

UNIVERSITÉ DE MONTRÉAL

IMPACTS DE L'INTERFÉRENCE
DANS LES RÉSEAUX SANS FIL IEEE 802.11g

RÉGIS DUMONT
DÉPARTEMENT DE GÉNIE INFORMATIQUE
ÉCOLE POLYTECHNIQUE DE MONTRÉAL

MÉMOIRE PRÉSENTÉ EN VUE DE L'OBTENTION
DU DIPLOME DE MAÎTRISE ÈS EN SCIENCES APPLIQUÉES
(GÉNIE INFORMATIQUE)
DÉCEMBRE 2006



Library and
Archives Canada

Bibliothèque et
Archives Canada

Published Heritage
Branch

Direction du
Patrimoine de l'édition

395 Wellington Street
Ottawa ON K1A 0N4
Canada

395, rue Wellington
Ottawa ON K1A 0N4
Canada

Your file Votre référence

ISBN: 978-0-494-25539-1

Our file Notre référence

ISBN: 978-0-494-25539-1

NOTICE:

The author has granted a non-exclusive license allowing Library and Archives Canada to reproduce, publish, archive, preserve, conserve, communicate to the public by telecommunication or on the Internet, loan, distribute and sell theses worldwide, for commercial or non-commercial purposes, in microform, paper, electronic and/or any other formats.

The author retains copyright ownership and moral rights in this thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without the author's permission.

AVIS:

L'auteur a accordé une licence non exclusive permettant à la Bibliothèque et Archives Canada de reproduire, publier, archiver, sauvegarder, conserver, transmettre au public par télécommunication ou par l'Internet, prêter, distribuer et vendre des thèses partout dans le monde, à des fins commerciales ou autres, sur support microforme, papier, électronique et/ou autres formats.

L'auteur conserve la propriété du droit d'auteur et des droits moraux qui protègent cette thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.

In compliance with the Canadian Privacy Act some supporting forms may have been removed from this thesis.

Conformément à la loi canadienne sur la protection de la vie privée, quelques formulaires secondaires ont été enlevés de cette thèse.

While these forms may be included in the document page count, their removal does not represent any loss of content from the thesis.

Bien que ces formulaires aient inclus dans la pagination, il n'y aura aucun contenu manquant.


Canada

UNIVERSITÉ DE MONTRÉAL

ÉCOLE POLYTECHNIQUE DE MONTRÉAL

Ce mémoire intitulé :

IMPACTS DE L'INTERFÉRENCE
DANS LES RÉSEAUX SANS FIL IEEE 802.11g

présenté par : DUMONT Régis

en vue de l'obtention du diplôme de : Maitrise ès sciences appliquées

a été dûment accepté par le jury d'examen constitué de :

Mme. CHERIET Farida, Ph.D., présidente

M. PIERRE Samuel, Ph.D., membre et directeur de recherche

M. QUINTERO Alejandro, Doct., membre

REMERCIEMENTS

Je tiens à remercier en premier lieu mon directeur de recherche, monsieur Samuel Pierre, professeur au département de génie informatique, pour la qualité de son encadrement et son encouragement. Je souhaite également remercier monsieur Sacha Varone pour sa disponibilité et pour ses suggestions pertinentes.

Je voudrais aussi remercier mes collègues du LARIM pour leurs critiques constructives très appréciées lors de nos échanges sur mon sujet de recherche.

Finalement, je tiens à exprimer ma reconnaissance à mes parents et à ma copine pour leur support et encouragement continuels tout au long de ce travail.

RÉSUMÉ

La norme IEEE 802.11 est un standard mondialement répandu pour les réseaux sans-fil. Il permet à des stations de communiquer entre elles ou avec un point d'accès sur une distance de quelques centaines de mètres. Les spécifications du standard sont définies pour la sous-couche MAC ainsi que la couche physique du modèle OSI. Le débit offert sur les réseaux sans-fil IEEE 802.11 peut être significativement affecté par le nombre limité de canaux disponibles.

Pour offrir une bonne couverture, un déploiement dense est inévitable. Alors qu'il est déjà complexe de gérer l'allocation des fréquences à l'intérieur de son réseau, il faut aussi tenir compte des autres appareils partageant également la même bande de fréquences sans licence. Il peut s'agir d'autres équipements sans-fil IEEE 802.11 ou de tout autre appareil opérant à la même fréquence. La bande ISM dans le 2.4 GHz est particulièrement populaire, ce qui la rend très vulnérable aux interférences. La modélisation ainsi que la caractérisation de l'interférence dans les réseaux sans fil IEEE 802.11g sont abordées dans la présente recherche. L'interférence générée et subie par les équipements IEEE 802.11g est étudiée par une série d'expérimentations réalisées avec de vrais équipements de réseautique sans fil.

L'analyse théorique des canaux du protocole IEEE 802.11g nous indique que les canaux 1, 6 et 11 ne se chevauchent pas et ne doivent donc pas s'interférer entre eux. Les résultats obtenus contredisent cette théorie et indiquent que l'interférence générée par un équipement IEEE 802.11g varie en fonction du manufacturier. Alors que de meilleurs résultats sont obtenus avec des cartes réseaux sans fil hautes gammes, ceux obtenus avec des cartes réseaux sans fil intégrées aux ordinateurs portables sont préoccupants. Ces derniers nous indiquent qu'un équipement opérant au canal 1 peut générer de l'interférence sur tous les canaux à l'exception des canaux 10 et 11. Ces résultats sont alarmants, compte tenu du large déploiement de ces cartes réseaux sans fil, et des réseaux dont les points d'accès utilisent les trois fréquences 1, 6 et 11.

ABSTRACT

The IEEE 802.11 standard is a widespread standard for the wireless networks. It makes it possible for the stations to communicate with each others or with an access point at a distance of a few hundred meters. The bandwidth offered on IEEE 802.11 wireless networks can be significantly affected by the limited number of channels available.

To offer a good coverage, a dense deployment is inevitable. Whereas it is already complex to manage the frequencies allocation inside its network, it is also necessary to take into account the other equipments using unlicensed frequency band. ISM band in the 2.4 GHz is particularly popular, which makes it very vulnerable to interferences.

Modeling as well as the characterization of the interference in the networks without wire IEEE 802.11g are approached in the present research. The interference generated by the IEEE 802.11g equipment is studied by a series of experiments carried out with real wireless network equipment. The theoretical analysis of the channels of IEEE 802.11g protocol indicates that channels 1, 6 and 11 do not overlap and do not interfere each other. The results obtained contradict this theory and indicate that the interference generated by IEEE 802.11g equipment varies according to the manufacturer. Whereas better results are obtained with expensive wireless cards, those obtained with wireless cards integrated in laptop computer are alarming. The latter indicate us that equipment operating at channel 1 can generate interference on all the channels except channels 10 and 11. According to the large deployment of these wireless networks card and networks with access points operating at channels 1, 6 and 11, these results are very interesting.

TABLE DES MATIÈRES

REMERCIEMENTS.....	iv
RÉSUMÉ	v
ABSTRACT.....	vi
TABLES DES MATIÈRES.....	vii
LISTE DES FIGURES	x
LISTE DES TABLEAUX	xii
LISTE DES ANNEXES	xiii
LISTE DES SIGLES ET DES ABRÉVIATIONS	xiv
1 CHAPITRE I: INTRODUCTION	1
1.1 DÉFINITIONS ET CONCEPTS DE BASE.....	1
1.1.1 Introduction aux réseaux locaux sans fil.....	1
1.1.2 Mode de fonctionnement d'un réseau sans fil	2
1.2 ÉLÉMENTS DE LA PROBLÉMATIQUE.....	4
1.3 OBJECTIFS DE LA RECHERCHE	5
1.4 PLAN DU MÉMOIRE.....	5
2 CHAPITRE II : TECHNOLOGIE IEEE 802.11 ET INTERFERENCE ASSOCIÉE	6
2.1 INTRODUCTION AU PROTOCOLE IEEE 802.11	6
2.1.1 La couche physique de IEEE 802.11	8
2.1.2 Sous-couche MAC du IEEE 802.11	9
2.2 ÉTAPES DE CONCEPTION D'UN RÉSEAU IEEE 802.11	11
2.2.1 Zone de couverture	11
2.2.2 Capacité du réseau	12
2.2.3 Nombre de points d'accès pour la zone de couverture	12
2.2.4 Positionnement des points d'accès et puissance d'émission	13
2.2.5 Sélection du canal utilisé par les points d'accès	13
2.2.6 Mesure physique du signal et de la capacité sur le site déployé.....	14

2.3	INTERFÉRENCE DANS LES RÉSEAUX SANS FIL IEEE 802.11	14
2.3.1	Interférence avec d'autres équipements IEEE 802.11	15
2.3.2	Interférence des fours à micro-ondes	18
2.3.3	Bluetooth.....	19
2.3.4	Zigbee	20
2.3.5	Autres technologies utilisant la même bande de fréquences	21
2.4	ALLOCATION DES CANAUX DANS LES RÉSEAUX IEEE 802.11	22
2.4.1	Allocation statique des canaux	23
2.4.2	Allocation dynamique des canaux	26
3	CHAPITRE III : MODÉLISATION ET ALGORITHME	32
3.1	GRAPHE D'INTERFÉRENCE D'UN RÉSEAU SANS FIL IEEE 802.11.....	32
3.2	MISE EN ÉQUATION DES INTERFÉRENCES	33
3.3	RÉSOLUTION DU SYSTÈME D'ÉQUATIONS D'INTERFÉRENCE	36
3.3.1	Résolution du système surdimensionné au sens des moindres carrés	37
3.3.2	Résolution d'une inconnue du système à la fois.....	42
3.4	UTILISATION DU GRAPHE D'INTERFÉRENCE POUR LA GESTION DES CANAUX DES RÉSEAUX SANS FIL	44
4	CHAPITRE IV : RÉSULTATS D'EXPÉRIMENTATION ET DE SIMULATION	46
4.1	ENVIRONNEMENT D'EXPÉRIMENTATION	46
4.1.1	Structure de la MIB IEEE 802.11	47
4.1.2	Scénarios expérimentaux permettant l'étude de l'interférence.....	50
4.2	PRÉSENTATION DES RÉSULTATS D'EXPÉRIMENTATION.....	54
4.3	ANALYSE DE L'INTERFÉRENCE OBSERVÉE LORS DE L'EXPÉRIMENTATION.....	62
4.4	ENVIRONNEMENT DE SIMULATION	68
4.5	RÉSULTATS ET ANALYSE DES SIMULATIONS.....	69
4.6	COMPARAISON DES RÉSULTATS PRATIQUES ET SIMULÉS	74
5	CHAPITRE V : CONCLUSION.....	76
5.1	SYNTHÈSE DES TRAVAUX.....	76

5.2	LIMITATIONS DES TRAVAUX.....	77
5.3	TRAVAUX FUTURS.....	78
BIBLIOGRAPHIE		79
ANNEXES		84

LISTE DES FIGURES

Figure 1.1 Pile de protocoles 802.11	2
Figure 1.2 Réseau opérant en mode ad hoc	2
Figure 1.3 Réseau opérant en mode infrastructure	3
Figure 2.1 Composantes d'un réseau 802.11	6
Figure 2.2 Le problème de la station cachée	11
Figure 2.3 Spectre du 802.11b/g.....	15
Figure 2.4 Interférence résultant d'un point d'accès en panne	27
Figure 3.1 Graphe d'interférence d'un réseau sans fil.....	33
Figure 3.2 Interférent potentiel pour le point d'accès #1	42
Figure 4.1 Structure de la MIB du protocole IEEE 802.11 [7].....	48
Figure 4.2 Architecture réseau pour le scénario 1	51
Figure 4.3 Architecture réseau pour le scénario 2	52
Figure 4.4 Architecture réseau pour le scénario 3	53
Figure 4.5 Débit maximal d'une station IEEE 802.11g en fonction du canal d'opération	55
Figure 4.6 Débit lorsque deux PA et stations communiquent avec le PA ayant le signal le plus fort.....	56
Figure 4.7 Répercussion de l'interférence générée sur les valeurs des OID.....	57
Figure 4.8 Débits obtenus lorsqu'un point d'accès est fixé au canal 1	58
Figure 4.9 Taux d'erreur de trame en fonction du canal d'opération du PA 1	59
Figure 4.10 Débit du point d'accès en fonction du canal d'opération (carte PCMCIA Cisco).....	60
Figure 4.11 Débit des points d'accès en fonction du canal d'utilisation du PA 1 (Carte PCMCIA Cisco).....	60
Figure 4.12 Taux d'erreur de trame en fonction du canal d'opération du PA 1 (Carte PCMCIA Cisco).....	61

Figure 4.13 Comparaison de la somme des débits de 2 PA canal (i,6) et de 3 PA canal (i,i,6)	68
Figure 4.14 Schéma du scénario à 2 points d'accès sous Opnet	69
Figure 4.15 Valeurs simulées du débit d'un point d'accès en fonction du canal utilisé...	70
Figure 4.16 Débits obtenus par deux PA dont un est fixé au canal 6 (simulation avec OPNET)	71
Figure 4.17 Débits obtenus par deux PA dont un est fixé au canal 1 (simulation avec OPNET)	72
Figure B.1 Interface du programme.....	87
Figure C.1 Création d'un nouveau projet avec Opnet.....	89
Figure C.2 Utilisation du système métrique	90
Figure C.3 Choix des technologies utilisées lors des simulations	90
Figure C.4 Schéma du scénario utilisant 2 points d'accès	91
Figure C.5 Configuration de l'objet "Application Config" (1 ^{ère} partie)	92
Figure C.6 Configuration de l'objet "Application Config" (2 ^e partie)	93
Figure C.7 Configuration de l'objet "Profil Config" (1 ^{ère} partie).....	95
Figure C.8 Configuration de l'objet "Profil Config" (2 ^e partie).....	96
Figure C.9 Configuration des serveurs (1 ^{ère} partie)	97
Figure C.10 Configuration des serveurs (2 ^e partie)	98
Figure C.11 Configuration des stations (1 ^{ère} partie)	99
Figure C.12 Configuration des stations (2 ^e partie)	100
Figure C.13 Configuration de la cueillette de statistiques	101
Figure C.14 Emplacement de l'option "Duplicate scenario"	102
Figure C.15 Écran de configuration pour la gestion des scénarios.....	103

LISTE DES TABLEAUX

Tableau 2.1 Comparaison des couches physiques 802.11	9
Tableau 2.2 Canaux utilisés dans différentes parties du monde	14
Tableau 3.1 Analyse de performances des deux méthodes de résolution.....	41
Tableau 4.1 Débit maximal d'un point d'accès opérant au canal #6	63
Tableau 4.2 Somme des débits de deux points d'accès opérant au canal #6	64
Tableau 4.3 Sommes des débits de trois points d'accès opérant au canal #6.....	65
Tableau 4.4 Données de la somme des débits de 2 PA canal (i,6) et de 3 PA canal (i,i,6)	67

LISTE DES ANNEXES

ANNEXE A : ÉQUIPEMENT UTILISÉ POUR LES DIFFÉRENTS SCÉNARIOS ...	84
ANNEXE B : DESCRIPTION DU PROGRAMME UTILISÉ POUR LES SIMULATIONS	86
ANNEXE C : CONFIGURATION DU LOGICIEL OPNET	89
ANNEXE D : L'ALPHABET IEEE 802.11	104

LISTE DES SIGLES ET DES ABRÉVIATIONS

ACK	Acknowledgement
ASN	Abstract Syntax Notation
BSS	Basic Service Set
BSSID	Basic Service Set Identifier
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance
CTS	Clear To Send
DCF	Distributed Coordination Function
DIFS	DCF Inter Frame Space
DSSS	Direct Sequence Spread Spectrum
ESS	Extended Service Set
ETSI	European Telecommunications Standards Institute
FCC	Federal Communication Commission
FCS	Frame Check Sequence
FHSS	Frequency Hopping Spread Spectrum
FTP	File Transfert Protocol
HR-DSSS	High Rate DSSS
IBSS	Independent Basic Service Set
IC	Industrie Canada
IEEE	Institute of Electrical and Electronic Engineers
ISM	Industrial, Scientific and Medical radio spectrum
LAN	Local Area Network
LLC	Link Layer Control
MAC	Media Access Control
MIB	Management Information Base
MIC	Ministry of Internal Affairs and Communications (Japon)
MIMO	Multiple Input Multiple Output
NAV	Network Allocation Vector

NP	Non Polynomial
OID	Object Identifier
OFDM	Orthogonal Frequency Division Multiplexing
OSI	Open Systems Interconnection
PCMCIA	Personal Computer Memory Card International Association
PDA	Personal Digital Assistant
PCF	Point Coordination Function
RF	Radio Frequency
RFID	Radio Frequency Identification
RTS	Ready To Send
SIFS	Short Inter Frame Space
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
WPP	Wireless Performance Prediction

CHAPITRE I

INTRODUCTION

Depuis quelques années, nous constatons que le monde devient de plus en plus mobile. C'est ce désir de mobilité qui encouragea le développement de nouvelles technologies n'étant plus reliées par les traditionnels fils ou câbles. L'un des premiers grands succès en matière de mobilité est sans aucun doute la téléphonie cellulaire qui est maintenant omniprésente dans nos vies. Cette technologie permet en effet à ses utilisateurs de pouvoir se rejoindre en tout temps et ce, quel que soit l'endroit où ils se trouvent. De nouvelles technologies en matière de réseautique sans fil tentent maintenant d'obtenir des résultats similaires, mais cette fois avec la connectivité à Internet. L'interférence dans ces réseaux sans fil fait l'objet du présent mémoire. Dans ce premier chapitre d'introduction, nous présentons d'abord quelques concepts de base permettant de mieux comprendre les réseaux sans fil. Nous exposons ensuite les éléments de la problématique ainsi que les objectifs de notre recherche

1.1 Définitions et concepts de base

La technologie la plus répandue en matière de réseaux sans fil est celle obéissant à la norme IEEE 802.11. La majorité des équipements conformes au standard IEEE 802.11 sont en mesure de transmettre de l'information sur quelques centaines de mètres dans un environnement ouvert.

1.1.1 Introduction aux réseaux locaux sans fil

Le projet IEEE 802.11 sur les réseaux locaux sans fil (WLAN) fut entamé en 1990 pour être finalement adopté en 1997 [1]. Le standard définit les services et les protocoles de la sous-couche MAC (Medium Access Control) ainsi que la couche physique du modèle OSI à sept couches [2]. Il est transparent au niveau des couches supérieures qui n'ont nullement besoin d'être modifiées pour fonctionner dans un

environnement sans fil. En effet, la norme 802.11 définit des services et des protocoles de la sous-couche MAC fonctionnant avec la sous-couche LLC (Logical Link Control). La Figure 1.1 illustre la pile de protocoles du 802.11.

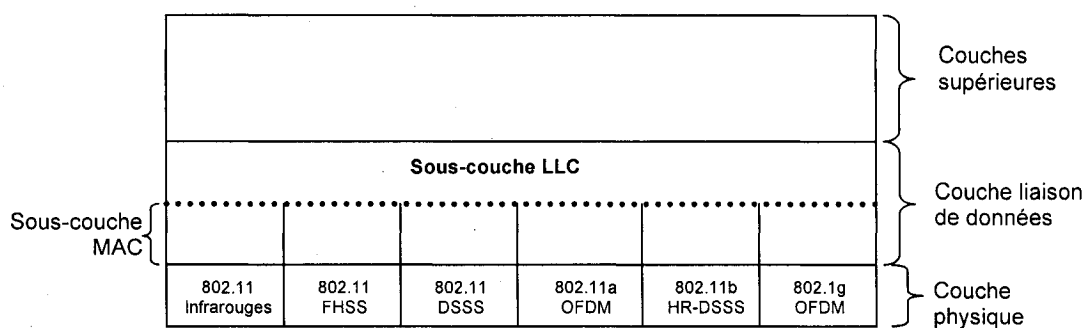


Figure 1.1 Pile de protocoles 802.11

1.1.2 Mode de fonctionnement d'un réseau sans fil

Un ensemble de stations 802.11 opérant dans un réseau sans fil fonctionnel se nomme un BSS (Basic Service Set). Il existe deux types de BSS. Lorsque le BSS n'a pas accès à un autre réseau câblé, on parle d'un BSS indépendant (IBSS). Le IBSS opère en mode ad hoc. Les stations s'échangent directement les informations sans l'intermédiaire d'un point d'accès, comme illustré à la Figure 1.2.

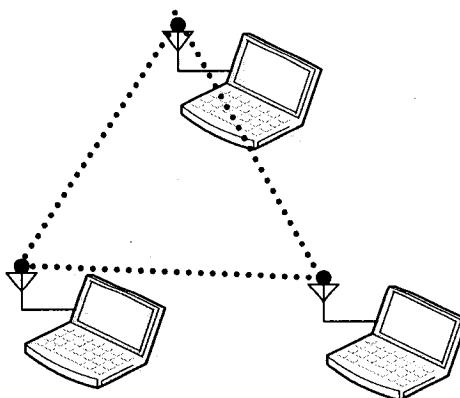


Figure 1.2 Réseau opérant en mode ad hoc

Le mode infrastructure est l'autre type de BSS. Dans un réseau opérant en mode infrastructure, un point d'accès est utilisé pour tous les types de communications. Même les communications entre deux stations appartenant au même BSS passeront à travers le point d'accès où ces deux stations sont associées. Un exemple de réseau sans fil en mode infrastructure est montré à la Figure 1.3.

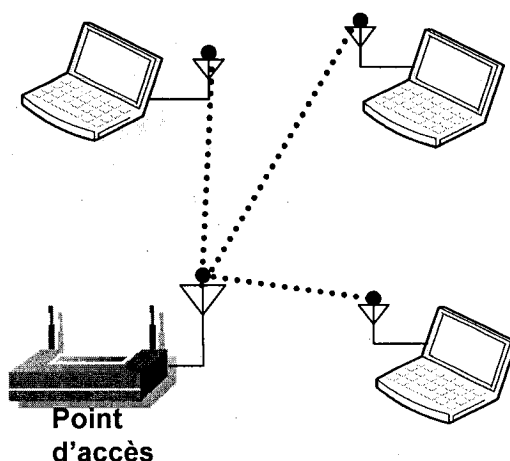


Figure 1.3 Réseau opérant en mode infrastructure

Les réseaux sans fil IEEE 802.11b/g utilisent la bande de fréquences comprise entre 2400 et 2485 MHz. Cette plage est constituée de 14 canaux occupant chacun une largeur de bande de 22 MHz. Pour chacun des pays, l'utilisation de ces canaux est régie par l'autorité gérant le spectre électromagnétique. Au Canada, par exemple, Industrie Canada permet l'utilisation des canaux 1 à 11. Le chevauchement spectral de ces canaux empêche cependant l'utilisation de canaux adjacents. En pratique, des points d'accès situés à faible distance les uns des autres doivent donc utiliser des canaux ayant un écart spectral significatif entre eux.

1.2 Éléments de la problématique

La conception des réseaux sans fil est un exercice qui peut s'avérer complexe à mesure que le réseau déployé grandit. Une des étapes de cette conception représente le choix du canal que chacun des points d'accès du réseau sans fil utilisera. En théorie, les réseaux IEEE 802.11b/g possèdent seulement trois canaux ne se chevauchant pas, alors que la norme IEEE 802.11a en possède 12. Dans un réseau contenant des dizaines ou même des centaines de points d'accès, le choix de la fréquence d'opération des points d'accès doit se faire très judicieusement. Le plan de fréquence de ces grands réseaux n'arrive très souvent pas à éliminer complètement l'interférence. Le but est alors de minimiser cette interférence en ayant une très bonne connaissance de celle-ci.

Le problème d'allocation des canaux dans les réseaux sans fil IEEE 802.11 est NP-complet [3]. Les solutions trouvées à ce problème sont valides uniquement dans le cas où il n'y a aucune source d'interférence autre que les équipements composant le réseau sans fil. Malheureusement, comme on peut s'y attendre dans une bande de fréquences non licenciée, il arrive très souvent que d'autres sources d'interférence viennent altérer les performances de notre réseau. Un choix de fréquences optimal lors de l'implantation d'un réseau peut ainsi perdre de son optimalité à mesure que le réseau évolue et subit des interférences. De plus, un plan de fréquences statique ne tient pas compte du taux d'utilisation des points d'accès. L'interférence engendrée par un point d'accès est proportionnel à son taux d'utilisation. Ainsi, lorsqu'un point d'accès n'émet pas, son impact sur le fonctionnement des points d'accès de son environnement est quasiment nul.

Il serait intéressant d'allouer dynamiquement les canaux en fonction des interférences que subissent les points d'accès. Les points d'accès du réseau devraient, pour ce faire être en mesure de détecter l'interférence qu'ils subissent. La compréhension de l'interférence dans les réseaux sans fil IEEE 802.11, ainsi que son impact sur les performances, sont primordiaux pour la réalisation d'une telle solution.

1.3 Objectifs de la recherche

L'objectif principal de ce mémoire est d'analyser l'interférence présente dans les réseaux sans fil IEEE 802.11, dans la perspective de maximiser le débit global du réseau en y minimisant l'interférence par un choix judicieux des fréquences de fonctionnement des points d'accès. Plus spécifiquement, ce mémoire vise à :

- comprendre le fonctionnement des réseaux sans fil et leurs vulnérabilités aux interférences ;
- modéliser l'interférence des réseaux sans fil IEEE 802.11 par la mise en œuvre de différents scénarios permettant d'analyser l'interférence sur des équipements IEEE 802.11 réels ;
- modéliser à l'aide d'un simulateur l'interférence provoquée et subie par des équipements IEEE 802.11 ;
- analyser les similarités et les incohérences entre le modèle théorique, les résultats expérimentaux ainsi que les résultats simulés.

1.4 Plan du mémoire

Le présent mémoire est constitué de cinq chapitres. Le deuxième chapitre est une revue de littérature sur la problématique de l'interférence dans les réseaux sans fil IEEE 802.11. Le troisième chapitre présente une modélisation de l'interférence dans les réseaux sans fil. Il est suivi du chapitre 4 où des expériences pratiques sur de vrais équipements IEEE 802.11g ainsi que des simulations avec le logiciel Opnet sont effectuées; une analyse des résultats obtenus est également présentée dans ce chapitre. Le chapitre 5, quant à lui, conclut le mémoire en présentant une synthèse des travaux et leurs limitations; nous y indiquons également quelques indications pour des recherches futures.

CHAPITRE II :

TECHNOLOGIE IEEE 802.11 ET INTERFÉRENCE ASSOCIÉE

Les réseaux locaux sans fil IEEE 802.11 utilisent la communication radio pour offrir les mêmes fonctionnalités que les réseaux câblés (LAN). L'avantage est de permettre la mobilité des usagers tout en maintenant une connexion au réseau local ou à Internet. La popularité de cette technologie ne cesse de croître, spécialement depuis qu'elle est intégrée aux ordinateurs portables et aux assistants numériques personnels (PDA). Cette importante utilisation soulève des questionnements et des préoccupations sur l'interférence générée et subie par les équipements communiquant par ce standard. Le présent chapitre débute par une explication du fonctionnement des réseaux sans fil IEEE 802.11 et des principales étapes nécessaires à leur déploiement efficace. Nous poursuivons ensuite par une étude de la problématique de l'interférence pouvant affecter le bon fonctionnement de ces réseaux. Nous terminons en analysant les approches présentées dans la littérature pour gérer l'allocation des canaux dans les réseaux sans fil, une problématique fortement liée à celle de l'interférence.

2.1 Introduction au protocole IEEE 802.11

La Figure 2.1 illustre les différents éléments d'un réseau sans fil de type IEEE 802.11.

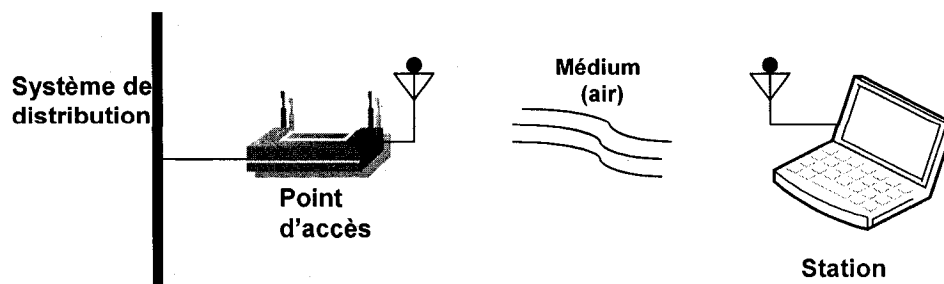


Figure 2.1 Composantes d'un réseau 802.11

Les stations

Les réseaux sans fil sont bâtis afin de permettre aux stations de communiquer entre elles. Les stations sont des composantes informatiques possédant une interface de communication sans fil. Outre les ordinateurs portables et les assistants personnels numériques (PDA), il n'est pas rare de voir des téléphones et même des serveurs posséder des cartes réseau sans fil. En fait, le sans fil peut être avantageux dans tous les cas où il est compliqué ou coûteux d'avoir accès aux méthodes de câblage traditionnelles.

Les points d'accès

Les points d'accès gèrent les stations qui leur sont associées et leur permettent de communiquer. Ils assurent aussi l'interface entre le réseau sans fil et le réseau câblé. Pour rejoindre les équipements réseaux n'utilisant pas d'interface sans fil, on doit convertir les trames 802.11. Ce sont les points d'accès qui assurent cette conversion. Dépendamment de l'équipement utilisé et de sa configuration, un point d'accès peut jouer le rôle d'un routeur ou d'une passerelle.

