

Université de Montréal

**Routage adaptatif et stabilité dans les réseaux maillés sans  
fil**

par

Mustapha Boushaba

Département d'informatique et de recherche opérationnelle

Faculté des arts et des sciences

Thèse présentée à la Faculté des arts et des sciences  
en vue de l'obtention du grade de Philosophiæ doctor (Ph.D.)  
en informatique

Mars, 2013

© Mustapha Boushaba, 2013

Université de Montréal  
Faculté des études supérieures

Cette thèse intitulée:

Routage adaptatif et stabilité dans les réseaux maillés sans fil

Présentée par:

Mustapha Boushaba

a été évaluée par un jury composé des personnes suivantes :

El Mostapha Aboulhamid, président-rapporteur

Abdelhakim Hafid, directeur de recherche

Michel Gendreau, codirecteur de recherche

Samuel Pierre, membre du jury

Ahmed Karmouch, Examineur externe

El Mostapha Aboulhamid, représentant du doyen

## Résumé

Grâce à leur flexibilité et à leur facilité d'installation, les réseaux maillés sans fil (WMNs) permettent un déploiement d'une infrastructure à faible coût. Ces réseaux étendent la couverture des réseaux filaires permettant, ainsi, une connexion n'importe quand et n'importe où. Toutefois, leur performance est dégradée par les interférences et la congestion. Ces derniers causent des pertes de paquets et une augmentation du délai de transmission d'une façon drastique. Dans cette thèse, nous nous intéressons au routage adaptatif et à la stabilité dans ce type de réseaux.

Dans une première partie de la thèse, nous nous intéressons à la conception d'une métrique de routage et à la sélection des passerelles permettant d'améliorer la performance des WMNs. Dans ce contexte nous proposons un protocole de routage à la source basé sur une nouvelle métrique. Cette métrique permet non seulement de capturer certaines caractéristiques des liens tels que les interférences inter-flux et intra-flux, le taux de perte des paquets mais également la surcharge des passerelles. Les résultats numériques montrent que la performance de cette métrique est meilleure que celle des solutions proposées dans la littérature.

Dans une deuxième partie de la thèse, nous nous intéressons à certaines zones critiques dans les WMNs. Ces zones se trouvent autour des passerelles qui connaissent une concentration plus élevée du trafic ; elles risquent de provoquer des interférences et des congestions. À cet égard, nous proposons un protocole de routage proactif et adaptatif basé sur l'apprentissage par renforcement et qui pénalise les liens de mauvaise qualité lorsqu'on s'approche des passerelles. Un chemin dont la qualité des liens autour d'une passerelle est meilleure sera plus favorisé que les autres chemins de moindre qualité. Nous utilisons l'algorithme de *Q-learning* pour mettre à jour dynamiquement les coûts des chemins, sélectionner les prochains nœuds pour faire suivre les paquets vers les passerelles choisies et explorer d'autres nœuds voisins. Les résultats numériques montrent que notre protocole distribué, présente de meilleurs résultats comparativement aux protocoles présentés dans la littérature.

Dans une troisième partie de cette thèse, nous nous intéressons aux problèmes d'instabilité des réseaux maillés sans fil. En effet, l'instabilité se produit à cause des

changements fréquents des routes qui sont causés par les variations instantanées des qualités des liens dues à la présence des interférences et de la congestion. Ainsi, après une analyse de l'instabilité, nous proposons d'utiliser le nombre de variations des chemins dans une table de routage comme indicateur de perturbation des réseaux et nous utilisons la fonction d'entropie, connue dans les mesures de l'incertitude et du désordre des systèmes, pour sélectionner les routes stables. Les résultats numériques montrent de meilleures performances de notre protocole en comparaison avec d'autres protocoles dans la littérature en termes de débit, délai, taux de perte des paquets et l'indice de Gini.

**Mots-clés** : Réseaux maillés sans fil, Métriques de routage, Performances, Mesures, Stabilité, Interférences,

# Abstract

Thanks to their flexibility and their simplicity of installation, Wireless Mesh Networks (WMNs) allow a low cost deployment of network infrastructure. They can be used to extend wired networks coverage allowing connectivity anytime and anywhere. However, WMNs may suffer from drastic performance degradation (e.g., increased packet loss ratio and delay) because of interferences and congestion. In this thesis, we are interested in adaptive routing and stability in WMNs.

In the first part of the thesis, we focus on defining new routing metric and gateway selection scheme to improve WMNs performance. In this context, we propose a source routing protocol based on a new metric which takes into account packet losses, intra-flow interferences, inter-flow interferences and load at gateways together to select best paths to best gateways. Simulation results show that the proposed metric improves the network performance and outperforms existing metrics in the literature.

In the second part of the thesis, we focus on critical zones, in WMNs, that consist of mesh routers which are located in neighborhoods of gateways where traffic concentration may occur. This traffic concentration may increase congestion and interferences excessively on wireless channels around the gateways. Thus, we propose a proactive and adaptive routing protocol based on reinforcement learning which increasingly penalizes links with bad quality as we get closer to gateways. We use *Q-learning* algorithm to dynamically update path costs and to select the next hop each time a packet is forwarded toward a given gateway; learning agents in each mesh router learn the best link to forward an incoming packet and explore new alternatives in the future. Simulation results show that our distributed routing protocol is less sensitive to interferences and outperforms existing protocols in the literature.

In the third part of this thesis, we focus on the problems of instability in WMNs. Instability occurs when routes flapping are frequent. Routes flapping are caused by the variations of link quality due to interferences and congestion. Thus, after analyzing factors that may cause network instability, we propose to use the number of path variations in routing tables as an indicator of network instability. Also, we use entropy function, usually used to measure uncertainty and disorder in systems, to define node stability, and thus, select the most

stable routes in the WMNs. Simulation results show that our stability-based routing protocol outperforms existing routing protocols in the literature in terms of throughput, delay, loss rate, and Gini index.

**Keywords** : Wireless Mesh Networks, Routing metrics, Performances, Measures, Stability, Interferences

# Table des matières

Chapitre 1 : Introduction .....	1
1.1. Contexte général .....	1
1.2. Motivations .....	4
1.3. Description des problèmes .....	6
1.4. Contributions .....	10
1.5. Organisation de la thèse .....	12
1.6. Articles publiés/soumis durant cette thèse .....	13
Chapitre 2 : Revue de la littérature .....	14
2.1. Les réseaux maillés sans fil .....	14
2.1.1. Architecture des réseaux maillés sans fil .....	15
2.1.2. Les communications sans fil .....	17
2.1.3. Les applications déployées dans les WMNs .....	19
2.1.4. Quelques problèmes liés à l'utilisation du canal sans fil .....	20
2.2. Routage dans les réseaux sans fil .....	23
2.2.1. Techniques de mesure des qualités des liens .....	24
2.2.2. Les métriques de routage .....	25
2.2.3. Les protocoles de routage .....	34
2.2.4. Stabilité des réseaux .....	39
Chapitre 3 : .....	43
Source-based Routing in Wireless Mesh Networks .....	43
3.1. Introduction .....	43
3.2. Related work .....	46
3.2.1. Routing metrics .....	46
3.2.2. Gateway discovery schemes .....	49
3.3. System model and Notations .....	50
3.3.1. Network Model .....	50
3.3.2. DACI, Distribution Available Capacity Indicator .....	51
3.3.3. Link Quality Metric (LQM) .....	52
3.3.4. Gateways Advertisement message (GWADV) .....	55

3.3.5. Path quality .....	55
3.4. BP2BG: Best Path to best Gateway scheme for multichannel multi-interface WMNs .	57
3.4.1. Path selection to the best gateway .....	57
3.4.2. Waiting before changing paths .....	58
3.4.3. BP2BG Algorithm .....	59
3.5. Simulation and results .....	60
3.6. Conclusion .....	64
Chapitre 4: .....	65
Reinforcement Learning Based Routing in Wireless Mesh Networks.....	65
4.1. Introduction .....	66
4.2. Related work.....	68
4.2.1. Routing metrics for wireless mesh networks.....	68
4.2.2. Learning in routing schemes .....	71
4.3. Reinforcement Learning Based Distributed Routing to Gateways .....	72
4.3.1. Gateway Load.....	73
4.3.2. Link Quality Metric (LQM) .....	73
4.3.3. Path quality.....	75
4.3.4. RLBDR.....	77
4.4. Simulation and results .....	82
4.5. Conclusion.....	90
Chapitre 5: .....	91
Node Stability-Based Routing in Wireless Mesh Networks .....	91
5.1. Introduction .....	92
5.2. Related work.....	94
5.3. Factors leading to instable networks .....	97
5.4. Entropy utility.....	98
5.5. Proposal description .....	99
5.5.1. Network Model and assumptions .....	99
5.5.2. Link Quality Metric and Node stability.....	101
5.6. Simulation and results .....	112
5.7. Conclusion.....	121



Chapitre 6 : Conclusion et travaux futurs.....	122
6.1. Contributions et résultats de la thèse.....	122
6.2. Perspectives et travaux futurs.....	125

## Liste des tableaux

Tableau 1.	Récapitulatif des métriques de routages.....	34
Table 2.	NS2 Simulation setup.....	60
Table 3.	NS2 simulation setup .....	82
Table 4.	Gateway Selection by S1 .....	107
Table 5.	Gateway Selection by S2 .....	107
Table 6.	Summary of operations performed by Algorithm 2 for Gateway G1 .....	111
Table 7.	Simulation setup.....	113

## Liste des figures

Figure 1.	Réseau maillé sans fil.....	2
Figure 2.	Dégradation des performances d'un réseau maillé sans fil.....	4
Figure 3.	Besoin de QoS pour différentes applications.....	6
Figure 4.	Problème d'utilisation d'une seule métrique.....	7
Figure 5.	Problème d'oscillation des routes.....	9
Figure 6.	Architecture des réseaux maillés sans fil: épine dorsale.....	15
Figure 7.	Architecture des réseaux maillés sans fil: cas client.....	16
Figure 8.	Architecture des réseaux maillés sans fil: cas hybride.....	17
Figure 9.	Classification des technologies sans fil.....	17
Figure 10.	Exemple des interférences dans un réseau maillé sans fil.....	21
Figure 11.	Exemple des portées.....	22
Figure 12.	Exemple de calcul de WCETT.....	30
Figure 13.	Classification récapitulative des protocoles de routage.....	39
Figure 14.	Inter-flow interference.....	45
Figure 15.	Intra-flow interference.....	45
Figure 16.	Load: GW-1 and GW-2.....	51
Figure 17.	Forward and reverse links asymmetry.....	53
Figure 18.	GWADV format.....	55
Figure 19.	Path with bottleneck link.....	56
Figure 20.	Paths to different Gateways.....	57
Figure 21.	Alternative paths.....	58
Figure 22.	End-to-end delay vs. data rate.....	61
Figure 23.	Mean delay.....	62
Figure 24.	Network throughput vs. data rate.....	63
Figure 25.	Packet loss vs. data rate.....	63
Figure 26.	WMN, multi-metrics routing case.....	67
Figure 27.	LQM vs PQ.....	76
Figure 28.	WMN topology used for simulations (16 MRs and 3 GWs).....	83
Figure 29.	Delay vs. data rate.....	84

Figure 30.	Mean delay vs. schemes .....	85
Figure 31.	Loss vs. data rate .....	85
Figure 32.	Loss due to collision in WMN .....	86
Figure 33.	Loss due to IFQ.....	87
Figure 34.	Network throughput vs. data rate .....	88
Figure 35.	Loss vs. data rate for different N-hops.....	88
Figure 36.	Delay vs. data rate for different N-hops.....	89
Figure 37.	Network throughput vs data rate for different N-hops.....	89
Figure 38.	Route flap scenario.....	94
Figure 39.	GWADV message .....	105
Figure 40.	Gateway selection illustration .....	106
Figure 41.	Topology for loop free illustration.....	110
Figure 42.	Spanning tree rooted at G1.....	110
Figure 43.	Directed forwarding graph to G1 .....	112
Figure 44.	Average throughput.....	113
Figure 45.	Delay vs. data rate .....	114
Figure 46.	Loss rate vs. data rate .....	115
Figure 47.	Loss rate due to collisions vs. data rate.....	115
Figure 48.	Loss rate due to IFQ vs. data rate.....	116
Figure 49.	Gini Index vs. Time for a data rate 1000 (kbps) .....	117
Figure 50.	Gini Index vs. Time for a data rate 2000 (kbps) .....	118
Figure 51.	Gini Index vs. Time for a data rate 3000 (kbps) .....	118
Figure 52.	Percentage of traffic served by gateways (NSR case) .....	119
Figure 53.	Percentage of traffic served by gateways (Load case) .....	119
Figure 54.	Average stability index .....	120

## Liste des algorithmes

Algorithm 1. Path and gateway selection at each Source MR.....	59
Algorithm 1. Gateway selection algorithm at source nodes .....	78
Algorithm 2. Next hop selection algorithm at MR $i$ .....	79
Algorithm 3. Loop free forwarding algorithm.....	80
Algorithm 1. Stability Index Algorithm (SIA) .....	102
Algorithm 2. Loop Free Forwarding Algorithm (LFFA) .....	108

## Liste des sigles et abréviations

ABR	Associativity-Based Routing
ACO	Ant Colony Optimization
ADB	Adaptive Dynamique Backbone
AODV	Ad hoc On-Demand Distance Vector
AP	Access Point
ATM	Asynchronous Transfer Mode
BER	Bit Error Rate
BP2BG	Best Path to Best Gateway
CBR	Constant Bit Rate
CPU	Central Processing Unit
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
DACI	Distribution Available Capacity Indicator
DSDV	Destination-Sequenced Distance Vector
DSR	Dynamic Source Routing
EAR	Efficient and Accurate Link quality monitor
ELQ	Expected Link Quality
ENT	Effective Number of Transmissions
ETT	Expected Transmission Time
ETX	Expected Transmission Count
FER	Frame Error Rate
GW	Gateway
GWADV	Gateways Advertisement
iAWARE	Interference Aware
IP	Internet Protocol
LFFA	Loop-Free Forwarding Algorithm
LLG	Least Loaded Gateway
LQM	Link Quality Metric
MAN	Metropolitan Area Network
MANET	Mobile ad-hoc network

MC	Mesh Client
mETX	modified ETX
MIC	Metric of Interference and Channel-switching
MIMO	Multiple-Input and Multiple-Output
ML	Minimum Loss
MMRP	Mobile Mesh Routing Protocol
MPR	Multipoint Relay
MR	Mesh Router
MTM	Medium Time Metric
NLOS	Non-Line-of-Sight
NS	Node Stability
NSR	Node Stability-based Routing
OBS	Optical burst switching
OLSR	Optimized Link-State Routing
P2P	Peer to Peer
PDA	Personal Digital assistant
PQ	Path Quality
QoS	Qualité de service
QoS	Quality of Service
RARE	Resource Aware Routing for mEsh
RLBDR	Reinforcement Learning-based Distributed Routing
RREP	Route Reply
RREQ	Route Request
RSSI	Received Signal Strength Indication
RTT	Round Trip Time
SIA	Stability Index Algorithm
SINR	Signal to Interference plus Noise Ratio
SNR	Signal-to-Noise Ratio
SSA	Signal Stability based Adaptive
TC	Topology Control

TCP	Transmission Control Protocol
TORA	Temporally Ordered Routing Algorithm
UDP	User Datagram Protocol
VANET	Vehicular Ad-Hoc Network
WCETT	Weighted Cumulative Expected Transmission Count
WCETT-LB	WCETT-Load Balancing
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WMN	Wireless Mesh Network
WPAN	Wireless Personal Area Network
WSN	Wireless Sensor Network
ZPQ	Zone-based Path Quality



*À mes parents.*

*À mon épouse.*

*À mes enfants.*

*À toute ma famille.*

*À toute ma belle-famille*

## Remerciements

Je tiens tout d'abord à adresser mes remerciements et ma gratitude à mon directeur de recherche Abdelhakim Hafid, professeur à l'université de Montréal, pour la qualité de son encadrement, sa patience, sa disponibilité, son aide et son support tout au long de cette thèse.

Mes remerciements s'adressent également à mon codirecteur de recherche Michel Gendreau, professeur à l'école polytechnique de Montréal, pour les discussions fructueuses et les précieux conseils qu'il m'a donné au cours de cette thèse.

Je tiens à remercier Monsieur El Mostapha Aboulhamid professeur à l'université de Montréal, Monsieur Samuel Pierre professeur à l'école polytechnique de Montréal et Monsieur Ahmed Karmouch professeur à l'université d'Ottawa d'avoir accepté de faire partie du jury pour examiner les travaux de recherche dans cette thèse.

Aussi, je tiens à remercier mes collègues au Laboratoire des Réseaux de Communications (LRC) et plus particulièrement Abdeltouab Belbekkouche et Ahmed Beljadid pour leur amitié et pour la collaboration fructueuse que nous avons pu établir.

J'aimerais remercier ma femme Soumia pour sa présence et son soutien permanents ainsi que mes enfants Aymane et Ayah, pour leur patience et leur sagesse.

Enfin, que tous celles et ceux qui m'ont apporté leur appui trouvent ici l'expression de mes sincères remerciements.

# Chapitre 1 : Introduction

Nous décrivons dans ce chapitre le contexte général de la thèse et les motivations pour nos travaux de recherche. Ensuite, nous décrivons les problèmes de routage dans les réseaux maillés sans fil ainsi que les contributions de la thèse. Finalement, nous terminons ce chapitre en donnant un aperçu sur les différents chapitres ainsi que sur les publications (*articles de revue et de conférence*) publiés ou soumis au cours de cette thèse.

## 1.1. Contexte général

De nos jours, grâce à la technologie avancée des semi-conducteurs, et plus particulièrement à l'évolution de la technologie radio et de la communication sans fil, les réseaux sans fil connaissent un essor considérable. Parmi eux figurent les réseaux de capteurs (WSNs [1, 2]), les réseaux véhiculaires (VANETs [3]) et les réseaux maillés sans fil (WMNs [4]). Ces derniers sont de plus en plus utilisés [5, 6, 7, 8] et constituent actuellement une technologie offrant un accès à haut débit à l'Internet, n'importe quand et n'importe où. Généralement, les WMNs (voir figure 1) se composent d'un ensemble de routeurs sans fil (*Mesh Router MRs*) dotés dans la plupart des cas de plus d'une carte sans fil utilisant les normes IEEE802.11 [9]/IEEE 802.16 [10]. Ces routeurs sont capables de recevoir, d'envoyer et d'acheminer du trafic à travers une transmission multi-sauts sans fil de/vers les passerelles qui représentent les points d'accès à l'Internet. À l'instar des réseaux ad-hoc mobiles [11] (*Mobile ad hoc networks* MANETs), les réseaux maillés sans fil se distinguent par trois caractéristiques principales :

- La position des routeurs sans fil est stationnaire ou à mobilité réduite contrairement aux réseaux ad-hoc, où les nœuds peuvent avoir une grande mobilité ;
- Le trafic est orienté vers les (ou en provenance des) passerelles qui représentent les points de sortie vers l'Internet, tandis que pour les réseaux ad-hoc, ce trafic peut être arbitraire entre des paires de nœuds ;
- Les routeurs sans fil dans les WMNs sont alimentés par du courant électrique, par conséquent, la contrainte de la consommation de l'énergie ne s'impose plus comme dans le cas des réseaux ad-hoc.

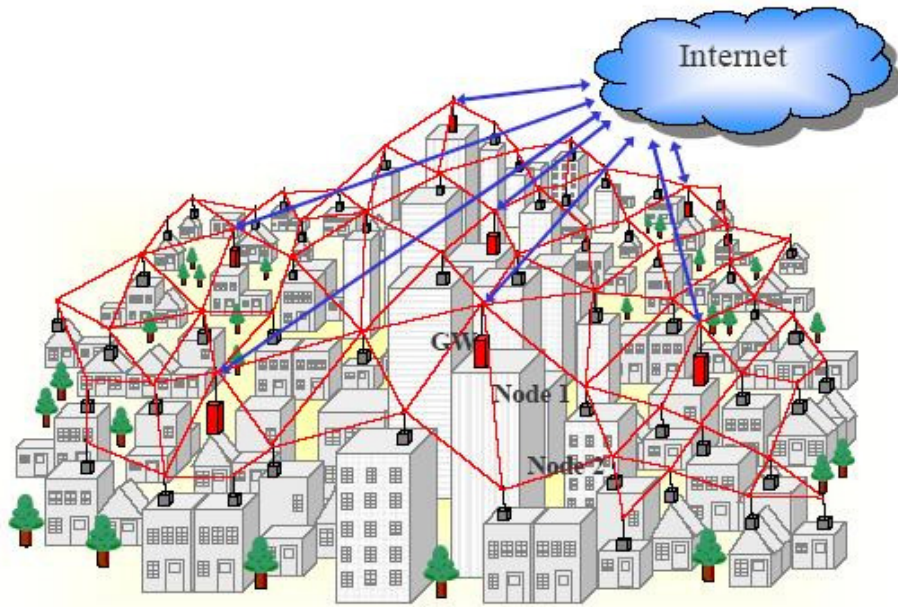


Figure 1. Réseau maillé sans fil

L'une des principales caractéristiques des WMNs est l'élimination des câbles. Compte tenu de cet aspect sans fil, les nœuds (MRs et passerelles) utilisent des transmissions sans ligne de vue pour communiquer entre eux. Malgré la présence des obstacles entre un émetteur et un récepteur, la communication peut s'établir, mais cela a pour effet de réduire considérablement la portée. Grâce à leurs faibles coûts d'installation et de maintenance, les WMNs sont donc devenus une solution intéressante pour les municipalités et les compagnies. Plusieurs villes des États-Unis, en l'occurrence Philadelphie, Medford, Chaska et Gilbert, [8] ainsi que des compagnies [12] les ont déjà déployés. Pour fournir une couverture et pour maintenir une connectivité aux clients, les routeurs sans fil s'auto-configurent et s'auto-organisent lors de leurs déploiements en formant une maille. Cette topologie possède plusieurs avantages (pour ne citer que quelques-uns d'entre eux) :

- L'interopérabilité : les WMNs sont capables d'interagir avec d'autres types de réseaux (filaire ou sans fil) et de relier plusieurs sources à l'Internet à travers une communication multi-sauts;
- La forte tolérance de pannes : lors de la communication entre deux nœuds distants, le trafic pourra être rerouté en cas de panne de l'un des éléments du réseau;

- L'équilibre de la charge : effectué grâce à l'existence de plusieurs chemins reliant les sources aux destinations;
- La forte capacité de mise en échelle : réalisée par un simple ajout de routeur sans fil ou de passerelle.

Typiquement, un réseau maillé sans fil se caractérise par le déploiement à l'intérieur ou à l'extérieur des routeurs sans fil et des passerelles. C'est une technologie prometteuse pour différentes applications, en l'occurrence, le *streaming* [13], la voix sur IP [14] et les applications multidiffusions [15]. L'ensemble de ces applications nécessite le routage de paquets au sein du WMN (depuis un point d'accès vers une passerelle et vice-versa en passant par les MRs). En outre, chaque application a ses propres besoins en termes de métrique de routage. Pour les applications temps réel, telles que la voix sur IP et les applications multidiffusions, le délai de bout-en-bout des paquets doit être contrôlé. Autrement, ces applications n'auront aucun intérêt auprès des utilisateurs. Quant aux applications classiques de l'Internet (non-temps réel), telles que le courriel, le web, le transfert de fichiers et les applications pair-à-pair (P2P), elles nécessitent plus de fiabilité de communication.

Grâce à leurs caractéristiques attrayantes, les réseaux maillés sans fil suscitent un grand intérêt auprès de la communauté de recherche dans le but d'évaluer et de proposer des solutions pour améliorer leurs performances. En effet, les métriques telles que la capacité, le délai et le taux de perte connaissent une dégradation lors d'une mise en place réelle de ces réseaux. Cette dégradation est due à de nombreux facteurs, tels que les effets de la propagation multi-sauts, les interférences, la congestion et les changements des conditions climatiques. La figure 2, présentée dans [16], montre jusqu'à quel niveau la bande passante dans un réseau maillé sans fil se dégrade en fonction du nombre de sauts traversés par les paquets envoyés depuis une source vers une destination. Il est à noter que dans cette figure, les routeurs sont dotés d'une seule carte réseau sans fil opérant dans les normes IEEE 802.11a/g ou IEEE 802.11 b [17].

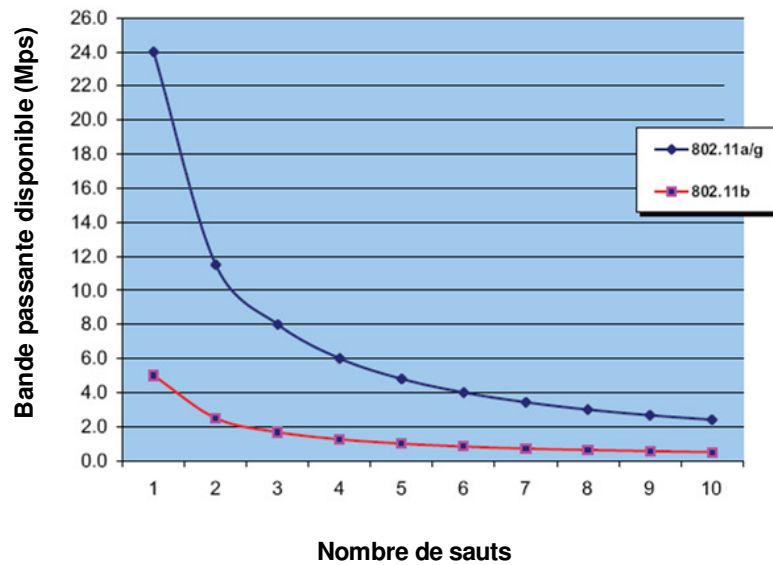


Figure 2. Dégradation des performances d'un réseau maillé sans fil

Ainsi, c'est dans le contexte des réseaux maillés sans fil que se situe ce travail de thèse. Plus particulièrement dans des réseaux (WMNs) multi-sauts où les routeurs sont statiques et dotés de plusieurs cartes réseau sans fil opérant dans les normes IEEE 802.11 et leur permettant de s'interconnecter. L'objectif de ce travail de thèse est de contribuer à mettre en place des solutions pour réaliser un routage adaptatif tout en maintenant la stabilité des réseaux.

## 1.2. Motivations

Les réseaux maillés sans fil visent à garantir une connectivité fiable aux utilisateurs. Ceci peut être réalisé grâce à l'épine dorsale, formée par les routeurs sans fil, qui produit une interopérabilité avec d'autres types de réseaux. Ils balayent un large spectre de technologies incluant les réseaux locaux sans fil utilisant la norme IEEE 802.11 (WLAN), les réseaux personnels sans fil (WPAN) utilisant la norme IEEE 802.15.4, les réseaux métropolitains sans fil (WMAN) utilisant la norme IEEE 802.16, pour ne citer que quelques-uns d'entre eux. Pour envoyer du trafic vers des destinations à l'extérieur du WMN, les points d'accès ne sont pas obligés d'avoir une connexion directe avec des passerelles. Ils peuvent envoyer le trafic vers des routeurs sans fil intermédiaires pour atteindre les passerelles. Par conséquent, le routage

dans les réseaux maillés sans fil joue un rôle important en étendant la connectivité du réseau aux utilisateurs finaux à travers une communication multi-sauts. Le routage est une fonctionnalité critique pour les WMNs vu la nature du médium partagé entre les routeurs sans fil et la variation de la capacité des liens. Plusieurs problèmes peuvent émerger émanant une dégradation des performances (augmentation des délais, par exemple); les causes majeures de ces problèmes sont la congestion et les interférences. La congestion fait référence à une situation où la quantité du trafic transmis à travers le réseau s'approche de sa capacité maximale. Pour leur part, les interférences sont causées par l'envoi simultané du trafic à partir de plusieurs routeurs sans fil voisins qui partagent le même canal de transmission.

Les performances des réseaux maillés sans fil peuvent être améliorées à l'aide de plusieurs approches, en l'occurrence, l'utilisation d'un système d'antennes directionnelles intelligentes [18], l'utilisation d'un système à multiples entrées et multiples sorties [19, 20] et l'utilisation d'un système multi-radios multi-canaux [21, 22]. Avec une seule radio et un seul canal, un routeur sans fil ne peut pas transmettre et recevoir simultanément. Toutefois, en raison du nombre restreint des canaux sans fil ainsi que de la nature limitée de leurs ressources (par exemple : la bande passante), d'un côté, et de la limite sur le nombre d'antennes de l'autre côté, la performance du réseau est fortement impactée par les interférences et la congestion. Ces derniers causent des pertes des paquets et une augmentation du délai de transmission d'une façon considérable. Dans ce cas, les techniques de routage peuvent jouer un rôle important dans l'amélioration des performances du réseau. Elles peuvent hautement améliorer les performances du réseau et assurer une bonne gestion des ressources. En effet, l'objectif principal d'un protocole de routage est de trouver des chemins optimaux en fonction de certains critères. Ces critères varient selon les besoins de chaque client (par exemple, la bande passante, le délai et la perte de paquets).

Pour assurer une bonne performance du réseau, un protocole de routage doit être qualifié par, entre autres, sa métrique de capturer les qualités des liens, son extensibilité, son temps de découverte des routes et sa stabilité. Dans la littérature, plusieurs protocoles de routage ont été proposés pour les réseaux ad-hoc. Certains ont considéré la mobilité des nœuds, d'autres, l'énergie consommée et d'autres, le nombre de sauts dans leur routage. Plusieurs chercheurs ont tenté d'appliquer ces protocoles de routage sur les réseaux maillés

sans fil. Cependant, dans les WMNs les routeurs sans fil ont une mobilité réduite/statique, et la contrainte d'énergie ne s'impose plus. Par conséquent, ces protocoles de routage ne peuvent pas être utilisés. Ainsi, des protocoles de routage mieux adaptés doivent être développés. Ils doivent maximiser le débit, minimiser le taux de perte, minimiser la latence et la gigue, prendre en compte la qualité des liens et assurer l'extensibilité du réseau.

### 1.3. Description des problèmes

Les réseaux maillés sans fil présentent l'avantage de supporter plusieurs types d'application contrairement aux autres réseaux sans fil (WSN, MANET). Parmi ces applications figurent les applications temps réel et les applications multimédias connues pour leurs fortes consommations de ressources. La figure 3 (extraite de [21]) présente pour chaque type d'application son besoin en terme de délai et de bande passante. Quelle que soit la nature de l'application à supporter, le routage joue un rôle important dans les WMNs. Pour router du trafic, chaque source doit trouver son chemin jusqu'au destinataire en s'appuyant sur une connaissance préalable des chemins ou en demandant un chemin partiel ou complet aux autres entités voisines.

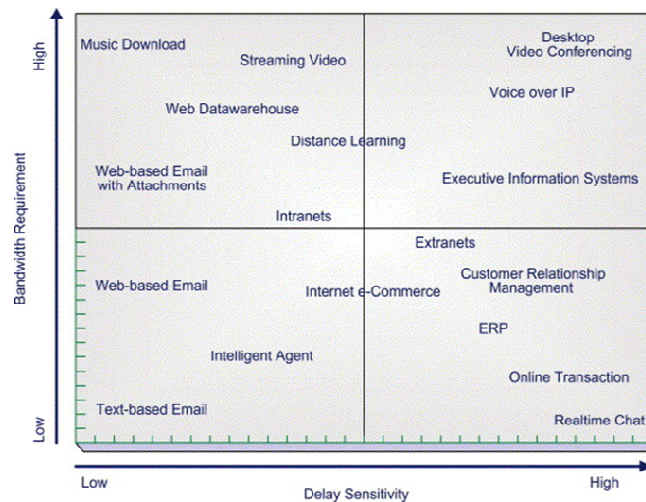


Figure 3. Besoin de QoS pour différentes applications

Les protocoles de routage dans les WMNs peuvent être classifiés en trois catégories : proactif, réactif ou hybride. Dans les protocoles proactifs, la stratégie de routage ressemble à celle utilisée dans les réseaux filaires. Chaque routeur sans fil connaît toute la topologie du



réseau et maintient une route vers n'importe quelle destination. Quant aux protocoles réactifs, la route est établie à la demande de la source au moment où elle dispose des paquets de données à envoyer. Finalement, les protocoles hybrides sont des solutions intermédiaires qui mixent les stratégies proactives et réactives dans le but de réduire la surcharge du réseau. L'ensemble de ces protocoles se heurte à de nombreuses difficultés étant donné qu'ils se basent sur des métriques dynamiques représentant la qualité des liens. Certains de ces protocoles ont essayé d'optimiser un seul objectif [24, 25], en l'occurrence les interférences, le taux de pertes et le délai. Or, il existe des situations où le choix d'une métrique à optimiser impacte négativement les performances du réseau en termes d'autres métriques. Prenons comme exemple la figure 4 (source [26]). Dans cette figure,  $A$ ,  $B$ ,  $C$ ,  $D$ ,  $E$  sont considérés des routeurs sans fil tandis que  $GW1$  et  $GW2$  sont des passerelles assurant une connectivité vers l'Internet. La charge de  $GW1$  et de  $GW2$  est de 40 % et de 60 % respectivement alors que la métrique de routage utilisée est une métrique additive représentant les interférences (IR). En se basant sur IR, quand une source  $S$  désire envoyer du trafic, elle va préférer le chemin  $S-D-A-GW2$  au chemin  $S-E-B-GW1$ . C'est le chemin ayant le moins d'interférence (somme des IR). Pourtant,  $GW2$  est plus congestionné que  $GW1$ . Il possède une charge à 60 %. Par contre, en choisissant la charge des passerelles comme étant une métrique de routage à utiliser, le protocole favorisera le chemin  $S-E-B-GW1$ .  $GW1$  est à 40 % de charge. Par conséquent, plusieurs métriques doivent être considérées en même temps lors de l'optimisation d'un protocole de routage multi-sauts.

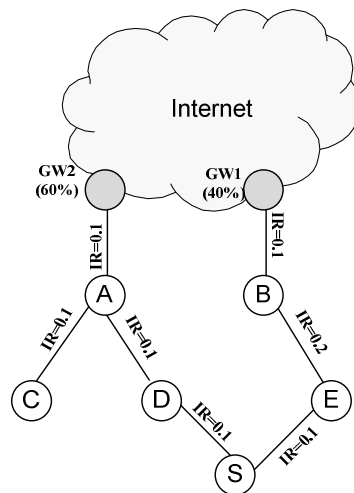


Figure 4. Problème d'utilisation d'une seule métrique

Trouver un chemin n'est qu'une partie des problèmes du routage dans les WMNs. L'une des utilisations fréquentes de ces réseaux est l'accès à l'Internet. Il est effectué grâce aux passerelles. En effet, en équipant un WMN d'une seule passerelle, le problème de routage devient simple. Chaque MR connaîtra la même passerelle et tous les flux vers ou en provenance de l'Internet passeront par elle. Par conséquent, cette dernière deviendra un goulot d'étranglement et un point unique de défaillance dans le réseau [27]. Généralement, un WMN contient plusieurs passerelles. Ainsi, le trafic prendra différents chemins vers différentes passerelles. Toutefois quand un MR connaît plus qu'une passerelle, le problème de routage devient non seulement de chercher le chemin optimal depuis une source, mais aussi de sélectionner la passerelle appropriée. Habituellement, les passerelles sont coûteuses et leur nombre est limité dans le WMN. Ainsi, dépendamment de la topologie du réseau, de la stratégie de routage et de la nature du trafic, d'autres problèmes, autres que le routage et la sélection des passerelles, peuvent exister. Une concentration du trafic autour des passerelles et les MRs qui leur sont voisins risque de se former en créant ainsi des zones critiques pour le trafic. Cela peut être le cas de la zone formée par la passerelle GW2 et le nœud A d'une part puis de la zone formée par la passerelle GW1 et le nœud B d'une autre part (voir figure 4). En outre, dans ces zones critiques, la congestion et le taux d'interférence sont plus élevés entraînant plus de pertes des paquets et de grands délais de transmission. Ainsi, les passerelles et les MRs identifiés faisant partie de la zone critique doivent bénéficier d'une attention particulière lors du calcul du chemin afin d'éviter les inconvénients susmentionnés et de permettre une amélioration des performances du réseau.

Les protocoles de routage dépendent des métriques de routage utilisées pour mesurer avec précision la qualité des liens. En général, une métrique de routage ne doit pas impacter négativement la stabilité du réseau; elle doit calculer les chemins dans un temps polynomial, capturer les caractéristiques du réseau (exemple, pertes de paquets et interférences) et éviter les boucles dans le routage. Parmi ces caractéristiques, la stabilité est considérée comme l'un des facteurs déterminants dans la performance du réseau. De nombreuses applications impliquant la Qualité de Service (QoS) comme la vidéo-conférence et les applications temps réel ont besoin d'un réseau stable pour assurer leurs continuités. Quand la qualité d'un lien change fréquemment, il devient instable. Ce phénomène se propage de MR à MR en créant

une oscillation des routes. Par conséquent, le réseau devient instable, ce qui a comme résultat la livraison en dehors de l'ordre (*Out-of-order delivery*) chez les destinations et une gigue élevée. En outre, l'instabilité du réseau peut provoquer également d'autres effets, en l'occurrence, le nombre de paquets perdus, le temps de convergence du réseau et la consommation des ressources (mémoire, CPU) qui augmentent. Pour illustrer ce phénomène, prenons comme exemple la figure 5 extraite de [28]. Dans cette figure R1, R2, R3, R4, R5 et R6 sont des MRs, R1 et R2, des sources du trafic vers l'Internet. G1 et G2 sont des passerelles, et la métrique utilisée par les chemins est une métrique cumulative représentée par le délai entre chaque paire MRs. Ainsi, le trafic entre R1 et G1 suivra le chemin R1-R4-G1 plutôt que R1-R3-R6-G1. C'est le chemin le moins coûteux entre les deux. Maintenant, supposons que les qualités des liens R3-R6 et R6-G1 deviennent 0.5 ms chacun. Le chemin R1-R3-R6-G1 sera plus favorisé que le chemin R1-R4-G1 pour envoyer du trafic de R1 en passant par G1. Par conséquent, certains paquets du même flux reroutés sur R1-R3-R6-G1 atteindront leur destination  $d$  dans l'Internet avant certains paquets déjà transmis sur R1-R4-G1. Ainsi, de nombreux paquets peuvent être livrés en dehors de l'ordre à la destination  $d$ .

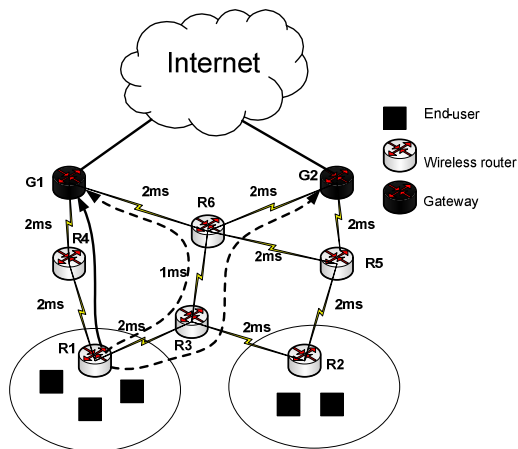


Figure 5. Problème d'oscillation des routes

La stabilité dans les réseaux maillés sans fil est donc un des problèmes à considérer. Contrairement aux liaisons filaires, les liaisons sans fil ont souvent de fréquentes variations de la bande passante. Des facteurs tels que les interférences et les variations des signaux dues aux effets de masque (*shadowing*) ou aux réflexions sur les obstacles (*fading*) en sont la cause. Ils créent des oscillations des routes lors de la transmission des données et par la suite, une

instabilité du réseau. Ce problème est d'autant plus critique relativement au nombre des routeurs sans fil et à la quantité du trafic qui circule dans le réseau.

## 1.4. Contributions

Face aux problèmes soulevés dans la section précédente, en l'occurrence, la conception d'une métrique de routage, la sélection des passerelles, l'utilisation des zones critiques et la stabilité, il convient donc de proposer des solutions afin d'améliorer les performances des réseaux maillés sans fil. Ainsi, comme solutions, nous présentons trois contributions représentant le corps de cette thèse. Elles concernent des métriques modélisant la qualité des liens, un routage adaptatif et des métriques modélisant la stabilité du réseau.

