ÉCOLE DE TECHNOLOGIE SUPÉRIEURE
UNIVERSITÉ DU QUÉBEC

MÉMOIRE PRÉSENTÉ À
L'ÉCOLE DE TECHNOLOGIE SUPÉRIEURE

COMME EXIGENCE PARTIELLE
À L'OBTENTION DE LA
MAÎTRISE EN GÉNIE
CONCENTRATION RÉSEAUX DE TÉLÉCOMMUNICATIONS
M.Ing.

PAR
Clément ROUSSEAU

CONCEVOIR UNE STRATÉGIE DE DÉFENSE FACE AUX COMPORTEMENTS ÉGOISTES DE NŒUDS UTILISANT LE PROTOCOLE MAC IEEE 802.11

MONTRÉAL, LE 2 SEPTEMBRE 2011

PRÉSENTATION DU JURY

CE MÉMOIRE A ÉTÉ ÉVALUÉ

PAR UN JURY COMPOSÉ DE :

M. Jean-Marc Robert, directeur de mémoire
Département de génie logiciel et des technologies de l'information à l'École de technologie supérieure

M. Michel Kadoch, président du jury
Département de génie électrique à l'École de technologie supérieure

M. Abdelouahed Gherbi, membre du jury
Département de génie logiciel et des technologies de l'information à l'École de technologie supérieure

IL A FAIT L'OBJET D'UNE SOUTENANCE DEVANT JURY ET PUBLIC

LE 24 AOÛT 2011

À L'ÉCOLE DE TECHNOLOGIE SUPÉRIEUR

REMERCIEMENTS

Je tiens à exprimer en premier lieu ma gratitude à mon directeur de recherche, Monsieur Jean-Marc Robert. Il a su me guider, m'accompagner tout au long de ma maîtrise à l'ÉTS. J'ai particulièrement apprécié son suivi et son soutien.

Merci également aux responsables respectifs des études internationales de Telecom Lille1 et de l'ÉTS, en particulier Monsieur Eric Doré qui m'ont permis de venir réaliser ce cursus à l'ÉTS.

Enfin, je tiens à remercier toutes les personnes que j'ai côtoyées durant cette maîtrise et sans lesquelles ce parcours n'aurait pas été aussi enrichissant.

CONCEVOIR UNE STRATÉGIE DE DÉFENSE FACE AUX COMPORTEMENTS ÉGOISTES DE NŒUDS UTILISANT LE PROTOCOLE MAC IEEE 802.11

Clément ROUSSEAU

RÉSUMÉ

La coopération de l'ensemble des nœuds d'un réseau ad-hoc permet de garantir le fonctionnement optimal de celui-ci. Un nœud peut toutefois avoir un comportement égoïste au niveau de la sous-couche MAC du protocole IEEE 802.11 qui gère le contrôle de l'accès au médium. Ce comportement égoïste peut se traduire par une diminution de la taille de la fenêtre de contention afin d'augmenter la priorité d'émission. La conséquence d'un tel comportement pour un nœud est une amélioration de sa capacité d'émission, de son débit, entrainant une dégradation de la bande passante de l'ensemble du réseau.

Dans cette étude nous concevons une stratégie de défense basée sur la stratégie Tit-for-Tat (TFT), développée en théorie des jeux pour faire face à ces comportements égoïstes. Nous démontrerons pourquoi et comment une telle stratégie vise à obtenir l'équité dans le partage de la bande passante. Nous introduirons des variantes de TFT comme un Tit-for-Tat généreux (GTFT), où l'introduction d'un facteur de générosité va permettre de s'adapter aux contraintes du médium. Enfin nous discuterons du choix et de l'influence des paramètres d'une telle stratégie sur le comportement d'un nœud et du réseau.

Mots clés : réseaux ad-hoc, MAC, CSMA/CA, TFT, GTFT

DESIGN A DEFENSE STRATEGY AGAINST THE SELFISH BEHAVIOR OF NODES USING IEEE 802.11 MAC PROTOCOL

Clément ROUSSEAU

ABSTRACT

The cooperation of all nodes of an ad hoc network guarantees the optimal performance of this network. However, a node can behave selfishly at the MAC sublayer of IEEE 802.11 protocol which manages the access control to the medium. Such a selfish behavior can decrease the size of the contention windows in order to increase the priority of the transmission. The consequence of such a behavior for a node is an improvement on its throughput. This should lead to a decrease of the network bandwidth.

In this research, we design a defense strategy based on the Tit-for-Tat strategy (TFT). TFT was designed in game theory to deal with selfish behaviors. We will demonstrate why and how such a strategy aims to achieve fairness in sharing bandwidth. We will introduce variations of the TFT strategy as generous Tit-for-Tat (GTFT). The generosity factor is going to allow us to adapt ourselves to the constraints of the medium. Finally we will discuss the choice and the parameters influence of such a strategy on the behavior of the node and the entire network.

Keywords: Ad-hoc Networks, MAC, CSMA/CA, TFT, GTFT

TABLE DES MATIÈRES

Page

INTRODUCTION 1

CHAPITRE 1 CONTEXTE 5
1.1 Les réseaux ad-hoc 5
1.1.1 Définition 5
1.1.2 Utilité 5
1.1.3 Inconvénients 6
1.2 Le Wifi et les normes IEEE 802.11 6
1.2.1 L'IEEE 6
1.2.2 Les différentes normes 6
1.3 Fonctionnement de la sous-couche MAC 7
1.3.1 Rôle 7
1.4 La fonction DCF 8
1.4.1 Accès au médium 8
1.4.2 BEB 8
1.4.3 Fiabilité de transmission 9
1.4.4 Problème du terminal caché 9
1.4.5 L'échange RTS/CTS 10
1.4.6 Temps d'attente 11
1.4.7 Schéma explicatif 11

CHAPITRE 2 PROBLÉMATIQUE 13
2.1 Le phénomène de la triche dans le partage du médium 13
2.1.1 Définition, qu'est-ce que la triche ? 13
2.1.2 La motivation, pourquoi tricher ? 13
2.1.3 Le moyen, comment tricher ? 13
2.1.4 Modèle de réseau utilisé pour les simulations 14
2.1.5 Test témoin 15
2.1.6 Test du phénomène de triche 16
2.1.7 Impacts et conséquences de la triche 18
2.2 Problématique 19
2.2.1 Constat 19
2.2.2 Définition de la problématique 19

CHAPITRE 3 REVUE DE LITTÉRATURE 21
3.1 La coopération dans les réseaux 21
3.1.1 Introduction 21
3.1.2 Le comportement égoïste 22
3.1.3 Détection du comportement 23
3.1.4 Réaction face à un nœud égoïste 26
3.2 Théorie des jeux et stratégies 27

3.2.1 Définition 27
3.2.2 Sources 27
3.2.3 Le dilemme du prisonnier 27
3.2.4 Extensions et applications du dilemme du prisonnier 29
3.2.5 Stratégies pour le dilemme du prisonnier répété 31
3.2.6 Tit For Tat 33
3.2.7 Generous Tit For Tat 34
3.2.8 Reputation Tit For Tat 35
3.3 Les jeux répétés dans les réseaux sans fils 36

CHAPITRE 4 TIT FOR TAT 41
4.1 Introduction 41
4.1.1 Nos objectifs 41
4.1.2 Implémentation dans NS2 41
4.1.2.1 Le scénario 42
4.1.2.2 La couche MAC dans NS2 42
4.2 Tit-For-Tat 43
4.2.1 Introduction de TFT dans le contexte 43
4.2.2 Comment détecter le comportement des autres nœuds ? 44
4.2.3 Comment copier le comportement adverse ? 45
4.2.4 Paramètres de TFT 47
4.2.5 Tests 48
4.2.5.1 Test TFT témoin 48
4.2.5.2 Diminution de la variation 49
4.2.5.3 Augmentation de la période 50
4.2.5.4 Augmentation de la marge d'erreur 51
4.2.6 Observations sur TFT 52
4.3 Generous Tit For Tat 53
4.3.1 Principe 53
4.3.2 Implémentation 54
4.3.3 Choix du facteur de générosité 55
4.3.4 Tests 55
4.3.4.1 Tests de pertes 55
4.3.4.2 Discussion des résultats 57
4.3.4.3 Tests d'introduction d'un tricheur 58
4.3.4.4 Discussion des résultats 59
4.3.5 Bilan de GTFT 60
4.4 RTFT 61
4.4.1 Le principe de la réputation 61
4.4.2 Implémentation 61
4.4.3 Influence de la relativité 62
4.4.4 Tests 62
4.4.5 Discussion des résultats 64
4.5 Conclusion et comparaison 65

CONCLUSION.....67

RÉFÉRENCES BIBLIOGRAPHIQUES.....71

LISTE DES TABLEAUX

Page

Tableau 1 Comparatif des normes 802.11 7

Tableau 2 Modèle de réseau pour la simulation 14

Tableau 3 Matrice de gains du dilemme du prisonnier.....28

Tableau 4 Matrice utilisée par Axelrod (1988).....32

Tableau 5 Impact des erreurs avec TFT.....34

Tableau 6 Impact des erreurs avec GTFT.....35

Tableau 7 Influence des paramètres.....65

LISTE DES FIGURES

Page

Figure 1.1 Problème du terminal caché 10

Figure 1.2 Fonctionnement de CSMA/CA 11

Figure 2.1 Graphique témoin du débit moyen 16

Figure 2.2 Apparition progressive de tricheurs 17

Figure 2.3 Apparition de tricheurs - débit moyen 18

Figure 3.1 CRISP (Konorski, 2006) 38

Figure 4.1 Graphique TFT témoin 49

Figure 4.2 TFT, variation 10% 50

Figure 4.3 TFT, période : 10secondes 51

Figure 4.4 TFT, marge d'erreur : 10% 52

Figure 4.5 GTFT, générosité : 10% 56

Figure 4.6 GTFT, générosité : 20% 57

Figure 4.7 GTFT, un tricheur, générosité : 10% 58

Figure 4.8 GTFT, un tricheur, générosité : 20% 59

Figure 4.9 RTFT, relativité : 50% 63

Figure 4.10 RTFT, un tricheur, relativité : 50% 64

LISTE DES ABRÉVIATIONS, SIGLES ET ACRONYMES

ACK	Acknowledgement
AP	Access Point
BEB	Binary Exponential Backoff
CTS	Clear-To-Send
CW	Contention windows
CWmin	Minimum Contention Windows
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
DCF	Distributed coordination Function
DIFS	DCF InterFrame Space
DSSS	Direct Sequence Spread Spectrum
GTFT	Generous Tit For Tat
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
LLC	Logical Link Control
MAC	Medium Access Control
MANET	Mobile Ad-hoc Network
NS2	Network Simulator 2
OFDM	Orthogonal Frequency Division Multiplexing
RTFT	Reputation Tit For Tat
RTS	Request To Send
SIFS	Short InterFrame Space

TCL	Tool Command Language
TFT	Tit for Tat
WEP	Wired Equivalent Privacy
WPA	Wifi Protected Access

INTRODUCTION

Le domaine des télécommunications a vécu des évolutions majeures ces dernières décennies. Tout d'abord il y a eu l'évolution des moyens de communications filaires et des machines informatiques. Ceci a entrainé la démocratisation des télécommunications dans de nombreux pays, ce qui a permis un accès de la population à des espaces de communication virtuels comme l'Internet.

Par la suite, les évolutions techniques de transmissions par radiofréquence ont fait émerger un nouveau type de communication par ondes radio : le Wifi. Ce dernier apporte la mobilité aux télécommunications, permettant une plus grande flexibilité et souplesse d'utilisation. Les usages deviennent alors de plus en plus importants. Des points d'accès sont déployés dans les réseaux de transport, les cafés, les parcs. Certaines villes déploient même leur propre réseau Wifi.

Après cette démocratisation et l'accès à cette mobilité, les MANETS pourraient permettre une libéralisation encore plus grande des télécommunications. Les MANETS sont des réseaux ad-hoc sans fils mobiles n'ayant aucune architecture préexistante (voir définition partie I). Le terme MANET signifie *Mobile Ad-hoc Network*, et provient du groupe de travail de l'IETF du même nom, il est couramment utilisé pour désigner un réseau ad-hoc. Notons que formellement un réseau MANET n'utilise pas forcément la technologie Wifi. Cependant, les normes Wifi de l'IEEE s'étant imposées dans le domaine des télécommunications, par pragmatisme, nous nous concentrerons uniquement dessus.

Cette absence d'infrastructure préalable permet à n'importe quel groupe de nœuds de créer un réseau ad-hoc. Au sein du réseau, un nœud peut être connecté à un autre réseau comme l'Internet par exemple, et d'en faire bénéficier l'accès aux utilisateurs du réseau ad-hoc. L'objectif ambitieux des MANETS est de donner aux nœuds la capacité de s'organiser et de former les espaces de communication. Ceux-ci ne seront plus limités à une structure ou à

l'emplacement des points d'accès mais définis suivant le besoin et la capacité des nœuds présents. C'est une libéralisation des télécommunications.

Cette auto-organisation des réseaux n'est possible que si les nœuds coopèrent entre eux afin de tenter de fournir les services demandés par l'ensemble des nœuds du réseau. En effet, pour un résultat attendu, normal, chaque nœud doit coopérer en suivant les protocoles de communication en vigueur et participer aux opérations de routage des paquets. Cependant chaque nœud étant indépendant, il peut être tenté par égoïsme d'augmenter son propre profit. Dans notre étude, nous faisons l'hypothèse qu'un utilisateur malicieux cherchant à obtenir plus que sa part juste et équitable de la bande passante peut modifier le firmware de sa machine mettant en œuvre la sous-couche MAC proposé par la norme IEEE 802.11. Nous verrons l'influence de ce comportement égoïste sur le réseau. Nous faisons aussi l'hypothèse que les utilisateurs malicieux sont rationnels. Ils se comporteront égoïstement tant et aussi longtemps qu'ils en obtiendront un avantage stratégique. Nous étudierons ses conséquences et tenterons d'étudier une stratégie de défense face à ce phénomène. Cette stratégie pourrait être une solution pouvant s'implémenter au niveau du standard utilisé.

Afin d'avoir les notions nécessaires à ces travaux, la partie I présentera le contexte, c'est-à-dire le type de réseaux, ses avantages et inconvénients, les normes ainsi que le fonctionnement de la sous-couche MAC qui seront des éléments indispensables pour la compréhension de la suite de l'étude.

Ensuite, nous pourrons établir un constat en caractérisant un comportement égoïste, ses motivations et impacts sur chaque nœud du réseau. Nous mettrons en évidence le dilemme posé et ceci nous permettra de définir la problématique : comment concevoir une stratégie de défense face à un tel comportement.

Puis nous analyserons les travaux de recherche préexistant sur ce sujet. Nous ferons un parallèle avec la théorie des jeux non-coopératifs en introduisant certaines stratégies et

certaines tentatives d'adaptation dans le même cadre, face à une même problématique. Nous verrons leurs avancées et limitations.

Enfin nous mettrons en place la stratégie Tit-for-Tat (TFT) ainsi que ces variantes dans notre contexte. Des tests simulés seront réalisés via NS2, un simulateur d'événements discrets qui est couramment utilisé pour la simulation de réseaux informatiques. Nous étudierons l'influence du choix des paramètres de la stratégie utilisée sur son fonctionnement et celui du réseau.

Ainsi nous présenterons dans ce mémoire, une tentative d'adaptation de stratégies issues de la théorie des jeux pour faire face à un comportement égoïste au niveau de la couche MAC du protocole IEEE 802.11, un problème dont nous verrons que les solutions existantes sont contraignantes ou limitées.

CHAPITRE 1

CONTEXTE

1.1 Les réseaux ad-hoc

1.1.1 Définition

Un réseau ad hoc est un réseau s'organisant de manière autonome. Il ne possède pas d'infrastructure préexistante et n'est donc pas rattaché à un point d'accès (qui s'occupe du routage). Lorsque les nœuds de ce réseau sont mobiles, nous pouvons parler de MANET. La mobilité des nœuds influant sur leurs performances, nous nous concentrerons uniquement sur des nœuds fixes. Nous parlerons ainsi de réseau ad-hoc et non de MANET dans la suite de cette étude.

> *«* Un réseau ad hoc comprend des plates-formes mobiles (par exemple, un routeur interconnectant différents hôtes et équipements sans fil) appelées nœuds qui sont libres de se déplacer sans contrainte. Un réseau ad hoc est donc un système autonome de nœuds mobiles. Ce système peut fonctionner d'une manière isolée ou s'interfacer à des réseaux fixes au travers de passerelles*»* (traduit de l'IETF, RFC 2501, 1999).

1.1.2 Utilité

Le fait de ne pas avoir d'infrastructure préexistante peut être un atout dans de nombreuses situations. Le réseau ad-hoc peut ainsi être déployé facilement et être décentralisé. Il se révèle donc très utile dans des situations d'urgence, des guerres ou des catastrophes naturelles. Grâce à son absence de hiérarchie, le mode ad-hoc à un fonctionnement très égalitaire, aucun nœud n'étant supérieur à un autre.

1.1.3 Inconvénients

L'absence d'infrastructure possède de nombreux défauts. En effet, il n'y a personne à qui faire confiance puisque aucune autorité n'existe. La sécurité est donc un problème majeur des réseaux ad-hoc. De plus, chaque nœud étant indépendant, il peut choisir de respecter ses propres règles de communication lui donnant un avantage certain sur les autres nœuds. Un tel nœud pourrait ne pas respecter les règles de communication pour augmenter ses propres performances. L'indépendance et l'absence de confiance permettent donc une forme de triche. Nous reviendrons tout particulièrement sur cet exemple dans la description de la problématique.

1.2 Le Wifi et les normes IEEE 802.11

1.2.1 L'IEEE

Les normes concernant les communications Wifi sont définies par l'IEEE (*Institute of Electrical and Electronic Engineers*). Les normes 802.11 définissent les services et protocoles de la couche physique et de la sous-couche MAC du modèle que l'on utilise. Les spécifications des normes et de la couche MAC présentées proviennent des standards de l'IEEE. La section qui suit présente les différentes normes.

1.2.2 Les différentes normes

Différentes versions de normes existent. Elles peuvent différer dans leur paramétrage mais aussi dans certains de leurs fonctionnements. Elles ont été créées suivant les différents besoins ou problèmes rencontrés. Ainsi, certaines peuvent avoir différentes utilités, comme être réservées pour l'armée, et d'autres sont des évolutions des normes précédentes.

Au niveau physique, les normes définissent les divers paramètres comme la vitesse, la bande de fréquence ou encore le type de modulation utilisé. Quelques différences sont présentées dans le tableau ci-dessous.

Tableau 1 Comparatif des normes 802.11

Norme	**Fréquence**	**Débit**	**Couverture**	**technologie**
802.11a	5GHz	54Mbit/s	50-300m	OFDM
802.11b	2.4GHz	11Mbit/s	100m	DSSS
802.11g	2.4GHz	54Mbit/s	150m	OFDM, DSSS
802.11n	2.4GHz ou 5GHz	540Mbit/s	150m	OFDM

Au niveau de la sous-couche MAC, les changements sont un peu moins importants. Nous verrons plus loin qu'il y a eu des évolutions comme l'échange RTS/CTS qui ont permis de résoudre certains problèmes. Il est à noter que malgré les évolutions, la couche MAC a du garder une compatibilité avec la couche LLC afin que l'évolution reste la plus transparente possible pour les autres couches du modèle, le but étant que la rétrocompatibilité puisse se faire aisément.