Le médium sans fil

Pour transmettre les données, IEEE 802.11 utilise un médium sans fil. Il s'agit en fait de la couche physique dont plusieurs implantations ont été définies afin de s'intégrer avec la couche MAC du 802.11.

Système distribué

Lorsque plusieurs points d'accès sont connectés ensemble pour former une large zone de couverture, ils doivent communiquer entre eux pour assurer une continuité de service aux usagers effectuant des déplacements. Le standard ne spécifie pas de technologie précise pour permettre cette fonctionnalité, ce qui laisse un peu de souplesse aux fabricants.

2.1.1 La couche physique de IEEE 802.11

Les réseaux locaux sans fil peuvent fonctionner à différentes fréquences du spectre électromagnétique. Une bande d'ondes infrarouges ainsi que deux bandes de fréquences micro-ondes peuvent être employées dans le protocole IEEE 802.11. L'utilisation des ondes infrarouges est peu répandue dans les produits commerciaux actuels. L'avantage d'utiliser les ondes radios est qu'elles assurent une connexion même dans les situations où il n'y a pas ligne de vue directe entre les appareils. Le principal inconvénient de l'utilisation des ondes radios est leur propagation électromagnétique qui peut créer de l'interférence avec les autres équipements opérant à la même fréquence. Ce problème est particulièrement présent dans les WLAN puisqu'ils utilisent des bandes de fréquences ISM (Industrial, Scientific and Medical) non licenciées. Par exemple, les protocoles 802.11b [4] et 802.11g [5] doivent fonctionner malgré la présence d'autres équipements utilisant la même bande de fréquences, soit la bande ISM de 2,4 à 2,486 Ghz. C'est ainsi que des téléphones sans fil, les appareils utilisant le protocole Bluetooth et même les fours à micro-ondes peuvent influencer négativement le bon fonctionnement des réseaux sans fil.

Comme nous l'avons vu à la Figure 2.1, IEEE 802.11 définit plusieurs types d'implantations au niveau de la couche physique. Un résumé de ces différentes technologies est présenté au Tableau 2.1. Il y a premièrement l'option de transmettre par ondes infrarouges, où des débits de 1 Mbit/s et 2 Mbit/s sont atteints. Cette technique est rarement utilisée à cause de la mauvaise propagation des ondes infrarouges qui ne traversent pas les murs et peuvent être interférées par les rayons du soleil.

Du côté radioélectrique, le standard original, publié en 1997, définissait deux types de couches physiques. La première utilisait l'étalement de spectre par saut de fréquences (FHSS) et la seconde l'étalement de spectre par séquence directe (DSSS). Les débits proposés par ces couches physiques demeurent cependant faibles (1 ou 2 Mbit/s).

L'évolution dans les travaux du groupe IEEE 802.11 a mené à de nouvelles implantations de la couche physique. La norme 802.11a [6], utilisant la technique de

multiplexage orthogonal en répartition de fréquences (OFDM), offre un débit pouvant atteindre 54 Mbit/s. Ce standard est paru en 2000 et utilise la bande de fréquences ISM dans les 5 GHz.

Le 802.11b fut standardisé en 2001 et utilise l'étalement de spectre à haut débit par séquence directe (HR-DSSS). Ce standard peut atteindre un débit de 11 Mbit/s et opère dans la bande de fréquences de 2.4 GHz. Moins rapide que le 802.11a, sa portée est toutefois sept fois plus grande, ce qui lui procure un avantage certain.

Le dernier de la liste, le 802.11g est en fait une version améliorée du 802.11b. Ce standard utilise la même technique de modulation que le 802.11a, soit le OFDM et peut atteindre un débit théorique de 54 Mbit/s. Ce standard a l'avantage d'être rétro compatible avec la norme 802.11b.

Tableau 2.1 Comparaison des couches physiques 802.11

Standard IEEE	Encodage	Bande de fréquences	Vitesse
802.11	FHSS ou DSSS	2.4 GHz	1, 2 Mbit/s
802.11a	OFDM	5 Ghz	Jusqu'à 54 Mbit/s
802.11b	HR-DSSS	2.4 GHz	1, 2, 5.5, 11 Mbit/s
802.11g	OFDM	2.4 GHz	Jusqu'à 54 Mbit/s

2.1.2 Sous-couche MAC du IEEE 802.11

Le protocole de la sous-couche MAC du modèle 802.11 est complètement différent de celui d'Ethernet. Cette différence résulte de la complexité de l'environnement sans fil par rapport au système filaire conventionnel. Le rôle de la sous-couche MAC est d'assumer la transmission fiable des données, de contrôler l'accès au réseau sans fil et d'assurer la protection des données échangées.

Le protocole de la sous-couche MAC du IEEE 802.11 transmet ses trames et attend de recevoir un accusé de réception (ACK) pour chacune d'entre elles, ce qui est

différent du CSMA/CD conventionnel. Si l'accusé de réception n'est pas reçu après un certain temps, la retransmission de la trame est initiée par la station émettrice.

Deux modes de fonctionnement sont possibles pour le contrôle de l'accès au réseau sans fil. La fonction de coordination distribuée (DCF) ne fait appel à aucune entité de contrôle centralisée et doit obligatoirement être supportée par toutes les implantations de la norme IEEE 802.11. L'autre mode de fonctionnement est l'utilisation de la fonction de coordination par point d'accès (PCF). Dans ce mode qui n'est pas obligatoirement supporté par tous les équipements sans fil de la norme 802.11, c'est le point d'accès qui contrôle l'activité de toute la cellule.

Lorsqu'il opère en mode DCF, ce qui est normalement le cas, IEEE 802.11 utilise le CSMA avec évitement de collision (CSMA/CA). Ce protocole régit deux formes d'écoute, une pour le canal physique et l'autre pour un canal virtuel. Si l'un de ces deux canaux indique que le médium est occupé, la sous-couche MAC le rapporte immédiatement aux couches supérieures. Le canal virtuel est connu sous le nom de signal d'allocation de réseau (NAV). Pendant la durée de la transmission, le NAV indique à toutes les stations du BSS le temps prévu et réservé par la station qui occupe la ligne. Ce système permet d'éviter toute transmission pendant qu'une station a réservé le médium et d'empêcher ainsi les collisions.

De plus, pour les longues trames, la couche MAC peut ajouter une option plus robuste pour la réservation du médium. Il s'agit d'un échange de trame, entre les stations émettrice et réceptrice indiquant à l'ensemble du BSS qu'une station veut transmettre. Cet échange porte le nom de RTS/CTS (Request to Send/Clear to Send). Cette procédure est utile pour résoudre le problème de la station cachée présenté à la Figure 2.2.

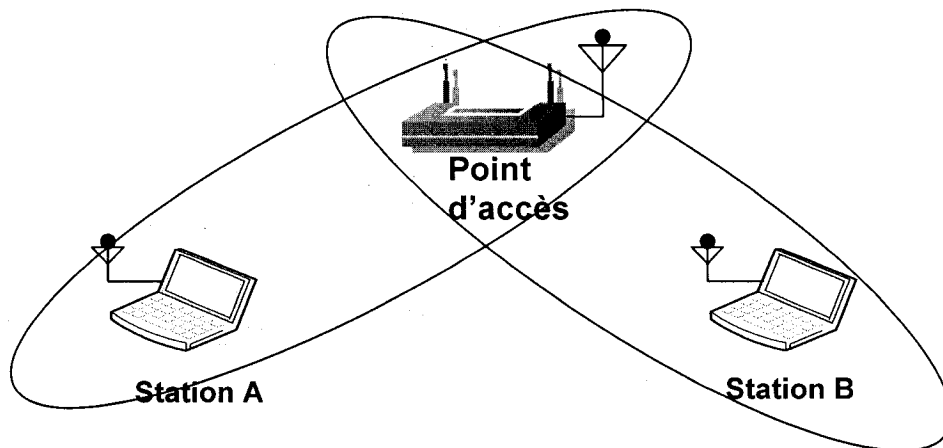


Figure 2.2 Le problème de la station cachée

Comme on le voit, les stations A et B peuvent rejoindre le point d'accès mais sont hors de portée l'une de l'autre. Ainsi la station B ne détecte pas d'activité lorsque la station A transmet. En utilisant la combinaison RTS/CTS, la station sera mise au courant qu'une station veut émettre par la trame CTS qu'elle recevra du point d'accès.

2.2 Étapes de conception d'un réseau IEEE 802.11

La problématique de gestion de l'interférence dans un réseau IEEE 802.11 s'inscrit dans un processus plus général de conception de réseau sans fil. Tous les gestionnaires de réseau sans fil doivent systématiquement cheminer à travers ces étapes pour créer un réseau fonctionnel et efficace.

2.2.1 Zone de couverture

La première étape de tout déploiement de réseau sans fil consiste à définir les zones où une couverture est nécessaire. Il est par exemple possible de choisir de couvrir certaines zones en particulier comme les salles de réunion ou un lobby. Il est maintenant aussi répandu de voir des entreprises désirer étendre leur réseau sans fil partout à

l'intérieur des édifices leur appartenant. Dans ce cas, il est très important d'apporter une attention particulière afin que le réseau sans fil se propage le moins possible en dehors des édifices pour une question évidente de sécurité.

2.2.2 Capacité du réseau

Une fois la zone de couverture déterminée, la capacité nécessaire doit être estimée. La capacité est fonction du nombre d'utilisateurs qui utilisent le réseau ainsi que de leur type d'utilisation. Ainsi, un utilisateur de services comme FTP nécessite une bande passante plus élevée qu'un usager surfant sur le web. La capacité nécessaire pour une zone donnée influence le nombre de points d'accès installés et même la technologie utilisée. On peut en effet favoriser le déploiement d'équipements IEEE 802.11a dans les zones de forte demande en capacité. Ceux-ci ont un rayon de couverture plus petit permettant ainsi de rapprocher les points d'accès les uns des autres et d'améliorer le ratio signal à bruit. Avec de faibles rayons de couverture, on obtient en général un taux de transfert plus intéressant entre les clients et les points d'accès.

2.2.3 Nombre de points d'accès pour la zone de couverture

Outre la capacité nécessaire, la zone de couverture peut aussi avoir une influence sur le nombre de points d'accès à mettre en service. Dans les zones où la capacité nécessaire est faible, le nombre de points d'accès est en effet fixé en fonction de la zone de couverture. Le nombre de points d'accès nécessaires peut alors être estimé par l'équation suivante :

$$N_{PA} = \frac{C_{Totale}}{C_{PA}} \quad (2.1)$$

où N_{PA} est le nombre de points d'accès requis pour la zone, C_{Totale} est la couverture totale de la zone, et C_{PA} est la couverture obtenue à l'aide d'un point d'accès émettant à sa puissance maximale.

2.2.4 Positionnement des points d'accès et puissance d'émission

Le positionnement des points d'accès est une tâche fastidieuse et elle dépend d'un grand nombre de facteurs. À l'intérieur d'un édifice, il n'est pas toujours possible de placer les points d'accès aux endroits optimums. Il est aussi très difficile de prévoir la propagation des ondes radioélectriques puisque celle-ci dépend de l'arrangement physique des lieux. D'excellentes notions de propagation d'ondes électromagnétiques sont nécessaires pour prédire la couverture offerte par un point d'accès. Pour plusieurs grandes entreprises, le nombre de points d'accès nécessaires est très grand, rendant la tâche de choisir l'emplacement de ceux-ci très complexe. Beaucoup de recherches s'effectuent sur le sujet pour tenter d'automatiser le processus de placement des points d'accès. La majorité des algorithmes proposés traitent uniquement le problème de la couverture sans tenir compte de la capacité nécessaire. Un problème connexe au positionnement des points d'accès est le choix de leur puissance d'émission. Une puissance élevée augmente la zone de couverture mais peut également résulter à l'augmentation de l'interférence sur les cellules voisines.

2.2.5 Sélection du canal utilisé par les points d'accès

Le but de l'allocation des canaux est de réduire l'interférence entre les différentes cellules se trouvant à portée l'une de l'autre. Le nombre de canaux disponibles dépend de la technologie utilisée. Ainsi, il y a 3 canaux qui ne se chevauchent pas dans les standards IEEE 802.11b et IEEE 802.11g, alors que le standard IEEE 802.11a en possède 12. Comme ils n'utilisent pas la même bande de fréquences, les standards IEEE 802.11b/g et IEEE 802.11a peuvent coexister à l'intérieur d'une même cellule. Le problème d'assignation des fréquences devient complexe à mesure que le nombre de cellules augmente et que leur zone de couverture est irrégulière.

2.2.6 Mesure physique du signal et de la capacité sur le site déployé

Une fois toutes les précédentes étapes complétées, il reste à valider tout le déploiement en mesurant la qualité de notre réseau. Cette étape consiste à parcourir le réseau pour s'assurer que la couverture, ainsi que la capacité disponible, rencontrent les attentes. Si des trous de couvertures sont découverts, la situation est immédiatement corrigée en changeant des paramètres dans le système. Il est alors possible de changer la puissance d'émission d'un point d'accès, de changer de type d'antenne ou même d'ajouter un nouveau point d'accès. Le modèle obtenu par simulation avant le déploiement peut rapidement ne plus être représentatif de l'environnement réel. Les changements apportés au réseau viennent également invalider le modèle de propagation initial.

2.3 Interférence dans les réseaux sans fil IEEE 802.11

Les normes 802.11b et 802.11g fonctionnent toutes les deux dans la bande de fréquences ISM de 2.4 Ghz. Le Tableau 2.2 [7] présente de façon plus précise la bande de fréquences allouée au WLAN pour différentes parties du monde.

Tableau 2.2 Canaux utilisés dans différentes parties du monde

Domaine de régulation	Canaux et bandes alloués
États-Unis (FCC) et Canada (IC)	1 à 11 (2.412 à 2.462 GHz)
Europe, excluant l'Espagne (ETSI)	1 à 13 (2.412 à 2.472 GHz)
Espagne	10 et 11 (2.457 à 2.462 GHz)
Japon (MIC)	1 à 13 (2.412 à 2.472 GHz) et 14 (2.484 GHz)

Les canaux sont espacés de 5 MHz entre eux. Cependant, l'énergie d'un canal s'étend sur une largeur de bande de 22 MHz. Les 13 canaux de la bande ISM se chevauchent donc comme illustré à la Figure 2.3 :

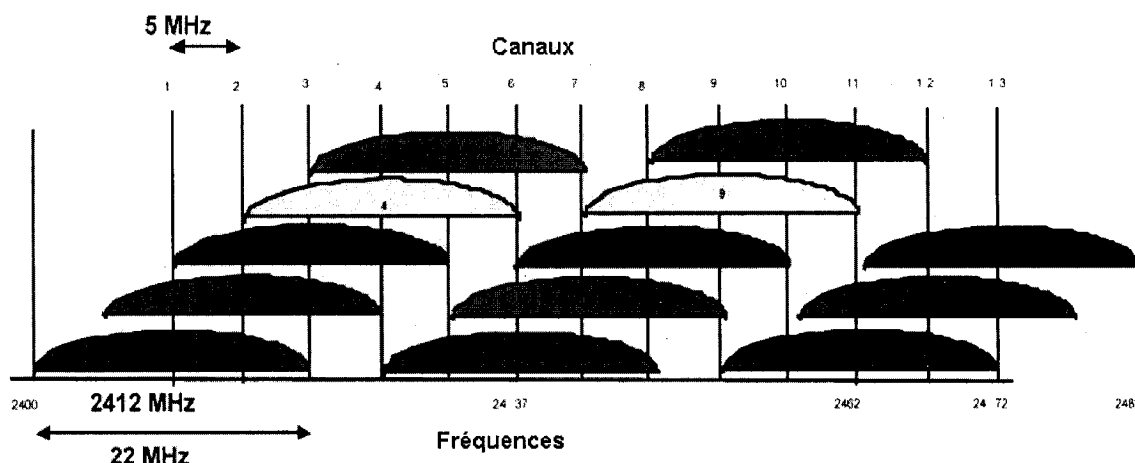


Figure 2.3 Spectre du 802.11b/g

On remarque qu'il est impossible d'avoir plus de trois canaux ne se chevauchant pas. Dans la pratique, on utilise souvent les canaux 1, 6 et 11 qui sont disponibles dans la majorité des pays du monde.

La norme IEEE 802.11a utilise quant à elle une bande de fréquences ISM dans le 5 GHz. Encore une fois, les organismes de régulation décident des fréquences utilisées dans les différents pays. Pour le Canada et les États-Unis, 12 canaux peuvent être alloués. Ces canaux ont une largeur de 20 MHz et ont l'avantage de ne pas se chevaucher.

En plus d'avoir une bande passante limitée, les réseaux IEEE 802.11 doivent partager cette bande ISM avec d'autres systèmes. Cette section explique de quelle façon les réseaux sans fil peuvent être affectés et coexistent avec d'autres équipements opérant aux mêmes fréquences.

2.3.1 Interférence avec d'autres équipements IEEE 802.11

La source d'interférence la plus importante dans les réseaux sans fil est sans aucun doute les autres équipements IEEE 802.11. Le nombre limité de canaux ne se chevauchant pas étant limité, la réutilisation fréquente de ces canaux est donc nécessaire.

Bien que la théorie nous indique un écart entre canaux à respecter afin d'éviter l'interférence, peu d'expérimentations ont été réalisées pour étudier les conséquences du non respect de cette recommandation. Il est intéressant de connaître l'ampleur de l'interférence générée en fonction du canal d'opération des équipements IEEE 802.11. Paruchuri [8] s'intéresse à l'auto-interférence des équipements IEEE 802.11b. Il présente une série de résultats obtenus par expérimentation avec des équipements réseau sans fil dans une chambre anéchoïque. Une chambre anéchoïque est une salle dont les murs et le plafond sont totalement absorbants aux ondes sonores ou électromagnétiques. Aucun écho ou réflexion ne peuvent perturber les mesures. Les mesures sont également immunisées par les interférences extérieures de la chambre. L'utilisation d'une telle chambre a cependant l'inconvénient d'offrir un environnement de test différent de l'environnement où les équipements réseau sans fil ont l'habitude de fonctionner. En effet, dans un réseau sans fil réel, les équipements sont affectés par les réflexions et l'affaiblissement multi chemins (multipath fading) ce qui n'est pas le cas dans la chambre anéchoïque. Le scénario expérimental consiste à la génération de deux flots de communication IEEE 802.11b. L'auteur mesure l'influence du deuxième flot sur le débit du premier. Le canal d'opération du flot interférent demeure constant alors que celui du premier varie. Les résultats obtenus montrent premièrement qu'aucune interférence n'est mesurée lorsqu'un écart de 5 canaux ou plus est respecté. L'interférence est cependant bien présente si l'on ne respecte pas cet écart. Un résultat inattendu est observé lorsque les deux flots de communication utilisent des canaux adjacents. Effectivement, c'est à cette situation que l'interférence mesurée est la plus élevée, dépassant le niveau atteint lorsque tous les équipements opèrent au même canal. Il aurait été intéressant que l'auteur répète ses expérimentations avec des équipements IEEE 802.11g. La technique de modulation OFDM utilisée par ce standard pourrait modifier l'influence qu'ont les équipements les uns sur les autres.

Il serait logique de penser que les problèmes liés à l'interférence entre équipement IEEE 802.11 peuvent être résolus par un choix judicieux des canaux d'opération. En effet, pour un réseau donné, le gestionnaire contrôle l'affectation des

canaux à chacun des points d'accès en opération. Malheureusement, il peut arriver qu'une station ou un point d'accès ne faisant pas partie de ce réseau vienne interférer. Il peut s'agir de deux personnes se connectant ensemble en mode ad hoc ou encore d'un employé installant un point d'accès sans autorisation dans son bureau. Si ces équipements non désirés utilisent un même canal qu'un point d'accès du réseau, ceux-ci occasionneront une interférence majeure et la qualité du canal de communication sera de beaucoup détériorée.

En plus de ces situations d'interférence, les performances des équipements IEEE 802.11g sont influencées par le type de stations sans fil constituant le réseau. Il ne s'agit pas d'interférence mais bien d'une façon de cohabiter avec les stations IEEE 802.11b moins performantes. Vassis dans son article [9], explique très bien ce mode d'opération devant être implanté dans tous les équipements respectant le standard IEEE 802.11g et qui assure l'interopérabilité avec les stations IEEE 802.11b. Les stations IEEE 802.11g utilisent normalement la modulation OFDM pour communiquer. Celle-ci est comprise par les stations IEEE 802.11b. Ces dernières utilisent plutôt la modulation DSSS dont les performances sont inférieures. Pour coexister sur le même réseau, ces technologies doivent être en mesure de se comprendre pour que les différentes réservations du canal soient respectées par toutes les stations. L'approche proposée demande aux équipements IEEE 802.11g d'utiliser les deux techniques de modulation. L'en-tête des trames peut être émis en utilisant la modulation DSSS alors que son contenu est transmis avec la modulation OFDM. Une autre façon de faire est de protéger la transmission de trames OFDM en l'encadrant avec des trames RTS et CTS transmises avec la modulation DSSS. Quelle que soit la technique utilisée, la coexistence d'équipement IEEE 802.11b et IEEE 802.11g a toujours des conséquences néfastes sur les performances des équipements IEEE 802.11g. Bien qu'il ne s'agisse pas d'interférence au sens propre du terme, ce comportement est à considérer lors de la conception d'un réseau sans fil. Dans un déploiement d'un réseau IEEE 802.11g, il pourrait devenir pertinent d'interdire l'accès aux stations IEEE 802.11b, pour optimiser les performances.

2.3.2 Interférence des fours à micro-ondes

Les fours à micro-ondes fonctionnent dans la même bande ISM que les réseaux IEEE 802.11b ou IEEE 802.11g. Prasad [10] expose la problématique dans une section de son article réservée à l'évaluation de performance des réseaux IEEE 802.11. Les fours à micro-ondes fonctionnent à une très grande puissance (~1000W) comparativement aux stations de réseautique sans fil (10-100 mW). Comme la construction de ces fours n'est pas parfaite, une partie des ondes s'échappe et cause des interférences avec les appareils IEEE 802.11. Prasad, dans son article, a effectué une mesure pratique de cette interférence à l'aide d'un four à micro-ondes (Samsung RF-570D). Le four à micro-ondes est placé à 1 mètre de la station IEEE 802.11b, et celle-ci est située à 3 mètres de son point d'accès. L'effet du four à micro-ondes sur le débit du réseau sans fil est considérable. Ainsi, on constate que le débit chute drastiquement lorsque le four à micro-ondes est en marche. Durant son fonctionnement, le four est actif et émet des ondes (2450 MHz – 2458 MHz) durant 8 ms chaque 20 ms (test effectué avec un réseau électrique de 50 cycles par seconde). Pendant cette émission, les stations opérant à une fréquence centrale de 2452 MHz sont complètement bloquées. Lorsque le four à micro-ondes est en marche mais dans un état inactif (12 ms à chaque 20 ms), la station et le point d'accès peuvent se rejoindre. Les trames peuvent alors être reçues correctement si elles sont transmises en totalité durant la période d'inactivité du four. L'expérience a montré que peu de trames réussissaient à être transmises. D'où la diminution du débit de près de 75%.

Un autre article [11] s'intéresse aux interférences des fours à micro-ondes sur les réseaux sans fil IEEE 802.11g. Miyamoto, l'auteur, analyse deux scénarios où un four à micro-ondes influence le fonctionnement d'équipements IEEE 802.11g. Dans le premier scénario, on suppose que le four à micro-ondes est placé à proximité de la station émettrice IEEE 802.11g. La baisse de performance calculée est alors de 40%, correspondant au temps où le four à micro-ondes est actif (8 ms sur 20 ms). Dans cette période où le four est actif, la station sans fil voulant émettre perçoit le canal comme occupé et retarde sa transmission. L'autre scénario consiste à placer la source

d'interférence (le four) près de la station réceptrice. Nous constatons alors que le débit utile de la station réceptrice est fortement influencé par le fonctionnement du four à micro-ondes. Cette influence est cependant variable en fonction du ratio signal/bruit mesuré par la station. Ainsi, un ratio signal/bruit élevé peut réussir à annuler l'influence négative sur le débit de la source d'interférence.

2.3.3 Bluetooth

Bluetooth est une spécification de l'industrie des télécommunications standardisée par l'IEEE [12]. Elle est conçue pour simplifier les connexions entre les appareils électroniques en utilisant une technologie radio courte distance. L'idée première derrière le développement de cette technologie est de remplacer les câbles entre les ordinateurs et les imprimantes, les scanners, les souris, les téléphones portables, et autres appareils similaires. La technologie Bluetooth utilise également la même bande ISM que les réseaux IEEE 802.11b/g. Bluetooth utilise l'une des techniques de modulation utilisée dans les réseaux sans fil, soit la répartition de spectre par sauts de fréquence (FHSS). À chaque instant dans le temps, la largeur de bande du signal Bluetooth est de 1 MHz. Ce signal change cependant de porteuse 1600 fois par seconde en choisissant aléatoirement un des 79 canaux disponibles. Bluetooth génère ainsi de l'énergie dans toute la bande de fréquences ISM qu'utilisent les standards IEEE 802.11b/g. La puissance de la majorité des équipements Bluetooth est cependant limitée à 1mW, ce qui limite l'interférence qu'ils peuvent apporter sur un réseau sans fil IEEE 802.11. Cette interférence est toutefois suffisante pour qu'on en mesure l'impact sur les performances des équipements de réseaux sans fil IEEE 802.11. Shuaib [13], dans son article, analyse l'influence de la coexistence d'équipements Bluetooth et d'équipements IEEE 802.11g sur les performances de ces derniers. L'auteur présente dans cet article une série de résultats pratiques issus d'expérimentations réalisées avec des équipements IEEE 802.11b, IEEE 802.11g et Bluetooth. Les résultats nous indiquent que le protocole IEEE 802.11g est moins sensible que le protocole IEEE 802.11b à l'interférence générée

par les équipements Bluetooth. En situation d'interférence, la diminution du débit moyen d'une station IEEE 802.11b atteint 38% alors que cette diminution est d'environ 22% pour l'équipement IEEE 802.11g.

Si les deux technologies doivent coexister dans un même environnement, il faudra aussi considérer l'interférence occasionnée sur les équipements Bluetooth par les équipements IEEE 802.11. Zeadally [14], s'intéresse justement à la problématique de la performance des équipements Bluetooth subissant de l'interférence. La proposition développée par l'auteur double le débit utile des équipements Bluetooth interféré par la technologie IEEE 802.11. Ce résultat est obtenu en modifiant dynamiquement la taille des paquets échangés en fonction de la qualité du médium.

L'IEEE étant conscient des difficultés de la coexistence de Bluetooth avec les autres technologies utilisant la bande ISM dans le 2.4 GHz, un groupe de travail a été formé. Le standard IEEE 802.15.2 [15] émet des recommandations pour faciliter cette coexistence.

2.3.4 Zigbee

ZigBee est un protocole permettant la communication de petites radios, à consommation réduite. Il est basé sur le standard IEEE 802.15.4 pour les réseaux à dimension personnelle (WPAN). Le but de cette technologie est de communiquer sur de courtes distances comme le proposait déjà Bluetooth. La différence se situe au niveau de la simplicité de la technologie utilisée par Zigbee. Cette simplicité lui apporte l'avantage d'être moins cher, en plus de permettre une autonomie de fonctionnement sur pile beaucoup plus longue. Zigbee est tout indiqué pour les environnements embarqués où la consommation est un critère de sélection. Les contrôles industriels, les applications médicales et la domotique résidentielle constituent le marché initialement visé.

Cette technologie étant relativement récente, son déploiement est encore limité. Il n'en reste pas moins que Zigbee partage la même bande de fréquences que les réseaux sans fil IEEE 802.11b et IEEE 802.11g. Sikora [16] s'intéresse à la coexistence de cette

technologie avec les autres utilisateurs de la bande ISM. Les résultats intéressants pour nous sont ceux obtenus lorsque des équipements IEEE 802.11b et IEEE 802.15.4 sont utilisés. La puissance d'émission des équipements IEEE 802.11b étant 30 fois plus élevée que celle des équipements IEEE 802.15.4, ces derniers sont fortement affectés. En fait, lorsque la station IEEE 802.11b transmet sur un canal englobant la largeur de bande du canal IEEE 802.15.4 (5 MHz), 90% des trames IEEE 802.15.4 sont perdues. Les performances du protocole IEEE 802.11b ne sont cependant pas significativement influencées par la présence d'équipement IEEE 802.15.4. L'auteur termine son article en proposant un choix de canaux pour le protocole IEEE 802.15.4 qui minimiserait l'impact du protocole IEEE 802.11b. Ce choix de fréquences suppose cependant que les équipements IEEE 802.11b opèrent aux canaux 1,6 ou 11.

2.3.5 Autres technologies utilisant la même bande de fréquences

Les bandes ISM peuvent être utilisées sans licence, devenant ainsi très attrayantes pour un bon nombre d'applications. Nous avons présenté les technologies les plus répandues et qui sont responsables de la majorité de l'activité observée dans la bande ISM du 2.4 GHz. Un article pertinent de Biggs [17] présente d'ailleurs l'occupation de cette bande de fréquences dans différents environnements visités (café Internet, aéroport, université, hôpital).

