pour trouver ces contours, mais il en existe d'autres.

Dans [60] l'auteur propose d'utiliser un modèle déformable pour analyser des images médicales. Dans cet article, D. Terzopoulos propose d'utiliser des courbes déformables pour identifier des contours dans les images médicales.

Une courbe sur une image plane de coordonnées $(x, y) \in \mathbb{R}^2$ peut être représentée par une fonction paramétrique $v(s) = (x(s), y(s))^T$ où $s \in [0, 1]$ représente l'abscisse curviligne. La forme de cette courbe est la résultante de différentes forces appliquées sur elle. Elle se traduit par la relation :

$$\mathcal{E}(v) = S(v) + \mathcal{P}(v) \tag{5.9}$$

La fonction $\mathcal{E}$ peut être vue comme l'énergie de la courbe qui est la somme de l'énergie de déformation S, représentant l'énergie interne qu'il faut pour courber la courbe et $\mathcal{P}$ une énergie potentielle liée à l'image. La courbe recherchée sera la courbe d'énergie minimale.

Énergie de déformation

L'énergie de déformation d'une courbe S traduit la force nécessaire pour modifier l'aspect de la courbe. Cette énergie dépend de la tension w_1 et de la rigidité w_2 et est donnée par la relation suivante :

$$S(v) = \int_0^1 w_1(s) \left| \frac{\partial v}{\partial s} \right|^2 + w_2(s) \left| \frac{\partial^2 v}{\partial s^2} \right|^2 ds \tag{5.10}$$

En augmentant le paramètre w_1 cela revient à avoir une plus grande tension, donc les boucles seront réduites. En augmentant le paramètre w_2 on augmente la rigidité et ceci donnera des courbes plus lisses.

5.3.7 Énergie potentielle

L'énergie potentielle d'une courbe traduit sa position dans l'image. L'énergie potentielle $\mathcal{P}$ est définie à partir d'une fonction scalaire P définie sur l'image, souvent liée à la luminosité. L'énergie potentielle est donnée par :

$$\mathcal{P}(v) = \int_0^1 P(v(s))ds \tag{5.11}$$

Une définition pour la fonction scalaire P est, par exemple, basée sur le filtre Gaussien :

$$P(x, y) = -c|\nabla[G_\sigma \times I(x, y)] \tag{5.12}$$

où c est une constante positive, G_σ le noyau du filtre Gaussien de caractéristique σ et ∇ l'opérateur gradient.

5.3.8 Courbe d'énergie minimale

La courbe v qui minimise l'énergie $\mathcal{E}(v)$ est solution de :

$$-\frac{\partial}{\partial s}\left(w_1 \frac{\partial v}{\partial s}\right) + \frac{\partial^2}{\partial s^2}\left(w_2 \frac{\partial^2 v}{\partial s^2}\right) + \nabla P(v) = 0 \tag{5.13}$$

L'équation (5.13) montre que l'énergie $\mathcal{E}(v)$ minimale se traduit par un équilibre entre les forces internes de courbure de la courbe et l'énergie potentielle. L'équation (5.13) n'est pas facile à résoudre, mais il existe une forme discrète qui permet d'avoir une approximation numérique.

5.3.9 Discrétisation

L'équation (5.9) peut s'exprimer sous forme discrète :

$$E(\mathbf{u}) = \frac{\mathbf{1}}{\mathbf{2}}\mathbf{u^T K u} + \mathbf{P(u)} \tag{5.14}$$

où $\mathbf{u}$ représente une suite de vecteurs qui modélise la courbe v, K une matrice représentant la rigidité de la courbe et P une version discrète de l'énergie potentielle. C'est cette équation qui sera utilisée pour créer des algorithmes de routage.

5.4 Algorithmes de routage

Dans cette section, nous proposons trois manières de router des données en utilisant une image en niveau de gris. Les deux premier algorithmes sont proposés dans la thèse de M. Yousef. Ils utilisent des filtres de convolution : un filtre de Sobel et un filtre moyen. Le troisième algorithme utilise une déformation de route et l'énergie de la courbe $E(v)$ définit dans l'équation (5.14).

5.4.1 Algorithme de routage utilisant Sobel

L'algorithme de routage que nous présentons ici modifie le protocole AODV pour envoyer, de préférence, les paquets vers des zones riches en énergie. Ces zones sont identifiées à l'aide d'un gradient calculé par les noyaux du filtre de Sobel. Le protocole présenté ici a fait l'objet d'une publication dans une conférence [GYL09]. Le protocole se fait en deux étapes : le calcul du gradient d'énergie et le routage utilisant un protocole AODV modifié.

Calcul du Gradient

Dans cette première étape, un capteur va à l'aide des Noyaux G_x et G_y, définit en (5.7) et (5.8), calculer son gradient d'énergie. La problématique est de savoir quelle matrice utilisée dans le produit de convolution avec ces noyaux. La solution est d'utiliser les secteurs d'énergie et la matrice Mv (5.1).

Voici l'algorithme de calcul utilisé par un capteur :

1. Si le capteur a une réserve d'énergie C insuffisante $C < C_0$ alors il ne participe plus à l'opération
2. Le capteur collecte les capacités des batteries C_i et les positions de ses voisins
3. Le capteur crée la matrice Mv à partir des informations précédentes.
4. Le capteur calcule le gradient (g_x, g_y) avec $g_x = -G_y * Mv$ et $g_y = -G_x * Mv$

Chaque capteur dispose donc d'un gradient $G = (g_x, g_y)$ qui est un vecteur allant dans la direction de plus forte énergie. Ce gradient sera utilisé dans un protocole de routage AODV modifié.

Protocole de routage

Le protocole de routage AODV (Ad-Hoc On-demande Distance Vector) est un protocole conçu pour les réseaux Ad-Hoc. Il essaye de découvrir les routes d'une source vers une destination en inondant le réseau de messages RREQ.

Voici la description du protocole AODV :

1. La source inonde le réseau de messages RREQ
2. Un noeud qui n'est pas la destination reçoit et retransmet le message RREQ à tous ses voisins. Il garde le noeud expéditeur et la source dans sa table de routage
3. Le noeud destination reçoit le message RREQ, il répond par un message RREP
4. si un noeud reçoit un message RREP il le retransmet à la source.
5. Si la source reçoit le message RREP, elle compare la nouvelle route avec les routes existantes et sélectionne le chemin le plus court.

La modification portera sur le choix de la route. Au lieu de prendre la route la plus courte, on intégrera une notion énergétique dans ce choix. On favorisera la route qui se rapproche le plus du gradient d'énergie. Ici "se rapprocher" signifie que l'angle entre le gradient d'un capteur et le vecteur V pointant du capteur vers le capteur suivant dans la route, diminue. Le cosinus de cet angle peut être calculé par le produit scalaire :

$$\cos(V, G) = \frac{V \times G}{||V|| \times ||G||} \tag{5.15}$$

Pour chaque route on retiendra la valeur minimale du cosinus. Cette valeur sera gardée par le message RREP. Finalement, la source choisira la route ayant le cosinus maximal dans RREP. La variation du cosinus étant dans le sens inverse de l'angle, choisir le cosinus minimal revient à chercher pour une route la déviation maximale par rapport au gradient. Puis est retenue la route dont la déviation sur l'ensemble du trajet est minimale.

Application

Le protocole de routage utilisant les noyaux de Sobel sera appliqué au réseau de la figure 5.11 :

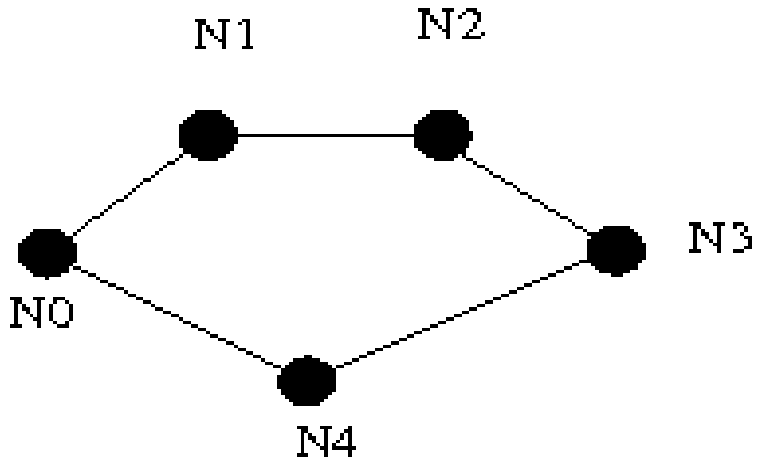

FIGURE 5.11 – Topologie de réseau à 4 capteurs

Le noeud source sera N_0 et le noeud destination N_3. Il y a deux chemins possibles : $P_1 = (N_0, N_1, N_2, N_3)$ et $P_2 = (N_0, N_4, N_3)$.

Deux scénarios seront étudiés :
— Dans le premier scénario, tous les noeud ont la même énergie initiale, de 10 par exemple.
— Dans le deuxième scénario, l'énergie du noeud N_4 est réduite de moitié, soit 5.
Nous pouvons calculer le vecteur gradient pour les différents noeuds dans les deux scénarios :

— Scénario 1

	G_0	G_1	G_2	G_3	G_4
x	20	10	-10	-20	0
y	0	10	10	0	-20

— Scénario 2

	G_0	G_1	G_2	G_3	G_4
x	15	10	-10	-15	0
y	-5	10	10	-5	-20

Pour chaque chemin, nous pouvons calculer les vecteurs qui donnent la direction de la route :

P_1	N_0	N_1	N_2
x	-1	-1	-1
y	1	0	-1

P_2	N_0	N_4
x	-1	-1
y	-1	1

A partir de ces informations, nous pouvons calculer le cosinus :

— Scénario 1 :

P_1	N_0	N_1	N_2
cos	-0.7	-0.7	0

P_2	N_0	N_4
cos	-0.7	-0.7

La valeur maximale du cosinus en valeur absolue est 0.7. La règle d'AODV s'applique et c'est le chemin le plus cours qui est retenu soit P_2.

— Scénario 2

P_1	N_0	N_1	N_2
cos	-0.8	-0.7	0

P_2	N_0	N_4
cos	-0.4	-0.7

P_1 a une valeur absolue minimale de cosinus de 0.7 et P_2 de 0.4. Ici la valeur maximale retenue est 0.7. C'est donc le chemin P_1 qui est retenu.

Dans l'exemple 2, le capteur N_4 a moins d'énergie que les autres capteurs. Le chemin privilégié est P_1 qui passe par N_1 et N_2 ce malgré le fait que le chemin P_2 est plus court. Le protocole a donc choisi une route avec des capteurs plus riche en énergie. Le choix est différent du protocole AODV et a bien tenu compte des contraintes énergétiques.

5.4.2 Protocole de routage utilisant un filtre moyen

Dans cette section nous présentons un protocole proposé dans [YGL10b] qui utilise le filtre moyen. Le calcul du filtre moyen se fait sur un capteur particulier CH, le cluster-head, choisi par l'administrateur. Les capteurs échangent des informations sur l'énergie disponible avec le CH en utilisant le protocole UDP. Un seuil, l'Energy Threshold (ET) limitera la participation des capteurs au routage en fonction de leur énergie disponible.

Paramètres utilisés

— X_i, Y_i les coordonnées du capteur N_i

— BC_i la capacité de la batterie du capteur N_i
— ET le seuil d'énergie
— $SEID$ Sending Energy Information Delay : délais entre l'émission de deux paquets de contrôle
— T : durée d'envoi du denier paquet de contrôle (heure courante - heure d'émission)
— R : rayon de communication des capteurs
— M_i : matrice d'énergie du capteur N_i
— K : noyau du filtre moyen
— ERP_i : Energy Routing Parametre : le produit de convolution $K * M_i$

Le noyau K du filtre moyen est donné par la matrice :

$$K = \begin{pmatrix} 1/12 & 1/12 & 1/12 \\ 1/12 & 4/12 & 1/12 \\ 1/12 & 1/12 & 1/12 \end{pmatrix} \tag{5.16}$$

Protocole de routage

Voici l'algorithme s'exécutant sur chaque capteur :

1. Envoi des informations d'énergie
   Si BC_i a changé alors
   si $(T > SEID)$ alors on envoie BC_i et X_i, Y_i au CH via un paquet de contrôle UDP
2. Calcul s'effectuant sur CH
   (a) CH reçoit les informations de tous les capteurs N_i.
   (b) CH met à jour sa table avec l'adresse IP de N_i et les valeurs de BC_i, X_i, Y_i
   (c) CH calcule $ERP_i = K_i * M_i$
   (d) CH renvoie la valeur ERP_i à N_i.
3. Sur les capteurs N_i
   (a) N_i reçoit la valeur ERP_i de CH
   (b) Si $(ERP_i < ET)$ alors N_i détruit les paquets qui ne sont pas des paquets de contrôle.

Simulations

Les simulations, présentées ici, utilisent le simulateur OMNeT++. Le réseau étudié est formé de 4 capteurs selon la figure 5.12. N_1 est le capteur source et N_0 la destination.

Le protocole de communication utilisé est 802.11 avec une consommation de 250mA en émission et 190mA en réception. En état de veille, le capteur consommera 8mA. Ces consommations sont celle d'un capteur de Nano WiReach. Le trafic est un flux UDP de N_1 vers N_0 en rafale de 0.01s et de taille de paquet de 512 octets. Le protocole de routage est AODV. L'énergie initiale disponible pour les capteurs N_0, N_1, N_4, N_4 sera respectivement de 400, 200, 20 et 100. Les résultats données sont la moyenne sur 10 simulations et chaque simulation est faite pour une durée de 1500s.

Les tables suivantes montrent le nombre de paquets transmis pour les valeurs de $SEID$ de 0.1, 0.5, 1 et 1.5. Le seuil ET aura comme valeurs 0, 25, 50, 75 et 100.

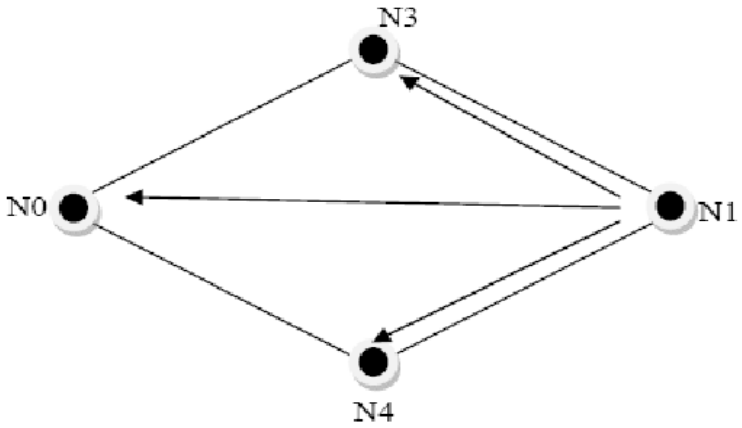

FIGURE 5.12 – Topologie de réseau à 4 capteurs

ET	N_0	N_1	N_3	N_4
0	14300	52500	34100	32800
25	14300	52500	9740	32200
50	14300	52500	10900	8380
75	1620	572	1200	1170
100	1600	571	1170	1180

TABLE 5.1 – Paquets envoyés avec $SEID = 0.1$

ET	N_0	N_1	N_3	N_4
0	2950	48800	24700	26900
25	2950	48800	1990	28500
50	2960	48800	2100	2020
75	1070	392	691	905
100	1030	377	664	871

TABLE 5.2 – Paquets envoyés avec $SEID = 0.5$

ET	N_0	N_1	N_3	N_4
0	1510	48300	25600	23700
25	1510	48300	1080	24500
50	1510	48300	1060	1110
75	237	93	203	158
100	237	93	203	158

TABLE 5.3 – Paquets envoyés avec $SEID = 1$

Les tableaux précédents montrent que N_1 est bien la source vu le nombre de paquets envoyées. Le capteur N_0 est la destination, il n'envoie donc que des paquets de contrôle. Les capteurs N_3 et N_4 relayent les paquets de N_1 vers N_0. L'augmentation du paramètre $SEID$ se traduit par une diminution de l'envoi des paquets de contrôle par N_0. Ceci est cohérent avec le fait que d'augmenter $SEID$ revient à augmenter le délai d'émission entre les paquets de contrôle. Une valeur $SEID \geq 1$ minimise la transmission des paquets de contrôle. Dans ce cas, les informations d'énergie sont mis à jour moins souvent et l'algorithme est moins efficace.