1.3 Fonctionnement de la sous-couche MAC

1.3.1 Rôle

La sous-couche MAC et la sous-couche LLC forment la couche liaison du modèle OSI. Dans les réseaux, elle se charge de la confidentialité des données (méthode WEP, WPA...).

La sous-couche MAC a trois objectifs :
- assurer la sécurité des données, cela peut être réalisé par une protection WEP ou WPA par exemple, pour des réseaux avec point d'accès,
- le contrôle d'accès, qui permet aux nœuds d'accéder au médium,
- la bonne transmission des données, avec un système d'accusés de réception.

Nous nous intéressons à la problématique du partage du médium, c'est donc le contrôle d'accès, permettant d'accéder à la ressource (le médium). La norme 802.11 définit deux fonctions d'accès au médium :

- PCF (*Point Coordination Function*) est une fonction qui n'est utilisée que dans de réseaux d'infrastructure, où les nœuds passent par un AP (*Access Point*) pour accéder au réseau. Ce n'est pas le cas des réseaux ad-hoc, cette fonction ne sera donc pas étudiée.
- DCF (*Distributed Coordination Function*) peut être utilisée dans tout type de réseaux. C'est le mécanisme de cette fonction qui sera étudié ici.

1.4 La fonction DCF

Elle est chargée du partage du médium entre les différentes entités du réseau. Nous allons maintenant étudier son fonctionnement.

1.4.1 Accès au médium

La quasi-totalité des équipements Wifi ne sont dotés que d'une seule antenne pour des raisons de coûts. En effet, une même antenne suffit pour pouvoir émettre et recevoir mais elle ne peut pas émettre et recevoir simultanément.
L'accès au médium est réalisé grâce au protocole CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*) qui est utilisé par la fonction DCF. Elle gère les accès au médium et évite les collisions. En effet, une collision peut survenir si deux paquets de données sont envoyés simultanément et se brouillent. CSMA/CA est dérivée de la méthode CSMA, utilisée dans les réseaux filaires.

Quand un nœud utilise la méthode CSMA/CA et qu'il veut envoyer un paquet, il écoute le canal durant une durée de temps d'un DIFS (*DCF Interframe Space*) avant l'envoi. S'il ne détecte aucune occupation du canal, le nœud émet son paquet, si le canal est occupé ou qu'une collision a eu lieu, le nœud doit attendre un temps défini par l'algorithme BEB (*Binary Exponential Backoff*) en plus d'un DIFS avant de tenter une nouvelle transmission.

1.4.2 BEB

L'algorithme BEB (*Binary Exponential Backoff*) va définir le temps d'attente après une collision ou lorsque le canal est occupé.

Le nombre à choisir est simplement tiré aléatoirement dans une fenêtre appelée fenêtre de contention (CW). Si ce temps n'était pas tiré aléatoirement mais fixé, alors, après une collision, les nœuds émettraient au même moment ce qui entrainerait surement une autre collision. Ce tirage aléatoire a pour objectif de répartir équitablement la priorité d'envoi sur le médium entre les différents nœuds.

À chaque collision, la taille de CW est doublée, jusqu'à une taille maximum, afin d'éviter une prochaine collision. Si un paquet est correctement transmis, la taille de la fenêtre est réinitialisée à son niveau minimum.

La taille initiale de la fenêtre dépend de la norme 802.11 utilisée. La plupart du temps on prendra une fenêtre de contention minimum égale à 16 ou 32 (dépendant de la norme utilisée). Notons bien que d'après les normes des l'IEEE, les nœuds s'alignent sur la fenêtre de contention la plus grande. C'est-à-dire que les nœuds pouvant utiliser une CW de 16 s'adaptent et utilisent une fenêtre de taille égale à 32 si un autre nœud du réseau ne peut pas choisir une fenêtre de contention de taille 16.

1.4.3 Fiabilité de transmission

Un paquet ACK, accusé de réception, permet de s'assurer de la transmission et annonce la fin de la communication. Si aucun ACK n'est reçu, le même paquet peut être renvoyé un certain nombre de fois. Par exemple la norme 802.11b utilise quatre tentatives.

1.4.4 Problème du terminal caché

Cependant, si les nœuds utilisent CSMA, le nombre de collisions augmente considérablement si la charge du réseau augmente. Ce problème a été résolu dans les réseaux filaires avec CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*), permet de détecter les collisions. Par contre, la détection de collisions ne peut pas être déployée dans les réseaux

Wifi, cela, à cause de la nature du médium lui-même et du problème du terminal caché expliqué.

Le problème du terminal caché est spécifique aux réseaux sans-fils. La figure 1.1 servira de support explicatif. Nous voyons dans cette figure que le nœud A et le nœud C ne peuvent pas communiquer directement, étant hors de portée l'un de l'autre. Mais, si B est en train d'écouter un paquet envoyé par A, C ne détecte pas d'occupation du canal. Il peut donc émettre lui aussi vers B, cela entrainant une possibilité de collision entre les paquets envoyés par A et par C. Ainsi, ni A ni C ne peuvent anticiper la collision, il n'est pas possible pour un nœud dans un réseau Wifi de prévenir les collisions comme sur un réseau filaire.

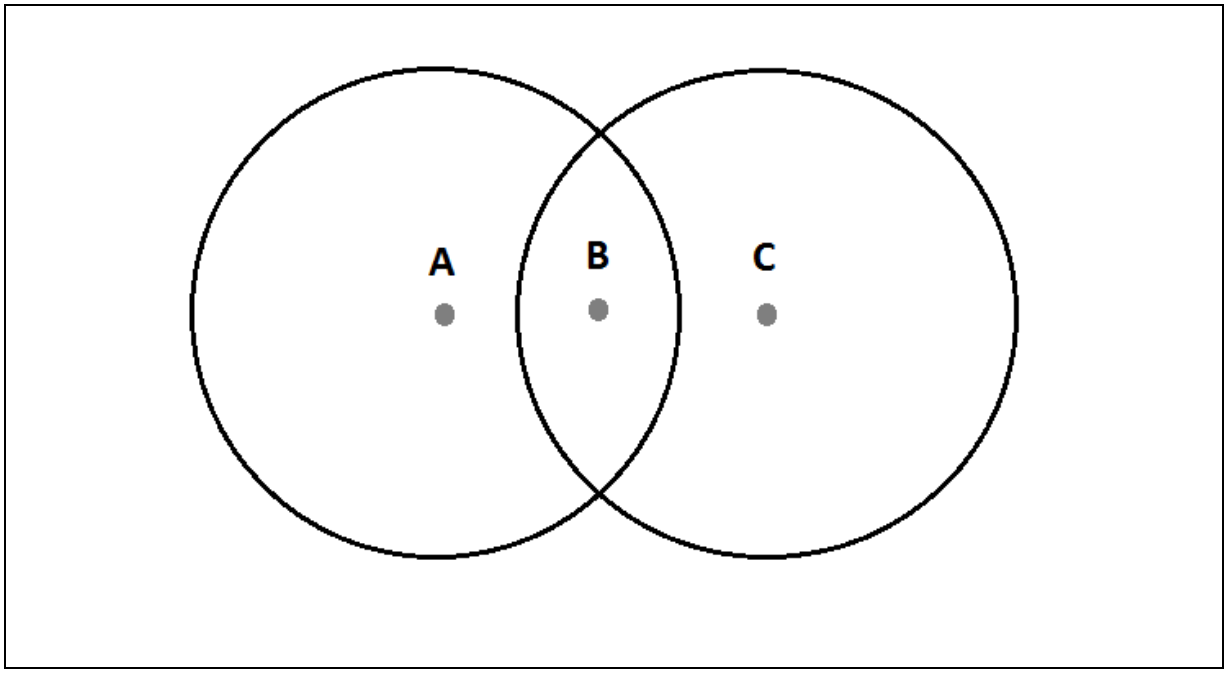

Figure 1.1 Problème du terminal caché

1.4.5 L'échange RTS/CTS

Le mécanisme RTS/CTS permet de pallier ce problème du terminal caché. Lors d'une transmission, la source envoie en premier un paquet RTS (*Request To Send*), le nœud destination répond avec un CTS (*Clear To Send*). Ces messages seront transmis a l'ensemble

des nœuds. Cet échange de messages va réserver le médium pour un temps défini dans les messages, et permet à tous les nœuds à portée de la source ou de la destination de connaître cette réservation.

Par rapport à notre exemple, si le nœud A souhaite communiquer avec B, A envoie un message RTS à B. Si B accepte la communication, il répond en émettant un CTS. Le nœud C reçoit le CTS du nœud B, C est donc averti de la durée de communication entre A et B et attendra avant d'émettre vers B. La collision est évitée.

1.4.6 Temps d'attente

Étant donné la nature du médium et afin d'assurer la communication, CSMA/CA utilise différents temps d'attente définis comme suit, du plus court au plus long:

- SIFS : Short Interframe Space
- Time Slot : intervalle utilisé par le mécanisme du backoff
- PIFS : PCF Interframe Space
- DIFS : DCF Interframe Space
- EIFS : Extended Interframe Space

1.4.7 Schéma explicatif

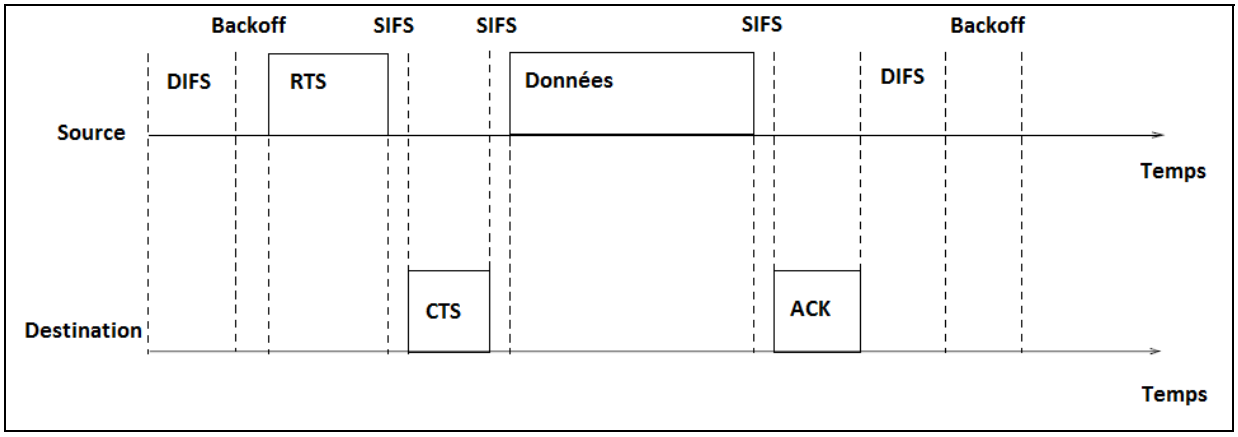

Figure 1.2 Fonctionnement de CSMA/CA

Cette figure nous présente le fonctionnement type de CSMA/CA. L'échange RTS/CTS permet d'initialiser la communication. L'ACK permet à la source de s'assurer de la bonne transmission des données. Sur le schéma, nous pouvons bien voir que les temps d'attente du backoff ne sont pas les mêmes, ils varient puisqu'ils sont tirés aléatoirement parmi la fenêtre de contention.

CHAPITRE 2

PROBLÉMATIQUE

2.1 Le phénomène de la triche dans le partage du médium

2.1.1 Définition, qu'est-ce que la triche ?

> «La triche est l'action de tricher, enfreindre certaines règles, conventions explicites ou d'usage en affectant de les respecter» (Encyclopédie Larousse, 2011).

2.1.2 La motivation, pourquoi tricher ?

Dans le cadre d'un réseau informatique, la motivation d'un nœud à tricher correspond à son intérêt purement égoïste d'augmenter son propre débit sans se préoccuper des conséquences pour l'ensemble du réseau.

2.1.3 Le moyen, comment tricher ?

Le contrôle de l'accès au médium est réglé par le mécanisme CSMA/CA explicité au chapitre précédent. Chaque nœud est sensé utiliser une même taille de fenêtre de contention (CW), afin de garantir une répartition équitable de l'accès au médium entre chaque entité du réseau.

Afin d'augmenter son débit, un nœud peut tenter de réduire la taille de sa CW par rapport aux autres nœuds. Un nœud ayant une CW plus petite va attendre en moyenne moins longtemps qu'un autre avant d'envoyer ses paquets. Ainsi, la répartition du médium s'en trouvera changée à l'avantage de ceux qui ont une CW réduite et qui seront prioritaires.

C'est cette méthode de triche que nous allons étudier par la suite. Nous utiliserons donc le terme triche pour désigner une baisse intentionnelle de la taille de la fenêtre de contention. Il y a de la triche quand, en état de saturation, un des nœuds du réseau à un pourcentage de la bande passante bien plus grand que ce qui serait escompté. Cette évaluation n'est possible

que sur une période d'une durée suffisamment longue car la méthode CSMA/CA est inéquitable sur une période trop courte (Koksal et al., 2000).

2.1.4 Modèle de réseau utilisé pour les simulations

Avant de commencer le premier test, nous allons définir le modèle de réseau utilisé lors des simulations. Il existe une multitude de réseaux différents, avec des architectures différentes. L'étude et les tests que nous allons réaliser doivent être cohérents avec un modèle relativement commun de réseau, et ceci pour des raisons de représentativité.

Nous définissons alors notre modèle de réseau comme suit :

Tableau 2 Modèle de réseau pour la simulation

Élément	**Description**
Nœuds et connections de flux	8 nœuds communiquant 2 à 2
Taille des paquets	2000 octets
Débit souhaité par nœuds	2000 kbps
Débit de données disponibles sur le canal	11mb
Terrain	100m*100m
Disposition et déplacement	Disposition aléatoire sans déplacement

Dans leur définition et leur fonctionnement, un réseau ad-hoc n'est pas limité en espace et en nombre de nœuds. Dans le cas présent, le modèle de réseau utilisé est une cellule de huit nœuds où les nœuds sont à portée les uns des autres. Ainsi, ils peuvent entendre toutes les transmissions sur le réseau. Ce modèle en cellule permet donc de réaliser une étude peu dépendante de la topologie. Cela permet d'éviter les goulots d'étranglement ou toute topologie spécifique qui pourraient diminuer les performances du réseau sur certaines simulations. La simulation en cellule des nœuds va donc uniformiser nos tests afin qu'ils soient comparables. De plus, chaque nœud est identique au niveau des caractéristiques physiques (comme la portée).

Le phénomène de triche que nous allons observer n'a de sens que si on prend un réseau fonctionnant à saturation. Ainsi, chaque nœud a réellement intérêt à avoir plus de bande passante. Nous avons donc choisi un débit souhaité par nœuds suffisamment important pour qu'il y ait une forte saturation.

La largeur ou la longueur du terrain n'excède pas la portée d'un nœud afin que chaque nœud puisse écouter l'ensemble des autres nœuds.

Dans notre étude, nous avons délibérément choisi d'avoir des nœuds ne se déplaçant pas afin de simplifier l'évaluation.

Lors des simulations, le débit sera relevé à intervalles réguliers de 5 secondes pour chacun des nœuds. Afin de faciliter la lecture des représentations graphiques, nous effectuerons une moyenne des observations sur 10 secondes pour les tests présentant des nœuds suivant une stratégie différente. Lorsque nous chercherons à observer la performance globale du réseau, l'échantillonnage correspondra à une moyenne des observations sur 10 secondes mais aussi sur 100 secondes pour lisser les courbes et pouvoir mieux observer les tendances.

2.1.5 Test témoin

La figure 2.1 nous présente un graphique témoin, où, pendant dix minutes tous les nœuds sont conformes au même protocole standard de l'IEEE 802.11b. Nous pouvons observer un débit moyen relativement constant. Ce niveau nous servira de référence comparative pour les tests à venir.

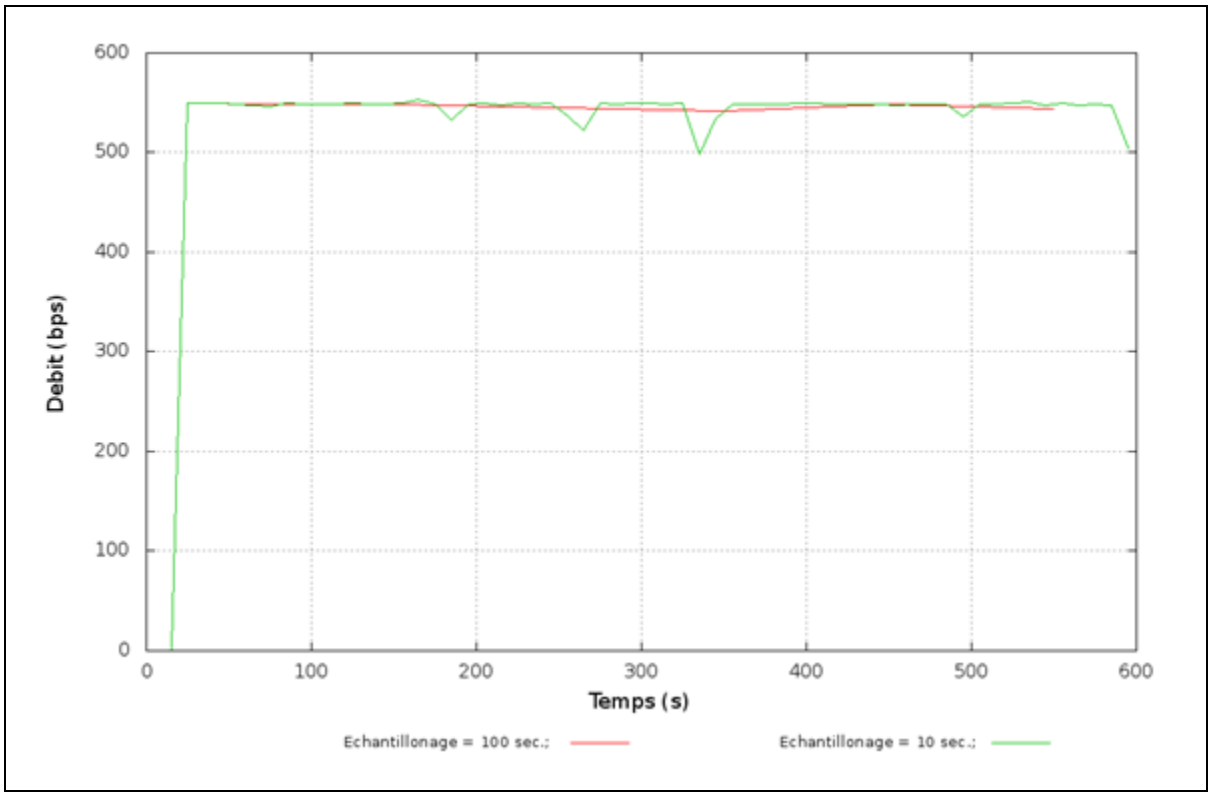

Figure 2.1 Graphique témoin du débit moyen

2.1.6 Test du phénomène de triche

Nous introduisons progressivement des tricheurs pour obtenir la figure 2.2. A partir de 100 secondes, un nœud réduit sa CW donc devient tricheur. Puis toutes les 50 secondes, un autre nœud réduit sa CW à un même niveau. Au bout de 500 secondes, tous les nœuds se sont mis à tricher. Un nœud qui triche réduit sa CW a 5% de sa taille originale en permanence. C'est-à-dire qu'un tricheur utilisera une fenêtre 20 fois plus petite que les autres nœuds, même après une collision. Nous avons choisi de montrer une triche plutôt agressive afin de se rendre compte de la possible ampleur du phénomène.