Plusieurs autres types d'équipements devant transmettre de l'information le font en utilisant la bande de fréquences ISM :

- téléphone sans fil de maison ;
- radio-étiquettes (RFID) ;
- liaison point à point, etc.

L'interférence que ces technologies peuvent provoquer sur les réseaux sans fil IEEE 802.11 n'a pas été étudiée en détail. Quelques raisons expliquent pourquoi ces technologies ne sont pas perçues comme des menaces au bon fonctionnement du protocole IEEE 802.11. Les téléphones sans fil de maison sont ainsi rarement utilisés

dans des environnements où les réseaux sans fil sont massivement déployés. Les autres équipements n'émettent pas assez fréquemment ou avec suffisamment de puissance pour perturber le fonctionnement d'un réseau sans fil.

2.4 Allocation des canaux dans les réseaux IEEE 802.11

L'interférence rencontrée dans les réseaux sans fil IEEE 802.11 influence grandement la gestion des canaux d'opération à l'intérieur de ceux-ci. Cette section présente l'état de l'art en ce qui concerne la problématique d'affectation des canaux dans les réseaux sans fil.

L'allocation des canaux dans les réseaux sans fil 802.11 s'apparente aux problèmes d'allocation de fréquences dans les réseaux cellulaires. Il est alors permis de se demander pourquoi il n'est pas possible d'appliquer directement les algorithmes développés pour la planification des fréquences dans les réseaux cellulaires. Deux différences importantes sont à noter dans les réseaux sans fil IEEE 802.11. Premièrement, le nombre de fréquences est très limité comparativement aux réseaux cellulaires où il n'est pas rare de voir des centaines de fréquences disponibles. Les algorithmes habitués à travailler avec un grand nombre de fréquences ne peuvent pas fonctionner correctement lorsque le nombre de canaux disponibles est peu élevé. Dans le cas d'un déploiement d'un réseau 802.11b, nous ne disposons que de 3 canaux ne se chevauchant pas.

La deuxième différence importante touche le ratio signal à bruit, celui-ci étant excessivement important dans les réseaux sans fil. En effet, l'encodage utilisé par les technologies 802.11 peut changer en fonction de la qualité du signal entre les deux stations communiquant entre elles. En améliorant ce ratio, il est possible d'utiliser des techniques d'encodage plus efficaces et ainsi obtenir des taux de transfert plus élevés. Dans les réseaux cellulaires, on ne cherche pas à maximiser ce ratio une fois qu'il a atteint la limite permise, puisqu'on utilise toujours la même technique d'encodage.

Dans un réseau sans fil, on cherche à maximiser le débit de données global. L'une des façons d'y arriver est de minimiser le niveau d'interférence à chaque station et point d'accès.

Nous allons maintenant discuter des différentes approches qui ont été explorées pour résoudre le problème d'allocation de canaux. Certaines de ces approches ont été développées pour les réseaux cellulaires et nous verrons comment elles peuvent être adaptées aux réseaux sans fil 802.11. L'allocation des canaux peut se diviser en deux catégories. Elle peut se faire de façon statique lors du design du réseau ou de façon dynamique lorsque le réseau est en fonction.

2.4.1 Allocation statique des canaux

Les méthodes favorisant une allocation statique fixent une fréquence à une zone de couverture. Comme le 802.11b/g possède seulement 3 canaux ne se chevauchant pas, il n'est pas possible d'avoir une grande variation dans l'assignation des canaux. Pour le 802.11a cependant, il y a 12 canaux disponibles, ce qui permet de mieux tirer partie des techniques d'optimisation statique d'allocation de fréquences. Plusieurs heuristiques ont été proposées pour résoudre le problème d'allocation des fréquences.

2.4.1.1 Coloriage de graphe

Dans un graphe d'interférence, chaque point d'accès est représenté par un nœud. Un arc est alors ajouté entre deux points d'accès si ceux-ci ont la possibilité de s'interférer. Une couleur est alors associée à chacun des nœuds de manière à ce que deux nœuds reliés par un arc possèdent des couleurs différentes. Physiquement, cette assignation de couleurs représente l'allocation d'une fréquence au point d'accès en tenant compte des contraintes d'interférence. L'algorithme DSatur est un exemple de coloriage de graphe. Bahri [18] l'utilise pour l'allocation des canaux lors de son design d'un réseau IEEE 802.11a. Il utilise cet algorithme pour l'allocation des canaux alors

qu'il met en œuvre la recherche avec liste Taboue pour optimiser le placement des points d'accès.

2.4.1.2 Descente

Cette technique commence par la génération d'une solution initiale de façon aléatoire ou autre. Cette solution est alors améliorée en explorant son voisinage. Cette façon de faire n'est pas très efficace car il est très facile de rester pris dans un minimum local. Cette inefficacité explique pourquoi la recherche locale n'est pas une technique représentée dans la littérature pour résoudre le problème d'affectation des canaux. Une version modifiée, appelée « recherche locale guidée » est présentée par Voudouris [19]. Cette version modifiée empêche l'algorithme de rester pris dans des minimums locaux et améliore ainsi la qualité des solutions trouvées.

2.4.1.3 Recherche avec liste tabou

La recherche avec liste Tabou est une forme de recherche locale qui permet la prise en compte de solutions qui n'améliorent pas la solution actuelle. Ceci permet de se libérer des minimums locaux. À chaque itération, l'algorithme explore le voisinage de la solution courante afin de trouver la meilleure solution. Un changement de fréquence d'un point d'accès est considéré comme un mouvement. À chaque itération, le mouvement ayant été sélectionné est placé dans une liste Tabou afin d'éviter les cycles.

L'implantation de Bouju [20] de la recherche avec liste Taboue pour l'affectation des fréquences dans les réseaux cellulaires fonctionne de la façon suivante. Une solution initiale est premièrement générée aléatoirement, c'est-à-dire que chaque cellule se voit assigner des fréquences au hasard. À chaque itération, une nouvelle solution est cherchée en explorant le voisinage de la solution courante. Le voisinage d'une solution est limité aux cellules causant le plus d'interférence. L'évaluation des différentes solutions se fait à partir d'une fonction d'évaluation qui mesure le nombre de violations de la contrainte d'interférence. Pour éviter les cycles sur un petit nombre de solutions, une liste Tabou des derniers mouvements est gardée en mémoire.

2.4.1.4 Recuit simulé

L'heuristique du recuit simulé ressemble un peu à la recherche avec liste Tabou. En effet, cette technique permet également d'accepter des solutions n'améliorant pas la meilleure solution courante pour permettre de se sortir de minimums locaux. Zomaya [21] décrit une implantation de la technique du recuit simulé pour l'allocation des fréquences dans un réseau cellulaire. Une solution initiale est premièrement choisie au hasard. Par la suite, à chaque mouvement, nous suivons les étapes suivantes :

- choisir une cellule au hasard ;
- localiser les cellules les plus proches tout en ayant la possibilité d'utiliser les mêmes fréquences que la cellule sélectionnée sans l'interférer (cochannel cells) ;
- parmi les canaux non utilisés dans la cellule sélectionnée, choisir celui qui est le plus utilisé dans les cellules trouvées à l'étape précédente ;
- allouer ce canal à la cellule et en désallouer un au hasard parmi ceux déjà attribués.

Les mouvements sont évalués en fonction du nombre de violations au niveau de l'interférence qu'ils ajoutent ou éliminent. Si un mouvement réduit le nombre de violations d'interférence, il est adopté. Par contre, s'il ajoute des violations d'interférence, il est accepté ou refusé selon le facteur de température. La température initiale ainsi que le facteur de refroidissement est fixé. Au départ, la température est élevée et il y a plus de chances qu'une solution ajoutant de l'interférence soit acceptée. Cependant, à mesure que le processus avance et que la température refroidit, la plupart des mouvements acceptés sont ceux réduisant l'interférence globale. L'algorithme se termine après avoir trouvé une solution sans aucune interférence ou lorsque la température est descendue au-dessous d'une certaine limite.

2.4.1.5 Algorithme génétique

L'algorithme génétique utilise une population de solutions qui sont améliorées en suivant les principes de la théorie de l'évolution. Ainsi les meilleures solutions sont

choisies pour engendrer les générations futures et peuvent aussi subir des mutations et des croisements. Cette approche a été utilisée par Lai et Coghil [22] pour l'allocation des fréquences dans les réseaux cellulaires. On crée alors un chromosome dont les gènes représentent les cellules du réseau de téléphone cellulaire et le code représente la fréquence utilisée dans cette cellule.

Wong [23], utilise les résultats obtenus avec l'algorithme génétique sur l'allocation de canal dans un réseau WLAN comme point de comparaison pour d'autres algorithmes qu'il désire valider.

2.4.2 Allocation dynamique des canaux

Les méthodes précédemment présentées étaient toutes statiques et exécutées lors de la mise en service d'un réseau. Bien qu'elles donnent de bons résultats, ces méthodes ont l'inconvénient de ne pas pouvoir s'adapter aux différents changements de réseau. À chaque fois qu'un changement survient, il faut reprendre le calcul menant à l'allocation des canaux aux différents points d'accès. Malheureusement, ces changements peuvent être nombreux et parfois soudains dans un réseau IEEE 802.11. Il n'est pas rare en effet que l'on doive ajouter un point d'accès au réseau pour répondre à une demande de bande passante grandissante.

Un réseau où l'allocation des canaux est statique est également plus vulnérable aux pannes. Un exemple est présenté à la Figure 2.4 où les points d'accès A et C fonctionnent sur le même canal alors que le point d'accès B se trouve sur un canal différent. Lorsque les 3 points d'accès sont en fonction, la station 802.11 est attachée au point d'accès B et tout fonctionne correctement. Cependant, si le point d'accès B tombe en panne, la station recevra un niveau de signal de même intensité provenant des points d'accès A et C. Comme A et C émettent sur le même canal, la station ne pourra s'associer à l'un des deux sans être considérablement interférée par l'autre. Cette situation où le niveau de service est diminué continuera jusqu'à ce que l'on réactive le point d'accès en panne.

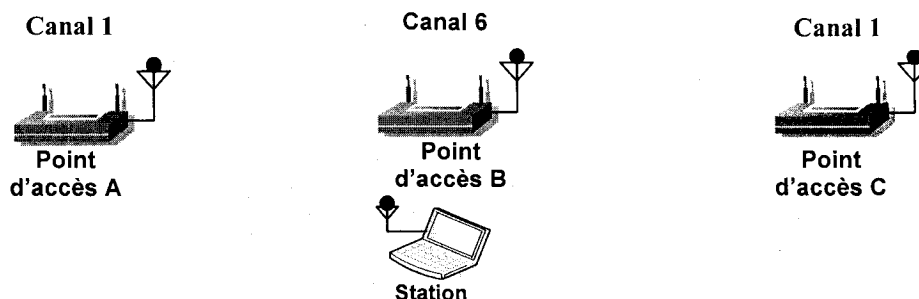


Figure 2.4 Interférence résultant d'un point d'accès en panne

Bien qu'elle occasionne quelques problèmes, la situation que nous venons de présenter est normalement découverte rapidement car elle implique la panne d'un équipement dont nous avons le contrôle. Une autre situation où la planification des canaux statiques n'est pas très efficace est celle qui se produit lorsque le réseau est victime d'une source externe et ponctuelle d'interférence. Comme nous l'avons vu dans la section 2.3, les sources d'interférences peuvent être nombreuses dans la bande de fréquences ISM où fonctionnent les réseaux sans fil IEEE 802.11. Un réseau où l'attribution des canaux aux points d'accès est fixe ne pourra s'adapter à de telles situations d'interférences et subira une dégradation du niveau de service.

L'allocation dynamique des canaux dans un réseau sans fil IEEE 802.11 est une solution attrayante. En effet, on déplace l'intelligence nécessaire à cette allocation au niveau du réseau qui devra faire l'allocation lui-même. Un tel réseau qui gère lui-même l'allocation des canaux utilisés par ses points d'accès pourra mieux s'adapter aux changements de topologie du réseau. Il pourra également tenter de contrer le mieux possible les sources externes d'interférences.

2.4.2.1 Mesure de la qualité du canal utilisé

Pour se gérer lui-même, un réseau doit être en mesure d'évaluer la qualité de son canal de communication. Il est nécessaire de baser cette évaluation sur un certain

nombre de métriques permettant de connaître l'état du lien IEEE 802.11 utilisé. Matsukawa [24] s'est attardé à la recherche d'une métrique pouvant servir à mesurer la dégradation d'un lien IEEE 802.11. Le ratio de paquets retransmis par rapport au nombre total de paquets est vraisemblablement un bon indicateur de la qualité du signal IEEE 802.11. Une augmentation du nombre de retransmission est directement liée à une dégradation du lien. Cette dégradation peut être causée par une augmentation de l'interférence ou d'un canal surchargé où des collisions surviennent.

2.4.2.2 Sélection de la nouvelle fréquence à assigner au point d'accès

Après avoir détecté une dégradation du canal de communication, un réseau où les fréquences sont allouées dynamiquement doit sélectionner une nouvelle fréquence pour le point d'accès interféré. Le but de ce changement de fréquence est d'améliorer le canal de communication. Il est donc important de faire un judicieux choix de fréquence de sorte que le point d'accès subisse moins d'interférences.

Il s'agit d'une problématique intéressante que Tandai [25] tente de résoudre. Dans son article, il propose d'utiliser les stations attachées à chacun des points d'accès pour prendre des mesures de l'activité sur les autres canaux. Ainsi, pendant que les stations n'émettent pas ou sont en attente pour émettre, elles peuvent changer de canal et mesurer le niveau de signal sur ce nouveau canal. Cette information est alors retransmise au point d'accès. Celui-ci traite l'information qu'il reçoit de toutes les stations qui lui sont rattachées. Le point d'accès connaît alors en temps réel l'état d'occupation de tous les canaux. Il peut alors faire un choix intelligent lorsque vient le temps de sélectionner une nouvelle fréquence suite à une augmentation de l'interférence sur le canal courant.

2.4.2.3 Allocation dynamique des canaux dans un réseau IEEE 802.11

Luo [26] nous présente un algorithme de gestion dynamique pour l'allocation des canaux dans un réseau IEEE 802.11. Sa proposition donne à chaque point d'accès la responsabilité de choisir le meilleur canal pour lui. Chaque point d'accès connaît la

topologie du réseau et analyse particulièrement le comportement des points d'accès qui lui sont voisins. Un voisin est un point d'accès dont le signal peut venir interférer la zone de couverture d'un autre point d'accès. Chaque point d'accès diffuse périodiquement le nombre de stations qui lui sont associées. Il décode par la même occasion l'information provenant de ses points d'accès voisins. Le but est alors de faire un choix de fréquence qui maximisera le débit du point d'accès à l'intérieur de son voisinage. L'algorithme de l'auteur utilise les 3 canaux ne se chevauchant pas dans les réseaux IEEE 802.11 b/g. Le canal choisi est celui le moins utilisé par les autres stations dans le voisinage. Toutes les stations effectuent ce même calcul et le plan de fréquence converge assez rapidement. Une faiblesse de cet algorithme se situe selon nous dans la façon dont est mesurée l'utilisation des canaux. En effet, le degré d'occupation d'un canal est basé sur le nombre de stations opérant avec lui. Le débit de données transférées dans les stations n'est ainsi pas pris en compte. Une autre limitation de cet algorithme est qu'il tient compte uniquement de l'équipement constituant le réseau sans fil dont nous avons le contrôle. En effet, les autres sources d'interférence pouvant détériorer les performances du réseau ne sont pas considérées.

Une autre approche a été implémentée par une équipe de chercheurs de Suisse [27]. Cette équipe a développé un moteur de gestion des ressources qu'ils nomment RME (Ressource Management Engine). Le RME a pour but d'optimiser la répartition des canaux radios afin de minimiser les interférences. En minimisant les interférences, on assure les meilleurs débits sur chacun des points d'accès. La gestion de l'algorithme est distribuée afin de faciliter son utilisation dans un réseau contenant un grand nombre de points d'accès. Des agents logiciels sont déployés partout dans le réseau et chacun d'entre eux est responsable de la gestion d'un point d'accès [28]. Un agent est défini par les auteurs de l'article comme étant un logiciel exécutant des tâches spécifiques et possédant un degré d'intelligence qui lui permet de gérer ses tâches de manière autonome et d'interagir avec son environnement de façon appropriée. Les agents interrogent et configurent les points d'accès à l'aide du protocole SNMP (Simple Network Management Protocol). Pour la simulation effectuée, une console de gestion

où la topologie est définie est utilisée. Cette topologie est connue des agents qui déterminent ainsi les autres points d'accès pouvant venir interférer celui qu'ils contrôlent. Les agents ne sont pas en mesure de détecter par eux-mêmes leur environnement, ce qui est une limitation de l'algorithme. Initialement, tous les points d'accès sont configurés pour fonctionner au canal 1. Aucun agent n'a alors le droit de modifier le canal utilisé par un point d'accès. Cette période où les interférences sont nombreuses est utilisée par les agents pour valider les sources d'interférence. Le processus d'optimisation est ensuite libéré. Une dizaine de secondes sont alors suffisantes pour obtenir un état stable où l'interférence est diminuée. Les détails de l'algorithme sont protégés par brevet. Les résultats sont intéressants puisque la diminution de l'interférence résulte en une augmentation du débit entre les stations. L'algorithme travaille uniquement avec l'allocation des canaux pour réduire l'interférence globale et ne touche aucunement à la puissance d'émission des points d'accès. Une gestion intelligente de la puissance d'émission permettrait sans aucun doute d'améliorer les performances obtenues par cet algorithme.

Un autre auteur a manifesté un intérêt pour la gestion dynamique des canaux dans les réseaux sans fil. Ming [29] définit en effet une méthode afin que l'allocation des canaux change automatiquement dans le but de minimiser l'interférence provenant des points d'accès utilisant le même canal (« co-channel interference »). Une diminution de l'interférence globale résulte en une augmentation du débit de données transitant sur le réseau. L'auteur suppose qu'il connaît la configuration du réseau et l'emplacement des différents points d'accès. Il assume également que la couverture des différents points d'accès peut être représentée par des hexagones formant un nid d'abeilles. L'algorithme de cet auteur tient compte du nombre de stations associées aux points d'accès ainsi qu'à leur taux d'occupation. L'avantage de l'algorithme est que ces mesures sont prises en temps réel pour ainsi permettre une bonne allocation de canaux. L'auteur utilise un algorithme qu'il a précédemment développé [30] afin d'estimer le nombre de stations associées à un point d'accès. Il utilise également un autre algorithme développé par un autre auteur [31] pour évaluer la grandeur de la fenêtre de contention

des points d'accès. Un choix de fréquence pour chaque point d'accès peut alors être fait afin de minimiser les interférences avec les points d'accès du voisinage. Cet algorithme assume que les zones de couverture des points d'accès ont une forme d'hexagone formant un nid d'abeilles parfait, ce qui représente une limitation. Cette hypothèse n'est malheureusement pas confirmée en pratique où les réseaux sans fil sont installés dans des endroits où la propagation des ondes est difficilement prévisible. En effet, deux points physiquement près l'un de l'autre peuvent ne pas s'interférer du tout dans le cas où un mur épais les sépare. De plus, cet algorithme ne tient pas compte des sources d'interférence provenant d'éléments externes au réseau. L'algorithme devrait être raffiné avant de pouvoir être implanté efficacement dans un réseau réel.

CHAPITRE III

MODÉLISATION ET ALGORITHME

L'interférence présente dans les réseaux sans fil IEEE 802.11 est proportionnelle à la popularité de ceux-ci et des autres équipements utilisant la même bande de fréquences. Parmi les différents types d'interférence décrits précédemment, nous nous intéressons particulièrement à celle générée par d'autres équipements IEEE 802.11. Dans le présent chapitre, nous présentons un modèle mathématique de l'interférence dans les réseaux sans fil IEEE 802.11. Ce modèle, accompagné d'une détection appropriée de l'interférence, pourrait améliorer l'affectation des canaux dans les réseaux sans fil. Nous présentons également les méthodes de résolutions du système d'équation généré par notre modèle.

3.1 Graphe d'interférence d'un réseau sans fil IEEE 802.11

Lorsqu'un réseau sans fil est mis en service, tous les points d'accès composant ce réseau sont connus. L'interaction entre ces points d'accès n'est cependant pas précisément connue et ceci, même si l'on situe les points d'accès sur un plan. La propagation des ondes dans un édifice où l'on utilise un réseau sans fil est difficilement prévisible puisqu'elle peut être influencée par plusieurs facteurs (murs, plafonds, mouvement des gens, etc.). Nous proposons de bâtir un graphe d'interférence qui est basé sur des valeurs pratiques calculées et non sur un modèle de propagation d'ondes.

Nous définissons un graphe non dirigé $G = (V, E, w)$ où

V = Points d'accès (PA) du réseau sans fil

E = Ensemble des arêtes $[i, j]$ où la transmission ou la réception du PA i peut perturber le fonctionnement du PA j

w = pondération des arêtes représentant l'interférence potentielle entre deux PA

Une illustration d'un tel graphe est présentée à la Figure 3.1

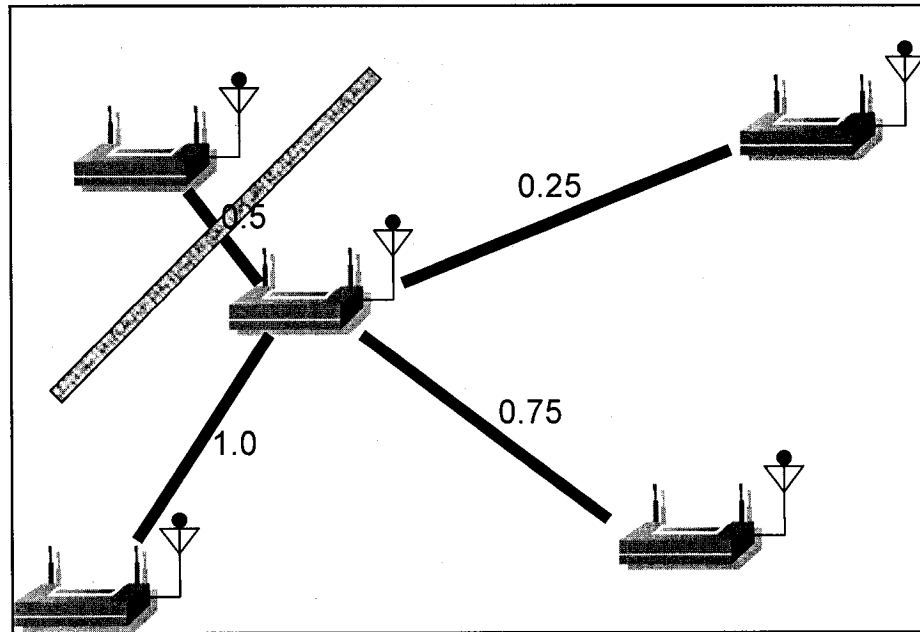


Figure 3.1 Graphe d'interférence d'un réseau sans fil

La pondération de l'interférence varie de 0 à 1. Une valeur de 1 signifie que l'interférence entre ces deux points d'accès est maximale. Cette pondération des arêtes n'est pas connue et doit être calculée à l'aide des autres valeurs mesurées.

3.2 Mise en équation des interférences

La première étape menant à la mise en équation de l'interférence consiste à définir la perturbation maximale provoquée par un point d'accès sur un autre en fonction du canal d'opération de ceux-ci. Deux points d'accès opérant avec des canaux adjacents auront une perturbation maximale plus élevée que dans le cas où l'écart entre les canaux utilisés est élevé. Pour établir cette perturbation maximale, nous mesurons d'abord le débit maximal qu'un point d'accès peut atteindre dans un environnement sans interférence. Nous plaçons ensuite à proximité (quelques mètres) un autre point d'accès

opérant lui aussi à saturation et dont on fait varier le canal d'opération. Nous sommes alors en mesure de constater l'influence de ce dernier sur le débit du premier point d'accès en fonction du canal utilisé. Prenons l'exemple où un point d'accès opérant au canal #1 est interféré par un autre opérant aussi au canal #1. Pour des valeurs fixées et non tirées d'expérimentation, nous obtenons alors :

Débit du point d'accès #1 opérant seul : 20 Mbps

Débit du point d'accès #1 lorsque qu'interféré : 10 Mbps

Débit du point d'accès interférent : 10 Mbps

Perturbation mesurée : 0,5

Cette perturbation mesurée est alors normalisée pour ainsi obtenir la perturbation maximale pour ce canal. Cette normalisation est effectuée de manière à ce que la perturbation maximale soit celle que l'on mesurerait si le point d'accès interférent opérerait à son débit utile maximal. Mathématiquement, nous avons :

$$P_{\text{maximale}} = P_{\text{mesurée}} \cdot \frac{\text{Débit interférent}_{\text{maximal}}}{\text{Débit interférent}_{\text{pratique}}}$$

où

P_{maximale} est la perturbation maximale engendrée par le point d'accès interférent,

$P_{\text{mesurée}}$ est la perturbation mesurée sur le point d'accès lors de l'expérimentation,

Débit interférent_{maximal} est le débit utile maximal du point d'accès interférent,

Débit interférent_{pratique} est le débit du point d'accès interférent lors de l'expérimentation.

Pour l'exemple précédent, la perturbation maximale se calculera donc ainsi :

$$P_{\text{maximale}} = P_{\text{mesurée}} \cdot \frac{\text{Débit interférent}_{\text{maximal}}}{\text{Débit interférent}_{\text{pratique}}}$$

$$P_{\text{maximale}} = 0,5 \cdot \frac{20 \text{ Mbps}}{10 \text{ Mbps}}$$

$$\boxed{P_{\text{maximale}} = 1}$$

Ce qui est la plus haute valeur de P_{maximale} acceptée dans notre modèle. Cela signifie que si un point d'accès interférant avait un débit de 20 Mbps, il paralyserait complètement un autre point d'accès tentant d'opérer au même canal. En pratique, l'interférence est mutuelle et aucun des 2 points d'accès n'atteindra son débit utile maximal. Dans ce modèle, nous faisons l'hypothèse que l'interférence entre deux points d'accès est maximale lorsque ceux-ci opèrent au même canal. Nous assumons également que deux points d'accès opérant au même canal se partagent efficacement celui-ci pour obtenir un débit pratique de 50% inférieur au débit maximal d'un point d'accès. Ces hypothèses seront vérifiées lors de nos expérimentations. Les valeurs des perturbations maximales en fonction de l'écart entre les canaux utilisés nous permettent de bâtir la suite de notre modèle.

Dans un réseau composé uniquement de 2 points d'accès, la perturbation mesurée à un point d'accès sera le produit de la perturbation maximale, du poids de l'arête d'interférence entre les 2 points d'accès ainsi que du taux d'utilisation du point d'accès créant l'interférence.

Mathématiquement, nous avons, pour un point d'accès i avec un voisin j :

$$P_{\text{mesurée}}(i) = P_{\text{maximale}}(i, j) \cdot w(i, j) \cdot u(j) \quad \text{où} \quad (3.1)$$

$P_{\text{mesurée}}(i, j)$ est la perturbation mesurée au point d'accès i $[0, 1]$;

$P_{\text{maximale}}(i, j)$ est la perturbation maximale dépendant des canaux d'opération $[0, 1]$;

$w(i, j)$ est le poids associé à l'influence d'un point d'accès j sur le point d'accès i $[0, 1]$;

$u(j)$ est le taux d'utilisation du point d'accès j $[0, 1]$.

Le poids de l'interférence est l'inconnue de cette équation simple lorsque seulement 2 points d'accès sont impliqués. Les réseaux d'aujourd'hui sont composés de dizaines et même de centaines de points d'accès pouvant générer de l'interférence les uns sur les autres.

En faisant l'hypothèse que l'interférence subie par un point d'accès peut être considérée comme étant la somme des perturbations apportées par les autres points d'accès du réseau, l'équation précédente se généralise alors à celle-ci :

$$P_{\text{mesurée}}(i) = \sum_{j \in N(i)} P_{\text{maximale}}(i, j) \cdot w(i, j) \cdot u(j) \quad (3.2)$$

Le nombre d'inconnues de cette équation, c'est-à-dire le nombre de poids w représentant l'interférence entre deux points d'accès, est fonction du nombre de points d'accès dans le réseau sans fil. De façon plus précise, nous avons :

$$\text{nombre de poids } w = \frac{n \cdot (n - 1)}{2} \quad (3.3)$$

où n = le nombre de points d'accès dans le réseau sans fil

Nous ne pouvons résoudre globalement ce système car le nombre de poids w à trouver est plus élevé que le nombre de mesures de perturbation prise à chacun des points d'accès. L'approche que nous proposons alors est de faire varier le canal d'opération de certains points d'accès et de mesurer à nouveau la perturbation subie par les points d'accès. Nous sommes alors en mesure de générer de nouvelles équations dont les inconnues sont toujours les poids w représentant l'influence d'un point d'accès sur un autre. Le système d'équations ainsi généré est surdimensionné, c'est-à-dire qu'il est composé de plus d'équations que d'inconnues. La section suivante est consacrée à la méthodologie utilisée pour résoudre ce système surdimensionné.

