Performances des couches MAC dans les réseaux sans fil ad hoc : problèmes et solutions

Tahiry Razafindralambo

▶ **To cite this version:**

Tahiry Razafindralambo. Performances des couches MAC dans les réseaux sans fil ad hoc : problèmes et solutions. Réseaux et télécommunications [cs.NI]. INSA de Lyon, 2007. Français. NNT : 2007ISAL0103 . tel-00532658

HAL Id: tel-00532658

https://theses.hal.science/tel-00532658

Submitted on 4 Nov 2010

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

N d'ordre 2007-ISAL-0103 Année 2007

Thèse

présentée devant
L'Institut National des Sciences Appliquées de Lyon
pour l'obtention
du Grade de Docteur

présentée et soutenue publiquement
le 03 Décembre 2007

par

Mr RAZAFINDRALAMBO Tahiry

Performances des couches MAC dans les réseaux sans fil *ad hoc* : problèmes et solutions

Après avis de :

Monsieur le Professeur M. CONTI	IIT-CNR Pise
Monsieur le Professeur A. DUDA	Institut National Polytechnique de Grenoble
Monsieur le Professeur D. SIMPLOT-RYL	Université Lille 1

Soutenue devant :

Monsieur A. DUDA	Institut National Polytechnique de Grenoble
Monsieur S. FDIDA	Université Pierre et Marie Curie Paris 6
Madame I. GUÉRIN LASSOUS	Université de Lyon
Monsieur L. REYNAUD	France Télécom R&D
Monsieur D. SIMPLOT-RYL	Université Lille 1
Monsieur S. UBÉDA	INSA Lyon

Les travaux présentés dans ce mémoire ont été réalisés au laboratoire CITI sous la direction du Pr. Isabelle GUÉRIN LASSOUS
et financés par France Télécom R&D

INSA Direction de la Recherche - Ecoles Doctorales 2007

SIGLE	ECOLE DOCTORALE	NOM ET COORDONNEES DU RESPONSABLE
CHIMIE	**CHIMIE DE LYON** **http://sakura.cpe.fr/ED206** M. Jean Marc LANCELIN Insa : R. GOURDON	M. Jean Marc LANCELIN Université Claude Bernard Lyon 1 Bât CPE 43 bd du 11 novembre 1918 69622 VILLEURBANNE Cedex Tél : 04.72.43 13 95 Fax : lancelin@hikari.cpe.fr
E.E.A.	**ELECTRONIQUE, ELECTROTECHNIQUE, AUTOMATIQUE** **http://www.insa-lyon.fr/eea** M. Alain NICOLAS Insa : D. BARBIER ede2a@insa-lyon.fr Secrétariat : M. LABOUNE AM. 64.43 – Fax : 64.54	M. Alain NICOLAS Ecole Centrale de Lyon Bâtiment H9 36 avenue Guy de Collongue 69134 ECULLY Tél : 04.72.18 60 97 Fax : 04 78 43 37 17 eea@ec-lyon.fr Secrétariat : M.C. HAVGOUDOUKIAN
E2M2	**EVOLUTION, ECOSYSTEME, MICROBIOLOGIE, MODELISATION** **http://biomserv.univ-lyon1.fr/E2M2** M. Jean-Pierre FLANDROIS Insa : S. GRENIER	M. Jean-Pierre FLANDROIS CNRS UMR 5558 Université Claude Bernard Lyon 1 Bât G. Mendel 43 bd du 11 novembre 1918 69622 VILLEURBANNE Cédex Tél : 04.26 23 59 50 Fax 04 26 23 59 49 06 07 53 89 13 e2m2@biomserv.univ-lyon1.fr
EDIIS	**INFORMATIQUE ET INFORMATION POUR LA SOCIETE** http://ediis.univ-lyon1.fr M. Alain MILLE Secrétariat : I. BUISSON	M. Alain MILLE Université Claude Bernard Lyon 1 LIRIS - EDIIS Bâtiment Nautibus 43 bd du 11 novembre 1918 69622 VILLEURBANNE Cedex Tél : 04.72. 44 82 94 Fax 04 72 44 80 53 ediis@liris.cnrs.fr - alain.mille@liris.cnrs.fr
EDISS	**INTERDISCIPLINAIRE SCIENCES-SANTE** M. Didier REVEL Insa : M. LAGARDE	M. Didier REVEL Hôpital Cardiologique de Lyon Bâtiment Central 28 Avenue Doyen Lépine 69500 BRON Tél : 04.72.35 72 32 Fax : Didier.revel@creatis.uni-lyon1.fr
	MATERIAUX DE LYON M. Jean Marc PELLETIER Secrétariat : C. BERNAVON 83.85	M. Jean Marc PELLETIER INSA de Lyon MATEIS Bâtiment Blaise Pascal 7 avenue Jean Capelle 69621 VILLEURBANNE Cédex Tél : 04.72.43 83 18 Fax 04 72 43 85 28 Jean-marc.Pelletier@insa-lyon.fr
Math IF	**MATHEMATIQUES ET INFORMATIQUE FONDAMENTALE** M. Pascal KOIRAN Insa : G. BAYADA	M.Pascal KOIRAN Ecole Normale Supérieure de Lyon 46 allée d'Italie 69364 LYON Cédex 07 Tél : 04.72.72 84 81 Fax : 04 72 72 89 69 Pascal.koiran@ens-lyon.fr Secrétariat : Fatine Latif - latif@math.univ-lyon1.fr
MEGA	**MECANIQUE, ENERGETIQUE, GENIE CIVIL, ACOUSTIQUE** M. Jean Louis GUYADER Secrétariat : M. LABOUNE PM : 71.70 –Fax : 87.12	M. Jean Louis GUYADER INSA de Lyon Laboratoire de Vibrations et Acoustique Bâtiment Antoine de Saint Exupéry 25 bis avenue Jean Capelle 69621 VILLEURBANNE Cedex Tél :04.72.18.71.70 Fax : 04 72 18 87 12 mega@lva.insa-lyon.fr
SSED	**SCIENCES DES SOCIETES, DE L'ENVIRONNEMENT ET DU DROIT** Mme Claude-Isabelle BRELOT Insa : J.Y. TOUSSAINT	Mme Claude-Isabelle BRELOT Université Lyon 2 86 rue Pasteur 69365 LYON Cedex 07 Tél : 04.78.69.72.76 Fax : 04.37.28.04.48 Claude-isabelle.brelot@univ-lyon2.fr

Remerciements

à Dina

Mais aussi à tous les autres qui se reconnaîtront...
De toute façon je l'aurai déjà fait de vive voix

Table des matières

1 Introduction **1**
- 1.1 Contexte . . . 2
- 1.2 Organisation du document . . . 3

2 Présentation de 802.11 et de quelques scénarii *ad hoc* **5**
- 2.1 Description générale . . . 6
- 2.2 Les contextes d'utilisation de 802.11 . . . 7
- 2.3 La méthode d'accès DCF . . . 8
- 2.4 Quelques problèmes de la méthode d'accès . . . 9
  - 2.4.1 Les stations cachées et le mécanisme de RTS/CTS . . . 9
  - 2.4.2 Les stations cachées asymétriques . . . 10
  - 2.4.3 Les trois paires . . . 11
- 2.5 Remarques . . . 11

3 Une évaluation analytique de IEEE 802.11 **13**
- 3.1 État de l'art . . . 14
- 3.2 Méthodologie et modèle de base . . . 16
  - 3.2.1 Les algèbres processus : PEPA . . . 16
  - 3.2.2 Méthodologie de modélisation . . . 19
  - 3.2.3 Le modèle . . . 21
- 3.3 Étude de cas : Performance et équité . . . 23
  - 3.3.1 Les topologies . . . 24
  - 3.3.2 Les algorithmes de backoff . . . 32
  - 3.3.3 Les métriques . . . 33
  - 3.3.4 Résultats . . . 35
- 3.4 Conclusions et travaux futurs . . . 42
  - 3.4.1 Modèle . . . 42
  - 3.4.2 Conclusions . . . 43
  - 3.4.3 Travaux futurs . . . 44

4 MadMac : Un protocole efficace et équitable **47**
- 4.1 État de l'art . . . 48
- 4.2 La capacité et l'équité . . . 51
  - 4.2.1 L'équité . . . 51
  - 4.2.2 La capacité, la capacité équitable . . . 52
- 4.3 MadMac . . . 53
  - 4.3.1 Le fonctionnement de base . . . 54
  - 4.3.2 La gestion des collisions . . . 56
  - 4.3.3 Le monopole du canal . . . 58
  - 4.3.4 Résumé . . . 58
  - 4.3.5 Remarques . . . 61
- 4.4 Performances . . . 61
  - 4.4.1 Description des protocoles de comparaison . . . 61
  - 4.4.2 Cellule de communication . . . 62
  - 4.4.3 Les stations cachées . . . 64
  - 4.4.4 Les trois paires . . . 66

4.4.5 Les stations cachées asymétriques . . . 67
4.4.6 Simulations complémentaires . . . 69
4.5 Conclusion . . . 72

5 Influence de la couche MAC sur les couches supérieures 75
5.1 Introduction . . . 76
5.2 La découverte de voisinage . . . 76
5.2.1 Description . . . 76
5.2.2 Paramètres de performance . . . 77
5.3 Évaluation de performance . . . 77
5.3.1 File d'attente $M/D/1/K$ . . . 78
5.3.2 Simulations . . . 81
5.4 Conclusion . . . 85

6 PAS : une solution équitable dans le temps 87
6.1 Introduction . . . 88
6.2 L'anomalie de performance . . . 89
6.3 État de l'art . . . 89
6.3.1 La fragmentation de paquet . . . 90
6.3.2 Approche basée sur l'adaptation de la fenêtre de contention . . . 91
6.3.3 Approche basée sur l'agrégation des paquets . . . 91
6.4 PAS : *Performance Anomaly Solution* . . . 92
6.4.1 Calcul du temps d'agrégation . . . 92
6.4.2 L'émission de paquets . . . 93
6.4.3 Autres mécanismes . . . 94
6.5 Analyse de performance . . . 95
6.5.1 Efficacité . . . 95
6.5.2 Équité . . . 96
6.5.3 Résultats analytiques . . . 97
6.6 Résultats de simulations . . . 98
6.6.1 Simulations basiques . . . 98
6.6.2 Réactivité . . . 100
6.6.3 Délais . . . 100
6.6.4 Effet de α . . . 103
6.6.5 Effet de t_rate . . . 104
6.6.6 Comparaison avec d'autres solutions . . . 104
6.7 Simulations spécifiques au couple 802.11/PAS . . . 107
6.7.1 Les stations cachées . . . 107
6.7.2 Flux TCP asymétriques . . . 108
6.7.3 Contexte hétérogène . . . 109
6.7.4 Un premier scénario *ad hoc* . . . 109
6.8 Conclusion . . . 111

7 Conclusion et Perspectives 113
7.1 Conclusion . . . 114
7.2 Perspectives . . . 115

Bibliographie 119

Table des figures

2.1 802.11 : Architecture et insertion dans la pile OSI. 6
2.2 802.11 : Mode de fonctionnement 7
2.3 802.11 : *Distributed Coordination Function* 8
2.4 802.11 : Les stations cachées 9
2.5 802.11 : Les stations cachées asymétriques 10
2.6 802.11 : Les trois paires 11

3.1 PEPA : Graphe de dérivation d'un modèle de file $M/M/1/N$ 18
3.2 PEPA : Chaîne de Markov associé à une file $M/M/1/N$ 19
3.3 PEPA : Méthodologie de découpage d'un réseaux en composantes 20
3.4 PEPA : Validation par simulation du modèle PEPA (deux stations à portée de communication) 24
3.5 PEPA : La topologie des stations cachées (Rappel) 25
3.6 PEPA : Validation par simulation du modèle PEPA (stations cachées) 26
3.7 PEPA : La topologie des stations cachées asymétriques 27
3.8 PEPA : Validation par simulation du modèle PEPA (stations cachées asymétriques) 29
3.9 PEPA : La topologie des 3 paires 29
3.10 PEPA : Validation par simulation du modèle PEPA (3 paires) 31
3.11 PEPA : Validation de la métrique d'équité α_i 35
3.12 PEPA : Résultats de performance (deux stations à portée de communication) 37
3.13 PEPA : Résultats de performance (stations cachées) 38
3.14 PEPA : Distribution sur les états du backoff (stations cachées) 39
3.15 PEPA : Résultats de performance (stations cachées asymétriques) 40
3.16 PEPA : α_i (stations cachées asymétriques) 41
3.17 PEPA : Résultats de performance (3*paires*) 43

4.1 Classification des protocoles MAC 49
4.2 Illustration du mécanisme de base de MadMac 56
4.3 Illustration du mécanisme de MadMac pour l'évitement de collision 58
4.4 Performance de MadMac sur une cellule de communication 63
4.5 Performance de MadMac sur le scénario des stations cachées 64
4.6 Performance de MadMac sur le scénario des stations cachées avec taille de paquet aléatoire . 65
4.7 Performance de MadMac sur le scénario des stations cachées multiples 65
4.8 Différent ordonnancement sur les 3 paires 67
4.9 Performance de MadMac sur le scénario des trois paires 68
4.10 Performance de MadMac sur plusieurs paires parallèles 68
4.11 Performance de MadMac sur le scénario des stations cachées asymétriques 69
4.12 MadMac : Résultats de performance sur des topologies aléatoire 70
4.13 MadMac : Résultats de performance sur une chaîne 71
4.14 MadMac topologie en grille 72
4.15 Performance de MadMac sur une grille 72

5.1 HELLO : Résultats d'analyse d'un protocole $HELLO$ avec une file $M/D/1/K$ 79
5.2 HELLO : Analyse du protocole $HELLO$ avec une file $M/D/1/K$ (différente intensité) 80
5.3 HELLO : MadMac vs. 802.11 - Résultats de simulation pour $K = 10$ 81
5.4 HELLO : MadMac vs. 802.11 - Résultats de simulation pour $K = 20$ et $K = 30$ 82
5.5 HELLO : MadMac vs. 802.11 - Résultats de simulation les stations cachées 82

5.6 HELLO : MadMac vs. 802.11 - Résultats de simulation les stations cachées avec des flux UDP 83
5.7 HELLO : MadMac vs. 802.11 - Résultats de simulation sur une cellule dense 1 flux UDP . . . 84
5.8 HELLO : MadMac vs. 802.11 - Résultats de simulation sur une cellule dense avec 4 flux UDP 85
5.9 HELLO : MadMac vs. 802.11 - Résultats de simulation sur une cellule dense avec 8 flux UDP 85

6.1 Effets de l'anomalie de performance dans 802.11b 90
6.2 PAS : Proportion du temps d'occupation pour deux stations 97
6.3 PAS vs. IEEE 802.11 in : Simulations avec deux stations 99
6.4 PAS vs. IEEE 802.11 in : Simulations avec quatre stations. 99
6.5 PAS vs. IEEE 802.11 : Simulations avec différentes densités de cellule 101
6.6 PAS vs. IEEE 802.11 : Utilisation du mécanisme ARF (*Auto Rate Fallback*). 102
6.7 PAS : Fonction de distribution cumulée des temps inter-rafales. 102
6.8 PAS : Influence de α sur deux stations. 103
6.9 PAS : Influence de α sur quatre stations. 103
6.10 PAS : influence de t_rate sur deux stations. 104
6.11 PAS : Débit agregé en fonction de la taille des paquets. 105
6.12 PAS : index d'équité en fonction de la taille des paquets. 105
6.13 PAS vs Modification de backoff. 106
6.14 PAS vs Fragmentation de paquets. 106
6.15 PAS vs Temps d'agrégation fixe. 107
6.16 PAS avec RTS/CTS sur les stations cachées. 108
6.17 PAS avec RTS/CTS et des tailles de paquets aléatoires. 108
6.18 PAS : scénario des flux TCP asymétriques 109
6.19 PAS : résultats sur les flux TCP asymétriques. 109
6.20 L'occupation du médium perçu par la paire centrale. 110

Liste des tableaux

4.1 Débit par stations pour une cellule de communication 63

6.1 PAS : résultats analytiques 98
6.2 PAS : Rafales 102
6.3 PAS vs. Temps d'agrégation fixe 107
6.4 PAS : dans un contexte hétérogène 110
6.5 PAS : résultats sur les trois paires 111

1 Introduction

« On lit plus vite quand on ne cherche pas à comprendre »

Bill Watterson,
Extrait de la bande dessinée Calvin et Hobbes.

1.1 Contexte

Depuis plusieurs années, la standardisation des réseaux sans fil connaît une activité et un essor fulgurant. Depuis Hiperlan [22] en passant par Bluetooth [43], Zigbee [43], Wimax [42] et 802.11 [40] (pour n'en citer que quelques uns), pratiquement tous les standards des réseaux sans fil suivent une évolution technologique. Chacun de ces standards tente de répondre à un besoin spécifique qui peut être le débit, l'économie d'énergie, etc. Parmi tous ces standards, 802.11 a su s'imposer comme le standard de fait des réseaux locaux sans fil.

La norme 802.11 propose deux modes de fonctionnement. Dans le premier cas, les communications entre stations doivent impérativement passer par un point d'accès central. Ce dernier gère les accès au canal de communication de chacune des stations. Ce mode de fonctionnement de 802.11 est connu sous le nom de PCF (*Point Coordination Function*). Pour le deuxième cas de fonctionnement, les stations utilisent un accès aléatoire, distribué et décentralisé, au canal de communication. Dans la norme 802.11, ce mode d'accès est connu sous le nom de DCF (*Distributed Coordination Function*).

La proposition du mode DCF dans la norme 802.11 a accru l'étude par la communauté scientifique d'un réseau plus ou moins nouveau. Ce réseau s'appuyant sur les propriétés distribuées et décentralisées du mode DCF de 802.11 a comme particularité son absence totale d'infrastructure fixe. D'un point de vue historique, c'est l'interêt de l'agence de défense américaine DARPA (*Defense Advanced Research Projects Agency*) pour les réseaux sans fil et l'apparition du protocole ALOHA [1] dans les années 1970 qui ont eu pour conséquence le développement des réseaux radio multisauts tels que les PRNETs (*Packet Radio Network*). L'un des intérêts principaux de ce type de réseau était sa facilité de déploiement : après son installation, le système devait pouvoir s'auto-configurer. Le réseau composé de stations, nœuds ou terminaux mobiles devait aussi pouvoir, si nécessaire, relayer les informations entre stations qui ne sont pas à portée directe de communication radio. Ce type de réseaux est maintenant plus connu sous le nom de réseaux *ad hoc*. La principale caractéristique d'un réseau *ad hoc* est donc l'absence d'infrastructure mais aussi l'absence d'entité centrale. Un réseau *ad hoc* doit pouvoir s'adapter à l'apparition et à la disparition des stations automatiquement tout en maintenant le service réseau. Si les stations sont mobiles, alors le réseau *ad hoc* est appelé MANET (*Mobile Ad hoc NETworks*). La popularité de 802.11 combinée à des idées d'applications autres que militaires pour les réseaux *ad hoc* [70, 64] ont fortement contribué à l'étude de ces réseaux par la communauté scientifique.

Dans les années 1990, le routage était l'une des problématiques principales des réseaux *ad hoc*. Plusieurs protocoles de routage ont été proposés et certains d'entre eux ont été standardisés. La grande majorité des ces protocoles de routage a été proposée en supposant que la technologie sans fil sous-jacente, le mode DCF de 802.11 étant souvent sous-entendu, fournissait des performances proches de l'optimale. Des travaux datant de la fin des années 90 et du début des années 2000 ont cependant montré que les performances de 802.11 étaient loin d'être optimales.

La littérature s'accorde à dire que les problèmes rendant 802.11 sous-optimal proviennent de la sous-couche MAC implémentée. Ces problèmes sont indépendants de la couche physique utilisée. La couche MAC, comme suggérée dans le modèle OSI [75], a un rôle principal : fournir une transmission fiable entre deux stations du réseau. La couche MAC doit fournir une correction ou une détection d'erreurs pouvant apparaître au niveau de la couche physique. De plus, la couche MAC est aussi responsable de la résolution de conflit pouvant survenir quand différentes stations tentent d'accéder au médium de communication en même temps. C'est donc le rôle de la couche MAC de résoudre les problèmes liés à la mobilité, l'asymétrie des liens, etc., ces problèmes provoquant souvent, la perte de paquets [2]. Les deux objectifs principaux de la couche MAC sont de fournir un accès au médium de communication à la station lui permettant de transmettre sa trame et de rendre cette

transmission fiable. Dans les réseaux filaires de type ethernet, l'accès et la fiabilité sont fournis par le protocole CSMA. Dans un contexte sans fil, et plus spécifiquement dans 802.11, l'accès et la fiabilité reposent sur CSMA/CA une méthode d'accès utilisant CSMA, un système d'acquittement explicite et un algorithme d'évitement de collision. Des travaux de la littérature montrent que la méthode d'accès CSMA/CA telle qu'elle est implémentée dans 802.11 ne peut pas fournir un accès fiable (accès sans collision) aux stations dans tous les cas de figure ; et dans certains cas particuliers, ne peut même pas fournir un accès à toutes les stations.

Depuis la fin des années 90 jusqu'au début de cette thèse, début 2005, plusieurs solutions ont été proposées pour résoudre les problèmes liés à l'accès fiable que doit fournir la couche MAC des réseaux sans fil et *ad hoc*. Les solutions issues de la littérature peuvent être classifiées dans deux grandes catégories. La première catégorie contient les solutions résolvant le problème de fiabilité en empêchant certaines stations d'émettre. Cette première catégorie de solution revient à fournir à un sous-ensemble de stations un accès fiable quasi permanent au médium radio. Ce sous-ensemble de stations est choisi de telle sorte que les transmissions de ces stations ne provoquent aucune collision entre elles. La seconde catégorie propose d'offrir un accès à toutes les stations en mettant en place des mécanismes plus ou moins complexes permettant une transmission sans collision de toutes les stations. Pour ce faire, les transmissions de chaque station sont ordonnancées pour éviter les collisions.

Les deux catégories de solutions proposées dans la littérature ont deux objectifs bien distincts et souvent opposés. Dans la première catégorie, les solutions cherchent à favoriser les stations étant dans les meilleures conditions pour transmettre correctement leurs trames. En favorisant ces stations, le protocole MAC permet ainsi d'augmenter l'efficacité du réseau. Dans la seconde catégorie, les solutions cherchent à fournir un accès à toutes les stations. En cherchant à fournir cet accès à toutes les stations, ces solutions sont plus équitables mais souvent moins efficaces que les solutions de la première catégorie.

Selon nous, les propositions de couche MAC faites dans la littérature se placent soit dans une catégorie, soit dans l'autre. Ces solutions ont pour objectif d'être soit efficaces ou équitables. Aucune solution, du moins au début de cette thèse et à notre connaissance, ne répondait au compromis équité-efficacité mis en avant par la littérature. L'objectif principal de cette thèse a donc été de concevoir un protocole MAC s'insérant dans une nouvelle catégorie de protocole équitable et efficace pour les réseaux *ad hoc*.

1.2 Organisation du document

Dans le second chapitre de cette thèse nous présentons le protocole MAC implémenté dans 802.11. Nous donnons quelques détails sur la méthode d'accès DCF et les mécanismes utilisés par 802.11 pour l'accès au médium. La fin de ce second chapitre est consacrée à la description de topologies de réseaux *ad hoc* identifiées dans la littérature comme pathologiques pour la méthode d'accès de 802.11.

Avant de nous intéresser aux protocoles MAC, nous avons étudié 802.11 d'un point de vue théorique. Bien que des études similaires existent dans la littérature, ces études ne nous ont pas apporté les intuitions nécessaires à la conception d'une couche MAC efficace et équitable. Dans le troisième chapitre, nous présentons une étude théorique des performances de 802.11. Cette étude théorique s'appuie sur les algèbres de processus stochastique. Ce chapitre a un double objectif. L'objectif principal est d'étudier le comportement de 802.11 dans des cas pathologiques bien connus mettant à défaut la méthode d'accès DCF de 802.11. Ces cas pathologiques sont présentés par des scénarii

d'utilisation simple de réseaux *ad hoc*. Nous nous sommes particulièrement attachés à étudier les performances de 802.11 tant d'un point de vue quantitatif que qualitatif sur ces scénarii. Le second objectif à été de proposer un modèle générique pour l'évaluation des performances de réseaux *ad hoc*. Pour ce faire, nous avons exploité l'approche compositionnelle proposée par les algèbres de processus pour concevoir un modèle aussi bien extensible que réutilisable pour faciliter l'étude des réseaux *ad hoc*.

Dans le quatrième chapitre, nous proposons MadMac, un protocole MAC efficace et équitable s'appuyant sur 802.11. MadMac découle des résultats théoriques obtenus dans le précédent chapitre. L'idée principale de MadMac est de fournir de l'équité entre les stations d'un réseau *ad hoc*. Cependant, pour concevoir ce protocole, nous nous sommes imposés quelques restrictions. La première et celle qui nous paraissait la plus importante, c'est la réduction de la surcharge protocolaire. Nous avons voulu, pour MadMac, aucun échange de messages comportant les informations nécessaires pour l'obtention d'une équité donnée. Ainsi, nous avons préféré que MadMac soit moins performant d'un point de vue de l'équité plutôt que de lui apporter des informations. Ce choix devait aussi permettre à MadMac d'être plus performant concernant la transmission des données utiles. La deuxième contrainte, moins forte, que nous nous sommes imposés est la simplicité. Nous avons voulu que les mécanismes de MadMac soient les plus simples possible et réutilisent au maximum les mécanismes déjà utilisés dans 802.11.

Le cinquième chapitre aurait pu être inclus dans le quatrième, mais nous avons voulu les séparer dans un souci d'équilibre. Dans ce chapitre, nous étudions l'impact des propriétés d'un protocole MAC sur un protocole de la couche 3. Nous évaluons les performances d'un protocole de découverte de voisinage en fonction de la couche MAC sous-jacente. Ce chapitre nous montre l'utilité ou non d'avoir des performances particulières au niveau de la couche MAC. MadMac et 802.11 sont évalués comme couche MAC sous-jacente à un protocole de découverte de voisinage. Ce chapitre présente les derniers résultats que nous avons obtenus durant cette thèse. Bien que ces résultats ne soient pas complètement aboutis, ils nous ont paru suffisamment intéressants pour faire l'objet d'un chapitre entier.

Le sixième chapitre est consacré à un problème d'équité particulier dans un réseau local sans fil. Dans ce chapitre, nous proposons une solution à l'anomalie de performance de 802.11b que nous regardons tel qu'il est présenté dans la littérature c'est-à-dire dans une cellule de communication 802.11b. PAS (*Performance Anomaly Solution*) est une solution dynamique et distribuée pour résoudre l'anomalie de performance. Cette solution, en plus de résoudre ce problème bien connu de 802.11 peut être utilisée au-dessus de n'importe quel protocole MAC utilisant une écoute active du médium. Dans ce chapitre, nous avons fait le choix d'évaluer les performances du couple 802.11/PAS.

Le septième chapitre conclut cette thèse et présente brièvement les suites à donner à ces travaux.

Présentation de 802.11 et de quelques scénarii *ad hoc*

2

« Une des choses remarquables de la vie, c'est que rien ne va jamais tout à fait mal. Tout peut toujours empirer »

Bill Watterson,
Extrait de la bande dessinée Calvin et Hobbes.

Dans ce chapitre nous décrivons rapidement la norme 802.11 et la méthode d'accès au médium utilisée dans celle-ci. Ce chapitre n'est pas une revue complète de la norme, elle constitue simplement un rappel permettant de fixer les principes importants et de définir quelques termes qui pourraient être ambigus.

La norme 802.11 [40] est devenue en quelques années le standard de fait au niveau mondial pour les réseaux locaux sans fil. Cette norme définit la couche physique ainsi que la couche Link Layer du modèle OSI [75]. Dans ce chapitre, nous ne décrivons pas les couches physiques disponibles dans le standard, mais nous nous attachons à décrire le fonctionnement de la couche Link Layer et plus particulièrement la sous-couche Medium Access Control (MAC).

Pour compléter ce chapitre nous y avons ajouté quelques configurations de réseaux ad hoc connues comme posant des problèmes à la méthode d'accès décrite dans le standard 802.11.

Sommaire

2.1 Description générale 6
2.2 Les contextes d'utilisation de 802.11 7
2.3 La méthode d'accès DCF 8
2.4 Quelques problèmes de la méthode d'accès 9
2.4.1 Les stations cachées et le mécanisme de RTS/CTS 9
2.4.2 Les stations cachées asymétriques 10
2.4.3 Les trois paires 11
2.5 Remarques 11

2.1 Description générale

La norme IEEE 802.11 décrit la couche physique (PHY), la couche *Medium Access Control* (MAC) et la couche *Logical Link Layer* (LLC) de la pile protocolaire OSI. La figure 2.1 présente l'architecture de la pile protocolaire 802.11.

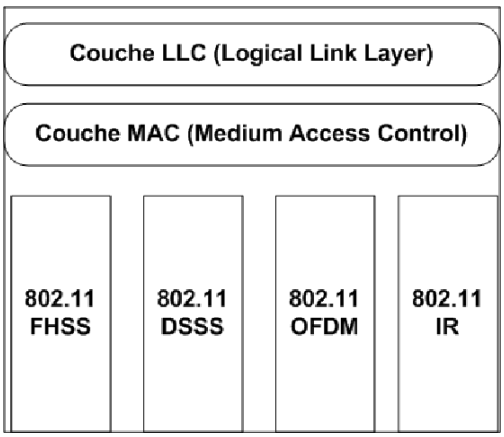


FIG. 2.1: 802.11 : Architecture et insertion dans la pile OSI.

Les quatres couches physiques, en même temps qu'elles définissent les caractéristiques du canal radio utilisé, définissent aussi les différents codages permettant de fiabiliser les transmissions. FHSS (*Frequency Hopping Spread Spectrum*) et DSSS (*Direct Sequence Spread Spectrum*) sont des techniques à étalement de spectre. Le premier est un étalement de spectre par saut de fréquence et le second, un étalement de spectre à séquence directe. OFDM (*Orthogonal Frequency Division Multiplexing*), quant à elle, est une technique de division du signal sur des porteuses orthogonales. IR (*Infra Red*) est une technique utilisant les communications infra-rouges.

Dans sa première version proposée en 1997 [40], la bande de fréquence utilisée était dans les 900 MHz. Les différentes extensions telles que 802.11a, 802.11b et 802.11g utilisent des bandes de fréquence dans les 2.4Ghz et dans les 5GHz.

Les différentes bandes de fréquence et les différents codages disponibles pour chaque version de la norme font que les débits de 802.11a, b, et g peuvent varier de 1 à 54 Mbps, avec quelques restrictions liées au codage utilisé. De plus, en fonction des technologies utilisées, les portées de communications varient de quelques dizaines à quelques centaines de mètre.

Au niveau de la couche MAC, il existe deux modes d'accès. Ces modes d'accès sont indépendants de la technologie utilisée au niveau PHY (hormis pour la couche PHY IR). Ces deux méthodes d'accès sont la méthode PCF (*Point Coordination Function*) et la méthode DCF (*Distributed Coordination Function*). L'utilisation de ces deux méthodes d'accès dépend de l'architecture du réseau, bien que la méthode DCF puisse être utilisée dans tous les types d'architectures. Nous reviendrons sur les modes de fonctionnement de la couche MAC dans les sections suivantes.

La couche LLC représente la gestion de la file d'attente contenant les paquets devant être traités par la couche MAC. Nous ne décrirons pas ici les spécificités de cette couche. Cette couche est similaire à celle d'ethernet.

2.2 Les contextes d'utilisation de 802.11

La norme 802.11 décrit deux modes de fonctionnement, donnés sur la figure 2.2. Le premier est le mode infrastructure. C'est le mode pour lequel 802.11 a été conçu. Dans ce mode, des stations de base ou points d'accès sont reliées entre elles par une infrastructure filaire. Les stations mobiles sont reliées à un point d'accès leur permettant ainsi d'accéder au service réseau. Pour communiquer entre elles, les stations doivent impérativement passer par la station de base. Le second mode est le mode *ad hoc* qui consiste simplement à autoriser les stations à communiquer entre elles tant qu'elles sont à portée de communication l'une de l'autre. Notons qu'un réseau *ad hoc* n'est pas forcément un réseau multi-saut.

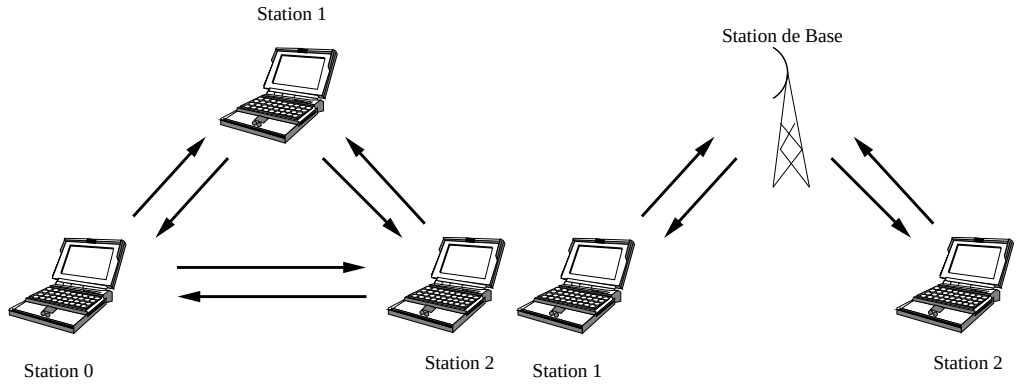


FIG. 2.2: 802.11 : Mode de fonctionnement. A gauche le mode *ad hoc* et à droite le mode infrastructure

Comme nous l'avons énoncé précédemment, 802.11 dispose de deux méthodes d'accès : PCF et DCF. Avec la méthode d'accès PCF, ce sont les stations de base qui ont la charge de l'accès au médium radio. Cet accès se fait de manière centralisée : c'est la station de base qui décide quand une station peut accéder au médium. Notons que très peu de cartes réseau sans fil implémente le mode PCF. Avec la méthode DCF, l'accès est totalement distribué et il n'y a aucune distinction entre les stations et les stations de base.

Les particularités des deux méthodes d'accès font que DCF est adapté aussi bien pour le mode *ad hoc* que pour le mode infrastructure, alors que le mode PCF ne peut être utilisé qu'en mode infrastructure. Dans la suite de ce manuscrit, quand nous ferons référence à la méthode d'accès de 802.11, nous supposerons que c'est la méthode d'accès DCF. Cette méthode d'accès est décrite plus en détail dans la section suivante.

2.3 La méthode d'accès DCF

La méthode d'accès DCF utilise les principes de CSMA [48] pour l'accès au médium. Contrairement à l'ethernet filaire, 802.11 utilise une variante de CSMA, appelée CSMA/CA (*Carrier Sense Multiple Access / Collision Avoidance*). Cette variante est due à la particularité du médium radio sur lequel il est difficile, contrairement au réseau filaire, de transmettre un paquet et de détecter en même temps une collision sur celui-ci.

CSMA/CA utilise les principes de base de CSMA. Ces protocoles sont basés sur une écoute active du canal radio afin de déterminer si le canal est libre ou non. Si un signal est reçu avec une puissance supérieure à un seuil appelé *seuil de détection de porteuse*, alors le médium est considéré comme occupé. Ce seuil de détection de porteuse est *a priori* différent du *seuil de communication* correspondant à la puissance minimale avec laquelle un signal doit être reçu pour pouvoir être décodé. Si deux stations sont à portée de communication, on suppose que chacune peut décoder les paquets de l'autre.

Si un terminal veut envoyer un paquet, il doit attendre que le médium soit libre pendant un temps d'attente fixe appelé DIFS (*DCF InterFrame Spacing*) à partir du moment où il commence à scruter le médium. Si le médium a été libre pendant tout ce temps, il peut alors envoyer son paquet. Si le médium est occupé au début de l'écoute du canal ou est devenu occupé pendant ce temps d'attente fixe, alors la station tire un nombre aléatoire appelé *backoff* dans un intervalle de temps $[0; CW_{min}]$ appelé *fenêtre de contention* et attend que le médium se libère. Le backoff correspond à un nombre entier de slots, le slot étant une unité de temps de 802.11. Lorsque le médium devient libre, la station attend de nouveau un temps DIFS avant de décrémenter son backoff slot par slot. Pendant toute cette opération, le médium doit rester libre. S'il devient occupé, le processus est arrêté et reprendra lorsque le médium deviendra libre à nouveau, *i.e.* la station devra attendre de nouveau un temps d'attente fixe DIFS et son nouveau backoff correspondra au nombre de slots de backoff restant lors de l'arrêt du processus. Une fois que le backoff atteint la valeur nulle, le paquet peut être émis par la station. Ce processus est décrit sur la figure 2.3.

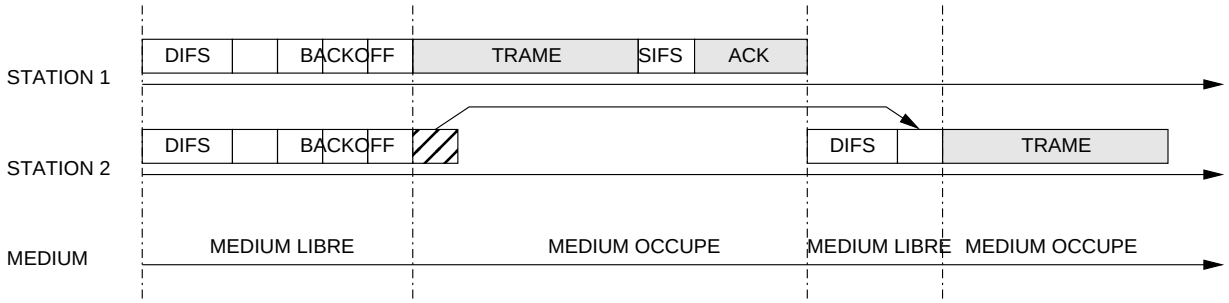


FIG. 2.3: 802.11 : *Distributed Coordination Function*. Au début, le medium est libre. Les deux stations attendent DIFS et leur backoff respectif. Le backoff de la station 1 est plus court. Celle-ci transmet son paquet occupant ainsi le médium. A la fin de sa transmission, c'est à dire à la réception de l'acquittement, la station 2 attend un DIFS et le reste de son backoff, puis transmet à son tour sa trame.

Pour savoir si le paquet émis a été correctement reçu par le destinataire, 802.11 utilise un mécanisme d'acquittement. En effet, il n'est pas possible pour un terminal de détecter la collision potentielle de son paquet tout en l'émettant. Par conséquent, le destinataire envoie, après un temps d'attente fixe SIFS, un paquet d'acquittement à l'émetteur s'il a correctement reçu son paquet. Si

au bout d'un certain temps, aucun acquittement n'est reçu par l'émetteur alors il considère qu'il y a eu collision sur son paquet. Il va alors tenter de le réémettre suivant l'algorithme BEB (*Binary Exponential Backoff*) : lorsqu'un émetteur considère que son paquet a subi une collision, il va doubler la taille de sa fenêtre de contention et choisir un backoff dans cette nouvelle fenêtre de contention lors de la réémission de son paquet. L'augmentation de cette fenêtre de contention revient à doubler la valeur de la borne supérieure de l'intervalle précédent. Si ce paquet subit une collision encore une fois, la taille de la fenêtre de contention est doublée à nouveau. Ce processus s'arrête si le paquet est transmis correctement ou si la fenêtre de contention a atteint une taille maximum (CW_{max}) définie par le standard. Dans 802.11, le nombre de retransmissions pour un paquet est limité. Ainsi, quand le nombre de retransmissions est atteint ou quand le paquet est transmis correctement, la fenêtre de contention est réinitialisée à CW_{min} qui est la taille initiale de la fenêtre de contention.

2.4 Quelques problèmes de la méthode d'accès

Dans cette section, nous décrivons les problèmes principaux liés à la méthode d'accès DCF utilisée dans la norme IEEE 802.11. Le protocole MAC est utile pour le partage du médium radio entre les stations sans fil concurrentes. Le rôle du protocole MAC est de fournir un accès à toutes les stations du réseau, et de faire en sorte que cet accès soit correct (sans collision).

Certains travaux de la littérature [14] ont cependant montré que 802.11 n'arrive pas à fournir systématiquement cet accès correct à toutes les stations. Ces problèmes d'accès sont dûs à des configurations (ou topologies ou scénarii) particulières des stations mettant en défaut la méthode d'accès CSMA/CA utilisé dans 802.11. Nous décrivons rapidement ces topologies dans les sous-sections suivantes.

2.4.1 Les stations cachées et le mécanisme de RTS/CTS

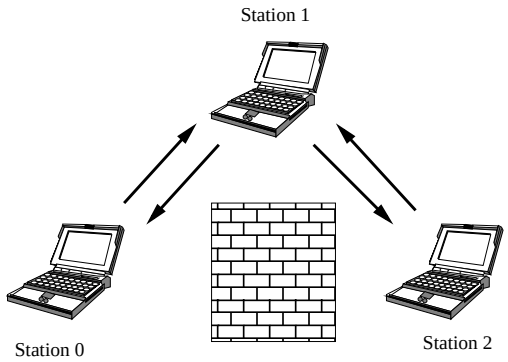


FIG. 2.4: 802.11 : Les stations cachées. La station 0 et la station 2 sont séparées par un obstacle mais ont un récepteur commun. Dans ce cas, les stations 0, et 2 perçoivent toujours le médium comme étant libre et ne sont ainsi jamais interrompues. Les transmissions simultanées des stations 0 et 2 provoquent des collisions au niveau de la station 1 qui n'émet jamais d'acquittement.

Un problème célèbre est le problème des "stations cachées" présenté sur la figure 2.4 : deux stations indépendantes, *i.e.* non à portée de communication l'une de l'autre et ni en détection de porteuse, cherchent à envoyer des paquets à un même destinataire. Dans cette configuration, elles ne

détectent pas leur activité réciproque sur le médium radio et donc considèrent que le médium est libre et qu'elles peuvent envoyer leurs paquets. Ces paquets peuvent alors entrer en collisions au niveau du récepteur qui ne comprend pas les paquets. Ces collisions provoquent l'augmentation des fenêtres de contention de chacune des stations. Cette augmentation permet d'accroître la probabilité pour une station de transmettre son paquet avec succès car le seul moyen qu'une transmission soit correcte est que celle-ci ait lieu pendant la période de décrémentation du *backoff* de la station en concurrence. La probabilité d'une transmission correcte augmente quand les paquets transmis par les stations sont de petite taille. Notons que l'apparition des collisions et l'augmentation de la fenêtre de contention réduisent les performances du protocole MAC. Pour empêcher l'apparition d'une telle situation, le mode DCF fournit un mode optionnel d'échange de paquets de contrôle de petite taille appelés RTS et CTS. Avant de transmettre ses données, un émetteur envoie un paquet de contrôle RTS (*Request to Send*) à son destinataire. Tous les mobiles à portée de communication de l'émetteur qui ont reçu ce RTS savent qu'une communication va avoir lieu. Comme la durée de la communication est précisée dans le paquet RTS, ces mobiles peuvent alors se bloquer et s'empêcher d'émettre pendant toute cette période. Cette opération est réalisée grâce au NAV (*Network Allocation Vector*) qui stocke la valeur de cette durée et qui joue le rôle d'horloge. Le récepteur qui reçoit le RTS renvoie un paquet de contrôle CTS (*Clear to Send*) s'il n'est pas lui-même bloqué par son NAV. Le CTS a le même effet que le RTS pour les mobiles à portée de communication du récepteur. À la réception du CTS, l'émetteur sait que le médium a été réservé et qu'il peut donc émettre ses données.

2.4.2 Les stations cachées asymétriques

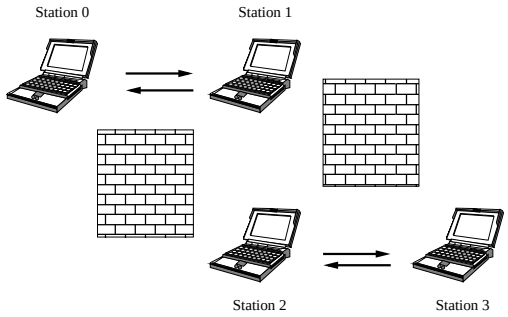


FIG. 2.5: 802.11 : Les stations cachées asymétriques. La station 0 et la station 2 sont séparées par un obstacle et ont chacune un récepteur : les stations 1 et 3 respectivement. Dans ce cas, la station 0 perçoit toujours le médium comme étant libre et transmet ces paquets après une attente ininterrompue de son *backoff*. La station 2 transmet elle aussi ces paquets quasiment sans interruption à la station 3. Les transmissions simultanées des stations 0 et 2 provoquent des collisions au niveau de la station 1 qui n'émet jamais d'acquittement. La station 3 reçoit toujours correctement les paquets envoyés par la station 2. On a ici un déséquilibre entre les deux stations.

Le scénario précédent (les stations cachées) présente une certaine symétrie. Dans le scénario des stations cachées asymétriques présenté sur la figure 2.5, seul un des deux émetteurs subit des collisions. Dans ce scénario, les deux émetteurs ont chacun deux récepteurs distincts. Ici, la station 0 se retrouve dans une situation de stations cachées alors que la station 2 se trouve dans une situation où ces transmissions sont correctes et elle ne perçoit jamais le médium comme étant occupé. Les collisions générées au niveau de la station 1 ainsi que l'augmentation du *backoff* qui s'ensuit pour la station 0 réduit fortement les performances du protocole MAC pour la station 0 et donc pour

l'ensemble du réseau. Notons que pour qu'une transmission soit correcte pour la station 0, elle ne doit pas excéder le temps de décrementation du *backoff* de la station 2. Le temps de décrémentation du *backoff* de la station 2 est toujours compris entre $[0; CW_{min}]$, ce qui n'était pas le cas dans le scénario des stations cachées. Il est aussi important de noter que bien que l'utilisation des RTS et CTS dans ce scénario permet de rééquilibrer l'accès au médium des deux stations, celui-ci ne résoud pas complètement le problème. En effet, la station 1 est bloqué par le NAV du RTS de la station 2 provoquant une non réponse aux RTS de la station 0.

2.4.3 Les trois paires

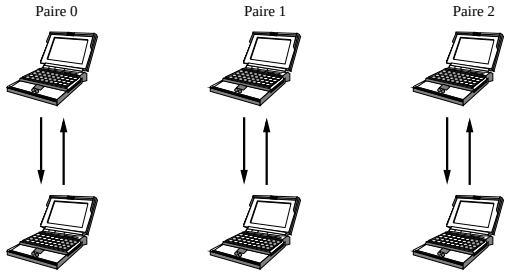


FIG. 2.6: 802.11 : Les trois paires. Les paires 0 et 2 sont complètement indépendantes l'une de l'autre mais partagent l'accès au médium avec la paire centrale (paire 1). Ce déséquilibre au niveau de la concurrence pour l'accès au médium entre les paires extérieures et la paire centrale provoque un défaut d'accès pour celle-ci. Dans ce scénario, la paire centrale doit attendre un recouvrement des périodes de décrémentation des paires extérieures pour pouvoir décrémenter son *backoff*. Les paires extérieures ayant complètement désynchronisées ses périodes de recouvrement sont très rares.

Le scénario des trois paires présenté sur la figure 2.6 montre un problème de défaut d'accès pour la paire centrale. Dans ce scénario, le problème ne vient pas des collisions mais de l'occupation du médium perçue par la paire centrale. Ici, les deux paires extérieures sont indépendantes l'une de l'autre, cependant elles sont en concurrence avec la paire centrale. Ce déséquilibre provoque un défaut d'accès pour la paire centrale car quand l'une des paires extérieures (paire 0 par exemple) accède au médium, elle bloque la paire centrale permettant ainsi à l'autre paire extérieure (paire 2) de décrémenter son *backoff* et d'envoyer son paquet. Quand la transmission de la paire 0 se termine, la transmission de la paire 2 peut encore être en cours, bloquant toujours la paire centrale. Ce blocage permet à la paire 0 d'accéder de nouveau au médium et ainsi de suite. Dans ce cas, la paire centrale ne perçoit quasiment jamais le médium comme étant libre et ne décrémente jamais son *backoff*.

2.5 Remarques

Dans ce chapitre, nous avons présenté brièvement le fonctionnement de la couche MAC de 802.11. Nous avons délibérément omis de préciser les durées des temporisateurs IFS et aussi les valeurs de CW_{min}, CW_{max} et du nombre de retransmission maximum autorisé pour un paquet. Dans la plupart des cas, ces valeurs sont liées à la couche physique utilisée et pour des raisons de clarté, nous ne les avons pas citées ici.

2.5 Remarques

Les scénarii présentés dans ce chapitre sont les scénarii de base identifiés dans la littérature comme posant des problèmes à la méthode d'accès. Il est possible d'aggraver les problèmes décrits ci-dessus en rajoutant par exemple plusieurs stations cachées ou en augmentant le déséquilibre dans le scénario des trois paires. Cependant, les deux problèmes basiques de 802.11 que l'on retrouve dans ces scénarii sont le problème de la gestion de collision et le problème du défaut d'accès.

Une évaluation analytique de IEEE 802.11

3

« Pourquoi apprendre alors que l'ignorance est instantanée ? »

Bill Watterson,
Extrait de la bande dessinée Calvin et Hobbes.

Ce chapitre propose une étude analytique du comportement de la couche MAC de 802.11 dans un contexte ad hoc. Cette étude se veut aussi bien qualitative que quantitative et a pour objectif d'améliorer nos connaissances sur la méthode d'accès proposée dans le standard 802.11. Elle nous permettra de mettre en avant aussi bien les points forts que les points faibles de cette méthode d'accès.

L'intérêt d'une étude analytique est qu'elle peut permettre d'isoler les causes de certains problèmes difficiles à identifier par simulation ou par expérimentation réelle. De plus les modèles conçus pour une étude analytique doivent permettre de facilement explorer l'espace d'état de tous les comportements possibles. De ce point de vue, nous pensons qu'un modèle analytique se doit avant tout d'être générique pour permettre cette exploration.