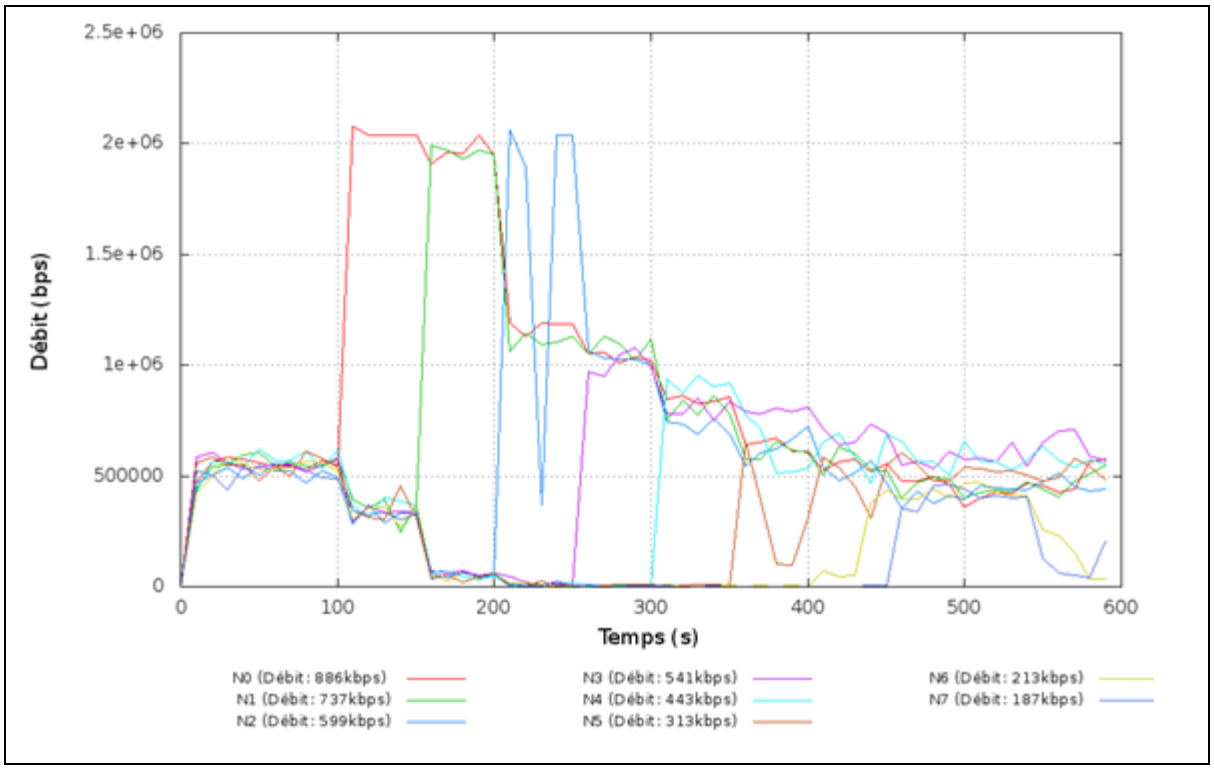

Figure 2.2 Apparition progressive de tricheurs

Nous pouvons alors observer l'impact de la triche. Dans la figure 2.2, on voit que les tricheurs profitent d'un avantage de débit considérable au début puis que cet avantage est réduit à chaque fois qu'un autre nœud se met à abaisser sa CW. Constatons bien qu'un nœud a un intérêt certain en terme de débit à avoir une fenêtre contention plus petite que les autres, c'est la tentation, ce qui l'incite à tricher.

La figure 2.3 nous permet d'observer de débit moyen de l'ensemble des nœuds, tricheurs et non-tricheurs, correspondant au même scénario que dans la figure 2.2. Nous pouvons voir une baisse du débit du réseau correspondant à l'arrivée progressive des tricheurs. La chute du débit est ainsi due à la réduction de la fenêtre des nœuds du réseau.

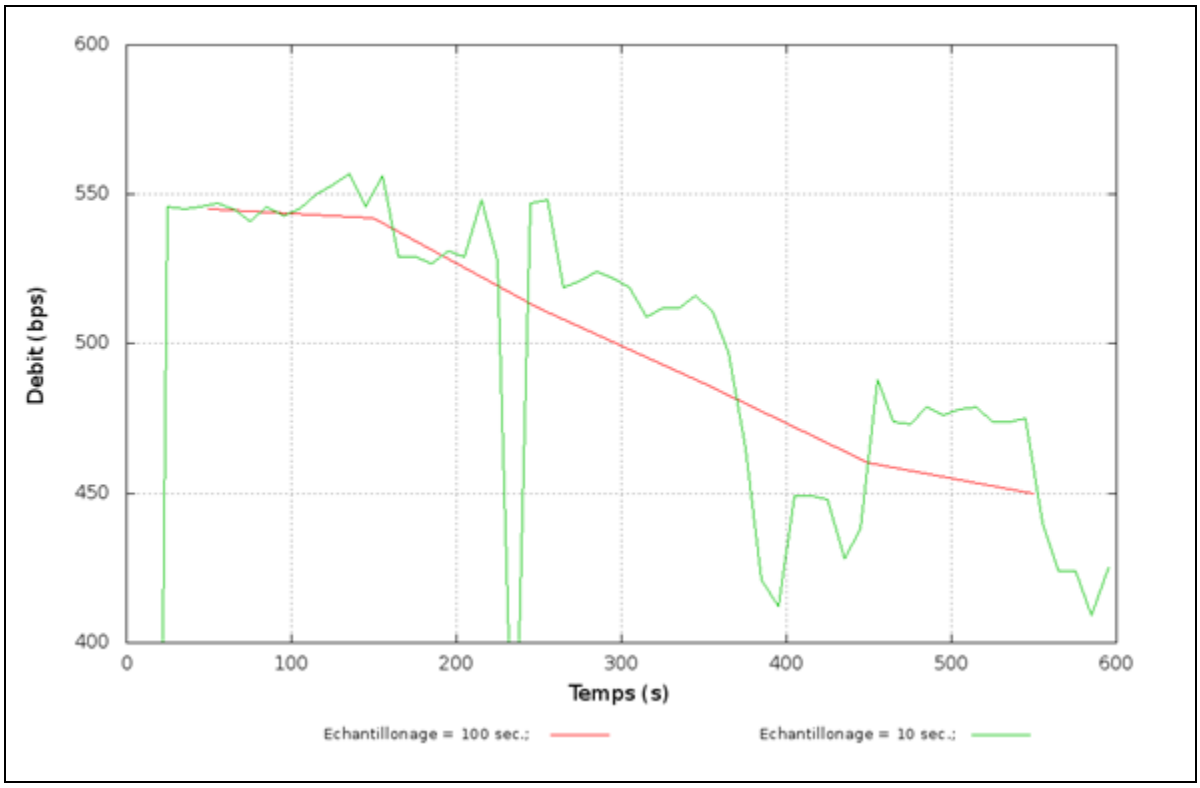

Figure 2.3 Apparition de tricheurs - débit moyen

2.1.7 Impacts et conséquences de la triche

Du point de vue d'un nœud, les conséquences de la triche sont une disproportion avantageuse du partage de l'accès au médium donc du débit. Chaque nœud a donc personnellement intérêt à abaisser sa CW en tout temps puisqu'il sera alors favorisé dans le mécanisme de contrôle d'accès.

Du point de vue du réseau, nous avons vu que la triche généralisé entraine une diminution du débit. Le réseau dans son ensemble n'a donc pas intérêt à ce que les nœuds trichent.

2.2 Problématique

2.2.1 Constat

Nous comprenons maintenant le problème de la triche sur le choix de la taille de la fenêtre de contention. Chaque nœud a personnellement un intérêt à tricher et si tous les nœuds trichent, c'est un engrenage fatal, un cercle vicieux où chaque nœud doit continuer à abaisser sa CW s'il veut augmenter son débit, il s'ensuit une chute du débit du réseau.

2.2.2 Définition de la problématique

Dans ce mémoire, nous tacherons de trouver comment réagir face aux conséquences du phénomène de l'abaissement de la taille de la CW dans le mécanisme du contrôle d'accès des réseaux ad-hoc. Nous utiliserons le terme triche par la suite pour décrire un tel comportement. Notons bien que nous ne nous intéresserons pas aux attaques malicieuses visant à perturber le réseau quel qu'en soit le prix. La triche, elle, est la recherche de profit de la part des nœuds. La simulation s'intéressera à une cellule de nœuds d'un réseau ad hoc et non au réseau global. Ceci afin d'éviter que la topologie ait une influence sur les performances. Nous étudierons cette réaction à la fois du point de vue d'un nœud, ainsi que de l'ensemble du réseau :

- chaque nœud cherche à s'assurer qu'il peut avoir accès à sa part juste et équitable de la bande passante,
- pour le réseau, l'objectif est d'éviter la présence de nœuds cherchant à obtenir plus que leur part de la bande passante empêchant ainsi les pertes de débit causées par le phénomène de triche.

Nous tenterons de satisfaire ces objectifs en comprenant comment mettre en place une stratégie de défense face aux comportements égoïstes au niveau MAC dans les réseaux ad-hoc.

CHAPITRE 3

REVUE DE LITTÉRATURE

Dans cette section, nous effectuerons un tour d'horizon et une évaluation critique de l'état de l'art dans ce qui a trait aux comportements égoïstes dans les réseaux sans-fils. Nous présenterons tout d'abord la coopération au sein du protocole IEEE 802.11, et tout particulièrement la détection et la réaction face à un comportement égoïste dans le choix du backoff. Par la suite nous expliciterons la théorie des jeux et le dilemme du prisonnier répété pour introduire différentes stratégies basée sur Tit-for-Tat. Enfin nous exposerons les applications de la théorie des jeux dans le cadre spécifique des réseaux utilisant le protocole MAC 802.11.

3.1 La coopération dans les réseaux

3.1.1 Introduction

Un réseau, en tant qu'élément de communication, fait nécessairement appel à la coopération entre les entités afin de transmettre les informations. Coopérer signifie respecter les règles imposées par le protocole de communication en vigueur. Dans le cadre des réseaux sans-fils, par convention, les normes de l'IEEE sont utilisées. A l'inverse, ne pas coopérer se traduit donc par le fait de ne pas respecter ces normes.

Le fait qu'un nœud ne coopère pas peut être volontaire mais aussi involontaire. Nous distinguerons donc bien la non-coopération de la triche, qui est un objectif volontaire d'augmentation des performances.

Le Wifi, de par la nature du médium utilisé, est sensible aux bruits (Desilva, Boppana, 2004). Par exemple, si un nœud écoute le canal et pense qu'il est libre alors qu'il était occupé nous aurons une non-coopération qui pourrait entraîner une collision. La mobilité des nœuds peut

impliquer des changements de topologie et être aussi à l'origine d'erreurs. La nature et la mobilité des réseaux sans-fils sont une cause de non-coopération non-volontaire.

La non-coopération peut être aussi volontaire, dans ce cas, c'est soit de la triche, soit une attaque malicieuse. Dans cette étude nous n'étudierons pas les attaques malicieuses, qui sont réalisée dans l'unique but de nuire au réseau sans forcément générer de profit, la plupart du temps étant même couteuses. La triche est donc un moyen et non pas un but. L'objectif pour le nœud est de réaliser un gain, un profit. Il existe différents types de profits réalisables dans les réseaux sans-fils qui correspondent à diverses utilisations de cette non-coopération. Celle-ci peut s'exprimer de différentes manières:

- au niveau du protocole de routage, empêchant ou falsifiant l'acheminement des informations de topologie, de routes,
- dans la transmission des paquets, en ne retransmettant pas les paquets pour économiser de l'énergie et du temps de transmission (Jaramillo, Srikant, 2010),
- au sein du contrôle d'accès (MAC), afin d'obtenir une priorité d'émission par rapport aux autres nœuds (cf. problématique).

3.1.2 Le comportement égoïste

Au niveau de la couche MAC, l'impact du comportement de nœuds a tout d'abord été étudié sur les réseaux utilisant Aloha, le premier protocole de réseau local. Jin et Kesidis (2002) analysent l'équilibre non-coopératif dans les réseaux Aloha en présence d'utilisateurs hétérogènes. C'est à dire que les nœuds sont pris en considération comme des entités propres dans leur choix de coopérer ou non. Ce sont eux qui choisissent leur probabilité de transmission. Les auteurs utilisent ces travaux afin de définir un mécanisme de prix qui s'adapte au réseau.

Le protocole Aloha discrétisé introduit une horloge, permettant de synchroniser les nœuds et ainsi de diminuer le temps d'attente dû aux collisions. La stabilité du protocole Aloha discrétisé est étudiée par MacKenzie et Wicher, (2003). Afin de modéliser une solution simple, les auteurs considèrent une information parfaitement connue de tous. Or dans les

réseaux, il n'est pas possible pour un nœud de connaître précisément toutes les informations d'un autre nœud, ne serait-ce qu'à cause du bruit. Dans ces conditions, les auteurs montrent qu'une stabilité peut être atteinte entre des nœuds non-coopératifs suivant les paramètres du réseau (nombre des nœuds, prix d'une transmission) et la capacité pour les nœuds à déterminer ou ignorer cet équilibre ce qui peut entraîner une forte dégradation des performances.

Dans un autre article (Altman, Azouzi, Jim, 2002), la méconnaissance de certaines informations (comme la probabilité de transmission) est prise en compte dans les réseaux utilisant Aloha discrétisé. Les auteurs lient le choix de la probabilité de transmission avec les collisions. Ils expliquent clairement le problème auquel ils sont confrontés : chaque nœud a intérêt à augmenter sa probabilité de transmission par rapport aux autres nœuds, suivant un comportement que l'on pourrait qualifier d'agressif. Le problème étant que progressivement, si tous les nœuds deviennent agressifs, c'est le débit de l'ensemble du réseau qui se détériore. Nous pouvons ainsi constater une forte ressemblance sémantique avec notre problématique de la triche telle que définie.

Cagalj et al. (2005) étudient les comportements égoïstes dans les réseaux IEEE 802.11 utilisant la méthode CSMA/CA. Dans cette étude, chaque nœud peut choisir la taille de sa CW pour maximiser son débit. Les auteurs démontrent qu'une petite portion de nœuds égoïstes va dégrader de façon considérable le débit de l'ensemble du réseau. Des résultats similaires sur le comportement des nœuds sont présentés par Park et al. (2009) et Kornorski (2006) menant aux mêmes conclusions sur le constat de la problématique. Ce dernier auteur présente également un mécanisme de défense que nous expliciterons après avoir introduit la théorie des jeux.

3.1.3 Détection du comportement

Le constat étant posé, il s'agit de savoir comment détecter un comportement non-coopératif. Le comportement égoïste qui nous intéresse est l'abaissement de la taille de la CW comme

explicité dans la problématique. Le fait est que dans un réseau ad-hoc, un nœud ne connait pas la taille de CW des autres nœuds.

Toledo et Wang (2007) proposent un détecteur de comportement que peut mettre en place chaque nœud sans modification à l'IEEE 802.11. En effet, un abaissement de la taille de la CW va entraîner une augmentation du nombre de collisions dans le réseau. Ces collisions sont visibles par les nœuds du réseau. C'est en évaluant la répartition de ces collisions au cours du temps et en fonction du nombre de nœuds qu'une modification de comportement peut être observée. Les auteurs proposent le test statistique Kolmogorov-Smirnov pour l'évaluation. Les résultats de leurs simulations montrent une grande efficacité du test. Notons que les petits tricheurs sont ignorés mais que le test détecte très bien les tricheurs agressifs, c'est-à-dire avec une forte diminution de la taille de la fenêtre de contention.

Rong et al.(2006) présentent un autre système de détection mathématique. Il basé sur une comparaison des probabilités d'émission d'un nœud. Cela permet de déterminer un ratio de densité de probabilité servant d'outil de détection face aux nœuds égoïstes. Cette méthode est parfois nommée SPRT (Sequential Probability Ratio Test). Au vu des résultats, les auteurs la considèrent comme une méthode très efficace pour ce qui est de la détection du comportement égoïste.

Une solution intéressante de modification de la norme 802.11 pour effectuer une détection est présentée par Kyasannur et Vaidya (2003). Les auteurs partent du principe que la destination est une entité de confiance. Dans cet article c'est le nœud de destination qui assigne la prochaine valeur de backoff (tiré aléatoirement parmi la CW) à la source. Puis la destination va mesurer si ce backoff est respecté en comptant le nombre d'intervalles de temps entre les émissions de la source. Si une collision intervient, une fonction connue de la source et de la destination va permettre un nouveau calcul du backoff.

Le principe de détection est le suivant : si la destination mesure un temps d'attente inférieur au backoff attendu, une pénalité sera appliquée au prochain backoff que choisira la

destination pour la source. Si la source respecte la pénalité, elle attend plus longtemps avant d'envoyer un paquet donc la répartition de la bande passante s'équilibre. Cela peut arriver en cas de déséquilibre passager, d'erreur de perception par exemple. Par contre si la source décide de ne pas respecter le temps de backoff imposé, la destination est de plus en plus sure d'être en présence d'un nœud au comportement égoïste. Le diagnostic est effectué.

Comme mentionnée par les auteurs, cette solution a de nombreuses limitations comme la nécessité de faire confiance au destinataire et le besoin de modifier le protocole 802.11 de telle manière qu'une rétrocompatibilité pourrait poser des problèmes. Mais surtout, Il n'y a pas de raison de penser que la destination est plus honnête que la source, recevoir des paquets plus rapidement est aussi une forme d'avantage.

DOMINO (Raya, Hubaux, 2004) est un outil de détection de comportement égoïste au niveau de la couche MAC dans les réseaux avec point d'accès. Il ne s'arrête pas à la détection d'une triche dans le choix de la CW mais à l'ensemble des comportements égoïstes au niveau de la couche MAC (touchant la sécurité par exemple). Dans le cas de la triche sur la CW, la solution proposée est de mesurer le backoff directement en relevant la durée entre chaque émission du nœud voisin quand il n'y a pas de collisions. A cette durée sont enlevés les temps pendant lesquels le backoff n'est pas décrémenté comme le DIFS ou quand le canal est occupé. On obtient alors le backoff utilisé par le nœud voisin. La moyenne des backoffs d'un nœud détermine alors une approximation de la taille minimale de fenêtre de contention (puisqu'il n'y a pas eu de collisions). Là encore les auteurs apportent de sérieuses limitations à leur détection de comportement au niveau du backoff. Un nœud pourrait tricher en ne doublant pas sa CW après une collision, évitant alors la détection. De plus, cette solution de mesure de backoff est prévue pour se déployer a partir d'un point d'accès, donc d'une entité fiable, à portée de tous, et surtout de confiance. Ce qui n'est pas possible directement dans un réseau ad-hoc.

