

Université de Montréal

Métriques de routage dans les réseaux maillés sans fil

par

Yaye Sarr

Département d'informatique et de recherche opérationnelle

Faculté des arts et des sciences

Mémoire présenté à la Faculté des arts et des sciences
en vue de l'obtention du grade de Maîtrise en sciences (M.Sc.)
en Informatique

Avril, 2011

© Yaye Sarr, 2011

Université de Montréal
Faculté des arts et des sciences

Ce mémoire intitulé :

Métriques de routage dans les réseaux maillés sans fil

Présenté par :
Yaye Sarr

a été évalué par un jury composé des personnes suivantes :

Marc Feeley, président-rapporteur
Abdelhakim Hafid, directeur de recherche
Gena Hahn, membre du jury

Résumé

Ces dernières années, les technologies sans fil ont connu un essor fulgurant. Elles ont permis la mise en place de réseaux sans fil à hautes performances. Les réseaux maillés sans fil (RMSF) sont une nouvelle génération de réseaux sans fil qui offrent des débits élevés par rapport aux réseaux Wi-Fi (Wireless Fidelity) classiques et aux réseaux ad-hoc. Ils présentent de nombreux avantages telles que leur forte tolérance aux pannes, leur robustesse, leur faible coût etc. Les routeurs des RMSF peuvent disposer de plusieurs interfaces radio et chaque interface peut opérer sur plusieurs canaux distincts, c'est des RMSF multiples-radios, multiples-canaux. Ce type de réseau peut accroître de manière considérable les performances des RMSF. Cependant plusieurs problèmes subsistent et doivent être résolus notamment celui du routage.

Le routage dans les RMSF demeure un défi majeur. Le but des protocoles de routage est de trouver les meilleures routes i.e. des routes qui maximisent les débits et minimisent les délais, lors de l'acheminement du trafic. La qualité des routes dans les RMSF peut être fortement affectée par les interférences, les collisions, les congestions etc. Alors les protocoles doivent être en mesure de détecter ces problèmes pour pouvoir en tenir compte lors de la sélection des routes. Plusieurs études ont été dédiées aux métriques et aux protocoles de routage dans les RMSF afin de maximiser les performances de celles ci. Mais la plupart ne prennent pas en considération toutes les contraintes telles que les interférences, le problème des stations cachées etc. Ce mémoire propose une nouvelle métrique de routage pour RMSF.

Nous avons mis en place une nouvelle métrique de routage pour RMSF appelée MBP (Metric Based on Probabilities). Cette métrique est destinée aux RMSF mono-radio ou multiples-radios. Elle permet d'éviter les routes à forte

interférence. Les résultats des simulations ont montré que MBP présente des améliorations par rapport à certaines métriques : ETT, WCETT et iAWARE qui sont connues dans le domaine.

Mots-clés : réseaux maillés sans fil, métriques de routage, performances, mesures.

Abstract

In recent years, wireless technologies have developed sharply. They allow the establishment of high performance wireless networks. Wireless Mesh Networks (WMNs) is a new generation of wireless networks that offer high throughput compared to classical Wi-Fi (Wireless Fidelity) or ad-hoc networks. WMNs have attracted significant research due to their features that include dynamic self organization, self configuration, easy maintenance and low cost. WMNs nodes can be equipped with multiples-radios and multiples-channels. This type of network can increase significantly the performance of WMNs. However, several problems must be solved including routing in WMNs.

Routing in WMNs is a great challenge. The main goal of routing protocols is to find best paths i.e. paths that maximize throughputs and minimize delays when transmitting packets. Route quality can be strongly affected by interference, collisions, congestions etc. Then protocols should be able to detect these problems and take them into account during route selection.

We propose a new routing metric for WMNs, called MBP that captures the impact of intra-flow and inter-flow interference in multi-radio, multi-channel networks. Results show that MBP has better performances than some existing and popular metrics like ETT, WCETT and iAWARE.

Keywords: wireless mesh networks, routing metrics, performances, measures.

Table des matières

CHAPITRE 1: INTRODUCTION	1
1.1 PRESENTATION DES RESEAUX MAILLES SANS FIL	1
1.2 AVANTAGES DE RMSF	3
1.3 COMPOSANTS D'UN RMSF	4
1.4 DOMAINES D'APPLICATION DES RMSF	5
1.5 MOTIVATION	6
1.6 DESCRIPTION DU PROBLEME DES METRIQUES DE ROUTAGE	7
1.7 CONTRIBUTIONS.....	8
1.8 ORGANISATION DU MEMOIRE	8
CHAPITRE 2: GENERALITES SUR LES RESEAUX MAILLES SANS FIL.....	10
2.1 TECHNOLOGIES SANS FIL	10
2.1.1 Différentes technologies sans fil	11
2.1.2 Problèmes liés à l'utilisation des technologies sans fil	12
2.2 ARCHITECTURE DES RMSF.....	14
2.3 RMSF MULTIPLES-RADIOS MULTIPLES-CANAUX ET AFFECTATION DES CANAUX.....	17
CHAPITRE 3: REVUE DE LITTERATURE DES METRIQUES ET	
PROTOCOLES DE ROUTAGE	19
3.1 METRIQUES DE ROUTAGE.....	19
3.1.1 Techniques de mesures.....	21
3.1.2 Composants d'une métrique.....	21
3.1.3 Caractéristiques d'une métrique pour RMSF	22
3.1.4 Métriques de routage existantes	24
3.2 PROTOCOLES DE ROUTAGE	36
3.2.1 Protocoles de routage proactifs	36
3.2.2 Protocoles de routage réactifs	37
3.2.3 Protocoles de routage hybrides	38
3.2.4 Quelques exemples de protocoles de routage.....	38

3.3	SYNTHESE DE L'ETAT DE L'ART	45
CHAPITRE 4: MBP UNE NOUVELLE METRIQUE DE ROUTAGE POUR RMSF		
47		
4.1	DESCRIPTION DE MBP	47
4.1.1	Interférence inter-flux	48
4.1.2	MBP pour un lien	49
4.1.3	Interférence intra-flux et MBP pour un chemin	49
4.1.4	MBP-AODV le protocole de routage associé	50
4.1.5	Surveillance de la qualité des liens	50
CHAPITRE 5: ÉVALUATION DES PERFORMANCES DE MBP.....		53
5.1	ENVIRONNEMENT DE TRAVAIL : LE SIMULATEUR NS2	53
5.2	CONDITIONS DE SIMULATION	54
5.3	METRIQUES DE PERFORMANCE	55
5.3.1	Le débit du réseau	55
5.3.2	Le délai moyen point-à-point	56
5.3.3	Le taux de perte	56
5.3.4	Le surdébit de routage (Routing Overhead)	56
5.3.5	Le Taux d'Efficacité Normalisé (Normalized Effectiveness Ratio)	56
5.4	RESULTATS DE SIMULATION	57
5.4.1	Premier scénario : topologie en grille	57
5.4.2	Deuxième scénario : topologie aléatoire	68
5.4.3	Variations des flux	79
5.4.4	Effet de l'interférence sur MBP	84
CHAPITRE 6: CONCLUSION ET PERSPECTIVES FUTURES		86
6.1	CONCLUSION	86
6.2	PERSPECTIVES FUTURES	87

Liste des tableaux

TABLE 1 : CARACTERISTIQUES DES METRIQUES.....	46
TABLE 2 : PARAMETRES DE SIMULATION	55

Liste des Figures

Chapitre 1

Fig.1.1:	Mode Infrastructure.....	2
Fig.1.2:	Mode Ad-hoc	2
Fig.1.3:	Architecture d'un réseau maillé sans fil.....	3
Fig.1.4:	Routeur maillé et interface radio.....	5

Chapitre 2

Fig.2.1:	Rayon de transmission et rayon d'interférence.....	12
Fig.2.2:	Interférences entre les nœuds.....	14
Fig.2.3:	Architecture " par épine dorsale " d'un réseau maillé.....	15
Fig.2.4:	Architecture client d'un réseau maillé	16
Fig.2.5:	Architecture hybride d'un réseau maillé.....	16
Fig.2.6:	Découpage en canaux de la bande de fréquence 2,4 GHz	18

Chapitre 3

Fig.3.1:	Stations cachées	20
Fig.3.2:	Exemple d'isotonicité.....	24
Fig.3.3:	Calcul de ETX sur le chemin ABCD	26
Fig.3.4:	Exemple d'isotonicité.....	26
Fig.3.5:	Probabilité de réussite sur le chemin AC	29
Fig.3.6:	Exemple de calcul de métrique avec WCETT	30
Fig.3.7:	WCETT interférence intra-flux sur lien distant	30
Fig.3.8:	Exemple d'inconvénient de WCETT et iAWARE	33
Fig.3.9:	Décomposition isotonique de MIC	35
Fig.3.10:	Exemple de table de routage avec le protocole de routage DSDV ...	40
Fig.3.11:	Illustration d'un cas de panne avec DSDV	42
Fig.3.12:	Recherche de route dans AODV	44

Chapitre 4

Fig.4.1:	Exemple surveillance de la qualité des liens.....	52
----------	---	----

Chapitre 5

Fig.5.1:	Topologie en grille.....	58
Fig.5.2:	Débits du réseau pour une topologie en grille avec un canal.....	59
Fig.5.3:	Délais moyens pour une topologie en grille avec un canal.....	59
Fig.5.4:	Taux de perte pour une topologie en grille avec un canal.....	60
Fig.5.5:	Taux d'efficacité normalisé pour une topologie en grille avec un canal	61
Fig.5.6:	Surdébits de routage pour une topologie en grille avec un canal.....	62
Fig.5.7:	Débits du réseau pour une topologie en grille avec multiples-canaux	63
Fig.5.8:	Délais pour une topologie en grille avec multiples-canaux.....	63
Fig.5.9:	Taux de perte pour une topologie en grille avec multiples-canaux ..	64
Fig.5.10:	Taux d'efficacité normalisé pour une topologie en grille à multiples-canaux	65
Fig.5.11:	Surdébits de routage pour une topologie en grille à multiples-canaux	66
Fig.5.12:	Comparaison des débits pour une topologie grille à un seul canal et une topologie grille à multiples-canaux.....	67
Fig.5.13:	Comparaison des délais pour une topologie grille à un seul canal et une topologie grille à multiples-canaux.....	67
Fig.5.14:	Topologie aléatoire.....	69
Fig.5.15:	Débits du réseau pour une topologie aléatoire avec un canal.....	70
Fig.5.16:	Délais pour une topologie aléatoire avec un canal.....	70
Fig.5.17:	Taux de perte pour une topologie aléatoire avec un canal.....	71
Fig.5.18:	Taux d'efficacité normalisé pour une topologie aléatoire avec un canal	72

Fig.5.19:	Surdébits de routage pour une topologie aléatoire avec un canal	72
Fig.5.20:	Débits du réseau pour une topologie aléatoire avec multiples-canaux	74
Fig.5.21:	Délais pour une topologie aléatoire avec multiples-canaux.....	74
Fig.5.22:	Taux de perte pour une topologie aléatoire avec avec multiples-canaux	75
Fig.5.23:	Taux d'efficacité normalisé pour une topologie aléatoire avec trois canaux	76
Fig.5.24:	Surdébits de routage pour une topologie aléatoire avec trois canaux	76
Fig.5.25:	Comparaison des débits pour une topologie aléatoire avec un et trois canaux	77
Fig.5.26:	Comparaison des délais pour une topologie aléatoire avec un et trois canaux	78
Fig.5.27:	Débits de réseau pour différents nombre de flux	79
Fig.5.28:	Délais pour différents nombre de flux	80
Fig.5.29:	Taux de perte pour différents nombre de flux.....	81
Fig.5.30:	Taux d'efficacité normalisé pour différents nombre de flux	82
Fig.5.31:	Surdébits de routage pour différents nombre de flux.....	83
Fig.5.32:	Débits pour une topologie aléatoire avec des liens interférents.....	84
Fig.5.33:	Délais moyens pour une topologie aléatoire avec des liens interférents	85

Liste des sigles et des abréviations

Acronyme	Description
AODV	Ad-hoc On-demand Distance Vector
CSMA/CA	Carrier Sense Multiples Access with Collision Avoidance
CBR	Constant Bit Rate
DSVD	Destination-Sequenced Distance Vector
ETX	Expected Transmission Count
ETT	Expected Transmission Time
IWARE	Interference Aware
IR	Interference Ratio
MAC	Media Access Control
MBP	Metric Based on Probabilities
MIC	Metric of Interference and Channel-switching
ML	Minimum Loss
MANET	Mobile Ad-hoc Networks
NS2	Network Simulator 2
QoS	Qualité de Service
RMSF	Réseaux Maillés Sans Fil
SINR	Signal Interference to Noise Ratio
SNR	Signal to Noise Ratio
TCL	Tool Command Language
UDP	User Datagram Protocol
WCETT	Weighted Cumulative Expected Transmission Time
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WPAN	Wireless Personal Area Network
WIMAX	Worldwide Interoperability for Microwave Access

Liste des Descriptions

Bande passante	La quantité de données maximale qui peut transiter dans le réseau.
Débit	La quantité de données reçues par unité de temps. Le débit est inférieur ou égal à la bande passante.
Délai	Temps de transmission d'un paquet de la source à la destination.
Canal de communication	Médium qui permet d'envoyer et de recevoir des données en utilisant les ondes.
Interférence	Collision qui se produit quand plusieurs stations émettent sur le même canal.
Rayon de transmission (r)	Zone dans laquelle tout nœud récepteur est capable de recevoir correctement les données envoyées par la source
Rayon d'interférence (R)	Zone dans laquelle le nœud détecte une activité du médium mais ne peut pas décoder correctement les signaux reçus.
Nœud	Un routeur ou un client maillé doté d'une ou plusieurs interfaces radios qui communiquent sur un ou plusieurs canaux.
Route	Ensemble de nœuds par lequel le trafic, depuis une source vers une destination, transite.

À mes parents
À toute ma famille

Remerciements

Tout d'abord, je remercie mon professeur Abdel Hakim Hafid qui, tout au long de ces deux années, m'a épaulée, écouté et contribué à la réussite de ce travail.

Ensuite, j'adresse mes sincères remerciements à mes parents et à tous les membres de ma famille qui ont toujours cru en moi, m'ont soutenu et m'ont encouragée à aller plus loin dans mes études.

Mes remerciements s'adressent également à Mustapha Boushaba pour ses précieux conseils et sa présence tout au long de ces deux laborieuses années.

Enfin, je remercie ainsi que tous ceux qui, de près ou de loin, ont participé à l'aboutissement de ce mémoire notamment tous les membres du Laboratoire de Réseau et de Communication de l'Université de Montréal.

Chapitre 1: Introduction

1.1 Présentation des réseaux maillés sans fil

Les technologies sans fil connaissent ces dernières années un essor prodigieux, ce qui a favorisé une utilisation massive d'appareils mobiles tels que les téléphones intelligents, les ordinateurs portables etc. Ces technologies ont permis la mise en place de réseaux de télécommunications sans fil à large bande avec une large couverture comme les réseaux maillés sans fil (RMSF). En phase de recherche depuis quelques années, les RMSF sont une nouvelle classe de réseau sans fil. Comme leurs noms l'indiquent, ce sont des réseaux basés sur une ou plusieurs technologies sans fil telles qu'IEEE 802.11 (WLAN) [31] et IEEE 802.16 (WIMAX) [13]. Ces réseaux ont une architecture maillée où tous les routeurs sont connectés de proche en proche sans hiérarchie centrale et où chaque nœud peut jouer le rôle d'émetteur, de récepteur ou de relai. Ainsi, chaque communication entre une source et une destination se fait à travers plusieurs sauts.

Les RMSF conviennent à tout type d'environnement. Ils peuvent aussi bien être déployés sur de petits espaces comme des maisons ou sur de plus grandes surfaces telles que des campus, des entreprises, ou même des villes entières. C'est le cas de certaines villes aux États-Unis comme Medford [11] et Chaska. Les RMSF offrent des liaisons à hauts débits. De plus, ces environnements mobiles offrent une grande flexibilité d'emploi, en particulier ils permettent la mise en réseau de sites pour lesquels le câblage serait trop onéreux ou complexe à déployer, voire même impossible.

Les réseaux sans fil ont deux modes de fonctionnement:

- Le mode *Infrastructure* (Fig.1.1 extraite de [28]): avec ce mode, la communication est gérée par des points d'accès fixe. Lorsqu'un nœud désire

envoyer des données, il les envoie au point d'accès qui, à son tour l'envoie au destinataire. Les communications entre routeurs ne se font pas directement et passent toujours par le point d'accès.

- Le mode *Ad-Hoc* (Fig.1.2 extraite de [28]): littéralement le terme "ad hoc" signifie "d'égal à égal". En effet, dans ce type de réseau tous les nœuds jouent le même rôle et sont tous mobiles. Il n'y a pas de point d'accès pour gérer le réseau, chaque nœud peut retransmettre les informations qu'il reçoit aux autres membres. La communication se fait sur plusieurs sauts.

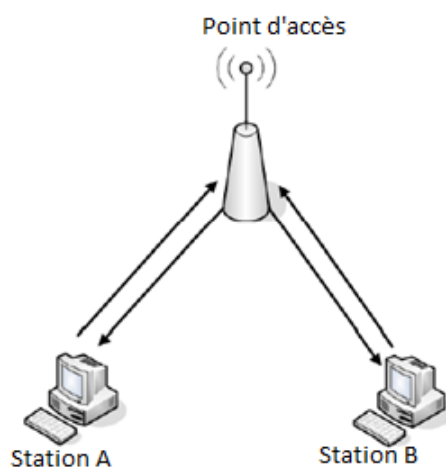


Fig.1.1: Mode Infrastructure

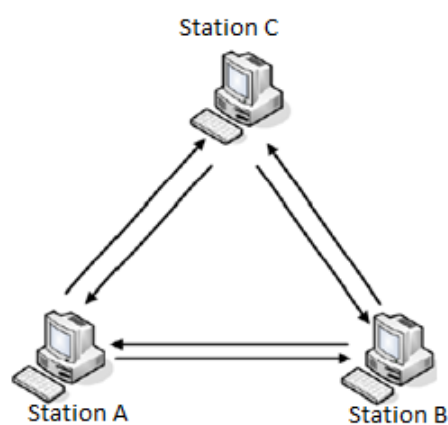


Fig.1.2: Mode Ad-hoc

Les RMSF peuvent être vus comme des réseaux ad hoc avec infrastructure. En effet l'architecture des RMSF est composée de routeurs maillés fixes qui forment l'épine dorsale (backbone) et de clients maillés mobiles (voir Fig.1.3 extraite de [34]). Lorsqu'un client veut communiquer avec un autre, il peut le faire directement ou passer par des routeurs maillés cela permet d'avoir plusieurs possibilités de routes. De ce fait la connectivité est maintenue en cas de panne routeur, ce qui rend cette architecture flexible.

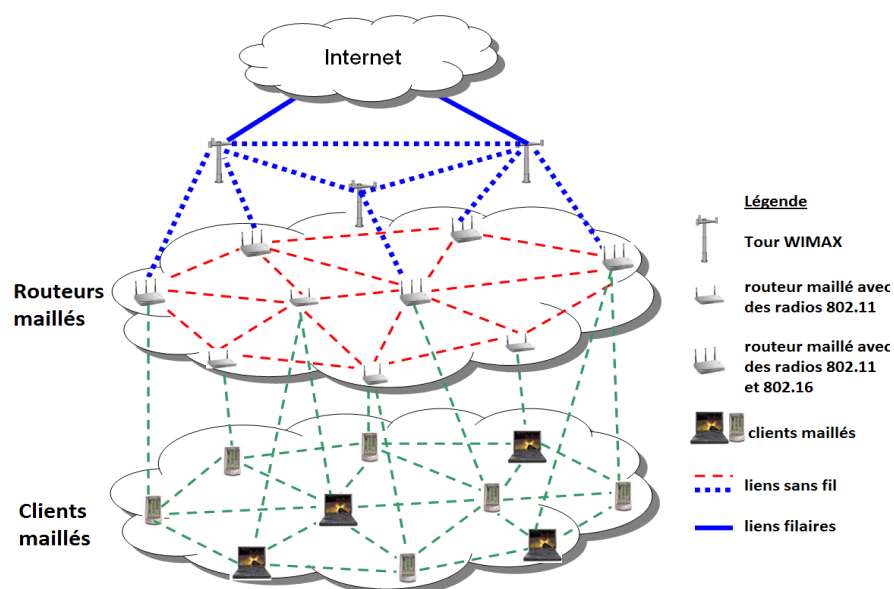


Fig.1.3: Architecture d'un réseau maillé sans fil

1.2 Avantages de RMSF

Les RMSF suscitent un grand intérêt dans la communauté des chercheurs en télécommunication grâce à ses nombreux avantages.

- *Le faible coût et l'élimination de câblage*: Le coût des équipements des RMSF est abordable comparé à d'autres solutions pour réseaux sans fil. De plus l'élimination totale de câblage facilite l'installation des RMSF et permet d'interconnecter des zones où le câblage serait difficile à réaliser.
- *L'auto-configuration et l'auto-organisation*: la connectivité est maintenue dynamiquement en cas de changement de topologie sans intervention humaine (retrait ou ajout d'un ou plusieurs routeurs) ce qui facilite l'installation et la maintenance.
- *Le maillage* permet d'avoir un large choix au niveau des routes, ce qui leur procure leur robustesse et leur forte tolérance aux pannes.
- *L'interopérabilité et l'extensibilité avec les réseaux existants* : un RMSF est une interconnexion de plusieurs réseaux sans fil utilisant différentes

technologies. Par exemple, dans un même RMSF, on peut retrouver des réseaux Wi-Fi, des réseaux cellulaires, des réseaux WiMax ou des réseaux de capteurs etc. L'interopérabilité et l'auto-configuration permet d'étendre facilement un RMSF avec d'autres réseaux existants.

Bien que les RMSF présentent de nombreux avantages, plusieurs problèmes restent à résoudre tels que la sécurité, la qualité de service (QoS), le routage etc. Ainsi plusieurs recherches sont actuellement consacrées aux RMSF pour apporter au mieux des solutions à ces problèmes.

1.3 Composants d'un RMSF

Les RMSF sont essentiellement composés de routeurs maillés, de clients maillés et de passerelles.

Les routeurs maillés peuvent être dotés de plusieurs interfaces radio, et chaque interface peut opérer sur plusieurs canaux de communication. Le fait d'utiliser plusieurs canaux peut augmenter de manière considérable les capacités des RMSF avec un coût abordable ce qui constitue un critère majeur de qualité de service (QoS). Néanmoins, le nombre d'interfaces radio par routeur n'est pas illimité et le nombre de canaux orthogonaux disponibles dépend de la technologie sans fil utilisée sur l'interface radio. Par exemple, le nombre de canaux orthogonaux est de trois pour IEEE 802.11b, 12 ou 13 canaux selon les pays pour l'IEEE 802.11a. Les canaux sont affectés aux interfaces radio des routeurs, c'est l'assignation de canaux. Une assignation optimale de canaux peut améliorer les performances de routage des RMSF. Elle constitue à elle seule un défi majeur mais ce point ne sera pas traité dans ce mémoire. Sur la Fig.1.4 nous avons un exemple de routeur maillé avec deux emplacements pour interface.

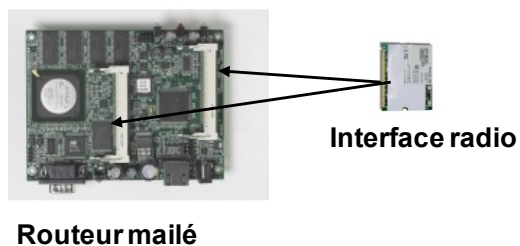


Fig.1.4: Routeur maillé et interface radio

Les clients sont les utilisateurs du réseau, ce sont des équipements sans fil tels que des ordinateurs, des téléphones etc. Il faut noter qu'un client peut jouer le rôle de routeur.

Les passerelles sont des routeurs, qui intègrent des fonctionnalités supplémentaires afin d'interconnecter différents réseaux sans fil ou les relier à l'Internet.

1.4 Domaines d'application des RMSF

À la base, les RMSF étaient destinés à des applications dans le domaine militaire mais très vite, ils ont été adoptés pour des applications domestiques quotidiennes. Les nombreux avantages qu'ils présentent ont favorisé leur expansion et sont désormais largement utilisés dans les villes, les universités, les entreprises ou même les maisons etc. L'interopérabilité des RMSF permet l'utilisation d'une large gamme d'appareils sans fil accessibles au grand public. De plus, l'absence de câblage offre une importante mobilité aux utilisateurs.

