République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Mémoire de Magister

Présenté à l'Université de Guelma
Faculté des sciences et sciences de l'ingénierie

Département de : **Informatique**
Ecole **D**octorale **N**ationale **S**cience et **T**echnologie de l'**I**nformation et de la **C**onnaissance
Spécialité : **Informatique**
Option : **SIC**

Présenté par : **Mlle ZOHRA MAHFOUF**

Adaptation d'un Protocole Filaire aux Réseaux Sans Fils

JURY

Président	**Pr.**	**Hamid Seridi**	**Université de Guelma**
Rapporteur	**M.C.**	**Nacira Ghoualmi**	**Université de Annaba**
Examinateur	**M.C.**	**H. F. Merouani**	**Université de Annaba**
Examinateur	**M.C.**	**Yamina Tlili**	**Université de Annaba**

2010

REMERCIEMENTS

Je remercie vivement mon encadrant Mme **Nacira Ghoualmi** pour son aide , ses conseils , sa patience et son soutien.

Je remercie Monsieur **Hamid Seridi** Professeur à l'Université de Guelma et directeur de **E**cole **D**octorale **N**ationale **S**cience et **T**echnologie del'**I**nformation et de la **C**onnaissance-Pole Est(Guelma), de m'y avoir donné l'occasion de mener à bien mes études et d'avoir accepté d'être le président des jurés des travaux présentés

Je remercie Monsieur **Ali Balador** de l'université Islamic Azad -Iran et Monsieur **Nauman Aslam** de Dalhousie University pour leurs collaborations et leurs précieux conseils qui m'ont permis de finir le chapitre d'évaluation.

Je suis reconnaissante à Madame **H. F. Merouani** , Maitre de conférence à l'université de Annaba et Madame **Yamina Tlili** Maitre de conférence à l'université de Annaba d'avoir accepté d'être les jurés des travaux présentés, je les remercie pour le temps qu'ils ont consacrés à cette tâche, l'intérêt qu'ils ont porté à mon travail, les remarques enrichissantes qu'ils ont formulées ainsi que d'avoir accepté de juger mon travail en participant au jury.

Je tiens aussi à adresser ma gratitude à toutes les personnes qui m'ont aidé pendant la préparation de ce mémoire, je pense notamment à **Mlle Sahraoui Sabrina** de l'université de Skikda et Mlle **Guefrouchi Ryma** de l'université de Constantine.
Je tiens à remercier profondément l'ensemble de mes collègues de l'école doctorale (**Souad, Sihem, Salima,…**) avec lesquels j'ai eu des échanges scientifiques, culturels ou autres pendant toute la durée de l'année théorique.

Merci à Monsieur **Garnine Zoubir** pour sa coordination et ses services et à tout le personnel de la faculté des sciences de l'ingénieur et du département d'Informatique de l'université de Guelma.

Je tiens également à remercier chaleureusement ma famille : **mon père**, **mes frères et mes sœurs** pour leur soutien moral.

Enfin, je ne saurais terminer cette liste, sans adresser un remerciement particulier et exprimer toute mon affection à **Ma mère** qui m'a apporté son soutien tout au long de ce travail et qui a toujours cru que je suis capable de le finir.

A M A M A,

T oute ma F amille,

T outes mes A mies,

et à toutes personnes qui m'a un jour enseigné, aidé à comprendre ou apprendre.

الملخص

لقد ادت التطورات التكنولوجية الحديثة الى توفر الشرائح الاكثرسرعة والأقل حجما و كلفة مما ساعد على الانتشار الواسع لشبكات الاتصال اللاسلكية.أن الهدف الأساسي لشبكات الاتصال اللسلكية المخصصة (ad hoc)هو امكانية تشكيل و المحافظة على الاتصال داخل الشبكة دون الحاجة الى بنى تحتية او وحدات مراقبة مركزية .يلعب هذا النوع من الشبكات دورا فاعلا في الحالات الطارئة مثل التدخلات والاسعافات اثناء الكوارث الطبيعية حيث لا وجود للبنى التحتية كما أن لها استخدامات واسعة في المجال العسكري و الصناعي,

يعتبر الحصول على حق الارسال للمشاركين في الشبكة و تنظيم وصول المستخدمين الى قناة الاتصال (MAC) من وضائف الطبقة الثانيةحسب النموذج المرجعي (OSI) ونضرا للخصائص المميزة لهذه الشبكات يجب على بروتوكولات هذه الطبقة توفير اليات أكبر من الشبكات اللاخطية العادية للتمكن من حل المشاكل الخاصة بها مثل(العقدة الخفية و استهلك الطاقة) ويعتبر تنظيم وصول المستخدمين الى قناة الاتصال من أهم التحديات في هذا النوع من الشبكات وهذا لغياب وحدات المراقبة المركزية.

بعد عرض خصائص الشبكات اللاسلكية الموجهة،وضعنا لمحة عن البروتوكولات الموجودة في هذا المجال ثم اقترحنا بروتوكولا جديدا يأخذ بعين الاعتبار المتطلبات الخاصة بنوعية الخدمات المطلوبة كما يحل مشكلة المستخدم الخفي عبر خمس مراحل تبدا بتقسيم الشبكةالى قطاعات ثم اختير المعطيات الأنسب داخل كل عقدة و تبادلها بين كل الستخدمين داخل القطاع من أجل اختيار افضل مستحدم للمرحلة القادمة وأخيرا ارسال معلومات المستخدم المختار .

DCC-MAC (Distributed Clustering and Communication MAC protocol)

Many technological factors, such as cheaper hardware, smaller transceivers, and faster processors, are fueling the increased interest in wireless ad hoc networks. The main goal of wireless ad hoc networks is to allow a group of communication nodes to set up and maintain a network among themselves, without the support of a base station or a central controller. From the applications perspective, wireless ad hoc networks are useful for situations that require quick or infrastructureless local network deployment, such as crisis response, conference meetings, sensor networks, military applications, and possibly home and office networks. Ad hoc networks could, for instance, empower medical personnel and civil servants to better coordinate their efforts during large-scale emergencies that bring infrastructure networks down, such as flood, earthquake...

In the OSI reference model, medium access is a function of the layer 2 sub-layer called the Medium Access Control (MAC) layer. MAC protocols for wireless networks must address the hidden node problem and must exercise power control. Accessing the wireless medium thus requires a more elaborate mechanism than what is required by wired networks to regulate user access to the channel. Ad hoc wireless networks present even greater challenges than infrastructure wireless networks at the MAC layer. The absence of a centralized controller creates the need for distributed management protocols at the MAC layer, and possibly at higher layers of the network stack.

In this thesis we present specific issue of ad hoc wireless networks than we conduct a study of some existing MAC protocols for wireless ad hoc networks, We than propose a novel distributed MAC protocol with quality of service support for a cluster based topology. Our protocol enclose five phases, clustering (using our loosely centralised Algorithm to avoid exposed and hidden node problems), intra-node traffic category election using service differentiation mechanism, candidature phase to exchange nodes need, inter-nodes distributed selection of the current high priority node and finally data transmission of the designed node

***Keywords**: Ad hoc networks; Wireless networks; MAC; Medium Access Control; Quality of Service (QoS);clustering, diffserv, 802.11e.*

Proposition D'un Protocole MAC distribué Basé Clusters avec Différenciation De Services

Plusieurs facteurs technologiques tels que la disponibilité des processeurs à grand vitesse de traitement et de petit taille avec la diminution des prix de matériel informatique en générale, ont accrut l'intérêt des réseaux sans fil .l'objectif principal des réseaux ad hoc sans fil est de permettre à un groupe de nœuds d'installer et de maintenir un réseau entre eux sans avoir besoins aux infrastructures ou à des stations de base. Ils sont utiles pour les situations qui exigent le déploiement rapide ou infrastructureless d'un réseau local, tel que la réponse aux crises (inondation, tremblement de terre...), les réunions dans les conférences, les réseaux de sonde (sensor), les applications militaires, ainsi que les réseaux domestiques et industriels.

Selon le modèle de référence OSI, le contrôle d'accès au medium (MAC) est une fonction de la couche liaison des données. Les protocoles MAC des réseaux sans fil doivent résoudre plusieurs problèmes spécifiques comme celui du nœud caché et de consommation d'énergie. L'accès au medium sans fil exige ainsi des mécanismes plus sophistiqué que ceux nécessaires aux réseaux filaires ; et en ajoutant L'absence d'un contrôleur centralisé pour le mode ad hoc, la proposition des protocoles distribués de gestion d'accès au medium (MAC) deviennent un axe très important dans les recherches de ce domaine.