ET	N_0	N_1	N_3	N_4
0	1030	48200	24700	24000
25	1030	48200	891	19500
50	1030	48200	764	780
75	85	36	68	70
100	85	36	68	70

TABLE 5.4 – Paquets envoyés avec $SEID = 1.5$

Pour une valeur $ET = 0$ les capteurs N_3 et N_4 relayent le même nombre de paquets, il n'y a pas d'influence de la capacité énergétique disponible. Le protocole AODV s'applique. Pour une valeur $ET = 25$ le capteur N_4 est favorisé car il a plus d'énergie. Une valeur $ET \geq 75$ coupe les communications. Cette valeur est trop élevée par rapport à l'énergie disponible.

Les tableaux suivants montrent la capacité énergétique restante.

ET	N_0	N_1	N_3	N_4
0	9950	9910	9000	9800
25	9960	9920	9070	9810
50	9960	9920	9130	9830
75	9970	9940	9420	9880
100	9970	9940	9420	9880

TABLE 5.5 – Énergie restante avec $SEID = 0.1$

ET	N_0	N_1	N_3	N_4
0	9960	9920	9150	9830
25	9960	9930	9220	9840
50	9970	9930	9280	9860
75	9970	9950	9450	9890
100	9970	9950	9470	9890

TABLE 5.6 – Énergie restante avec $SEID = 0.5$

ET	N_0	N_1	N_3	N_4
0	9960	9920	9170	9830
25	9970	9930	9240	9850
50	9970	9930	9300	9860
75	9990	9980	9830	9960
100	9990	9980	9830	9960

TABLE 5.7 – Énergie restante avec $SEID = 1$

Le capteur N_3 est celui qui a le moins d'énergie. Nous focalisons donc notre étude sur ce capteur. Pour la valeur $SEID = 0.1$ et $ET = 0$, N_3 a consommé 10% de son énergie. Cette valeur tombe à 8.5% pour un $SEID = 0.5$. L'envoi de paquets de contrôle excessif est pénalisant pour l'énergie. Pour les valeurs $SEID \geq 1$ il n'y a plus de grandes différences, l'algorithme n'est plus efficace. La valeur $SEID = 0.5$ est donc retenue pour la suite.

A une valeur $SEID = 0.5$ et $ET = 0$ la consommation d'énergie pour E_3 est de 8.5%, pour $ET = 25$ elle tombe à 7.8%. Pour une valeur $ET = 50$ la consommation baisse encore, mais l'impacte sur le nombre de paquets transmis est très négatif.

ET	N_0	N_1	N_3	N_4
0	9960	9920	9180	9840
25	9960	9930	9260	9850
50	9970	9930	9300	9850
75	9990	9990	9900	9980
100	9990	9990	9900	9980

TABLE 5.8 – Énergie restante avec $SEID = 1.5$

Ce protocole de routage montre comment à l'aide d'un filtre moyen on peut détecter les zones pauvres en énergie et les évités.

5.5 Protocole de routage utilisant les déformations

Dans cette section, nous proposons un protocole de routage qui utilise des déformations de routes pour minimiser l'énergie du chemin $E(u)$ qui a été définie dans l'équation 5.14. Pour cela il faut définir la matrice de rigidité K, l'énergie potentiel P et ce qu'est une déformation de route.

5.5.1 La matrice de rigidité

Une route est composée d'une suite de n capteurs, par exemple $N_0, N_1, \dots N_n$. Entre deux capteurs successifs, un vecteur $u^i = \overrightarrow{N_i N_{i+1}}$ existe. Une route est représentée par un vecteur u de longueur $2n$ constitué des différentes coordonnées des vecteurs u^i :

$$u = (u_x^1, u_y^1, \dots, u_x^n, u_y^n)^T \in \mathbb{R}^{2n}$$

Si les capteurs se situent sur une grille, alors on a $(u_x^i, u_y^i) \in \{-1, 0, 1\}^2$

La matrice de rigidité $\mathbf{K}$ va favorisée la forme de la route. Elle intervient dans l'expression de l'énergie de déformation :

$$S(u) = \frac{1}{2} u^T \mathbf{K} \mathbf{u}$$

Le chemin en ligne droite est favorisé et donc il minimisera l'énergie de déformation $S(u)$. Ceci permet d'introduire la matrice $\mathbf{K}$:

Définition 13. Soit u une route de longueur n. Alors la matrice de rigidité $\mathbf{K}$ du chemin u est de taille $2n \times 2n$ et est donnée par :

$$\mathbf{K} = \begin{pmatrix} 1 & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 2 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & 2 & \dots & 0 & 0 \\ \vdots & & & & \ddots & & \vdots \\ 0 & 0 & 0 & 0 & \dots & n & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & n \end{pmatrix}$$

Le lemme suivant montre que pour des longueurs de chemins différents, l'énergie de déformation est moins importante pour les petites longueurs.

Lemme 5.5.1. *Soit $S(u)$ l'énergie de déformation donnée par :*

$$S(u) = \frac{1}{2} u^T \mathbf{K} u$$

Soit u une route de longueur n et w une route de longueur m avec même source et destination alors la relation suivante est vérifiée :

$$n < m \Rightarrow S(u) \leq S(w)$$

Démonstration. On a :

$$S(u) = \frac{1}{2} \sum_{i=1}^{n} i \left((u_x^i)^2 + (u_y^i)^2 \right)$$
$$S(w) = \frac{1}{2} \sum_{i=1}^{m} i \left((w_x^i)^2 + (w_y^i)^2 \right)$$

La preuve se fait par récurrence sur $m \geq 2$.

Pour $m = 2$, comme les capteurs sont sur une grille on a $u_\bullet^1 \in \{-1, 0, 1\}$ et $S(u)$ est égale à 1 ou $1/2$. Si $S(u) = 1/2$ alors u est un vecteur vertical ou horizontal. Comme w est une déformation de u, w a même source et destination que u. Ceci implique que w se compose d'une diagonal et d'un vecteur horizontal ou vertical et que $S(w) = 3/2$. Si $S(u) = 1$, alors u est diagonal et w se compose d'un vecteur vertical et horizontal. on a alors $S(w) = 3/2$. Finalement $n < m = 2 \Rightarrow S(n) \leq S(w)$.

La relation $n < m \Rightarrow S(u) \leq S(w)$ est obtenue par récurrence en décomposant la route w par la somme d'une route w' de longueur m et une route de longueur 1.

□

5.5.2 Énergie potentielle

L'énergie potentielle d'une route est définie comme la somme des énergies disponibles des différents capteurs composant la route.

Définition 14. Soit u une route de longueur n. Chaque capteur $S^i(S_x^i, S_y^i), \quad 0 \leq i \leq n$ composant cette route a $I(S_x^i, S_y^i)$ énergie disponible dans ses batteries. Alors, l'*énergie potentielle* de la route u est noté $P(u)$ et est définie comme suite :

$$P(u) = -\sum_{i=1}^{n} I \left(u_x^0 + \sum_{k=1}^{i} u_x^k, u_y^0 + \sum_{k=1}^{i} u_y^k \right)$$

où (u_x^0, u_y^0) sont les coordonnées du capteur source et (u_x^k, u_y^k) est le vecteur reliant le capteur S^{k-1} au capteur S^k.

5.5.3 Déformations de routes

Une route est une succession de capteurs. Nous considérons qu'une route est une déformation d'une autre route si les deux routes ont la source et la destination en commun et si sa longueur ne dépasse pas la longueur d'origine.

Définition 15. Supposons que les capteurs sont sur une grille. Soit u une route de capteur source $S_0(u_x^0, u_y^0)$, de capteur de destination $S_n(u_x^n, u_y^n)$, et de longueur n. Une route w de longueur m est

une déformation de u si et seulement si elle vérifie les conditions :

$$\begin{cases} u_x^0 = w_x^0 \\ u_y^0 = w_y^0 \\ \sum_{i=1}^{n} u_x^i = \sum_{j=1}^{m} w_x^j \\ \sum_{i=1}^{n} u_y^i = \sum_{j=1}^{m} w_y^j \\ m \leq n \end{cases}$$

Par un calcul direct, il est possible de donner une classification des déformations de longueur 1 et 2 :

Lemme 5.5.2. *Soit u une route de longueur 2 et w une déformation de u de longueur 1. Alors cette déformation est de type D_1 :*

$$\begin{pmatrix} u_x^1 \\ 0 \\ 0 \\ u_y^2 \end{pmatrix} \to \begin{pmatrix} u_x^1 \\ u_y^2 \end{pmatrix} \quad \begin{pmatrix} 0 \\ u_y^1 \\ u_x^2 \\ 0 \end{pmatrix} \to \begin{pmatrix} u_x^2 \\ u_y^1 \end{pmatrix}$$

$$\begin{pmatrix} u_x^1 \\ u_y^1 \\ -u_x^1 \\ 0 \end{pmatrix} \to \begin{pmatrix} 0 \\ u_y^1 \end{pmatrix} \quad \begin{pmatrix} u_x^1 \\ 0 \\ -u_x^1 \\ u_y^2 \end{pmatrix} \to \begin{pmatrix} 0 \\ u_y^2 \end{pmatrix}$$

$$\begin{pmatrix} u_x^1 \\ u_y^1 \\ 0 \\ -u_y^1 \end{pmatrix} \to \begin{pmatrix} u_x^1 \\ 0 \end{pmatrix} \quad \begin{pmatrix} 0 \\ u_y^1 \\ u_x^2 \\ -u_y^1 \end{pmatrix} \to \begin{pmatrix} u_x^2 \\ 0 \end{pmatrix}$$

La figure 5.13 représente une déformation D_1.

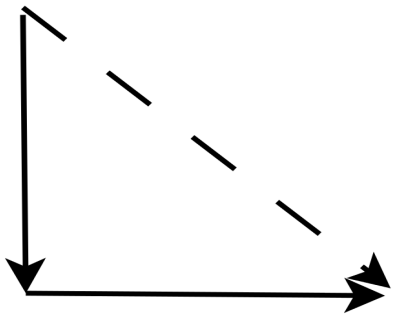

FIGURE 5.13 – Déformation D_1

Lemme 5.5.3. *Soit u une route de longueur 2 et w une déformation de u de longueur 2. Alors cette déformation est de type D_2 :*

$$\begin{pmatrix} u_x^1 \\ u_y^1 \\ u_x^1 \\ 0 \end{pmatrix} \to \begin{pmatrix} u_x^1 \\ 0 \\ u_x^1 \\ u_y^1 \end{pmatrix} \quad \begin{pmatrix} u_x^1 \\ 0 \\ u_x^1 \\ u_y^2 \end{pmatrix} \to \begin{pmatrix} u_x^1 \\ u_y^2 \\ u_x^1 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} u_x^1 \\ u_y^1 \\ 0 \\ u_y^1 \end{pmatrix} \rightarrow \begin{pmatrix} 0 \\ u_y^1 \\ u_x^1 \\ u_y^1 \end{pmatrix} \quad \begin{pmatrix} u_y^1 \\ 0 \\ u_x^1 \\ u_y^2 \end{pmatrix} \rightarrow \begin{pmatrix} u_x^1 \\ u_y^2 \\ u_y^1 \\ 0 \end{pmatrix}$$

La figure 5.14 représente une déformation D_2.

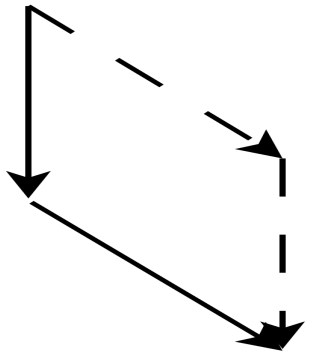

FIGURE 5.14 – Déformation D_2

Le lemme 5.5.4 établit une relation entre la déformation d'une route et son énergie.

Lemme 5.5.4. *Soit u une route de longueur 2 allant du capteur S_{n-1} au capteur S_{n+1} via S_n et $D_1(u)$ sa déformation de longueur 1 alors :*

— *L'énergie de la route déformé $S(D_1(u))$ est inférieur à celle de $S(u)$*

$$S(D_1(u)) \leq S(u)$$

— *L'énergie potentielle de $D_1(u)$ et u sont liée par la relation :*

$$P(D_1(u)) = P(u) - I(S_n)$$

Soit D_2 une déformation de type 2 :

— *Si $u_\bullet^0 \neq 0$ alors :*

$$S(D_2(u)) \geq S(u)$$

— *S'il existe $u_\bullet^0 = 0$ alors :*

$$S(D_2(u)) \leq S(u)$$

— *L'énergie potentielle de $D_2(u)$ et de u sont liée par la relation :*

$$P(D_2(u)) = P(u) + I(S_n) - I(S'_n)$$

où $D_2(u)$ est le chemin (S_{n-1}, S'_n, S_{n+1})

Les déformations D_1 réduisent l'énergie d'une courbe. Ils seront appliqués systématiquement. Les déformations D_2 réduisent l'énergie d'une courbe si l'énergie potentielle du capteur intermédiaire S_n diminue. Cette déformation sera appliquée selon la situation.

5.5.4 Protocole de routage

Le protocole de routage consiste, pour une route donnée, à appliquer des déformations pour minimiser l'énergie E. Il cherche à appliquer en premier les déformations de type D_1. Ensuite

les déformations D_2 sont appliquées si elles réduisent l'énergie E. L'application de ces différentes déformations se fait au niveau de chaque capteur dans une boucle infinie. Comme la longueur maximale des déformations utilisées est de 2, un capteur a besoin de connaître ses voisins et les voisins de ses voisins.

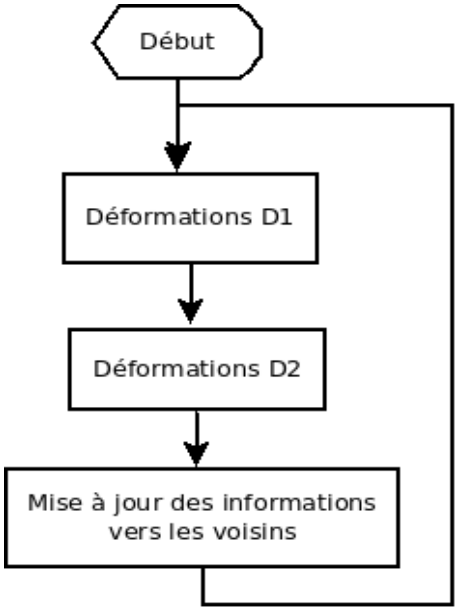

FIGURE 5.15 – Boucle infinie

Une déformation D_x agit sur 3 capteurs successifs. La route u est scindée en des triplets disjoints. La déformation est alors appliquée à chaque triplet. La figure 5.16 montre cette application pour les différentes familles de triplets. Les déformations D_2 ne sont appliquées que si l'énergie du triplet $E(S_{n-1}, S_n, S_{n+1})$ diminue.