DOMINO a été comparé à la solution SPRT, solution mathématique de détection explicitée brièvement plus tôt. Cardenas et al.(2009) montrent que SPRT est une solution beaucoup

efficace que DOMINO pour la détection de comportements. Les auteurs critiquent le fait que la variation de réaction à l'égard des nœuds égoïste n'est pas proportionnelle à l'état observé du réseau. Une modification est apportée pour tenter de compenser cela ce qui augmente les performances de DOMINO mais SPRT reste plus efficace pour la détection.

3.1.4 Réaction face à un nœud égoïste

Après avoir vu comment détecter le comportement des nœuds, nous allons maintenant nous intéresser à la réaction que peut avoir un nœud qui sait que son voisin triche. Que peut faire un nœud face à un autre nœud soupçonné d'abaisser son backoff ?

Une réaction mesurée consiste à ralentir la communication du nœud soupçonné tricheur. C'est d'ailleurs ce qui est proposé comme réaction initiale par Kyasannur et Vaidya (2003). Cela peut être une réaction temporaire tant que l'on n'est pas certain d'avoir affaire à un tricheur.

Une réaction plus drastique consiste à gêner le nœud tricheur dans sa communication. Un brouillage de ses communications est envisagé par Kornorski (2002) comme une punition à la triche. Le brouillage peut même être progressif suivant le degré de certitude envers le nœud trichant.

Si un nœud honnête détecte la triche, il peut également choisir de se mettre a tricher lui aussi afin de rééquilibrer les probabilités d'émission entre les nœuds. Cependant il deviendrait lui aussi un tricheur du point de vue des autres nœuds honnêtes qui pourraient réagir, nous reviendrons particulièrement sur cette forme de réaction dans la suite de la revue de littérature.

Enfin, la réaction la plus totale contre un nœud soupçonné de triche est une ignorance pure et simple de ce nœud. S'il ne peut pas participer aux opérations de routage, il ne pourra plus communiquer, il aura tout perdu. C'est la solution proposée par Kyasannur et Vaidya (2003)

quand le seuil de confiance est dépassé et qu'on est certain d'avoir affaire à un tricheur. Les différentes réactions permettent une réponse graduée par rapport à la situation.

3.2 Théorie des jeux et stratégies

3.2.1 Définition

La théorie des jeux permet d'étudier les prises de décisions et les comportements de différents acteurs lors d'interactions entre eux, chacun ayant leurs propres objectifs. Les principes fondamentaux de la théorie des jeux ont été découverts durant la première moitié du XXème siècle par J. Von Neumann et O. Morgenstern (1944) qui ont exposé la méthode de résolution des jeux à somme nulle. Par la suite, la théorie des jeux est devenue une branche reconnue des mathématiques qui est venue enrichir des nombreux domaines d'études, de la biologie aux relations internationales en passant par l'économie et l'informatique.

3.2.2 Sources

Pour cette partie de revue littéraire sur la théorie des jeux et en particulier le dilemme du prisonnier, nous prendrons appui sur l'ouvrage d'Axelrod (1988). Dans ce livre, l'auteur étudie la coopération dans un dilemme du prisonnier répété, nous y reviendrons par la suite.

3.2.3 Le dilemme du prisonnier

Le dilemme du prisonnier est l'exemple le plus célèbre de la théorie de jeux. Il est particulièrement intéressant car il va nous permettre d'avoir une autre vision de notre problématique.

Deux suspects, Alice et Bob sont en prison. Le commissaire propose le même marché à chacun :

- si Alice dénonce Bob et que Bob ne dénonce personne, Alice sera libérée et Bob croupira 5 ans en prison,

- si Alice et Bob se dénoncent mutuellement, les deux suspects resteront 3 ans en prison,
- si ni Alice, ni Bob ne se dénoncent pas mutuellement, ils encourront une peine de 1 an de prison.

C'est un exemple théorique donc les peines constituent l'unique enjeu de la partie. Restons objectif et retirons tout enjeu moral, sentimental ou autre. Nous pouvons alors définir une matrice de gains.

Tableau 3 Matrice de gains du dilemme du prisonnier

Alice/Bob	**Se tait**	**Dénonce**
Se tait	(1,1)	(5,0)
dénonce	(0,5)	(3,3)

L'objectif du commissaire quand il propose un tel marché est bien évidement de favoriser la dénonciation. Observons un peu le raisonnement logique qui pourrait être effectuée par Alice :
- si Bob ne dit rien, Alice a intérêt à le dénoncer pour ne pas aller en prison,
- si Bob dénonce Alice, Alice a intérêt à le dénoncer pour réduire sa peine de prison.

Si l'on suit ce raisonnement logique, chacun des deux suspects a intérêt à dénoncer son collègue donc chacun devrait croupir en prison pour 3 ans. Mais en observant le tableau, il est clair qu'il existe une meilleure stratégie. Il est possible que chaque joueur ne passe qu'une année en prison, d'où le dilemme. On comprend alors pourquoi le commissaire présente ce marché sensé empêcher la coopération.

Pour qu'il y ait un tel dilemme, le gain associé à la tentation (je dénonce, l'autre se tait, je suis libéré) doit être plus élevé que si chacun ne dit rien (1 an de prison), lui même supérieur à la dénonciation mutuelle (3 ans) qui doit encore être plus intéressante que de se faire duper (je me tais, l'autre joueur me dénonce).

Formellement, un dilemme du prisonnier n'a lieu que lorsque l'équation suivante, pour un tel tableau de résultat, est vérifiée.

$$tentation > coopération\ mutuelle > égoïsme\ mutuel > duperie \tag{3.1}$$

Il est à noter que pour avoir un dilemme, les gains associés à la tentation et à la duperie associés doivent être inférieurs au double du gain lié à la coopération. Concrètement cela s'explique par le fait que si ce n'était pas le cas, les joueurs pourraient former une coalition pour partager leurs gains, choisir que l'un coopère et pas l'autre afin d'avoir plus de profit. Il n'y aurait alors plus de dilemme. Notons bien que dans l'exemple présenté, si les deux suspects n'ont aucun moyen de s'entendre sur l'action à mener, les peines de prison n'étant pas échangeables, cette règle n'est pas obligatoire.

$$2 \times coopération\ mutuelle > (tentation + duperie) \tag{3.2}$$

Le dilemme du prisonnier incarne le conflit fondamental entre l'intérêt privé des joueurs et leur intérêt collectif. Notons bien que pour un dilemme du prisonnier simple, dénoncer son complice donc ne pas coopérer est le choix dominant.

3.2.4 Extensions et applications du dilemme du prisonnier

Nous avons présenté la version initiale du dilemme du prisonnier où la situation est réduite à un cas simple. En effet, un dilemme du prisonnier peut faire intervenir plusieurs joueurs. De plus, le choix d'action des joueurs peut s'avérer plus complexe qu'un choix binaire : coopérer ou ne pas coopérer. En effet dans certains jeux un joueur peut choisir de coopérer partiellement. De ce fait, le nombre de résultats dans la matrice de gains augmente, le jeu est alors de plus en plus complexe à étudier.

Le jeu peut aussi être joué de manière répétée, on parle de dilemme du prisonnier répété ou itératif (Axelrod, 1988). Dans un tel jeu itératif, les joueurs peuvent prendre en compte les résultats passés pour choisir leur action future. La différence est importante car l'objectif d'un

joueur est la maximisation des gains sur l'ensemble des jeux et non pas sur un seul. Il est évident que si le joueur adverse ne coopère jamais, le joueur n'est en aucun cas incité à coopérer et l'ensemble des gains restera faible. Partant de cela, les joueurs peuvent faire naitre une coopération mutuelle qui sera plus avantageuse. La coopération devient possible à partir du moment où le jeu est répété donc que le choix de l'action présent a une influence sur le choix futur de l'adversaire, donc des résultats futurs des deux parties. Nous utiliserons le terme tour de jeu pour désigner une manche : chaque choix et sa résolution.

Il apparaît logique que si les joueurs connaissent le nombre de parties jouées, ils ont intérêt à ne pas coopérer lors de la dernière partie. En effet, ne pas coopérer cette fois-là n'entrainera pas de répercussion sur les futurs gains puisque c'est la dernière partie. De la même manière, en revenant une partie en arrière, l'avant dernière partie devrait donc mener aussi sur une non-coopération, les joueurs ayant déjà fixé leur stratégie pour la dernière partie. Nous comprenons ici que dans un dilemme du prisonnier répété, il est nécessaire que les joueurs ne connaissent pas la fin du jeu, cela afin de pouvoir entreprendre des actions sur le long terme et faire naitre la coopération. La solution utilisée dans le cadre du dilemme du prisonnier est l'introduction d'une probabilité très faible et connue des joueurs que le jeu s'arrête au prochain tour.

Il est possible de trouver des analogies au dilemme du prisonnier dans de nombreux contextes. C'est sans doute ce qui a suscité un tel engouement pour ce dilemme. Nous en donnerons quelques exemples choisis en économie et politique militaire qui nous permettront de mieux comprendre les situations dans lesquelles ce dilemme apparaît et quel rôle il peut jouer.

L'économie fourmille d'applications du dilemme du prisonnier (répété ou non). Il apparait quand deux entreprises souhaitent baisser leur prix ou rajouter de la publicité afin de gagner des parts de marchés. Logiquement, si les deux entreprises sont similaires, ont le monopole sur un produit, et que la consommation est considérée constante, l'impact de la baisse des prix et de la publicité n'est pas remarqué car il s'annule. Coopérer, au niveau des deux

entreprises serait de prendre la décision de garder des prix constants et de ne pas faire de publicité. Cette coopération permettrait le maximum de profit pour les entreprises. Cependant c'est cela qui a mené à réaliser les lois anti-trust aux USA (et leur équivalent européen et dans les autres continents et pays bien sûr) pour protéger les consommateurs. Les lois antitrust ont pour objectif de changer la matrice de gains en mettant une forte pénalité à la coopération mutuelle pour ne plus se retrouver dans un dilemme du prisonnier.

En politique militaire, deux états voisins ont le choix d'entretenir une armée ou non. Si les deux pays ont une armée, cela va leur couter cher et ils ne s'attaqueront pas, les tailles d'armées étant similaires, l'issue du combat se révèle incertaine et couteuse, la dissuasion fonctionne. Si un pays n'a pas d'armée mais que son voisin en a une, ce dernier va pouvoir attaquer sans problème. Dans ce cas, la coopération consiste à ce que les pays se fassent confiance et ne créent pas d'armées. Cette solution serait profitable économiquement pour chacun des pays, mais l'incitation à la construction d'une armée (les gains potentiels d'une attaque si la partie adverse ne fait rien) peut rendre la situation instable, la tentation étant forte. L'exemple le plus frappant de cette analogie est la guerre froide où chaque belligérant amasse des armées pour prévenir toute invasion. Notons bien qu'une situation concrète est soumise à beaucoup plus de facteurs comme les enjeux personnels, moraux et nationalistes. Ces éléments devraient être pris en compte pour une modélisation parfaite du conflit, en réalité le niveau de complexité devient tellement élevé qu'une prédiction parfaite s'avère quasi-impossible. Néanmoins, différents acteurs internationaux tentent de l'utiliser pour prédire l'évolution des situations et conflits.

3.2.5 Stratégies pour le dilemme du prisonnier répété

Le choix d'action d'un joueur à chaque tour est défini par sa stratégie. Il en existe de très simples comme le fait de toujours coopérer. Une stratégie peut aussi prendre en compte les résultats et les choix adverses précédents afin de définir son action, dans ce cas elle est réactive. Une part d'aléatoire peut également être introduite, elle a la capacité empêcher l'adversaire d'analyser la stratégie, de prévoir le résultat.

Il existe de nombreuses applications à ce dilemme dans la vie de tous les jours mais que leur étude peut s'avérer très complexe en raison du nombre de paramètres à prendre en compte. Si nous souhaitons étudier l'impact des diverses stratégies, il convient de les étudier en simplifiant au maximum le jeu d'étude.
Axelrod (1988) étudie les différentes stratégies dans un dilemme du prisonnier répété. Il a organisé deux tournois où différentes stratégies sont proposées et s'affrontent lors de dilemme du prisonnier répété. Les stratégies proviennent de chercheurs de différents domaines, de la physique à l'économie en passant par la psychologie. La matrice de gains observée est la suivante.

Tableau 4 Matrice utilisée par Axelrod (1988)

choix	**coopère**	**ne coopère pas**
coopère	(3,3)	(5,0)
ne coopère pas	(0,5)	(1,1)

Les stratégies jouent un nombre défini (mais non connue par la stratégie des joueurs) de tours de jeu. Chaque stratégie affronte successivement chacune des autres stratégies. La stratégie gagnante du tournoi étant celle ayant amassé le plus de points.

En premier lieu, notons qu'il n'existe pas une meilleure stratégie qui conviendrait à l'ensemble des situations. En effet, contre un adversaire qui ne coopèrerait jamais, coopérer une seule fois suffit à ne pas obtenir le résultat optimum puisque l'adversaire a pu nous duper une fois. De même, contre un adversaire qui aurait choisi de coopérer tant que l'autre joueur coopère, ne jamais coopérer va signifier une perte de gains car il n'y aura pas de coopération mutuelle.

Les stratégies qui ont bien réussi en tournoi ont deux points communs :
- elles coopèrent au premier tour, donnant le ton de la coopération,
- elles ne coopèrent pas si, auparavant, le joueur adverse n'a pas coopéré. L'objectif étant de se faire duper le moins possible en réagissant rapidement. Cela peut paraître logique mais il

est essentiel qu'une stratégie s'adapte à celle de son adversaire afin d'influencer ses choix donc les résultats futurs.

Nous allons par la suite présenter la stratégie gagnante des tournois ainsi que deux de ses variantes. Ces stratégies et la logique qui va avec sont à la base de ce mémoire.

3.2.6 Tit For Tat

Tit for Tat est la stratégie qui a remporté les deux tournois proposés par Axelrod. TFT est une des stratégies les plus simples qui soit : un joueur qui suit une stratégie TFT va coopérer au premier tour, puis, au prochain tour il réalisera l'action qu'a choisie l'adversaire au tour précédent.

L'objectif de ce mimétisme est d'empêcher l'adversaire de profiter plus d'une fois de la trahison. Ainsi la différence en résultat entre TFT et un de ses adversaires n'est jamais supérieure à l'écart possible sur un tour de jeu. Ce petit écart est d'autant moins significatif que le nombre de tours de jeu est élevé (supérieur à 500). C'est une attitude de minimisation de l'écart de points entre les joueurs, une attitude visant l'égalitarisme mais prônant la coopération dans sa première action.

Une stratégie optimum dans tous les cas n'existant pas, aucune stratégie n'a remporté tous ses duels. En réalité TFT réalise des résultats souvent très légèrement inférieurs à ceux de ses adversaires dans chaque duel. Cependant c'est TFT qui a largement obtenu les meilleurs résultats d'ensemble. En effet, aucune stratégie ne peut gagner un avantage considérable de points face à TFT.

L'extrême simplicité de cette stratégie fait qu'elle est aisément compréhensible par les autres stratégies. C'est en fait un grand avantage, les adversaires pouvant comprendre qu'ils ne pourront pas profiter de TFT, le choix le plus judicieux devient la coopération mutuelle.

3.2.7 Generous Tit For Tat

TFT réagit très bien dans un contexte où les décisions du joueur adverse et les résultats sont connus donc quand on peut qualifier l'information de parfaite. On considère qu'il n'y a pas d'erreur dans la réalisation des actions ou dans la perception de ces actions.

Molander (1985) s'est intéressé au sujet et a prouvé que TFT n'est plus forcément une bonne stratégie quand une probabilité d'erreur est introduite. Cette probabilité d'erreur ne permet pas de savoir à coup sûr ce qu'a réellement voulu faire l'adversaire au tour précédent.

Prenons un exemple illustré par le tableau 5, si Alice et Bob sont deux joueurs qui utilisent TFT, tant qu'il n'y a pas d'erreur, les joueurs coopèrent. Si une erreur fait qu'Alice ne coopère pas au troisième tour, Bob va la punir et ne plus coopérer au prochain tour et Alice ferra de même au tour suivant. La coopération ne pourra plus se faire. TFT est donc une stratégie efficace dans un jeu à information parfaite mais elle est sensible aux erreurs d'interprétation.

Tableau 5 Impact des erreurs avec TFT

Action			**erreur**						
Alice	C	C	D	C	D	C	D	C	D
Bob	C	C	C	D	C	D	C	D	C
C : coopération, D : non-coopération									

Pour pallier ce problème, Molander conseille d'apporter de la générosité dans TFT. Concrètement la générosité est la capacité à coopérer avec une certaine probabilité même quand l'adversaire n'a pas coopéré au dernier tour. Cette probabilité est le facteur de générosité. La stratégie nouvellement définie est nommée GTFT ou TFT avec pardon. Nous utiliserons le terme GTFT par la suite. Grâce à cette générosité, le joueur utilisant GTFT va pouvoir pardonner au joueur adverse les possibles erreurs qui pourraient survenir. Nous pouvons observer ce résultat dans le tableau suivant où Bob fait preuve de générosité au tour de jeu numéro six ce qui permet de retrouver la coopération mutuelle.

Tableau 6 Impact des erreurs avec GTFT

Action			**erreur**			**générosité**			
Alice	C	C	D	C	D	C	C	C	C
Bob	C	C	C	D	C	C	C	C	C
C : coopération, D : non-coopération									

L'apport de la générosité n'a pas que des avantages. Face à un joueur qui décide de ne jamais coopérer, un joueur suivant la stratégie GTFT perdra plus qu'un joueur suivant TFT. En effet, dans ce sens, le facteur de générosité va entrainer le joueur suivant GTFT à coopérer donc à se faire plus duper que s'il avait choisi TFT.

La détermination du facteur de générosité dépend donc du contexte du jeu. Plus la probabilité d'erreur est importante, plus le facteur de générosité doit être augmenté en compensation mais plus grande sont les pertes face à des joueurs qui essaient de profiter de cette générosité.

3.2.8 Reputation Tit For Tat

Face à l'introduction d'erreurs d'interprétations, Wu et Axelrod (1995) proposent une solution différente dans des dilemmes du prisonnier répétés de nombreuses fois. Il apparaît assez trompeur de baser son action future uniquement sur l'action précédente, en particulier si l'on sait que cette action précédente peut-être due à une erreur. L'idée apportée est qu'en raisonnant sur l'ensemble des actions passées de l'adversaire, nous aurons une image de son comportement sur le long terme ce qui pourrait être plus juste qu'une interprétation basée uniquement sur la dernière action. Nous utiliserons le terme RTFT pour *Reputation Tit-For-Tat.*

Un score de réputation réactualisé à chaque nouveau tour de jeu permettra d'obtenir l'image de ce comportement sur le long terme. L'action choisie par le joueur suivant la stratégie RTFT dépendra alors du score de réputation adverse et non pas de l'action de l'adversaire au dernier tour de jeu.