Dans ce mémoire nous présentant les contrainte spécifiques des réseaux ad hoc et on présente quelques protocole MAC déjà existant dans la littérature pour le mode ad hoc pour proposer un nouveaux protocole distribué basé cluster avec support de qualité de service, notre protocole comporte cinq phases : clustering (avec un algorithme distribué pour résoudre le problème du nœud caché),Choix intra-nœud de la catégorie d'accès prioritaire, Candidature(transmission en robin round des besoins des nœuds), Choix inter-nœud du nœud prioritaire du cluster et finalement transmission des données du nœud élu-

Mots-clés : Ad hoc networks; Wireless networks; MAC; Medium Access Control; Quality of Service (QoS);clustering

Table des matières

Chapitre1
Introduction générale

Sommaire

1.1 Contexte général

Depuis que la téléphonie mobile s'est imposée dans notre vie quotidienne et que les réseaux locaux sans fil ont connu un grand succès, de nouveaux horizons vers des applications utilisant ces technologies sans fil sont apparues. Bien qu'initialement prévus pour des services sans aucune garantie, les réseaux mobiles actuels ont tendance à acheminer des flux de toutes sortes d'applications : FTP, mail, téléphonie, visiophonie, web, etc.. Ainsi, poussée par plusieurs facteurs économiques, la mobilité est devenue de plus en plus un élément fédérateur des réseaux de communication.

A l'origine, ce sont les militaires qui se sont intéressés les premiers aux réseaux de communication sans fil fonctionnant de proche en proche tout en restant fonctionnels en cas de mobilité ou de perte d'éléments de routage. Tout a commencé au début des années 70, lorsque les techniques de commutation de paquets ont poussé l'Agence des Projets de Recherche du Département de la Défense américaine **DARPA** (*Defense Advanced Research Projects Agency*) à développer une nouvelle génération de réseaux appelée PRNet (*Packet Radio Network*) [14]. A l'époque, cette nouvelle génération de réseaux disposait déjà d'une architecture distribuée, permettant un partage dynamique du canal de diffusion par une combinaison des protocoles **CSMA** et **Aloha**. Cependant, en milieu des années 80, la DARPA a développé une nouvelle génération de réseaux appelée **SURAN** (*Survivable Radio Networks*) [21], dont l'objectif était d'éviter certaines lacunes du projet PRNet et de permettre entre autre, le passage vers des réseaux comportant jusqu'à une dizaine de milliers de nœuds mobiles supportant des protocoles évolués, avec des mécanismes radio simples, où la consommation d'énergie et le coût restent faibles. En revanche, ce projet est resté exclusivement militaire, jusqu'à son passage vers la fin des années 90 pour être utilisé par des applications civiles, où des recherches ont permis d'étudier la possibilité de passer vers des réseaux mobiles totalement dynamiques et spontanés. Ceci a donné naissance aux réseaux mobiles ad hoc. Ces recherches sur les réseaux ad hoc dans le domaine civil ont en fait, pris leur essor avec l'arrivée des premières technologies radio, principalement la norme IEEE 802.11 et ses différentes dérivées. Cette norme a été standardisée en 1999 par l'IEEE (*Institute of Electrical and Electronics Engineers*), dans le but d'assurer la communication entre ordinateurs utilisant le médium radio. Cependant les contraintes et les problèmes imposés par ce type de réseau restent nombreux et substantiellement différents de ceux des réseaux filaires (absence d'infrastructure fixe, changements fréquents de la topologie, manque de fiabilité des liens radio, etc..).

L'objectif des réseaux ad hoc est d'offrir aux utilisateurs un accès transparent à l'information indépendamment de la position géographique de chaque utilisateur. Un autre objectif est de permettre d'atteindre des débits compatibles avec le transfert de flux multimédia, soumis à de fortes contraintes. Cependant, l'aspect distribué et l'utilisation d'interfaces de communication radio partagées imposent un certain nombre de problèmes, notamment en ce qui concerne les services offerts aux différentes applications. En effet, obtenir une qualité équivalente à celle fournie par des réseaux filaires s'avère une tâche difficile. De nombreuses contraintes doivent être vaincues afin de tirer les bénéfices d'un réseau ad hoc : l'accès au canal radio, la gestion de la mobilité, la gestion de l'énergie, la sécurité et les solutions pour la qualité de service (QdS ou QoS) comme le délai, la bande passante et le taux de pertes de paquets.

La littérature s'accorde à dire que les problèmes rendant tous les standard (Hiperlan [3] [5], Bluetooth [34], Zigbee [34], Wimax [7], et 802.11 [13] ; pour ne pas citer que quelques un)sous optimal proviennent de la sous-couche MAC implémenté. Ces problèmes sont indépendants de la couche physique utilisée. La couche MAC, comme si suggérée dans le modèle OSI [31], a un rôle principale : fournir une transmission fiable entre deux stations du réseau. La couche MAC doit fournir une correction ou une détection d'erreurs pouvant apparaitre, au niveau de la couche physique. De plus la couche MAC est aussi responsable de la résolution de conflit pouvant survenir quand différentes station tentent d'accéder au medium de communication en même temps. C'est donc le rôle de la couche MAC de résoudre les problèmes liés à la mobilité, l'asymétrie des liens, etc.

Les solutions issues de la littérature peuvent être classifiées dans deux grandes catégories ; la première catégorie contient les solutions résolvant le problème de fiabilité en empêchant certaines stations d'émettre. Cette première catégorie de solution revient à offrir à un sous ensemble de station un accès fiable quasi permanant au medium radio. ce sous ensemble de station est choisi de telle sorte que les transmissions de ces stations ne provoquent aucune collision entre elles. La seconde catégorie propose d'offrir un accès à toutes les stations en mettant en place un accès plus au moins complexe permettant une transmission sans collision à toute les stations avec un ordonnancement.

Selon nous les catégories d'accès proposés dans la littérature se classe soit dans une catégorie soit dans l'autre, l'objectif principale de ce mémoire est de proposer un protocole MAC qui essaye de profiter des avantages des deux catégories citées ci-dessus en implémentant un mécanisme de

différentiation de service intra-nœud et une garantie d'accès à l'aide du polling distribué inter-nœud.

1.2 Organisation du document

Ce mémoire s'organise autour de six chapitres. Le premier constitue une introduction générale qui présente le contexte général. Le deuxième chapitre donne un état de l'art des réseaux locaux sans fil et des différents concepts liés à ce type de réseaux, ainsi qu'une description de la notion de qualité de service et de clustering. Dans le troisième chapitre, nous introduisons les standard 802.11 avant de détailler la version 802.11e et focaliser sur le mécanisme d'implémentation de qualité de service dans cette dernière

Dans le quatrième chapitre, nous présentons notre proposition (Protocole DCC-MAC) avec les détailles de ses quatre phases, avant de passer à la simulation présentée dans le chapitre cinq avec l'analyse et l'explication des résultats. Enfin, le sixième chapitre conclut ce mémoire.

Chapitre 2
Des réseaux sans fil aux réseaux ad hoc

Sommaire

2.1 Les réseaux locaux sans fil

2.1.1 Introduction

Les réseaux sans fil (Wireless Networks) constituent de plus en plus une technologie émergente permettant à ses utilisateurs un accès à l'information et aux services électroniques indépendamment de leurs positions géographiques. Le succès de ce type de réseaux ces dernières années est suscité par un grand intérêt de la part des particuliers, des entreprises et du milieu industriel. En effet, ce type de réseaux est perçu comme une nouvelle alternative complémentaire aux réseaux filaires traditionnels, car ils sont autant utilisés dans le cadre des réseaux locaux d'entreprise pour une utilisation purement professionnelle, que dans le cadre des réseaux locaux personnels à domicile.

Aujourd'hui les débits atteints avec les réseaux sans fil rendent possible le transfert de flux multimédia soumis à de fortes contraintes. Le respect de certaines contraintes telles que : la bande passante, le délai ou encore le taux de pertes de paquets devient primordial. Cependant les solutions qui ont été introduites dans le monde des réseaux filaires deviennent inadaptées pour des réseaux dont l'administration n'est pas centralisée et qui utilisent un médium radio partagé.
Dans le cadre des réseaux sans fil, le standard IEEE 802.11 [11] définit deux modes de fonctionnement différents : **le mode infrastructure**, où les clients sont connectés à un point d'accès et **le mode sans infrastructure** ou **Ad hoc** ; où les clients sont connectés les uns aux autres d'une façon spontanée.