3.3 Résolution du système d'équations d'interférence

Plusieurs méthodes peuvent être utilisées pour résoudre le système d'équations et ainsi déterminer les poids w représentant l'influence des points d'accès les uns sur les autres. Une première approche consiste à résoudre le système dans son ensemble pour

ainsi découvrir simultanément la valeur de tous les poids w . Il est également possible de déterminer un seul poids à la fois en résolvant un système d'équations particulièrement adapté.

3.3.1 Résolution du système surdimensionné au sens des moindres carrés

Le système d'équation à résoudre peut être représenté sous la forme

$$A x = b \quad (3.4)$$

Où la matrice $A \in \mathbb{R}^{m \times n}$ et le vecteur $b \in \mathbb{R}^m$. Le système est surdimensionné et ne possède donc pas de solution unique. On définit alors le vecteur résidu r de la manière suivante :

$$r = b - A x \quad (3.5)$$

Le but est alors de trouver un vecteur solution x qui minimise la taille du vecteur résidu. Une mesure appropriée de la taille de r est la somme du carré de ses composantes, ce qui est équivalent au carré de la norme euclidienne de ce vecteur :

$$\|r\|^2 = r^T \cdot r = \sum_{i=1}^m r_i^2 \quad (3.6)$$

Le vecteur solution x représente la solution au sens des moindres carrés du système surdimensionné. Mathématiquement, nous devons trouver x tel que :

$$x = \min \{r^T \cdot r : r \in \mathbb{R}^n\} = \min \{(b - A y)^T \cdot (b - A y) : y \in \mathbb{R}^n\} \quad (3.7)$$

Le minimum est atteint lorsque le gradient de $(b - A y)^T \cdot (b - A y)$ est nul, soit :

$$\begin{aligned} \nabla \{(b - A y)^T \cdot (b - A y)\} &= 0 \\ \frac{d}{dy} (b^T b - b^T A y - A^T y^T b + A^T y^T A y) &= 0 \Leftrightarrow -2 A^T (b - A y) = 0 \end{aligned} \quad (3.8)$$

En développant cette équation, nous obtenons :

$$(A^T \cdot A) y = A^T b \quad (3.9)$$

L'unique solution de cette équation est aussi la solution du système surdimensionné au sens des moindres carrés. Le vecteur solution x du système initial est alors la solution du système carré ($n \times n$) :

$$(A^T \cdot A)x = A^T b \quad (3.10)$$

Exemple d'application

Trouvons la solution au sens des moindres carrés de l'équation $Ax = b$ où

$$A = \begin{bmatrix} 1 & -2 \\ -1 & 2 \\ 0 & 3 \\ 2 & 5 \end{bmatrix} \quad \text{et} \quad b = \begin{bmatrix} 3 \\ 1 \\ -4 \\ 2 \end{bmatrix}$$

Ce système est surdimensionné puisqu'il est composé de 4 équations et de seulement deux inconnues. La solution au sens des moindres carrés vérifie $(A^T \cdot A)x = A^T b$. Nous avons donc :

$$A^T \cdot A = \begin{bmatrix} 1 & -1 & 0 & 2 \\ -2 & 2 & 3 & 5 \end{bmatrix} \begin{bmatrix} 1 & -2 \\ -1 & 2 \\ 0 & 3 \\ 2 & 5 \end{bmatrix} = \begin{bmatrix} 6 & 6 \\ 6 & 42 \end{bmatrix}$$

Ainsi que,

$$A^T \cdot b = \begin{bmatrix} 1 & -1 & 0 & 2 \\ -2 & 2 & 3 & 5 \end{bmatrix} \begin{bmatrix} 3 \\ 1 \\ -4 \\ 2 \end{bmatrix} = \begin{bmatrix} 6 \\ -6 \end{bmatrix}$$

Il suffit alors de résoudre le système,

$$\begin{bmatrix} 6 & 6 \\ 6 & 42 \end{bmatrix} x = \begin{bmatrix} 6 \\ -6 \end{bmatrix}$$

$$\text{On trouve alors, } x = \begin{bmatrix} 4/3 \\ -1/3 \end{bmatrix}$$

L'erreur associée à cette solution est la norme du vecteur résidu $r = b - Ax$. Pour notre exemple, nous avons :

$$\begin{aligned} \text{erreur} &= \|r\| = \|b - Ax\| \\ \text{erreur} &= \left\| \begin{bmatrix} 3 \\ 1 \\ -4 \\ 2 \end{bmatrix} - \begin{bmatrix} 1 & -2 \\ -1 & 2 \\ 0 & 3 \\ 2 & 5 \end{bmatrix} \begin{bmatrix} 4/3 \\ -1/3 \end{bmatrix} \right\| = \left\| \begin{bmatrix} 3 \\ 1 \\ -4 \\ 2 \end{bmatrix} - \begin{bmatrix} 2 \\ -2 \\ -1 \\ 1 \end{bmatrix} \right\| = \left\| \begin{bmatrix} 1 \\ -3 \\ -3 \\ 1 \end{bmatrix} \right\| \\ \text{erreur} &= \sqrt{1^2 + (-3)^2 + (-3)^2 + 1^2} \\ \boxed{\text{erreur} &= 2\sqrt{5}} \end{aligned}$$

Utilisation de la décomposition QR pour la résolution aux moindres carrés

Une autre méthode peut être utilisée pour obtenir la résolution aux moindres carrés d'un système d'équation. Il s'agit de la décomposition QR. Cette méthode exprime la matrice A sous forme du produit d'une matrice orthogonale Q, par une matrice triangulaire supérieure R :

$$A = Q \cdot R \quad (3.11)$$

Le système devient alors,

$$QRx = b \quad (3.12)$$

En multipliant par Q^T des deux côtés de l'équation, nous obtenons,

$$Q^TQRx = Q^Tb \quad (3.13)$$

Puisque $Q^TQ = I$ (la matrice identité), nous simplifions alors pour obtenir,

$$Rx = Q^Tb \quad (3.14)$$

On résout ce système en tenant compte de la forme triangulaire de la matrice R.

Si nous reprenons l'exemple où nous avons les matrices A et b telles que,

$$A = \begin{bmatrix} 1 & -2 \\ -1 & 2 \\ 0 & 3 \\ 2 & 5 \end{bmatrix} \quad \text{et} \quad b = \begin{bmatrix} 3 \\ 1 \\ -4 \\ 2 \end{bmatrix}$$

Le système à résoudre en utilisant la décomposition QR deviendra :

$$R x = Q^T b \quad \text{où,}$$

$$Q = \begin{bmatrix} -0,41 & 0,5 \\ 0,41 & -0,5 \\ 0 & -0,5 \\ -0,82 & 5 \end{bmatrix} \quad \text{et} \quad R = \begin{bmatrix} -2,45 & -2,45 \\ 0 & -6 \end{bmatrix}$$

Ces deux matrices vérifient bien l'équation $A = Q R$. La décomposition QR a été obtenue par la méthode Householder dont le développement n'est pas présenté ici. Nous poursuivons en calculant le produit :

$$Q^T \cdot b = \begin{bmatrix} -0,41 & 0,41 & 0 & -0,82 \\ 0,5 & -0,5 & -0,5 & -0,5 \end{bmatrix} \begin{bmatrix} 3 \\ 1 \\ -4 \\ 2 \end{bmatrix} = \begin{bmatrix} -2,45 \\ 2 \end{bmatrix}$$

Ce qui nous amène au système simplifié suivant :

$$\begin{bmatrix} -2,45 & -2,45 \\ 0 & -6 \end{bmatrix} x = \begin{bmatrix} -2,45 \\ 2 \end{bmatrix}$$

Comme on peut le voir, la forme triangulaire de la matrice R simplifie la résolution qui peut alors s'effectuer par substitution.

$$\text{On trouve alors : } x = \begin{bmatrix} 4/3 \\ -1/3 \end{bmatrix}$$

Qui est bien le même résultat obtenu avec la méthode précédente.

Comparaison de performance pour la résolution du système d'équations

Afin de choisir laquelle des deux méthodes de résolution allait être implantée dans notre logiciel de gestion de réseaux sans fil, nous avons effectué des tests de performance. Les deux méthodes ont été mises en œuvre en java, puis nous avons recueilli les temps de traitement pour résoudre des systèmes de diverses grandeurs.

Nous avons également recueilli les valeurs du résidu à chaque fois qu'un système était résolu. Plus la valeur du résidu est petite, plus la solution est bonne au sens des moindres carrés. Les matrices A et b ont été générées aléatoirement avec des valeurs situées entre 0 et 1. Nous avons simulé avec des matrices A carrées ainsi que rectangulaires. Une synthèse des résultats obtenus se trouvent au Tableau 3.1. Ces résultats indiquent que la méthode par décomposition QR est généralement plus performante que la méthode résolvant le système $(A^T \cdot A)x = A^T b$. En effet, pour les matrices A carrées, le temps d'exécution ainsi que le résidu du système réduit sont toujours meilleurs avec la méthode utilisant la décomposition QR. Cette méthode ne semble cependant pas la meilleure pour les matrices rectangulaires de grandes tailles où ses performances sont alors diminuées.

Tableau 3.1 Analyse de performances des deux méthodes de résolution

Dimensions de la matrice A (m x n)	Par résolution de $(A^T \cdot A)x = A^T b$		Décomposition QR $Rx = Q^T b$	
	Temps de traitement (ms)	résidu	Temps de traitement (ms)	Résidu
10 x 10	0	$9,3258 \times 10^{-14}$	0	$7,7715 \times 10^{-14}$
50 x 50	16	$5,1688 \times 10^{-12}$	0	$8,5487 \times 10^{-15}$
100 x 100	78	$2,2706 \times 10^{-11}$	16	$1,2989 \times 10^{-14}$
500 x 500	2562	$6,0915 \times 10^{-8}$	1297	$1,3483 \times 10^{-12}$
1000 x 1000	20765	$1,9352 \times 10^{-9}$	13844	$1,1546 \times 10^{-13}$
100 x 10	15	0,6635	0	0,6635
500 x 50	78	0,6227	16	0.6227
1000 x 100	79	0.6134	203	0.6134
1000 x 500	3360	0.5979	3687	0.5979

3.3.2 Résolution d'une inconnue du système à la fois

Une autre méthode peut être utilisée pour trouver les poids représentant l'influence d'un point d'accès sur un autre. Au lieu de résoudre le système dans son ensemble, on propose plutôt d'isoler une seule inconnue pour en connaître la valeur. Prenons par exemple un réseau sans fil composé de cinq points d'accès tel qu'illustré à la Figure 3.2. Seuls les poids associés au point d'accès #1 sont représentés, montrant que celui-ci peut être perturbé par quatre autres points d'accès.

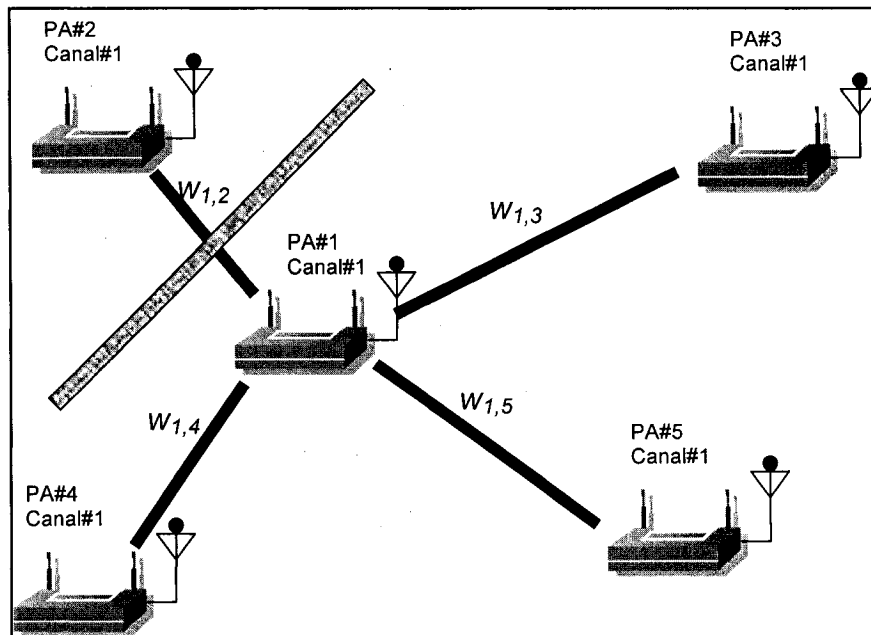


Figure 3.2 Interférant potentiel pour le point d'accès #1

Adaptée de l'équation (3.2), l'équation représentant les perturbations mesurées au point d'accès #1 est :

$$P_{\text{mesurée}}(1) = \sum_{j=2}^4 P_{\text{maximale}}(1, j) \cdot w(1, j) \cdot u(j) \quad (3.11)$$

Cette équation possède quatre inconnues $w(1, j)$ qui ne dépendent pas du canal d'opération des différents points d'accès. Pour isoler un de ces poids, on propose de changer le canal d'opération du point d'accès associé. Par exemple, si nous voulons

trouver le poids $w(1,3)$, nous allons changer le canal d'opération du point d'accès #3. Ce changement de fréquence aura un impact sur la mesure de la perturbation au point d'accès #1 car la valeur $P_{\text{maximale}}(1,3)$ sera alors modifiée. En supposant que les taux d'utilisation $u(j)$ des points d'accès (autre que le point d'accès #3) ne varieront pas pendant ce court intervalle de temps, il est alors facile d'isoler l'inconnue $w(1,3)$. Il s'agit de soustraire l'équation obtenue lorsque le point d'accès #3 opérait au canal #1 de celle obtenue alors que ce dernier opérait à un autre canal. Les autres inconnues s'annulent alors pour nous dévoiler la valeur de $w(1,3)$.

$$P_{\text{mesurée}}(1) \Big|_{\text{PA\#3} \rightarrow \text{ch\#1}} - P_{\text{mesurée}}(1) \Big|_{\text{PA\#3} \rightarrow \text{ch\#6}} = w(1,3) \cdot u(3) \left[P_{\text{maximale}}(1,3) \Big|_{\text{PA\#3} \rightarrow \text{ch\#1}} - P_{\text{maximale}}(1,3) \Big|_{\text{PA\#3} \rightarrow \text{ch\#6}} \right]$$

$$w(1,3) = \frac{P_{\text{mesurée}}(1) \Big|_{\text{PA\#3} \rightarrow \text{ch\#1}} - P_{\text{mesurée}}(1) \Big|_{\text{PA\#3} \rightarrow \text{ch\#6}}}{u(3) \left[P_{\text{maximale}}(1,3) \Big|_{\text{PA\#3} \rightarrow \text{ch\#1}} - P_{\text{maximale}}(1,3) \Big|_{\text{PA\#3} \rightarrow \text{ch\#6}} \right]} \quad (3.12)$$

Nous devons refaire cette manipulation pour chacun des autres poids dont nous voulons trouver la valeur. Un inconvénient à utiliser cette méthodologie pour les poids $w(i,j)$ est qu'elle occasionne un grand nombre de changements de canaux des points d'accès. En fait, le nombre de changements de canaux sera égal au nombre de poids w donné par l'équation 3.3. Bien que les systèmes d'exploitation récents des stations sans fil supportent bien les changements de fréquence, ceux-ci peuvent occasionner des pertes de service de quelques secondes. La plupart des usagers du réseau sans fil ne seront pas affectés par ces courtes pertes de service. Cependant les applications demandant une qualité de services très élevée pourront être durement touchées. C'est le cas de la téléphonie IP qui subira alors une dégradation de la voix et possiblement une coupure de l'appel en cours. Il s'agit d'un inconvénient important qui survient à chaque fois qu'on désire résoudre le système pour obtenir la valeur des poids $w(i,j)$. Cet inconvénient important nous amène à ne pas privilégier cette méthode de résolution. Nous choisissons la méthode résolvant le système dans son ensemble et demandant un nombre limité de changements de canaux.

3.4 Utilisation du graphe d'interférence pour la gestion des canaux des réseaux sans fil

La résolution du graphe d'interférence nous permet d'obtenir une vue précise d'un réseau sans fil. Ce portrait des interférences du réseau est plus pertinent que la simple représentation sur un plan de l'emplacement physique des points d'accès. Le graphe d'interférence tient en effet compte de l'environnement physique où les points d'accès sont installés. Nous proposons d'utiliser ce graphe pour effectuer une gestion dynamique des canaux utilisés par les points d'accès d'un réseau IEEE 802.11

Nous avons vu à la section précédente comment l'on pouvait estimer la perturbation subie par un point d'accès en fonction de son entourage. En effectuant ce calcul pour tous les points d'accès du réseau, nous obtenons le portrait global de l'interférence dans le réseau en fonction des canaux utilisés. Notre but devient alors de minimiser cette interférence globale, ce qui résulte de la fonction objective suivante :

$$\text{Objectif} = \min \sum_i P_{\text{mesurée}}(i) \quad (3.13)$$

Cette fonction tient compte de la perturbation subie par tous les points d'accès du réseau sans fil. Un point d'accès étant fortement perturbé provoquera une hausse de la fonction objective. En pratique, il est cependant possible que ce point d'accès ne desserve aucun client et que sa forte perturbation subie ne diminue en rien la performance du réseau. Pour tenir compte de cette possibilité, nous modifions la fonction objective qui devient :

$$\text{Objectif} = \min \sum_i P_{\text{mesurée}}(i) \cdot A(i) \quad \text{où} \quad (3.14)$$

$P_{\text{mesurée}}(i)$ est la perturbation mesurée au point d'accès i

$A(i)$ est l'activité du point d'accès i

Le paramètre $A(i)$ peut tenir compte à la fois du débit du point d'accès et du nombre de clients associés à ce point d'accès. De cette façon, un point d'accès ayant un débit très faible mais offrant le service à plusieurs clients peut influencer le résultat de la fonction objective. La résolution de la fonction objective nous permet d'obtenir le canal d'utilisation de chacun des points d'accès qui minimise l'interférence globale du système. Dans un réseau réel, cette résolution peut être effectuée à intervalle régulier pour ainsi s'adapter aux comportements des utilisateurs. La tendance sera alors de minimiser la perturbation subie par les points d'accès les plus actifs. Il n'est cependant pas conseillé de résoudre la fonction objective de façon trop fréquente. En effet, cette résolution engendre, la plupart du temps, des changements de canal d'utilisation sur un certain nombre de points d'accès pouvant résulter à des pertes de service chez les clients.

CHAPITRE IV

RÉSULTATS D'EXPÉRIEMENTATIONS ET DE SIMULATIONS

Dans le chapitre précédent, nous avons présenté un modèle mathématique pour l'interférence dans les réseaux sans fil IEEE 802.11. Pour être utilisé, ce modèle demande une compréhension et une analyse approfondie de l'interférence inter-canaux. Une bonne façon d'analyser celle-ci est d'observer son influence sur le fonctionnement d'équipements IEEE 802.11 réels. Ce chapitre expose les détails des expérimentations permettant la validation de certaines caractéristiques de cette interférence. Dans un premier temps, nous décrivons l'environnement pratique dans lequel nous avons effectué nos expérimentations. Les résultats obtenus sont par la suite présentés et analysés. Ce chapitre contient également les détails d'implantation et les résultats obtenus, d'une série de simulations que nous avons effectuée avec le logiciel Opnet.

4.1 *Environnement d'expérimentation*

Les réseaux IEEE 802.11 doivent être en mesure de s'adapter à l'environnement dans lequel ils sont installés. Il est ainsi nécessaire de pouvoir évaluer la qualité d'un lien sans fil qui se comporte très différemment d'un lien filaire. La nature très changeante du médium cause également des fluctuations imprévisibles du débit, rendant les mesures faites sur le réseau difficilement reproductibles.

Le défi de l'évaluation de la qualité d'un réseau IEEE 802.11 est amplifié par le manque de métriques standardisées. En 2004, l'IEEE a formé le groupe 802.11T pour définir des métriques pouvant servir à évaluer les réseaux sans fil. En plus de définir les métriques, ce groupe définira l'environnement dans lequel les différents tests devront être effectués. Les travaux résultants seront très utiles pour les manufacturiers et les consommateurs qui pourront ainsi évaluer les performances de différents équipements en fonction de tests standards.

Bien que le groupe 802.11T n'ait encore spécifié aucune métrique pour l'évaluation des réseaux 802.11, on peut s'attendre à ce que celles-ci soient plus nombreuses que celles définissant la qualité d'un réseau filaire Ethernet. L'environnement sans fil est plus propice à des erreurs de transmission dues principalement au médium (l'air) qui est beaucoup moins fiable qu'un fil de cuivre. La mobilité des usagers peut également influencer la qualité d'un réseau sans fil. Un usager s'éloignant d'un point d'accès verra peu à peu la qualité de sa liaison se détériorer.

La complexité du protocole IEEE 802.11 exige des métriques additionnelles pour mesurer les performances au niveau des trames transmises, de la sécurité, de la qualité de service, de l'adaptation du taux de transfert et du mécanisme de relève. Il est ainsi important de définir une ou des métriques permettant de mesurer les interférences subies par les points d'accès. En déterminant expérimentalement l'impact de l'interférence sur les métriques d'un réseau sans fil, il serait ensuite possible de créer un réseau qui détecterait lui-même les interférences en analysant les valeurs de ces métriques. L'utilisation de points d'accès supportant le protocole de gestion SNMP nous aide pour la définition de nos métriques.

4.1.1 Structure de la MIB IEEE 802.11

Pour définir ces métriques, nous avons utilisé le protocole SNMP (Simple Network Management Protocol). Chacun des points d'accès est caractérisé par sa MIB (Management Information Base) qui nous procure un certain nombre d'OID (Object Identifier) permettant d'évaluer les performances du réseau en temps réel. La MIB du protocole IEEE 802.11 est basée sur une structure en arbre utilisant la notation ASN.1 (Abstract Syntax Notation). La structure de cette MIB est composée de quatre branches comme présentées à la Figure 4.1

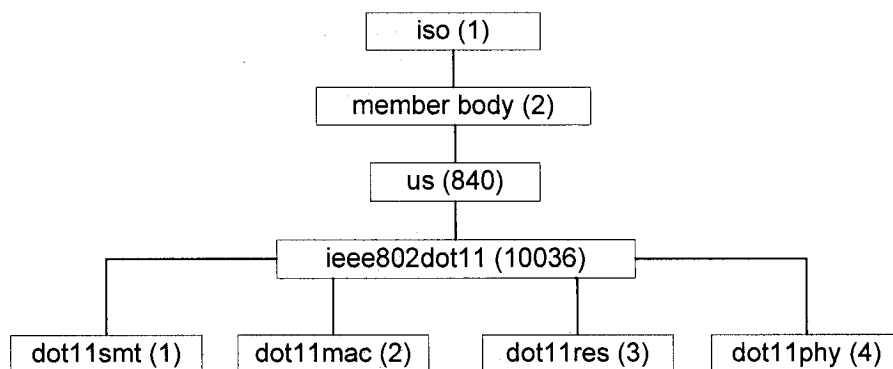


Figure 4.1 Structure de la MIB du protocole IEEE 802.11 [7]

La branche `dot11smt` contient les OID reliés à la gestion des stations ne faisant pas partie de la couche MAC. On y retrouve en autres l'information sur l'authentification des stations et sur l'utilisation de mécanisme de sécurité comme WEP. Quelques OID de cette branche peuvent être utiles pour l'évaluation de la zone de relèvements. En effet, les OID `DisassociateReason` (1.2.840.10036.1.1.1.15) et `DisassociateStation` (1.2.840.10036.1.1.1.16) peuvent être utilisés pour traquer les stations quittant la zone de couverture d'un point d'accès. Ces deux OID indiquent l'identité de la dernière station désassociée du point d'accès, ainsi que la raison ayant mené à cette dissociation.

La branche `dot11mac`, comme son nom l'indique, procure toutes les OID nécessaires à la surveillance et à l'ajustement des paramètres de la couche MAC. Les OID de type compteur de cette branche sont particulièrement intéressants pour l'évaluation du taux de perte de trame. L'OID `dot11FCSErrorCount` (1.2.840.10036.2.2.1.12) est incrémenté à chaque fois qu'une trame reçue est en erreur. Pour obtenir le taux d'erreur, il suffit de diviser ce compteur par la valeur de l'OID `dot11ReceivedFragmentCount` (1.2.840.10036.2.2.1.10) qui représente le total des fragments de trame reçus. Pour les trames envoyées par le point d'accès, l'OID `dot11RetryCount` (1.2.840.10036.2.2.1.4) peut être utilisé. Cet OID est incrémenté à chaque fois qu'une trame est retransmise suite à la non-réception d'un accusé de réception. L'augmentation subite de cet OID est un bon indicateur d'une augmentation

du nombre de trame perdues ou en erreur. Cet OID peut être utilisé conjointement avec l'OID `dot11TransmittedFrameCount` (1.2.840.10036.2.2.1.13) pour obtenir le ratio du nombre de retransmission par rapport au nombre total de trames transmises.

La troisième branche de la MIB du protocole IEEE 802.11, `dot11res`, contient les OID décrivant les ressources disponibles. L'information sur le manufacturier ainsi que sur le nom de produit sont des exemples d'information retrouvée dans cette branche. Aucun OID de cette branche n'est utile pour l'évaluation de l'interférence.

La dernière branche, `dot11phy`, est plus intéressante puisqu'elle contient les OID décrivant le statut de la couche physique. Les OID de cette branche peuvent être utilisés pour configurer l'interface radio du point d'accès. Ainsi l'OID `dot11CurrentFrequency` (1.2.840.10036.4.11.1.1) représente le canal d'opération du point d'accès et peut être réglé à distance par le protocole SNMP. Il est également possible de régler la puissance d'émission du point d'accès à l'aide de l'OID `dot11CurrentTxPowerLevel` (1.2.840.10036.4.3.1.10).

En complément à la MIB du protocole IEEE 802.11, chaque manufacturier peut créer ses propre OID qu'il sauvegarde dans sa MIB privée. Le contenu des MIB privées peut être très intéressant pour l'évaluation de métriques reliées au réseau sans fil. Cisco System, un joueur majeur dans le marché des points d'accès, possède une MIB privée très bien garnie. Un premier OID utile de cette MIB permet de connaître le nombre de stations présentement associées au point d'accès. Il s'agit de l'OID `cDot11ActiveWirelessClients` (1.3.6.1.4.1.9.9.273.1.1.2.1.1). Deux autres OID de cette MIB permettent d'obtenir de l'information pertinente sur les stations associées au point d'accès. L'OID `cDot11ClientSignalStrength` (1.3.6.1.4.1.9.9.273.1.3.1.1.3) donne la puissance du signal provenant de la station et l'OID `cDot11ClientCurrentTxRateSet` (1.3.6.1.4.1.9.9.273.1.3.1.1.1) nous informe sur le taux de transmission qu'utilise la station. Le taux de transmission de la station change en fonction de la qualité de la liaison sans fil. Pour l'évaluation de l'interférence, nous n'utilisons pas les OID de la MIB privée. Nous voulons en effet produire une analyse indépendante des manufacturiers des points d'accès.

4.1.2 Scénarios expérimentaux permettant l'étude de l'interférence

Lorsque plusieurs points d'accès se retrouvent radio électriquement près l'un de l'autre, le choix de la fréquence d'opération de ceux-ci devient très importante. En pratique, il est courant d'utiliser seulement les canaux 1, 6 et 11 qui sont reconnus pour ne pas s'interférer l'un à l'autre. Ces résultats ont guidé la configuration de plusieurs réseaux sans fil d'entreprises. Dans cette section, nous nous attardons à l'ampleur des interférences qui sont observées lorsque des points d'accès utilisent des canaux proches l'un de l'autre. Nous mesurons l'impact que ces interférences ont sur le débit maximal d'un point d'accès.

La configuration réseau que nous utilisons pour nos différentes expérimentations est assez simple. Les stations IEEE 802.11g communiquent avec un serveur en passant par un point d'accès IEEE 802.11g. Le serveur est, lui, relié au réseau filaire à l'aide d'une carte Ethernet pouvant atteindre une vitesse de 1 Gbps lors de ces communications avec le commutateur. Les points d'accès sont reliés à ce même commutateur à l'aide de leur interface Ethernet pouvant communiquer à 100 Mbps. Pour s'assurer de saturer le canal entre les points d'accès et les stations, du trafic est généré à l'aide de l'outil Iperf. Ce dernier est un programme « Open Source » conçu et réalisé par l'entreprise DAST ayant pour fonction la génération de trafic entre un client et un serveur. Le détail des équipements utilisés lors des expérimentations est présenté à l'annexe A. Cette infrastructure réseau permet de s'assurer que le goulot d'étranglement se situe au niveau de la connexion sans fil. Lors des simulations impliquant plusieurs stations sans fil, un programme Java (Voir annexe B) a été utilisé pour s'assurer que les sessions iperf démarraient simultanément sur chaque station.

4.1.2.1 Scénario 1 : Une station communiquant avec un point d'accès

Le premier scénario mis en œuvre est présenté à la Figure 4.2. Un seul point d'accès offre du service à une station sans fil pour que celle-ci communique avec le serveur. Cette configuration a pour but de mesurer le débit maximal atteint par une station sans fil ne subissant aucune interférence.