Dans ce chapitre, nous ne nous restreignons pas à l'étude du comportement de 802.11. Contrairement aux travaux présentés dans la littérature nous avons, avec des modifications minimes d'un même modèle, étudié le comportement de 802.11 suivant différents algorithmes de backoff, étudié plusieurs topologies et étudié plusieurs métrique de performance. C'est grâce à cette généricité mais aussi pour les nouveaux résultats obtenus que notre travail se démarque des travaux présentés dans la littérature.

Sommaire

3.1 État de l'art 14
3.2 Méthodologie et modèle de base 16
3.2.1 Les algèbres processus : PEPA 16
3.2.2 Méthodologie de modélisation 19
3.2.3 Le modèle 21
3.3 Étude de cas : Performance et équité 23
3.3.1 Les topologies 24
3.3.2 Les algorithmes de backoff 32
3.3.3 Les métriques 33
3.3.4 Résultats 35
3.4 Conclusions et travaux futurs 42
3.4.1 Modèle 42
3.4.2 Conclusions 43
3.4.3 Travaux futurs 44

3.1 État de l'art

Si nous voulons étudier les performances théoriques de 802.11, c'est d'abord pour mieux en comprendre le fonctionnement. L'objectif principal est de comprendre et de connaître les paramètres de 802.11 qui en affectent les performances pour pouvoir concevoir un protocole MAC ayant de meilleures propriétés. La première intuition que beaucoup de chercheurs ont eu, c'est que 802.11 est un bon protocole mais mal paramétré. Ceci explique le nombre incalculable de propositions d'algorithme de backoff. Malgré le nombre important de solutions présentées dans la littérature, nous restons convaincu qu'il est possible de faire encore mieux, du moins dans un contexte de réseaux *ad hoc*. Cette étude théorique est donc utile pour nous apporter quelques éclaircissements non réalisées dans les propositions faites dans la littérature.

Étude théorique de 802.11 Le protocole 802.11 et de nombreuses modifications qui lui ont été apportées ont été étudiés analytiquement dans la littérature. Nous ne faisons pas dans cette section une revue de toutes les modifications de 802.11 proposées. Nous nous penchons sur les principales méthodologies analytiques employées pour évaluer 802.11 et ses modifications.

La méthodologie la plus utilisée pour évaluer les performances de 802.11 s'appuie sur les chaînes de Markov. La plus connue est celle proposée par Bianchi [6] en 2000. Cette étude évalue les performances, comme le taux d'occupation du canal et le taux d'erreur de 802.11 dans un contexte de réseau avec station de base. Elle propose une évaluation asymptotique du comportement de l'algorithme du backoff dans ce contexte. Plusieurs travaux étudiant d'autres algorithmes de backoff pour 802.11 sont dérivés de ce modèle. Les principaux avantages du modèle proposé par Bianchi sont sa précision sur le comportement asymptotique et sa facilité d'extension entre autre à l'étude d'autres algorithmes de backoff. Des modifications ont aussi été apportées sur le modèle de Bianchi pour prendre en compte une arrivée poissonnienne de paquets [27]. Le principal inconvénient du modèle proposé par Bianchi se situe dans l'impossibilité d'étendre le modèle pour l'étude de scénarii *ad hoc*. Bien qu'un travail dans ce sens ait été proposé dans [32], celui-ci est assez limité car il ne prend pas en compte les différentes interactions possibles entre les nœuds. Ce travail suppose aussi

que tous les nœuds ont en moyenne le même comportement ; ce qui dans un réseau *ad hoc* n'est pas forcément vrai. L'autre inconvénient lié au modèle de Bianchi est l'impossibilité d'étudier d'autres critères de performance.

Deux autres approches utilisant les chaînes de Markov et proposant une étude de 802.11 sont proposées dans [55] et [15]. Ces deux approches étudient deux scénarii *ad hoc* particuliers. La première propose une évaluation de 802.11 dans le contexte des stations cachées [5] et la seconde dans le contexte des 3 paires [14]. Ces deux approches cherchent à mettre en avant les problèmes d'équité inhérents à ces deux scénarii. Les deux approches proposent des résultats précis sur le comportement général de 802.11 mettant en avant les causes du déséquilibre, provoquant ainsi un problème d'équité. Tout comme le modèle proposé par Bianchi, la faiblesse de ces deux approches est l'extension à d'autres scénarii. La combinaison des résultats de Bianchi [6], Chaudet et al. [15] et Li et al. [55] permettent d'avoir un panel important de résultats concernant 802.11. Cependant, il existe d'autres scénarii qu'aucune modification des trois modèles ne permet de modéliser simplement.

La méthodologie proposée dans [29] et [28] s'appuie sur un processus semi-markovien de renouvellement et de récompense. Le modèle proposé permet d'étudier plusieurs topologies *ad hoc* du point de vue du débit. Pour obtenir les résultats de performance sur un réseau *ad hoc* les auteurs procèdent en deux étapes. Durant la première étape, les auteurs cherchent à obtenir les probabilités de transition entre les différents états du médium, les probabilités de collision et de transmission de chaque station. L'obtention de ces probabilités se fait à partir du modèle de Bianchi et/ou de [52][1] et d'analyse complémentaire des interactions entre les stations. Une fois ces probabilités obtenues, elles sont injectées dans la chaîne de Markov permettant ainsi d'avoir les métriques de performances. La difficulté dans l'approche proposée est la détermination de ces probabilités qui est souvent faite à partir d'approximation du comportement de l'algorithme de *backoff* et d'approximation des effets des interactions de chaque station. Selon nous les approximations faites apporte un biais au résultats. De ce fait, les résultats obtenus sur les stations cachées et sur les trois paires (par exemple) sont beaucoup moins précis que les résultats obtenus avec les méthodologies décrites dans [55] et [15].

L'étude de 802.11 proposée dans [10] approxime le comportement du protocole par un protocole p-persitant. Cette approche permet, comme pour la méthode de Bianchi, d'extraire les performances du protocole 802.11. Les résultats montrent que le modèle utilisé présente des résultats très proches des résultats de simulations de 802.11. Mais tout comme le modèle de Bianchi, ce modèle est destiné à étudier le comportement de 802.11 dans le mode infrastructure. L'extension de ce modèle pour l'étude de réseaux *ad hoc* ou l'étude d'autres algorithmes de backoff reste complexe. Nous avons voulu citer ce travail car il fait partie des modèles se démarquant du modèle de Bianchi. Notons qu'il existe une multitude de modèles et de méthodes comme ceux proposés par [10] et [6] pour évaluer analytiquement les performances de 802.11 dans une cellule de communication. Cependant, il nous paraît utile de citer aussi les résultats présentés dans [4] qui se démarquent des autres résultats car les auteurs n'évaluent pas l'efficacité mais l'équité de 802.11 dans une cellule de communication.

En règle générale, la littérature montre que les modèles les plus adaptés à l'étude de 802.11 sont les modèles probabilistes, markoviens (stochastiques). Sans déroger à cette règle, nous avons voulu proposer un modèle permettant d'évaluer les performances de 802.11 ayant les avantages suivants : **1)** Le modèle doit permettre d'extraire en même temps que des mesures de performances classiques, des mesures en termes d'équité si nécessaire ; **2)** Le modèle doit permettre d'étudier facilement différents algorithmes de backoff ; **3)** Le modèle doit permettre d'étudier différentes topologies ; **4)** Le modèle doit être facilement extensible pour le faire évoluer en fonction des besoins ; **5)** Bien sûr, le modèle doit rester de taille raisonnable pour qu'il soit exploitable ; **6)** La précision doit pouvoir être modifiée selon la qualité des résultats recherchée. Selon nous, il n'existe pas dans la littérature

[1] Ce modèle étudie le comportement de 802.11 dans une cellule.

un modèle ayant ces propriétés.

Notre modèle s'appuie sur celui proposé dans [50]. Nous proposons d'étendre celui-ci pour une meilleure généricité. Ce modèle se propose d'étudier plusieurs scénarii de réseau *ad hoc* connus pour les problèmes d'équité qu'ils engendrent avec l'utilisation de 802.11. De notre point de vue, la faiblesse de cette approche est qu'elle est difficilement extensible à l'étude d'autres algorithmes de backoff, car les auteurs de [50] n'ont pas conçu le modèle dans ce sens et n'ont donc pas isolé le comportement de backoff du comportement général du nœud. Le travail que nous exposons par la suite est une généralisation du travail de [50].

3.2 Méthodologie et modèle de base

3.2.1 Les algèbres processus : PEPA

Nous avons choisi comme formalisme de modélisation les algèbres de processus stochastiques, plus particulièrement PEPA (*Performance Evaluation Process Algebra*). Ce formalisme a été développé en 1994 par J. Hilston [36] et étend l'algèbre des processus classiques en assignant une variable aléatoire, représentant une durée, à chaque action. Ces variables sont distribuées exponentiellement ce qui conduit à une relation évidente entre un modèle décrit sous forme d'algèbre de processus et un processus de Markov en temps continu. C'est à partir de ce processus markovien que les mesures de performances peuvent être extraites.

Le principale avantage de ce formalisme, selon nous, est l'approche compositionnelle qu'elle propose. Ainsi, un modèle est construit à partir de composante représentant une partie du système à modéliser. Cette approche compositionnelle permet de diviser le modèle pour une meilleure compréhension de celui-ci mais aussi pour une réutilisation ultérieure des composantes déjà décrites.

De plus, PEPA inclut une technique de simplification des modèles qui exploitent l'équivalence des comportements pour réduire l'espace d'état. Cette technique est présentée dans [36] et est connue sous le nom d'agrégation. Ajouter à cela, pour répondre au problème d'explosion de l'espace d'état, PEPA propose une technique permettant d'avoir une version compacte de la chaîne de Markov sous-jacente au modèle PEPA [37].

Bien que l'aspect compositionnel et/ou les techniques d'agrégation se retrouvent dans plusieurs autres formalismes comme les réseaux d'automates stochastiques [65], les réseaux de Petri stochastiques [20] etc., PEPA à l'avantage d'être simple d'utilisation grâce à un ensemble réduit d'opérateurs. PEPA est aussi utilisé comme formalisme pour un nombre important d'outils comme PEPA workbench [30], Mobius [19] et PRISM [18], permettant ainsi d'exploiter au mieux les modèles PEPA.

Le formalisme de PEPA

Les modèles PEPA sont décrits comme des interactions de plusieurs *composantes*. Chaque composante peut suivre le comportement d'une ou de plusieurs *actions* : une action $a \in \mathcal{A}ct$ est décrite par le couple (α, r) où $\alpha \in \mathcal{A}ct$ est le *type* de l'action et $r \in \mathbb{R}^+$ est le paramètre de la loi exponentielle liée à cette action. Un ensemble d'opérateurs est proposé dans PEPA pour construire des modèles complexes à partir de composantes exprimées simplement. Ce sont les opérateurs classiques des algèbres de processus : *Prefix*, *Choice*, *Parallel composition*, *Abstraction*. Dans la suite, nous décrivons les opérateurs que nous utilisons. Pour plus de renseignements sur le formalisme PEPA, nous vous invitons à consulter [36].

- *Prefix :* Une composante peut avoir un comportement séquentiel dans lequel elle suit une succession d'actions avant de suivre le comportement d'une autre composante. Dans ce cas, l'opérateur *prefix*, noté ".", est utilisé pour désigner la première action, *e.g.* $(\alpha, r).P$ se comportera d'abord comme une activité de type α avec une durée moyenne de $1/r$, puis aura le comportement de la composante P. Dans certains cas, le taux de l'activité n'est pas spécifié, car non connu lors de l'écriture du modèle. Ce taux sera alors acquis par synchronisation avec une autre composante possédant le taux. Dans ce cas, le taux d'activité est spécifié avec un symbole particulier $\top$ et on parle d'action passive.

- *Choice :* Cet opérateur modélise le choix entre deux comportements, *e.g.* $(\alpha, r).P + (\beta, s).Q$. La nature continue des distributions de probabilités nous garantit que ces deux actions ne peuvent pas se produire simultanément. Le comportement final sera celui de la première activité à se terminer.

- *Parallel composition :* Cet opérateur est utilisé lorsque deux composantes doivent collaborer à travers certaines actions. Il permet donc la synchronisation entre deux composantes. Par exemple, le système $P \underset{L}{\bowtie} Q$ décrit deux composantes P et Q devant collaborer dans les actions définies dans l'ensemble de synchronisation L. Les actions non spécifiées dans L demeurent indépendantes et se déroulent dans P et Q sans être en concurrence. Les actions spécifiées dans L doivent nécessairement se dérouler simultanément dans P et Q pour modéliser la synchronisation. L'action résultant de cette synchronisation conserve le même *type* que celle définie dans P et Q, mais le taux résultant est le plus petit taux d'activité des deux composantes. Cela implique que le taux d'une action passive sera le taux de l'action avec laquelle elle se synchronise.

Le processus de Markov associé

Dans un modèle PEPA, lorsqu'une composante P suit une activité (α, r) puis se comporte comme la composante P', on dit que P' est dérivée de P. Pour chaque composante PEPA P, il est possible de construire récursivement un ensemble de dérivations (noté $ds(P)$). À partir de cet ensemble de dérivations, nous pouvons construire le *graphe de dérivation*. Ce graphe de dérivation est un graphe orienté tel que l'ensemble des nœuds est $ds(P)$ et un arc entre deux nœuds représente la possibilité d'une transition entre les deux composantes associées.

Grâce à l'utilisation de variables aléatoires suivant des distributions exponentielles, un modèle PEPA conduit à une chaîne de Markov en temps continu. La construction de cette chaîne est basée sûr le graphe de dérivation du modèle. Un état est associé à un nœud du graphe et les transitions entre les états de la chaîne sont les arcs du graphe.

Pour résoudre le processus markovien, il existe plusieurs outils comme PEPA Workbench [30] qui est un outil capable de résoudre numériquement les modèles PEPA en générant la distribution stationnaire du système. PRISM [18] propose également une interface permettant de traiter les modèles PEPA et de calculer un état stationnaire du processus markovien sous-jacent.

Un exemple d'application : La file M/M/1/N

Pour mieux se rendre compte de l'utilisation, prenons de PEPA l'exemple d'une file $M/M/1/N$ déja étudiée dans [49]. Dans cet exemple, le système est composé d'un serveur et d'une file d'attente de capacité N représentant la file d'attente $M/M/1/N$. Bien sur, ici nous supposons que le temps de service et les arrivées suivent une distribution exponentielle de paramètres μ et λ.

Le système peut être représenté comme l'interaction de deux composantes *Serveur* et *File*. La composante représentant le serveur est le suivant :

$$Serveur \stackrel{def}{=} (service, \mu).Serveur;$$

La composante représentant la $File$ d'attente est la suivante :

$$\begin{array}{lll}
File_0 & \stackrel{def}{=} & (arrive, \lambda).File_1; \\
File_1 & \stackrel{def}{=} & (arrive, \lambda).File_2 + (service, \top).File_0; \\
... & \stackrel{def}{=} & ... \\
File_i & \stackrel{def}{=} & (arrive, \lambda).File_i + 1 + (service, \top).File_i - 1; \\
... & \stackrel{def}{=} & ... \\
File_N - 1 & \stackrel{def}{=} & (arrive, \lambda).File_N + (service, \top).File_N - 2; \\
File_N & \stackrel{def}{=} & (service, \top).File_N - 1;
\end{array}$$

Sur cette composante, la durée de l'action service n'est pas définie. L'action $(service, \top)$ prend sa durée à partir de l'action $service$ de la composante $Serveur$. Cette relation entre les deux composantes est représentée sur le modèle général suivant :

$$System \stackrel{def}{=} Serveur \underset{service}{\bowtie} File$$

Nous voyons sur cette composante que l'action service fait partie des éléments de synchronisation des deux éléments $Serveur$ et $File$. Nous pouvons aussi noter que la composante $Serveur$ peut facilement être supprimée. Pour obtenir les mêmes résultats, il suffit pour cela d'enlever la composante et de modifier l'action $(service, \top)$ de la composante $File$ par une action $(service, \mu)$. Tout l'intérêt de PEPA est de pouvoir modéliser le système en plusieurs composantes permettant ainsi une réutilisation des modèles.

Comme dit précédemment, PEPA n'est pas un formalisme paramétré. Tous les paramètres du modèle doivent être connus dès le départ. Ainsi dans notre exemple, la valeur de N doit être fixée.

Si on suppose que $N = 2$, le graphe de dérivation du système est présenté sur la figure 3.1. La chaîne de markov sous-jacente au modèle est présentée sur la figure 3.2

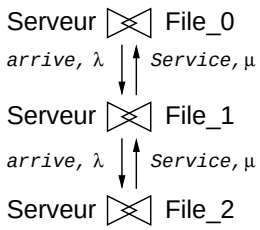


FIG. 3.1: PEPA : Graphe de dérivation d'un modèle de file $M/M/1/N$. Dans ce modèle, le paramètre N est égal à 2. Le graphe de dérivation est tiré de la composante $Systeme$ dans laquelle un état est représenté par un couple $Serveur$-$File$

La résolution de la chaîne de Markov dérivée du modèle PEPA peut se faire avec plusieurs techniques. La plus simple est d'utiliser des outils comme PEPA workbench ou Prism. Ces outils permettent de résoudre le système d'équation :

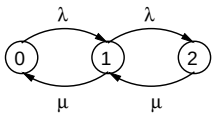


FIG. 3.2: PEPA : Chaîne de Markov associée à une file $M/M/1/N$. Cette chaîne de Markov est la chaîne sous-jacente au graphe de dérivation du modèle PEPA de la file $M/M/1/N$ avec $N = 2$

$$\Pi \times Q \quad = \quad 0$$

Où $\Pi = (\pi_0, \pi_1, \pi_2)$ est la distribution à l'état stationnaire de la chaîne de Markov, et Q est le générateur infinitésimal correspondant.

$$\begin{pmatrix} -\lambda & \lambda & 0 \\ \mu & -(\lambda+\mu) & \lambda \\ 0 & \mu & -\mu \end{pmatrix}$$

3.2.2 Méthodologie de modélisation

Généralités

Pour modéliser un réseau *ad hoc*, il est important d'en extraire les caractéristiques principales. Par définition, un réseau *ad hoc* est un ensemble de nœuds ou stations interagissant les uns avec les autres. De par la nature des réseaux *ad hoc*, ces interactions peuvent être différentes suivant le voisinage de chaque nœud. Il est donc important de modéliser ces interactions qui représenteront la topologie du réseau.

Pour une meilleure généricité du modèle, il est important de dissocier le nœud des interactions qui influent sur celui-ci. Ainsi, un nœud peut être défini (sans considérer les interactions) par l'application qu'il exécute. Cette application, dans notre cas, est représentée par une source de trafic. Chaque paquet ainsi créé par l'application doit être envoyé sur le réseau. Le réseau, plus précisément le médium radio, est une ressource partagée par les nœuds suivant les interactions définies précédemment.

Tous les nœuds du réseau vont accéder à la ressource partagée. Pour ce faire, chaque nœud dispose d'un moyen d'accès au médium radio. Ce moyen d'accès, dans un terminal sans fil, est représenté par la couche MAC (*Medium Access Control*). Dans le cas d'un réseau sans fil utilisant 802.11, cette méthode d'accès est CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*).

La topologie, la source de trafic et la méthode d'accès constituent des informations nécessaires pour l'étude des réseaux. La précision de la description de chacune de ces trois composantes feront que le modèle sera plus ou moins précis. Dans la section suivante, nous décrivons plus en détails chacune de ces trois composantes et d'autres composantes annexes qui leurs sont associées.

Il faut noter que dans un réseau *ad hoc*, le récepteur des flux se comporte toujours de la même façon. Nous entendons par là que le récepteur n'a qu'un rôle, c'est à lui d'envoyer ou non des acquittements suivant la validité de la donnée qu'il reçoit. Ainsi, c'est la réception ou non de cet acquittement qui fait évoluer le comportement du nœud émetteur. En revanche, la réception, correcte

ou non, d'une trame de données va dépendre des interactions entre le récepteur et tout son voisinage. Ainsi, nous avons décidé, par souci de simplification du modèle, de modéliser le récepteur de chaque flux dans la composante qui représente l'interaction. Pour résumer, la composante représentant les interactions entre les nœuds représente les interactions entre un émetteur et son voisinage en même temps que le récepteur et son voisinage.

Méthodologie complète

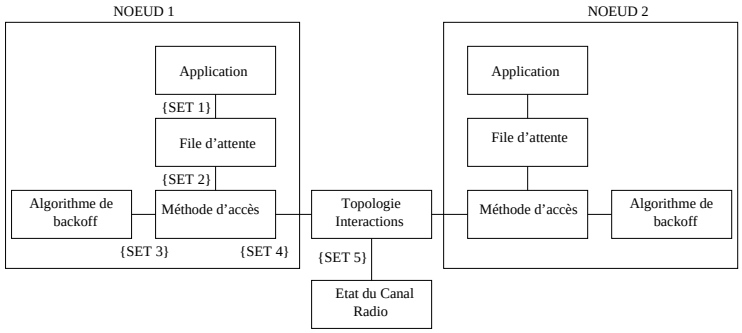


FIG. 3.3: PEPA : Méthodologie de découpage d'un réseau en composantes. Ce découpage permet d'isoler les fonctionnalités caractéristiques d'un réseau *ad hoc* en composante. Chaque rectangle représente une composante et $\{SET\}$ représente l'ensemble des actions de synchronisation entre chaque composante

La figure 3.3 montre le découpage que nous utilisons pour représenter un réseau *ad hoc*. Nous modélisons, notre application par un générateur de trafic qui peut simplement être une arrivée poissonnienne.

Contrairement à la description faite plus haut, plusieurs composantes forment notre modèle de réseau *ad hoc*. Nous avons ainsi modélisé une file d'attente servant de *buffer* à chaque paquet créé par l'application. La relation entre le générateur de trafic et la file d'attente correspond à une action simple qui consiste à mettre un paquet dans la file d'attente.

La file d'attente sert de composante liant le générateur de trafic (l'application) à la méthode d'accès. Cette dernière représente la manière dont le nœud va accéder à la ressource partagée. La relation entre la file d'attente et la méthode d'accès est une action dépilant la file d'attente.

La méthode d'accès est liée à deux composantes. La première est la composante représentant la topologie du réseau ou les interactions entre les nœuds. Les actions qui relient la topologies et la méthode d'accès sont les actions permettant de tester si la ressource partagée est libre ; une action permettant de libérer la ressource partagée ; une action permettant de prendre possession de la ressource partagée ; et enfin dans notre cas, une action permettant de décider si la prise de possession de la ressource partagée est correcte ou si plusieurs nœuds y ont accès en même temps. Dans le dernier cas, ceci provoque une collision au niveau de la transmission. La seconde composante avec laquelle est liée la méthode d'accès est l'algorithme de backoff. Cette composante permet de faire évoluer la fenêtre de contention. Ces deux composantes sont liées par trois actions. Deux d'entre elles permettent de faire évoluer le *backoff* en cas de collision ou de transmission correcte. La dernière représente le temps d'attente du *backoff* utilisé avant d'accéder au médium.

La composante représentant la topologie du réseau est reliée à une composante représentant l'état du canal radio. Ces deux composantes sont reliées par une action représentant une probabilité. Cette

probabilité permet de rajouter une composante aléatoire à une transmission qui bien que correcte au niveau de la méthode d'accès peut être erronée, due à une mauvaise qualité du lien radio.

Le découpage que nous présentons ici cherche à atomiser un réseau *ad hoc*. Nous voulons isoler tous les mécanismes et tous les comportements mis en jeu dans un réseau pour permettre une meilleur compréhension de certains mécanismes ou comportements qui peuvent être difficiles à comprendre et/ou à interpréter. Pour contourner ce problème, si le découpage est bien fait, il est possible de remplacer simplement la composante mise en cause par une autre composante dont nous connaissons les propriétés. Ce découpage apporte aussi un moyen de comparaison simple de plusieurs mécanismes. C'est selon nous, ce découpage qui manque aux travaux présentés dans [50]. Par exemple dans ces travaux, l'algorithme de *backoff* n'est pas séparé de la méthode d'accès.

3.2.3 Le modèle

La méthode d'accès

Comme nous étudions le comportement de 802.11 et ses dérivées, la méthode d'accès que nous modélisons est CSMA/CA plus spécifiquement le mode DCF. Le modèle PEPA correspondant à la méthode CSMA/CA décrite dans le standard 802.11 est le suivant :

$$
\begin{aligned}
E_i_000 &\stackrel{def}{=} (free, \mu_trans).E_i_001;\\
E_i_001 &\stackrel{def}{=} (difs, \mu_difs).E_i_002;\\
E_i_002 &\stackrel{def}{=} (free, \mu_trans).E_i_003 + (occ, \mu_data).E_i_000;\\
E_i_003 &\stackrel{def}{=} (db_i, \top).E_i_004;\\
E_i_004 &\stackrel{def}{=} (free, \mu_trans).E_i_005 + (occ, \mu_data).E_i_000;\\
E_i_005 &\stackrel{def}{=} (send, \mu_trans).E_i_006;\\
E_i_006 &\stackrel{def}{=} (ack, \top).E_i_007 + (collision, \top).E_i_008;\\
E_i_007 &\stackrel{def}{=} (succ_i, \mu_trans).E_i_009;\\
E_i_008 &\stackrel{def}{=} (coll_i, \mu_trans).E_i_000;\\
E_i_009 &\stackrel{def}{=} (out_i, \mu_trans).E_i_000;
\end{aligned}
$$

Dix actions sont utilisées pour modéliser le mécanisme d'accès au médium CSMA. L'action $(free, \mu_trans)$ sert à tester si le canal radio est libre ou non. Si le canal est libre, cette action sert à synchroniser la station avec le canal radio. Si le médium est occupé, le nœud retourne à son état initial grâce à l'action (occ, μ_dada). L'action $(difs, \mu_difs)$ et l'action $(db_i, \top)$ représentent l'écoulement des temps DIFS et du *backoff*. $(db_i, \top)$ est une synchronisation avec l'algorithme de *backoff*. L'action $(send, \mu_trans)$ représente la capture du médium. Ici cette capture est représentée par un temps très court. Le temps de transmission s'écoule au niveau de la composante représentant le médium. Les actions $(ack, \top)$ et $(collision, \top)$ sont des synchronisations venant du médium spécifiant si la transmission s'est bien déroulée ou non. Les actions $(succ_i, \mu_trans)$ et $(coll_i, \mu_trans)$ servent à faire évoluer la composante représentant le backoff après une collision ou une transmission correcte. L'activité (out_i, μ_trans) est utilisée pour se synchroniser à la file d'attente.

Nous pouvons remarquer ici que toutes les durées sont approximées par une distribution exponentielle. Ainsi, même les temps d'attente déterministes de 802.11 comme le DIFS (50 μs) sont approximés par une distribution exponentielle dont la moyenne est 50. Les actions ayant pour durée μ_trans représentent des actions ne consommant pas de temps, comme par exemple le fait de tester si le médium est libre ou non, car dans PEPA, toutes les actions doivent avoir une durée. Ainsi,

μ_trans représente un temps de l'ordre du dixième de μs.

L'algorithme de backoff

Le principe général de l'algorithme du *Binary Exponential Backoff* est le suivant : si la transmission d'un nœud entre en collision, associée à la non réception d'un acquittement, la taille de la fenêtre de contention est doublée. Dans le cas d'une transmission correcte, la taille de la fenêtre de contention est réduite à sa taille minimale. L'algorithme du *Binary Exponential Backoff* de 802.11 est représenté par le modèle PEPA suivant :

$$
\begin{array}{lcl}
BO_{i_0} & \stackrel{def}{=} & (db_i, f_0).BO_{i_0} + (succ_i, \top).BO_{i_0} + (coll_i, \top).BO_{i_1} \\
... & \stackrel{def}{=} & ... \\
BO_{i_j} & \stackrel{def}{=} & (db_i, f_j).BO_{i_j} + (succ_i, \top).BO_{i_0} + (coll_i, \top).BO_{i_(j+1)}, \forall j \in [1..6] \\
... & \stackrel{def}{=} & ... \\
BO_{i_7} & \stackrel{def}{=} & (db_i, f_7).BO_{i_7} + (succ_i, \top).BO_{i_0} + (coll_i, \top).BO_{i_0}
\end{array}
$$

La composante BO_{i_x} est associée au nœud i et représente l'algorithme de backoff de 802.11. 8 tentatives de transmission sont autorisées pour un même paquet. La durée de l'action db_i, ici f_j avec $j \in \{0,7\}$[2], dépend du nombre de collisions successives subies par le paquet en cours de transmission. Due à la propriété sans mémoire de la distribution exponentielle, f_j est la durée moyenne du backoff dans la fenêtre de contention utilisée après j collisions. Par exemple, f_0 est égal à $20\mu s \times (2^5 - 1)/2$, qui est la durée moyenne du backoff tiré aléatoirement dans une fenêtre de $[0; 32]$ *slots*. Plus généralement, $\forall i \in \{0..5\}, f_i$ est la durée moyenne du backoff tiré dans la fenêtre $[0..2^{5+i}]$. Ce tirage du backoff fait que notre modèle approxime le comportement du backoff de 802.11. L'action de synchronisation $coll_i$ (respectivement $succ_i$) sert à faire évoluer le backoff après une collision (respectivement après une transmission correcte).

Les interactions ou la topologie

$$
\begin{array}{lcl}
Med_{00_00} & \stackrel{def}{=} & (free, \top).Med_{00_00} + (transmit, \top).Med_{00_01}; \\
Med_{00_01} & \stackrel{def}{=} & (free, \top).Med_{00_01} + (go_{next}, \mu_{slot}).Med_{00_02} + (transmit, \top).Med_{00_04}; \\
Med_{00_02} & \stackrel{def}{=} & (ack, \mu_{trans}).Med_{00_03}; \\
Med_{00_03} & \stackrel{def}{=} & (sync, \mu_{data}).Med_{00_00}; \\
Med_{00_04} & \stackrel{def}{=} & (collision, \mu_{trans}).Med_{00_05}; \\
Med_{00_05} & \stackrel{def}{=} & (collision, \mu_{data}).Med_{00_00};
\end{array}
$$

Presque toutes les activités de cette composante sont partagées soit avec la composante représentant la méthode d'accès. Med_{00_00} représente l'état initial de la composante représentant la méthodologie. L'action $free$ est synchronisée avec la méthode d'accès et permet de spécifier si le médium est libre ou pas. Notons que Med_{00_00} et Med_{00_01} représentent l'état libre du médium, à la seule différence que Med_{00_01} représente un état où un accès simultané à la ressource partagée est possible. C'est ainsi que notre modèle gère les collisions. La composante évolue de l'état Med_{00_00} à l'état Med_{00_01} quand une station se synchronise sur l'action $transmit$. Le médium reste dans l'état Med_{00_01} pendant une durée de $20\mu s$, représentant la durée d'un slot durant laquelle le mé-

[2]Ici $f_7 = f_6 = f_5 = 20\mu s \times (2^{10} - 1)/2$.

dium est toujours libre. Les synchronisations avec l'action $free$ sont encore possibles pour les autres stations, et durant lesquelles une autre station peut aussi se synchroniser sur une action $transmit$, provoquant ainsi une collision. On peut noter que due à la nature continue de la distribution de probabilités, les actions ne peuvent pas se produire simultanément. Ainsi, le fait de rester dans l'état Med_{00_01} pendant la duré d'un slot autorise la modélisation des accès simultanés. Si durant ces $20\mu s$, aucune action $transmit$ n'est reçue par la composante méthode d'accès, celle-ci evolue vers l'état Med_{00_02} correspondant à l'envoi d'un acquittement (action ack). L'état Med_{00_03} représente l'écoulement réel du temps de transmission de la donnée. Ici, la durée de la donnée inclut la durée de l'échange DATA-ACK. L'action $sync$ est utile à des fins de calcul particulier de performance. Avoir deux actions $sync$ et deux actions ack permettrait de calculer le débit de chacun des nœuds et d'avoir des tailles de paquets différentes sur chaque nœud. Dans le cas où une transmission simultanée se produit, le médium se retrouve dans l'état Med_{00_04} au cours duquel une action de synchronisation $collision$, d'une durée négligeable est envoyée à l'un des nœuds. Ensuite, une autre synchronisation d'une durée de la collision est envoyée à l'autre nœud. Dans ce cas, l'ordre dans lequel les nœuds reçoivent les actions de synchronisation n'est pas important car dans tous les cas, le médium n'est de nouveau libre qu'après l'écoulement de la durée d'une collision.

Notons ici que la composante présentée montre une topologie avec deux stations. Dans le cas où plusieurs stations devaient être modélisées, le même modèle peut être utilisé en faisant l'approximation que les collisions ne se font que deux à deux. Si on veut relâcher cette hypothèse il faudrait dupliquer l'état Med_{00_05} pour refléter le nombre de nœuds pouvant entrer en collision.

Validation du modèle

Dans cette sous-section, nous présentons les premiers résultats permettant de valider notre modèle. Le simulateur que nous avons utilisé est NS-2 [60] dans sa version 2.27. Nous avons modifié les paramètres de NS-2 pour refléter la couche physique DSSS décrite dans le standard 802.11b. Les résultats de simulations sont obtenus en simulant 2 nœuds à portée de communication transmettant des paquets à une même destination. Les deux nœuds travaillent à saturation.

La figure 3.4 montre la précision de notre modèle par rapport au débit obtenu par simulation. Dans cette figure, les débits sont calculés à partir des probabilités à l'état stationnaire de la chaîne de Markov dérivée du modèle PEPA. La probabilité qui nous intéresse est la probabilité pour le modèle d'être dans l'état Med_{00_03}. À partir de cette probabilité que nous notons P_{occ}, nous pouvons calculer le débit de la manière suivante :

$$Th \quad = \quad P_{occ} \times \frac{T_{donnee}}{T_{donnee} + T_{entete}} \times D$$

Où T_{donnee} équivaut au temps nécessaire pour transmettre les données utiles et T_{entete} au temps nécessaire à la transmission des entêtes du paquet. D est le débit de transmission physique utilisé. Dans notre cas, nous avons choisi $D = 11$ Mbps.

3.3 Étude de cas : Performance et équité

Dans cette section, nous présentons une série de résultats de performance et d'équité de certaines configurations de réseaux sans fil. Cette partie s'attache particulièrement a étudier le comportement de 802.11 dans différentes situations. Pour cela, nous nous proposons d'étudier le comportement de

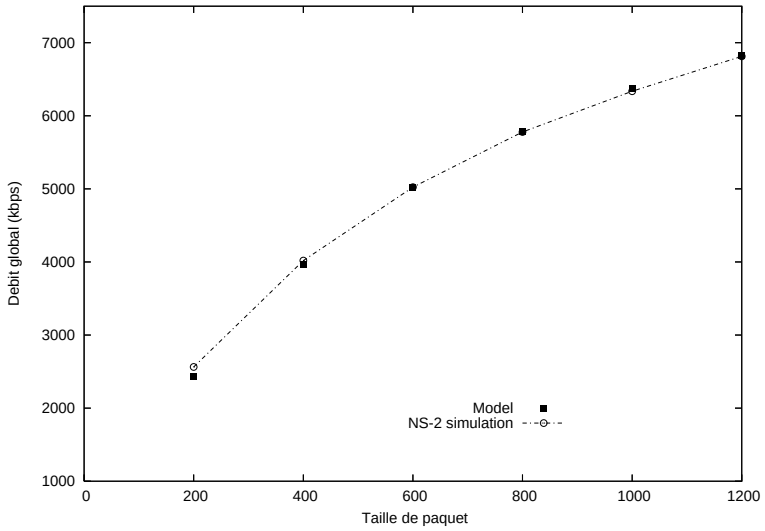


FIG. 3.4: PEPA : Validation par simulation du modèle PEPA (deux stations à portée de communication). Les simulations sont réalisées avec le simulateur NS-2. On compare ici les débits obtenus par simulation et à partir de notre modèle.

802.11 dans le cadre classique de deux stations à portée de communication ayant un récepteur commun (scénario 1). Puis nous étudions le comportement de 802.11 dans le cas classique des stations cachées (scénario 2). Nous nous intéressons ensuite à un cas particulier des stations cachées dans lequel une asymétrie renforce les problèmes liés au stations cachées (scénario 3). Enfin, nous évaluons les performances de 802.11 dans le cadre des 3 paires (scénario 4).

Le scénario 1 est un scénario classique dans lequel très peu de collisions sont présentes grâce au mécanisme d'écoute active du canal. Même si des collisions peuvent survenir, celles-ci peuvent et devraient être évitées/réduites par l'algorithme de backoff employé. Tous les scénarii *ad hoc* (scénarii 2, 3 et 4) ont été présentés dans le chapitre précédent.

À notre avis, ces quatres situations représentent un bon panel des modes d'utilisations du protocole 802.11. Pour bien comprendre l'influence des mécanismes mis en place dans 802.11 tel que le backoff, nous proposons en plus de l'étude de l'algorithme implanté dans 802.11, le Binary Exponential Backoff, d'étudier trois autres algorithmes qui ne servent dans notre cas que de références.

Le reste de cette section est organisé comme suit : nous décrivons d'abord les trois modèles liés aux scénarii 2, 3 et 4. Nous donnons ensuite quelques détails sur les algorithmes de backoff étudiés. Les métriques utilisées pour évaluer les performances de chacun des scénarii sont discutées. Enfin, des résultats de performances sont donnés.

3.3.1 Les topologies

Dans cette sous-section, nous présentons les différentes topologies pour lesquelles nous avons étudié le comportement de 802.11.

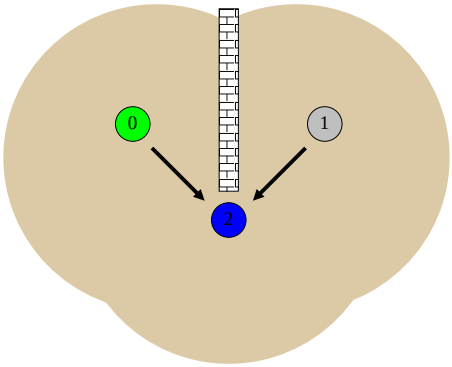


FIG. 3.5: PEPA : La topologie des stations cachées.

Les stations cachées

Dans cette topologie, deux stations sont indépendantes l'une de l'autre mais ont un récepteur commun. Cette situation est présentée sur la figure 3.5. Dans ce scénario, les nœuds émetteurs perçoivent le médium comme occupé, par une transmission autre que la leur, seulement quand ceux-ci reçoivent les acquittements destinés à l'autre station émettrice. Contrairement à la topologie où deux émetteurs sont à portée de communication, les collisions dans ce scénario n'ont pas lieu seulement au début de la transmission. Outre ces deux propriétés, le scénario des nœuds cachés est le même, du moins d'un point de vue de la modélisation, que celui où les deux émetteurs sont à portée de communication.

Le modèle PEPA des nœuds cachés est représenté ci-après :

$$
\begin{array}{lcl}
Med_{00_00} & \stackrel{def}{=} & (transmit, \top).Med_{00_01} \\
Med_{00_01} & \stackrel{def}{=} & (frag, \mu_data10).Med_{00_02} + (transmit, \top).Med_{00_14} \\
... & \stackrel{def}{=} & ... \\
Med_{00_j} & \stackrel{def}{=} & (frag, \mu_data10).Med_{00_(j+1)} + (transmit, \top).Med_{00_14}, \forall j \in [2...9] \\
... & \stackrel{def}{=} & ... \\
Med_{00_10} & \stackrel{def}{=} & (Ack_0, \mu_trans).Med_{00_11} + Ack_1, \mu_trans).Med_{00_12} \\
Med_{00_11} & \stackrel{def}{=} & (sync_0, \mu_data10).Med_{00_00} \\
Med_{00_12} & \stackrel{def}{=} & (sync_1, \mu_data10).Med_{00_00} \\
Med_{00_13} & \stackrel{def}{=} & (collision, \mu_collision).Med_{00_00} + (transmit, \top).Med_{00_14} \\
Med_{00_14} & \stackrel{def}{=} & (collision, \mu_data10).Med_{00_13}
\end{array}
$$

Nous pouvons remarquer dans ce modèle l'absence de l'action de synchronisation $free$ qui n'est pas indispensable dans ce scénario. Pour des raisons de simplification du modèle et de réduction de l'espace d'états cette action à été enlevée. Nous remarquons aussi que la transmission d'un paquet de données, représentée par l'action $frag$, se fait en plusieurs étapes. Ceci est dû au fait que dans PEPA, les actions sont atomiques et une action déclenchée ne peut plus être interrompue. Cette action a une durée de 1/10 de la durée de transmission du paquet entier. Cette valeur a été choisie après plusieurs tests et a montré le meilleur compromis entre le la précision des résultats et la taille de l'espace d'état.

Dans l'état Med_{00_00}, le médium est libre, et peut recevoir une synchronisation sur l'action *trasmit* de l'un des deux émetteurs. L'émetteur ayant envoyé une action de synchronisation commence la transmission de son paquet de données. Durant la transmission de chaque fragment, le

médium peut recevoir une autre action *transmit* provenant de l'autre émetteur. La synchronisation avec ce deuxième accès concurrent provoque une collision modélisée par les états Med_{00_13} et Med_{00_14}. Dans l'état Med_{00_14}, le médium envoie la synchronisation *collision* à la première station et dans l'état Med_{00_13}, il l'envoie à la deuxième. Dans l'état Med_{00_13}, en attendant que la durée de la collision soit écoulée, la première station peut émettre un paquet de données, d'où la présence de l'action *transmit* en concurrence avec l'action *collision*. La durée $mu_collision$ est la même que la durée d'une transmission car elle conduit à la même occupation du canal radio. Notons ici que nous faisons une première hypothèse en supposant que la transmission de l'acquittement n'interrompt pas la décrémentation du backoff de l'autre nœud. La deuxième hypothèse que nous faisons ici est que le temps qui s'écoule dans l'état Med_{00_14} représente le temps de transmission d'un fragment. L'accès à cet état se fait à partir des états Med_{00_j}, $\forall j \in [1...10]$. Ainsi, quel que soit l'état précédent l'état Med_{00_14}, nous supposons que le temps restant à la transmission de la donnée est de μ_data10. Cette hypothèse provoquera clairement une sous-estimation de la probabilité de collision. Enfin, la troisième hypothèse que nous faisons est la non distinction des deux émetteurs après une collision. Cette hypothèse est vraie en moyenne car le choix des deux émetteurs se fait suivant un tirage uniforme, et la durée d'une collision est en moyenne la même pour les deux émetteurs.

La figure 3.6 montre la comparaison du débit d'une station, obtenu par simulation et ceux obtenu par notre modèle. Comme attendu, notre modèle surestime le débit dû aux hypothèses faites précédemment.

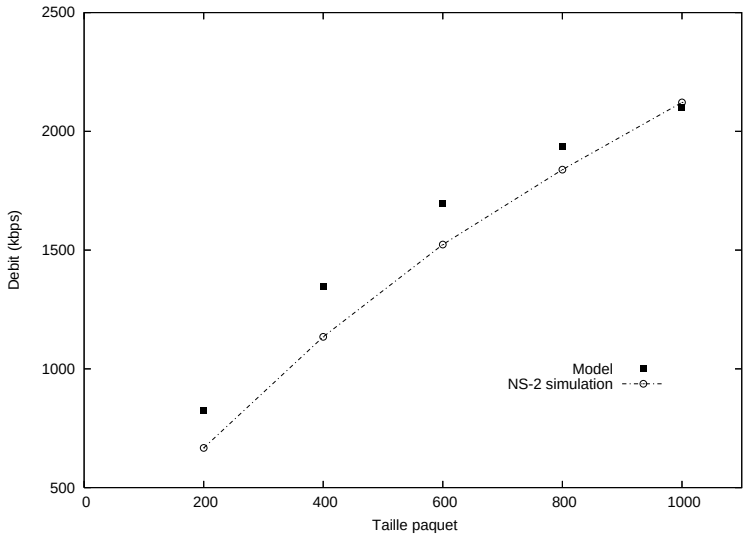


FIG. 3.6: PEPA : Validation par simulation du modèle PEPA (stations cachées). Les simulations sont réalisées avec le simulateur NS-2. On compare ici les débits obtenus par simulations et à partir de notre modèle.

Comme indiqué plus haut, nous avons retiré l'action de synchronisation $free$ de notre composante pour ce modèle. Il y a deux manières simples de modifier le modèle pour prendre ce changement en compte. La première est de retirer l'action $free$ de l'ensemble de synchronisation dans le modèle général. La deuxième est de modifier la composante méthode d'accès en retirant l'action $free$. Bien que la première soit plus commode, la deuxième méthode à l'avantage de réduire encore plus l'espace d'état du modèle. Toutes les autres composantes ne subissent aucune modification.

Ce premier modèle est celui représentant la méthode d'accès basique de 802.11. Le modèle suivant

montre la méthode d'accès avec RTS/CTS. Ce modèle est plus simple que le précédent car la transmission du paquet n'est pas fragmentée. Nous supposons ici que les collisions ne sont effectives que sur le paquet RTS, et que si celui-ci est transmis correctement, alors, le reste de l'echange (CTS/DATA/ACK) sera aussi correct. L'état Med_{00_00} est l'état initial de la composante dans lequel celle-ci attend la réception d'un RTS. Chacune des deux stations peut prendre possession du médium dans cet état et les deux stations ne sont pas différenciées. C'est dans l'état Med_{00_01} que la transmission du RTS est vraiment effective celle-ci étant en concurrence avec la transmission de la seconde station. En cas de transmission simultanée, la composante progresse dans l'état Med_{00_07} puis Med_{00_06} dans lesquels une notification de collision est envoyée à chaque station. Notons ici que la collision a une durée de μ_rts. Si au contraire, la transmission du RTS se fait correctement, un acquittement est envoyé, cet acquittement ayant comme durée μ_data, du reste de l'échange (CTS/DATA/ACK).

$$
\begin{array}{lcl}
Med_{00_00} & \stackrel{def}{=} & (transmit, infty).Med_{00_01}; \\
Med_{00_01} & \stackrel{def}{=} & (RTS, \mu_rts).Med_{00_02} + (transmit, infty).Med_{00_07}; \\
Med_{00_02} & \stackrel{def}{=} & (stop, \mu_trans).Med_{00_03}; \\
Med_{00_03} & \stackrel{def}{=} & (Ack_1, \mu_data).Med_{00_04} + (Ack_0, \mu_data).Med_{00_05}; \\
Med_{00_04} & \stackrel{def}{=} & (sync_1, \mu_trans).Med_{00_00}; \\
Med_{00_05} & \stackrel{def}{=} & (sync_0, \mu_trans).Med_{00_00}; \\
Med_{00_06} & \stackrel{def}{=} & (collision, \mu_rts).Med_{00_00} + (transmit, infty).Med_{00_07}; \\
Med_{00_07} & \stackrel{def}{=} & (collision, \mu_trans).Med_{00_06};
\end{array}
$$

Les stations cachées asymétriques

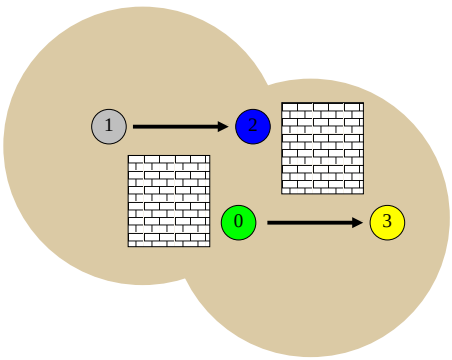


FIG. 3.7: PEPA : La topologie des nœuds cachés asymétriques.

Cette topologie est similaire à celle des nœuds cachés hormis le fait que les deux stations émettrices, ici $\{0, 1\}$ n'ont pas le même récepteur (figure 3.7). Dans cette situation, les deux stations perçoivent toujours le médium comme libre. dans ce cas comme dans le cas du nœud caché nous pouvons retirer l'action $free$ du modèle. En revanche, toutes les transmissions de la station 0 seront correctes tandis que celles de la station 1 pourront entrer en collision. Dans cette optique, et contrairement au modèle des nœuds cachées, il faudra différencier la transmission des deux stations.

Le modèle PEPA de ce scénario est présenté ci-après :

$$
\begin{array}{lcl}
Med_{00_00} & \stackrel{def}{=} & +(transmit_0, \top).Med_{00_01} + (transmit_1, \top).Med_{00_05}; \\
Med_{00_(i)} & \stackrel{def}{=} & (frag, \mu_{data25}).Med_{00_(i+1)} + (transmit_1, \top).Med_{00_(i+8)}; i \in [1 \ldots 3] \\
Med_{00_04} & \stackrel{def}{=} & (Ack_0, \mu_{data25}).Med_{00_00} + (transmit_1, \top).Med_{00_12}; \\
Med_{00_(i)} & \stackrel{def}{=} & (frag, \mu_{data25}).Med_{00_(i+1)} + (transmit_0, \top).Med_{00_(i+8)}; i \in [5 \ldots 7] \\
Med_{00_08} & \stackrel{def}{=} & (Ack_1, \mu_{data25}).Med_{00_00} + (transmit_0, \top).Med_{00_16}; \\
Med_{00_09} & \stackrel{def}{=} & (Ack_0, \mu_{data100}).Med_{00_20}; \\
Med_{00_10} & \stackrel{def}{=} & (Ack_0, \mu_{data75}).Med_{00_19}; \\
Med_{00_11} & \stackrel{def}{=} & (Ack_0, \mu_{data50}).Med_{00_18}; \\
Med_{00_12} & \stackrel{def}{=} & (Ack_0, \mu_{data25}).Med_{00_17}; \\
Med_{00_13} & \stackrel{def}{=} & (collision_1, \mu_{collision100}).Med_{00_04}; \\
Med_{00_14} & \stackrel{def}{=} & (collision_1, \mu_{collision75}).Med_{00_03}; \\
Med_{00_15} & \stackrel{def}{=} & (collision_1, \mu_{collision50}).Med_{00_02}; \\
Med_{00_16} & \stackrel{def}{=} & (collision_1, \mu_{collision25}).Med_{00_01}; \\
Med_{00_(i)} & \stackrel{def}{=} & (frag, \mu_{collision25}).Med_{00_(i+1)} + (transmit_0, \top).Med_{00_(i-4)}; i \in [17 \ldots 19] \\
Med_{00_20} & \stackrel{def}{=} & (collision_1, \mu_{collision25}).Med_{00_00} + (transmit_0, \top).Med_{00_16};
\end{array}
$$

Dans ce modèle, les actions indiquées par 0 (respectivement 1) sont les actions utilisées pour la station 0 (respectivement 1). Dans l'état Med_{00_00}, les deux stations peuvent transmettre leurs paquets. Il faut noter que comme pour les stations cachées, une fragmentation de la transmission est faite. Dans ce cas, le meilleur compromis de fragmentation est 4 fragments. Quand la station 1 transmet, le modèle se retrouve dans les états [5..8] durant lesquels, le nœud transmet son paquet. Durant la transmission, la station 0 peut aussi commencer sa transmission d'où les activités concurrentes avec $transmit_0$. De manière analogue, si la première station à transmettre est la station 0, la composante se retrouve dans les états [1..4] et ces actions sont concurrentes avec l'action $transmit_1$. Supposons maintenant que la station 1 est la première à transmettre, l'état du médium est ensuite Med_{00_05}. Pendant que la station 1 transmet son premier fragment si la station 0 débute à son tour sa transmission, la composante évolue dans l'état Med_{00_13}. Notons que la durée $\mu_{collisionX}$ où $X = \{25, 50, 75, 100\}$ représente le temps restant à transmettre pour le paquet en cours de la station 1. Suivant le moment où la station 0 débute sa transmission, la composante va évoluer vers les états Med_{00_13} à Med_{00_16}. Durant ces états, le médium spécifie à la station 1 que sa transmission est entrée en collision avec l'action $collision_1$. Après cette action, la composante évolue dans l'un des états Med_{00_01} à Med_{00_04} pour terminer la transmission de la station 0. Durant la fin de la transmission de la station 0, la station 1 peut de nouveau accéder au médium. Dans ce cas, la transmission de la station 0 est terminée par l'envoi d'un acquittement (états Med_{00_09} à Med_{00_12}) dont la durée dépend des fragments déjà transférés. La composante évolue ensuite dans l'un des états Med_{00_17} à Med_{00_20} qui correspondent à l'envoi des fragments de paquet restant et déjà entrés en collision de la station 1.