Se souvenir des résultats passés est à la base du principe de réputation, mais rationnellement le passé proche devrait influer plus sur le futur, donc il a plus d'importance que le passé lointain. Une pondération des résultats devrait donc être effectuée pour que le passé proche soit valorisé dans le score de réputation.

L'apport de cette approche basée sur le score de réputation a aussi son défaut. Par exemple si un joueur qui était coopératif pendant longtemps décide de ne plus coopérer, alors son adversaire, s'il suit la stratégie RTFT, va mettre plus de temps à se rendre compte du changement de comportement que s'il suivait TFT. Il y a une perte de réactivité.

3.3 Les jeux répétés dans les réseaux sans fils

La capacité et les performances d'un réseau Wifi quand tous les nœuds respectent les normes de communication en vigueur ne sont pas un problème puisque chaque nœud est alors identique. Cependant comme nous l'avons expliqué les nœuds peuvent choisir de ne pas suivre les normes de communication en espérant augmenter leurs performances. Dans ce cadre-là, une modélisation du réseau via la théorie des jeux peut se révéler un outil d'analyse très utile.

Un nœud est alors considéré comme un joueur, la configuration de ses protocoles est sa stratégie car c'est d'elle que vont dépendre les actions qu'il va effectuer. Dans notre cas, nous nous concentrerons uniquement sur la stratégie de choix de la taille de CW qui joue sur la priorité d'émission comme décrit dans notre problématique. Sur une période, le résultat du jeu est la quantité de bande passante obtenue par chacun des nœuds.

L'objectif ici est donc de faire naitre la coopération entre les nœuds afin qu'aucun ne soit tenté de modifier son choix de backoff en abaissant sa CW pour tenter d'augmenter son débit d'émission. Rappelons qu’un nœud qui suit le protocole standard coopèrera dans tous les cas en choisissant un backoff tiré aléatoirement parmi une CW de taille défini par le standard IEEE choisi.

Konorski (2006) est un auteur ayant bien étudié les problèmes liés aux comportements égoïstes dans les réseaux Wifi. Il a proposé un mécanisme de défense nommé CRISP (*Cooperation via Randomized Inclinaison to Selfish/Greedy Play*) face à ces comportements. CRISP fonctionne par état. Notons que l'auteur différencie 3 types d'états :

- honnête (H), le nœud suivant CRISP utilise une fenêtre de taille standard telle que défini par le protocole utilisé,
- égoïste (S), le nœud diminue sa fenêtre de contention au minimum possible,
- cupide (G), le nœud effectue ses transmissions sans attendre de temps tiré aléatoirement.

CRISP réagit au comportement des autres nœuds. La détection du comportement est réalisée en fonction du débit. La détection s'appuie sur des seuils de valeurs suivant le nombre de nœuds du réseau. L'auteur ne considère pas le cas de petits tricheurs qui ne diminuerait leur fenêtre de contention que d'un petit peu.

La figure 3.1 va nous permettre de mieux expliquer le fonctionnement du mécanisme de défense.

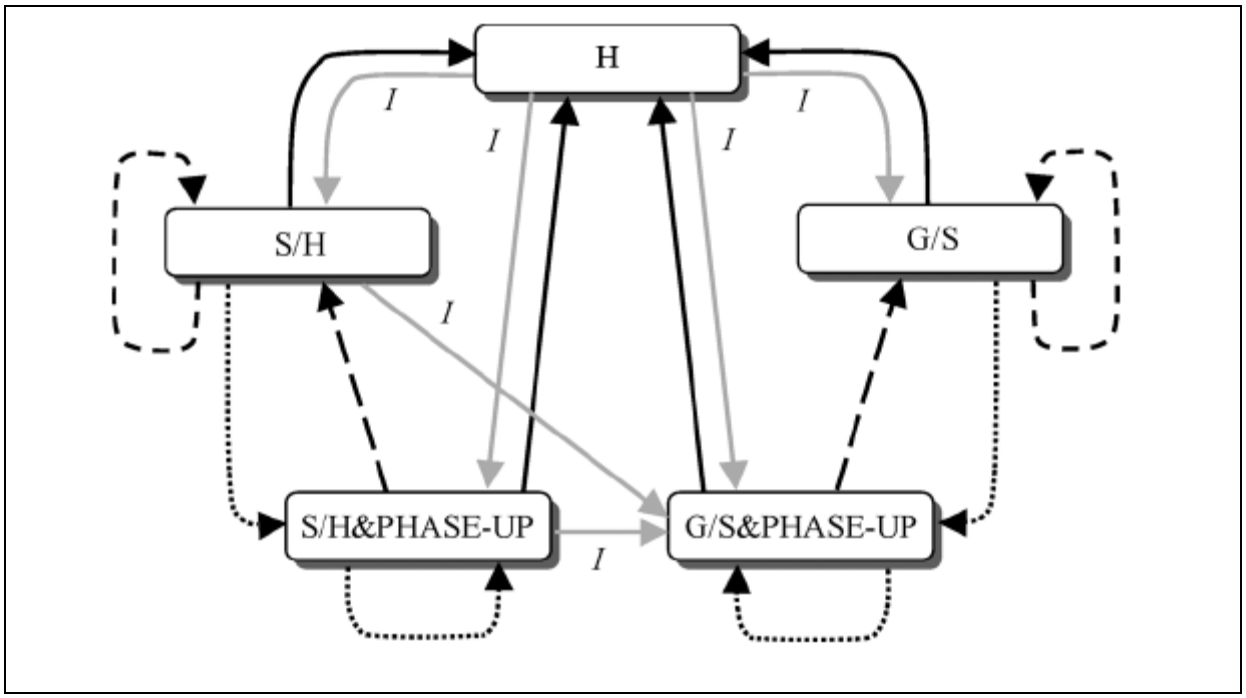

Figure 3.1 CRISP (Konorski, 2006)

Les transitions sont effectuées selon l'état estimé du réseau. Les lettres I marquent la réaction face aux tricheurs qui viendraient envahir le réseau. Sur le schéma, les flêches pleines correspondent à un état d'amélioration du réseau (moins de tricheurs detectés), à l'opposé, les flêches en pointillés montrent les transitions quand la situation se dégrade. Les flêches en ligne coupées montrent un état de stabilité. CRISP réagit face au comportent des autres nœuds du réseau comme décrit ci-dessous :

- Si tous les autres nœuds sont honnêtes, le nœud suivant CRISP se positionnera sur l'état honnête (H).
- Si des nœuds égoïstes sont détectés, CRISP basculera vers l'état S/H. À chaque choix de backoff, il choisira son attitude, honnête ou égoïste, suivant une certaine probabilité. Si les autres nœuds sont de plus en plus égoïstes, cette probabilité sera renforcée en faveur de l'attitude égoïste (état S/H&PHASE-UP). Si par la suite, aucune triche n'est détectée, alors on aura un repositionnement sur l'état honnête (H).
- Si des nœuds cupides sont détectés, CRISP se positionnera sur l'état G/S, il alternera alors les attitudes cupide et égoïste suivant une probabilité définie. De la même manière, cette

probabilité sera augmentée en faveur de l'attitude cupide si les autres nœuds sont eux même de plus en plus cupides (état G/S&PHASE-UP). Tandis que si les nœuds sont de moins en moins cupides, le nœud se positionnera de nouveau sur l'état S/H.

Cette solution a pour but de rendre les attitudes égoïstes ou cupides sans aucun intérêt pour les autres nœuds. L'auteur montre que CRISP est une stratégie particulièrement efficace même si peu de nœuds utilisent la même stratégie. Par rapport à DOMINO, vu précédemment, CRISP est basé sur plus de suppositions, comme la détermination d'uniquement trois attitudes. L'auteur rajoute que le temps n'est également pas pris en compte dans CRISP alors qu'il devrait l'être pour généraliser son résultat, une action présente ayant plus de valeur qu'une action passée.

Inspiré par la popularité et les résultats de TFT et GTFT dans le dilemme du prisonnier répété, Chen et Leneutre (2007) ont été les premiers à étudier la possibilité d'utiliser ces stratégies dans le jeu du CSMA/CA. Ils ont choisi d'appliquer une telle stratégie car elle remplissait les critères suivant :

- TFT permet de prendre une décision rapidement, basé sur peu de paramètres,
- la nature du médium de transmission permet d'observer le comportement des joueurs adverses,
- TFT vise à assurer l'égalité entre tous les joueurs, les nœuds.

GTFT est préféré à TFT à cause des différents facteurs influant la mesure du comportement. Cela permet donc d'être plus tolérant. D'après leurs résultats, si tous les nœuds suivent une stratégie basée sur TFT/GTFT et qu'ils ont une vision à long terme, alors le résultat pour l'ensemble du réseau est quasi-optimal.

Néanmoins les auteurs s'appuient sur la solution de Kyasannur et Vaidya (2003) pour la mesure du backoff des autres nœuds. Cette dernière, comme nous l'avons expliqué auparavant, entraine de sérieuses limitations comme le besoin d'avoir une entité de confiance comme destinataire. De plus, cette solution a été prévue pour les réseaux avec point d'accès et non pas ad-hoc.

CHAPITRE 4

TIT FOR TAT

4.1 Introduction

4.1.1 Nos objectifs

Notre objectif premier est la mise en place d'un protocole qui puisse résoudre la problématique de la triche dans les réseaux ad-hoc, ceci afin de garantir une certaine équité.
Les critères d'appréciation de notre protocole seront donc les suivants :
- les pertes par rapport au protocole standard,
- la réaction face à la triche.

Les pertes se mesurent grâce au débit total du réseau dans le cas où il n'y aurait pas de tricheur. La réaction sera évaluée en comparant l'évolution du débit des différents nœuds en présence d'un tricheur.

4.1.2 Implémentation dans NS2

Afin de réaliser nos tests, nous utiliserons le logiciel de simulation de réseaux Network Simulator 2 (Issariyakul et Hossain, 2008). C'est un simulateur d'évènements discrets (un ordonnanceur) orienté objet. NS2 va modéliser un réseau d'après le scenario décrit dans un script en langage OTCL (Object Tool Command Language). Le langage de l'outil de simulation est le C++.

Pour réaliser nos simulations, il faut donc créer un nouveau scénario et créer de nouveaux protocoles MAC dans NS2.

4.1.2.1 Le scénario

Le scénario n'est que le script du déroulement de la simulation. On peut le subdiviser en différentes parties :

- la déclaration des variables de simulation, comme la durée, le nombre de nœuds, le type de MAC à utiliser, etc,
- le corps du programme, c'est à dire la création des nœuds, des liens et le lancement de la simulation,
- les procédures d'enregistrement, qui vont être actives pendant la simulation à intervalles réguliers, elles vont enregistrer périodiquement les données comme le débit d'un nœud, la perte de paquets...
- la procédure d'arrêt, déclenchée juste à la fin de la simulation. C'est dans celle-ci que nous pourrons réaliser les graphiques de résultats à partir des données enregistrées.

4.1.2.2 La couche MAC dans NS2

La couche MAC est implémentée en C++ dans NS2. Elle gère l'ensemble des opérations relatives au traitement standard de la couche MAC et également une partie du travail de la couche physique.

Notre objectif est de tester différents comportements au niveau du choix de CW. Nous souhaitons donc faire interagir plusieurs protocoles MAC entre eux. Nous avons alors dupliqué le protocole MAC initial pour avoir deux nouveaux protocoles : TFT et tricheur.

Dans ces nouveaux protocoles, nous avons introduit une fonction calculant un facteur que nous nommerons FCW (pour facteur de fenêtre de contention). Ce facteur sera systématiquement multiplié à chaque résultat d'un tirage aléatoire sur CW. FCW représentera donc l'état de triche du nœud. Un nœud « normal » utilisera un FCW égal à 1, de même un nœud tricheur qui souhaite réduire la taille de sa fenêtre de 50% réduira FCW à 0.5.

C'est la fonction de calcul de FCW qui mettra en place notre stratégie TFT. Ainsi périodiquement un nouveau FCW sera calculé ce qui changera bien le comportement du nœud.

Il est à noter que la périodicité et l'activation de la fonction ne peuvent pas être gérées par le protocole lui-même. Les paramètres temporels, comme la durée de simulation ou le choix d'un changement de stratégie d'un noeud sont fixés dans le scénario car le temps n'est pas réel mais simulé.

4.2 Tit-For-Tat

4.2.1 Introduction de TFT dans le contexte

Comme nous l'avons introduit plus tôt, TFT est une stratégie bien connue et souvent utilisée dans le cadre des jeux, en particulier lors du dilemme des prisonniers répété. TFT vise à coopérer au premier tour puis à copier le comportement de la partie adverse.

Le but de TFT est de renvoyer les adversaires devant leurs propres choix. De cette façon, aucun adversaire ne peut profiter d'un changement de comportement.

Le grand avantage de TFT est sa simplicité. Étant aisément compréhensible pour ses adversaires, la dissuasion stratégique s'avère rapide. Ce qui rend cette stratégie particulièrement efficace dans un jeu répété à long terme (voir chapitre 3). C'est donc une stratégie bien adaptée à notre contexte puisque l'envoi de paquets est joué rapidement et de très nombreuses fois.

Dans ce jeu de l'envoi de paquets, le comportement des joueurs est traduit par le choix de la fenêtre de contention (CW). Cette modification de fenêtre va influer sur la répartition du débit, comme expliqué dans la problématique. Un joueur coopératif appliquera une fenêtre de contention de taille standard, comme décrit dans la norme 802.11 de l'IEEE. Un joueur

souhaitant augmenter son débit peut tenter d'utiliser une fenêtre plus petite afin d'augmenter son débit.

Rappelons que dans notre cas, tricher signifie abaisser sa fenêtre de contention (CW) par rapport aux autres joueurs, le but étant de obtenir un plus grand débit.

L'implication de TFT au sens pur du terme serait d'utiliser le même comportement, donc la même fenêtre de contention que les parties adverses. Cependant celle-ci n'étant pas connue par nature par les autres nœuds, il s'agit de trouver un moyen de l'estimer, de s'en approcher un maximum.

4.2.2 Comment détecter le comportement des autres nœuds ?

Dans un réseau ad-hoc, chaque nœud étant indépendant, les seules mesures pouvant être relevées sont celle des types de paquets transitant par le médium, chaque nœud étant à portée l'un de l'autre. Les différents types de paquets transmis fournissent une information sur l'activité du réseau. Un nœud peut ainsi évaluer sa propre activité par rapport à l'activité de l'ensemble du réseau.

Dans un réseau sans tricheur (toujours dans un état de saturation bien sûr), chaque nœud devrait avoir une activité proche à la moyenne de l'activité des autres nœuds. La présence de tricheur(s) serait alors détectée par une baisse de l'activité des nœuds normaux par rapport à l'ensemble du réseau. Chaque nœud peut alors mettre en place un système de détection de triche en surveillant l'activité du réseau.

Pour évaluer ce rapport d'utilisation du médium, nous mettons en place un ratio d'activité. Le type de paquet que nous utiliserons pour l'évaluation de l’activité d’un nœud est le RTS car il initialise le transfert de données, il est bien donc représentatif de l'activité des nœuds, c'est un bon indicateur.

Rappelons que dans notre simulation nous utilisons une cellule où les nœuds sont à portée les uns des autres. Le choix du type de message à mesurer (RTS) est important pour appliquer cette solution à un réseau global. L'utilisation du compte des messages CTS et ACK ne donnerai pas toute l'information pour mesurer les paquets envoyés par les nœuds proches à des nœuds lointains dont le CTS ne serait pas écouté. Notons bien que la détection de l'activité par les messages RTS est une solution applicable à un réseau global puisqu'il permet bien d'évaluer l'activité d'émission des nœuds à portée.

$$\textit{Ratio d'activité(A)=(n-1)(RTSenvoye(A))/(RTSenvoye(nœuds différents de A))} \quad (4.1)$$

où n représente le nombre de nœuds

A représente le noeud

Ce ratio, calculé périodiquement, permet de juger si l'activité du nœud A est inférieure, supérieure ou égale à la moyenne d'activité des autres nœuds. C'est donc un ratio d'activité global du reste du réseau.

Le ratio étant calculé périodiquement, une marge d'erreur peut-être mise en place afin d'éviter les aléas qui peuvent survenir (la valeur du backoff étant tiré aléatoirement dans la CW).

4.2.3 Comment copier le comportement adverse ?

Du point de vue d'un nœud, le ratio permet uniquement de détecter si les autres nœuds trichent en moyenne plus ou moins que lui-même mais ne permet pas de connaître de combien les adversaires trichent ni bien sûr qui triche puisqu'il est calculé globalement.

Autrement dit, le ratio ne nous permettra pas de connaître la taille de la fenêtre de contention, mais uniquement si la fenêtre moyenne des autres noeuds est plus grande ou plus petite que la nôtre.

De plus, le tirage aléatoire du backoff ayant lieu après une collision où quand le médium est occupé, l'action n'a pas systématiquement lieu au même moment chez tous les joueurs, le jeu n'est pas synchrone. Pour pallier ceci, il faudra donc raisonner par périodes.

Ainsi un nœud ne peut s'approcher du comportement adversaire que par tâtonnements et évaluations successives. Périodiquement, un nœud devra recalculer son ratio afin de savoir qui de lui ou de l'ensemble des autres nœuds, abaisse le plus CW afin d'obtenir plus de débit. La modification de la taille de sa fenêtre de contention sera traduite dans notre implémentation de TFT par l'utilisation du facteur multiplicatif de la fenêtre de contention (FCW) compris entre 0 et 1.

Le niveau de FCW représente l'état du niveau de coopération (ou de triche donc). Ainsi les états 0 et 1 représentent respectivement la triche et la coopération totale. Périodiquement, un nœud utilisant TFT peut alors estimer son ratio et agir en conséquence en faisant varier son facteur de fenêtre de contention.

L'algorithme de TFT se situe dans l'actualisation de FCW. Comme nous pouvons le voir dans le pseudo algorithme ci-dessous, à chaque période d'actualisation de FCW, un ratio est calculé. Ce ratio va déterminer le sens de la variation apportée à FCW.

Algorithme 1 TFT, actualisation de FCW

```
Ratio(A)=(n-1)(RTSenvoye(A))/(RTSenvoye(nœuds différents de A))

si ratio_a>1+marge d'erreur {
        FCW=FCW/variation;
        }
si ratio_a<1+marge d'erreur{
        FCW=FCW*variation;
        }
si (FCW>1) {FCW=1;}
RTSenvoye=0;
```

```
nbRTSdetectes=0;
```

4.2.4 Paramètres de TFT

Les différents paramètres influant sur notre protocole TFT sont :
- la variation effectuée sur le facteur, qui va définir la taille de l'ajustement du facteur de CW,
- la période d'actualisation, qui régit la vitesse de TFT,
- la marge d'erreur, introduite pour compenser le hasard du tirage sur CW dans une courte période d'évaluation.

Nous formulons différentes hypothèses logiques sur l'impact de chacun des paramètres sur l'utilisation de TFT.

La taille de la variation, effectuée sur le facteur, représente l'ampleur de notre réaction face au comportement adverse à chaque tour. Une augmentation de cette variation traduit donc une adaptation, une réponse plus rapide, avec une modification plus importante de CW face au contexte. Cependant si la variation est plus grande, cette adaptation sera également moins précise et ainsi plus coûteuse en terme de bande passante.