Pour la première contribution, nous abordons le problème du choix des passerelles et le routage dans un réseau maillé sans fil. Pour cela, nous proposons un routage à la source basé sur une nouvelle métrique appelée BP2BG (*Best Path to Best Gateway*). BP2BG est calculée en fonction de plusieurs paramètres : (1) les interférences (*Interference Ratio* (IR)) où, en nous basant sur un modèle physique existant, nous capturons différents types d'interférences dites « *interférences inter-flux* » et « *interférences intra-flux* »; (2) le taux de pertes des paquets (*Expected Link Quality* (ELQ)) dont la technique de mesure est légèrement semblable à ETX (*Expected Transmission Count*), mais à poids différents pour chaque sens de liaison d'un lien (*backward/forward*); et (3) la surcharge des passerelles représentée par la métrique DACI (*Distribution Available Capacity Indicator*) qui donne, en plus de l'information sur la capacité, de l'information sur la distribution du trafic entre les différentes interfaces de la passerelle. Tous ces paramètres sont encapsulés dans des messages GWADV (*Gateways Advertisement message*) initiés et envoyés périodiquement par les passerelles dans les réseaux. BP2BG améliore de façon considérable les performances du réseau WMN par rapport aux travaux antérieurs trouvés dans la littérature. Cette contribution fera l'objet du chapitre 3 de cette thèse. Le contenu de ce chapitre a été soumis pour publication à la revue *Wireless Communications and Mobile Computing* : Mustapha Boushaba, Abdelhakim Hafid et Michel Gendreau, *Source-based Routing in Wireless Mesh Networks*.

La deuxième contribution est consacrée aux problèmes des zones critiques qui se trouvent autour des passerelles et à leurs impacts sur le routage. Comme nous l'avons précisé

dans la section précédente, une concentration du trafic autour des passerelles et des MRs qui leur sont voisins risque de se former créant ainsi des zones critiques dans les WMNs. Pour cela, nous proposons un routage proactif et adaptatif, appelé RLBDP (*Reinforcement Learning-based Distributed Routing*) capable de prendre en considération ces zones en attribuant plus d'importance (poids) aux liens aux alentours des passerelles. RLBDP utilise l'apprentissage par renforcement et plus particulièrement le *Q-learning* pour apprendre le meilleur routeur sans fil (MR) voisin pour transmettre un paquet entrant vers une passerelle donnée. Dans RLBDP, l'apprentissage par renforcement est utilisé pour mettre à jour dynamiquement les coûts de chemin et pour choisir le prochain nœud voisin chaque fois qu'un paquet est transmis. Pour cela, des agents sont placés dans chaque nœud du réseau WMN et apprennent continuellement le meilleur lien pour transmettre les paquets entrants, exploitent ce qui a été appris dans le passé et explorent de nouvelles solutions pour découvrir de meilleures actions dans le futur. RLBDP est constitué de quatre phases principales : (1) Échange des messages d'avertissement, GWADV, entre les MRs; ces messages sont périodiquement envoyés par les passerelles; (2) mesure de la qualité des liens en termes de certaines métriques, en l'occurrence les interférences et le taux de pertes; (3) sélection, par chaque routeur sans fil, de la meilleure passerelle pour accéder à l'Internet; (4) utilisation des agents d'apprentissage afin de choisir le nœud voisin prochain approprié pour transmettre le trafic. Cette contribution fera l'objet du chapitre 4 de cette thèse. Le contenu de ce chapitre a été accepté pour publication dans la revue pour publication à la revue *ACM Wireless Networks (WINET)* : Mustapha Boushaba, Abdelhakim Hafid, Abdeltouab Belbekkouche et Michel Gendreau, *Reinforcement Learning Based Routing in Wireless Mesh Networks*.

La troisième contribution est consacrée aux problèmes de la stabilité dans les WMNs. En effet, l'instabilité de ces réseaux est la plupart du temps causée par le changement fréquent des routes à cause de la variation de la qualité des liens entre les MRs. Un niveau élevé d'instabilité risque de créer des interférences et des pertes de données et augmente le délai de transmission des paquets. Pour cette contribution, nous considérons, d'abord, les facteurs clés susceptibles de provoquer l'instabilité des WMNs puis nous présentons un protocole de routage proactif basé sur une nouvelle métrique appelée NS (*Node Stability*). L'objectif est de router les paquets à travers des routeurs sans fil stables afin de ne pas impacter négativement

la stabilité du réseau. NS utilise le principe de la fonction d'entropie, connu dans les mesures de l'incertitude et du désordre des systèmes, pour quantifier la stabilité de chaque routeur sans fil dans le WMN. Ainsi, grâce à l'utilisation de NS et lors de la réception d'un paquet, un MR sélectionne le prochain routeur le plus stable pour transmettre des paquets vers une passerelle sélectionnée. En plus des problèmes de stabilité, nous soulevons également à ce niveau le problème de sélection des passerelles pour envoyer du trafic vers l'Internet. Ainsi, nous proposons une nouvelle technique de sélection des passerelles basée sur des probabilités plutôt que sur la surcharge des passerelles permettant de contribuer à la réduction du nombre de routes dans le réseau. Cette contribution fera l'objet du chapitre 5 de cette thèse. Le contenu de ce chapitre a été soumis pour publication à la revue *ACM Transactions on Autonomous and Adaptive Systems* : Mustapha Boushaba, Abdelhakim Hafid et Michel Gendreau, *Node Stability Based Routing in Wireless Mesh Networks*.

## **1.5. Organisation de la thèse**

Le corps de cette thèse est organisé comme suit : après ce chapitre introductif, le chapitre 2 présente une brève description des réseaux WMNs et une revue de la littérature sur les sujets reliés à cette thèse, plus particulièrement, nous allons aborder les techniques de mesure, les métriques, le routage et la stabilité dans les WMNs. Dans le chapitre 3, nous présentons en format article notre première contribution sur le routage basé sur la nouvelle métrique BP2BG. Dans le chapitre 4, nous proposons notre deuxième contribution, RLBDR, qui consiste en un protocole de routage proactif adaptatif basé sur la technique d'apprentissage par renforcement et qui attribue plus de poids aux routeurs aux alentours des passerelles. Dans le chapitre 5, nous présentons notre troisième contribution basée sur la stabilité dans les WMNs. Elle a pour objet de définir la stabilité d'un routeur comme métrique et de l'utiliser dans notre protocole de routage. Finalement, nous concluons ce travail avec le chapitre 6 en dressant quelques perspectives de recherche pour les travaux futurs.

## **1.6. Articles publiés/soumis durant cette thèse**

1. Mustapha Boushaba, Abdelhakim Hafid et Michel Gendreau, Source-based Routing in Wireless Mesh Networks, soumis dans Wireless Communications and Mobile Computing, 2013
2. Mustapha Boushaba, Abdelhakim Hafid, Abdeltouab Belbekkouche et Michel Gendreau, Reinforcement Learning Based Routing in Wireless Mesh Networks, accepté pour publication dans ACM Wireless Networks (WINET) , 2013
3. Mustapha Boushaba, Abdelhakim Hafid et Michel Gendreau, Node Stability Based Routing in Wireless Mesh Networks, soumis dans ACM Transactions on Autonomous and Adaptive Systems, 2013
4. Mustapha Boushaba, Abdelhakim Hafid and Michel Gendreau, Local Node Stability-Based Routing for Wireless Mesh Networks, WCNC 2013
5. Mustapha Boushaba, Abdelhakim Hafid and Abdeltouab Belbekkouche, Reinforcement Learning-based Best Path to Best Gateway Scheme for Wireless Mesh Networks, IEEE WIMOB, 2011
6. Ahmed Beljadid, Abdelhakim Hafid and Mustapha Boushaba, Design of Reliable Wireless Mesh Networks, IEEE GLOBECOM, 2011
7. Mustapha Boushaba and Abdelhakim Hafid, Best Path to Best Gateway Scheme for Multichannel Multi-interface Wireless Mesh Networks, IEEE WCNC, 2011
8. Mustapha Boushaba, Abdelhakim Hafid and Sarr Yayé, MBP: Routing Metric Based on Probabilities for Multiradio Multi-channel Wireless Mesh Networks, IEEE IWCMC 2011

## **Chapitre 2 : Revue de la littérature**

Dans ce chapitre, nous présentons en premier les réseaux maillés sans fil, leurs architectures, leurs fonctionnalités ainsi que les applications qui les utilisent. Par la suite nous passons en revue les travaux réalisés dans le contexte des métriques de routage, les protocoles de routage et la stabilité dans les WMNs.

### **2.1. Les réseaux maillés sans fil**

Les WMNs ont été introduits dans le but d'assurer un accès à haut débit n'importe où et n'importe quand. En effet, ces réseaux produisent une meilleure connectivité et à faible coût comparativement aux réseaux filaires qui en plus de leurs coûts élevés supposent que les clients sont immobiles. Les WMNs sont des réseaux dont la communication entre les nœuds s'effectue à travers des connexions sans fil. Deux nœuds sans fil communiquent s'ils se trouvent dans le même rayon de transmission et s'ils partagent le même canal de communication. À l'aide des connexions sans fil, les WMNs permettent de transférer des données depuis une source vers une destination en passant par plusieurs nœuds intermédiaires. Ainsi, on parle d'une communication multi-sauts.

Une maille dans les WMNs est constituée par plusieurs nœuds qui peuvent être de deux types : clients maillés (MCs) et MRs. Un client maillé (MC) peut être la source ou la destination des connections ; ainsi, il joue le rôle d'utilisateur final. Parfois, les MCs se caractérisent par leur mobilité et leur participation au routage des données mais avec moins de performance que les MRs. Souvent, les MCs sont équipés d'une seule carte réseau sans fil et les batteries représentent leurs sources d'énergie. Ensemble, les MCs peuvent coopérer pour former une maille avec une grande variété d'équipements (ordinateurs portatifs, assistants personnels PDA, téléphone IP, etc.). Les MRs disposent de plusieurs fonctionnalités (p.ex., routage et inter-connectivité) qui les rendent assez performants. Une des caractéristiques techniques des MRs c'est qu'ils opèrent avec une ou plusieurs cartes réseau sans fil munis de plusieurs canaux et transmettant les données sur de très grands rayons. Selon leurs fonctions, les MRs peuvent être : des points d'accès, des relais, ou des passerelles. Les points d'accès (AP) sont des nœuds permettant de recevoir et d'acheminer le trafic des utilisateurs vers le



reste du réseau ; ce sont des points d'entrées des MCs vers le réseau. Quant aux relais, ils représentent l'ensemble des nœuds intermédiaires permettant de relier deux utilisateurs finaux. Leurs fonctions principales est d'étendre la connectivité et de router les paquets en tentant de satisfaire la QoS (Qualité de Service) requise par les utilisateurs. Finalement, les passerelles sont des routeurs sans fils assez spéciaux qui possèdent au moins deux types de cartes réseaux : une carte sans fil permettant de les relier au WMN et une autre carte filaire ou sans fil (p.ex., WiMAX) pour les connecter à l'Internet.

### 2.1.1. Architecture des réseaux maillés sans fil

Il existe une multitude de variantes des réseaux maillés sans fil. Typiquement, ils sont classés par leur utilisation finale et par la mobilité des nœuds (MCs, MRs) qui les constituent. On distingue trois différentes architectures [4]: architecture avec infrastructure/épine dorsale, architecture client et architecture hybride.

#### 2.1.1.1. Architecture Infrastructure/épine dorsale

Dans ce type d'architecture, le réseau est constitué d'un ensemble de MRs qui fournissent une infrastructure pour les clients afin de les connecter entre eux ou vers l'Internet en passant par des passerelles. La figure 6 extraite de [4] illustre un exemple de cette architecture.



Figure 6. Architecture des réseaux maillés sans fil: épine dorsale [4]

Menés d'une technologie sans fil multi-radio multi-canaux, le plus souvent IEEE 802.11, les MRs dans un réseau avec infrastructure jouent un rôle important dans le routage, l'auto-configuration et la tolérance aux pannes. De plus, ils permettent d'intégrer facilement d'autres réseaux sans fil. Les réseaux de senseurs (WSNs) et les réseaux WiMAX (*Worldwide Interoperability for Microwave Access*) sont, entre autres, des exemples des technologies pouvant utiliser cette architecture.

### 2.1.1.2. Architecture client

Les WMNs clients sont des réseaux auto-organisés et auto-configurables permettant, ainsi, d'assurer le bon fonctionnement des applications. Dans cette architecture (voir figure 7 extraite de [4]), les MCs s'interconnectent pour former une maille permettant d'assurer une connexion paire-à-paire entre différents utilisateurs. Les MCs sont les seuls constructeurs de la maille ; ils sont dotés d'une seule technologie radio, peuvent être mobiles et participent au routage des données.

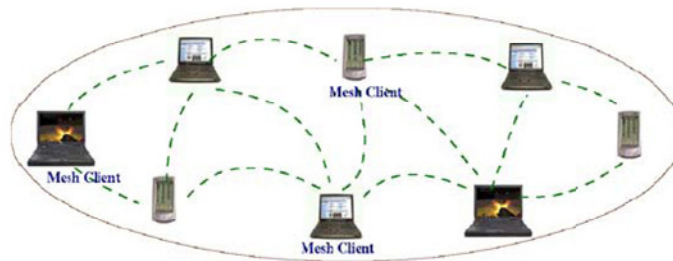


Figure 7. Architecture des réseaux maillés sans fil: cas client [4]

### 2.1.1.3. Architecture hybride

Cette architecture (voir la figure 8 [4]) est une combinaison des deux architectures précédentes (Infrastructure et client). Elle permet aux clients maillés d'accéder au réseau maillé sans fil à travers des MRs maillés ou directement en utilisant les autres clients maillés. Dans ce cas, les MRs maillés auront la fonction d'assurer la couverture tandis que les clients maillés vont permettre de renforcer la connectivité et d'améliorer la couverture.

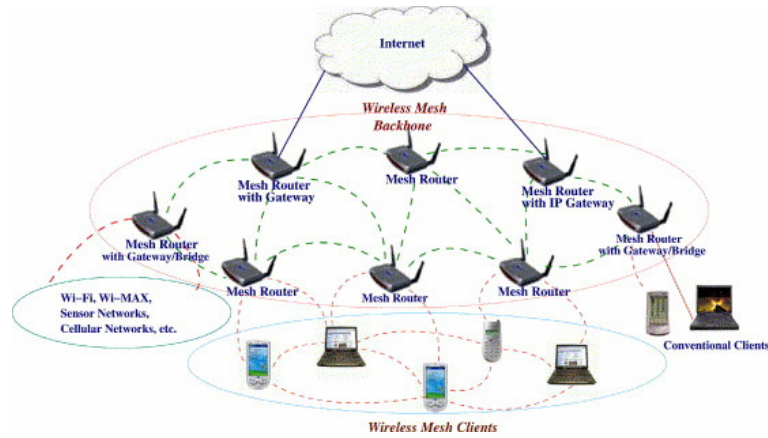


Figure 8. Architecture des réseaux maillés sans fil: cas hybride [4]

## 2.1.2. Les communications sans fil

Afin d'établir des communications, les nœuds d'un réseau sans fil se basent principalement sur des liaisons radio ou infrarouge. Il existe plusieurs technologies de communication sans fil permettant d'offrir un accès à haut débit. La figure 9 présente quelques exemples de ces technologies classées selon leurs portées et leurs débits.

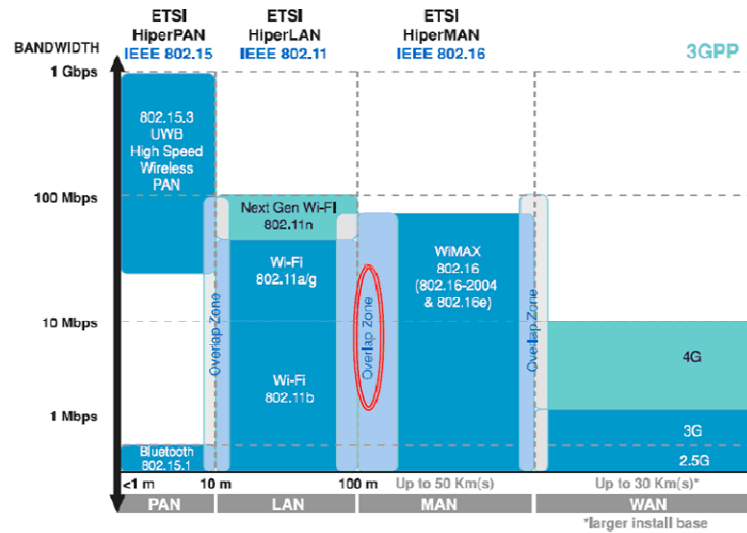


Figure 9 . Classification des technologies sans fil [29]

Parmi ces technologies figurent le WiFi et le WiMAX comme étant les plus répandues et qui permettent d'avoir un accès vers l'Internet. Ils utilisent les normes IEEE 802.11 et IEEE 802.16, respectivement.

La norme IEEE 802.11 s'impose de plus en plus dans le marché et devient la plus utilisée dans les WMNs. Généralement, les équipements qui l'implémentent ont des portées qui varient de quelques dizaines à quelques centaines de mètres en fonction des débits et de l'environnement. Toutefois, ils peuvent s'interconnecter pour assurer une communication multi-sauts. Dépendamment de la bande de fréquence utilisée, il existe une multitude de versions basées sur IEEE 802.11. Parmi ces versions figurent IEEE 802.11b, IEEE 802.11g qui utilisent la bande de fréquence 2,4 Ghz, IEEE 802.11a qui utilise la bande de fréquence 5 GHz et IEEE 802.11n qui utilise aussi bien la bande de fréquence 2,4 Ghz que la bande de fréquence 5 Ghz. Les débits possibles peuvent varier de 1 à 54Mbps dépendamment de la version utilisée (IEEE 802.11, IEEE 802.11a, IEEE 802.11b, IEEE 802.11g). Toutefois, ils peuvent atteindre 100 Mbps pour la version IEEE 802.11n.

La norme IEEE 802.16, connue aussi sous le nom « commercial WiMAX », est destinée à offrir un accès à haut débit à l'Internet dans des régions métropolitaines et des secteurs périurbains. Initialement, la norme IEEE802.16 a été mise en place grâce aux liaisons fixes point à multipoints, où un ou plusieurs émetteurs/récepteurs centralisés par zone de couverture desservant plusieurs terminaux (*Subscriber Stations- SS*). Par la suite, le standard a évolué en donnant naissance à la notion de maille [30]. Dans ce mode maillé, les *SSs* peuvent non seulement établir des connections directes aux stations de base (cas du point à multipoints), mais également établir des connections entre eux. Ainsi, même si une *SS* ne se trouve pas dans la zone de couverture d'une station de base, le trafic lui sera transmis d'une façon multi-sauts. Par conséquent, les *SSs* participeront au routage.

La norme IEEE 802.16 a l'avantage de permettre des connexions de haut débit sur des dizaines de kilomètres par rapport à la norme IEEE 802.11. Toutefois certaines limitations s'imposent, en l'occurrence, le problème de la QoS de bout-en-bout [31]. L'ensemble des deux normes peuvent être supportées par un même routeur sans fil offrant d'une part une interface WiFi lui permettant de se connecter à un réseau WLAN [32] et d'autre part une interface WiMAX pour se connecter à un réseau MAN [32]

### 2.1.3. Les applications déployées dans les WMNs

Vu l'importance des WMNs, plusieurs applications ont été proposées dans la littérature. Nous en résumons quelques unes [4, 12] dans cette section. Le *Broad Home Networking* qui consiste à échanger les données entre les équipements d'un même foyer et éventuellement les connecter à l'Internet à travers des points d'accès. C'est une application basée principalement sur la norme IEEE 802.11 qui présente certaines limites. La présence des zones non couvertes dans le foyer et les communications entre les équipements qui doivent passer impérativement par les points d'accès (APs) ne sont que quelques exemples de ces limites. L'introduction des MRs au lieu des APs afin de former un WMN comme infrastructure de communication pour ce type d'application devient une solution prometteuse.

La sûreté publique est l'une des applications prometteuse des WMNs. Elle peut être utilisée par tous les services publics, en l'occurrence, la police, les pompiers et les services d'urgences médicales. Dépendamment de l'utilité de l'application, elle nécessite dans la plupart du temps l'utilisation d'autres équipements (p.ex., ordinateurs portables, PDAs et des caméras de surveillance mobiles). Actuellement, plusieurs de ces services utilisent des WMNs comme infrastructure de communication au lieu des réseaux câblés pour connecter les différents équipements. Toutefois, les images et les vidéos restent le plus important trafic qui circule dans ce réseau ; par conséquent, cette application exige beaucoup plus de capacité que d'autres applications.

L'utilisation des WMNs dans les régions métropolitains [4, 12] présente beaucoup d'avantages dont: (1) Le taux de transmission dans la couche physique est beaucoup plus élevé que n'importe quel autre réseau cellulaire actuel; (2) De point de vue du déploiement, il est plus économique d'utiliser les WMNs pour les accès à haut débit plutôt que les réseaux filaires ou optiques; (3) Grâce à l'utilisation d'une communication NLOS (*Non-Line-of-Sight*) et multi-sauts entre les nœuds, une zone de service plus large est offerte. Étant donné la largeur de ces zones, qui dépasse bien celle des foyers, des entreprises et des bâtiments, la mise en échelle devient un facteur important à considérer dans ces applications.

Dans les systèmes de transport, au lieu de limiter les accès à l'aide des normes IEEE 802.11 ou IEEE 802.16 aux gares ou aux arrêts, les WMNs peuvent l'étendre aux autobus, aux

trains et aux véhicules. Par conséquent, plusieurs informations seront à la portée des voyageurs. En outre, la surveillance à distance et la communication inter-véhiculaires peuvent être supportées.

Pour plusieurs autres applications, les WMNs sont utilisés dans le but de réduire les coûts d'installation et de maintenance d'une part et d'améliorer la fiabilité et la mise à l'échelle d'autre part. Pour plus de détails, nous référons le lecteur aux références [4, 33].

#### **2.1.4. Quelques problèmes liés à l'utilisation du canal sans fil**

Malgré les avantages que présentent les WMNs, plusieurs facteurs dégradent leur performance. Parmi ces facteurs figurent les techniques radios utilisées, l'atténuation du signal, les interférences pour ne citer que quelques exemples liés à la radio.

##### **2.1.4.1. Les techniques radios utilisées**

Grâce à l'évolution technologique et plus particulièrement à l'évolution des semi-conducteurs et la radio fréquence, les cartes radios ont fait l'objet d'une importante révolution. Actuellement, de nombreuses approches ont été proposées pour augmenter la capacité et la flexibilité des réseaux maillés sans fil. Les technologies MIMO (*Multiple-Input Multiple-Output*) [19, 20], multi-radios/multi-canaux [21, 22] et les antennes directionnelles intelligentes [18] en sont quelques exemples. Toutefois, l'utilisation de ces technologies nécessite une conception révolutionnaire dans les protocoles des couches supérieures. Par exemple, lorsque les antennes directionnelles ou plusieurs interfaces sont utilisées dans des réseaux IEEE 802.11, un protocole de routage doit tenir compte de la sélection d'antenne directionnelle ou de l'interface adéquate.

##### **2.1.4.2. L'atténuation du signal**

Elle peut être due à l'augmentation de la distance entre une source et une destination ou à la présence d'obstacles qui interrompent la ligne de visée (p.ex., immeubles et collines). Par conséquent, le signal radio devient plus faible et la portée des signaux diminue.

### 2.1.4.3. Les interférences

Une interférence se produit à chaque fois que deux nœuds, qui utilisent le même canal de transmission dans la même portée transmettent des données en même temps. C'est un des facteurs majeurs qui affecte considérablement les performances des WMNs [34] en augmentant le taux de perte de paquets. Dans la littérature, on distingue principalement deux types d'interférences : interférences inter-flux et interférences intra-flux. Les interférences inter-flux sont causées par les flux qui utilisent le même canal de transmission et qui provoquent une complétion au support. La figure 10 (a) illustre ce type d'interférences. Dans ce cas, les nœuds *C* et *E* provoquent des interférences inter-flux en envoyant du trafic vers *D* et *F*, respectivement (on suppose que *C*, *D*, *E* et *F* utilisent le même canal de transmission). Il est donc primordial pour une métrique de routage de capturer ce phénomène et d'aider le protocole de routage à balancer la charge du trafic et réduire les interférences.

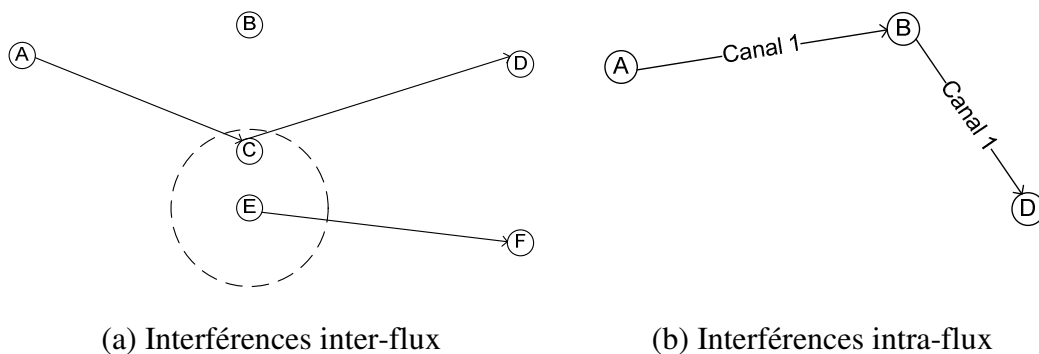


Figure 10. Exemple des interférences dans un réseau maillé sans fil

Les interférences intra-flux se produisent quand deux ou plusieurs liens successifs sur le même chemin partagent le même canal. La figure 10 (b) illustre ce problème, où l'interférence est créée à chaque fois que les nœuds *A* et *B* envoient des données en même temps (*A*, *B* et *C* utilisent le même canal). Par conséquent, le taux de pertes des paquets augmente et la bande passante disponible se réduit à moitié [35]. Une des solutions envisageables est d'augmenter la diversité des canaux [34], autrement dit utiliser plusieurs canaux distincts sur un même chemin.

Pour éviter les interférences, il a été proposé d'utiliser plusieurs interfaces radios par nœud opérant sur des canaux distincts [21, 22, 36]. Toutefois, cette solution ne résout que

partiellement le problème des interférences étant donné que le nombre des canaux est limité. Le problème devient plus complexe quand le nombre de nœuds dans le WMN augmente. Le coût de déploiement du WMN augmente aussi.

Dans le cadre des WMNs basés sur la norme IEEE 802.11, le taux d'interférence dépend de plusieurs facteurs tels que la topologie du réseau et le trafic entre les nœuds. Il existe trois principaux modèles d'interférence dans la littérature : modèle protocole, modèle logique et modèle physique [37, 38]. Ces trois modèles sont influencés par trois types de portées des radios [39, 40] à savoir la portée de transmission ( $R_{tx}$ ), la portée de détection de porteuse ( $R_{cs}$ ) (*Carrier sensing range*) et la portée d'interférence ( $R_i$ ). Comme illustré dans la figure 11, une portée de transmission ( $R_{tx}$ ) désigne la portée depuis un émetteur dont le signal radio peut être correctement reçu au moment où il n'y a aucune interférence du côté des nœuds voisins. La portée de détection de porteuse ( $R_{cs}$ ) est la portée à partir de laquelle un nœud peut détecter un signal sans qu'il soit nécessairement bien reçu. Dans la figure 11, le nœud C est dans la portée de détection de porteuse du nœud B. Finalement, la portée d'interférence ( $R_i$ ) est la portée à partir de laquelle des nœuds en mode réception peuvent s'interférer avec un nœud émetteur. Il est à noter que dans tous les cas  $R_{tx} < R_i < R_{cs}$  [34]. Ainsi, en se basant sur ces définitions, les nœuds cachés [39] qu'on retrouve assez souvent dans ces réseaux et qui sont la source de plusieurs collisions et de pertes de paquets seront les nœuds qui se situent dans la portée d'interférence d'un nœud récepteur et hors de la portée de détection de porteuse d'un nœud émetteur. Tel est le cas pour le nœud C dans la figure 11.

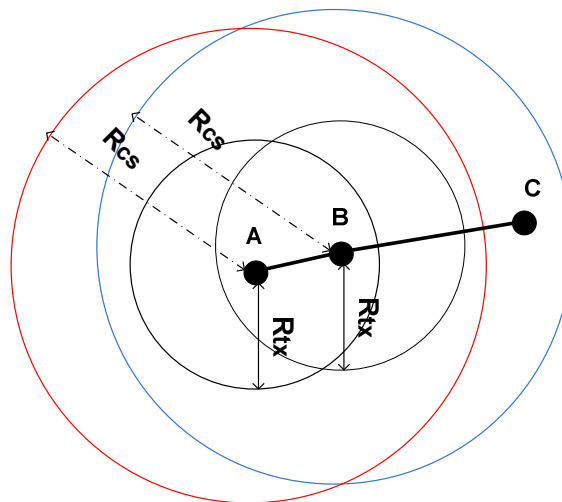


Figure 11. Exemple des portées



Dans le premier modèle d'interférence (modèle protocole) [34] la réussite d'une transmission entre deux nœuds nécessite la satisfaction de deux conditions: (1) le nœud récepteur doit être dans la portée de transmission de l'émetteur; et (2) un nœud ne peut ni envoyer ni recevoir ni transmettre à plus d'un autre nœud en même temps. De plus, ce modèle a été conçu pour garantir que les liens ne s'interfèrent pas. Toutefois, il ne s'intéresse qu'à l'interférence qui se produit avant la transmission [41]. Le modèle d'interférence logique [42] connu aussi sous le nom de *Channel Contention Interference* fait référence au protocole avec écoute de porteuse (p.ex., CSMA/CA) qui oblige la station émettrice d'attendre jusqu'à ce que le canal soit libre pour commencer à transmettre. Ainsi, l'interférence est mesurée en fonction du temps que prend un nœud pour accéder au canal. Ce temps varie en fonction du nombre de nœuds qui tentent d'utiliser le canal (nœuds en interférences). Comme le modèle protocole, le modèle logique donne une information sur l'interférence avant la transmission [41]. Finalement, le modèle d'interférence physique capture les interférences dans la couche physique. Cette interférence physique représente la superposition des ondes provoquant des altérations des signaux. Il détermine qu'une transmission d'un nœud A vers un nœud B est réussie seulement si la force du signal à B dépasse un certain seuil. Ainsi, le modèle d'interférence physique dépend des caractéristiques réelles du canal et représente l'interférence qui se produit lors de la transmission. Pour mesurer l'interférence au niveau physique, plusieurs techniques ont été proposées dans la littérature en l'occurrence RSSI (*Received Signal Strength Indication*), BER (*Bit Error Rate*), FER (*Frame Error Rate*) et SINR (*Signal to Interference plus Noise Ratio*). Pour plus de détails, nous référons le lecteur à [41, 43, 44].

## **2.2. Routage dans les réseaux sans fil**

Le routage est une fonctionnalité principale dans les réseaux sans fil. Il consiste à sélectionner un ou plusieurs chemins pour acheminer du trafic d'une source vers une destination. Cette sélection se base principalement sur l'utilisation des métriques issues des mesures et associées aux liens et aux chemins. Contrairement aux réseaux ad-hoc, le routage dans les WMNs nécessite plus de particularités puisque dans la plupart du temps les nœuds sont multi-radios, multicanaux et stationnaires. Dans cette section, nous passerons en revue les

techniques de mesures, les métriques de routage, les protocoles de routage, la prédiction et la stabilité dans les réseaux sans fil.

### **2.2.1. Techniques de mesure des qualités des liens**

Dans les WMNs la qualité des liens varie constamment à cause de l'existence de certains facteurs en l'occurrence les interférences et le trafic qui circule. Ainsi, des mesures précises des qualités des liens serviront de base pour définir d'une part des métriques aux protocoles de routage [4] et d'assignation des canaux [45], et d'autre part pour aider à diagnostiquer le réseau en cas de pannes [46]. Nous classifions les techniques de mesure en trois grandes classes : les mesures actives, les mesures passives et les mesures hybrides.

Le principe des mesures actives consiste à injecter périodiquement du trafic de contrôle dans le réseau à étudier, puis observer les effets des composants et protocoles sur ce trafic (p.ex., taux de perte, délai, RTT (*Round Trip Time*) et topologie). Il existe de nombreux outils de test et de validation qui implémentent ce principe depuis les réseaux filaires parmi lesquels les célèbres commandes *Ping* et *traceroute*. En effet, l'approche des mesures actives reste la seule qui permet à un utilisateur de mesurer les paramètres du service dont il pourra bénéficier. De plus, elle est exclusivement dédiée à des mesures de performance du réseau. En revanche, l'inconvénient majeur des mesures actives est la perturbation introduite par le trafic de mesure qui peut faire évoluer l'état du réseau et ainsi fausser les mesures. Dans les WMNs, les métriques ETX (*Expected Transmission Count* [24]) et ETT (*Expected Transmission Time* [25]), utilisées par certains algorithmes de routage et les mesures de la bande passante de bout-en-bout [47] que nous décrivons plus tard dans ce chapitre, sont quelques exemples qui utilisent la technique de mesure active.

Les mesures passives nécessitent des systèmes relativement avancés de capture du trafic en transit. D'habitude, ces mesures sont faites par la couche MAC de la carte réseau sans fil à condition que cette dernière le permette. Le principe des mesures passives est d'observer le trafic et d'étudier ses propriétés en un ou plusieurs points du réseau sans injecter des paquets de contrôle. Toutes les métriques qui implémentent le modèle d'interférence physique en l'occurrence RSSI, BER, FER et SINR [41, 43, 44] sont des exemples de mesures passives. Cette technique de mesure a l'avantage d'être correcte et ne change en rien l'état du réseau car

elle exploite le trafic réel. Par contre, son inconvénient majeur réside dans le cas où la quantité de trafic est basse. En effet, avec peu de trafic dans le réseau les mesures prises sur les états des liens ne refléteront plus la réalité. Ces mesures risquent d'être influencées par les variations climatiques ou par simplement l'existence d'un nœud en panne.

Les mesures hybrides se situent entre les mesures actives et les mesures passives. Elles sont utilisées dans le but de résoudre le problème de la surcharge du réseau créé par l'injection des paquets de mesures utilisés par les techniques actives d'une part et par l'imprécision des techniques passives due parfois au manque du trafic à mesurer. Leur principe repose sur un mécanisme d'adaptation automatique entre les deux techniques de mesures (active et passive). EAR (*Efficient and Accurate Link quality monitoR*) [46] est un exemple des méthodes hybrides. Dans le but de réduire la surcharge du réseau, EAR utilise trois méthodes de mesure et d'échange d'information : passive, active et coopérative. La méthode passive est utilisée quand il y a suffisamment de trafic sortant. À cet effet, une trace de mesure basée sur les paquets envoyés est conservée par chaque nœud actif. Par ailleurs, la migration vers une technique coopérative est observée dans des situations où un lien dit  $A-B$  n'est pas actif alors que celui d'un autre dit  $A-C$  est actif ( $A$ ,  $B$  et  $C$  utilisent le même canal de communication). Lors d'une diffusion, un nœud  $B$  peut écouter et recenser le trafic depuis  $A$  vers  $C$  et aviser des voisins par cette mesure. Finalement, quand le trafic est inférieur à un seuil prédéfini, le protocole passe en mode de mesures actives et permet à un nœud  $A$  d'envoyer périodiquement des paquets de mesure à un autre nœud  $B$  au sommet de chaque intervalle tant que le lien  $A-B$  reste stable. L'avantage d'EAR réside dans le fait qu'il réduit le nombre de paquets de mesure et améliore la précision des mesures. Cependant, il souffre d'un ensemble d'inconvénients liés au choix des métriques utilisées et non pas à la technique utilisée. En l'occurrence, les interférences ne sont pas prises en considération et le calcul de la capacité des liens est imprécis.

### **2.2.2. Les métriques de routage**

Une métrique est une propriété d'un lien ou un ensemble de liens (formant une route) utilisée par des algorithmes de routage pour distinguer la qualité des différentes routes. Sur une route, elle pourra être calculée de différentes façons, en l'occurrence l'addition, la

multiplication et le maximum des différentes métriques des liens. Pour garantir de meilleures performances, une métrique de routage doit satisfaire certaines exigences d'ordre général comme la mise en échelle et l'équilibre de la charge [48]. Dans la littérature, il existe plusieurs métriques de routage pour les WMNs [49] que nous résumons et classifions en deux catégories : métriques non-basées sur les interférences et métriques basées sur les interférences.

### 2.2.2.1. Les métriques non-basées sur les interférences

Le nombre de sauts est une métrique qui a été initialement utilisée par les réseaux ad-hoc et qui consiste à attribuer un poids égal à 1 pour chaque lien dans réseau. Ainsi, le coût du chemin d'une source vers une destination dans le réseau sera la somme de ces poids (nombre de sauts). C'est une métrique facile à utiliser et qui ne nécessite aucun paquet de contrôle. Toutefois, elle ne représente pas correctement la qualité des liens dans les WMNs. D'autres qualités, en l'occurrence, la charge des liens et les interférences ne sont pas prises en compte. Or, il se peut que le nombre de sauts d'un chemin soit optimal mais que le chemin présente plus d'interférences, comme il se peut qu'il ne soit pas optimal mais que le chemin présente moins d'interférences. Ainsi, en choisissant le chemin ayant le minimum de sauts, on risque de choisir celui ayant le plus d'interférences. De plus, il a été démontré que le nombre de sauts n'est pas nécessairement une métrique optimale pour trouver des chemins ayant des débits élevés [50].

La métrique ETX (*Expected Transmission Count*) proposée par [24] est une métrique qui estime le nombre de transmissions moyen pour envoyer un paquet correctement sur un lien. C'est une métrique active où chaque nœud dans le réseau échange périodiquement des paquets de petite taille (sondes) avec ses voisins. Au bout de chaque période de temps  $T$ , les voisins répondent aux nœuds émetteurs par des paquets qui indiquent le nombre de sondes bien reçues. Ainsi, en fonction du nombre de paquets envoyés et des notifications reçues, la métrique ETX d'un lien  $l$  se calcule comme suit :

$$ETX_l = \frac{1}{d_f \times d_r} \quad (2.1)$$

où  $d_f$  et  $d_r$  représentent les taux des paquets de contrôle bien reçus en avant (*forward delivery ratio*) et en arrière (*reverse delivery ratio*), respectivement.

La métrique relative à un chemin se calcule comme étant la somme des ETX des liens qui le forme. Ainsi, pour un chemin  $p$  formé des liens  $l$  :

$$ETX(p) = \sum_{l \in p} ETX_l \quad (2.2)$$

La métrique ETX prend en considération le taux de pertes des paquets et le nombre de sauts. Il s'agit d'une métrique additive dont la valeur augmente avec l'augmentation du nombre de sauts. De plus, il a été prouvé qu'elle assure un routage sans boucle [48] lors de son implémentation dans certains protocoles de routage. Néanmoins, elle présente certains inconvénients : elle ne considère pas les interférences intra-flux. Elle ne détecte que les interférences inter-flux mais d'une façon indirecte : plus l'interférence est grande plus le nombre de paquets perdus est plus grand et ainsi la valeur de ETX sera plus grande. Un autre inconvénient que présente ETX est qu'elle est basée sur l'hypothèse que les liens dans le réseau sont symétriques [46] (c'est-à-dire le taux de transmission sur un lien est le même dans les deux sens). Or, il se peut que sur un lien entre deux nœuds A et B, A envoie avec un taux de transmission  $T_A$  vers B et B envoie avec un taux de transmission  $T_B$  vers A avec  $T_A \neq T_B$ .

Certaines métriques ont étendu le principe d'ETX. ML (*Minimum Loss*) [51] en est un exemple basé aussi sur l'utilisation de paquets *sondes*. ML est une métrique multiplicative plutôt qu'additive comme c'est le cas d'ETX. Elle multiplie le ratio des paquets délivrés en avant ( $d_f$  chez ETX) par le ratio des 'ACK' en arrière ( $d_r$  chez ETX). Le but est de trouver les chemins qui minimisent les taux de perte de bout-en-bout. L'une des raisons d'utiliser une métrique multiplicative est de réduire le changement fréquent des routes ce qui permet d'améliorer les performances du réseau [51]. mETX (*modified ETX*) et ENT (*Effective Number of Transmissions*) sont deux autres métriques proposées par [52] et dérivées d'ETX; les auteurs se sont intéressés particulièrement à l'amélioration de la précision des mesures des taux de pertes. Ils argumentent que les métriques basées sur des valeurs moyennes calculées sur un intervalle de temps, comme ETX, ne peuvent pas suivre les variations des qualités des liens. mETX et ENT sont deux métriques basées sur les mesures de la variance et la moyenne

des qualités des liens, respectivement. L'objectif principal est de refléter les variations de la couche physique dans une métrique de routage. mETX calcule la qualité des liens d'une façon active en émettant des sondes. Toutefois, elle diffère d'ETX dans le fait qu'elle s'intéresse plutôt aux bits qu'aux paquets. mETX calcule la probabilité des erreurs des bits en fonction de la position de bits corrompus dans les sondes et leurs dépendances dans les transmissions successives. La métrique ENT, quant à elle, mesure le nombre de retransmissions successives par lien en considérant l'écart-type. ENT émet aussi des sondes et limite le calcul des routes à des liens ayant un nombre de retransmissions acceptable. Ce nombre doit être inférieur à un seuil prédéfini par les exigences des couches supérieures (exemple TCP). Les deux métriques, mETX et ENT, ont l'avantage d'améliorer le taux de pertes dans le réseau comparativement à ETX mais elles souffrent des mêmes problèmes qu'ETX (p.ex., interférences).