2.1.2 Généralités

Un réseau sans fil peut être considéré comme un système de transmission de données, dont le but est d'assurer une liaison indépendante de l'emplacement des entités informatiques qui composent le réseau. Plutôt que d'utiliser une infrastructure câblée, dans un réseau sans fil, l'ensemble des nœuds communiquent via des interfaces radios sous forme de cartes réseaux PCI, PCMCIA, etc.. Ces cartes sans fil peuvent se connecter directement aux machines des utilisateurs et interagir avec toute la pile de protocoles de communication.

D'un autre côté, les réseaux locaux sans fil sont généralement utilisés pour faire le lien final entre le réseau câblé existant et des machines clientes, offrant aux utilisateurs un accès sans fil à l'ensemble des ressources et des services offerts par le réseau de l'entreprise, sur un ou plusieurs bâtiments. Pour cela, ce type de réseaux est en passe de devenir l'une des principales solutions de connexion pour de nombreuses entreprises. Ainsi, le marché du sans fil s'est développé rapidement dès lors que les entreprises constatent les gains de productivité qui découlent de la disparition des câbles. Selon le cabinet américain **Frost and Sullivan** (spécialisé dans le domaine de la croissance mondiale), le marché des abonnements à des réseaux sans fil est évalué à plus d'un milliard d'euros en 2006. Tandis qu'il n'était que de 18 millions d'euros en 2002.

Du point de vu technique et pour mieux comprendre le fonctionnement des réseaux sans fil, nous allons essayer de donner plus de détails sur les modes de fonctionnement des couches physique et MAC, par lesquelles se distingue ce type de réseaux.

2.1.3 Couche physique

La couche physique représentée par la figure 2.1 définit en général, les aspects électriques, mécaniques et fonctionnels de l'accès au canal de communication, ainsi que les protocoles d'échange de données via le réseau. Elle assure entre autres, les relations entre les couches supérieures et le matériel. Le service rendu par la couche physique est défini par la norme ISO ou la recommandation X211 du **CCITT** (Comité Consultatif International Téléphonique et Télégraphique) [21].

1. Infrarouge

Le mode de communication par infrarouge est simple, peu réglementé et peu coûteux. En utilisant un faisceau de lumière, ce mode est basé sur l'utilisation des mêmes fréquences que celles utilisées sur les fibres optiques. Malgré que la lumière infrarouge possède une large bande passante offrant par conséquent des débits relativement importants, la portée de ce type de communications reste faible. En revanche, les infrarouges peuvent pénétrer à travers le verre, mais pas à travers des obstacles opaques, ce qui représente un avantage en terme de sécurité. Mais, comme les réseaux infrarouges sont sensibles aux interférences lumineuses, la coupure du faisceau lumineux implique l'interruption de la transmission.

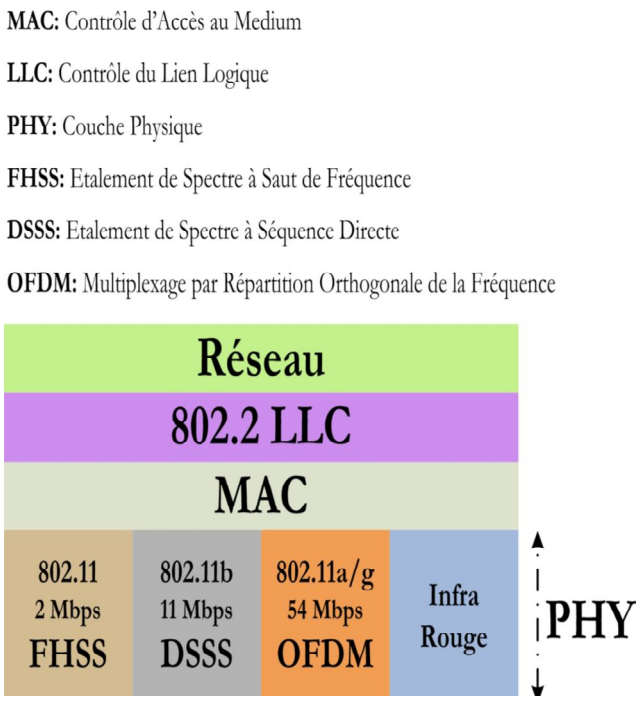


Fig. 2.1 – La couche PHYSIQUE dans les réseaux sans fil

Il existe dans la pratique quatre types de réseaux infrarouges :

– Les réseaux à visibilité directe.

– Les réseaux infrarouges à diffusion.

– Les réseaux réflecteurs.

– Les réseaux à liaison optique à large bande.

2. OFDM(*Orthogonal Frequency Division Multiplexing*) **:** Multiplexage par Répartition Orthogonale de la Fréquence

L'OFDM est une technique née dans les années 50 - 60. Cependant, dans les années 80, on a commencé à prendre conscience de l'intérêt que représentent l'OFDM et ses applications. Cette technologie représente une technique de modulation numérique des signaux, utilisée entre autres pour les systèmes de transmissions mobiles à haut débit de données. Elle consiste à répartir le signal sur un grand nombre de sous-porteuses orthogonales modulées individuellement à bas débit.

L'OFDM est particulièrement bien adapté aux réseaux locaux ou métropolitains mais perd de son intérêt sur des réseaux à grandes échelles. Car, cette technique élimine les phénomènes de bruits ponctuels ou d'évanouissements temporaires du signal sans recourir à des techniques complexes. En revanche, cette technologie apparaît moins efficace lorsque les perturbations s'amplifient, car il faut mettre en place des méthodes de filtrages ou de codages qui réduisent de manière significative les débits. Actuellement l'OFDM est utilisé dans plusieurs applications telles que les satellites, l'ADSL ou le câble pour la diffusion des données, du son ou de l'image. Mais, de plus en plus, cette technologie s'oriente vers les systèmes de communications sans fil. Ainsi, des normes telles que 802.11a et 802.11g peuvent offrir des débits théoriques jusqu'à 54 Mbps, là où la norme 802.11b qui n'est pas OFDM, se limite à 11 Mbps.

3. DSSS *(Direct Sequence Spread Spectrum)***:** Étalement de Spectre à Séquence Directe

Le DSSS est une couche physique utilisant une technique radio. C'est une technologie de transmission par spectre étalé, où la porteuse est successivement modulée par l'information et par un code pseudo aléatoire de débit beaucoup plus important. Le signal résultant occupe donc une bande très importante. Dans cette technique, la bande des 2.4 GHz est divisée (comme le montre la figure 2.2) en 14 sous-canaux de 22MHz qui fournissent un signal très bruité, car les canaux adjacents (en cas d'utilisation de deux plages dans la même zone géographique) se recouvrent partiellement et peuvent donc se perturber mutuellement (seuls trois sous-canaux sur les 14 étant entièrement isolés).

Cette technique offre des débits de transmission allant de 5.5 à 11 Mbps. Avec comme avantages :

– Une densité spectrale faible du signal transmis, car ce dernier est large bande,

– Une sécurité assurée, tant que le code d'étalement reste secret,

– Une tolérance obtenue vis à vis du multi-trajet en choisissant des codes avec des facteurs d'auto-corrélation faibles.

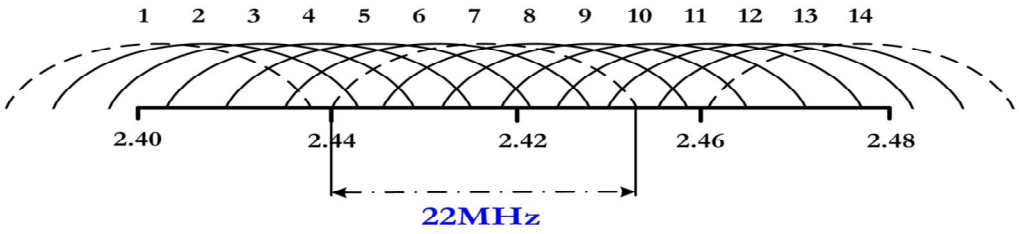


Fig. 2.2 – Le Direct Sequence Spread Spectrum (DSSS)

4. FHSS (Frequency-hopping spread spectrum): Étalement de Spectre avec Saut de Fréquence

La technologie FHSS utilisée dans les réseaux 802.11b et d'autres technologies sans fil, a été créée et brevetée en 1942. En utilisant la transmission sur des canaux changeant en permanence de fréquence de manière pseudo-aléatoire, cette technologie utilise la technique de saut de fréquence. Son principe est de diviser la bande passante en 79 sous-canaux, de 1 MHz de largeur de bande offrant chacun, un débit allant de 1 à 2 Mbps avec un codage binaire.L'émetteur et le récepteur s'accordent sur une séquence de sauts de fréquence porteuse et les données sont envoyées successivement sur les différents sous canaux en évitant (de manière temporaire) d'utiliser les sous-canaux fortement perturbés. Chaque communication sur le réseau s'effectue suivant un schéma de saut différent et cela de façon à minimiser le risque que deux émissions utilisent le même sous-canal.