Les RMSF offrent de très hauts débits, qui supportent des applications telles que la VoIP (voix sur IP), la ToIP (téléphonie sur IP), la vidéo en streaming entre autres, des types d'applications qui, jadis, ne seraient supportés que par des réseaux filaires. Les nombreux atouts des RMSF ont séduit un large public pour une utilisation à petite ou grande échelle.

1.5 Motivation

Un réseau maillé est un réseau multi-sauts basé sur une infrastructure contrairement à un réseau ad hoc (MANET) qui lui ne nécessite aucune infrastructure préexistante. Il offre naturellement un accès sans fil, avec un coût attractif, des débits élevés et une latence contrôlée. Un réseau maillé est interconnecté à l'Internet par un ensemble de passerelles et le trafic des clients est véhiculé en utilisant un système de communication multi-sauts. Au sein d'un réseau maillé, il peut subsister différentes technologies sans fil. Plusieurs technologies sans fil supportent la communication des réseaux maillés, par exemple IEEE 802.11 (Wi-Fi) pour les réseaux locaux sans fil (WLAN), IEEE 802.15.4 destiné aux réseaux personnels sans fil (WPAN) et IEEE 802.16 (WIMAX) pour les réseaux métropolitains sans fil (WMAN).

Les performances des réseaux multi-sauts tels que les RMSF dépendent pour une grande part des protocoles de routage et de leur manière de choisir les routes. Ces protocoles devraient être en mesure de gérer le trafic et de garantir la QoS pour tout type de trafic y compris les applications multimédia, mais cela demeure un défi dans le domaine de la recherche. Le choix de route se fait selon une ou plusieurs métriques qui permettent de différencier les "bonnes" des "mauvaises" routes. Une métrique de routage permet de quantifier la qualité d'un lien ou un chemin selon certains critères tels que le taux de perte, l'interférence, la longueur des routes, le délai etc. Selon les applications, on peut avoir différentes contraintes, pour la voix par exemple on devrait donner un meilleur coût aux chemins avec moins de délai quitte à accepter un léger taux de perte.

Vu l'importance des métriques dans les choix des routes, plusieurs recherches se sont penchées sur ce problème. Dans un premier temps, les métriques pour réseau ad-hoc ont été utilisées mais vu leurs caractéristiques qui diffèrent de celles des RMSF, on peut voir qu'elles vont à l'encontre des celles-ci. La métrique se basant sur le minimum de saut destinée à la base aux réseaux ad

hoc a été adoptée pour les RMSF. Mais leur mobilité réduite et l'absence de contrainte d'énergie font qu'elle ne constitue pas une solution idéale pour les RMSF [5]. Par la suite, des métriques pour RMSF ont été proposées mais la plupart ne prennent pas en considération toutes les contraintes qui entrent en jeu dans le routage telles que l'interférence, l'asymétrie des liens, la performance de calcul des métriques qui sont autant de facteurs qui peuvent influencer sur la qualité du protocole de routage.

Vu la popularité et les nombreux avantages des RMSF, il nous a semblé primordial de se pencher sur ces métriques et de nous assurer qu'elles sont précises, qu'elles reflètent au maximum l'état du réseau en tout temps et qu'elles sont mises à jour régulièrement ou en cas de changement pour offrir des protocoles de routage de qualité.

1.6 Description du problème des métriques de routage

Durant la conception des métriques de routage, il faut répondre à deux exigences :

- Premièrement, les mesures doivent être précises. Une métrique se basant par exemple sur le taux de perte ou le taux d'interférence doit être en mesure d'estimer correctement ces valeurs avant de les utiliser. En plus de cela, elles doivent être mises à jour régulièrement parce que le protocole doit pouvoir détecter les changements au niveau de la qualité des routes, voir celles qui ne sont plus bonnes et en changer en conséquence.

- Deuxièmement, la méthode la plus courante pour mesurer la qualité des liens consiste à injecter régulièrement des paquets dit paquets de contrôle. Il ne faut pas que ces paquets de contrôle surchargent le réseau et consomment trop de ressources car cela pourrait affecter le trafic réel et ainsi dégrader les performances du protocole.

La métrique doit être adaptable au protocole de routage. Dans la majeure partie des cas, les métriques sont mises en place puis implémentées dans un protocole de routage existant. Mais toute métrique ne fonctionnera pas avec tout protocole de routage. En effet, il existe certaines restrictions. Par exemple une métrique non-isotonique [30] ne fonctionnera pas avec un protocole de routage proactif. Nous allons approfondir cet aspect dans la suite du document.

1.7 Contributions

Dans ce mémoire nous avons considéré le problème des métriques de routage dans les RMSF. Nous avons étudié les travaux réalisés à ce sujet puis nous avons dégagé pour chacune d'elles les points forts et les faiblesses. À partir de cela, nous avons proposé deux contributions :

- Metric Based on Probabilities (MBP) : une nouvelle métrique MBP qui se base sur la probabilité de réussite des liens pour déterminer les meilleures routes. Elle prend en considération le taux de perte et l'interférence.
- MBP-AODV : une amélioration du protocole de routage Ad-hoc On-demand Distance Vector (AODV) [14]. MBP-AODV intègre notre nouvelle métrique MBP et y ajoute un système de surveillance des liens qui détecte toute dégradation qui pourrait perturber le trafic.

Nous avons proposé l'article : *MBP: Routing Metric Based on Probabilities for Multi-radio Multi-channel Wireless Mesh Networks*, qui a été accepté dans IEEE, Wireless Communications and Mobile Computing Conference, 2011 (IWCMC' 2011).

1.8 Organisation du mémoire

Le corps du mémoire est organisé comme suit : dans le chapitre 2 nous allons présenter les réseaux maillés sans fil de manière générale pour mieux

cerner le contexte de recherche avec ses caractéristiques. Ensuite, le chapitre 3 passe en revue les métriques et protocoles de routage existants. Nous ferons par la suite une étude critique de ces métriques et protocoles ce qui nous permettra de mettre en évidence leurs forces et leurs faiblesses. Le chapitre 4 nous fournit une description de MBP, une nouvelle métrique de routage que nous avons mise en place et le protocole de routage associé. Puis, le chapitre 5 présente les résultats expérimentaux de notre nouvelle métrique de routage comparés aux métriques de routage existantes sur deux types de topologies. Enfin, le chapitre 6 conclut ce travail et fournit des perspectives futures.

Chapitre 2: Généralités sur les réseaux maillés sans fil

Dans ce chapitre nous allons décrire de manière générale les RMSF pour mieux comprendre le contexte de recherche. Les RMSF constituent une nouvelle classe de réseaux sans fil. C'est une technologie en pleine expansion et très prometteuse. Les RMSF sont destinés à offrir des services sans fil à une large variété d'applications pour des clients fixes ou mobiles. Elle permet d'interconnecter avec des liaisons à hauts débits des zones où le câblage serait difficile voire impossible à réaliser.

Néanmoins, il subsiste des axes de recherche à explorer ou à approfondir pour améliorer les RMSF. Parmi ces axes, on peut citer la planification et le déploiement, l'assignation des canaux, le routage, le contrôle d'admission, la sécurité, etc. Certains protocoles destinés aux réseaux ad hoc ont été utilisés dans les RMSF [2, 14, 15, 26] mais ils ne sont pas toujours adaptés et présentent très vite des limites vues leurs particularités.

2.1 Technologies sans fil

La mise en place de réseaux sans fil nécessite une technologie sans fil qui permet aux nœuds de communiquer entre eux par le biais d'ondes radios ou infrarouges. Cette technologie permet aux routeurs d'accéder au canal radio, de gérer l'accès concurrentiel du canal afin d'éviter qu'il soit monopolisé par certaines stations. Les technologies sans fil diffèrent selon le type, la taille, les débits et les applications des réseaux utilisés.

2.1.1 Différentes technologies sans fil

Il existe plusieurs technologies sans fil qui permettent la mise en place de réseaux sans fil. Ces technologies peuvent être classifiées selon les normes du sans fil [12] utilisés :

- L'IEEE 802.15 (Bluetooth) utilise les ondes radio dont la bande de fréquence est située entre 2,4 et 2,4835 GHz. Cette technologie est destinée à la communication entre différents appareils à très courte distance (souris sans fil). Elle est destinée uniquement aux WPAN;
- l'IEEE 802.11 (Wi-Fi) est la norme la plus utilisée à ce jour dans les réseaux maillés sans fil. Elle a été conçue pour des réseaux de courtes distances (une centaine de mètres en moyenne). Il existe plusieurs versions de cette norme selon la bande de fréquence utilisée. La version IEEE 802.11a a une bande de fréquence située autour de 5 GHz, l'IEEE 802.11b et IEEE 802.11g opèrent sur 2,4 GHz. L'IEEE 802.11n peut fonctionner aussi bien avec la bande 2,4 GHz qu'avec 5 GHz. Les débits varient de 1 à 54 Mbps suivant la norme et ses éventuelles extensions. C'est la technologie qu'on utilise dans nos travaux.
- l'IEEE 802.16 (WIMAX) est de plus en plus prise en compte dans les RMSF. Elle permet des connexions de plusieurs dizaines de kilomètres avec des débits pouvant atteindre 100 Mbps. Elle est destinée au WMAN.

Il faut noter que dans un réseau maillé, différentes technologies sans fil peuvent subsister. Par exemple, un nœud peut avoir une interface Wi-Fi connecté à un WLAN et une interface WIMAX (cf. Fig.1.3).

2.1.2 Problèmes liés à l'utilisation des technologies sans fil

Le canal radio est le moyen qui permet d'envoyer et de recevoir des données à travers les ondes. Plusieurs problèmes sont liés à la nature même du canal radio. En particuliers, il faut prendre en compte:

- *L'atténuation du signal* due à la distance entre les nœuds. L'environnement peut contribuer à l'atténuation du signal avec la présence d'immeubles, de collines etc.
- *Le partage du canal avec les nœuds interférents* : Le rayon de transmission est la zone dans laquelle tout nœud récepteur est capable de recevoir correctement les données envoyées par la source, tandis que le rayon d'interférence est la zone dans laquelle le nœud détecte une activité du médium mais ne peut pas décoder correctement les signaux reçus (Fig.2.1). Tout nœud dans le rayon d'interférence ne peut émettre en même temps que l'émetteur. Le partage du médium se fait aussi bien avec les nœuds se trouvant dans le rayon de transmission que dans le rayon d'interférence.

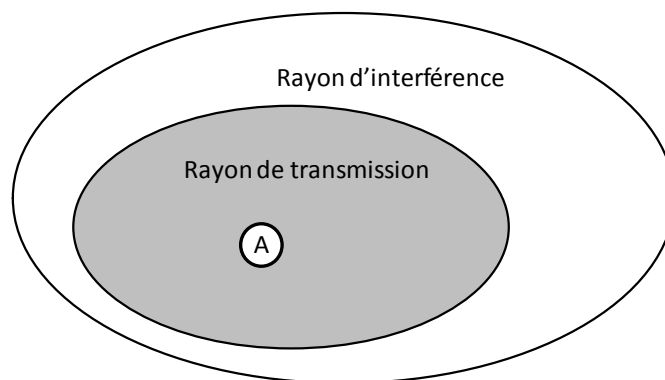


Fig.2.1: Rayon de transmission et rayon d'interférence

- *Les interférences* : en télécommunication lorsque plusieurs communications ont lieu sur le même canal, ils se partagent la bande passante disponible du

canal radio. Ces communications peuvent interagir les unes sur les autres et ainsi dégrader le signal : c'est le phénomène des interférences. Les interférences constituent une limite importante dans les communications sans fil qui peut fortement dégrader la qualité des transmissions [7]. Ainsi la recherche se penche justement sur cette problématique en essayant de trouver des architectures qui minimisent l'interférence [16] ou, comme dans notre travail, proposer des protocoles de routage capables d'éviter les routes à forte interférence. On distingue principalement deux types d'interférence (1) l'*interférence inter-flux* qui a lieu quand deux nœuds dans le même rayon d'interférence opèrent sur le même canal de communication tel qu'illustré sur la Fig.2.2 en (a) pour les nœuds B et D; (2) l'*interférence intra-flux* se produit lorsque deux ou plusieurs liens sur la même route dans un même rayon d'interférence opèrent sur le même canal. Seul un des liens peut être actif à la fois en (b). Les nœuds A et B ne peuvent pas émettre en même temps, il a été démontré par les auteurs [4] que ce phénomène réduit de moitié la bande passante disponible sur le chemin A-B-C. La diversité des canaux consiste à utiliser différents canaux sur un même chemin et permet d'éviter l'interférence intra-flux. Pour éviter les interférences, une solution serait d'équiper les routeurs de plusieurs interfaces radios et des canaux différents pour des liens qui sont dans le même rayon d'interférence. Cette solution ne résout pas entièrement le problème des interférences car le nombre d'interfaces radio par routeur est limité et le nombre de canaux orthogonaux disponibles dépend de la technologie sans fil utilisée. Nous discuterons en détail de la solution multiples-radios, multiples-canaux dans la section 2.3.

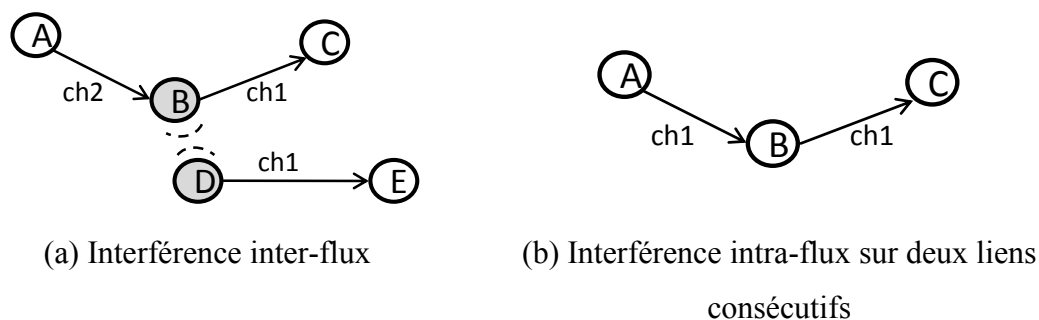


Fig.2.2: Interférences entre les nœuds

Liens bidirectionnels : les liens radio ne sont pas toujours bidirectionnels. Ainsi un mobile peut recevoir des données de la part d'un autre mobile sans que la réciproque soit vraie. Ce phénomène pose un problème dans le processus de découverte de route car lorsqu'un chemin est créé, les informations de réponse ne peuvent pas toujours emprunter le chemin inverse, nécessitant la construction d'une nouvelle route. Ce phénomène pose aussi un problème dès lors qu'on utilise des échanges point-à-point avec 802.11 puisque ces échanges ne peuvent fonctionner que sur des liens bidirectionnels.

Des nouvelles versions de ces technologies sont proposées afin de pallier à certains problèmes en occurrence IEEE 801.11n, IEEE 802.11g. Ces limites technologiques devraient être prises en compte dans la conception des réseaux en choisissant des environnements propices à une transmission. De même, les protocoles de routage doivent prendre en compte ces limites afin d'éviter qu'ils aient un impact négatif sur le routage du trafic.

2.2 Architecture des RMSF

La conception de réseau sans fil est une entreprise importante où plusieurs aspects doivent être gérés. Elle exige de faire des compromis entre plusieurs facteurs tels que le coût, la facilité de gestion, la disponibilité des

ressources et la mobilité. Les composants de base des RMSF sont les nœuds sans fil. Ces nœuds peuvent être de deux types : les routeurs maillés et les clients maillés. En plus des fonctionnalités des routeurs sans fil classiques, les routeurs maillés intègrent d'autres fonctionnalités. En effet, les routeurs maillés peuvent être équipés de plusieurs interfaces radios. Les RMSF sont extensibles grâce à la couche MAC des routeurs maillés qui a été améliorée afin de supporter cette extensibilité.

L'ensemble des nœuds sans fil peut être interconnecté pour former une architecture particulière. Il existe trois types d'architecture dans les RMSF:

- *L'architecture " par épine dorsale " d'un réseau maillé* (Fig.2.3 extraite de [1]): elle est composée de routeurs et de clients maillés. Les routeurs maillés fixes constituent l'épine dorsale qui assure la connectivité. Ils peuvent jouer le rôle de passerelle et être connectés à Internet. Les clients peuvent communiquer directement avec les routeurs de l'épine dorsale s'ils utilisent la même technologie sans fil, ou passer par un point d'accès.

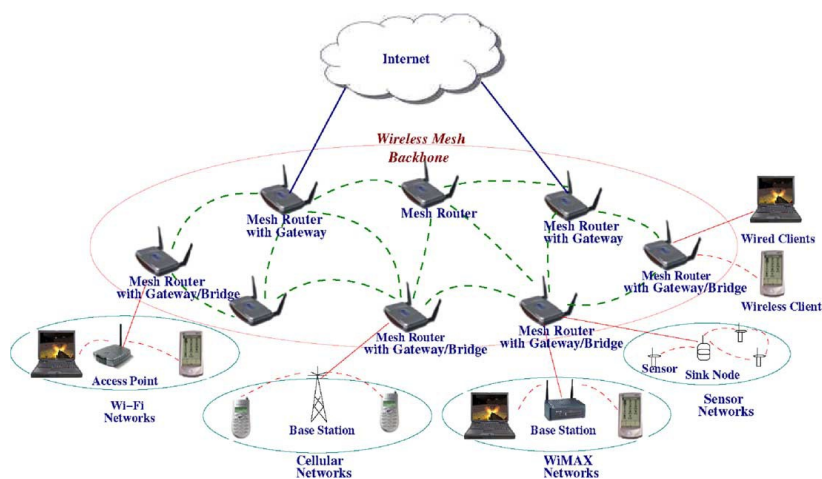


Fig.2.3: Architecture " par épine dorsale " d'un réseau maillé

- *Architecture client* (Fig.2.4 extraite de [1]): Dans cette architecture, le réseau maillé est composé uniquement de clients qui jouent en même temps le

rôle de client et de routeur. Les fonctionnalités supplémentaires de routage et d'auto-configuration des clients maillés sont supportées par des logiciels. La communication est une communication point à point.

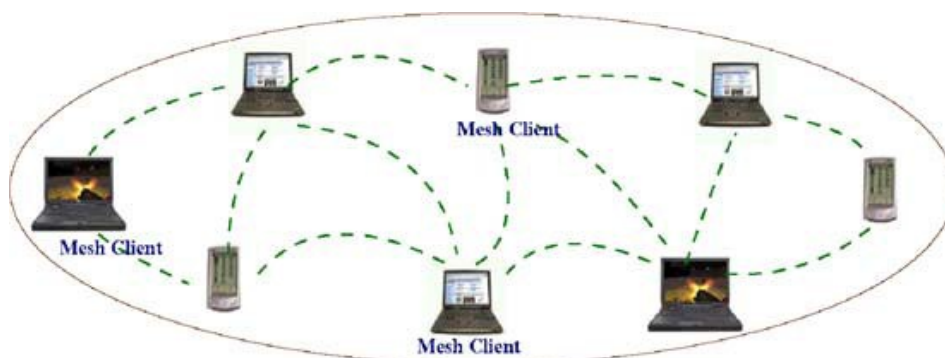


Fig.2.4: Architecture client d'un réseau maillé

- *Architecture hybride* (Fig.2.5 extraite de [1]): c'est une combinaison entre l'architecture épine dorsale et l'architecture client.

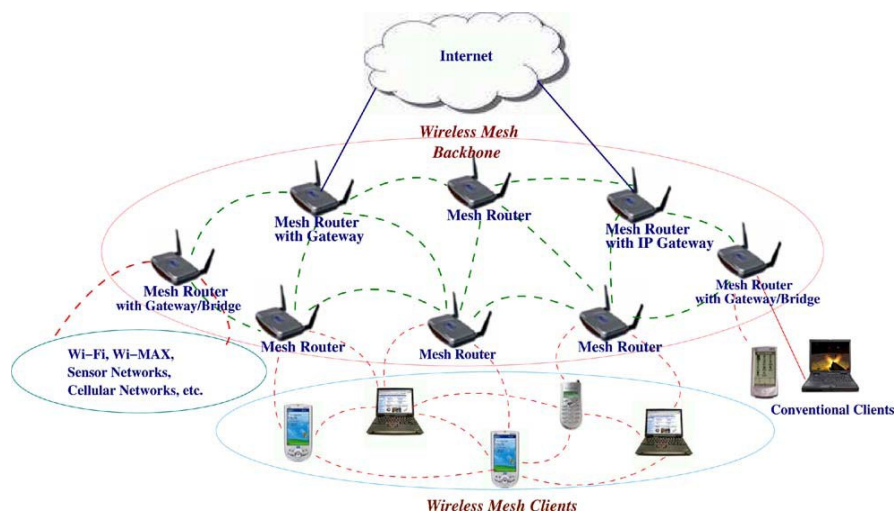


Fig.2.5: Architecture hybride d'un réseau maillé

Le routage est un des points sensibles dans la recherche dans les RMSF. Le choix des routes et l'utilisation adéquates des ressources disponibles peuvent avoir une forte influence sur les performances des RMSF.

2.3 RMSF multiples-radios multiples-canaux et affectation des canaux

Les routeurs maillés peuvent être munis de plusieurs interfaces radios. C'est un moyen peu coûteux qui peut considérablement augmenter les capacités des réseaux. La bande passante dans un RMSF diminue rapidement lorsque le nombre de sauts augmente et quand le même canal est réutilisé. Ce phénomène est dû à l'interférence intra-flux. Le fait d'utiliser plusieurs interfaces radio et plusieurs canaux permet aux nœuds de transmettre et de recevoir simultanément des données sur des canaux différents.

L'assignation des canaux est le fait d'attribuer des canaux aux différentes interfaces radio des nœuds du réseau. Elle vise à répartir entre les nœuds les canaux disponibles de manière optimale i.e. de manière à maximiser les capacités du réseau et minimiser les interférences. L'assignation des canaux reste un point sensible dans la recherche dans les RMSF car même avec une connaissance totale de la topologie, elle reste un problème NP-complet [3] quand le nombre de canaux est supérieur à 2.

Les bandes de fréquence des technologies sans fil sont divisées en plusieurs canaux. La Fig.2.6 extraite de [20] nous donne un exemple de découpage de la bande de fréquence d'IEEE 802.11b qui correspond à 2.4Ghz. Chaque canal s'étend sur une longueur de 22Mhz et les canaux sont séparés de 5Mhz les uns des autres, de ce fait on a 14 canaux disponibles. Mais les canaux adjacents se chevauchent et doivent partager la bande passante, ce qui crée de l'interférence lorsqu'ils sont utilisés en même temps. Pour que les canaux ne se chevauchent pas il faut que leur bande de fréquence respective soient séparées

d'au moins 25 MHz, ils sont dit alors orthogonaux. Par exemple le canal 1 opère sur la bande 2,412 GHz et le canal 2 sur 2,417 GHz ils se chevaucheront lors d'une communication simultanée sur ces deux canaux. Tandis que les canaux 1 et 6 sont séparés de 25MHz et par conséquent on peut voir toujours sur Fig.2.6 que les 3 canaux 1, 6 et 11 ne se chevaucheront pas. Ainsi IEEE 802.11b disposera d'au maximum trois canaux orthogonaux qui sont les canaux 1, 6 et 11.

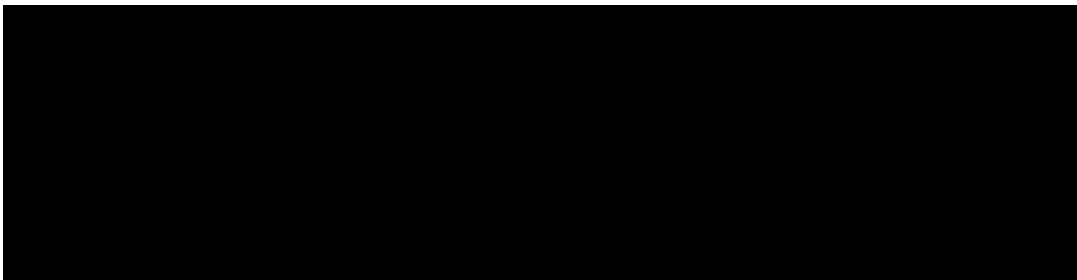


Fig.2.6: Découpage en canaux de la bande de fréquence 2,4 GHz

Le même découpage est fait pour l'IEEE 802.11a sur la bande de fréquence 5 GHz sauf qu'on aura 24 canaux disponibles dont 12 canaux orthogonaux.