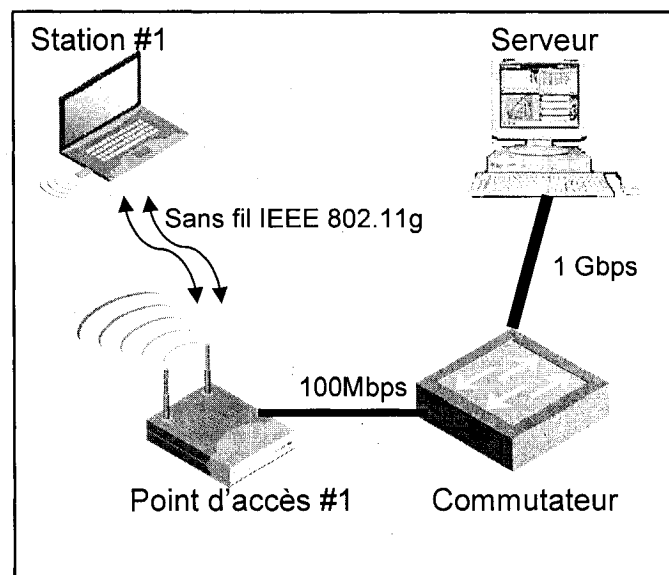


Figure 4.2 Architecture réseau pour le scénario 1

4.1.2.2 Scénario 2 : Deux PA et stations communiquant avec le PA ayant le signal le plus fort

La configuration réseau nécessaire au scénario 2 est présentée à la Figure 4.3. Les stations s'associent au point d'accès qui offrent le plus haut niveau de signal. Chacune des stations établit par la suite une session Iperf avec un serveur afin d'utiliser au maximum la bande passante disponible. Le canal utilisé par le point d'accès 1 est alors modifié pour balayer les onze canaux disponibles pour la norme IEEE 802.11g en Amérique du Nord. Pendant ce temps, le point d'accès 2 ne change pas de configuration et demeure au canal 6 pour la durée de la simulation. À chaque changement de canal du point d'accès 1, une mesure du débit obtenu par la session Iperf est prise. Cette mesure

évalue directement l'impact de l'interférence sur le débit utile de la connexion IEEE 802.11g. En plus du débit, les valeurs des OID de la MIB IEEE 802.11 sont enregistrées tout au long de la simulation.

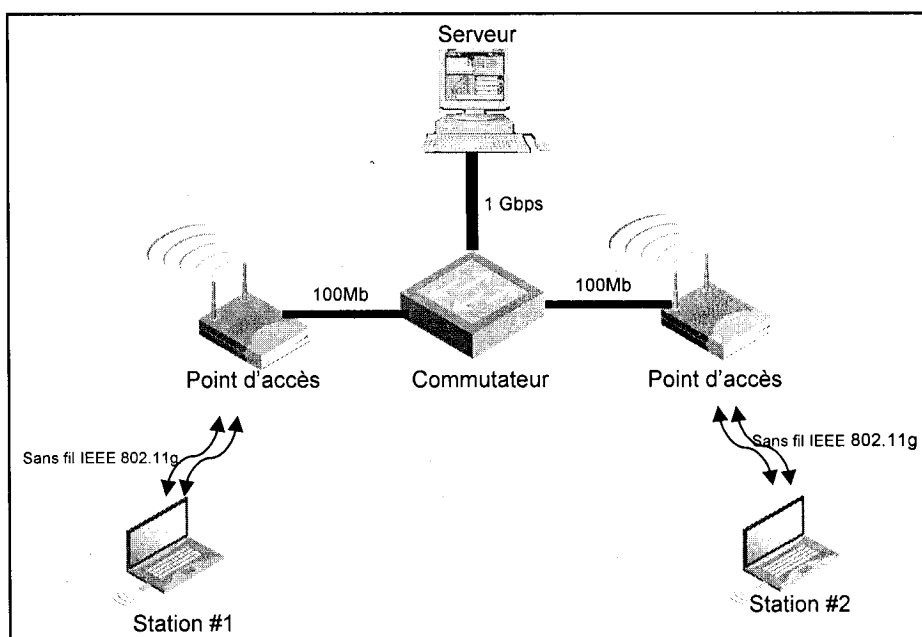


Figure 4.3 Architecture réseau pour le scénario 2

4.1.2.3 Scénario 3 : Trois PA et stations communiquant avec le PA ayant le signal le plus fort

La configuration réseau nécessaire au scénario 3 est présentée à la Figure 4.4. Les stations s'associent au point d'accès qui offrent le plus haut niveau de signal. Chacune des stations établit par la suite une session Iperf avec le serveur afin d'utiliser au maximum la bande passante disponible. Le canal utilisé par les points d'accès 1 et 2 est alors modifié pour balayer les onze canaux disponibles. Pendant ce temps, le point d'accès 3 ne change pas de configuration et demeure au canal 6 pour la durée de la simulation. À chaque changement de canal du point d'accès 1 ou 2, une mesure du débit obtenu par la session Iperf est prise pour un total de 121 simulations. Ces simulations

permettent d'identifier si l'impact de l'interférence sur le débit est proportionnel au nombre de sources d'interférence.

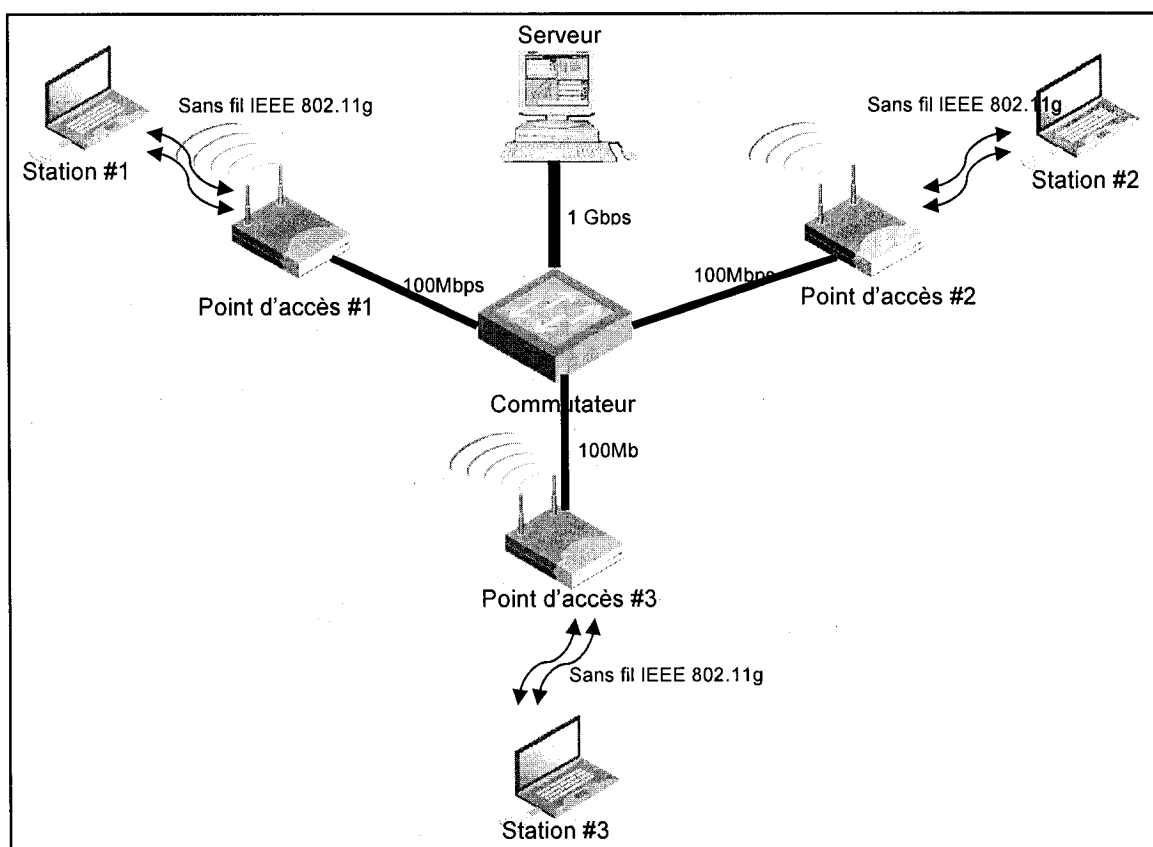


Figure 4.4 Architecture réseau pour le scénario 3

4.2 Présentation des résultats d'expérimentation

Les résultats obtenus lorsqu'une seule carte réseau sans fil est utilisée sont présentés à la Figure 4.5. Il s'agit des débits maximaux moyens atteints par une station sans fil qui est la seule à émettre dans son entourage. À première vue, les résultats obtenus peuvent paraître faibles compte tenu que le protocole IEEE 802.11g opère théoriquement à un débit de 54 Mbps. Les valeurs obtenues représentent la charge utile transférée en utilisant le protocole TCP à la couche transport. Chacune des transmissions est donc constituée des étapes suivantes :

Émission du segment de donnée TCP :

- attente d'un temps DIFS qui assure qu'aucun autre échange n'est en cours sur le réseau ;
- envoi de la trame IEEE 802.11 qui contient le segment TCP ;
- attente d'un temps SIFS qui est un court intervalle entre l'émission de la trame et son acquittement ;
- envoi de la trame d'acquittement IEEE 802.11.

Émission de l'acquittement du segment TCP :

- attente d'un temps DIFS ;
- envoi de la trame IEEE 802.11 qui contient l'acquittement TCP ;
- attente d'un temps SIFS ;
- envoi de la trame d'acquittement IEEE 802.11.

Le protocole IEEE 802.11 acquitte chacune des trames transmises, ce qui diminue de beaucoup le débit de données des couches supérieures qui peuvent être transférées. Les valeurs mesurées lors de la simulation se rapprochent de celles présentées par Tianlin [32].

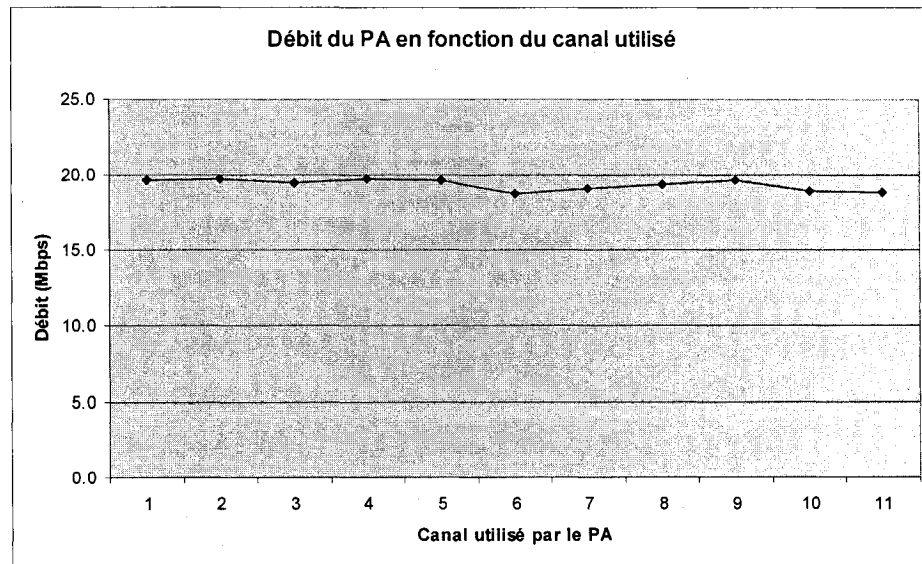


Figure 4.5 Débit maximal d'une station IEEE 802.11g en fonction du canal d'opération

Nous poursuivons l'expérimentation avec le scénario impliquant deux points d'accès tel qu'illustré à la section précédente. Les résultats pour ce scénario sont présentés à la Figure 4.6. Ces résultats sont surprenant puisque quelque soit le canal utilisé par le point d'accès #1, celui-ci influence le débit du point d'accès #2 de façon importante. Même lorsque qu'un écart de cinq canaux est respecté, les points d'accès continuent d'avoir une influence les uns sur les autres. Ces résultats sont à première vue en désaccord avec la théorie indiquant que les canaux 1, 6 et 11 n'ont pas d'influence les uns sur les autres.

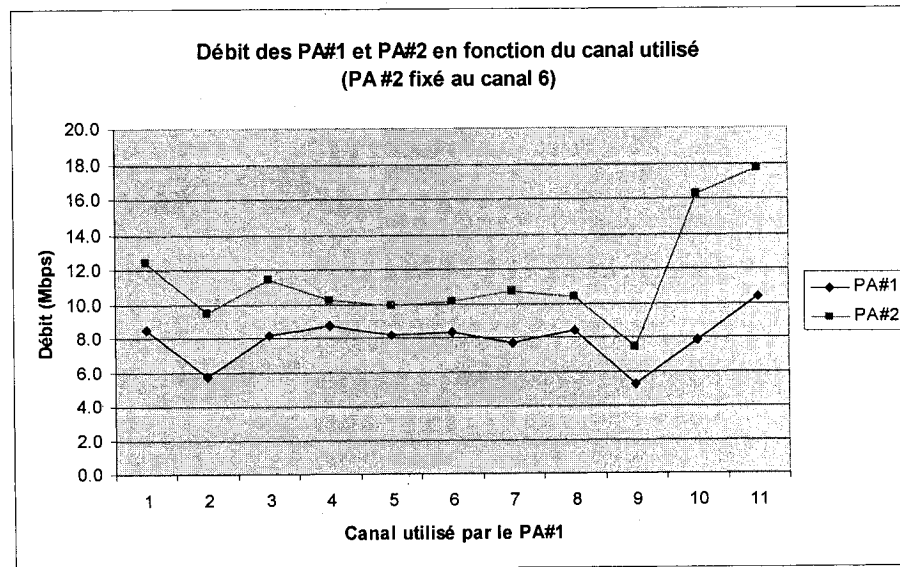


**Figure 4.6 Débit lorsque deux PA et stations communiquent
avec le PA ayant le signal le plus fort**

Comme prévu, l'interférence générée par le deuxième point d'accès se reflète au niveau des OID de type compteur de la MIB IEEE 802.11. À titre d'exemple, la Figure 4.7 illustre le ratio des trames reçues avec des erreurs sur le nombre total de trames reçues. Pour générer ce graphique, nous avons additionné les valeurs des OID obtenues sur les deux points d'accès. Nous remarquons un plus grand nombre d'erreurs lorsque les canaux utilisés sont rapprochés. La relation entre la valeur des OID et le débit obtenu n'est cependant pas simple à déduire.

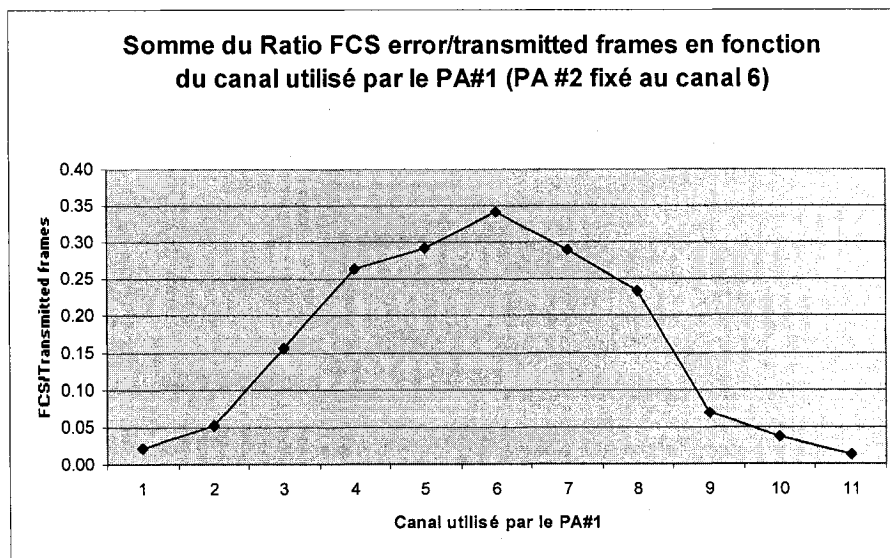


Figure 4.7 Répercussion de l'interférence générée sur les valeurs des OID

En conservant la même topologie physique, nous effectuons une autre expérimentation pour déterminer l'importance de l'interférence occasionnée par un point d'accès en fonction de son canal d'opération. Le but premier est de voir dans quelle mesure l'interférence est présente lorsque les fréquences d'opération des deux points d'accès ont un écart de plus de 5 canaux. Nous reprenons pour ce faire l'expérience en fixant le point d'accès #2 au canal 1 alors que le point d'accès #1 balaie quant à lui les fréquences 1 à 11. Les résultats obtenus sont présentés à la Figure 4.8

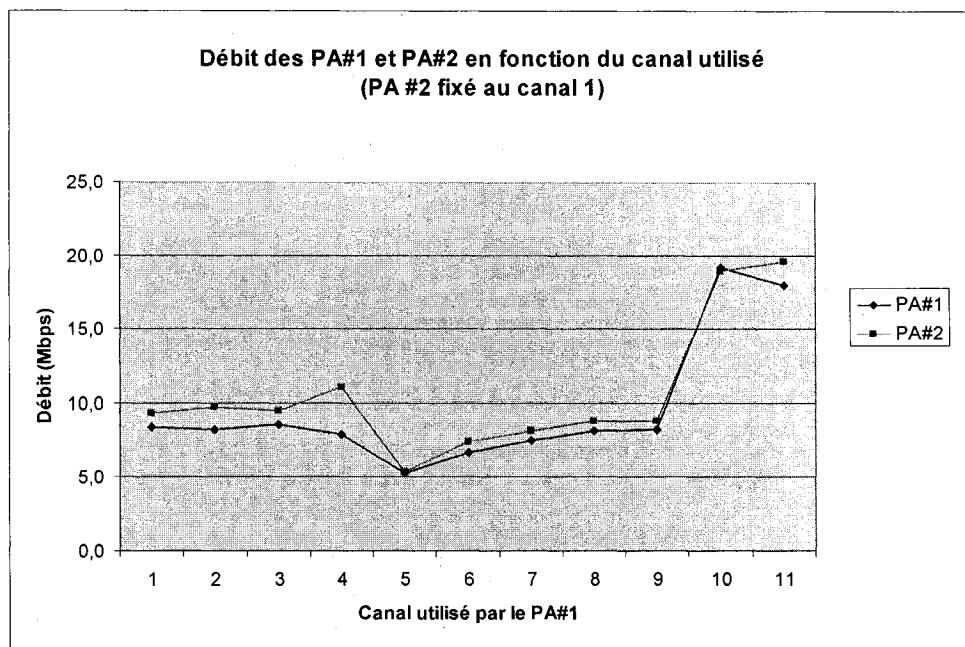


Figure 4.8 Débits obtenus lorsqu'un point d'accès est fixé au canal 1

Les résultats obtenus sont très surprenants. En effet, l'interférence est importante tout au long de l'expérimentation sauf lorsque le point d'accès 1 fonctionne au canal 10 ou 11. Pour ce qui est des valeurs recueillies par SNMP, on remarque que les taux d'erreur de trame diminuent à partir du canal 6 comme illustré à la Figure 4.9.

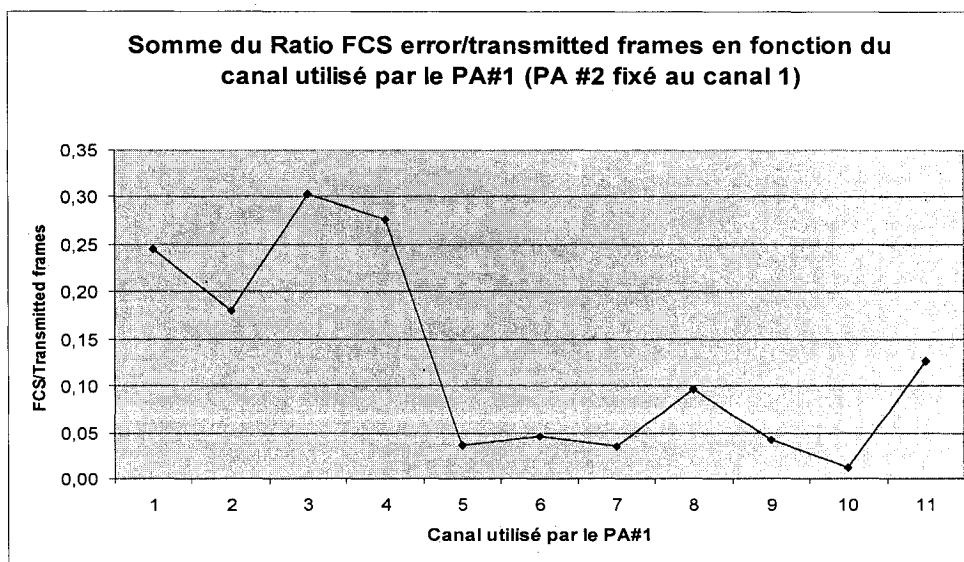


Figure 4.9 Taux d'erreur de trame en fonction du canal d'opération du PA 1

Selon ces résultats, on ne devrait pas effectuer les plans de fréquences des réseaux IEEE 802.11g en utilisant les canaux 1, 6 et 11. Pour s'assurer d'un environnement sans interférence, on devrait plutôt uniquement utiliser les canaux 1 et 11, ce qui rendrait quasiment impossible l'assignation des fréquences à l'intérieur d'un grand réseau. Cette expérience a été répétée à quelques reprises et en changeant même les ordinateurs portables utilisés. Les résultats obtenus ne sont pas significativement différents.

Toutes les simulations précédentes ayant été réalisées avec des cartes réseau sans fil intégrées aux ordinateurs portables, nous avons jugé pertinent d'effectuer une série de tests avec un autre type de carte. C'est ainsi que nous avons repris les mêmes expérimentations mais cette fois-ci avec des cartes externes de type PCMCIA. Les cartes utilisées (Cisco Aironet 802.11a/b/g) sont considérées de haute gamme de par leur prix très élevé (~200\$). Nous avons premièrement validé le taux de transfert maximal de la carte en reprenant l'expérimentation avec un point d'accès et une carte. Les résultats obtenus sont présentés à la Figure 4.10. Ceux-ci sont semblables à ceux obtenus avec les cartes sans fil intégrées aux ordinateurs portables bien que les débits soient légèrement supérieurs.

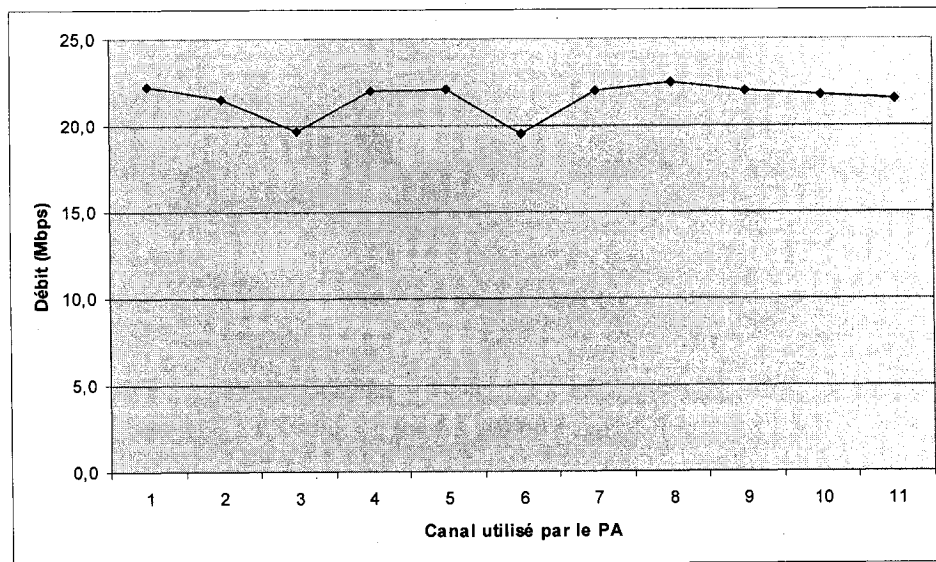


Figure 4.10 Débit du point d'accès en fonction du canal d'opération (carte PCMCIA Cisco)

Les résultats les plus intéressants sont ceux obtenus lorsque deux points d'accès sont en opération. Ces résultats, présentés à la Figure 4.11, sont très différents de ceux obtenus précédemment avec les cartes intégrées.

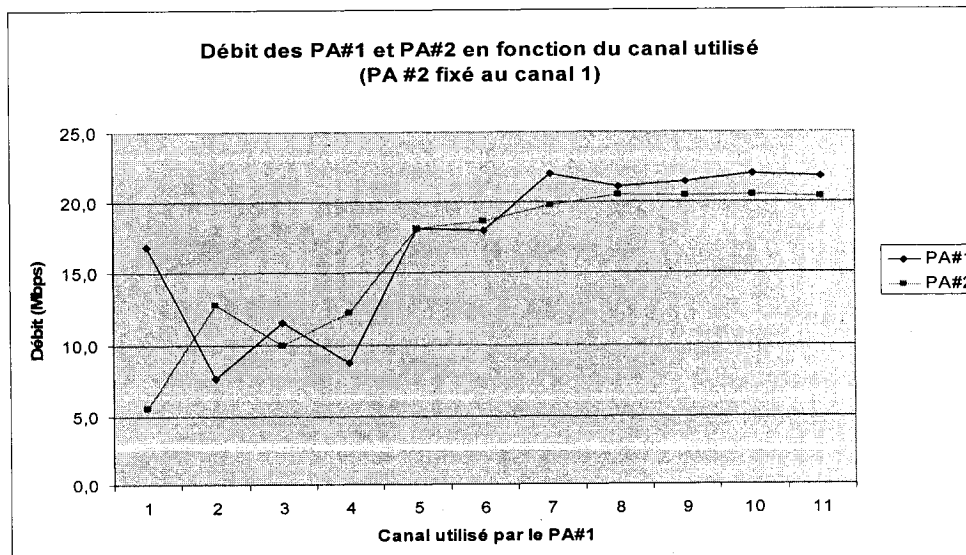


Figure 4.11 Débit des points d'accès en fonction du canal d'utilisation du PA 1 (Carte PCMCIA Cisco)

L'interférence est importante pour les premiers canaux mais diminue rapidement aussitôt qu'un écart de 4 canaux est présent entre les deux points d'accès. Ainsi, nous obtenons un débit de près de 20 Mbps pour les 2 points d'accès lorsque ceux-ci opèrent respectivement aux canaux 1 et 6. De plus, l'interférence est à toute fin pratique inexistante lorsque le point d'accès 1 utilise les canaux 7 à 11.

L'évolution du taux de trames reçues en erreur a également été enregistrée lors de ces expérimentations et est présentée à la Figure 4.12. Nous remarquons premièrement que ce ratio est presque nul lorsque le point d'accès 1 utilise les canaux 6 à 11. En comparant les valeurs obtenues avec celles recueillies avec les cartes sans fil intégrées aux ordinateurs portables, nous constatons également qu'elles sont inférieures. En effet le taux maximal atteint avec les cartes PCMCIA est de 0,07 alors qu'il s'élève jusqu'à 0,30 avec les cartes intégrées. Ce taux d'erreur plus faible avec les cartes PCMCIA est certainement une des causes des débits légèrement supérieurs obtenus avec ces mêmes cartes.

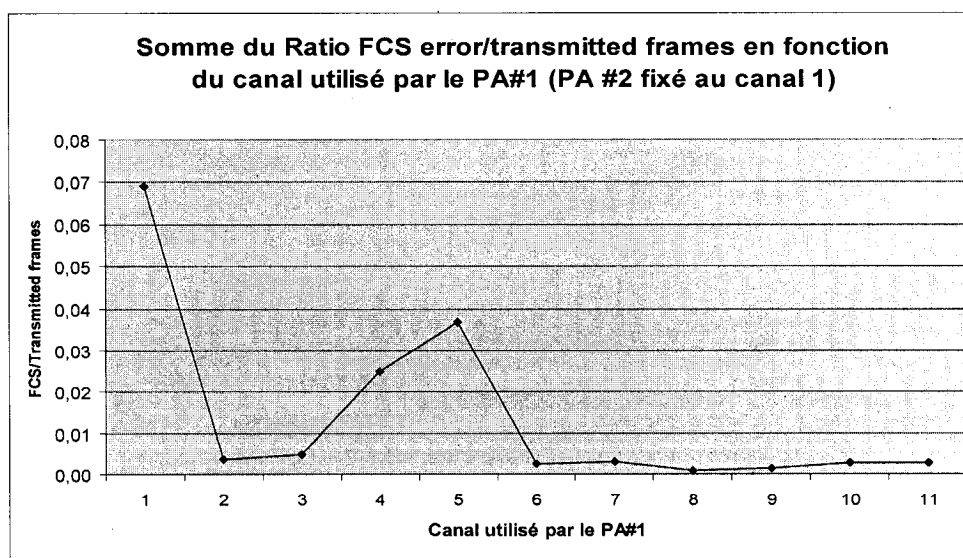


Figure 4.12 Taux d'erreur de trame en fonction du canal d'opération du PA 1 (Carte PCMCIA Cisco)

Les dernières expérimentations effectuées sont celles nécessitant 3 points d'accès et 3 stations IEEE 802.11g. La quantité d'informations recueillies pour ce scénario est considérable et ne sera pas présentée de façon exhaustive. Il est à noter cependant que c'est en partie avec ces résultats que nous pouvons valider certaines propriétés de l'interférence dans les réseaux sans fil IEEE 802.11.