La technologie FHSS est plus simple à mettre en œuvre, car l'utilisation d'un simple microcontrôleur suffit à la gestion des fonctions de sauts de fréquences pour la conception des systèmes en FHSS. En effet, cette technique coûte moins chère que des systèmes utilisant la technologie DSSS qui nécessite l'utilisation de circuits **LSI** (*Large-Scale Integration*) pour la conception des algorithmes de codages. De plus elle offre une meilleure portée due à une plus grande sensibilité de l'étage de réception, ainsi qu'une bonne réjection des interférences. Les modules développés en FHSS peuvent

être considérés comme des récepteurs à bande étroite changeant continuellement de fréquences et disposant d'un très bon niveau de réjection vis-à-vis des signaux d'interférences.

2.1.4 Couche de liaison de données

La couche de liaison de données est la couche se trouvant au dessus de la couche physique dans le modèle de référence OSI. Elle a pour objectif de réaliser l'acheminement sans erreur de blocs d'informations sur la liaison physique c'est à dire sur le circuit de données reliant deux commutateurs adjacents. Afin d'effectuer une transmission correcte, la couche de liaison de données attache des en-têtes et des caractères aux paquets de données à transmettre. Dans ce cas, les messages échangés sont appelés trames MAC ou **MPDU** (*MAC Protocol Data Unit*). Ceux ci seront encapsulés par la suite dans des trames de niveau physique appelées **PLCP-PDU** (*Physical Level Control Protocol-PDU*).

La couche de liaison de données comprend essentiellement deux sous-couches :

– la sous-couche LLC (*Logical Link Control*)

La sous-couche LLC (spécification IEEE 802.2), qui est indépendante des mécanismes d'accès au support physique, représente une partie de la couche de liaison de données. Elle présente les caractéristiques de fiabilité grâce au séquencement et à la retransmission des données en cas de détection d'erreurs.

– la sous-couche MAC (*Medium Access Control*)

La sous-couche MAC, qui permet entre autres à un hôte de communiquer avec plusieurs périphériques en même temps, représente une deuxième partie de la couche de liaison de données. En effet, la sous-couche MAC est nécessaire pour gérer les accès au canal de communication car, l'un des problèmes majeurs des réseaux LAN consiste à savoir qui a le droit d'émettre à un moment donné. Ainsi des protocoles ont été proposés afin de résoudre ces problèmes d'accès. Ces protocoles qui visent à déterminer qui est le prochain hôte qui sera autorisé à envoyer des données sur le réseau, sont définis au niveau de la sous-couche MAC qui s'occupe de la gestion du contrôle d'accès au canal. La sous-couche MAC définit un ensemble de techniques d'accès au canal permettant à un ensemble d'utilisateurs de

partager les ressources réseaux. Dans la suite nous allons présenter un échantillon de ces techniques dans le cadre des réseaux sans fil.

1. FDMA (*Frequency Division Multiple Access*) : Accès Multiple par Répartition en Fréquence

Cette technique qui était la seule utilisée lorsque le téléphone était totalement analogique, est la plus ancienne. L'idée est de diviser le spectre en canaux et d'affecter à chaque interlocuteur ou chaque message (un à la fois), un canal fréquentiel [21]. Cette affectation est alors basée sur le principe du premier arrivé, premier servi ou **FIFO** (*First In First Out*).

En pratique, le message utilisé sert à moduler une fréquence porteuse (à l'origine en amplitude, parfois avec suppression de porteuse) et les différentes porteuses ainsi modulées sont juxtaposées. Du côté du récepteur, des filtres sélectifs isolent les différentes porteuses démodulées et si les fréquences porteuses sont parfaitement connues ou restituées, une démodulation cohérente (synchrone) est effectuée.

2. TDMA (*Time Division Multiple Access*): Accès Multiple par Répartition dans le Temps

Dans cette technique, les canaux sont multiplexés sous la forme d'intervalles de temps de telle façon que chaque correspondant ou chaque message occupe la totalité de la bande mais pendant un temps très court (accès à toute la bande passante allouée pour le système de transmission) [21]. Avec le TDMA, les échantillons issus d'un message sont intercalés avec ceux des autres. Ainsi, le tri de ses échantillons se fait du côté du récepteur.

Le fait que le TDMA présente une gestion complexe, il faut ajouter des bits de signalisation et de synchronisation, mais cette technique offre un coût réduit pour la station de base, ainsi qu'une souplesse de modification sur les débits transmis.

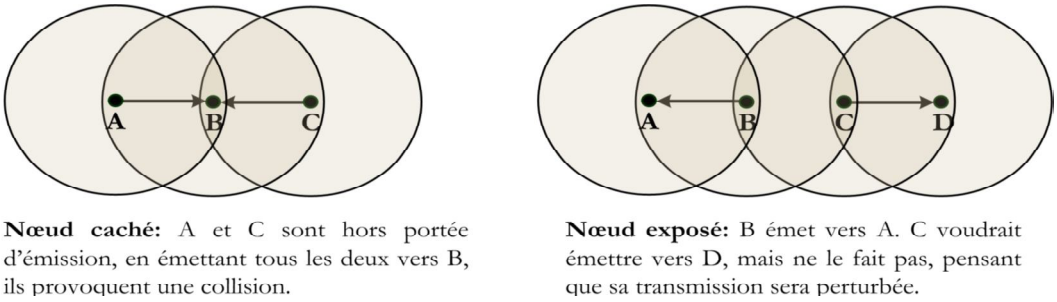
3. CDMA (*Code division multiple access*): Accès Multiple par Répartition en Code

Ici tous les utilisateurs accèdent simultanément à la totalité de la bande, ils sont distingués à la réception grâce à des codes pseudo-aléatoires personnels. Ce qui permet d'avoir une bonne immunité au bruit et la possibilité d'utiliser la diversité de fréquences, ainsi que le cryptage. La technique CDMA [21] utilise des modulations à étalement de spectre qui peuvent être réalisées par saut de fréquence ou par séquence directe. En

effet, le CDMA est très souple au niveau des débits transmis, mais relativement complexe car elle peut nécessiter une égalisation à la réception et un contrôle de la puissance d'émission.

4. CSMA/CA *(Carrier Sense Multiple Access with Collision Avoidance)*: Accès Multiple avec Écoute de Porteuses/Évitement de Collisions

Le CSMA/CA [22] est une technique d'accès au médium utilisée dans les réseaux sans fil IEEE 802.11. Elle permet de traiter les problèmes des stations cachées et des stations exposées illustrés par la figure 2.3 et d'éviter les collisions en utilisant le principe appelé évitement de collisions (*Collision Avoidance*).



Nœud caché: A et C sont hors portée d'émission, en émettant tous les deux vers B, ils provoquent une collision.

Nœud exposé: B émet vers A. C voudrait émettre vers D, mais ne le fait pas, pensant que sa transmission sera perturbée.

Fig. 2.3 – Le problème du nœud caché et du nœud exposé

Dans cette technique (figure 2.4), chaque nœud (souhaitant émettre des données) doit écouter le canal avant de tenter d'obtenir l'accès. Si le canal est libre le nœud envoie ses paquets. Sinon (si le canal est occupé) le nœud doit attendre la fin de la transmission en cours pour avoir le droit d'accès au médium. Pour cela, le nœud choisi un temps de temporisation (ou backoff) et lorsque la temporisation expire, si le canal est inoccupé, il peut commencer l'envoi de ses paquets. Dans le cas de plusieurs nœuds qui veulent accéder au canal, celui qui a choisi la temporisation la plus courte est donc celui qui gagne le droit d'accès et les autres doivent attendre simplement la fin de la transmission pour avoir le droit de tenter à nouveau l'accès au médium. Ce mécanisme garantie une équitabilité en terme d'accès au médium puisque la temporisation est aléatoire et effectuée pour chaque paquet. Cependant le CSMA/CA est dit sans connexion et offre un service de type best effort. De plus, il est impossible qu'un nœud écoute et transmet en même temps. Car, même si un nœud pouvait écouter le lien pendant qu'il est en train d'émettre, la puissance de son signal masquerait les autres signaux.