Chapitre 3: Revue de littérature des métriques et protocoles de routage

Une métrique de routage est une valeur attribuée à un lien ou à une route dans un réseau. Elle permet de déterminer si il/elle est de bonne qualité ou non. Les métriques de routage se basent sur plusieurs paramètres tels que le taux de perte, le taux d'interférence, le délai etc. pour quantifier la qualité de la route. Par la suite, ces métriques seront utilisées par les protocoles de routage pour choisir les meilleures routes afin d'acheminer les flux de trafic. Par conséquent, la précision des métriques est fondamentale car en déterminant les meilleures routes, elles permettront de maximiser les débits, de réduire les délais de transmission et donc d'améliorer les performances.

Dans ce chapitre, nous passerons en revue les métriques de routage et pour chacune d'entre elles, nous dégagerons leurs points forts et leurs faiblesses. Nous allons aussi voir le principe de fonctionnement de certains protocoles de routage susceptibles d'utiliser ces métriques afin d'assurer un routage du trafic depuis chaque source vers chaque destination.

3.1 Métriques de routage

Les métriques de routage sont des valeurs généralement appelée *coûts* ou *poids* calculées selon un ou plusieurs paramètres tels que le nombre de saut, le taux de perte, la bande passante etc. Généralement plus la métrique est petite, plus le lien/route est de bonne qualité. La métrique d'une route est le cumul (addition, multiplication, moyenne etc.) des métriques des liens qui composent cette route, cependant d'autres paramètres tels que la diversité des canaux (voir section 2.1.2) peuvent entrer en compte lors de ce cumul.

Les défis majeurs du choix des métriques sont : de minimiser les interférences, d'éviter le problème des stations cachées [29], de récupérer des informations précises sur l'état des liens. La Fig.3.1 illustre le problème des stations cachées. Supposons que le nœud A veuille envoyer du trafic au nœud B à travers le canal ch1, et que C veuille envoyer à D à travers le canal ch1 aussi. Une émission de C vers D va créer des collisions au niveau du récepteur B. Les nœuds A et D ne sont pas le rayon d'interférence l'un de l'autre, d'où l'expression " stations cachées ". Plus le nombre de collisions est élevé, plus la bande passante sur le lien (A, B) est faible. Selon [29], si A émet à plus de 60% du débit maximum, C ne peut plus émettre à cause du nombre élevé des collisions, les paquets seront donc rejetés. Le problème des stations cachées peut considérablement réduire les débits et augmenter les pertes dues aux collisions.

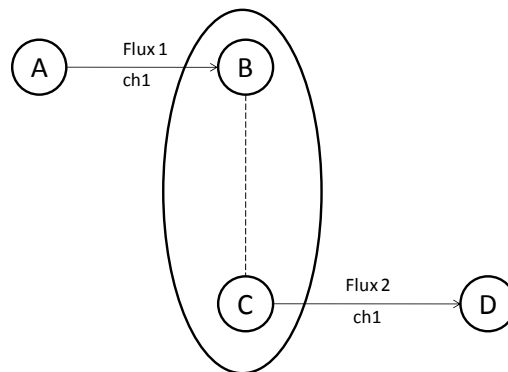


Fig.3.1: Stations cachées

Une métrique doit pouvoir quantifier de manière précise l'état du réseau pour que le protocole de routage puisse choisir les routes les plus adéquates en tout temps. La récupération de ces informations peut se faire avec différentes méthodes.

3.1.1 Techniques de mesures

Les métriques de routage se basent sur l'état du réseau. Il existe principalement trois méthodes pour obtenir ces informations :

Les méthodes dites *actives* consistent à injecter périodiquement des paquets de contrôle dans le réseau et récupérer les informations utiles telles que le taux de perte, le délai, la puissance de réception etc. L'avantage est que les mesures sont relativement précises, les inconvénients sont que : (1) les paquets de contrôle sont différents du trafic réel (taille des paquets, débit) et ne reflètent pas toujours la réalité; (2) l'envoi périodique de paquets consomment des ressources notamment la bande passante qui peut créer une surcharge du réseau (overhead). Les métriques telles que Expected Transmission Count (ETX), Expected Transmission Time (ETT) (voir section 3.1.4) utilisent une méthode active en injectant périodiquement des paquets de contrôle.

Les méthodes dites *passives* utilisent le trafic courant pour effectuer ces mesures. Cette méthode évite la surcharge inutile du réseau. L'inconvénient est que les mesures ne peuvent se faire qu'en présence de suffisamment de trafic ce qui d'avance ne peut pas être garanti. L'hétérogénéité du trafic aussi peut fausser les mesures.

Les méthodes dites *hybrides* utilisent en même temps les méthodes passives et actives. Si le trafic est suffisant les mesures sont faites grâce à une méthode passive, sinon on utilise les paquets de contrôle pour faire les mesures. Ces méthodes regroupent les avantages des deux types de méthodes. Efficient and Accurate link-quality monitor (EAR) [10] est un exemple de protocole qui utilise une méthode de mesure hybride.

3.1.2 Composants d'une métrique

Dans un réseau plusieurs paramètres peuvent influencer sur le routage. Il est donc important de prendre en considération le maximum de métriques possible.

Les métriques peuvent prendre en compte la capacité des liens, le nombre de saut, le délai, la diversité des canaux, le taux de perte, l'interférence etc. Les composants peuvent être combinés les uns aux autres selon les besoins du protocole. On peut aussi donner plus de poids à une des composantes dans l'établissement de la métrique. Le fait de combiner plusieurs paramètres augmente les probabilités d'avoir des métriques précises qui correspondent à la qualité du lien ou de la route.

3.1.3 Caractéristiques d'une métrique pour RMSF

Des recherches se sont penchées sur les caractéristiques que doit avoir une bonne métrique de routage pour RMSF. On distingue deux types de métriques :

Les métriques dites "*sensible à la charge*" (*load-sensitive*) pour lesquelles le coût est affecté en fonction de la charge du trafic courant dans le réseau. Ces métriques favorisent les chemins avec une plus large bande passante disponible. Les valeurs des métriques sont estimées en fonction de la charge or dans les RMSF les charges sont très variables ce qui cause des changements fréquents au niveau des valeurs de ces métriques. Ces fréquents changements peuvent créer une instabilité au niveau des routes qui peut se manifester par des changements de routes fréquents et brusques au niveau du protocole.

Les métriques dites "*dépendant de la topologie*" (*topology-dependent*): elles déterminent les poids/coûts en fonction de la topologie du réseau (nombre de sauts, capacité des routes). Étant donné que les RMSF ont une architecture relativement fixe, les paramètres qui dépendent de la topologie ne varient quasiment pas. Par conséquent les métriques dites *dépendant de la topologie* offrent une meilleure stabilité au niveau des routes.

Selon [30], le protocole de routage idéal pour RMSF devrait répondre à quatre critères :

- La stabilité des routes : les fréquents changements de routes peuvent perturber ou même interrompre le trafic. La stabilité dépend des composants capturés. Si le composant est fortement variable, la valeur de la métrique va constamment varier et entraîner de fréquent changement de routes. Comme composant variable, on peut citer le taux d'interférence. Les métriques dites *dépendant de la topologie* sont préférable pour les RMSF car plus stable.

-Les meilleures performances pour les chemins à coût minimum. Cela signifie que plus le coût d'un chemin est moindre, plus le chemin sera de bonne qualité. Cela permet de réduire le problème de recherche de route au problème de recherche du plus court chemin.

- Les routes devraient être trouvées avec des algorithmes efficaces [8] (avec une complexité en $O(n)$). L'isotonicité est une propriété qui voudrait que, durant la découverte des routes, si on rajoute le coût d'un même lien sur deux chemins différents, il faut que la différence soit préservée. Considérons l'exemple de la Fig.3.2 avec les arcs a et b . notons leur coût respectif $C(a)$ et $C(b)$, en ajoutant le coût de l'arc c à celui de l'arc a ou b , la propriété voudrait que l'inégalité soit conservée. Si on devait par exemple prendre en compte des paramètres tels que la diversité des canaux en ajoutant un coût supplémentaire s quand on réutilise le même canal, on aurait $C(a+b) = C(a) + C(b) + s$. Et donc l'inégalité ne sera pas conservée à cause du terme s . Cette propriété permet d'éviter les boucles lors de la recherche de routes. Comme démontré dans [30], la propriété d'isotonicité est une condition nécessaire et suffisante pour que des protocoles basés sur les algorithmes de Bellman-Ford et Dijkstra tels qu'OLSR puissent trouver les chemins de moindres coûts

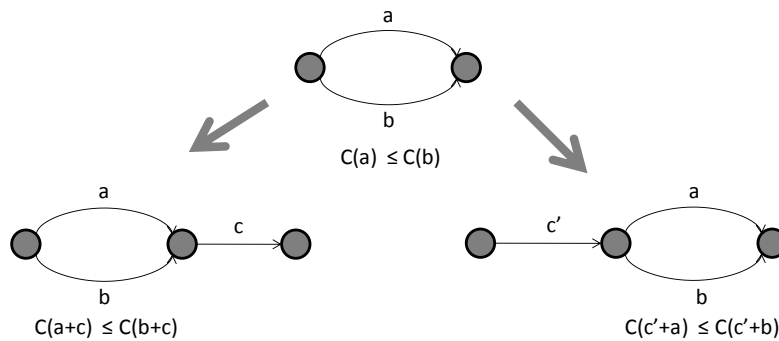


Fig.3.2: Exemple d'isotonicit 

-Sans boucle : le protocole devrait pouvoir choisir des routes sans boucle i.e de ne pas repasser par les m mes nœuds lors de l'envoi des paquets.

Très peu de m triques pour RMSF existantes r pondent   tous ces crit res. Nous allons en pr senter quelques unes dans la section suivante.

3.1.4 M triques de routage existantes

Dans cette partie, nous allons pr senter quelques contributions sur les m triques de routages.

3.1.4.1 Nombre de saut

Elle consiste   choisir le plus court chemin en termes de nombre de sauts de la source vers la destination dans un r seau. Chaque lien a un co t de 1. Cette m trique a  t  emprunt e aux MANets. Elle est simple   mettre en place, ne n cessite aucun calcul suppl mentaire et est isotonique. La m trique nombre de saut ne n cessite pas beaucoup de paquet de contr le, le nombre de sauts est calcul  durant la d couverte des routes. N anmoins, elle ne convient pas aux RMSF car elle ne prend pas en compte la qualit  des liens [5].

3.1.4.2 Expected Transmission Count (ETX)

Cette métrique est considérée comme la première métrique de routage dédiée entièrement au RMSF. Elle a été proposée en 2003 par Couto et al [4]. ETX estime les nombre de transmissions et de retransmissions nécessaires pour acheminer un paquet sur un lien. ETX pour un lien est défini comme suit :

$$ETX = \frac{1}{d_f \times d_r} \quad (1)$$

Où d_f et d_r représente les taux de réussite à l'avant et en arrière sur le lien. Pour calculer ces valeurs, chaque nœud envoie périodiquement des paquets de contrôle à ses voisins.

$$d_f = \frac{N_s}{N_t} \quad (2)$$

Où N_s et N_t sont respectivement le nombre de paquets de control reçus, sur le nombre de paquets total envoyés.

ETX pour un chemin p est la somme des ETX des liens l qui composent ce chemin

$$ETX_p = \sum_{l \in p} ETX_l \quad (3)$$

Sur la Fig.3.3, considérons les routeurs sans fil A , B , C et D . Appelons P le chemin allant de A à D , P est composé des liens AB , BC et CD . Calculons l'ETX pour le chemin P .

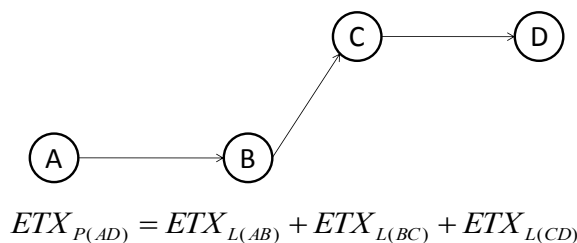


Fig.3.3: Calcul de ETX sur le chemin ABCD

L'isotonicit  est une propri t  qui voudrait que, lors la d couverte d'une route, si on rajoute le co t d'un m me lien sur deux chemins diff rents, il faut que la diff rence soit pr serv e. Prenons l'exemple de la Fig.3.4 avec les arcs a et b . Notons leurs co ts respectifs $C(a)$ et $C(b)$, en ajoutant le co t de l'arc c   celui de l'arc a ou b , la propri t  voudrait que l'in galit  soit conserv e. Si on devait par exemple prendre en compte des param tres tels que la diversit  des canaux en ajoutant un co t suppl mentaire s quand on r utilise le m me canal, on aurait $C(a+b) = C(a) + C(b) + s$. Ainsi, l'in galit  ne sera pas conserv e   cause du terme s . Cette propri t  permet d' viter les boucles. Seules les m triques isotoniques peuvent fonctionner avec des protocoles de routage proactifs sinon il risquerait d'avoir des boucles lors de la d couverte des routes [30].

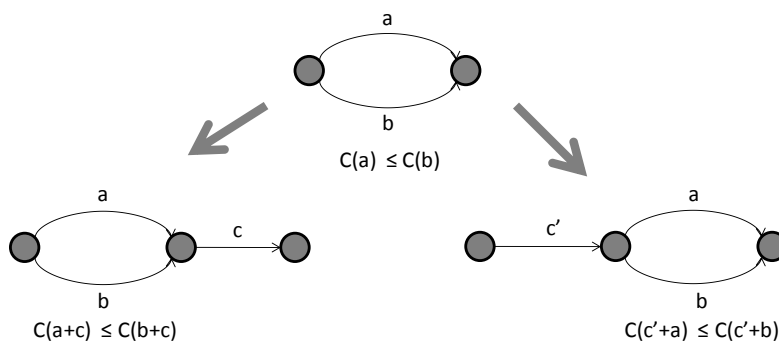


Fig.3.4: Exemple d'isotonicit 

ETX est isotonique, facile à calculer. Il assigne un coût plus élevé aux liens avec une forte probabilité de perte ce qui constitue une amélioration par rapport à la métrique nombre de saut. Néanmoins, elle ne capture pas l'effet de l'asymétrie [10] et peut choisir un chemin avec un taux de réussite à l'envers élevé mais avec un taux de réussite avant faible alors que lors de l'envoi seul le sens avant est utilisé. De ce fait en faisant la moyenne comme indiqué dans l'équation (1), le coût du lien peut être considéré comme acceptable. L'autre inconvénient est qu'il ne capture pas l'effet de l'interférence. Enfin, ETX ne considère ni la charge des liens, ni la taille des paquets, ni la bande passante lors de la sélection des routes (un même paquet sur deux liens avec des bandes passantes différentes auront des délais de transmission différents). ETX est une *topology-dependent* métrique.

3.1.4.3 Expected Transmission Time (ETT)

C'est une extension/amélioration d'ETX [6] qui considère la charge du réseau. Elle estime le temps nécessaire à un paquet pour être transmis sur un lien. ETT pour un lien l est défini comme suit :

$$ETT_l = ETX_l \times \frac{S}{B} \quad (4)$$

où S représente la taille du paquet et B la bande passante disponible sur ce lien. Le calcul de bande passante se fait avec la technique du " packet pair " [9]. Chaque nœud envoie deux paquets de contrôle quasi simultanément à ses voisins chaque minute. Le premier est un petit paquet de taille 137 octets et le second, plus grand, est de 1137 octets. Les voisins qui reçoivent les paquets calculent le temps Δt entre la réception du premier et du second paquet. Après un période de 10 secondes, le nœud récupère la plus petite des valeurs de Δt et estime la bande passante par le rapport $1137 / \min(\Delta t)$. Cette estimation de bande passante n'est

pas exacte, mais elle permet de distinguer les liens avec des bandes passantes sensiblement différentes.

ETT estime le temps d'acheminement d'un paquet sur un lien. Comme pour ETX, la valeur d'ETT pour un chemin est la somme des ETTs des liens qui constituent ce chemin.

L'amélioration d'ETT par rapport à ETX réside dans le fait qu'elle prend en compte la charge, la bande passante et la taille des paquets. Les problèmes de l'asymétrie et de l'interférence demeurent irrésolus.

3.1.4.4 ML (minimum loss)

Passos et al. [27] ont montré que les chemins choisis par ETX peuvent être instables et mener à des taux de perte élevés. Ils ont donc proposé la métrique ML qui interprète les taux de réussite des liens comme des probabilités. Par exemple la probabilité de réussite de la transmission d'un paquet sur le lien A-B est :

$$P_{AB} = d_f \times d_r \quad (5)$$

Sur un chemin à plusieurs sauts, la probabilité de réussite sera le produit des probabilités des liens qui constituent ce chemin. Sur la Fig.3.5, la métrique du chemin de A à C passant par B sera le produit des probabilités des liens A-B et B-C: $P_{AC} = P_{AB} \times P_{BC}$

La probabilité de réussite correspond à la probabilité pour qu'un paquet soit transmis correctement sur un lien.

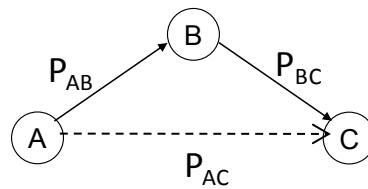


Fig.3.5: Probabilité de réussite sur le chemin
AC

Les résultats ont montré que ML est plus stable, accuse moins de perte de paquets, et améliore légèrement le débit par rapport à ETX.

Dans la suite nous allons voir les métriques qui prennent en charge l'interférence.

3.1.4.5 Weighted Cumulative Expected Transmission Count (WCETT)

WCETT [6] est une extension d'ETT pour les réseaux multiples-radios multiples-canaux. Elle essaie d'éviter l'interférence de type intra-flux causée par la réutilisation d'un même canal sur plusieurs liens d'un même chemin.

$$WCETT_p = (1 - \beta) \times \sum_{l \in P} ETT_l + \beta \times \max_{i \leq j \leq k} X_j \quad (6)$$

où $0 \leq \beta \leq 1$ ($\beta = 0,5$ a été choisie comme valeur optimale selon [6]), ETT_l est le coût du lien l , X_j est la somme des coûts pour chaque lien opérant sur le canal j , k est le nombre de canaux (de 0 à k canaux). La Fig.3.6 donne un exemple de calcul de WCETT sur un chemin.

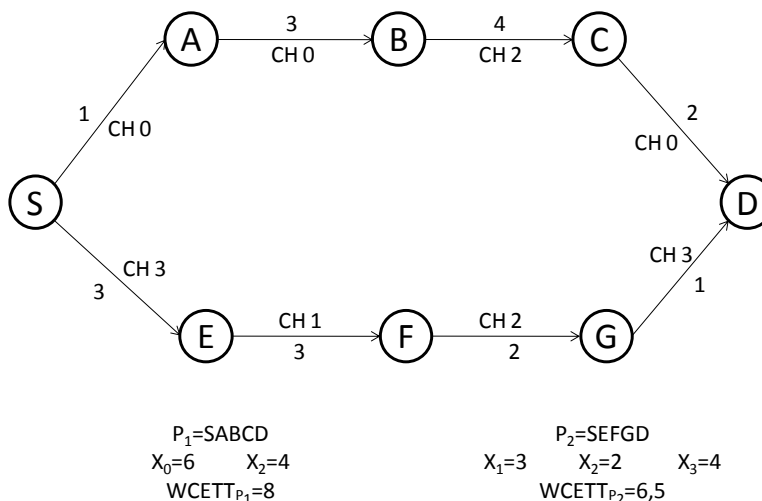


Fig.3.6: Exemple de calcul de métrique avec WCETT

Deux liens utilisant le même canal et qui sont dans le même rayon d'interférence ne peuvent pas opérer en même temps. Considérons un chemin à plusieurs sauts (Fig.3.7), les liens (A, B) et (E, F) sont distants et ne sont pas dans le rayon l'un de l'autre néanmoins WCETT considèrera qu'ils s'interfèrent dans le calcul de X_j ce qui peut fausser l'estimation de l'interférence intra-flux. WCETT prend en compte l'interférence intra-flux mais ignore l'interférence inter-flux. De plus, WCETT n'est pas isotonique à cause du terme X_j qui capture l'effet de la diversité des canaux.

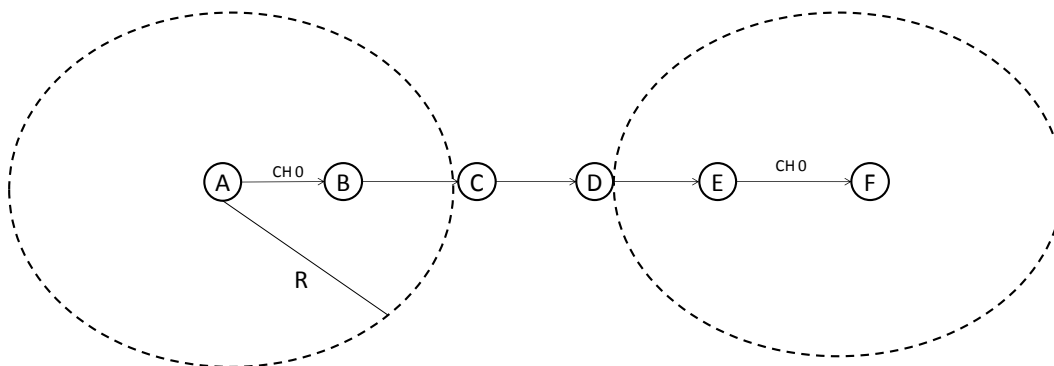


Fig.3.7: WCETT interférence intra-flux sur lien distant

3.1.4.6 interference AWARE (iAWARE)

iAWARE [18] palie aux insuffisances des autres métriques en considérant les deux types d'interférence, inter-flux et intra-flux. iAWARE approxime le temps moyen durant lequel le médium est occupé à cause de l'interférence due aux transmissions des nœuds voisins. Il utilise le SINR (Signal Interference to Noise Ratio) et le SNR (Signal to Noise Ratio) pour continuellement estimer le taux d'interférence. Le SINR est la puissance de réception d'un paquet en considérant l'interférence et le bruit tandis que le SNR est la puissance de réception d'un paquet en ne considérant que le bruit. S'il y a beaucoup d'interférence le SINR devient faible. Le SINR est inférieur ou égal au SNR. Ils sont définis comme suit :

$$SINR(u, v) = \frac{P_v(u)}{N + \sum_{k \in v'} P_v(k)} \quad (7)$$

$$SNR(u, v) = \frac{P_v(u)}{N} \quad (8)$$

où N est le bruit, $P_v(u)$ est la puissance de réception de u vers v , v' est l'ensemble des nœuds interférents et $\sum_{k \in v'} P_v(k)$ est cumule des bruits causés par les nœuds interférents.

Les interférences réduisent la puissance de réception d'un paquet, SINR. Soit un lien i avec les nœuds u et v comme extrémités, on définit l'Interférence Ratio (IR) pour un nœud comme suit :

$$IR_i(u, v) = \frac{SINR_i(u)}{SNR_i(u)} \quad (9)$$

$$0 \leq IR_i(u, v) \leq 1$$

Quand il y a beaucoup d'interférence le SINR devient faible et la valeur d' IR tend vers 0 sinon si l'interférence est nulle, le SINR est égal au SNR et la valeur d' IR est égale à 1.

L' IR représente le taux d'interférence. L' IR pour un lien est défini comme étant le minimum des IR des nœuds qui constituent le lien.

$$IR_i(u, v) = \min(IR_i(u), IR_i(v)) \quad (10)$$

Ainsi, $iAWARE$ calcule le coût d'un lien comme suit :

$$iAWARE_i = \frac{ETT_i}{IR_i} \quad (11)$$

$iAWARE$ [18] capture l'effet du taux de perte et du taux de transmission grâce à ETT et l'interférence avec l' IR . Un lien avec un ETT élevé et un fort taux d'interférence IR aura un $iAWARE$ faible. Il faut noter que plus la valeur de $iAWARE$ est petite plus le lien est bon.

$iAWARE$ pour un chemin se calcule avec (12). Il correspond à la somme des $iAWARE$ des liens qui composent le chemin pondéré avec le terme $\max X_j$ qui est le même que pour $WCETT$ afin de prendre en compte l'interférence intra-flux.

À l'instar de $WCETT$, $iAWARE$ prend en compte l'interférence intra-flux en favorisant la diversité des canaux et est aussi non isotonique à cause du terme X_j .

$$iAWARE_p = (1 - \beta) \times \sum_{l \in P} iAWARE_l + \beta \times \max_{i \leq j \leq k} X_j \quad (12)$$

où $0 \leq \beta \leq 1$, $iAWARE_l$ est le coût du lien l , X_j est la somme des coûts pour chaque lien opérant sur le canal j , k est le nombre de canaux.