Ici, contrairement au modèle des nœuds cachés, nous n'avons aucune hypothèse forte liée au modèle. La figure 3.8 montre les résultats obtenus avec notre modèle et ceux obtenus par simulations.

Les autres composantes ne sont modifiées que pour les noms des nouvelles actions et pour la suppression de l'action $free$.

Les trois paires

Nous présentons dans cette section, le modèle PEPA associé au trois paires (voir figure 3.9). Dans cette topologie, les deux paires extérieures sont indépendantes alors que la paire centrale est

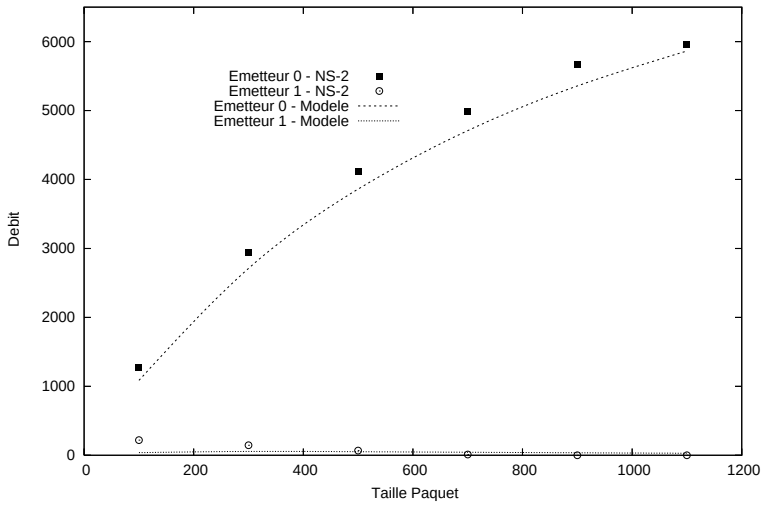


FIG. 3.8: PEPA : Validation par simulation du modèle PEPA (stations cachées asymétriques). Les simulations sont réalisées avec le simulateur NS-2. On compare ici les débits obtenus par simulation et à partir de notre modèle. Les résultats montrent le débit obtenu par les stations 0 et 1.

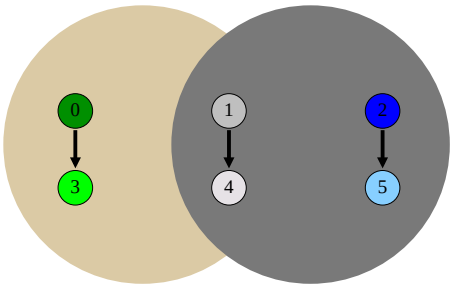


FIG. 3.9: La topologie des 3 paires.

à portée de communication des deux autres paires. Ici, nous supposons qu'aucune collision ne peut se produire car l'émetteur est le récepteur de chaque paire sont assez proches pour pouvoir décoder le paquet correspondant.

Le modèle PEPA correspondant à ce scénario est présenté ci-après. Dans ce modèle, les actions sont indiquées par rapport au numéro de la station. Ici comme dans les modèles précédents, la transmission des deux paires extérieures a été divisée en fragments car la transmission d'une paire extérieure peut commencer à n'importe quel moment de la transmission de l'autre paire extérieure.

$$
\begin{aligned}
Med_{00_00} &\overset{def}{=} (free_0, \top).Med_{00_00} + (transmit_0, \top).Med_{00_02} \\
&\quad + (free_1, \top).Med_{00_00} + (transmit_1, \top).Med_{00_01} \\
&\quad + (free_2, \top).Med_{00_00} + (transmit_2, \top).Med_{00_09}; \\
Med_{00_01} &\overset{def}{=} (Ack_1, \mu_{data}).Med_{00_00}; \\
Med_{00_02} &\overset{def}{=} (frag, \mu_{data25}).Med_{00_03} + (free_2, \mu_{trans}).Med_{00_02}; \\
Med_{00_03} &\overset{def}{=} (frag, \mu_{data25}).Med_{00_04} + (free_2, \mu_{trans}).Med_{00_03} + (transmit_2, \top).Med_{00_06}; \\
Med_{00_04} &\overset{def}{=} (frag, \mu_{data25}).Med_{00_05} + (free_2, \mu_{trans}).Med_{00_04} + (transmit_2, \top).Med_{00_07}; \\
Med_{00_05} &\overset{def}{=} (Ack_0, \mu_{data25}).Med_{00_00} + (free_2, \mu_{trans}).Med_{00_05} + (transmit_2, \top).Med_{00_08}; \\
Med_{00_06} &\overset{def}{=} (Ack_0, \mu_{data75}).Med_{00_11}; \\
Med_{00_07} &\overset{def}{=} (Ack_0, \mu_{data50}).Med_{00_10}; \\
Med_{00_08} &\overset{def}{=} (Ack_0, \mu_{data25}).Med_{00_09}; \\
Med_{00_09} &\overset{def}{=} (frag, \mu_{data25}).Med_{00_10} + (free_0, \mu_{trans}).Med_{00_09}; \\
Med_{00_10} &\overset{def}{=} (frag, \mu_{data25}).Med_{00_11} + (free_0, \mu_{trans}).Med_{00_10} + (transmit_0, \top).Med_{00_13}; \\
Med_{00_11} &\overset{def}{=} (frag, \mu_{data25}).Med_{00_12} + (free_0, \mu_{trans}).Med_{00_11} + (transmit_0, \top).Med_{00_14}; \\
Med_{00_12} &\overset{def}{=} (Ack_2, \mu_{data25}).Med_{00_00} + (free_0, \mu_{trans}).Med_{00_12} + (transmit_0, \top).Med_{00_15}; \\
Med_{00_13} &\overset{def}{=} (Ack_2, \mu_{data75}).Med_{00_04}; \\
Med_{00_14} &\overset{def}{=} (Ack_2, \mu_{data50}).Med_{00_03}; \\
Med_{00_15} &\overset{def}{=} (Ack_2, \mu_{data25}).Med_{00_02};
\end{aligned}
$$

Dans ce modèle, l'action $free$ est restaurée. Après avoir testé si le médium est libre, l'un des nœuds peut transmettre son paquet. Si c'est la paire centrale, elle transmet son paquet entièrement en bloquant l'accès ($free$) aux deux autres stations. Si en revanche, l'une des paires extérieures accède au médium, celle-ci bloque la paire centrale mais ne bloque pas l'autre paire extérieure, d'où la présence des actions concurrentes $free$ dans les états Med_{00_02} à Med_{00_04} et Med_{00_09} à Med_{00_12}, suivant laquelle des deux paires extérieures a accédé la première au médium. Comme pour le modèle des nœuds cachés asymétriques, si deux transmissions des paires extérieures se chevauchent, la première est d'abord terminée (états Med_{00_05} à Med_{00_08} et Med_{00_12} à Med_{00_15}) en s'appuyant sur le temps restant en fonction des fragments déjà transmis, ensuite la deuxième transmet le reste de ses fragments. Durant cette transmission, l'autre nœud peut de nouveau accéder au médium. Si aucun autre accès simultané des paires extérieures n'a lieu, le médium revient dans l'état Med_{00_00} à la fin des transmissions.

Pour ce modèle, nous avons modifié la composante représentant la méthode d'accès pour refléter le déclenchement ou non du mécanisme de l'EIFS décrit dans le standard 802.11. Ce mécanisme est déclenché pour remplacer le DIFS quand une transmission ne pouvant être décodée a lieu sur le médium radio. Notons que la durée d'un EIFS correspond à la durée de transmission d'un acquittement incluant le SIFS. C'est le cas observé quand les paires sont assez éloignées pour ne pas pouvoir décoder les paquets les uns des autres mais assez proches pour se gêner et percevoir le médium comme occupé. Le modèle de la méthode d'accès est représenté ci-après.

$$
\begin{aligned}
E_{i_000} &\stackrel{def}{=} (free_i, \mu_{trans}).E_{i_001};\\
E_{i_001} &\stackrel{def}{=} (difs, \mu_{difs}).E_{i_002};\\
E_{i_002} &\stackrel{def}{=} (free_i, \mu_{trans}).E_{i_003} + (occ, \mu_{slot}).E_{i_007};\\
E_{i_003} &\stackrel{def}{=} (db_i, \top).E_{i_004};\\
E_{i_004} &\stackrel{def}{=} (free_i, \mu_{trans}).E_{i_005} + (occ, \mu_{slot}).E_{i_007};\\
E_{i_005} &\stackrel{def}{=} (transmit, \mu_{trans}).E_{i_006};\\
E_{i_006} &\stackrel{def}{=} (ack_i, \top).E_{i_000};\\
E_{i_007} &\stackrel{def}{=} (free, \mu_{trans}).E_{i_008};\\
E_{i_008} &\stackrel{def}{=} (eifs, \mu_{difs}).E_{i_002};
\end{aligned}
$$

Ce modèle correspond exactement au modèle du nœud donné dans la section précédente. La seule différence est que si le médium est perçu comme occupé dans les états E_{i_002} et E_{i_004} dû à l'impossibilité pour l'action $free$ de se synchroniser, au lieu de revenir dans l'état E_{i_000} la composante évolue vers l'état E_{i_007}. Dans cet état l'attente d'un EIFS est déclenché. De E_{i_007} la composante évolue vers l'état E_{i_008} et ensuite reprend la procédure de transmission normale. Un fois une transmission effectuée correctement, le nœud retourne dans l'état E_{i_000} (à partir de l'état E_{i_006}) et utilise un DIFS pour sa nouvelle transmission. Notons que ce mécanisme rend 802.11 moins équitable dans ce cas, car un nœud ayant accédé au médium attendra moins longtemps qu'un nœud n'ayant pas accédé au médium quand le médium sera de nouveau libre.

Ici, aucune hypothèse de modélisation n'a été faite. La figure 3.10 compare les résultats des débits obtenus avec notre modèle et ceux obtenus par simulation. Notons que sur la figure, nous n'avons tracé les courbes que de l'une des paires extérieures car les deux paires présentent le même comportement. Dans les résultats montrés ici, les nœuds utilisent le mécanisme d'EIFS. Sur cette figure, nous voyons encore une fois la précision de notre modèle.

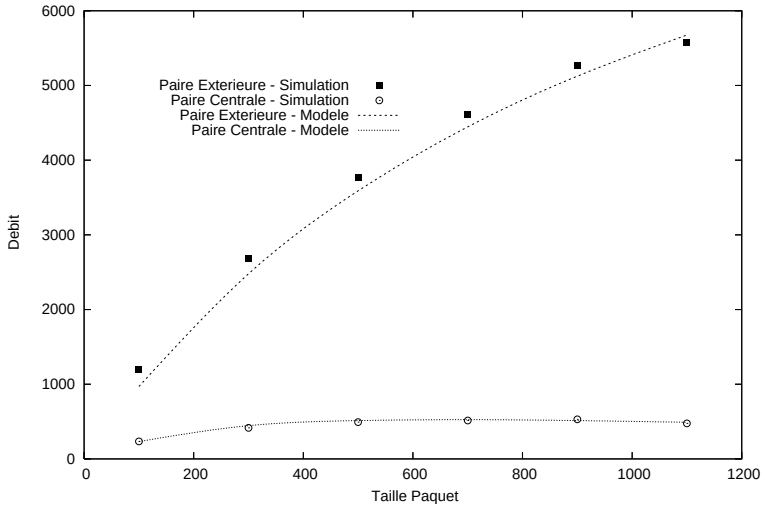


FIG. 3.10: PEPA : Validation par simulation du modèle PEPA (3 paires). Les simulations sont réalisées avec le simulateur NS-2. On compare ici les débits obtenus par simulation et à partir de notre modèle. Les résultats montrent le débit obtenu par la paire centrale et une des paires extérieures.

3.3.2 Les algorithmes de backoff

Dans cette section, nous présentons quelques algorithmes de backoff que nous avons modélisés en utilisant PEPA. Comparée aux autres composantes, la modélisation de nouveaux algorithmes de backoff est très simple. Les deux caractéristiques principales des algorithmes de backoff conçus pour les réseaux sans fil sont la méthode d'incrémentation et la méthode de décrementation, étant données les tailles de fenêtre de contention minimale et maximale.

Un algorithme simple a modéliser est l'algorithme nommé *Double Increase, Double Decrease* [12] ou DIDD. Cet algorithme est conçu pour être moins agressif que l'algorithme BEB implémenté dans le standard de 802.11. Dans DIDD, après une collision, la fenêtre de contention est doublée, comme avec BEB, et après une collision, celle-ci est divisée par deux. Dans cet algorithme, la fenêtre de contention n'est pas réinitialisée après un certain nombre de transmissions incorrectes. Le modèle PEPA correspondant à cet algorithme est le suivant :

$$
\begin{array}{lcl}
BO_{i_0} & \stackrel{def}{=} & (db_i, f_0).BO_{i_0} + (succ_i, \top).BO_{i_0} + (coll_i, \top).BO_{i_1} \\
... & \stackrel{def}{=} & ... \\
BO_{i_j} & \stackrel{def}{=} & (db_i, f_j).BO_{i_j} + (succ_i, \top).BO_{i_(j-1)} + (coll_i, \top).BO_{i_(j+1)}, \forall j \in [1..4] \\
... & \stackrel{def}{=} & ... \\
BO_{i_5} & \stackrel{def}{=} & (db_i, f_5).BO_{i_5} + (succ_i, \top).BO_{i_4} + (coll_i, \top).BO_{i_5}
\end{array}
$$

De la même manière, nous pouvons modéliser d'autres algorithmes de backoff tels que *Multiplicative Increase*, *Linear Decrease* [5] (MILD) où la méthode de décrémentation est encore moins agressive que celle de DIDD, la méthode d'incrémentation restant la même. Le modèle de cet algorithme de backoff est le suivant :

$$
\begin{array}{lcl}
BO_{i_0} & \stackrel{def}{=} & (db_i, f_0).BO_{i_0} + (succ_i, \top).BO_{i_0} + (coll_i, \top).BO_{i_1} \\
... & \stackrel{def}{=} & ... \\
BO_{i_j} & \stackrel{def}{=} & (db_i, f_j).BO_{i_j} + (succ_i, \top).BO_{i_(j-1)} + (coll_i, \top).BO_{i_(2\times j+1)}, \forall j \in [1..30] \\
... & \stackrel{def}{=} & ... \\
BO_{i_31} & \stackrel{def}{=} & (db_i, f_31).BO_{i_31} + (succ_i, \top).BO_{i_30} + (coll_i, \top).BO_{i_31}
\end{array}
$$

Pour cet algorithme de backoff, nous avons choisi une décrémentation linéaire de 32, c'est-à-dire qu'après une transmission correcte, la valeur de la nouvelle fenêtre de backoff est : $CW_{new} = CW - 32$. Ceci permet de limiter à 32 le nombre d'états de backoff possible.

Le dernier backoff que nous avons modélisé est un simple exemple pour montrer les possibilités de modélisation offertes par notre modèle. Nous l'avons appelé BEB inversé. Cet algorithme diminue sa fenêtre de contention par deux après une collision et se place dans l'état le plus grand après une transmission avec succès. Le modèle PEPA de cet algorithme est le suivant :

$$
\begin{array}{lcl}
BO_{i_0} & \stackrel{def}{=} & (db_i, f_0).BO_{i_0} + (succ_i, \top).BO_{i_5} + (coll_i, \top).BO_{i_0} \\
... & \stackrel{def}{=} & ... \\
BO_{i_j} & \stackrel{def}{=} & (db_i, f_j).BO_{i_j} + (succ_i, \top).BO_{i_5} + (coll_i, \top).BO_{i_(j-1)} \\
... & \stackrel{def}{=} & ... \\
BO_{i_5} & \stackrel{def}{=} & (db_i, f_5).BO_{i_5} + (succ_i, \top).BO_{i_5} + (coll_i, \top).BO_{i_4}
\end{array}
$$

Il faut noter que dans tous ces algorithmes, les valeurs de f_j peuvent être différentes.

3.3.3 Les métriques

Efficacité

Comme métrique d'efficacité nous considérons les différents taux liés aux états du canal. Nous donnons par exemple le taux d'occupation correcte du médium, le taux de collision, et le taux correspondant à un médium radio libre. Ces taux ou probabilités sont faciles à obtenir à partir de notre modèle. Par exemple, on peut facilement obtenir la probabilité de collision en calculant la probabilité pour la chaîne de Markov dérivée du modèle PEPA de se trouver dans les états Med_{00_04} et Med_{00_05} pour une topologie où les deux nœuds sont à portée de communication.

Équité

Une nouvelle métrique : La métrique d'équité que nous utilisons n'est pas celle généralement utilisée dans la littérature qui s'appuie sur la différence des débits de chaque émetteur. La métrique d'équité que nous proposons s'affranchit du calcul du débit, bien qu'il soit possible de le calculer avec notre modèle. De plus, cette métrique, contrairement aux métriques liées au débit, fournit une indication sur le partage à court terme de l'accès au médium. Nous proposons comme métrique d'équité la probabilité qu'une station monopolise le médium radio. Ce que nous entendons ici par monopoliser, c'est qu'une des stations transmet successivement et correctement plusieurs de ces paquets. Pour ce faire, nous donnons la probabilité pour qu'un émetteur ayant transmis correctement et successivement i paquets transmette le $i+1^{eme}$ paquet correctement (sans retransmission), et ce sans qu'aucun autre émetteur n'ait transmis de paquet avant la transmission de ce $i+1^{eme}$ paquet.

Pour calculer cette métrique, il nous a fallu modifier le modèle des topologies comme suit.

$Med_{(i-1)_j}$	$\stackrel{def}{=}$	$j = 0...6$
...	$\stackrel{def}{=}$	...
Med_{i_00}	$\stackrel{def}{=}$	$(free, \top).Med_{i_00} + (transmit, \top).Med_{i_01}$;
Med_{i_01}	$\stackrel{def}{=}$	$(free, \top).Med_{i_01} + (go_{next}, \mu_{slot}).Med_{i_02} + (transmit, \top).Med_{i_05}$;
Med_{i_02}	$\stackrel{def}{=}$	$(ack_n, \mu_{trans}).Med_{i_03} + (ack_m, \mu_{trans}).Med_{i_04}$;
Med_{i_03}	$\stackrel{def}{=}$	$(sync_n, \mu_{data}).Med_{0_00}$;
Med_{i_04}	$\stackrel{def}{=}$	$(sync_m, \mu_{data}).Med_{(i+1)_00}$;
Med_{i_05}	$\stackrel{def}{=}$	$(collision, \mu_{trans}).Med_{i_06}$;
Med_{i_06}	$\stackrel{def}{=}$	$(collision, \mu_{data}).Med_{0_00}$;
...	$\stackrel{def}{=}$	...
$Med_{(i+1)_j}$	$\stackrel{def}{=}$	$j = 0...6$

Ce modèle représente la topologie pour deux nœuds à portée de communication. Ici, le médium change d'étape i quand le nœud m transmet un paquet correctement. Ce changement d'étape est fait dans l'état Med_{i_04}. S'il y a une collision durant cette transmission, l'étape du médium revient à 0 (ceci est fait dans l'état Med_{i_06}) et si le nœud n transmet correctement un paquet, le médium revient dans l'étape 0 (état Med_{i_03}). À chaque étape i, la probabilité α_i que la transmission de m soit correcte est donnée par le rapport : $\alpha_i = \dfrac{P_{Med_{i_04}}}{P_{Med_{i_03}} + P_{Med_{i_04}} + P_{Med_{i_06}}}$ où $P_{Med_{i_04}}$ est la probabilité d'être dans l'état Med_{i_04}. Tous les modèles de médium que nous avons permettent

d'obtenir notre métrique d'équité en faisant cette duplication. Il faut noter qu'en calculant cette métrique, nous augmentons considérablement le nombre d'états dans le modèle.

Ainsi, si la courbe des α_i est croissante, cela veut dire qu'un nœud qui transmet correctement et successivement sur le médium aura tendance à monopoliser le médium et ainsi à empêcher les autres stations émettrices d'accéder au médium. Une fonction décroissante ou constante de α_i est alors un comportement équitable.

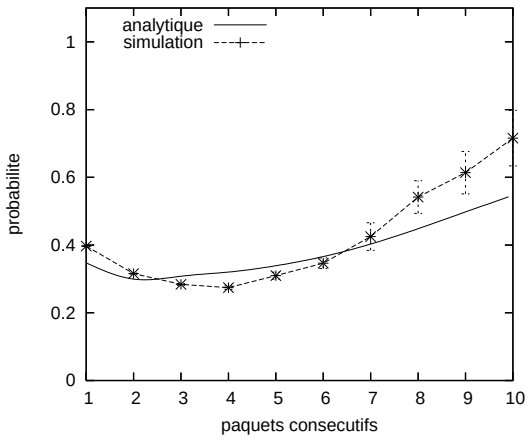
Notons que cette métrique peut être facilement calculée avec notre modèle alors que par simulation, celle-ci est un peu plus complexe à mettre en œuvre. Ceci est dû au fait que nous représentons toutes les interactions dans une même composante. En simulation, la simplicité de mise en œuvre de cette métrique dépend de la topologie. Mais dans un cas général, le calcul de cette métrique doit être mis en place sur l'émetteur et le récepteur d'un flux (sous-entendu à un saut), et un traitement *a posteriori* doit être effectué pour obtenir les α_i.

Il est aussi important de noter que les résultats dérivés de cette métrique sont très dépendants des hypothèses de modélisation faites précédemment, notamment, de l'approximation des temps fixes, et de la représentation du tirage aléatoire du *backoff*. Les résultats d'équité donnent donc une idée du comportement du protocole et non pas un comportement précis de celui-ci.

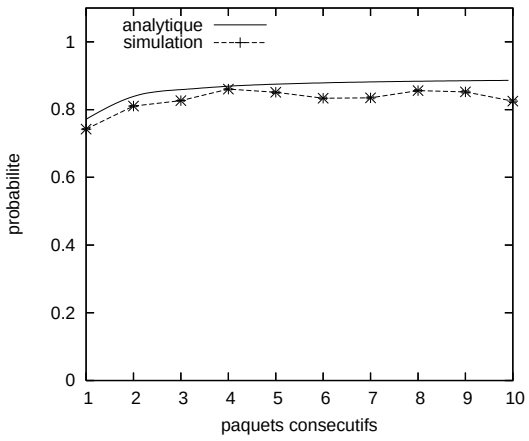
Validation : Pour valider cette métrique d'équité, nous avons modifié le simulateur NS-2 [60] pour permettre le calcul des α_i. Les simulations ont été menées sur 3 scénarii : 2 stations à portée de communication, les stations cachées et les 3 paires. Les résultats présentés sur les figures 3.11(a), 3.11(b) et 3.11(c) montrent la comparaison entre les résultats obtenus par simulation et les résultats obtenus à partir de notre modèle. Ces résultats sont obtenus avec 802.11 utilisant l'algorithme du *Binary Exponential Backoff*.

Ces figures montrent que même si les courbes obtenus à partir de notre modèle ne correspondent pas exactement, les allures des courbes sont les mêmes, plus spécialement pour le scénario avec deux stations à portée de communication et pour les stations cachées. Pour le scénario des trois paires, nous présentons les résultats obtenus quand les paires extérieures sont à portée de communication de la paire centrale. L'écart entre les résultats de simulation et les résultats tirés de notre modèle est dû à l'approximation des durées du DIFS et du backoff (ce sont les hypothèses importantes que nous faisons sur ce scénario). Notons que la taille des intervalles de confiance au point k donne une idée du nombre de fois où la station a atteint α_k. Par exemple dans le cas du scénario des trois paires, l'intervalle de confiance pour $i = 4$ dénote le fait que durant les simulations, la paire centrale a très peu réussi à envoyer 4 paquets consécutivement. Quand cet intervalle est grand, la valeur obtenue n'est, dans la plupart des cas, pas significative.

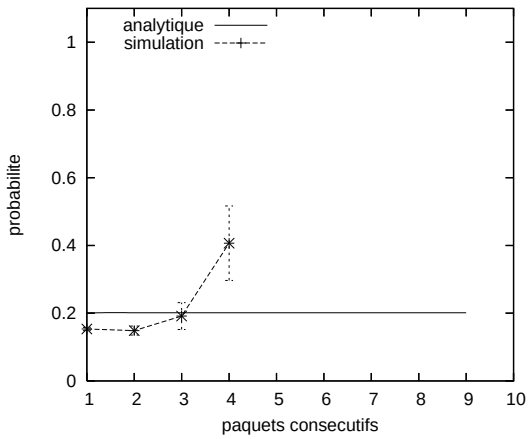
Nous pouvons voir pour le scénario avec deux stations à portée de communication et pour les stations cachées que l'approximation des temps fixes tels que le DIFS n'a aucune influence. En reglè générale les hypothèses réalisées sur ces deux scénarii n'influent pas les résultats d'équité. Ceci est dû au fait que le temps DIFS n'est pas en concurrence comme pour les 3 paires avec un temps EIFS. Nous pouvons aussi remarquer que pour les deux premiers scénarii, l'approximation du backoff par sa moyenne n'influence pas fortement la métrique d'équité. La validation pour les stations cachées asymétriques n'a pas été présentée, car pour une taille de paquet de 1000 octets transmis à 11 Mbps et avec 802.11, la probabilité de collision pour la paire subissant les collisions est de 1 et de 0 pour la paire n'en subissant pas.



(a) 2 stations à portée de communications



(b) Les stations cachées



(c) Les trois paires

FIG. 3.11: PEPA : Validation de la métrique d'équité α_i.

3.3.4 Résultats

Dans cette section, nous présentons une sélection de résultats numériques extraits de notre modèle. Les résultats présentés ont les hypothèses communes suivantes :

- Les nœuds génèrent du trafic à saturation.
- La couche radio est idéale ; les seules pertes sont dues aux collisions au niveau MAC.
- Les résultats d'équité sont obtenus en utilisant des paquets 1000 octets.

Le scénario normal

Dans cette section, nous présentons les résultats liés a notre modèle pour le scénario où deux nœuds à portée de communication transmettent vers un récepteur commun. Les résultats présentés dans la figure 3.12(a) montrent le taux d'occupation correcte du canal radio en fonction du temps. Dans ce scénario, l'augmentation de la taille du paquet augmente le taux d'occupation correcte

du canal radio. Ce taux d'occupation reste inférieur à 1 à cause de la surcharge due au protocole (backoff).

Cette figure montre que les trois algorithmes de backoff MILD, DIDD, et BEB ont le même comportement d'un point de vue de l'efficacité. Ceci est confirmé par la figure 3.12(c) qui montre le taux de collision et la figure 3.12(b) qui montre le taux durant lequel le canal radio est libre. Ce comportement similaire est dû à l'état initial des 3 algorithmes de backoff et au faible taux de collision. Le cas de BEB INV montre clairement l'influence du choix de l'état initial de l'algorithme du backoff dans ce scénario.

La figure 3.12(d) montre l'évolution de α_i pour les 4 algorithmes de backoff étudiés. Je rappelle que les courbes des α_i ne sont pas des résultats précis, à cause des hypothèses faites dans notre modèle, plus particulièrement, concernant les approximations des temps fixes et le tirage aléatoire du backoff. Cependant, les courbes tracées sur la figure 3.12(d) sont de bonnes indications sur le comportement, des algorithmes de backoff d'un point de vue de l'équité. Cette figure montre un comportement équitable de BEB INV avec une fonction α_i constante. Les fonctions de DIDD, MILD et BEB sont, quant à elles croissantes, ce qui peut s'interpréter comme un comportement inéquitable de ces algorithmes.

Il est cependant à noter que les α_i décroissent pour BEB, DIDD, et MILD pour les valeurs de $i \leq 2$. Ceci traduit le comportement des algorithmes de backoff qui décrémentent un backoff restant en cas d'interruption.

Pour $i > 2$, les α_i croissent. Cet accroissement est dû aux collisions pouvant survenir dans ce scénario et provoquant une asymétrie dans les tailles des fenêtres de contention utilisées pour le tirage du *backoff*. En cas de collision, les deux stations augmentent leur fenêtre de contention. La première station qui finit de transmettre réduit sa fenêtre de contention et augmente ainsi sa probabilité d'accéder au médium, tandis que l'autre station maintient une grande fenêtre de contention.

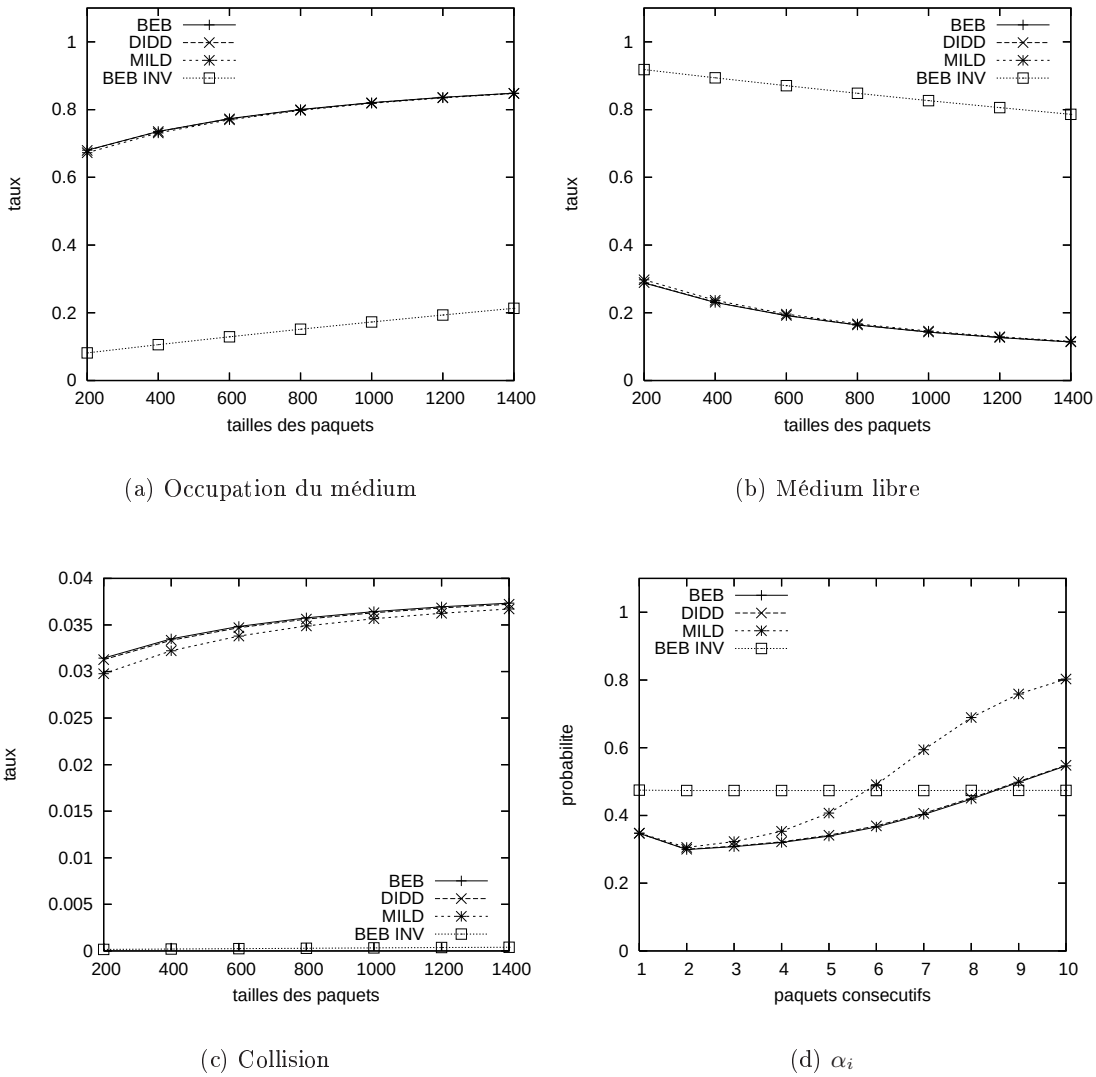
Bien que les α_i représentent clairement une métrique d'équité à court et à long terme, celle-ci est à prendre avec précaution. Dans la figure 3.12(d), on montre que la probabilité pour MILD de transmettre le 10^{ime} paquet successivement et avec succès est de 80%. Ceci exprime bien un comportement inéquitable de l'agorithme. Cependant, la probabilité de transmettre 10 paquets consécutifs est très faible (multiplication de chaque α_i).

Ce premier scénario ne présente pas de problème de performance et d'équité particulier. Bien sûr les performances pourraient être optimisées s'il était possible de réduire le ratio entre les entêtes protocolaires (temps passé à décrémenter le backoff) et la transmission des données elle-même. Pour ce faire une solution serait d'introduire un accès TDMA. Cet accès TDMA aurait aussi une bonne influence sur l'équité car elle réduirait à 0 la probabilité de transmettre 2 paquets consécutifs. Même si l'idéal pour ce scénario est d'avoir un accès TDMA, les résultats obtenus ici sont acceptables. Il est même possible d'augmenter les performances simplement en réduisant la taille de la fenêtre de l'algorithme de backoff . Cette réduction augmenterait le taux de collision mais celui-ci étant très faible, nous pensons que les performances seraient améliorées.

Les nœuds cachés

Dans cette section, nous présentons les résultats obtenus à partir de notre modèle sur le scénario des nœuds cachés. Les résultats des figures 3.13(a), 3.13(b), 3.13(c) montrent respectivement les taux d'occupation correcte du médium, le taux durant lequel le médium est libre et le taux de collision.

Nous voyons sur la figure 3.13(a) pour BEB et DIDD que l'augmentation de la taille des paquets



(a) Occupation du médium

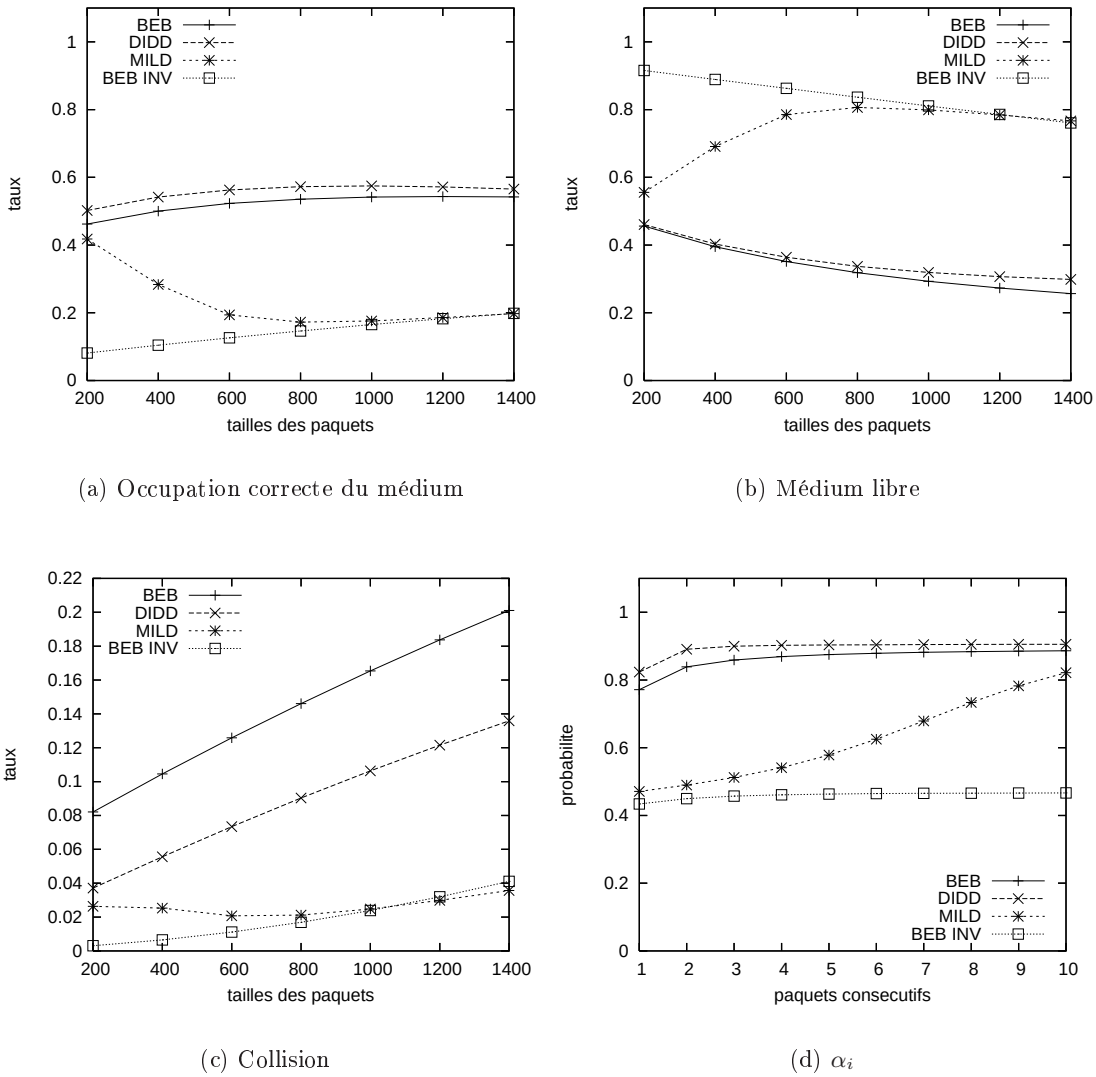
(b) Médium libre

(c) Collision

(d) α_i

FIG. 3.12: PEPA : Résultats de performance (deux stations à portée de communication). Les performances caclculées sont : le taux d'occupation correcte du médium, le taux de médium libre, le taux de collision et les courbes des α_i. Ces performances sont données pour différentes taille de paquet et pour les 4 algorithmes de backoff. Les α_i sont calculés pour une taile de paquet de 1000 octets

n'augmente pas considérablement le taux d'utilisation correcte du canal radio. Ceci est dû au fait que, dans le scénario des stations cachées, une transmission n'est correcte que si celle-ci a lieu dans l'intervalle de backoff de l'autre station. De ce fait, l'augmentation de la taille des paquets peut réduire le taux d'occupation du médium. Ce comportement est confirmé par la figure 3.13(c) qui montre clairement l'évolution du taux de collision en fonction de la taille des paquets pour BEB et DIDD. Si le taux de collision de BEB et plus élevé que celui de DIDD, ceci est dû au fait que DIDD est moins agressif dans la réduction de sa fenêtre de contention et permet ainsi plus de transmissions correctes.



(a) Occupation correcte du médium

(b) Médium libre

(c) Collision

(d) α_i

FIG. 3.13: PEPA : Résultats de performance (stations cachées). Les performances caclculées sont le taux d'occupation correcte du médium, le taux de médium libre, le taux de collision et les courbes des α_i. Ces performances sont données pour différentes tailles de paquets et pour les 4 algorithmes de backoff. Les α_i sont calculés pour une taille de paquets de 1000 octets

Pour l'algorithme MILD, le taux d'occupation correcte du médium diminue puis augmente doucement. La courbe montre que pour MILD, il existe une taille des paquets (< 800) pour laquelle la réduction du nombre de transmissions correctes permet encore de réduire la fenêtre de contention et ainsi de gagner en efficacité. Lorsque la taille des paquets dépasse 800 octets, MILD se comporte comme BEB INV, c'est-à-dire que les stations utilisent la plus grande fenêtre de contention pour la transmission de leurs paquets. Ce comportement est confirmé par la figure 3.13(b) dans laquelle nous voyons bien l'évolution de la proportion de temps libre pour l'algorithme MILD.

La figure 3.13(d) montre l'évolution de α_i pour les 4 algorithmes de backoff. BEB INV montre un comportement équitable, dû à sa fenêtre de contention initiale qui permet l'envoi presque sans

collision des paquets. En revanche, DIDD et BEB montrent un comportement inéquitable. Ce comportement est dû à un comportement asymétrique des algorithmes BEB et DIDD que l'on peut voir sur la figure 3.14. Cette figure montre les différentes étapes de backoff en abscisse et la probabilité d'être dans cet état en ordonnée. Cette figure illustre bien qu'il existe deux comportements différents pour l'algorithme DIDD : Soit la station est dans la plus grande fenêtre de backoff soit dans la plus petite. Cette différence explique le comportement inéquitable de cet algorithme. Pour BEB, il faut noter que les trois dernières étapes (5, 6 et 7) représentent le plus grand état du backoff. En sommant ces trois dernières probabilités, on peut facilement voir que BEB exhibe le même comportement que DIDD. Cependant, l'utilisation du *retry limit* dans BEB le rend un peu plus équitable que DIDD. Notons que le même phénomène d'asymétrie apparaît dans MILD.

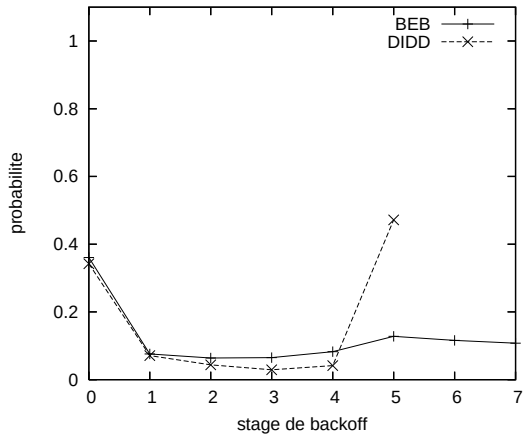


FIG. 3.14: PEPA : Distribution sur les états du backoff (stations cachées). Ce résultat donne la probabilité pour une station d'être dans un état de backoff donné.

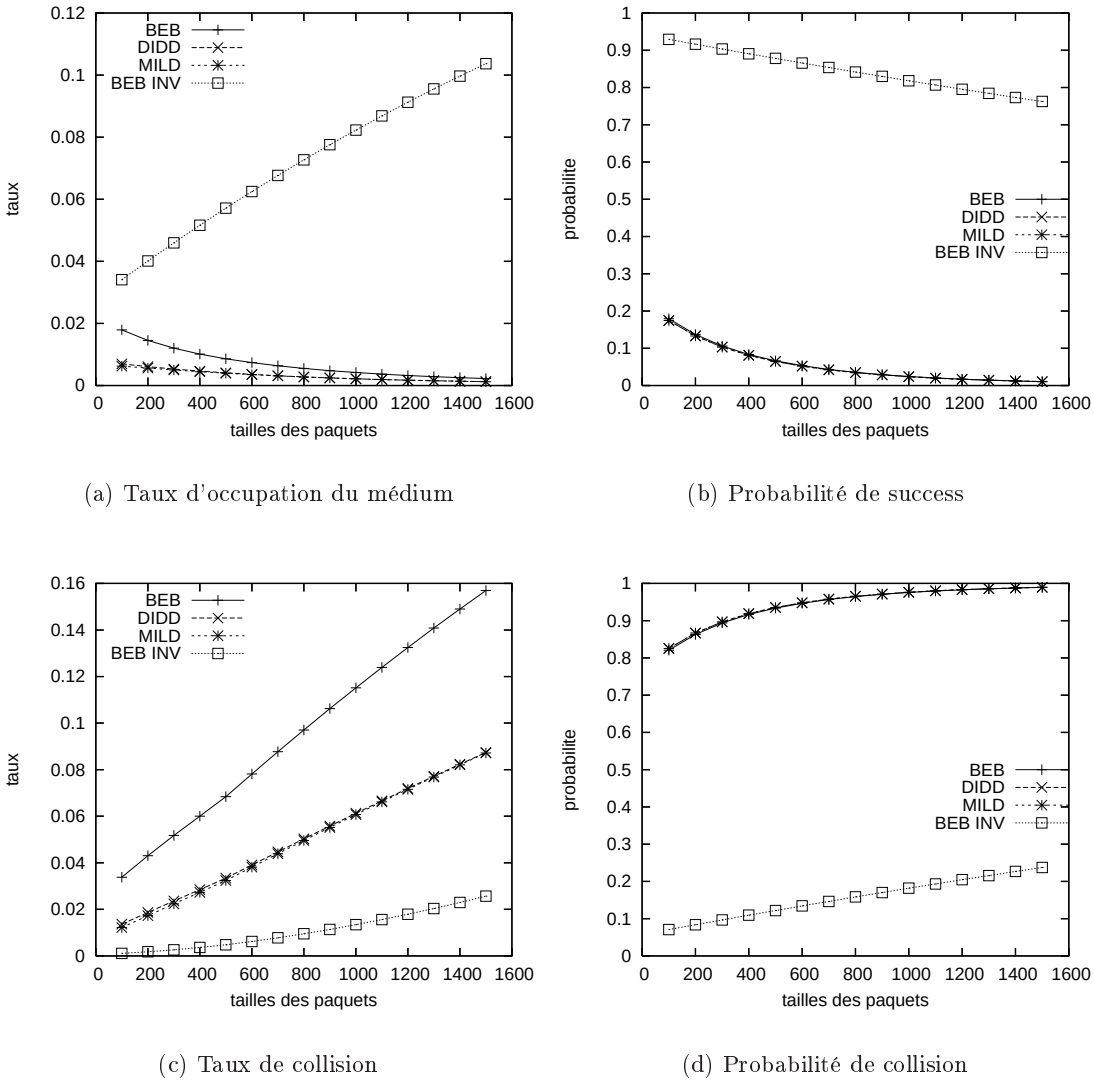
Ce scénario montre bien le compromis équité-efficacité entre l'algorithme DIDD et l'algorithme BEB INV, et dans un cas moins extrême, entre DIDD et BEB.

Dans ce scénario la perte de performance est due à l'influence conjointe des collisions et du temps passé à décrémenter le backoff. Dans ce scénario un accès TDMA, ou tout autre accès permettant de supprimer les collisions, résoudrait à la fois le problème de performance et le problème d'équité dans ce scénario. Selon nous ce type de solutions, avec une alternance des transmissions des deux stations est la seule permettant d'avoir un bon compromis équité-efficacité.

Les nœuds cachés asymétriques

Dans cette section, nous présentons les résultats issus de notre modèle sur le scénario des stations cachées asymétriques. Les figures 3.15(a) et 3.15(b) tracent respectivement le taux de succès (au niveau du médium) et la probabilité de succès pour la station 1. Les figures 3.15(c) et 3.15(d) tracent le taux de collisions et la probabilité de collisions pour la station 1.

Les figures 3.15(a) et 3.15(b) montrent que même si les taux d'occupation correcte du médium sont différents pour BEB et (DIDD,MILD), la probabilité de succès est la même pour ces trois algorithmes. Cette différence s'explique par l'agressivité de l'algorithme de BEB après une transmission avec succès, mais aussi par la politique du *retry limit* qui permet a BEB d'envoyer en moyenne plus de paquets que les deux autres algorithmes. Le même phénomène explique les courbes des figures 3.15(c) et 3.15(d).



(a) Taux d'occupation du médium

(b) Probabilité de success

(c) Taux de collision

(d) Probabilité de collision

FIG. 3.15: PEPA : Résultats de performance (stations cachées asymétriques). Les performances calculées sont : le taux d'occupation correcte du médium, la probabilité de succès, le taux de collisions et la probabilité de collisions pour la paire $(1-2)$. Ces performances sont données pour différentes tailles de paquets et pour les 4 algorithmes de backoff.

D'un point de vue équité, la figure 3.16 montre que la station 1 a une probabilité presque constante d'accéder au médium pour tous les algorithmes. Cependant, cette probabilité est très faible pour BEB, DIDD et MILD ; ce qui montre un problème d'équité à long terme. Pour BEB INV, cette probabilité est proche de 0.5, ce qui montre un comportement équitable a long terme. Notons qu'ici nous avons un problème d'approximation de notre modèle, car les α_i des algorithmes BEB, DIDD et MILD devraient être égaux à 0. Le fait d'approximer les durées par une loi exponentielle fait que cette probabilité n'est pas 0 dans notre modèle.