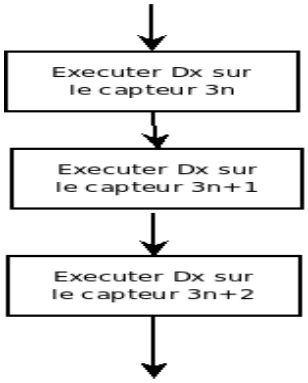

FIGURE 5.16 – Application des déformations D_x

Simulations

Pour les simulations le logiciel scilab est utilisé. Le réseau est représenté par une image en niveau de gris de 300x300 pixels. L'énergie est distribuée selon la loi uniforme sur l'intervalle $[e_{min}, 1]$ avec $e_{min} = 10/256$. L'énergie minimale pour router les informations est de $1/256$. Le capteur source est positionné en $(0, 0)$ et le capteur destination en $(300, 300)$. La route initiale est un chemin vertical et horizontal passant par le capteur $(300, 0)$. La figure 5.17 montre la route initiale sous l'aspect d'une ligne noire.

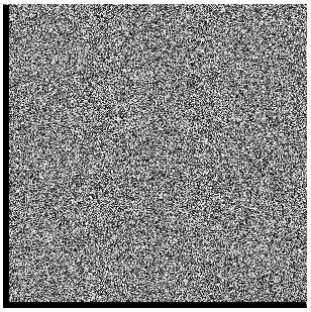

FIGURE 5.17 – Route initiale

La figure 5.18 montre la route après 2000 itérations. La route se situe à la frontière entre la partie noire et l'image en niveaux de gris. Une diagonale commence à apparaître dans le coin en-bas à gauche. C'est l'amorce du chemin le plus cours entre la source et la destination.

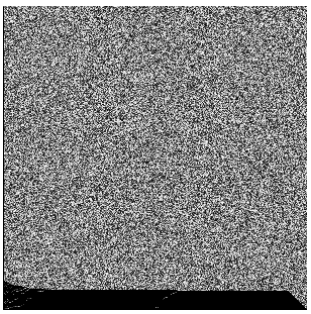

FIGURE 5.18 – Route après 2000 itérations

La figure 5.19 montre la route après 10000 itérations. La diagonale en bas à gauche se prolonge. La partie droite de la route n'a pas encore rejoint la position optimale. Il en résulte un chemin courbe qui se positionne en fonction de l'énergie disponible. Les points claires en partie basse de l'image représente les capteurs dont la grande énergie initiale n'a pas été consommée.

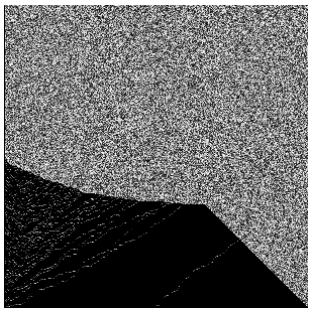

FIGURE 5.19 – Route après 10000 itérations

La figure 5.20 montre la route après 24000 itérations. La route a atteint le chemin le plus cours entre la source et la destination.

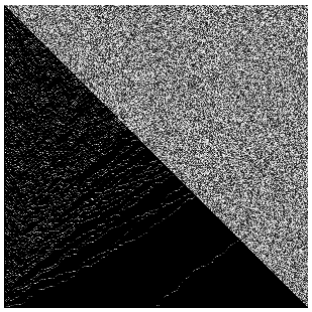

FIGURE 5.20 – Route après 24000 itérations

5.6 Conclusion

Dans cette partie, qui a fait l'objet d'un chapitre de livre [Gil17], nous avons montré comment établir une analogie entre un réseau de capteurs sans fil et une image en niveau de gris. Puis en utilisant des algorithmes de traitement d'image, nous avons créé plusieurs algorithmes de routages qui intègrent des contraintes énergétiques. Finalement, nous avons proposé une approche utilisant des déformations de route pour trouver une route optimale.

Dans le chapitre suivant, nous continuons sur la thématique des algorithmes de routage avec une efficacité énergétique, mais cette fois-ci basée sur l'algorithme de routage multi-chemins AOMDV.

Chapitre 6

Routage multi-chemins pour les réseaux Ad-Hoc à faible consommation

6.1 Introduction

Dans le chapitre précédent, nous avons proposé des protocoles de routage pour les réseaux Ad-Hoc à faible consommation se basant sur les algorithmes de traitement d'image. Or il existe déjà des protocoles de routage pour les réseaux Ad-Hoc. Un protocole très utilisé est le protocole AODV (Ad hoc On-Demand Distance Vector) [71]. Ce protocole est de type réactif, c'est à dire qui construit la route à la demande. Le principe de ce protocole est d'inonder un réseau Ad-Hoc de messages pour découvrir une route vers la destination. Dans AODV, la route la plus courte est conservée si plusieurs routes sont découvertes.

Une variante de ce protocole est AOMDV (Ad-Hoc On-demand Multipath Distance Vector)[58]. Ce protocole, contrairement à AODV, conserve plusieurs routes disjointes d'une source vers une destination. C'est ce protocole qu'a enrichi un étudiant en thèse Amir Adbelkader AOUIZ pour augmenter la durée de vie d'un réseau de capteurs sans fil. Le principe de ce protocole, qui a été présenté dans l'article [LGSH17], est de choisir les routes selon la variation d'énergie des noeuds sur le trajet. Dans ce chapitre nous présentons ces travaux.

6.2 Le protocole de routage AOMDV

Le protocole de routage AOMDV est un protocole de routage réactif. C'est à dire qu'il se déclenche au moment où un noeud d'un réseau Ad-Hoc cherche a communiqué avec un autre noeud.

Supposons qu'un noeud source noté S cherche à se mettre en relation avec un noeud destination D. Si S n'a pas de route vers D, dans sa table de routage, il initie une découverte de routes comme suite :

— S envoie un message de demande de route RREQ (Route Request) à tout ses voisins, leurs demandant une route vers le noeud D.
— Si après un certain temps, S n'a pas de réponse, il revoie la demande
— S'il n'y a pas de réponse, après plusieurs tentatives, S abandonne.

La figure 6.1 montre la propagation des messages RREQ :

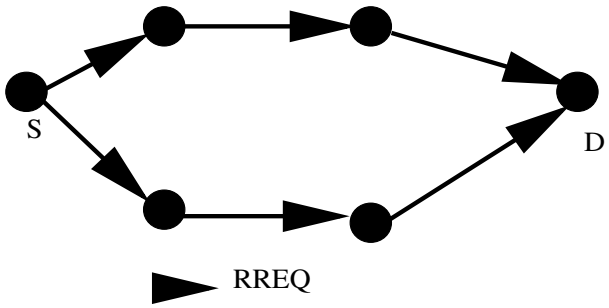

FIGURE 6.1 – Propagation des messages RREQ

Si un noeud reçoit un message RREQ, il effectue le traitement suivant :
— si c'est un nouveau message RREQ :
  — s'il est en relation directe avec S, il met son adresse dans le champ *first_hop*
  — le noeud sauvegarde le chemin retour dans sa table de routage
  — si le noeud connaît une route vers la destination, ou s'il est lui-même la destination, il répond par un message RREP
  — sinon le noeud propage le message RREQ à ses voisins si le nombre maximal de retransmissions n'est pas atteint.

— si le message RREQ a déjà été reçu (par un autre chemin par exemple) :
  — le noeud vérifie le champ *first_hop* pour savoir si c'est une nouvelle route retour à rajouter dans la table de routage
  — si le champ *first_hop* correspond à une entrée dans la table de routage, cette entrée est mise à jour
  — si le noeud connaît une route vers la destination, ou s'il est lui-même la destination, il répond par un message RREP
  — le message RREQ n'est pas propagé

Le champ *fist_hop* permet d'éliminer les chemins commençant par un même lien et donc de garantir qu'on ne mémorise que des chemins avec des liens disjoints. La figure 6.2 est un exemple où la destination reçoit 3 messages RREQ, mais seul deux chemins distincts sont conservés dans la table de routage de D.

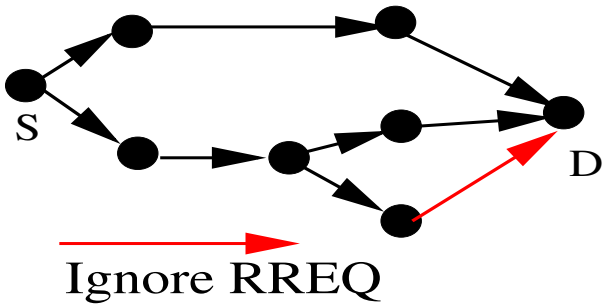

FIGURE 6.2 – Chemins non disjoints, message RREQ ignoré

Si un noeud reçoit un message RREP alors :
— le noeud ajoute le chemin vers la destination D dans sa table de routage
— le noeud renvoie le message RREP vers la source S.
A la fin de ce processus, chaque noeud possède une table de routage contenant les routes disjointes vers la source S et la destination D. Le protocole limite le nombre de routes disjointes enregistrées dans la table de routage.

La figure 6.3 montre un exemple de réseau Ad-Hoc :

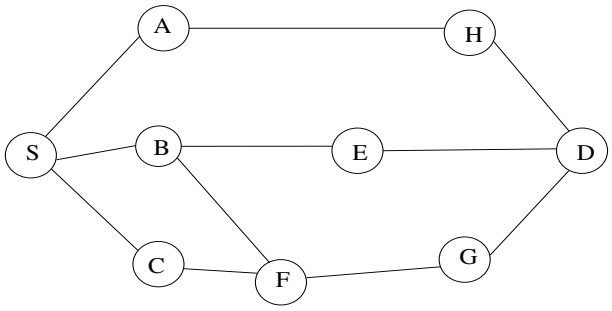

FIGURE 6.3 – Réseau Ad-Hoc

La table de routage de S vers D est :

Dest	Next_hop	Hop_count	Last_hop
D	A	3	H
D	B	3	E
D	C	4	G

L'avantage d'avoir conservé plusieurs routes vers la destination permet en cas de rupture de liens de choisir une route alternative sans avoir à refaire une recherche de routes, comme ce serai le cas dans le protocole AODV.

Pour détecter une rupture de liens, des paquets HELLO sont envoyés régulièrement aux voisins. Si un paquet HELLO n'est plus reçu après un certain temps, le voisin est déclaré défaillant et la source est informée par un message RERR (route error), que les routes passant par le noeud défaillant ne sont plus actifs. A la réception d'un message RERR, la source choisit un autre chemin dans sa table de routage. Si la table est vide, un nouveau processus de découverte de liens est initié.

6.3 Protocole de routage multi-chemins prenant en compte la variation d'énergie

Nous avons modifié le protocole de routage AOMDV pour prendre en compte la variation d'énergie des noeuds. Le but de la modification du protocole AOMDV est d'augmenter la durée de vie des réseaux de capteurs sans fil qui sont alimentés par une source d'énergie limitée, comme une batterie par exemple.

Le protocole de routage utilise deux seuils Eng_{th1} et Eng_{th2}, tel que $Eng_{th1} > Eng_{th2}$.

Le premier seuil Eng_{th1} sert à exclure du processus de calcul de route, les noeuds qui ont une forte consommation d'énergie, et qui s'épuisent rapidement.

Le deuxième seuil Eng_{th2}, quand à lui, permet de sélectionner en priorité des chemins qui

contiennent des noeuds à faible consommation d'énergie. Cela permet de favoriser des chemins qui ont une durée de vie plus longue.

Chaque chemin présent dans la table de routage est marqué d'un drapeau $ForteVariation$ qui est mis à *vrai* si le chemin contient un noeud à forte variation d'énergie.

6.3.1 Calcul de la variation d'énergie

Pour assurer la maintenance des liens, un noeud envoie régulièrement des messages HELLO à ses voisins. Le message HELLO, ainsi que les messages RREQ et RREP, vont être surchargé par une variable contenant la dernière variation d'énergie calculée, sur un intervalle de temps I, par la formule suivante :

$$\Delta Eng = \frac{Eng_{t+I} - Eng_t}{Eng_t} * 100 \tag{6.1}$$

où Eng_t représente l'énergie disponible dans les batteries du noeud à l'instant t.

Cette valeur est calculée à chaque envoi de paquets HELLO, RREP et RREQ et est transmis par ces paquets. Nous allons maintenant voir comment le protocole prend en compte cette information.

6.3.2 Traitement des paquets HELLO

Quand un noeud reçoit un paquet HELLO de l'un de ses voisins V, il vérifie si son voisin n'a pas une consommation d'énergie excessive en comparant le champ ΔEng_{HELLO} du paquet HELLO au seuil Eng_{th2} :
Si $\Delta Eng_{HELLO}(V) > Eng_{th2}$ alors tout les chemins de la table de routage content le noeud V sont marqués $ForteVariation = vrai$.

6.3.3 Traitement des paquets RREQ et RREP

Si un noeud reçoit un paquet RREQ ou RREP, il commence par vérifier si sa variation d'énergie n'est pas excessive pour participer au protocole de routage. Il calcule sa variation d'énergie ΔEng et la compare au seuil Eng_{th1}.
Si $\Delta Eng > Eng_{th1}$, il ignore le paquet et ne participe pas au routage.

Si $\Delta Eng \leq Eng_{th1}$, le noeud traite le paquet comme le ferai le protocole AOMDV, mais s'il rajoute une route à sa table de routage, il la marque $ForteVariation = vrai$ si le champ ΔEng présent dans le paquet RREQ ou RREP est supérieur au seuil Eng_{th2}. Cela signifie que l'expéditeur du message RREQ ou RREP est un noeud à forte variation d'énergie et que le chemin qui le contient sera marqué $ForteVariation = vrai$.

A bout de ce processus, nous avons donc des chemins avec le drapeau $ForteVariation$ activé, nous allons voir comment ce marquage intervient dans le choix de la route.

6.3.4 Choix de la route

La table de routage d'un noeud contient après le processus précèdent deux types de routes, celles marquées par le drapeau $ForteVariation$ à *vrai* et celle qui ne sont pas marquées.

Lors de l'envoi d'un paquet, l'algorithme consiste à choisir la route parmi les chemins de la table qui ne sont pas marqués, comme le ferai AOMDV. Si un tel chemin n'existe pas, on considère les routes avec le drapeau $ForteVariation$ à vrai et on applique l'algorithme de sélection de AOMDV à cet ensemble de chemins.

Par cet algorithme, nous privilégions donc les routes avec des noeuds ayant une faible variation d'énergie. Les simulations suivantes permettent de montrer l'efficacité de ce protocole.

6.4 Simulations

Les simulations suivantes sont réalisées avec le logiciel NS2. Le protocole de routage AOMDV, et le protocole modifié PCEV_AOMDV, sont comparés. La transmission et la réception de paquets sont consommatrice en énergie, et au bout d'un certain temps un noeud ne va plus avoir assez d'énergie pour fonctionner. Nous allons donc comparer le nombre de noeuds actifs à différentes durées de simulations.