Les auteurs dans [25] résolvent certains problèmes d'ETX et proposent la métrique ETT (*Expected Transmission Time*) basée sur l'utilisation de différents taux de transmission et sur la taille des paquets. Le but est d'estimer le temps nécessaire pour qu'un paquet soit transmis correctement entre un nœud et son voisin. ETT nécessite la connaissance à la fois de ETX d'un lien  $l$ , la bande passante ( $B$ ) estimée sur ce lien et la taille des paquets ( $S$ ). La métrique se calcule comme suit :

$$ETT_l = ETX_l \times S/B \quad (2.3)$$

Les auteurs préfèrent estimer la bande passante périodiquement plutôt que de se baser sur l'information récupérée sur le taux de transmission à cause des limites du standard IEEE 802.11. L'estimation de la bande passante [49, 53] s'effectue en se basant sur l'envoi périodique de deux paquets de contrôle de taille différente : un petit suivi d'un autre plus grand. Quand un nœud reçoit ces paquets, il calcule la différence entre les temps d'arrivées et retourne une notification sur cette différence à l'émetteur. Ainsi, le nœud émetteur sera en mesure de calculer la bande passante en divisant la taille du plus grand paquet par la plus petite différence des temps d'arrivées durant chaque intervalle de temps.

Une métrique similaire, appelée MTM (*Medium Time Metric*), a été proposée dans [54]. Elle permet d'éviter la sélection des liens à grandes portées qui sont dans la plupart du

temps choisis par les protocoles de routage basés sur le nombre de sauts. Pour un lien  $l$  et un paquet  $p$ , la métrique est définie comme suit :

$$\tau(l, p) = \frac{\text{overhead}(l) + \frac{\text{size}(p)}{\text{rate}(l)}}{\text{reliability}(l)} \quad (2.4)$$

où  $\text{overhead}(l)$  représente l'information ajoutée au paquet  $p$  (bits de contrôles, les entêtes),  $\text{reliability}(l)$  représente la fraction des paquets correctement envoyés à travers le lien  $l$  et  $\text{rate}(l)$  est le taux de transmission sur le lien  $l$ .

ETT et MTM d'un chemin  $p$  donné sont cumulatives. Elles se calculent en additionnant les  $ETT_l$  et les  $\tau(l, p)$  des liens  $l$  qui forment  $p$ .

#### 2.2.2.2. Les métriques basées sur les interférences

WCETT (*Weighted Cumulative Expected Transmission Count*) [25] est basée sur ETT et considère les interférences intra-flux (voir section 2.1.4.3). Cette métrique est la somme de deux composantes qui sont le délai et la diversité des canaux de bout-en-bout. Elle se calcule sur un chemin  $p$  comme suit :

$$WCETT = (1 - \beta) \times \sum_{l \in p} ETT_l + \beta \times \max_{1 \leq j \leq k} X_j \quad (2.5)$$

où  $\beta$  est un paramètre ajustable dont la valeur est comprise entre 0 et 1 (0,5 comme valeur optimale trouvée dans [25]),  $k$  est le nombre de canaux et  $X_j$  est la somme des  $ETT_s$  pour chaque lien utilisant le canal  $j$  dans le chemin  $p$ ,

$$X_j = \sum_{\text{lien } l \text{ sur le canal } j} ETT_l, 1 \leq j \leq k \quad (2.6)$$

La première partie de WCETT essaie de trouver les chemins qui minimisent la métrique ETT tandis que la deuxième partie favorise les chemins dont la diversité des canaux est grande permettant ainsi de capturer les interférences inter-flux.

Pour illustrer le calcul de WCETT, considérons la figure 12 composée de 4 nœuds,  $S$ ,  $A$ ,  $B$  et  $D$ . Les valeurs sur chaque lien représentent la métrique ETT et le canal sur lequel opère le lien. En considérant  $\beta = 0.5$ , WCETT du chemin  $S-A-B-D$  sera 0.4 (soit  $0.5(0.2+0.2+0.1)+0.5 \times 0.3$ )

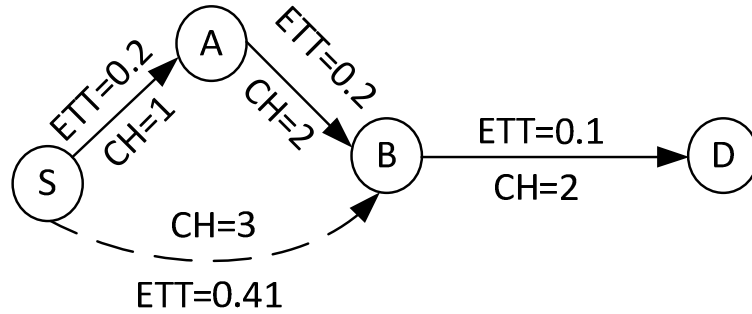


Figure 12 Exemple de calcul de WCETT []

En plus des avantages susmentionnés d'ETX et ETT, WCETT possède l'avantage de capturer des interférences de type intra-flux. Toutefois, WCETT ne garantit pas le plus court chemin pour router les paquets et des boucles de routage peuvent se former [49]. En plus de ces inconvénients, WCETT ne capture pas les interférences inter-flux. Par conséquent, du trafic pourra être envoyé dans des régions denses où des congestions peuvent se produire provoquant une dégradation de la bande passante.

La métrique MIC (*Metric of Interference and Channel-switching*) a été proposée par [48] comme une amélioration de WCETT. Elle prend en considération les interférences de types inter-flux et intra-flux. Sur un chemin  $p$  la métrique MIC se calcule comme suit :

$$MIC(p) = \frac{1}{N \times \min(ETT)} \sum_{i \in p} IRU_l + \sum_{i \in p} CSC_i \quad (2.7)$$

où  $N$  est le nombre total des nœuds dans le réseau et  $\min(ETT)$  est la plus petite ETT dans le réseau.  $IRU$  représente l'*Interference aware Ressource Usage* alors que  $CSC$  est le *Channel Switching Cost* qui représente le coût additionnel attribué à l'interférence intra-flux.  $IRU$  et  $CSC$  sont calculées comme suit :



$$IRU_l = ETT_l \times N_l \quad (2.8)$$

$$CSC_i = \begin{cases} w_1, & \text{if } CH(prev(i)) \neq CH(i) \\ w_2, & \text{if } CH(prev(i)) = CH(i) \end{cases} \quad (2.9)$$

avec  $0 \leq w_1 < w_2$ ,  $N_l$  est l'ensemble des nœuds voisins qui s'interfèrent sur le lien  $l$ ,  $CH(i)$  est le canal assigné à un nœud  $i$  tandis que  $prev(i)$  est le canal attribué au nœud prédécesseur de  $i$ . Ainsi,  $IRU_l$  représente le temps écoulé pour que des nœuds voisins transmettent sur un canal [48]; ceci permet de capturer l'interférence inter-flux. Pour CSC, quand deux liens qui se suivent utilisent le même canal, les auteurs suggèrent d'utiliser un poids  $w_2$  assez élevé pour discriminer contre les chemins avec de l'interférence intra-flux.

MIC présente l'avantage de capturer les interférences intra-flux et inter-flux. Cependant, elle présente certains inconvénients notamment : (1) elle suppose que tous les liens dans la portée des interférences ont le même degré d'interférences; (2) la composante CSC ne capture que l'interférence entre deux nœuds consécutifs; et (3) la complexité du calcul de MIC augmente avec le nombre d'interfaces radios utilisées dans le réseau [37].

Comme MIC, iAWARE [55] (*Interference Aware*) considère les interférences inter-flux et intra-flux dans son calcul de la métrique. Elle considère les interférences au niveau physique plutôt que logique (voir section 2.1.4.3). Plus particulièrement, iAWARE utilise la mesure du SINR et le SNR (*Signal to Noise Ratio*) pour calculer le taux d'interférence. La métrique s'intéresse également au temps d'occupation du canal lors des transmissions qui peut être un autre indicateur d'interférence. Plus ce temps est grand, plus l'interférence est grande et par conséquent la valeur de iAWARE sera grande. Pour un lien  $l$  entre deux nœuds  $u$  et  $v$ , iAWARE se calcule comme suit :

$$iAWARE_l = \frac{ETT_l}{IR_l} \quad (2.10)$$

où  $IR_l$  est le taux d'interférence compris entre 0 et 1. La valeur 1 signifie l'absence totale des interférences; dans ce cas, iAWARE jouera le même rôle qu'ETT.  $IR_l$  se calcule selon la formule suivante :

$$IR_l(u) = \frac{SINR_l(u)}{SNR_l(u)} \quad (2.11)$$

où  $SINR_l(u)$  est la puissance du signal à la réception calculée au nœud  $u$  en considérant l'interférence et le bruit.

$$SINR_l = \frac{P_u(v)}{N + \sum_{w \in \eta(u)-v} \tau(w) P_u(w)} \quad (2.12)$$

avec  $\eta(u)$  est l'ensemble des nœuds qui se trouvent dans la portée d'interférence de  $u$  et  $P_u(v)$  est la puissance du signal pour qu'un paquet arrive de  $u$  vers  $v$ .  $N$  est le bruit et  $\tau(w)$  est un coefficient de pondération qui dépend de la fraction de temps qu'occupe le nœud  $w$  pour accéder au canal.  $SNR_l$  est la puissance de réception d'un signal sans considération du bruit.

$$SNR_l = \frac{P_u(v)}{N} \quad (2.13)$$

La présence des interférences influence la puissance du signal SINR en réduisant sa valeur. Ainsi, quand il y a beaucoup d'interférences le taux IR tend vers 0 (vs 1 en cas de faible ou absence d'interférence). Pour calculer la métrique sur un chemin  $p$ , les auteurs proposent une formule similaire à WCETT qui est la suivante:

$$iAWARE(p) = (1 - \beta) \times \sum_{l \in p} iAWARE_l + \beta \times \max_{i \leq j \leq k} X_j \quad (2.14)$$

où  $0 \leq \beta \leq 1$  et  $X_j$  est la somme des  $iAWARE$  sur le canal  $j$  et  $k$  est le nombre des canaux dans le réseau.

$iAWARE$  a l'avantage de prendre en considération dans son calcul les pertes des paquets et la variation des taux de transmission. Elle hérite également des mêmes avantages que WCETT avec une capture de l'interférence inter-flux et intra-flux. Toutefois, il présente certains désavantages en l'occurrence, quand la valeur IR est supérieure à la valeur ETT d'un lien  $l$  la métrique  $iAWARE$  est petite ce qui explique que  $iAWARE$  peut choisir des routes dont les liens ont des valeurs ETT plus petites et de grandes valeurs IR. Dans ce cas une route ayant plus d'interférences sera sélectionnée.

Certaines métriques combinent les interférences et la charge des nœuds en l'occurrence la métrique RARE [56] (*Resource Aware Routing for mEsh*) et d'autres métriques similaires se trouvent dans [41]. La métrique RARE utilise les techniques de mesure passive pour mesurer la qualité des liens. Parmi les métriques de la qualité on retrouve, la capacité des liens ( $C_l$ ), la bande passante disponible ( $B_l$ ), la force du signal ( $RSSI$ ) et la contention moyenne ( $C_0$ ). RARE se calcule comme suit :

$$RARE_l = \alpha \times \frac{C_l - B_l}{B_l} + \beta \times \frac{RSSI_{max} - RSSI}{RSSI} + \gamma \times C_0 \quad (2.15)$$

où  $\alpha$ ,  $\beta$  et  $\gamma$  sont des coefficients de pondération dont les valeurs trouvées selon une heuristique sont égales à 1, 1 et 10, respectivement.  $RSSI_{max}$  est la valeur maximale des RSSI qui dépend de la carte réseau.  $B_l$  est calculé en fonction de la durée pendant laquelle le canal est occupé. Les intervalles d'inactivité du canal (*idle*) et le taux de transmission sont calculés de la façon suivante :

$$B_l = \frac{T_{idle}}{T_{idle} + T_{busy}} \times TX_{rate} \quad (2.16)$$

où  $TX_{rate}$  est le taux de transmission,  $T_{busy}$  est le temps d'occupation du canal et  $T_{idle}$  est la contention moyenne. RARE possède des avantages comparativement aux métriques susmentionnées. Elle utilise des mesures passives qui permettent de réduire la surcharge du réseau. Toutefois, elle présente aussi certains défauts. Tout d'abord, la diversité des canaux n'a pas été considérée par RARE ce qui rend la métrique incapable de choisir des chemins avec un minimum d'interférences intra-flux et inter-flux. De plus, la mesure de l'indicateur RSSI n'est pas précise pour décrire les interférences.

Le tableau 1 présente un récapitulatif des métriques de routage et leurs caractéristiques présentées dans cette section. Nous constatons que certaines caractéristiques, en l'occurrence le taux de perte des paquets, les interférences inter-flux et/ou intra-flux et la charge des nœuds, ont été utilisées d'une façon individuelle dans la plupart des métriques. Parmi ces métriques certaines ont été réutilisées par d'autres métriques. Par exemple, ETX et ETT ont été réutilisées par WCETT, MIC et iAWARE. iAWARE a réutilisé la même technique que

WCETT pour calculer la métrique d'un chemin. Outre les inconvénients et les avantages qu'on a vu pour ces métriques, certains travaux basés sur ETX et ETT ont considéré que tous les nœuds utilisent le même taux de transmission ce qui peut rendre les mesures incorrectes. Pour pallier à ces problèmes, il serait intéressant d'explorer une solution pour un routage qui d'une part considère la qualité des liens comme étant asymétrique, et d'autre part capture les interférences, la charge des passerelles, et le taux des pertes. Cette solution sera présentée dans le chapitre 3.

Tableau 1, récapitulatif des métriques de routages

Métriques	Taille des paquets	Interférence Intra-flux	Interférence Inter-flux	La charge aux passerelles	Stabilité des nœuds	Combinaison des métriques
Nombre de Saut	x	x	x	x	x	x
ETX	x	x	x	x	x	x
ML	x	x	x	x	x	x
mETX	√	x	x	x	x	x
ENT	√	x	x	x	x	x
ETT	√	x	x	x	x	√
MTM	√	x	x	x	x	√
WCETT	√	√	x	x	x	√
MIC	√	√	√	x	x	√
iAWARE	√	√	√	x	x	√
RARE	√	√	x	x	x	√

### 2.2.3. Les protocoles de routage

Le routage est un aspect essentiel pour transférer des paquets dans le réseau. Il consiste à trouver un ou plusieurs chemins selon une métrique d'une source à une destination. Dans les WMNs, Il existe trois classes de protocoles de routage qui diffèrent selon leurs techniques pour découvrir les routes, la maintenance des routes, et la reprise en cas de panne. Ainsi, les protocoles de routage peuvent être de type réactif, proactif ou hybride.

#### 2.2.3.1. Les protocoles de routage réactifs

Dans les protocoles de routage réactifs, dites aussi protocoles de routage à la demande, les routes sont calculées au besoin. Ainsi, lorsqu'une route est désirée par un nœud source, un

mécanisme de découverte de route est lancé dans le but d'obtenir une information spécifiée et inconnue au préalable. Cette information restera valide tant que la destination est joignable ou jusqu'au moment où la route devient inutile. Ces techniques réduisent considérablement la charge du réseau en utilisant moins de paquets de contrôle entre les nœuds. Toutefois, le délai de communication risque d'être grand car la connaissance des routes n'est pas instantanée (elles doivent être découvertes). Parmi ces protocoles nous survolons les plus répandus AODV (*Ad hoc On-Demand Distance Vector*) et DSR (*Dynamic Source Routing*). D'autres protocoles se trouvent dans [57].

AODV [58] a été initialement conçu en se basant sur le nombre de sauts comme métrique. Quand un nœud source a besoin d'envoyer des paquets de données à une destination, il débute la procédure de découverte des routes en diffusant des paquets RREQs (*Route Request*) dans le réseau. Les nœuds intermédiaires enregistrent le premier RREQ reçu et construisent un chemin de retour vers la source. Ces nœuds peuvent envoyer directement des messages RREPs (*Route Reply*) s'ils disposent de suffisamment d'informations récentes vers la destination. Dans le cas contraire, ils rediffusent le message RREQ reçu. À la réception du message RREQ, la destination répond la source par un message RREP qui contient la liste des nœuds intermédiaires formant le chemin depuis la source à la destination. AODV ne maintient que les routes actives sur lesquelles du trafic passe. Les routes non actives sont supprimées des tables de routage des nœuds intermédiaires. Afin de maintenir la connectivité entre les nœuds d'une route active, AODV propose d'utiliser des messages HELLO. Ces messages sont échangés périodiquement entre les nœuds. Au bout d'une certaine période, si le message HELLO ne parvient pas à un voisin, ce dernier déclare l'émetteur en panne et génère un message d'erreur RERR qui sera envoyé à la source qui réinitialisera la procédure de découverte des routes.

DSR [59] est un protocole de routage à la demande basé sur le principe du routage à la source où chaque nœud source détermine la séquence des nœuds à traverser par les paquets vers une destination donnée. DSR a été conçu en premier pour les réseaux MANET afin d'assurer le routage entre les nœuds mobiles et réduire le nombre de paquets de contrôle. En effet, chaque nœud qui implémente DSR utilise un mécanisme de découverte des routes et un autre de maintenance des routes. Le mécanisme de découverte des routes est similaire à celui

d'AODV où chaque nœud source qui ne dispose d'aucune route vers la destination diffuse un message RREQ. Chaque nœud intermédiaire qui n'a pas reçu auparavant ce message RREQ ajoute son adresse dans l'entête et le rediffuse vers la destination. Cette dernière ajoute également son adresse et répond la source par un message RREP à travers un chemin construit lors de la propagation de la requête. Cette technique ne nécessite aucun enregistrement de l'information de routage par les nœuds intermédiaires. Par contre, chaque source maintient les chemins complets vers n'importe quelle destination dans le réseau. Pour la phase de maintenance, DSR n'utilise pas les paquets HELLO semblablement à AODV. En effet, un nœud peut détecter que son voisin est en panne lorsque plusieurs tentatives d'envoi des paquets échoue. Ainsi, un message d'erreur est généré puis envoyé à la source. Un des inconvénients de DSR est la surcharge du réseau. En effet, chaque nœud source ajoute, dans l'entête des paquets, le chemin vers la destination. Une fois le paquet passe par un nœud intermédiaire, ce dernier retire son adresse de l'entête et l'envoie au prochain nœud jusqu'à ce qu'il arrive à destination.

### **2.2.3.2. Les protocoles de routage proactifs**

Dans les protocoles de routage proactifs, l'information de routage vers chaque nœud du réseau est maintenue par chaque nœud sous forme d'une ou plusieurs tables de routage. Tous les nœuds mettent à jour ces tables, à travers un ensemble de messages échangés périodiquement afin de maintenir une vue consistante du réseau. Ainsi, et en cas de besoin, une route est immédiatement disponible. Il existe deux types de protocoles proactifs : (1) les protocoles à état de liens où chaque nœud maintient la topologie du réseau et calcule les routes sans se soucier des autres nœuds. Parmi ces protocoles on retrouve le protocole OLSR (*Optimized Link-State Routing*) que nous survolons dans cette section; et (2) les protocoles à vecteur de distance où chaque nœud partage sa table de routage avec ses voisins sans connaître la topologie du réseau. Parmi ces protocoles on retrouve DSDV (*Destination-Sequenced Distance Vector*).

OLSR [60] est un protocole de routage proactif utilisé par plusieurs réseaux sans fil en l'occurrence les réseaux ad-hoc et les WMNs. Ce protocole propose une optimisation permettant de réduire la taille des messages de contrôle et de minimiser leurs inondations dans

le réseau. Ceci est réalisé grâce à une sélection des nœuds MPRs (*Multipoint Relay*) parmi des nœuds voisins qui assurent la retransmission des paquets de contrôle. Il existe deux types de paquets de contrôle échangés périodiquement entre les nœuds : les paquets HELLO et les paquets TC (*Topology Control*). Les paquets HELLO contiennent la liste des voisins, les nœuds MPRs et la qualité des liens ; ces informations permettront aux nœuds qui les reçoivent de maintenir à jour leurs tables de routage. Les messages topologiques TC sont diffusés par chaque MPR et contiennent la liste de leurs voisins les ayant sélectionnés ; cette information permettra aux autres nœuds de connaître la topologie du réseau. Ainsi, grâce aux messages HELLO et TC, chaque nœud est capable de calculer son chemin vers n'importe quel nœud dans le réseau. Compte tenu que des informations sur les états des liens sont échangées périodiquement, un nœud pourra facilement détecter une panne de son voisin (information de contrôle non reçue au bout d'une certaine période). Dans ce cas, le nœud ayant détecté la panne changera systématiquement la route en se basant sur les informations dont il dispose dans sa table de routage. Un des avantages des protocoles proactifs (exemple OLSR et DSDV) est la disposition et l'accès aux informations de routage. Chaque nœud pourra trouver rapidement son chemin vers un destinataire sans devoir lancer une procédure de recherche comme c'est le cas pour le protocole AODV.

DSDV [61] est aussi un protocole de routage proactif. Contrairement au protocole OLSR où les nœuds conservent tout le chemin pour atteindre une destination, les nœuds qui implémentent DSDV ne conservent que l'information du prochain saut pour atteindre une destination. En effet, avec DSDV, chaque nœud maintient une table de routage contenant les informations vers chaque destination joignable dans le réseau incluant l'adresse de destination, le coût pour l'atteindre, le prochain saut, et le numéro de séquence. Ce dernier champ est généré puis incrémenté par les destinations à chaque envoi de paquets de contrôle. Il permet aux autres nœuds du réseau de ne conserver que des informations récentes du routage. DSDV permet aux nœuds de diffuser les mises à jour des tables de routage dans le réseau de deux façons différentes : soit à l'aide d'un envoi périodique ou bien lorsqu'un changement est détecté par un nœud dans sa table de routage. En effet, dépendamment du nombre de changement dans la table de routage, un nœud peut diffuser soit toute sa table de routage comme il peut diffuser juste la partie concernée par le changement. Cette technique présente

l'avantage de minimiser la surcharge du réseau en limitant le nombre de paquets de contrôle qui représentent la fraction de la table de routage ayant subi des modifications et qui nécessite une diffusion. Toutefois, lors de l'envoi de toute la table de routage, plusieurs paquets de contrôle peuvent être créés dépendamment de la taille du réseau ce qui crée une surcharge du réseau. De plus, et dans certains cas, des boucles de routage peuvent se former créant ainsi une augmentation de délai de transmission et des pertes des paquets.

### **2.2.3.3. Les protocoles de routage hybrides**

Les protocoles hybrides combinent les techniques proactives et réactives afin d'optimiser le routage. Ils résolvent le problème de surcharge du réseau causé par l'échange périodique des paquets de contrôle observé chez les protocoles proactifs et le problème de non disponibilité immédiate des routes observé chez les protocoles réactifs.

TORA (*Temporally Ordered Routing Algorithm*) est un exemple de protocole de routage hybride basé sur le principe du lien inversé (*Link Reversal*) [62] et mieux adapté pour les réseaux dont la topologie change fréquemment. TORA combine les techniques proactives et réactives et produit trois fonctions de base : la découverte des routes, la maintenance des routes et la suppression des routes. Comme le protocole AODV, TORA ne conserve pas les chemins vers toutes les destinations. Leur découverte s'effectue d'une façon réactive initiée par la source. Par contre, TORA utilise des graphes acycliques orientés dont les racines sont les nœuds destinataires. Ainsi, en cas de lien défaillant le principe du lien inversé est utilisé en rétablissant localement le graphe. Dans un réseau dont les nœuds implémentent TORA, certains nœuds sont plus sollicités que d'autres en l'occurrence les passerelles, les points d'accès etc. Ainsi, afin de réduire la surcharge du réseau, TORA permet à seulement quelques nœuds de s'échanger périodiquement leurs paquets de contrôle comparativement à DSDV et OLSR. Il s'agit des nœuds les plus sollicités dans le réseau en l'occurrence les passerelles et les points d'accès.

Dans cette section, nous avons discuté les principales classes des protocoles de routage et nous avons donné quelques exemples de ces protocoles (DSR, AODV, OLSR, DSDV et TORA). La figure 13 présente une classification récapitulative de ces protocoles. En effet, à partir de ces exemples de protocoles d'autres protocoles ont été proposés dans la littérature



dont le principe de fonctionnement reste le même mais qui diffèrent seulement dans les métriques utilisées. On cite comme exemple OLSR-ML (*OLSR- Minimum Losses*) [51] et OLSR-MD (*OLSR Minimum Delay*) [63] utilisant comme métrique les pertes de paquets et le délai de bout-en-bout, respectivement. D'autres protocoles se trouvent dans [51, 64].

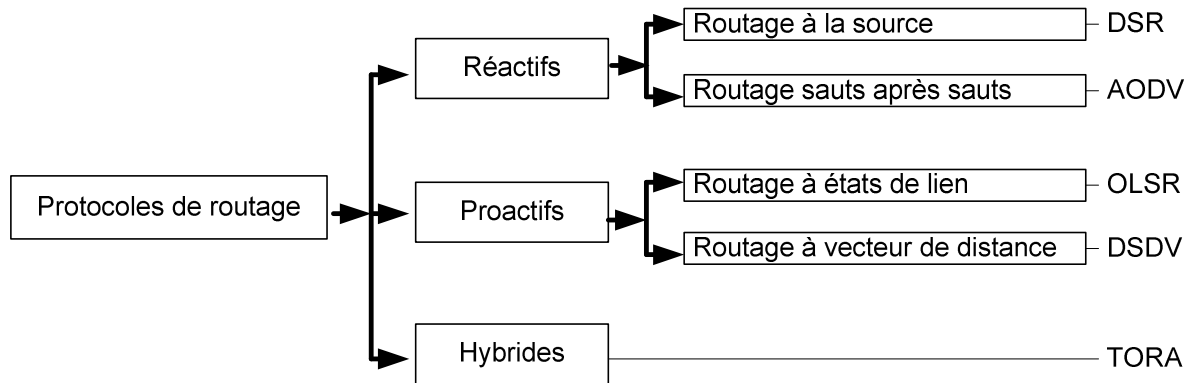


Figure 13 . Classification récapitulative des protocoles de routage

L'ensemble de ces protocoles de routage s'intéressent particulièrement à trouver les routes pour acheminer des paquets vers des destinations en se basant sur les métriques associées aux liens. Certains de ces protocoles provoquent des surcharges du réseau à cause des paquets de contrôle. D'autres nécessitent un délai pour trouver le chemin approprié vers une destination donnée. Cependant, tous ont considéré que tous les nœuds dans un WMN contribuent de la même façon au routage. Or, dans un WMN le trafic est plus souvent orienté vers les passerelles. Donc les nœuds aux alentours des passerelles devraient être plus déterminants que le reste des nœuds dans la sélection des routes. Pour pallier à ces problèmes, il serait intéressant de réduire la surcharge du réseau et d'attribuer différents poids aux nœuds dans un WMN. Cette solution sera présentée au chapitre 4.

#### 2.2.4. Stabilité des réseaux

Le terme « stabilité » est difficile à définir. Il a été utilisé dans différents domaines pour désigner l'état ou la qualité d'un système. Dans la littérature, la stabilité a été largement étudiée dans plusieurs types de réseaux en l'occurrence les réseaux ad-hoc, réseaux filaires, les réseaux de capteurs, les réseaux ATM (*Asynchronous Transfer Mode*), mais très rarement dans les réseaux WMNs.

SSA (*Signal Stability based Adaptive*) [65] et ABR (*Associativity-Based Routing*) [66] est considéré parmi les premiers protocoles à introduire la notion de stabilité dans les réseaux ad-hoc. Ils mesurent la stabilité des liens en se basant sur des mesures réelles des signaux. SSA estime la stabilité des liens en fonction de la force du signal. Ainsi, chaque nœud mobile mesure la force des signaux en provenance des voisins. Les auteurs distinguent entre les liens fortement connectés et faiblement connectés. Un lien est fortement connecté si la force du signal dépasse un certain seuil prédéfini. Ce qui est généralement le cas lorsque deux nœuds sont proches l'un de l'autre. Le lien est faiblement connecté dans le cas contraire. En se basant sur ces deux concepts (fortement connecté et faiblement connecté) un lien est stable s'il est fortement connecté durant une longue période de temps. SSA essaie de trouver les routes formées des liens stables sans minimiser le nombre de sauts. Il a été prouvé qu'avec cette technique le délai de bout-en-bout peut-être amélioré. Toutefois, si les liens sont instables le protocole propose de trouver les routes avec toutes les liaisons possibles.

La mesure de la force du signal n'est pas effectuée par ABR sur tous les signaux comme c'est le cas pour SSA mais plutôt sur un signal spécifique. En effet, dans ABR, chaque nœud émet périodiquement un message HELLO. C'est sur ce message que chaque nœud détermine la force du signal. Ainsi, même en cas d'absence de trafic, un nœud est en mesure d'estimer la qualité des liens. En se basant sur la force du signal, un lien entre deux nœuds est défini comme étant stable si l'un des nœuds reçoit continuellement des signaux de son voisin et que le nombre de ces signaux dépasse un seuil prédéfini durant une période de temps. Dans le cas contraire, le lien est déclaré instable. Pendant le calcul des routes, ABR considère tous les liens stables, même ceux qui sont longs avec une force de signal faible comparativement à SSA.

Dans les réseaux ATM, et MANETS la stabilité a été introduite. Les auteurs [67] se focalisent dans le développement de critères pour tester la stabilité des réseaux ATM. En effet, ils définissent un réseau comme étant stable si pour toutes les connexions, le délai de bout-en-bout dans le pire cas est inférieur ou égal à un seuil  $D$ . Ce délai représente la somme des délais par serveur (commutateur ATM) traversé par les paquets lors d'une connexion. Dans MANETS, les auteurs dans [68] définissent un lien stable comme étant un lien dont au moins un pourcentage  $p$  de paquets est reçu pendant une durée de temps  $T_s$ . Ce pourcentage  $p$ , doit

être assez petit pour se conformer aux exigences minimales des applications et assez grand pour tolérer les variations rapides des signaux alors que le temps  $T_s$  doit être choisi de sorte qu'il soit assez petit pour refléter les variations rapides de l'état des liens entre les nœuds et assez grand pour prévenir les découvertes de route inutiles.

Les réseaux maillés sans fil sont formés par un ensemble de nœuds qui coopèrent et contribuent aux ressources du réseau. Pour les WMNs, la découverte des routes, des services et des ressources est indispensable pour le support de différentes applications. Dans ce type de réseau, Aydin et al [69] proposent une architecture en couche pour sélectionner d'une façon autonome un sous ensemble de nœuds de l'épine dorsale pour former un système quorum. Afin de réaliser cette sélection, les auteurs proposent un protocole ADB (*Adaptive Dynamic Backbone*) qui explore les informations de stabilité maintenues par chaque nœud. Parmi ces informations on retrouve *nodeStability* et *pathStability*. *nodeStability* représente pour chaque nœud la probabilité de stabilité de la zone formée par l'ensemble de ses voisins. Cette probabilité notée  $P_i$  pour un nœud  $i$  peut être calculée de différentes façons entre autre la probabilité que la connexion entre  $i$  et son voisin  $k$  reste valable (ne s'interrompe pas) pendant une fenêtre de temps prédéfinie. Alors que *pathStability*, représente la stabilité d'une route estimée depuis un nœud vers son épine dorsale. Cette métrique mesure la probabilité pour qu'un chemin reste valide durant une prochaine fenêtre de temps et elle se calcule comme suit:

$$pathstability_i = pathStability_{parent\ of\ i} \times P_i \quad (2.17)$$

Ramachandran et al. [70] motivent l'utilité d'une analyse de la stabilité des routes par son importance pour la conception des protocoles de routage dans les WMNs. Ainsi, une analyse a été faite en se basant sur deux bancs d'essai UCSB Meshnet [71] et MIT Roofnet [5] où ils montrent que les raisons principales de l'instabilité des réseaux est la variation de la qualité des liens causée par les interférences, par les effets d'évanouissement (*fading*) dûs aux multi-trajets et par les conditions climatiques. Durant cette étude, les auteurs ont utilisé d'une part WCETT comme métrique de routage et trois autres métriques pour désigner la stabilité d'une route d'une autre part. La première métrique est la *prévalence* qui représente la probabilité que le nombre de fois qu'un chemin a été rencontré dans le passé. La deuxième métrique est la *persistance* qui représente la probabilité pour qu'une route reste inchangée sur

une longue période de temps. Finalement, la troisième métrique est *l'oscillation des routes* (*route flapping*) qui représente la variation des chemins durant une période de temps. Pendant l'analyse de la stabilité et plus particulièrement en considérant les métriques de prévalence et de persistance les auteurs constatent que les routes dans les WMNs sont de nature instable et peu dominées par une seule route. De plus, les routes qui oscillent souvent, pour minimiser leurs métriques, vont contribuer à une légère amélioration des performances du réseau (p.ex., légère améliorations du débit)

La stabilité des routes est un facteur déterminant dans la performance des réseaux. Grâce à elle, de nombreuses applications impliquant la Qualité de Service (QoS) comme la vidéoconférence et les applications en temps réel peuvent être supportées. Quand l'instabilité se produit plusieurs paquets seront perdus et le temps de convergence du réseau et la consommation des ressources seront augmentés. Dans la littérature, plusieurs protocoles de routage basés sur la stabilité ont été proposés pour différents types de réseaux mais très rare pour les WMNs. Dans ces derniers, nous avons besoin des protocoles de routage intelligent capables d'identifier les chemins stables pour aider à réduire le nombre de paquets de contrôle et le nombre d'oscillation. Dans ce contexte, nous présentons notre solution de routage basée sur la stabilité locale des nœuds d'une part et la probabilité des choix des passerelles d'autre part dans le chapitre 5.

## Chapitre 3 :

# Source-based Routing in Wireless Mesh Networks

Mustapha Boushaba, Abdelhakim Hafid, Michel Gendreau

### Abstract

This paper addresses the problem of optimal gateways selection and route selection to Internet in backbone wireless mesh networks (WMNs) where each mesh router (MR) is equipped with multiple radio interfaces and a subset of nodes serve as gateways to Internet.

Several schemes have been proposed to route packets in WMNs or to select appropriate gateways to connect clients to Internet. However, most of these schemes consider packet loss, interferences, load at gateways, or ETX (*Expected Transmission Count*) as routing metrics; only a few schemes consider two some of these metrics at the same time. Moreover, most of these metrics consider either inter-flow interferences or intra-flow interferences and a few consider both types of interferences. In this paper, we propose an efficient path and gateway selection scheme, called BP2BG (*Best Path to Best Gateway*), that aims to choose paths with high throughput, low intra-flow and inter-flow interferences between a source and a selected best gateway.

Simulation results show that BP2BG can significantly improve the overall network performance compared to schemes using either ETX, nearest gateway (i.e., shortest path to gateway), load at gateways or interferences as metrics for path and gateway selection.

**Keywords:** WMN; Interferences; ETX; Gateway; Routing metrics; Performance; Measurement

### 3.1. Introduction

Wireless Mesh Networks (WMNs) [4] have attracted significant research due to their features that include dynamic self-organization, self-configuration, easy maintenance and low

cost. In case of link failure, the network is able to automatically establish alternative paths. A WMN can be seen as a multi-hop Mobile Ad-hoc Network (MANET) with extended connectivity. In opposition to MANETs, WMNs are characterized by a relatively static architecture and low mobility.

To increase WMN performance and capacity, nodes can be equipped with multiple radios and multiple channels. Otherwise, with a single channel, a node cannot transmit and receive simultaneously. An efficient channel assignment (CA) can considerably improve WMN capacity. The ideal scenario would be the routing protocol provides the CA according to the available resources. But, the CA itself remains an open research issue.

The main goal of a routing protocol is to find better paths according to some requirements. These requirements vary depending on client needs (e.g, bandwidth, delay, loss). Nevertheless, in general, routing protocols determine low delay, high throughput or minimum loss paths. There exists a vast literature on routing protocols [57, 58, 59, 60, 62, 64, 71]. They may be roughly divided into three categories: (1) reactive routing protocols (e.g., *Ad hoc On-demand Distance Vector AODV* [58], *Dynamic Source Routing DSR* [59]): when a node has data to send, it starts looking for paths; (2) proactive routing protocols (e.g., *Optimized Link State Routing Protocol OLSR* [60] and *Mobile Mesh Routing Protocol MMRP* [71]): it maintains up-to-date routing tables so that when a node wants to send data, the path is found immediately. Mesh nodes have to get, periodically, information about the state of the network to maintain fresh paths from any source to any destination; and (3) hybrid protocols (e.g., *Temporally-ordered routing algorithm TORA* [62]) are both proactive and reactive; they proactively maintain partial routing tables (include paths to only a subset of the network nodes); when a node needs to send traffic to another node, not in the routing tables, it reactively searches for a path.

Interferences can sensibly impact wireless network performance [34]. There are two main types of interferences: (1) Inter-flow interferences: happen when nodes, that are in the interference range of each other, operate simultaneously on the same channel as shown in Figure 14 for nodes *B* and *D*; and (2)

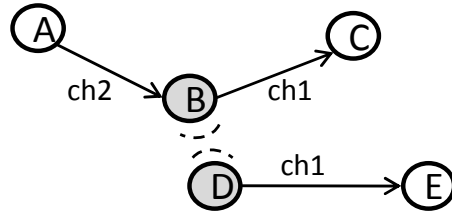


Figure 14. Inter-flow interference

Intra-flow interferences: occur when two consecutive links operate on the same channel (see Figure 15). Since links *A-B* and *B-C* cannot operate simultaneously, only one link can be active at any given time.

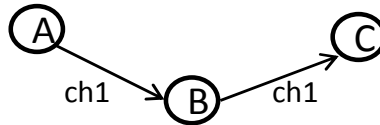


Figure 15. Intra-flow interference

In WMNs, the traffic usually passes through gateways (GWs) to reach the Internet. In this case, mesh routers (MRs) act as intermediate nodes and forward user traffics to GWs. Therefore, optimal gateway and path selection become crucial to the performance of the network. By equipping a WMN topology with a single GW to connect MRs to the Internet the gateway selection problem is simple. Since all upstream/downstream traffic must traverse the same GW, this node will often become the bottleneck in the network [27]. To mitigate this problem, usually, multiple gateways are installed to distribute load and improve performance. However, increasing the number of GW does not necessarily increase the network capacity. This has to do with the network connectivity and the GWs placement which are an open research issues in WMNs and out of scope for this paper.

When a MR knows more than one GW, the routing problem is not only concerned with finding the best path to a GW but also with selecting the best GW. Therefore, the proposed scheme extends our contribution in [73] and defines a metric, called BP2BG (*Best Path to Best Gateway*), that will be used by our source routing protocol to select the appropriate (and thus the appropriate GW) path to send traffic between a source to a node in the Internet taking into account the proposed metric computed using a number of parameters including intra-flow interferences, inter-flow interferences, data losses and the loads of GWs. We evaluate the

performance of the proposed scheme against four other schemes: nearest gateway selection, gateway load based selection, ETX metric and interference metric in terms of delay, loss and throughput.

The remainder of the paper is organized as follows. In Section 3.2, we present related work. Section 3.3 presents a network model, notations and definitions we use throughout the paper. In Section 3.4, we present our proposed algorithm based on BP2BG metric. Simulation results are presented and discussed in Section 3.5. Section 3.6, concludes the paper.

## 3.2. Related work

In this section, we provide an overview of some existing routing metrics, gateway discovery schemes and gateway and path selection schemes.

### 3.2.1. Routing metrics

In general, a routing metric is used, by a routing protocol, to select the path having high throughput, low delay and/or low loss rate. Recently, several routing metrics have been proposed for WMNs; among those metrics are Hop-count, ETX, ETT, WCETT, MIC *and* iAWARE; more details about routing metrics in WMNs can be found in [4].

Hop-count is a most known scheme for addressing the routing problem. However, for WMN, it is a poor choice; there may be a shorter path between a source and a destination that presents heavy interferences and high packet losses.