4.3 Analyse de l'interférence observée lors de l'expérimentation

Les différentes données recueillies vont nous permettre de valider ou de rejeter certaines hypothèses sur l'interférence dans les réseaux sans fil. Une analyse statistique de ces données est nécessaire pour tenir compte des fluctuations légères lors des mesures pratiques. L'intervalle de confiance résultant de cette analyse statistique est utile pour la comparaison des données entre elles. Pour toutes nos expérimentations, nous avons 6 mesures pratiques, desquelles nous calculons la moyenne et un intervalle de confiance pour cette moyenne. Puisqu'on considère que cet échantillonnage s'effectue à partir d'une population normale de variance inconnue et que la taille d'échantillon est petite ($n < 30$), l'estimation de la variance σ^2 n'est plus fiable. Elle varie trop d'échantillon en échantillon. Dans ce cas, l'écart réduit $\frac{\bar{X} - \mu}{\frac{s}{\sqrt{n}}}$ n'est plus distribué selon la loi normale

centrée réduite (le théorème central limite ne s'applique pas, puisque $n < 30$). Sous ces conditions, on ne peut donc pas établir un intervalle de confiance pour μ avec les valeurs tabulées de la loi normale centrée réduite. Ceci exige une autre distribution, soit la distribution de Student. La distribution de Student est symétrique par rapport à l'origine et est un peu plus aplatie que la distribution normale centrée réduite. Elle ne dépend que d'une seule quantité, soit ν , le nombre de degrés de liberté qui peut être n'importe quel

entier positif. À mesure que le nombre de degrés de liberté augmente ($v \rightarrow \infty$), la distribution de Student s'approche de la loi normale centrée réduite.

Intervalle de confiance pour μ (Population normale, variance σ^2 inconnue, $n < 30$)

On définit, en prenant comme estimation ponctuelle de μ la moyenne $\bar{X}$ de l'échantillon, un intervalle de confiance ayant un niveau de confiance $100(1-\alpha)\%$ de contenir la vraie valeur de μ comme suit :

$$\bar{X} - t_{\alpha/2;v} \cdot \frac{s}{\sqrt{n}} \leq \mu \leq \bar{X} + t_{\alpha/2;v} \cdot \frac{s}{\sqrt{n}} \quad (4.1)$$

où $v = n-1$ degrés de liberté, s représente l'écart-type de l'échantillon et $t_{\alpha/2;v}$, la valeur tabulée de la distribution de Student avec v degrés de liberté telle que la probabilité que t soit compris entre $-t_{\alpha/2;v}$ et $t_{\alpha/2;v}$ et $1 - \alpha$.

Nous pouvons maintenant déterminer l'intervalle de confiance pour le débit maximal moyen atteint par un point d'accès. Prenons premièrement le scénario où seulement un point d'accès et une seule station sont utilisés. Lorsque le point d'accès utilise le canal #6 nous avons pris 6 mesures de débit qui sont résumés au Tableau 4.1.

Tableau 4.1 Débit maximal d'un point d'accès opérant au canal #6

Débit (Mbit/s)
19,1
18,5
19,1
18,8
18,7
17,9

La moyenne $\bar{X}$ de cet échantillonnage est 18,7 Mbit/s et l'écart type s est 0,45 Mbit/s. Le nombre de degrés de liberté ν est 5 ($n-1$), donnant à l'intervalle de confiance la forme suivante :

$$18,7 - t_{0,10/2;5} \cdot \frac{0,45}{\sqrt{6}} \leq \mu \leq 18,7 + t_{0,10/2;5} \cdot \frac{0,45}{\sqrt{6}} \quad (4.2)$$

Où nous avons fixé α à 0,10 pour avoir un niveau de confiance de 90%. En consultant une table de distribution de Student nous trouvons que $t_{0,05;5} = 2,015$, ce qui nous permet d'obtenir,

$$18,33 \text{ Mbit/s} \leq \mu \leq 19,07 \text{ Mbit/s} \quad (4.3)$$

Cet intervalle de confiance a 90 chances sur 100 de contenir la valeur vraie de μ qui est le débit maximal moyen d'un point d'accès opérant au canal #6 et communiquant avec une seule station.

Il est intéressant de comparer ce débit avec celui atteint par deux points d'accès opérant au même canal et communiquant chacun avec une station. L'hypothèse est que la somme des débits des deux points d'accès sera égale au débit atteint par le point d'accès opérant seul. Ainsi les deux points d'accès se partagent intelligemment la bande passante disponible en émettant seulement lorsqu'aucun autre équipement ne transmet. Lors de simulations, nous avons obtenu 6 mesures pour la somme des débits de deux points d'accès opérant au canal #6 que nous présentons au Tableau 4.2.

Tableau 4.2 Somme des débits de deux points d'accès opérant au canal #6

Débit (Mbit/s)
17,9
17,9
17,8
19,2
18,6
19,1

La moyenne $\bar{X}$ de cet échantillonnage est 18,4 Mbit/s et l'écart type s est 0,62 Mbit/s. Avec 5 degrés de liberté, l'intervalle de confiance prend la forme suivante :

$$18,4 - t_{0,10/2;5} \cdot \frac{0,62}{\sqrt{6}} \leq \mu \leq 18,4 + t_{0,10/2;5} \cdot \frac{0,62}{\sqrt{6}} \quad (4.4)$$

Où nous avons choisi un niveau de confiance de 90%. De la table de distribution de Student nous trouvons que $t_{0,05;5} = 2,015$, ce qui nous permet de d'obtenir,

$$17,88 \text{ Mbit/s} \leq \mu \leq 18,91 \text{ Mbit/s} \quad (4.5)$$

Cet intervalle a 90% des chances de contenir la valeur réelle de la somme des débits de 2 points d'accès opérant au canal #6. En comparant cet intervalle avec celui obtenu pour le débit d'un seul point d'accès, on remarque qu'ils se chevauchent en partie. Nous ne pouvons donc pas rejeter l'hypothèse selon laquelle la somme des débits de deux points d'accès opérant au même canal est égale au débit atteint d'un point d'accès opérant seul au canal #6.

En généralisant le raisonnement, nous pouvons faire l'hypothèse que la somme des débits de 3 points opérant au même canal sera la même que le débit d'un seul point d'accès opérant seul. Les sommes de débits obtenues lorsque 3 points d'accès utilisent le canal #6 sont présentées au Tableau 4.3.

Tableau 4.3 Sommes des débits de trois points d'accès opérant au canal #6

Débit (Mbit/s)
18,1
17,7
17,7
18,0
17,7
18,2

La moyenne $\bar{X}$ de cet échantillonnage est de 17,9 Mbit/s et l'écart type s est de 0,25 Mbit/s. En utilisant toujours un niveau de confiance de 90%, nous obtenons l'intervalle :

$$17,70 \text{ Mbit/s} \leq \mu \leq 18,10 \text{ Mbit/s} \quad (4.6)$$

L'écart-type peu élevé contribue à restreindre l'étendue de cet intervalle de confiance. Celui-ci ne chevauche pas l'intervalle obtenu pour évaluer le débit d'un seul point d'accès opérant au canal #6. Nous devons donc rejeter l'hypothèse supposant que la somme des débits de 3 points d'accès opérant au même canal est égale au débit d'un point d'accès opérant seul à ce canal. La somme des débits légèrement inférieure pour le scénario à 3 points d'accès est probablement liée au mécanisme d'accès au médium du CSMA/CA. En effet, lorsqu'une station ou un point d'accès veut émettre et qu'il perçoit le canal comme occupé, il attend un temps aléatoire avant d'essayer de réémettre. Lors du deuxième essai, si le canal est toujours occupé, le temps aléatoire d'attente devient deux fois plus long. Dans le scénario à 3 points d'accès, la probabilité qu'une station ou un point d'accès tente d'émettre et que le canal soit déjà occupé est plus grande. Le temps d'attente moyen augmente donc et la situation où le canal est libre sans qu'aucune station ne puisse émettre, peut alors survenir.

Une autre hypothèse que nous aimerions valider, est que le débit global obtenu par 3 points d'accès dont deux utilisent le même canal, est identique au débit atteint par 2 points d'accès utilisant ces deux mêmes canaux. Par exemple, la somme des débits de deux points d'accès opérant respectivement aux canaux 1 et 6 devrait correspondre à la somme des débits de 3 points d'accès dont deux opèrent au canal 1 et un au canal 6. Le Tableau 4.4 présente les résultats obtenus suite aux mêmes manipulations statistiques que nous venons de présenter.

Tableau 4.4 Données de la somme des débits de 2 PA canal (i,6) et de 3 PA canal (i,i,6)

Canal	Somme 2 PA	Somme 3 PA
1	$18,03 \text{ Mbit/s} \leq \mu \leq 23,73 \text{ Mbit/s}$	$24,98 \text{ Mbit/s} \leq \mu \leq 28,32 \text{ Mbit/s}$
2	$11,63 \text{ Mbit/s} \leq \mu \leq 18,64 \text{ Mbit/s}$	$12,09 \text{ Mbit/s} \leq \mu \leq 14,09 \text{ Mbit/s}$
3	$19,36 \text{ Mbit/s} \leq \mu \leq 19,90 \text{ Mbit/s}$	$17,73 \text{ Mbit/s} \leq \mu \leq 19,55 \text{ Mbit/s}$
4	$18,73 \text{ Mbit/s} \leq \mu \leq 19,11 \text{ Mbit/s}$	$18,41 \text{ Mbit/s} \leq \mu \leq 18,97 \text{ Mbit/s}$
5	$17,15 \text{ Mbit/s} \leq \mu \leq 18,89 \text{ Mbit/s}$	$18,13 \text{ Mbit/s} \leq \mu \leq 18,70 \text{ Mbit/s}$
6	$17,88 \text{ Mbit/s} \leq \mu \leq 18,91 \text{ Mbit/s}$	$17,70 \text{ Mbit/s} \leq \mu \leq 18,10 \text{ Mbit/s}$
7	$18,18 \text{ Mbit/s} \leq \mu \leq 18,53 \text{ Mbit/s}$	$18,59 \text{ Mbit/s} \leq \mu \leq 18,92 \text{ Mbit/s}$
8	$18,74 \text{ Mbit/s} \leq \mu \leq 18,84 \text{ Mbit/s}$	$18,95 \text{ Mbit/s} \leq \mu \leq 22,32 \text{ Mbit/s}$
9	$10,64 \text{ Mbit/s} \leq \mu \leq 14,60 \text{ Mbit/s}$	$18,82 \text{ Mbit/s} \leq \mu \leq 19,50 \text{ Mbit/s}$
10	$19,05 \text{ Mbit/s} \leq \mu \leq 29,20 \text{ Mbit/s}$	$13,21 \text{ Mbit/s} \leq \mu \leq 14,82 \text{ Mbit/s}$
11	$33,20 \text{ Mbit/s} \leq \mu \leq 34,28 \text{ Mbit/s}$	$16,81 \text{ Mbit/s} \leq \mu \leq 18,42 \text{ Mbit/s}$

On constate que l'hypothèse est en partie vérifiée. Les intervalles de confiance se chevauchent pour certains canaux seulement. La Figure 4.13 montre une représentation des résultats obtenus, ainsi que leur intervalle de confiance.

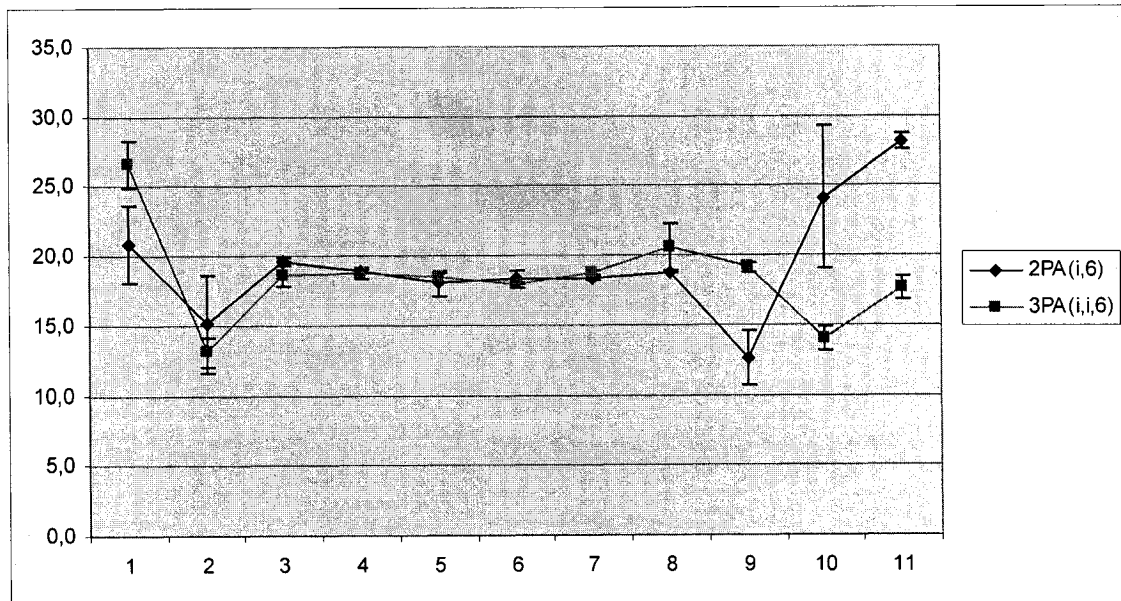


Figure 4.13 Comparaison de la somme des débits de 2 PA canal (i,6) et de 3 PA canal (i,i,6)

4.4 Environnement de simulation

Nous effectuons quelques simulations avec le logiciel OPNET afin de comparer les résultats simulés à ceux obtenus expérimentalement.

OPNET (OPen NETwork)¹ est un simulateur à événements discrets permettant de modéliser et d'évaluer les performances des réseaux de communication et des systèmes distribués. L'environnement d'OPNET incorpore plusieurs outils pour les phases d'étude d'un système, y compris la conception des modèles, la simulation, la collection et l'analyse des données. Pour effectuer les simulations, nous utilisons le modèle supportant le protocole IEEE 802.11g fourni par le logiciel OPNET. Nous sommes ainsi en mesure de recréer fidèlement les scénarios présentés à la section précédente. Les stations sont situées à 1 mètre du serveur avec lequel elles communiquent et les serveurs sont espacés de 5 mètres l'un de l'autre. Les serveurs sont

¹ <http://www.opnet.com>

munis d'une interface IEEE 802.11g et jouent également le rôle de point d'accès. Le schéma représentant notre scénario de simulation est présenté à la Figure 4.9. Le détail de la configuration d'OPNET pour les simulations est présenté à l'annexe C.

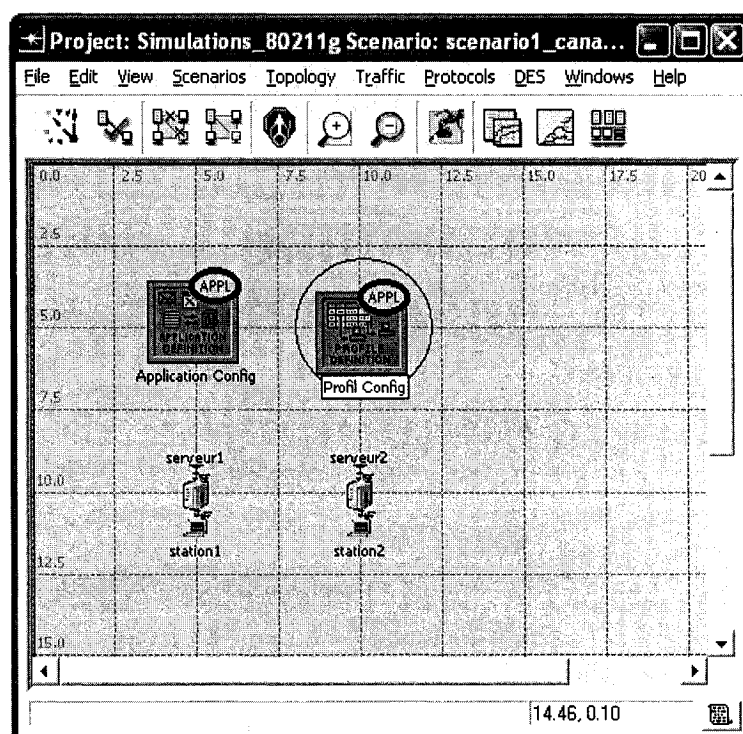


Figure 4.14 Schéma du scénario à 2 points d'accès sous Opnet

Lors de ces simulations, nous configurons les stations pour qu'elles saturent le lien IEEE 802.11g avec le serveur. Les stations sont en effet configurées pour faire des requêtes de transfert de fichier par le protocole FTP dépassant la capacité maximale du lien IEEE 802.11g. Nous avons ainsi un trafic se rapprochant de celui généré par Iperf lors des simulations sur de vrais équipements.

4.5 Résultats et analyse des simulations

La première simulation effectuée met en œuvre un seul point d'accès pour mesurer le débit maximal que celui-ci peut atteindre. Nous mesurons ce débit maximal

pour chacun des onze canaux utilisés par le IEEE 802.11g. Les résultats obtenus sont présentés à la Figure 4.15. Quel que soit le canal utilisé, le débit maximal moyen est constant à 23,37 Mbps.

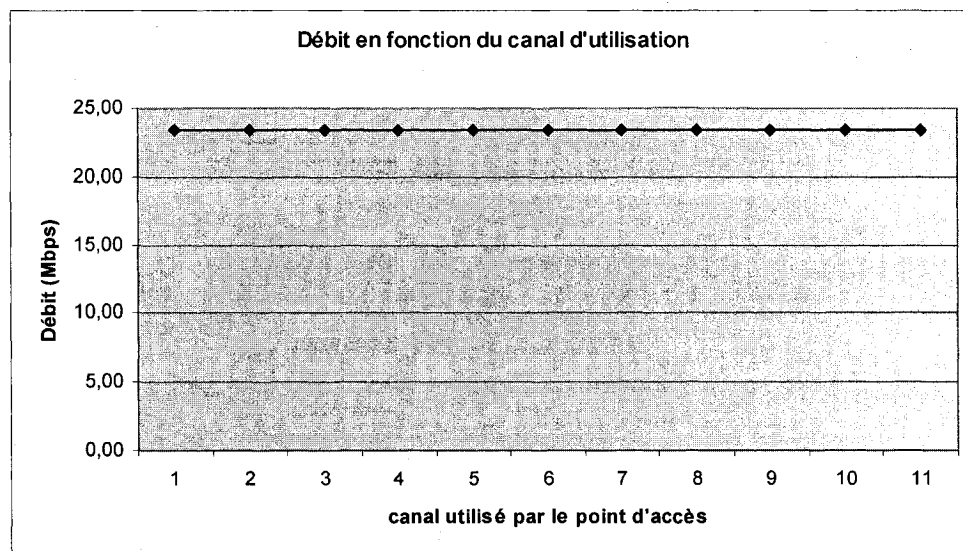


Figure 4.15 Valeurs simulées du débit d'un point d'accès en fonction du canal utilisé

Nous avons poursuivi les simulations avec le scénario à 2 points d'accès. Pour toute la durée de ces simulations, la station 2 et le serveur 2 opéraient au canal #6. Nous avons fait varier le canal d'opération de la station 1 et du serveur 1 de 1 à 11. Pour chacun de ces changements de canaux nous avons effectué une simulation d'une durée de 60 secondes. Ces simulations avaient pour but de mesurer le débit atteint par les stations 1 et 2 et ainsi découvrir l'interférence associée au choix de canal. Un résumé des résultats obtenus est illustré à la Figure 4.16.

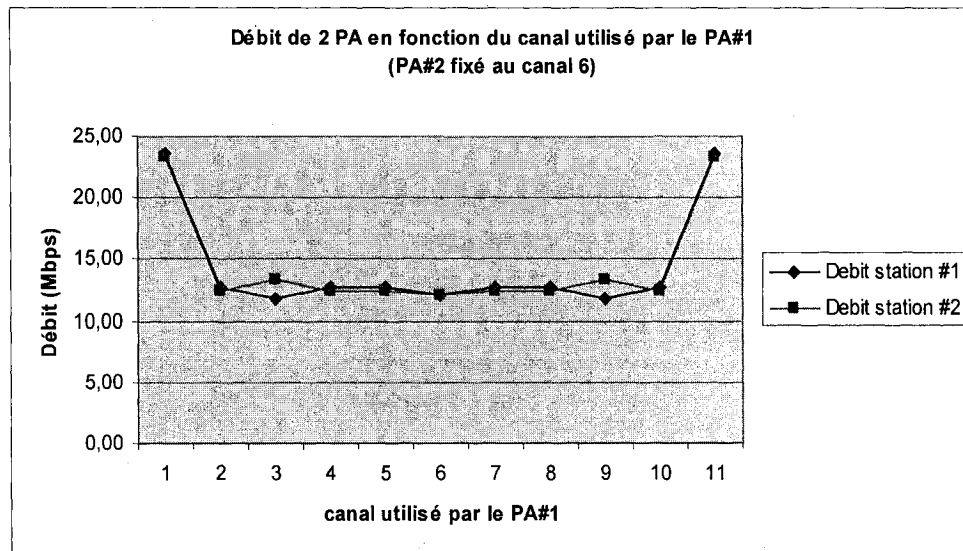


Figure 4.16 Débits obtenus par deux PA dont un est fixé au canal 6 (simulation avec OPNET)

Nous remarquons premièrement que les résultats sont parfaitement symétriques par rapport au point où les deux stations utilisent le canal 6. Par exemple, les débits obtenus lorsque la station 2 opère au canal 4 et au canal 8 sont exactement les mêmes. Nous constatons également que ces résultats sont en accord avec la théorie voulant que les canaux 1,6 et 11 ne s'interfèrent pas. Le débit obtenu lorsque la station 2 utilise les canaux 1 et 11 est en effet égal au débit théorique obtenu lorsqu'une station opère seule dans son environnement. La Figure 4.16 illustre clairement que l'utilisation des canaux 2 à 10 par la station 2 interfère avec la station 1 qui communique sur le canal 6. La diminution du débit qu'occasionne cette interférence est pratiquement identique pour les canaux 2 à 10. Ces résultats nous laissent croire qu'il est difficile d'identifier le canal d'opération d'un point d'accès interférant en analysant uniquement les variations de débit sur le réseau sans fil. Le simulateur Opnet ne nous permet pas de simuler l'évolution des différents OID de type compteur de la MIB du protocole IEEE 802.11. Il aurait été très intéressant d'observer comment un simulateur pourrait évaluer le nombre de trames reçues en erreur (FCS).

Comme nous l'avons fait lors des expérimentations pratiques, nous avons refait des simulations avec deux stations sans fil mais en fixant cette fois ci la station 2 au canal 1. Les résultats alors obtenus en faisant varier le canal d'utilisation de la station 2 de 1 à 11 sont présentés à la Figure 4.17.

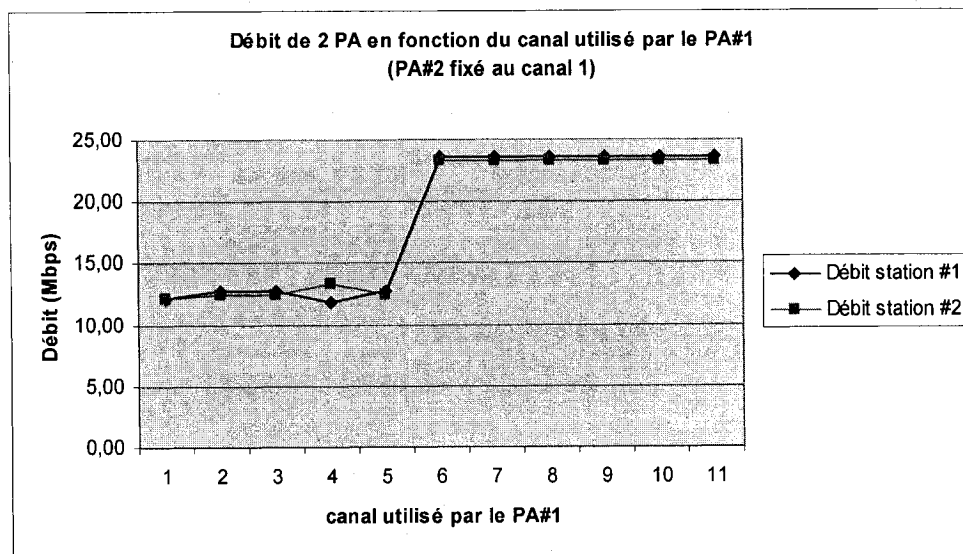


Figure 4.17 Débits obtenus par deux PA dont un est fixé au canal 1 (simulation avec OPNET)

Comme on pouvait s'y attendre, l'interférence cesse systématiquement lorsqu'un écart de cinq canaux est respecté. Le débit des stations est alors aussi élevé que si elles opéraient seules.

Comme nous avons fait avec les résultats pratiques, nous nous intéressons maintenant à valider certaines propriétés de l'interférence. Pour chacune des valeurs de débit simulé, nous avons calculé un intervalle de confiance ayant 90% des chances de contenir la valeur vraie du débit. Le nombre d'échantillons étant suffisants (~100), il est convenu que ces échantillons ont les propriétés d'une distribution normale. Pour les simulations à une station sans fil, les débits obtenus étaient les mêmes quelque soit le

canal d'opération. L'intervalle de confiance ayant 90 chances sur 100 de contenir la valeur vraie de μ qui est le débit maximal moyen d'une station IEEE 802.11g communiquant avec un serveur est :

$$23,31 \text{ Mbit/s} \leq \mu \leq 23,43 \text{ Mbit/s} \quad (4.7)$$

Il est intéressant de comparer ce débit avec la somme de deux points d'accès opérant au même canal. Encore une fois, quels que soient les canaux utilisés, tous les débits simulés étaient égaux. Un traitement statistique approprié nous a permis de calculer un intervalle de confiance ayant 90% des chances de contenir la valeur vraie de la moyenne de la somme des débits maximaux de 2 stations sans fil :

$$24,18 \text{ Mbit/s} \leq \mu \leq 24,26 \text{ Mbit/s} \quad (4.8)$$

Cet intervalle ne chevauche pas celui obtenu pour la moyenne du débit maximal d'une station. Étonnamment, la somme des débits de 2 stations opérant au même canal est plus élevée que celle d'une station opérant seule. Pour la simulation à deux stations, celles-ci étaient physiquement près l'une de l'autre, ce qui maximisait l'interférence. Nous nous attendions donc à une somme de débits égale ou légèrement inférieure au débit obtenu par une station opérant seule.

Nous avons également effectué des simulations permettant de comparer la somme des débits de 3 stations opérant au même canal que celui d'une station opérant seule. Selon ces simulations, la moyenne de la somme des débits maximums obtenue lorsque 3 stations utilisent le même canal a 90% de chance de se retrouver dans l'intervalle suivant :

$$22,70 \text{ Mbit/s} \leq \mu \leq 22,75 \text{ Mbit/s} \quad (4.9)$$

Encore une fois, cet intervalle ne chevauche pas celui obtenu avec la simulation à une station. Cependant, contrairement au scénario avec 2 stations sans fil, l'intervalle obtenu est inférieur à celui atteint par une seule station. En effet, on remarque que la

somme des débits de trois stations est environ de 0,65 Mbps inférieure au débit maximal moyen d'une station opérant seule.

4.6 Comparaison des résultats pratiques et simulés

La première constatation que nous faisons face aux résultats est que les résultats pratiques ont une nature beaucoup plus changeante que ceux simulés. Bien que nous ayons pris toutes les précautions nécessaires pour éliminer les sources d'interférence externes, les débits mesurés fluctuaient passablement. Les écarts types des valeurs mesurées sont ainsi supérieurs à ceux des valeurs simulées avec Opnet. Nous remarquons également que les débits obtenus lors des simulations sont tous plus élevés que ceux obtenus lors des expérimentations utilisant de vrais équipements IEEE 802.11g. Par exemple, la moyenne du débit maximal atteint par une carte sans fil intégrée à un ordinateur portable est 18,7 Mbps alors qu'il atteint 23,4 Mbps lors d'une simulation sous Opnet.

Une autre différence se situe au niveau de la somme des débits de 2 points d'accès situés près l'un de l'autre et opérant au même canal. Avec Opnet, cette somme était supérieure au débit maximal moyen d'une station opérant seule. Nous comprenons mal ce résultat puisque, opérant au même canal, les deux stations doivent compétitionner pour l'accès au médium. Lorsqu'une station tente d'émettre alors que l'autre occupe déjà le canal, elle passe dans un état d'attente pour un temps aléatoire. Si le canal est toujours occupé lorsque la station tente à nouveau d'émettre, le temps d'attente aléatoire est alors doublé. L'augmentation exponentielle du délai d'attente continue tant que la station ne perçoit pas le canal libre. Lorsque le canal se libère, la station voulant émettre ne peut pas utiliser le médium immédiatement, devant d'abord transiter par le mode attente. Ce raisonnement nous laisse croire que la somme des débits de deux stations ne peut être supérieure au débit d'une station saturant le canal. De plus, des collisions peuvent survenir si les deux stations tentent d'émettre au même moment. Bien que la plupart des collisions soient évitées de par la nature du protocole CSMA/CA, une collision peut survenir si deux stations sortent du mode attente au même moment. Nos

résultats pratiques tendent à confirmer ce raisonnement puisque la somme des débits de deux points d'accès opérant au même canal n'est pas supérieure au débit maximal atteint par une station opérant seule. Nos résultats pratiques nous font ressortir une autre conséquence liée à la croissance exponentielle du temps d'attente que subissent les stations détectant le médium occupé. En effet, le temps d'attente de la station qui a détecté le canal occupé par l'autre station sera toujours supérieur à celui de cette dernière. Ainsi, la station qui vient d'émettre aura l'avantage pour réémettre immédiatement. Lors des expérimentations avec deux points d'accès opérant à la même fréquence, il était fréquent qu'un des deux points d'accès ait un débit beaucoup plus élevé que l'autre. Il est logique de penser que la station ayant le plus faible débit était alors victime de temps d'attente plus élevé.