$iAWARE$ et $WCETT$ présentent un inconvénient dans le calcul de leur métrique que nous allons illustrer dans l'exemple qui suit (Fig.3.8).

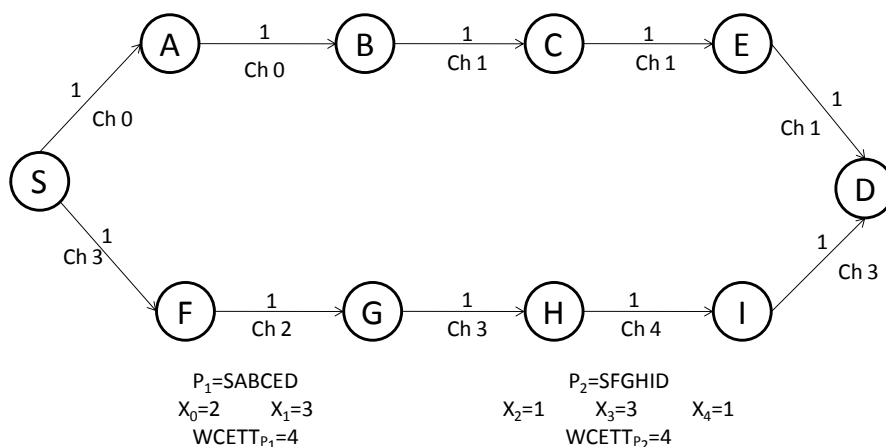


Fig.3.8: Exemple d'inconvénient de WCETT et iAWARE

Les chemins P_1 et P_2 ont les mêmes valeurs de WCETT mais en analysant les chemins on peut voir que P_2 est meilleur que P_1 . L'effet de l'interférence intra-flux est plus forte sur P_1 car on a les liens (S, A) et (A, B) qui utilisent le canal 0 et (B, C), (C, E) et (E, D) qui utilisent le canal 1 alors que sur P_2 seul (S, F) (G, H) et (I, D) s'interfèrent sur le canal 3. De plus les liens (S, F) et (I, D) ne s'interfèrent pas car ils sont distants donc ils ne sont pas dans le rayon d'interférence l'un de l'autre. WCETT et iAWARE ne distinguent pas toujours les meilleures routes en termes d'interférence intra-flux comme l'illustre la Fig.3.8.

3.1.4.7 Metric of Interference and Channel-switching (MIC)

MIC [23] résout le problème de non-isotonie et capture l'interférence inter-flux et intra-flux. MIC introduit l'*Interference aware Resource Usage (IRU)* pour un lien (i, j) , il est défini comme suit :

$$IRU_{ij}(c) = ETT_{ij}(c) \times |N_i(c) \cup N_j(c)| \quad (13)$$

c désigne le canal sur lequel le lien (i, j) opère, IRU capture l'effet de l'interférence inter-flux grâce au nombre de nœud qui interfère avec les nœuds i

et j ($|N_i(c) \cup N_j(c)|$). Il prend aussi en considération le taux de perte et la différence des débits de transmission en mesurant la valeur de ETT défini plus haut. Il peut être défini comme étant le temps que met le lien (i,j) pour acheminer un paquet en tenant compte de l'interférence des nœuds voisins i.e. si il y a 3 nœuds interférents (i.e. $|N_i(c) \cup N_j(c)|=3$), ils supposent que la transmission prendra 3 fois plus de temps ($ETT_{ij} \times 3$).

MIC pour un chemin est défini comme suit :

$$MIC(p) = \alpha \sum_{link l \in P} IRU_l + \sum_{node a \in P} CSC_i \quad (14)$$

Où $\alpha = \frac{1}{N \times \min(ETT)}$

Le *Channel Switching Cost* (CSC) capture l'effet de l'interférence intra-flux.

$$CSC_i = \begin{cases} w_1 & \text{if } CH(prev(i)) \neq CH(i) \\ w_2 & \text{if } CH(prev(i)) = CH(i) \end{cases} \quad (15)$$

$$0 \leq w_1 < w_2$$

CSC est un coût supplémentaire qui représente l'interférence intra-flux. Il rajoute un coût relativement élevé w_2 si deux liens consécutifs utilisent le même canal, sinon w_1 (généralement égal à 0) si ils utilisent des canaux différents.

Le terme α représente un compromis (trade-off) entre l'interférence intra-flux et inter-flux. N est le nombre de nœud dans le réseau, $\min(ETT)$ est la plus petite d'ETT du réseau.

À priori, comme les autres métriques présentées plus haut (WCETT, iAWARE), MIC n'est pas isotonique à cause du terme CSC . Mais les auteurs ont proposé une décomposition isotonique de leur protocole. Ceci représente un avantage par rapport aux autres protocoles. Mais cette décomposition est assez

complexe à implémenter. Ils introduisent des nœuds virtuels tels qu'illustré sur la Fig.3.9

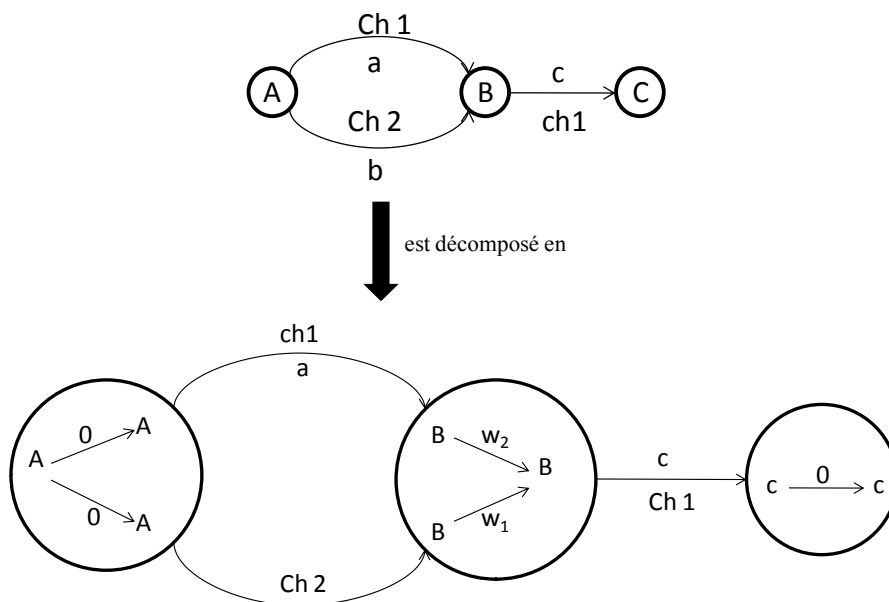


Fig.3.9: Décomposition isotonique de MIC

Calculons la métrique du chemin AC : $C(a+c)=C(a)+C(c)+w_2$ ou $C(b+c)= C(b)+ C(c)+w_1$. Si $C(a) < C(b)$ on ne peut pas conclure quand à la relation entre $C(a+c)$ et $C(b+c)$ à cause des termes w_1 et w_2 donc MIC n'est pas isotonique. Ils ont alors décomposé chaque nœud en trois nœuds virtuels et dépendant de l'interface sur laquelle on reçoit les données et sur lequel on les réachemine, on crée un lien virtuel. Si le canal est le même, le lien virtuel aura un coût w_2 , sinon w_1 .

Le nombre de nœuds interférents n'est pas une bonne estimation de l'interférence inter-flux car les nœuds dans le rayon d'interférence ont un impact différent selon leur distance, leur débit.

Les métriques *dépendantes de la topologie* sont, selon [30], plus stable que les métriques *sensibles à la charge* car les topologies des RMSF varient très peu mais elles ne peuvent pas souvent éviter les routes encombrées par le trafic.

MBP combine les deux, c'est une métrique dite *dépendante de la topologie* mais lorsqu'il y a un changement important qui cause beaucoup d'interférence le protocole cherche un chemin alternatif.

3.2 Protocoles de routage

Un protocole de routage est une politique de sélection de route entre chaque paire de nœuds dans le réseau. Le fonctionnement d'un protocole de routage peut être divisé en trois étapes : la découverte des nœuds voisins, le calcul de la métrique et le calcul des itinéraires optimums. La mise en place de protocoles de routage constitue un grand défi dans les RMSF, car ils permettent l'exploitation des réseaux en organisant le trafic. Ces protocoles peuvent être divisés en trois catégories : les protocoles de routage proactifs, réactifs et hybrides.

3.2.1 Protocoles de routage proactifs

Les nœuds dans RMSF qui implémentent les protocoles de routage proactifs maintiennent à jour une table de routage, de sorte que, lorsqu'une application désire envoyer des données, la route est immédiatement connue. Ces protocoles ont l'avantage de la disponibilité immédiate des routes vers tous les nœuds du réseau. Au niveau de la table de routage, chaque nœud stocke pour chaque destination, l'identité du nœud à contacter. La mise à jour de cette table de routage nécessite l'échange régulier de messages de contrôle, consommant une part non négligeable des ressources radio, même en l'absence de trafic. Comme dans les réseaux filaires, deux principales méthodes sont utilisées : le routage par état de lien et le routage par vecteur de distance.

Le routage par état de lien (à la source) consiste à diffuser périodiquement aux mobiles voisins l'état de la liaison qui les sépare. De cette façon, chaque nœud est capable de dresser une carte de l'état du réseau et par

conséquent de choisir la route la plus appropriée pour un message donné. Un des avantages de ce type de protocole est sa capacité à pouvoir facilement trouver des routes alternatives en cas de rupture de lien i.e Link Quality Source Routing (LQSR) [6], Optimized Link State Routing Protocol (OLSR) [2].

- *Le routage par vecteur de distance (hop by hop routing)* permet à chaque nœud de diffuser à ses voisins la distance qui les sépare (en nombre de sauts). Les seules informations conservées sont la liste des nœuds du réseau et l'identité du prochain nœud par lequel passer pour atteindre la destination i.e Destination-Sequenced Distance Vector (DSDV) [15].

L'inconvénient des protocoles proactifs réside dans le coût du maintien des informations de topologie et de routage même en cas d'absence de trafic de données ce qui implique une consommation continue de la bande passante. Comme exemples de protocoles de routage proactifs, nous pouvons citer OLSR [2] et DSDV [15].

3.2.2 Protocoles de routage réactifs

Les nœuds dans un RMSF qui implémentent les protocoles de routage réactifs restent inactifs tant qu'aucune application ne sollicite l'envoi de données. Ceci permet d'économiser de la bande passante. La procédure de découverte de route n'est enclenchée que lorsqu'un nœud souhaite envoyer des paquets vers un destinataire pour lequel aucune route n'est connue. Une demande de route explicite vers ce destinataire est alors propagée à travers le réseau. Cette inondation surcharge localement le réseau puisque tous les nœuds atteints doivent répéter la requête. Le principal avantage des protocoles de routage réactifs est de ne générer du trafic que si nécessaire mais cela implique une inondation du réseau coûteuse en ressources et une augmentation du délai du trafic. Nous pouvons citer Ad hoc On Demand Distance Vector (AODV) [14] et Dynamic Source Routing (DSR) [26] comme protocoles de routage réactifs.

3.2.3 Protocoles de routage hybrides

Les protocoles de routage hybrides combinent les approches proactive et réactive. Le principe est de connaître le voisinage de manière proactive jusqu'à une certaine distance (deux ou trois sauts par exemple), et lorsqu'une application cherche à envoyer des données à un nœud hors de cette zone, une recherche réactive est enclenchée. Une zone de routage est définie pour chaque nœud et inclut l'ensemble des nœuds qui sont à une distance inférieure à une valeur fixée représentant le rayon de routage. Grâce à cette combinaison, le réseau est partagé en plusieurs zones et la recherche de route en mode réactif est améliorée. À la réception d'une requête de recherche réactive, un nœud a la possibilité d'indiquer immédiatement si la destination est dans son voisinage ou non. ZRP [25] est le protocole hybride le plus connu, nous pouvons également citer Temporally-Ordered Routing Algorithm (TORA) [33] comme exemple.

Les protocoles de routage pour RMSF sont les mêmes que pour les MANets dans leur fonctionnement mais avec des métriques de routage différentes. Parmi ces protocoles, nous pouvons citer Load and Interference Balanced Routing Algorithm (LIBRA) qui est un protocole de routage proactif avec MIC (Metric of Interference and Channel-switching) comme métrique que nous avons présenté dans la section 3.1.4.7 ; LQSR est basé sur DSR, c'est donc un protocole réactif avec WCETT (Weighted Cumulative Expected Transmission Count) comme métrique.

3.2.4 Quelques exemples de protocoles de routage

Dans cette section, nous allons vous donner une description de quelques protocoles de routage proactif, réactif et hybride.

3.2.4.1 OLSR

OLSR (Optimized Link State Routing Protocol) [2] est un protocole de routage proactif destiné aux réseaux ad hoc qui est actuellement très utilisé dans les RMSF. OLSR fait partie de la classe des protocoles de routage par état des liens (à la source). Il utilise un mécanisme d'inondation optimisé qui permet de limiter l'émission de paquets de contrôle.

Avec OLSR, chaque nœud sélectionne parmi ses voisins immédiats (un saut) un ensemble de nœuds qui seront des relais multipoints (Multi-Points Relays MPRs) chargés de router ses paquets dans le réseau en cas de communication. Des paquets de contrôle sont périodiquement envoyés pour maintenir à jour les tables de routage. OLSR utilise deux types de paquets de contrôle, des messages "hello " et "TC " (Topology Control). Chaque nœud envoie périodiquement un "hello " contenant les informations sur son voisinage, les MPRs retransmettent ce "hello " ainsi les voisins sur deux sauts recevront le message. Le message "TC " nous donne les informations sur l'état des liens. Combiné aux messages "hello ", les nœuds peuvent calculer le coût des chemins vers tout le réseau.

Dans le cas de réseaux multiples-radios multiples-canaux, chaque nœud conserve en plus dans sa table de routage les informations sur les interfaces des autres nœuds du réseau. Ces informations s'échangent grâce à des messages "MID " (Multiples Interface Declaration). Notons que seuls les nœuds à plusieurs interfaces envoient des messages MID avec la liste des interfaces radios dont il dispose. Les messages MID sont aussi régulièrement mis à jour.

OLSR est un protocole de routage proactif et les routes sont mises à jour régulièrement, en cas de panne les nœuds ne recevront pas de paquets de contrôle de la part du nœud en panne et donc les routes changeront automatiquement en empruntant d'autres nœud du réseau.

3.2.4.2 DSDV

DSDV [15] est un protocole de routage proactif basé sur l'algorithme *Bellman-Ford* [22]. C'est un protocole de routage par vecteur de distance. Il a été proposé par Charles Perkins et Pravin Bhagwat en 1994. Avec ce protocole, chaque nœud maintient une table de routage qui répertorie toutes les destinations disponibles, le nombre de sauts ou la métrique de la route pour atteindre la destination et la séquence attribuée par le nœud destination. Le numéro de séquence est utilisé pour distinguer les anciennes routes obsolètes des nouvelles afin d'éviter les boucles. Les nœuds transmettent périodiquement ou lors d'un changement important, leurs tables de routage à leurs voisins immédiats. Les mises à jour des tables de routage peuvent être envoyées de manière *totale* ou *incrémentielle*. Lors d'une mise à jour *totale* le nœud envoie toute la table de routage à ses voisins et cela pourrait engendrer l'envoi de nombreux paquets alors que lors d'une mise à jour *incrémentielle*, seules les entrées de la table qui ont subi un changement de métrique sont envoyées et cela nécessite l'envoi de peu de paquets. Les mises à jour incrémentielles limitent l'envoi de paquets de contrôle et la surcharge du réseau. La Fig.3.10 donne un exemple de la table de routage d'un nœud A dans un réseau avec trois nœuds (A, B, C).

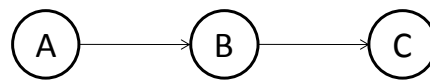


Table de routage du nœud A

Destination	Prochain saut	Nombre de sauts	Numero de sequence
A	A	0	3
B	B	1	2
C	B	2	5

Fig.3.10: Exemple de table de routage avec le protocole de routage DSDV

DSDV étant un protocole de routage proactif, il diffuse périodiquement des paquets de contrôle pour maintenir les tables de routage. Lorsqu'un nœud tombe en panne, il ne peut plus émettre ses paquets de contrôle. Par conséquent les autres nœuds ne recevront pas de paquets et si ils restent un certain temps sans recevoir de paquets de la part d'un nœud en panne, ils mettent la valeur de la métrique à l'infini ou un nombre assez élevé qui dépasse la limite autorisée par le protocole pour être sûr qu'elle ne sera pas choisie. Ensuite on incrémente le numéro de séquence. Enfin, les mises à jour périodiques trouveront une route alternative pour les routes qui passaient par le nœud en panne. Fig.3.11 nous donne une illustration d'un cas de panne avec DSDV. Considérons un réseau avec 6 nœuds (A, B, C, D, E et F), nous analyserons le comportement de la table de routage du nœud A. Le nœud B tombe en panne après. Les métriques des routes passant par B sont mises à l'infini jusqu'à ce que l'on trouve une route alternative.

(a) Réseau initial

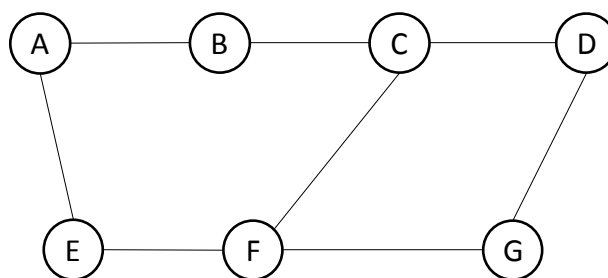


Table de routage du noeud A			
Destination	Prochain saut	Nombre de sauts	Numero de sequence
A	A	0	3
B	B	1	2
C	B	2	5
D	B	3	6
E	E	1	3
F	E	2	9

(b) Panne du nœud B

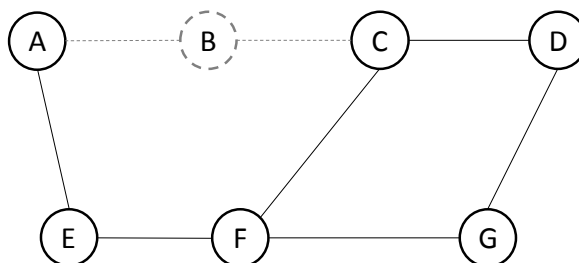


Table de routage du nœud A			
Destination	Prochain saut	Nombre de sauts	Numero de sequence
A	A	0	3
B	X	∞	3
C	X	∞	6
D	X	∞	7
E	E	1	3
F	E	2	9

(c) Établissement automatique de nouvelles routes

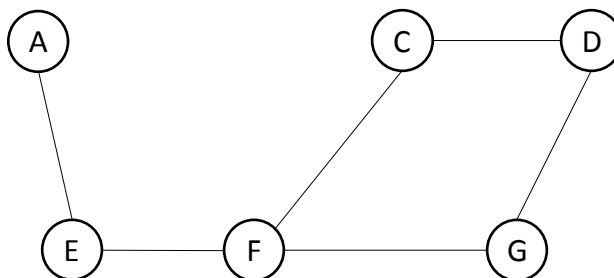


Table de routage du nœud A			
Destination	Prochain saut	Nombre de sauts	Numero de sequence
A	A	0	3
C	E	3	7
D	E	4	8
E	E	1	3
F	E	2	9

Fig.3.11: Illustration d'un cas de panne avec DSDV

DSDV convient aux réseaux de petite taille (inférieur à 10 nœuds) car chaque nœud stocke dans sa table les routes vers tous les nœuds du réseau. Quand

le nombre de nœuds dans le réseau est élevé, les tables de routage deviennent grandes. La taille des tables est de l'ordre de $O(n)$ ou n est le nombre de nœuds. Plus le nombre de nœuds est grand, plus les routeurs nécessiteront un large espace de stockage sachant que les routeurs ont des espaces mémoire limités.

Avec DSDV les nœuds conservent juste le prochain saut et non toute la route contrairement à OLSR qui conserve la route en entier et lui permet d'en changer facilement quand une route devient obsolète.

3.2.4.3 AODV

AODV [14] fait partie de la famille des protocoles réactifs. Lorsqu'une application désire trouver une route vers un destinataire, AODV inonde le réseau avec des paquets Route Request (RREQ). Le nœud source diffuse un RREQ sur tous les canaux disponibles et les nœuds qui reçoivent ce RREQ mettent à jour la route qui mène vers la source. Ces voisins à leur tour diffusent ce RREQ vers les autres nœuds. Chaque nœud traversé par un paquet de RREQ stocke des informations sur le numéro de séquence du paquet, l'adresse des nœuds source et destination ainsi que l'adresse du nœud précédent. Lorsque ces paquets RREQ arrivent à la destination, un paquet de réponse Route Reply (RREP) est envoyé suivant le chemin inverse vers le nœud émetteur (voir Fig.3.12).

La Fig.3.12 donne un exemple de recherche de route dans un réseau avec AODV. Le nœud *Source* veut envoyer du trafic au nœud *Dest*. Il génère un paquet RREQ qu'il diffuse à ses voisins A et B. Ces deux nœuds à leur tour retransmettent le RREQ à leurs voisins. Ce paquet permet, au niveau de chaque nœud, de mettre à jour le saut suivant pour la route construite vers la *Source*. À chaque saut, le nœud calcule le nombre de sauts depuis la *Source*. Le RREQ arrive au niveau au nœud *Dest* qui voit qu'il est le nœud destination, il génère alors un paquet RREP qui fait le chemin inverse et informe le nœud source du chemin à prendre.

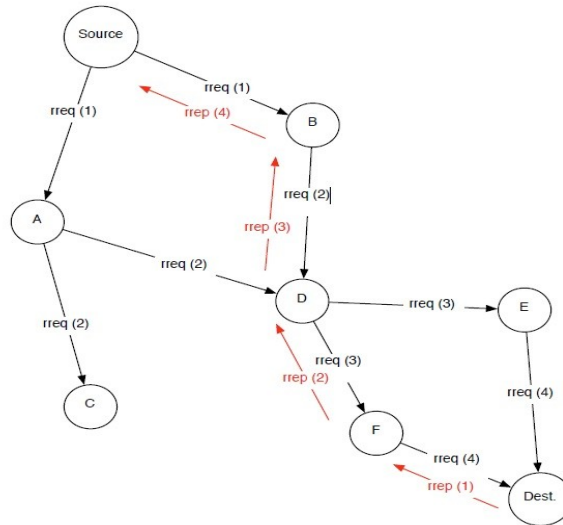


Fig.3.12: Recherche de route dans AODV

Dans cet exemple, la métrique est le nombre de sauts avec un poids de 1 pour chaque lien mais on aurait pu affecter des poids différents tels qu'ETX, ETT vus dans la section 3.1.4. Le problème revient à trouver le plus court chemin dans un réseau.

AODV diffuse périodiquement des messages Hello à ses voisins pour vérifier l'état des liens. Si un nœud reste pendant une période sans recevoir de paquets Hello de la part d'un de ses voisins, et que les paquets Hello qu'il envoie vers cette destination sont perdus, il considère que le lien est tombé en panne et entame une nouvelle procédure de recherche de route pour toutes les routes qui passaient par ce lien.

3.2.4.4 TORA

TORA [33] est un protocole de routage hybride pour les réseaux multiples-sauts. L'établissement et la maintenance des routes se fait en même temps de manière réactive et proactive. Pour l'approche réactive, la source procède à une

recherche de route à la demande comme pour un protocole de routage réactif. En effet il n'est pas nécessaire de conserver les routes vers toutes les destinations. D'un autre côté, les nœuds maintiennent de manière proactive les routes vers certaines destinations qui sont généralement très sollicitées telles que les passerelles, les serveurs, les points d'accès etc. De ce fait les messages de contrôle ne seront échangés périodiquement que pour un nombre réduit de nœuds dans le réseau ce qui aide à réduire la surcharge du réseau comparé aux protocoles de routage proactifs.

La découverte et la maintenance de route sont basées sur la création d'un graphe acyclique orienté entre la source et la destination. Si un des liens du graphe devient défaillant, le concept d'inversion de liens permet de rétablir le graphe localement.