Les paramètres de simulations sont :

Eng_{th1}	10%
Eng_{th2}	0,5%
Taille du terrain	1500x1500
Nombre de noeuds	100
débit	8 packets/s
Consommation de Réception	1W
Consommation de Transmission	1W
Énergie initiale	100j

La figure 6.4 montre l'évolution du nombre de noeuds actifs en fonction du temps de simulation.

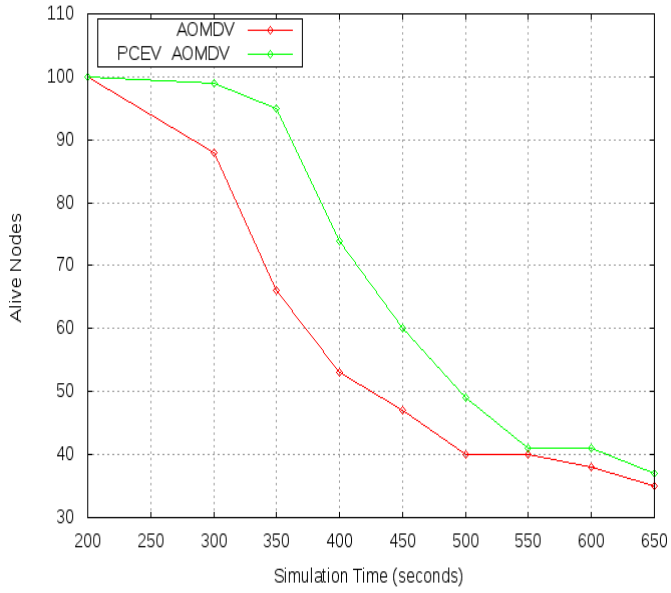

FIGURE 6.4 – Nombre de noeuds actifs en fonction du temps

La figure 6.4 montre bien que le nombre de noeuds actifs du protocole PCEV_AOMDV est supérieur au protocole AOMDV. L'écart est maximal à 350 secondes où PCEV_AOMDV a 30% de noeuds actifs en plus. Cela est dû au fait que les noeuds à forte variation en énergie ne participent

plus au routage, et donc leur capacité énergétique est préservée. Puis l'écart diminue. Cela est dû au fait que tous les noeuds s'épuisent dans le temps.

6.5 Conclusion

Dans ce chapitre, nous avons introduit un nouveau protocole de routage basé sur une modification de AOMDV qui prend en compte la variation d'énergie pour sélectionner des routes moins gourmandes en énergie. Des simulations ont montrées l'efficacité de ce protocole.

Dans le chapitre suivant, nous allons nous intéresser à un autre protocole de routage pour les réseaux Ad-Hoc : le protocole OLSR qui est un protocole de routage proactif.

Chapitre 7

Sécurisation du protocole de routage OLSR

7.1 Introduction

Ce chapitre présente le travail réalisé par l'étudiant en thèse Kamel Saddiki qui a donné lieu à une publication dans un journal [LGSH17]. Dans son travail, il utilise le protocole de routage proactif OLSR. Le protocole OLSR [44] introduit des noeuds particuliers MPR qui permettent de réduire le nombre de messages nécessaires à l'apprentissage de la topologie du réseau. Ce protocole présente une vulnérabilité : si un noeud malveillant parvient à devenir MPR, il pourra détourner le trafic, voir l'interrompre. Avec monsieur Saddiki, nous proposons un moyen de détecter les noeuds malveillants qui essayent de modifier la topologie du réseau pour devenir MPR.

7.2 Le protocole de routage OLSR

Le protocole de routage OLSR est un protocole de routage proactif. C'est à dire que le protocole ne se déclenche pas à la demande, mais maintient les routes du réseau. L'avantage d'un tel protocole est la réactivité lors de la mise en oeuvre d'une communication, car il n'y a pas de délais pour construire la route. Mais son inconvénient est la nécessité de connaître la topologie du réseau. OLSR optimise l'échange des messages nécessaires pour le routage en introduisant des noeuds particuliers appelés relais multipoints ou "Multipoint Relays" (MPR). Chaque noeud choisit les noeuds MPR parmi ses voisins qui ont une forte connectivité. Les noeuds MPR sont utilisés pour acheminer les informations dans le réseau. Pour établir la liste des noeuds MPR il faut connaître ses voisins à un ou deux sauts.

7.2.1 Découverte des voisins

Chaque noeud diffuse à intervalle régulier un message HELLO à un saut (TTL=1) contenant :
- La liste de ses voisins avec qu'il a établi un lien bi-directionel
- La liste des voisins dont il a reçu un message HELLO
- La liste des noeuds qu'il a désignés comme MPR
- Un paramètre *willigness* qui permet de forcer la sélection d'être MPR pour ses voisins ou, au contraire, de ne jamais être sélectionné.

Quand un noeud reçoit un message HELLO, il effectue les tâches suivantes :

— il met à jour la liste des voisins dont il a reçu un message HELLO
— s'il est présent dans la liste des voisins, il en déduit un lien bidirectionnel vers l'émetteur du paquet HELLO
— il met à jour la liste des voisins à deux sauts joignables par un lien bidirectionnel
— il met à jour la liste des noeuds qui l'ont choisi comme MPR
— le paramètre *willigness* est sauvegardé avec le noeud dans les différentes listes

Après cette opération, le noeud a connaissance de ses voisins à un et deux sauts qui sont joignables par un lien bidirectionnel. Ces informations lui permettent de calculer son ensemble de noeud MPR.

7.2.2 Sélection des noeuds MPR

Un noeud MPR sélectionné par un noeud N du réseau à pour but de relayer les informations à destination de N. Il est donc un voisin direct de N, qui dans un souci d'optimisation, a une connectivité maximale avec les voisins à deux sauts de N. Ceci pour limiter le nombre de noeuds MPR.

Le noeud N utilise l'algorithme suivant pour déterminer son ensemble de noeuds MPR :
— Il définit la liste N_1 des noeuds voisins à un saut
— Il définit la liste N_2 des noeuds à exactement deux sauts
— Il ajoute les voisins ayant le paramètre *willigness* à "Allways" à sa listes MPR
— S'il existe un noeud I de N_2 qui a un unique voisin $N_{I,1}$ dans N_1, il ajoute $N_{I,1}$ à MPR et retire I de N_2.
— Il cherche les noeuds de N_1 qui ont une connectivité maximale vers N_2 et les ajoutes à MPR
— Il retire les noeuds de N_2 qui sont joignable par les noeuds de MPR
— si N_2 n'est pas vide, il refait l'étape précédente

La figure 7.1 montre un exemple de sélection de noeuds MPR pour le noeud N :

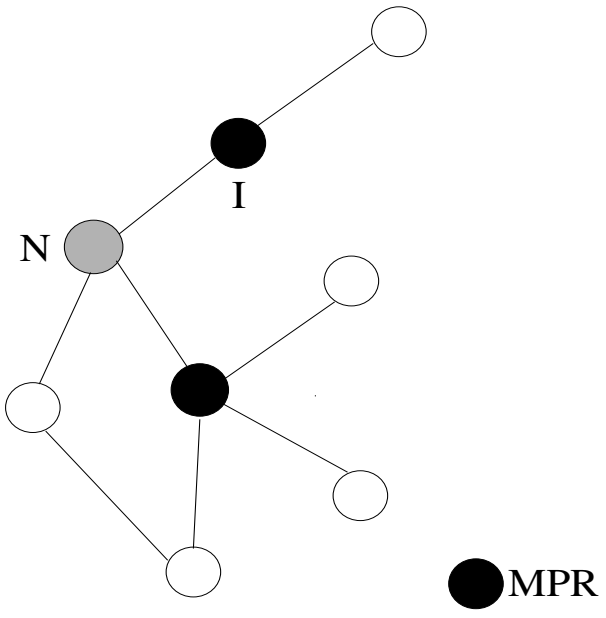

FIGURE 7.1 – Les noeuds MPR de N

7.2.3 Apprentissage de la topologie

Comme OLSR est un protocole proactif, chaque noeud doit connaître la topologie du réseau pour calculer sa table de routage.

Par les paquets HELLO, chaque noeud sait s'il a été sélectionné comme MPR par un de ses voisins. Il peut ainsi établir une liste des voisins pour lesquels il est MPR.

Si un noeud est MPR, il diffuse la liste des noeuds qui l'ont désigné par des messages *Topologie Control (TC)*. Ces messages sont diffusés dans tout le réseau.

Tous les noeuds du réseau ont finalement connaissance des noeuds MPR et de la liste des noeuds qu'ils permettent de joindre. Cela permet le calcul de la table de routage.

7.2.4 Calcul de la table de routage

La table de routage est calculée à l'aide des informations collectées par les messages TC. Les messages TC permettent de donner un lien entre un noeud MPR et un de ses voisins qu'il permet de joindre. Les routes sont construites de proche en proche.

La table de routage à la forme :

Dest_ADDR	Last_hop	Dist	interface

où :
— *Dest_ADDR* est l'adresse du noeud destination
— *Last_hop* l'adresse du noeud MPR de la destination (c'est le dernier noeud de la route avant destination)
— *dist* est la distance, c'est à dire le nombre de sauts jusqu'à destination
— *interface* est l'interface via laquelle le noeud est joignable
Pour trouver un chemin vers la destination, il faut partir de la destination et "remonter" la table de routage jusqu'à la source. La figure 7.2 montre un tel chemin.

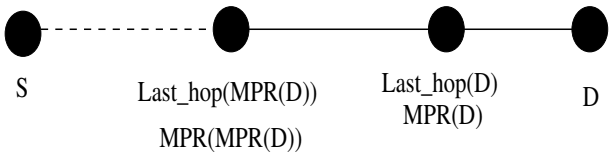

FIGURE 7.2 – Un chemin de S vers D

Ce protocole présente de nombreuses vulnérabilités. L'une d'elle consiste à ce qu'un noeud malveillant devient MPR. Nous présentons cela dans la prochaine section.

7.3 Attaque du protocole OLSR de type "trou noir"

OLSR utilise des noeuds MPR pour acheminer le trafic. Une attaque de type "trou noir" ou "black hole" est faite par un noeud malveillant M qui essaie de devenir un noeud MPR de sa victime V. S'il y parvient, il peut intercepter, voir interrompre, le trafic à destination de V.

Pour devenir un noeud MPR de V, M va envoyer des messages HELLO à V avec des informations erronées pour se faire désigner comme MPR. Il a plusieurs possibilités pour y arriver :

— il force sa désignation en mettant le paramètre *willingness* à *Allways*
— il annonce un noeud qui n'existe pas dont il est le seul voisin, il sera donc choisi car seule passerelle possible pour le noeud fictif, voir figure 7.3
— il annonce des liens bidirectionnels fictifs vers d'autres noeuds du réseau. Il augment ainsi sa connectivité pour être choisi, voir figure 7.4

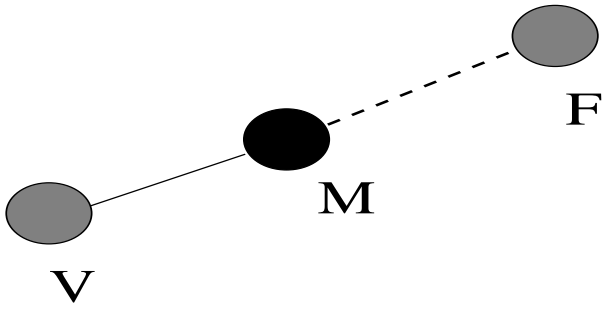

FIGURE 7.3 – Attaque avec un noeud fictif F

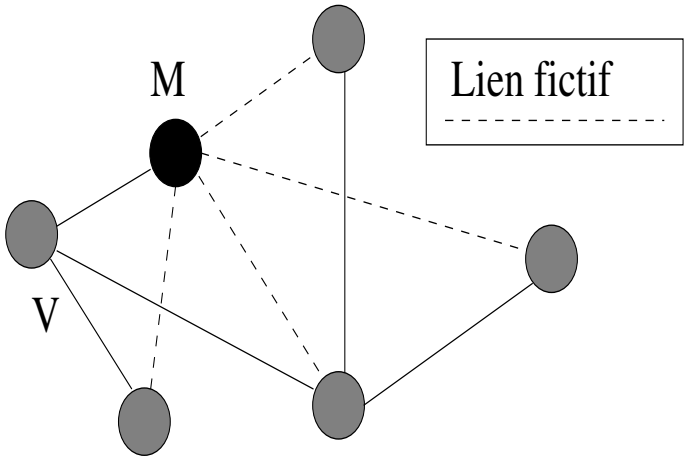

FIGURE 7.4 – Attaque avec des liens fictifs

Dans notre travail, nous proposons une façon de détecter la dernière attaque, celle de l'annonce des liens fictifs.

7.4 Détection des noeuds MPR malveillants

7.4.1 Tentative d'attaque

Supposons qu'un noeud malveillant M souhaite être sélectionner MPR pour le noeud A. Il va attaquer le noeud A en plusieurs étapes :

— Dans un premier temps, le noeud M va écouter le réseau et capter les paquets TC pour connaître les noeuds à deux et trois sauts de A.
— Puis il va envoyer des messages HELLO à A qui annoncent des liens bidirectionnels fictifs vers les noeuds à deux et trois sauts de A.
— Le noeud M va avoir une connectivité maximale vers les voisins à deux sauts de A et donc être choisi comme MPR de A

— A va supprimer tous les autres noeuds MPR de sa liste car M permet d'être joint par tous les noeuds
— A annonce dans les paquets HELLO que M est le noeud MPR de A.
— M reste donc la seule "passerelle" vers A et donc il peut bloquer le trafic vers A.

Dans notre proposition, le noeud A va détecter que M est malveillant avant de l'ajouter à la liste des MPR.

7.4.2 Détection du noeud malveillant

La détection se fait en deux phases. La première phase consiste à calculer la moyenne des liens par noeuds et déterminer un seuil par rapport auquel on suppose qu'un noeud annonce un nombre de liens anormalement élevé. La deuxième phase est une vérification des liens annoncés.

Phase une

Cette phase commence par calculer le seuil de détection par l'algorithme suivant :

— Après réception des paquets HELLO, le noeud A calcule la moyenne du nombre de liens annoncés par ses voisins et de lui-même à l'aide de la formule :

$$Avg(A) = \sum_{V=1}^{\deg(A)} \frac{\deg(V)}{\deg(A)+1} + \frac{\deg(A)}{\deg(A)+1} \tag{7.1}$$

— Le noeud A ajoute le résultat de $Avg(A)$ au paquet HELLO et le diffuse à ses voisins
— A la réception d'un paquet HELLO du voisin V, le noeud A vérifie que le champ $Avg(V)$ est positif, sinon V est suspecté
— le noeud A calcule la moyenne $LAvg(A)$ des moyennes des voisins et de lui-même :

$$LAvg(A) = \sum_{V=1}^{\deg(A)} \frac{Avg(V)}{\deg(A)+1} + \frac{Avg(A)}{\deg(A)+1} \tag{7.2}$$

— A fixe le seuil de détection SD à :

$$SD = \lfloor LAvg(A) \rfloor + 1 \tag{7.3}$$

Si un voisin de A annonce un nombre de liens supérieur au seuil SD il est suspecté.

Phase deux

Dans cette phase, le noeud A va vérifier les liens déclarés par chaque noeud M qui est suspecté. Pour cela A diffuse une demande d'information INF_REQ aux noeuds à deux sauts (avec un TTL=2).