Couto et al. [24] defined a metric called Expected Transmission Count (ETX); it was the first metric proposed specifically for WMNs. ETX estimates the number of transmissions and retransmissions needed to successfully transmit a frame on a link. ETX of a link is defined as follows:

$$ETX = \frac{1}{d_f \times d_r} \quad (3.1)$$

where  $d_f$  and  $d_r$  denote the forward and the reverse delivery ratio on the link respectively. ETX of a path is then defined as the sum of the ETX of each link on that path. Thus, the routing



protocol chooses a path with the smallest value of ETX which is supposed to give the smallest loss ratio. ETX fails in capturing asymmetric [46] link effect. It can choose a path that has a good reverse but also a bad forward delivery ratio; indeed, when we compute the average in this case, the cost can be considered as acceptable. ETX does not also consider the current load and the available bandwidth of links when selecting a path.

To overcome ETX limitations, Expected Transmission Time (ETT) [25] was proposed. It estimates the time a data frame needs to be successfully transmitted on a link. ETT of a link is defined as follows:

$$ETT = ETX \times S/B \quad (3.2)$$

where  $S$  represents the packet size and  $B$  the bandwidth of the link. ETT improves ETX by considering the load and the bandwidth; however, it does not resolve the asymmetry issue. Furthermore, both ETX and ETT do not capture interferences and suffer in dense networks.

Weighted Cumulative Expected Transmission Time (WCETT) [25] has been proposed as an extension of ETT to take into account intra-flow interferences caused by channel diversity. WCETT, for a path, is defined as follows:

$$WCETT = (1 - \beta) \times \sum_{i=1}^n ETT_i + \beta \times \max_{1 \leq j \leq k} X_j \quad (3.3)$$

where  $0 < \beta < 1$ ,  $n$  is the number of links in the path,  $ETT_i$  is the ETT of link  $i$  ( $1 \leq i \leq n$ ),  $X_j$  represent the sum of ETT for each link operating on channel  $j$ , and  $k$  is the total number of channels. Thus, WCETT favors paths with high channel diversity. One key shortcoming of WCETT is that it considers that two links, on the same path, that share the same channel automatically interfere with each other even if they are out of the interference range. Furthermore, WCETT does not consider inter-flow interferences which are present in WMNs.

Metric of interference and channel switching (MIC) [48] was designed to improve WCETT by considering inter-flow and intra-flow interferences at the same time. MIC for a path is defined as follows:

$$MIC(p) = \frac{1}{N \times \min(ETT)} \sum_{link l \in p} IRU_l + \sum_{node i \in p} CSC_i \quad (3.4)$$

where  $p$  is the path,  $N$  is the number of nodes in the network and  $\min(ETT)$  is the smallest ETT in the network.  $IRU$  (Interference aware Resource Usage) and  $CSC$  (Channel Switching Cost) are defined as follows:

$$IRU_l = ETT_l \times N_l \quad (3.5)$$

where  $N_l$  is the number of neighbors that interfere when transmitting on link  $l$ .

$$CSC_i = \begin{cases} w_1, & \text{if } CH(\text{prev}(i)) \neq CH(i) \\ w_2, & \text{if } CH(\text{prev}(i)) = CH(i) \end{cases} \quad (3.6)$$

where  $w_1$  and  $w_2$  are costs ( $0 \leq w_1 < w_2$ ),  $CH(\text{prev}(i))$  is the channel used by the previous hop to node  $i$  and  $CH(i)$  is the channel used for next hop at node  $i$ .  $MIC$  tries to avoid consecutive hops in a path operating on identical channels, by adding a high cost  $w_2$  when using the same channel and a small cost  $w_1$  if different channels are used (usually  $w_1=0$ ). Using  $MIC$  encourages channel diversity by increasing the cost when a channel is reused.  $MIC$  captures inter-flow interferences by assuming that all the nodes located in the collision range of a particular link contribute similarly to interferences; this assumption is not accurate since the impact of interferences mainly depends on the operating data rate and the distance.

Interference Aware (iAWARE) [55] considers both inter-flow and intra-flow interferences. iAWARE estimates the average time the medium is busy because of transmissions from interfering neighbors. It uses Signal to Noise Ratio ( $SNR$ ) and Signal to Interference and Noise Ratio ( $SINR$ ) to continuously estimate neighboring interference variations into routing metrics. For a given link  $i$  between nodes  $u$  and  $v$ , the interference ratio of node  $u$  is defined as follows:

$$IR_i(u) = \frac{SINR_i(u)}{SNR_i(u)} \quad (3.7)$$

The interference ratio for link  $i$  ( $u, v$ ) is defined as follows:

$$IR_i(u, v) = \min(IR_i(u), IR_i(v)) \quad (3.8)$$

$i$ AWARE of link  $i$  is then defined as follows:

$$iAWARE_i = \frac{ETT_i}{IR_i} \quad (3.9)$$

### 3.2.2. Gateway discovery schemes

Gateway discovery is a key component in providing Internet connectivity. In WMNs, a *MR* must discover an Internet GW prior to communicating with an Internet correspondent node. Gateways discovery schemes may be broadly divided into three categories: (1) proactive, (2) reactive and (3) hybrid.

In proactive schemes [74], wireless routers passively hear periodic advertisements (messages) from GWs. Each GW broadcasts messages that contain up-to-date information about its state. Upon receipt of these messages, intermediate wireless routers record the necessary information and/or add other metrics to be rebroadcasted to the network. However, by flooding the backbone mesh network, excessive network resources may be consumed and more interferences can be created. Consequently, optimization techniques making the appropriate balance between Advertising Interval and the network performance are needed.

In reactive schemes [75], each source *MR* is allowed to actively discover GWs when necessary. Thus, a request message will be generated and broadcasted or unicasted to reach GWs. As a response, a GW may broadcast or unicast an advertisement to the source. Indeed, these techniques can reduce interferences, but remain ineffective in wireless mesh networks with large demand.

The hybrid schemes [76, 77] combine reactive and proactive techniques to discover GWs. The objective is to reduce advertisements flooding and thus overhead. The key challenge in hybrid approaches is the definition of the optimal proactive region and the optimal flooding interval.

In the literature, several solutions have been proposed to select the best paths to GWs. The selection of these paths is based on each GW state. Among these techniques, the authors in [78, 79] propose to use the load at GWs as metric for selecting the best GW; the objective is to balance traffic among different GWs. However, taking into consideration just the load as a metric to select the best path may not be a good solution. Indeed, there are cases where the load at the *GW* is low while interferences and packet losses are higher on paths towards this gateway. Ashraf et al. [80] propose a technique that uses a combination of metrics, and estimates logical interferences, to select path to gateway. However, the metric is used in one-radio one-channel wireless mesh networks topology.

In this context, we propose a BP2BG-based routing protocol able to combine a best GW selection and a best path selection between a source and a node in the Internet by considering intra-flow interferences, inter-flow interferences, data losses and the loads of GWs.

### 3.3. System model and Notations

In this section, we present the network model, definitions and concepts used in the rest of the paper.

#### 3.3.1. Network Model

We consider a multi-hop infrastructure WMNs with two sets of nodes: MRs and GWs. *MRs* form a multi-hop wireless backbone to relay traffic between users and Internet. To reach the Internet, traffic passes through GWs which are MRs with more functionality (i.e., more buffer size, wired and wireless interfaces ...). Each MR may be equipped with multiple wireless interfaces and multiple channels on each interface. We formally model the backbone WMN as a graph  $G=(V, E)$  where  $V$  is the set of MRs and  $E$  is the set of links. Each node in  $V$  is equipped with two or more wireless interfaces. We assume that the interfaces of a MR are assigned different channels. In  $V$ , there are GWs that provide connectivity to Internet. Like in [81, 82], we define the GW load as the average interface queue length. It can be measured by monitoring the number of packets buffered in the GW interface over a time period.

### 3.3.2. DACI, Distribution Available Capacity Indicator

During the operation of the network, GWs may have very different loads (e.g., lightly loaded gateways, overloaded gateways); to forward traffic to the Internet, a simple GW selection protocol may select the least loaded gateway (*LLG*) [83]. The problem with this approach is that we may select a lightly loaded GW, with all interfaces having similar queue length  $L$ , and not select a GW, with one of its interfaces having a queue length far smaller than  $L$  (e.g. 0). Thus, an indicator of the load distribution/available capacity among gateway interfaces is needed to help in the selection of GWs. Let us consider the example shown in Figure 16. It illustrates the load on each of the three interfaces of 2 GWs.

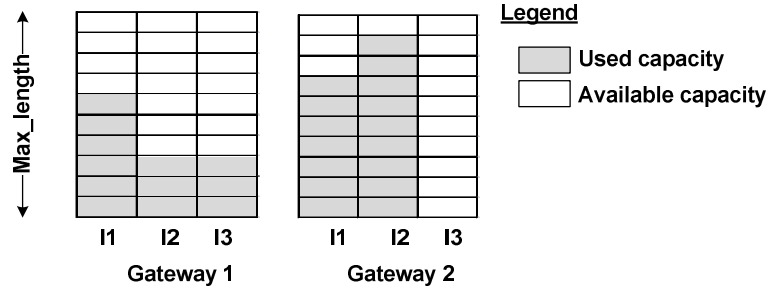


Figure 16. Load: GW-1 and GW-2

The available capacity ( $AC_g$ ) of GW  $g$  is defined as the sum of the available capacity on each of its interfaces. In the example shown in Figure 16,  $AC_g$  is expressed as follows:

$$AC_g = \sum_{i=1}^3 (\max\_length - L_i) \text{ where } \max\_length \text{ is the maximum capacity of the interfaces and } L_i \text{ is the load on interface } i.$$

For GW-1, if we assume that the maximum queue length for each interface is equal to 100 and the load at the interfaces  $I1$ ,  $I2$  and  $I3$  are 60, 30 and 30 respectively, then, the available capacity will be 180 (140 for GW-2)

In this context, we define *DACI* as the indicator for the available capacity and the traffic distribution among interfaces for each gateway  $g$  *DACI* is defined as follows:

$$DACI_g = \frac{\sum_{i \in g} \frac{(1 + \gamma_i)}{2} (C_i - L_i)}{\sum_{i \in g} C_i} \quad (3.10)$$

where for each interface  $i$ ,  $C_i$  and  $L_i$  are the maximum queue length and the load respectively,  $\gamma_i$  represents the distribution coefficient based on the available capacity  $AC$ . For example, if we consider the following values for  $\gamma_i$  (these values were determined running simulations using our setup; see Section 3.5):

$$\gamma_i = \begin{cases} 0, & \text{if } AC_i \in [0, 60[ \\ 1/4, & \text{if } AC_i \in [60, 80[ \\ 1/2, & \text{if } AC_i \in [80, 90[ \\ 1, & \text{if } AC_i \in [90, 100[ \end{cases} \quad (3.11)$$

then  $DACI$  for GW-1 (resp. GW-2) is equal to  $(40/2 + 70 (1+1/4)/2 + 70 (1+1/4)/2)/300 = 0.35$  (resp. 0.4). We consider the gateway with the biggest  $DACI$  is the most suitable to access the Internet.

### 3.3.3. Link Quality Metric (LQM)

We define the quality of a link as a function of two main parameters: Expected Link Quality ratio ( $ELQ$ ) and interference ratio ( $IR$ ).

#### 3.3.3.1. Expected Link Quality (ELQ)

$ELQ$  is similar to ETX; however, in  $ELQ$ , we use only forward link delivery ratio rather than forward and reverse delivery ratios of the link. ETX computes the expected link quality by assigning equal weight to the forward and backward delivery ratios; it has been proved in [80] that this technique cannot be applied in real networks.

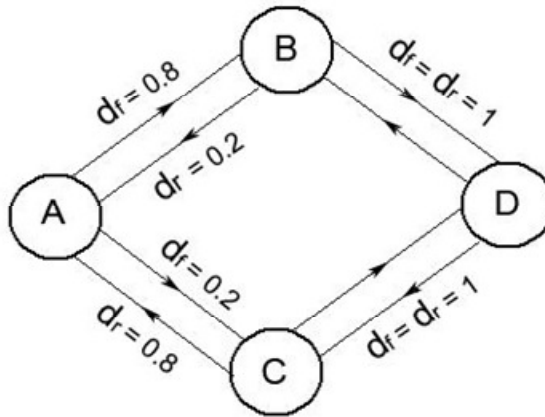


Figure 17. Forward and reverse links asymmetry

Let us consider the example shown in Figure 17 where  $A$  wants to send data to  $D$ ; ETX assigns the same weight to forward ( $d_f$ ) and reverse ( $d_r$ ) links. We compute  $ETX(AB)$  and  $ETX(AC)$  and find that they assume the same value 6.25 ( $ETX(AB) = 1/0.8*0.2$  ,  $ETX(AC) = 1/0.2*0.8$ ). Hence, paths  $A-B-D$  and  $A-C-D$  are considered to be of the same quality and the choice would be arbitrary whereas in reality, we can reasonably expect link  $(A, B)$  to perform better than link  $(A, C)$  because of the asymmetry in the size of data packets and ACKs. ACKs are more resistant to poor delivery ratios and get through even under high link loss conditions because of their tiny size compared to data packets. Hence, the reverse delivery ratio which accounts for ACK packets is relatively less important than the forward delivery ratio which represents the larger data packets.

In our scheme, we use the same technique used in ETX where each node broadcasts periodically small probe packets. Thus, based on their success rate an approximation of the link quality can be made. Thus,  $ELQ$  can be computed by each MR as follows:

$$ELQ = \frac{1}{d_f} \tag{3.12}$$

where,  $d_f$  is the number of successfully transmitted probe packets. To avoid unidirectional links, we check for every period if at least one packet is received in the reverse direction.

### 3.3.3.2. Interference Ratio (IR)

The performance of multi-hop wireless networks is considerably impacted by co-channel interferences; these interferences can be classified into inter-flow and intra-flow interferences. The proposed *IR* metric is based on the well-known physical model presented in [84] to describe the interference among different MRs. In such a model, a wireless transmission from a sender  $S$  to a neighboring receiver  $R$  is successful if the Signal to Interference and Noise Ratio (*SINR*) at  $R$  is bigger than a threshold  $SINR_T$ :

$$\frac{P_R(S)}{N + \sum_{k \in \nu'} P_R(k)} \geq SINR_T \quad (3.13)$$

where  $P_R(S)$  denotes the received power at  $R$  from  $S$ ,  $N$  is the background noise,  $\nu'$  is the set of nodes in the interference range of  $R$ , and  $P_R(k)$  is the interference power from an interfering node  $k$ .

Thus, by considering  $P_{max}$  as the maximum tolerable interference at the receiver and which can be computed as follows:

$$P_{max} = \frac{P_R(S)}{SINR_T} \quad (3.14)$$

We define similarly to [2, 3] the Interference Ratio (IR) on link  $S$ - $R$  as

$$IR(SR) = \frac{\sum_{k \in \nu'} P_R(k)}{P_{max}} \quad (3.15)$$

*IR* value is between 0 (i.e., idle channel) and 1 (busy channel). It is worth noting that the proposed *IR* measurement technique does not use any extra probing packets; however, it is inaccurate in the absence of traffic in the network.

### 3.3.3.3. LQM formulation

The interference metric measures the interference present on the link. Usually, this interference is due to the activity in the neighborhood. It is a fact that high interferences may cause a bad delivery ratio. But, it is also possible for a link to have zero interference and a



poor SNR or high bit error rates due to physical factors such as obstructions. Thus, it is necessary to take into consideration both  $IR$  and  $ELQ$  metrics to measure link quality (in opposition to  $ETX$  that takes into account only delivery ratio). Let  $X$  be a network node and let  $n$  be the number of 1-hop neighboring nodes of  $X$  that share the same channel  $i$  (number of interfering nodes). We define  $LQM$  as a weighted function of  $IR$  and  $ELQ$  for link  $l$ :

$$LQM_l(IR, ELQ) = \left(1 - \left(\frac{1}{2}\right)^n\right) \times IR + \left(\frac{1}{2}\right)^n \times ELQ \quad (3.16)$$

### 3.3.4. Gateways Advertisement message (GWADV)

Periodically, each GW broadcasts GWADV to MRs. The format of GWADV is as follows:

ID_M	ID_G	DACI	Metics_R
------	------	------	----------

Figure 18. GWADV format

where (1)  $ID_M$  is the unique identifier of the message; (2)  $ID_G$  is the identifier of the GW sending GWADV message; (3)  $DACI$  is the indicator at the gateway  $ID_G$ ; and (4)  $Metrics_R$  is a list of routing metrics ( $ELQ, IR$ )

Upon receipt of GWADV, a MR updates its routing table to the GW, adds its metrics related to the neighboring MR sending GWADV and then decides to rebroadcast or not the updated message; a previously received GWADV is rebroadcasted again only if it is received from a different neighboring MR or a more optimal path is discovered.

### 3.3.5. Path quality

Based on links quality, each MR can compute the quality of a path to the known GWs (i.e., GW in the routing table). We define path quality  $PQ$  of path  $p$  from MR  $s$  to GW  $g$  as follows:

$$PQ_{s \rightarrow g} = \text{Max}_{k \in p} (LQM_k) + \prod_{k \in p} LQM_k \quad (3.17)$$

One can argue that  $\prod_{k \in p} LQM_k$  is sufficient to represent path quality (i.e. path with smallest value has best quality); let us consider the example illustrated in Figure 19 to show that this is not the case.  $A, B, C, D$  and  $E$  are MRs and black nodes are interfering neighbors. Let us assume  $A$  wants to communicate with  $E$ ;  $A$  can send traffic to  $E$  either over  $A-B-C-E$  or  $A-D-E$ .

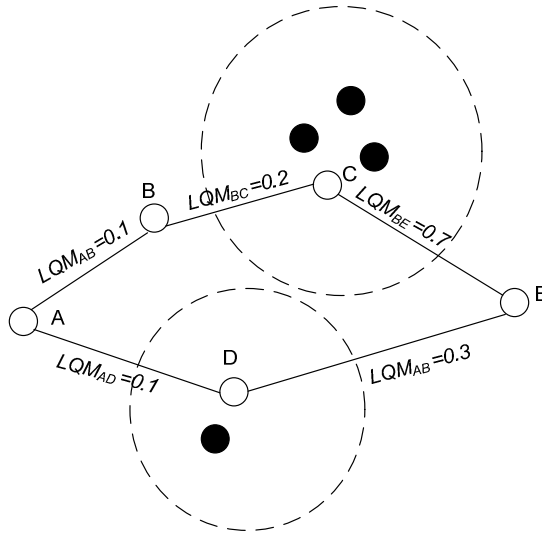


Figure 19. Path with bottleneck link

If we consider the product of  $LQMs$  as the path quality, then, the quality of path  $A-B-C-E$  (resp.  $A-D-E$ ) will be equal ( $LQM_{AB} \times LQM_{BC} \times LQM_{CE} = 0.1 \times 0.2 \times 0.7 = 0.014$  (resp.  $0.03$ )). In this example, the path with the smallest value cannot be considered as the best path. Indeed, by revisiting the quality of the links of each path, we observe that link  $C-E$  is a bottleneck link in  $A-B-C-E$ ; thus,  $A-B-C-E$  is a path that must be rejected.

Now, if we use equation (3.17) to compute path quality, path quality of  $A-B-C-E$  (resp.  $A-D-E$ ) will be equal  $0.714$  (resp.  $0.33$ ); in this case,  $A-D-E$  will be selected as best path.

### 3.4. BP2BG: Best Path to best Gateway scheme for multichannel multi-interface WMNs

In this section, we first define the BP2BG as a metric for path selection. Then, we present the algorithm used by each MR to compute best path to be gateway.

#### 3.4.1. Path selection to the best gateway

Figure 20 shows a network topology where  $S1$  and  $S2$  are two traffic sources.  $G1$ ,  $G2$  are the GWs and  $A$ ,  $B$ ,  $C$ ,  $D$  are intermediate MRs.

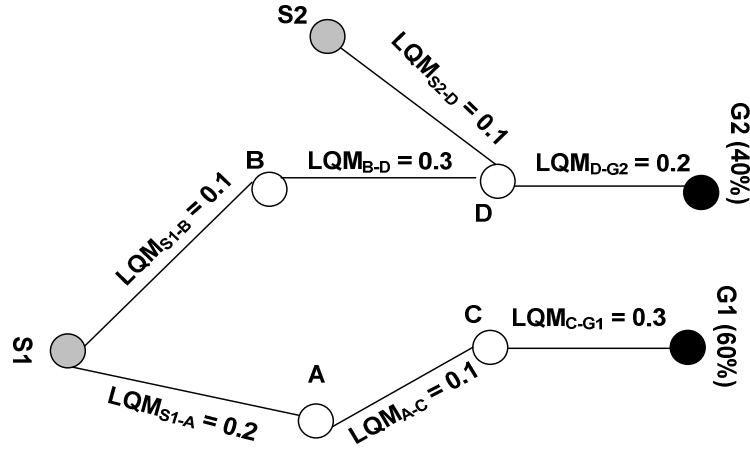


Figure 20. Paths to different Gateways

In this example,  $PQ_{S1 \rightarrow G1} = PQ_{S1 \rightarrow G1} = 0.306$ .  $S1$  may decide to randomly select one of the gateways; however, such a selection may result in choosing the path with the overloaded gateway ( $G1$  in the example). In this paper, we propose to use a combination of  $PQ$  and  $DACI$  (called BP2BG) in order to select best path. We define BP2BG as follows:

$$BP2BG_{(g,p)} = \alpha (1 - DACI) + (1 - \alpha)PQ \quad (3.18)$$

where  $0 < \alpha < 1$

According to BP2BG, each source can select best path to best GW. This will not only balance the load among gateways but also reduce traffic passing through the same gateway.

### 3.4.2. Waiting before changing paths

Let us consider the topology shown in Figure 21 where  $G1$ ,  $G2$  and  $G3$  are GWs,  $R_i$  ( $i=1..10$ ) are MRs, solid lines represent current paths and dashed ones represent alternative paths. A number on a link represents the assigned channel to this link. For  $R8$ , the path to  $G2$  is  $R8-R5-R1-G2$  and it uses channels 9, 8 and 7.

Now, let us assume that  $R8$  and  $R9$  receive GWs Advertisement Messages (GWADV) from  $G1$  and  $G2$ .  $G2$  does not have enough available capacity. In this case,  $R8$  and  $R9$  will select alternative paths with better quality. If they perform this selection at the same time, traffic from  $R8$  will be carried by  $R8-R4-R1-G1$  and traffic from  $R9$  will be carried by  $R9-R6-R2-G2$ . So, because links  $R9-R6$  and  $R10-R7$  use the same channel, the traffic through the path  $R9-R6-R2-G2$  will create interferences with one from  $R10$  to  $G3$ .

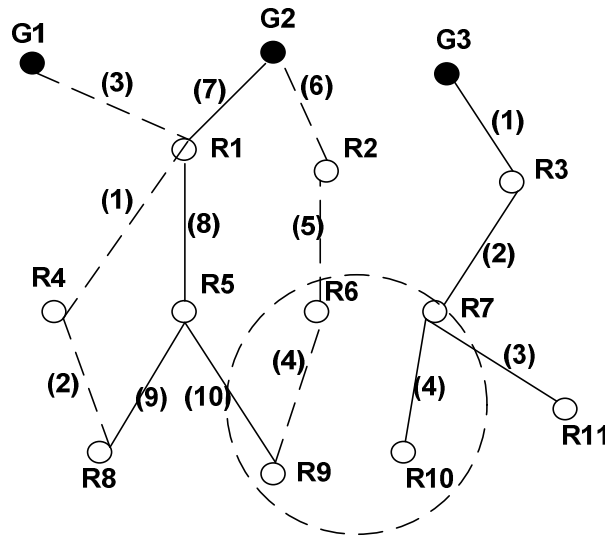


Figure 21. Alternative paths

If only traffic from  $R8$  is rerouted over  $R8-R4-R1-G1$  and  $R9$  does not switch to an alternative path the overload situation will be resolved. Therefore, we conclude that it is not appropriate for sources to change paths immediately upon determining BP2BG change; we propose that sources wait a randomly generated period of time  $T$  before making changes.  $T$  is computed as follows:

$$T = \frac{1}{k_i \times \sum_j k_j} \times S_{Time} \quad (3.19)$$

where  $k_i$  is the degree of source node  $I$  (the sum runs over the  $j$  neighbors of node  $i$ ) and  $S_{Time}$  is a predefined time window. The rationale behind using  $T$  is to enable source nodes that have high degrees and neighbors with high degrees to change their paths first in case of problems. Furthermore, the difference between the quality of the current path and the quality of alternative path should exceed a predefined threshold before deciding to change.

### 3.4.3. BP2BG Algorithm

Algorithm 1 shows the pseudo code of the proposed path selection algorithm.

Algorithm 1: Path and gateway selection at each Source MR

---

**Input:** GWADV

**Output:** Selected path to selected gateway

**Variables:** Best\_Path; Current\_pathy; Timer T = period; L /\*List of paths\*/

---

Begin

- 1- Receive GWADV from a gateway
- 2- Update the routing table /\*corresponding GW and path entry\*/
- 3- Put in L the path with the minimum PQ for each GW
- 4- Best\_path  $\leftarrow$  the path with the minimum BP2BG in L
- 5- If (Best\_path  $\neq$  Current\_path){
- 6-     Trigger timer T
- 7-     If (T expires without receiving GWADV)
- 8-     Current\_path  $\leftarrow$  Best\_path
- 9- }

End

---

Upon receipt of GWADV, a source node executes BP2BG Algorithm (Algorithm 1); it computes the path and updates its routing table to the transmitter GW. In case of the path quality change, the source node computes a waiting time period (see Equation 3.19); indeed; the path is changed if the waiting time period expires before receiving a new GWADV.

### 3.5. Simulation and results

We study the performance of BP2BG by using ns2 simulator with the module implementing multi-radio and multi-channel WMNs [85]. We compare BP2BG to four other schemes: nearest gateway selection, gateway load based selection, ETX metric and interference metric. If nearest gateway selection scheme is used, the path with the minimum number of hops to a gateway will be selected to route traffic; if the gateway load based selection scheme is used, the path with the minimum gateway load is selected; if ETX metric is used, the path that minimizes the product of the ETXs (of links that form the path) is selected; if interference metric is used, the path that minimizes the product of interference ratios (of links that form the path) is selected. The terms X (where X assumes ETX, Load, nearest gateway or interference) and X based scheme are used interchangeably in the rest of this Section. The performance is evaluated in terms of (1) network throughput: represents the total number of bits that are correctly received by all nodes of the WMN in the unit of time (kbps); (2) average end to end delay: represents the delay for sending CBR packets from source nodes to GWs; and (3) average packet loss: represents the percent of CBR packets dropped during simulation.

Table 2- NS2 Simulation setup

<b>Simulation Parameters</b>	<b>Values</b>
Simulation Time	100 seconds
Network Area	1000x1000
MAC Layer used	802.11b
Data rate	11Mbps
Frequency	9.14e+08
Traffic Type	CBR (UDP)
Network Load	1000-3000 Kbps
Packet Size	1000 bytes

The topology used in the Backbone Wireless Mesh Networks consists of 15 MRs randomly placed and 3 GWs. To each interface is assigned one channel [86]. Every node can

send and receive traffic. The traffic generated from a source node may cross several intermediate nodes (i.e., multi-hop routing) to reach the Internet through a GW. During channel assignment phase, we create six interfering links in order to show the capability of BP2BG to react to interferences compared to the other algorithms.

Figure 22 shows that the delay increases with the network load. We observe that BP2BG outperforms all the four schemes. More specifically, BP2BG outperforms nearest gateway, load-based, ETX and interference based schemes by 15%, 56%, 25% and 11% respectively in the case of high data rates (and by 2%, 3%, 11% and 1%.in the case of low data rates). These results are expected since (1) nearest gateway and ETX-based schemes use a single routing metric without taking into account interferences and available capacity at gateways; and (2) interference and load based schemes use also a single routing metric; thus, paths with low interferences to overloaded gateways or paths with high interferences to lightly loaded gateways can be selected resulting in more packet losses/retransmissions and thus longer end-to-end delays.

We conclude that BP2BG that combines all metrics in selecting a path and a gateway to route traffic from a source to the Internet produces paths with shortest delays.

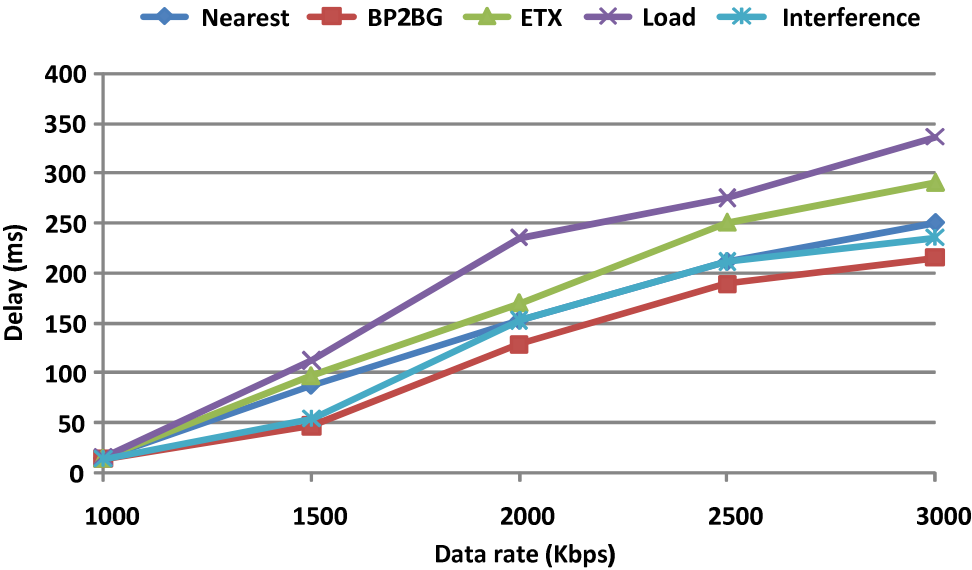


Figure 22. End-to-end delay vs. data rate

Figure 23 shows the mean end-to-end delay over all the loads (1000, 1500, 2000, 2500 and 3000 kbps). We observe similar trend as shown in Figure 22. In general *BP2BG* provides smaller average delays compared to other metrics. This is due to (1) the nature of the metric which tries to select the links that have less interferences and less packets losses; and (2) the avoidance of paths with bottleneck links.

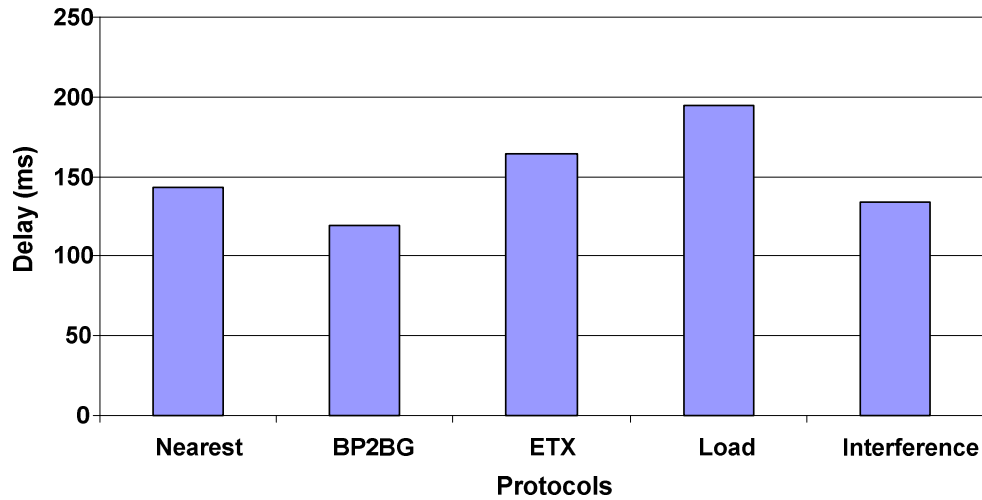


Figure 23. Mean delay

In the next set of simulations, we study the performance of *BP2BG* compared to other metrics when increasing the data rate. Figure 24 shows that *BP2BG* outperforms all other schemes in terms of throughput. More specifically, *BP2BG* outperforms nearest gateway, ETX, interference and load based schemes by 30%, 20%, 16% and 10% respectively. Nearest gateway, ETX and Load select the path without considering interferences. Indeed, a path with intra-flow interferences can be selected; thus, only one link can be active at a given time causing more packets to be stored in interface queues. This will lead to excess delay, packet losses and less throughput especially when these queues are full; this happens more frequently for high data rates. These results are expected since *BP2BG* selects paths taking into account all metrics resulting in significantly less packet losses/retransmissions.



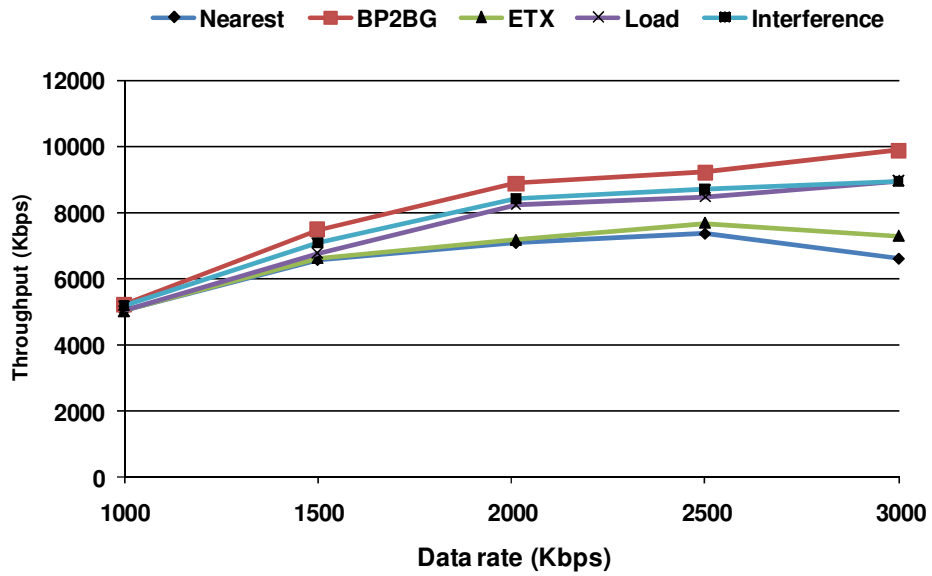


Figure 24. Network throughput vs. data rate

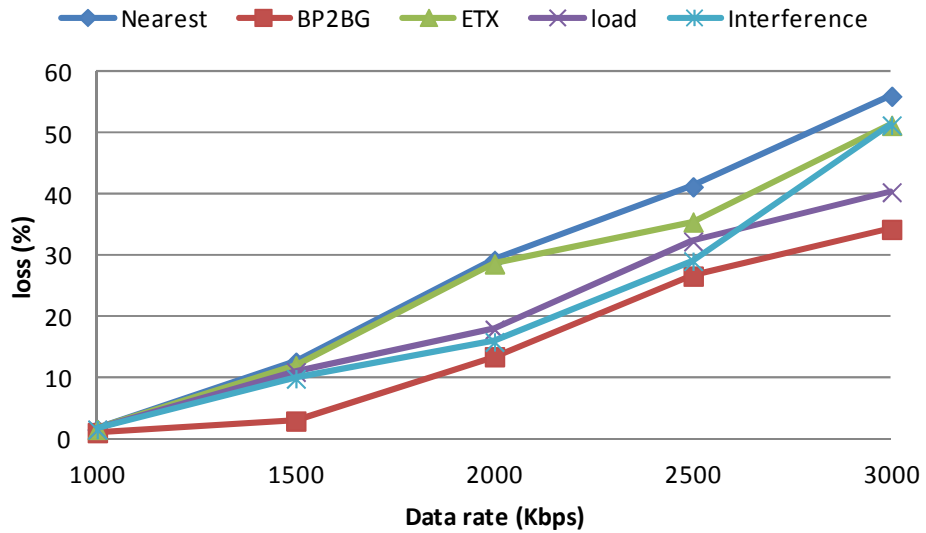


Figure 25. Packet loss vs. data rate

Figure 25 shows the impact of data rate variation on packet loss ratio. We observe that BP2BG outperforms all other schemes in terms of packet loss ratio when data rate increases. More specifically, at high data rates (e.g., 2500 kbps) BP2BG outperforms nearest gateway, ETX, interference and load based schemes by 35%, 25%, 17% and 10% respectively. By increasing data rates, interferences increase, Interface Queues overflow and gateways become

overloaded leading to more packet losses. These problems are avoided by BP2BG during path selection.

### **3.6. Conclusion**

In this paper, we investigated the impact of using metrics individually to select paths and/or gateways in multi-channel backbone WMNs. After identifying the shortcoming of existing routing and gateway selection metrics, we proposed a new metric, called BP2BG, that takes into account packet losses, interferences (intra-flow and inter-flow) and load at gateways together to select best paths to best gateways. Simulations results show that BP2BG outperforms all existing schemes in terms of throughput, delay and loss.

## **Chapitre 4:**

# **Reinforcement Learning Based Routing in Wireless Mesh Networks**

Mustapha Boushaba, Abdelhakim Hafid, Abdeltouab Belbekkouche, Michel Gendreau

### **Abstract**

This paper addresses the problem of efficient routing in backbone wireless mesh networks (WMNs) where each mesh router (MR) is equipped with multiple radio interfaces and a subset of nodes serve as gateways to the Internet. Most routing schemes have been designed to reduce routing costs by optimizing one metric, e.g., hop count and interference ratio. However, when considering these metrics together, the complexity of the routing problem increases drastically. Thus, an efficient and adaptive routing scheme that takes into account several metrics simultaneously and considers traffic congestion around the gateways is needed.

In this paper, we propose an adaptive scheme for routing traffic in WMNs, called RLBD (Reinforcement Learning-based Distributed Routing), that (1) considers the critical areas around the gateways where mesh routers are much more likely to become congested and (2) adaptively learns an optimal routing policy taking into account multiple metrics, such as loss ratio, interference ratio, load at the gateways and end-to end delay.

Simulation results show that RLBD can significantly improve the overall network performance compared to schemes using either interference and channel switching (MIC), Best Path to Best Gateway (BP2BG), Expected Transmission count (ETX), nearest gateway (i.e., shortest path to gateway) or load at gateways as a metric for path selection.

**Keywords:** WMN; Interferences; ETX; Reinforcement Learning; Routing.

## 4.1. Introduction

During last several years, wireless communications technologies have increasingly gained importance in our daily lives. These technologies have given rise to several types of wireless networks, such as WSNs (wireless sensor networks), VANETs (vehicular area networks) and WMNs (wireless mesh networks). Among these networks, WMNs [4, 87] have attracted significant research due to their features that include dynamic self organization, self configuration, easy maintenance and low cost. In case of link failures, the network is able to automatically establish alternative routes. A WMN can be seen as a multi-hop Mobile Ad-hoc Network (MANET) with extended connectivity at the difference that WMNs are characterized by a relatively static architecture and low mobility.

To increase WMN performance and capacity, nodes can be equipped with multiple radios and multiple channels. Otherwise, with a single channel, a node cannot transmit and receive simultaneously. Indeed, due to the scarce nature of wireless channel resources and to the limited number of channels supported by radios, network performance is highly impacted by interferences and congestion causing considerable packet losses and higher delays.

Communications between two nodes in a multi-hop WMN can be supported by several intermediate, nodes called Mesh Routers (MRs). The role of MRs is to relay information from one node to another. Usually, MRs send traffic to the gateway (GW) that connects nodes to the Internet. Indeed, by equipping a WMN topology with a single GW to connect MRs to the Internet, the gateway selection problem becomes simple; this is because all upstream/downstream traffic flows must traverse the same GW to the internet; this node is more likely to become the bottleneck/single point of failure in the network [27]. To mitigate this problem, multiple gateways are installed to distribute load among them, and hence, improve performance. However, increasing the number of GWs does not necessarily increase the network capacity of WMNs. Indeed, network capacity is closely related to network connectivity and the placement of GWs; these issues are out of scope of this paper.