Ce qu'il est intéressant de noter dans ce scénario, c'est l'impossibilité de l'algorithme de backoff à résoudre les collisions, sous-entendu au niveau de la station 1. Dans ce scénario précis, pour

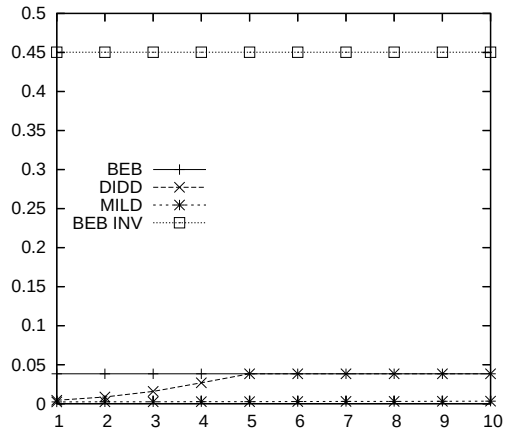


FIG. 3.16: PEPA : α_i (stations cachées asymétriques). Cette courbe donne l'évolution de α_i pour la station 1 sur des paquets de 1000 octets.

que l'algorithme soit plus efficace il faudrait que la station transmette sans accroître sa fenêtre de contention. Ou dans un cadre plus général, que la station 0 soit avertie de l'activité de la station 1. L'utilisation des RTS/CTS permet d'avertir la station 0 de la présence de la station 1. Cependant, l'utilisation des RTS/CTS ne résout pas entièrement le problème des collisions. Notons que l'utilisation des RTS/CTS, revient à étudier le comportement des algorithmes sur l'envoi des petits paquets.

Le scénario des stations cachées asymétriques est selon nous un problème intéressant d'équité dans les réseaux *ad hoc*. La solution à ce scénario exige que la station ne subissant pas de collision partage le médium avec une station qu'elle ne perçoit pas. Cette situation implique que malgré le bon fonctionnement apparent sur la station ne subissant pas de collision, celle-ci doit "deviner" qu'elle gêne une autre communication. Dans ce cas, seul un accès TDMA pourrait permettre au protocole d'être efficace et équitable. La propriété de TDMA qui nous intéresse dans ce scénario est la synchronisation. Selon nous il est difficile d'avoir un accès distribué qui permettrait de résoudre le problème d'équité de ce scénario sans réduire l'efficacité.

Les 3 paires

Dans cette section, nous montrons les résultats obtenus à partir de notre modèle sur le scénario des trois paires. Les figures 3.17(a) et 3.17(b) montrent l'occupation du canal quand les paires sont éloignées, de telle sorte que la transmission de la paire centrale provoque l'utilisation d'un DIFS (respectivement EIFS) sur les paires extérieures et vice-versa.

Ces figures montrent bien un problème d'équité à long terme au niveau des débits de la paire centrale et des paires extérieures. On voit aussi à partir de ces figures que l'utilisation de l'EIFS provoque une baisse des débits.

Les figures 3.17(c) et 3.17(d) montrent l'évolution des α_i suivant le déclenchement des temps fixes EIFS et DIFS. Il n'est pas surprenant de constater que l'utilisation de l'EIFS accroît l'équité. Dans ce scénario, le problème d'équité provient du fait que l'émetteur central n'arrive pas à accéder au médium. Le déclenchement de l'EIFS permet à la paire centrale de repousser l'accès des paires extérieures en forçant celles-ci à attendre un EIFS. On pourrait penser en regardant les courbes de la figure 3.17(d) que le scénario est équitable. Cependant, la figure 3.17(b) nous montre le

contraire. Nous revenons ici a la limitation de notre métrique d'équité qui fournit la probabilité de transmission correcte et successive du i^{eme} paquet sachant que les $i-1$ précédents paquets ont été transmis correctement et successivement. Le problème dans ce scénario vient de la probabilité du premier accès correct, qui est très faible pour la paire centrale et qui est donnée dans ce cas particulier par α_0 (environ 7%)[3]. Cependant, nos résultats montrent qu'une fois ce premier accès effectué, la probabilité d'émettre les paquets suivants sont de l'ordre de 50%. Il faut aussi noter que la valeur de α_0 est plus petite avec l'utilisation de l'EIFS.

Notons, que les résultats sur les α_i sont à prendre avec précaution car dans notre modèle, les durées fixes sont approximées par une loi exponentielle. De ce fait, il existe une probabilité non nulle pour laquelle une inversion de priorité peut se produire dans notre modèle.

Ce qu'il est important de retenir à partir de ces résultats, c'est que la modification de l'algorithme de backoff ne change rien car il n'y a aucune collision dans ce scénario. De plus, le déclenchement de l'EIFS réduit les performances et aggrave le phénomène d'iniquité au vu des différences de débits de la paire centrale et des paires extérieures sur les figures 3.17(a) et 3.17(b). Dans ce scénario, les courbes des α_i n'apportent pas plus d'information sur les problèmes d'équité de ce scénario. Néanmoins les courbes nous apportent une bonne piste pour résoudre le problème de la paire centrale. Nous voyons sur la figure 3.17(d) que l'utilisation du DIFS sur la paire centrale et l'utilisation de l'EIFS sur les paires extérieures permet d'avoir une courbe de α_i presque équitable. À partir de cette courbe nous pouvons donc en déduire le comportement de la paire centrale. Une fois que la paire centrale accède au médium, celui-ci a une probabilité de 1/2 de transmettre un second paquet consécutif. Au cas où celui-ci ne réussit pas à transmettre ce paquet et perd l'accès au médium, la paire centrale n'a plus qu'une probabilité de moins de 1/10 d'accéder au médium une nouvelle fois. Pour résoudre ce problème, il faut augmenter cette probabilité de premier accès de 1/10 à 1/2 et ensuite maintenir la probabilité 1/2 de transmettre successivement des paquets pour la paire centrale. Notons que d'un point de vue distribué, mettre en place un tel système peut être coûteux car il faut que chaque paire de communication identifie le scénario et utilise le mécanisme correspondant.

3.4 Conclusions et travaux futurs

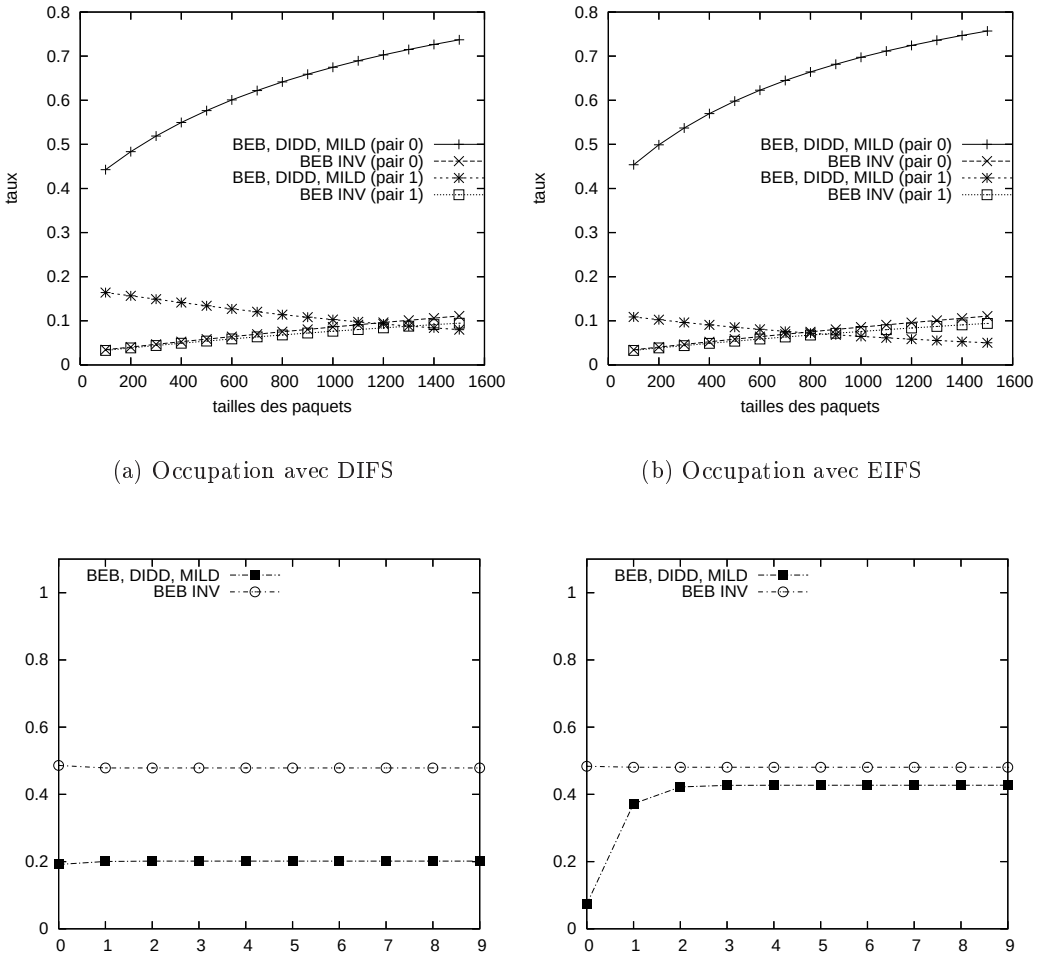
3.4.1 Modèle

Nous avons montré dans ce chapitre un modèle générique permettant l'évaluation de performance de réseaux sans fil. Ce modèle s'applique particulièrement à l'évaluation des performances tant d'un point de vue quantitatif (taux de collisions, taux de pertes, ...) que d'un point de vue qualitatif (équité).

La généricité de notre modèle s'appuie surtout sur les possibilités d'extension que celle-ci offre pour l'étude de 802.11. Notre modèle permet, grâce à l'approche compositionnelle fournie par les algèbres de processus, de modéliser simplement un réseau sans fil. La méthodologie que nous proposons s'appuie sur une décomposition en plusieurs entités d'un réseau sans fil : une source de trafic, une gestion de file d'attente, un protocole d'accès, un algorithme d'évitement de collision, l'interaction entre chaque entité sans fil et finalement les caractéristiques du canal radio.

L'étude de plusieurs topologies, de plusieurs algorithmes de *backoff*, de différentes sources de trafic, *etc.*, nécessite de développer ces composantes mais ne requiert que peu ou pas de modifications sur les autres composantes. De plus, dans un souci d'optimisation, des composantes peuvent ne pas être

[3] L'écriture α_0 est un abus de langage. Ici, nous donnons simplement la probabilité du premier accès.



(a) Occupation avec DIFS

(b) Occupation avec EIFS

(c) α_i avec DIFS

(d) α_i avec EIFS

FIG. 3.17: PEPA : Résultats de performance (3*paires*). Les performances calculées sont : le taux d'occupation correcte du médium pour la paire centrale et l'une des paires extérieures avec l'utilisation du DIFS ou de l'EIFS, Les α_i pour une taille de paquet de 1000 octets pour la paire centrale avec respectivement l'utilisation du DIFS ou de l'EIFS. Ces performances sont données pour différentes tailles de paquet et pour les 4 algorithmes de backoff.

intégrées au modèle. C'est cette possibilité de décliner à l'infini les réseaux pouvant être étudiés qui, selon nous, justifie l'appellation de modèle générique.

3.4.2 Conclusions

Dans cette section, nous avons présenté une évaluation analytique de 802.11. Nous avons essayé par les quatres scénarii que nous avons présentés dans ce chapitre de montrer les fonctionnements possibles et posant problèmes des 802.11.

Le premier scénario avec deux stations à portée de communication et d'une station réceptrice commune représente l'utilisation de 802.11 dans un scénario avec un taux très faible de collision qui

pourrait être évité par la couche MAC. Dans ce scénario, seule compte la taille de la fenêtre initiale de l'algorithme de backoff. C'est celle-ci qui influe sur les performances et l'équité de 802.11.

Dans le second scénario des stations cachées, nous sommes dans un scénario avec un taux de collisions élevé mais qui peut être évité par la couche MAC. Les résultats de performance nous montrent que la réinitialisation de la fenêtre de contention, après une émission avec succès, contribue à réduire l'efficacité du protocole. Cependant, une décroissance trop lente de celle-ci résulte elle aussi en une perte d'efficacité. Du point de vue de l'équité, ce scénario nous montre que l'utilisation d'un *retry limit* a une influence bénéfique sur l'équité, même si celle-ci contribuera à réduire l'efficacité. Dans ce contexte, il est clair que le compromis équité-efficacité prend tout son sens.

Dans le troisième scénario présenté, les stations cachées asymétriques, nous sommes dans un scénario avec un taux de collision élevé pour la station 1. Ces collisions peuvent être évitées par la mise en place d'une couche MAC adéquate sur les deux stations, par exemple TDMA. Cependant, d'un point de vue d'un algorithme de backoff comme ceux étudiés dans ce chapitre, il semble très difficile de résoudre les collisions de ce scénario. Dans ce cas précis, l'agressivité de l'algorithme BEB couplé au *retry limit* font que cet algorithme est le plus performant dans ce cas. Du point de vue de l'équité, ce scénario exhibe un cas précis du problème d'équité à long terme.

Le dernier scénario, les 3 paires, est un scénario montrant le déséquilibre dans l'accès au médium. Dans ce scénario précis, les résultats montrent que la modification seule de l'algorithme de backoff ne suffit pas à rééquilibrer l'accès au médium. Ces résultats nous montrent qu'un bon paramétrage des temps d'attentes, par exemple DIFS et EIFS, peut rétablir l'équilibre au niveau de l'accès au médium.

3.4.3 Travaux futurs

Les composantes développées pour notre modèle révèlent quelques approximations, comme par exemple au niveau du tirage du backoff. La généricité de notre modèle nous permet facilement de développer des composantes permettant de modéliser plus finement le tirage du backoff. Bien qu'il soit facile d'améliorer la modélisation de ce tirage, le coût au niveau de la complexité du modèle croît très rapidement. Il nous paraît donc indispensable de chercher un moyen de construire des composantes plus précises, mais n'ayant qu'un faible impact sur la complexité du modèle.

Les résultats présentés dans cette section nous ont permis de mieux comprendre le comportement de 802.11 et de mettre en évidence plusieurs cas de fonctionnement de la pile protocolaire. Dans cette partie, nous nous sommes attachés à une étude approfondie du comportement de quatre algorithmes de backoff sur quatre scénarii particuliers. Il est évident que la généricité de notre modèle permet l'étude de plusieurs autres types de backoff sur des scénarii différents.

Nous sommes actuellement en train d'étudier le comportement de 36 algorithmes de backoff différents dans différentes situations de collision. Cette étude devra, par exemple, permettre de comprendre l'influence des politiques du *retry limit* sur l'équité et l'efficacité des algorithmes de backoff mais aussi de donner un guide sur la conception de l'algorithme de backoff. Comme dans les résultats exposés dans ce chapitre, les résultats préliminaires montrent qu'aucun algorithme de backoff n'est parfait. Et que bien souvent, le compromis équité-efficacité reste d'actualité.

Les résultats obtenus dans ce chapitre nous ont permis dans un premier temps de mettre en lumière les problèmes d'équité et d'efficacité de la couche MAC de 802.11. Hormis les résultats de performance déjà montrés dans la littérature nous avons montré et complété les résultats d'équité à court et à long terme des 802.11. Les résultats obtenus ici et ceux présentés dans la littérature nous ont permis d'avoir quelques intuitions qui pourraient permettre une amélioration de 802.11 sur les scénarii présentés. Ces intuitions sont par exemple la modification des IFS pour le scénario des trois

paires ou une alternance entre les stations du scénario des nœuds cachés. Dans le chapitre suivant, nous vérifions nos intuitions en proposant un protocole MAC qui serait une alternative à 802.11.

MadMac : Un protocole efficace et équitable

4

« Un bon compromis laisse toujours tout le monde en colère. »

Bill Watterson,
Extrait de la bande dessinée Calvin et Hobbes.

Le chapitre précédent nous a montré que concevoir un protocole MAC efficace et équitable en modifiant seulement l'algorithme de backoff est difficile. Cependant, ce chapitre nous a montré qu'en modifiant l'algorithme de backoff et les paramètres tels que les IFS (Inter-Frame Space) de 802.11, il est possible d'atteindre un "bon" niveau d'équité et d'efficacité.

Dans ce chapitre, nous proposons un protocole équitable et efficace. Ce protocole s'appuie sur 802.11 en essayant de garder les qualités de celui-ci. Si nous modifions 802.11, c'est que nous pensons que 802.11 peut être amélioré, tout en restant compatible avec la version originale. MadMac est ainsi une alternative à 802.11, tout en s'appuyant sur celui-ci. La philosophie du protocole est "le compromis". MadMac se veut équitable, tout en restant efficace. Dans ses premiers balbutiements, le protocole était très simple, les mécanismes se sont complexifiés avec l'âge. Mais, MadMac, dans sa version actuelle, a su rester relativement simple car tous les mécanismes utilisés sont déjà disponibles dans les cartes commerciales actuelles.

Les résultats montrent que MadMac est plus équitable que 802.11 et dans certains cas plus performant.

Sommaire

4.1 État de l'art 48
4.2 La capacité et l'équité 51
4.2.1 L'équité 51
4.2.2 La capacité, la capacité équitable 52
4.3 MadMac 53
4.3.1 Le fonctionnement de base 54
4.3.2 La gestion des collisions 56
4.3.3 Le monopole du canal 58
4.3.4 Résumé 58
4.3.5 Remarques 61
4.4 Performances 61
4.4.1 Description des protocoles de comparaison 61
4.4.2 Cellule de communication 62
4.4.3 Les stations cachées 64
4.4.4 Les trois paires 66
4.4.5 Les stations cachées asymétriques 67
4.4.6 Simulations complémentaires 69
4.5 Conclusion 72

4.1 État de l'art

Dans cette sous-section, nous reprenons en partie et complétons les travaux de la bibliographie réalisée dans [53] et dans [11] . Ces travaux ont proposé, au moment de leur publication, une classification et une revue plus ou moins complète des travaux réalisés sur les couches MAC pour les réseaux sans fil dans [11] et plus spécifiquement pour les réseaux *ad hoc* dans [53].

Dès le début des réseaux sans fil, les propositions de protocole MAC n'ont cessé de se multiplier. Depuis la première version du protocole ALOHA[1] jusqu'à aujourd'hui, l'exploitation de la ressource partagée qu'est le médium sans fil reste un problème ouvert. Le nombre de propositions de protocole MAC pour les réseaux sans fil a explosé avec la popularisation des réseaux *ad hoc*. L'évolution de la technologie a aussi permis d'explorer d'autres moyens d'accéder au médium sans fil. Plusieurs méthodes d'accès et de partage ont vu le jour. On peut citer la famille des protocoles CSMA et plus particulièrement les protocoles CSMA/CA, les protocoles TDMA, les protocoles FDMA ou CDMA. Le point commun de toutes ces approches vient du fait qu'elles cherchent à diviser le médium radio en plusieurs sous-canaux logiques ou physiques et de répartir ces sous-canaux entre les stations. Cette division en sous-canaux devrait permettre la réduction des collisions. Le problème fondamental de toutes ces solutions reste leur mise en œuvre et leur efficacité.

Dans [53] les auteurs proposent une classification des protocoles MAC que nous allons reprendre ici. Les deux grandes catégories des protocoles MAC sont les protocoles sans contention (TDMA, FDMA, CDMA) et les protocoles avec contention. Cette classification est présentée sur la figure 4.1.

L'avantage des protocoles sans contention est qu'ils proposent des solutions souvent efficaces pour les problèmes liés au médium radio. Les problèmes de collisions sont complètement résolus avec la mise en place d'un protocole sans contention. L'inconvénient principal de ces protocoles est leur mise en œuvre qui le plus souvent, nécessite un contrôle central ou la mise en place de systèmes

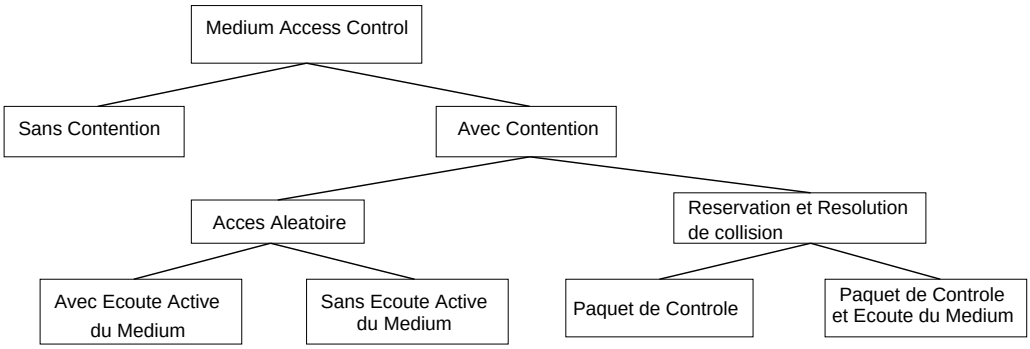


FIG. 4.1: Classification des protocoles MAC pour les réseaux *ad hoc*. Cette classification est tirée de [53]

complexes tels que l'allocation de codes comme dans [58], de fréquences comme dans [51] ou de *slots* de temps comme dans [74]. De plus, ces protocoles supportent très mal la dynamique des réseaux *ad hoc*.

L'approche avec contention se divise en deux sous-groupes : *1)* Les protocoles dits à accès aléatoire et *2)* les protocoles avec réservation et résolution de collisions.

Dans le premier sous-groupe, nous avons encore deux types de protocoles. Les protocoles du type ALOHA [1] ou *slotted* ALOHA. L'accès au médium de ces protocoles se fait simplement sur un choix aléatoire du moment de la transmission et ne se préoccupe pas de la présence de transmission concurrente. La version *slotted* ALOHA introduit une synchronisation sur les instants de transmission n'autorisant les stations à transmettre au débit de chaque slot. Dans le sous-groupe des "Accès Aléatoire", il y a aussi les protocoles utilisant l'écoute active du médium avant de transmettre. L'utilisation de l'écoute active du médium permet de réduire encore plus les collisions. L'accès distribué décrit dans le standard 802.15.4 [43] (ZigBee) peut être classé dans cette catégorie. ZigBee propose un accès aléatoire slotté. Avant de transmettre, une station choisit un temps aléatoire d'attente. À la fin de ce temps, la station effectue une écoute active du médium. Si celui-ci n'est pas occupé, la station transmet son paquet ; si celui-ci est occupé, l'attente est prolongée de manière aléatoire. L'avantage principal des protocoles de la catégorie "Accès Aléatoire" est leur simplicité. Cependant le plus grand inconvénient de ces protocoles vient des faibles performances qu'ils fournissent.

Dans le second groupe de protocoles utilisant une réservation et une résolution de collisions, nous avons encore deux sous-groupes. Les protocoles n'utilisant que des paquets de contrôle et les protocoles utilisant l'écoute active du médium en même temps que des paquets de contrôle. Parmi les protocoles n'utilisant que des paquets de contrôle, nous pouvons citer MACAW [5] et MACA [47]. Ces protocoles consacrent une grande partie des mécanismes implémentés à la résolution du problème des stations cachées. Ces protocoles utilisent un système dynamique de réservation du médium radio (RTS/CTS) permettant bien souvent de réduire l'impact des collisions. L'autre catégorie de protocoles utilisant un système de réservation couplé à l'écoute active du médium permet de réduire encore ces collisions. Dans cette catégorie, nous pouvons placer les protocoles tels que 802.11[40] et bien d'autres encore [25, 73].

Nous avons ici classé 802.11 dans la catégorie de protocole utilisant l'écoute active du médium et utilisant des messages de contrôle. Il est clair que sans l'utilisation des paquets RTS/CTS qui sont optionnels dans le standard, 802.11 se classerait dans le groupe des protocoles à accès aléatoire utilisant l'écoute active du médium tel que ZigBee. La classification proposée par [53] peut être

remise en cause car un protocole de réservation peut utiliser un mécanisme à accès aléatoire, avec ou sans écoute active du médium radio. La proposition d'une telle classification est au-delà des objectifs de ce travail. Cependant, cette classification nous donne un bon aperçu des catégories dans lesquelles on peut classer les protocoles existants.

La différence fondamentale entre les approches avec et sans contention est leur complexité de mise en œuvre dans le contexte des réseaux *ad hoc*. L'allocation des sous-canaux pour les méthodes telles que TDMA, FDMA et CDMA nécessite souvent une première phase de planification qui est souvent incompatible avec l'aspect dynamique et distribué des réseaux *ad hoc*. De plus, dans les protocoles de types FDMA et CDMA, il y a souvent moins de codes ou de fréquences que de stations ; ce qui implique un partage entre plusieurs stations d'un même code ou d'une même fréquence. Ce second partage complique encore plus la mise en œuvre de ces protocoles. L'aspect dynamique et distribué des réseaux *ad hoc* pose aussi un problème d'asynchronisme qui pose un problème au système TDMA. Mettre en place de la synchronisation peut s'avérer très complexe dans les réseaux *ad hoc*. Bien que complexes à mettre en œuvre, les solutions telles que FDMA, CDMA et TDMA ont l'avantage de permettre un accès concurrent et sans collisions au médium de communication. Néanmoins, Les solutions de type CSMA semblent être les plus adaptées pour les réseaux *ad hoc*, pour leur simplicité et pour leur possibilité de passage à l'échelle.

Le choix de CSMA [48] dans plusieurs travaux présentés dans la littérature a aussi été dicté par la diffusion du standard 802.11 [40]. Un nombre certain de solutions et de techniques tournant autour de la méthode d'accès CSMA a été proposé pour les réseaux *ad hoc*. On trouve essentiellement deux grandes approches dans la littérature. Dans la première des informations sont échangées explicitement entre les stations. Dans la deuxième aucune autre information hormis celles déjà fournies par la méthode d'accès CSMA n'est nécessaire. Dans les deux cas, l'objectif est de fournir un ordonnancement en exclusion mutuelle à la ressource partagée. La qualité de l'ordonnancement fourni est le principal critère de qualité d'un protocole MAC pour les réseaux *ad hoc*. Cet ordonnancement est souvent évalué en prenant en compte le débit des flux circulant entre chaque station du réseau. Ainsi, non seulement le débit global du réseau (la somme de tous les débits de toutes les stations) mais aussi la présence ou non de famine (équité) sur les débits sont devenus des critères de performance d'un protocole MAC.

Pour fournir cet ordonnancement indiquant à chaque nœud le moment où il peut accéder au médium, deux solutions émergent de la littérature. La première approche tente d'obtenir le meilleur ordonnancement possible entre les stations. Pour ce faire, des informations sont échangées entre les stations leur permettant ainsi de connaître plus ou moins les instants où elles peuvent accéder au médium et même plus souvent les instants où elles ne doivent pas accéder au médium. L'objectif étant d'obtenir un accès proche de celui proposé par un protocole TDMA évitant ainsi les collisions et la famine. Ces informations fournissent au protocole la synchronisation qui manque à un accès TDMA. Le principal défaut de ces protocoles nécessitant un échange d'information comme [56, 57, 66, 38, 59, 62, 33, 71, 61] provient du fait que ceux-ci utilisent le médium de communication pour les échanger. Non seulement, la bande passante nécessaire à l'envoi des données est réduite mais en plus, les informations transmises peuvent entrer en collision. Plusieurs protocoles minimisent l'importance des collisions pour les informations échangées ainsi que pour les données. Ces collisions sont pourtant importantes car elles peuvent aussi provoquer de la famine sur des stations. Beaucoup des protocoles proposés dans la littérature supposent que l'utilisation de l'aléa, dans le protocole CSMA/CA, permet d'éviter les collisions. Cet aléa sert aussi à certains protocoles de garantir, d'un point de vue statistique, l'équité. Le protocole EHATDMA proposé dans [33], lui concentre son approche sur l'évitement de collision. Les résultats de simulations de ce protocole montrent que la mise en place d'un système performant d'évitement de collisions permet d'aug-

menter l'équité. Cependant, les performances sont réduites à cause des informations échangées pour mettre en place cet évitement de collisions. Le protocole proposé dans [71] est particulier dans le sens où celui-ci n'effectue aucun échange d'information particulier. Cependant, il nécessite l'insertion dans les paquets envoyés d'une information supplémentaire. Ce protocole pourrait être considéré comme ne nécessitant pas d'information supplémentaire s'il ne nécessitait pas, comme le suggère les auteurs, un mécanisme efficace d'évitement de collisions comme celui proposé dans [26] s'appuyant sur une variante des RTS/CTS qui nécessite en plus une connaissance du nombre de stations dans le voisinage.

Pour éviter ces échanges et essayer ainsi d'augmenter l'efficacité, il existe dans la littérature plusieurs protocoles sans échange explicite d'informations [13, 35, 3, 23, 8, 9]. Dans ces protcoles, les stations exploitent des informations locales pour prendre une décision sur l'accès au médium. Comme les informations utilisées sont celles fournies par l'écoute CSMA, l'ordonnancement de ces protocoles s'appuie sur un comportement aléatoire. Ce comportement aléatoire, qui est plus prononcé que pour les protocoles avec échanges d'informations, a un double objectif : l'obtention d'un ordonnancement équitable d'un point de vue statistique et l'évitement de collisions. En règle générale, les résultats obtenus par ces protocoles sont soit une efficacité accrue au détriment de l'équité comme 802.11, soit une équité accrue au détriment de l'efficacité comme dans [3, 23]. Les protocoles tels que [9, 13] semblent ne pas vraiment s'attaquer aux problèmes d'évitements des collisions. Ils consacrent leurs principaux mécanismes à fournir une meilleure équité d'accès. Cependant, les résultats semblent différents, le protocole présenté dans [13] nous semble plus équitable qu'il n'est efficace et celui présenté dans [9] est l'inverse. Les protocoles proposés dans [8, 35] sont particuliers, car ils sont spécialement et exclusivement conçus pour des réseaux où toutes les stations sont à portée de communication. Il existe une foule de protocoles similaires à ceux présentés dans [8, 35], mais nous ne citerons que ces deux protocoles car ils sont selon nous les plus efficaces et les plus équitables dans ce type de scénario. Concevoir un protocole MAC avec un bon compromis équité-efficacité reste donc encore un travail d'actualité. MadMac, le protocle que nous proposons dans la suite de ce chapitre essaie de répondre à ce compromis.

4.2 La capacité et l'équité

4.2.1 L'équité

Le dictionnaire donne la définition suivante du mot équité : "Justice naturelle ou morale, considérée indépendamment du droit en vigeur". Cette définition nous paraît bien vague. Dans plusieurs cas, la justice naturelle (la loi du plus fort) est bien souvent opposée à la justice morale (protection de la veuve et de l'orphelin) [1]. Il semble donc difficile de définir une "bonne" équité.

Dans [7] les auteurs définissent l'équité comme étant un partage du médium congestionné pour lequel aucun flux n'est pénalisé. Cette définition peut s'appliquer aux réseaux *ad hoc* même si dans un réseau *ad hoc* la congestion n'est pas la seule source de problème. Dans un réseau de communication, favoriser un flux revient souvent a en pénaliser plusieurs autres. Dans ce cas, quelles sont les pénalités à appliquer aux flux ? Autoriser une pénalité sur certains flux revient à fournir un schéma d'équité. Un schéma d'équité est par exemple l'allocation du même débit pour toutes les stations. D'autres schémas d'équité existent comme l'équité MaxMin, l'équité proportionnelle ou alors la maximisation du débit global, la minimisation des écart-types et bien d'autres encore. Dans les réseaux, un schéma d'équité populaire est l'équité MaxMin. Cette équité cherche à maximiser le ou les débits mimimun

[1] sauf si le plus fort décide de protéger la veuve et l'orphelin

sur le réseau tel qu'aucun débit ne puisse être augmenté sans diminuer un débit plus petit. Cette allocation est considérée comme la plus équitable.

Les travaux présentés dans [38] décrivent un algorithme distribué d'allocation de bande passante suivant un schéma d'équité MaxMin pour les réseaux *ad hoc*. L'algorithme et le protocole dérivé reposent sur un échange explicite d'informations pour obtenir une telle allocation. Bien qu'aucune preuve n'ait été donnée, il nous semble très difficile de fournir un algorithme suivant un schéma d'équité donné sans échange d'informations. Cependant, il existe dans la littérature des moyens d'évaluer le rapprochement entre deux schémas d'équité.

Jain *et al.* dans [45] définissent un index d'équité comme suit :

$$\frac{(\sum_i^n x_i)^2}{n \times \sum_i^n (x_i)^2}$$

Où n est le nombre total de flux dans le réseau et

$$x_i = \frac{d(i)}{d^*(i)} \qquad \forall i \in [1...n]$$

Où $d(i)$ est le débit obtenu pour le flux i et $d^*(i)$ est le débit du flux i suivant un schéma d'équité donné.

L'index de Jain a l'avantage de fournir un index entre 0 et 1 qui donne la corrélation entre les débits obtenus et les débits recherchés par le schéma d'équité. Cependant, le problème de déterminer le meilleur schéma d'équité et ainsi le $d^*(i)$ à atteindre reste entier. Dans ce manuscrit, nous avons choisi une équité MaxMin comme référence car c'est celle qui est la plus utilisée dans la littérature. Notons que le calcul de l'index de Jain, ainsi que toutes les métriques d'équité s'appuyant sur le partage de la bande passante, peuvent être biaisés. Ces métriques dépendent de différentes propriétés du trafic présent sur chaque station du réseau. C'est une des raisons pour laquelle nous utilisons ici un trafic UDP à saturation sur toutes les stations pour l'évaluation.

4.2.2 La capacité, la capacité équitable

La capacité d'un réseau *ad hoc*, en terme de débit, est définie comme étant le débit maximum pouvant être obtenu sur ce réseau. Ici, nous entendons par débit maximum la somme des débits des flux du réseau sous la contrainte que ces débits soient faisables. Ainsi, la maximisation du débit global peut être vue comme un schéma d'équité particulier. Il est ainsi important de noter que comparer simplement les débits agrégés entre deux allocations n'a pas de vrai sens si ces deux allocations n'ont pas le même objectif. Par exemple, le débit agrégé obtenu par une allocation cherchant à atteindre la capacité du réseau sera supérieure ou égale au débit agrégé d'une allocation cherchant à atteindre une allocation MaxMin. Ainsi, nous définissons la capacité équitable comme étant le débit maximum pouvant être obtenu suivant un schéma d'équité donné.

La notion de capacité équitable est en fait une double mesure. Nous la mesurons avec deux métriques. La première est l'index de Jain qui définit le rapprochement entre notre allocation et l'allocation recherchée. La seconde est le débit agrégé, qui définit les performances en terme d'efficacité de notre allocation. Le fait de combiner ces deux mesures est indispensable car l'index de Jain bien qu'il reflète le rapprochement avec un schéma d'équité donné, peut fournir des valeurs proches de 1 même si les débits obtenus ne sont pas si proches. L'exemple suivant confirme cette hypothèse. Dans cet exemple, nous supposons deux flux qui ont obtenu le même débit x et le débit recherché par le schéma d'équité est x^* pour les deux flux. Le calcul de l'index de Jain est le suivant et est vrai $\forall x$

$$
\begin{aligned}
index &= \frac{(\frac{x}{x^*} + \frac{x}{x^*})^2}{2 \times \left((\frac{x}{x^*})^2 + (\frac{x}{x^*})^2\right)} \\
&= \frac{\frac{4x^2}{x^{*2}}}{\frac{4x^2}{x^{*2}}} = 1
\end{aligned}
$$

Il est clair que le débit global obtenu est différent suivant les valeurs de x mais que l'index de Jain reste à 1 dans cet exemple. Il est donc aussi important de considérer le débit global mais pas uniquement le débit global car il ne donnerait aucun renseignement sur le schéma d'équité recherché. Un protocole efficace et équitable (selon un certain schéma d'équité) est donc un protocole pour lequel le débit global est élevé et proche de la capacité équitable et l'index de Jain est proche de 1. Le calcul du débit que nous effectuons est le suivant : Si la taille moyenne des paquets est de P bits dont k bits pour l'entête, et que le temps moyen de transmission d'un paquet est de T secondes alors le débit est donné par $\nu = ((P-k)/P) \times T$. L'autre intérêt du calcul du débit et de maximiser celui-ci est qu'il revient aussi à minimiser le délai T. En plus, si l'intervalle de confiance de la moyenne du débit (dans le temps) est petit, cela signifie que les délais sont quasiment constants pour cette station.

Il faut noter que la comparaison de protocole n'est pas facile dans ce contexte, car il faut définir le schéma d'équité qui servira de base à la comparaison. Déjà sur ce point, le choix arbitraire d'une équité MaxMin peut être sujet à discussion. Par exemple dans la littérature, les solutions proposées sont souvent comparées à 802.11. Ces solutions sont souvent moins efficaces mais plus équitables par rapport au schéma d'équité donné ; mais en fonction d'un autre schéma, les résultats peuvent être différents. Dans ce manuscrit, nous choisissons une équité MaxMin pour tous les protocoles que nous comparons à notre solution pour les raisons énoncées ci-dessus. De plus, lors de la comparaison des solutions, il est difficile de déterminer si une solution est meilleure qu'une autre. Si l'index de l'une des solutions est proche de 1 mais que son débit agrégé est faible, il est difficile de dire si cette solution est meilleure qu'une solution avec un débit élevé et un index inférieur à 1.

4.3 MadMac

Les solutions proposées dans la littérature modifient de manière probabiliste la méthode d'accès au médium. Cette modification de la méthode d'accès permet de diminuer ou d'augmenter de manière statistique les débits des stations de chaque station. Peu de solutions hormis celle proposée dans [56], cherchent à fournir un ordonnancement explicite entre les stations. Or cet ordonnancement explicite est, selon nous, la clé pour l'obtention d'un bon compromis équité-efficacité.

L'objectif de MadMac est de fournir un ordonnancement entre les stations sans fil cherchant à accéder au médium radio. Avec MadMac, nous cherchons à obtenir un ordonnancement le moins probabiliste possible qui ne dépend pas de la topologie et qui ne nécessite pas d'échange d'informations contrairement à [33] par exemple. Nous voulons un protocole qui ne s'appuie, pour prendre les décisions d'ordonnancement, que sur des informations locales ou les informations fournies par l'écoute active du canal, comme celles données par 802.11 par exemple. Notre protocole peut être vu comme une modification de 802.11. Il est clair qu'obtenir un ordonnancement parfait avec ces contraintes est difficile mais les simulations présentées dans les sections suivantes montrent un bon comportement de MadMac, du moins sur les topologies étudiées.

4.3 MadMac

4.3.1 Le fonctionnement de base

L'idée sous-jacente du protocole provient des deux remarques suivantes :

- RM1 : Si une station perçoit une autre activité sur le canal radio, cela signifie que cette station n'est pas la seule sur le réseau. Ici, nous entendons par une autre activité sur le canal, une activité qui n'est pas liée à l'activité de la station ; par exemple les acquittements provoqués par l'envoi d'un message en unicast. Si RM1 est vrai, cela signifie qu'il y a au moins deux stations en activité sur le réseau et ces deux stations sont dépendantes d'un point de vue de l'accès au médium.
- RM2 : Si une station subit une ou plusieurs collisions sur ces paquets, alors nous pouvons supposer que la station n'est pas la seule sur le réseau. De ce fait, cette station doit partager le médium radio avec une autre station. Ici, nous supposons que le canal radio est idéal, c'est-à-dire que les pertes ne sont jamais dues à un mauvais état du canal radio mais à une collision au niveau de l'accès au médium. Même si cette hypothèse reste forte pour le moment, nous comptons sur la technologie de la couche physique pour fournir à notre protocole une telle robustesse.

La remarque RM2 est différente de la première car dans cette deuxième remarque, le partage du médium peut se faire entre des stations qui ne s'entendent pas, c'est-à-dire qui ne sont pas en zone de détection de porteuse. Cependant, du point de vue d'une station qui subit une collision, celle-ci partage le médium radio car cette station ne peut transmettre correctement ses paquets dû à des transmissions concurrentes. Il faut noter que les remarques RM1 et RM2 ne donnent aucune indication sur le nombre de nœuds en compétition. Pour obtenir une valeur exacte ou une meilleure approximation de cette valeur, d'autres mécanismes sont nécessaires. Ces mécanismes sont par exemple le décodage de tous les paquets de données et les acquittements pour obtenir ces informations en fonction des adresses source et destination de ces paquets. Même en utilisant le décodage de tous les paquets, il est difficile de connaître exactement le nombre de nœuds car certains paquets ne peuvent pas être décodés, et d'autres ne peuvent même pas être capturés. Comme notre objectif nous pousse à éviter tout échange d'informations, nous supposons que d'après les deux remarques RM1 et RM2, une station peut seulement déduire qu'elle partage le médium avec au moins une autre station.

Si la remarque RM1 est vraie, une variable booléenne appelée ACT est mise à 1. Si RM2 est vraie, une variable COL est mise à 1. Comme le partage du médium n'est pas permanent, ces deux variables sont remises périodiquement à 0, tous les $Delta_Slot$. La période $Delta_Slot$ est une fenêtre glissante dont la taille est strictement supérieure au temps de transmission d'un paquet. Quand $ACT = 1$ ou $COL = 1$ pour une station, celle-ci considère qu'elle partage le médium avec au moins une autre station et réduit ainsi son débit MAC par deux. Pour cela, elle introduit un temps d'attente avant l'émission[2] de chaque paquet. Le but de ce temps d'attente est d'introduire un ordonnancement entre les stations en compétition.

Comme nous n'autorisons pas l'usage d'informations contenues dans les paquets qui peuvent être décodés, chaque station suppose que les nœuds en compétition envoient des paquets de la même taille qu'elle. Cette hypothèse a l'avantage de simplifier la division du débit par deux évitant ainsi le maintien d'un historique de la taille des paquets envoyés. Avec cette hypothèse, le temps d'attente introduit avant l'envoi de chaque paquet est $T_{WAIT} = T_{DIFS} + M + T_p + T_{SIFS} + T_{ACK}$, où T_p est le temps de transmission du paquet à envoyer, M est le backoff moyen de 802.11 (soit $310\mu s$), T_{SIFS}, T_{DIFS} et T_{ACK} sont respectivement la durée d'un SIFS, d'un DIFS et d'un acquittement. Il faut noter que dans le cas où le paquet ne nécessite pas la réception d'un acquittement, comme c'est

[2] L'émission se fait en utilisant 802.11. Nous y reviendrons plus tard dans ce manuscrit.

le cas des paquets de *broadcast*, $T_{WAIT} = T_{DIFS} + M + T_p$. L'introduction de M doit permettre une décrémentation complète du backoff de la station en compétition, quelle que soit la valeur de T_p. Notons que T_{WAIT} est utilisé avant l'envoi de chaque paquet tant que $ACT = 1$ ou $COL = 1$. Ce temps ne s'applique pas aux paquets déja entrés dans la phase de contention de 802.11. Contrairement au temps de *backoff*, ce temps n'est jamais stoppé. A la fin de l'écoulement de ce temps d'attente, notre protocole utilise 802.11 comme méthode d'accès, c'est-à-dire l'attente d'un DIFS, d'un *backoff* aléatoire et de l'algorithme du *Binary Exponential Backoff* pour la modification de la fenêtre de contention. Il faut noter qu'il n'est pas possible de se passer d'un accès aléatoire pour plusieurs raisons. Tout d'abord parce que chaque station ne connaît pas le nombre de stations avec lesquelles elle est en compétition. Mais aussi parce que le calcul de T_{WAIT} s'appuie sur un *backoff* moyen et sur une taille de paquet hypothétique. L'introduction de cet aléa ne donnera pas un ordonnancement parfait et il est donc probable que plusieurs stations cherchent à accéder au médium radio au même instant. C'est dans cette optique que nous gardons 802.11 comme méthode d'accès. En revanche, l'introduction de ce temps d'attente permet d'avoir une certaine alternance entre les transmissions et donc de réduire les collisions. Nous utilisons donc une fenêtre de contention initiale plus petite que celle du BEB classique de 802.11.

Si aucune des remarques RM1 et RM2 n'est vraie, alors notre protocole se comporte exactement comme 802.11. Dans ce cas, la station considère qu'elle est la seule à accéder au médium, il n'y a donc aucune considération d'ordonnancement. Notons quand même que l'utilisation de 802.11 permet à une station nouvellement arrivée d'accéder quand même au médium radio durant la décrémentation du backoff de la station déjà présente pour après entrer dans un processus d'alternance.

La figure 4.2 donne une illustration du fonctionnement de MadMac. Dans cette figure, les 3 stations sont à portée de communication. Les stations 0 et 2 sont les émetteurs et la station 1 est le récepteur des deux flux. Les stations émettrices ont toujours des paquets à transmettre et la valeur de $Delta_Slot$ dépasse la taille de la figure. La figure indique les opérations effectuées par chaque station. Au début du diagramme, les deux stations ont des paquets à transmettre. Les deux stations se croyant seules sur le médium utilisent 802.11 pour leur transmission respective. La station 2 transmet la première. La station 0 détecte cette activité et met sa variable $ACT = 1$. Cependant, le premier paquet de la station 0 étant déjà entré dans le processus de *backoff* de 802.11, celle-ci continue d'essayer de transmettre son paquet en utilisant 802.11. Entre temps, la station 2 essaie de transmettre son second paquet. N'ayant toujours pas détecté d'activité celle-ci entre dans le processus de transmission de 802.11. Sur notre figure, nous supposons que la station 2 accède une nouvelle fois au médium avant la station 0. La station 2 essaie alors de transmettre son troisième paquet et n'ayant toujours pas détecté d'activité, elle entre dans le processus classique de 802.11. Entre temps, la station 0 a réussi à transmettre son premier paquet, ce qui provoque la détection d'une activité au niveau de la station 2 qui met sa variable ACT à 1. A ce stade, les deux stations sont chacune consciente de la présence de l'autre. Avant d'essayer de transmettre son deuxième paquet en utilisant 802.11, la station 0 introduit un temps T_{WAIT}. Ce temps permet à la station 2 de transmettre son troisième paquet. A la fin de cette transmission et avant la transmission de son quatrième paquet, la station 2 introduit un temps d'attente. L'ajout de ces temps par les deux stations permet ainsi une alternance parfaite entre les transmissions des stations 0 et 2.

Notons que sur la figure 4.2, pour que les stations perçoivent l'activité l'une de l'autre, nous nous appuyons sur le fait que 802.11 fournit un accès équitable d'un point de vue statistique au médium radio.

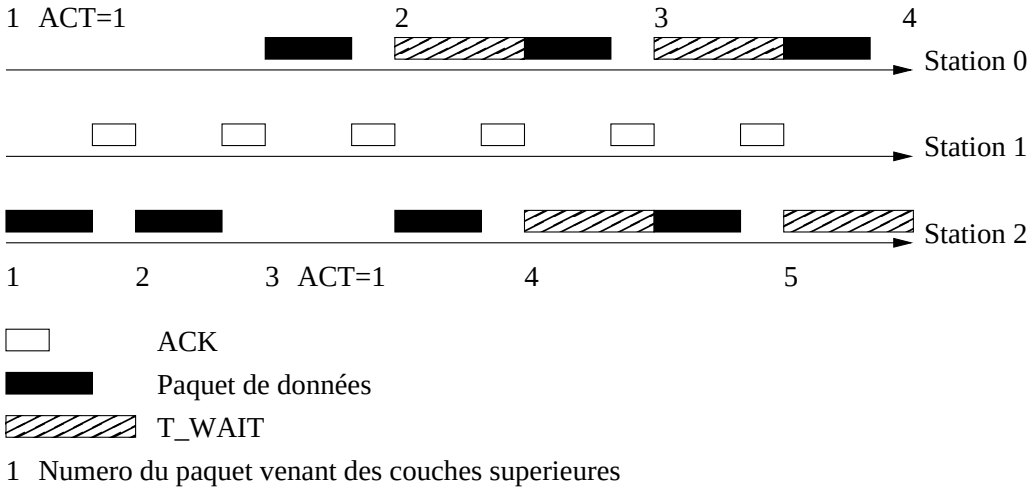


FIG. 4.2: Illustration du mécanisme de base de MadMac. Dans ce scénario, la station 0 et la station 2 sont à portée de communication et transmettent vers la station 1

4.3.2 La gestion des collisions

Pour la gestion des collisions, notre protocole utilise l'algorithme du *Binary Exponential Backoff* couplé au mécanisme expliqué précédemment avec la variable COL. Cependant dans certains cas, comme dans celui des stations cachées, ces mécanismes ne sont pas suffisants. En plus de ces deux mécanismes, chaque station maintient le nombre de collisions successives subies pour sa précédente transmission. Cette valeur est stockée dans la variable NB_COL. Cette variable est réinitialisée pour chaque nouveau paquet. Pour éviter les situations telles que les stations cachées, une station peut entrer dans une phase d'évitement de collision en s'appuyant sur les valeurs de ACT, COL et NB_COL.

Une station entre dans une phase d'évitement de collision, variable $coll_avoid = 1$, quand la variable $ACT = 1$ et que la variable $NB_COL \geq k$, k est un paramètre de notre algorithme. Notons que si la variable $NB_COL \geq 1$, cela implique que $COL = 1$. Trouver la valeur optimale de k n'est pas évident, une trop petite valeur ferait entrer systématiquement le protocole dans une phase d'évitement de collision alors qu'une trop grande valeur de k empêcherait le protocole d'entrer dans cette phase. À partir d'un ensemble de simulations et de résultats de [55], nous avons choisi $k = 2$. Si une station entre dans la phase d'évitement de collision, nous supposons qu'il y a une forte probabilité pour que celle-ci soit dans une situation de stations cachées. Pour éviter une baisse du débit global à cause des collisions dues à cette situation et aussi afin d'éviter un problème d'équité à court terme, nous essayons de forcer les stations cachées à émettre alternativement. Pour ce faire, dès que le paquet ayant subi les k collisions est transmis, et sous réserve que ACT soit égal à 1, nous introduisons pour le paquet suivant un autre temps d'attente $T_{ALT} = T_{WAIT} + T_{MTU}$ où T_{MTU} est le temps nécessaire à la transmission d'une trame de la taille du MTU. T_{ALT} est divisé en deux phases. Durant la première phase, T_{WAIT}, T_{ALT} ne peut être stoppé. En revanche, durant la partie T_{MTU}, T_{ALT} est arrêté dès que de l'activité est perçue sur le médium (comme un acquittement par exemple). A la fin de T_{ALT}, qu'il ait été interrompu ou non, l'algorithme utilise 802.11 pour accéder au médium et transmettre son paquet. Une fois entrée dans cette phase d'évitement de collision, la station y reste tant que $ACT = 1$ ou $COL = 1$. En revanche, si $ACT = 0$ et $COL = 0$ alors la station retourne à un processus normal décrit précédemment, dans ce cas $coll_avoid$ est mis à 0.