Les résultats pratiques et simulés du scénario à trois points d'accès et trois stations sont plus cohérents. En effet, dans les deux cas, la somme des débits des trois équipements IEEE 802.11g est inférieure au débit maximal moyen atteint par un point d'accès ou station opérant seul. Ce résultat est en accord avec la théorie expliquée au paragraphe précédent.

Du côté des résultats expérimentaux, nous avons pu observer des écarts importants de performance entre les différents équipements utilisés. Nous avons effectivement constaté que les cartes sans fil intégrées aux ordinateurs portables génèrent des interférences sur une bande de fréquences supérieures au 22 Mhz prévu. En réalité, lorsqu'une de ces cartes opère au canal 1, elle produit de l'interférence sur tous les canaux du IEEE 802.11g à l'exception des canaux 10 et 11. De plus, si une telle carte utilise le canal 6, elle créera de l'interférence sur tous les canaux sans exception. Ce résultat est alarmant pour tous les gestionnaires de réseaux sans fil. En effet, bien que ceux-ci puissent sélectionner les points d'accès de leurs réseaux, ils n'ont généralement aucune influence quant au choix des cartes réseaux sans fil des utilisateurs.

CHAPITRE V

CONCLUSION

Dans le présent mémoire, nous avons étudié l'interférence pouvant affecter les réseaux sans fil IEEE 802.11. Les résultats de nos expérimentations nous ont montré quel pouvait être l'impact de cette interférence sur les performances d'un réseau sans fil. Ce dernier chapitre présente dans un premier temps une synthèse de l'ensemble de nos travaux. Puis, nous présentons les limitations liées à notre recherche, avant de conclure en proposant des orientations vers lesquelles des travaux futurs pourraient être réalisés.

5.1 Synthèse des travaux

La popularité des réseaux locaux sans fil de type IEEE 802.11 ne cesse de croître. Un inconvénient à cette popularité est la surutilisation des bandes de fréquences utilisées par ces réseaux. Les canaux d'opération des points d'accès de grands réseaux sans fil doivent être choisis judicieusement afin de minimiser l'interférence. Ce mémoire nous a permis d'étudier et de quantifier les interférences générées et subies en fonction des canaux d'opération de points d'accès opérant à proximité.

Dans un premier temps, nous avons proposé un modèle pour représenter les interférences d'un réseau IEEE 802.11. Nous avons ainsi généré un graphe, où les sommets représentent les points d'accès, et les arcs l'interférence potentielle entre les points d'accès. Nous avons par la suite traduit ce modèle en un système d'équation pour lequel nous avons proposé une méthodologie de résolution.

Nous avons poursuivi notre étude de l'interférence des réseaux sans fil en effectuant une série d'expérimentations utilisant de vrais équipements IEEE 802.11g ainsi que le logiciel de simulation Opnet. Ces expérimentations nous ont permis de mesurer l'impact du choix de canal d'opération d'un point d'accès sur les interférences subies par les autres points d'accès de son entourage. Alors que la théorie et les

simulations avec Opnet nous indiquaient que les canaux 1, 6 et 11 ne s'interfèrent pas, nos expérimentations sur de vrais équipements nous démontraient le contraire. En fait, nous avons obtenu des performances qui différaient grandement en fonction des cartes réseaux clients utilisées. Ainsi, l'utilisation de cartes intégrées aux ordinateurs portables générait de l'interférence sur pratiquement tous les canaux de la bande de fréquences. En contrepartie, les mêmes expérimentations effectuées avec des cartes réseaux sans fil haut de gammes ont permis d'obtenir des résultats se rapprochant plus de la théorie. Il est très inquiétant de constater de telles différences de performances entre des équipements supposément conformes au même standard. Ces résultats sont d'autant plus préoccupants pour les gestionnaires réseaux qui ne contrôlent que rarement le choix des cartes clients se connectant à leur réseau.

5.2 Limitations des travaux

Notre recherche nous a permis d'analyser l'interférence dans les réseaux sans fil IEEE 802.11. Nos travaux présentent néanmoins quelques limitations. La première limitation que nous pouvons noter se situe au niveau du protocole IEEE 802.11 utilisé. L'ensemble de nos travaux ont été effectués avec des points d'accès et des cartes réseaux IEEE 802.11g. L'interférence générée était donc toujours similaire au niveau de la couche physique puisque le protocole IEEE 802.11g utilise la modulation OFDM. Il aurait pu être intéressant de voir l'impact qu'aurait eu une station utilisant un autre type de modulation comme le DSSS utilisé par les stations IEEE 802.11b. L'étude de l'interaction entre ces deux types de modulation est pertinente puisque la majorité des réseaux sans fil d'aujourd'hui doivent desservir simultanément les stations IEEE 802.11b et IEEE 802.11g. De plus, nous n'avons pas analysé dans quelle mesure les autres équipements opérant dans la même bande de fréquences pouvait interférer l'équipement IEEE 802.11. La bande ISM du 2.4 GHz est particulièrement sollicitée par une panoplie de technologies (Bluetooth, téléphone sans fil, four à micro-ondes, etc) dont la puissance d'émission et la technique de transmission sont très variables.

Une autre limitation sur nos travaux concerne la diversité des manufacturiers des cartes que nous avons utilisées pour nos expérimentations. Bien qu'un bon nombre de manufacturiers commercialisent des produits IEEE 802.11, nous avons utilisé les équipements de seulement deux d'entre eux.

5.3 Travaux futurs

Outre les limitations que nous venons de présenter, les travaux futurs pourraient porter sur la détection automatique de l'interférence par les points d'accès. Il serait alors possible de concevoir un logiciel de gestion de réseaux sans fil qui effectuerait l'allocation des canaux aux points d'accès de façon dynamique. Un réseau sans fil contrôlé de cette façon serait en mesure de s'adapter aux sources d'interférence et ainsi d'optimiser en tout temps ses performances.

La recherche d'un débit plus rapide sur les réseaux sans fil a entraîné la création du groupe de travail IEEE 802.11n. Le but de ce groupe est d'offrir une vitesse de transfert nette supérieure à 100 Mbps. Il sera intéressant d'étudier l'impact de l'interférence sur cette nouvelle technologie qui utilisera à la fois les bandes de fréquences ISM de 2.4 GHz et de 5 GHz.

BIBLIOGRAPHIE

- [1] Institute of Electrical and Electronic Engineers (IEEE), "IEEE Std 802.11-1997 Information Technology- telecommunications And Information exchange Between Systems-Local And Metropolitan Area Networks-specific Requirements-part 11: Wireless Lan Medium Access Control (MAC) And Physical Layer (PHY) Specifications," *IEEE Std 802.11-1997*, pp. 445, 1997.

- [2] H. Zimmermann, "OSI Reference Model-The ISO Model of Architecture for Open Systems Interconnection," *IEEE Transactions on Communications*, vol. 28, pp. 425-432, 1980.

- [3] K. K. Leung and B.-J. Kim, "Frequency assignment for IEEE 802.11 wireless networks," *Vehicular Technology Conference, 2003. VTC 2003-Fall. 2003 IEEE 58th*, vol. 3, pp. 1422-1426, 2003.

- [4] IEEE, "IEEE standard for information technology - telecommunications and information exchange between systems - local and metropolitan area networks - specific requirement. Part 11: wireless LAN medium access control (MAC) and Physical layer (PHY) specifications. Amendment 2: higher-speed physical layer (PHY) extension in the 2.4 GHz band - corrigendum 1," *IEEE Std 802.11b-1999/Cor 1-2001*, 2001.

- [5] IEEE, "IEEE standard for information technology- telecommunications and information exchange between systems- local and metropolitan area networks-specific requirements Part II: wireless LAN medium access control (MAC) and physical layer (PHY) specifications," *IEEE Std 802.11g-2003 (Amendment to IEEE Std 802.11, 1999 Edn. (Reaff 2003) as amended by IEEE Stds 802.11a-*

1999, 802.11b-1999, 802.11b-1999/Cor 1-2001, and 802.11d-2001), pp. 67, 2003.

- [6] IEEE, "Information technology- telecommunications and information exchange between systems- local and metropolitan area networks- specific requirements part 11: wireless lan medium access control (MAC) and physical layer (PHY) specifications amendment 1: high-speed physical layer in the 5 GHz band," *ISO/IEC 8802-11:1999/Amd 1:2000(E); IEEE Std 802.11a-1999*, pp. i-83, 2000.
- [7] M. S. Gast, *802.11 Wireless Networks, The Definitive Guide 2ed*: O'Reilly & Associates, 2005.
- [8] R. C. Paruchuri and P. Agrawal, "Interference Study of 802.11b Networks for Proactive Performance Management," 2006.
- [9] D. Vassis, G. Kormentzas, A. Rouskas, and I. Maglogiannis, "The IEEE 802.11g standard for high data rate WLANs," *Network, IEEE*, vol. 19, pp. 21-26, 2005.
- [10] A. R. Prasad, N. R. Prasad, A. Kamerman, H. Moelard, and A. Eikelenboom, "Performance evaluation, system design and network deployment of IEEE 802.11," *Wireless Personal Communications*, vol. 19, pp. 57-79, 2001.
- [11] S. Miyamoto, S. Harada, and N. Morinaga, "Performance of 2.4 GHz-band wireless LAN system using orthogonal frequency division multiplexing scheme under microwave oven noise environment," *International Symposium on Electromagnetic Compatibility*, 2005.
- [12] IEEE, "IEEE Std 802.15.1 - 2005 IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements. - Part 15.1: Wireless

medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPANs)," *IEEE Std 802.15.1-2005 (Revision of IEEE Std 802.15.1-2002)*, pp. 580, 2005.

- [13] K. Shuaib, M. Boulmalf, F. Sallabi, and A. Lakas, "Performance analysis co-existence of IEEE 802.11g with Bluetooth," *International Conference on Wireless and Optical Communications Networks*, 2005.
- [14] S. Zeadally, A. Banda, and A. Kumar, "Improving Bluetooth performance in 802.11 interference environments," *Computer Communications*, vol. 27, pp. 616-621, 2004.
- [15] IEEE, "IEEE recommended practice for information technology - telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements part 15.2: coexistence of wireless personal area networks with other wireless devices operating in unlicensed frequency bands," *IEEE Std 802.15.2-2003*, pp. 115, 2003.
- [16] A. Sikora and V. F. Groza, "Coexistence of IEEE802.15.4 with other Systems in the 2.4 GHz-ISM-Band," *Instrumentation and Measurement Technology Conference*, 2005.
- [17] M. Biggs, A. Henley, and T. Clarkson, "Occupancy analysis of the 2.4 GHz ISM band," *Communications, IEE Proceedings-*, vol. 151, pp. 481-488, 2004.
- [18] A. Bahri, "Conception des réseaux d'ordinateurs sans fil," 2003, 120 p, Mémoire de maitrise, Département de génie informatique, École polytechnique de Montréal.

- [19] C. Voudouris and E. P. K. Tsang, "Solving the radio link frequency assignment problem using guided local search," NATO Symposium on Radio Length Frequency Assignment, Sharing and Conservation Systems Aalborg, Denmark, 1998.
- [20] A. Bouju, J. F. Boyce, C. H. D. G. Dimitropoulos, V. Scheidt, and J. G. Taylor, "Tabu search for the radio links frequency assignment problem," Applied Decision Technologies (ADT'95), Uxbridge, U.K., 1995.
- [21] A. Y. Zomaya, A. Smith, and F. Seredynski, "On the Use of the Simulated Annealing Algorithm for Channel Allocation in Mobile Computing," *Wireless Communications and Mobile Computing*, vol. 3, pp. 239-253, 2003.
- [22] W. K. Lai and G. G. Coghill, "Channel Assignment Through Evolutionary Optimization," *Transactions on Vehicular Technology*, vol. 45, pp. 91-96, 1996.
- [23] S. H. Wong and I. J. Wassell, "Channel allocation for broadband fixed wireless access," *Wireless Personal Multimedia Communications, 2002. The 5th International Symposium on*, vol. 2, pp. 626-630, 2002.
- [24] T. Matsukawa, T. Satake, and J. Yamada, "Metrics for detection of QoS degradation over wireless LAN," *Applications and the Internet, 2005. Proceedings. The 2005 Symposium on*, pp. 198-203, 2005.
- [25] T. Tandai, T. Adachi, and K. Toshimitsu, "Optimum real-time data transmission scheduling for channel searching in IEEE 802.11 wireless LANs," *Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th*, vol. 4, pp. 2645-2649 2004.

- [26] L. Hui and N. K. Shankaranarayanan, "A distributed dynamic channel allocation technique for throughput improvement in a dense WLAN environment," *2004 IEEE International Conference on Acoustics, Speech, and Signal Processing*, vol. 5, pp. 345-348, 2004.
- [27] J.-F. Wagen, V. Inguscio, and E. Marchon, "Autonomous Wireless LAN Management," 2003.
- [28] J.-F. Wagen, F. Gamba, and D. Rossier, "A Simple Agent-based Framework for Adaptive WLAN Frequency Management," *MOBICOM*, San Diego, CA, 2003.
- [29] Y. Ming, N. Karmarkar, and A. Malvankar, "A dynamic radio channel allocation scheme for wireless LANs," *Advances in Wired and Wireless Communication, 2005 IEEE/Sarnoff Symposium on*, pp. 17-20, 2005.
- [30] Y. Ming and L. Hui, "An adaptive radio resource management technique for APs in WLANs," *12th IEEE International Conference on Networks*, Singapore, 2004.
- [31] F. Cali, M. Conti, and E. Gregori, "Dynamic tuning of the IEEE 802.11 protocol to achieve a theoretical throughput limit," *Networking, IEEE/ACM Transactions on*, vol. 8, pp. 785-799, 2000.
- [32] W. Tianlin and H. H. Refai, "Network performance analysis on IEEE 802.11g with different protocols and signal to noise ratio values," *Second IFIP International Conference on Wireless and Optical Communications Networks*, Dubai, United Arab Emirates, 2005.

ANNEXE A

ÉQUIPEMENT UTILISÉ POUR LES DIFFÉRENTS SCÉNARIOS

Matériel utilisé pour les différents scénarios :

Station #1 :

- IBM Thinkpad T43 Pentium M 750 (1.86GHz)
- 1 gigaoctet de mémoire vive
- carte réseau sans fil Intel Pro wireless 2200BG
- Windows XP, SP 2

Station #2 et 3:

- IBM Thinkpad R52 Pentium M 740 (1.73GHz)
- 1 gigaoctet de mémoire vive
- carte réseau sans fil Intel Pro wireless 2200BG
- Windows XP, SP 2

Serveur :

- IBM S51 Pentium 4 - 3,2 GHz
- 1 gigaoctet de mémoire vive
- Carte réseau Broadcom NetXtreme Gigabit Ethernet
- Windows XP, SP 2

PA#1 et #2:

- Cisco Aironet 1131AG
- Version logiciel: 12.3(2)JA2

PA#3:

- Cisco Aironet 1100G
- Version logiciel: 12.3(2)JA2

Commutateur:

- Cisco Catalyst 4500
- Carte 48 ports 10/100/1000 Mbps
- Supervisor IV (64 Gbps)
- Version IOS 12.2(25)EWA3

ANNEXE B

DESCRIPTION DU PROGRAMME UTILISÉ POUR LES SIMULATIONS

Afin d'automatiser les simulations, la création d'un programme a été essentielle. Le logiciel utilisé est une version modifiée d'un programme ayant été développé par M. Frédéric Jutras, un ancien étudiant de maîtrise de l'école Polytechnique de Montréal. Développé en Java et utilisant le protocole SNMP, ce programme facilite la collecte de données et automatise la simulation.

Basé sur le mode client-serveur, le programme présente une interface facile d'utilisation. L'utilisation de bouton radio permet de sélectionner le mode client ou le mode serveur. En premier lieu, l'application est démarrée en mode « Serveur » sur l'ordinateur communiquant avec les stations IEEE 802.11. Chacune des stations sans fil démarre par la suite l'application en mode « Client » en indiquant l'adresse IP du serveur. Pour démarrer la simulation, il suffit alors d'appuyer sur le bouton « Démarrer Simulation » de la machine configurée comme serveur. La simulation s'exécute alors en suivant les instructions se trouvant dans un fichier de configuration sauvegardé sur le serveur. C'est à l'intérieur de ce fichier de configuration que l'on indique les changements de canaux qui auront lieu pendant la simulation. Le serveur configure donc les points d'accès en plus de communiquer avec les stations clientes.

SNMP Inquisitor

File

Device address: 132.211.191.126 Serveur IP perf: 132.211.191.42 ☐

Community: public ☐ Serveur ☐ Client

timer field (ms): 0

Durée Iperf (s): 35

Iteration Sans Iperf: 5

OID/File: 500

OID:

Valeur (pour Set): SNMPInteger ▼

Get OID Get next OID Get table Démarrer simulation Set OID

Ne pas prendre les zéros ☒ Utiliser fichiers multiples ☐ Effacer écran

Version 1.2 Régis Dumont, Janvier 2006

Figure B.1 Interface du programme

Une fois la connexion établie, les communications entre les clients et le serveur sont directes, ce qui permet au serveur d'envoyer à tous les clients ses directives simultanément. Lorsque le canal d'utilisation d'un point d'accès est modifié, la connexion entre le client et le serveur est interrompue. Le programme attend alors que cette communication soit rétablie avant de continuer la simulation. L'utilisation de la commande PING permet de contrôler cette opération. Le serveur vérifie la connectivité avec tous les clients connectés et continue sa simulation dès que tous les clients redeviennent accessibles.

L'utilisation d'Iperf dans cette application se fait de façon complètement transparente. Dès son ouverture, le processus serveur lance Iperf en mode serveur. Il envoie par la suite un message aux différents clients connectés afin de lancer Iperf côté client avec une durée prédéterminée par le serveur. Une fois la simulation terminée, les données sauvegardées peuvent être retrouvées dans le répertoire indiqué dans le fichier de configuration.

ANNEXE C

CONFIGURATION DU LOGICIEL OPNET

Cette section a pour but de définir les différentes étapes de configuration que nous avons suivies pour effectuer nos simulations avec le logiciel OPNET. Ainsi, il suffit de suivre cette procédure pour reproduire les résultats que nous avons présentés précédemment.

C.1 Création du projet

Nous démarrons premièrement l'outil Opnet Modeler (nous utilisons la version 11.0). Nous créons alors un nouveau projet en sélectionnant l'option « new » sur menu « Fichier ». La Figure C.1 représente la fenêtre qui apparaît alors pour nous demander d'entrer un nom pour notre nouveau projet.

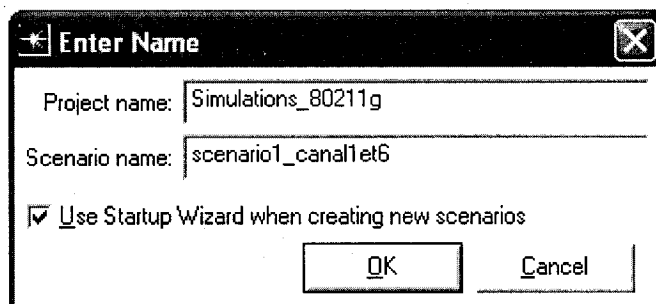


Figure C.1 Création d'un nouveau projet avec Opnet

Nous entrons alors un nom au projet, et cliquons sur "Ok". À l'écran suivant nous demandons le type de scénario que nous voulons créer. Nous choisissons alors "Create empty scenario" et appuyons sur le bouton "Next". La fenêtre suivante nous demande le type de réseau que nous voulons créer. Nous sélectionnons alors « Office » en prenant soin d'également cocher la case "Use metric Units" comme le montre la Figure C.2.

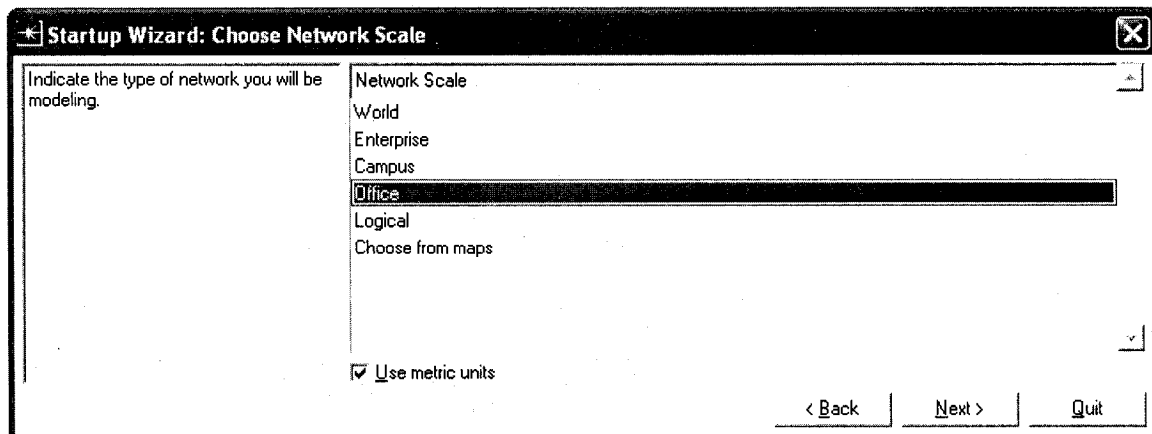


Figure C.2 Utilisation du système métrique

L'étape suivante consiste à entrer les dimensions de notre environnement de simulation. Pour nos simulations, nous avons utilisé un espace de 25 mètres par 25 mètres.

La dernière fenêtre de configuration du projet nous permet de sélectionner les technologies que nous allons utiliser dans nos simulations. Dans la colonne "Include", nous nous assurons que les champs "Wireless_lan" et "Wireless_lan_adv" sont à "Yes" tel qu'illustré à la Figure C.3.

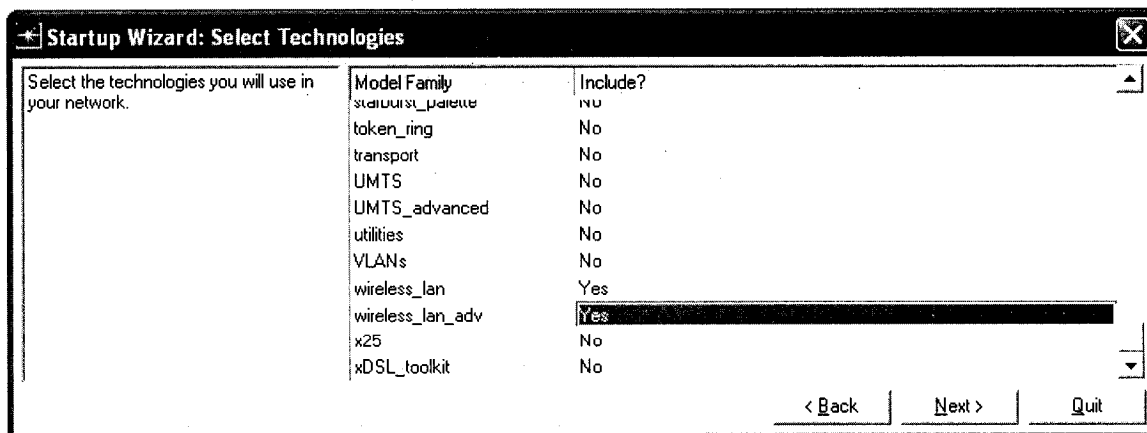


Figure C.3 Choix des technologies utilisées lors des simulations

Nous obtenons alors une surface quadrillée sur laquelle nous plaçons les différents objets nécessaires à nos simulations. C'est ainsi que de la palette d'outils, nous déplaçons sur la surface quadrillée les éléments "Application_Config", "Profile_Config", "wlan_server_adv (fix)" et "wlan_wkstn_adv (fix)". La Figure C.4 présente l'état de notre environnement de travail une fois ces éléments ajoutés. Nous remarquons que nous avons 2 stations wlan et 2 serveurs dans le but d'effectuer les simulations montrant l'interférence entre les stations.

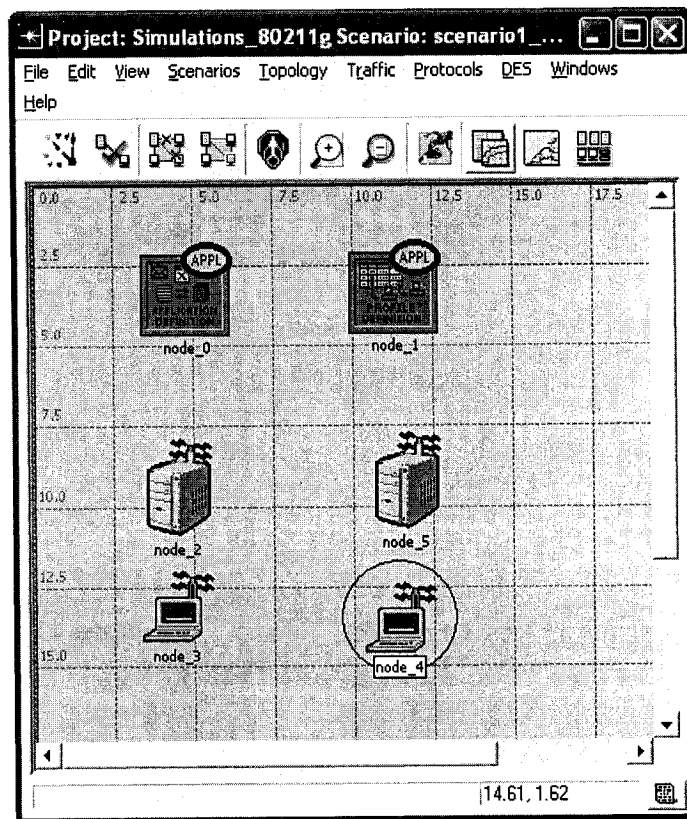


Figure C.4 Schéma du scénario utilisant 2 points d'accès

C.2 Configuration de l'élément « Application Config »

L'objet "Application Config" permet de définir le type d'applications (Email, Ftp, etc...) pouvant être exécutées lors de la simulation. Pour configurer cet objet, nous choisissons l'option « Edit Attribute » après avoir effectué un clic droit sur celui-ci.

Dans le champ "Name" nous entrons "Application Config" puis dans le champ "Value " de "Application Definitions", nous sélectionnons "Default" comme le montre la Figure C.5.

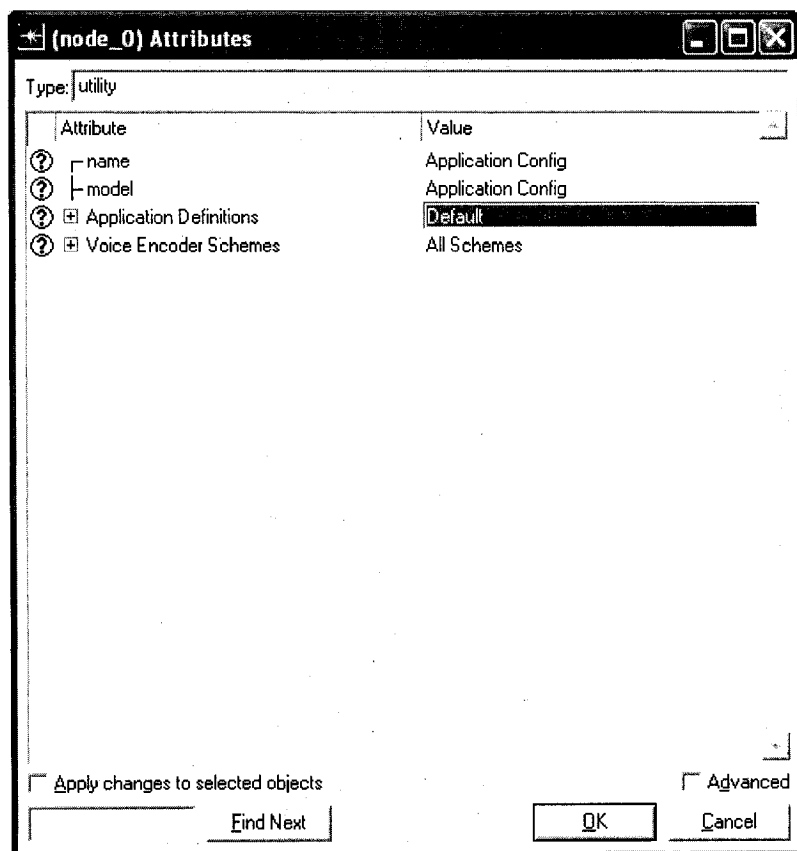


Figure C.5 Configuration de l'objet "Application Config" (1^{ère} partie)

Nous poursuivons la configuration déployant la branche « Application Definition » en appuyant sur le symbole « + ». Nous choisissons alors la ligne 4 (File Transfert Heavy), puis nous déployons le menu « Description ». Nous cliquons alors sur le choix « Ftp » puis nous passons en mode édition tel qu'illustré sur la Figure C.6.