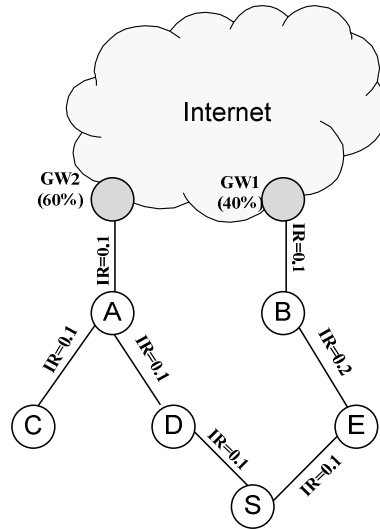


Figure 26. WMN, multi-metrics routing case

The main goal of a routing protocol is to find better routes according to some requirements. These requirements vary according to client needs (e.g., bandwidth, delay, and packet loss). In general, routing protocols are designed to optimize only one of these goals [24, 25]; however, there exist several situations in WMNs where the choice of one metric, to optimize, impacts negatively the performance in terms of another metric. This situation is illustrated in Figure 26 where nodes *A*, *B*, *C*, *D*, *E* are MRs, node *S* is the source and nodes *GW1* and *GW2* are gateways. In this example, we consider, as a routing metric, Interference Ratio (*IR*) or the load at the gateways (*GW1* and *GW2*). Obviously, solving the optimization of these metrics separately does not lead to an optimal solution. If *S* wants to send traffic to the Internet, the best path to choose, when using *IR*, will be *S-D-A-GW2*; it is the path with the smallest interference ratio. On the other hand, the best path, when using load at the gateways, will be *S-E-B-GW1*; it is the path that traverses the least loaded gateway. This shows that choosing different metrics could yield different (may be conflicting) results. Thus, taking into consideration several metrics simultaneously is necessary to optimize multi-hop routing in WMNs.

In WMNs, multiple users intend to communicate to the Internet through gateways. In such environment, depending on the network topology and the routing strategy, traffic concentration may be observed not only at certain gateways but also in mesh routers (in the neighborhood of gateways) which become traffic “hot-spots” (i.e., nodes *A* and *B* in Figure.

26). Therefore, this concentration may increase congestion and interferences excessively on the wireless channels around the gateways. Thus, the neighborhood of gateways is identified as a critical area that routing protocols for WMNs should take into consideration. More specifically, gateways and mesh routers in the critical area should be given particular attention during path computation to prevent drastic performance degradation in that area.

In this paper, we propose to use reinforcement learning, namely *Q-learning* algorithm to route traffic in multi-hop and multi-radio wireless mesh networks. In the proposed mechanism (RLBDR), reinforcement-learning is used to update dynamically path costs and to select the next hop each time a packet is forwarded; learning agents in each mesh router learn the best link to forward an incoming packet by continuously exploiting what they have learned in the past and exploring new alternatives to discover better actions in the future. RLBDR consist of (a) exchanging advertisement messages GWADV between gateways and mesh routers; (b) measuring the quality of links, e.g., interference ratio and loss ratio; (c) selecting the best gateway; and (d) using a learning agent in each node to learn the best neighbor to send an incoming packet towards a given gateway.

The remainder of the paper is organized as follows. In Section 4.2, we present related work on metrics and routing protocols in wireless mesh networks.. In Section 4.3, we present the network model, notations and definitions we use throughout the paper; then, we describe RLBDR in detail. Simulation results are presented and discussed in Section 4.4. Section 4.5 concludes the paper.

## **4.2. Related work**

In this paper, we propose a reinforcement learning-based routing scheme, in WMNs, that uses a novel routing metric. Thus, in this section, we present an overview of (a) routing metrics proposed in the context of WMNs; and (b) learning techniques used in routing schemes.

### **4.2.1. Routing metrics for wireless mesh networks**

Many routing schemes have been proposed in the literature for different types of wireless networks [49, 88, 89, 90]. Most of these schemes could be roughly divided into three

categories: (1) proactive routing protocols (e.g., Optimized Link State Routing OLSR [60]); (2) reactive routing protocols (e.g., Ad hoc On-demand Distance Vector AODV [58]); and (3) hybrid protocols (e.g., Temporally-ordered routing algorithm TORA [62]).

Based on the aforementioned routing techniques, several routing metrics have emerged. In general, a routing metric is used, by a routing protocol, to select the path having the highest throughput, the lowest delay and/or the lowest packet loss ratio. Hop-count is the simplest metric in routing problems. However, for WMNs, hop-count is a poor choice; indeed, there may be a shorter path between source and destination nodes that present heavier interferences and higher packet losses than a longer path in terms of hop count. ETX [24] is a routing metric that estimates the number of transmissions and retransmissions needed to successfully transmit a frame on a link. ETT [25] estimates the time a data frame needs to be successfully transmitted on a link. ETX is defined in Eq. (4.1):

$$ETX = \frac{1}{d_f \times d_r} \quad (4.1)$$

where  $d_f$  and  $d_r$  denote the forward and the reverse delivery ratio on the link, respectively. The ETT metric is defined in Eq. (4.2).

$$ETT = ETX \times \frac{S}{B} \quad (4.2)$$

$S$  represents the packet size and  $B$  the bandwidth of the link.

The key shortcoming of ETX and ETT is that they do not consider interferences when selecting a path.

Among the metrics that are based on ETX and/or ETT, we have Weighted Cumulative Expected Transmission Time (WCETT) [25], Metric of Interference and Channel switching (MIC) [48] and Best Path to Best Gateway (BP2BG) [73].

WCETT [25] has been proposed as an extension of ETT to take into account intra-flow interferences caused by channel diversity. For a given path, WCETT is defined as follows:

$$WCETT = (1 - \beta) \times \sum_{i=1}^n ETT_i + \beta \times \max_{1 \leq j \leq k} X_j \quad (4.3)$$

where  $0 < \beta < 1$ ,  $n$  is the number of links in the path.  $ETT_i$  is the ETT of link  $i$  ( $1 \leq i \leq n$ ),  $X_j$  represents the sum of ETT for each link operating on channel  $j$ , and  $k$  is the total number of channels. WCETT selects paths with high channel diversity (i.e., with the most balanced number of channels used in the path [91]). However, it assumes that all the links of a path operating on the same channel interfere; this can lead to the selection of non-optimal paths. Moreover, traffic to the Internet may pass through a path that has less interference but through a congested gateway. WCETT-LB (WCETT-Load Balancing) [92], has been proposed as an extension to WCETT to take into account load balancing; indeed, it makes use of a load factor that consists of the average queue length and the degree of traffic concentration.

MIC [48] was proposed to improve WCETT. For a path  $p$ , MIC is defined as follows:

$$MIC(p) = \frac{1}{N \times \min(ETT)} \times \sum_{link\ l \in p} IRU_l + \sum_{node\ i \in p} CSC_i \quad (4.4)$$

where  $N$  is the number of nodes in the network and  $\min(ETT)$  is the smallest  $ETT$  in the network.  $IRU$  (Interference-aware Resource Usage) and  $CSC$  (Channel Switching Cost) are defined as follows:

$$IRU_l = ETT_l \times N_l \quad (4.5)$$

$$CSC_i = \begin{cases} w_1 & \text{if } CH(\text{prev}(i)) \neq CH(i) \\ w_2 & \text{if } CH(\text{prev}(i)) = CH(i) \end{cases} \quad (4.6)$$

where  $N_l$  is the number of neighbors that interfere when transmitting on link  $l$ .  $w_1$  and  $w_2$  are costs ( $0 \leq w_1 < w_2$ ), and  $CH(\text{prev}(i))$  is the channel used by the previous hop to node  $i$  and  $CH(i)$  is the channel used for next hop at node  $i$ .  $MIC$  tries to avoid consecutive links in the same path operating on identical channels, by adding a high cost  $w_2$  when using the same channel, and a small cost  $w_1$  when different channels are used (usually  $w_1=0$ ). Using  $MIC$  encourages channel diversity by increasing the cost when a channel is reused.  $MIC$  captures



inter-flow interferences by assuming that all nodes located in the collision range of a particular link contribute evenly to interferences; this assumption is not accurate since the impact of interferences depends mainly on data rate and the distance between nodes.

In a previous work, we have proposed BP2BG [73]; it is a source routing protocol able to combine a best GW selection and a best path selection between a source and a destination in the Internet. BP2BG considers that the reverse delivery ratio, which uses small ACK packets, is relatively less important than the forward delivery ratio, which uses larger data packets. Thus, the Link Quality Metric (*LQM*) is defined as a relation between the Expected Link Quality (*ELQ*), which considers only the forward link delivery ratio, and the Interference Ratio (*IR*).

#### 4.2.2. Learning in routing schemes

Reinforcement learning is a technique in machine learning which consists of finding the optimal action to perform in a dynamic environment. Generally, decisions are made by an agent, based on the learning from trial-and-error, while it is interacting with its environment. The ultimate goal is to learn an optimal policy that maximizes the reward of the agent on the long run. One of the challenges in reinforcement learning is the exploitation versus exploration problem: the agent must exploit its knowledge from previous learning but it has to explore new actions and states in its environment in order to look for better policies. Reinforcement learning has been applied successfully in a variety of network schemes, including routing and admission control [93 94, 95, 96, 97, 98, 99, 100, 101, 102]. Generally, Reinforcement learning is used when an optimal behavior is to be learned; applying reinforcement learning to routing in communication networks was firstly introduced by Boyan and Littman [94] and developed by several authors in different types of networks. Some of these protocols, using reinforcement learning, are based on Q-Learning (e.g., [95] for OBS networks, [96] for VANET, [97] for Ad Hoc networks, [98] for wireless mesh networks and [93] for wireless sensor networks). The core of Q-learning algorithm is given by Eq. (4.7):

$$Q(s_t, a_t) \leftarrow Q(s_t, a_t) + \alpha \times \left[ r_{t+1} + \gamma \max_{a'} Q(s_{t+1}, a_{t+1}) - Q(s_t, a_t) \right] \quad (4.7)$$

where  $\alpha$  is the learning rate,  $\gamma$  is the discount factor,  $s_t$  and  $a_t$  are the state and the selected action at time  $t$ , respectively and  $r_{t+1}$  is the reward at time  $t+1$ . The value  $Q(s_t, a_t)$ , called Q-value, is defined as an estimate of the quality of choosing an action at time  $t$  and following an optimal policy thereafter.

Ant Colony Optimization (ACO) which is a special case of distributed reinforcement learning [103] has been studied in different network environments [104, 105, 106, 107, 108, 109, 110]. It has been inspired from operating principles of ants behavior which is the learning of the shortest path from a source food to the nest. This information will then be shared with other ants through stigmergy [104] which consists of the use of a certain amount of pheromone. Subramanian et al. [105] focused on routing in packet-switched networks based on ACO; they make use of messages transporting the cost information from a source to a destination to enhance the update of routing tables and probabilities used by each router. Iima et al. [106] propose a swarm reinforcement learning method based on ACO; the proposed method is an information exchange method where each agent updates its own Q-values by using pheromone-Q values like the trail pheromones of real ants. Good surveys on the use of Ant Colony Optimization technique can be found in [107, 108, 109, 110].

In this paper, we propose a new routing scheme *RLBDR* (Reinforcement Learning based distributed Routing) for wireless mesh networks that adaptively learns an optimal routing policy, taking into account multiple routing metrics, such as loss ratio and interference ratio. The proposed scheme extends our contribution in [26] by (1) defining a new metric for path selection; more specifically, MRs in the neighborhood of gateways are given more weight when computing paths from a source to a gateway; (2) proposing a loop-free routing algorithm; and (3) using and comparing two reward functions (in the context of reinforcement learning) taking into account the critical area around the gateways in two different ways.

### **4.3. Reinforcement Learning Based Distributed Routing to Gateways**

We consider WMNs with two sets of nodes: MRs and GWs. MRs form a multi-hop wireless backbone to relay traffic between users and Internet. To reach the Internet, traffic

passes through GWs which are MRs with additional functionalities (i.e., more buffer size, wired and wireless interfaces, etc.). In the rest of this Section, we present the details of the proposed RLBDR scheme.

### 4.3.1. Gateway Load

Periodically, each GW broadcasts to MRs an advertisement message GWADV that includes information about its load. GW load can be measured by monitoring the amount of buffered data (received from the WMN) in the GW interface over a time period. We assume that this estimation is performed according to a moving average. At every generated advertisement, the current load  $L_g[t]$  is based on the previous estimated load  $L_g[t-1]$  and the volume of traffic  $V[t]$  that gateway  $g$  has processed since the last advertisement.

$$L_g[t] = \alpha \frac{V[t]}{C_g} + (1-\alpha)L_g[t-1] \quad (4.8)$$

where  $\alpha \in [0, 1]$  is a weighting coefficient to choose the impact of the new load measurement and  $C_g$  is the maximum queue length of gateway  $g$ .

### 4.3.2. Link Quality Metric (LQM)

The interference metric measures the interference present on the link. Usually, this interference is due to communication activity in the link neighborhood. In fact, high interferences may cause a bad delivery ratio. But, it is also possible for a link to have no interference and a poor Signal to Noise Ratio (*SNR*) or high bit error rates due to physical factors, such as obstructions. Thus, we define  $LQM_l$  as a weighted function of two key parameters *IR* (Interference Ratio) and *CL* (Congestion Level) for link  $l$ .

#### 4.3.2.1 Interference Ratio (IR)

The performance of multi-hop wireless networks is considerably impacted by co-channel interferences; these interferences can be classified into interflow and intra-flow interferences [111]. The proposed *IR* (Eq. (4.9)) for a node  $u$  in a link  $l$  is similar to the one proposed in [55]. It estimates the interference level in the network through the Signal to Noise

Ratio ( $SNR$ ) and the Signal to Interference-plus-Noise Ratio ( $SINR$ ). Let us define  $l$  as a link between two neighboring MRs  $u$  and  $v$  operating on the same channel  $i$ .

$$IR_l(u) = \frac{SINR_l(u)}{SNR_l(u)} \quad (4.9)$$

where,  $SINR_l(u)$  and  $SNR_l(u)$  for a node  $u$  are defined in Eq. (4.10) and Eq. (4.11):

$$SINR_l(u) = \frac{P_l}{Noise + \sum_{w \in N_{l-v}} \tau_w \cdot P_w} \quad (4.10)$$

$$SNR_l(u) = \frac{P_l}{Noise} \quad (4.11)$$

where,  $P_l$  is the signal strength at link  $l$ ,  $N_l$  is the set of nodes from which node  $u$  can hear a packet that interferes with link  $l$  and  $\tau_w$  gives the amount of time that node  $w$  occupies the channel.

#### 4.3.2.2. Congestion Level (CL)

The motivation behind using  $CL$  is to use paths with smaller link utilization. Consider link  $l$  and let  $Succ(l, t)$  denotes the set of packets that have successfully traversed link  $l$  during a period of time  $t$  and let  $Size_i$  denotes the size of packet  $i$ . The utilization  $U$  of link  $l$  is defined as follows:

$$U(l, t) = \frac{\sum_{i \in Succ(l, t)} Size_i}{BW_l} \quad (4.12)$$

where,  $BW_l$  is the bandwidth capacity of link  $l$ . To avoid fluctuations/oscillations, we use a moving average for *congestion level*. Thus, we define  $CL$  as follows:

$$CL(l, t) = \beta U(l, t) + (1 - \beta) CL(l, t - 1) \quad (4.13)$$

where  $\beta \in [0, 1]$

### 4.3.2.3. LQM formulation

Let  $X$  be a network node and let  $n$  be the number of 1-hop neighboring nodes of  $X$  that share the same channel  $i$  (number of interfering nodes). We define  $LQM_l$  for link  $l$  operating on channel  $i$ , as follows:

$$LQM_l = \left(1 - \left(\frac{1}{2}\right)^n\right) \times IR_l + \left(\frac{1}{2}\right)^n \times CL_l \quad (4.14)$$

The rationale behind the definition of  $LQM_l$  shown in Eq. (4.14) is our intention to capture interferences and congestion, in computing the link quality, while giving dynamically more weight to interferences (they impact considerably the network performance). A bigger value of  $n$ , gives more importance to interferences in computing the link quality; For  $n = 1$ , interferences and congestion have the same weight (0.5 each) to compute the link quality. Obviously, the smaller is the  $LQM_l$  of a given link, the better its quality.

### 4.3.3. Path quality

In RLBDR, the goal is not only to minimize  $LQM_l$  but also to select, when suitable, shorter paths that traverse less congested routers in the neighborhood of gateways. Indeed, the objective is to determine a route from a source to a selected gateway while ensuring minimum interferences and losses around the selected gateway. By using link quality, each MR can compute the path quality to a given GW (i.e., a GW in the routing table). We propose two metrics to compute the path quality: (a)  $PQ$  (*Path Quality*); and (b)  $Z-PQ$  (*Zone Path Quality*).

#### 4.3.3.1. PQ

We define the *Path Quality*  $PQ$  of path  $p$  having  $n$  hops from MR  $s$  to GW  $g$  as follows:

$$PQ_s^g(p) = \sum_{l=1}^n \frac{(LQM_l)^{d_g(l)}}{1 - LQM_l} \quad (4.15)$$

where  $d_g(l)$  is the hop distance of link  $l$  starting from gateway  $g$ .

For a given path, a low value of  $PQ$  means a good quality path and vice-versa. Given that the values of  $LQM_l$  vary between 0 and 1, the ratio  $LQM_l/1-LQM_l$  will increase significantly for high values of  $LQM_l$  as shown in Figure 27; thus,  $PQ$  gives more importance/weight to links in the neighborhood of gateways; this means that paths with high quality links in the neighborhood of gateways will be preferred over other paths.

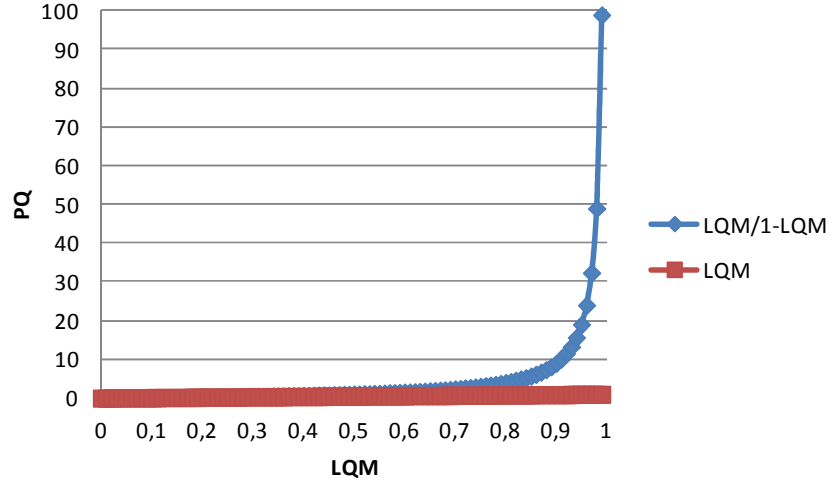


Figure 27. LQM vs PQ

The decision to select best path  $P_g$  to gateway  $g$  is given by Eq. (4.16) where  $Pz$  is the set of candidate paths for routing packets from source node  $s$  to gateway  $g$ ,  $m$  is the cardinality of  $Pz$ ,  $p_z$  is a path belonging to  $Pz$ , and  $|p_z|$  is the size of  $p_z$  (i.e., number of hops).

$$P_g = \arg \min_{1 \leq z \leq m} \left( \frac{PQ_s^g(p_z)}{|p_z|} \right) \quad (4.16)$$

#### 4.3.3.2. ZPQ

We define the critical zone ( $GZ$ ) of gateway  $g$  as the set of MRs that are at most  $N$ -hops away from  $g$  where  $N$  assumes a predefined value (e.g., 2). In the critical zone, traffic concentration increases congestion and interferences significantly. Our Objective is to give more importance/weight to nodes in  $GZ$  to help reducing interferences around the gateway and improving packet delivery in the wireless mesh network. Therefore, we propose a new metric

gives more importance/weight (in the path selection process) to nodes in neighborhood of gateways.

We define the function  $f_l(n, LQM_l)$  as:

$$f_l(n, LQM_l) = \begin{cases} \frac{LQM_l}{1 - LQM_l} + LQM_l * A, & n \leq N \\ \frac{LQM_l}{1 - LQM_l}, & n > N \end{cases} \quad (4.17)$$

where  $N$  is the maximum number of hops in the critical zone ( $GZ$ ),  $n$  is the current hop starting from the gateway.  $A$  assumes a predefined constant value; a big enough value of  $A$  (e.g., 100) allows to differentiate good paths from bad paths and eliminate the bad ones from the routing tables. Thus, the nodes around the gateway will participate with a cost amplified by  $A$  compared to nodes outside  $GZ$ . Hence, these nodes will have more impact in the routing decision.

By using  $f_l(n, LQM_l)$ , each source router can compute the path quality to a given GW. In this case, we define Zone-based Path Quality  $ZPQ$  of path  $p$  having  $m$  hops from MR  $s$  to GW  $g$  as follows:

$$ZPQ_s^g(p) = \sum_{l=1}^m f_l(n, LQM_l) \quad (4.18)$$

#### 4.3.4. RLBDP

##### 4.3.4.1. Gateway and next hop selection

RLBDP is a distributed routing scheme where a learning agent in each node learns the best neighbor to send an incoming packet towards a given gateway. The gateway is determined in the source node according to the received advertisement messages GWADV containing the gateway load information; this means that each source node selects the best gateway based on the load. Each time a node  $i$  forwards a packet to neighbor  $j$ , node  $j$  responds by a feedback packet  $f_{ji}$  representing its (measured) appreciation of the best path to reach the corresponding gateway (i.e., the path traversing the best neighboring node of  $j$  to send the

incoming packet). In our case, the feedback is the best path metric  $PQ_g$  to the selected gateway  $g$ . We note that  $f_{ji}$  represents the reward in Eq (4.7). Upon receipt of this feedback, node  $i$  updates the corresponding Q-value entry in the Q-table (i.e., the routing table in this scheme) as follows:

$$Q_i(g) \leftarrow Q_i(g) + \alpha (f_{ji} - Q_i(g)) \quad (4.19)$$

where  $\alpha$  is the learning rate. The discount factor  $\gamma$  in this case is set to 0; this means that the agent in our scheme is opportunistic by considering only the current reward. It is worth noting that Q-tables are initialized at the beginning of the WMN operation based on the shortest path in terms of the number of hops between each MR and GW; this is to ensure that RLBDR converges to shortest path routing, when  $IR$  and  $CL$  are negligible, and thus optimizes resource utilization.

The convergence of RLBDR is guaranteed since a look-up representation of Q-values (Q-table) is used [112]. To cope with exploration issue (i.e., explore new actions and new regions in the environment that could yield better decisions), we used an epsilon greedy policy [113]; it makes the decision of sending an incoming packet to its next hop with a low probability  $\varepsilon$  (e.g.,  $\varepsilon = 0.1$ ) to be sent to a non-optimal next hop and with a high probability ( $1 - \varepsilon = 0.9$ ) to be sent to the optimal neighbor.

Based on the load at gateways (contained in GWADV messages), each source router selects the appropriate gateway and executes the pseudo code of gateway selection algorithm (Algorithm 1).

Algorithm 1 Gateway selection algorithm at source nodes

---

**Input :** *GWADV*

**Output :** least loaded gateway

**Variables :** *Best\_GW*: /\* the current best gateway\*/; *GW\_Table* : /\* load table of gateways\*/

---



Begin

- 1- Receive GWADV from a gateway
- 2- Update corresponding entry in GW\_Table
- 3- Best\_GW  $\leftarrow$  The GW with the minimum Load

End

---

The gateway selection algorithm is executed by source routers. Each gateway broadcasts periodically its load (Eq. (4.8)) using *GWADV* messages. Upon receipt of a *GWADV* message, a source router updates its gateways table and determines the current best gateway (i.e., the least loaded gateway).

At each source and intermediate MR, next hop selection algorithm (Algorithm 2) is executed. At the start, when a source router selects a gateway as its own default gateway the routing protocol selects the next hop based on the minimum hop policy to a specific gateway. Once the data transfer begins, feedbacks will be received and Q-table updated.

Algorithm 2 Next hop selection algorithm at MR *i*

---

**Input** : Packet with gateway destination *g*

**Output** : best next hop to gateway *g*

**Variables** : *Routing\_Table, j* /\*Next Hop\*/

---

Begin

- 1- Receive a packet with destination gateway *g*
- 2- Determine the next hop *j* corresponding to the path with the smallest *PQ* (or *ZPQ*); see Eq. (4.16) and Eq. (4.18)
- 3- Send packet to *j*
- 4- Receive feedback  $f_{ji}$  from *j*.
- 5- Update the corresponding entry in the *Routing\_Table* (using Eq (4.19))

End

---

When an intermediate node *i* receives a packet to forward, it knows a priori the gateway *g* to reach. Thus, each time node *i* forwards a packet to its neighbor *j*, node *j* responds by a feedback packet  $f_{ji}$  representing its appreciation of the best path to reach the

corresponding gateway.  $f_{ij}$  will be then stored in the routing table for serving to select the best next hop in future iteration.

#### 4.3.4.2. Loop-free RLBDR

Routing loops represent a serious problem for routing protocols. They occur when packets continue to be routed in endless circles through the same set of routers. This problem can have a negative impact on a wireless network because (1) It increases the network load and consequently increases the packet loss ratio and decreases the throughput; (2) Router processors are also overloaded with unnecessary packet forwarding, which slows down traffic and the convergence of the routing protocol; and (3) Routing updates can be lost or may not be processed timely. Thus, RLBDR must prevent loops.

Finding a set of alternatives to forward packets towards a given gateway can be formulated as a graph theory problem. Let us model WMN by a network graph  $G(V, E)$  where  $V = \{1, \dots, n\}$  is the set of nodes (mesh routers) and  $E$  is the set of directed links. Assume  $GW \subseteq V$  be the set of gateways in WMN. We associate to each node  $v$  a directed spanning tree  $T_g$  rooted at gateway  $g$  and having edges  $E_{T_g}$  directed towards  $g$ .  $T_g$  is obtained by selecting for each node (other than  $g$ ), in the network, its outgoing link that is traversed by the shortest path between this node and  $g$ ; this can be performed using *Dijkstra* algorithm. Having  $G(V, E)$  and  $|GW|$  spanning trees for each gateway  $g$ , the problem consists of determining a set of links  $E_{F_g} \subset E$  such that the directed graph  $F_g = (V; E_{T_g} \cup E_{F_g})$  is acyclic. Algorithm 3 shows the pseudo-code of the proposed loopless forwarding algorithm.

Algorithm 3 Loop free forwarding algorithm

---

**Input :**  $G(V, E)$

$GW$  is the set of gateways

$|GW|$  spanning trees  $T_g = (V, E_{T_g})$ ; each tree is rooted at gateway  $g \in GW$

**Output :**

$E_{F_g}, \forall g \in GW$  the set of forwarding links for gateway  $g$

$F_g = (GW, E_{T_g} \cup E_{F_g}), \forall g \in GW$ , a directed forwarding graph.

---

Step 0:

- 1- Set  $GW^* = GW$
- 2- Set  $E_{Fg} = \{ \}, \forall g \in GW$

Step 1:

- 3- Select a gateway  $g \in GW^*$
- 4- Set  $E^* = \{E - E_{Tg}\}$
- 5- Let  $d_g$  be the depth of tree  $T_g$
- 6- Let  $L_i, i \in \{1, 2, \dots, d_g\}$  be the set of nodes which are at distance  $i$  from gateway  $g$
- 7- Set  $k = d_g$

Step 2:

- 8- Select node  $u \in L_k$  such that the degree of node  $u, \delta(u) = \min_{u' \in L_k} \delta(u')$

Step 3:

- 9- Set  $E_{Fg} = E_{Fg} \cup e(u, w), \forall e(u, w) \in E^*$  directed link between  $u$  and  $w$

Step 4:

- 10- Remove all links  $e(w, u), \forall w \in V$  from  $E^*$
- 11- Remove node  $u$  from  $L_k$
- 12- If  $L_k = \{ \}$  then  $k = k - 1$
- 13- If  $k \neq 0$  then go to step 2, otherwise go to 5.

Step 5:

- 14- Set  $F_g = (V, E_{Tg} \cup E_{Fg})$
- 15- Remove node  $g$  from  $GW^*$ .
- 16- If  $GW^* \neq \{ \}$  then go to step 1, otherwise STOP

---

The spanning tree can be constructed once during network deployment or whenever a MR joins or leaves the network. By using spanning trees, we can first create a topological sorting between a source node and gateways and second ensure that the link on the shortest path between each other node and the selected gateway will be in the list of forwarding alternatives. Thus, in step 1 the algorithm chooses one gateway and creates a spanning tree rooted at the selected gateway. In step 2, the algorithm selects the farthest node with the

minimum node degree in the spanning tree. In step 3, all the alternatives of the selected node are added to the list of forwarding alternatives. In step 4, we remove all incoming links to the selected node from the list of forwarding alternatives; this ensures that no packet forwarded from the selected node will return to it in the future.

#### 4.4. Simulation and results

We study the performance of RLBDP by using ns-2 simulator with the module implementing multi-radio and multi-channel WMNs [85] and the simulation parameters shown in table 3. We have implemented and compared the performance of *RLBDP* using *PQ* (see section 4.3.3.1), RLBDP using *ZPQ* (see section 4.3.3.2) and various other routing schemes: MIC [48], ETX [24], BP2BG [73], nearest gateway (Nearest-G) and gateway load based metric (Load-G). RLBDP-PQ refers to RLBDP using *PQ* (see Eq. (4.15) and Eq. (4.16)) and RLBDP-ZPQ refers to RLBDP using *ZPQ* (see Eq. (4.17) and Eq. (4.18)). When nearest gateway selection scheme is used, the path with the minimum number of hops to a gateway will be selected to route traffic; when the gateway load based selection scheme is used, the path leading to the minimum loaded gateway is selected; with ETX metric, the path that minimizes the product of the ETXs (of the links composing the path) is selected; with MIC or BP2BG, the path that minimizes these metrics is selected.

Table 3. NS2 simulation setup

Simulation Parameters	Values
Network Area	1000mx1000m
MAC protocol	802.11
Link data rate	11Mbps
Frequency	9.14e+08 Hz
Traffic Type	CBR (UDP)
Network Load	1000-3000 Kbps
Packet Size	1000 bytes

The topology used for the backbone Wireless Mesh Networks consists of 16 MRs randomly placed in 1000x1000 area and 3 GWs (nodes 1, 2 and 3) as depicted in Figure 28. One channel is assigned to each interface. We use at most 4 interfaces per mesh router and we consider a multi-channel network where 11 non-overlapping (orthogonal) channels are available. The channel assignment is performed using the design model presented in [86]. For accurate evaluation, we use a realistic reception model by taking Bit Error Rate (*BER*) used in Intersil HFA3861B radio hardware [114] and the corresponding Frame Error Rate (*FER*) into consideration. We use Constant Bit-Rate traffic (CBR) based on the transport protocol UDP. Since most traffic is destined to the Internet, we assume that the traffic generated from a source node may cross several intermediate nodes (i.e., multi-hop routing) to reach the Internet through a GW. For RLBDP-ZPQ (see Eq. (4.17)) we empirically set the value of  $A$  to 100 and the learning rate  $\alpha$  (see Eq. (4.19)) to 0.1, i.e., old Q-values are given more importance for stability than newly acquired Q-values; experiments did show that this value yields best results for RLBDP-PQ and RLBDP-ZPQ.

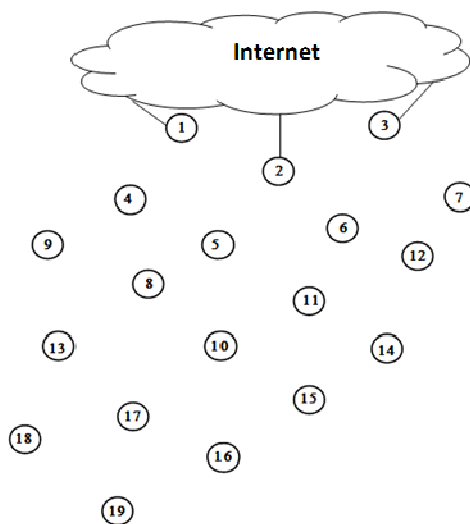


Figure 28. WMN topology used for simulations (16 MRs and 3 GWs)

The performance is evaluated in terms of the following metrics: (1) network throughput: represents the total number of bits that are correctly received by all nodes of the WMN during one second (kbps); (2) average end-to-end delay: represents the average delay for sending CBR packets from source nodes to GWs; this includes all possible delays caused by buffering during route discovery latency, queuing at the interfaces, retransmission delays at

the MAC, propagation and transfer times; and (3) packet loss ratio: represents the average number of packets dropped inside the WMN over the number of packets that are sent. The parameters  $\beta$  in Eq. (4.13) has been set empirically to 0.5 and all the simulations results are obtained after 100 runs.

In the first set of simulations, we study the performance of RLBDR-PQ, RLBDR-ZPQ and the other metrics when increasing data rate (Figure 29). We observe clearly that RLBDR-PQ and RLBDR-ZPQ perform better than MIC, ETX, NEAREST-G, BP2BG and LOAD-G. In fact, at low data rate (1000 kbps), the delay performance is better than the above metrics by around 49%, 64%, 64% and 63%, respectively. At high data rate (3000 kbps), RLBDR-PQ and RLBDR-ZPQ delay performance is better than the other metrics by around 29%, 46%, 37%, 27% and 44%, respectively. RLBDR-PQ and RLBDR-ZPQ provide almost the same performance especially at low data rate.

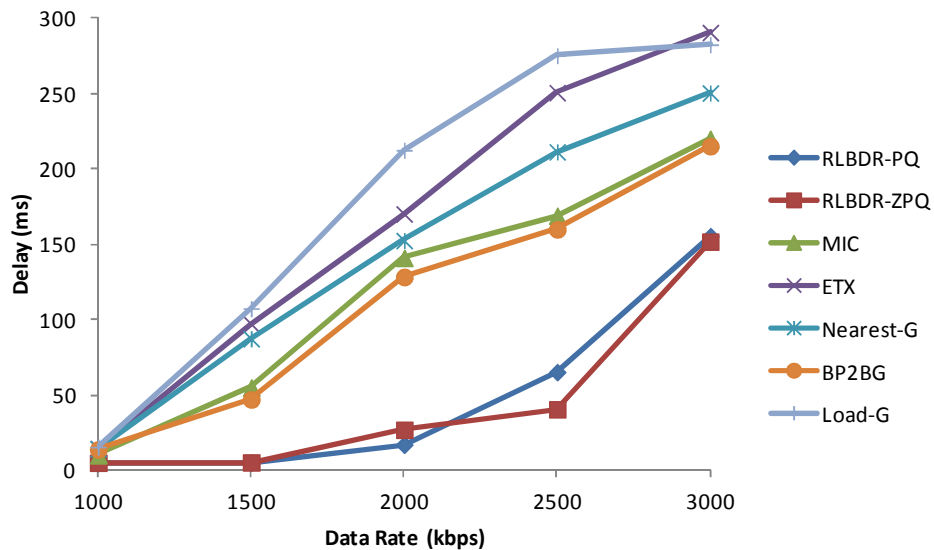


Figure 29. Delay vs. data rate

Similar behavior can be observed in Figure 30 that shows the mean end-to-end delay over all loads (i.e., 1000, 1500, 2000, 2500 and 3000 kbps). The improvement provided by RLBDR-PQ and RLBDR-ZPQ in terms of end-to-end delay is due to their choice of paths. For the other metrics (i.e., MIC, ETX, Nearest-G, BP2BG and Load-G) the routes used to reach gateways are often of poor quality in terms of interferences and capacity. Therefore, routes quickly become congested causing bigger end-to-end delay.

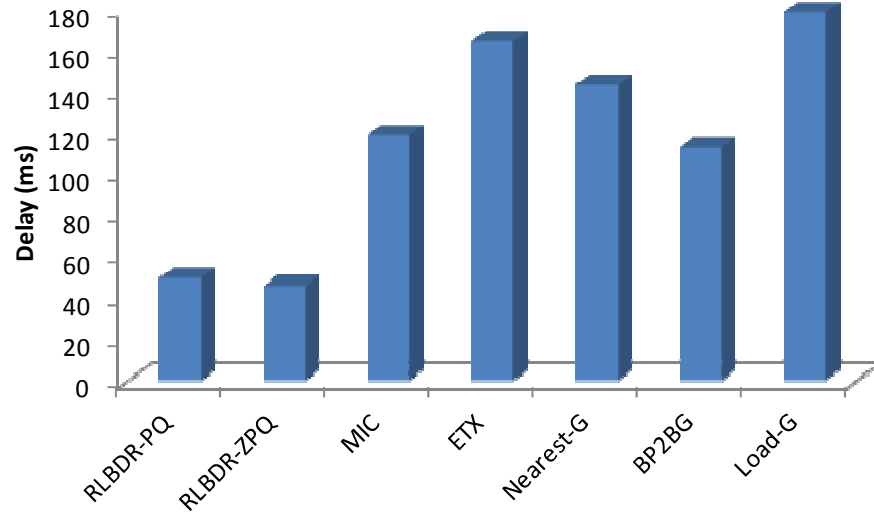


Figure 30. Mean delay vs. schemes

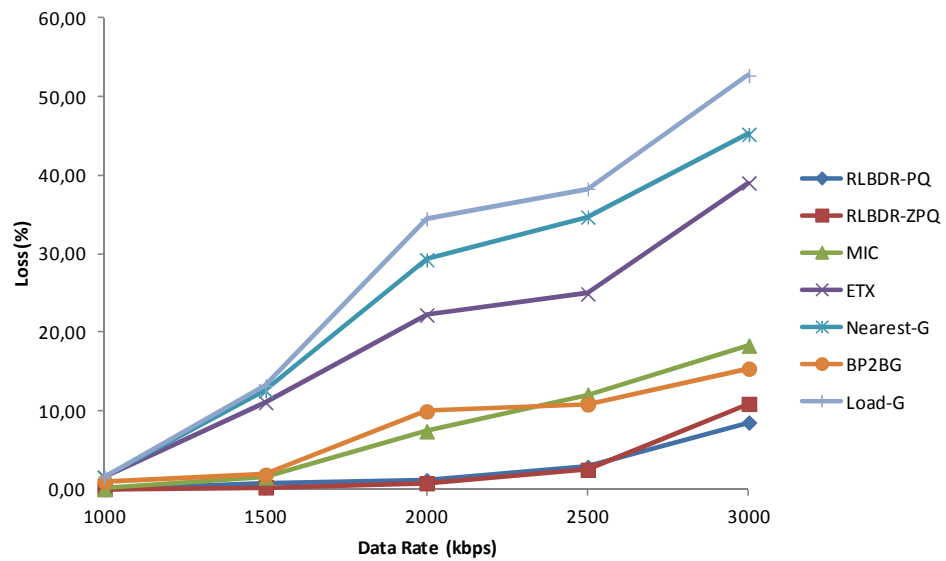


Figure 31 Loss vs. data rate

In the second set of simulations, we study the impact of data rate variation on the packet loss ratio. In Figure 31 we observe that RLBDR-PQ, RLBDR-ZPQ, MIC and BP2BG perform better than ETX, Nearest-G and Load-G. Indeed, at 1500 kbps, *RLBDR-PQ* and *RLBDR-ZPQ* are around 91% better than ETX, Nearest-G and Load-G. But starting from a

data rate of 2000 kbps, RLBDR-PQ and RLBDR-ZPQ perform better than MIC and BP2BG. More specifically, for high data rates (e.g., 3000 kbps) RLBDR-PQ outperforms MIC, ETX, Nearest-G, BP2BG and Load-G schemes by 53%, 78%, 80%, 44% and 83%, respectively (versus 41%, 72%, 76%, 29% and 79% respectively for RLBDR-ZPQ). This improvement is due to the use of the learning technique and the combination of factors (i.e., interferences, congestion level and load at gateways) that play a key role in the wireless network performance.

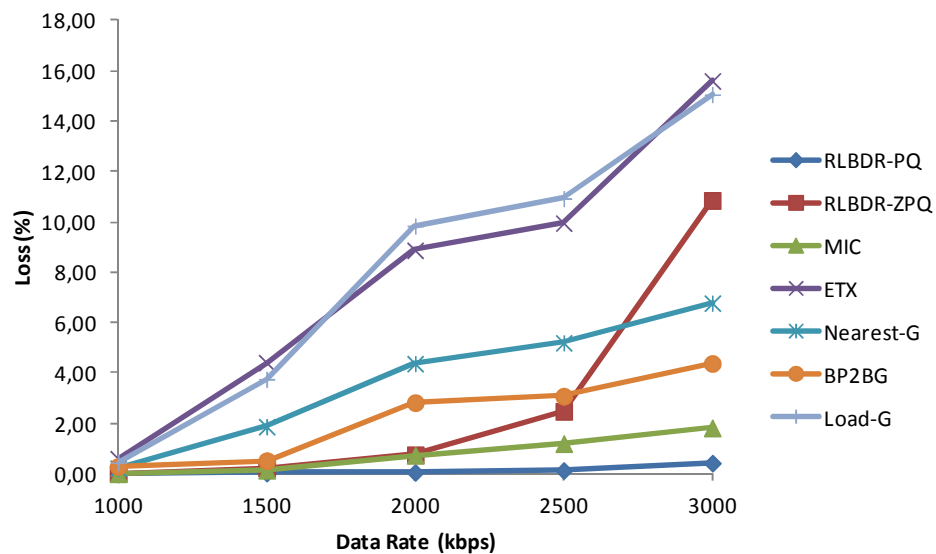


Figure 32. Loss due to collision in WMN

Interferences represent a key source of performance degradation; indeed, they cause packet loss. In Figure 32, we measure packet loss ratio due to collisions/interferences when varying data rate. We observe that for low data rates (e.g., 1500 kbps) RLBDR, MIC and BP2BG provide better performance than ETX, Nearest-G, Load-G. But for high data rates (e.g., starting from a data rate of 2500 kbps) RLBDR-PQ outperforms MIC, RLBDR-ZPQ and BP2BG, This can be explained by the fact that RLBDR-PQ reacts better to interferences than RLBDR-ZPQ, BP2BG and MIC. Figure 32 shows that Load-G and ETX are the worst in terms of packet loss; this is expected since they don't take into account interferences as a routing metric.