Comme il peut y avoir plus de deux stations cachées, nous avons introduit une autre variable permettant de gérer le cas des stations cachées multiples. Avec une variable appelée n_hidden, la station essaie de compter le nombre de stations cachées. Nous avons aussi modifié le temps d'attente T_{ALT} pour refléter ces stations cachées multiples. L'entrée dans la phase d'évitement de collision se fait en mettant la variable $coll_avoid$ à 1. Si $coll_avoid = 0$ et $NB_COL \geq k$, sous la condition que $ACT = 1$, cela veut dire que la station va entrer dans la phase d'*é*vitement de collision pour son prochain paquet. Dans ce cas, $coll_avoid$ et n_hidden sont mis à 1. Le processus décrit dans le paragraphe précédent est utilisé. Si $coll_avoid$ est déjà égal à 1 et $NB_COL \geq k$ alors n_hidden est incrémenté de 1 et une nouvelle valeur de T_{ALT} est utilisée. Dans ce cas, $T_{ALT} = n_hidden \times T_{WAIT} + n_hidden \times T_{MTU}$. Comme précédemment, la partie $n_hidden \times T_{MTU}$ peut être interrompue si la station a détecté n_hidden activités[3]. Le nombre de périodes d'occupation est conservé dans une variable appelée $nb_activity$. Comme le nombre de stations cachées peut aussi décroître dû à des départs de stations, la valeur de n_hidden est décrémentée de 1 quand T_{ALT} est décrémenté jusqu'a la fin. Cela veut dire qu'il n'y a pas assez d'activité ayant été detectée, et donc probablement qu'une des stations cachées a cessé d'émettre.

L'utilisation de la phase d'évitement de collision a deux avantages. Premièrement il permet sans échange d'informations, y compris les RTS/CTS, d'avoir un fonctionnement proche de l'optimal dans un scénario de stations cachées (multiple ou pas). Deuxièmement, en réduisant les collisions il permet d'accroître le débit global. Notons que dans le cas d'une cellule dense, la phase d'évitement de collision est aussi utilisée car le nombre de collisions peut vite croître. Nous entendons ici par cellule un réseau dans lequel toutes les stations sont a portée de communication les unes des autres. Notons aussi que comme pour le fonctionnement normal de MadMac, le fonctionnement en évitement de collisions s'appuie sur des qualités statistiques de 802.11. Il peut arriver que parmi toutes les stations cachées seul un sous-ensemble des stations subit des collisions. D'un point de vue statistique (tirage du backoff), toutes les stations ont la même probabilité de collisions. Nous nous appuyons sur cette hypothèse pour le déclenchement de la phase d'évitement de collision.

La figure 4.3 montre un exemple de diagramme de transmission pour deux stations cachées. Dans cette figure, les stations 0 et 2 sont cachées et ont un récepteur commun. Dans cet exemple, nous prenons $k = 2$. Au début, les deux premières transmissions des stations 0 et 2 entrent en collision. La variable COL des deux émetteurs est mise à 1 et NB_COL est aussi incrémenté. Supposons que grâce à l'algorithme du *Binary Exponential Backoff*, la station 0 réussit à transmettre son premier paquet. La réussite de cette transmission provoque la transmission d'un acquittement par la station 1 qui provoque de l'activité pour la station 2 ($ACT = 1$). Avant l'émission de son second paquet, la station 1 attend un temps T_{WAIT} avant de transmettre son paquet. Ici nous supposons que la troisième tentative de transmission de la station 2 entre en collision avec la première tentative pour le deuxième paquet de la station 0. Supposons maintenant que la quatrième tentative de la station 2 se déroule avec succès toujours grâce à l'algorithme du *Binary Exponential Backoff*. Cette transmission provoque de l'activité sur la station 0 qui a sa variable ACT à 1. Comme $NB_COL \geq 2$ que $ACT = 1$ et que $COL = 1$ pour la station 2, celle-ci entre dans une phase d'évitement de collisions ($coll_avoid = 1$). De ce fait, la station 2 attend un T_{ALT} avant de tenter de transmettre son deuxième paquet. Cette attente plus longue permet à la station 1 de transmettre son deuxième paquet. L'envoi de l'acquittement de la station 1 interrompt l'attente de la station 2 qui peut transmettre son deuxième parquet. La figure montre qu'il est ainsi possible d'avoir une alternance entre les transmissions des deux stations. Les résultats de simulations vont confirmer cette hypothèse. Nous pouvons remarquer que cette alternance parfaite peut se produire même si les deux stations ont des vues différentes du médium. Dans l'exemple donné, la station 2 se considère

[3] activité séparée par des périodes où le médium est libre

comme étant dans une situation de stations cachées alors que la station croit être dans une situation de partage classique.

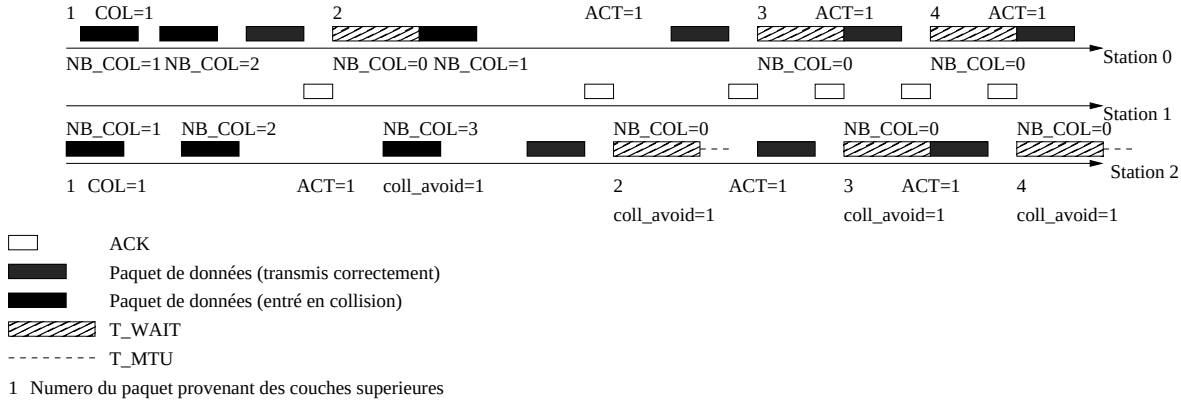


FIG. 4.3: Illustration du mécanisme de MadMac pour l'évitement de collision. Dans ce scénario, la station 0 et la station 2 ne sont pas à portée de communication et transmettent vers la station 1. Les stations 0 et 2 sont les stations cachées.

4.3.3 Le monopole du canal

Dans certaines configurations comme celles des trois paires [14], des stations peuvent monopoliser le médium radio ce qui peut empêcher d'autres stations d'y accéder. Ces stations, ayant le monopole de l'accès au canal, ne subissent que très rarement des collisions et perçoivent le médium comme libre la plupart du temps car les autres stations n'arrivent pas ou très peu à accéder au médium. Le protocole MadMac tel qu'il vient d'être décrit ne fournit aucun mécanisme permettant de résoudre ce type de problème. Par conséquent, et pour éviter ce problème de monopole, la fenêtre de contention est modifiée pour certains paquets autorisant ainsi les stations lésées à accéder au médium. Pour ce faire, après x transmissions successives et correctes de paquets pour lesquelles $ACT = 0$ et donc $COL = 0$, le $x + 1^{eme}$ et le $2x + 1^{eme}$ sont envoyés avec une fenêtre de contention plus grande, deux fois puis quatre fois la taille de la fenêtre de contention de 802.11 (respectivement). Ce processus est répété pour les paquets suivants pour permettre aux stations pénalisées d'accéder au médium et ainsi faire évoluer la variable ACT des stations tenant le monopole et d'y mettre un terme.

4.3.4 Résumé

Dans ce paragraphe nous présentons des algorithmes simplifiés du fonctionnement de MadMac comme complément aux explications données dans les sections précédentes. L'algorithme 1 présente le processus d'envoi de MadMac.

Notons qu'au début de l'algorithme $n_hidden = 1$. Cet algorithme montre les quatre cas possibles de transmission suivant les valeurs de COL et de ACT. Ces cas sont présentés sur les lignes 1, 14, 17 et 20 de l'algorithme 1.

Le premier cas considéré (ligne 1 à 13) présente le cas où la station a subi des collisions et a perçu de l'activité. Le premier test effectué permet de savoir si la station est dans une phase d'évitement de collisions. Si le nœud est déjà dans une phase d'évitement de collisions, celui-ci incrémente la valeur de n_hidden suivant le nombre de collisions subies pour le paquet précédent

Algorithm 1 MadMac : Processus d'envoi

```
1: if (COL = 1 && ACT = 1) then
2:   if (coll_avoid = 1) then
3:     if (NB_COL > K) then
4:       n_hidden++;
5:     end if
6:   else
7:     if (NB_COL > K) then
8:       coll_avoid = 1;
9:       n_hidden = 1;
10:    end if
11:  end if
12:  x = 0; nb_activity = 0; NB_COL = 0;
13:  send_after_madmac(n_hidden × T_WAIT, n_hidden × T_MTU, coll_avoid);
14: else if (COL = 0 && ACT = 1) then
15:  x = 0; nb_activity = 0; NB_COL = 0;
16:  send_after_madmac(n_hidden × T_WAIT, n_hidden × T_MTU, coll_avoid);
17: else if (COL = 1 && ACT = 0) then
18:  x = 0; nb_activity = 0; NB_COL = 0;
19:  send_after_madmac(n_hidden × T_WAIT, n_hidden × T_MTU, coll_avoid);
20: else if (COL = 0 && ACT = 0) then
21:  x++; nb_activity = 0; NB_COL = 0;
22:  n_hidden = 1; coll_avoid = 0;
23:  send_after_backoff(Backoff_Process, x);
24: end if
```

(conservé dans la variable NB_COL). Si la station n'est pas dans une phase d'évitement de collisions, le nombre de collisions est aussi testé et permet si $NB_COL > K$, d'entrer dans une phase d'évitement de collisions. Ensuite, les variables x, $nb_activity$ et NB_COL sont initialisées à 0. Pour rappel, NB_COL représente le nombre de collisions consécutives sur un paquet, x est le nombre de paquets consécutifs transmis avec $ACT = 0$ et $COL = 0$ et est utilisé pour éviter le monopole du canal, $nb_activity$ compte le nombre d'interruptions dues à une activité sur la canal et permet d'interrompre les temps d'attente dans la phase d'évitement de collisions. La fonction $send_after_madmac()$, décrite plus tard dans cette section, est appelée pour l'envoi du paquet.

Les cas où ($ACT = 0$ et $COL = 1$) et ($ACT = 1$ et $COL = 0$) sont décrits aux lignes 14 et 17 de l'algorithme 1. Dans ces deux cas, x, $nb_activity$ et NB_COL sont initialisés à 0 et la procédure $send_after_madmac()$ est appelée pour la transmission du paquet.

Pour le cas où ($ACT = 0$ et $COL = 0$), la station considère qu'elle ne partage pas le médium. La variable x est incrémentée et les variables $nb_activity$ et NB_COL sont initialisées à 0. Les variables n_hidden et $coll_avoid$ sont elles aussi remises à 1 et 0 respectivement pour signifier que le protocole n'est plus dans un processus d'évitement de collisions. L'envoi du paquet est déclenché par la procédure $send_after_backoff()$ qui sera décrite plus loin dans cette section.

L'algorithme 2 représente la fonction $send_after_madmac()$.

Dans cet algorithme, la variable $TIME$ définit le temps écoulé depuis le début de la fonction. Durant l'attente T_{WAIT} (ligne 1 de l'algorithme) le nombre d'interruptions est compté et si une activité est perçue, la variable ACT est mise à jour. La fin du temps T_{WAIT} est représentée par la sortie de la boucle *while* (ligne 1 à 6). A la sortie de cette boucle, deux cas peuvent se présenter : soit la station n'est pas dans une phase d'évitement de collisions, donc il n'est pas nécessaire d'attendre un T_{MTU} en plus et le paquet est transmis en utilisant la procédure $send_after_backoff()$ après

4.3 MadMac

Algorithm 2 MadMac : $send_after_madmac(n_hidden \times T_{WAIT}, n_hidden \times T_{MTU}, coll_avoid)$

```
1: while (TIME ≤ n_hidden × T_WAIT) do
2:    compter le nombre d'interruption (nb_activity)
3:    if (une activite est percue) then
4:       ACT = 1 ;
5:    end if
6: end while
7: if (coll_avoid = 0) then
8:    x = 0 ;
9:    send_after_backoff(Backoff_Process, x);
10: else
11:   TIME = TIME − n_hidden × T_WAIT;
12:   while (TIME ≤ n_hidden × T_MTU || nb_activity ≤ n_hidden ) do
13:      compter le nombre d'interruptions (nb_activity)
14:      if (une activite est percue) then
15:         ACT = 1 ;
16:      end if
17:   end while
18:   if (nb_activity < n_hidden) then
19:      n_hidden = n_hidden − 1;
20:   end if
21:   x = 0 ;
22:   send_after_backoff(Backoff_Process, x);
23: end if
```

que x ait été remis à 0 ; soit la station est dans une phase d'évitement de collisions ($coll_avoid = 1$ à la ligne 10). Dans ce second cas, la station attend soit la fin du temps $T_{MTU} = n_hidden \times T_{MTU}$ soit que le nombre d'interruptions dues à une activité soit supérieur ou égal à n_hidden. Ces conditions sont les conditions de sortie de la boucle *while* (ligne 12). Durant cette boucle *while*, le nombre d'interruptions est compté et la variable ACT peut être mise à jour. A la sortie de cette boucle, si le nombre d'interruptions $nb_activity < n_hidden$ alors n_hidden est décrémenté d'une unité, et x est remis à 0, la procédure $send_after_backoff()$ est ensuite utilisée pour transmettre le paquet.

L'algorithme 3 décrit la fonction $send_after_backoff()$. Cette fonction se comporte différemment suivant les valeurs que prennent x (lignes 1, 3 et 5). Ces conditions sont liées au monopole du médium radio par la station et permettent de modifier la fenêtre de contention utilisée pour transmettre le paquet. L'accès au médium et la transmission et retransmission du paquet se font en utilisant 802.11. Durant cette procédure les variables ACT, COL et NB_COL sont mises à jours.

Algorithm 3 MadMac : $send_after_backoff(Backoff_Process, x)$;

```
1: if (x = 10) then
2:    Use CW_min × 2
3: else if (x = 21) then
4:    Use CW_min × 4 ; x = 0;
5: else
6:    Use CW_min
7: end if
8: utiliser la methode d'acces de 802.11 ;
9: Les variables ACT, COL et NB_COL sont mises a jours ;
```

4.3.5 Remarques

1. On peut tout d'abord noter que notre protocole ne s'appuie que sur des informations simples et déjà présentes dans 802.11. Aucune information supplémentaire n'est nécessaire et nous ne nous autorisons même pas à tirer des informations des paquets qui peuvent être décodés, afin d'obtenir une approximation du nombre de stations en compétition par exemple.
2. Le temps sur chaque station est divisé en *Delta_Slot*, mais rien ne requiert dans notre protocole une synchronisation des stations. Le dimensionnement de ce temps requiert un compromis entre la réactivité du protocole face au changements de voisinage, plus particulièrement le départ d'une station, et la considération de l'historique dans les décisions d'accès. On peut noter que rien n'empêche une valeur de *Delta_Slot* dynamique et/ou différente sur chaque station.
3. Le paramètre k est aussi un paramètre important de notre protocole. En effet, c'est celui-ci qui détermine si la station décide d'entrer dans une phase d'évitement de collisions ou non. Or les collisions ne proviennent pas que des collisions mais peuvent aussi provenir d'une mauvaise qualité du canal radio. Là aussi, il y a un compromis entre une petite valeur de k qui fera perdre de l'efficacité si le canal radio est de mauvaise qualité et une grande valeur de k, qui empêchera une station d'entrer dans la phase d'évitement de collisions.

4.4 Performances

Dans cette section, nous présentons les résultats de performance et d'équité de notre protocole MadMac. Notre protocole a été évalué en utilisant le simulateur de réseau NS-2 [60]. NS-2 a été modifié pour prendre en compte les débits de 802.11b (1, 2, 5,5 et 11 Mbps). Un trafic CBR saturant a été utilisé dans tous les scénarii simulés pour essayer d'avoir les pires cas de fonctionnement de notre protocole. Toujours pour essayer de refléter ces pires cas, un ensemble de scénarii a été testé reflétant, selon nous, les différents cas d'utilisation de notre protocole.

Dans le but de mieux comprendre le comportement de notre protocole, nous avons supprimé le protocoles ARP et créé un protocole de routage statique (utilisé si nécessaire). Toujours dans un souci d'évaluation, nous avons comparé notre protocole à quelques protocoles classiques de la littérature.

Les simulations présentées dans cette section sont conduites avec des paquets de 1000 octets, et les mêmes paramètres de MadMac pour toutes les simulations. Le débit physique utilisé est de 11 Mbps.

4.4.1 Description des protocoles de comparaison

Nous comparons MadMac à 802.11, MBFAIR et PNAV. Dans cette sous-section nous décrivons plus en détail les protocoles MBFAIR et PNAV.

Dans MBFAIR [24], chaque station ajuste sa fenêtre de contention en fonction du ratio entre les paquets qu'elle envoie et les paquets qu'elle perçoit dans son voisinage. Cette approche est similaire a celle proposée dans [38]. Cependant dans [24], il est inutile de connaître l'état du voisinage à deux sauts. Ce travail s'appuie sur une notion d'index d'équité présentée dans [3], qui joue le rôle de seuil pour l'adaptation de la fenêtre de contention. Le protocole proposé ne nécessite pas d'information particulière du voisinage mais permet d'avoir une meilleure performance si des paquets comme les RTS/CTS sont utilisés. Le principe du protocole proposé dans [24] est le suivant : les auteurs définissent Φ_i comme étant la proportion du canal radio que chaque émetteur essayera d'obtenir

et W_i le débit associé. Le protocole proposé cherche à ajuster la taille de la fenêtre de contention pour égaliser les rapports W_i/Φ_i dans le réseau. D'un point de vue pratique, une station voit "Elle et les autres". Chaque station calcule un W_{ei} qui est son estimation de bande passante, et W_{eo} l'estimation de la bande passante consommée par les autres stations. Chaque fois qu'un paquet est reçu, le temps de transmission de ce paquet est ajouté à W_{ei} ou W_{eo} en fonction de la destination et du type de paquet. Ensuite, la station calcule $FI_e = (W_{ei}/\Phi_i)/(W_{eo}/\Phi_o)$ où $\Phi_o = 1 - \Phi_i$. La fenêtre de contention est ajustée suivant les valeurs de FI_e comparées à une constante C. Par exemple, si $FI_e > C$ pour $C > 1$, alors la fenêtre de contention est augmentée jusqu'à au plus CW_{max}. Le calcul de W_{ei} et particulièrement W_{eo} se fait sur une estimation d'un temps d'envoi de paquet. Pour plus de détails, voir [72] et [24]. Les résultats présentés montrent que le protocole est plus équitable que 802.11, mais moins efficace. Une des limitations de ce protocole vient du fait que le calcul de l'index d'équité ne se fait que sur les paquets reçus correctement (RTS, CTS, DATA et ACK). Il ne prend pas en compte les paquets entrés en collision ni même les paquets transmis par des stations en zone de détection de porteuse.

Les auteurs de PNAV [13] proposent d'introduire un temps d'attente fixe entre deux transmissions successives suivant une certaine probabilité. Cette probabilité dépend des évènements tels que l'accès successif au médium par une même station, l'occupation ou non du médium par une autre station. La particularité du temps d'attente introduit par PNAV est que celui-ci ne peut pas être interrompu. Le protocole PNAV, conçu en même temps que MadMac, est l'un des premiers protocoles à avoir introduit un ordonnancement explicite qui ne s'appuie pas sur le tirage d'un backoff. Même si cet ordonnancement est utilisé en fonction d'une probabilité, l'utilisation d'un ordonnancement explicite semble fournir de bons résultats d'équité. Cependant, le temps d'attente introduit étant fixe, le dimensionnement de celui-ci reste problématique. Plus ce temps sera grand, plus le comportement du protocole est équitable mais plus les performances seront dégradées. Les auteurs proposent un temps d'attente équivalent à la durée d'une transmission d'un paquet ayant la taille du MTU au débit le plus bas disponible sur le réseau. Le fonctionnement de PNAV est le suivant : à chaque fois qu'une station transmet un paquet, la probabilité p d'introduire un temps d'attente est augmentée. Avant chaque transmission un tirage aléatoire est fait pour décider avec une probabilité p si un temps d'attente sera ajouté avant la transmission du paquet. Quand ce temps d'attente est ajouté, la station regarde si une transmission a eu lieu durant ce temps d'attente. Si une transmission a eu lieu, la station met la valeur de p à 1 sinon elle met la valeur de p à 0 et recommence le processus d'augmentation de la probabilité p. Plus de détails sur le protocole peuvent être trouvé dans [13].

4.4.2 Cellule de communication

Le premier scénario correspond a une communication entre une station de base et plusieurs stations mobiles. Dans ce scénario, nous ne nous intéressons pas à l'équité. Nous supposons et acceptons que l'équité obtenue par MadMac est proche de l'équité statistiquement fournie par 802.11. Ce que nous regardons particulièrement dans ce scénario est l'efficacité (le débit agrégé) de notre protocole. La figure 4.4 montre l'évolution du débit agrégé en fonction du nombre de stations dans la cellule de communication. Notons que dans ce scénario, la taille de chaque paquet est tirée uniformément entre $[550; 1450]$ octets.

Dans ce scénario, l'augmentation du nombre de stations diminue le débit global. Cette diminution est due a l'augmentation du nombre de collisions. Avec l'augmentation du nombre de collisions, les stations utilisant MadMac entrent dans une phase d'évitement de collisions. L'utilisation de cette phase permet de réduire les collisions grâce à l'alternance fournie par MadMac durant cette phase. La figure 4.4 montre que MadMac est plus efficace que 802.11, PNAV, et MBFAIR quand le nombre

de stations augmente.

Sur cette figure, nous voyons que le débit global de MadMac diminue plus lentement que celui des autres protocoles. Cette diminution est due au temps de convergence du protocole. L'alternance fournie par MadMac dans sa phase d'évitement de collisions dépend du nombre de collisions subies. Par conséquent, quand le nombre de stations augmente, le temps nécessaire pour atteindre la bonne valeur de n_hidden est plus long. Ici, les intervalles de confiance ne sont pas renseignés car ils sont très proches des valeurs moyennes obtenues.

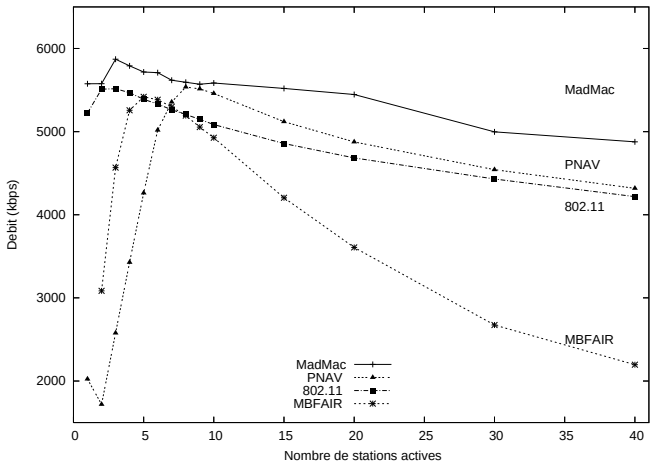


FIG. 4.4: Performance de MadMac sur une cellule de communication. Le débit global du réseau est tracé en fonction du nombre de stations dans la cellule de communication

D'un point de vue de l'équité sur ce scénario, les performances de MadMac sont moins bonnes que celles de 802.11. Ceci est dû au fait que l'ajout d'un temps d'attente avant la transmission dans MadMac pénalise la station ayant déjà subi des collisions. Ainsi, le moindre déséquilibre entre le nombre de collisions subies par les stations entraîne un plus gros écart sur les débits de chaque station. Le tableau 4.1 montre l'ampleur de cet écart sur l'intervalle de confiance de la moyenne des débits pour les stations. Cette simulation a été jouée sur une cellule de 30 stations. Les intervalles de confiance montrent que dans ce cas, 802.11 est plus équitable que MadMac. Néanmoins, ces intervalles de confiance restent acceptables.

	Moyenne (kbps)	Int. de Conf (0.05)
802.11	147.54	$[145.20; 149.89]$
MadMac	166.59	$[150.32; 182.86]$

TAB. 4.1: Débit par station pour une cellule de communication avec 30 stations

Dans la suite de ce manuscrit, nous considérons que la capacité du médium radio est C. C correspond à la transmission d'une seule station à saturation. Cette capacité est différente suivant les protocoles et la simulation précédente nous permet d'obtenir ces capacités pour les différents protocoles. Pour MadMac, (respectivement 802.11, PNAV et MBFAIR), cette capacité est de 5.6 Mb/s (respectivement 5.2 Mb/s, 2 Mb/s et 3 Mb/s). Cette capacité sera utilisée pour le calcul de l'index de Jain dans la suite du manuscrit.

4.4.3 Les stations cachées

Le second scénario que nous avons testé est le scénario bien connu des stations cachées. Ce scénario est intéressant car la résolution du problème est liée à la qualité de l'ordonnancement fourni par la couche MAC. Une couche MAC de type TDMA permet d'avoir un ordonnancement parfait et d'atteindre ainsi la capacité équitable du réseau.

La figure 4.5 montre les performances de MadMac et des autres protocoles du point de vue de l'efficacité et du point de vue de l'équité. Les résultats d'équité montrent que tous les protocoles sont équivalents avec un index de Jain égal à 1. Cependant d'un point de vue de l'efficacité, MadMac est plus performant que les autres protocoles. Nous pouvons aussi noter que le débit global obtenu avec MadMac est de 5.6 Mb/s, qui correspond à la capacité du protocole. Ceci est aussi vrai pour MBFAIR. Pour 802.11 et PNAV, le débit global est inférieur à la capacité. L'obtention de la capacité du réseau dans ce scénario et d'un index égal à 1 permettent de conclure que MBFAIR et MadMac fournissent un ordonnancement proche d'un ordonnancement TDMA, ce qui n'est pas le cas pour 802.11 (avec ou sans RTS/CTS) et PNAV.

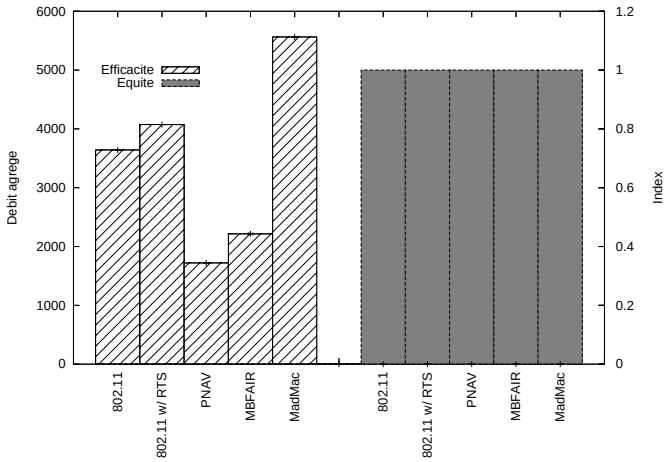


FIG. 4.5: Performance de MadMac sur le scénario des stations cachées. Le débit global du réseau et l'index d'équité sont tracés respectivement par rapport aux ordonnées à gauche et à droite de la figure.

L'équité et les performances obtenues avec MadMac sont liées à la qualité de l'ordonnancement fourni par celui-ci. Notons que l'obtention de cet ordonnancement efficace ne nécessite aucun échange d'information. Cependant, cet ordonnancement dépend du temps d'attente introduit avec MadMac et de ce fait, de la taille des paquets transmis par les stations. Les résultats des simulations suivantes montrent les résultats obtenus avec MadMac, quand la taille des paquets transmis est aléatoirement et uniformément choisie entre $[550; 1450]$ octets. Ces résultats présentés sur la figure 4.6 montrent que malgré une taille aléatoire de paquets, l'ordonnancement fourni par MadMac sur le scénario des stations cachées est efficace et équitable.

Nous avons étendu nos simulations à un scénario de stations cachées multiples. Les résultats sont présentés sur la figure 4.7. L'indice d'équité n'est pas tracé dans cette figure car elle est proche de 1 pour toutes les simulations. Cette figure montre que l'ordonnancement fourni par MadMac est efficace, car il permet d'atteindre la capacité du réseau dans tous les cas de figure. Pour 802.11, le débit agrégé diminue car le taux de collisions augmente, preuve que l'ordonnancement fourni par

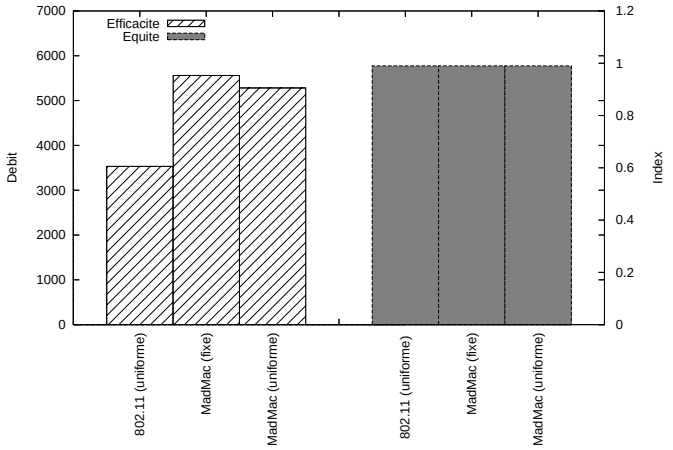


FIG. 4.6: Performance de MadMac sur le scénario des stations cachées avec une taille de paquets aléatoire. Le débit global du réseau et l'index d'équité sont tracés respectivement par rapport aux ordonnées à gauche et à droite de la figure.

802.11 n'est pas efficace. Pour PNAV et MBFAIR, les performances restent en-deçà de la capacité quand le nombre de stations cachées augmente. Par exemple pour 4 stations cachées, la capacité de MBFAIR devrait être d'environ 3.5 Mb/s[4].

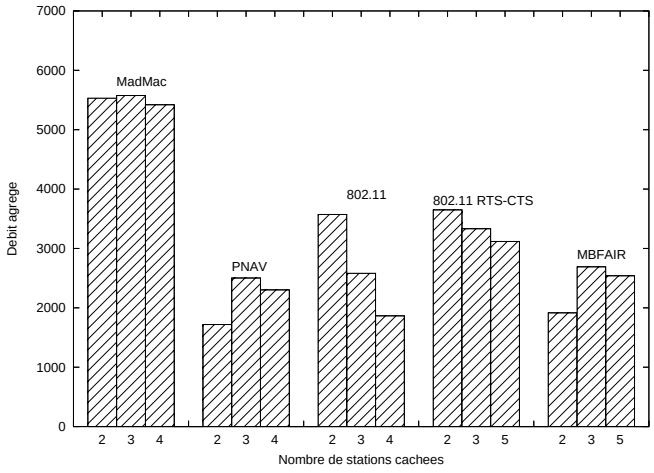


FIG. 4.7: Performance de MadMac sur le scénario des stations cachées. Seul le débit global du réseau est tracé. L'index d'équité est toujours égal à 1 pour tous les protocoles.

Ces simulations confirment l'importance des collisions dans les performances d'un ordonnancement. Elles montrent que même si 802.11 fournit un accès équitable au médium radio, il faut que ces accès soient des accès aboutissants à des transmissions avec succès.

[4]Cette valeur est déduite à partir des performances sur une cellule pour 4 stations mobiles.

4.4.4 Les trois paires

Bien que 802.11 fournisse un accès équitable au médium radio dans une cellule de communication, la littérature a montré les faiblesses de cet accès dans le cadre des réseaux *ad hoc*. Cette faiblesse est flagrante dans le cas des trois paires.

L'étude de ce scénario est intéressante, car il montre un problème d'accès au médium qui n'est pas lié aux collisions. Dans ce cas, la paire centrale lutte pour l'accès au médium contre les deux paires extérieures. Ce déséquilibre peut provoquer une baisse drastique du nombre d'accès au médium pour la paire centrale. Celle-ci ne pouvant accéder au médium que quand les périodes de silence des deux paires extérieures se superposent.

Dans ce cas précis, plusieurs schémas d'équité pourraient être utilisés. Ces schémas d'équité peuvent prendre en compte ou non le déséquilibre présent dans le scénario. Ces schémas d'équité peuvent ainsi prendre la forme de plusieurs ordonnancements différents aboutissant ainsi à différents résultats de performance. La figure 4.8 montre quelques exemples d'ordonnancement possibles dans ce scénario. Les rectangles représentent la transmission de chacune des stations et plus particulièrement le rectangle blanc représente les transmissions de la paire centrale.

- La figure 4.8(a) représente un ordonnancement TDMA entre les 3 paires. Même si les transmissions des paires extérieures peuvent être concurrentes, un accès TDMA interdit l'accès simultané au médium radio. Cet ordonnancement fournit un débit global de C, si c'est la capacité du médium radio et de $C/3$ pour chacunes des stations émettrices.
- La figure 4.8(b) représente un ordonnancement aboutissant a une allocation MaxMin. Dans ce cas, les paires extérieures et la paire centrale alternent leurs transmissions. Avec cet ordonnancement, le débit global du réseau est de $3C/2$ et le débit de chaque station et de $C/2$.
- La figure 4.8(c) représente un ordonnancement où la position de chaque paire compte. Dans ce cas, la paire centrale est pénalisée car elle partage le médium avec deux fois plus de stations que les paires extérieures. Le débit global obtenu en suivant cet ordonnancement est de $5C/3$. Le débit des paires extérieures est de $2C/3$ et le débit de la paire centrale et de $C/3$.
- La figure 4.8(d) représente un ordonnancement maximisant le débit global. Dans cet ordonnancement, la paire centrale n'accède pas au médium. Le débit global du réseau vaut $2C$ et les deux paires extérieures obtiennent chacune un débit de C.

Nous ne nous intéressons par la suite qu'au schéma d'équité MaxMin, qui selon nous fournit le meilleur compromis équité-efficacité dans ce cas.

La figure 4.9 montre les résultats de simulations pour différents protocoles MAC. Cette figure montre que PNAV, MBFAIR et MadMac ont le même index d'équité sur ce scénario. Cet index d'équité est proche de 1, ce qui peut signifier que les trois stations émettrices ont le même débit. Cependant, nous pouvons voir que les débits globaux obtenus sont différents. Pour MBFAIR, le débit global obtenu est inférieur à la capacité d'une seule station. Nous pouvons donc supposer que l'ordonnancement obtenu avec MBFAIR suit plus ou moins l'ordonnancement décrit sur la figure 4.8(a). Pour PNAV, le débit global correspond à trois fois la capacité d'une station. Il y a deux explications possibles à cette valeur. Soit la capacité obtenue pour une station est très en-deçà de la capacité possible pour PNAV, soit les trois paires transmettent toutes en même temps et tout le temps. Nous penchons plus vers la première hypothèse, car PNAV s'appuie sur les mécanismes de CSMA/CA pour accéder au médium. Avec MadMac, le débit global obtenu correspond à $3C/2$, ce qui correspond à un ordonnancement MaxMin (figure 4.8(b)). Dans cet ordonnancement, toutes les stations ont le même débit ce qui permet d'obtenir un index d'équité égal à 1. Le débit global obtenu par 802.11 équivaut à $2C$. Nous supposons donc que l'ordonnancement fourni par 802.11 sur

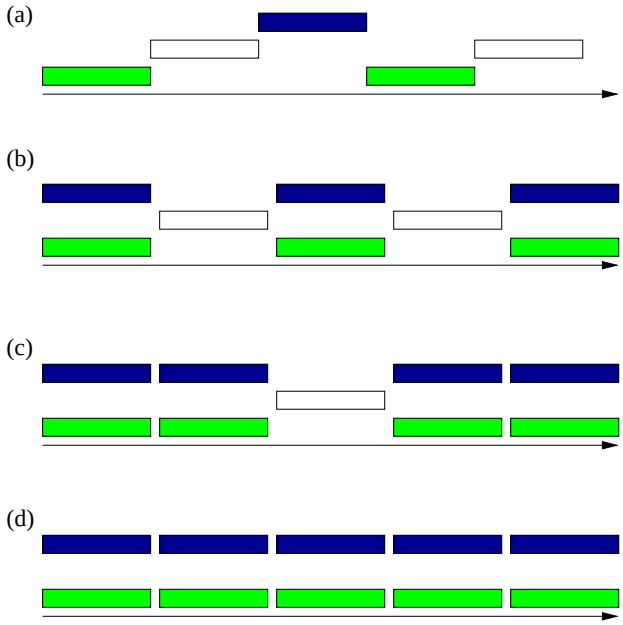


FIG. 4.8: Exemple de différents ordonnancements sur le scénario des trois paires. Les différentes rectangles représentent la transmission de chacune des stations. Plus particulièrement le rectangle blanc représente la transmission de la paire centrale.

ce scénario est l'ordonnancement décrit sur la figure 4.8(d). Ceci explique un index d'équité inférieur de à 0.7. Nous rappelons que le calcul et la valeur de l'index d'équité dépendent du schéma choisi. Ici nous avons choisi un schéma d'équité MaxMin.

Nous avons étendu nos simulations à plusieurs paires de communications parallèles. Dans ce scénario, chaque paire partage le médium avec ses voisins de gauche et de droite s'ils existent. La figure 4.10 montre les résultats de simulations pour différents protocoles MAC en fonction du nombre de paires parallèles. Les index d'équité ne sont pas tracés, car pour MadMac, PNAV et MBFAIR ils sont proches de 1 ; et pour 802.11, cet index dépend du nombre de paires. Cette figure montre que MadMac est le protocole le plus efficace comparé aux autres protocoles. La différence de débits entre i et $i+1$ est égale à $C/2$, ce qui signifie que MadMac permet d'avoir un bon ordonnancement sans perte de bande passante.

4.4.5 Les stations cachées asymétriques

La topologie des stations cachées asymétriques est intéressante à étudier car elle met en avant une interaction à deux sauts entre les émetteurs. L'asymétrie due à la topologie provoque un problème d'équité important au niveau des débits obtenus par les deux flux. Cette asymétrie provient du fait que l'une des stations ne subit jamais de collision.

La figure 4.11 présente les résultats de performance et d'équité sur ce scénario. D'un point de vue de l'équité, MadMac est meilleur que PNAV et que 802.11 avec ou sans le mécanisme de RTS/CTS. Cette équité accrue de MadMac vient tout d'abord de l'augmentation de la fenêtre de contention de l'émetteur favorisé qui permet à la station subissant des collisions, de transmettre un paquet. La transmission de ce paquet provoque la réception d'un acquittement sur l'émetteur ne subissant

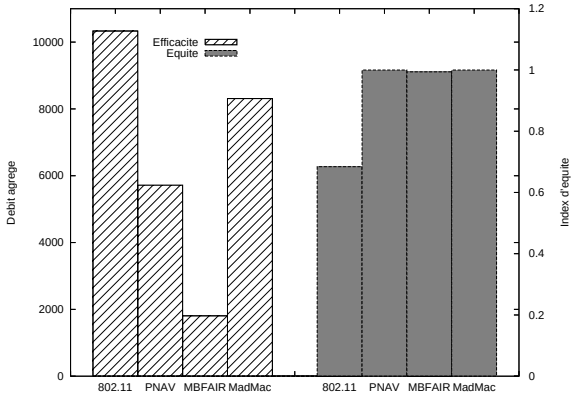


FIG. 4.9: Performance de MadMac sur le scénario des trois paires. Le débit global et l'index d'équité sont tracés suivant les deux axes des ordonnées (respectivement).

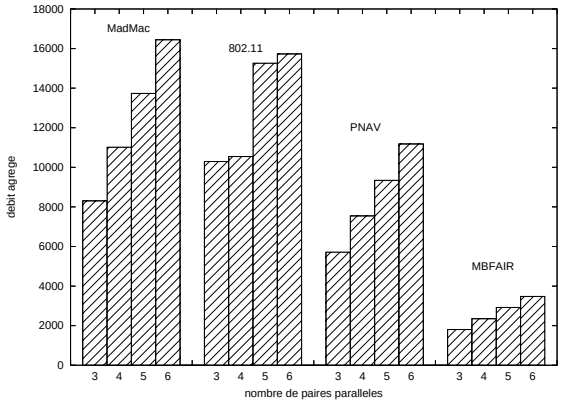


FIG. 4.10: Performance de MadMac sur plusieurs paires parallèles. Seul le débit global est tracé.

jamais de collision, faisant ainsi évoluer sa variable $ACT = 1$ et introduit une temps d'attente T_{WAIT} au niveau de l'émetteur favorisé. Il faut noter que la durée de transmission d'un paquet de 1000 octets est d'environ $1000\mu s$. Comme le temps maximum d'attente d'un backoff est de $620\mu s$, il est donc impossible dans cette situation pour la station subissant des collisions de transmettre le moindre paquet correctement avec 802.11. Dans ce scénario, la combinaison du mécanisme d'alternance et du mécanisme permettant d'éviter le monopole du canal permet à MadMac d'avoir de bonnes performances d'équité et d'efficacité. Si MBFAIR est plus équitable que MadMac, c'est que celui-ci réduit considérablement les débit des deux stations permettant ainsi d'avoir cette équité. Sur ce scénario, le comportement de MBFAIR rappel le comportement de 802.11 avec l'algorithme BEB inversé présenté dans le chapitre précédent.

Du point de vue de l'efficacité, MadMac est moins performant que 802.11 qui atteint la capacité du réseau. Avec 802.11, seule une station réussit à transmettre. MadMac lui ne peut atteindre la capacité du réseau car l'alternance entre les deux émetteurs n'est pas permanente. Quand la station subissant les collisions réussit enfin à transmettre son premier paquet, le mécanisme d'alternance est enclenché sur la deuxième station ($ACT = 1$) mais aussi sur la première ($COL = 1$). Avant que cette alternance ne soit enclenchée, des collisions ont lieu provoquant une perte de débit. Une

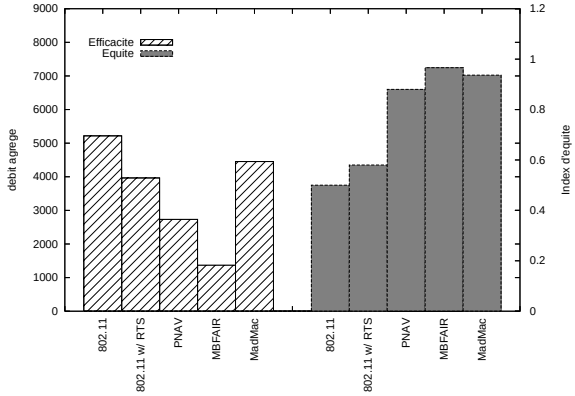


FIG. 4.11: Performance de MadMac sur le scénario des stations cachées asymétriques. Le débit global et l'index d'équité sont tracés suivant les deux axes des ordonnées (respectivement).

fois le mécanisme enclenché, ACT reste toujours égal à un pour la seconde station car elle reçoit systématiquement les acquittements de la première station. De son côté, la première station ne subit plus de collision. Néanmoins après un $Delta_Slot$, les stations se réinitialisent. Cette réinitialisation provoque de nouveau des collisions et une perte d'efficacité. Un simple dimensionnement de $Delta_Slot$ à un temps infini permettrait de résoudre ce problème. Néanmoins, les performances obtenues par MadMac restent acceptables. Notons que dans toutes les simulations menées, la valeur de $Delta_Slot$ vaut environ le temps de transmission de 10 paquets de la taille d'un MTU transmis au débit le plus bas ($Delta_Slot = .15$s). Ici, l'augmentation du temps $Delta_Slot$ permet non seulement d'accroître l'efficacité mais aussi l'équité.

Plusieurs autres topologies ont été testées mais nous ne présenterons pas les résultats dans ce manuscrit. Ces résultats peuvent être trouvés dans [67]. Nous pensons que les résultats donnés dans cette section permettent de présenter l'essence du protocole. Ces résultats résument dans un cadre très général l'utilisation d'un protocole MAC dans un réseau sans fil.

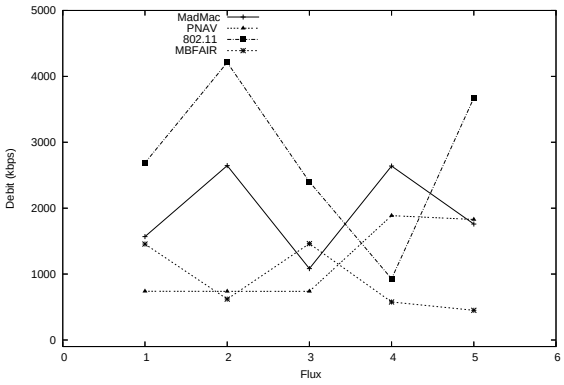
4.4.6 Simulations complémentaires

Dans cette sous-section, nous avons évalué les performances de MadMac par simulation sur d'autres topologies plus générales.

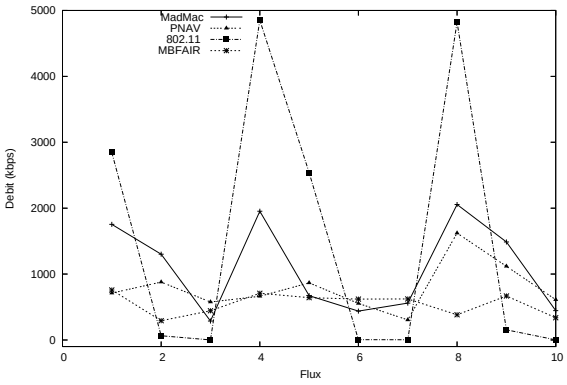
Topologies aléatoires

Ici, nous présentons les résultats obtenus sur une topologie aléatoire. La position des stations se fait de manière aléatoire et uniformément distribuée sur un plan de dimension 1000×1000. Les émetteurs sont choisis aléatoirement, et le récepteur d'un flux est choisi aléatoirement parmi le voisinage de l'émetteur. Le nombre généré de stations est 50. Dans ces scénarii, nous n'avons pas calculé l'index d'équité car il est difficile d'obtenir dans un scénario aléatoire le débit servant d'objectif. Dans ce scénario, chaque station essaie de saturer le médium avec un flux UDP ayant des tailles de paquets aléatoires et uniformément distribuées entre $[600; 1400]$.

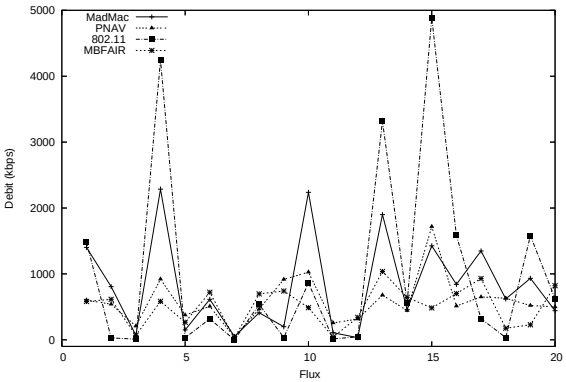
Les figures 4.12(a), 4.12(b) et 4.12(c) montrent les résultats pour des simulations impliquant 5, 10 et 20 flux respectivement. Bien que les résultats peuvent avoir des interprétations difficiles et



(a) 5 flux



(b) 10 flux



(c) 2à flux

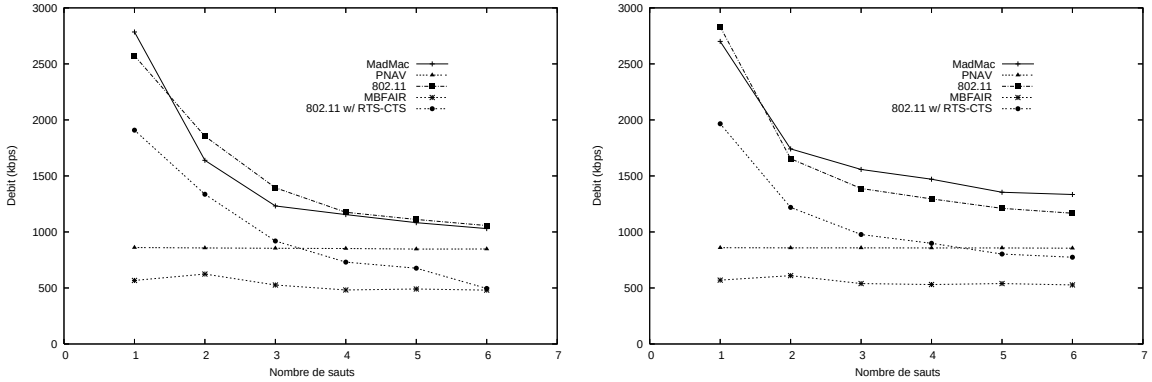
FIG. 4.12: MadMac : Résultats de performance sur des topologies aléatoires. Sur l'abscisse se trouve l'identifiant de chaque flux et sur l'ordonnée le débit obtenu par ce flux. MadMac, 802.11, PNAV et MBFAIR sont comparés.

multiples, nous pouvons voir sur ces figures que MadMac est un bon compromis entre l'équité et l'efficacité. On voit sur ces figures que MadMac maintient un bon débit sur chaque flux (quand c'est possible) tout en ayant des débits élévés sur chaque flux.

Flux multisauts

Dans cette section, nous présentons les débits obtenus par MadMac sur un flux multi-saut. Dans ce scénario, nous voulons voir comment MadMac réagit aux interférences intra-flux. Ce scénario présente un cas d'utilisation fréquent des réseaux *ad hoc* dans lequel une station veut transmettre des données à une autre station hors de sa portée de communication. L'utilisation d'un ou plusieurs relais pose des problèmes de collision comme les stations cachées et les stations cachées asymétriques mais aussi les trois paires. Les phénomènes impliqués dans ce scénario sont difficiles à identifier et les interactions entre ces phénomènes le sont encore plus [54]. Ici, nous regardons seulement les débits

obtenus pour chaque flux en fonction du nombre de sauts à parcourir pour atteindre la destination.