Le paquet INF_REQ contient :
— L'adresse du noeud A : SI (Solicited information)
— L'adresse source du paquet (qui peut être l'adresse d'un voisin de A qui relaie le paquet)
— L'adresse du noeud malveillant M
Si un noeud reçoit un paquet INF_REQ, il vérifie si M est un voisin. Si ce n'est pas le cas, il répond avec un paquet INF_REP contenant :

— L'adresse du noeud qui répond AN (acknowledment node)

— L'adresse du demandeur A qui est l'adresse de destination du paquet
— L'adresse source du paquet

Remarquons que les paquets INF_REP sont une réponse négative à la requête, et ne sont envoyé que par les noeuds qui n'ont pas de liens avec M. Cela évite que M puisse répondre à la requête en confirmant les liens fictifs.

Si le noeud A reçoit un message INF_REP, alors A comptabilise un lien invalide pour le noeud M.

Après un certain temps, A calcule le pourcentage de liens invalide pour le noeud M et compare cette valeur au seuil de classement SC :

$$\frac{\text{nombre de liens invalides de } M}{\deg(M)} \times 100 > SC \qquad ? \tag{7.4}$$

Si le pourcentage de liens invalides est supérieur au seuil SC, il marque le noeud M avec le champ *willingness* à *never* et donc le noeud n'est jamais choisi comme noeud MPR. L'utilisation du seuil SC est dû au fait que certains liens peuvent être temporairement invalides dû à la mobilité des noeuds ou à des perturbations de la communication sans fil.

Les simulations suivantes montrent l'efficacité de l'algorithme.

7.5 Simulations

Les simulations sont faites avec le logiciel NS2. Une simulation comporte 25 noeuds avec au plus 3 noeuds malveillants. Nous comparons trois scénarios : OLSR qui est un fonctionnement normal du réseau avec le protocole OLSR, BH_OLSR qui représente un réseau attaqué utilisant le protocole OLSR et New_OLSR qui est un réseau attaqué utilisant notre protocole de routage.

Les paramètres de NS2 sont les suivants :

Version simulateur	2.35
Temps de simulation	100s
Rayon de transmission	250m
Type de trafique	CBR
Taille des paquets	512 octets
Débit	4 paquets/s
Nombre de noeuds	25
Nombre de noeuds attaquants	1,2,3

7.5.1 Taux de paquets délivrés

Nous allons comparer le taux de paquets délivrés pour les trois scénarios. Le taux PDR est calculé à l'aide de la formule :

$$PDR = 100 \times \frac{\sum \text{Paquets reçus}}{\sum \text{paquets envoyés}} \tag{7.5}$$

La figure 7.5 compare les trois scénarios en fonction du nombre de noeuds malveillants :

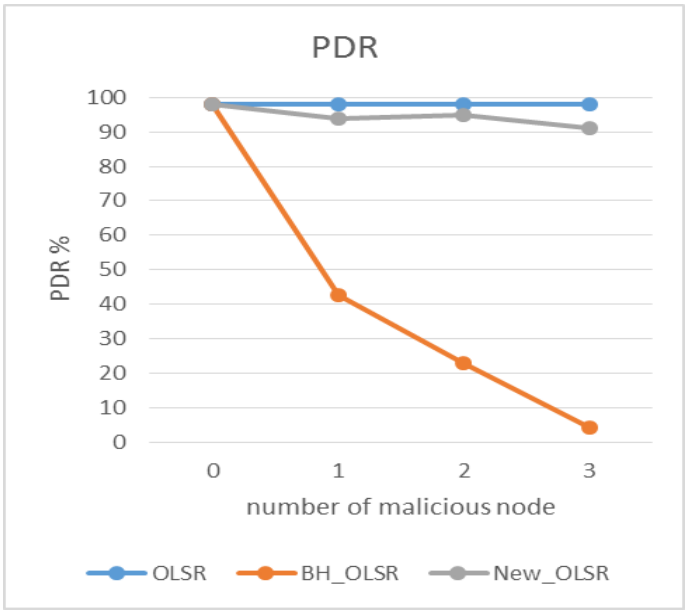

FIGURE 7.5 – Taux de paquets délivrés

Nous constatons un effondrement du taux de paquets reçus pour le protocole OLSR si le nombre de noeuds malveillants augmente. Par contre, le taux PDR pour notre protocole de routage reste très proche du taux normal. Notre protocole est donc efficace.

7.5.2 Nombre de paquets perdus

La figure 7.6 nous donne le nombre de paquets perdus en fonction des différents scénarios :

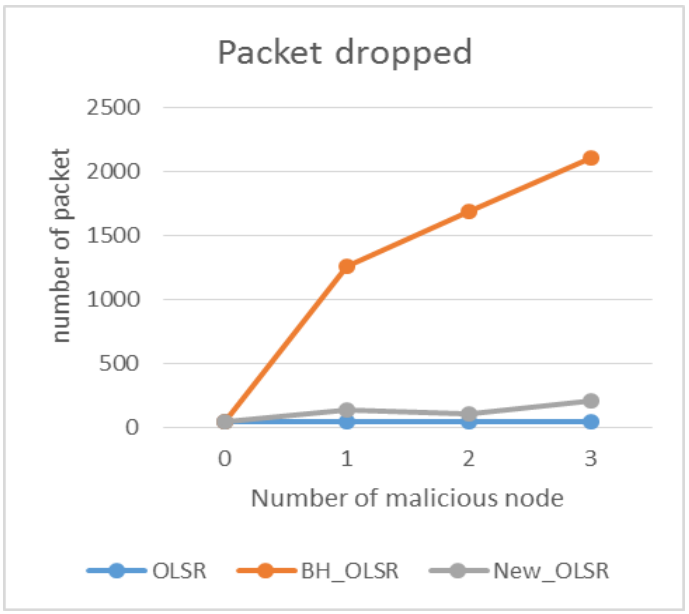

FIGURE 7.6 – Nombre de paquets perdus

Ce graphique est en cohérence avec la figure 7.5 et montre l'efficacité de notre protocole.

7.5.3 Surcharge du protocole

Nous avons introduit de nouveaux paquets de contrôles : INF_REQ et INF_REP. On peut se demander si cela ne surcharge pas le réseau. Comparons donc cette surcharge pour les différents scénarios donnés dans la figure 7.7 :

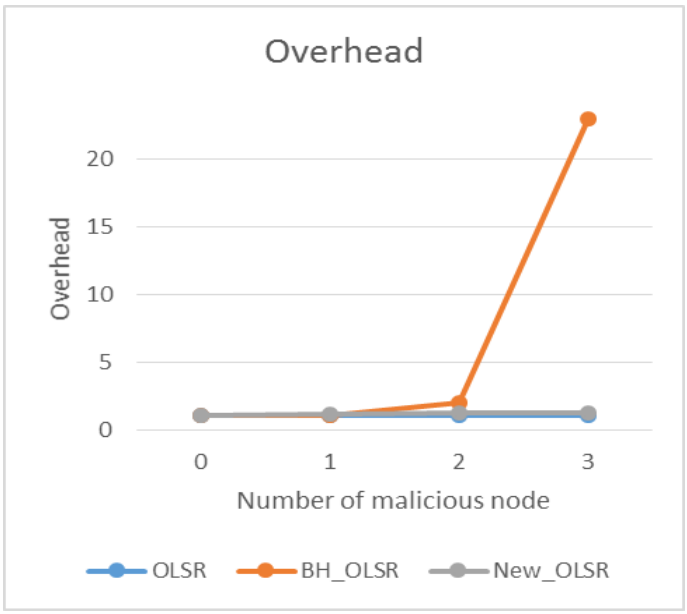

FIGURE 7.7 – Surcharge du réseau

Dans la figure 7.7, nous constatons que la différence de surcharge entre le protocole OLSR et le notre est minime. Notre protocole n'introduit pas une surcharge du réseau. Par contre, lors d'une attaque avec le protocole OLSR cette surcharge augmente. Cela est dû au trafique généré par les noeuds malveillants et par la tentative de rechercher une route pour contrer la coupure réseau.

7.6 Conclusion

Dans ce chapitre, nous nous sommes intéressés à un protocole de routage proactif : OLSR. Nous avons étudié une attaque de ce protocole par des noeuds malveillants qui diffusent de faux liens. Nous avons introduit une métrique pour détecter ces noeuds. Finalement nous avons proposé un protocole OLSR modifié qui résiste à ces attaques.

Chapitre 8

Résumé, perspectives et conclusion

8.1 Résumé et conclusion des travaux réalisés

L'ensemble de mes travaux présentés ici portent sur le contrôle d'accès et le routage des réseaux sans fils. Après avoir étudié la congestion des réseaux Ad-Hoc, nous avons proposé d'évaluer leur équité par une approche théorique utilisant des réseaux étoiles. L'idée était d'évaluer des propriétés d'un réseau sans fils en l'approchant par des réseaux particuliers qui permettent de les calculer. Dans un deuxième chapitre, nous avons introduit une analogie des réseaux de capteurs sans fil avec une image en niveau de gris dans le but de créer des algorithmes de routage à faible consommation d'énergie.

Cette deuxième partie, particulièrement innovante, fait un lien entre le routage dans les réseaux de capteurs et les outils disponibles pour le traitement d'image. Une notion de déformation de route a aussi été donnée dans le but d'optimisation d'une route par "approche successive".

Des travaux plus conventionnels ont été présentés dans les chapitres suivants. Ces travaux portent sur la modification d'un protocole de routage réactif AOMDV et d'un protocole de routage proactif OLSR. Le protocole AOMDV a été modifié dans le but de prolonger la durée de vie d'un réseau de capteurs sans fil en favorisant des routes avec des noeuds à faible évolution de la consommation d'énergie. Le protocole OLSR a été modifié dans le but de combattre une attaque de type trou noir. Ceci est une ouverture vers l'aspect sécurisation des protocoles.

D'autres travaux n'ont pas été présentés dans ce mémoire dans un souci de cohérence. Les travaux effectués avec madame Karima Chemoun [CGLL18] portent sur les bâtiments intelligents. Nous nous sommes intéressés à l'analyse de trames d'un réseau domotique pour y découvrir des scénarios dans le but d'automatiser le fonctionnement d'une maison. Pour cela, un cadre a été défini pour utiliser la théorie des croyances. Cette théorie permet de donner des critères probabilistes pour compléter un début de scénario. Ces travaux ont récemment été acceptés dans un journal [CGLL18] et la thèse est en cour de rédaction.

Avec monsieur Tayeb Diab nous explorons des problèmes de sécurisation des réseaux véhiculaires. S'inspirant d'un protocole annonymisant I2P pour les réseaux filaires, nous avons identifié plusieurs problématiques. La première est la diffusion de clés de chiffrement de type Diffie-Hellman dans un réseau véhiculaire. Dans le travail proposé, un protocole de diffusion de clés a été validé par rapport à différentes attaques. Un travail en cours proposera un protocole de création de tunnels chiffrés pour créer des groupes de véhicules communicant de manière sécurisé et anonyme.

L'ensemble de ces travaux ouvrent des perspectives de recherches.

8.2 Perspectives

8.2.1 Invariants topologiques pour la QOS

Dans la première partie de nos travaux, nous avons étudié les problèmes de contention en utilisant les cliques maximales. Ces cliques sont issues de la théorie des graphes. Il existe des invariants triviaux comme le degré d'un noeud, le nombre d'arêtes qui a une influence indéniable sur la congestion des réseaux Ad-Hoc. Nous suspectons qu'il **doit exister des invariants plus complexes, que nous devons construire pour mieux cerner la qualité de service dans les réseaux**.

La connectivité d'un graphe est aussi intéressante pour notre étude.

Les graphes k-arête-connexe sont des graphes qui cessent d'être connexe seulement si on supprime k arêtes. Les graphes k-sommet-connexe, quant à eux, perdent leurs connectivités quand on retire k sommets du graphe. Il existe aussi les graphes fortement connexes qui caractérisent une connectivité entre tous les noeuds. Un graphe peut aussi contenir des cycles, chaines dont les sommets de départ et de fin sont les mêmes. Il existe aussi la notion de graphe expenseur, qui prend en compte les liaisons entre un sous-graphe et le graphe dont il est inclu. **Il y a encore beaucoups d'autres notions et certaines restent à inventer**.

Nous proposons de lier ces notions à des caractéristiques de qualité de service d'un réseau Ad-Hoc : bande passante, débit, équité, contraintes temporelles, etc .. Il est évident que la topologie du réseau induit des contraintes sur ces facteurs.

Nous proposons d'utiliser un prolongement et la méthodologie adoptés pour définir l'équité d'un réseau. Cette méthodologie consiste a approché des réseaux par des réseaux à topologie simple, dont on sait évaluer certaines propriétés. Nous espérons par cette approche pouvoir démontrer certaines limitations pour des réseaux Ad-Hoc ayant une certaine structure.

Ainsi, après avoir construit des **graphes élémentaires**, sur lesquels nous avons **évalué théoriquement les paramètres de qualité de service**, nous souhaitons **élargir ces résultats à des graphes de topologie de réseaux quelconques**. Par exemple si une topologie de réseaux sans fil contient un sous-graphe de tel type, alors, sa bande passante s'en trouvera limitée.

Ces **informations sur les sous-graphes** peuvent aussi être **étendues au routage**. Nous avons proposé une **approche d'optimisation de routes par déformations de chemins**. Cette approche consiste à définir une matrice de rigidité pour un chemin, et l'énergie nécessaire pour le déformer. Nous avons aussi défini une énergie potentielle, en fonction de la contrainte que nous souhaitons imposer à notre route. Nous l'avons appliqué à une contrainte énergétique, mais cela peut être une autre contrainte. Nous avons donné des **déformations élémentaires** pour **réduire l'énergie de déformation**.

Nous souhaitons poursuivre cette approche.

Connaissant la construction optimale d'une **route pour un sous-graphe**, nous espérons **étendre cette route à la topologie du réseau par déformation**.

Lors de la mobilité des noeuds, cette méthode permettra en cas de conservation des sous-graphes de reconstruire la route plus efficacement. Cela réduira l'échange de messages pour redécouvrir la nouvelle topologie du réseau.

Les réseaux Ad-Hoc que nous avons étudiés sont constitués de *noeuds se situant sur un plan.*

Leur rayon de communication est modélisé par un cercle. Les simulations sont faites sur une répartition plane des capteurs. En réalité, cela est souvent très différent. Les capteurs peuvent être utilisés dans des milieux hostiles difficiles d'accès, comme en montage par exemple. Leur position est donc liée au relief. Les capteurs ne se situent plus sur un plan mais se **répartissent dans l'espace**. De plus, nous pouvons imagier que ces capteurs sont **mobiles**.

Ceux capteurs peuvent *être des drones* qui ont besoin de communiquer entre eux pour se coordonner. Par exemple ces drones peuvent servir de relais de communications ou faire des mesures au-dessus d'une zone hostile. Leurs déplacements peuvent aussi dépendre de l'application et de la zone à couvrir. Nous retrouvons ici toutes les problématiques des réseaux de capteurs que nous avons étudiées en deux dimensions, **la troisième dimension apportant une complexité supplémentaire**.

Les rayons de communications sont des **sphères**, les graphes représentant la topologie du réseau sont dans l'espace. Mais nous pouvons nous poser la question de savoir si **une projection de ce graphe sur un plan permet d'avoir des informations** sur les paramètres de qualité de service comme la congestion, l'équité, etc ... Paramètre que nous avons étudié dans un espace à deux dimensions.