Figure 33 shows the variation of packet loss ratio, due to Interface Queue (*IFQ*) overflow, when increasing data rate. We observe that RLBDR-PQ, RLBDR-ZPQ and BP2BG



perform better than ETX (starting from 2000 kbps), MIC, Nearest-G and Load-G. This can be explained by the fact that RLBDR-PQ, RLBDR-ZPQ and BP2BG take into consideration both the congestion level at intermediate nodes and load at gateways.

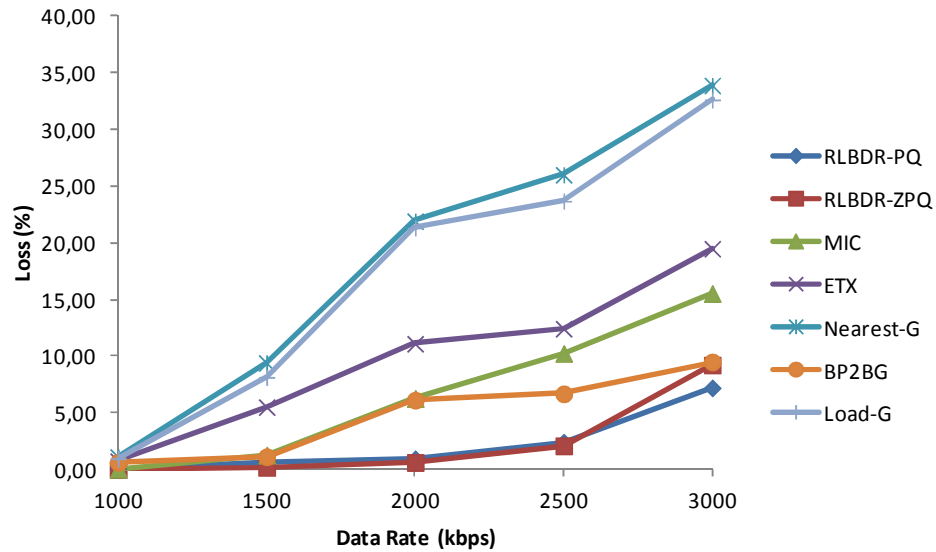


Figure 33. Loss due to IFQ

*IFQ* generally limits the maximum number of packets to be transmitted and establishes a maximum timeout policy for those packets. Any packet that exceeds this maximum timeout will be dropped. Also, packets arriving when the queue is full are systematically dropped. It is clear that by increasing *IFQ* size, we can maintain high network utilization with large queuing delay; this will impact negatively delay sensitive applications. Thus, a tradeoff between *IFQ* size and acceptable end-to-end delay is needed.

In the third set of simulations, we study the impact of data rate variation on the throughput. Figure 34 shows that RLBDR-PQ, RLBDR-ZPQ, outperform MIC, BP2BG, ETX, NEAREST-G and LOAD-G at high data rates. For example, at 3000 kbps. *RLBDR-PQ* and *RLBDR-ZPQ*, outperform MIC, BP2BG, ETX, Nearest-G and Load-G by 11%, 7%, 33%, 40% and 48% respectively. Also, at low data rates (i.e. 1500 kbps) RLBDR-PQ, RLBDR-ZPQ, MIC and BP2BG outperform ETX, Nearest-G and Load-G by around 11%.

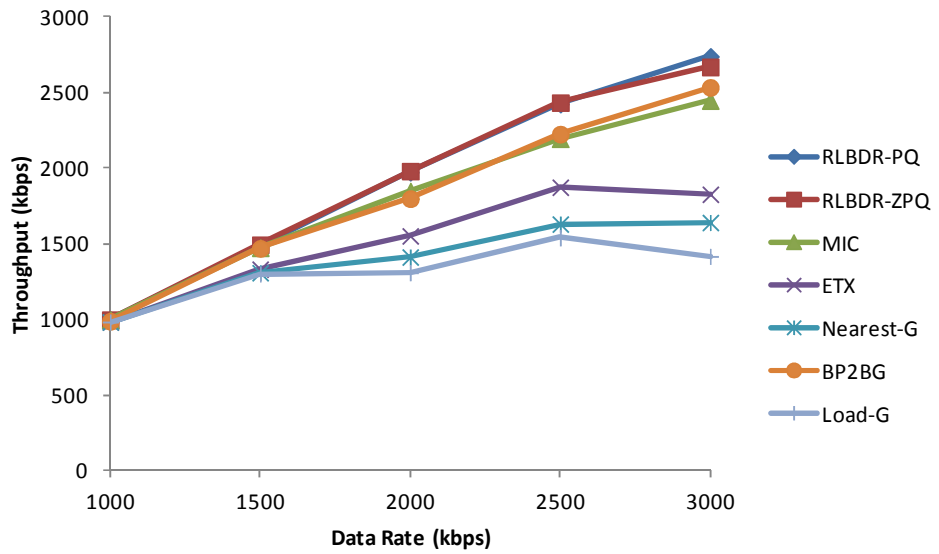


Figure 34. Network throughput vs. data rate

In the fourth set of simulations, we analyze the impact of the critical zone size on the network performance. We refer to N-hop by the number of hops (N) at most from the gateway as seen in Eq. (4.17).

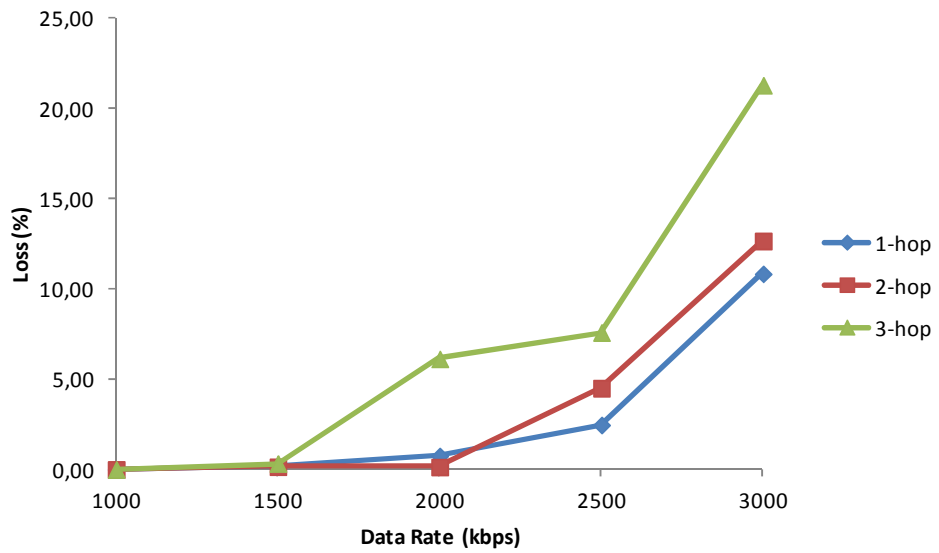


Figure35. Loss vs. data rate for different N-hops

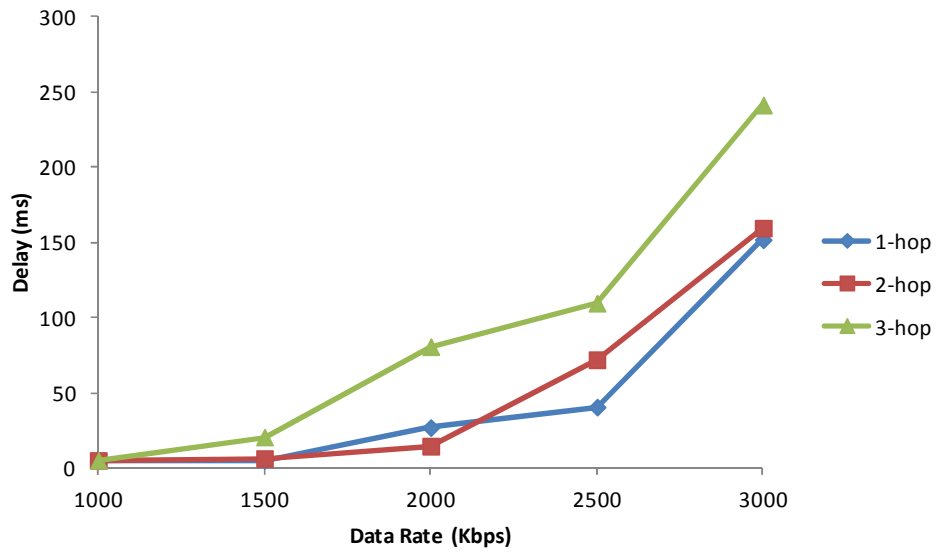


Figure 36. Delay vs. data rate for different N-hops

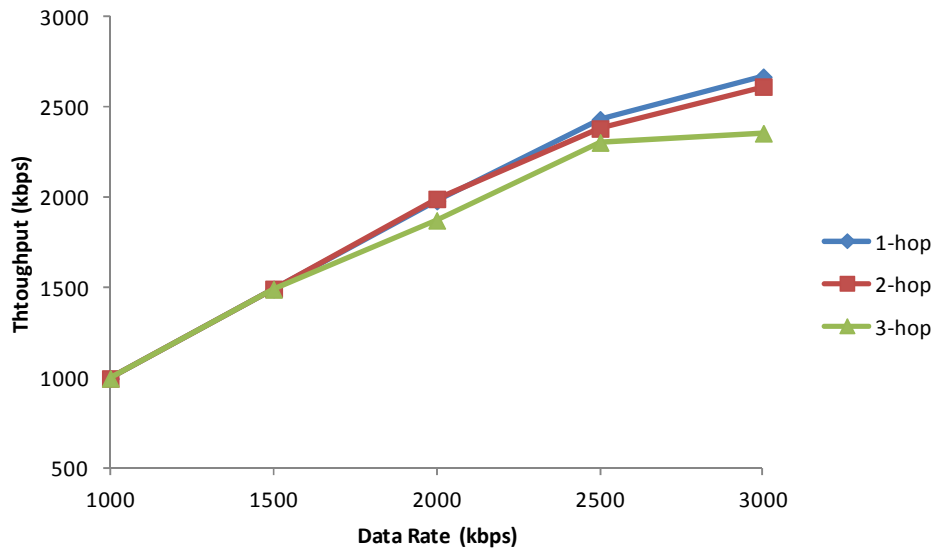


Figure 37. Network throughput vs. data rate for different N-hops

As shown in Figure 35, Figure 36 and Figure 37, the number of hops at most from gateways has an impact on the performance of RLBDR-ZPQ. Starting from a data rate of 2000 kbps, Figure 35 shows that using 1-hop for the critical zone yields better performance than using 2-hop and 3-hop in terms of packet loss ratio. For high data rates (i.e., 3000 kbps) 1-hop outperforms 2-hop and 3-hop by 14% and 49% respectively (which is nearly the same at low

data rates). Figure 36 shows that at low data rates (1000, 1500 and 2000 kbps), there is a slight delay performance improvement when using 2-hop compared to using 1-hop and 3-hop. Whereas, at high data rates (i.e. 2500 kbps) using 1-hop is better than using 2-hop and 3-hop by 43% and 62% respectively. For throughput, see Figure 37, 1-hop outperforms 2-hop and 3-hop by 3% and 11% at high data rates respectively.

Thus, we conclude that it is preferable to use 1-hop instead of 2-hop or 3-hop to construct the critical zone used by *RLBDR-ZPQ*. Indeed, when using 2-hop or 3-hop for the critical zone, the detour for an in the alternative path (in case the route break) may be significant; this increases delay and the risk of packet losses and interferences.

## 4.5. Conclusion

In this paper, we investigated the impact of using routing metrics to select paths and/or gateways in multi-channel backbone WMNs. After identifying the shortcomings of existing routing and gateway selection metrics, we proposed a new routing protocol, called *RLBDR* (Reinforcement Learning-based Distributed Routing, that adaptively learns an optimal routing policy.

We proposed two versions of *RLBDR* (1) *RLBDR-PQ*: it penalizes links with bad quality as we get closer to the gateway; and (2) *RLBDR-ZPQ*: it gives more importance/weight to nodes in the neighborhood of the gateway (N-hops away from the gateway) to help reducing interferences around the gateway and improving packet delivery. For both schemes we use the load at gateways to select best gateway and reinforcement learning to select the next hop towards the gateway. Simulation results did show that *RLBDR-PQ* and *RLBDR-ZPQ* outperform existing schemes in terms of loss ratio, end-to-end delay and throughput.

## Acknowledgment

We would like to thank Mr Vinicius da Cunha Martins Borges [41] for providing us with code for simulation. The research reported in this manuscript has been supported in part by Natural Sciences and Engineering Research Council of Canada (NSERC) and Bell Canada.

## **Chapitre 5:**

# **Node Stability-Based Routing in Wireless Mesh Networks**

Mustapha Boushaba, Abdelhakim Hafid, Michel Gendreau

### **Abstract**

Network stability is a key performance metric in supporting real time communication over wireless networks. Because of high bandwidth demand and dynamic traffic variation, several paths in Wireless Mesh Networks (WMNs) are expected to be unstable. High levels of network instability can lead to interferences, packet losses and high delays.

In this paper, we address the stability problem of WMNs; instability in these networks is caused mainly by link quality fluctuations and frequent route flapping. Indeed, most routing protocols try to optimize a routing metric locally or globally without considering network stability. First, we present the key factors that may cause network instability; then, we propose a new technique, called Node Stability-based Routing (NSR), using the entropy function (known as a measure of the uncertainty and the disorder in a system) to define a node stability and a probability function to select an appropriate gateway. Simulation results show that NSR can significantly improve the overall network performance compared to schemes using interference and channel switching (MIC), Expected Transmission count (ETX) or load at gateways as a routing metric, Reinforcement learning-based best path to best gateway (RLBDR), and nearest gateway (i.e., shortest path to gateway).

**Categories and Subject Descriptors:** C.2.2 [Computer-Communication Networks]: Network Protocols

**General Terms:** Algorithms, Interferences, Stability

**Additional Key Words and Phrases,** Multi-channel, Routing, Wireless Mesh Networks

## 5.1. Introduction

In the last several years, wireless communication has emerged as promising technology for next-generation networks. Among those networks, Wireless Mesh Networks (WMNs) [4] have become quite popular allowing communication to the Internet, anytime and anywhere. WMNs have the potential to eliminate cables and thus dramatically reduce installation and maintenance costs and improve adaptability, flexibility and scalability.

A WMN can be seen as a multi-hop Mobile Ad-hoc Network (MANET) with extended connectivity; the key difference is that WMNs are characterized by a relatively static architecture and low mobility. WMNs combine wired and wireless networks with wireless Mesh Routers (MRs) as backbone and mobile stations as users. The role of MRs is to relay information from one MR to another via multi-hop communications. Usually, MRs send traffic to a gateway (GW) that connects nodes to the Internet. In the case of a WMN with a single gateway, the gateway selection problem becomes simple; indeed, all upstream/downstream traffic flows traverse the same GW to the Internet; thus, the GW is more likely to become the bottleneck/single point of failure in the network [27]. To mitigate this problem, multiple gateways are installed to distribute load and improve performance. However, increasing the number of GWs does not necessarily increase the capacity of WMNs. Indeed, network capacity is closely related to the network connectivity and the placement of GWs; these issues are out of scope of this paper.

WMN performance is highly impacted by interferences and (GW) congestion causing considerable packet losses and higher delays. To improve WMN performance, many schemes using directional and smart antennas [18], multiple input multiple output (MIMO) systems [19, 20], and multiple radios and multiples channels [21; 22] have been proposed. Particularly, routing schemes can play a major role impacting (positively or negatively) the network performance; indeed, the main goal of routing is to find better routes, according to specific routing metrics, from sources to destinations. To achieve a good network performance, a routing metric should (a) not impact negatively the network stability; (b) capture the characteristics of mesh networks; (c) compute paths in polynomial time; and (d) avoid forwarding loops [48]. Network stability is considered one of the most determinant network

performance metrics which has not been considered by most routing protocols. Network instability occurs whenever the frequency of rerouting increases considerably; this increase is generally caused by one or more links that exhibit considerable quality fluctuations.

Many applications (e.g., multimedia applications) require a stable wireless mesh network for acceptable quality. Indeed, instability (frequent route flapping) may cause out of order delivery, high jitter, packet losses and/or high delays which are unacceptable for multimedia applications. For better understanding, let us consider the network configuration shown in Figure 38 where nodes  $R1$ ,  $R2$ ,  $R3$ ,  $R4$ ,  $R5$  and  $R6$  are MRs, nodes  $R1$  and  $R2$  are source routers optionally equipped with traffic aggregation devices and nodes  $G1$  and  $G2$  are gateways. In this example, we consider delay as a routing metric; thus, traffic from  $R1$  to  $G1$  follows the path  $R1-R4-G1$ . Now, let us assume that the estimated value of the metrics of links ( $R6-G1$ ) and ( $R3-R6$ ) change to 0.5 ms; thus, the delay to send packets from  $R3$  to  $G1$  through  $R6$  is now 1 ms; in this case, the routing protocol selects the path  $R1-R3-R6-G1$  to send traffic from  $R1$  to  $G1$ . Hence, some packets (of the same flow) rerouted on  $R1-R3-R6-G1$  will reach their destination  $d$  in the Internet before the packets already transmitted on  $R1-R4-G1$ ; consequently, many packets may be out-of-order at the destination  $d$  [115]. The problem becomes very critical when the route flapping is consistent. The destination will be overloaded with handling the out-of-order packets and therefore delay and jitter will increase making the quality of some multimedia applications, such as video-conferencing, unacceptable.

Wireless Mesh Networks rely on routing protocols to find optimal paths. Generally, these protocols do not consider the instability of the network which may occur when the volume of traffic and demand for wireless capacity increase. Unlike wired links, wireless links often have frequent bandwidth fluctuations; factors, such as interference, fading and shadowing impact considerably the state of the link. Therefore, they increase the possibility of route breaks, during data transmission, which impact the network stability. In WMNs, generally multiple users intend to communicate to the Internet through gateways. Since the transmission coverage of wireless communication is limited, traffic need to be forwarded in multi-hop manner to gateways (generally, WMNs consist of many MRs and only one or a few gateways). This architecture (many-to-one and hop-by-hop network) makes the gateway a

bottleneck and causes a kind of congestion, called funneling effect [133, 134], near the gateway and thus influences delay and reliability

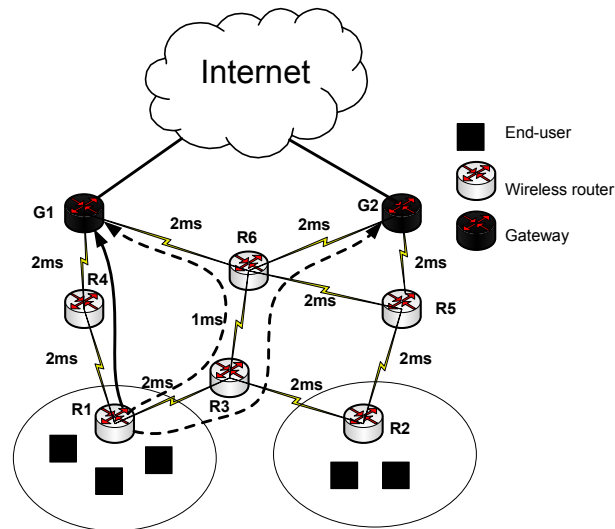


Figure 38. Route flap scenario

This paper extends our contribution in [28] and proposes a new routing scheme, in WMNs, that takes into account network stability; indeed, the objective of the proposed scheme is not to impact negatively the network stability. The key contribution of the paper is the definition of a novel routing metric, called *Node Stability*, that quantifies the stability of Mesh routers. Using NSR, upon receipt of a packet, a MR selects a most stable mesh router as the next hop, towards a selected gateway. Simulations show that our proposed Node Stability-based routing outperforms existing routing protocols.

The remainder of the paper is organized as follows. In Section 5.2, we present related work. Section 5.3 presents some factors leading to instable networks. Section 5.4 presents the entropy function and its usefulness. In Section 5.5, we present the details of the proposed Node Stability-based Routing scheme. Section 5.6 evaluates the performance of our proposal. Section 5.7 concludes the paper and presents future work.

## 5.2. Related work

Many routing schemes have been proposed in the literature for WMNs [49, 88]. These schemes could be roughly divided into three categories: (1) proactive routing protocols (e.g.,



Optimized Link State Routing OLSR [60]); (2) reactive routing protocols (e.g., Ad hoc On-demand Distance Vector AODV [58]); and (3) hybrid protocols (e.g., Temporally-ordered routing algorithm TORA [62]). Based on the aforementioned routing techniques, several routing metrics have emerged. In general, a routing metric is used, by a routing protocol, to select a path having the highest throughput, the lowest delay and/or the lowest packet loss ratio. However, most routing protocols do not take into consideration network stability. We believe that network stability has a considerable impact on network performance; indeed, a stable network outperforms an instable network.

Stability is hard to define; it has been used in different domains and networks to indicate a state or quality of the system under consideration. In the open literature, several contributions [65, 66, 67, 68, 69, 70, 116] have been made to study stability in ATM networks, wireless sensor networks and wired networks, however, few in WMNs. Li et al. [67], in the context of ATM networks, stated that a network is stable if and only if all packets experience a bounded delay. More specifically, they compute the upper delay bounds (of a cell/packet) per server; then, they compute the end-to-end delay of a connection as the sum of the upper delay bounds of servers (ATM switches) used by the connection. The end-to-end delay (of all packets) should be below a threshold to consider the network stable.

Gaertner et al. [68], in the context of MANETS, define a stable link as a link where at least a percentage  $p$  of packets are received in a time period  $T_s$ . They choose  $T_s$  to be (a) small enough to reflect rapid changes in link states; and (b) large enough to tolerate some effects of fading and to prevent unnecessary route discoveries; they choose  $p$  to be (a) small enough to meet the link quality requirements; and (b) large enough to tolerate fast signal fading.

Routing, service and resource discovery capabilities are needed to enable applications and services over large scale WMNs. In this context, Aydin et al.[69] propose a layered architecture to autonomously select a set of backbone nodes to create a quorum system. They propose an algorithm called ADB that consists of three components (a) neighbor discovery; (b) backbone selection; and (c) backbone connection. ADB explores stability information, maintained by each mesh node, that consists of two metrics: (1) *nodeStability*, is the estimated stability of the area surrounding a node. It consists of a set of probabilities (the cardinality of this set is equal to the number of the node's neighbors); an element of this set represents an

approximation of the probability  $P_i$  that a link from the node (let us denote it by  $node_i$ ) to its neighbor will not break within the next predefined time window; and (2) *pathStability*: is the estimated path stability from the node (denoted by  $node_i$ ) to its current backbone. This metric measures the probability that a path will still exist within the next time window; it is computed as follows:  $pathStability_i = pathStability_{(parent\ of\ i)} * P_i$ .

For Ad-hoc networks [65, 66], Associativity-Based Routing (ABR) [66] is considered as one of the earliest contributions whose fundamental objective is to find longer-lived routes. Periodically, each node broadcasts a hello message to signify its existence and to compute the lifetime of links even if there is no traffic to send. ABR tries to choose stable links over transient links; a link between two neighboring nodes is defined as stable if one node continuously receives signals from its neighboring node and the number of hello messages exceeds a threshold. Otherwise, the link is unstable. Thus, the shortest and stable route is selected as the optimal route by the destination. Signal Stability Adaptive Routing (SSA) [65] estimates link stability based on signal strength. Each mobile node measures the signal strength to its neighbors. The authors distinguish between strongly connected links and weakly connected links; a link is considered to be strongly connected if the signal strength exceeds a certain predefined threshold; this is typically the case when two nodes are close to each other. Thus, the authors define a stable link as the link which exhibits the strongest signal for the maximum amount of time. SSA tries to find a path using only stable links; however, if no stable path is found, the protocol tries to find a path by using all possible links.

Ramachandran et al. [70] reported, after experiments on UCSB Meshnet [71] and MIT Roofnet [5], that the main reason of network instability is the fluctuating quality of links caused by the effect of multipath fading, interference and weather conditions. Their analysis of routing stability is based on link quality information and uses three route-level characteristics [70]: (1) *prevalence*: represents the probability or the number of times that a path has been met in the past; (2) *persistence*: represents the probability that a route remains unchanged over a long time period; and (3) *route flapping*: represents the variation of the paths during a time period. Their findings can be summarized as follows: (1) By analyzing the persistence and prevalence, the authors found that routes in wireless mesh networks are inherently unstable; indeed, they are weakly dominated by a single route; and (2) a routing protocol that always

flaps routes will likely achieve only minimal gains (i.e., marginal improvement in throughput) in a large number of instances.

In order to improve the routing stability, the authors recommend to use a route flap dampening, such as using a route which offers 10% throughput improvement over the old one or using an alternate route which is consistently stable for a specified amount of time.

### **5.3. Factors leading to instable networks**

High levels of network instability can lead to packet losses and increase network latency. There are several factors that lead to network instability; these factors include: (1) Interferences: they are one of the major factors that impact network performance by creating instability. In wireless networks, channels are shared among nodes; thus, when nodes, sharing the same channel, transmit at the same time, they can cause inter-flow interferences and intra-flow interferences; (2) Routing protocols: particularly, in link-state protocols, the inappropriate number of advertisement messages to update routes may consume an excessive amount of resources in the network and cause route flaps. Consequently, it degrades performance and creates an instable network; (3) Network topology and traffic patterns: they have an impact on the behavior of routing and thus network stability. In particular, the shortest path routing protocol, which has seen enormous success in wired networks, is inadequate in WMNs. In fact, shortest path routing, using congestion as the link cost, is very prone to instability under heavy loads and bursty traffic; (4) Congestion: it is the result of MAC queue buildup at intermediate nodes; it can be observed by a forwarding node when packets arrival rate is bigger than its forwarding rate. There are many factors that contribute to congestion, namely network topology, number of flows, traffic characteristics of the flows and their routes, as well as channel capacity and the available transmission rate at the physical layer. The presence of congestion in the network impacts the network throughput, causes peer failures in routers and leads to routing failures and thus network instability; (5) route flapping: it occurs when a MR alternately advertises a destination network first via one route then via another (e.g., unavailable route and then available again). This phenomenon is undesirable in WMNs; it often forces MR to compute a new preferred route to a destination which causes network delay and requires extra CPU cycles. Whenever Route Flapping occurs, it causes

unnecessary delay in packets forwarding; and (6) Effects of exploration: One of the major difficulties in the development of reinforcement learning algorithms is managing the trade-off between the execution of the best known policy, the exploitation and the exploration. In a multi-agent environment, exploration can contribute to instability since the agents switch their respective actions from time to time. The problem is even greater when the number of nodes that contribute to exploration is high.

## 5.4. Entropy utility

Entropy was first introduced in [117] as a thermodynamic property; it measures the reversible change in thermal energy concerning the absolute temperature. It was also defined by Boltzmann [118] in statistical mechanics as a combination of microstates statistic entropy to characterize the order and the self-organization of a system. Later, Shannon and Weaver [119] defined information entropy; it is used to quantify the uncertainty of the information and to quantify the capacity of a transmission channel.

Several contributions [120, 121, 122, 123, 124, 125, 126, 127, 128] extended/adapted these definitions in different domains. Lu et al. [120] apply the notion of entropy to ad hoc wireless networks; they use it to quantify the internal organization state generated by different self-organization schemes. This organization exhibits two levels: (1) microscopic level (based on logic links between nodes) and (2) macroscopic level (formation of flexible structure). The authors make use of entropy because (a) wireless networks and thermal dynamic systems are similar in terms of organization; (b) it describes the degree of order in the network; and (c) it exhibits the behavior of self-organization protocols compared to changes of inherent parameters in the network, such as link and node reliability. The authors define the entropy of a link as  $-p(u, v) \log(p(u, v))$ , where  $p(u, v)$  is the probability that a link exists between nodes  $u$  and  $v$ ; the entropy of the network is then defined as the sum of the entropies of its links.

Sneppen et al. [121] define two entropies, namely road entropy and target entropy. The road entropy quantifies the predictability or the order/disorder of traffic around a node whereas the target entropy measures the predictability of traffic to a specified node. To improve the network performance, the authors propose a fast and accurate technique to

classify connection types [122]; they classify the type of an access link into Ethernet, wireless LAN and low-bandwidth wired connection by using the median and the entropy of packet-pair inter-arrival times (i.e., inter-arrival times between back-to-back packets that travel from source to destination). The rationale behind their use of entropy instead of variance is that entropy is much better in capturing the randomness of a random variable than variance.

In the context of wireless sensor networks and MANET, a number of contributions propose to use entropy to determine stability of paths. Chen et al. [123] propose EQMGA algorithm to construct a new metric-entropy in order to select long-life paths; the goal is to reduce, via the use of entropy, the number of route reconstructions (i.e., rerouting) to provide QoS guarantees. An et al. [124] propose an Entropy-based Routing Protocol using Mobility (ERPM) in Mobile Ad-hoc Wireless Sensor Networks; the objective of ERPM is to select the most stable route between any source and destination based on mobility of sensor nodes to increase the route lifetime. Gui et al. [125] propose an Entropy-based Long-life Multipath Routing algorithm in MANET; the algorithm, via the use of entropy, provides an accurate estimation of routing stability; Lian et al. [126] propose a QoS-Aware routing protocol for MANETs. The objective is to compute stable routes, based on entropy, that satisfy bandwidth constraints and optimize delay and jitter.

## **5.5. Proposal description**

One of the key symptoms of network instability is the disappearance and the reappearance of routes in the routing table in an intermittent manner. Thus, the number of these disappearances/reappearances of routes may characterize the intensity of the perturbation in the network.

### **5.5.1. Network Model and assumptions**

We consider multi-hop infrastructure WMNs with two sets of nodes: MRs and GWs. MRs form a multi-hop wireless backbone to relay traffic between users and Internet. To reach the Internet, traffic passes through GWs which are MRs with more functionality (e.g., more buffer size and wired and wireless interfaces). Each MR may be equipped with multiple wireless interfaces and multiple channels on each interface. We assume that the interfaces of a

MR are assigned different channels. We formally model the backbone WMN as a graph  $G=(V, E)$  where  $V$  is the set of nodes (MRs and GWs) and  $E$  is the set of links. Let  $l_{ij}$  denotes the link between two MRs  $v_i$  and  $v_j$  ( $v_i, v_j \in V$ ). In  $V$ , there are GWs that provide connectivity to Internet. We define the load  $L_g[t]$ , of gateway  $g$ , at time  $t$  as the average interface queue length [20, 21]. It can be measured by monitoring the size of packets buffered in the GW interface over a time period. The current load  $L_g[t]$ , at time  $t$ , is based on the previous estimated load  $L_g[t-1]$  and the volume of traffic  $V[t]$  that gateway  $g$  has processed during the last time period  $[t-1, t]$ :

$$L_g[t] = \alpha \frac{V[t]}{C_g} + (1-\alpha)L_g[t-1] \quad (5.1)$$

where  $\alpha \in [0, 1]$  and  $C_g$  is the maximum queue length of gateway  $g$ .

We assume that each node  $v_i$  maintains routing table  $RT_i$  that stores routing information to each destination  $d$ ;  $|RT_i| = N$  is the size of  $RT_i$ . For MR  $v_i$  ( $i = 1, 2, \dots, |V|$  and  $v_i \in V$ ), we denote by  $RT_i^t$  its routing table at time  $t$ . Each entry in  $RT_i^t$  includes  $\{d, (f_1, f_2, \dots, f_n), k_{ij}, v_j\}$  where  $n > 0, j \neq i, k_{ij}$  is the channel used on link  $l_{ij} \in E, v_j$  is next hop towards destination  $d$ , and  $f_1 \dots f_n$  represent the characteristics (e.g., Interference Ratio and Loss Ratio) of  $l_{ij}$  when using  $k_{ij}$ . For each incoming packet,  $v_i$  uses the information stored in its routing table  $RT_i^t$  to assign the outgoing link to be used to forward the packet towards its destination.

Let us define  $RT_i^{t+1}$  as the routing table at time  $t+1$  of node  $v_i$ .  $RT_i^{t+1}$  is a combination of three sub routing tables: (1)  $r_{nc}^t$ : contains links that experience no changes between  $t$  and  $t+1$ ; (2)  $r_c^{t+1}$ : contains links at time  $t$  that experience some changes at time  $t+1$  (this change may be an improvement or a degradation of the quality of the link); and (3)  $r_n^{t+1}$ : contains new links observed at time  $t+1$  that were not present at time  $t$ .

$$RT_i^{t+1} = r_{nc}^t + r_c^{t+1} + r_n^{t+1} \quad (5.2)$$

## 5.5.2. Link Quality Metric and Node stability

### 5.5.2.1. Link Quality Metric ( $LQM_l$ )

$LQM_l$  is considered as one of the link characteristics stored in the routing table. According to [26]  $LQM_l$  is defined as a weighted function of two parameters: IR (Interference Ratio) and CL (Congestion Level). IR estimates the interference level in the network through the Signal to Noise Ratio (SNR) and the Signal to Interference-plus-Noise Ratio (SINR). IR for a node  $u$  on link  $l$  ( $u$  and  $v$  are the ends of link  $l$  operating on the same channel  $i$ ) is defined as follows:

$$IR_l(u) = \frac{SINR_l(u)}{SNR_l(u)} \quad (5.3)$$

where  $SINR_l(u)$  and  $SNR_l(u)$  are defined in Eq. (5.4) and Eq. (5.5):

$$SINR_l(u) = \frac{P_l}{Noise + \sum_{w \in N_{l-v}} \tau_w \cdot P_u(w)} \quad (5.4)$$

$$SNR_l(u) = \frac{P_i}{Noise} \quad (5.5)$$

where,  $P_l$  is the signal strength,  $N_l$  is the set of nodes from which node  $u$  can hear a packet that interferes with link  $l$  and  $\tau_w$  gives the amount of time that node  $w$  occupies the channel.

CL is closely related to link utilization ( $U(l, t)$ ) during time period  $t$ .  $U(l, t)$  is defined as follows:

$$U(l, t) = \frac{\sum_{i \in Succ(l, t)} Size_i}{BW_l} \quad (5.6)$$

where,  $Succ(l, t)$  denotes the set of packets that have successfully traversed link  $l$  during period time  $t$  and  $Size_i$  denotes the size of packet  $i$  ( $i \in Succ(l, t)$ ).

Thus, by using the moving average, we define CL as follows:

$$CL(l, t) = \beta U(l, t) + (1 - \beta) CL(l, t - 1) \quad (5.7)$$

where  $\beta \in [0, 1]$

By grouping IR and CL, LQMI for link  $l$  operating on channel  $i$  is defined as follows:

$$LQM_l = \left(1 - \left(\frac{1}{2}\right)^n\right) \times IR_l + \left(\frac{1}{2}\right)^n \times CL_l \quad (5.8)$$

where,  $n$  is the number of  $l$ -hop neighboring nodes that share channel  $i$  (number of interfering nodes) with the node computing its  $LQM_l$ .

### 5.5.2.2. Node stability-based routing

Before defining the stability of a node let us discuss the stability index which we associate to a link in a routing table. The stability index of a link is computed using the link quality history including the current quality; a link is said to be acceptable (resp. unacceptable) when its  $LQM_l$  is smaller (resp. bigger) than a predefined threshold. It is clear that a link that changes frequently between acceptable and unacceptable will not be chosen to route packets; indeed, these changes will create oscillations in the network causing its instability.

We propose an algorithm, called Stability Index Algorithm (SIA), that computes link stability index using link oscillations between acceptable and unacceptable, link persistence, and link quality improvement/deterioration. In the following, we present the pseudo-code of the algorithm used to compute the stability index ( $S_l^{t+1}$ ) of link  $l$  at time  $t+1$ . SIA is executed by each node (mesh router)  $i \in V$ .

Algorithm 1: Stability Index Algorithm (SIA)

---

#### Variables

$l$ : link

$(LQM_l)^t$ : Link quality of  $l$  measured at time  $t$

$(LQM_l)^{t+1}$ : Link quality of  $l$  measured at time  $t+1$

$S_l^t$ : Stability index of link  $l$  at time  $t$

$S_l^{t+1}$ : Stability index of link  $l$  at time  $t+1$



$\varepsilon$ : Predefined threshold.

$\beta$ : is a constant belonging to [0,1]

---

### Algorithm

```
1- For (each  $l \in RT_i^{t+1}$ ) do
2-   if ( $l \notin RT_i^t$ ) /* new link*/
3-     if ( $(LQM_l)^{t+1} < \varepsilon$ ) /*accepted link*/
4-        $S_l^{t+1} \leftarrow 1$ 
5-     else
6-        $S_l^{t+1} \leftarrow 0$ 
7-     end if
8-   else /* the link already exists*/
9-     if ( $|(LQM_l)^{t+1} - (LQM_l)^t| \leq \beta$ ) /* the link quality has not changed*/
10-       $S_l^{t+1} \leftarrow S_l^t + 1$ 
11-    else /* the link quality has changed*/
12-      if ( $(LQM_l)^{t+1} < (LQM_l)^t$ ) /* the link quality has improved*/
13-         $S_l^{t+1} \leftarrow S_l^t + 2$ 
14-      else /*the link quality worsened and  $(LQM_l)^{t+1} > (LQM_l)^t$  */
15-        if ( $(LQM_l)^{t+1} < \varepsilon$ )
16-           $S_l^{t+1} \leftarrow S_l^t / 2$ 
17-        else
18-           $S_l^{t+1} \leftarrow 0$ 
19-        endif
20-      endif
21-    endif
22-  endif
23- end for
```

---

The algorithm starts by adding acceptable or unacceptable links (link quality bigger or smaller than a predefined threshold) in the routing table. Even if a link is unacceptable, it will

be added in the routing table with a stability index equal to 0 (an acceptable link is added with stability index equal to 1) which corresponds to line 6 (vs. line 4) in the algorithm. Thus, based on these values at the initialization, the routing protocol will avoid selecting newly created links ( $S_l^t = 1$ : links having no history in the past) or bad quality links ( $S_l^t = 0$ ). After each period where the link quality does not change (line 9 with a small  $\beta$  value) we increment by 1 the stability index of the link. If the link quality has improved relative to the past value, its stability index will be incremented by 2 (line 13 of the algorithm); otherwise, if the link quality has deteriorated but still acceptable ( $<\epsilon$ ) we divide its accumulated stability index by 2 (line 16); thus, if link degradation continues, its index stability will exponentially approaches zero. In the case of a link degradation above the threshold ( $\epsilon$ ), the stability index will be set to 0 (line 18).

To compute the stability of a node  $v_i$  we use (1) the stability index of the links that  $v_i$  maintains in its routing table (see SIA for details); and (2) the entropy function: a measure of the uncertainty and the disorder in a system.

Using Equation (5.10), that defines the probability of the stability of a link relative to other links (in the routing table of node  $v_i$ ) having a non-zero stability index, we define the entropy  $H_i(\Delta_t)$  at node  $v_i$  during time interval  $\Delta_t$  in Equation (5.11).

$$p_l = \frac{S_l^{t+1}}{\sum_{l \in RT_i^{t+1}} (S_l^{t+1})} \quad (5.10)$$

$$H_i(\Delta_t) = \frac{-\sum p_l \log p_l}{\log N_i} \quad (5.11)$$

where  $N_i = |RT_i^{t+1}|$  (number of entries in the routing table of  $v_i$ ). Let us note that a high value of the entropy (varies between 0 and 1) means a more stable node.

At time  $t$ , every node computes its entropy (see Equation 5.11) and broadcasts it to its  $l$ -hop neighbors. Upon receipt of this information, a node stores it in its routing table and uses it for best next hop to forward data packet to its destination. Indeed, a node will select a best path, from a set of possible paths (in its routing table) to a given destination, that has the most stable node (i.e., the node with the biggest entropy) as next hop.