(a) Interférence = 2xCommunication

(b) Interférence = Communication

FIG. 4.13: MadMac : Résultats de performance sur une chaîne. Ces courbes tracent les débits obtenus par un flux en fonction du nombre de sauts parcourus par ce flux. La première figure donne les résultats quand la zone de détection de porteuse est de deux fois la taille de la zone de communication. La seconde figure donne les même résultats quand la zone de détection de porteuse est la même que la zone de communication. Notons que les relais se trouvent en bordure de la zone de communication.

Les figures 4.13(a) et 4.13(b) montrent les résultats quand la zone de détection de porteuse est deux fois plus grande que la zone de communication et quand la zone de détection de porteuse est équivalente à la zone de communication respectivement. Les stations servant de relais se trouvent toutes en bordure de la zone de communication. Ces figures montrent que le comportement de 802.11 et de MadMac sont quasiment identiques.

Nous avons aussi voulu tester MadMac sur une grille sur laquelle des flux multi-sauts sont lancés (figure 4.14). Ce scénario revient à avoir plusieurs chaînes de communication en parallèles. Dans ce scénario, la zone de détection de porteuse est égale à deux fois la zone de communication. Sur la grille, toutes les stations sont espacées d'une distance égale à la zone de communication (que ce soit verticalement ou horizontalement). Nous avons choisi d'avoir une grille de 5×6. Les flux suivent une direction horizontale de gauche vers la droite. Il y a donc 5 flux parcourant chacun des 5 sauts pour arriver à leur destination respective.

Le figure 4.15 montre les performances de MadMac sur ce scénario. Ici, nous voyons que MadMac fournit encore une fois un bon compromis entre l'équité et l'efficacité. Dans ce contexte particulier, avec PNAV, la chaîne centrale n'obtient qu'un très bas débit car le partage n'est pas fait correctement. Cet accès réduit le débit de la chaîne centrale, permet au chaînes extérieures d'obtenir des débits plus élevés et ainsi à PNAV d'accroître sont débit global. Cependant, nous pouvons voir que l'écart des débits globaux de MadMac et de PNAV est faible de l'ordre de 5%, alors que la différence entre les index d'équité est de l'ordre de 12%. Notons que le comportement de PNAV pour l'un des maillons de la chaîne centrale correspond ou presque au comportement sur une cellule de plus de 12 stations sur laquelle PNAV à presque le même comportement que 802.11. Ceci explique pourquoi la chaîne centrale à un débit faible qui profite aux chaînes extérieures mais aussi au débit global.

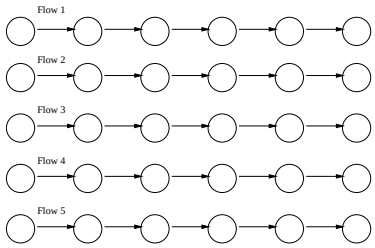


FIG. 4.14: MadMac : La topologie en grille avec des flux partant de gauche vers la droite. La distance entre deux stations voisines est équivalente à la portée de communication et la zone d'interférence correspond à deux fois la zone de communication.

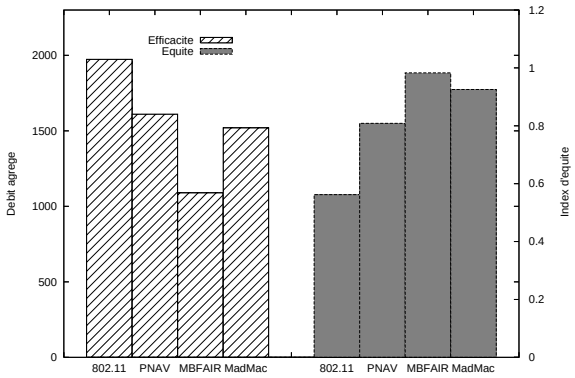


FIG. 4.15: Performance de MadMac sur une grille. Le débit global et l'index d'équité sont tracés suivant les deux axes des ordonnées (respectivement).

4.5 Conclusion

Dans cette section, nous avons proposé et décrit un nouveau protocole MAC appelé MadMac. L'objectif de ce protocole est de fournir un compromis entre l'efficacité et l'équité dans un réseau *ad hoc*. Pour obtenir une meilleure efficacité, MadMac n'effectue aucun échange d'informations. De plus, MadMac ne s'appuie que sur des informations déjà disponibles dans 802.11. Le principe de MadMac est d'obtenir un partage équitable du médium radio et d'éviter les collisions. Pour ce faire, des temps d'attente sont insérés entre chaque transmission de paquets permettant ainsi aux stations concurrentes d'accéder au médium.

Des simulations ont été menées pour évaluer les performances de MadMac. Une comparaison avec d'autres protocoles de la littérature a aussi été effectuée. Dans ce manuscrit, nous n'avons présenté que quelques scénarii mettant en avant la capacité du protocole à résoudre les problèmes d'accès à une ressource partagée. Ces résultats montrent que MadMac permet, contrairement à 802.11, de fournir un bon compromis équité-efficacité.

Bien que le protocole MadMac présente de bonnes performances, celles-ci sont liées aux paramètres qui le régissent. Les variables telles que $Delta_Slot$, x et k peuvent modifier considérablement les performances du réseau si elles sont mal dimensionnées. Néanmoins, les résultats de simulations présentés montrent qu'il pourrait exister des valeurs optimales pour ces paramètres. Cependant,

l'obtention de ces valeurs optimales nous semble complexe que ce soit de manière analytique ou par des simulations. Il faut noter que le dimensionnement de ces valeurs et leur optimalité vont très souvent dépendre du scénario d'utilisation.

Les contraintes que nous nous sommes imposées pour la conception de MadMac sont très strictes. Il est clair que relaxer ces contraintes permettrait d'accroître l'équité et l'efficacité de notre protocole. Par exemple, utiliser les informations contenues dans les paquets ou alors la table de voisinage et de routage du niveau 3 permettrait de mieux dimensionner les temps d'attentes de MadMac. Une des suites de ce travail est donc de mesurer l'impact de l'apport de telles informations.

Influence de la couche MAC sur les couches supérieures

5

« Plus tu en sais sur les choses, plus elles semblent bizarres. »

Bill Watterson,
Extrait de la bande dessinée Calvin et Hobbes.

Ce chapitre est consacré à l'étude de l'influence de la couche MAC sur les protocoles des couches supérieures. Cette étude met en avant l'utilité (ou non) d'une couche MAC efficace et équitable dans une pile protocolaire complète.

MadMac, décrit dans le chapitre précédent, est un protocole qui s'attache simplement à fournir un accès équitable et efficace au médium radio. Il nous paraissait donc naturel de savoir comment les protocoles des couches supérieures réagiraient à ce type d'accès. Intuitivement, on pourrait penser que l'amélioration de la couche MAC ne pourrait qu'améliorer les performances des couches plus hautes. Cependant, une autre question se pose : les performances des couches hautes sont elles améliorées de manière significative ? Cette question est importante car elle justifie ou non le déploiement et la création d'un nouveau standard.

C'est donc pour répondre à la question de l'influence de la couche MAC sur les couches supérieures que des simulations on été menées. Les résultats de ces simulations sont présentés dans ce chapitre.

Sommaire

5.1 Introduction 76
5.2 La découverte de voisinage 76
5.2.1 Description 76
5.2.2 Paramètres de performance 77
5.3 Évaluation de performance 77
5.3.1 File d'attente $M/D/1/K$ 78
5.3.2 Simulations 81
5.4 Conclusion 85

5.1 Introduction

Dans ce chapitre, nous présentons les derniers résultats (d'un point de vue chronologique) de cette thèse. Nous nous sommes posés la question de l'utilité d'une couche MAC efficace et/ou équitable. Cette question n'est apparue que vers la fin des travaux de thèse, alors qu'elle aurait peut-être due en être le centre. Une explication possible de ce questionnement tardif est qu'au début de la thèse, les applications des réseaux *ad hoc* n'étaient pas encore bien définies. Ces applications sont maintenant de plus en plus claires. On peut citer comme exemple les réseaux maillés, les réseaux véhiculaires, les réseaux de capteurs et bien d'autres encore.

Avec l'émergence de ces applications il nous a paru intéressant de connaître l'impact de notre protocole sur les protocoles utilisés dans les réseaux *ad hoc*. Ne pouvant être exhaustifs sur les protocoles que nous pourrions tester au dessus de MadMac, nous avons dû faire un choix[1]. C'est ainsi que nous avons choisi d'étudier l'apport d'un protocole MAC équitable et efficace sur un protocole de découverte de voisinage.

Un protocole de découverte de voisinage comme le protocole *HELLO* est selon nous l'un des protocoles les plus importants pour les réseaux *ad hoc*. La spontanéité, la mobilité et l'apparition et la disparition des stations dans un réseau *ad hoc* font de ce protocole l'un des plus importants pour maintenir les services tels que le routage ou l'auto-organisation.

Un autre avantage non négligeable de ce protocole est sa simplicité du point de vue du fonctionnement mais aussi du point de vue de l'évaluation de ces performances. Ainsi, il sera facile de voir l'effet de différentes couches MAC sur le protocole.

5.2 La découverte de voisinage

5.2.1 Description

Le but d'un protocole de découverte de voisinage est :
– De découvrir le voisinage.
– De se faire découvrir pas ses voisins.
Pour cela, chaque station utilisant le protocole envoie périodiquement, en *broadcast*, des messages contenant son identifiant (et peut-être d'autres informations) dans un paquet appelé souvent *HELLO*. La réception d'un tel paquet permet à une station de maintenir une table de voisins utile pour les protocoles de routage ou les protocoles d'auto-organisation.

[1] Du moins pour le temps imparti à la thèse

Un protocole *HELLO* possède deux paramètres : *1*) La fréquence d'envoi des paquet *HELLO* et *2*) la fréquence de rafraîchissement de la table de voisinage. Une fréquence d'envoi trop faible pose un problème de réactivité, alors qu'une fréquence trop élevée surcharge le réseau en paquets de contrôle. De même, un taux de rafraîchissement trop lent fausse la vue du réseau. Un taux de rafraîchissement trop rapide ne permettrait pas à d'autres protocoles d'utiliser les informations de la table de voisinage. Nous ne discuterons pas ici des paramètres optimaux pour un protocole de voisinage. Nous utiliserons simplement les paramètres utilisés dans la plupart des protocoles comme OLSR [16] ou ADOV [63]. Ces protocoles ont choisi une fréquence d'envoi de 1 paquet par seconde et un rafraîchissement toutes les 3 secondes. Ceci veut dire que toutes les entrées de la table de voisinage de plus de 3 secondes sont supprimées.

Il faut noter que les messages *HELLO* sont transmis en *broadcast*. Ceux-ci ne bénéficient donc pas de la fiabilité de la couche MAC, fiabilité apportée par les acquittements au niveau MAC. La couche MAC a donc un double objectif : *1*) minimiser le délai de transmission d'un message *HELLO*, mais aussi *2*) éviter les collisions lors de la transmission de ces messages. Ainsi, l'état de la table de voisinage est fortement lié aux performances de la couche MAC, et surtout de la fiabilité et au délai de celui-ci.

5.2.2 Paramètres de performance

L'évaluation de l'impact de la couche MAC sur le protocole de découverte de voisinage décrit ci-dessus est très simple. Pour cela, nous utilisons l'état de la table de voisinage. Nous nous concentrons sur deux points principaux :

- La découverte de tous les voisins. Cette métrique montre simplement si tous les voisins possibles, c'est-à-dire à portée de communication d'un paquet *HELLO*, ont été découverts. Cette métrique permet de dire si au bout d'un temps infini, un voisin sera découvert.
- La consistance de la table de voisinage. Cette métrique est plus restrictive que la précédente. Cette métrique permet de vérifier si à un instant donné, tous les voisins et seulement les voisins d'une station sont présents dans sa table de voisinage. C'est une métrique de fréquence de paquet *HELLO* et de rafraîchissement de la table car l'inconsistance peut correspondre à un voisin non découvert ou à une entrée dans la table de voisinage correspondant à un voisin déjà parti.

Ici nous utiliserons la deuxième métrique concernant l'inconsistance par rapport à des voisins non découverts. Nous n'utilisons que cette métrique car en plus d'inclure la première métrique, elle est suffisante pour permettre d'analyser l'influence de la couche MAC sur le protocole de découverte de voisinage. Cette métrique est un critère de performance important. Selon nous, la connaissance complète du voisinage est fondamentale pour les autres protocoles. Cette connaissance permet le choix des bonnes routes pour les protocoles de routage. Elle permet aussi l'élection correcte de tête de *cluster* ou la construction correcte de dorsale pour certains protocoles d'auto-organisation.

5.3 Évaluation de performance

Dans cette section, nous présentons quelques résultats d'évaluation de performance d'un protocole de découverte de voisinage comme décrit précédemment. Nous n'étudions qu'un seul scénario dans cette section. Nous étudions l'état de la table de routage d'une station précise pour laquelle nous connaissons le nombre de voisins, qui est fixe. Dans ce scénario, toutes les stations sont à portée de communication. Nous cherchons donc à voir comment l'utilisation d'une couche MAC altère la

table de voisinage d'une station.

5.3.1 File d'attente $M/D/1/K$

Pour modéliser l'état de la table de voisinage d'une station, nous utilisons une file d'attente $M/D/1/K$.

Arrivée suivant une loi de Poisson : La génération d'un paquet *HELLO* sur chaque station est un évènement rare généré avec une fréquence bien précise à laquelle est ajoutée une dérive aléatoire pour éviter la synchronisation entre les stations. Ainsi, nous choisissons de modéliser la somme des émissions de tous les voisins d'une station par une inter-arrivée suivant une loi de poisson sur la station étudiée.

Temps de service déterministe : Comme une entrée dans la table de voisinage est supprimée toutes les 3 secondes, nous avons représenté cette suppression par une loi déterministe de moyenne constante et de variance nulle.

1 **seul serveur :** Les paquets *HELLO* ne pouvant pas arriver en même temps sur la station étudiée, un seul serveur suffit à modéliser la suppression d'une entrée de la table de voisinage.

K **places dans la file d'attente :** La file d'attente ne comporte que k places qui sont le nombre voisins maximum que la station peut avoir. Une file d'attente pleine signifie donc que tous les voisins sont découverts et que la table de voisinage est consistante.

Les résultats suivants donnent les probabilités $\Pi = (\pi_0, \pi_1, ..., \pi_k)$ à l'état stationnaire de la file d'attente. Les résultats de la file $M/D/1/K$ présentés ne donne qu'une manière de calculer numériquement les probabilités π_i et ne représentent pas la formule close pour ces probabilités. Les résultats sur les files $M/D/1/K$ présentés ci-dessous et les formules closes peuvent être retrouvés dans [31].

Les π_i s'écrivent :

$$\pi_0 = \left[\sum_{j=0}^{K} \nu_j\right]^{-1} \tag{5.1}$$

$$\pi_i = \nu_i \pi_0 \qquad i = 1, 2, ..., K \tag{5.2}$$

Où les ν_i se calculent de la manière récursive suivante :

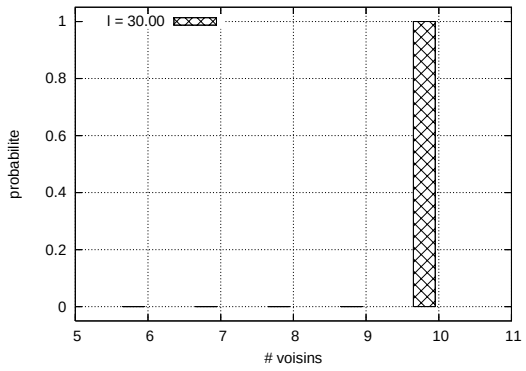


FIG. 5.1: Résultats d'analyse d'un protocole $HELLO$ avec une file $M/D/1/K$. La figure trace les probabilités π_i d'avoir i clients dans le système pour $K = 10$.

$$\nu_0 = 1 \tag{5.3}$$

$$\nu_1 = \frac{1-k_0}{k_0} \tag{5.4}$$

$$\nu_2 = \frac{1-k_1}{k_0}.\nu_1 - \frac{k_1}{k_0} \tag{5.5}$$

$$... \tag{5.6}$$

$$\nu_j = \frac{1-k_1}{k_0}.\nu_{j-1} - \frac{k_2}{k_0}.\nu_{j-2} - ...\frac{k_{j-1}}{k_0}.\nu_1 - \frac{k_{j-1}}{k_0} \tag{5.7}$$

Les k_i se calculent de la manière suivante :

$$k_i = e^{\lambda}.\frac{\lambda^j}{j!} \tag{5.8}$$

Notons que le calcul factoriel au dénominateur de l'expression de k_j devient vite difficile à calculer quand j augmente.

La figure 5.1 montre les probabilités π_i. π_i représente la probabilité pour la table de voisins de contenir i entrées. Cette figure montre les probabilités π_i obtenues avec la file $M/D/1/K$ précédente pour $K = 10$. Pour un nombre de voisin $K = 10$ la fréquence de génération total de paquet $HELLO$ pour toutes les stations est de 30 paquets par unité de temps, car chacune des 10 stations génère 3 paquets par unité de temps. De ce fait, sur cette figure $\lambda = 30$ et la fréquence de rafraîchissement de la table de voisinage est de 1 unité de temps. La figure montre que dans le cas présenté, la probabilité d'avoir un état consistent est de 100%

Cependant, ici, nous ne considérons pas les pertes de messages dues aux collisions au niveau MAC. Ces collisions affectent la valeur de λ dans les équations précédentes. En effet, dans les calculs précédents, λ correspond au taux de réception de messages correctes sur la station observée. En réalité, la valeur de λ doit être modulée par les probabilités de collision des paquets $HELLO$ entre eux.

Si nous considérons que les stations sont complètement désynchronisées, nous pouvons supposer

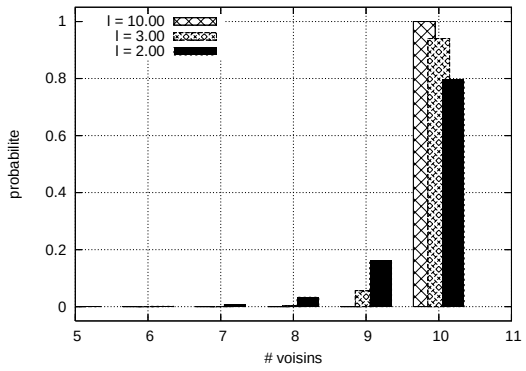


FIG. 5.2: Résultats d'analyse d'un protocole $HELLO$ avec une file $M/D/1/K$ avec des intensités de trafic différentes. La figure trace les probabilités π_i d'avoir i clients dans le système pour $K = 10$.

que le choix de l'instant de transmission de chaque station est tiré aléatoirement et uniformément dans un intervalle de $[0; 1]$ seconde. En s'appuyant sur les paramètres de 802.11, on peut diviser la seconde en *slot* de $20\mu s$. La probabilité de collision de deux ou plusieurs paquets $HELLO$ reste très faible. Elle s'écrit :

$$P_{col} = 1 - \frac{\omega!}{\omega^K \times (\omega - K)!} \tag{5.9}$$

Où $\omega = 50000$ est le nombre de *slots* de $20\mu s$ possible dans une seconde. Cette probabilité est proche de 0 pour $K = 10$. Notons que ce calcul n'est pas le calcul précis de la probabilité de collision pour les paquets $HELLO$ qui dépend de la taille des paquets $HELLO$, des instants de déclenchement des transmissions, etc. Cette probabilité selon nous reste faible.

Les premiers résultats montrent que dans ces conditions ($K = 10$ stations, $\lambda = 30$ et le temps de service de la file $\mu = 1$), le cas idéal est que 100% des voisins se trouvent dans la table de voisinage à chaque instant. Les résultats sont similaires pour $K = 20$ et $K = 30$. Il s'avère que tant que la valeur de λ ne diminue pas, les voisins d'une station seront toujours systématiquement présents dans la table de voisinage. La figure 5.2 montre trois valeurs de λ pour lesquelles la probabilité de consistance de table de voisinage n'est pas 1. Les résultats pour $\lambda = 3$ sur cette figure signifie que dans environ 95% des cas la table de voisinage est complète et dans 5% des cas elle ne contient que 9 entrées sur les 10. Cette intensité $\lambda = 3$, pour $K = 10$ signifie que chacun des paquets $HELLO$ envoyé aura une probabilité de 90% de ne pas être reçu correctement. Nous voyons sur cette figure que la diminution de λ diminue la probabilité pour une station d'avoir une table de voisinage complète. Ainsi pour $\lambda = 2$ cette probabilité est encore plus faible.

Ces premiers résultats sont indépendants de la couche MAC et supposent que celle-ci ne génère aucune collision. On peut supposer que pour $K = 10$ stations, $\lambda = 30$ et le temps de service de la file $\mu = 1$, la probabilité décrite dans l'équation 5.9 reste faible et est inférieure à 90%. Ainsi, l'utilisation d'une couche MAC qu'elle soit équitable et/ou efficace n'influe pas, dans ces conditions, l'état de la table de voisinage. Nous confirmons cette hypothèse par des simulations dans la section suivante.

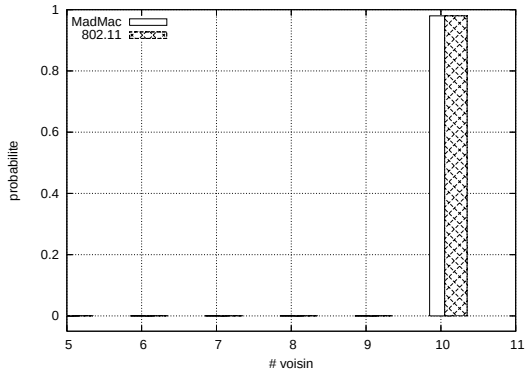


FIG. 5.3: Résultats de simulation et comparaison de MadMac et 802.11 pour $K = 10$ dans une cellule de communication. Les résultats présentés sont les statistiques obtenues sur la moyenne de toutes les stations.

5.3.2 Simulations

Cas sans collisions

Nous avons voulu confirmer par simulations les hypothèses que nous avons faites dans la section précédente. Nous voulons vérifier que l'utilisation d'une couche MAC n'influe pas sur les performances du protocole de découverte de voisinage. Les simulations ont été menées avec le simulateur NS-2. Les paquets de contrôle tels que les paquets ARP ont été supprimés pour ne pas interférer avec les paquets $HELLO$. Notons que nous avons développé un protocole $HELLO$ spécifique nous permettant d'en contrôler tous les paramètres.

La figure 5.3 montre la moyenne des résultats de 30 simulations de $100s$ dans une cellule de communication. Dans ce scénario, toutes les stations sont à portée de communication. Le nombre de voisins que devrait découvrir chaque station est $K = 10$. Pour cette simulation, MadMac et 802.11 ont été utilisés comme couche MAC. La figure confirme notre hypothèse précédente. L'utilisation de MadMac ou de 802.11 fournit le même résultat pour l'état de la table de voisinage. Dans cette simulation, que ce soit avec MadMac ou 802.11, tous les voisins sont toujours présents dans la table de voisinage à chaque instant de la simulation.

Les mêmes résultats sont présentés sur la figure 5.4 pour $K = 20$ et $K = 30$. Comme sur la figure 5.3, les résultats confirment notre hypothèse précédente sur le fait que la couche MAC, du moins 802.11 et MadMac, n'a aucune influence sur le protocole de découverte de voisinage.

Dans ce contexte, MadMac et 802.11 sont assez efficaces pour l'évitement de collisions, ce qui permet au protocole de découverte de voisinage de fonctionner correctement. Les paramètres du protocole $HELLO$ liés à l'évitement de collisions fourni par l'une ou l'autre des couches MAC testées fournissent un couple permettant d'avoir des performances optimales pour le protocole $HELLO$. Cependant, il est possible que la modification des paramètres du protocole $HELLO$, tels que la réduction du temps de rafraîchissement de la table influe sur les performances du protocole. De plus, l'augmentation du taux de collisions dans la cellule de communication peut aussi influer sur les performances du protocole.

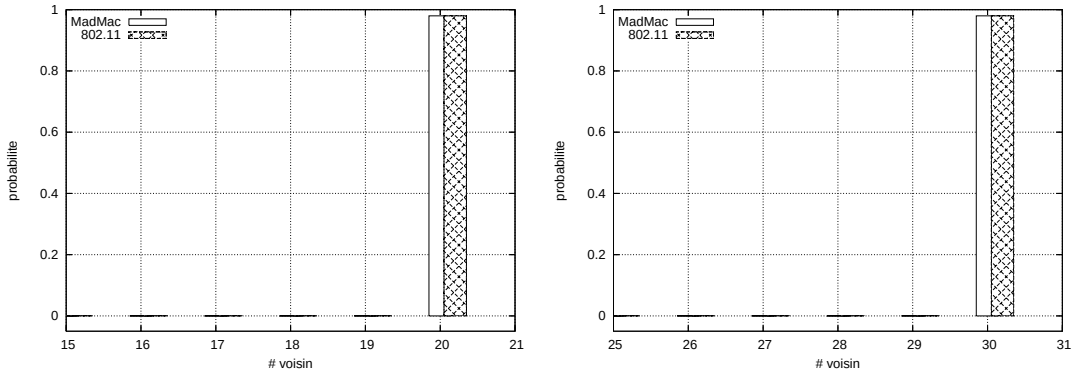


FIG. 5.4: Résultats de simulation et comparaison de MadMac et 802.11 pour $K = 20$ (à gauche) et $K = 30$ (à droite) dans une cellule de communication. Les résultats présentés sont les statistiques obtenues sur la moyenne de toutes les stations.

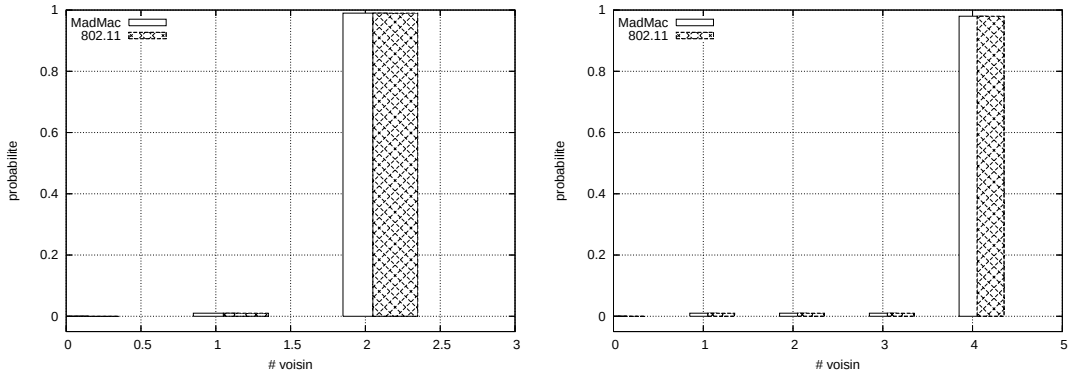


FIG. 5.5: Résultats de simulations et comparaison de MadMac et 802.11 sur le scénario des stations cachées avec 2 stations cachées (à gauche) et 4 stations cachées (à droite). Les résultats présentés sont les statistiques obtenues pour la station qui "voit" toutes les stations.

Cas avec collisions : Les stations cachées

Pour mieux voir l'influence de la couche MAC sur le protocole de découverte de voisinage, nous avons testé le protocole *HELLO* dans des cas pathologiques d'utilisation de la couche MAC. Pour cela, nous avons cherché à générer des collisions au niveau MAC. Une manière simple de générer des collisions au niveau MAC est de considérer le scénario des stations cachées.

Les résultats de simulations présentés sur la figure 5.5 sont les résultats pour le scénario des stations cachées avec 2 stations cachées (à gauche) et 4 stations cachées (à droite) respectivement. Ici encore, les résultats de MadMac et de 802.11 sont les mêmes. Les performances du protocole de découverte de voisinage sont optimales. Ces performances sont normales, car comme indiqué dans la section précédente, il faudrait plus de 90% de collisions pour altérer le comportement du protocole de découverte de voisinage. Or dans les stations cachées avec 2 stations, cette probabilité de collision est inférieure à 5% pour 802.11 (voir chapitre 3). Nous supposons que le taux de collisions de MadMac est lui aussi inférieur à 5%. Pour les 4 stations cachées, nous supposons en fonction des résultats obtenus sur le protocole *HELLO*, que cette probabilité de collision est en-deçà de 90%.

Ici, le scénario des stations cachées ne génèrent pas assez de collisions pour bien voir l'effet de la

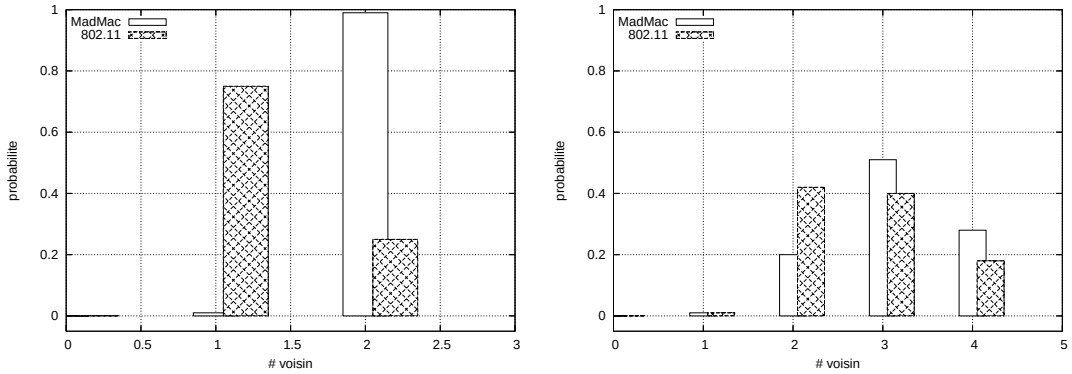


FIG. 5.6: Résultats de simulations et comparaison de MadMac et 802.11 sur le scénario des stations cachées avec 2 stations cachées (à gauche) et 4 stations cachées (à droite) en présence de flux UDP à saturation. Les résultats présentés sont les statistiques obtenues pour la station qui "voit" toutes les stations.

couche MAC sur le protocole de découverte de voisinage. De plus dans ce scénario, les mécanismes d'évitement de collisions de 802.11 et de MadMac ne sont pas utilisés ce qui ne met pas en avant l'influence de la couche MAC. En effet, les paquets *HELLO* étant envoyés, en mode *broadcast*, la couche MAC ne sait pas si celle-ci est entrée en collision ou non. De ce fait, les mécanismes comme la phase d'évitement de collisions dans MadMac et l'augmentation de la fenêtre de contention de 802.11 ne sont jamais utilisés.

Pour que les protocoles MAC utilisent ce type de mécanisme, nous avons rajouté des flux UDP à saturation issus des 2 stations cachées, ou 4 selon le scénario considéré. Ces flux ne sont générés que pour provoquer des collisions sur les paquets *HELLO*. De plus, sur chaque station, les paquets *HELLO* ont la priorité sur les paquets CBR. En fait, les paquets *HELLO* sont insérés au début de la file d'attente avant la couche MAC pour s'assurer que tous les paquets *HELLO* seront transmis et que les paquets rejetés au niveau de la couche *Link Layer* ne sont que des paquets de données et non des paquets *HELLO*.

Les résultats présentés sur la figure 5.6 montrent les résultats sur les stations cachées (2 à gauche et 4 à droite) en présence de flux UDP. Sur ces courbes, nous voyons clairement l'influence des couches MAC sur les performances du protocole de découverte de voisinage.

La figure 5.6 à gauche montre que l'utilisation de MadMac permet d'avoir durant presque toute la totalité des simulations un état consistant de la table de voisinage. L'utilisation de 802.11 ne permet d'avoir un état consistant que 25% du temps. Dans 75% du temps, la station considère qu'elle n'a qu'un seul voisin. Les meilleures performances de MadMac sont essentiellement dues au fait qu'entre chaque transmission d'un paquet de données, un temps d'attente est inséré, ce qui permet aux paquets *HELLO* des autres stations d'être reçus correctement.

La figure 5.6 à droite montre aussi que l'utilisation de MadMac permet d'avoir de meilleures performances que 802.11, même si ces performances ne sont pas optimales. Dans le cas des 4 stations cachées, le nombre de collisions est bien trop élevé pour permettre l'obtention de performances optimales que ce soit pour MadMac ou pour 802.11. On peut voir sur les histogrammes que la forme de la distribution de probabilité de MadMac est proche d'une distribution normale, alors que celle de 802.11 est plus proche d'une distribution uniforme. En calculant le nombre moyen d'entrées dans la table de voisinage pour MadMac (3.06 avec une variance de 0.50) et pour 802.11 (2.73 avec une variance de 0.57), on peut voir clairement que MadMac est plus adapté que 802.11 comme protocole

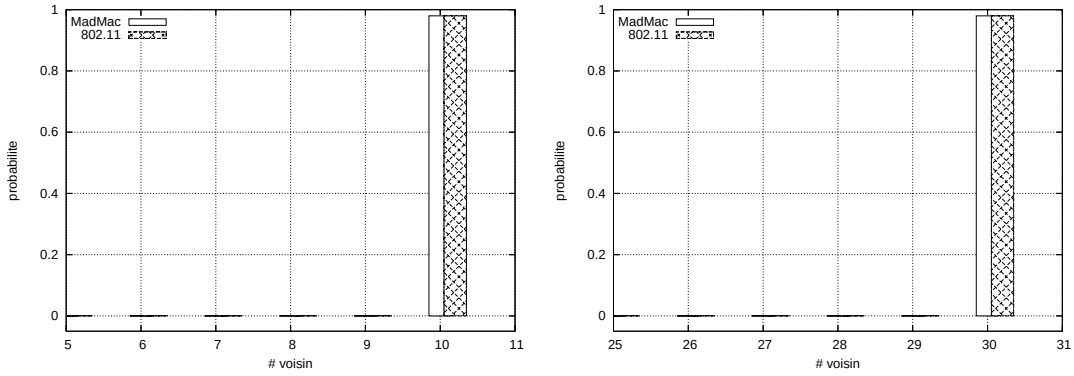


FIG. 5.7: Résultats de simulations et comparaison de MadMac et 802.11 sur une cellule de densité 10 (gauche) et 30 (droite) avec 1 flux UDP à saturation. Les résultats présentés sont les statistiques obtenues sur toutes les stations.

sous-jacent d'un protocole de découverte de voisinage, du moins sur ces scénarii.

Cas avec collisions : La cellule de communication

Le cas des stations cachées présenté précédemment est un cas particulier et extrême d'évaluation du protocole de découverte de voisinage. Dans cette sous-section, nous avons voulu évaluer les performances du protocole *HELLO* dans des conditions moins extrêmes. Pour ce faire, nous avons simulé une cellule de communication avec une densité donnée de stations. Et nous avons généré un nombre croissant de flux entre des stations choisies aléatoirement.

Le premier cas que nous avons testé, dont les résultats sont présentés sur la figure 5.7, est le résultat d'une simulation d'une cellule de 10 et 30 stations avec 1 flux UDP à saturation. Ces résultats montrent que le trafic généré n'affecte en rien le fonctionnement du protocole de découverte de voisinage. Dans ce cas, la figure montre que le comportement du protocole *HELLO* est idéal indépendamment du protocole MAC utilisé.

Les résultats présentés sur la figure 5.8 sont obtenus en mettant 4 flux aléatoires dans la cellule de densité 10 et 30. Ces résultats montrent que le protocole de découverte de voisinage ne se comporte plus de manière idéale quelle que soit la couche MAC utilisée. On voit aussi que MadMac et 802.11 ont quasiment la même influence sur le protocole de découverte de voisinage avec un léger avantage pour MadMac. Cette figure montre aussi que la densité de la cellule a un impact sur le comportement du protocole de découverte de voisinage. En effet, plus la cellule de communication est dense, plus les trafics générés par les paquets *HELLO* s'intensifient et plus la probabilité de collision augmente. Ces résultats montrent que le choix d'une couche MAC n'est pas d'une grande importance, car pour les deux couches MAC, les performances des protocoles *HELLO* sont sous-optimales et sont quasiment similaires.

La figure 5.9 montre les résultats de simulation quand le nombre de flux est augmenté à 8 dans une cellule de communication. Dans ce cas, le comportement du protocole de découverte de voisinage est bien entendu sous-optimal. En revanche, le choix du protocole MAC permet d'avoir des performances complètement différentes surtout pour une densité de cellule égale à 30. Pour cette densité, l'utilisation de MadMac permet un gain d'environ 30% par rapport à 802.11. Ce gain se calcule sur la probabilité d'avoir une table de voisinage complète. Ce gain s'élève à environ 8% quand la densité de la cellule de communication est de 10. Ces gains sont, selon nous, assez significatifs pour

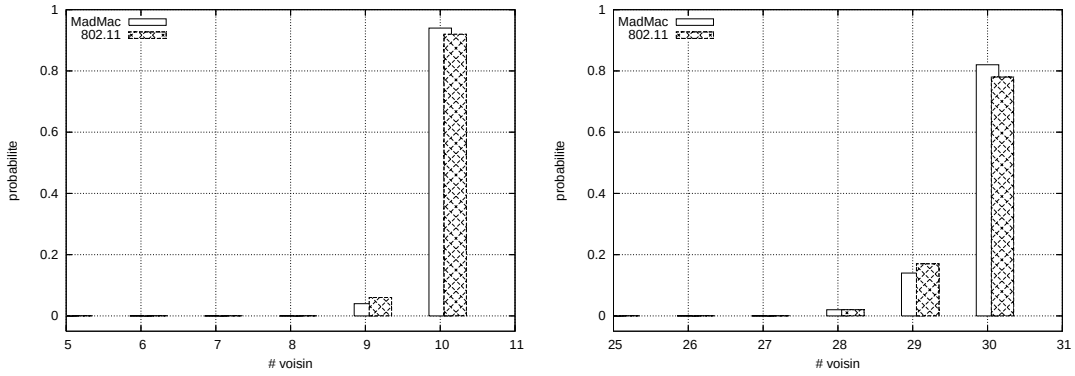


FIG. 5.8: Résultats de simulations et comparaison de MadMac et 802.11 sur une cellule de densité 10 (gauche) et 30 (droite) avec 4 flux UDP à saturation. Les résultats présentés sont les statistiques obtenues sur toutes les stations.

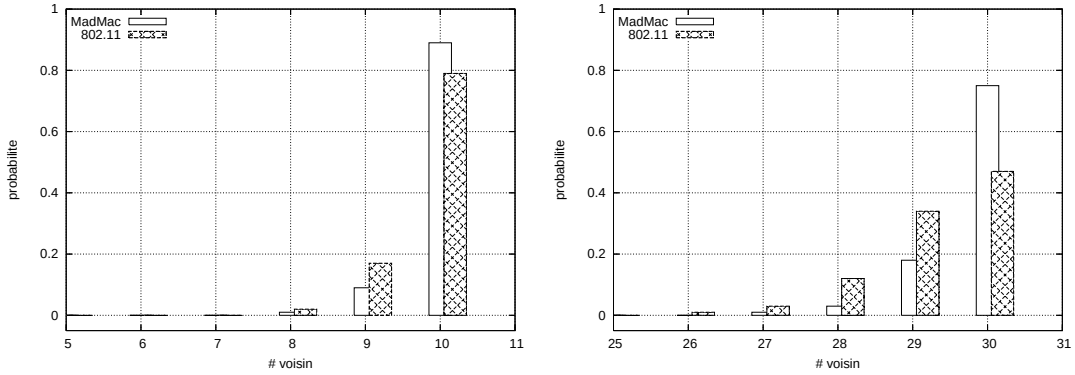


FIG. 5.9: Résultats de simulations et comparaison de MadMac et 802.11 sur une cellule de densité 10 (gauche) et 30 (droite) avec 8 flux UDP à saturation. Les résultats présentés sont les statistiques obtenues sur toutes les stations.

justifier le choix de MadMac comme protocole MAC, dans ces conditions de densité et de flux. De plus, nous avons aussi mesuré le débit global obtenu dans le réseau. Le débit obtenu par 802.11 est de 5038.09 kbps et celui obtenu par MadMac est de 5063.15. Les débits globaux résultants étant les mêmes, on peut considérer que l'utilisation de MadMac est plus judicieux pour obtenir de meilleures performances dans le réseau.

5.4 Conclusion

Dans cette section, nous avons montré l'utilité et l'influence d'une couche MAC équitable et efficace sur un protocole de niveau 3 du modèle OSI. Nous avons évalué les performances d'un protocole de découverte de voisinage utilisé au-dessus de 802.11 et de MadMac. Comme décrit dans le chapitre précédent, MadMac se veut être un protocole fournissant un bon compromis entre équité et efficacité alors que 802.11 est un protocole plus efficace qu'il n'est équitable.

Les résultats de ce chapitre montrent l'influence de l'une ou de l'autre des deux couches MAC sur un protocole de découverte de voisinage. On peut séparer les résultats et les présenter en deux

catégories : *1)* Les résultats du protocole de découverte de voisinage seul ; *2)* Les résultats du protocole de découverte de voisinage en présence de flux UDP.

Dans le premier cas, les deux couches MAC ont exactement la même influence sur le protocole de découverte de voisinage. Les deux couches MAC n'affectent pas le comportement du protocole, et celui-ci se comporte d'une manière idéale, c'est-à-dire qu'a chaque instant, la table de voisinage est complète et représente la vue réelle du voisinage.

Dans le second cas, l'ajout de flux UDP provoque des collisions sur les paquets de découverte de voisinage. Ces pertes peuvent altérer l'état de la table de voisinage des stations. Dans ce cas, c'est le rôle de la couche MAC de fournir aux paquets un accès correct au médium qu'ils proviennent du protocole de découverte de voisinage ou des flux UDP. Les résultats de performances du protocole de découverte de voisinage sont différents suivant la couche MAC utilisée. Dans toutes les simulations effectuées et présentées dans ce chapitre, l'utilisation de MadMac permet d'avoir de meilleures performances.

Ce chapitre montre bien l'utilité d'avoir une couche MAC adaptée aux les réseaux *ad hoc*. Cependant, il nous semble prématuré de dire qu'une couche MAC efficace et équitable, quelle qu'elle soit, soit la solution universelle pour les réseaux *ad hoc*. Tout d'abord, cette étude est préliminaire. Néanmoins, les premiers résultats m'ont paru suffisamment intéressants pour faire l'objet d'un chapitre dans cette thèse. Il faudra regarder l'influence d'une couche MAC sur d'autres protocoles de couches supérieures. De plus, bien que l'équité et l'efficacité soient des problèmes importants, les nouvelles applications pour les réseaux *ad hoc*, comme les réseaux de capteur, ont d'autres objectifs au niveau MAC, comme par exemple gf l'économie d'énergie.

PAS : une solution équitable dans le temps

6

« La créativité, ça ne s'ouvre pas comme un robinet, il faut l'humeur adéquate »

Bill Watterson,
Extrait de la bande dessinée Calvin et Hobbes.

Nous avons vu dans le chapitre précédent que MadMac est un protocole efficace et équitable pour les réseaux ad hoc. Ce protocole fournit un accès efficace au médium radio. Nous entendons par efficace qu'il est rare, avec MadMac, qu'une station se trouve en situation de famine. De plus, le protocole possède aussi un bon système d'exclusion mutuelle pour l'accès à la ressource partagée.

Néanmoins, dans le chapitre précédent, nous avons omis un autre problème d'équité : celui du temps d'accès à la ressource. Ce problème vient du fait que la méthode d'accès au médium de 802.11 fournit à chaque station le même nombre d'accès à la ressource partagée sur un intervalle de temps, alors que les temps d'occupation de la ressource peuvent être différents suivant les stations. Dans les réseaux sans fil, ce problème est connu sous le nom "d'anomalie de performance" (Performance Anomaly).

Dans ce chapitre, nous proposons une solution dynamique et distribuée à cette anomalie de performance. Notre protocole appelé PAS (Performance Anomaly Solution) utilise les informations obtenues par l'écoute active du médium pour agréger l'envoi de paquets et ainsi permettre à chaque station d'obtenir un même temps d'accès à la ressource partagée. Notons que dans ce chapitre, nous utilisons 802.11 comme base de PAS. 802.11 nous fournit de manière statistique un nombre équitable d'accès entre toutes les stations. Cependant, rien ne nous empêche d'utiliser un autre protocole tel que MadMac qui fournit un accès équitable à chaque station.

Sommaire

6.1 Introduction . . . 88
6.2 L'anomalie de performance . . . 89
6.3 État de l'art . . . 89
6.3.1 La fragmentation de paquet . . . 90
6.3.2 Approche basée sur l'adaptation de la fenêtre de contention . . . 91
6.3.3 Approche basée sur l'agrégation des paquets . . . 91
6.4 PAS : *Performance Anomaly Solution* . . . 92
6.4.1 Calcul du temps d'agrégation . . . 92
6.4.2 L'émission de paquets . . . 93
6.4.3 Autres mécanismes . . . 94
6.5 Analyse de performance . . . 95
6.5.1 Efficacité . . . 95
6.5.2 Équité . . . 96
6.5.3 Résultats analytiques . . . 97
6.6 Résultats de simulations . . . 98
6.6.1 Simulations basiques . . . 98
6.6.2 Réactivité . . . 100
6.6.3 Délais . . . 100
6.6.4 Effet de α . . . 103
6.6.5 Effet de t_rate . . . 104
6.6.6 Comparaison avec d'autres solutions . . . 104
6.7 Simulations spécifiques au couple 802.11/PAS . . . 107
6.7.1 Les stations cachées . . . 107
6.7.2 Flux TCP asymétriques . . . 108
6.7.3 Contexte hétérogène . . . 109
6.7.4 Un premier scénario *ad hoc* . . . 109
6.8 Conclusion . . . 111

6.1 Introduction

L'équité dans un réseau sans fil ne se résume pas à un nombre identique d'accès pour chaque station. L'anomalie de performance décrite dans [34] montre les limites de ce type de protocole pour les réseaux sans fil et plus particulièrement de 802.11b. Cette anomalie de performance est due à la possibilité pour les stations d'utiliser des débits différents pour la transmission de leurs paquets. Considérons par exemple deux stations, l'une transmettant à un débit élevé physique (station rapide) et l'autre transmettant à un débit physique plus faible (station lente). La transmission d'un paquet de la station lente prendra plus de temps et occupera ainsi le médium radio plus longtemps que la transmission de la station rapide pour une même taille de paquet. Ce mauvais partage du temps provoque une perte de performance pour le réseau en terme de débit.

Plusieurs solutions ont été proposées dans la littérature pour résoudre ce problème. La plupart d'entre elles utilise une répartition statique et prédéfinie du temps d'occupation du médium par les stations lentes et rapides en introduisant une contrainte sur la taille maximale des paquets (*Maximum Transmission Unit* - MTU) en fonction du débit de transmission utilisé. Une autre approche

consiste, comme dans la norme IEEE 802.11e, à introduire un temps fixe, le TXOP (*Transmit Opportunity*), fixant le temps maximum durant lequel une station peut occuper le canal radio. D'autres approches essaient d'adapter la taille de la fenêtre de contention utilisée par IEEE 802.11 dans son algorithme de *backoff* en fonction du débit de transmission de la station.

Les solutions existantes sont principalement statiques et/ou centralisées. Ici nous abordons ces deux limitations et nous proposons une solution dynamique et distribuée au problème de l'anomalie de performance. Notre solution utilise un intervalle de temps semblable au TXOP mais qui dépend du temps d'occupation du canal perçu par chaque station. Cette occupation peut évoluer en fonction des débits ou de la taille des paquets de chaque station, ce qui rend notre approche dynamique. Pour ce faire, chaque nœud (ou station sans fil) calcule le temps d'occupation maximal du canal grâce au mécanisme d'écoute active de la porteuse fourni par la norme IEEE 802.11. Étant donné que ce mécanisme est local à chaque station, il permet d'avoir une approche distribuée. Une fois qu'un nœud accède au canal radio, il peut envoyer autant de paquets que la durée de ce temps d'occupation maximal lui permet. Nous montrerons qu'avec une telle approche, le problème de l'anomalie de performance est résolue permettant, d'augmenter le débit global du réseau.

6.2 L'anomalie de performance

Dans cette section, nous décrivons plus en détails l'anomalie de performance de 802.11. Une étude plus complète peut être trouvée dans [34].

Le standard IEEE 802.11b [41] fournit un accès distribué au médium radio appelé DCF. De plus, pour accroître la fiabilité des transmissions, 802.11b fournit plusieurs types de modulation. L'utilisation de ces modulations permet d'augmenter ou de réduire (suivant les points de vue) le débit de transmission au niveau physique et ainsi de rendre les transmissions plus fiables. La présence de ces différentes modulations autorise la cohabitation sur un réseau sans fil de stations lentes et de stations rapides.

Heusse *et al.* ont montré dans [34] que la présence de stations lentes dans un réseau 802.11 diminue le débit de toutes les autres stations. Durant la transmission d'une station lente, le médium est occupé pour une période plus longue que pendant la transmission d'une station rapide en supposant que les paquets transmis ont la même taille. Nous savons que 802.11 fournit un accès équitable (d'un point de vue statistique) à chaque station dans une cellule de communication [4]. Ceci signifie qu'à long terme, chaque station aura statistiquement envoyé le même nombre de paquets. Cependant sur une base temporelle, les stations lentes auront occupé le médium plus longtemps.

Ce problème d'équité dans le temps d'accès surgit chaque fois que plusieurs débits différents sont utilisés dans un réseau 802.11. La figure 6.1 montre l'effet de l'anomalie de performance sur une cellule avec deux stations. Dans cette simulation, les deux stations commencent toutes les deux avec un débit de 11Mbps, et toutes les 50s, la station lente diminue son débit à $5,5$, 2 puis 1 Mbps. Les résultats montrent que la station lente, en réduisant son débit, réduit aussi celui de la station rapide et donc le débit global du réseau.