8.2.2 Utilisation d'une Intelligence Artificielle pour les réseaux sans fils et les réseaux SDN

Nous avons proposé une analogie entre un réseau de capteurs sans fil et une image en niveau de gris.

Nous proposons d'**étendre cette analogie à d'autres paramètres de QOS que l'énergie**, voir même utiliser des **images en couleurs** pour représenter plusieurs paramètres. Au lieu d'utiliser des algorithmes de traitements d'images, nous souhaitons **utiliser des réseaux de neurones et des méthodes de reconnaissances d'image**.

Un neurone est constitué de plusieurs entrées, chacune pondérée par un coefficient. La somme de ces entrées est ensuite donnée à une fonction non linéaire appelée fonction d'activation. Le résultat de cette fonction constitue la sortie du neurone. Un réseau de neurones est formé en interconnectant plusieurs neurones.

De tels réseaux sont utilisés dans la reconaissance d'images. Le principe est de faire apprendre aux neurones des images types. On donne en entrée une image, et en sortie on obtient la catégorie à laquelle appartient l'image. La difficulté de l'apprentissage est d'ajuster les coefficients de pondération des entrées et de déterminer la bonne fonction d'activation pour obtenir le résultat souhaité.

Pourquoi ne pas **faire apprendre à un réseau de neurones plusieurs scénarios de routage ?** Il faudra par exemple constituer **une base d'images de réseaux Ad-Hoc** et **calculer les routes par un protocole de routage classique**, type AODV ou OLSR. Cela constituera l'**échantillon d'apprentissage**. Le réseau de neurones recevra en entrée l'image du réseau, et en sortie produira la sélection de noeuds pour former la route.

Nous pouvons espérer qu'avec le développement des processeurs neuronaux, par exemple Intel Movidius ou Nvidia Jetson, chaque capteur pourra dans le futur embarquer un tel processeur et une base de données de "chemins types" pour faire leur routage.

Nous souhaitons aussi **appliquer les réseaux de neurones aux réseaux SDN**. Les réseaux SDN (Software Defined Network) sont une nouvelle approche des réseaux. Leur organisation se fait autour d'un contrôleur qui centralise les actions de commutation, de routage et de filtrage. Le contrôleur communique par un protocole de contrôle, comme openflow par exemple, avec des commutateurs réseaux dépourvus d'intelligence. Cette *technologie émergente* permet une grande

agilité du réseau en orientant les flux en fonction des demandes.

Dans ces réseaux, le plan de contrôle est centralisé. Ce qui permet d'avoir une vision de l'état du réseau et des trafics qui s'y établissent. Dans ce plan de contrôle, toutes les fonctions réseaux sont regroupées : fonction de commutation, fonction de filtrage du trafic et fonction de routage. Il y a aussi une interaction entre ces fonctions, les applications et les machines virtuelles présentes sur l'infrastructure.

Nous proposons d'**introduire des fonctions de qualité de service au niveau du contrôleur**. Par exemple construire des routes pour maîtriser la consommation d'énergie, comme nous l'avons déjà fait pour les réseaux Ad-Hoc. La vision globale que procure le plan de contrôle permet de connaître les flux, les répartitions de charges, etc .. Nous avons donc les mêmes avantages que lors de l'utilisation d'un protocole de routage proactif : la connaissance de la topologie du réseau. Nous pouvons **ajouter au contrôleur des algorithmes pour améliorer la qualité de service** en cherchant l'optimisation de la bande passante, la maîtrise de la congestion ou de l'équité.

Nous proposons aussi d'introduire une **intelligence artificielle dans le contrôleur** pour assurer la sécurité des flux. Pour cela, un **apprentissage** des différents états normaux de commutations et de routage permettra à un réseau de neurones d'identifier un trafic potentiellement malveillant. La solution à mettre en œuvre devra **être évolutive dans le temps pour s'adapter à l'agilité du réseau**.

8.2.3 Objets communicants et bâtiments intelligents : utilisation d'une intelligence artificielle pour l'auto-configuration et la sécurisation

Dans notre quotidien, de plus en plus d'**équipements électroniques sont pourvu de moyens de communication**. Cela va des montres connectées, capables de transmettre des données biométriques, de luminaires ayant la possibilité de changer d'intensité ou de couleur, de robots pouvant transmettre images et sons pour surveiller sa maison, d'une baignoire qui permet de régler la température de l'eau à distance, d'un pot de fleur qui assure l'arrosage en surveillant l'humidité de la terre, voire d'autres applications aux possibilités infinies. Tous ces objets communicants utilisent un protocole IP compatible avec l'internet et donc ils sont accessibles à des applications tierces sur un téléphone ou un ordinateur.

Malheureusement, la provenance très hétérogène de ces objets limite l'interaction entre eux et souvent l'objet a la seule fonction de communiquer avec une application dédiée, conçue par le même fabriquant. Nous proposons de créer un protocole ou une passerelle pour **accroître l'interopérabilité des objets communicants**. Cette intéropérabilité devra se faire de manière transparente pour l'utilisateur.

Par exemple, l'utilisateur qui vient d'acquérir un tel objet pourra l'insérer dans son environnement sans configuration. L'objet sera reconnu par les objets existants et leur annoncera les fonctions pour lesquelles il a été conçu. Ce n'est donc pas une simple configuration des paramètres de communication (adresse IP par exemple) qui est attendu, mais bien une extension des possibilités applicatives du système. Ce même système devra être en capacité de se **prévenir de l'introduction d'objets malveillants** et avoir des capacités de sécurisation des communications. Une intelligence artificielle pourra acquérir l'ensemble des objets présents et veiller à leur optimisation en proposant des scénarios adaptés.

L'internet des objets augmente la surface d'attaque des réseaux. Nous proposons de **développer des moyens de chiffrement et d'authentification adaptés à des systèmes embarqués** qui sont souvent limités en ressources de calculs et de mémoires. Nous pouvons aussi développer des protocoles d'authentification et d'établissement de tunnels chiffrés, qui permettent de garantir la confidentialité et la protection contre l'introduction d'objets malveillants dans le système. L'**intelligence artificielle**, que nous développerons, pourra aussi participer à la sécurisation

de l'environnement en *surveillant la légitimité des ordres* circulant sur le réseau domotique.

Effectivement, les **bâtiments intelligents comportent de plus en plus d'objets communicants** qui génèrent d'énormes quantités de données. Les protocoles utilisés sont très variés : réseaux IP (support d'internet), LoRaWan (utilisé dans l'internet des objets), KNX, mobius, BACnet (protocoles spécifiques à la domotique). Tout ce monde communique, et donc est potentiellement **vulnérable à des cyberattaques** qui peuvent être désastreuses : coupures de congélateurs, de chauffage, perturbation d'un système d'alarme, blocage d'un ascenseur, etc ... Dans le domaine des réseaux, il existe des **détecteurs d'intrusion** qui analysent le trafic réseau pour prévenir et anticiper les attaques. Le travail que nous proposons est l'*élaboration d'un tel équipement pour les bâtiments intelligents.*

Cet équipement ne sera pas limité à la seule action de protection. L'idée sera d'utiliser l'analyse des différentes communications bâtimentaires pour assurer une fonction de protection (détection des menaces) mais aussi de proposer des **scénarios pour automatiser la gestion du bâtiment** dans le but de réduire la consommation d'énergie.

Pour cela nous utiliserons des **outils d'intelligence artificielle**, notamment l'apprentissage profond, pour assurer l'adaptation de l'équipement à son environnement. Une analyse spécifique du comportement du bâtiment permettera de définir les normes de fonctionnement.

Nous proposons d'étendre notre champ du bâtiment vers les **réseaux électriques intelligents**. Le développement des sources d'énergie renouvelable (éolien ou solaire) nécéssite que les réseaux électriques deviennent communicant, pour gérer au mieux la production d'énergie en fonction de la consommation. La mise en oeuvre des *compteurs communicants* chez le consommateur, des *postes de transformation intelligents* et des *systèmes de production à la demande* augmente la nécessité d'échange de données d'un réseau électrique pour un contrôle en temps réel. **Cela augmente la surface d'attaque de ces réseaux qui sont vitaux**.

Nous proposons de tenir compte des contraintes liées à la production d'énergie et à son transport pour valider les transactions circulant sur le réseau. Pour cela nous proposons le dévelopement d'un **système basé sur l'apprentissage profond** pour **valider en temps réel les ordres de configuration**. Cela nécessite aussi le développement de protocoles spécialisés pouvant répondre rapidement aux besoins d'analyse du réseau.

8.2.4 Réseaux applicatifs sécurisés pour réseaux véhiculaires

Les **réseaux véhiculaires** sont des réseaux Ad-Hoc particuliers, où les noeuds se déplacent à grande vitesse en suivant des routes bien définies. Leur *densité est très variable* d'un milieu urbain très dense à un milieu rural peu fréquenté. Sur ce réseau, des applications se développent : applications liées à la sécurité routière, applications de diffusions de média ou jeux en ligne pour les passagers.

Nous proposons d'étudier les contraintes de sécurité liées à ces applications. Ces contraintes peuvent être de type temps réel ou de validation d'information pour les applications de type sécurité routière par exemple. D'autres peuvent être du type confidentialité ou d'authentification comme pour les diffusions multimédias ou jeux. D'autres encore devront garantir un certain anonymat pour les communications.

Ces contraintes peuvent se traduire par la **nécessité d'échanger des clés où d'établir des tunnels entre les noeuds**. Du fait de la forte mobilité des noeuds et de leur positionnement géographique, il sera intéressant de dévellopper de nouvelles normes pour l'échange de clés et l'authentification en fonction des contraintes applicatives dans les réseaux véhiculaires.

8.3 Conclusion

Dans la perspective d'être habilité à diriger les recherches, je souhaiterai créer une nouvelle équipe de recherche qui allierait la force des mathématiques et de l'intelligence artificielle pour répondre aux défis que nous impose l'évolution exponentielle des usages numériques. Ces défis sont aussi bien techniques liées à l'accroissement et l'accessibilité de l'information pour des usages quotidients nécessitant des réseaux mobiles de plus en plus fiables et agiles, que sécuritaires, englobant la protection des données et l'intégritées de celles-ci.

Nous voyons quotidiennement l'empleur des attaques qui se développent. Le cyberespace devenant ainsi un continent où s'affrontent différents intérêts : étatiques, groupes de pressions, voire mafieux. Ainsi la maîtrise de l'information (ou de la désinformation) devient un enjeu majeur, pouvant avoir un impact sur les populations. Nous pouvons citer comme exemple les manipulations supposées de différentes élections. Il est donc indispensable d'avoir des moyens de protection à la hauteur de l'enjeu et c'est ce que je souhaiterais développer avec mon équipe.

Le numérique devient aussi un objet du quotidien, se banalisant à travers des objets de plus en plus communicants.

Dans cette évolution, l'homme devra pouvoir s'appuyer sur son environnement digital doté d'intelligence, pour se soulager de tâches répétitives, mais aussi pour être accompagner sur certains choix, comme la maîtrise energétique. Tout cela devra bien se faire avec une sécurité maîtrisée. Ainsi, dans le futur, nous devrons créer des processus d'intelligence artificielle répondant à ces critères.

Les Universités, les organismes de rechercher et les entreprises du numérique sont déja dans cette démarche stratégique qui est fortement soutenue par les financeurs publics et privés.

Finalement, je pense qu'être habilité à diriger les recherches me donnera l'indépendance pour exprimer pleinement mes ambitions de recherche et donnera accès à des ressouces, qu'elles soient humaines, comme la possibilité d'avoir des doctorants, ou financières en sollicitant des finances à un plus haut niveau de responsabilité.

Bibliographie Personnelle

[AHLG18] Amir Abdelkader AOUIZ, Sofiane BOUKLI HACENE, Pascal Lorenz, and Marc GILG. Network life time maximization of the AOMDV protocol using nodes energy variation. *Network Protocols and Algorithms*, 10(2) :73–94, jun 2018.

[CGLL18] Karima Chemoun, Marc Gilg, Mourad Laghrouche, and Pascal Lorenz. Evidence theory-based framework for improving automation in home automation system. *International Journal of Communication Systems*, 0(0) :1–22, August 2018.

[Gil17] Marc Gilg. 2 - representation of networks of wireless sensors with a grayscale image : Application to routing. In Smain Femmam, editor, *Building Wireless Sensor Networks*, pages 31 – 66. Elsevier, 2017.

[GKL08] Marc Gilg, Jean-Marc Kelif, and Pascal Lorenz. Power allocation problem in homogeneous and perturbated homogeneous CDMA networks. In *2008 IEEE International Conference on Communications*, volume 1-13, pages 343–348. IEEE, 2008. (ICC 2008), Beijing, MAY 19-23, 2008.

[GL04] M Gilg and P Lorenz. An adjustable scheduling algorithm in wireless ad hoc networks. In *Universal Multiservice Networks,* , volume 3262 of *Lecture Notes in Computer Science*, pages 216–226. Springer-Verlag BERLIN, 2004. Oporto, PORTUGAL, OCT 25-27, 2004.

[GL05] M. Gilg and P. Lorenz. A totally distributed and adjustable scheduling algorithm in wireless ad-hoc networks. *Autonomic and Autonomous Systems and International Conference on Networking and Services, Joint International Conference on*, 0 :1–7, 2005.

[GLM08] Marc Gilg, Pascal Lorenz, and Abderrahim Makhlouf. Fairness in a static wireless network. *Systems and Networks Communication, International Conference*, 0 :17–22, 2008.

[GLR11] M. Gilg, P. Lorenz, and J. Rodrigues. Location-aided routing using image representation for wireless sensor networks. In *2011 IEEE International Conference on Communications (ICC)*, pages 1–5, June 2011.

[GML09] M. Gilg, A. Makhlouf, and P. Lorenz. Fairness index in single and double star network. *International Journal On Advances in sytems and Measurements*, 2 :109–118, 2009.

[GYL09] Marc Gilg, Yaser Yousef, and Pascal Lorenz. Using image processing algorithms for energy efficient routing algorithm in sensor networks. *Future Computing, Service Computation, Cognitive, Adaptive, Content, Patterns, Computation World*, 0 :132–136, 2009.

[LGGL11] J. Lloret, M. Gilg, M. Garcia, and P. Lorenz. A group-based protocol for improving energy distribution in smart grids. In *2011 IEEE International Conference on Communications (ICC)*, pages 1–6, June 2011.

[LGSH17] Pascal Lorenz, Marc Gilg, Kamel Saddiki, and Sofiane Boukli Hacene. Black hole attack detection and ignoring in OLSR protocol. *International Journal of Trust Management in Computing and Communications*, 4(1) :75–93, 2017.

[MGL09] Abderrahim Makhlouf, Marc Gilg, and Pascal Lorenz. Fairness in double star ad hoc networks. *Networking and Services, International conference*, 0 :107–111, 2009.

[PLGN10] Manuela Popescu, Pascal Lorenz, Marc Gilg, and Jean Marc Nicod. Event management ontology : Mechanisms for semantic-driven diagnosis. *Networking and Services, International conference on*, 0 :129–136, 2010.

[SBHLG18] Kamel Saddiki, Soufiane Boukli-Hacene, Pascal Lorenz, and Marc Gilg. Trust-neibours-base to mitigate the cooperative black hole attack in olsr protocol. In *SSCC-2018*, 2018.