Le but de TORA est de trouver des routes stables qui puissent être réparées rapidement et localement. Il ne cherche pas en priorité à trouver les routes optimales ou les plus courts chemins. Il conserve plusieurs routes vers la même destination afin d'éviter de déployer le mécanisme de découverte de route trop fréquemment.

3.3 Synthèse de l'état de l'art

La métrique basé sur le nombre de saut ignore les paramètres tels que l'interférence et la qualité des liens [5] néanmoins elle reste très utilisée par des protocoles comme AODV à cause de sa simplicité. Elle est facile à implémenter, et isotonique donc fonctionne avec les protocoles proactifs tels qu'OLSR. ETX estime la qualité des liens en envoyant périodiquement des paquets de contrôle sans considérer la capacité des liens (bande passante disponible). ETT a donc été proposé comme une extension d'ETX, elle prend en compte la capacité des liens et la charge du réseau.

Dans un environnement multiples-radios et multiples-canaux, WCETT améliore ETT en favorisant la diversité des canaux et réduit ainsi l'effet de l'interférence intra-flux. Les principales limitations de WCETT sont (1) il considère que deux liens sur le même chemin opérant sur le même canal s'interfère. Cette supposition est erronée car les liens peuvent ne pas être dans le rayon d'interférence l'un de l'autre. (2) WCETT ne prend pas en considération les interférences inter-flux.

iAWARE fonctionne sur le même principe que WCETT en intégrant l'effet de l'interférence inter-flux. WCETT et iAWARE ne sont pas isotoniques, de ce fait il n'existe aucun algorithme efficace qui peut trouver le meilleur chemin. MIC a été proposé, son point fort est qu'il possède une décomposition isotonique mais assez complexe à mettre en place.

MIC estime l'interférence inter-flux par le nombre de nœuds interférant sans prendre en compte le fait que les nœuds ont des impacts différents. L'interférence intra-flux n'est capturée que sur deux sauts. La Table 1 donne un résumé des caractéristiques des différentes métriques présentées.

	Nombre de saut	ETX	ETT	WCETT	iAWARE	MIC
Interférences Intra-flux	V	F	F	V	V	V
Interférences inter-flux	F	V	V	V	V	V
Isotonicité	V	V	V	F	F	V
Charge	F	F	V	V	V	V

Table 1 : Caractéristiques des métriques

Chapitre 4: MBP une nouvelle métrique de routage pour RMSF

Dans ce chapitre, nous allons décrire une nouvelle métrique pour RMSF appelé Metric Based on Probabilities (MBP). Les contributions majeures de cette nouvelle métrique sont que, premièrement, elle prend en compte le taux de perte et les interférences de type inter-flux et intra-flux; elle contourne le problème de l'asymétrie ; ensuite, comme la qualité des liens peut changer au cours du temps, nous avons rajouté un système de surveillance, quand un lien se dégrade sévèrement, MBP corrige les routes passant par ce lien pour éviter qu'il constitue un goulot d'étranglement. Enfin, ce travail permet de tester avec les probabilités une méthode de calcul de métrique multiplicative car toutes celles que nous avons étudiées jusqu'à présent sont additives sauf ML [27]. Mais ML est une métrique pour un RMSF avec un seul canal et ne prend pas en compte les interférences. MBP se base sur la métrique ML décrite dans le chapitre précédent pour, comme son nom l'indique, calculer les probabilités de réussite de transmission sur les liens et les chemins. Ce calcul de probabilité se fait sur la base de l'interférence inter-flux et intra-flux et du taux de perte sur les liens.

4.1 Description de MBP

MBP assigne des probabilités de réussite à chaque lien dans le réseau. Chaque nœud, à l'aide de ML, calcule les taux de réussite des liens avec ses nœuds voisins. Pour palier au problème de l'asymétrie, on considère uniquement le taux de réussite à l'avant et on s'assure que le chemin retour est actif quand on reçoit au moins un paquet sur les liens bidirectionnels. $ML_l = d_f$.

Pour calculer les taux de réussite d_f sur les liens, on utilise la méthode de diffusion de paquet décrite par Couto et al. dans [4]. En résumé, chaque routeur envoie périodiquement (une fois par seconde) à ses voisins un paquet de contrôle. Les nœuds comptent le nombre de paquets reçus (N_r) durant un

intervalle de temps (dix secondes) et fait le rapport entre le nombre de paquets reçus et le nombre de paquets envoyés. Notons que les paquets de contrôle ne sont pas retransmis en cas d'échec. Et donc :

$$d_f = \frac{N_r}{N_s}$$

où N_r est le nombre de paquet reçus, N_s est le nombre de paquets envoyés ou qu'on aurait dû recevoir (10 dans notre cas). Notons que d_f est une valeur comprise entre 0 et 1.

MBP est une métrique *dépendante de la topologie*. MBP-AODV adopte une approche proactive pour le calcul et la mise à jour des métriques et une approche réactive pour la recherche de routes.

4.1.1 Interférence inter-flux

Nous utilisons le model physique présenté dans [7]. Ce modèle indique qu'une transmission de u vers v est réussie si le SINR est supérieur à un seuil prédéfini.

$$\frac{P_v(u)}{N + \sum_{k \in v'} P_v(k)} \geq SINR_thresh \quad (16)$$

où N est le bruit, $P_v(u)$ est la puissance de réception de u vers v , v' est l'ensemble des nœuds interférents et $\sum_{k \in v'} P_v(k)$ est cumul des bruits causés par les nœuds interférents.

L'interférence inter-flux est causée par du trafic externe opérant sur le même canal. Cette interférence réduit la puissance de réception des paquets qui peuvent être perdus si la puissance devient inférieure au seuil. Nous allons considérer I_{max} comme la puissance interférente maximum tolérable pour que le paquet soit transmis. De (16) on peut en déduire que :

$$I_{\max} = \frac{P_v(u)}{SINR_thresh} \quad (17)$$

Nous allons définir le ratio d'interférence (IR) sur le lien (u, v) comme suit :

$$IR(u, v) = \frac{\sum_{k \in v'} P_v(k)}{I_{\max}} \quad (18)$$

$\sum_{k \in v'} P_v(k)$ est la puissance interférente sur le canal et I_{\max} la puissance interférente maximum tolérable. IR peut être vu comme le taux d'occupation du canal. Notons que $0 \leq IR \leq 1$, si $IR=0$ alors la puissance interférente $\sum_{k \in v'} P_v(k)$ est nulle donc le canal est libre sinon si $IR=1$, le canal est totalement occupé. L' IR est calculé de manière passive en utilisant le trafic actuel et est mise à jour périodiquement (chaque deux secondes). Le calcul ne nécessite aucun paquet de contrôle supplémentaire.

4.1.2 MBP pour un lien

La qualité du lien (u, v) est défini comme la probabilité pour qu'un paquet soit transmis sur ce lien. Elle combine le ML et l' IR :

$$MBP(u, v) = ML_{uv} \times (1 - IR(u, v)) \quad (19)$$

Par opposition à la plupart des métriques, dans notre cas plus le lien est bon, plus la probabilité de réussite de la transmission sur ce lien est élevée.

4.1.3 Interférence intra-flux et MBP pour un chemin

Pour un chemin composé de plusieurs liens, la valeur de MBP sera le produit des MBPs des liens. Si deux liens adjacents partagent le même canal, la valeur de MBP est divisée par deux pour éviter l'effet de l'interférence intra-flux. En théorie, si deux liens consécutifs partagent le même canal, la bande passante du chemin est divisée par deux.

$$MBP(p) = \begin{cases} \prod_{l \in p} MBP_l & \text{if } ch(prev(i)) \neq ch(i) \\ \frac{1}{2} \prod_{l \in p} MBP_l & \text{if } ch(prev(i)) = ch(i) \end{cases} \quad (20)$$

MBP n'est pas isotonique et fonctionne avec des protocoles réactifs. MBP est une nouvelle métrique de routage qui utilise ML et l'IR pour calculer la qualité des liens. Pendant la découverte des routes, il prend en compte l'interférence intra-flux en pénalisant les chemins qui utilisent le même canal sur des liens consécutifs.

4.1.4 MBP-AODV le protocole de routage associé

Nous avons implémenté et testé notre nouvelle métrique avec le protocole de routage AODV [14]. MBP-AODV est un protocole de routage réactif mais elle mesure la qualité des liens de manière proactive en injectant périodiquement des paquets de contrôle. De plus, nous avons rajouté un système de surveillance de la qualité des liens.

Par défaut, AODV utilise le nombre de sauts comme métrique, nous avons modifié le protocole en changeant la métrique par MBP. Dans le RREQ nous ajoutons un champ où on stocke la valeur de MBP qui est mise à jour à chaque saut. Après avoir trouvé la meilleure route (avec la plus grande probabilité de réussite), AODV la maintient tant que cette dernière est active. Lorsqu'une route se n'est plus valide, AODV enclenche une nouvelle procédure de recherche de route pendant ce temps les paquets sont stockés dans la file d'attente ce qui augmente le délai de transmission et peut causer des pertes lorsque les files sont pleines.

4.1.5 Surveillance de la qualité des liens

AODV est un protocole de routage réactif qui maintient les routes jusqu'à ce qu'elles ne soient plus actives. Cependant une route peut rester active, mais sa

qualité peut se dégrader pour diverses raisons telles que l'interférence, la surcharge des liens, un goulot d'étranglement... AODV attend jusqu'à ce que la route ne soit plus fonctionnelle avant d'envoyer une nouvelle demande de route (RREQ) pour trouver un autre chemin.

Une de nos contributions majeures est que nous avons rajouté un système de surveillance de la qualité des liens pour prévenir la défaillance des routes. Les RMSF sont caractérisés par leur mobilité réduite et leur forte connectivité par conséquent les ruptures au niveau des routes sont principalement dues aux interférences. Ainsi, nous avons rajouté un système de surveillance d'interférence, quand la probabilité de réussite sur un lien diminue jusqu'à atteindre un certain seuil appelé th , MBP-AODV enclenche une nouvelle procédure de recherche de route. Si une meilleure route est découverte, le trafic est redirigé sur ce nouveau chemin. Nous avons fait varier ce seuil en lui affectant différentes valeurs (ex : $th=0,4$; $th=0,5$; $th=0,6...$). L'exemple de Fig.4.1 illustre notre mécanisme de surveillance de qualité. On souhaite envoyer du trafic entre les nœuds S et D. À l'instant t , la meilleure route trouvée est S-B-G-F-D. Mais après un laps de temps, on remarque que le lien G-F s'est dégradé alors on prévient la source S qui enclenche une nouvelle procédure de recherche de route. Le trafic continue d'emprunter le même chemin jusqu'à ce qu'une nouvelle route soit trouvée. Ensuite, le trafic est réacheminé sur la nouvelle route.

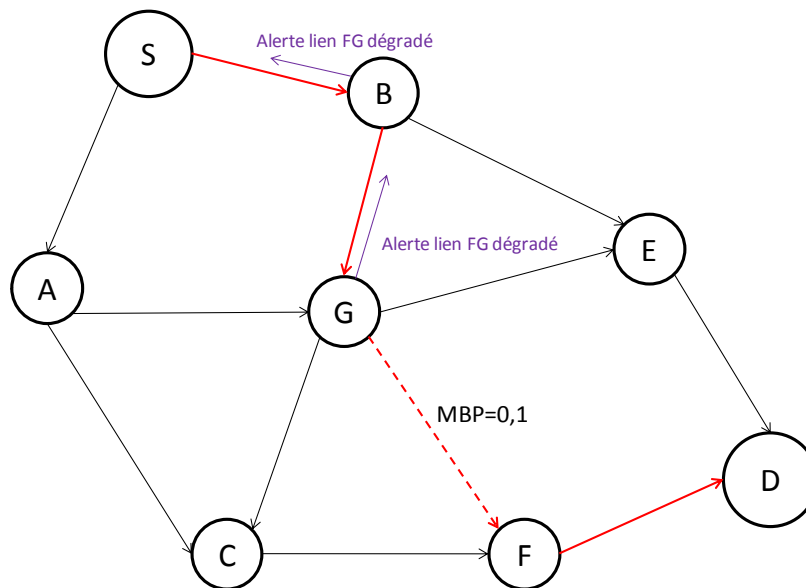


Fig.4.1: Exemple surveillance de la qualité des liens

Il s'agit là d'anticiper les éventuelles ruptures au niveau des routes et les conséquences qu'elles peuvent entraîner notamment l'augmentation du délai de transmission et la perte des paquets au niveau des files d'attentes.

Avec cette technique, on remarque une réduction des délais de transmission et on évite de longues files d'attente au niveau des routeurs qui peuvent entraîner des pertes. Les simulations présentées dans le chapitre suivant nous donnent une meilleure vision de l'amélioration apportée de notre protocole.

Chapitre 5: Évaluation des performances de MBP

Nous présentons dans ce chapitre les performances de notre protocole de routage MBP pour les RMSF. Nous effectuerons nos tests sur un réseau maillé où tous les nœuds utilisent une interface radio et un canal d'une part, puis sur un réseau multiples-radios multiples-canaux d'autre part. Nos tests ont été effectués avec le simulateur de réseau NS2 [21]. Nous comparons les performances de MBP avec d'autres métriques que nous avons décrites dans le chapitre 3. Nous avons implémenté les métriques ETT, WCETT et iAWARE avec le protocole de routage AODV. Ensuite nous avons simulé des réseaux maillés et généré du trafic. Nous avons étudié le comportement et les performances de chacune des métriques susmentionnées en calculant débit, le délai, le taux de perte, le taux d'efficacité normalisé et le nombre de paquets de contrôle générés.

5.1 Environnement de travail : le simulateur NS2

NS2 (Network Simulator) [21] est un simulateur de réseaux à événements discrets développé dans un but de recherche. NS2 prend en entrée un fichier TCL (Tools Command Language) qui contient toutes les informations sur le réseau, il décrit les conditions de la simulation et fixe les valeurs de certains paramètres tels que les positions des nœuds, les caractéristiques des liens physiques, les protocoles utilisés, les communications qui ont lieu, etc. Les protocoles sont codés avec le langage C++. La simulation doit d'abord être saisie sous forme de fichier texte que NS va utiliser pour produire un fichier trace contenant les événements qui se sont déroulés durant la simulation à chaque instant.

À la base NS2 ne supporte pas les RMSF vu ses particularités mais par la suite nous avons modifié la version de base de NS afin de pouvoir simuler des réseaux maillés multiples-radios et multiples-interfaces. Plus particulièrement, nous avons

utilisé la version NS2.33 que nous avons améliorée grâce à [23]. Cette amélioration consiste en un ensemble de modifications à effectuer sur des fichiers de TCL et C++ de NS2. Elle vise à, d'un côté, augmenter le nombre d'interfaces radios par routeur et que chaque interface radio puisse communiquer sur plusieurs canaux différents. D'un autre côté, mettre à niveau le protocole de routage (AODV dans notre cas) pour pouvoir router du trafic sur les multiples interfaces disponibles.

5.2 Conditions de simulation

Toutes les simulations ont été faites sous NS2 avec des topologies en grilles ou aléatoires. Nous utilisons la couche physique WirelessPhyExt [24] et la couche MAC 802.11Ext associée. Cette dernière est basée sur le SINR qui permet de capturer l'interférence au niveau de la couche physique pour calculer l'IR. On utilise le modèle de propagation Nakagami qui est le modèle associé aux couches MAC et physique. Le protocole de transport utilisé pour toutes les simulations est UDP (User Datagram Protocol) avec du trafic CBR (Constant Bit Rate). La taille des paquets est de 1000 octets, le rayon de transmission est de 250 mètres alors que le rayon d'interférence est de 550m. Comme nous utilisons la norme IEEE 802.11b, le nombre de canaux orthogonaux disponibles sera de 3. La taille de la grille est de $1000m \times 1000m$ et on fait varier le nombre de nœuds dans cette grille pour varier la densité. Chaque simulation dure 100 secondes. Afin de produire des résultats fiables nous avons exécuté les simulations 100 fois puis nous avons pris leurs moyennes. La valeur du paramètre β pour les métriques WCETT et iAWARE est fixée à 0,5 comme dans [18]. Table 2 présente un récapitulatif des paramètres de simulations.

Paramètres	Valeurs
Protocole de routage	AODV
Protocole MAC	IEEE 802.11b
Taille des paquets	1000 octets
Modèle de propagation	Nakagami
Modèle physique	WirelessPhyExt
Type de trafic	CBR
Rayon de transmission (r)	250m
Rayon d'interférence (R)	550m

Table 2 : Paramètres de simulation

5.3 Métriques de performance

Pour comparer les performances des différentes métriques de routage à celle que nous avons proposé, nous avons besoin de critères de comparaison. Ces critères sont des métriques de performance. Les métriques de performance varient selon les critères recherchés par le protocole de routage. Dans notre cas, nous cherchons à maximiser les débits, réduire les délais du trafic dans le réseau et limiter la surcharge due aux paquets de contrôle. Nous utiliserons le débit du réseau, le délai, le taux de perte, le taux d'efficacité normalisée (normalized effectiveness ratio) et le surdébit de routage (routing overhead) comme métriques de performance.

5.3.1 Le débit du réseau

Il est défini comme étant le nombre total de bits de données reçus par toutes les destinations par unité de temps (bits/seconde).

5.3.2 Le délai moyen point-à-point

Le délai point-à-point d'un paquet représente le temps total que met le paquet pour aller de la source vers la destination. Après avoir mesuré le délai de chaque paquet, nous faisons la moyenne pour en déduire le délai moyen point-à-point.

5.3.3 Le taux de perte

C'est le rapport entre le nombre de paquets perdus et le nombre de paquets envoyés par la source. Le taux de perte est une valeur comprise entre 0 et 1.

5.3.4 Le surdébit de routage (Routing Overhead)

Le surdébit de routage [17] représente la taille totale des paquets de contrôle (RREQ, RREP, (Route Error) RERR) générés par le protocole de routage.

5.3.5 Le Taux d'Efficacité Normalisé (Normalized Effectiveness Ratio)

Le taux d'efficacité normalisé (TEN) [17] estime le nombre de paquets de contrôle utilisés par paquets de données reçues. Cette métrique mesure l'efficacité du protocole de routage. Le taux d'efficacité normalisé prend en considération non seulement le taux de perte, mais aussi le surdébit de routage dû aux paquets de contrôle. TEN est donné par la formule suivante :

$$TEN = \frac{\text{Taille paquets bien reçu} - \text{Taille paquets de contrôle nécessaire}}{\text{Taille paquets envoyés}} \quad (21)$$

La valeur du taux d'efficacité normalisé est comprise entre 0 et 1. La valeur maximale de 1 est atteinte lorsque tous les paquets sont reçus sans générer de paquets de contrôle, c'est le cas idéal. Dans le cas contraire, le taux d'efficacité

normalisé tend vers 0 lorsque le taux de perte est élevé (i.e. *Nb paquets reçus* faible) et/ou le nombre de paquets de contrôle est grand (i.e. *Nb paquets de contrôle nécessaire* élevé).

5.4 Résultats de simulation

On utilise deux types de topologie, une topologie en grille et une aléatoire; dans les deux cas les tests sont effectués sur des RMSF opérant sur un ou plusieurs canaux.

5.4.1 Premier scénario : topologie en grille

Dans cette première partie des simulations, on utilise une topologie en grille, avec 25 nœuds (grille de 5×5). Les nœuds sont uniformément répartis sur une surface de $1000m \times 1000m$ divisée en cellule de $200m \times 200m$ et on place un nœud par cellule. On démarre alors successivement 5 flux entre 5 sources et 5 destinations. Le but est d'étudier l'impact des flux sur les autres les changements de routes, les collisions etc. La Fig.5.1 représente le réseau grille utilisé lors des simulations.

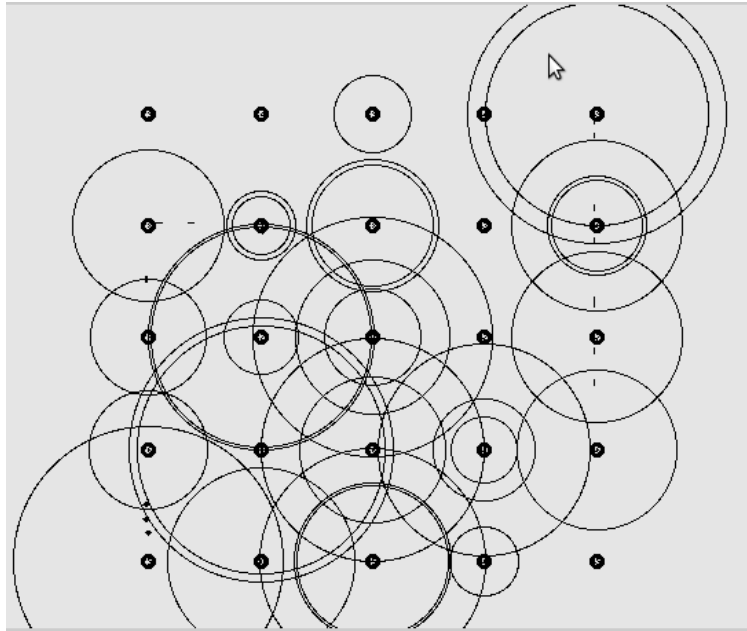


Fig.5.1: Topologie en grille

5.4.1.1 Topologie grille à un seul canal

Dans un premier temps, nous travaillons avec un RMSF où chaque routeur opère sur une seule interface et un seul canal. Les résultats donnent les débits, les délais moyens, le taux de perte, le taux d'efficacité normalisé et le surdébit de routage du protocole de routage AODV avec ETT, iAWARE et MBP comme métrique de routage.

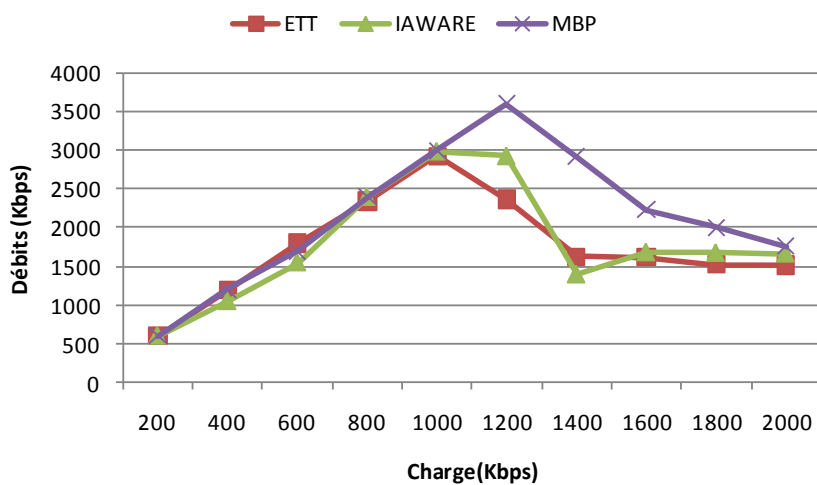


Fig.5.2: Débits du réseau pour une topologie en grille avec un canal

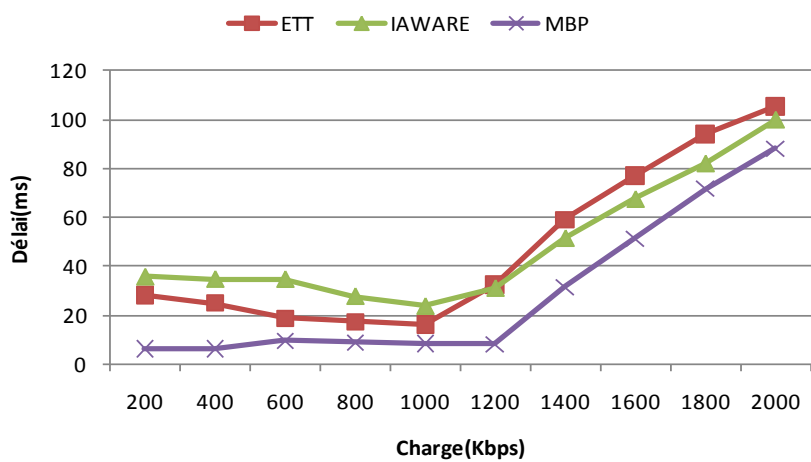


Fig.5.3: Délais moyens pour une topologie en grille avec un canal

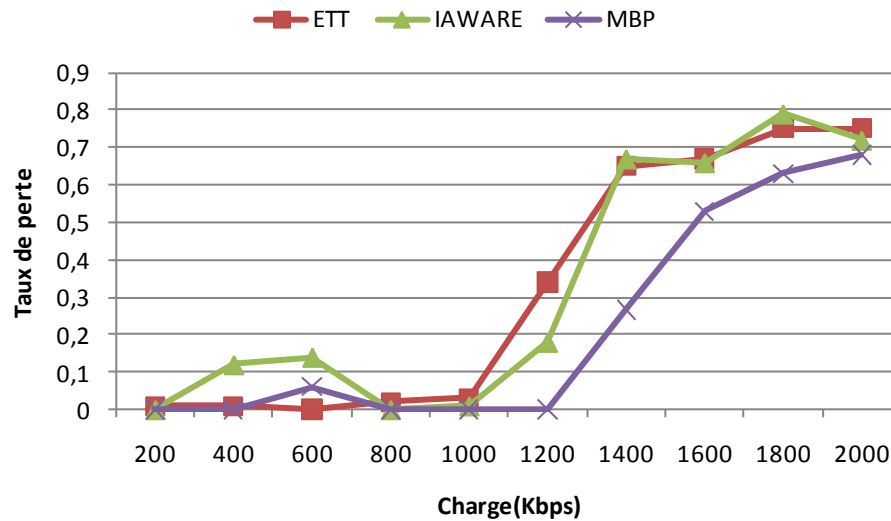


Fig.5.4: Taux de perte pour une topologie en grille avec un canal

Les Fig.5.2, Fig.5.3 et Fig.5.4 nous donnent les performances pour le réseau en grille avec un seul canal. Sur la Fig.5.2, on peut voir que pour des charges inférieures à 1000 Kbps, les trois métriques ont pratiquement les mêmes débits. À partir de ce point, le débit des trois métriques commence à diminuer car elles ont atteint le débit dit de *saturation*. Dans la Fig.5.2, on remarque que MBP réagit mieux aux charges élevées. MBP présente de meilleurs débits qu'ETT et iAWARE. Notons que dans le réseau à un seul canal, on ne prend pas en compte l'interférence intra-flux vu que tous les liens partagent le même canal. MBP et iAWARE prennent en considération l'interférence inter-flux et ainsi ils peuvent éviter les routes à fortes interférence ce qui améliore leurs débits par rapport à ETT.