6.3 État de l'art

L'anomalie de performance de IEEE 802.11 a été abordée de plusieurs manières différentes, avec des solutions placées à différents niveaux de la pile protocolaire OSI. Ici, nous décrivons essentiellement les approches les plus importantes décrites dans la littérature qui tentent de résoudre l'anomalie de performance avec des modifications de la norme IEEE 802.11, car notre proposition

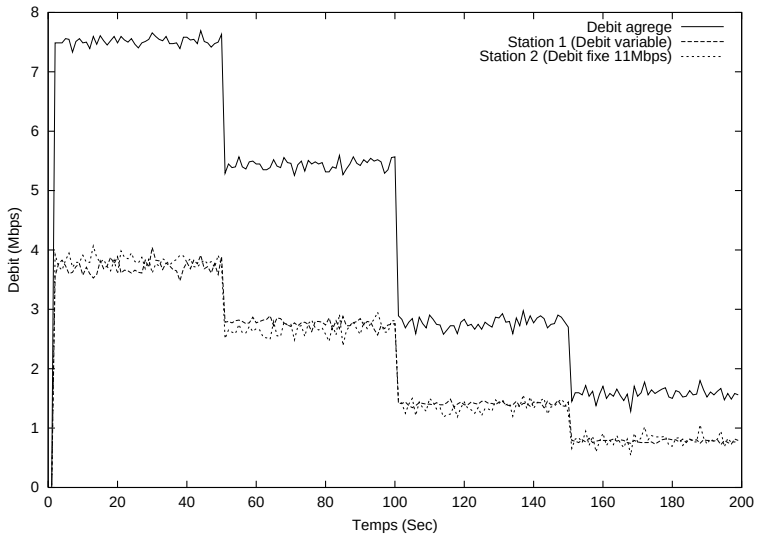


FIG. 6.1: Effets de l'anomalie de performance dans 802.11b. Résultats des débits obtenus par une station rapide et une station lente sur une cellule à deux stations. La station lente diminue son débit toutes les 50s.

se place dans cette catégorie de solution.

Dans ce contexte, il y a trois grandes familles d'approche : *(i)* la fragmentation de paquets, *(ii)* la modification de la fenêtre de contention et *(iii)* l'agrégation de paquet. Dans les sous-sections suivantes, nous décrivons brièvement chacune de ces approches et commentons quelques approches proposées dans la littérature.

6.3.1 La fragmentation de paquet

L'approche basée sur la fragmentation des paquets transmis est la plus simple. Dans [39], les auteurs proposent une solution utilisant un schéma virtuel de division du temps qui réduit l'anomalie de performance de IEEE 802.11. Dans cette solution, les paquets des couches hautes sont divisés en fragments selon le débit de transmission auquel ils sont envoyés au niveau de la couche MAC 802.11. La taille de chaque fragment de paquets est fixe. Les résultats des simulations présentés dans ce travail montrent que cette solution réduit l'anomalie de performance et augmente le débit utile global du réseau. Néanmoins, la nature statique de la solution proposée est efficace, seulement pour des stations transmettant avec des débits élevés et une taille de paquets égale au MTU (*Maximum Transmission Unit*). Le débit global du réseau diminue quand seules des stations lentes sont présentes dans le réseau, en raison de la surcharge protocolaire due au nombre élevé de fragments. La solution proposée dans [21] est également basée sur la réduction de la taille des paquets mais cette réduction est réalisée sur une couche plus élevée du modèle OSI. La procédure de découverte de la MTU est modifiée et employée pour déterminer la taille des paquets selon le débit de transmission. Le même problème que dans [39] peut apparaître si seules des stations lentes sont présentes dans le réseau.

6.3.2 Approche basée sur l'adaptation de la fenêtre de contention

La deuxième approche utilise une modification du mécanisme de backoff de 802.11 en modifiant la taille de la fenêtre de contention. Dans [35], les auteurs proposent un algorithme en deux étapes : la première consiste à atteindre une taille optimale de la fenêtre de contention CW_{opt}, puis une fois cette fenêtre obtenue, celle-ci est modifiée en fonction du débit d'émission de chaque station et du débit maximum disponible sur le réseau. La solution proposée réduit l'anomalie de performance tout en améliorant le débit utile. Les auteurs posent comme limitation de leur protocole le calcul de la fenêtre de contention optimale qui est faîte de manière statique et *a priori*. L'approche par la modification de la fenêtre de contention contrairement à la fragmentation de paquets et à l'agrégation (voir sous-section suivante) modifie le nombre moyen d'accès de chaque station. Cette solution peut ainsi être pénalisante du point de vue du débit global s'il n'y a que des stations lentes sur le réseau.

6.3.3 Approche basée sur l'agrégation des paquets

La troisième catégorie est l'approche utilisant l'agrégation des paquets, dans laquelle notre solution est également incluse. Ce type de solutions a été présenté la première fois par [68]. Les auteurs de cet article proposent une méthode opportuniste d'accès au canal pour les réseaux *ad hoc* multi-débits. La solution est basée sur le fait qu'une station transmettant à un débit élevé a probablement un bon état du canal et peut donc envoyer plus d'un paquet pour profiter de ces conditions favorables. Le nombre de paquets successifs à transmettre est calculé selon le débit de transmission le plus bas du réseau. Par exemple, si le débit de base est de 2 Mbps et l'état du canal permet une transmission à 11 Mbps, un temps d'accès au canal permettant d'envoyer $\lceil 11/2 \rceil = 5$ paquets est utilisé par l'émetteur. Avec cette solution, l'anomalie de performance peut être résolue. Cependant s'il y a seulement des stations rapides sur le réseau, l'accès au canal devient inéquitable à court terme dû à une agrégation inutile des stations. L'approche basée sur l'agrégation des paquets est aussi proposée dans la norme IEEE 802.11e [44]. Dans cette norme, une occasion de transmission (TXOP - T*ransmission Opportunity*), *i.e.* un temps maximal d'occupation du canal, est accordée à chaque station. Ce temps est annoncé à chaque nœud par la station de base. Le calcul du TXOP n'est pas vraiment limpide dans la norme, mais durant ce temps les stations rapides peuvent agréger leur envoi de paquets, alors que les stations lentes ne peuvent envoyer qu'un seul paquet. À notre connaissance, le TXOP est calculé selon le temps nécessaire pour envoyer un paquet de taille maximale (MTU) au débit de transmission le plus bas. Le principal problème de cette solution est qu'elle est centralisée et qu'elle ne peut pas être appliquée aux réseaux sans infrastructure. En conclusion, les approches utilisant une agrégation des paquets le font sur un temps calculé statiquement et *a priori*. L'anomalie de performance est résolue, mais un problème d'équité à court terme se présente.

Pour résoudre l'anomalie de performance et en même temps le problème d'équité à court terme, nous proposons une politique dynamique d'agrégation des paquets. Notre solution est différente des autres solutions car elle n'est pas centralisée, mais totalement distribuée. Le temps d'agrégation est calculé dynamiquement grâce à l'information obtenue sur l'occupation du canal radio. Notre protocole n'a besoin d'aucune information particulière hormis celle fournie et nécessaire à la norme IEEE 802.11.

La solution que nous proposons décorrèle l'accès au médium du temps d'accès. Ainsi notre solution peut être utilisée avec une autre méthode d'accès équitable en nombre d'accès. Par exemple, PAS peut être implémenté au-dessus de 802.11 (c'est cette option que nous présentons dans la suite de ce chapitre) mais elle pourrait aussi être implémentée au-dessus de MadMac, de Idle Sense [35], de AOB [8] ou de n'importe quel autre protocole fournissant un accès équitable.

Algorithm 4 *Performance Anomaly Solution* - Ecoute du canal

```
1: t_p_max := 0 ;
2: repeat
3:   if (un signal est percu au niveau physique) then
4:     t_p_current := signal's channel occupancy time ;
5:     if (t_p_current > t_p_max) then
6:       t_p_max := t_p_current ;
7:     end if
8:     if (type paquet == ACK) and (Destination == moi)  then
9:       t_p_max := 0 ;
10:    end if
11:  end if
12: until 1 ;
```

6.4 PAS : *Performance Anomaly Solution*

L'idée de notre protocole, appelé PAS (*Performance Anomaly Solution*), s'appuie sur le fait que chaque station doit disposer du même temps de transmission sur le canal. Par conséquent, si une station émettrice perçoit un temps d'occupation du canal qui est plus important que le temps de transmission du paquet qu'elle va émettre, alors elle peut agréger ses paquets pour obtenir un plus grand temps d'occupation. L'agrégation est faite en laissant un temps SIFS entre la réception de l'acquittement du paquet précédent et l'envoi du prochain paquet. PAS comporte deux parties principales : *(i)* L'écoute du médium permettant de calculer le temps disponible pour l'agrégation et *(ii)* La transmission des paquets.

6.4.1 Calcul du temps d'agrégation

L'algorithme 4 présente la procédure de calcul du temps d'occupation maximum du médium. La station écoute en permanence le canal radio et conserve dans une variable le temps d'occupation du canal radio, définie comme étant une durée ininterrompue d'occupation du canal radio. Ce temps d'occupation est le temps durant lequel le canal est occupé soit par une transmission, soit par une transmission ne pouvant être décodée (incluant la superposition de plusieurs signaux). Le temps d'occupation maximum est conservé par chaque station dans une variable appelée t_p_max. Ce temps constitue le temps de référence pour la station émettrice. Cette variable est réinitialisée à 0 après chaque transmission correcte de la station. Remettre cette variable à 0 évite le monopole du médium par une station et rend le protocole plus réactif. Elle permet aussi de réduire l'iniquité à court terme qui pourrait être introduite quand une station accède au médium plusieurs fois de suite. Elle empêche ainsi l'envoi de plusieures séries de paquets agrégés.

Il faut noter que le temps calculé dans cet algorithme ne correspond pas à la durée d'une transmission comprenant les échanges DATA-ACK ou RTS-CTS-DATA-ACK. En effet, ce temps est calculé par rapport a un signal continu, perçu sur le canal radio. Cependant, il est difficile de déterminer ces échanges car notre calcul n'utilise pas les informations contenues dans les paquets, d'abord pour des raisons de sécurité mais aussi parce que tous les paquets ne peuvent pas être décodés. Il n'est donc pas toujours possible de distinguer un paquet de données d'un paquet de contrôle si ceux-ci ont la même durée de transmission.

6.4.2 L'émission de paquets

L'algorithme 5 présente la procédure d'émission de PAS. La station peut soit émettre son paquet normalement en utilisant le mode d'accès au médium de 802.11 soit agréger certains paquets. Pour savoir, si elle peut agréger, elle se base sur la variable t_p_max : si son temps d'occupation du canal pour le paquet à transmettre est plus petit que la valeur de cette variable alors elle peut agréger. t_my_packet est le temps nécessaire à la transmission du paquet en cours et t_my_left correspond au temps de transmission qui est autorisé. La valeur de cette dernière variable évolue au cours du temps en fonction des paquets précédemment émis. Lorsque cette valeur devient trop petite, il n'est alors plus possible de continuer l'envoi agrégé car alors le temps d'occupation du médium de la station deviendrait plus important que le temps d'occupation maximum perçu sur le canal.

La variable booléenne *sending* indique si le paquet à envoyer est le premier paquet à envoyer (*sending* à $false$). Dans ce cas, le paquet doit suivre le processus classique d'accès au médium de 802.11 ou s'il fait partie d'une suite de paquets agrégés (*sending* à *true*) et dans ce cas, deux paquets consécutifs sont seulement séparés d'un SIFS.

Algorithm 5 Performance Anomaly Solution - Emission

```
1:  sending := false ;
2:  t_my_left := 0 ;
3:  for (Chaque paquet a envoyer) do
4:    if (t_my_left ≤ 0) then
5:      t_my_left := t_p_max ;
6:    end if
7:    α = (⌈t_my_left / t_my_packet⌉ − t_my_left / t_my_packet) ∗ t_my_packet ;
8:    t_my_left := t_my_left − t_my_packet ;
9:    if (sending == true) then
10:     if (t_my_left + α > 0) then
11:       aggregated_sending() ;
12:     else
13:       t_my_left := 0 ;
14:       sending := false ;
15:       classical_sending() ;
16:     end if
17:   else
18:     if (t_my_left + α > 0) then
19:       sending := true ;
20:       classical_sending() ;
21:     else
22:       t_my_left := 0 ;
23:       classical_sending() ;
24:     end if
25:   end if
26: end for
```

La variable α est utilisée pour maintenir un bon débit agrégé. En effet, considérons un scénario avec deux émetteurs, une station lente à 5.5Mbps et une station rapide à 11Mbps ayant des paquets de même taille. Dû à la taille fixe de l'entête créé au niveau de la couche physique, la durée de

transmission de deux paquets par la station rapide prend plus de temps que la transmission d'un paquet pour la station lente. Par conséquent, sans l'utilisation de α la station rapide n'agrègera pas de paquets et l'anomalie de performance restera. En calculant α de la manière suivante :

$$\alpha = (\lceil \frac{t_my_left}{t_my_packet} \rceil - \frac{t_my_left}{t_my_packet}) \times t_my_packet$$

l'agrégation est favorisée. En effet, il n'y a aucune raison pour que le rapport entre t_p_max et t_my_packet soit un entier. Pour maintenir un bon débit agrégé, nous permettons parfois, grâce à α, que le temps de transmission d'une station soit légèrement supérieur au temps d'occupation maximum perçu. Une nouvelle valeur de α est calculée à chaque arrivée de paquet au niveau MAC. Ceci permet d'avoir une approche réellement dynamique adaptée à l'environnement en cours. En outre, une telle approche ne nécessite aucune hypothèse sur la taille des paquets.

Si un paquet subit une collision, la retransmission est faite de manière agrégée après un SIFS si t_my_left est assez grand pour permettre la retransmission. Si t_my_left est trop petit, le paquet est réémis normalement avec une fenêtre de contention évoluant suivant l'algorithme du backoff exponentiel (de 802.11). Dans ce cas, la valeur de *sending* est remise à $false$ et la valeur de t_my_left à 0. Pour des raisons de lisibilité, ce processus n'est pas présenté dans l'algorithme 5.

6.4.3 Autres mécanismes

Pénalisation des petits paquets

Notons que le temps de transmission de chaque paquet inclut les entêtes et réduit donc le débit utile. Si une station rapide agrège des petits paquets, une grande partie de la bande passante est perdue pour la transmission. La transmission de petits paquets par une station rapide peut donc réduire le débit global.

Pour éviter ce type de problème et ainsi améliorer le débit global, il est possible de pénaliser les stations transmettant des petits paquets. Une manière simple de le faire est de calculer le rapport entre les données utiles et les entêtes de chaque paquet. Dans la suite de ce travail, nous appellerons ce rapport t_rate et nous utiliserons ce paramètre pour limiter l'agrégation. Pour ce faire, nous conditionnons le calcul de t_my_left par la valeur de t_rate. L'instruction 8 de l'algorithme 5 est remplacée par les instructions de l'algorithme 6.

Algorithm 6 Performance Anomaly Solution - t_rate

```
if (t_rate < 1) then
  t_my_left := t_my_left − ((1/t_rate) ∗ t_my_packet);
else
  t_my_left := t_my_left − t_my_packet;
end if
```

À chaque étape, le temps restant pour l'agrégation est réduit pour les stations transmettant des petits paquets. Le calcul précédent est effectué pour chaque paquet et permet de moduler dynamiquement le temps restant pour l'agrégation en fonction des paquets transmis ou à transmettre.

Utilisation des RTS/CTS

Notre premier choix d'utiliser 802.11 comme méthode d'accès équitable nous a poussé à fournir un mécanisme permettant l'exploitation des informations contenues dans les RTS/CTS pour PAS.

PAS utilise les durées présentes dans les paquets RTS et CTS pour mettre à jour la valeur du temps maximum d'occupation. C'est la seule modification à apporter à PAS dans la phase d'écoute du médium.

Pour la transmission d'un paquet, quand $t_p_max \geq t_my_left$ et que $packet_{length} \geq RTS_{threshold}$ alors la transmission se fait avec l'échange suivant : RTS-CTS-DATA-ACK-SIFS-DATA-ACK-SIFS... et ainsi de suite. Pour une série de paquets agrégés, seul le premier paquet nécessite l'envoi d'un RTS. Les autres paquets de la série sont transmis comme dans l'algorithme 5.

La durée contenue dans les paquets RTS et CTS est la durée de transmission du premier paquet et non la valeur t_p_max de la station. Il y a pour cela deux raisons :

- Comme le nombre de paquets à agréger n'est pas connu à l'avance, il est impossible de donner *a priori* la durée de l'échange pour le paquet RTS. Prendre la valeur t_p_max peut empêcher des émetteurs potentiels d'émettre alors que la station devant agréger ses paquets ne dispose plus de paquets dans sa file d'attente.
- On peut ainsi accroître la réactivité. Par exemple, supposons que nous avons deux stations rapides et une station lente : les deux stations rapides agrègent leurs paquets sur la base de l'occupation de la station lente. Si la station lente cesse de transmettre des paquets et que t_p_max a été annoncé dans un RTS ou un CTS, les deux stations rapides vont maintenir leur agrégation sur la base d'une information obsolète. Maintenir cette agrégation provoque ainsi un problème d'équité à court terme alors qu'il ne devrait pas y en avoir.

Avec l'utilisation des RTS/CTS, les collisions sont résolues de la manière suivante : si la collision se produit sur le RTS alors celui-ci est retransmis en utilisant 802.11. Si la collision se produit sur le paquet de données, celui-ci est retransmis après un SIFS si t_my_left est assez grand pour permettre la retransmission. Dans le cas contraire, le processus normal d'envoi est utilisé.

6.5 Analyse de performance

Dans cette section, nous cherchons à évaluer l'efficacité et l'équité de PAS. Tan *et al.* [69] ont proposé une notion d'équité temporelle qui cherche a fournir à chaque station approximativement un temps égal d'occupation sur le canal radio. Ils ont montré que fournir une équité temporelle est efficace comparée à une équité en nombre d'accès. La solution qu'ils proposent prend en compte le temps nécessaire pour l'échange DATA-ACK pour le calcul du temps de transmission. Cette solution n'a pas été présentée dans la section précédente car elle se fait sur les couches supérieures du modèle OSI. Dans PAS, le calcul du temps de transmission ne s'appuie par sur un échange DATA-ACK mais seulement sur l'occupation du médium. Dans la section suivante, nous montrons simplement comment le mécanisme de PAS est plus efficace que le mécanisme proposé par Tan *et al.*.

6.5.1 Efficacité

Le temps de transmission dans notre protocole s'appuie sur le temps de transmission d'un paquet et non sur le temps nécessaire à l'échange. Le temps d'échange est défini par $T_ex = t_my_packet + T_SIFS + T_PHY + T_ACK$ où T_SFIS est la durée d'un SIFS, T_PHY est la durée de transmission de l'entête physique pour l'acquittement, T_ACK est la durée de l'acquittement et t_my_packet, le temps nécessaire à la transmission d'un paquet (la durée de l'entête physique est déjà incluse dans ce temps). Notons t_p_max la durée d'occupation maximum du canal radio ; et $T_ack = T_SIFS + T_PHY + T_ACK$. Notons que la durée de T_ack est indépendante du débit de transmission des stations.

Prenons l'exemple de deux stations : une rapide et une lente à portée de communication l'une de l'autre. Ces deux stations transmettent des paquets de même taille. Le nombre de paquets transmis par la station rapide utilisant PAS est :

$$n_a = \frac{t_p_max}{t_my_packet} \tag{6.1}$$

Alors que le nombre de paquets transmis par la station rapide s'appuyant sur la solution de Tan *et al.* est :

$$n_{et} = \frac{t_p_max + T_ack}{t_my_packet + T_ack} \tag{6.2}$$

Nous avons $t_my_packet \leq t_p_max$. Donc avec cette hypothèse :

$$n_a \geq n_{et} \tag{6.3}$$

Chaque fois que la station lente transmet un paquet, la station rapide agrègera ses transmissions. Le nombre de paquets envoyés par la station rapide utilisant PAS est plus élevé que le nombre de paquets envoyés par une station utilisant la solution de Tan *et al.*. Si nous supposons que le nombre d'accès est le même, pour la station lente et la station rapide alors, plus le nombre de paquets envoyés par la station rapide sera élevé plus le débit global sera élevé.

6.5.2 Équité

Dans cette sous-section, nous analysons l'équité fournie par PAS. Pour des raisons de simplicité, nous supposons, dans cette analyse, que les stations utilisent une même taille de paquet de $L = 1000$ octets. Posons T_i le temps de transmission d'un paquet au débit i avec $i = 1, 2, 5, 5$ ou 11 Mbps. T_i inclue les entêtes des couches transport, IP, MAC et physique. On calcule facilement le temps de transmission d'une station émettant au débit i :

$$Agg_i = n_{a_i} \times (T_i + T_ACK) + (n_{a_i} - 1) \times SIFS \tag{6.4}$$

Agg_i est le temps utilisé pour l'envoi agrégé des paquets d'une station émettant au débit i avec $n_{a_i} = \lceil t_p_max/T_i \rceil$.

D'un point de vue du médium, la proportion de temps utilisé pour l'agrégation de paquets d'une station est :

$$T_Occ_i = \frac{T_Agg_i}{\sum_j (T_Agg_j \times N_j) + N \times DIFS} \tag{6.5}$$

Où N_j est le nombre de stations utilisant le débit j, avec $\sum_j N_j = N$. Nous supposons que la probabilité d'accès au médium est la même pour toutes les stations et que durant un intervalle de temps donné, chaque station a accédé au médium exactement une fois. Le nombre de paquets émis par une station utilisant le débit i dans un intervalle de temps t est :

$$NBp_i = \frac{n_{a_i}}{\sum_j (Agg_j \times N_j) + N \times (DIFS + Avg_{bckf})} \times t \tag{6.6}$$

où Avg_{bckf} correspond au temps de *backoff* moyen de 802.11 (sans collision et vaut ici $310\mu s$). Nous pouvons ainsi calculer le débit moyen en octets par seconde d'une station utilisant le débit i :

$$TH_i = NBp_i \times L \times 8 \tag{6.7}$$

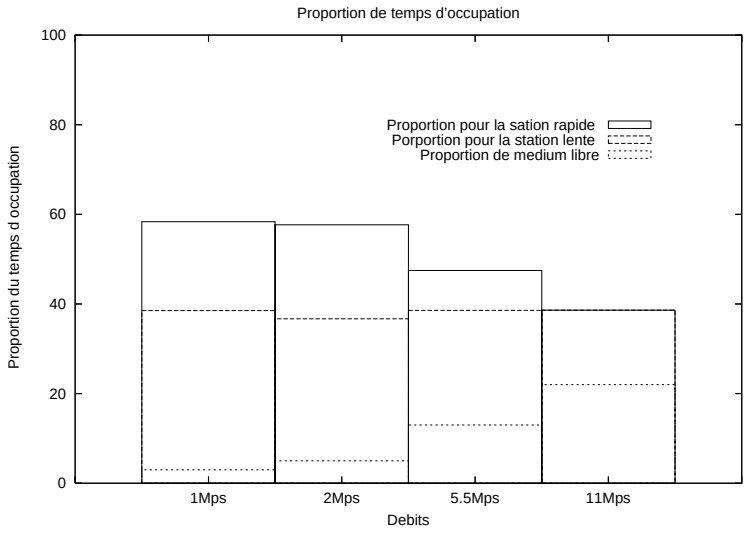


FIG. 6.2: PAS : Résultat analytique pour la proportion du temps d'occupation pour deux stations

Tous les résultats précédents peuvent être étendus à des paquets de tailles différentes, le plus important étant d'avoir la valeur de t_p_max. Dans cette analyse, nous supposons que l'accès au canal radio est ordonnancé comme dans un accès TDMA (où toutes les stations émettent les unes après les autres). De ce fait, pour chaque station, la valeur de t_p_max est toujours la même et chaque transmission est une transmission "agrégée" par rapport à t_p_max. Cette hypothèse pourrait être suffisamment réaliste du fait que l'algorithme de backoff de 802.11 offre en moyenne un accès équitable au canal radio. Néanmoins, nous verrons que les différences obtenues entre les résultats analytiques et les simulations sont dues à cette hypothèse car 802.11 ne se comporte pas comme un accès TDMA à court terme.

6.5.3 Résultats analytiques

La figure 6.2 montre la proportion de temps alloué (temps d'échange) obtenue analytiquement pour deux stations. Dans cette figure, l'une des deux stations transmet toujours à 11 Mbps et l'autre à 1, 2, 5,5 ou 11 Mbps. Sur l'abscisse, i Mbps indique que la deuxième station transmet à i Mbps et que la première transmet à 11 Mbps. La taille des paquets est de 1000 octets. Pour chaque i, la figure donne la proportion du temps d'occupation pour la station rapide (11 Mbps) et pour la station lente (i Mbps) et la proportion de temps où le médium est libre. Nous pouvons voir sur cette figure que la station rapide obtient une plus grande occupation du médium que la station lente. Il faut aussi remarquer que la proportion du temps d'occupation n'est pas de 50% comme il devrait l'être dans une équité temporelle parfaite. Ceci peut s'expliquer par le fait que l'occupation calculée par PAS n'inclut pas le temps d'échange. Nous pouvons aussi remarquer que le débit de la station lente augmente car la proportion de temps libre augmente. Ceci est dû à la proportion de temps consommé en décrémentation de backoff.

La table 6.1 montre les différences de débits obtenus à partir de l'équation 6.7 pour deux stations (une rapide et une lente). Nous avons inclus dans ce tableau l'index d'équité de Jain que nous rappelons sur la formule suivante :

	Débit (kbps)	Nb de paquets (/s)	Index
5.5Mbps	1547.2	193.4	0.98
11Mbps	3095.2	386.9	
2Mbps	624.8	78.1	0.93
11Mbps	3749.6	468.7	
1Mbps	344.8	43.1	0.92
11Mbps	3791.2	473.9	

TAB. 6.1: PAS : résultats analytiques

$$FI = \frac{(\sum_i r_i/r_i^*)^2}{n\sum_i (r_i/r_i^*)^2} \tag{6.8}$$

où r_i^* est le débit recherché pour le flux i, r_i est le débit obtenu et n est le nombre de flux. Nous prenons comme valeur de r_i^* la valeur définie dans Tan *et al.*. Cette valeur est le débit qu'obtiendrait le flux i si tous les flux du réseau utilisaient le même débit que le flux i. Par exemple, si nous avons deux stations transmettant l'une à 11 Mbps (Flux 1) et l'autre à 1 Mbps (Flux 2), r_1^* serait le débit de flux 1 si le flux 2 était transmis à 11 Mbps. De même pour le r_2^*. La valeur de r_i^* est la valeur obtenue si les temps d'occupation étaient les même. C'est pour cette raison que les index ne sont pas égaux à 1 dans le tableau 6.1.

6.6 Résultats de simulations

Pour évaluer PAS, nous l'avons implémenté dans le simulateur NS-2 [60]. De plus, nous avons aussi ajouté à NS-2 la possibilité de composer avec différents débits pour refléter les modulations présentes dans le standard 802.11b. Tous les résultats présentés dans cette section sont tirés de plus de 30 simulations de $100s$ et avec des intervalles de confiance à 0.95. Les protocoles tels que ARP et les protocoles de routage ont été enlevés pour réduire tous les échanges de messages qui ne seraient pas liés à l'application. Dans toutes les simulations, un flux UDP à saturation est utilisé si le contraire n'est pas spécifié. Nous avons aussi choisi d'effectuer la plupart des simulations avec des paquets de 1000 octets. Cependant, nous avons aussi effectué des simulations avec des tailles de paquet tiré aléatoirement et suivant une distribution uniforme. Les index d'équité sont aussi donnés.

6.6.1 Simulations basiques

Cette section contient les premières simulations effectuées pour évaluer les performances de Mad-Mac. Ces simulations comprennent deux stations, une lente et une rapide. La figure 6.3 montre les résultats de simulation pour ce scénario. L'axe des abscisses donne le protocole utilisé, le débit de chaque station dans le scénario et l'index d'équité obtenu. La partie hachurée est le débit obtenu pour la station rapide et la partie en blanc donne le débit obtenu pour la station lente. La somme fournit le débit agrégé.

Cette figure montre que quand les débits de la station rapide et de la station lente sont différents, le débit agrégé de PAS est toujours meilleur que celui de 802.11. On peut aussi observer sur cette figure qu'avec l'utilisation de PAS, le débit de la station rapide reste élevé et plus ou moins équivalent, indépendamment du débit de la station lente. Ceci est dû au fait que le temps d'accès au médium est

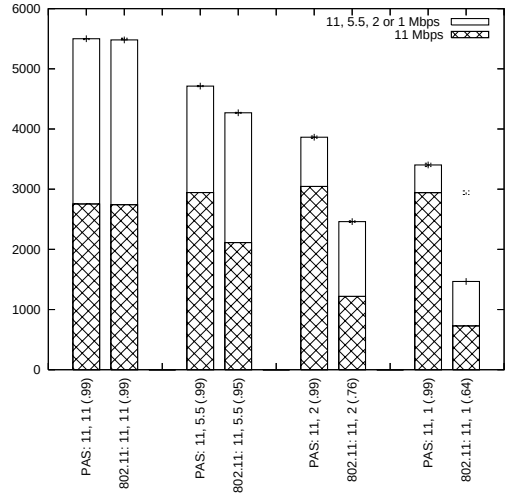


FIG. 6.3: PAS vs. IEEE 802.11 in : Simulations avec deux stations. Cette figure montre les débits globaux, les débits individuels de chaque station et les index d'équité (entre parenthèses sur l'axe des abscisses) obtenus sur le réseau. La légende sur l'axe des x indique : le protocole utilisé, le debit utilisé par chacune des stations et l'index d'équité obtenu.

partagé presque équitablement entre les stations. L'index d'équité donné entre parenthèses montre aussi que PAS est plus équitable que 802.11.

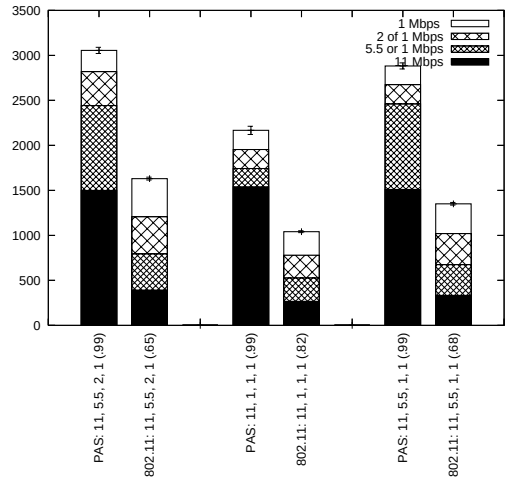


FIG. 6.4: PAS vs. IEEE 802.11 in : Simulations avec quatre stations. Cette figure montre les débits globaux, les débits individuels de chaque station et les index d'équité (entre parenthèses sur l'axe des abscisses) obtenus sur le réseau. La légende sur l'axe des x indique : le protocole utilisé, le débit utilisé par chacune des stations et l'index d'équité obtenu.

La figure 6.4 montre les résultats de simulations avec 4 stations. On voit clairement que le débit agrégé obtenu avec PAS est plus élevé que le débit obtenu avec 802.11. En plus, comme pour la

figure précédente, on voit que le débit de la station rapide reste toujours à peu près le même. L'index d'équité montre lui aussi que PAS est plus performant que 802.11.

La différence entre les résultats analytiques obtenus dans le tableau 6.1 et les résultats obtenus ci-dessus peut être expliquée par le comportement de l'algorithme de backoff de 802.11. En effet, 802.11 ne fournit pas un accès TDMA mais un accès aléatoire au médium. Cet aspect aléatoire peut autoriser deux accès successifs à une même station rapide ou lente. Dans les deux cas, ces accès successifs réduisent le débit global car la station lente occupe le médium longtemps pour l'envoi d'une quantité de données limitées et l'accès successif d'une station rapide ne l'autorise pas à agréger ces paquets pour le deuxième accès (réinitialisation de t_p_max). Ainsi, la différence entre les débits obtenus par simulations et analytiquement est plus prononcée quand la différence des débits entre les stations lentes et rapides augmente.

La figure 6.5 donne les résultats de simulation avec différents nombres de stations. Dans ces simulations, la moitié des stations sont des stations rapides et l'autre moitié sont des stations lentes. Les débits des stations lentes sont 11, 5,5, 2 et 1 Mbps. La taille des paquets par station est tirée uniformément et aléatoirement pour chaque paquet entre $[550; 1450]$ octets. La figure montre le débit agrégé sur ces scénarii avec un nombre croissant de stations. Nous voyons que PAS est plus performant que 802.11. La différence de performance est plus grande quand les débits des stations lentes sont plus faibles. Nous pouvons aussi remarquer que même si toutes les stations transmettent à 11 Mbps, PAS est plus performant que 802.11. Ceci est dû au fait que le tirage aléatoire de la taille des paquets peut parfois autoriser des stations à agréger des paquets. Si les intervalles de confiance de PAS sont plus larges que ceux de 802.11, c'est dû à l'agrégation des paquets qui permet au débit global de fluctuer plus que pour 802.11.

6.6.2 Réactivité

Un moyen simple de tester la réactivité de PAS est d'introduire le mécanisme d'*Auto Rate fallback* (ARF) utilisé par les stations sans fil pour adapter leur débit en fonction des conditions du canal radio. Nous avons implémenté le protocole ARF et réalisé une simulation pour voir le comportement de PAS quand le débit d'une station varie dans le temps. La simulation se présente sous la forme de deux stations transmettant des paquets de même taille à une station de base. Au début de la simulation, les deux stations sont proches de la station de base et transmettent toutes les deux avec un débit de 11 Mbps. Ensuite, l'une des deux stations s'éloigne de la station de base tandis que l'autre reste proche de celle-ci. L'éloignement de la station provoque une dégradation de son canal radio et cette station, doit ainsi diminuer son débit de transmission au fur et à mesure qu'elle s'éloigne. La station s'éloignant du point d'accès suit une trajectoire rectiligne avec une vitesse constante. Aucun modèle de mobilité n'est utilisé et le modèle de mobilité utilisé ne devrait pas avoir d'impact sur les résultats de réactivité car nous nous considérons dans une cellule de communication où toutes les stations sont à portée de communication.

La figure 6.6 montre les résultats de la simulation avec PAS et 802.11. Nous pouvons voir sur cette figure que pour la station rapide utilisant PAS, le débit utile reste constant, alors que le débit de la station lente diminue. Dans le cas de 802.11. le débit utile des deux stations diminue.

6.6.3 Délais

Dans cette section, nous présentons une simulation de 20 secondes avec deux émetteurs : l'un à 11 Mbps et l'autre à 1 Mbps. Durant la simulation, nous avons calculé le temps entre deux agrégations. Ce temps est défini comme le temps séparant l'envoi de deux rafales de paquets agrégés. Pour la

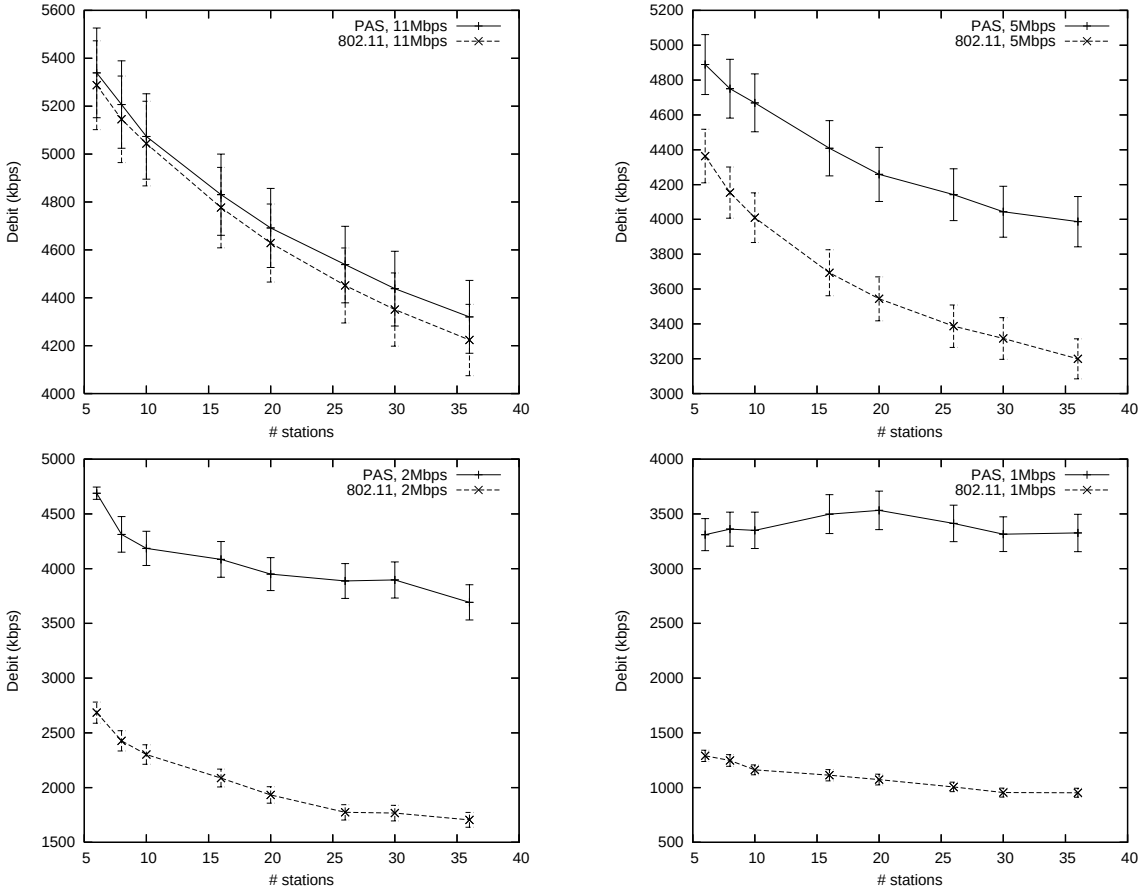


FIG. 6.5: PAS vs. IEEE 802.11 : Simulations avec différentes densités de cellule. Dans toutes les simulations, toutes les stations sont à portée de communication. La tailles des paquets de chaque station est tirée aléatoirement et uniformément. La première figure (en haut à gauche) montre les résultats de simulations où toutes les stations transmettent à 11 Mbps. La deuxième figure (en haut à droite) montre les résultats où la moitié des stations transmettent à 11 Mbps et l'autre moitié à 5.5 Mbps. La troisième figure (en bas à gauche) montre les même résultats avec une moitié des stations à 11 Mbps et l'autre à 2 Mbps. La dernière figure (en bas à droite) montre les résultats de simulations avec une moitié de stations à 11 Mbps et l'autre moitié à 1 Mbps

station lente, une rafale est toujours constituée d'un seul paquet. Pour la station rapide cette rafale peut être constituée de plusieurs paquets ou d'un seul si la station rapide accède plusieurs fois successivement au médium radio.

Le tableau 6.2 donne le nombre de rafales envoyées par la station lente et la station rapide ainsi que le temps moyen entre chaque rafale. Ces résultats montrent que la méthode d'accès de PAS (ici 802.11) fournit un nombre équitable d'accès aux deux stations. De plus, le temps moyen entre chaque rafale est proche du temps de transmission d'un paquet de la station lente $8576\mu s$.

La figure 6.7 montre la fonction de distribution cumulée pour la station rapide et la station lente des temps inter-rafales. Cette distribution est une courbe par paliers pour la station rapide et la station lente. On peut voir aisément sur ces courbes que l'accès fourni par 802.11 est loin d'être un accès TDMA. Ceci se voit sur le grand pallier proche de 0 pour les deux courbes. Ce premier palier

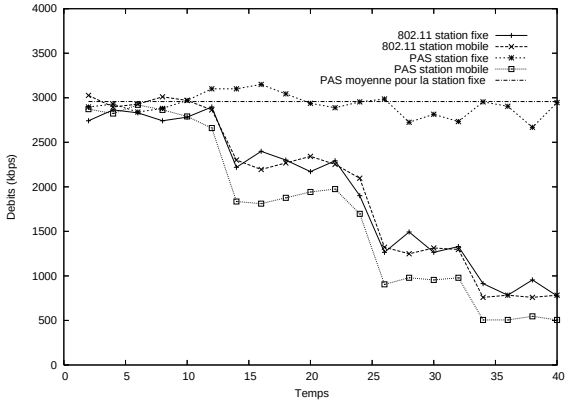


FIG. 6.6: PAS vs. IEEE 802.11 : Utilisation du mécanisme ARF (*Auto Rate Fallback*).

	Nb bursts	Inter-bursts moyen
RAPIDE	5911	9867.70μs
LENT	6004	8776.46μs

TAB. 6.2: PAS : Rafales

signifie qu'il y a un nombre non négligeable de paquets qui sont transmis séparés seulement par le temps d'un *backoff*, donc envoyés successivement. Un tel comportement réduit les performances de PAS. Nous voyons aussi sur cette figure que pour la station rapide, chaque palier équivaut environ au temps de transmission d'un paquet pour la station lente. La présence de plusieurs paliers nous indique que la station lente peut transmettre plusieurs paquets successivement. Ceci confirme les différences entre notre analyse théorique et les simulations. Pour la station lente nous voyons que le temps inter-rafales est proche du temps nécessaire à la station rapide pour envoyer une rafale. Nous pouvons aussi voir que les deux distributions sont différentes car la station rapide, même si elle réussit à accéder plusieurs fois successivement au médium, ne peut pas systématiquement agréger ses paquets. Ainsi, contrairement à la station rapide, la distribution cumulée de de la station lente ne comporte qu'un seul pallier. Ceci explique aussi que le temps moyen inter-rafales de la station lente soit plus court que celui de la station rapide.

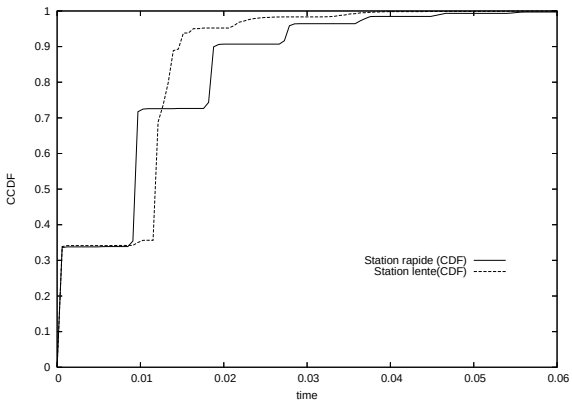


FIG. 6.7: PAS : Fonction de distribution cumulée des temps inter-rafales.

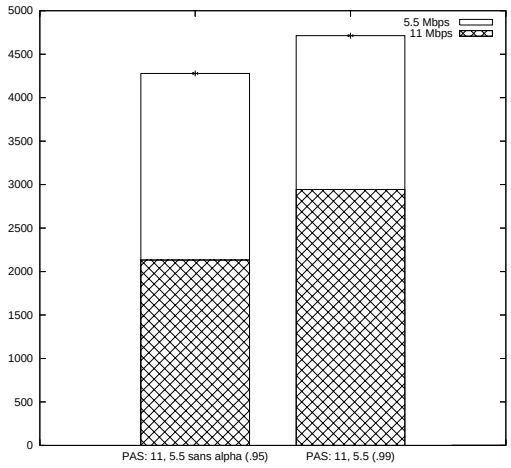


FIG. 6.8: PAS : Influence de α sur deux stations.

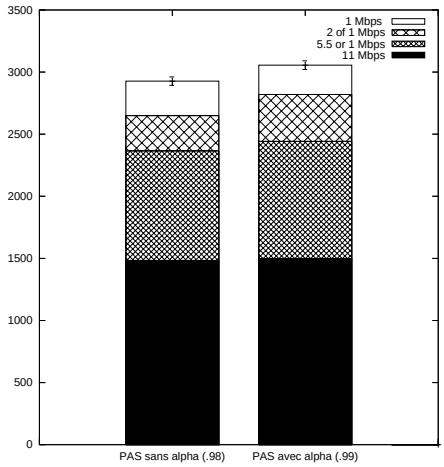


FIG. 6.9: PAS : Influence de α sur quatre stations.

6.6.4 Effet de α

Ici nous montrons l'effet de l'utilisation ou non de α. Nous simulons deux stations sans fil transmettant 1000 octets de données à 11Mbps et à 5,5Mbps. Nous pouvons voir sur la figure 6.8 que dans cette simulation spécifique, quand α n'est pas utilisé, il n'y a aucune agrégation pour la station rapide. En effet, pour le deuxième paquet de la station rapide, la condition $t_my_left - t_my_packet > 0$, n'est jamais vraie. En revanche, l'utilisation de α permet à la station rapide d'augmenter son temps d'agrégation pour arrondir au nombre supérieur le nombre de paquets pouvant être transmis dans une série de paquets agrégés. Son utilisation permet aussi d'obtenir un meilleur débit agrégé global.

La même simulation a été menée avec quatre stations avec des débits de 11, 5,5, 2 et 1 Mbps. La figure 6.9 montre que l'utilisation de α accroît dans ce cas aussi les performances de PAS. De plus, les figures 6.8 et 6.9 montrent que l'utilisation de α augmente l'équité.

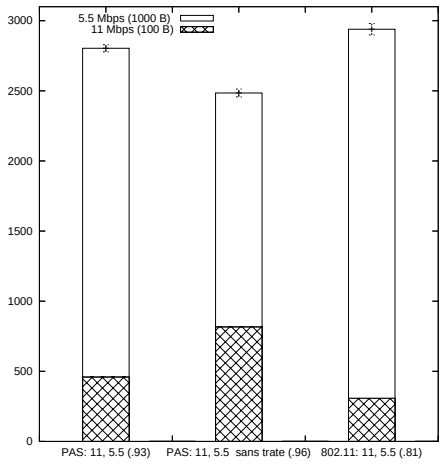


FIG. 6.10: PAS : influence de t_rate sur deux stations.

6.6.5 Effet de t_rate

t_rate est un autre paramètre important de PAS. Ce paramètre permet de moduler le temps restant pour l'agrégation en fonction du rapport entre les données et les entêtes. Pour voir l'effet de t_rate sur PAS, nous avons simulé deux stations : l'une transmettant des paquets de 100 octets à 11 Mbps et l'autre émettant des paquets de 1000 octets à 5.5 Mbps. La figure 6.10 montre que l'utilisation de t_rate améliore les performances globales du réseau mais ces performances restent en-deçà de ceux de 802.11. Cependant, la figure 6.10 montre aussi l'effet néfaste de t_rate sur l'équité, car celui-ci réduit le temps d'agrégation pour la station rapide. Notons en revanche que PAS avec ou sans l'utilisation de t_rate reste plus équitable que 802.11. Dans ce scénario particulier, il existe un compromis entre efficacité et équité.

Il y a plusieurs possibilités pour l'utilisation de t_rate. Il est possible de mettre t_my_left à 0 si $t_rate < 1$. Cette utilisation permettrait d'avoir les même performances que 802.11 dans le scénario décrit ici. Cependant, nous ne pensons pas que cette solution soit la bonne, car elle réduirait les performances dans le cas où les stations ont des petits et des grands paquets à envoyer.

Nous pensons que PAS permet d'obtenir un bon compromis. Pour montrer ce compromis, des simulations ont été menées avec différentes tailles de paquets pour la station rapide. Comme les figures 6.11 et 6.12 le montrent, avec l'utilisation de t_rate, PAS n'est pas aussi efficace que 802.11 pour des petits paquets. Cependant, les débits sont assez proches. En revanche, pour des tailles de paquets plus grandes, PAS (avec ou sans t_rate) est plus efficace que 802.11. On voit aussi sur la figure 6.12 que l'index d'équité de PAS avec l'utilisation t_rate est inférieur à PAS sans t_rate pour des petites tailles de paquet mais reste acceptable et bien supérieur à celui de 802.11.

6.6.6 Comparaison avec d'autres solutions

La modification du backoff

Nous avons comparé PAS à un protocole qui cherche à résoudre l'anomalie de performance en modifiant la fenêtre de contention de 802.11. La solution que nous avons développée s'appuie sur la solution proposée dans [35]. La taille de la fenêtre de contention (CW) est adaptée de la manière suivante :

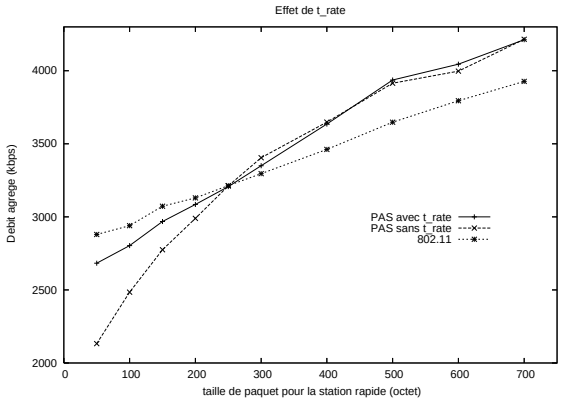


FIG. 6.11: PAS : Débit agregé en fonction de la taille des paquets.

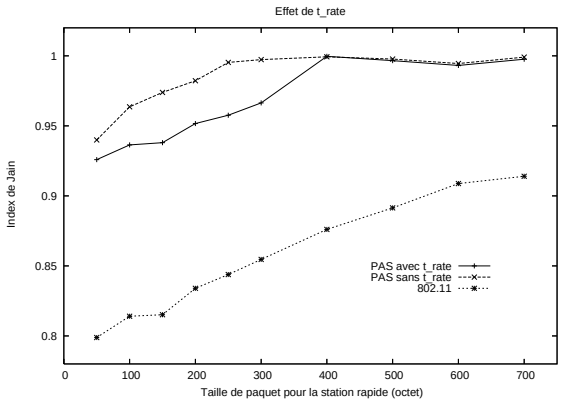


FIG. 6.12: PAS : index d'équité en fonction de la taille des paquets.

$$CW = CW * \frac{11e6}{dataRate} \tag{6.9}$$

La simulation de deux stations avec des tirages uniformes de la taille des paquets entre $[550; 1450]$ montre que les deux solutions résolvent le problème de l'anomalie de performance (figure 6.13). Cependant PAS est plus efficace car la solution de comparaison ajoute un temps de backoff avant chaque transmission. Un autre problème lié a cette approche est l'envoi de petits paquets par la station rapide. Dans ce cas, la solution modifiant le backoff perd en efficacité. Pour PAS, ce problème est résolu par l'utilisation de t_rate.