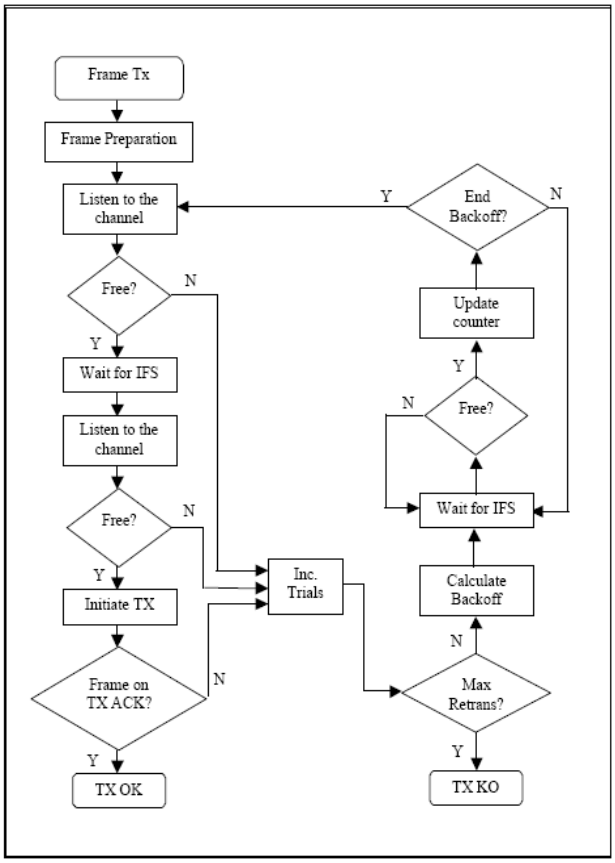


Fig. 2.4 – Diagramme de flux pour CSMA/CA

En terme de modes d'accès au médium, la norme IEEE 802.11 définit deux schémas différents :

– Dans le premier schéma, le nœud vérifie si le médium est libre en écoutant la porteuse. Si un autre nœud est déjà en train d'émettre, l'émetteur attend que le médium soit libre, avant d'attendre un temps aléatoire et essayer d'émettre à nouveau. Si aucun autre nœud n'est en train d'émettre, il peut commencer à émettre ses données. En revanche, lors de la transmission, chaque paquet doit être acquitté et si aucun acquittement n'est reçu, le paquet en question doit être retransmis.

– Dans le deuxième schéma, un nœud vérifie si le médium est libre. Si le médium est occupé, l'émetteur attend qu'il se libère, puis attend un temps aléatoire avant d'émettre. Si personne n'est en train d'émettre, le nœud envoie un message de type **RTS** (*Request To Send*) contenant l'adresse de destination et la durée de la transmission pour demander la parole (figure 2.5). Les autres nœuds savent donc que le médium sera occupé pendant

cette durée. Le destinataire répond avec un message de type **CTS** (*Clear To Send*) qui indique qu'il est prêt à recevoir les données sans aucun risque de collision. Chaque paquet doit être acquitté et si aucun acquittement n'est reçu, le paquet est retransmis.

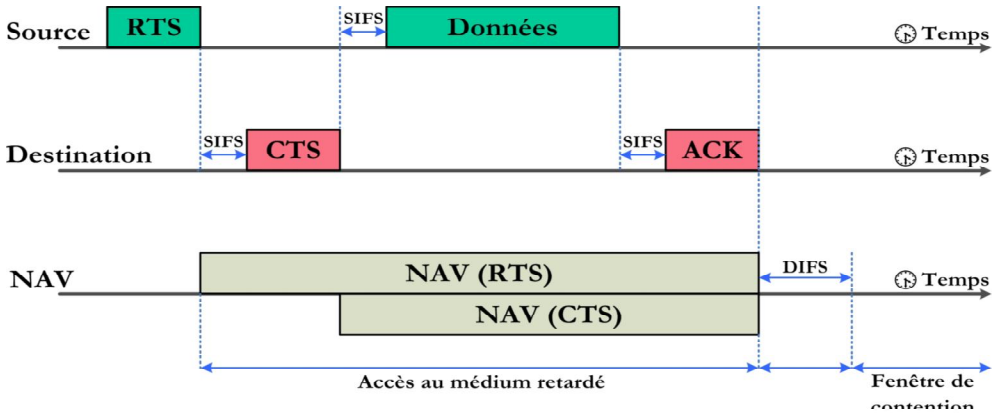


Fig. 2.5 – Le mécanisme RTS/CTS

Une autre fonction important appelée écoute de la porteuse virtuelle est fournie par le vecteur **NAV** (*Network Allocation Vector*). Le NAV représente une minuterie indiquant la durée pendant laquelle le médium sera réservé. Chaque nœud fixe le NAV à sa durée d'utilisation du médium, en incluant les trames nécessaires à la terminaison de l'opération en cours [11].

2.3 Réseaux Ad hoc

2.3.1 Définition et objectifs

Les réseaux ad hoc sont des réseaux qui ont attiré l'attention des chercheurs depuis les années 1970. Mais une définition claire pour ce type de réseaux était une tâche pour le moins difficile. Cependant, l'**IETF** (*Internet Engineering Task Force*), qui représente l'organisme responsable de l'élaboration de standards pour Internet, définit les réseaux ad hoc de la manière suivante :

" Un réseau ad hoc est un système autonome de plates-formes mobiles (par exemple un routeur interconnectant différents hôtes et équipements sans fil) appelées nœuds qui sont libres de se déplacer aléatoirement et sans contrainte. Ceci provoque des changements rapides et imprédictibles de la topologie du réseau. Ce système peut fonctionner d'une

manière isolée ou s'interfacer à des réseaux fixes au travers de passerelles. Dans ce dernier cas, un réseau ad hoc est un réseau d'extrémité"

Un réseau ad hoc se distingue par une absence totale de toute administration centralisée ou d'infrastructure fixe. Il peut être créé par l'association temporaire de nœuds mobiles communicants connectés via des liens radio (figure 2.6), où les tables de routage entre ces nœuds sont déterminées par des graphes multi-saut.

Les réseaux ad hoc sont utilisés en général dans plusieurs domaines d'applications : tels que les communications, les applications militaires, les situations d'urgence, le travail collaboratif, l'informatique embarquée et les réseaux de capteurs.

A partir de cette définition des réseaux ad hoc, il est important de mettre en avant les différentes contraintes imposées par ce type de réseaux et qui permettent de les distinguer des réseaux classiques.

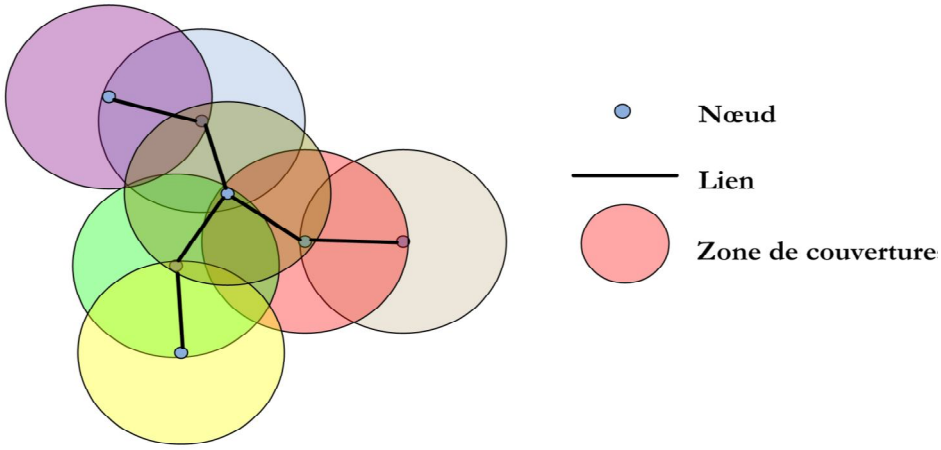


Fig. 2.7 – Exemple de réseau Ad Hoc

2.3.2 Contraintes spécifiques aux réseaux ad hoc

L'évolution des technologies de communication sans fil a poussé au développement de protocoles permettant un accès efficace à l'information et ceci, sans contraintes temporelles ni spatiales. Ainsi, un réseau ad hoc essaie d'étendre les notions de la mobilité à toutes les composantes de l'environnement. Ce type de réseaux est caractérisé par sa topologie, qui peut évoluer avec le temps et cela en fonction du déplacement des nœuds, de la puissance d'émission et des caractéristiques du médium radio. Cependant, ce type de réseaux impose un certain nombre de contraintes qui

doivent être prises en compte, surtout lorsqu'il est question de faire le transfert de flux multimédia ou de communiquer en mode temps réel. Parmi ces contraintes, nous pouvons citer :

1. Une topologie dynamique, qui évolue très rapidement, d'où la nécessité de mécanismes de routage qui s'adaptent avec la connectivité des nœuds à un instant donné.