### 5.5.2.3. Gateway Selection

In WMNs, traffic usually passes through gateways (GWs) to Internet. In this paper, we concentrate on selecting stable routes to a selected gateway. Thus, we need to select the most appropriate gateway to Internet; then, we determine the most stable path from a source to this gateway. Load has been used as a metric for gateway selection. [129; 79; 130; 78]; however, using exclusively load to select a gateway may considerably degrade the network performance. Indeed, if each source selects a least loaded gateway, then most of the sources will send traffic towards this gateway making it more loaded than others. These changes will cause rerouting to least loaded gateways; this process will be repeated causing major oscillations and thus network instability.

In this paper, we propose a probability-based scheme to select Gateways. Let us assume that each GW broadcasts Gateways Advertisement messages GWADV to MRs. The format of GWADV message is as follows:

idM	idG	iface	Load
-----	-----	-------	------

Figure 39. GWADV message

where  $idM$  is the  $id$  of the message,  $idG$  is the identifier of the gateway broadcasting the advertisement message GWADV, and  $iface$  is the interface whose load is measured. The load at each gateway is computed using Equation (5.1).

Once a source MR receives GWADV, it selects the gateway to Internet; the proposed selection scheme makes use of probabilities. More specifically, we compute the probability to use a given gateway (among all gateways in the network). The probability  $P_{ig}^t$  that node  $i$  selects gateway  $g$  at time  $t$ , is defined as follows:

$$P_{ig}^t = \alpha P_{ig}^{t-1} + (1-\alpha) I(g = \underset{g' \in G_i}{\operatorname{argmin}} q_{g'}^t) \quad (5.12)$$

where  $q_{g'}^t$  is the load of gateway  $g'$  (see Equation 5.1),  $I()$  is a function whose value is either 1 if  $g'$  is the least loaded gateway (LLG), otherwise 0,  $G_i$  is the set of gateways known to node  $i$  and  $\alpha$  is a tunable parameter whose value is between 0 and 1.

In order to achieve convergence, the proposed probability function needs to be initialized; we define  $P_{ig}^0$  (probability at time 0) as follows:

$$P_{ig}^0 = \frac{1/hop_g}{\sum_{g' \in G_i} 1/hop_{g'}} \quad (5.13)$$

where  $hop_g$  is the number of hops to gateway  $g$  and  $G_i$  is the set of gateways known to node  $i$ .

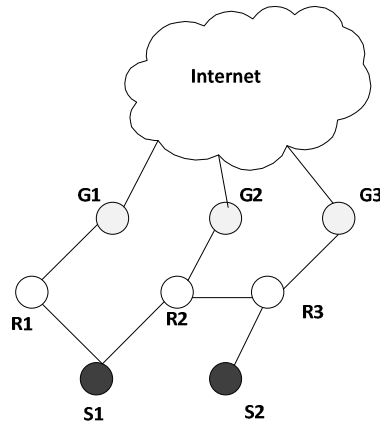


Figure 40. Gateway selection illustration

For better understanding of the selection scheme, let us consider the example shown in Figure 40. The sample WMN consists of (a) three gateways G1, G2 and G3; (2) three intermediate MRs R1, R2 and R3; and (c) two sources S1 and S2.

Let us assume that (a) periodically, each gateway sends advertisements (i.e., GWADV messages) to MRs; (b) the number of hops from S1 to G1, G2 and G3 is 2, 2, 3 respectively; and (c) for the number of hops from S2 to G1, G2 and G3 is 5, 3, 2 respectively. At the start-up, upon receipt of GWADV from gateways, S1 and S2 compute, using Equation 5.13, their probabilities to each Known gateway. The probabilities that S1 (resp. S2) selects G1, G2 and G3 are 0.37 (resp. 0.19), 0.37 (resp. 0.32) and 0.25 (resp. 0.48) respectively. If  $\alpha = 0.77$  and at  $t = 1$  G1 is the LLG (least loaded gateway), then  $I(G1) = 1$ ,  $I(G2) = 0$  and  $I(G3) = 0$ . The probabilities for S1 to select G1, G2 and G3 are (using Equation 5.12)  $P_{S1G1}^1 = 0.77 P_{S1G1}^0 +$

$0.23 * 1$ ,  $P_{S1G2}^1 = 0.77 P_{S1G1}^0 + 0.23 * 0$ , and  $P_{S1G3}^1 = 0.77 P_{S1G3}^0 + 0.23 * 0$ . Tables 4 and 5 show the probabilities to select the gateways G1, G2, and G3 by S1 and S2 respectively; the gateway with the biggest probability is selected.

Table 4: Gateway Selection by S1

Period	LLG	$P_{S1G1}^t$	$P_{S1G2}^t$	$P_{S1G3}^t$	Selected Gateway
t = 0		0,37	0,37	0,25	G1
t = 1	G1	0,51	0,28	0,19	G1
t = 2	G2	0,40	0,45	0,15	G2
t = 3	G3	0,31	0,35	0,34	G2
t = 4	G3	0,24	0,27	0,49	G3
t = 5	G2	0,18	0,44	0,38	G2
t = 6	G1	0,37	0,34	0,29	G1
t = 7	G1	0,51	0,26	0,23	G1
t = 8	G2	0,40	0,43	0,17	G2
t = 9	G2	0,30	0,56	0,13	G2

Table 5: Gateway Selection by S2

Period	LLG	$P_{S2G1}^t$	$P_{S2G2}^t$	$P_{S2G3}^t$	Selected Gateway
t = 0		0,19	0,32	0,48	G3
t = 1	G1	0,38	0,25	0,37	G1
t = 2	G2	0,29	0,42	0,28	G2
t = 3	G3	0,22	0,32	0,45	G3
t = 4	G3	0,17	0,25	0,58	G3
t = 5	G2	0,13	0,42	0,44	G3
t = 6	G1	0,33	0,32	0,34	G3
t = 7	G1	0,49	0,25	0,26	G1
t = 8	G2	0,37	0,42	0,20	G2
t = 9	G2	0,29	0,56	0,16	G2

We observe that S1 and S2 do not select the same gateway all the time (e.g.,  $t=0$ ,  $t=3$ ,  $t=5$ ,  $t=6$ ); thus, a source does not always select the least loaded gateway.

#### 5.5.2.4. Loop Free

Routing loops are serious problem for distributed routing protocols. They occur when packets continue to be routed indefinitely through the same set of routers. This problem may cause (1) An increase of network load and consequently an increase of packet losses and a decrease of available bandwidth; (2) the overload of routers processors, with unnecessary packet forwarding, slowing down traffic flows and the convergence of the routing protocol; and (3) the loss or the untimely processing of routing updates.

In order to prevent loops in NSR, we propose a loop-free algorithm (LFFA); the basic idea behind the proposed algorithm is to find a set of alternative links to forward packets towards a given gateway. This can be formulated as a graph theory problem. We model the Wireless Mesh Network as a network graph  $G(V, E)$  where  $V = \{1, \dots, n\}$  is the set of nodes (mesh routers) and  $E$  is the set of directed links. Let  $GW \subseteq V$  be the set of gateways in the WMN. We associate to each gateway  $g$  in  $GW$  a directed spanning tree  $T_g$  rooted at gateway  $g$  and having edges  $E_{T_g}$  directed towards  $g$  and all the vertices in  $V_g = \{V \setminus GW\} \cup g$ .  $T_g$  is obtained by selecting for each node in  $V_g$  (other than  $g$ ) its outgoing link that is traversed by the shortest path between this node and  $g$ ; This can be realized using Dijkstra algorithm. Having the graph  $G(V, E)$  and  $|GW|$  spanning trees for each gateway  $g$ , the problem consists of determining a set of directed links  $E_{F_g} \subset E$  such that the directed graph  $F_g = (V; E_{T_g} \cup E_{F_g})$  is acyclic. Algorithm 2 shows the pseudo-code of the proposed LFFA.

Algorithm 2 Loop Free Forwarding Algorithm (LFFA)

---

**Input :**

A graph  $G(V, E)$

$GW$  is the set of gateways

$|GW|$  spanning trees  $T_g = (V, E_{T_g})$ ; each tree is rooted at gateway  $g \in GW$

**Output :**

$E_{F_g}, \forall g \in GW$  the set of forwarding links for gateway  $g$

$F_g = (GW, E_{T_g} \cup E_{F_g}), \forall g \in GW$ , a directed forwarding graph.

---

Step 0:

- 1- Set  $GW^* = GW$
- 2- Set  $E_{Fg} = \{ \}, \forall g \in GW$

Step 1:

- 3- Select a gateway  $g \in GW^*$
- 4- Set  $E^* = \{E - E_{Tg}\}$
- 5- Let  $d_g$  be the depth of tree  $T_g$
- 6- Let  $L_i, i \in \{1, 2, \dots, d_g\}$  be the set of nodes which are at distance  $i$  from gateway  $g$
- 7- Set  $k = d_g$

Step 2:

- 8- Select node  $u \in L_k$  such that the degree of node  $u, \delta(u) = \min_{u' \in L_k} \delta(u')$

Step 3:

- 9- Set  $E_{Fg} = E_{Fg} \cup e(u, w), \forall e(u, w) \in E^*$  directed link between  $u$  and  $w$

Step 4:

- 10- Remove all links  $e(w, u), \forall w \in V$  from  $E^*$
- 11- Remove node  $u$  from  $L_k$  and all links  $e(u, w)$  from  $E^*$
- 12- If  $L_k = \{ \}$  then  $k = k - 1$
- 13- If  $k \neq 0$  then go to step 2, otherwise go to 5.

Step 5:

- 14- Set  $F_g = (V, E_{Tg} \cup E_{Fg})$
- 15- Remove node  $g$  from  $GW^*$ .
- 16- If  $GW^* \neq \{ \}$  then go to step 1, otherwise STOP

---

By using spanning trees, we can (1) create a topological sorting between a source node and gateways; and (2) ensure that the link on the shortest path between each node and the selected gateway will be included in the list of forwarding alternatives. Thus, in step 1, the algorithm chooses one gateway and creates a spanning tree rooted at the selected gateway. In step 2, the algorithm selects the farthest node with the minimum node degree in the spanning tree. In step 3, all outgoing links of the selected node are added to the list of forwarding alternatives. In step 4, all incoming links to the selected node are removed from the list of

forwarding alternatives; this ensures that no packet forwarded from the selected node will return to it again in the future.

To better understand LFFA, let us consider the WMN shown in Figure 41;

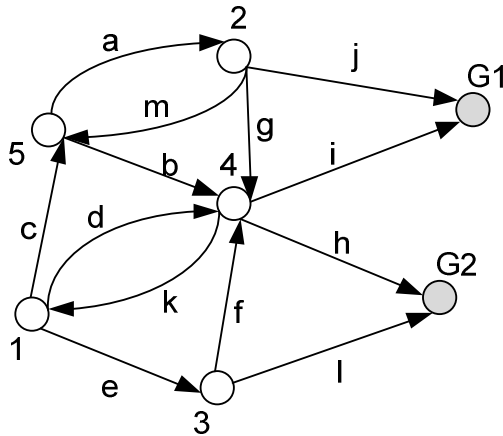


Figure 41. Topology for loop free illustration

The network consists of (a) two gateways G1 and G2; and (b) Five mesh routers 1, 2, 3, 4 and 5. a, b, c, d, e, f, g, h, i, j, k, l are directed links (e.g., d is the link between MR 1 and MR 4 and k is the link between MR 4 and MR 1). Algorithm 2 takes as input the graph representing the WMN, the set of gateways  $GW = \{G1, G2\}$  and two spanning trees  $T_{G1}$  and  $T_{G2}$  rooted at G1 and G2 respectively. Figure 42 shows the construction (Step 1) of the spanning tree rooted at G1; this spanning tree can be constructed once during network deployment or whenever a MR joins or leaves the network.

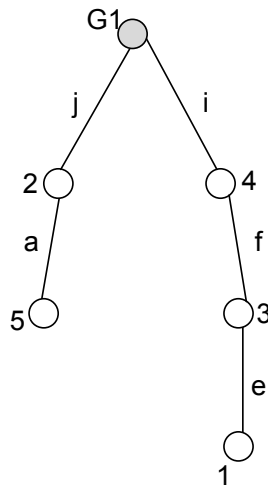


Figure 42. Spanning tree rooted at G1



Table 6 summarizes all the operations performed by the algorithm for G1. (Similar operations for G2). Figure 42 shows that the depth of the spanning tree is equal to 3; thus, 3 sets ( $L_k$  with  $k = 3, 2$  and  $1$ ) are computed in the initialization phase; each set represents the MRs at a given level.

Table 6: Summary of operations performed by Algorithm 2 for Gateway G1

Initialization	Step 0	$GW^* = \{G_1, G_2\}, E_{FG1} = \{ \}, E_{TG1} = \{a, e, f, i, j\}$
	Step 1	$E^* = \{b, c, d, g, k\}, d_{G1} = 3$ $L_1 = \{2, 4\}, L_2 = \{5, 3\}, L_3 = \{1\}$
K=3	Step 2	$u = 1$ (we select MR 1 from $L_3$ )
	Step 3	$E_{FG1} = \{ \} \cup \{d, c\}$
	Step 4	$E^* = \{b, g\}, L_3 = \{ \}$
K=2	Step 2	$u = 3$ (we select MR 3 from $L_2$ )
	Step 3	$E_{FG1} = \{d, c\}$ (the set is not changed)
	Step 4	$E^* = \{b, g, h\}, L_2 = \{5\}$
	Step 2	$u = 5$ (we select MR 5 from $L_2$ )
	Step 3	$E_{FG1} = \{b, c, d\}$
	Step 4	$E^* = \{g\}, L_2 = \{ \}$
K=1	Step 2	$u = 2$ (we select MR 2 from $L_1$ )
	Step 3	$E_{FG1} = \{b, c, d\} \cup \{g\}$
	Step 4	$E^* = \{ \}, L_1 = \{4\}$
	Step 2	$u = 4$ (we select MR 4 from $L_1$ )
	Step 3	$E_{FG1} = \{b, c, d, g\}$ (the set is not changed)
	Step 4	$E^* = \{ \}, L_1 = \{ \}$
Final Result	Step 5	$F_{G1} = E_{TG1} \cup E_{FG1} = \{a, e, f, i, j, b, c, d, g\}$ $GW^* = \{G2\}$

The final result for gateway G1 is the set  $E_{FG1}$  of alternative links towards it, Figure 43 shows that  $E_{FG1} = \{a, e, f, i, j, b, c, d, g\}$ .

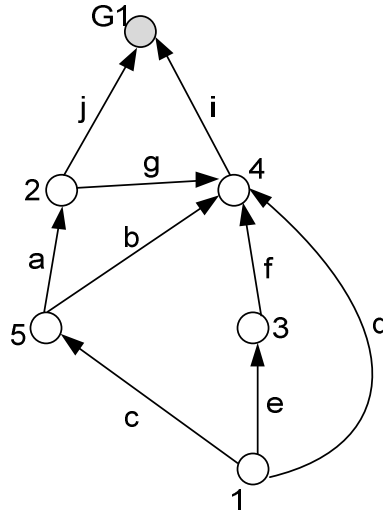


Figure. 43. Directed forwarding graph to G1

## 5.6. Simulation and results

We study the performance of the proposed routing scheme (NSR) using ns-2 with the module implementing multi-radio and multi-channel WMNs [85]; Table 7 shows the simulation parameters.

Table 7. Simulation setup

Simulation Parameters	Values
Network Area	1000mx1000m
Link data rate	11Mbps
Frequency	9.14e+08 Hz
Traffic Type	CBR (UDP)
Network Load	1000-3000 Kbps

The topology used for the backbone Wireless Mesh Network consists of 16 MRs randomly placed in 1000x1000 area and 3 GWs (nodes 1, 2 and 3). The MAC layer protocol is IEEE 802.11 and the channel assignment is performed using the scheme in [86]. We use a

realistic reception model by taking into consideration Bit Error Rate (BER) used in Intersil HFA3861B radio hardware [114] and the corresponding Frame Error Rate (FER). We use Constant Bit-Rate traffic (CBR) with UDP having a packet size of 1,000 bytes. Since most traffic is destined to the Internet, we assume that traffic is randomly generated from different source nodes and may cross several intermediate nodes (i.e., multi-hop routing) to reach the Internet through a GW.

We have implemented and compared the performance of NSR against RLBDR [26], MIC [48], ETX [24] and NEAREST-G (minimum number of hops to a gateway) based routing. The performance is evaluated in terms of (1) network average throughput: the amount of successfully transmitted bytes in a given time interval; (2) average end to end delay: the delay for sending CBR packets from source nodes to one of the gateways; (3) the loss rate: the average number of packets dropped inside the WMN over the number of sent packets; (4) the Gini index: measures the inequality of distributed traffic among gateways; and (5) the network stability: the mean of the stability index of MRs.

In the first set of simulations, we study the performance of NSR compared to other approaches when increasing the data rate. Figure 44 shows that NSR outperforms RLBDR, MIC, ETX, NEAREST-G. Particularly, at high data rates (3000 kbps), NSR achieves 7%, 17%, 36% and 41% more throughput than RLBDR, MIC, ETX, NEAREST-G respectively.

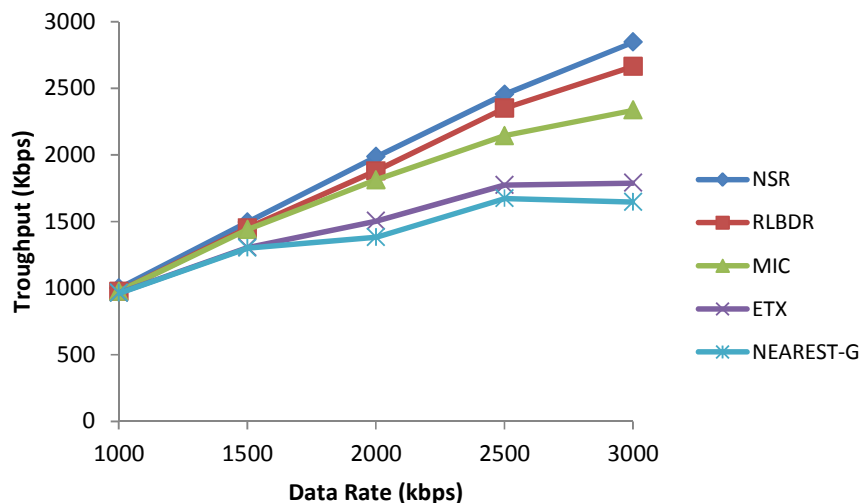


Figure 44. Average throughput

In the second set of simulations, we study the performance in terms of delay. Figure 45 shows clearly that NSR outperforms MIC, ETX, NEAREST-G. Particularly, at 1000 kbps, the NSR delay performance is better than MIC, ETX and NEAREST-G by 31%, 29%, 16%, respectively. However, for data rates between 1000 kbps and 2000 kbps, RLBDR outperforms NSR by around 25%. This can be explained by the fact that NSR is not interested in minimizing the number of hops (from sources to gateways) but using the most stable nodes to route traffic. For data rates bigger than 2500 kbps, NSR outperforms RLBDR (e.g., at 2500 kbps, NSR outperforms RLBDR by 49% and by 25% at 3000 kbps); this is expected since at high data rates, interferences are high causing instability of nodes (in this case, a scheme that uses stable nodes to route traffic performs better)

In the third set of simulations, we study the impact of data rate variation on the packet loss ratio. Figure 46 shows the total loss rate variation while Figure 47 and Figure 48 show loss rate variation due to collisions and IFQ respectively. We observe that NSR outperforms RLBDR, MIC, ETX and NEAREST-G especially when data rate increases. It is obvious that increasing data rates increases interferences (Figure 47) and packet loss rate due to Interface Queue (IFQ) overflow (Figure 48); this creates oscillations making the network instable. This explains the performance of NSR since it uses paths with the most stable nodes.

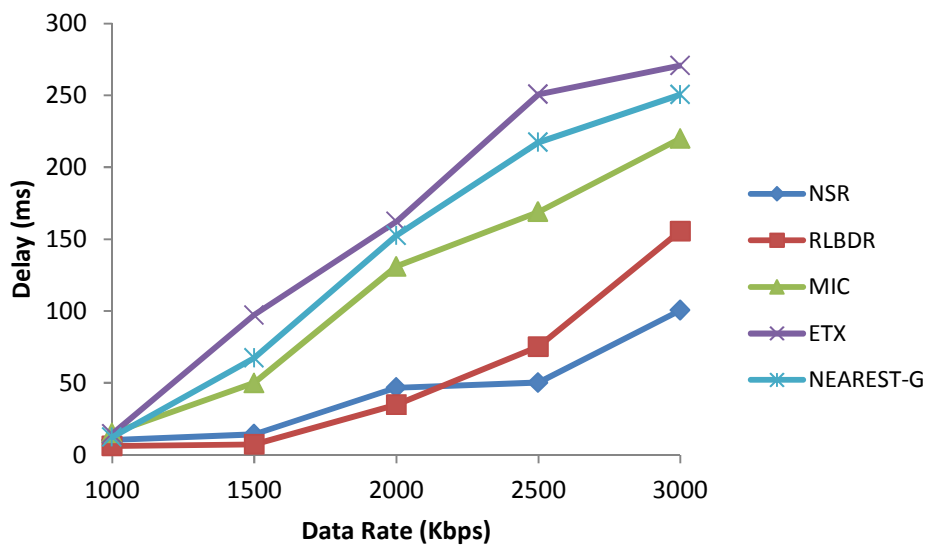


Figure 45. Delay vs. data rate

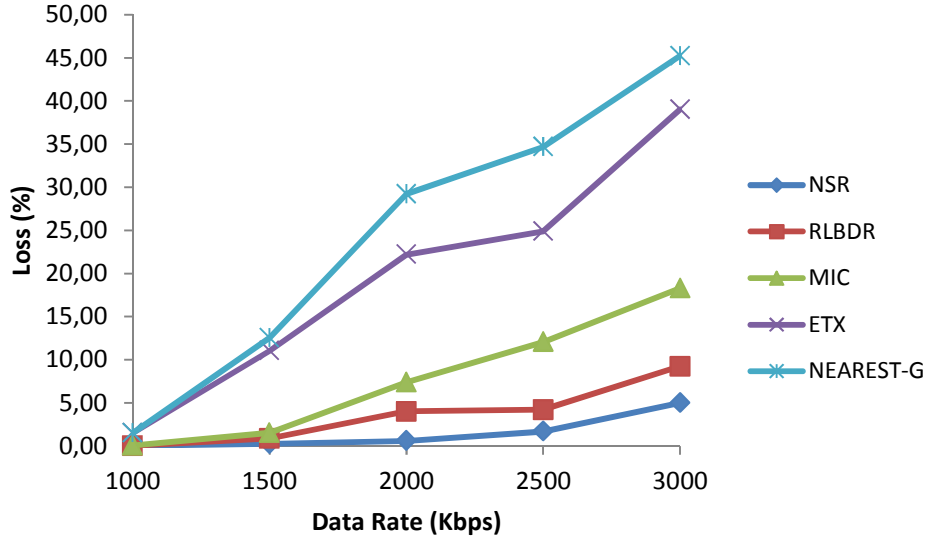


Figure 46. Loss rate vs. data rate

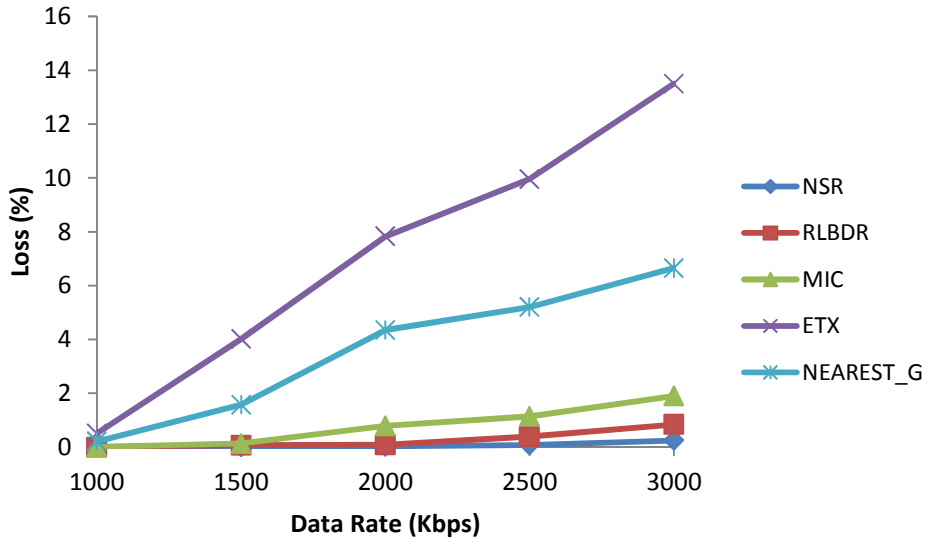


Figure 47. Loss rate due to collisions vs. data rate

Thus, we conclude that a routing protocol must not only consider routing metrics that capture the effect of interferences and packet losses but also metrics representing stability of nodes. Indeed, by considering the stability of nodes, the routing protocol can avoid/reduce the well known problem of oscillations in WMNs and thus improve the network performance.

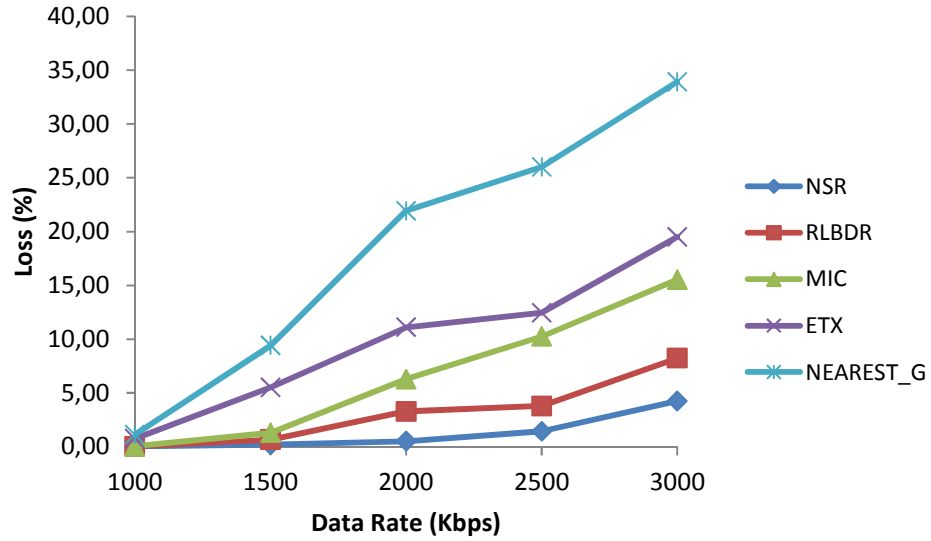


Figure 48. Loss rate due to IFQ vs. data rate

In the fourth set of simulations we study the behavior of our proposed gateway selection method in terms of traffic fairness between gateways; To perform this study, we make use of Gini index. Originally the Gini index was proposed in the field of economics [131] to describe the distribution of wealth in human populations. It is a summary statistic of the Lorenz curve and a measure of inequality in a population. Gini index was adopted in [132] to measure the instantaneous fairness of scheduling algorithms. In this paper, we use this index to measure the inequality in the distribution of traffic among gateways. Therefore, Gini index will be the area between the Lorenz curve of the actual traffic served by gateways and the ideally Lorenz curve corresponding to a fair distribution of traffic among gateways. Gini index  $G$  It is defined as follows:

$$G = \left( \frac{2}{n^2 \bar{x}} \right) \sum_{i=1}^n \left( \left( i - \frac{n+1}{2} \right) x_i \right) \quad (5.14)$$

where:  $\bar{x} = \frac{1}{n} \sum_{i=1}^n x_i$ ,  $n$  is the number of gateways and  $x_i$  is the total amount of traffic in gateway  $i$ .  $G$  assumes values between 0 and 1; a low value of  $G$  indicates a more equal traffic distribution (fairness) among gateways.

In this set of simulations, we compare NSR with any load-based protocol (Load curves) where the selected gateway is the least loaded gateway. We generated traffic with data rates of 1000, 2000 and 3000 kbps (see Figure 49, Figure 50 and Figure 51 respectively). At 1000 kbps, Figure 49 shows that during 79% of the simulation time, the value of Gini index is around 0.2 for NSR whereas it is around 42% for the load curve. At 2000 kbps, Figure 50 shows that during 74% of simulation time the Gini index is around 0.2 for NSR whereas it is around 34% for the load curve. Finally, at 3000 kbps, Figure 51 shows that 57% of the simulation time the Gini index for NSR is around 0.2 whereas it is 34% for the load curve. Thus, by choosing the least loaded gateway (load curves) the traffic is not fairly distributed among gateways compared to NSR. Since our proposed gateway selection scheme has a small Gini index during simulation time (around 0.20), we conclude that it achieves far better fairness than load-based selection schemes.

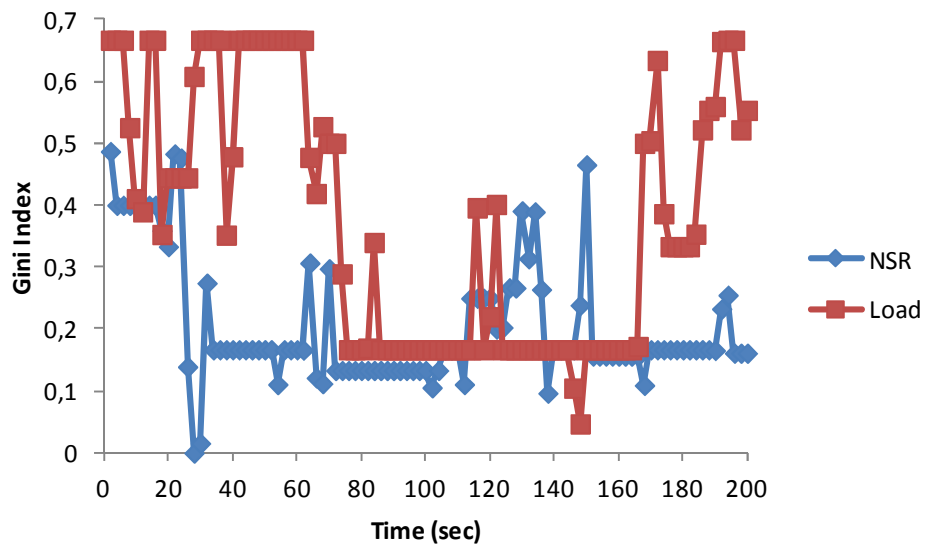


Figure 49. Gini Index vs. Time for a data rate 1000 (kbps)

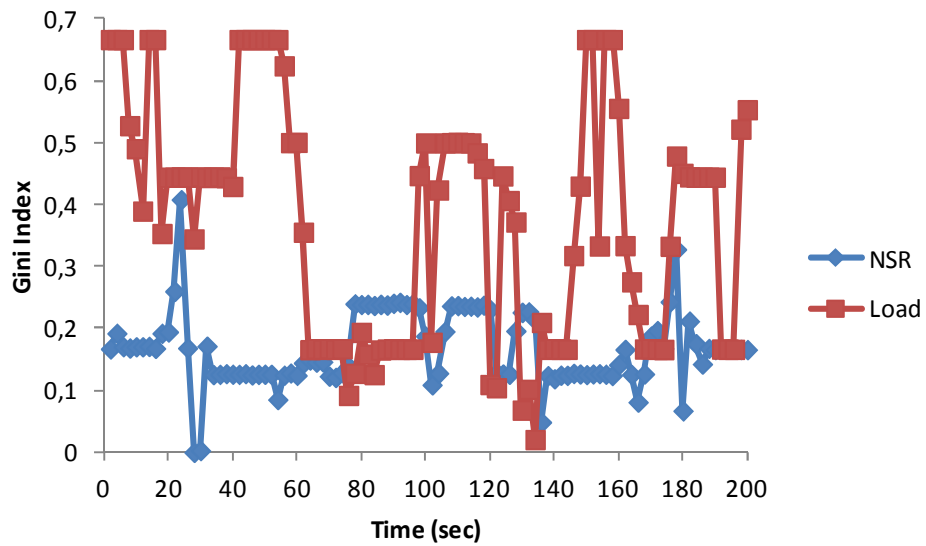


Figure 50. Gini Index vs. Time for a data rate 2000 (kbps)

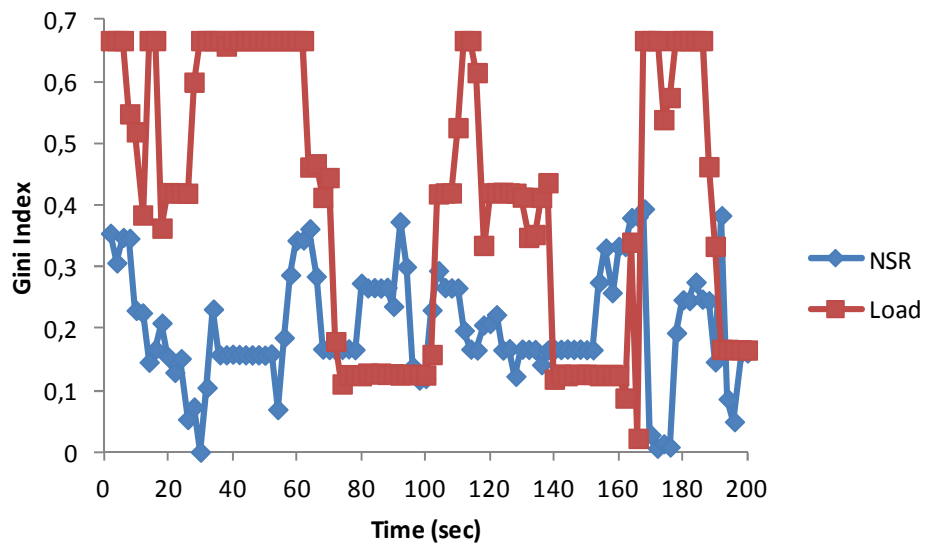


Figure 51. Gini Index vs. Time for a data rate 3000 (kbps)

Figure 52 and Figure 53 show the percentage of traffic being served by different Gateways. Lorenz\_1000, Lorenz\_2000, and Lorenz\_3000 are Lorenz curves when generating traffic at 1000, 2000 and 3000 kbps respectively. Line of equality is the curve indicating a perfect load balancing among gateways. Figure 52 shows that NSR forwards 27% of traffic to the Internet through one gateway and 58% of traffic through two gateways (i.e., 27% through the first gateway and 31% through the second gateway) compared to 33,33% and 66,66%



respectively in the best case scenario (represented by Line of Equality curve). At 3000 kbps, by using NSR, 20% of traffic passes through one gateway and 49% through two gateways. Figure 53 shows that for the load case, at 1000 kbps 20% of traffic passes through one gateway and 44% through two gateways whereas at 3000 kbps 13% of traffic passes through one gateway and 37% through two gateways. We conclude that fairness decreases with the traffic load (for all schemes) and NSR outperforms (in all cases) load-based selection schemes.

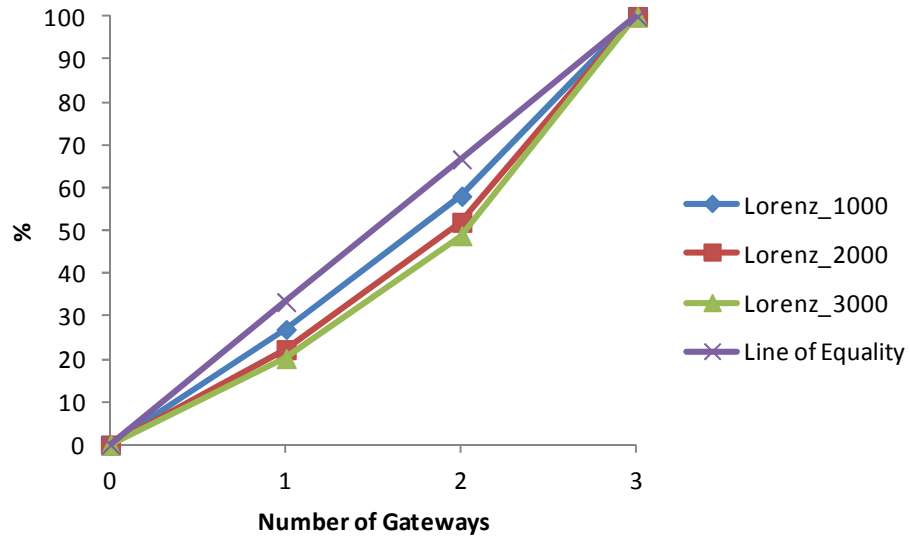


Figure 52. Percentage of traffic served by gateways (NSR case)

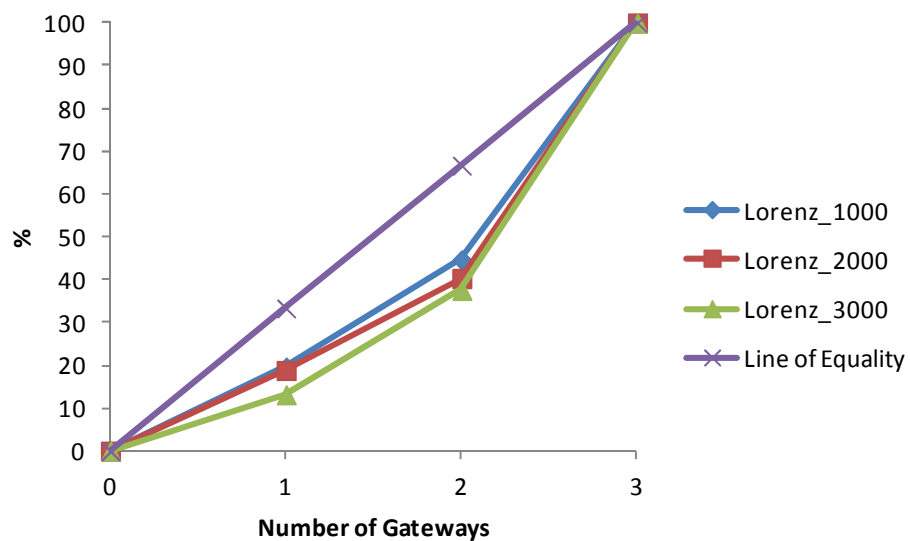


Figure 53. Percentage of traffic served by gateways (Load case)

In the fifth set of simulation, we measure the stability of the network when using NSR. The network stability is computed as the average stability index of active nodes during a period of time. We classify the network stability into three classes (1) stable: when stability index is between 0.75 and 1; (2) marginally stable: when stability index is between 0.5 and 0.75; and (3) unstable: when stability index is below 0.5.

Figure 54 shows that the network stability increases with stability index. For example, with a data rate of 1000 kbps, the average stability index is around 0.9 (i.e., a stable network); this is expected since in a lightly loaded network, the quality of links is good (less interferences and data losses); thus, nodes are more stable (see Equation 5.11). When data rate increases, more interferences and losses are introduced degrading the quality of links and thus the stability of nodes (e.g., at 2000 kbps, the average stability index is around 0.8 and at 3000 kbps the average stability index is around 0.7).

We observe that, using NSR, the network does not become unstable even when we increase data rate; it is either stable or marginally stable. These findings show that by considering local stability (NSR selects most stable nodes to destination), one can achieve global stability (network stability)

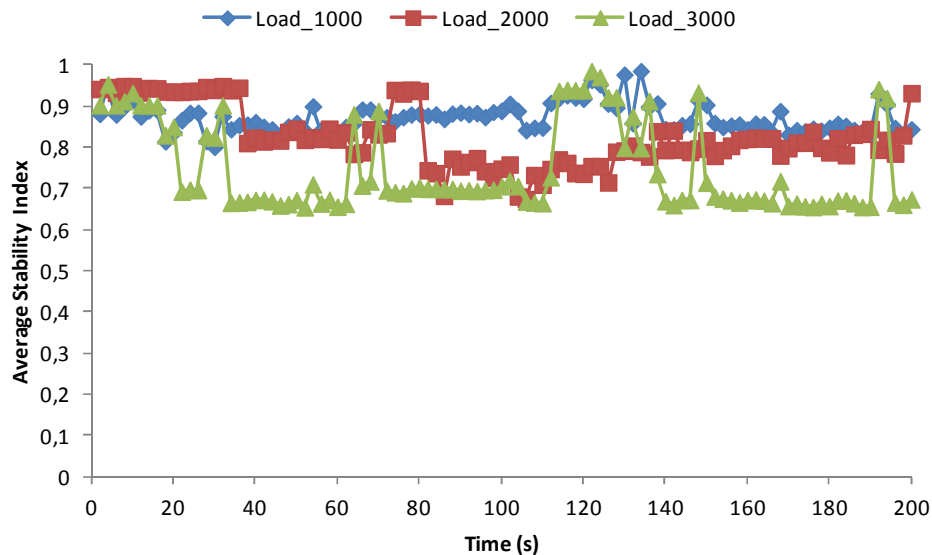


Figure 54. Average stability index

## **5.7. Conclusion**

In this paper, we did study the impact of routing metrics on the performance of WMNs; our study findings led us to consider stability when routing traffic from sources to gateways. Thus, we did propose a novel routing protocol, called NSR, that selects the most stable nodes in computing paths a source to a given gateway. We also proposed a new gateway selection scheme that not only helps in avoiding frequent rerouting (and thus network instability) but also achieves fairness in distributing traffic among the gateways in the network. Simulations results show that NSR outperforms all existing routing protocols (in terms of throughput, delay, loss rate, Gini index and stability index. In particular, it outperforms RLBDR, MIC, ETX and NEAREST-G.