La période d'actualisation de TFT peut jouer un rôle décisif. Sur une période plus courte, le hasard du tirage aléatoire sur CW est globalement moins équitable. Par conséquence, on devrait observer un déséquilibre plus important en terme d'envoi de paquets par nœud. Le ratio est alors moins précis que sur une longue période.

De plus, une période d'actualisation courte entrainera naturellement plus de choix, donc de variations de la part de TFT. Il s'ensuivrait une amélioration de la rapidité de réponse.

La marge d'erreur, est sensée compenser le hasard du tirage aléatoire entre plusieurs joueurs sur une fenêtre donnée. Une augmentation de la marge rend le protocole plus permissif,

moins précis en dégradant la détection de la triche. D'un autre côté, le coût global s'en trouve réduit car il y a moins de faux positifs.

4.2.5 Tests

Le premier scenario à effectuer est celui du débit du protocole TFT par rapport au protocole standard. En effet, de ces pertes dépend la viabilité du protocole. Nous observons le débit total du réseau afin d'observer le résultat de TFT sur l'ensemble du réseau, et non pas du point de vue d'un seul nœud. Ainsi dans ces tests, tous les nœuds seront coopératifs et utiliseront la stratégie TFT telle que définie

L'objectif étant de vérifier les hypothèses d'impact des paramètres, quatre tests seront réalisés pour tester les impacts de ces paramètres. Nous changerons successivement la variation, la période puis la marge d’erreur.

4.2.5.1 Test TFT témoin

Le premier test est un test témoin qui nous permettra par la suite de comparer la variation des paramètres lors des prochains tests. Pour ce premier test, la variation est fixée à 20%, la marge d’erreur utilisée est de 1% et la période d’actualisation est de 5 secondes.

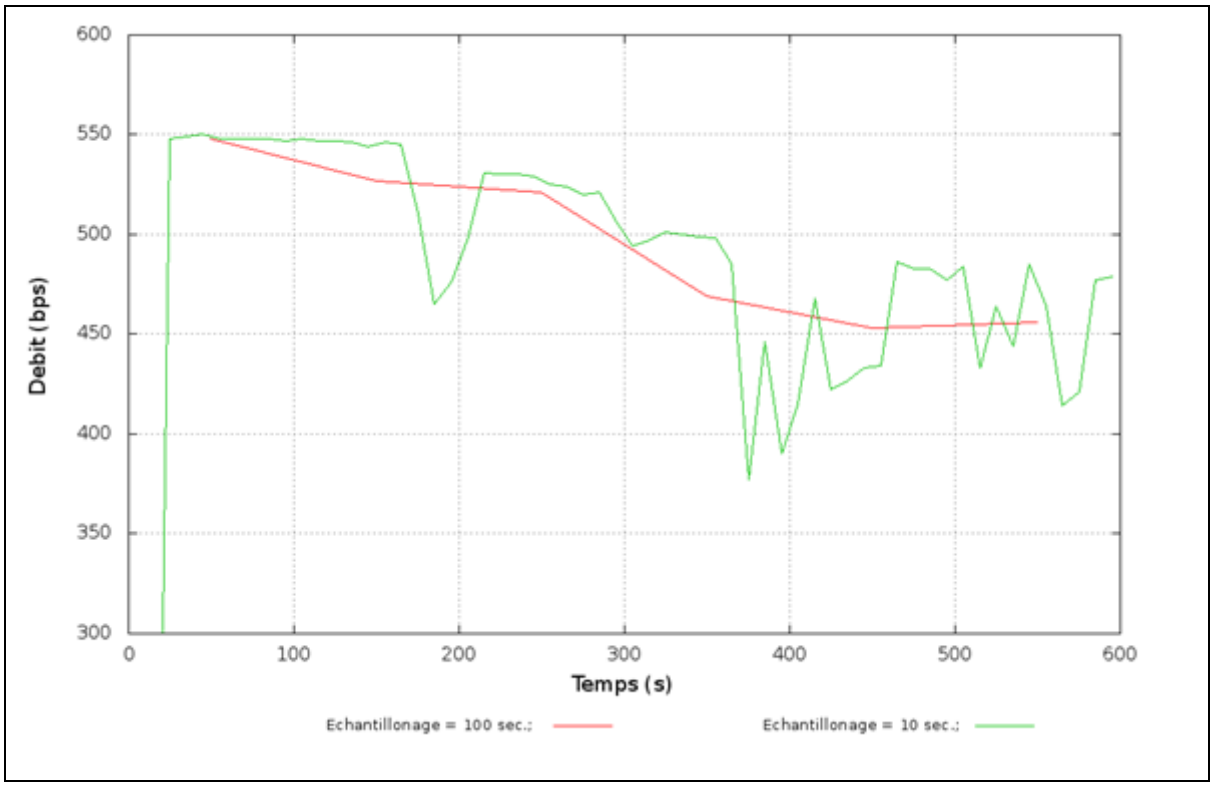

Figure 4.1 Graphique TFT témoin

4.2.5.2 Diminution de la variation

Nous réalisons maintenant le même test que précédemment en utilisant une stratégie TFT avec une variation de 10%.

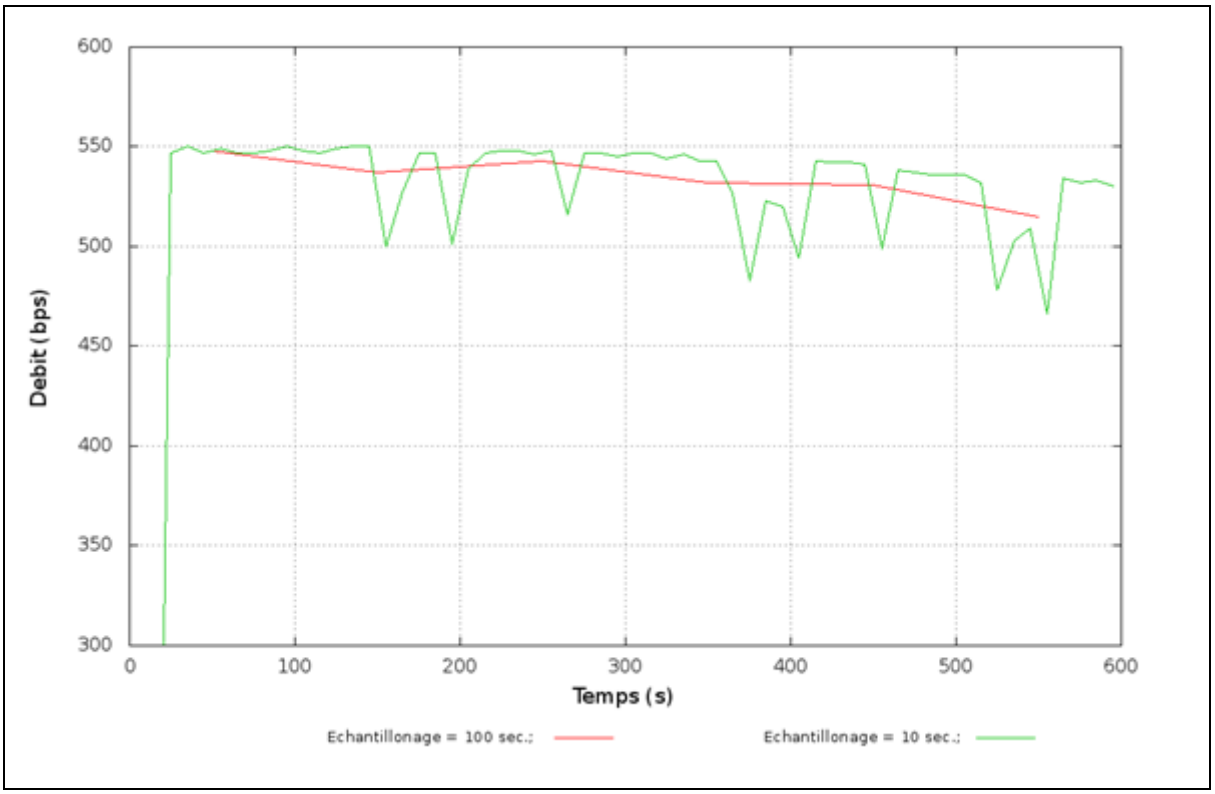

Figure 4.2 TFT, variation 10%

Nous voyons que les nœuds utilisant la variation de 20% subissent une chute plus sévère que ceux avec une variation de 10%. Les pertes du réseau en débit sont donc plus élevées avec une variation plus importante. Nous vérifions donc bien l'hypothèse d'augmentation des pertes avec la variation formulée auparavant.

4.2.5.3 Augmentation de la période

Afin d'observer l'influence de la période, comparons notre graphique TFT témoin avec ce test où nous ne changeons que la période, fixée à 10 secondes.

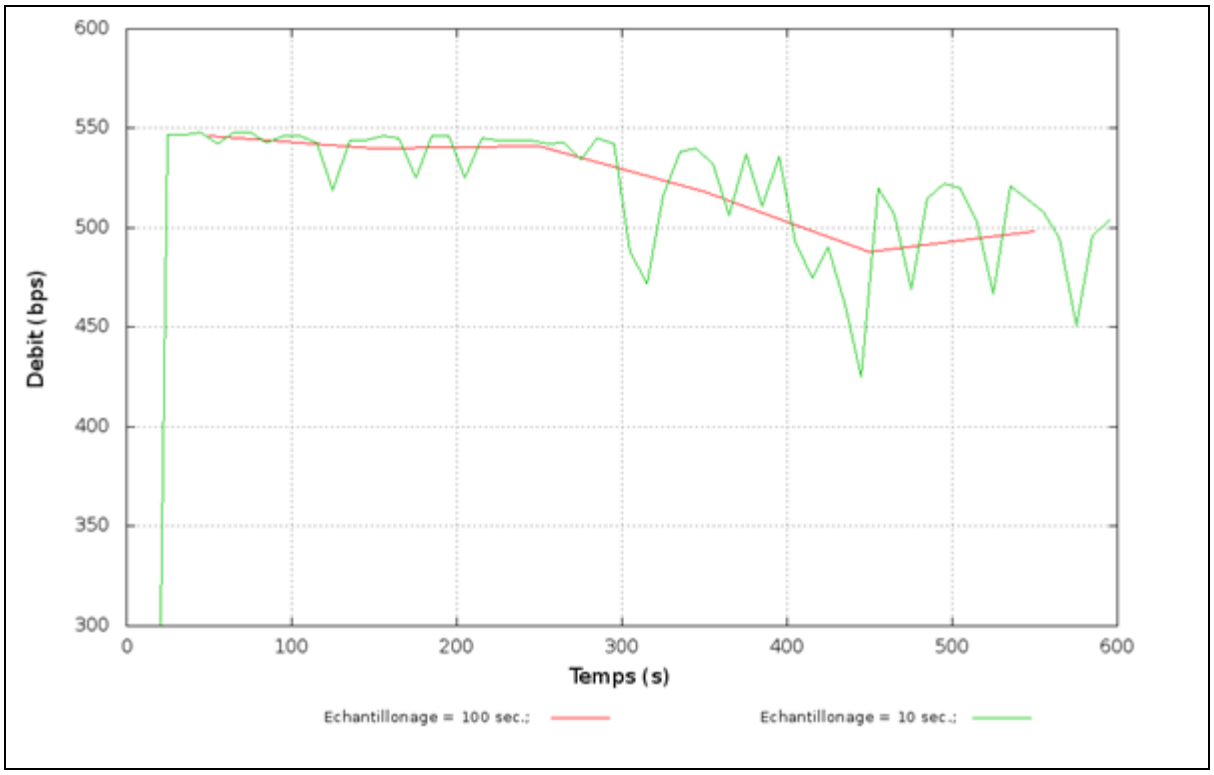

Figure 4.3 TFT, période : 10 secondes

La figure 4.3 présente les résultats obtenus en utilisant une période d'actualisation de FCW plus grande que celle dans la figure 4.1. Les pertes observées retardées dans la figure 4.3 ou la chute est atténuée par rapport au graphique témoin. Une plus grande période entraine donc une réaction plus lente, mais plus précise car les faux-positifs devraient être moins nombreux avec une plus grande période. L'hypothèse logique est vérifiée.

4.2.5.4 Augmentation de la marge d'erreur

Nous procédons de la même manière pour la marge d'erreur avec un test où cette marge est de 10%.

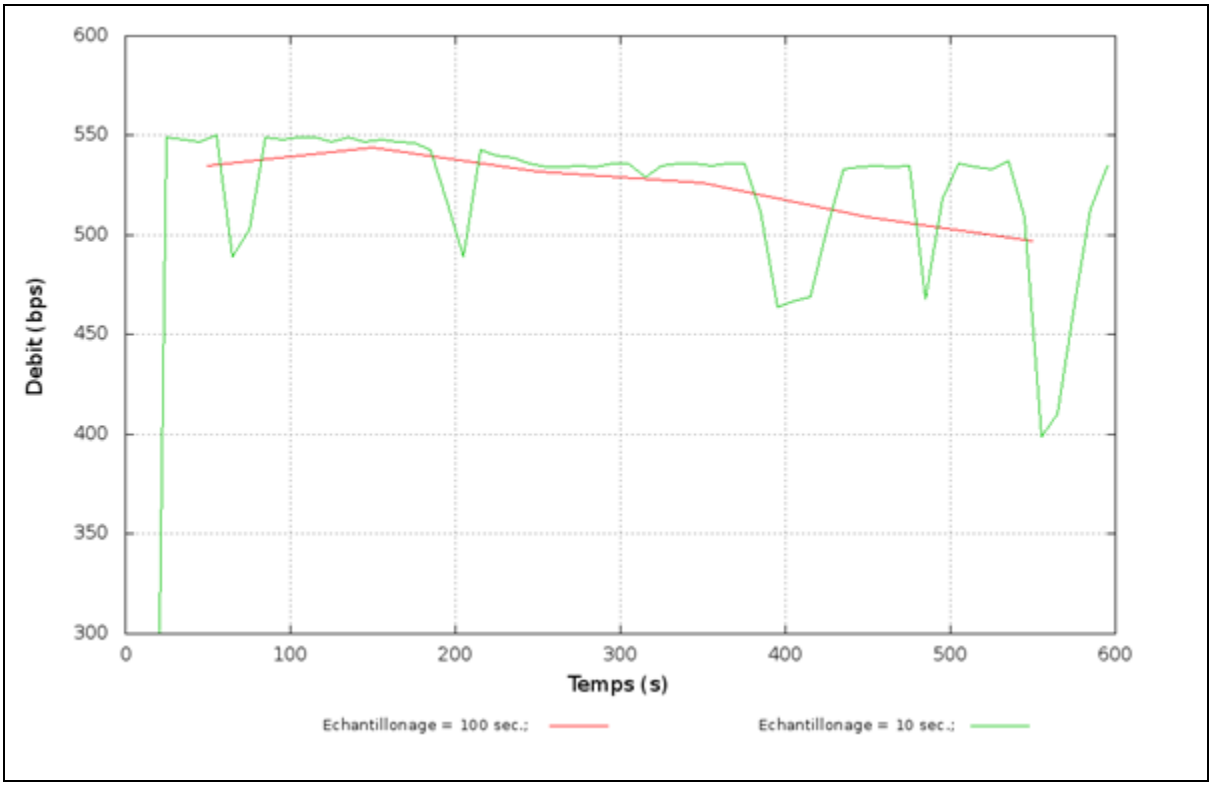

Figure 4.4 TFT, marge d'erreur : 10%

En augmentant la marge d'erreur, de 1% (pour le graphique 4.1) à 10%, nous obtenons la figure 4.4. La marge d'erreur diminue la chute du débit, le coût est moins élevé avec une marge d'erreur de 10%.

Il est à noter qu'en prenant des valeurs extrêmes, aucun des paramètres ne permet d'avoir un résultat parfait. Une marge d'erreur de 100% rendrait TFT aveugle aux tricheurs, de même qu'une période trop longue n'aurait aucun impact car la réaction serait bien trop lente. Les paramètres changent donc les caractéristiques de TFT, un compromis est nécessaire pour avoir un protocole équilibré.

4.2.6 Observations sur TFT

Dans chaque figure, une chute plus ou moins rapide du débit peut être relevée. Cette chute de débit rend le protocole TFT coûteux sur le long terme. Le protocole TFT en l'état ne peut pas

être efficacement utilisé, le coût de l'égalité qu'impose TFT va progressivement se révéler élevé pour le réseau.

La raison de ce coût est à chercher dans les conditions du jeu par rapport à un dilemme de prisonnier classique. Comme nous l'avons introduit dans l'étude de la littérature, TFT est un protocole fonctionnant très bien dans un modèle parfait. Cependant l'introduction du bruit dans l'environnement de jeu est une des conditions de défaillances, de perte de performance de TFT. Or ce bruit est bien présent dans les communications wifi. De plus, l'observation s'effectue sur une seule période et les réseaux ad-hoc sont connus pour souffrir d'iniquité a cours terme (Koksal et al, 2000 ; Nandagopal et al, 2000). Cette iniquité et ce bruit entrainent une mauvaise appréciation du comportement adverse qui dérègle progressivement TFT. Ce n'est donc pas une stratégie appropriée.

Un ajustement important de la marge d'erreur réduirait les pertes et rendrait le protocole performant si tous les nœuds l'utilisent. Cependant un tricheur pourrait abaisser sa fenêtre de contention, juste assez pour rester indétectable par TFT. Il s'agit donc de trouver un moyen de réduire les pertes liés au bruit et aux aléas du réseau sans pénaliser la détection de la triche.

4.3 Generous Tit For Tat

4.3.1 Principe

Nous avons introduit brièvement *Generous Tit For Tat* dans la partie précédente. C'est une stratégie dérivée de TFT qui, comme nous l'avons dit, peut être utilisée dans des dilemmes des prisonniers répétés avec une présence de bruit.

Un joueur suivant la stratégie GTFT coopère au premier tour. Ensuite il copie le comportement adverse au tour précédent, mais quand la partie adverse ne coopère pas, il y a une petite probabilité que le joueur utilisant GTFT coopère quand même. Cette probabilité est le facteur de générosité.

Ce facteur de générosité a donc pour objectif de pouvoir rétablir la coopération en cas d'erreur d'interprétation de comportement. C'est un outil incitatif pour la coopération, il a vocation à réduire les pertes liées à l'abaissement de la taille de CW.

4.3.2 Implémentation

D'un point de vue pratique, la générosité se traduit par une probabilité de coopérer, donc d'augmenter FCW même avec un ratio négatif.

Algorithme 2 - GTFT, actualisation de FCW

```
Ratio(A)=(n-1)(RTSenvoye(A))/(RTSenvoye(nœuds différents de A))
si ratio(A)>1+margeerreur {
        FCW=FCW/variation;
        }
si ratio_a<1+margeerreur {
        x=random(0-1)   //valeurs continues
        if  x>G
                FCW=FCW/variation; }
                else {
        FCW=FCW*variation;
        } }
si (FCW>1) {FCW=1;}
RTSenvoye=0;
nbRTSdetectes=0;
```

L'implémentation de GTFT dans notre algorithme ne modifie donc que la réaction face à la triche. Le facteur G est la probabilité de générosité accordée.