[YGL10a] Yaser Yousef, Marc Gilg, and Pascal Lorenz. Using convolution filters for energy efficient routing algorithm in sensor networks. *International Journal On Advances in Intelligent Systems*, 3(1 and 2) :150–161, September 2010.

[YGL10b] Yaser Yousef, Marc Gilg, and Pascal Lorenz. Using matrix convolutions and clustering for energy efficient routing algorithm in sensor networks. *Sixth Advanced International Conference on Telecommunications*, 0 :275–279, 2010.

Bibliographie

[1] AbdelSalam, H. S., and Olariu, S. Toward adaptive sleep schedules for balancing energy consumption in wireless sensor networks. *IEEE Transactions on Computers 61* (2012), 1443–1458.

[2] Abuzanat, H., Trouillet, B., and Toguyeni, A. Fair Queuing Model for EDCA to optimize QoS in Ad-hoc Wireless Network. In *8th International Conference on Networks (ICN)* (2009), IEEE, pp. 306–311. Gosier, FRANCE, MAR 01-06.

[3] Abuzanat, H., Trouillet, B., and Toguyeni, A. FQ-EDCA : An Extension of EDCA to improve Fairness in Ad-hoc Wireless Network. In *CIE :International Conference on Computers and Industrial Engineering* (2009), vol. 1-3, IEEE, pp. 1617–1622.

[4] Akyol, U., Andrews, M., Gupta, P., Hobby, J. D., Saniee, I., and Stolyar, A. Distributed Dynamic Control of Multi-Hop Wireless Networks : From Theory to Practice. *Bell Labs Technical Journal 14*, 3 (FAL 2009), 139–155.

[5] Alam, M. M., Berder, O., Menard, D., and Sentieys, O. Traffic-aware adaptive wake-up-interval for preamble sampling mac protocols of wsn. *Cross Layer Design, International Workshop on 0* (2011), 1–5.

[6] Alawieh, B., Zhang, Y., and Assi, C. A Distributed Power and Rate Control Scheme for Mobile Ad hoc Networks. In *6th International Symposium on Modeling and Optimization in Mobile, Ad-Hoc, and Wireless Networks* (2008), vol. 1 and 2, IEEE, pp. 321–329. Berlin, GERMANY, APR 01-03.

[7] Alonso-Zarate, J., Gregoratti, D., Giotis, P., Verikoukis, C., and Alonso, L. Medium Access Control Priority Mechanism for a DQMAN-Based Wireless Network. *IEEE Communications Letters 13*, 7 (JUL 2009), 495–497.

[8] Ammar, I., Awan, I., and Min, G. An improved s-mac protocol based on parallel transmission for wireless sensor networks. *Network-Based Information Systems, International Conference on 0* (2010), 48–54.

[9] Anastasi, G., Ancillotti, E., Conti, M., and Passarella, A. Design and Performance Evaluation of a Transport Protocol for Ad hoc Networks. *Computer Journal 52*, 2 (2009), 186–209.

[10] Antonopoulos, C., and Koubias, S. Congestion Control Framework for Ad-Hoc Wireless Networks. *Wireless Personnal Communications 52*, 4 (MAR 2010), 753–775.

[11] Ashraf, M., Jayasuriya, A., and Perreau, S. Channel MAC Protocol for Opportunistic Communication in Ad Hoc Wireless Networks. *EURASIP Journal on Advances in Signal Processing* (2009).

[12] Augustson, J. G., and Radhakrishnan, J. An analysis of some graph theoretical cluster technics. *Journal of the Association for Computer Machinery 17*, 4 (1970), 571–586.

[13] Babic, Z., and Mandic, D. An efficient noise renioval and edge preserving convolution filter. In *6th International Conference on Telecommunications in Modern Satellite* (2003), vol. 1 and 2, IEEE, pp. 538–541.

[14] Bassem, C., and Bestavros, A. CSR : Constrained Selfish Routing in Ad-Hoc Networks. In *Wireless Algorithms, Systems and Applications* (2009), vol. 5682 of *Lecture Notes in Computer Science*, SPRINGER-VERLAG BERLIN, pp. 179–189. Boston, MA, AUG 16-18.

[15] Basu, M. Gaussian-based edge-detection methods-a survey. *IEEE Transactions on Systems, Man, and Cybernetics, Part C : Applications and Reviews 32*, 3 (Aug. 2002), 252 – 260.

[16] Begum, S., Helmy, A., and Gupta, S. Modeling and Test Generation for Worst-case Performance Evaluation of MAC Protocols for Wireless Ad Hoc Networks. In *MASCOTS : 17th IEEE International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems* (2009), IEEE, pp. 205–214.

[17] Boppana, S., and Shea, J. M. Impact of Overlapped Transmission on the Performance of TCP in Multihop Ad Hoc Networks. In *MILCOM 2008 :IEEE Military Communications Conference* (2008), vol. 1-7, IEEE, pp. 2509–2515. San Diego, CA, NOV 16-19.

[18] Bouharras, M., Dziong, Z., Gagnon, F., and Haider, M. Scheduling Optimization in Multiuser detection based MAC design for Ad-Hoc Networks. In *33rd Annual IEEE Conference on Local Computer Networks* (2008), vol. 1 and 2, IEEE, pp. 640–645. Montreal, CANADA, OCT 14-17.

[19] Chen, F., Zhai, H., and Fang, Y. Available Bandwidth in Multirate and Multihop Wireless Sensor Networks. In *2009 29TH IEEE International Conference on Distributed Computing Systems* (2009), IEEE, pp. 281–288. Montreal, CANADA, JUN 22-26, 2009.

[20] Chen, G., Zhang, X., Yu, J., and Wang, M. An improved leach algorithm based on heterogeneous energy of nodes in wireless sensor networks. *Computing, Measurement, Control and Sensor Network, International Conference on 0* (2012), 101–104.

[21] Chen, Q., Zhang, Q., and Niu, Z. A Graph Theory Based Opportunistic Link Scheduling for Wireless Ad Hoc Networks. *IEEE Transactions on Wireless Communications 8*, 10 (OCT 2009), 5075–5085.

[22] Chunjiang, Z., and Yong, D. A Modified Sobel Edge Detection Using Dempster-Shafer Theory. In *2nd International Congress on Image and Signal Processing* (2009), Qiu, PH and Yiu, C and Zhang, H and Wen, XB, Ed., vol. 1-9, IEEE, pp. 1635–1638.

[23] Cui, H.-X., and Wei, G. A Novel Backoff Algorithm based on the tradeoff of Efficiency and Fairness for Ad hoc Networks. In *WRI International Conference on Communications and Mobile Computing* (2009), vol. 2, IEEE, pp. 81–86. Kunming,CHINA, JAN 06-08.

[24] Dai, L., Chen, W., Cimini, Jr., L. J., and Letaief, K. B. Fairness Improves Throughput in Energy-Constrained Cooperative Ad-Hoc Networks. *IEEE Transactions on Wireless Communications 8*, 7 (JUL 2009), 3679–3691.

[25] Dong, L., Shu, Y., Sanadidi, M., and Gerla, M. A Method for Improving the TCP Fairness in Wireless Ad Hoc Networks. In *4th International Conference on Wireless Communications, Networking and Mobile Computing* (2008), vol. 1-31, IEEE, pp. 2631–2634. Dalian, CHINA, OCT 12-17.

[26] Doohan, N. V., Mishra, D. K., and Tokekar, S. Energy aided shortest path routing protocol (easprp) for highly data centric wireless sensor networks. *Intelligent Systems, Modelling and Simulation, International Conference on 0* (2012), 652–656.

[27] Durvy, M., Dousse, O., and Thiran, P. On the Fairness of Large CSMA Networks. *IEEE Journal on Selected Areas in Communications 27*, 7 (SEP 2009), 1093–1104. IEEE INFOCOM Conference 2008, Phoenix, AZ, APR 13-18, 2008.

[28] Durvy, M., Dousse, O., and Thiran, P. Self-Organization Properties of CSMA/CA Systems and Their Consequences on Fairness. *IEEE Transactions on Information Theory 55*, 3 (MAR 2009), 931–943.

[29] Falcon, R., Liu, H., Nayak, A., and Stojmenovic, I. Controlled straight mobility and energy-aware routing in robotic wireless sensor networks. *Distributed Computing in Sensor Systems and Workshops, International Conference on 0* (2012), 150–157.

[30] Geng, R., Li, Z., and Song, L. AQMP : An Adaptive QoS MAC protocol based on IEEE802.11 in Ad Hoc Networks. In *5th International Conference on Wireless Communications, Networking and Mobile Computing* (2009), vol. 1-8, IEEE, pp. 2878–2881. Beijing, CHINA, SEP 24-26.

[31] Giang, P. T., and Nakagawa, K. Achieving Fairness over 802.11 Multihop Wireless Ad Hoc Networks. *IEICE Transactions on Communications E92B*, 8 (AUG 2009), 2628–2637.

[32] Giang, P. T., and Nakagawa, K. Contention Window Size Control for QoS Support in Multi-hop Wireless Ad Hoc Networks. In *Management Enabling the Future Internet for Changing Business and New Computing Services* (2009), vol. 5787 of *Lecture Notes in Computer Science*, SPRINGER-VERLAG BERLIN, pp. 261–272. 12th Aisia-Pacific Network Operations and Management Symposium, Jeju Isl, SOUTH KOREA, SEP 23-25, 2009.

[33] Goyal, D., and Tripathy, M. R. Routing protocols in wireless sensor networks : A survey. *Advanced Computing & Communication Technologies, International Conference on Anvanced Computing and Communication Technologies 0* (2012), 474–480.

[34] Han, Z., and Poor, H. V. Coalition Games with Cooperative Transmission : A Cure for the Curse of Boundary Nodes in Selfish Packet-Forwarding Wireless Networks. *IEEE Transactions on Communications 57*, 1 (JAN 2009), 203–213.

[35] Haneef, M., and Deng, Z. Comparative analysis of classical routing protocol leach and its updated variants that improved network life time by addressing shortcomings in wireless sensor network. *2010 Sixth International Conference on Mobile Ad-hoc and Sensor Networks 0* (2011), 361–363.

[36] Hanzo, II, L., and Tafazolli, R. Admission Control Schemes for 802.11-Based Multi-Hop Mobile Ad hoc Networks : A Survey. *IEEE Communications Surveys and Tutorials 11*, 4 (2009), 78–108.

[37] Hou, T.-C., and Hsu, C.-W. Achieving Fair Throughput among TCP Flows in Multi-Hop Wireless Mesh Networks. *IEICE Transactions on Communications E93B*, 4 (APR 2010), 916–927.

[38] Hu, J., Ma, Z., and Sun, C. Energy-efficient mac protocol designed for wireless sensor network for iot. *2010 International Conference on Computational Intelligence and Security 0* (2011), 721–725.

[39] Huang, C.-W., Loiacono, M., Rosca, J., and Hwang, J.-N. Airtime Fair Distributed Cross-Layer Congestion Control for Real-Time Video Over WLAN. *IEEE Transactions on Circuits and Sustems for Video Technology 19*, 8 (AUG 2009), 1158–1168.

[40] Huang, J.-H., and Kao, Y.-F. Price-based resource allocation strategies for wireless ad hoc networks with transmission rate and energy constraints. In *16th International Conference on Computer Communications and Networks* (2007), vol. 1-3, IEEE, pp. 1065–1070. Honolulu, HI, AUG 13-16, 2007.

[41] Huang, J.-W., Hung, C.-M., Yang, K.-C., and Wang, J.-S. Energy-efficient probabilistic target coverage in wireless sensor networks. *Networks, IEEE International Conference on 0* (2011), 53–58.

[42] Huang, Y.-F., Wang, L.-M., Tan, T.-H., and Chen, C.-M. Performance of a novel energy-efficient data relaying in wireless sensor networks. *Computer, Consumer and Control, International Symposium on 0* (2012), 793–796.

[43] Hui, T., Fan, J., and Weijun, C. A Game Theory based Load-Balancing Routing with Cooperation Stimulation for Wireless Ad hoc Networks. In *HPCC, 11th IEEE International Conference on High Performance Computing and Communications* (2009), IEEE, pp. 266–272. Seoul, SOUTH KOREA, JUN 25-27.

[44] Jacquet, P., Muhlethaler, P., Clausen, T., Laouiti, A., Qayyum, A., and Viennot, L. Optimized link state routing protocol for ad hoc networks. In *Proceedings. IEEE International Multi Topic Conference, 2001. IEEE INMIC 2001. Technology for the 21st Century.* (2001), IEEE, pp. 62–69.

[45] Jaiswal, S. K., Ganz, A., and Mettu, R. An Optimization Framework for Demand-based Fair Stream Allocation in MIMO Ad Hoc Networks. *Mobile Networks & Applications 14*, 4 (AUG 2009), 451–469.

[46] Jianlai, W., Chunling, Y., and Chao, S. A Novel Algorithm for Edge Detection of Remote Sensing Image Based on CNN and PSO. In *2nd International Congress on Image*

and Signal Processing (2009), Qiu, PH and Yiu, C and Zhang, H and Wen, XB, Ed., vol. 1-9, IEEE, pp. 2862–2866.

[47] Jin-Yu, Z., Yan, C., and Xian-Xiang, H. Edge Detection of Images Based on Improved Sobel Operator and Genetic Algorithms. In *International Conference on Image Analisys and Signal Processing* (2009), Min, Y and Zhao, XM and Zhang, ZJJ and Sun, L and Francia, G, Ed., IEEE, pp. 32–35.

[48] Kasi, M. K., Hinze, A., Legg, C., and Jones, S. Sepsen : semantic event processing at the sensor nodes for energy efficient wireless sensor networks. In *Proceedings of the 6th ACM International Conference on Distributed Event-Based Systems* (New York, NY, USA, 2012), DEBS '12, ACM, pp. 119–122.

[49] Khanna, V. K., Gupta, H. M., and Maheshwari, S. A high throughput and low power ad-hoc wireless LAN protocol. *Wireless Networks 14*, 1 (FEB 2008), 1–16.

[50] Lahmar, K., Cheour, R., and Abid, M. Wireless sensor networks : Trends, power consumption and simulators. *Asia International Conference on Modelling & Simulation 0* (2012), 200–204.

[51] Li, Z., and Shen, H. A kautz-based real-time and energy-efficient wireless sensor and actuator network. *2012 IEEE 32nd International Conference on Distributed Computing Systems 0* (2012), 62–71.

[52] Lihong, D., and Yan'an, J. A novel MAC protocol for hidden receiver problem in ad hoc networks. In *2007 IEEE International Conference on Automation and Logistics* (2007), vol. 1-6, IEEE, pp. 2345–2348. Jinan,CHINA, AUG 18-21, 2007.

[53] Lin, F. Y. S., and Wen, Y. F. Fair inter-TAP routing and backhaul assignment for wireless mesh networks. *Wireless Communications & Mibile Computing 9*, 6 (JUN 2009), 785–803.

[54] Lin, Y., and Wong, V. W. S. An admission control algorithm for multi-hop 802.11e-based WLANs. *Computer Communications 31*, 14 (SEP 5 2008), 3510–3520. International Conference on Quality of Service in Heterogeneous Wired/Wireless Networks, Waterloo, CANADA, AUG, 2006.

[55] Lodi, A., Malaguti, E., and Stier-Moses, N. E. Efficient and fair routing for mesh networks. *Mathematical Programming 124*, 1-2 (JUL 2010), 285–316.