2. Le seul moyen de communication entre les nœuds mobiles au sein d'un réseau ad hoc est l'utilisation d'un canal radio. En effet, les liaisons sont à débits variables et la bande passante est limitée.

3. Une autonomie réduite en terme d'énergie vu que les nœuds fonctionnent avec des batteries. Chaque nœud joue le rôle d'un routeur et utilise par conséquent sa propre énergie pour acheminer des paquets destinés à d'autres nœuds du réseau. Sachant qu'une partie de cette énergie est déjà consommée par le mécanisme de routage, ceci limite les services et les applications supportés par chaque nœud mobile.

4. Les liens radios ne sont pas isolés et le nombre de canaux disponibles est limité. Par conséquent, les interférences augmentent le nombre d'erreurs sur la transmission. De plus, à cause du partage de l'interface radio, chaque donnée est réceptionnée par tous les nœuds avec des puissances variables. Il faut ajouter également, que des interférences ou des changements persistants dans l'environnement conduisent à une grande versatilité des liens qui peuvent apparaître ou être coupés de manière durable et à tout moment.

5. La puissance du signal qui, non seulement, est atténuée rapidement avec la distance, mais est soumise à des réglementations très strictes, ceci empêche un émetteur de dépasser une certaine puissance lors de l'émission.

6. Une sécurité physique limitée est justifiée par le fait que le canal de communication radio est relativement vulnérable et peut être une cible facile pour espionner de manière passive.

7. De nombreuses applications multimédia ou temps réel ont besoin de certaines garanties relatives liées par exemple au débit, au délai ou encore à la gigue.

Dans un réseau ad hoc, il est très difficile d'obtenir ces garanties. Ceci est dû d'une part à la nature du canal radio (interférences et taux d'erreurs élevés) et d'une autre part au fait que des liens entre les nœuds mobiles partagent les ressources disponibles. De ce fait, les protocoles de qualité de service habituels ne sont pas utilisables directement dans le monde des réseaux ad hoc et des solutions spécifiques doivent être proposées [30].

2.4 Notion de qualité de service

Le terme **QoS** (acronyme de « Quality of Service », en français « Qualité de Service ») désigne la capacité à fournir un service (notamment un support de communication) conforme à des exigences en matière de temps de réponse et de bande passante. Appliquée aux réseaux à commutation de paquets (réseaux basés sur l'utilisation de routeurs) la QoS désigne l'aptitude à pouvoir garantir un niveau acceptable de perte de paquets, défini contractuellement, pour un usage donné (voix sur IP, vidéoconférence, etc.). En effet, contrairement aux réseaux à commutation de circuits, tels que les réseaux téléphonique commuté, où un circuit de communication est dédié pendant toute la durée de la communication, il est impossible sur internet de prédire le chemin emprunté par les différents paquets. Ainsi, rien ne garantit qu'une communication nécessitant une régularité du débit puisse avoir lieu sans encombre. C'est pourquoi il existe des mécanismes, dits mécanismes de QoS, permettant de différencier les différents flux réseau et réserver une partie de la bande passante pour ceux nécessitant un service continu, sans coupures.

2.4.1 Niveaux de service

Le terme « **niveau de service** » (en anglais *Service level*) [26] définit le niveau d'exigence pour la capacité d'un réseau à fournir un service point à point ou de bout en bout avec un trafic donné. On définit généralement trois niveaux de QoS :

Meilleur effort (en anglais *best effort*), ne fournissant aucune différenciation entre plusieurs flux réseaux et ne permettant aucune garantie. Ce niveau de service est ainsi parfois appelé *lack of QoS*.

Service différencié [19] (en anglais *differenciated service* ou *soft QoS*), permettant de définir des niveaux de priorité aux différents flux réseau sans toutefois fournir une garantie stricte.

Service garanti (en anglais *guaranteed service* ou *hard QoS*), consistant à réserver des ressources réseau pour certains types de flux. Le principal mécanisme utilisé pour obtenir un tel niveau de service est **RSVP** (*Resource reSerVation Protocol*, traduisez *Protocole de réservation de ressources*).

2.4.2 Facteurs de qualité de service

Les principaux critères permettant de juger la qualité de service sont les suivants :

Débit (en anglais *bandwidth*), parfois appelé *bande passante* par abus de langage, il définit le volume maximal d'information (bits) par unité de temps.

Gigue (en anglais *jitter*) : elle représente la fluctuation du signal numérique, dans le temps ou en phase. Exemple la téléphonie sur IP qui a pour but de pouvoir converser en temps réel sans entre-coupures engendrées par des délais supplémentaires, ce qu'on peut qualifier de facteur de gigue

Latence, **délai** ou **temps de réponse** (en anglais *delay*) : elle caractérise le retard entre l'émission et la réception d'un paquet. Exemple le téléchargement d'une application volumineuse nécessite une assez large bande passante pour récupérer les fichiers de l'application le plus vite possible. Dans ce cas nous parlons de facteur du délai

Perte de paquet (en anglais *packet loss*): elle correspond à la non-délivrance d'un paquet de données, la plupart du temps due à un encombrement du réseau. la plupart des applications exigent des garanties en terme de réception de l'intégralité des paquets. Elles sont de ce fait sensibles au facteur de pertes de paquets.

Déséquencement (en anglais *desequencing*) : il s'agit d'une modification de l'ordre d'arrivée des paquets.

2 .5 Le Clustering

La clustérisassions (clustering) [33] d'un réseau est son découpage en zones de diamètre constant. Formellement, chaque cluster comprend un clusterhead, sorte de centre du cluster. Ensuite, tout nœud du réseau doit être voisin d'un clusterhead. La clusterisation est donc l'élection des nœuds devenant clusterhead. Usuellement, les algorithmes de clusterisation cherchent à minimiser le nombre de clusterheads élus afin d'obtenir un nombre réduit de clusters.

Un algorithme de clustering est basé sur les étapes suivantes :

Formation (élection) des cluster-heads : le réseau est ainsi divisé en plusieurs clusters, La phase d'élection ou de *(cluster set up phase)* utilise des heuristiques comme le plus grand/plus petit ID dans le voisinage, le degré de connectivité, la zone géographique, la puissance de transmission ou la vitesse de déplacement (ex : utiliser les nœuds les moins mobiles), ou bien en utilisant un poids pour chaque nœud qui représente une combinaison des derniers attributs,

Communication entre les cluster-heads : dans un cluster, chaque deux nœuds sont à 2 sauts de distance entre eux. De plus, comme les cluster-heads ne sont pas directement reliés, des nœuds passerelles sont aussi élus et utilisés pour les communications entre cluster-heads,

Maintenance des cluster-heads : dans le but de s'adapter aux changements de topologie fréquents dans le réseau, une mise à jour des cluster heads élus est dynamiquement réalisée.

Ci-dessous un exemple d'algorithme de clustering basé sur le plus petit ID (utilisé dans *Adaptive Clustering for Mobile Wireless Networks*, de Chunhung Richard Lin et Mario Gerla) [6] .

T : l'ensemble des ID des voisins à un saut et ID du nœud courant

```
{
  si (my_id ==min(T)){
    my_cid = my_id ;
    diffuser cluster(my_id, my_cid) ;
    T= T - {my_id};
    }
 for (;;){
à la réception du cluster (id,cid){
    mettre le cluster ID du nœud id à cid;
    si(id ==cid ET my_cid==UNKNOWN OU my_cid > cid) my_cid = cid;
    T = T - {id};
    si (my_id==min(T)){
       si(my_cid== UNKNOWN) my_cid=my_id;
       diffuser cluster(my_id, my_cid);
       T=T - {my_id};
    }
 }
  si ( T==vide) stop;
}
}
```

2.6 Conclusion

Les réseaux sans file ont plusieurs spécificités par à port au réseaux filaire et leurs surtout le type ad hoc qui a plusieurs contrainte à prendre en compte pour leurs développer des protocoles à n'importe quel couche,

Dans ce chapitre nous avions présenté ces contraintes spécifiques aux réseaux ad hoc avec une brève présentation de leurs physiques, comme on a présenté la notion de QOS et ses principaux facteurs pour finir avec le concept de clustering.

Ces informations générales sont nécessaires pour comprendre les prochains chapitres.