4.3.3 Choix du facteur de générosité

Nous allons observer le choix du facteur de générosité. Intuitivement, si on prend G au maximum, 1, il n'y aura pas de problème s'il n'y a pas de tricheur, mais le joueur suivant GTFT coopérera dans tous les cas, quoique fasse la partie adverse. A l'opposé, si G est à 0, c'est en fait TFT qui est appliqué, et il n'y a plus d'incitatif à la coopération, les pertes ne sont alors pas réduites.

Nous comprenons maintenant qu'augmenter la générosité va abaisser les pertes de fonctionnement normal (sans tricheur) mais diminuer l'efficacité face au(x) tricheur(s).

4.3.4 Tests

Nous allons tout d'abord tester les pertes du protocole lui-même avec différents facteurs de générosité et tous les nœuds coopératifs, comme nous l'avions fait avec TFT. Puis nous introduirons un tricheur et tenterons encore de faire varier le facteur de générosité afin de comprendre son impact. Dans ces tests, les paramètres précédemment étudiés : la variation, la marge d'erreur et la période, seront systématiquement les mêmes que ceux choisis pour la simulation, soit respectivement 20%, 1% et 5 secondes.

4.3.4.1 Tests de pertes

Nous effectuons un premier test avec tous les nœuds coopératifs avec un facteur de générosité de 10% puis un second avec une valeur de 20%.

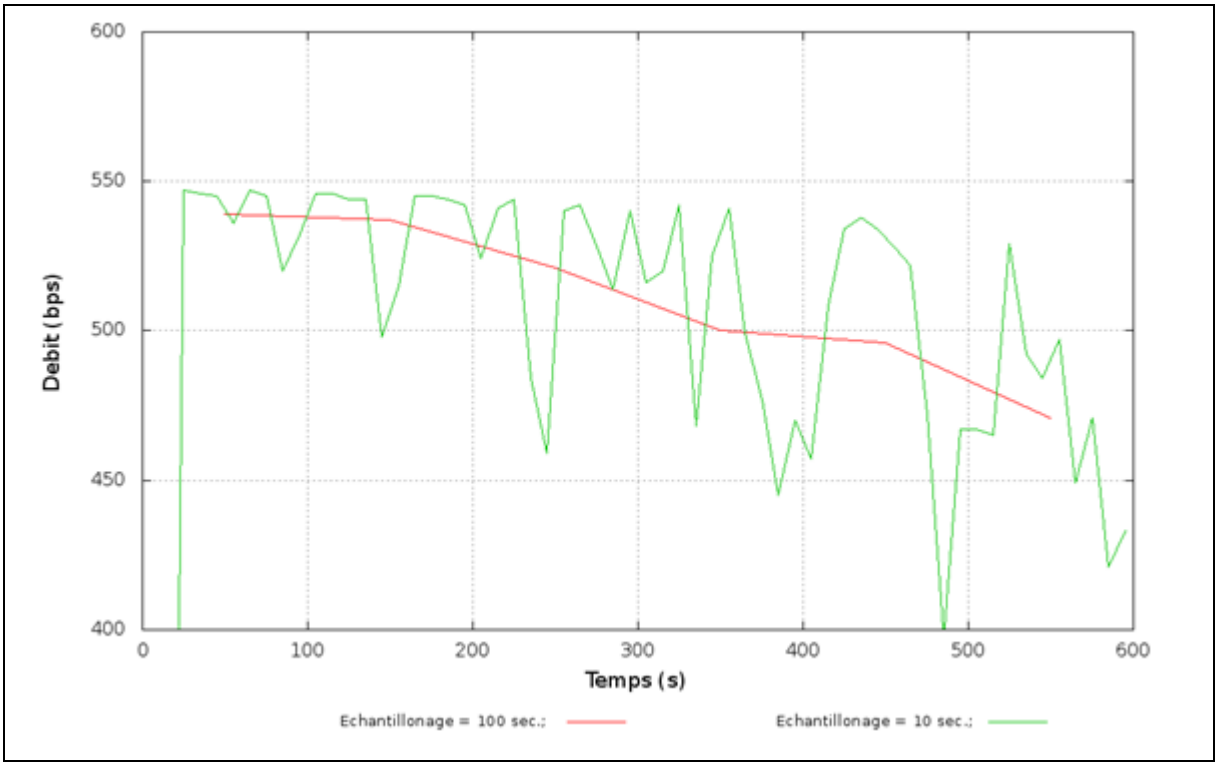

Figure 4.5 GTFT, générosité : 10%

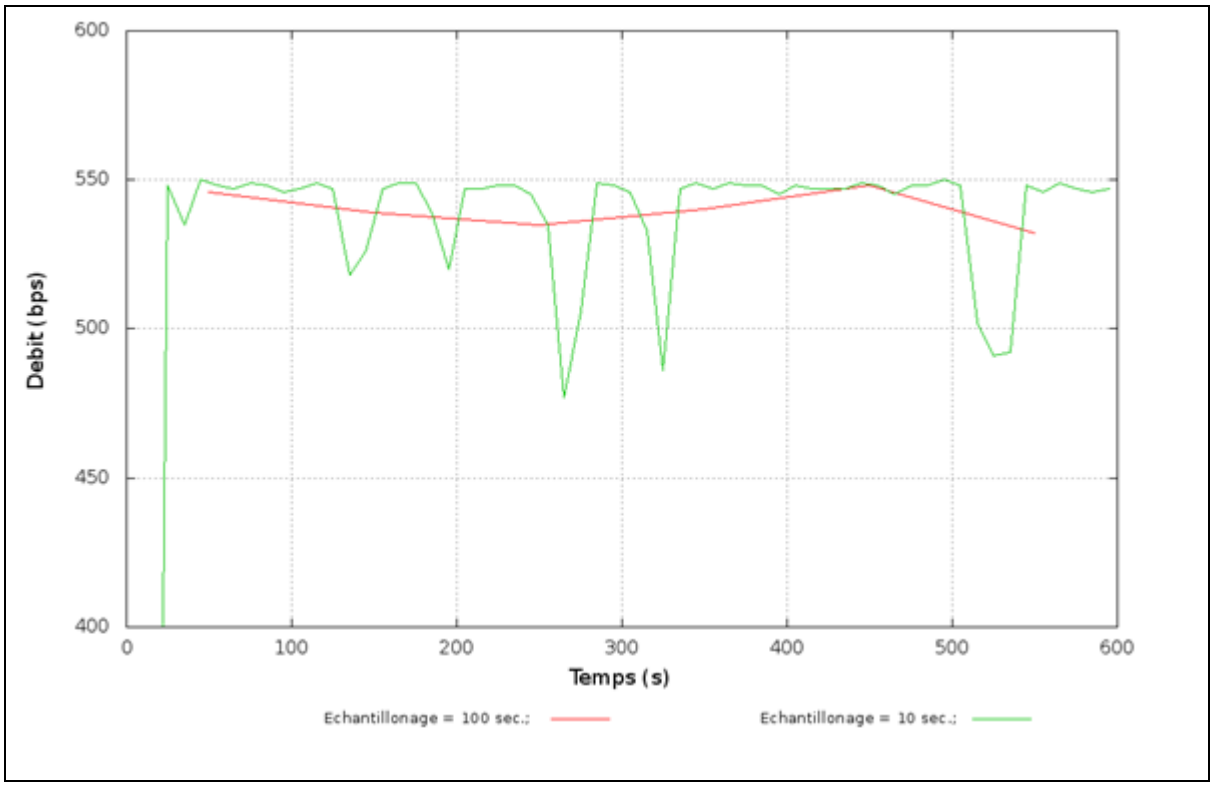

Figure 4.6 GTFT, générosité : 20%

4.3.4.2 Discussion des résultats

La figure 4.5 présente le test de coût avec une générosité de 10%, nous pouvons observer que cette générosité ne suffit pas à empêcher la diminution du débit. Remarquons que cette diminution est plus faible que dans le cas où il n'y aurait pas de générosité (figure 4.1).

Dans la figure 4.6 nous observons que la perte de débit est maintenue à un seuil suffisant et relativement constant. Comparé aux figures 4.1 et 4.5, les pertes sont bien constantes et maitrisées, l'objectif du facteur de générosité est atteint, il permet bien de diminuer les pertes. Nous comprenons alors l'impact du facteur de générosité avec ces résultats et les précédents (TFT). Un facteur de générosité trop faible ou inexistant entraîne des pertes plus ou moins importantes du débit du réseau.

4.3.4.3 Tests d'introduction d'un tricheur

Pour une première fois, nous allons maintenant comparer la réaction de GTFT face à un tricheur pour nos deux facteurs de générosité différents, les autres paramètres restant inchangés. Un nœud parmi les 8 va, au bout de 100 secondes, diminuer sa fenêtre de contention de moitié, c'est le tricheur.

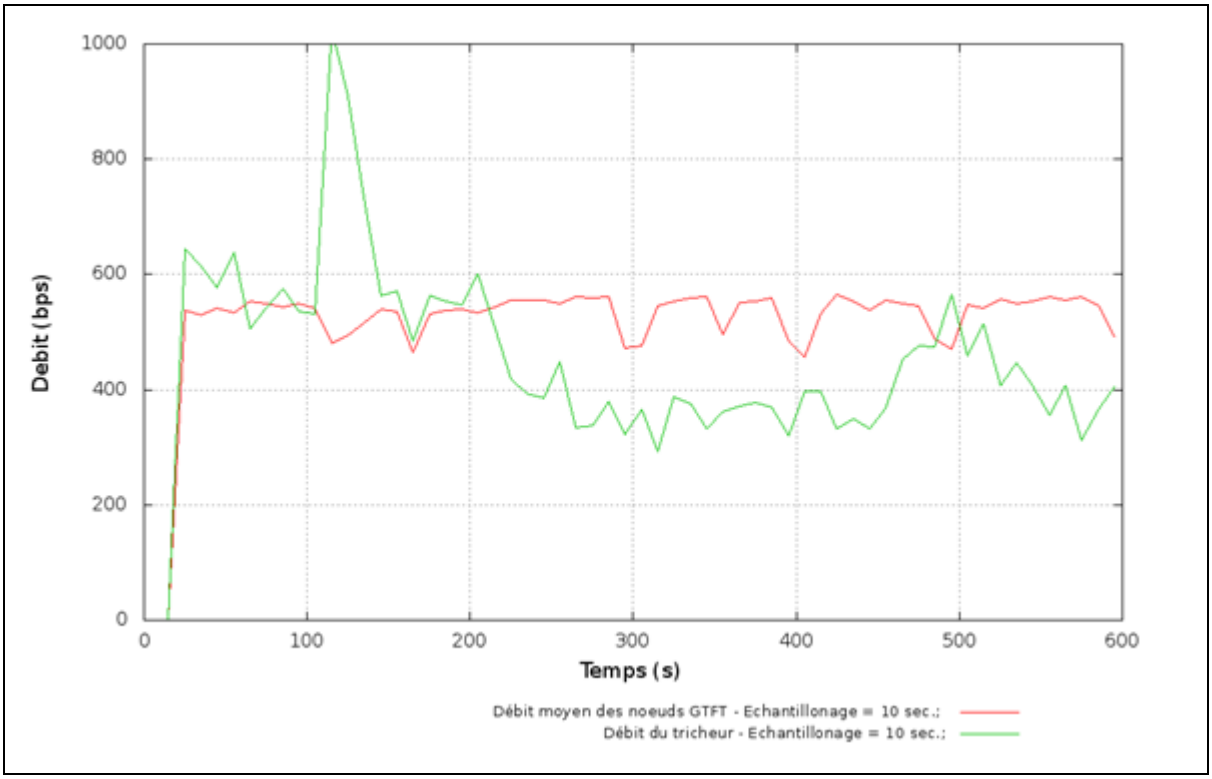

Figure 4.7 GTFT, un tricheur, générosité : 10%

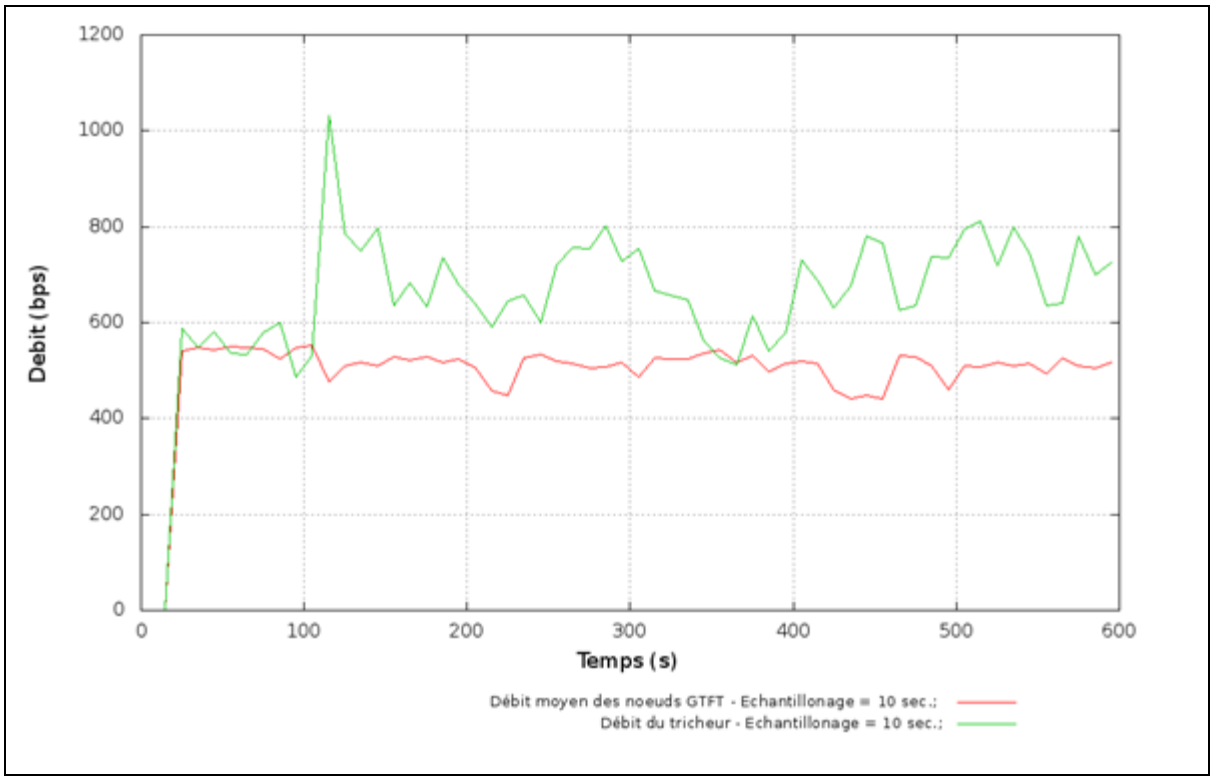

Figure 4.8 GTFT, un tricheur, générosité : 20%

4.3.4.4 Discussion des résultats

La figure 4.7 nous permet d'observer la réaction de GTFT face à un tricheur. La réaction des nœuds utilisant GTFT est directement visible, le nœud tricheur commence à abaisser sa fenêtre de contention à partir de 100 secondes. Il s'ensuit tout de suite un très net avantage de débit en sa faveur. On observe presque un doublement de son débit. Puis la répartition du débit s'équilibre jusqu'à devenir légèrement favorable aux nœuds suivant GTFT.

L'augmentation soudaine du débit du nœud tricheur est la conséquence directe de la diminution de moitié de la taille de sa fenêtre de contention. Le rééquilibrage progressif de la répartition de la bande passante est dû à la réaction des nœuds utilisant GTFT qui, progressivement, s'adaptent et diminuent leur fenêtre de contention. Nous voyons que le facteur de générosité de 10% ne suffit pas empêcher une trop grande diminution de CW de la part des nœuds avec GTFT, et ne permet donc pas de maintenir l'équilibre en terme de

partage de bande passante entre le tricheur et les nœuds suivant GTFT. Celui-ci devient donc favorable à ces derniers.
En testant l'utilisation d'une stratégie GTFT avec un facteur de générosité à 20% contre ce même tricheur, on obtient la figure 4.8. Nous observons un pic de débit similaire lors du déclenchement de la triche sur la CW. Ensuite, la répartition du débit s'équilibre mais reste favorable au nœud tricheur.

L'impact négatif du facteur de générosité se révèle en comparant la figure 4.7 et la figure 4.8. Dans les deux cas, une période d'adaptation est observée, puis une stabilisation a lieu. Nous pouvons voir qu'après cette période d'adaptation, une différence de débit est observée entre le tricheur et les nœuds utilisant GTFT. De plus, cette différence en terme de débit est plus avantageuse pour le tricheur dans la figure 4.8, donc avec un facteur de générosité plus élevé. Nous comprenons alors l'impact négatif d'un facteur de générosité élevé, une diminution de l'efficacité face aux tricheurs. Cette perte est due directement au facteur de générosité qui tente d'inciter le tricheur à la coopération.

4.3.5 Bilan de GTFT

GTFT nous a permis de diminuer les pertes liés aux erreurs d'appréciation et d'avoir un incitatif à la coopération. Cependant, cela se compense par une efficacité moindre face à un ou plusieurs tricheurs comme nous l'avons vu.

Le problème de GTFT réside dans le fait qu'il est difficile de choisir un facteur de générosité optimum. Il serait surement astucieux de garder un facteur de générosité faible pour être efficace comme stabilisateur, tout en restant un tant soit peu incitatif à la coopération et de trouver un autre moyen pour réduire les pertes liées aux erreurs passagères.

4.4 RTFT

4.4.1 Le principe de la réputation

Dans les stratégies de jeu, la réputation est un outil régulièrement utilisé. Un score de réputation attribué à un joueur correspond à l'observation de ses actions passées, on peut donc dire que ce score représente l'ensemble du passé du joueur, sensé représenter son comportement sur le long terme. Généralement, la réputation est calculée telle qu'un bon score de réputation indique une forte coopération dans le passé et vice versa.

La réputation va permettre d'avoir un outil plus stable, moins sensible aux perturbations passagères qui sont multiples dans le cas d'un réseau Wifi.

Cependant il apparaît qu'un score de réputation qui prend en compte toutes les périodes passées de manière équivalente serait, au fur et à mesure, de plus en plus incohérent avec la stratégie présente de la partie adverse. Il est donc nécessaire de valoriser le passé proche par rapport au passé lointain afin de conserver une réactivité cohérente.

4.4.2 Implémentation

L'utilisation de la réputation se traduit par une insertion d'un facteur de relativité dans la formule de calcul du ratio. Celui-ci dépend maintenant du ratio précédent, tel une fonction itérative. C'est une moyenne pondérée des observations successives.

$$Ratio(A) = (n-1)*(RTSenvoye(A)/RTSenvoye(\text{nœuds différents de A}))*(1-Relativite)+Ratio(A)*(Relativite) \quad (4.2)$$

où n représente le nombre de nœuds, 0<Relativite<1

Notons qu'ici une relativité égale à 0 signifierait que le passé ne serait pas pris en compte et le protocole fonctionnerait comme TFT ou GTFT pour ce calcul du ratio d'activité.

4.4.3 Influence de la relativité

D'après la formule (4.2), plus la relativité diminue, moins le passé proche influe sur notre considération. Ainsi, le déclenchement de la réaction aura tendance à être de plus en plus retardé. Prendre en compte plus de passé donnera un protocole plus stable.