[56] Madhu, Dahiya, A., and Dahiya, B. Energy efficient data tranfer in secure wireless sensor networks. *Advanced Computing & Communication Technologies, International Conference on 0* (2012), 495–499.

[57] Mamun-Or-Rashid, M., Alam, M. M., Hamid, M. A., and Hong, C. S. Flow rank based probabilistic fair scheduling for wireless ad hoc networks. *Wireless Networks 16*, 3 (APR 2010), 713–729.

[58] Marina, M. K., and Das, S. R. Ad hoc on-demand multipath distance vector routing. *SIGMOBILE Mob. Comput. Commun. Rev. 6*, 3 (June 2002), 92–93.

[59] Mazinani, S. M., Naderi, A., Setoodefar, M., and Shirazi, A. Z. An energy-efficient real-time routing protocol for differentiated data in wireless sensor networks. *Engineering of Complex Computer Systems, IEEE International Conference on 0* (2012), 302–307.

[60] McInerney, T., and Terzopoulos, D. Deformable models in medical image analysis : a survey. *Medical Image Analysis 1*, 2 (June 1996), 91–108.

[61] Meerja, K. A., and Shami, A. Analysis of new distributed-media access-control schemes for IEEE 802.11 wireless local-area networks. *IEEE Transactions on Vehicular Technology 56*, 4, Part 1 (JUL 2007), 1797–1812. IEEE Globecom 2006, San Francisco, CA, DEC 01, 2006.

[62] Mohsenian-Rad, A. H., Huang, J., Chiang, M., and Wong, V. W. S. Utility-Optimal Random Access : Reduced Complexity, Fast Convergence, and Robust Performance. *IEEE Transactions on Wireless Communications 8*, 2 (FEB 2009), 898–911. IEEE Military Communication Conference (MILCOM 2008), San Diego, CA .

[63] Moseng, T. K., and Kure, O. Evaluation of Path Dependent Scheduling in Ad Hoc Networks : a Suitable Fairness Mechanism ? In *WONS : 6th International Conference on Wireless On-Demand Network Systems and Services* (2009), IEEE, pp. 191–197. Snowbird, UT, FEB 02-04, 2009.

[64] Nadeem, T., and Parthasarathy, S. Mobility control for throughput maximization in ad hoc networks. *Wireless Communications & Mobile Computing 6*, 7 (NOV 2006), 951–967.

[65] Nilsson, J., and Sterner, U. Admission Control in Wireless Multihop Networks. In *MILCOM 2008 : IEEE Military Communications Conference* (2008), vol. 1-7, IEEE, IEEE, pp. 3779–3786. San Diego, CA, NOV 16-19.

[66] nosuke Toyoda, S., and Sato, F. Energy-effective clustering algorithm based on adjacent nodes and residual electric power in wireless sensor networks. *Advanced Information Networking and Applications Workshops, International Conference on 0* (2012), 601–606.

[67] Ofuji, Y., Abeta, S., and Sawahashi, M. Fast packet scheduling algorithm based on instantaneous SIR with constraint condition assuring minimum throughput in forward link. In *WCNC 2003 : IEEE Wireless Communications and Networking Conference Record* (2003), vol. 1-3, IEEE, pp. 860–865. New Orleans,LA, MAR 16-20, 2003.

[68] Oh, J.-H., and Lim, J.-T. Throughput Improvement in Wireless Multi-Hop Ad-Hoc Networks Using Load Control. *IEICE Transactions on Communications E92B*, 1 (JAN 2009), 314–317.

[69] Pathak, A., Zaheeruddin, Lobiyal, D., and Tiwari, M. K. Improvement of lifetime of wireless sensor network by jointly effort of exponential node distribution and mixed routing. *Communication Systems and Network Technologies, International Conference on 0* (2012), 316–319.

[70] Peng, J., Sikdar, B., and Cheng, L. Multicasting with Localized Control in Wireless Ad Hoc Networks. *IEEE Transactions on Mobile Computing 8*, 1 (JAN 2009), 52–64.

[71] Perkins, C., and Royer, E. Ad-hoc on-demand distance vector routing. In *Proceedings WMCSA'99. Second IEEE Workshop on Mobile Computing Systems and Applications* (1999), IEEE, pp. 90–100.

[72] Pirzada, A. A., Portmann, M., and Indulska, J. Performance analysis of multi-radio AODV in hybrid wireless mesh networks. *Computer Communications 31*, 5 (MAR 25 2008), 885–895. 4th ACM International Workshop on Mobility Management and Wireless Access (MobiWac 2006), Torremolinos, SPAIN, OCT 02, 2006.

[73] Prokkola, J., and Braeysy, T. A detailed study of a CDMA based approach to enhance ad hoc network performance. *Ad Hoc Networks 5*, 7 (SEP 2007), 1149–1172.

[74] R. Jain and D. Chiu and W. Hawe. A Quantitative Measure Of Fairness And Discrimination For Resource Allocation In Shared Computer Systems. Tech. Rep. TR-301, DEC Research, September 1984.

[75] Razafindralambo, T., and Lassous, I. G. SBA : A Simple Backoff Algorithm for Wireless Ad Hoc Networks. In *Networking 2009* (2009), vol. 5550 of *Lecture Notes in Computer Science*, SPRINGER-VERLAG BERLIN, pp. 416–428. 8th International IFIP TC 6 Network Conference 2009, Aachen, GERMANY, MAY 11-15, 2009.

[76] Romaszko, S., and Blondia, C. Cross Layer PHY-MAC Protocol for Wireless Static and Mobile Ad Hoc Networks. *EURASIP Journal on Advances in Signal Processing* (2009).

[77] Rossi, M., Bui, N., and Zorzi, M. Cost- and Collision-Minimizing Forwarding Schemes for Wireless Sensor Networks : Design, Analysis, and Experimental Validation. *IEEE Transactions on Mobile Computing 8*, 3 (MAR 2009), 322–337. IEEE INFOCOM 2007 Conference, Anchorage, AK, MAY, 2007.

[78] Ruan, S., Wang, C., and Lee, T. T. Improving the MAC Layer Performance of Ad Hoc Networks by Congestion Control Algorithms. In *ISWCS : 5th International Symposium on Wireless Communication Systems* (2008), IEEE, pp. 21–25. Reykjavik, ICELAND, OCT 21-24.

[79] Sarangi, S., and Kar, S. Genetic algorithm based mobility aware clustering for energy efficient routing in wireless sensor networks. *Networks, IEEE International Conference on 0* (2011), 1–6.

[80] Sharma, M., and Sharma, K. An energy efficient extended leach (eee leach). *Communication Systems and Network Technologies, International Conference on 0* (2012), 377–382.

[81] Shifrin, M., and Cidon, I. C3 : Collective Congestion Control in Multi-Hop Wireless Networks. In *WONS :7th International Conference on Wireless On-Demand Network Systems and Services* (2010), IEEE, pp. 31–38. Kranjska Gora, SLOVENIA, FEB 03-05.

[82] Shisong, X., Xiangling, Z., Feng, Z., and Hui, F. Energy-based cluster partition method in wireless sensor networks. *Computational and Information Sciences, International Conference on 0* (2012), 912–915.

[83] Su, H., and Zhang, X. Modeling Throughput Gain of Network Coding in Multi-Channel Multi-Radio Wireless Ad Hoc Networks. *IEEE Journal on Selected Areas in Communications 27*, 5 (JUN 2009), 593–605.

[84] Tao Ma, Xinming Zhang, G. C. A Maximal Clique Base Packet Scheduling Algorithm in Mobile Ad Hoc Network. *IEEE Ineternational Conference on Networking* (2004), 690–696.

[85] Tian, H., Bose, S. K., Law, C. L., and Xiao, W. Joint routing and flow rate optimization in multi-rate ad hoc networks. *Computer Networks 52*, 3 (FEB 22 2008), 739–764.

[86] Touati, H., Lengliz, I., and Kamoun, F. Adapting TCP Exponential Backoff to Multihop Ad Hoc Networks. In *Symposium on Computers and Communications ISCC* (2009), vol. 1 and 2, IEEE, pp. 611–616. Sousse,TUNISIA, JUL 05-08.

[87] Wakuda, K., Kasahara, S., Takahashi, Y., Kure, Y., and Itakura, E. A packet scheduling algorithm for max-min fairness in multihop wireless LANs. *Computer Communications 32*, 13-14 (AUG 17 2009), 1437–1444.

[88] Wang, B., and Zhao, D. Scheduling for Long Term Proportional Fairness in a Cognitive Wireless Network with Spectrum Underlay. *IEEE Transactions on Wireless Communications 9*, 3 (MAR 2010), 1150–1158.

[89] Wang, L., and Li, L. A combined algorithm routing protocol based on energy for wireless sensor network. *Computer Science and Electronics Engineering, International Conference on 1* (2012), 224–228.

[90] Wang, X., Wang, J., Lu, K., and Xu, Y. Gkar : A novel geographic k-anycast routing for wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems 99*, PrePrints (2012).

[91] Wang, X., Wen, X., Liang, C., Liu, Y., and Lin, X. Fair Security Protocols with off-line TTP. In *International Symposium on Intelligent Ubiquitous Computing and Education* (2009), Luo, Q, Ed., IEEE, pp. 109–112. Chengdu, CHINA, MAY 16-17.

[92] Wang, X., Wen, X., Liu, Y., Lin, X., and Wang, Y. A Fair Non-Repudiation Security Protocol with off-line TTP. In *IEEE International Conference on Service Operations and Logistics and Informatics* (2009), IEEE, pp. 173–178. Chicago, IL, JUL 22-24, 2009.

[93] Wang, Y., and Garcia-Luna-Aceves, J. Throughput and fairness in a hybrid channel access scheme for ad hoc networks. In *WCNC 2003 : IEEE Wireless Communications and Networking Conference Record* (2003), vol. 1-3, IEEE, pp. 988–993. New Orleans,LA, MAR 16-20, 2003.

[94] Warrier, A., Rhee, I., and Kim, J. H. Experimental Evaluation of MAC Protocols for Fairness and QoS Support in Wireless Networks. In *ICNP'08 : 16th IEEE International Conference on Network Protocols* (2008), IEEE International Conference on Network Protocols Proceedings, IEEE, pp. 298–307. Orlando, FL, OCT 19-22.

[95] Wen, J., and Arcak, M. A unifying passivity framework for network flow control. In *IEEE INFOCOM 2003 : The Conference on Computer Communications* (2003), vol. 1-3, IEEE, pp. 1156–1166. San Francisco, CA, MAR 30-APR 03, 2003.

[96] Wen, S., Fang, Y., and Sun, H. Differentiated Bandwidth Allocation with TCP Protection in Core Routers. *IEEE Transactions on Parallel and Distributed Systems 20*, 1 (JAN 2009), 34–47.

[97] Wu, K.-D., and Liao, W. Flow allocation in multi-hop wireless networks : A cross-layer approach. *IEEE Transactions on Wireless Communications 7*, 1 (JAN 2008), 269–276.

[98] Ye, M. H., Lau, C. T., and Premkumar, A. B. Traffic scheduling mechanism based on graph theory for Power Saving mode of IEEE 802.11 distributed coordinator function. *International Journal of Ad Hoc and Ubiquitous Computing 4*, 2 (2009), 84–94.

[99] Yi, X.-S., Jiang, P.-J., Wang, X.-W., and Zhang, S.-C. Survey of energy-saving protocols in wireless sensor networks. *International Conference on Robot, Vision and Signal Processing 0* (2011), 208–211.

[100] Zhai, H., Chen, X., and Fang, Y. Improving transport layer performance in multihop ad hoc networks by exploiting MAC layer information. *IEEE Transactions on Wireless Communications 6*, 5 (MAY 2007), 1692–1701.

[101] Zhang, J., Dziong, Z., Gagnon, F., and Kadoch, M. Multiuser Detection Based MAC Design for Ad Hoc Networks. *IEEE Transactions on Wireless Communications 8*, 4 (APR 2009), 1836–1846.

[102] Zhang, Q., and Qu, W. An energy efficient clustering approach in wireless sensor networks. *Computer Science and Electronics Engineering, International Conference on 1* (2012), 541–544.

[103] Zheng, D., Ge, W., and Zhang, J. Distributed Opportunistic Scheduling for Ad Hoc Networks With Random Access : An Optimal Stopping Approach. *IEEE Transactions on Information Theory 55*, 1 (JAN 2009), 205–222.

[104] Zhu, X. Z., and Li, Y. F. Simulation of coverage problem research in wireless sensor networks based on energy saving. *Computer Science and Electronics Engineering, International Conference on 1* (2012), 270–273.

Accès, routage et sécurisation pour les réseaux sans fil : une nouvelle approche

Marc GILG

Table des matières

Abstract

This manuscript gathers several works presented to obtain the autorization to direct research. There are studied the wireless networks communications in an Ad-Hoc manner. The nodes that make up these networks exchange information through radio communications. This entails constraints related to the limitation of the wireless transmission.

The first work presented is the study of congestion and fairness of Ad-Hoc networks. A theoretical method, based on star and double star networks, allows to evaluate the equity of networks based on a fairness index. After this study, new access protocols are given.

The second part focuses on wireless sensor networks that are Ad-Hoc networks with additional constraints, including energy consumptions. A new approach using grayscale images analogies is given. Each sensor is represented by a pixel of the image, and its energy is encoded in the brightness of the pixel. This analogy allowed us to propose routing protocols, using image processing algorithms. A notion of deformation of paths is also proposed.

The last part proposes improvements to the AOMDV and OLSR routing protocols. The AOMDV routing protocol is modified to account for the variation of energy along a path, in order to increase the lifetime of the network. The OLSR protocol has been modified to resist black hole attacks.

keywords :
Wireless network,Ad-Hoc, WSN, Routing, Acess, QOS, Congestion, Images Processing, AOMDV, OLSR, Deformations

Résumé

Ce mémoire regroupe plusieurs travaux présentés pour obtenir l'Habilitation à Diriger les Recherches. Y sont étudié particulièrement les réseaux sans fils communiquant de manière Ad-Hoc. Les noeuds qui composent ces réseaux échangent des informations par des communications radios. Cela entraine des contraintes liées à la limitation de la transmission sans fils.

Le premier travail présenté est l'étude de la congestion et de l'équité des réseaux Ad-Hoc. Une méthode théorique basée sur des réseaux de type étoiles permet d'évaluer l'équité des réseaux en utilisant un index d'équité. Après cette étude théorique, des nouveaux protocoles d'accés sont données.

La deuxième partie se focalise sur les réseaux de capteurs sans fils qui sont des réseaux Ad-Hoc avec des contraintes supplémentaires, notamment énergétique. Une nouvelle approche utilisant une modélisation par des images en niveaux de gris est donnée. Chaque capteur est représenté par un pixel de l'image, et son énergie est codée par l'intensité lumineuse du pixel. Cette analogie nous a permis de proposer des protocoles de routages utilisant des algorithmes de traitements d'images. Une notion de déformation de routes est aussi proposée.

La dernière partie propose des améliorations des protocoles de routage AOMDV et OLSR. Le protocole de routage AOMDV est modifié pour tenir compte de la variation d'énergie le long d'un chemin dans le but d'augmenté la durée de vie du réseau. Le protocole OLSR est quant à lui modifié pour résister à des attaques de type trou-noir.

Mots clés :
Réseaux sans fils, Ad-Hoc, Capteurs, Accès, Routage, Congestion, Traitement d'images, AOMDV, OLSR, Déformations