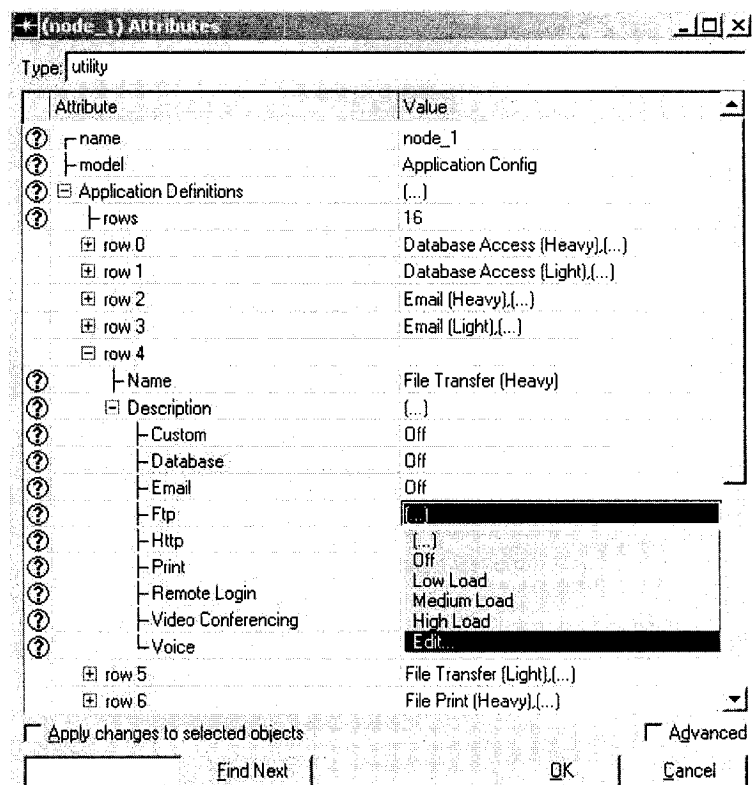


Figure C.6 Configuration de l'objet "Application Config" (2^e partie)

Nous entrons alors la configuration suivante :

Paramètres	Valeur
Command Mix (Get/Total)	100%
Inter-Request Time	Constant(0.05)
File Size	Constant(250000)
Symbolic Server Name	FTP Server
Type of Service	Best Effort(0)
RSVP Parameters	None
Back-end Custom Application	Not Used

Les champs "Inter-Request Time" et "File Size" permettent de définir la taille des

fichiers à télécharger, de même que le débit. Dans le cas de cette configuration, nous avons défini des fichiers de 2 Mbits (250000 octets) et un débit maximal de 40Mbps (20 requêtes par seconde). Une fois ces paramètres saisis, nous appuyons sur « Ok » pour valider la configuration de l'application Ftp.

Pour terminer la configuration de l'objet « Application Config », nous faisons montrer l'application « File Transfert Heavy » de la ligne 4 à la première ligne. Pour ce faire, nous effectuons un clic droit sur « row 4 » et sélectionnons l'option « Move Row Up ». Nous répétons cette dernière manœuvre jusqu'à ce que l'application « File Transfert Heavy » soit configurée sur la première ligne (row 0).

C.3 Configuration de l'élément « Profil Config »

L'objet "Profil Config" permet de définir comment l'application Ftp que nous avons définie sera utilisée durant la simulation. Pour configurer cet objet, nous choisissons l'option « Edit Attribute » après avoir effectué un clic droit sur celui-ci.

Dans le champ "Name" nous entrons "Profil Config" puis nous déployons la branche « Profile Configuration ». Nous choisissons ensuite la valeur 1 dans le sous menu rows comme le montre Figure C.7.

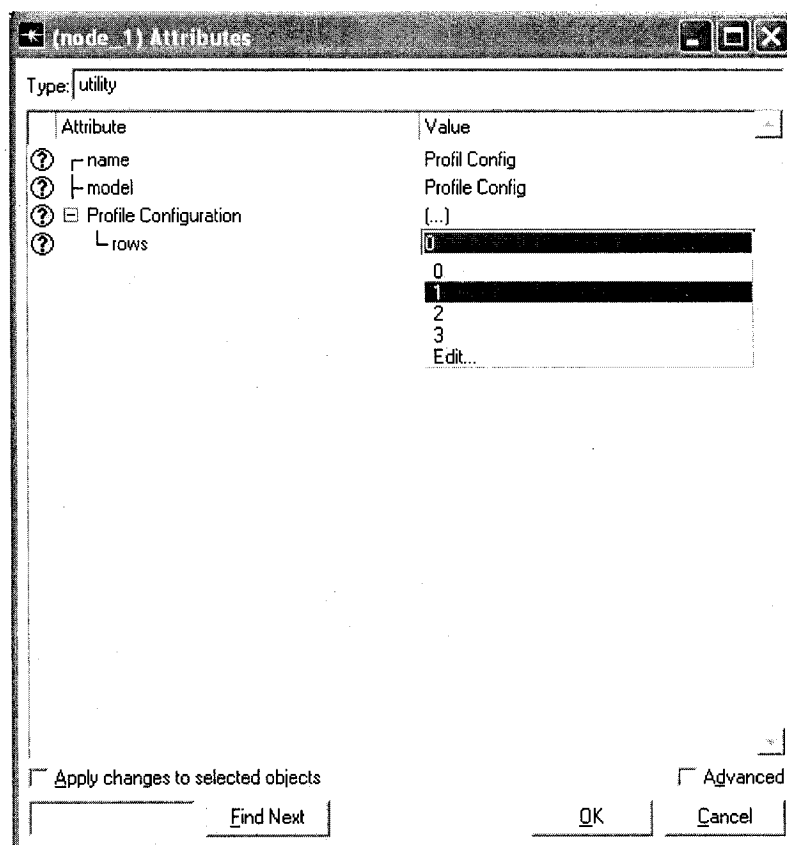


Figure C.7 Configuration de l'objet "Profil Config" (1^{ère} partie)

Nous configurons alors la rangée 0 avec les paramètres qui sont présentés à la Figure C.8.

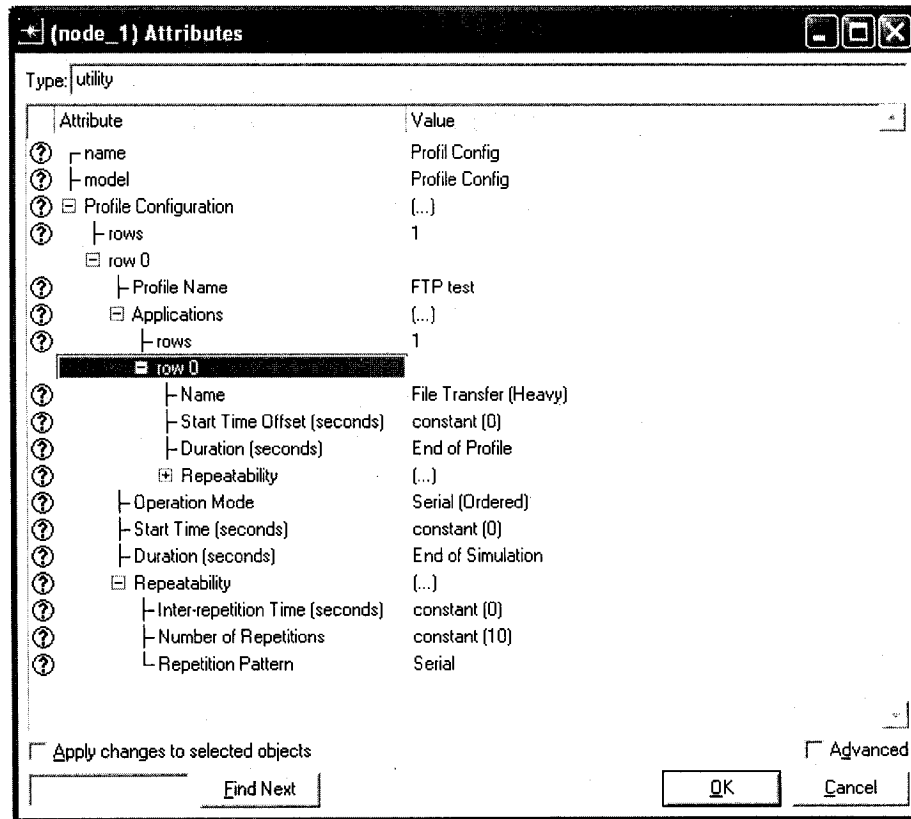


Figure C.8 Configuration de l'objet "Profil Config" (2^e partie)

Ces paramètres définissent un profil qui utilise l'application « File Transfert (Heavy) » sans arrêt pour toute la durée de la configuration. Pour valider ces nouveaux paramètres nous terminons la configuration en appuyant sur le bouton « Ok ».

C.4 Configuration des serveurs

Pour configurer les serveurs, nous choisissons l'option « Edit Attributes » de leur menu contextuel. Pour le premier serveur, nous entrons « serveur1 » pour nom ainsi que pour le champ « Server Address ». La position du serveur peut être fixée précisément grâce aux champs "x position" et "y position".

Nous poursuivons alors la configuration du serveur en entrant la configuration propre au protocole IEEE 802.11. Nous entrons les valeurs des paramètres comme illustrées à la Figure C.9. Il est important de noter que c'est ici que nous configurons le serveur pour qu'il agisse en point d'accès à l'aide du paramètre « Access Point Functionality ». C'est également ici que nous définissons le canal utilisé ainsi que le taux de transfert du serveur.

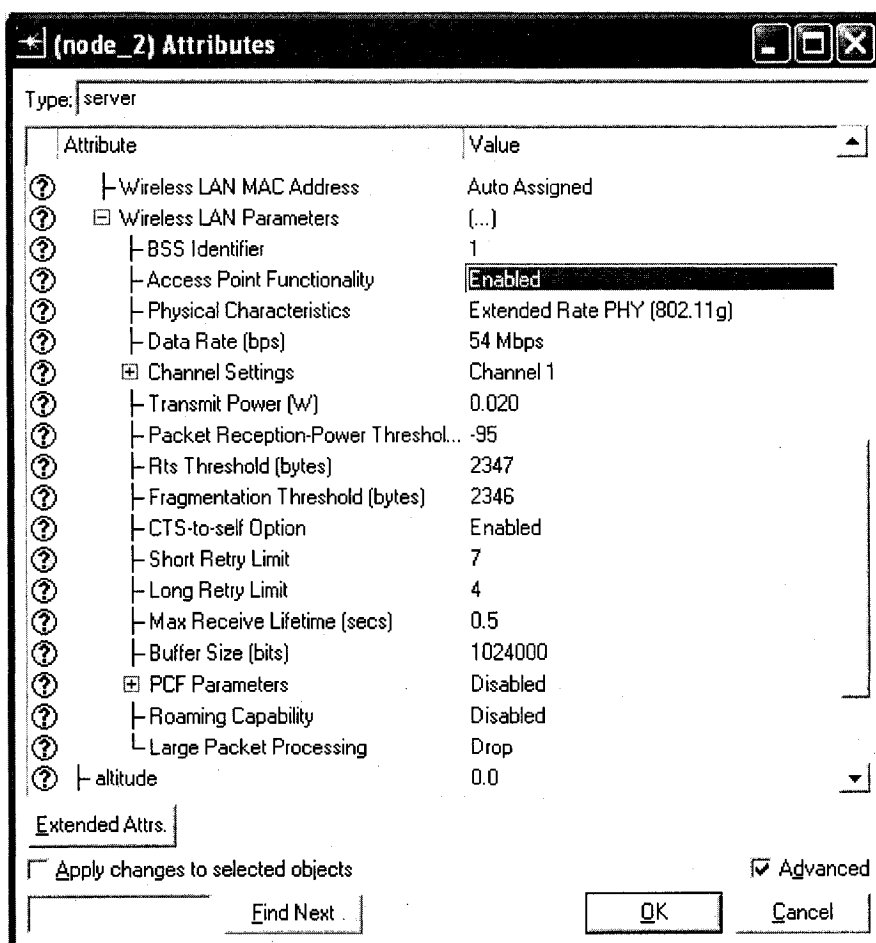


Figure C.9 Configuration des serveurs (1^{ère} partie)

Nous définissons maintenant les applications que ce serveur supportera. Pour ce faire nous cliquons dans le champ "Value" de "Application : Supported Services" et choisissons « edit ». Une nouvelle fenêtre apparaît alors. Nous cliquons dans le champ "Description", choisissons "Edit", puis configurons tel qu'illustré sur la Figure C.10.

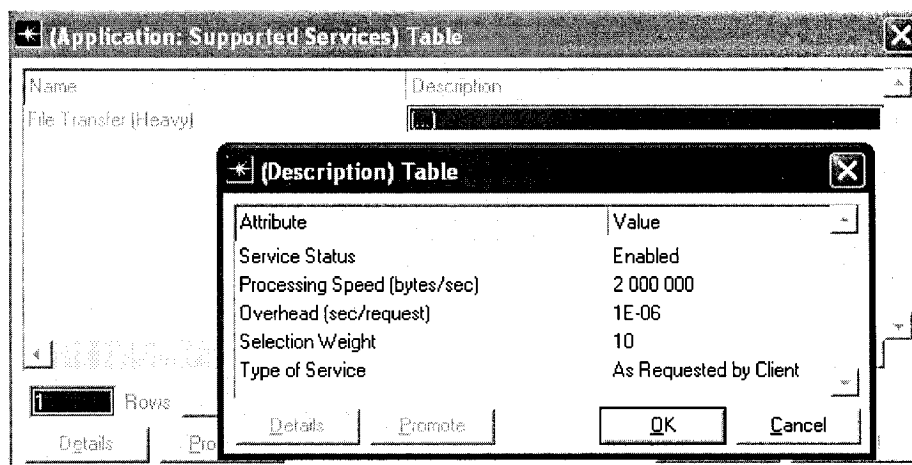


Figure C.10 Configuration des serveurs (2^e partie)

Cette étape termine la configuration du serveur. Nous répétons les mêmes étapes pour le serveur 2. Nous prenons cependant soin de changer son nom, son adresse, son emplacement, le BSSId ainsi que son canal de communication.

C.5 Configuration des stations

La configuration des stations clientes se fait sur le même principe que les serveurs. Seule la partie configuration de l'application change. Ainsi nous cliquons sur le champ "Value" de "Application Supported Profile" et choisissons "Edit". Dans le champ "Rows", nous sélectionnons "1", cliquons sur "None", puis choisissons "Ftp Test". La Figure C.11 illustre la configuration désirée.

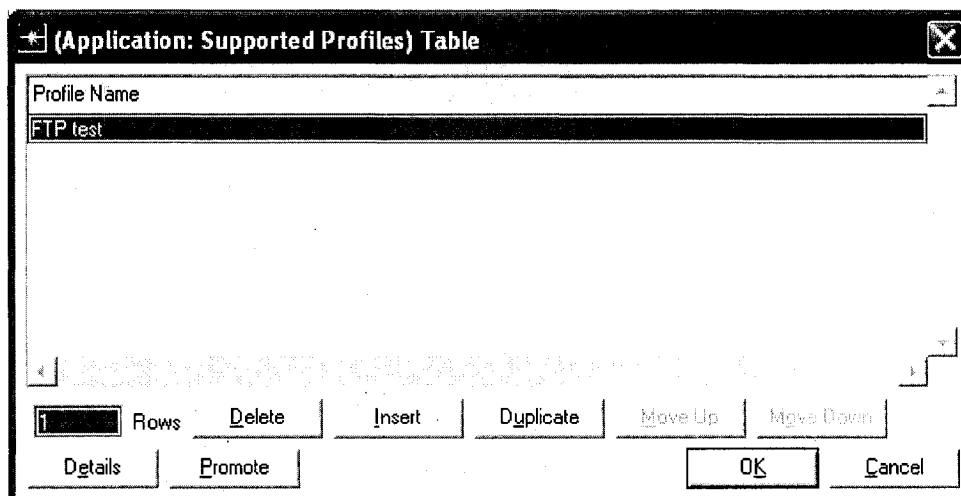


Figure C.11 Configuration des stations (1^{ère} partie)

Nous devons ensuite choisir le serveur vers lequel le client dirige ses requêtes. Pour ce faire, nous éditons le champ « Value » de « Application Destination Preferences ». Nous choisissons alors l'application désirée en plus de choisir le serveur en éditant le champ « Actual Name » (voir Figure C.12).

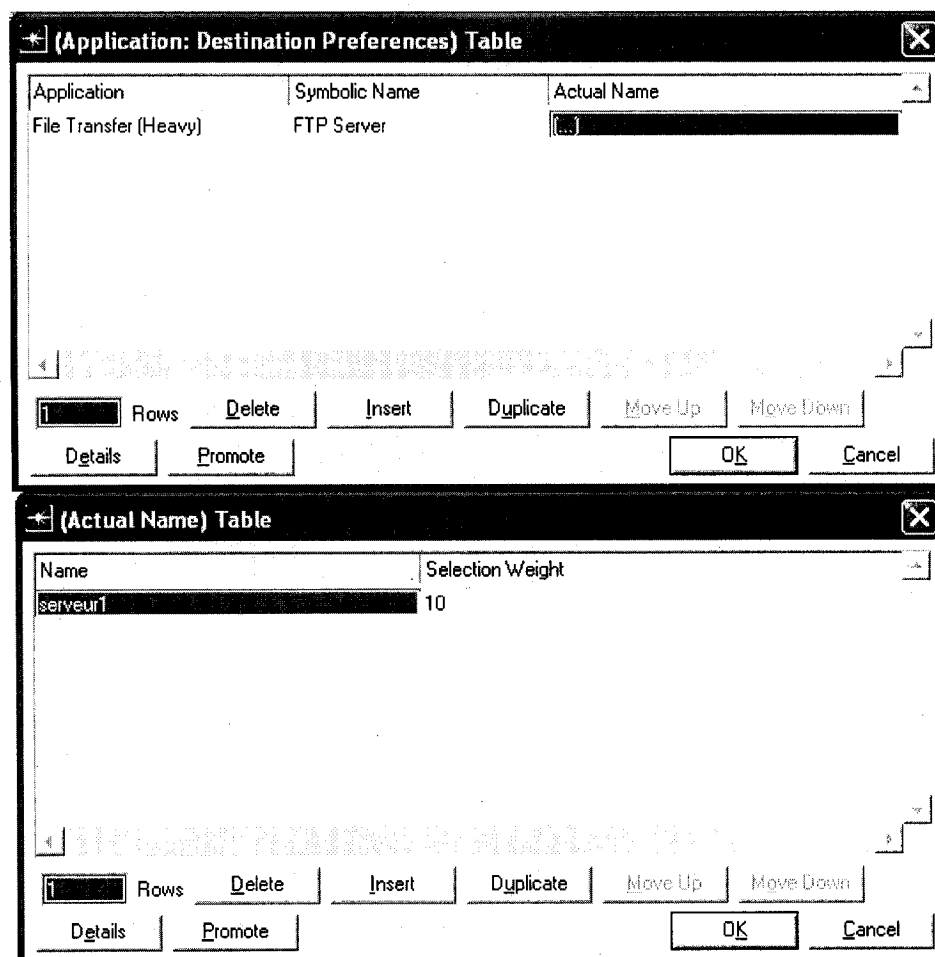


Figure C.12 Configuration des stations (2^e partie)

C.6 Configuration de la cueillette de statistiques

Avant d'effectuer des simulations, nous devons sélectionner les statistiques que nous désirons recueillir. Pour ce faire il suffit de sélectionner l'option "Choose Individual DES Statistics" à partir du menu contextuel d'un serveur ou d'une station. Nous cochons alors simplement les statistiques que nous voulons recueillir lors des simulations. La Figure C.13 présente le menu de configuration pour la cueillette de statistiques.

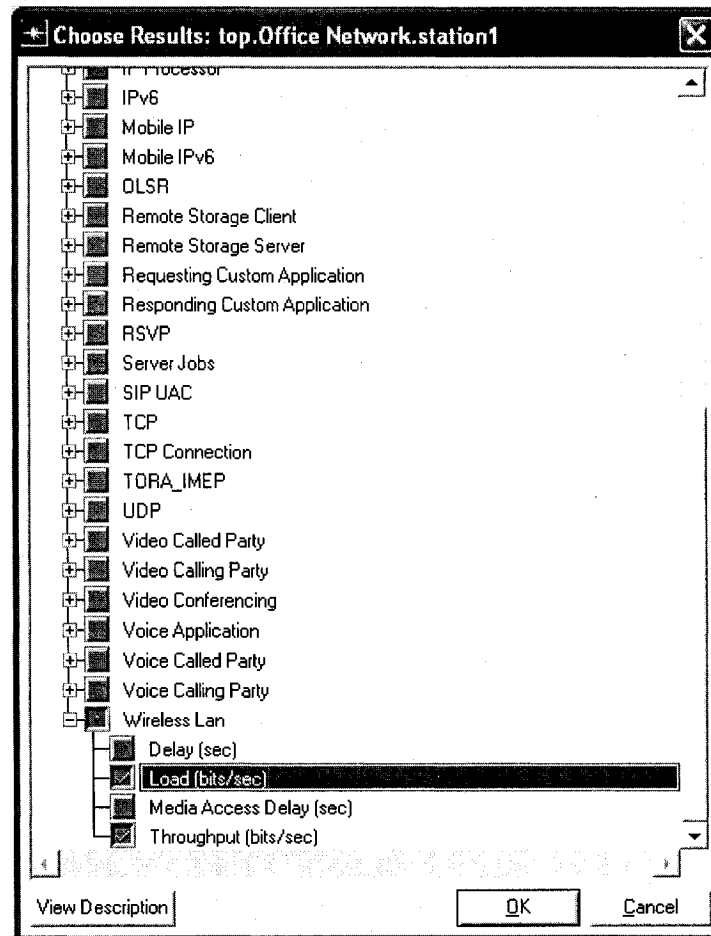


Figure C.13 Configuration de la cueillette de statistiques

C.7 Copie des scénarios et simulations

L'environnement étant configuré, les simulations peuvent être effectuées. Un moyen permettant de gagner du temps lors de la réalisation des simulations est d'effectuer une duplication de scénarios. En effet dans notre cas, nous avons besoin de faire varier les canaux des stations afin de mesurer leur effet sur les communications. Au lieu de créer plusieurs projets, nous créons plusieurs scénarios dans le même projet de manière à gagner du temps. Pour ce faire, nous choisissons l'option "Duplicate Scenario" du menu "Scenarios" d'OPNET (voir Figure C.14). Nous entrons alors un nom pour le scénario dupliqué et effectuons les modifications pour ce scénario

(changement de canal d'opération). Nous répétons ces étapes pour générer tous les scénarios que nous voulons créer.

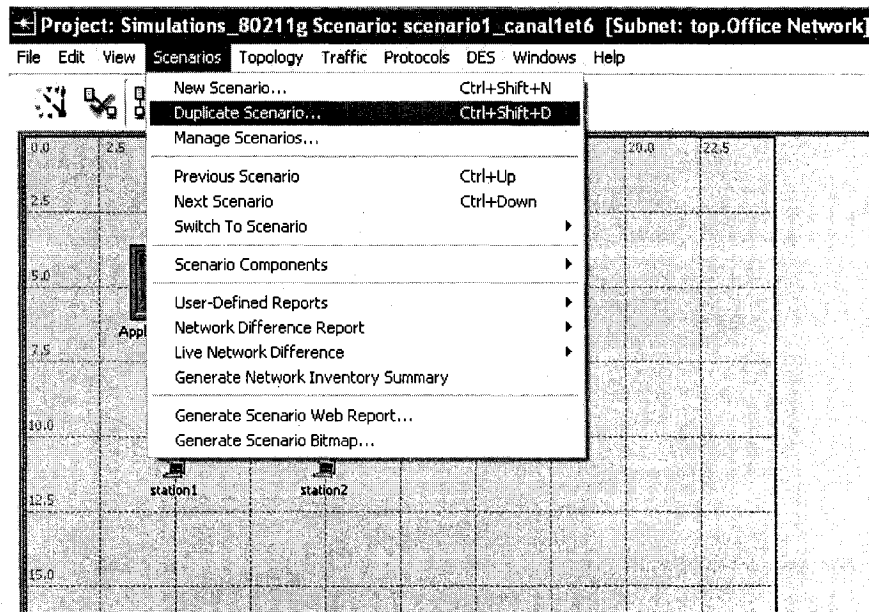


Figure C.14 Emplacement de l'option "Duplicate scenario"

Une fois tous les scénarios créés, nous cliquons sur "Manage Scenarios" dans l'onglet "Scenarios" pour configurer les scénarios à simuler. Un scénario sera simulé si nous sélectionnons l'option « collect » dans la colonne résultats de ce scénario. La Figure C.15 montre cette fenêtre de configuration où il suffit de cliquer sur "Ok" pour lancer les simulations.

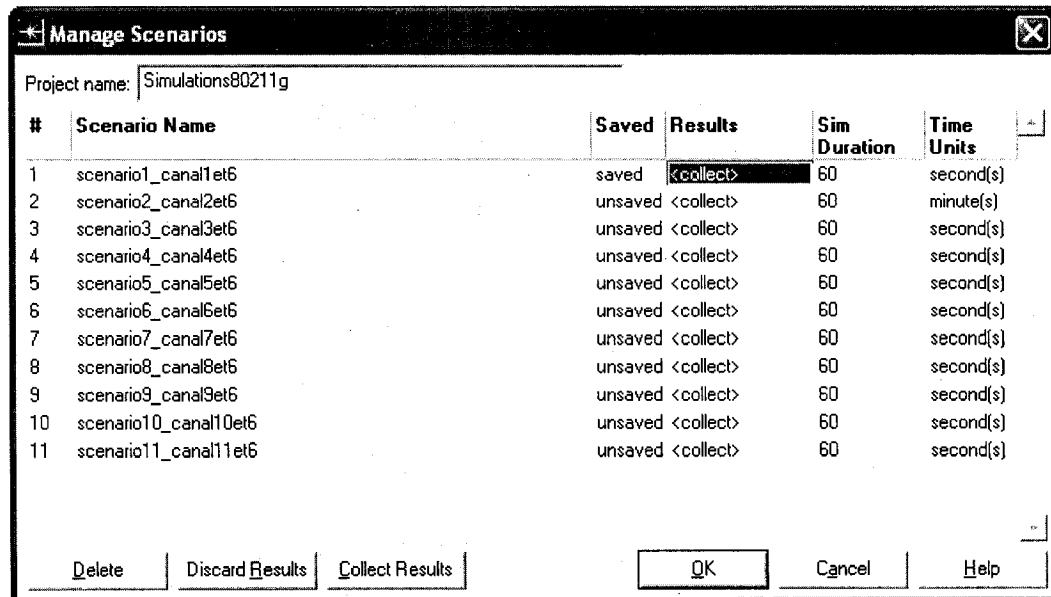


Figure C.15 Écran de configuration pour la gestion des scénarios

ANNEXE D

L'ALPHABET IEEE 802.11

IEEE 802.11	Le standard original opérant à 1 Mbit/s et 2 Mbit/s dans la bande 2.4 GHz RF et la bande infrarouge (1999)
IEEE 802.11a	Standard atteignant 54 Mbit/s dans la bande 5 GHz (1999, 1er produit en 2001)
IEEE 802.11b	Amélioration du 802.11 original pour supporter des vitesses de 5.5 et 11 Mbit/s (1999)
IEEE 802.11c	Modification au standard LAN pour accommoder les trames 802.11; inclus dans le standard IEEE 802.1D (2001)
IEEE 802.11d	Assure l'harmonisation des standards dans les différents pays (2001)
IEEE 802.11e	Défini des améliorations au niveau de la qualité de service (2005)
IEEE 802.11F	Communication entre les points d'accès(2003) Retiré en 2005
IEEE 802.11g	Standard atteignant 54 Mbit/s dans la bande 2.4 GHz (rétro-compatible avec b) (2003)
IEEE 802.11h	Gestion du spectre (5 GHz) dans le 802.11a pour la compatibilité européenne (2004)
IEEE 802.11i	Amélioration de la sécurité (2004)
IEEE 802.11j	Extensions pour le Japon utilisant la bande 4,9 GHz à 5 GHz (2004)
IEEE 802.11k	Amélioration de l'utilisation des ressources radio
IEEE 802.11m	Maintenance des standards 802.11 et ses spécifications
IEEE 802.11n	Amélioration de la vitesse de transfert par utilisation d'antennes MIMO
IEEE 802.11p	Amélioration au standard 802.11 pour supporter la transmission de données entre véhicule se déplaçant à grande vitesse
IEEE 802.11q	Réservé, pour éviter la confusion avec le <u>802.1Q</u> (VLAN trunking)
IEEE 802.11r	Standard définissant la relève rapide (Fast roaming)
IEEE 802.11s	Configuration automatique des chemins dans un réseau ESS en maille
IEEE 802.11T	Wireless Performance Prediction (WPP) – méthodologie de tests et métriques
IEEE 802.11u	Interoperabilité avec des réseaux non-802 (i.e. cellulaire)
IEEE 802.11v	Gestion des réseaux sans fil
IEEE 802.11w	Amélioration de la sécurité des trames de gestion

802.11F et 802.11T sont des recommandations et non des standards ce qui est indiqué par la lettre majuscule.