### **Acknowledgment**

We would like to thank Mr Vinicius da Cunha Martins Borges [41] for providing us with code for simulation. Also, we address our thanks to Dr. Abdeltouab Belbekkouche for valuable discussions. The research reported in this manuscript has been supported in part by Natural Sciences and Engineering Research Council of Canada (NSERC) and Bell Canada.

## **Chapitre 6 : Conclusion et travaux futurs**

Dans ce chapitre, nous résumons les contributions et les résultats de cette thèse puis nous proposons des perspectives pour des travaux de recherche futurs.

### **6.1. Contributions et résultats de la thèse**

La performance des réseaux maillés sans fil multi-canaux multi-interfaces est fortement impactée par les interférences et la congestion. Ces derniers causent des pertes de paquets et une augmentation du délai de transmission d'une façon considérable. Ainsi, dans cette thèse, nous avons contribué à l'amélioration des performances et à la bonne gestion des ressources de ces réseaux à travers des protocoles de routages adaptatifs. Ces protocoles sont capables d'améliorer le débit, de réduire le taux de perte et d'assurer une bonne stabilité.

Au cours de cette thèse, nous avons, d'abord, identifié une série de problèmes qui impactent les réseaux maillés sans fil et sur lesquels il faut agir pour assurer une amélioration de la performance de ces réseaux. Parmi ces problèmes on retrouve, la conception d'une métrique de routage, la sélection des passerelles, l'utilisation des zones critiques et la stabilité. Le problème des métriques de routage consiste à atteindre plus qu'un seul objectif en l'occurrence réduire les interférences et réduire les pertes des paquets dans un chemin. Par ailleurs, trouver un chemin n'est qu'une partie du problème du routage dans les WMNs. Comme le trafic est orienté dans la plus part du temps vers les passerelles, la sélection de ces derniers doit donc être faite de façon appropriée, faute de quoi, tout le trafic s'orientera vers la même passerelle provoquant ainsi des goulots d'étranglement. L'exploitation des zones critiques est aussi une solution à considérer dans les WMNs. En effet, tous les nœuds dans le réseau ne peuvent pas contribuer de la même façon au routage. Plus on s'approche des passerelles, plus une concentration du trafic est observée pouvant provoquer de la congestion, et par conséquent, des pertes de paquets. Finalement, la stabilité est considérée comme l'un des facteurs déterminants des WMNs et nécessaires pour plusieurs types d'applications. Une instabilité se produit quand le volume du trafic et les demandes aux capacités augmentent

provoquant ainsi des fréquentes variations dans la qualité des liens. Pour proposer des solutions à ces problèmes de routage, nos trois contributions dans cette thèse se résument comme suit:

Dans la première contribution, présentée au chapitre 3, nous nous sommes intéressés à la conception d'une métrique de routage et à la sélection des passerelles. Ainsi, nous avons proposé BP2BG (*Best Path to Best Gateway*) en tant que métrique pour notre protocole de routage à la source. Dans BP2BG, en plus de capturer les caractéristiques d'un lien en l'occurrence les interférences et le taux de pertes des paquets, nous avons considéré également la surcharge des passerelles. Pour les interférences, BP2BG considère dans son calcul du ratio d'interférence (IR) les interférences inter-flux et intra-flux tout en se basant sur un modèle physique existant et sur le nombre de voisins d'un nœud qui opèrent sur le même canal (c-à-d qui s'interfèrent). Pour mesurer le taux de perte des paquets, nous avons utilisé des techniques de mesures actives où des sondes sont échangées périodiquement sur chaque lien. Aussi, sur chaque sens du lien des mesures indépendantes sont prises ; en effet, il a été prouvé dans la littérature qu'on ne peut pas attribuer la moyenne des métriques mesurées sur les deux sens d'un lien pour désigner sa qualité. Finalement, à l'aide des coefficients de pondérations nous avons déterminé la surcharge des passerelles, nommé DACI (Distribution Available Capacity Indicator), avec l'ensemble des mesures prise sur les liens pour établir une métrique de chemin. DACI se base principalement sur le nombre d'interfaces qu'une passerelle dispose (habituellement plus que deux) et sur leurs charges. Ainsi en se basant sur BP2BG, nous avons non seulement choisi le chemin approprié, qui présente moins d'interférences et moins de perte des paquets, mais également la passerelle servant à diriger le trafic vers l'Internet. Nous avons démontré à l'aide des simulations l'impact d'utiliser les métriques de routage d'une façon individuelle. Les résultats obtenus confirment que la combinaison de l'interférence et le taux de perte des paquets d'une part et le choix des passerelles d'une autre part sont capables d'améliorer la performance des WMNs. En outre, les résultats numériques ont montré que la performance de notre solution BP2BG est meilleure que celle des solutions proposées dans la littérature [24] en termes de délai et de débit.

La deuxième contribution, proposée dans le chapitre 4, a été consacrée aux problèmes des zones critiques dans les WMNs. En effet, il a été observé que parmi les nœuds critiques

dans un WMN on retrouve les nœuds autour des passerelles. Ainsi, en se basant sur le principe de la métrique BP2BG qui combine l'interférence et le taux de perte et en explorant la capacité du routage proactif et adaptatif nous avons proposé le protocole RLBDP (Reinforcement Learning-based Distributed Routing). L'idée derrière RLBDP est d'utiliser l'apprentissage par renforcement pour calculer les routes dans le WMN de façon distribuée. À cet égard, nous avons proposé deux versions de RLBDP : RLBDP-PQ et RLBDP-ZPQ. RLBDP-PQ pénalise les liens de mauvaise qualité lorsqu'on s'approche des passerelles; un chemin dont la qualité des liens autour d'une passerelle est meilleure sera plus favorisé que les autres. RLBDP-ZPQ donne plus d'importance aux nœuds qui se trouvent à N-sauts des passerelles (N étant un nombre prédéfini qui peut être de valeur 1, 2 ou 3). De plus, RLBDP utilise l'algorithme du *Q-learning* pour mettre à jour dynamiquement les coûts des chemins, sélectionner les prochains nœuds pour faire suivre les paquets vers des passerelles choisies et explorer d'autres nœuds voisins. Les résultats numériques ont montré que RLBDP, dans ces deux versions, présente de meilleurs résultats comparativement aux protocoles dans la littérature utilisant les métriques MIC, ETX, Nearest-G, BP2BG and Load-G [48, 24, 73] en termes de délai, taux de perte des paquets et débit. Toutefois, RLBDP-PQ reste meilleur que RLBDP-ZPQ dans les situations où le taux de trafic généré dans le réseau est grand. Ceci s'explique par le fait que RLBDP-PQ est capable de réagir mieux aux interférences comparativement à RLBDP-ZPQ.

Finalement, la troisième contribution, proposée dans le chapitre 5, a été consacrée à la stabilité qui représente un des facteurs importants dans la performance des WMNs. Il a été prouvé [70] lors d'analyses effectuées sur des bancs d'essai que l'instabilité se produit à cause des changements fréquents des routes (causés par les variations instantanées de la qualité des liens, présence d'interférences ou de congestion, par exemple). À cet égard, nous avons proposé un routage proactif basé sur la métrique NS (Node Stability). L'objectif est de choisir le nœud le plus stable comme nœud prochain pour acheminer le trafic. Afin de calculer NS, nous avons relié la stabilité d'un nœud à la stabilité de sa table de routage. En effet, un des symptômes de l'instabilité des réseaux est l'apparition et la disparition des routes des tables d'une façon intermittente. Ainsi, en exploitant le nombre de variations des chemins dans les tables de routages comme indice de perturbation des réseaux et en utilisant la fonction d'entropie, connue dans les mesures de l'incertitude et du désordre des systèmes [120, 121,

122, 123, 124, 125, 126, 127, 128], nous avons pu définir la métrique NS. En plus des problèmes de stabilité, nous avons contribué dans la sélection des passerelles en proposant une nouvelle approche basée sur des probabilités plutôt que sur la surcharge des passerelles comme était le cas dans les contributions 1 et 2. En effet, nous avons constaté qu'avec une sélection basée sur la surcharge des passerelles, des oscillations dans le réseau risquent de se produire provoquant ainsi plus de perte de paquets et d'interférences. Ainsi, cette nouvelle technique a permis une répartition du trafic entre les passerelles d'une façon équitable. Nous avons évalué notre protocole NSR (node stability routing) basé sur NS ; les résultats numériques montrent de meilleures performances de NSR, en comparaison avec des protocoles dans la littérature, en termes de débit, délai, taux de perte des paquets, l'indice de Gini et l'indice de stabilité.

## **6.2. Perspectives et travaux futurs**

Les contributions présentées dans cette thèse ouvrent des perspectives intéressantes pour des travaux futurs. Nous mettons en évidence trois directions principales:

- Étude comparative des métriques basées sur les interférences : dans la revue de littérature nous avons signalé l'existence de plusieurs modèles d'interférences. Parmi ces modèles on retrouve le modèle protocole, le modèle logique et le modèle physique. Ainsi, étudier en détail l'impact de ces modèles sur les protocoles de routages d'une part et sur la performance des réseaux d'autre part, notamment en termes de débit et de délai de bout-en-bout sera un apport important dans la recherche. Par conséquent, il est possible d'identifier dans quel type de scénario l'un des modèles est plus approprié que l'autre permettant ainsi une convergence dans les choix des modèles.
- Protocole de réassignation des canaux : dans ce travail nous avons considéré le routage comme étant une alternative pour améliorer les performances des réseaux maillés sans fil. La réassignation des canaux pourra être aussi une autre solution. En effet, nous pensons que les métriques développées dans cette thèse pourront servir de base pour des protocoles d'assignation des canaux. Par exemple, l'exploitation de la stabilité d'un nœud et plus spécifiquement le nombre de variations de la qualité des liens dans une table de routage pourra être un bon indicateur pour le besoin d'une réassignation des canaux.

- Joindre l'assignation des canaux au routage : dans cette thèse nous nous sommes concentrés sur le routage dans les WMNs. En cas de panne une procédure de reroutage est lancée pour rétablir le chemin. Alors que dans le point précédent, nous avons évoqué une deuxième alternative qui consiste à assigner les canaux. En cas de panne, une procédure de réassignation des canaux pourra être lancée. Ainsi, il existe deux solutions pour contourner une panne, soit une réassignation des canaux ou un reroutage. Cependant, le choix entre ces deux techniques n'est pas trivial en termes de temps de réaction afin de trouver les routes alternatives. La meilleure technique est celle qui offre plus de stabilité au réseau, réduit le nombre de paquets de contrôle, améliore le temps de transmission et réagit rapidement en cas de panne. Une analyse des différents scénarios pour déterminer le meilleur d'entre eux s'avère nécessaire. Par conséquent, des protocoles joignant l'assignation des canaux au routage peuvent être développés pour une meilleure amélioration de la performance du réseau.



## Bibliographie

- [1] J. Yick, B. Mukherjee, and D. Ghosal, *Wireless sensor network survey*. Computer Networks, Vol. 52(12): p. 2292-2330, 2008.
- [2] M. Boushaba, A. Hafid, and A. Benslimane, *High accuracy localization method using AoA in sensor networks*. Computer Networks, Vol. 53(18): p. 3087–3088, 2009.
- [3] H. Hartenstein, and K. Laberteaux, *A tutorial survey on vehicular ad hoc networks*. Communications Magazine, Vol. 46(6): p. 164-171, 2008.
- [4] I.F. Akyildiz, X. Wang, and W. Wang, *Wireless mesh networks: a survey*. Computer Networks, Vol. 47(4): p. 445–487, 2005.
- [5] MIT Roofnet. <http://www.pdos.lcs.mit.edu/roofnet>
- [6] Wireless leiden. <http://www.wirelessleiden.nl>
- [7] Mesh@Purdue. <http://www.engineering.purdue.edu/MESH>
- [8] F. Li, Y. Wang, X. Y. Li, A. Nusairat, and Y. Wu, *Gateway placement for throughput optimization in wireless mesh networks*. Mobile Networks and Applications, Vol. 13(1): p. 198-211, 2008.
- [9] P. Mühlenthaler, *802.11 et les réseaux sans fils*. Editions Eyrolles, 2002.
- [10] F. Ohrtman, *WiMAX handbook*. McGraw-Hill, 2005.
- [11] M. Rubinstein, I. Moraes, M. Campista, L. Costa, and O. Duarte, *A survey on wireless ad hoc networks*. Mobile and Wireless Communication Networks, Vol. 211: p. 1-33. 2006.
- [12] L. Chen, *Wireless Mesh Networks (WMNs)*. Technical Report UIUCDCS-R-2006-2874, Dept. of Computer Science, UIUC, 2006.

- [13] Y. Andreopoulos, N. Mastronarde, and M. van der Schaar, *Cross-layer optimized video streaming over wireless multihop mesh networks*. IEEE Journal on Selected Areas in Communications, Vol. 24(11): p. 2104-2115, 2006.
- [14] D. Niculescu, S. Ganguly, K. Kim and R. Izmailov, *Performance of VoIP in a 802.11 wireless mesh network*. in Proceedings of IEEE INFOCOM'06, Barcelona, Spain, 2006.
- [15] S. Roy, D. Koutsonikolas, S. Das, and Y. C. Hu, *High-throughput multicast routing metrics in wireless mesh networks*. Ad Hoc Networks, Vol. 6(6): p. 878-899, 2008.
- [16] *Capacity of Wireless Mesh Networks*, white paper, BelAir Networks, 2006.  
[http://www.belairnetworks.com/resources/pdfs/Mesh\\_Capacity\\_BDMC00040-C02.pdf](http://www.belairnetworks.com/resources/pdfs/Mesh_Capacity_BDMC00040-C02.pdf)
- [17] <http://www.ieee802.org/11/>
- [18] J. A. Stine, *Exploiting smart antennas in wireless mesh networks using contention access*. IEEE Wireless Communications, Vol. 13(2): p. 38-49, 2006.
- [19] K. Sundaresan, and R. Sivakumar, *Routing in ad-hoc networks with MIMO links*. in Proceedings of the 13th IEEE International Conference on Network Protocols (ICNP'05), Boston, Massachusetts, USA, 2005.
- [20] W. Jaafar, W. Ajib, and S. Tabbane, *The capacity of MIMO-based wireless mesh networks*. in Proceedings of the 15th IEEE International Conference on Networks (ICON'07), Adelaide, Australia, 2007.
- [21] P. Kyasanur, and N. H. Vaidya, *Capacity of multi-channel wireless networks: impact of number of channels and interfaces*. in Proceedings of the 11<sup>th</sup> ACM annual international conference on Mobile computing and networking (MobiCom'05), Cologne, Germany, 2005.

- [22] M. Kodialam, and T. Nandagopal, *Characterizing the capacity region in multi-radio multi-channel wireless mesh networks*. in Proceedings of the 11th ACM annual international conference on Mobile computing and networking (MobiCom'05), Cologne, Germany, 2005.
- [23] T. Gyires, and H. J. Wen, *Extension of Multiprotocol Label Switching for long-range dependent traffic: QoS routing and performance in IP networks*. Computer Standards & Interfaces, Vol. 27(2): p. 117-132, 2005.
- [24] D. De Couto, D. Aguayo, J. Bicket, and R. Morris. *A high-throughput path metric for multi-hop wireless routing*. Wireless Networks, Vol. 11(4): p. 419-434. 2005.
- [25] R. Draves, J. Padhye, and B. Zill, *Routing in multi-radio, multi-hop wireless mesh networks*. in Proceedings of the 10th ACM annual international conference on Mobile computing and networking (MobiCom'05), Philadelphia, U.S.A, 2004.
- [26] M. Boushaba, A. Hafid, and A. Belbekkouche, *Reinforcement learning-based best path to best gateway scheme for wireless mesh networks*. in Proceedings of the 7th International Conference on Wireless and Mobile Computing Networking and Communications (WiMob'2011), Shanghai, China.
- [27] J. Jun and M. L. Sichitiu. *The nominal capacity of wireless mesh networks*. Wireless Communications, IEEE, Vol. 10(5): p. 8-14, 2003.
- [28] M. Boushaba, A.Hafid, and M. Gendreau, *Local Node Stability-Based Routing for Wireless Mesh Networks*. in proceedings of IEEE Wireless Communications and Networking Conference (WCNC'2013), Shanghai, China, 2013.
- [29] Intel Corporation, *Understanding Wi-Fi and WiMAX as Metro-Access Solutions*, Intel White Paper, Wi-Fi and WiMAX Solutions, 2004.

- [30] IEEE 802.16 Working Group, *IEEE Standard for Local and Metropolitan Area Networks*, Part 16: Air Interface for Fixed Broadband Wireless Access Systems, IEEE Std, 802.16, 2004.
- [31] M.El Masri, S. Abdellatif, and G. Juanole, *An uplink bandwidth management framework for IEEE 802.16 with QoS guarantees*. Ifip Networking, Aachen Germany, 2009.
- [32] D.Niyato, and E. Hossain, *Integration of IEEE 802.11 WLANs with IEEE 802.16-based multihop infrastructure mesh/relay networks: A game-theoretic approach to radio resource management*. IEEE Network, Vol. 21(3): p. 6-14, 2007.
- [33] R. Bruno, M. Conti, and E. Gregori, *Mesh networks: commodity multihop ad hoc networks*. IEEE Communications Magazine, Vol. 43(3): p.123-131, 2005.
- [34] K. Jain, J. Padhye, V. N. Padmanabhan, and L. Qiu, *Impact of interference on multi-hop wireless network performance*. Wireless networks, Vol. 11(4): p. 471-487, 2005.
- [35] D. S. D.Couto, D.Aguayo, J.Bicket, and R. Morris, *A high-throughput path metric for multi-hop wireless routing*. Wireless Networks, Vol. 11(4): p. 419-434, 2005.
- [36] A. Raniwala, and T. C. Chiueh, *Architecture and algorithms for an IEEE 802.11-based multi-channel wireless mesh network*. in Proceedings of 24th Annual Joint Conference of the IEEE Computer and Communications Societies, (INFOCOM 2005), Miami, FL, USA, 2005.
- [37] V. C. M. Borges, M. Curado, and E. Monteiro, *Cross-layer routing metrics for mesh networks: Current status and research directions*. Computer Communications, Vol. 34(6): p. 681-703, 2011.

- [38] P. Gupta and P. R. Kumar, *The capacity of wireless networks*. IEEE Transactions on Information Theory, Vol. 46(2): p. 388-404, 2000.
- [39] K. Xu, M. Gerla, and S. Bae. *How effective is the IEEE 802.11 RTS/CTS handshake in ad hoc networks*. in Proceedings of Global Telecommunications Conference, (GLOBECOM'02), Taipei, Taiwan, 2002.
- [40] J. Lee, S.-J. Lee, W. Kim, D. Jo, T. Kwon, and Y. Choi, *Understanding interference and carrier sensing in wireless mesh networks*. IEEE Communications Magazine, Vol. 47(7): p. 102-109, 2009.
- [41] V. Borges, D. Pereira, M. Curado, and E. Monteiro, *Routing metric for interference and channel diversity in multi-radio wireless mesh networks*. in Proceedings of Ad-Hoc, Mobile and Wireless Networks, (ADHOC-NOW'09), Murcia, Spain, 2009.
- [42] M. Genetzakis, and V. A. Siris, *A contention-aware routing metric for multi-rate multi-radio mesh networks*. in Proceedings of the 5th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON'08), California, USA, 2008.
- [43] A. Vlavianos, L. K. Law, I. Broustis, S. V. Krishnamurthy, and M. Faloutsos. *Assessing link quality in iee 802.11 wireless networks: Which is the right metric?*. in Proceedings of the 19th International Symposium on Personal, Indoor and Mobile Radio Communications, (PIMRC'08), Cannes, France, 2008.
- [44] D. M. Shila, and T. Anjali, *Load aware traffic engineering for mesh networks*. Computer Communications, Vol. 31(7): p. 1460-1469, 2008.

- [45] G. K. Audhya, K. Sinha, S. C. Ghosh, and B. P. Sinha, *A survey on the channel assignment problem in wireless networks*. *Wireless Communications and Mobile Computing*, Vol. 11(5): p. 583-609, 2011.
- [46] K. H. Kim, and K. G. Shin, *On accurate measurement of link quality in multi-hop wireless mesh networks*. in Proceedings of the 12th ACM annual international conference on Mobile computing and networking (MobiCom'06), Los Angeles, California, USA, 2006.
- [47] M. Jain, and C. Dovrolis, *End-to-end estimation of the available bandwidth variation range*. in ACM SIGMETRICS Performance Evaluation Review, Vol. 33(1): p. 265-276, 2005.
- [48] Y. Yang, J. Wang, and R. Kravets, *Designing routing metrics for mesh networks*. In IEEE Workshop on Wireless Mesh Networks (WiMesh'05), Santa Clara, CA, USA, 2005.
- [49] M. M. E. Campista, P. M. Esposito, I. M. Moraes, L. H. M. K. Costa, O. C. M. B. Duarte, D. G. Passos, C. V. N. de Albuquerque, D. C. M. Saade, and M. G. Rubinstein, *Routing Metrics and Protocols for Wireless Mesh Networks*. *IEEE Network*, Vol. 22 (1): p. 6-12, 2008.
- [50] D. S. De Couto, D. Aguayo, B. A. Chambers, and R. Morris, *Performance of multihop wireless networks: Shortest path is not enough*. *ACM SIGCOMM Computer Communication Review*, Vol. 33(1): p. 83-88, 2003.
- [51] D. Passos, D. V. Teixeira, D. C. Muchaluat-Saade, L. C. S. Magalhaes, and C. V. N. de Albuquerque, *Mesh network performance measurements*. I2TS, Cuiabá, MT, Brazil, 2006.

- [52] C. E. Koksal and H. Balakrishnan, *Quality-aware routing metrics for time-varying wireless mesh networks*. IEEE Journal on Selected Areas in Communications, Vol. 24 (11), p. 1984–1994, 2006.
- [53] S. Keshav, *A control-theoretic approach to flow control*. SIGCOMM Computer Communication, Vol. 21(4), p. 3-15, 1991.
- [54] B. Awerbuch, D. Holmer, and R. Rubens, *The Medium Time Metric: High throughput route selection in multi-rate ad hoc wireless networks*. Springer Mobile Networks and Applications, Vol. 11(2): p. 253-266, 2006.
- [55] A. P. Subramanian, M. M. Buddhikot, and S. C. Miller, *Interference aware routing in multi-radio wireless mesh networks*. in IEEE Workshop on Wireless Mesh Networks, (WiMesh'06), Reston, Virginia, USA , 2006.
- [56] K. Kowalik, B. Keegan, and M. Davis, *Rare-resource aware routing for mesh*. in Proceedings of in International Conference on Communications, (ICC'07), Glasgow, UK, 2007.
- [57] S. Taneja, and A. Kush, *A Survey of routing protocols in mobile ad hoc networks*. International Journal of innovation, Management and technology, Vol. 1(3), p. 2010-0248, 2010.
- [58] C.E. Perkins, and E.M. Roye, *Ad-hoc on-demand distance vector routing*. in Proceedings of the Second Workshop on Mobile Computing Systems and Applications, (WMCSA'99), New Orleans, Louisiana, USA, 1999.
- [59] D. B. Johnson, D. A. Maltz, and J. Broch, *DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks*. Ad hoc networking, Addison-Wesley, Boston, MA, USA, 2001.

- [60] T. Clausen and P. Jacquet, *Optimized Link State Routing Protocol (OLSR)*. RFC 3626, IETF Network Working Group, 2003.
- [61] C. E. Perkins, and P. Bhagwat, *Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers*. ACM SIGCOMM Computer Communication Review, Vol. 24(4), p. 234-244, 1994.
- [62] V. D. Park and M. S. Corson, *A highly adaptive distributed routing algorithm for mobile wireless networks*. in Proceedings of Sixteenth Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'97), Kobe, Japan, 1997.
- [63] W. Cordeiro, E. Aguiar, W. Moreira, A. Abelém, and M. Stanton, *Providing quality of service for mesh networks using link delay measurements*. in Proceedings of 16th International Conference on Computer Communications and Networks, (ICCCN'07), Honolulu, Hawaii, USA, 2007.
- [64] S. Waharte, R. Boutaba, Y. Iraqi, and B. Ishibashi, *Routing protocols in wireless mesh networks: challenges and design considerations*. Multimedia Tools and Applications, Vol. 29(3): p. 285-303, 2006.
- [65] R. Dube, C. D. Rais, K. Y. Wang, and S. K. Tripathi, *Signal stability-based adaptive routing (SSA) for ad hoc mobile networks*. Wireless Personal Communications, Vol. 4(1): p. 36-45, 1997.
- [66] C. K. Toh, *Associativity-based routing for ad hoc mobile networks*. Wireless Personal Communications, Vol. 4(2): p. 103-139, 1997.
- [67] C. Li, A. Raba, and W. Zhao, *Stability in ATM networks*. in the Proceedings of Sixteenth Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'97), Kobe, Japan, 1997.



- [68] G. Gaertner, E. ONuallain, A. Butterly, K. Singh, and V. Cahill, *802.11 Link Quality and its Prediction -An Experimental Study*. Personal Wireless Communications, Lecture Notes in Computer Science, Vol. (3260): p. 147-163, 2004.
- [69] I. Aydin, C. Jaikao, and C. C. Shen, *Quorum-based match-making services for wireless mesh networks*. in Proceedings of the International Conference on Wireless And Mobile Computing, Networking And Communications (WiMob'05), Montreal, Canada, 2005.
- [70] K. Ramachandran, I. Sheriff, E. Belding, and K. Almeroth, *Routing Stability in Static Wireless Mesh Networks*. in Proceedings of the 8th Internatinoal Conference on Passive and Active Network Measurement (PAM'07), Louvain-la-neuve, Belgium, 2007.
- [71] MeshNet, UCSB, <http://moment.cs.ucsb.edu/meshnet/>
- [72] K. Grace, *Mobile Mesh Routing Protocol*. draft-grace-manet-mmrip-00.txt - work in progress, 2000.
- [73] M. Boushaba, and A. Hafid, *Best path to best gateway scheme for multichannel multi-interface wireless mesh networks*. in Proceedings of Wireless Communications and Networking Conference (WCNC'2011), Cancun, Mexico, 2011.
- [74] Y. Sun, E. M. Belding-Royer, and C. E. Perkins, *Internet connectivity for ad hoc mobile networks*. International Journal of Wireless Information Networks, Vol. 9(2): p. 75-88, 2002.
- [75] J. Broch, D. A. Maltz, and D. B. Johnson, *Supporting hierarchy and heterogeneous interfaces in multi-hop wireless ad hoc networks*. in Proceedings of Fourth International Symposium on Parallel Architectures, Algorithms, and Networks, (I-SPAN'99), Perth, Australia, 1999.

- [76] J. Lee, D. Kim, J. J. Garcia-Luna-Aceves, Y. Choi, J. Choi, and S. Nam, *Hybrid gateway advertisement scheme for connecting mobile ad hoc networks to the internet*. in Proceedings of the 57th IEEE Semiannual Vehicular Technology Conference, (VTC 2003-Spring), Seoul, Korea, 2003.
- [77] U. Javaid, F. Rasheed, D. E. Meddour, and T. Ahmed, *Adaptive distributed gateway discovery in hybrid wireless networks*. in Proceedings of Wireless Communications and Networking Conference, (WCNC'08), Las Vegas, Nevada, USA, 2008.
- [78] Y. Kim, Y. Jeong, M. Seo, and J. Ma, *Load-balanced mesh portal selection in wireless mesh network*. in Military Communications Conference, (MILCOM'07), Orlando, Florida, USA, 2007.
- [79] R. Kumar, M. Misra, and A. K. Sarje, *An efficient gateway discovery in ad hoc networks for internet connectivity*. in Proceedings of International Conference on Computational Intelligence and Multimedia Applications, (ICCIMA'07), Sivakasi, Tamilnadu, India, 2007.
- [80] U. Ashraf, S. Abdellatif, and G. Juanolet, *Gateway selection in backbone wireless mesh networks*. in Proceedings of Wireless Communications and Networking Conference, (WCNC'09), Budapest, Hungary, 2009.
- [81] S. J. Lee, and M. Gerla, *Dynamic load-aware routing in ad hoc networks*. in Proceedings of International Conference on Communications, (ICC'01), Helsinki, Finland, 2001.
- [82] V. Saigal, A. K. Nayak, S. K. Pradhan, and R. Mall, *Load balanced routing in mobile ad hoc networks*. Computer Communications, Vol. 27(3): p. 295-305, 2004.

- [83] K. Ramachandran, M. Buddhikot, G. Chandranmenon, S. Miller, E. Belding-Royer, and K. Almeroth, *On the design and implementation of infrastructure mesh networks*. In IEEE Workshop on Wireless Mesh Networks (WiMesh'05), Santa Clara, California, USA, 2005.
- [84] H. Li, Y. Cheng, C. Zhou, and W. Zhuang, *Minimizing end-to-end delay: a novel routing metric for multi-radio wireless mesh networks*. in Proceedings of 28th Annual Joint Conference of the IEEE Computer and Communications Societies, (INFOCOM 2009), Rio de Janeiro, Brazil, 2009.
- [85] R. A. Calvo, J. P. Campo, *Adding Multiple Interface Support in NS-2*, <http://personales.unican.es/aguerocr/>, 2007
- [86] A. Beljadid, A. Hafid, M. Gendreau, *Optimal design of broadband wireless mesh networks*. in Proceedings of Global Telecommunications Conference, (GLOBECOM'07), Washington, DC, USA, 2007.
- [87] D. Benyamina, A. Hafid, M. Gendreau, *Design of scalable and efficient multi-radio wireless networks*. ACM-Springer Journal of Wireless Networks, Vol 18(1): p. 75-94, 2012.
- [88] A. Boukerche, *Performance evaluation of routing protocols for ad hoc wireless networks*. Mobile Networks and Applications, Vol. 9(4): p.333-342, 2004.
- [89] R. Fantacci, D. Tarchi, and A. Tassi, *A novel routing algorithm for mobile pervasive computing*. in Proceedings of Global Telecommunications Conference, (GLOBECOM'2010), Miami, FL, USA, 2010.

- [90] R. Fantacci, D.Tarchi and A.Tassi, *Wireless Communication Protocols for Distributed Computing Environments, Advanced Trends in Wireless Communications*, Mutamed Khatib (Ed.), ISBN: 978-953-307-183-1, 2011.
- [91] S. M. Das, Y. Wu, R. Chandra, and Y. C. Hu, *Context based routing: Technique, applications and experience*. in USENIX NSDI, 2008.
- [92] L. Ma and M.K. Denko, *A Routing Metric for Load-Balancing in Wireless Mesh Networks*. in Proceedings of Advanced Information Networking and Applications Workshop (AINA'07), Niagara Falls, Canada, 2007.
- [93] K. Shah, M. Di Francesco, M. Kumar, *Distributed resource management in wireless sensor networks using reinforcement learning*. ACM-Springer Journal of Wireless Networks, p. 1-20, 2012.
- [94] J. Boyan and M. Littman, *Packet routing in dynamically changing networks: A reinforcement learning approach*. in Proceedings Advances in Neural Information Processing Systems (NIPS'1994), Denver, CO, USA, 1994.
- [95] A.Belbekkouche, A.Hafid, M.Gendreau, *Novel reinforcement learning-based approaches to reduce loss probability in buffer-less OBS networks*. Computer Networks, Vol. 53(12), p. 2091-2105, 2009.
- [96] C. Wu, K. Kumekawa, and T. Kato, *Distributed Reinforcement Learning Approach for Vehicular Ad Hoc Networks*. IEICE transactions on communications, Vol. 93(6), p. 1431-1442, 2010.
- [97] K. S. P. Beyens, M. Peeters and A. Nowe, *Routing with compression in wireless sensor networks: a q-learning approach*. in Proceedings of Fifth European Workshop on Adaptive Agents and Multi-Agent Systems (AAMAS'2005), Paris, France, 2005.

- [98] M. Lee, D. Marconett, X. Ye, S. J. Yoo. *Cognitive Network Management with Reinforcement Learning for Wireless Mesh Networks*. in Proceedings of the 7th IEEE International Workshop on IP Operations & Management (IPOM'07), San José, California, USA, 2007.
- [99] A. F. Atlasis, N. H. Loukas, and A. V. Vasilakos, *The use of learning algorithms in ATM networks call admission control problem: a methodology*. Computer Networks Vol. 34(3): p. 341-353, 2000.
- [100] A. Vasilakos, M. P. Saltouros, A. F. Atlasis, and W. Pedrycz, *Optimizing QoS routing in hierarchical ATM networks using computational intelligence techniques*. IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, Vol. 33(3): p. 297-312, 2003.
- [101] A. Vasilakos, C. Ricudis, K. Anagnostakis, W. Pedryca, A. Pitsillides, *Evolutionary-fuzzy prediction for strategic QoS routing in broadband networks*. IEEE World Congress on Computational Intelligence, (WCCI'98), Anchorage, Alaska, USA, 1998.
- [102] Y. Zeng, K. Xiang, D. Li, and A. V. Vasilakos, *Directional routing and scheduling for green vehicular delay tolerant networks*. Wireless Networks, Vol. 19(2): p.161-173. 2013.
- [103] L.M. Gambardella, M. Dorigo, *Ant-Q: A reinforcement learning approach to the traveling salesman problem*. in Proceedings of the 11th International Conference on Machine Learning, Morgan Kaufmann, San Francisco, CA, 1995.
- [104] M. Dorigo, G. D. Caro, and L. M. Gambardella, *Ant algorithms for discrete optimization*. Artificial life, Vol. 5(2), p. 137–172, 1999.

- [105] D. Subramanian, P. Druschel and J. Chen, *Ants and reinforcement learning: a case study in routing in dynamic networks*. in Proceedings of the Fifteenth International Joint Conference on Artificial Intelligence (IJCAI'97), San Francisco, CA, 1997.
- [106] H. Iima, Y. Kuroe and S. Matsuda, *Swarm reinforcement learning method based on ant colony optimization*. in Proceedings of International Conference on Systems Man and Cybernetics (SMC'2010), Istanbul, TURKEY, 2010.
- [107] A. Forster, *Machine Learning Techniques Applied to Wireless Ad-Hoc Networks: Guide and Survey*. in Proceedings of the 3rd International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), Melbourne, Australia, 2007.
- [108] L. P. Kaelbling, L. M. Littman, and A. W. Moore, *Reinforcement learning: A survey*. Journal of Artificial Intelligence Research, Vol. 4, p. 237-285, 1996.
- [109] K.M. Sim and W.H. Sun, *Ant colony optimization for routing and load-balancing: Survey and new directions*. IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, Vol. 33(5), p. 560-572, 2003.
- [110] C-C.Shen, Z.Huang, C.Jaikaeo, *Ant-Based Distributed Topology Control Algorithms for Mobile Ad hoc Networks*. ACM-Springer Journal of Wireless Networks, Vol. 11 (3): p. 299-317, 2005.
- [111] J.Xu, W.Liu, Z.Yang, J.Chen and X.Chen, *A Delay-Aware Routing Metric for Multi-Radio Multi-Channel Wireless Mesh Networks*. in Proceedings of the 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM'2010), Chengdu, China, 2010

- [112] P.D. Christopher and J.C.H. Watkins, *Q-Learning*. Machine Learning, Vol. 8, p. 279–292, 1992.
- [113] R.S. Sutton and A.G. Barto, *Reinforcement Learning: An Introduction*. The MIT Press, Cambridge, Massachusetts, 1998.
- [114] Intersil HFA3861B Chip Specification, <http://www.chipdocs.com/pndecoder/datasheets/INTRS/HFA3861B.html>
- [115] B. Ye, A. P. Jayasumana, and N. M. Piratla, *On monitoring of end-to-end packet reordering over the Internet*. in Proceedings of the International conference on Networking and Services, (ICNS'06). Silicon Valley, USA, 2006.
- [116] H. Zhang, L. Sang, and A. Arora, *On the convergence and stability of data-driven link estimation and routing in sensor networks*. ACM Transactions on Autonomous and Adaptive Systems (TAAS), Vol. 4(3), p. 18. 2009.
- [117] R. Clausius, *Annalen der Physik und Chemie*. 79: p. 368-397, 1850.
- [118] L. Boltzmann. *Über die Beziehung zwischen dem zweiten Hauptsatze der mechanischen Wärmetheorie und der Wahrscheinlichkeitsrechnung respective den Sätzen über das Wärmegleichgewicht*. Wiener Berichte, Vol. 2 (76), p. 373–435, 1877.
- [119] E. C. Shannon and W. Weaver, *The Mathematical Theory of Communication*, Urbana, IL: University of Illinois Press Vol. 19 (7), 1949.
- [120] J. L. Lu, F. Valois, M. Dohler, and D. Barthel, *Quantifying Organization by Means of Entropy*. IEEE Communication Letters, Vol. 12 (3): p. 185-187, 2008.
- [121] K. Sneppen, A. Trusina, and M. Rosvall, Hide-and-seek on complex networks. EPL (Europhysics Letters), Vol. 69(5): p. 853-859, 2007.

- [122] W. Wei, B. Wang, C. Zhang, J. Kurose, and D. Towsley, *Classification of access network types: Ethernet, wireless LAN, ADSL, cable modem or dialup?*. Computer Networks Journal. Vol. 52 (17): p. 3205-3217, 2008.
- [123] Hua Chen, Baolin Sun, and Yue Zeng, *QoS multicast routing algorithm in MANET: an entropy-based GA*. Computational Intelligence. Vol. 4114, p. 1279-1289, 2006.
- [124] B. An, J. S. Lee, and N. S. Kim, *An Entropy-based Routing Protocol using Mobility in Mobile Ad-hoc Wireless Sensor Networks*. in Proceedings of the 11th International Conference on Advanced Communication Technology, (ICACT 2009), Gangwon-Do, South Korea, 2009.
- [125] C. Gui, B. Sun, and C. Xia, *An Entropy-Based Long-Life Multipath Routing Algorithm in MANET*. in Proceedings of the Fourth International Conference on Natural Computation, (ICNC'08), Jinan, China, 2008.
- [126] J. Lian, L. Li, X. Zhu, and B. Sun, *A QoS-aware routing protocol based on entropy for mobile ad hoc network*. in Proceedings of the 4th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM'08), Dalian, China, 2008.
- [127] A. Forestiero, C. Mastroianni, and G. Spezzano, *So-Grid: A self-organizing Grid featuring bio-inspired algorithms*. ACM Transactions on Autonomous and Adaptive Systems (TAAS), Vol. 3(2), Article. 5, 2008.
- [128] G. Chen, A. Sarrafzadeh, C. P. Low, and L. Zhang, *A self-organization mechanism based on cross-entropy method for P2P-like applications*, ACM Transactions on Autonomous and Adaptive Systems (TAAS), Vol. 5(4), Article 15, 2010.



- [129] C. F. Huang, H. W. Lee, and Y. C. Tseng, *A two-tier heterogeneous mobile Ad Hoc network architecture and its load-balance routing problem*. Journal of Mobile Networks and Applications, Vol 9(4): p. 379-391, 2004.
- [130] J. Shin, H. Lee, J. Na, A. Park, and S. Kim, *Load balancing among internet gateways in ad hoc networks*. in Proceeding of 62nd Vehicular Technology Conference (VTC'05), Dallas, Texas, USA, 2005.
- [131] F. A. Cowell, *Measuring Inequality: Techniques For The Social Sciences*, New York: John Wiley, 1977.
- [132] H. Shi, H. Sethu, and S. S. Kanhere, *An evaluation of fair packet schedulers using a novel measure of instantaneous fairness*. Computer communications, Vol 28(17): p. 1925-1937, 2005.
- [133] R. N. Rao, and G. Kesidis, *On the Relation Between Capacity and Number of Sinks in an Sensor Network*. In Global Telecommunications Conference, 2006. (GLOBECOM'06), San Francisco, California, USA, 2006.
- [134] A. Neishaboori, and G. Kesidis, *Sinr-sensitive routing in wireless 802.11 mesh networks*. in Proceedings of the 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems, (MASS 2008), Atlanta, Georgia, 2008.