Au niveau du délai, la Fig.5.3 montre que MBP offre de plus faibles délais qu'ETT et iAWARE. On peut aussi voir que les délais d'ETT et de iAWARE dépassent 20 ms tandis que ceux de MBP ne dépassent pas les 10 ms pour des charges comprises entre 200 et 1000 Kbps. À partir de 1200 Kbps les délais des trois protocoles subissent une augmentation. Néanmoins, MBP offre de meilleurs délais grâce à son système de surveillance du taux d'interférence qui met à jour

les routes à fortes interférence qui peut dégrader les performances des protocoles de routage. Les interférences empêchent l'acheminement normal des paquets. En effet, quand un lien subit une forte interférence, il ne peut plus communiquer correctement, les paquets sont alors stockés dans les files d'attente des nœuds jusqu'à ce que le lien se libère ou le délai du temporisateur relatif aux files d'attente expire, ce qui peut considérablement augmenter les délais. Quand les files d'attente sont pleines et/ou le délai du temporisateur expire, les paquets sont éliminés ce qui augmente le taux de perte.

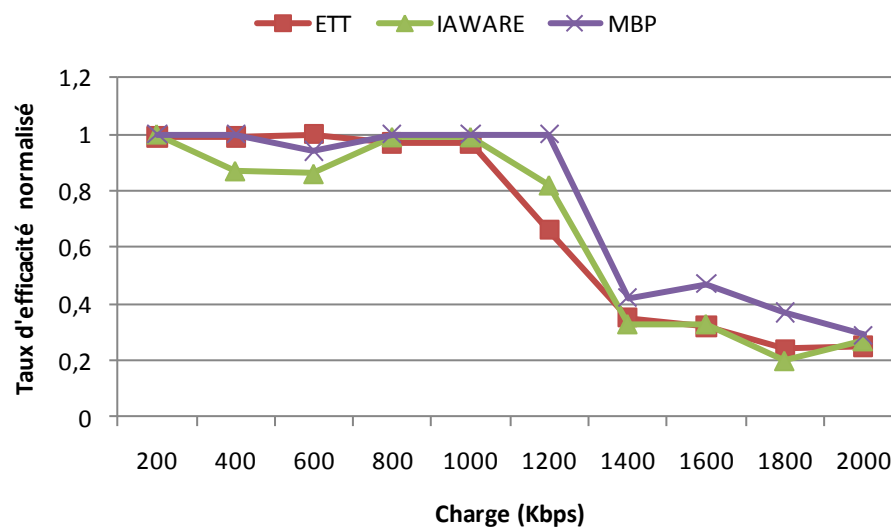


Fig.5.5: Taux d'efficacité normalisé pour une topologie en grille avec un canal

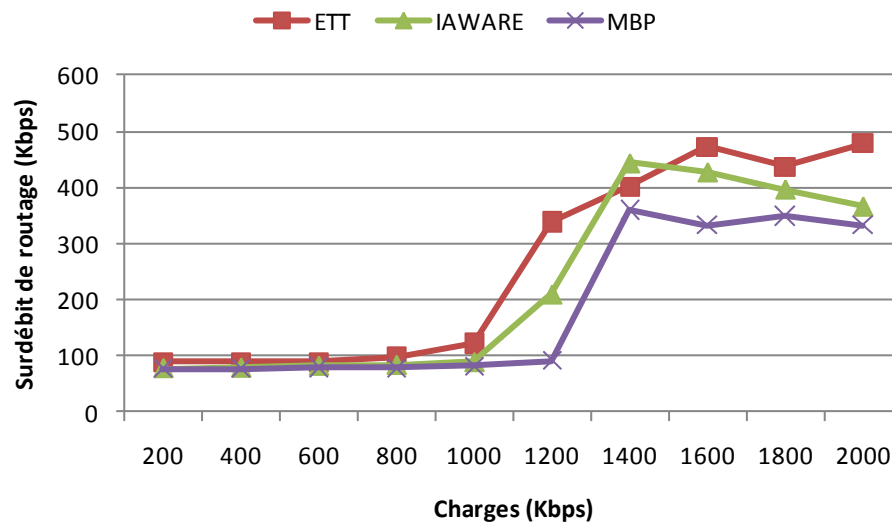


Fig.5.6: Surdébits de routage pour une topologie en grille avec un canal

Les Fig.5.5 et Fig.5.6 nous donnent respectivement le taux d'efficacité normalisé et le surdébit de routage des trois métriques pour le réseau grille un seul canal. On constate que pour des charges de 200 à 1000 Kbps les performances sont pratiquement les mêmes tandis qu'à partir de 1200 Kbps, on voit nettement que MBP surpasse les autres métriques. Le taux d'efficacité normalisé de MBP est plus élevé que celui de ETT et iAWARE. MBP occasionne moins de perte (Fig.5.4) et donc on aura plus de paquets reçus ce qui améliore le taux d'efficacité normalisé selon l'équation (21). En moyenne MBP serait 10% plus efficace qu'ETT et iAWARE.

On remarque aussi que MBP engendre moins de surdébit de routage qu'ETT et iAWARE. En effet, à l'instar de ETT et iAWARE, MBP envoie périodiquement des paquets de contrôle pour mettre à jour les routes mais son système de surveillance d'IR prévient la rupture des routes en stockant des routes alternatives pour éviter l'envoi inutile de nouveaux RREQ.

5.4.1.2 Topologie grille avec multiples-canaux

Dans un second temps nous considérerons un réseau multiples-radios multiples-canaux avec trois canaux orthogonaux.

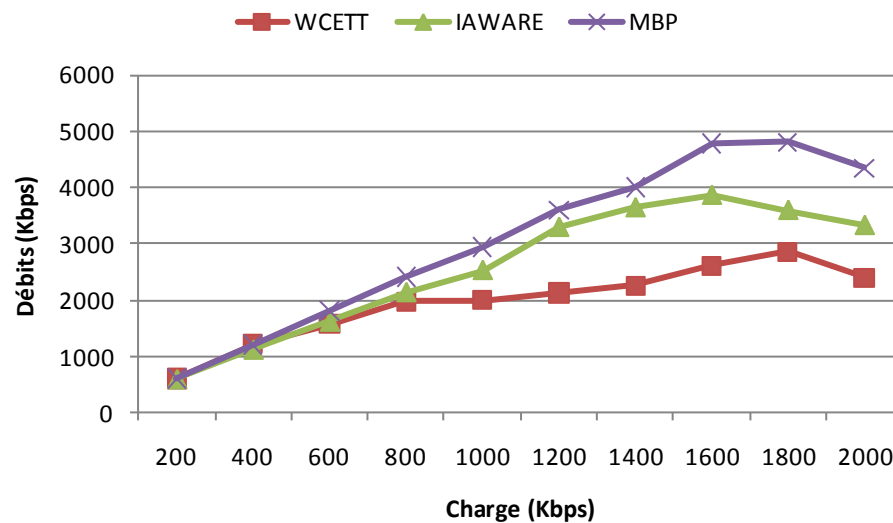


Fig.5.7: Débits du réseau pour une topologie en grille avec multiples-canaux

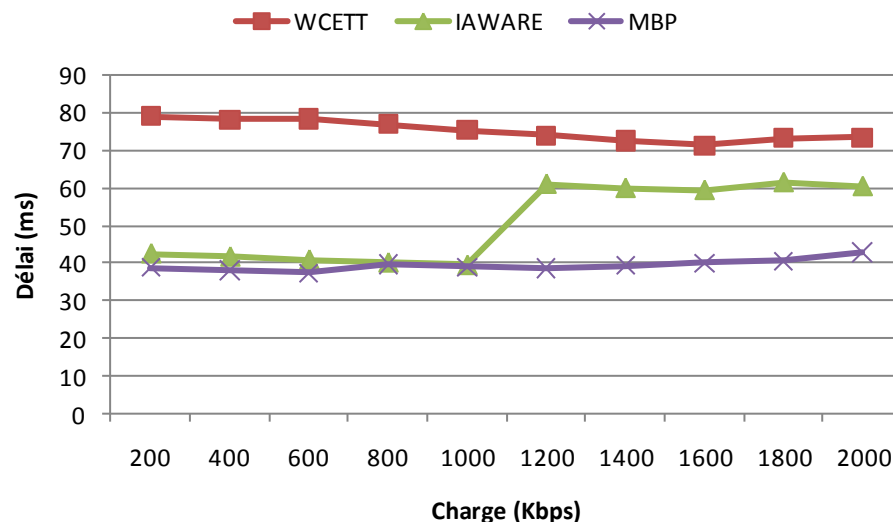


Fig.5.8: Délais pour une topologie en grille avec multiples-canaux

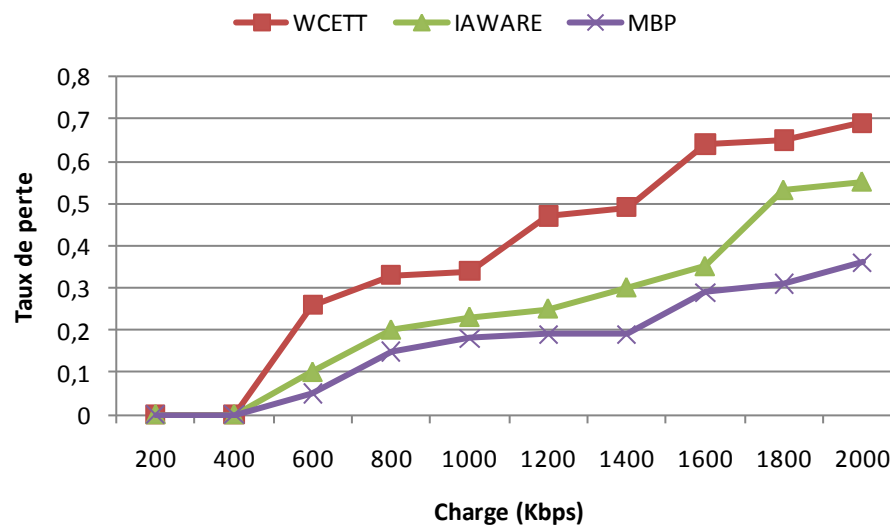


Fig.5.9: Taux de perte pour une topologie en grille avec multiples-canaux

AODV maintient les routes tant qu'elles sont valides. Il se peut que la qualité des routes se dégrade en cours d'utilisation. C'est pour cela que MBP vérifie régulièrement l'IR des routes et quand il atteint un seuil, fixé à 0.5 dans nos simulations, on lance une nouvelle requête pour trouver une meilleure route et procéder au changement de route.

Les Fig.5.7, Fig.5.8 et Fig.5.9 représentent respectivement le débit, le délai et le taux de perte de WCETT, iAWARE et MBP dans un RMSF avec une topologie grille multiples-canaux. À première vue, les débits sont plus grands pour le réseau multiples-canaux que pour le réseau à un seul canal vu dans la section précédente. Fig.5.7 montre que MBP obtient de meilleurs débits que WCETT et iAWARE avec une plus nette amélioration pour des charges élevées (1600 Kbps).

Au niveau des délais, WCETT a de plus grands délais. La principale raison c'est que WCETT ne prend pas en compte l'interférence inter-flux lors de la sélection des routes. Les routes à forte interférence peuvent occasionner de longues attentes au niveau des files d'attente des routeurs ce qui peut se répercuter négativement sur les délais des paquets. Le fait que WCETT et iAWARE

prennent en compte l'interférence intra-flux sur tous les liens d'un chemin fausse son estimation. En effet dans notre topologie grille avec 25 nœuds, les routes sont de 5 sauts (1000m) au minimum et les liens n'interfèrent plus au delà de 3 sauts (600m) vu que le rayon d'interférence est de 550m. MBP a les mêmes délais qu'iAWARE pour des charges de 200 à 1000 Kbps, mais à partir de 1200 Kbps, les délais d'iAWARE augmentent de 20ms tandis que ceux de MBP restent stables.

On peut aussi voir sur Fig.5.9 que MBP occasionne moins de perte que les autres métriques. WCETT atteint 70% de perte tandis iAWARE et MBP ont moins de perte. Particulièrement MBP ne dépasse pas 40% de perte.

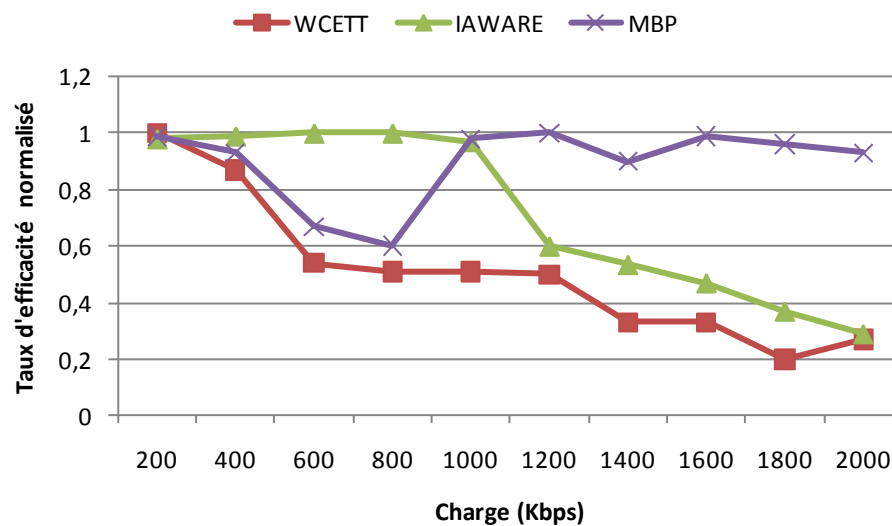


Fig.5.10: Taux d'efficacité normalisé pour une topologie en grille à multiples-canaux

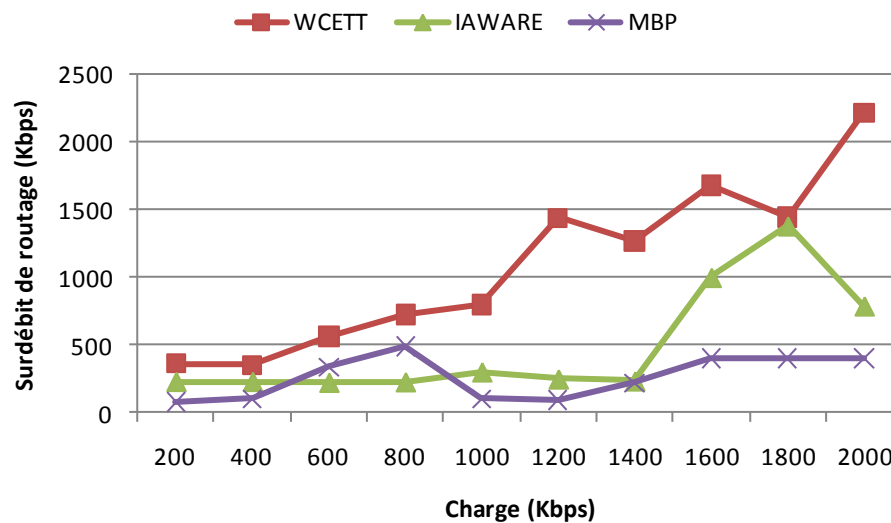


Fig.5.11: Surdébits de routage pour une topologie en grille à multiples-canaux

On voit sur la Fig.5.10 que de 200 à 1000 Kbps de charge, iAWARE est plus efficace que MBP et WCETT. Ceci s'explique par le fait que MBP génère plus de paquets de contrôle lorsque la qualité des routes est dégradée. Cependant, pour des charges relativement basses, l'interférence n'entraîne pas forcément des ruptures de route. De ce fait, ces paquets de contrôle supplémentaires sont inutiles. Par contre, pour des charges plus élevées, les ruptures des routes sont plus fréquentes et l'anticipation de ces ruptures améliore l'efficacité de MBP par rapport à WCETT et iAWARE. Pour des charges plus élevées, à partir de 1200 Kbps, MBP devient plus efficace que WCETT et iAWARE. On remarque aussi que MBP génère moins de paquets de contrôle, il ne dépasse pas les 500 Kbps tandis qu'iAWARE atteint 1500 Kbps et WCETT atteint 2000 Kbps. MBP limite considérablement la surcharge des paquets de contrôle par rapport à WCETT et iAWARE. MBP, dans son choix de route, prend en considération plusieurs facteurs : le taux de perte, l'interférence inter-flux et intra-flux ce qui permet aux différents trafics d'emprunter des routes avec une certaine qualité de service. Ce

qui améliore les performances de MBP par rapport à WCETT et iAWARE. De plus, en choisissant ce type de routes, on évite considérablement les ruptures qui entraînent de nouvelles requêtes qui peuvent augmenter le nombre de paquets de contrôle.

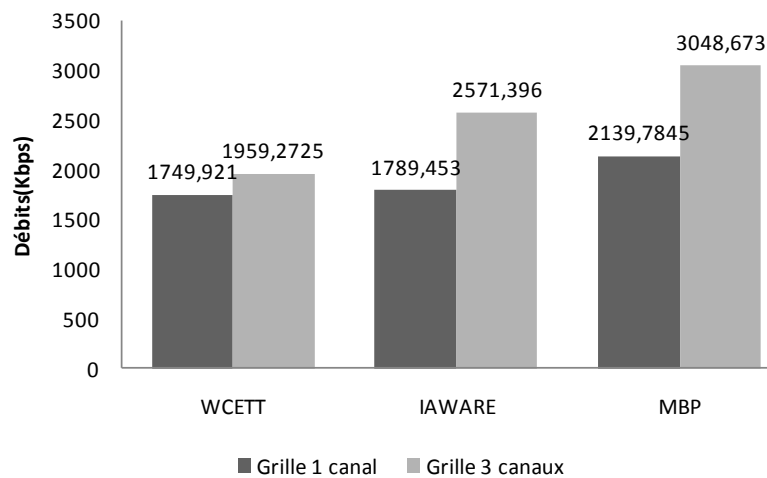


Fig.5.12: Comparaison des débits pour une topologie grille à un seul canal et une topologie grille à multiples-canaux

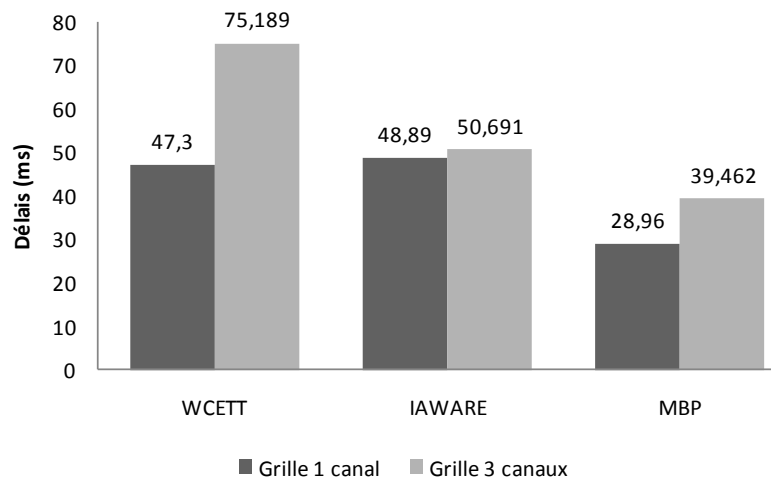


Fig.5.13: Comparaison des délais pour une topologie grille à un seul canal et une topologie grille à multiples-canaux

Les Fig.5.12 et Fig.5.13 présentent une comparaison des débits et délais obtenus pour le réseau grille avec un et plusieurs canaux. On remarque une nette différence entre le réseau un seul canal et le réseau à multiples-canaux. Les débits du réseau à multiples-canaux sont plus élevés que le réseau à un seul canal. Ce qui montre l'apport considérable des RMSF à multiples-radios par rapport aux RMSF à un seul canal. En effet, en utilisant un canal pour tout le réseau, le partage du medium est plus complexe et la bande passante est très limitée. Les paquets doivent attendre au niveau de chaque nœud que le canal se libère pour pouvoir être routés. De plus, une trop longue attente peut entraîner la perte des paquets dans la file particulièrement quand la charge augmente ce qui diminue les débits. Au niveau du réseau avec un canal, le débit moyen de MBP est supérieur à celui de WCETT et d'iAWARE . On constate une amélioration de 18% et 16% respectivement par rapport à WCETT et iAWARE. L'amélioration de MBP est plus marquée pour les réseaux à multiples-canaux avec respectivement 35% et 15% plus de débits que WCETT et iAWARE.

On remarque sur la Fig.5.13 que les délais sont plus élevés dans le réseau à multiples-canaux que pour le réseau à un seul canal. Le nombre de paquets de données reçus est plus élevé dans le réseau à multiples-canaux que dans le réseau à un seul canal ce qui augmente les délais moyens. On peut voir sur Fig.5.13 qu'en un seul canal et multiples-canaux, les délais de MBP sont plus bas que les autres WCETT et iAWARE. Il s'agit d'une diminution de 47% par rapport à WCETT et 22% par rapport à iAWARE dans le réseau à un seul canal; puis 38% et 40% par rapport à WCETT et iAWARE respectivement dans le réseau à multiples-canaux.

5.4.2 Deuxième scénario : topologie aléatoire

Dans cette partie, on génère aléatoirement des nœuds sur une surface de 1000m x 1000m et on démarre successivement 5 flux. Nous avons affecté les

canaux de manière à interconnecter tous les nœuds du réseau. La Fig.5.14 donne un exemple de topologie aléatoire qu'on a utilisé pendant nos simulations.

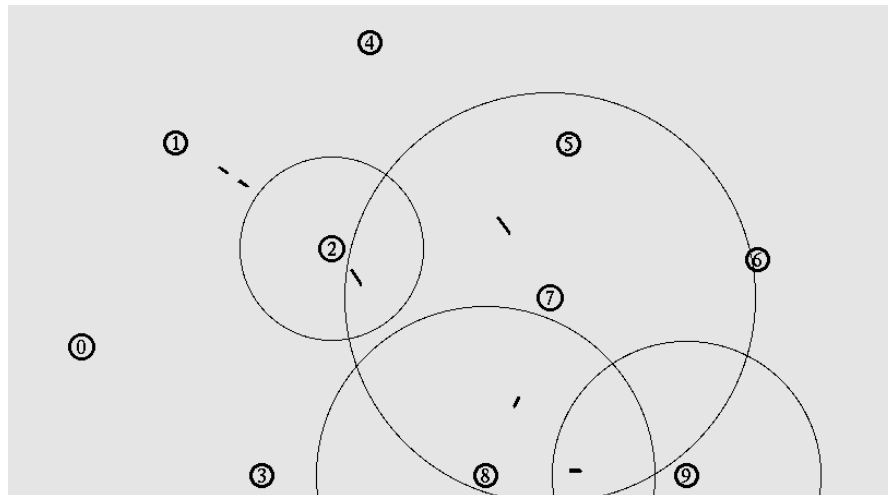


Fig.5.14: Topologie aléatoire

5.4.2.1 Topologie aléatoire un seul canal

Cette partie présente les résultats pour une topologie aléatoire un seul canal. On rappelle qu'on démarre successivement 5 flux, on augmente graduellement la charge et on étudie le comportement de chaque protocole.