Chapitre 3
Protocoles 802.11 et 802.11e

Sommaire

3.1 Introduction

Le support de la qualité de service (**QoS**) dans l'Internet représente aujourd'hui un verrou technologique important. Cependant, les réseaux locaux sans-fil IEEE 802.11qui sont de plus en plus utilisés actuellement, n'offrent pas en général de garanties concernant la qualité de service. Or, pour pouvoir maintenir une certaine QoS, des services différenciés sont nécessaires, surtout pour les applications multimédia et temps réel. Ainsi, de nombreuses propositions ont été faites pour supporter la QoS dans les réseaux 802.11. Chacune d'elles propose un mode de fonctionnement particulier du protocole.

La sous-couche MAC IEEE 802.11 définit deux fonctions de coordinations relatives à l'accès au canal radio, une fonction de coordination distribuée **DCF** (*Distributed Coordination Function*), et une fonction facultative dite à point de coordination **PCF** (*Point Coordination Function*). En effet, le canal de transmission peut fonctionner en deux modes différents : le mode avec contention (DCF) et le mode sans contention (PCF). Ainsi, le protocole MAC IEEE 802.11 fournit deux types de transmission : asynchrone et synchrone. Le type de transmission asynchrone est fourni par la fonction DCF qui implémente la méthode d'accès de base du protocole 802.11. DCF est basée sur le **CSMA/CA** (*Carrier Sense Multiple Access with Collision Avoidance*) [22] qui utilise un mécanisme d'esquive de collision basé sur le principe d'accusé de réceptions réciproques entre l'émetteur et le récepteur. Le service synchrone (également appelé service sans contention) est fourni par la fonction PCF qui utilise principalement une méthode de centralisation des accès. Le PCF emploie une approche centralisée de vote qui requiert l'utilisation de stations de base et de mobiles l'implémentant. Un point d'accès joue dans ce cas le rôle de coordonnateur de point (PC). Ce dernier vote cycliquement des stations pour leur donner l'occasion de transmettre les paquets. À la différence du DCF, l'exécution du PCF est facultative. Toutefois, aucun de ces deux modes ne fait de distinction entre les différents types de trafics.

Le standard 802.11e a proposé d'ajouter des extensions aux deux modes afin d'améliorer la qualité de service pour les applications multimédia. Toutefois, il n'y a aucune garantie de qualité de service, qui limiterait la viabilité des implémentations lourdes.

Une autre amélioration de la fonction PCF serait une fonction de coordination hybride qui permet d'activer les stations durant les périodes calmes et d'assurer à chacune d'entre elles un instant de démarrage spécifique, ainsi qu'une durée maximale de transmission. Dans le cas de la spécification IEEE 802.11e, la principale préoccupation du groupe de travail

est de répondre aux exigences de qualité de service (QoS) sans pour autant sacrifier les intérêts des acteurs industriels concernés.
Dans ce chapitre, nous allons décrire dans un premier temps la norme IEEE 802.11 et ses dérivés, ainsi que les limitations de support QOS dans cette dernière, avant de développer les différentes techniques de QoS dans la norme IEEE 802.11e.

3.2 La norme IEEE 802.11

La norme IEEE 802.11 a été crée en 1997. Elle décrit les couches physiques et MAC d'interfaces réseaux radio et infrarouges. Par la suite, des extensions ont été publiées, lui ajoutant des améliorations et des modes de fonctionnement plus performants. Les portées prévues varient entre quelques dizaines et quelques centaines de mètres en fonction de la vitesse choisie et de l'environnement. Cette norme cible deux contextes d'utilisation : les réseaux dits avec infrastructures et les réseaux sans infrastructures (ou en mode ad hoc). Dans ce qui va suivre, nous allons présenter ces deux modes de fonctionnement, ainsi que les différentes améliorations apportées à la norme IEEE 802.11.

3.2.1 Le mode infrastructure

En mode infrastructure le réseau sans fil consiste au minimum en un point d'accès **AP** (*Access Point*) connecté à l'infrastructure du réseau filaire et un ensemble de stations sans fil. L'ensemble formé par le point d'accès et les stations situés dans la zone de couverture de ce point d'accès est appelé l'ensemble de services de base **BSS** (Basic Service Set). Chaque BSS constitue une cellule et est identifié par un BSSID, un identifiant de 6 octets (48 bits).

Dans le mode infrastructure (figure 4.1), le **BSSID** (*Basic service set Identifier*) correspond à l'adresse MAC du point d'accès. Les points d'accès peuvent être reliés entre eux (plusieurs BSS) par une liaison appelée système de distribution **DS** ((Distribution System)qui est une dorsale ou backbone responsable du transfert des trames entre les différents BSS) afin de constituer un ensemble de services étendu **ESS** (*Extended Service Set*). Le système de distribution (DS) peut être aussi bien un réseau filaire, qu'un câble entre deux points d'accès ou même un réseau sans fil.

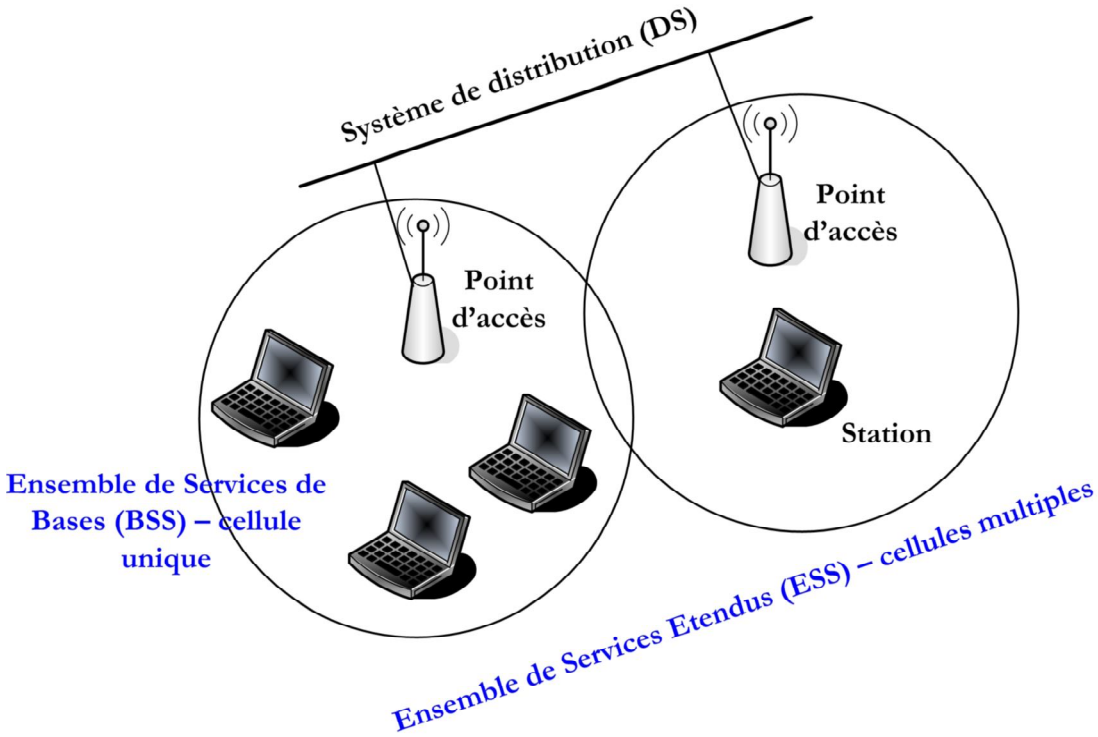


Fig. 3.1 – Exemple de réseau en mode infrastructure

Un ESS est repéré par un **ESSID** (*Service Set Identifier*) qui est un nom du réseau, c'est-à-dire un identifiant de 32 caractères de long (au format ASCII). L'ESSID ou SSID, représente le nom du réseau, ce qui peut être considéré comme un premier niveau de sécurité dans la mesure où la connaissance du SSID est nécessaire pour qu'une station se connecte au réseau étendu.

Lorsqu'un utilisateur nomade passe d'un BSS à un autre lors de son déplacement au sein de l'ESS, la carte d'accès sans fil de sa machine a la possibilité de changer de point d'accès selon la qualité de réception des signaux provenant des différents points d'accès. Les points d'accès communiquent entre eux grâce au système de distribution DS afin d'échanger des informations sur les stations et permettre le cas échéant de transmettre les données des stations mobiles. Cette caractéristique qui permet aux stations de passer de façon transparente d'un point d'accès à un autre est appelée itinérante (ou roaming).