Il est bon de noter que cet impact est à différencier de l'impact de la diminution de la période. En effet, celle-ci ralentirait la réaction, tandis que l'augmentation de la relativité va uniquement retarder cette réaction, pas la ralentir.

Entre l'augmentation de la période et la diminution de la relativité, l'objectif est le même : la diminution des pertes liées aux aléas, mais les conséquences sur le comportement sont un peu différentes puisque la relativité joue plus sur la réactivité tandis que la période sur la rapidité uniquement.

4.4.4 Tests

De la même manière pour TFT et GTFT, nous allons d'abord effectuer un test mesurant les pertes intrinsèques avant d'introduire un tricheur. Les paramètres précédemment étudiés (la variation, la marge d’erreur et la période) resteront inchangés (soit respectivement 20%, 1% et 5 secondes). Nous utiliserons une générosité de 10% afin de comparer l'impact du facteur de relativité sur la bande passante avec les résultats de GTFT dans la section précédente.

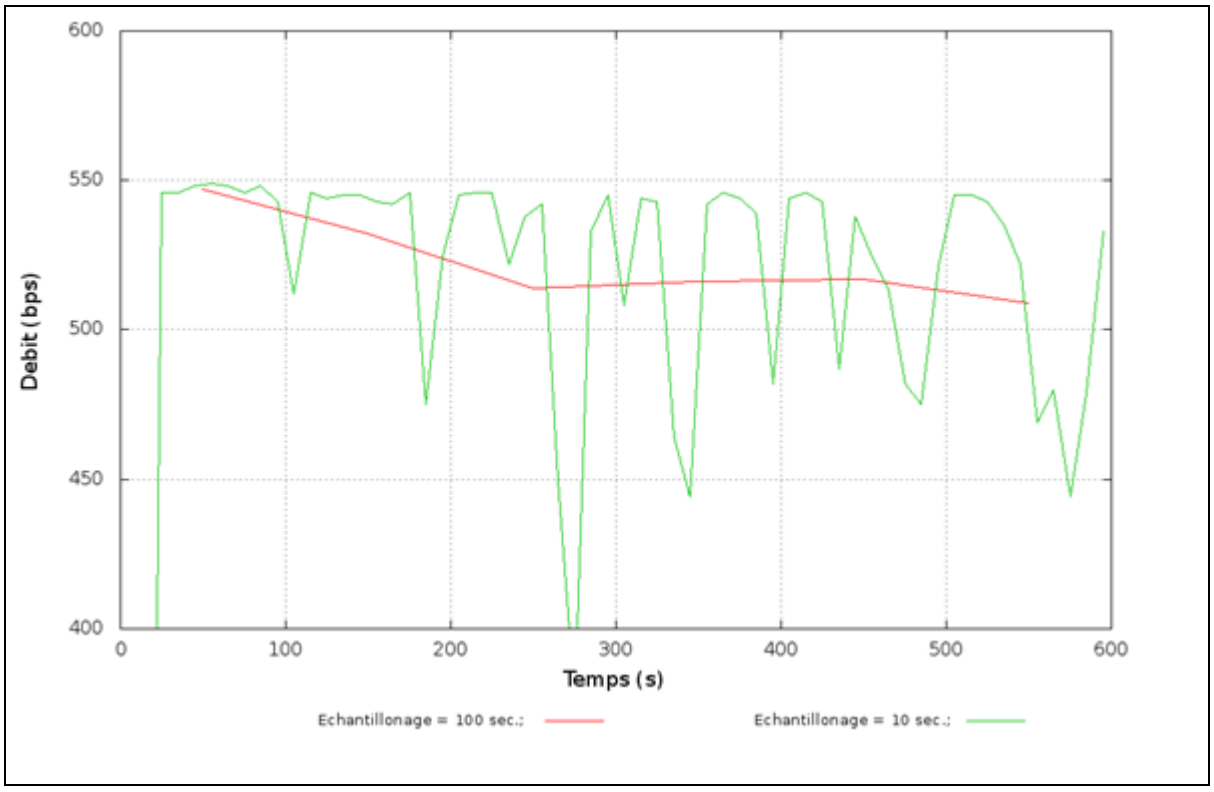

Figure 4.9 RTFT, relativité : 50%

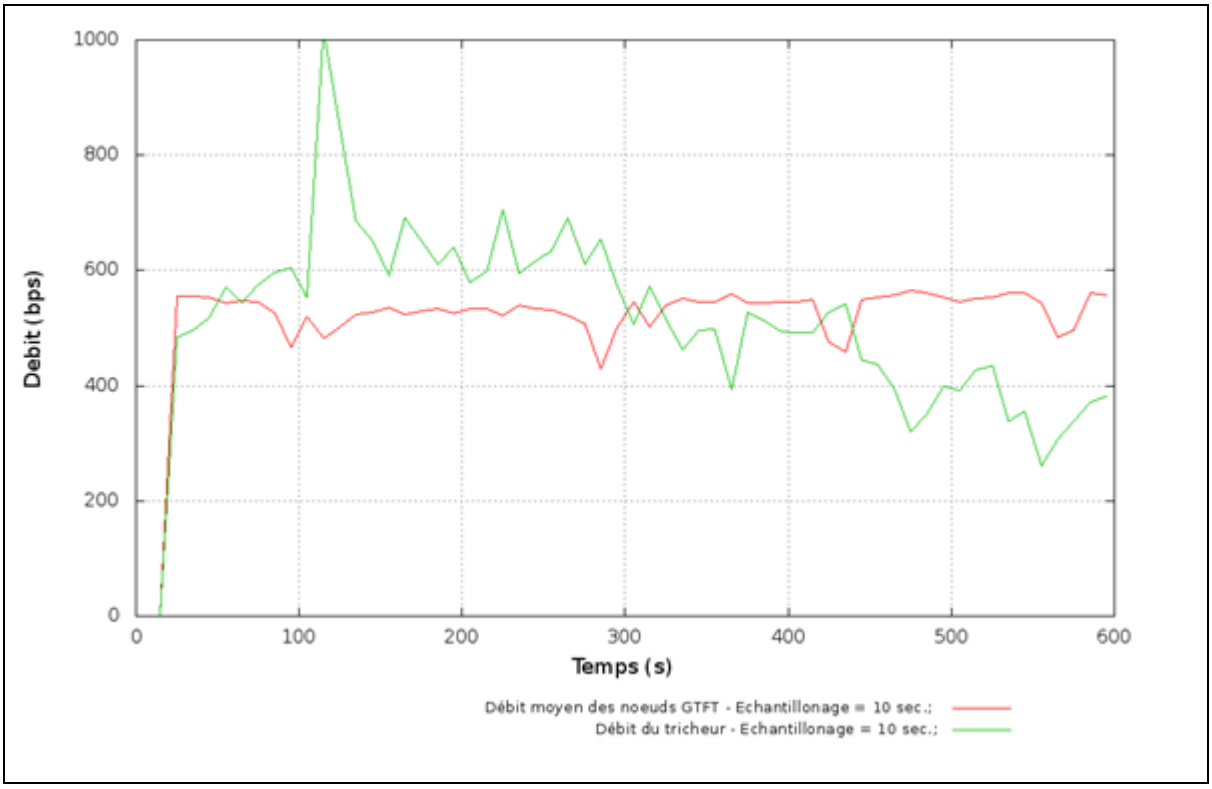

Figure 4.10 RTFT, un tricheur, relativité : 50%

4.4.5 Discussion des résultats

Le test de coût simulé dans la figure 4.9 nous montre des pertes moins importantes avec un facteur de relativité à 0.5. La chute du débit est moins rapide qu'avec un facteur de générosité de 0 (GTFT, figure 4.5). La relativité permet de rendre les aléas de bruits moins représentatifs et par cela de faire baisser les pertes.

Dans la figure 4.10, nous voyons maintenant la réaction de RTFT face à un tricheur. Nous observons que la différence avec la situation sans facteur de relativité se voit surtout par un retard dans la réaction des nœuds. La chute de débit est en décalage par rapport à la figure 4.7. La réaction face à la triche est un peu retardée si l'on augmente la relativité. L'hypothèse est vérifiée.

4.5 Conclusion et comparaison

Nous avons maintenant analysé l'impact de chacun des facteurs de TFT ainsi que les conséquences de l'implication d'un facteur de générosité et de la réputation. Notons bien qu'utiliser GTFT avec G=1 ou RTFT avec R=0 revient à utiliser TFT. Nous ne faisons que prendre en compte d'autres variations de facteurs mais la nature de la stratégie reste la même.

Dans nos résultats, il apparaît que chaque variation de facteur à un impact positif, et un impact négatif. C'est la combinaison de ces facteurs qui donne les résultats trouvés.

Tableau 7 Influence des paramètres

Paramètre en augmentation	**Impact positif**	**Impact négatif**
Variation	Accélération de la vitesse d'ajustement (rapidité)	Augmentation des pertes d'ajustement (coûts)
Marge d'erreur	Diminution du nombre de faux-positifs	Augmentation du seuil de punition de la triche
Période	Augmentation de la précision dans la détection de tricheurs	Diminution de la vitesse d'ajustement (rapidité)
Facteur de générosité	Rétablissement de la coopération, diminution des coûts induits par les faux-positifs	Diminution de l'efficacité face aux tricheurs
Facteur de relativité	Diminution de la réactivité	Augmentation de la précision dans la détection de tricheurs

Il n'y a pas une variante de TFT idéale avec les paramètres idéaux fixés. Chacun des paramètres peut être ajusté afin d'obtenir le protocole voulu.

Par exemple, si l'on a un réseau destiné à être relativement stable, sans grand changement de comportement parmi les nœuds, il peut être préférable d'augmenter la période et d'augmenter le facteur de relativité, la baisse de rapidité et de réactivité engendrée entrainera une augmentation de la précision. La stratégie TFT doit s’adapter au contexte.

CONCLUSION

La forte croissance des réseaux Wifi est une composante majeure du développement des télécommunications. Les réseaux ad-hoc, tout d'abord limités à des usages d'urgence ou militaires, sont parfois déployés dans le cadre d'autres utilisations, comme dans les villes et les réseaux communautaires. Ils permettent de s'affranchir de la contrainte du point d'accès qui limite la flexibilité du déploiement des réseaux sans-fils. Ils souffrent néanmoins du fait de ne pas avoir d'entité de confiance sur le réseau.

Dans ce mémoire nous avons exposé une problématique importante au niveau du comportement des nœuds dans la sous-couche MAC. Nous avons démontré en quoi la coopération est nécessaire car elle maximise l'utilité, soit la bande passante disponible, du réseau. Nous avons exploré les différents travaux qui ont soulevé cette problématique et par quel biais ils l'ont fait.

Inspiré par la théorie des jeux. Nous avons cherché à mettre en place une stratégie de défense face à ce comportement égoïste au niveau de la sous-couche MAC. Nous avons fait l'analogie entre le dilemme du prisonnier répété et le jeu du backoff entre les nœuds. Cela nous a amené à introduire TFT et des variantes, GTFT et RTFT, comme stratégies pour les nœuds.

Des contraintes liées à la nature du jeu ont imposé des paramètres de fonctionnement de TFT :

- le tirage du backoff est aléatoire, nous avons donc introduit une marge d'erreur pour compenser les disparités,
- le comportement adverse est une information cachée, on choisit de l'approcher par tâtonnements, nous avons introduit la variation,
- les tirages du backoff ne se font pas forcément au même moment chez les joueurs, le jeu n'est pas synchrone, nous utiliserons donc une période d'actualisation pour raisonner par intervalles.

Nous avons exprimé les variantes de TFT grâce à d'autres paramètres, la générosité pour GTFT et la relativité pour RTFT. Nous avons alors pu réaliser des simulations afin d'observer l'impact de nos stratégies entre elles et face à un nœud égoïste.

Les résultats ont montré que TFT était défaillant, des erreurs étant générées par le bruit présent dans les réseaux sans-fils. L'ajout d'un facteur de générosité par contre rend GTFT viable et réactif face aux comportements égoïstes.

Nous utilisons nos simulations pour déterminer l'influence des paramètres sur le fonctionnement de la stratégie et les conséquences pour le nœud ainsi que pour le réseau. La conclusion qui en ressort est que chaque variation de paramètre entraine à la fois une réaction positive et une autre négative pour le nœud. Il n'y a donc pas de choix de facteurs optimaux pour contre n'importe quelle stratégie. La stratégie doit s'adapter au contexte.

Grace à notre implémentation originale de stratégies dérivées de TFT, nous avons prouvé que l'introduction de ces stratégies au niveau du jeu de tirage du backoff peut bien permettre de répondre au comportement égoïste au niveau MAC dans les réseaux ad-hoc sans fils. Il peut aussi aisément être introduit sans avoir besoin de modifier les autres équipements, assurant ainsi une rétrocompatibilité. Le fonctionnement n'est pas limité au mode ad-hoc et la compréhension de l'impact des paramètres permet de réaliser des choix pertinents face au contexte du jeu.

Cette adaptation de stratégies n'est pas nouvelle dans le domaine des télécommunications mais l'originalité de l'implémentation au niveau de la sous-couche MAC peut permettre d'ouvrir des perspectives intéressantes. Il serait possible de suivre ce principe pour adapter d'autres stratégies connues pour fonctionner dans des dilemmes du prisonnier répétés avec bruit à la sous-couche MAC. Une analyse et une comparaison de ces stratégies pourraient être effectuées pour tenter de démontrer si un meilleur choix existe ou pas. L'influence des paramètres naturels comme le niveau de bruit, le nombre de

nœuds ou la topologie sur les stratégies suivies par les nœuds pourrait être étudiée. Il sera également ingénieux d'étudier l'impact de la mobilité des nœuds. Ainsi le modèle pourrait être validé de manière plus rationnelle et moins empirique.

RÉFÉRENCES BIBLIOGRAPHIQUES

E. Altman et R. El Azouzi, et T. Jiménez, *"Slotted Aloha as a stochastic game with partial information"*. In Proc. of the International Symposium on Modeling and Optimization in Mobile Ad Hoc and Wireless Networks (WiOpt), pp.1–9, 2002.

Axelrod R et Dion D. "*The further evolution of cooperation*". Science 1988 ; 242(4884): pp.1385–1390.

G. Bianchi. "*Performance analysis of the IEEE 802.11 distributed coordinated function*". IEEE Journal of Selected Areas in Communications, vol. 18, no.3, pp. 535–547, 2000.

M. Cagalj, S. Ganeriwal, I. Aad et J.-P. Hubaux, "*On Selfish Behavior in CSMA/CA Networks*". In Proc. of the Annual IEEE International Conference on Computer Communications (IEEE INFOCOM), pp.1–12, 2005.

A.A. Cardenas, S. Radosavac et J.S. Baras, "*Evaluation of Detection Algorithms for MAC Layer Misbehavior: Theory and Experiments*". IEEE/ACM Transactions on Networking, vol 17, no.2, pp.605–617, 2009.

L. Chen et J. Leneutre, "*Selfishness, Not Always A Nightmare: Modeling Selfish MAC Behaviors in Wireless Mobile Ad Hoc Networks*". In Proc. International Conference on Distributed Computing Systems (ICDCS), pp.1–8, 2007.

J. Choi, D. Kim, J. Chiang, et Y. Hu. "*Partial Deafness: A Novel Denial-of-Service Attack in 802.11 Networks*". In Proc. of the Sixth International ICST Conference on Hetereneous Networking for Quality, Reliability, Security and Robustness (ICST QShine 2009), pp.1–18, 2009.

S. Desilva, et R. Boppana. "*On the Impact of Noise Sensitivity on Performance in 802.11 Based Ad -Hoc Networks*". In Proc. of the IEEE International Conference on Communication, pp.4372–4376, 2004.

IEEE Standard for Wireless LAN-Medium Access Control and Physical Layer Specification, P802.11, 1999.

J.J.Jaramillo et R. Srikant, "*A game theory based reputation mechanism to incentivize cooperation in wireless ad hoc networks*". Ad Hoc Networks, vol.8, no.4 pp.416–429, 2010.

Y. Jin et G. Kesidis, "*Equilibria of a noncooperative game for heterogeneous users of an ALOHA network*". IEEE Communication Letters, vol. 6, no. 7, pp.1–3, 2002.

C. E. Koksal, H. Kassab, et H. Balakrishnan, "*An analysis of short-term fairness in wireless media access protocols*" in Proceedings of the ACM Special Interest Group on Performance Evaluation (ACM SIGMETRICS), pp.1–2, 2000.

J. Konorski, "*Multiple Access in Ad Hoc Wireless LANs with Noncooperative Stations*" In Proc. Networking Conference, pp.1–6, 2002.

J. Konorski, "*A game-theoretic study of CSMA/CA under a backoff attack*" IEEE/ACM Transactions on Networking, vol. 14, No. 6, pp. 1167–1178, 2006.

P. Kyasanur et N. Vaidya. "*Selfish MAC Layer Misbehavior in Wireless Networks*". In *IEEE* Transactions on Mobile Computing, pp. 1–35, 2004.

T. Issariyakul et E. Hossain , "*Introduction to Network Simulator NS2*" Springer, ISBN: 978-0-387-71759-3, 2008.

A.B. MacKenzie et S. B. Wicher, "*Stability of Multipacket Slotted Aloha with Selfish Users and Perfect Information*". In Proc. of the Annual IEEE International Conference on Computer Communications (IEEE INFOCOM), pp. 1583–1590, 2003.

P. Molander, "*The optimal level generosity in a selfish, uncertain environment*". Journal of Conflict Resolution, vol. 29, no. 1, pp. 611–618, 1985.

T. Nandagopal, T.Kim, X. Gao, et V. Bharghavan, "*Achieving MAC Layer Fairness in Wireless Packet Networks*". In Proc. of the Annual International Conference on Mobile Computing and Networking (ACM/IEEE MobiCom), pp. 87–98, Août 2000.

J.V.Neumann et O. Morgenstern, "*Theory of Games and Economic Behaviour*". Princeton University Press, 1944.

K. J. Park, J. Choi, K. Kang, et Y. C.Hu, "*Malicious or selfish? Analysis of carrier sense misbehavior in IEEE 802.11 WLAN*". Quality of Service in Heterogeneous Networks, vol. 22, pp. 351–362, 2009.

G. Tan et J. Guttag, "The *802.11 MAC protocol leads to inefficient equilibria*". In Proc of the Annual IEEE International Conference on Computer Communications (IEEE INFOCOM), pp.1–11, 2005.

A. Lopez-Toledo et Wang X. "*A robust Kolmogorov-Smirnov detector for misbehavior in IEEE 802.11 DCF*". In Proc. of the IEEE International Conference on Communications (ICC'07), pp.1564–1569, 2007.

M. Raya, J.-P. Hubaux, et I. Aad, "*DOMINO: A System to Detect Greedy Behavior in IEEE 802.11 Hotspots*" In Proc. of the Annual International Conference on Mobile Systems, Applications, and Services (MobiSys), pp.1–14, 2004.

Wu, J., & Axelrod, R, "*How to cope with noise in the iterated prisoner's dilemma*". Journal of Conflict Resolution 39, pp. 183–189, 2007.