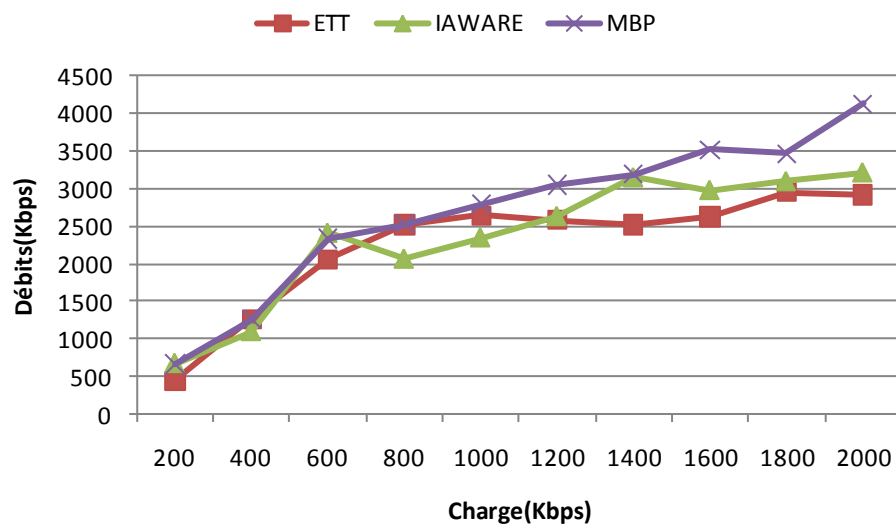


Fig.5.15: Débits du réseau pour une topologie aléatoire avec un canal

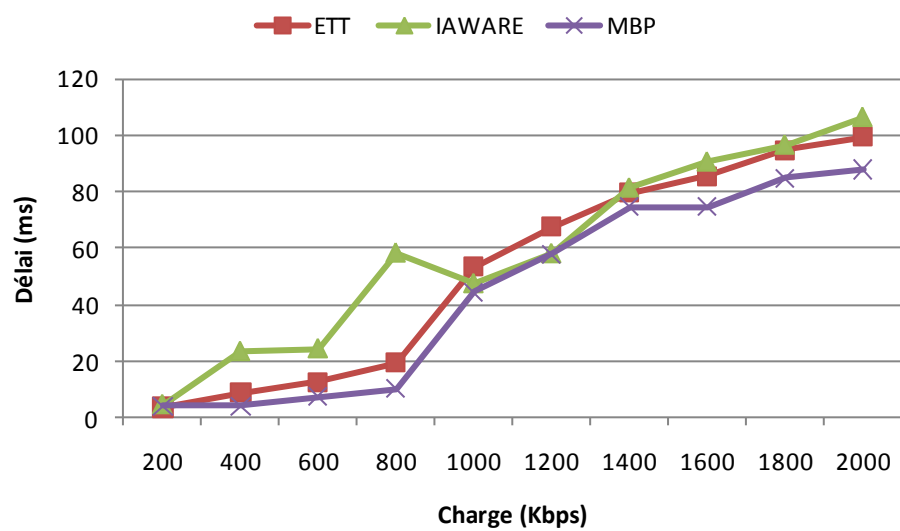


Fig.5.16: Délais pour une topologie aléatoire avec un canal

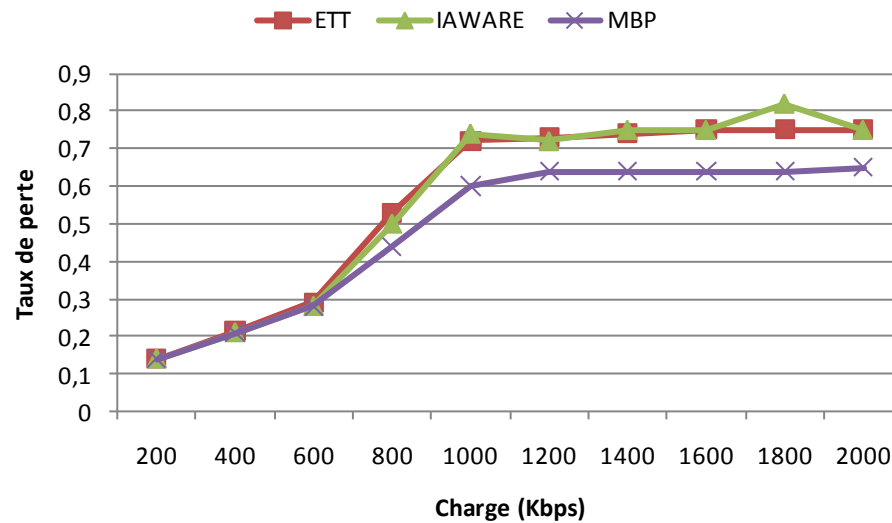


Fig.5.17: Taux de perte pour une topologie aléatoire avec un canal

Les Fig.5.15, Fig.5.16 et Fig.5.17 donnent respectivement les débits, délais moyens et taux de perte des métriques ETT, iAWARE et MBP dans un réseau à un seul canal. Sur la Fig.5.17 on note que MBP occasionne moins de perte que les autres métriques. La capacité, du réseau aléatoire à un seul canal, est très limitée et ne dépasse pas 4000 Kbps (Fig.5.15). La Fig.5.16 présente les délais de bout en bout suivant les différentes métriques. On remarque que MBP a légèrement moins de délai que ETT et iAWARE.

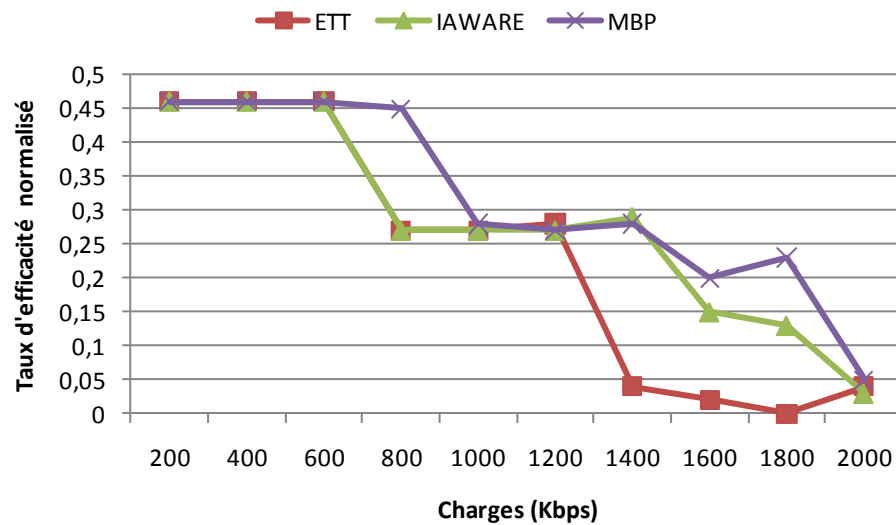


Fig.5.18: Taux d'efficacité normalisé pour une topologie aléatoire avec un canal

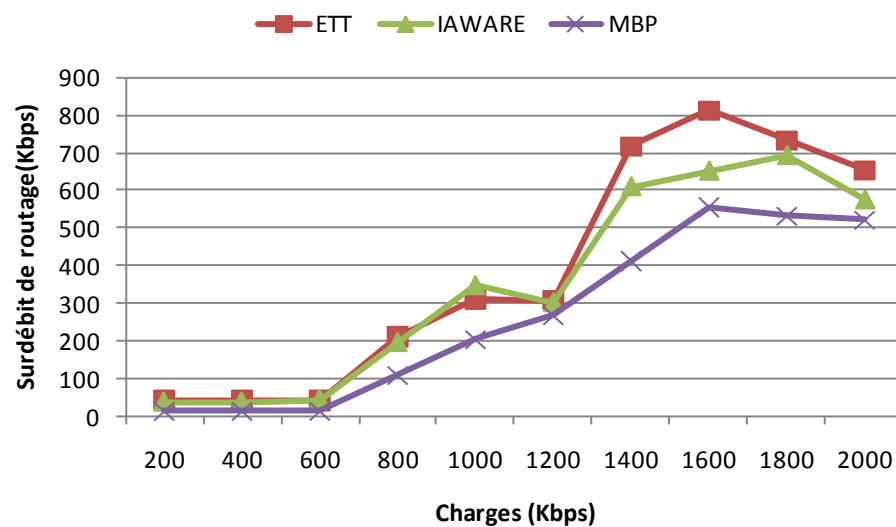


Fig.5.19: Surdébits de routage pour une topologie aléatoire avec un canal

Les Fig.5.18 et Fig.5.19 présentent respectivement le taux d'efficacité normalisé et le surdébit de routage pour WCETT, iAWARE et MBP. On remarque dans cette situation que MBP est plus efficace que WCETT et iAWARE

pour des charges différentes. Pour des charges de 800 ou 1600 Kbps (Fig.5.18), on voit que MBP est deux fois plus efficace que WCETT ou iAWARE.

Dans certains cas on peut voir que MBP a plus de surdébit de routage qu'iAWARE, c'est le cas pour les charges de 800 et 1400 Kbps. En effet dès que la qualité d'un lien diminue jusqu'à un certain seuil, une nouvelle recherche de route est enclenchée. Dans le réseau à un seul canal, comme tous les liens utilisent le même canal, le taux d'interférence est élevé. Par conséquent, la qualité de plusieurs liens se dégrade. Ce qui engendre plusieurs nouvelles requêtes de route et augmente le nombre de paquets de contrôle.

De même sur la Fig.5.19, on voit que MBP génère moins de paquets de contrôle que WCETT et iAWARE. MBP prend en considération les interférences inter-flux et intra-flux lors de la sélection des routes ce qui évite les collisions qui peuvent causer des pertes de paquets. De plus, MBP contrôle régulièrement le taux d'interférence des liens et anticipe les ruptures en recherchant des routes alternatives dès que la qualité diminue. De ce fait il évite les pertes de paquets causées par les longues files d'attente dues à la rupture des routes.

5.4.2.2 Topologie aléatoire à multiples-canaux

Dans cette partie on présente les résultats de simulations pour la topologie aléatoire à multiples-radios, multiples-canaux.

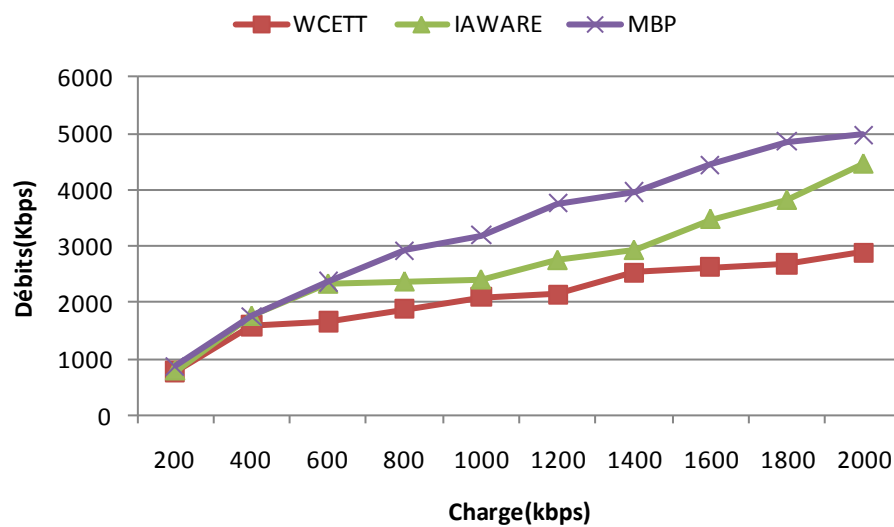


Fig.5.20: Débits du réseau pour une topologie aléatoire avec multiples-canaux

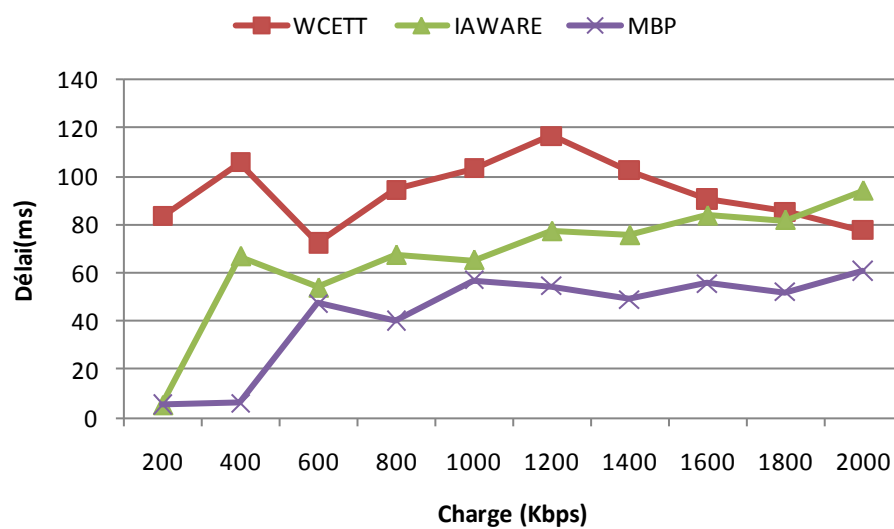


Fig.5.21: Délais pour une topologie aléatoire avec multiples-canaux

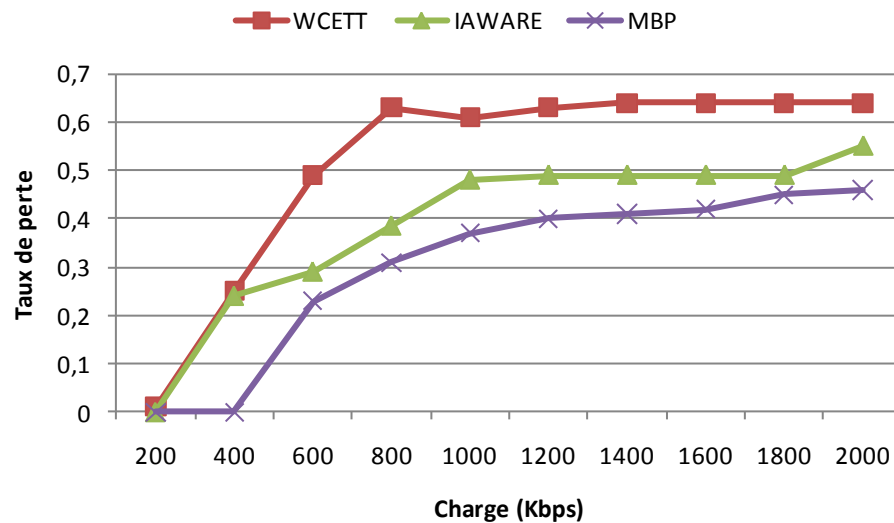


Fig.5.22: Taux de perte pour une topologie aléatoire avec avec multiples-canaux

Les Fig.5.20, Fig.5.21 et Fig.5.22 donnent les performances des différentes métriques dans un réseau à multiples-radios et multiples-canaux. Les réseaux à multiples-radios offrent une plus grande capacité que les réseaux à un seul canal. Sur la Fig.5.20, on note que pour des charges peu élevées, allant jusqu'à 600 Kbps, MBP et iAWARE ont les mêmes débits tandis que WCETT commence déjà à décroître. On note aussi que les délais de MBP (Fig.5.21) sont moins élevés que ceux des deux autres métriques et ne dépasse pas les 60 ms tandis que WCETT atteint 120 ms pour une charge de 1200 Kbps et iAWARE dépasse les 70ms.

Fig.5.22 montre les taux de perte des différents protocoles de routage. On remarque que MBP performe mieux que les autres métriques en occasionnant moins de perte. Les RMSF offrent de hautes performances quand le réseau est bien exploité. Le routage permet l'exploitation du réseau en choisissant les routes adéquates pour acheminer le trafic. MBP offrent de meilleures performances que WCETT et iAWARE grâce à son estimation correcte de l'interférence et l'anticipation des ruptures de routes.

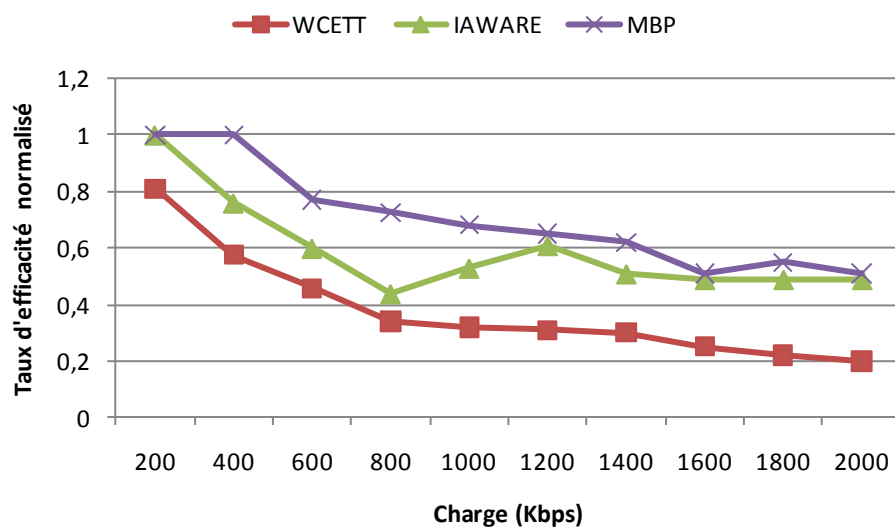


Fig.5.23: Taux d'efficacité normalisé pour une topologie aléatoire avec trois canaux

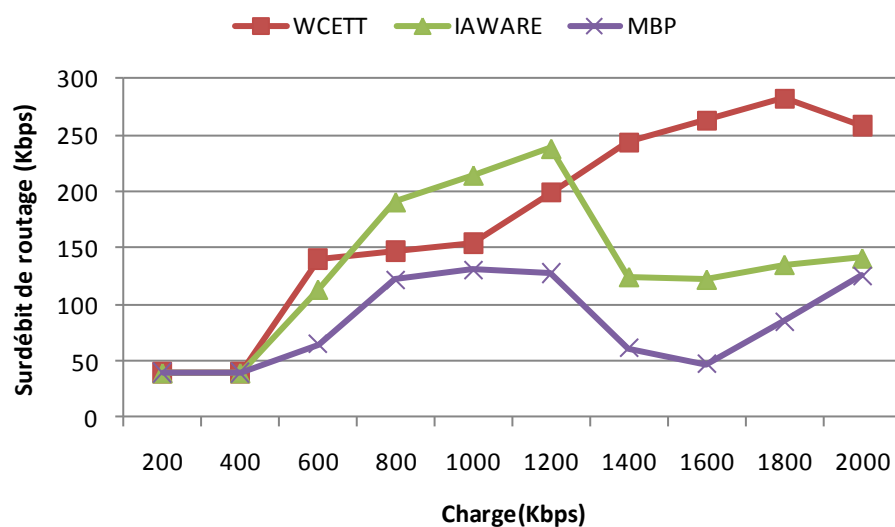


Fig.5.24: Surdébits de routage pour une topologie aléatoire avec trois canaux

Les Fig.5.23 et Fig.5.24 donnent respectivement le taux d'efficacité normalisé et le surdébit de routage des différentes métriques pour le réseau

aléatoire à multiples-canaux. Sur la Fig.5.23 nous remarquons que l'efficacité de nos trois métriques décroît au fur et à mesure que les charges augmentent mais MBP reste plus efficace que WCETT et iAWARE. En étudiant la correspondance entre le taux de perte (Fig.5.22) et le taux d'efficacité (Fig.5.23), on remarque qu'entre 200 et 800 Kbps, le taux de perte de WCETT passe de 0 à 60% puis varie faiblement jusqu'à une charge de 2000 Kbps. Alors que le taux d'efficacité passe de 80% à 34% puis reste quasi constant.

Sur la Fig.5.24 nous pouvons observer le surdébit de routage pour une topologie aléatoire à multiples-canaux. MBP utilise moins de paquets de contrôle que WCETT et iAWARE.

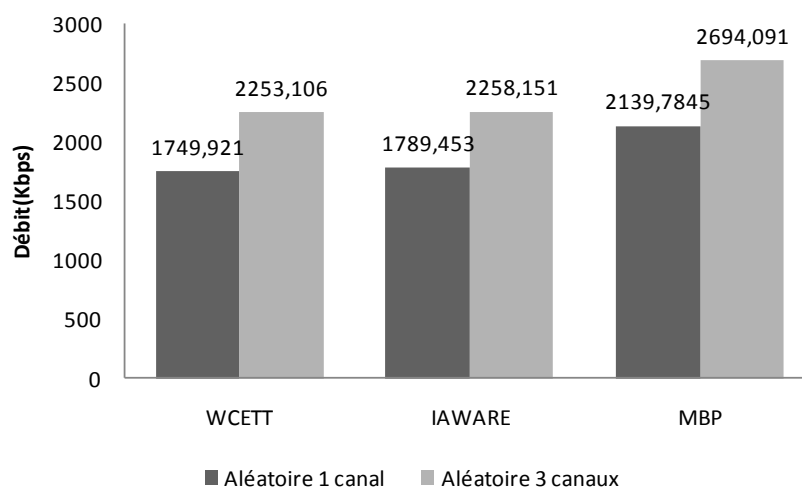


Fig.5.25: Comparaison des débits pour une topologie aléatoire avec un et trois canaux

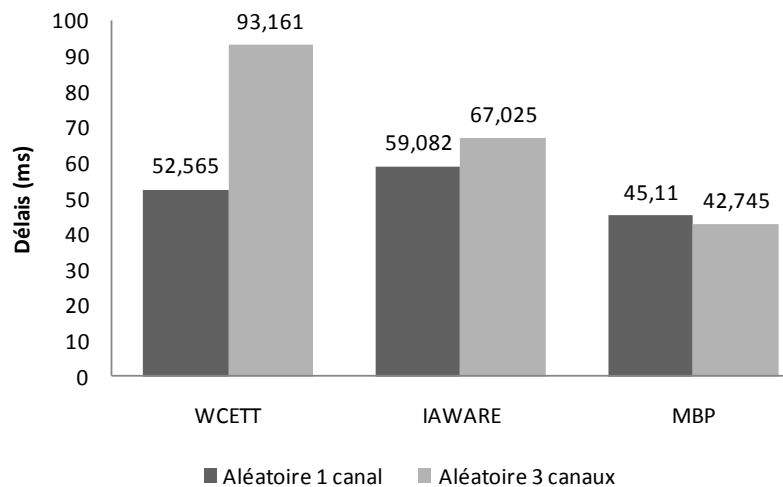


Fig.5.26: Comparaison des délais pour une topologie aléatoire avec un et trois canaux

Pour une meilleure vision des différentes performances, Fig.5.25 et Fig.5.26 donnent respectivement les moyennes des débits et délais obtenues par chacune des métriques. Les performances du réseau à multiples-canaux sont meilleures en termes de débits et de délais que le réseau à un seul canal. Ainsi nous remarquons d'une part que MBP a 16% plus de débit que WCETT et iAWARE pour le réseau multiples-canaux. D'autre part MBP améliore les débits de 16% et 18% respectivement WCETT et iAWARE pour le réseau à un seul canal. Au niveau du délai, MBP performe mieux que WCETT et iAWARE avec respectivement 14% et 23% d'amélioration pour le réseau à un seul canal. De même on note une réduction des délais de 54% et 36% par rapport à WCETT et iAWARE respectivement pour le réseau multiples-canaux.

Dans les deux cas de réseaux, grille et aléatoire, on voit clairement que les débits sont plus élevés pour les réseaux à multiples-canaux que pour le réseau à un seul canal. De même les délais sont plus petits pour le réseau multiples-canaux. Ceci montre l'amélioration considérable qu'apportent les RMSF multiples-canaux. On voit aussi que MBP offre de meilleures performances que ETT, WCETT et iAWARE pour des topologies grille ou aléatoire grâce à son

estimation correcte de l'interférence et son système de surveillance de l'interférence qui anticipe les ruptures des routes.