La fragmentation de paquets

Nous avons aussi comparé notre solution à la solution proposée par Iannonne *et al.* [39]. Dans cette simulation, deux stations, une rapide (11 Mbps) et une lente (5.5 Mbps), transmettent des paquets de 1500 octets. Pour la solution avec fragmentation de paquets, les paquets de la station lente sont divisés au niveau IP en deux paquets de 727 octets. La figure 6.14 montre que les deux solutions résolvent l'anomalie de performance mais que la fragmentation est moins efficace que PAS. Ceci est dû à l'utilisation du backoff entre chaque transmission. La fragmentation pose aussi un problème s'il n'y a que des stations lentes sur le réseau car les paquets seront fragmentés et les performances

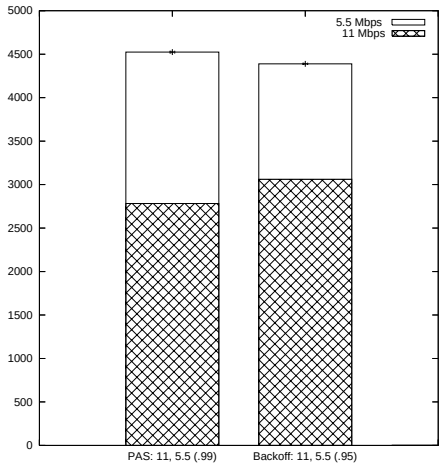


FIG. 6.13: PAS vs Modification de backoff.

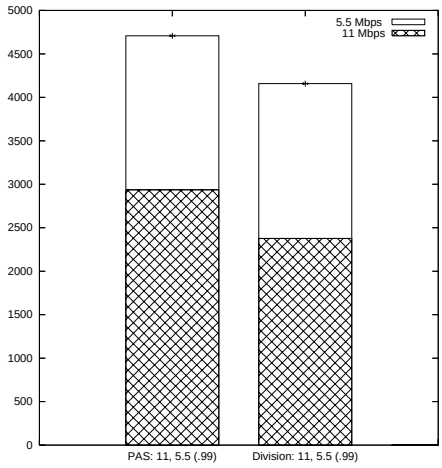


FIG. 6.14: PAS vs Fragmentation de paquets.

seront diminuées à cause du ratio entre les données et les entêtes protocolaires.

Temps d'agrégation fixe

Pour comparer notre solution à une solution utilisant un temps d'agrégation fixe, nous avons modifié PAS et utilisé $t_p_max = 8000\mu s$. Avec cette valeur, une station ayant un paquet de 1500 octets à transmettre à 1 Mbps ne peut envoyer qu'un seul paquet. La figure 6.15 montre que l'agrégation sur un temps fixe est plus efficace que PAS. Ceci est dû au fait que les deux stations rapide (11 Mbps) et lente (5.5 Mbps) agrègent des paquets sur chaque transmission accroissant ainsi le débit global.

Cependant, la table 6.3 montre que le nombre de rafales est plus élevé pour PAS et que le temps inter-rafales de PAS est beaucoup plus court que celui du protocole utilisant un temps d'agrégation fixe.

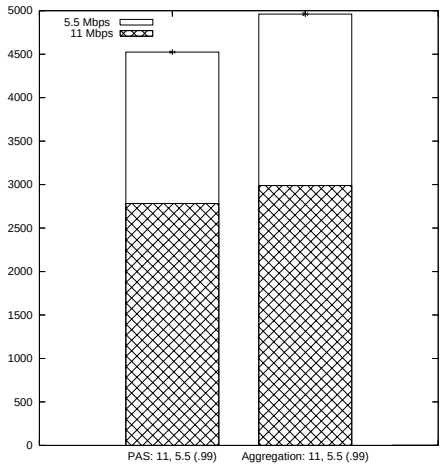


FIG. 6.15: PAS vs Temps d'agrégation fixe.

		Nombre de rafales	Temps moyen inter-rafales
FIXE	5.5Mbps	7123	11230.07 μs
	11Mbps	6666	12000.80 μs
PAS	5.5Mbps	19570	4087.80 μs
	11Mbps	19346	4135.11 μs

TAB. 6.3: PAS vs. Temps d'agrégation fixe

6.7 Simulations spécifiques au couple 802.11/PAS

6.7.1 Les stations cachées

Pour montrer l'utilisation des RTS/CTS, nous avons voulu voir le comportement de PAS dans le contexte des stations cachées. Dans la simulation présentée ici, le seuil de déclenchement des RTS/CTS est de 200 octets et les paquets sont de taille 1000 octets. Dans ce scénario, l'une des stations cachées est une station lente (1, 2 , 5.5 ou 11 Mbps) et l'autre une station rapide (11 Mbps). La figure 6.16 montre que la différence entre 802.11 et PAS ne se voit que pour les stations lentes ayant un débit de 2 ou 1 Mbps. Ceci est dû au fait que la station rapide peut agréger plus de paquets. Pour une station lente transmettant à 5.5 Mbps les performances de PAS et de 802.11 sont les mêmes. Dans ce cas, l'agrégation est possible mais la probabilité de collision du deuxième paquet agrégé est très forte et réduit ainsi le débit global. Pour une station lente à 5.5 Mbps, t_my_left n'est pas assez grand pour permettre la retransmission d'un paquet ayant subi une collision alors que pour une station lente à 2 ou 1 Mbps, cette retransmission agrégée est possible et permet ainsi d'accroître un peu le débit global.

La figure 6.17 montre les résultats d'une simulation avec une station lente (1 Mbps) et une station rapide (11 Mbps) avec des paquets de taille aléatoire tirée entre [550; 1450] octets et un seuil d'utilisation de RTS à 1000 octets. On voit que malgré l'utilisation de tailles de paquet aléatoires, PAS est plus efficace et équitable que 802.11. Il faut noter que dans ce scénario, quand les RTS ne sont pas utilisés, t_p_max est le temps de transmission d'un acquittement.

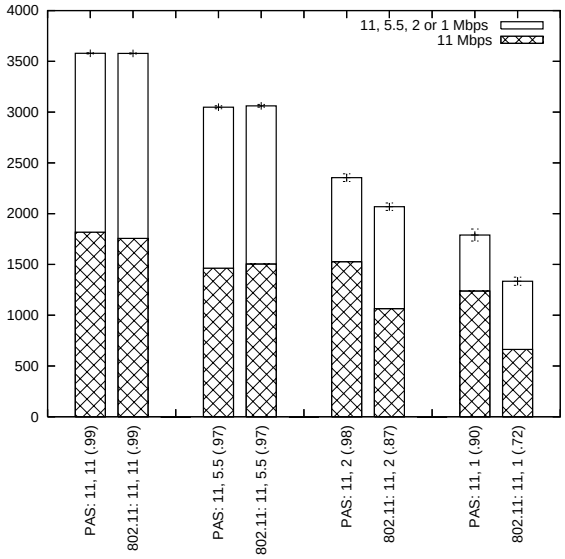


FIG. 6.16: PAS avec RTS/CTS sur les stations cachées.

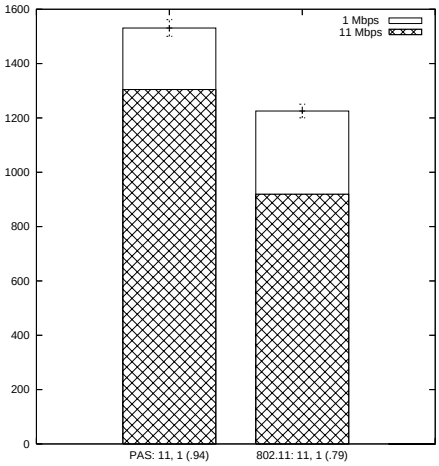


FIG. 6.17: PAS avec RTS/CTS et des tailles de paquets aléatoires.

6.7.2 Flux TCP asymétriques

Pour évaluer les performances de PAS avec des flux TCP [17], nous avons simulé le scénario bien connu des flux TCP asymétriques [46]. La figure 6.18 montre ce scénario où la station rapide (11 Mbps) est la station A et la station lente (2 Mbps) est la station B. Chaque station doit envoyer un flux TCP saturant TCP_{ab} pour le flux de A vers B et TCP_{ba} pour le flux de B vers A. Il faut noter que les flux TCP utilisent la même file d'attente pour l'envoi des paquets et des acquittements. De ce fait, le débit de la station rapide sera dégradé à cause du délai dans la file d'attente de la station lente mais aussi des pertes au niveau de celle-ci.

La figure 6.19 montre les débits obtenus pour les deux flux. On voit clairement que les performances de PAS sur ce scénario sont meilleures que celles de 802.11. Ceci est dû au fait que la station lente peut agréger les acquittements, ce qui accroît le débit de la station rapide. Ces résul-

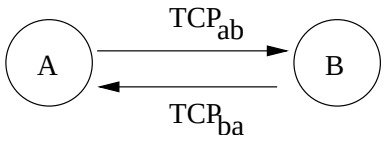


FIG. 6.18: PAS : scénario des flux TCP asymétriques

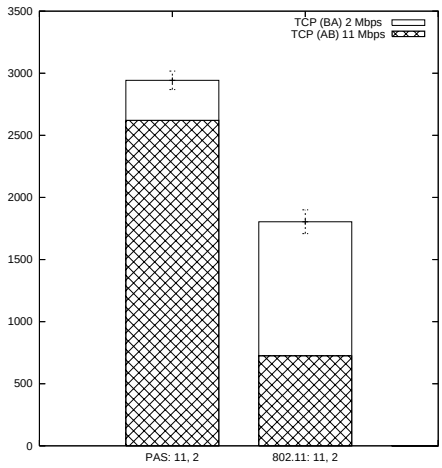


FIG. 6.19: PAS : résultats sur les flux TCP asymétriques.

tats montrent qu'une modification au niveau MAC peut améliorer les performances des protocoles de niveau supérieur. Ces résultats sont néanmoins à prendre avec précaution et d'autres analyses et simulations doivent être faites pour obtenir l'influence réelle de PAS sur TCP.

6.7.3 Contexte hétérogène

Le choix de l'utilisation du couple PAS/802.11 nous permet d'utiliser PAS dans un contexte hétérogène, c'est-à-dire des stations utilisant PAS et des stations utilisant 802.11. Le tableau 6.4 montre les résultats de simulations en présence de quatre stations : deux utilisant PAS dont l'une rapide (11 Mbps) et l'autre lente (2 Mbps) et les deux autres utilisant 802.11 dont l'une rapide et l'autre lente. Chaque station envoie un flux UDP à saturation. Les résultats montrent que dans un contexte hétérogène, la station rapide utilisant PAS réussit à obtenir un meilleur débit que les autres stations augmentant ainsi le débit global du réseau.

6.7.4 Un premier scénario *ad hoc*

Bien que PAS soit conçu au départ pour les cellules de communication comme 802.11, sa nature distribuée lui permet d'être utilisé dans un réseau *ad hoc*. Le scénario que nous avons testé ici est le scénario des trois paires [14]. Comme les transmissions des paires extérieures (qui sont indépendantes l'une de l'autre) se superposent, l'occupation du médium perçu par la paire centrale est montrée sur la figure 6.20. Il est facile d'observer que la valeur de t_p_max pour la paire centrale sera au plus $t_p0 + t_p2$ où $t_pi_{i\in\{0,2\}}$ est le temps de transmission d'un paquet pour la paire i.

Le tableau 6.5 montre les résultats de simulations pour les paires $P0$ et $P2$ transmettant des paquets de 1000 octets à 2 Mbps et la paire $P1$ transmettant des paquet de 1000 octets à 11 Mbps. On voit que même si l'utilisation de PAS ne résout pas le problème des trois paires (les partages

		Débits (kbps)	Intervalle de confiance (0.05)
Hétérogène	Rapide (802.11)	445.62	[431.30 ; 459.94]
	Rapide (PAS)	1815.40	[1777.37 ; 1853.44]
	Lente (802.11)	477.73	[465.98 ; 489.48]
	Lente (PAS)	478.76	[468.64 ; 488.87]
	Total	3217.51	[3185.84 ; 3249.17]
Toutes 802.11	Rapide	566.04	[548.81 ; 583.27]
	Rapide	581.13	[566.05 ; 596.21]
	Lente	583.42	[570.67 ; 596.18]
	Lente	611.37	[599.62 ; 623.12]
	Total	2341.97	[2321.05 ; 2362.89]
Toutes PAS	Rapide	1484.23	[1435.37 ; 1533.09]
	Rapide	1511.53	[1471.98 ; 1551.07]
	Lente	403.10	[394.02 ; 412.18]
	Lente	395.38	[386.01 ; 404.75]
	Total	3794.24	[3759.19 ; 3829.29]

TAB. 6.4: Ce tableau montre les résultats de simulation de l'utilisation de PAS dans un contexte hétérogène. Sur un même réseau, plusieurs protocoles MAC sont utilisés, ici PAS et 802.11

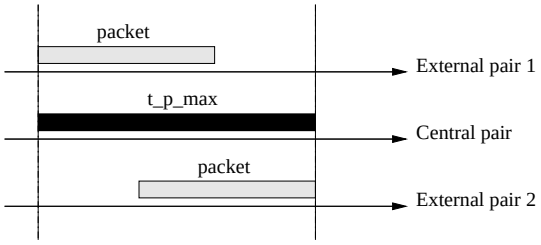


FIG. 6.20: L'occupation du médium perçu par la paire centrale.

		Débit (kbps)	Int. de Conf.
PAS	P0	1592.49	[1584.16 ; 1600.82]
	P1	102.21	[68.28 ; 136.15]
	P2	1592.49	[1584.09 ; 1600.89]
802.11	P0	1634.15	[1632.03 ; 1636.27]
	P1	6.44	[1.78 ; 11.11]
	P2	1632.86	[1630.23 ; 1635.49]

TAB. 6.5: PAS : résultats sur les trois paires

temporels sont encore très différents) le débit de la paire centrale est meilleur quand PAS est utilisé à la place de 802.11.

6.8 Conclusion

Conclusion

Dans ce chapitre, nous proposons un mécanisme dynamique d'agrégation des paquets résolvant l'anomalie de performance de la norme IEEE 802.11. Notre solution s'appuie sur le fait que chaque station dispose du même temps de transmission. Bien que des solutions similaires ont déjà été proposées, comme par exemple dans la norme IEEE 802.11e, notre solution est différente parce que ce temps de transmission est calculé dynamiquement et de manière totalement distribuée, ne nécessitant que des informations disponibles localement. Ce calcul utilise simplement le mécanisme d'écoute active du médium pour obtenir le temps de transmission utilisé.

Nous avons montré qu'en utilisant PAS, l'anomalie de performance est résolue et que le débit global dans le réseau est augmenté. Nous avons également montré que notre approche n'a pas besoin d'information supplémentaire et peut être facilement implémentée au-dessus de 802.11. Cependant, rien n'empêche l'implémentation de PAS au-dessus d'une couche MAC telle que MadMac, Idle Sense [35] ou AOB [8].

Perspectives

Dans chapitre nous avons fait le choix d'utiliser PAS au-dessus de 802.11. Dans la suite de ces travaux, nous aimerions évaluer les performances de PAS au-dessus d'autres protocoles. Ces résultats nous permettront de savoir avec quel protocole PAS exhibe les meilleures performances pour résoudre l'anomalie de performance.

L'approche totalement distribuée de cette solution nous laisse penser qu'il est possible d'utiliser PAS au-dessus de solutions MAC pour les réseaux *ad hoc* telles que MadMac, PNAV ou MBFAIR. De plus, les résultats prometteurs de PAS sur les flux TCP asymétriques restent une piste de recherche ouverte sur comment concevoir une couche MAC pour les réseaux sans fil permettant d'accroître les performances de TCP.

7 Conclusion et Perspectives

« Pourquoi apprendre alors que l'ignorance est instantanée ? »

Bill Watterson,
Extrait de la bande dessinée Calvin et Hobbes.

Ce dernier chapitre conclut ce manuscrit de thèse. Nous revenons rapidement sur les travaux présentés dans cette thèse et développons les perspectives et suites à donner aux travaux présentés ici.

7.1 Conclusion

Les applications pour les réseaux sans fil et particulièrement les réseaux *ad hoc* sont de plus en plus claires. Ces applications ne demandent pas toutes les même performances. Un réseau de capteur va attacher plus d'importance à l'économie d'énergie alors qu'un réseau maillé va chercher à maximiser la capacité du réseau. Ces différents besoins et les contraintes qui y sont liées nécessitent bien souvent l'élaboration d'une pile protocolaire spécifique.

Au début de cette thèse, les applications des réseaux pour lesquelles les protocoles conçus seraient destinés n'etaient pas tout à fait claires. Néanmoins, nous avons voulu nous attaquer à un problème ouvert et qui selon nous l'est encore, celui de l'équité. Nous nous sommes attachés à étudier l'effet de l'équité au niveau 2 de la couche OSI et l'impact que celle-ci à sur les protocoles situés au niveau 3 et sur le débit des applications.

Dans la première partie de cette thèse, nous avons voulu connaître les paramètres qui influent sur l'équité dans 802.11. Nous avons donc étudié 802.11. En effet, 802.11 étant le standard de fait dans les réseaux *ad hoc*, il nous paraissait utile et nécessaire de bien comprendre son fonctionnement avant même de proposer une alternative ou de l'améliorer. Dans le premier chapitre de cette thèse, nous avons élaboré un modèle de 802.11 en utilisant le formalisme des algèbres de processus stochastiques. Ce modèle nous a permis de mieux comprendre les performances de 802.11 dans des cas pathologiques mettant en défaut l'équité de 802.11. Nous avons vu comment les collisions au niveau MAC pouvaient réduire les performances de 802.11 mais surtout, comment la présence de collisions pouvait affecter l'équité dans 802.11. Nous avons aussi vu comment des situations de famine pouvaient améliorer les performances tout en réduisant l'équité. Les résultats de ce chapitre montrent que l'algorithme de *backoff* et l'ordonnancement aléatoire fournis par 802.11 sont en grande partie responsables des problèmes d'équité dans 802.11.

En nous appuyant sur les résultats obtenus dans cette première partie, nous avons conçu MadMac : un protocole MAC pour les réseaux *ad hoc* qui se veut équitable et efficace. Le principe de MadMac est simple : tenter d'ordonnancer l'accès au médium radio. Pour cela, une station utilisant MadMac considère les autres stations comme un seul adversaire et partage le médium en deux (elle et les autres). Ce partage en deux permet d'avoir une meilleure équité que celle de 802.11 (comparée à une équité MaxMin) tout en maintenant une bonne efficacité. De plus, MadMac intègre un mécanisme efficace d'évitement de collisions. L'implémentation de ce mécanisme résulte de l'interprétation des résultats du premier chapitre, qui montrent que la principale source d'iniquité et d'inefficacité est la collision. Ces deux mécanismes, partage et évitement de collisions, font de MadMac un protocole équitable et efficace.

Les premières évaluations de performance de MadMac ont été réalisées en regardant les débits des flux obtenus dans différents réseaux avec des flux UDP à saturation. Dans ces conditions, MadMac est performant. Cependant, l'utilisation de flux UDP à saturation est le pire cas de fonctionnement et les réseaux *ad hoc* seront peut être utilisés dans des cas moins extrêmes. C'est dans cette optique que nous avons essayé d'évaluer les performances d'un protocole de découverte de voisinage en utilisant MadMac et 802.11 comme couche MAC. Les résultats ont confirmé notre intuition. MadMac et 802.11 ont exactement le même comportement et la même influence sur le protocole de découverte de voisinage quand aucun flux n'est présent sur le réseau. L'utilisation de MadMac n'a une influence conséquente sur les performances du protocole de découverte de voisinage que quand le nombre de flux dans le réseau augmente. Les résultats présentés dans ce chapitre semblent néanmoins montrer que l'utilisation de MadMac est recommandée car lorsque la charge augmente, il permet d'accroître les performances des protocoles des couches supérieures.

Après une étude dans les trois premiers chapitres de ce manuscrit sur l'équité d'accès menant à des

transmissions correctes, la quatrième contribution présente une solution à un problème bien connu de la norme 802.11b, l'anomalie de performance. Dans ce chapitre, nous proposons une solution dynamique et distribuée pour résoudre l'anomalie de performance utilisant l'agrégation de paquets. Cette solution, bien que pouvant être adaptée sur tous les protocoles utilisant l'écoute active du canal radio, a été testée avec 802.11. Notre protocole PAS (*Performance Anomaly Solution*) se démarque des protocoles présentés dans la littérature par son aspect dynamique et distribué. De plus, la comparaison avec les autres types de solutions trouvées dans la littérature montre que l'approche choisie dans PAS résout le problème de l'anomalie de performance en étant soit plus performant soit plus équitable que ses concurrents.

7.2 Perspectives

Nous avons étendu l'évaluation de performance de 802.11 proposée dans le premier chapitre par une évaluation de 36 algorithmes de *backoff*. Ces résultats devraient permettre de concevoir un algorithme de *backoff* selon les besoins du réseau, en terme par exemple d'équité, d'efficacité ou de compromis. Il nous semble utile, avec le recul, de repenser à des solutions utilisant une modification intelligente des algorithmes de *backoff*. Ces solutions pourraient fournir de meilleurs résultats que l'actuel algorithme de *backoff* de 802.11, dans certains cas d'utilisation bien précis, et ne nécessiteraient peut-être pas le déploiement de solution telle que MadMac.

Pour la conception de MadMac, nous avons choisi de considérer une hypothèse forte qui est aucun échange d'informations explicites. Cette contrainte paraît simple mais elle a néanmoins posé un problème d'un point de vue de l'équité. Bien que personne ne l'ait démontré, il semble très difficile d'obtenir une équité donnée sans échange d'informations explicites. En voulant respecter cette contrainte, nous avons donc fait de MadMac un protocole dont l'objectif est d'être équitable mais sans vraiment déterminer une équité comme objectif. Ainsi, pour évaluer l'équité de MadMac, nous l'avons arbitrairement comparé à une allocation MaxMin. Les résultats ont montré que l'allocation obtenue avec MadMac est proche d'une allocation MaxMin. Il nous semble maintenant important d'essayer de déterminer précisément vers quelle allocation MadMac tend. Nous cherchons aussi à modifier les paramètres de MadMac pour comparer l'allocation obtenue avec d'autres allocations telle que l'allocation proportionnelle par exemple.

Nous travaillons aussi actuellement sur la combinaison PAS/MadMac. Dans les travaux présentés dans cette thèse, nous n'avons pas abordé le problème de l'équité temporelle dans les réseaux *ad hoc*. La possibilité d'intégrer PAS au-dessus de MadMac nous pousse à regarder dans ce sens. Intuitivement, nous pensons que la combinaisons PAS/MadMac devrait améliorer l'équité dans les réseaux *ad hoc* dans lesquels les stations auraient des débits différents. Cette intuition reste à confirmer.

Il nous paraît ainsi difficile d'imposer une couche MAC pour tous les réseaux *ad hoc*. Cette intuition est confirmée par le nombre de protocoles MAC standardisés, comme 802.11, Bluetooth, ZigBee, et le nombre de propositions de protocoles MAC dans la littérature. Cependant, la clarification des applications de réseaux *ad hoc* étant de plus en plus précise, la tendance sera peut-être dans la conception de couches MAC paramétrées pouvant s'adapter à la plupart des applications, si ce n'est à tous les contextes d'utilisation.

Nous pensons que l'avenir des nouveaux protocoles MAC réside dans leur polyvalence. Cette polyvalence pour MadMac pourrait venir d'un dimensionnement particulier de ses paramètres suivant le contexte d'utilisation. Cette approche pose cependant un problème de définition et de reconnaissance du contexte d'utilisation. Malgré tous les problèmes liés à la dynamicité, à l'adaptation et à la

mobilité des stations, nous pensons qu'une telle approche reste l'avenir des protocoles MAC. Cette approche permettrait par exemple en modifiant quelques paramètres, d'utiliser MadMac pour les réseaux de capteur ou pour les réseaux maillés. Par exemple si MadMac devait être utilisé dans les réseaux de capteurs la réduction de l'écoute du canal nécessaire à l'économie d'énergie pourrait se faire en éteignant le capteur pendant les temps d'attente insérés par le protocole. Pour une utilisation dans un réseau maillé, MadMac pourrait tirer partie des informations liées à la topologie pour mieux adapter ses temps d'attente.

L'identification des applications pour lesquelles le protocole MAC sera utilisé pourra nous permettre d'approfondir les analyses concernant l'impact de la couche MAC sur les performances des couches supérieures. Nous regardons actuellement comment le comportement du protocole MAC influe sur un protocole d'auto-organisation. Ce travail fait suite au travail présenté dans le chapitre 5.

D'un point de vue plus pragmatique, il manque à MadMac et PAS une évaluation réelle du protocole. Car bien que les simulations montrent de bons comportements, selon nous, rien ne vaut les aléas liés à l'expérimentation pour avoir une idée précise du comportement du protocole. L'utilisation des cartes sans fil actuelles pour implémenter nos protocoles reste complexe car les constructeurs ne permettent pas de modifier le code de la couche MAC implémentée. Nous nous tournons en ce moment vers les capteurs qui eux permettent, dans quelques cas, la modification des couches MAC pour pouvoir réaliser des expérimentations de nos protocoles.

L'apparition et l'identification précises des applications pour les réseaux *ad hoc* permettent de concevoir des protocoles MAC de plus en plus spécifiques. Il nous paraît important, à plus long terme, d'intégrer les caractéristiques des applications dans le processus de conception de la couche MAC. Cependant, deux choix peuvent s'offrir : on peut concevoir un protocole MAC optimal par application ou concevoir un protocole MAC générique fournissant des performances correctes pour un grand nombre d'applications. Dans les deux cas, nous pensons que l'accroissement du nombre d'applications pour les réseaux *ad hoc* ne fera qu'accroître l'intérêt de la communauté scientifique pour les problèmes de la méthode d'accès dans ces réseaux.

Liste de publications

Journaux internationaux avec comité de lecture

[1] **Dynamic and Distributed Packet Aggregation to Solve Performance Anomaly in 802.11 Wireless Networks**, by Tahiry RAZAFINDRALAMBO, Isabelle GUERIN-LASSOUS, Luigi IANNONE, Serge FDIDA. In *COMPUTER NETWORKS JOURNAL (ELSEVIER)*, Accepted for publication (2007)

[2] **Increasing Fairness and Efficiency using the MadMac Protocol in Ad Hoc Networks**, by Tahiry RAZAFINDRALAMBO, Isabelle GUERIN-LASSOUS. In *AD HOC NETWORKS JOURNAL (ELSEVIER)*, Accepted for publication (2007)

Conférences et workshop internationaux avec comité de lecture

[1] **Analysis of the Impact of Hello Protocol Parameters over a Wireless Network Self-Organization**, by Tahiry RAZAFINDRALAMBO, Nathalie MITTON In*The 4th ACM International Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks (PE-WASUN'07)* October 2007 - Chania, Crete.

[2] **Performance Evaluation of Backoff algorithms in 802.11 Ad-Hoc Networks**, by Tahiry RAZAFINDRALAMBO, Fabrice VALOIS. In*The 3rd ACM International Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks (PE-WASUN'06)* October 2006 - Torremolinos, Malaga, Spain.

[3] **Dynamic Packet Aggregation to Solve Performance Anomaly in 802.11 Wireless Networks**, by Tahiry RAZAFINDRALAMBO, Isabelle GUERIN-LASSOUS, Luigi IANNONE, Serge FDIDA. The*9-th ACM/IEEE International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWIM'06)* October 2006 - Torremolinos, Malaga, Spain.

[4] **Modeling Methodology for Wireless LANs Performance Evaluation**, by Tahiry RAZAFINDRALAMBO, Fabrice VALOIS. In*4th International Working Conference on Performance Modelling and Evaluation of Heterogeneous Networks (Het-Nets)* September 2006 - Ilkely, West Yorkshire, U.K.

[5] **Stochastic Behavior Study of Backoff Algorithms in Case of Hidden Terminals**, by Tahiry RAZAFINDRALAMBO, Fabrice VALOIS. The*17th Annual IEEE International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC'06)* September 2006 - Helsinki, Finland.

[6] **Increasing Fairness and Efficiency using the MadMac Protocol in Ad Hoc Networks**, by Tahiry RAZAFINDRALAMBO, Isabelle GUERIN-LASSOUS. In*5-th International Conference on Networking (NETWORKING'06)* May 2006 - Coimbra, Portugal.

[7] **Formal Evaluation and Comparison of Real Time Embedded Automotive Networks**, by Tahiry RAZAFINDRALAMBO, Isabelle AUGE-BLUM. In *International Conference on Industrial Technology (ICIT'04)* Dec 2004 - Hammamet, Tunisia.

Conférences nationales avec comité de lecture

[1] **Influence du médium radio sur le phénomène d'équité dans les réseaux ad hoc**, by Tahiry RAZAFINDRALAMBO, Jean-Marie GORCE, Fabrice VALOIS. In*9ème rencontres francophones sur les aspects algorithmiques de télécommunications (AlgoTel'07)* Ile d'Oléron, 29 mai - 1 juin 2007 (to be published)

[2] **Agrégation dynamique de paquets pour résoudre l'anomalie de performance des réseaux sans fil IEEE 802.11**, by Tahiry RAZAFINDRALAMBO, Isabelle GUERIN-LASSOUS, Luigi IANONE, Serge FDIDA. In *Colloque Francophone sur l'Ingenierie des Protocoles (CFIP'06)* November 2006 - Tozeur, Tunisie. (2nd student best paper award).

[3] **Modélisation et évaluation de performances de stratégies de backoff**, by Tahiry RAZAFINDRALAMBO, Fabrice VALOIS. In*Colloque Francophone sur l'Ingenierie des Protocoles (CFIP'06)* November 2006 - Tozeur, Tunisie.

[4] **MadMac : un protocole équitable et efficace pour les réseaux ad hoc basés sur 802.11**, by Tahiry RAZAFINDRALAMBO, Isabelle GUERIN-LASSOUS. In*7e Journees Doctorales Informatique et Reseau (JDIR'05)* December 2005 - Troyes, France.

Rapport de recherche

[1] **Dynamic Packet Aggregation to Solve Performance Anomaly in 802.11 Wireless Networks**, by Tahiry RAZAFINDRALAMBO, Isabelle GUERIN-LASSOUS, Luigi IANNONE, Serge FDIDA. ResearchReport 5958, Institut National de Recherche en Informatique et en Automatique (INRIA) July 2006.

[2] **Increasing Fairness and Capacity using MadMac Protocol in 802.11-based Ad Hoc Networks**, by Tahiry RAZAFINDRALAMBO, Isabelle GUERIN-LASSOUS. ResearchReport 5633, Institut National de Recherche en Informatique et en Automatique (INRIA) July 2005.

Bibliographie

[1] N. Abramson. The ALOHA system. *Computer Networks*, 25 :501–518, 1973.

[2] I.F. Akyildiz, J. McNair, L.C. Martorell, R. Puigjaner, and Y. Yesha. Medium Access Control Protocols for Multimedia Traffic in Wireless Networks. *IEEE Network Magazine*, 13 :39–47, July/August 1999.

[3] Brahim Bensaou, Y. Wang, and C. C. Ko. Fair Medium Access in 802.11 based Wireless Ad-Hoc Networks. In *ACM Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC)*, pages 99–106, Boston, Massachusetts, 2000.

[4] G. Berger-Sabbatel, A. Duda, O. Gaudoin, M. Heusse, and F. Rousseau. Fairness and its Impact on Delay in 802.11 Networks. In *GLOBECOM*, November 29-December 3 2004.

[5] V. Bharghavan, A. Demers, S. Shenker, and L. Zhang. MACAW : a media access protocol for wireless LAN's. In *ACM SIGCOMM Computer Communication Review*, pages 212–225, London, United Kingdom, 1994.

[6] G. Bianchi. Performance Analysis of the IEEE 802.11 DCF. *IEEE Journal on Selected Areas in Communication (JSAC)*, 18 :535–547, 2000.

[7] T. Bonald and L. Massoulie. Impact of Fairness on Internet Performance. In *SIGMETRICS/Performance*, pages 82–91, 2001.

[8] L. Bononi, M. Conti, and E. Gregori. Runtime Optimization of IEEE 802.11 Wireless LANs Performance. *IEEE Transactions on Parallel and Distributed Systems (TPDS)*, 15(1) :66–80, 2004.

[9] R. Bruno, C. Chaudet, M. Conti, and E. Gregori. A Novel Fair Medium Access Control for 802.11-based Multi-Hop Ad hoc Networks. In *14th IEEE Workshop on Local and Metropolitan Area Networks (LanMan)*, September 2005.

[10] R. Bruno, M. Conti, and E. Gregori. Optimal capacity of p-persistent CSMA protocols. *IEEE Communications Letters*, 7(3) :139–141, 2003.

[11] A. Chandra, V. Gummalla, and J. O. Limb. Wireless Medium Access Control Protocols. *IEEE Communications Surveys and Tutorials*, 3(2) :2–15, 2000.

[12] P. Chatzimisios, A. C. Boucouvalas, V. Vitsas, A. Vafiadis, A. Oikonomidis, and P. Huang. A simple and effective backoff scheme for the IEEE 802.11 MAC protocol. In *Cybernetics and Information Technologies, Systems and Applications (CITSA)*, July 2005.

[13] C. Chaudet, G. Chelius, H. Meunier, and D. Simplot-Ryl. Adaptive Probabilistic NAV to Increase Fairness in Ad Hoc 802.11 MAC. *Ad Hoc and Sensor Wireless Networks : an International Journal (AHSWN)*, In Press., June 2005.

[14] C. Chaudet, D. Dhoutaut, and I. Guérin-Lassous. Performance Issues with IEEE 802.11 in Ad Hoc Networking. *IEEE Communications Magazine*, 43(7) :110–116, July 2005.

[15] C. Chaudet, I. Guérin-Lassous, E. Thierry, and B. Gaujal. Study of the Impact of Asymmetry and Carrier Sense Mechanism in IEEE 802.11 Multi-hops Networks through a Basic Case. In *ACM Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks (PE-WASUN)*, 2004.

[16] T. Clausen and P. Jacquet. Optimized Link State Routing Protocol (OLSR). RFC 3626, IETF, 2003.

[17] DARPA. Transmission Control Protocol Specifications. RFC 793, Defense Advanced Research Projects Agency Information Processing Techniques Office, September 1981.

[18] L. De Alfaro, M. Kwiatkowska, g. Norman, D. Parker, and R. Segala. Symbolic Model Checking of Concurrent Probabilistic Processes Using MTBDDs and the Kronecker Representation. In S. Graf and M. Schwartzbach, editors, *Proc. 6th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'00)*, volume 1785 of *LNCS*, pages 395–410. Springer, 2000.

[19] D. D. Deavours, G. Clark, T. Courtney, D. Daly, S. Derisavi, J. M. Doyle, W. H. Sanders, and Webster P. G. The Möbius Framework and Its Implementation. *IEEE Transactions on Software Engineering*, 28(10) :956–969, 2002.

[20] S. Donatelli. Superposed Generalized Stochastic Petri Nets : Definition and Efficient Solution. In *Proceedings of the 15th International Conference on Application and Theory of Petri Nets*, volume 3-540-58152-9, pages 258–277, London, UK, 1994. Springer-Verlag.

[21] J. Dunn, M. Neufeld, A. Sheth, D. Grunwald, and J. Bennet. A practical Cross-Layer Mechanism for Fairness in 802.11 Networks. In *BROADNETS*, 2004.

[22] ETSI. ETS 300 652 High Performance Radio Local Area Network (HiperLAN) type 1 - Functionnal Specification.

[23] Z. Fang and Brahim Bensaou. Fair Bandwidth Sharing Algorithms based on Game Theory Frameworks for Wireless Ad-hoc Networks. In *IEEE INFOCOM*, 2004.

[24] Z. Fang, Brahim Bensaou, and Y. Wang. Performance evaluation of a fair backoff algorithm for IEEE 802.11 DFWMAC. In *ACM Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC)*, pages 48–57, Lausanne, Switzerland, 2002.

[25] C.L. Fullmer and J.J. Garcia-Luna-Aceves. Floor Acquisition Multiple Access (FAMA) for packet-radio networks. In *ACM SIGCOMM Computer Communication Review*, Cambridge MA, August 28-September 1 1995.

[26] R. Garcés and J.J. Garcia-Luna-Aceves. A Near-Optimum Channel Access Protocol Based on Incremental Collision Resolution and Distributed Transmission Queues. In *IEEE INFOCOM*, pages 158–165, 1998.

[27] M. Garetto and C-F. Chiasserini. Performance Analysis of 802.11 WLANs Under Sporadic Traffic. In Lecture Notes in Computer Science, editor, *IFIP Netwoking*, volume 3462/2005, pages 1343–1347, 2005.

[28] M. Garetto, T. Salonidis, and E. W. Knightly. Modeling Per-Flow Throughput and Capturing Starvation in CSMA Multi-Hop Wireless Networks. In *IEEE INFOCOM*, pages 1–13, April 2006.

[29] M. Garetto, J. Shi, and E. Knightly. Modeling media access in embedded two-flow topologies of multi-hop wireless networks. In *ACM Conference on Mobile Computing and Networking (MOBICOM)*, pages 200–214, Cologne, Germany, 2005.

[30] S. Gilmore and J. Hillston. The PEPA Workbench : A Tool to Support a Process Algebra-based Approach to Performance Modelling. In *International Conference on Modelling Techniques and Tools for Computer Performance Evaluation*, pages 353–368, 1994.

[31] D. Gross and C. M. Harris. *Fundamentals of Queueing Theory*. Wiley, 1998.

[32] J. He. Performance modeling and evaluation of IEEE 802.11 distributed coordination function in multihop wireless networks. In *ICON*, 2004.

[33] J. He and H. K. Pung. Fairness of Medium Access Control Protocols for Multi-hop Qd Hoc Wireless Networks. *Computer Networks*, 48(6) :867–890, 2005.

[34] M. Heusse, F. Rousseau, G. Berger-Sabbatel, and A. Duda. Performance Anomaly of 802.11b. In *IEEE INFOCOM*, San Francisco, USA, April 2003. IEEE.

[35] M. Heusse, F. Rousseau, R. Guillier, and A. Duda. Idle Sense : an Optimal Access Method for High Throughput and Fairness in Rate Diverse Wireless LANs. In *ACM SIGCOMM Computer Communication Review*, pages 121–132, Philadelphia, Pennsylvania, USA, 2005.

[36] J. Hillston. *A Compositional Approach to Performance Modelling*. PhD thesis, 1994.

[37] J. Hillston and L. Kloul. An Efficient Kronecker Representation for PEPA Models. In *PAPM-PROBMIV '01 : Proceedings of the Joint International Workshop on Process Algebra and Probabilistic Methods, Performance Modeling and Verification*, pages 120–135, London, UK, 2001. Springer-Verlag.

[38] X. L. Huang and B. Bensaou. On Max-Min Fairness and Scheduling in Wireless Ad-Hoc Networks : Analytical Framework and Implementation. In *ACM Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC)*, pages 221–231, Long Beach, CA, USA, 2001.

[39] L. Iannone and S. Fdida. SDT.11b : Un Schéma à Division de Temps pour éviter l'anomalie de la couche MAC 802.11b. In *Colloque Francophone sur l'Ingénierie des Protocoles (CFIP)*, 2005.

[40] IEEE and Information Exchange between Systems. *Local and Metropolitan Area Network – Specific Requirements –Part 11 : Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. The Institute of Electrical and Electronics Engineers, 1997.

[41] IEEE and Information Exchange between Systems. *Local and Metropolitan Area Network – Specific Requirements –Part 11 : Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications — Higher-speed physical layer extension in the 2.4 GHz band*. The Institute of Electrical and Electronics Engineers, 1999.

[42] IEEE and Information Exchange between Systems. *Local and Metropolitan Area Network – Committee of the IEEE Computer Society and the IEEE Microwave Theory and Techniques Society. – Part 16 : Air interface for fixed broadband wireless access systems*. The Institute of Electrical and Electronics Engineers, 2001, 2002.

[43] IEEE and Information Exchange between Systems. IEEE Std 802.15.4 : Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks(LR-WPANs), 2003.

[44] IEEE and Information Exchange between Systems. IEEE 802.11e/D12.0. Draft Supplement to Part 11 : Wireless Medium Access Control (MAC) and physical layer (PHY) specifications : Medium Access Control (MAC) Enhancements for Quality of Service (QoS), 2004.

[45] R. Jain, A. Durresi, and Babic G. Throughput Fairness Index : An Explanation. In *ATM Forum Document Number : ATM Forum/990045*, February 1999.

[46] L. Kalampoukas, A. Varma, and K. K. Ramakrishnan. Improving TCP throughput over two-way asymmetric links : analysis and solutions. *SIGMETRICS Performnace Evalaluation Review*, 26(1) :78–89, 1998.

[47] P. Karn. MACA- a new Channel Access Method for Packet Radio. In *Proceedings of the ARRL/CRRL Amateur Radio 9th Computer Networking Conference*, September 1990.

[48] L. Kleinrock and F. A. Tobagi. Packet switching in radio channels : Part I - carrier sense multiple access modes and their throughput - delay characteristics. *IEEE Transaction on Commununication*, 23 :1400 – 1416, 1975.

[49] L. Kloul and A. Mokhtari. Algèbre des Processus pour l'Analyse des Performances des Nœuds Actifs. *Techniques et Sciences Informatiques*, 24(2-3) :279–310, 2005.

[50] L. Kloul and F. Valois. Investigating unfairness scenarios in MANET using 802.11b. In *ACM Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks (PE-WASUN)*, Montreal, Canada, Oct. 2005.

[51] M. Kulkarni, G.and Srivastava. A channel assignment scheme for FDMA based wireless ad hoc networks in Rayleigh fading environments. In *VTC*, pages 1082–1085, Sept 2002-Fall.

[52] A. Kumar, E. Altman, D. Miorandi, and M. Goyal. New Insights From a Fixed-Point Analysis of Single Cell IEEE 802.11 WLAN. *IEEE/ACM Transactions on Networking*, 15(3) :588–601, 2007.

[53] S. Kumar, V. S. Raghavan, and J. Deng. Medium Access Control protocols for ad hoc wireless networks : A survey. *Ad Hoc Networks*, 4(3) :326–358, 2006.

[54] J. Li, C. Blake, D. S. J. De Couto, H. I. Lee, and R. Morris. Capacity of Ad Hoc Wireless Networks. In *ACM Conference on Mobile Computing and Networking (MOBICOM)*, Roma, Italy, July 2001. ACM.

[55] Z. Li, S. Nandi, and A. K. Gupta. Modeling the Short-Term Unfairness of IEEE 802.11 in Presence of Hidden Terminals. In *IFIP NETWORKING*, pages 613–625, 2004.

[56] H. Luo, S. Lu, and V. Bharghavan. A new model for packet scheduling in multihop wireless networks. In *ACM Conference on Mobile Computing and Networking (MOBICOM)*, pages 76–86, Boston, Massachusetts, United States, 2000.

[57] H. Luo, P. Medvedev, J. Cheng, and S. Lu. A Self-Coordinating Approach to Distributed Fair Queueing in Ad Hoc Wireless Networks. In *IEEE INFOCOM*, pages 1370–1379, 2001.

[58] A. Muquattash and M. Krunz. CDMA-Based MAC Protocol for Wireless Ad Hoc Networks. In *ACM Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC)*, pages 153–164, Annapolis, USA, June 2003. ACM.

[59] T. Nandagopal, T. Kim, X. Gao, and V. Bharghavan. Achieving MAC Layer Fairness in Wireless Packet Networks. In *ACM Conference on Mobile Computing and Networking (MOBICOM)*, pages 87–98, Boston, Massachusetts, United States, 2000.

[60] NS-2. The Network Simulator. `http://www.isi.edu/nsnam/ns/`.

[61] T. Ozugur, M. Naghshineh, P. Kermani, C.M. Olsen, B. Rezvani, and J.A. Copeland. Balanced media access methods for wireless networks. In *ACM Conference on Mobile Computing and Networking (MOBICOM)*, pages 21–32, New York, NY, USA, 1998. ACM Press.

[62] T. Ozugur, M. Naghsineh, P. Kermani, and J. A. Copeland. Fair media access for wireless LANs. In *IEEE Global Telecommunications Conference (GLOBECOM)*, 1999.

[63] C. Perkins, E. Belding-Royer, and S. Das. Ad hoc on-demand distance vector (aodv) routing. RFC 3561, IETF, 2003.

[64] Charles E. Perkins. *Ad Hoc Networking*. Addison-Wesley, 2001. 370 p.

[65] B. Plateau. On the stochastic structure of parallelism and synchronization models for distributed algorithms. In *SIGMETRICS conference on Measurement and modeling of computer systems*, pages 147–154. ACM Press, 1985.

[66] D. Qiao and K. Shin. Achieving Efficient Channel Utilization and Weighted Fairness for Data Communications in IEEE WLAN under the DCF. In *IEEE International Workshop on QoS*, pages pp.227–36., 2002.

[67] T. Razafindralambo and I. Guérin-Lassous. Increasing Fairness and Efficiency using the Mad-Mac Protocol in Ad Hoc Networks. *Ad Hoc Networks Journal, Elsevier Ed.*, Accepted for publication, to appear.

[68] B. Sadeghi, V. Kanodia, A. Sabharwal, and E. Knightly. Opportunistic media access for multirate ad hoc networks. *Proceedings of the 8th annual international conference on Mobile computing and networking*, 2002.

[69] G. Tan and J.V. Guttag. Time-based Fairness Improves Performances in Multi-Rate WLANs. In *In USENIX Annual Technical Conference, General Track*, 2004.

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

[71] N.H. Vaidya, P. Bahl, and S. Gupta. Distributed Fair Scheduling in a Wireless LAN. In *ACM Conference on Mobile Computing and Networking (MOBICOM)*, pages 167–78, 2000.

[72] Y. Wang and B. Bensaou. Achieving Fairness in IEEE 802.11 DFWMAC with Variable Packet Lengths. In *IEEE Global Telecommunications Conference (GLOBECOM)*, 2001.

[73] W. Ye, J. Heidemann, and D. Estrin. An Energy-Efficient MAC Protocol for Wireless Sensor Networks. In *IEEE INFOCOM*, volume 3, pages 1567–1576, New York, NY, USA, June 2002. IEEE.

[74] C.D. Young. USAP : a Unifying Dynamic Distributed Multichannel TDMA Slot Assignment Protocol. In *MILCOM*, volume 1, pages 235–239, 1996.

[75] H. Zimmermann. OSI Reference Model - The ISO Model of Architecture for Open Systems Interconnection. *IEEE Transactions on Communications*, 28(4) :425 – 432, April 1980.

RAZAFINDRALAMBO Tahiry
ARES - INRIA, Laboratoire CITI
INSA de Lyon
21, Av. J. Capelle 69621 Villeurbanne, France
tahiry.razafindralambo@insa-lyon.fr
http ://perso.citi.insa-lyon.fr/trazafin

FOLIO ADMINISTRATIF

THESE SOUTENUE DEVANT L'INSTITUT NATIONAL DES SCIENCES APPLIQUEES DE LYON

NOM : RAZAFINDRALAMBO
(avec précision du nom de jeune fille, le cas échéant)

DATE de SOUTENANCE : 03 Décembre 2007

Prénoms : Tahiry Ndrianaivonavalona

TITRE : Performances des couches MAC dans les réseaux sans fil *ad hoc* : problèmes et solutions

NATURE : Doctorat

Numéro d'ordre : 2007-ISAL-0103

Ecole doctorale : Ecole Doctorale Informatique Information et Société

Spécialité : Informatique

Cote B.I.U. - Lyon : T 50/210/19 / et bis

CLASSE :

RESUME :

Un réseau *ad hoc* est une collection de stations communicant au travers d'un lien sans fil sans l'aide d'aucune autre infrastructure ou d'entité centrale. Les réseaux *ad hoc* ont plusieurs applications pratiques incluant les opérations d'urgence ou de secours, les opérations militaires et les réseaux personnels. Durant mes travaux de thèse, je me suis intéressé à plusieurs domaines de recherche dans les réseaux *ad hoc*. J'ai été particulièrement intéressé par la conception, et l'analyse d'algorithmes et de protocoles pour les réseaux sans fil et les réseaux *ad hoc*.

L'un des principaux défis dans la conception de protocoles pour ce type de réseaux est l'accès au médium. Le standard IEEE 802.11 définit un mode appelée DCF (*Distributed Coordination Function*) totalement distribué et qui convient aux réseaux *ad hoc*. Cependant, le protocole MAC (*Medium Access Control*) décrit dans ce standard montre des problèmes d'équité et d'efficacité. L'équité garantit à une station un accès correcte au médium radio, tandis que l'efficacité garantit la bonne utilisation du lien radio. La plupart des solutions existantes fournissent soit l'équité soit l'efficacité.

Mes travaux de recherches se sont articulés autour de deux grand axes. Mon premier axe de recherche est l'évaluation de performance d'algorithmes et de protocoles MAC existants et plus spécialement 802.11. Dans ce travail j'ai mis en évidence les problèmes de performance de 802.11 grâce à un modèle exploitant le formalisme des algèbres de processus stochastiques. Mon second axe de recherche est la conception de nouveaux protocoles MAC équitables et efficaces pour les réseaux *ad hoc* et les réseaux locaux sans fil. Les résultats obtenus dans mon premier axe de recherche m'ont permis de concevoir de tels protocoles MAC. Nos protocoles sont différents de ceux présentés dans la littérature car nous essayons de répondre au compromis équité-efficacité et les solutions que nous proposons sont à la fois équitables et efficaces.

MOTS-CLES : Réseaux *ad hoc*, protocoles MAC, performance, équité, évaluation de performance, 802.11

Laboratoire (s) de recherche : Centre d'Innovations en Télécommunications et Services (CITI)

Directeur de thèse: Pr Isabelle GUERIN LASSOUS

Président de jury : Pr. S. FDIDA

Composition du jury : Pr A. DUDA -- Pr. S. FDIDA -- Pr. I. GUERIN LASSOUS -- Mr. L. REYNAUD -- Pr. D. SIMPLOT-RYL -- Pr. S. UBEDA