5.4.3 Variations des flux

Dans cette partie nous utilisons la topologie aléatoire à multiples-canaux décrite dans la section précédente, nous faisons varier le nombre de flux de un à cinq et nous étudions le comportement des différentes métriques. Tous les flux sont des flux CBR avec un taux de transmission de 500 Kbps et des paquets de taille 1000 octets. Ces tests nous permettent de voir l'effet du nombre de flux sur les différentes métriques.

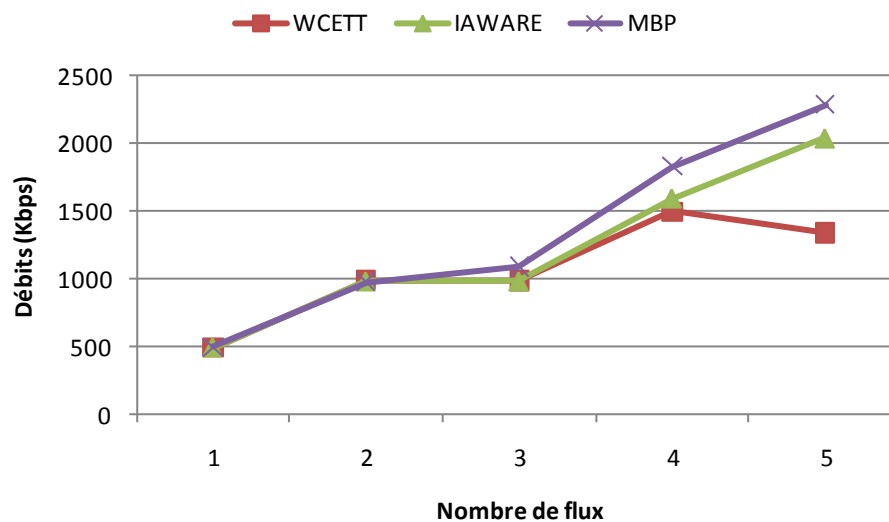


Fig.5.27: Débits de réseau pour différents nombre de flux

La Fig.5.27 nous donne le débit du réseau par rapport au nombre de flux. On remarque que pour 1 et 2 flux, les débits de toutes les métriques atteignent leur valeurs maximales qui sont de 500 et 1000 Kbps respectivement ce qui signifie qu'aucune perte n'a eu lieu lors de la communication (voir Fig.5.29). Mais quand le nombre de flux augmente, on remarque que les débits ne sont plus maximaux et les métriques commencent à se démarquer les unes des autres. L'augmentation du

nombre de flux entraîne une hausse du taux d'interférence inter-flux qui dégrade les performances des protocoles de routage. Néanmoins, on voit que MBP réagit mieux à cette augmentation de flux en offrant de meilleurs débits que WCETT et iAWARE.

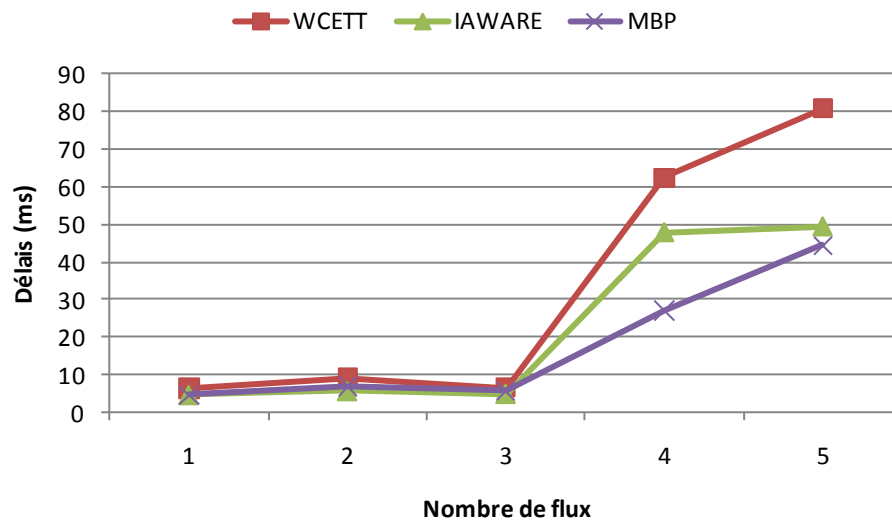


Fig.5.28: Délais pour différents nombre de flux

La Fig.5.28 présente les délais moyens des métriques de routage pour différents nombre de flux. De 1 à 3 flux, les délais sont tous inférieurs à 10ms. Mais à partir de 4 flux, on note une augmentation des délais qui dépassent 60ms pour WCETT. Cette hausse du délai est causée par le taux d'interférence inter-flux qui provoque une attente au niveau des files d'attente. Malgré cette hausse des délais, on note toujours que MBP occasionne moins de délais que WCETT et iAWARE.

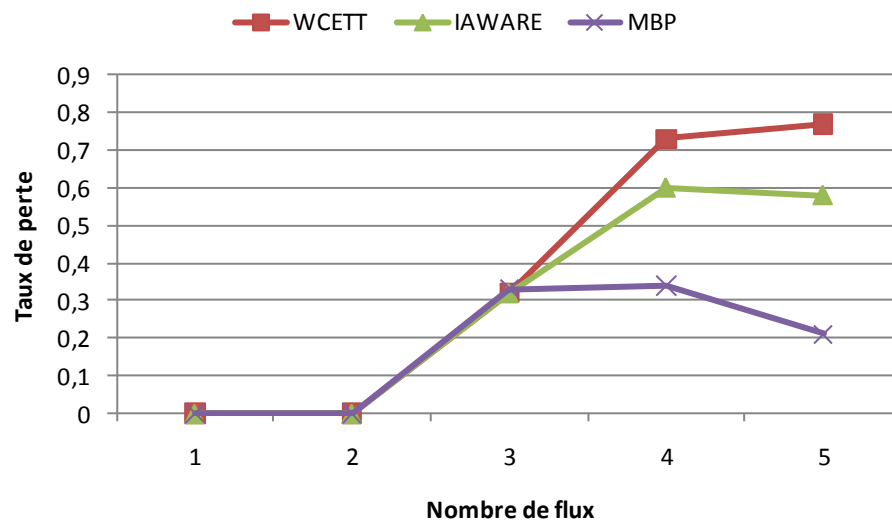


Fig.5.29: Taux de perte pour différents nombre de flux

Les observations sont les mêmes pour le taux de perte (Fig.5.29) où on peut voir que plus le nombre de flux augmente, plus les pertes sont importantes pour les mêmes raisons citées dans les paragraphes précédents. Plus le nombre de flux augmente, plus la bande passante diminue et le taux d'interférence augmente. Ce qui entraîne une perte des paquets. Mais on remarque que MBP réagit mieux à cette augmentation de flux en occasionnant moins de perte que WCETT et iAWARE.

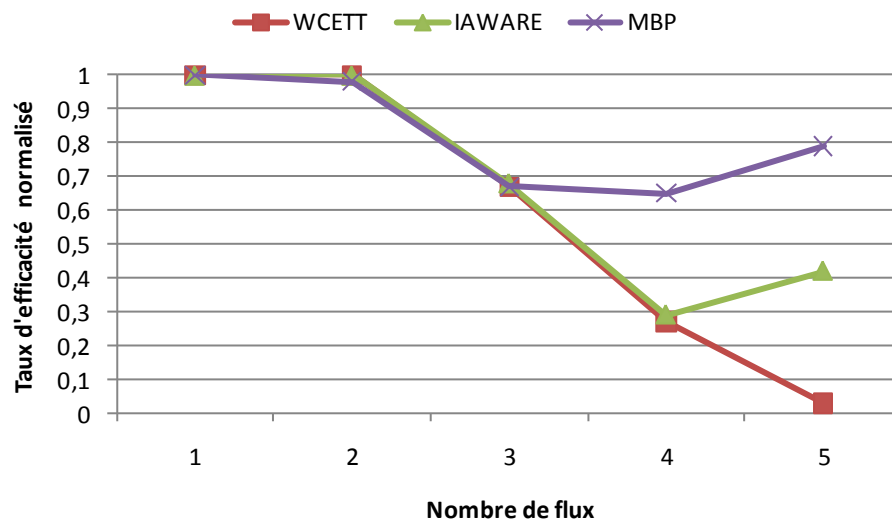


Fig.5.30: Taux d'efficacité normalisé pour différents nombre de flux

Le taux d'efficacité normalisé (Fig.5.30) est lié au nombre de paquets reçus. On peut aisément comprendre que plus le taux de perte est élevé plus l'efficacité du protocole de routage baisse. Ce phénomène est d'autant plus remarquable que le nombre de flux augmente.

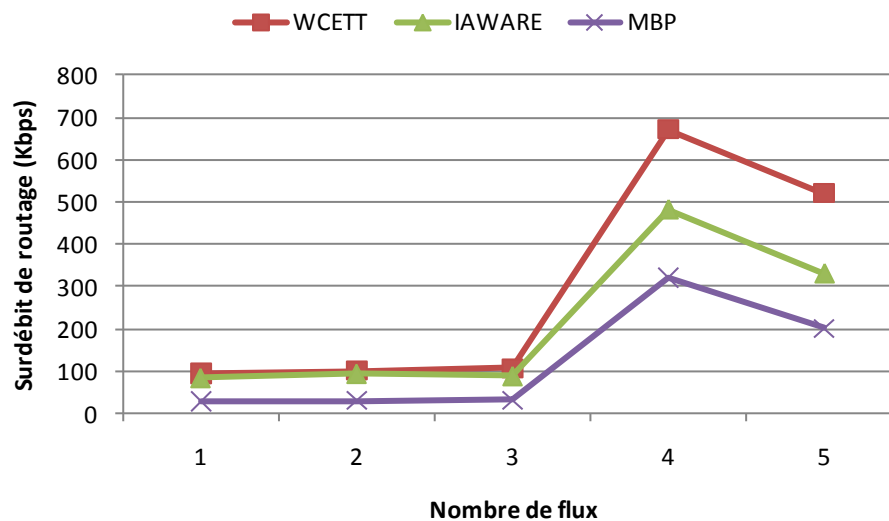


Fig.5.31: Surdébits de routage pour différents nombre de flux

La Fig.5.31 nous présente le surdébit de routage des WCETT, iAWARE et MBP. On remarque que le surdébit de routage est plus élevé pour 4 et 5 flux car dans ces situations, les protocoles de routage doivent générer plus de paquets de contrôle pour la recherche et la maintenance des routes. Pour 1, 2 et 3 flux les surdébits de routage sont faibles et ne dépassent pas 100 Kbps. Ensuite pour 4 flux, on note une augmentation remarquable du surdébit de routage. En effet, l'augmentation des flux entraîne la diminution de la bande passante dans le réseau et l'augmentation du taux d'interférence. De ce fait, les ruptures de routes sont plus fréquentes et entraînent plus de recherche de nouvelles routes. Ceci nécessite des paquets de contrôle supplémentaires ce qui augmente le surdébit de routage. Néanmoins, on remarque que MBP occasionne moins de surdébit que WCETT et iAWARE. WCETT génère plus de paquets de contrôle car il ne tient pas compte de l'interférence inter-flux ce qui engendre une sélection de route qui n'est pas toujours de bonne qualité. Ainsi, les routes deviennent vite obsolètes.

5.4.4 Effet de l'interférence sur MBP

Dans les paragraphes précédents, nous avons étudié les différentes métriques de routage pour des topologies où l'assignation était aléatoire. Dans cette partie, nous étudions MBP dans des topologies particulières. Le but est de montrer l'impact de l'interférence sur MBP. Pour cela, dans un premier temps, nous affectons les canaux de sorte qu'il n'y ait aucune interférence entre les liens et nous générons du trafic. Par la suite, nous changeons l'assignation des canaux pour créer des liens interférents. On augmente graduellement le nombre de liens interférents. Nous procédons ainsi avec des topologies où on a respectivement deux, trois et quatre liens interférents.

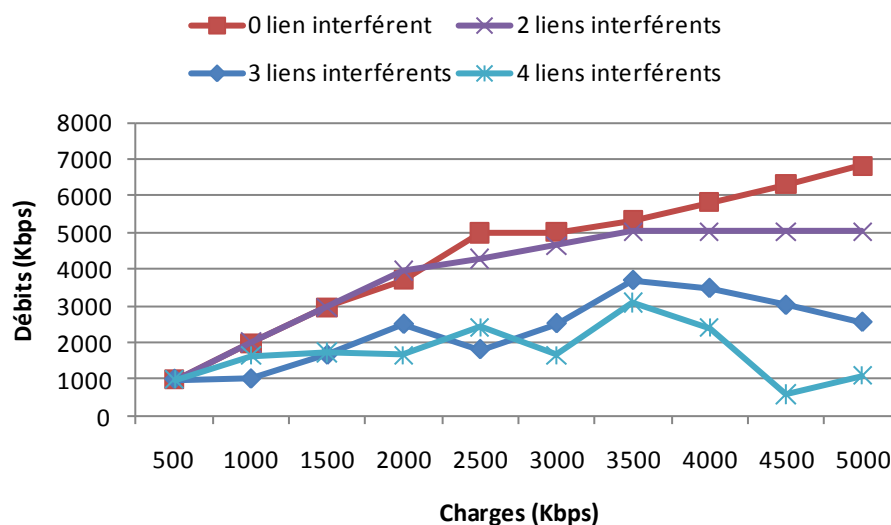


Fig.5.32: Débits pour une topologie aléatoire avec des liens interférents

La Fig.5.32 présente les débits de MBP pour une topologie avec 0, 2, 3 et 4 liens interférents. On peut clairement voir que les débits de MBP sont plus élevés pour une topologie sans interférence. Plus le nombre de liens interférents augmente, plus les débits sont faibles. Ce phénomène montre clairement que l'interférence dégrade les débits de MBP. Les débits de MBP dans la topologie sans interférence sont en moyenne 4 fois plus élevés que pour la topologie avec 4

liens interférents. Ce qui montre l'impact négatif des interférences sur les débits du réseau.

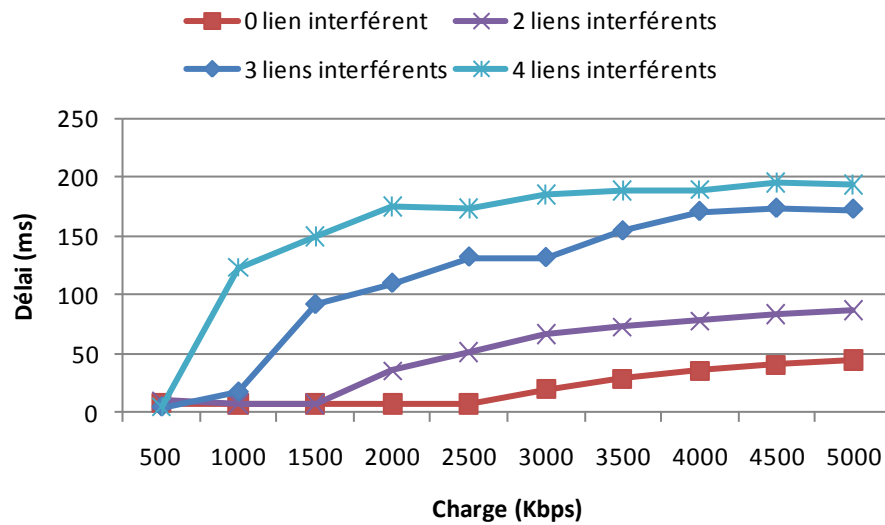


Fig.5.33: Délais moyens pour une topologie aléatoire avec des liens interférents

Sur la Fig.5.33, on peut voir que les délais sont plus importants pour les topologies avec plusieurs liens interférents que pour la topologie sans interférence. Les interférences occupent les canaux de ce fait les paquets sont stockés dans les files d'attente ce qui augmente les délais des paquets. Quand les files deviennent pleines, les paquets sont rejetés ce qui augmente le taux de perte. Ceci a un impact sur le débit (voir Fig 32).

Chapitre 6: Conclusion et perspectives futures

6.1 Conclusion

La facilité de déploiement et l'absence de gestion centralisée des communications dans les RMSF en font une solution présentant plusieurs avantages. Les RMSF essaient de répondre à l'augmentation croissante du nombre d'utilisateurs et de leurs applications qui demandent de plus en plus de ressources comme les applications multimédias. Cependant, nous avons vu tout au long de ce mémoire que les caractéristiques propres des réseaux maillés sans fil rendent plus complexe le routage.

Ce mémoire aborde le problème des métriques de routage dans les RMSF à une seule interface radio et un seul canal et dans les RMSF à plusieurs interfaces radios et plusieurs canaux. Dans un premier temps, nous nous sommes intéressés aux RMSF en mettant l'accent sur leurs caractéristiques et leurs particularités ainsi que les différentes technologies sans fil utilisées. Ensuite, nous avons fourni un état de l'art sur les protocoles et métriques de routage qui sont utilisés dans les RMSF et nous avons identifié leurs limites.

Nous avons proposé une nouvelle métrique appelée MBP qui améliore les performances des réseaux RMSF, en occurrence le débit et de délai. MBP est une nouvelle métrique qui se base sur le taux de perte, l'interférence intra-flux et inter-flux pour estimer la qualité des liens et des routes. De plus, elle intègre un système de surveillance de la qualité des liens. En cas de dégradation d'une route ou d'un lien, MBP lance une nouvelle procédure de recherche de route et en change dès que possible. Cette méthode améliore les délais et les pertes au niveau des files d'attente sur les routes de mauvaise qualité. Nous avons implémenté notre nouvelle métrique MBP sous NS-2 ainsi qu'ETT, WCETT et

iAWARE, ensuite nous avons comparé leurs performances. Les résultats des simulations ont montré que les performances de MBP surpassent celles des autres métriques grâce à son estimation assez précises de la qualité des liens et son système de surveillance de liens qui prévient d'éventuels ruptures de routes dues à un taux élevé d'interférence.

6.2 Perspectives futures

Dans l'optique d'améliorer les performances des métriques de routage, certains développements futurs peuvent être envisagés. En occurrence, MBP ne capture que les interférences sur deux sauts, nous pensons donc améliorer l'estimation de l'interférence intra-flux. Il serait aussi intéressant de combiner le routage à l'assignation des canaux.

La perte des paquets peut être due à plusieurs raisons : collision, lien de mauvaise qualité, stations éloignées ou présence des interférences. Ainsi le taux de perte peut aussi refléter l'interférence, donc en le combinant avec le taux d'interférence comme le font plusieurs métriques telles que iAWARE, MIC ainsi que notre métrique MBP, on risque dans certains cas de pénaliser doublement le lien. Il est donc intéressant de pouvoir déterminer les causes des pertes des paquets pour une meilleure estimation des métriques.

NS2 est certes un simulateur très utilisé dans la recherche dans les réseaux sans fil mais il n'est pas totalement fiable donc il serait aussi intéressant de tester notre travail sur un banc d'essai (testbed) avec des vrais routeurs sans fil afin de valider nos résultats.

Bibliographie

- [1] Akyildiz, I.F., Wang, X. and Wang, W. (2005) *Wireless mesh networks: a survey*, Computer Networks, 47, 445-487.
- [2] Clausen, T., et al. *Optimized Link State Routing Protocol (OLSR)*.
- [3] Cook, S.A. (1971) *The complexity of theorem-proving procedures*. Proceedings of the third annual ACM symposium on Theory of computing. ACM, Shaker Heights, Ohio, United States, 151-158.
- [4] Couto, D.S.J.D., et al. (2005) *A high-throughput path metric for multi-hop wireless routing*, Wireless Networks, 11, 419-434.
- [5] Couto, D.S.J.D., et al. (2003) *Performance of multihop wireless networks: shortest path is not enough*, SIGCOMM Comput. Commun. Rev., 33, 83-88.
- [6] Draves, R., Padhye, J. and Zill, B. (2004) *Routing in multi-radio, multi-hop wireless mesh networks*. Proceedings of the 10th annual international conference on Mobile computing and networking. ACM, Philadelphia, PA, USA, 114-128.
- [7] Jain, K., et al. (2005) *Impact of Interference on Multi-Hop Wireless Network Performance*, Wireless Networks, 11, 471-487.
- [8] Johnson, D.B. (1977) *Efficient Algorithms for Shortest Paths in Sparse Networks*, J. ACM, 24, 1-13.
- [9] Keshav, S. (1991) *A control-theoretic approach to flow control*, SIGCOMM Comput. Commun. Rev., 21, 3-15.
- [10] Kim, K.-H. and Shin, K.G. (2006) *On accurate measurement of link quality in multi-hop wireless mesh networks*. Proceedings of the 12th annual international conference on Mobile computing and networking. ACM, Los Angeles, CA, USA, 38-49.
- [11] Li, F., et al. (2008) *Gateway Placement for Throughput Optimization in Wireless Mesh Networks*, Mobile Networks and Applications, 13, 198-211.

- [12] Marks, R.B., Gifford, I.C. and O'Hara, B. (2001) *Standards in IEEE 802 unleash the wireless Internet*, Microwave Magazine, IEEE, 2, 46-56.
- [13] Ohrtman, F. (2005) *WiMAX handbook : building 802.16 wireless networks*. McGraw-Hill communications. McGraw-Hill, New York ; Toronto.
- [14] Perkins C. E and M, R.E. (1999) *Ad-hoc On-Demand Distance Vector Routing*.
- [15] Perkins, C.E. and Bhagwat, P. (1994) *Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers*, SIGCOMM Comput. Commun. Rev., 24, 234-244.
- [16] Raniwala, A. and Tzi-cker, C. (2005) *Architecture and algorithms for an IEEE 802.11-based multi-channel wireless mesh network*. INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE. 2223-2234 vol. 2223.
- [17] Ruiz, P.M. and Gomez-Skarmeta, A.F. (2004) *Maximal Source Coverage Adaptive Gateway Discovery for Hybrid Ad Hoc Networks*. In Nikolaidis, I., Barbeau, M. and Kranakis, E. (eds), *Ad-Hoc, Mobile, and Wireless Networks*. Springer Berlin / Heidelberg, 630-630.
- [18] Subramanian, A.P., Buddhikot, M.M. and Miller, S. (2006) *Interference aware routing in multi-radio wireless mesh networks*. Wireless Mesh Networks, 2006. WiMesh 2006. 2nd IEEE Workshop on. 55-63.
- [19] Zhang, Y., Luo, J. and Hu, H. (2006) *Wireless mesh networking: architectures, protocols and standards*. Wireless networks and mobile communications series. Auerbach, Boca Raton, Fla.
- [20] http://en.wikipedia.org/wiki/File:2.4_GHz_WiFi_channels_%28802.11b,g,WLAN%29.svg
- [21] The network simulator-ns2, <http://www.isi.edu/nsnam/ns/>.
- [22] Bellman, R. (1958) *On a Routing Problem*, In Quarterly of Applied Mathematics, 87-90.
- [23] Calvo, R.A. and Campo, J.P. (2007) *Adding Multiples Interface Support in NS2*.

- [24] Chen, Q., Schmidt-Eisenlohr, F. and D. Jiang (2008) *Overhaul of IEEE 802.11 Modeling and Simulation in NS2 (802.11Ext)*.
- [25] Haas, Z.J., Pearlman, M.R. and Samar, P. (2002) *The Zone Routing Protocol (ZRP) for Ad Hoc Networks*.
- [26] Hu, Y.C., Johnson, D.B. and Maltz, D.A. (2003) *The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)*.
- [27] Passos, D. (2006) *Mesh Network Performance Measurements*. Info and Telecommun Technologies Symp.
- [28] SARR, C. (2007) *De l'apport d'une évaluation précise des ressources pour la Qualité de Service des réseaux ad hoc basés sur IEEE 802.11*. INSA, Lyon.
- [29] SARR, C., et al. (2006) *ABE Un protocole de réservation de bande passante pour les réseaux ad hoc basés sur IEEE 802.11*. CFIP. Tunisie.
- [30] Yang, Y., Wang, J. and Kravets, R. (2005) *Designing Routing Metrics for Mesh Networks*. IEEE Workshop on Wireless Mesh Networks (WiMesh).
- [31] Paul, M. (2002) *802.11 et les réseaux sans fil*. Eyrolles.
- [32] Yang, Y., Wang, J. and Kravets, R. (2005) *Interference-aware Load Balancing for Multihop Wireless Networks*. Technical Report UIUCDCS-R-2005-2526,
- [33] Park, V. and Corson, M.S. (1997) *A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks*. IEEE INFOCOM.
- [34] <http://www.ece.gatech.edu/research/labs/bwn/substation/>