3.2.2 Le mode sans infrastructure

Le mode ad hoc ou sans infrastructure représente simplement un ensemble de stations sans fil 802.11 qui communiquent directement entre elles sans point d'accès ni connexion à un réseau filaire. Ce mode permet de créer rapidement et simplement un réseau sans fil (dit peer to peer ou point à point) là où il n'existe pas d'infrastructure filaire ou encore là où une telle infrastructure n'est pas nécessaire pour les services attendus. Les différentes stations constituent l'ensemble de services de base indépendants ou **IBSS** (*Independent Basic Service Set*). Comme le montre la figure 4.2, un IBSS est ainsi un réseau sans fil constitué au minimum de deux stations et n'utilisant pas de point d'accès. L'IBSS constitue donc un réseau éphémère permettant à des stations situées dans un certain périmètre d'échanger des données dans un mode point à point, où chaque machine peut jouer en même temps le rôle de client et le rôle de point d'accès (serveur). Cet IBSS est identifié par un identificateur appelé SSID, comme l'est un ESS en mode infrastructure.

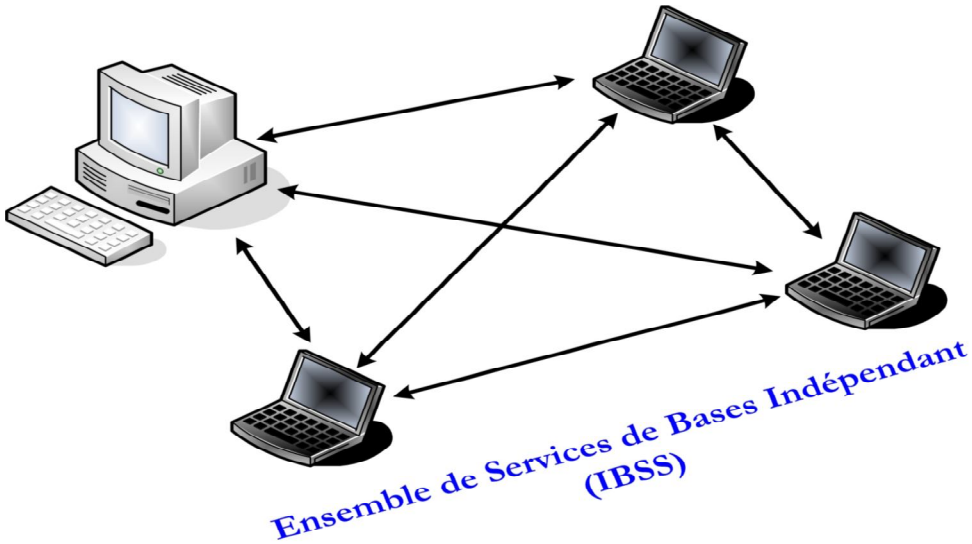


Fig. 3.2 – Exemple de réseau en mode sans infrastructure

Dans un réseau de ce type, la portée du BSS Indépendant est déterminée par la portée de chaque station. Cela signifie que si deux stations du réseau sont hors de portée l'une de l'autre, elles ne pourront pas communiquer, même si elles peuvent voir ou détecter la présence d'autres stations. En effet, l'inconvénient majeur de ce mode est que les stations ne peuvent pas jouer le rôle de routeurs. Ainsi, une station connectée à Internet ne peut partager sa connexion qu'avec les stations qui se trouvent dans sa zone de couverture, en jouant dans cette architecture le rôle d'un point d'accès.

Comme nous l'avons montré dans cette section, le standard IEEE 802.11 définit deux modes différents de fonctionnement. Cependant

plusieurs variantes de ce standard ont été proposées afin de prendre en compte certains paramètres majeurs des réseaux sans fil.

3.2.3 Différentes dérivées de la norme 802.11

Dans le but de palier certaines lacunes des réseaux sans fil et plus particulièrement du standard 802.11b, plusieurs nouvelles extensions ont été proposées :

– 802.11a : appelé également WiFi5, cette norme spécifie 8 canaux radio dans la bande de fréquence des 5 GHz. Elle permet d'obtenir un débit théorique de 54 Mbps (30 Mbps réels) ;

– 802.11b : est considérée comme la première norme sans fil exploitée par le grand public et les professionnels. Cette norme offre un débit théorique de 11 Mbps (6 Mbps réels) dans la bande des 2.4 GHz, avec une portée importante pouvant atteindre jusqu'à 300 mètres dans un environnement dégagé ;

– 802.11c : cette norme ne représente aucun intérêt pour le grand public, car elle représente uniquement une modification de la norme 802.1d afin de pouvoir établir un pont avec les trames 802.11 au niveau liaison de données ;

– 802.11d : qui représente un supplément à la norme 802.11 dont le but est de permettre aux différents points d'accès d'échanger des informations sur des plages de fréquences et des puissances selon les restrictions réglementaires autorisées dans différents pays ;

– 802.11e : qui vise à donner des possibilités en matière de qualité de service au niveau de la couche liaison de données pour les applications multimédia et temps réels.

– 802.11f : cette norme a été définie afin de permettre une meilleure utilisation d'infrastructures multi-vendeur. En proposant un protocole appelé **IAPRP** (*Inter Access Point Roaming Protocol*), 802.11f permet à un utilisateur itinérant de changer de point d'accès de façon transparente lors d'un déplacement dans l'infrastructure réseau.

– 802.11g : cette norme qui est plus performante (au moins en terme de débit et de sécurité) est directement compatible avec 802.11b et utilise une modulation OFDM (*Orthogonal Frequency Division Multiplexing*). Elle offre un haut débit théorique de 54 Mbps (30 Mbps réels) sur la bande de fréquence des 2.4 GHz.

– 802.11h : le but de cette norme est de respecter l'utilisation des systèmes WLANs dans les pays européens dans la bande 5 GHz (**HiperLAN 2** [8], d'où ce "h" de 802.11h) pour être en conformité avec la réglementation européenne en matière de fréquence et d'économie d'énergie.

– 802.11i : qui a été définie afin de remédier au problème de la sécurité des transmissions (gestion et distribution des clés, chiffrement et authentification).

Cette norme s'appuie sur l'**AES** (*Advanced Encryption Standard*) et s'applique aux technologies 802.11a, 802.11b et 802.11g.

– 802.11j : dont la spécification a été proposé dans le but d'incorporer la réglementation japonaise, au même titre que 802.11h par rapport à la réglementation européenne.
– 802.11Ir : cette technologie qui utilise des signaux infrarouges, a pour caractéristique principale d'utiliser une onde lumineuse pour la transmission de données. En effet le caractère non dissipatif des ondes lumineuses permet d'offrir un niveau de sécurité plus élevé. Le fait qu'elle soit toujours utilisée, cette norme est techniquement dépassée.
– 802.11n : cette nouvelle norme a été ratifiée à l'unanimité au sein de l'**IEEE (***Institute of Electrical Electronic Engineers***)** en début 2006. Elle sera la première norme 802.11 à implémenter la technologie **MIMO** (*Multiple Input Multiple Output*). 802.11n devrait être à priori dix fois plus rapide que la norme 802.11g puisque les débits théoriques annoncés sont de plus de 500 Mbps, tout en restant compatible avec les normes 802.11b et 802.11g.

3.2.4 Description de la fonction DCF

En général, dans le monde filaire, lorsqu'un émetteur veut envoyer un signal sur le câble, il peut y lire en même temps la valeur qui y est effectivement présente.
Si cette valeur lue est différente de celle émise, c'est qu'un autre émetteur est actif au même moment et qu'il y a eu une collision. L'écoute du signal sur le câble au moment de l'émission représente la clé de base du mécanisme d'accès **CSMA/CD** (*Carrier Sense Multiple Access with Collision Detection*) bien connue d'Ethernet.
Le CSMA/CD permet entre autre, de détecter une collision et dans ce cas là de retransmettre le paquet après un certain temps d'attente (aléatoire). Cependant, dans le cas des communications radio, l'atténuation du signal en fonction de la distance est bien plus importante que sur un câble. En effet, au niveau d'un émetteur, le signal qu'il envoie est reçu avec une puissance très supérieure à un signal venant de n'importe quel autre mobile. Un signal émis localement est reçu avec une puissance tellement supérieure aux autres signaux qu'il les occulte complètement. De cette façon pour l'émetteur, il n'y a donc jamais de collision en radio. Mais le problème peut se poser au niveau du récepteur, qui peut recevoir simultanément plusieurs signaux avec différentes puissances.

Dans la pratique, les cas de collisions se produisent uniquement au niveau des récepteurs. L'une des caractéristiques de la couche MAC 802.11 est donc d'utiliser des acquittements pour détecter les collisions et permettre par la suite la retransmission des paquets en cas de non réception des acquittements. Une autre caractéristique du protocole 802.11 est qu'il permet d'envoyer une trame vers une destination spécifique (**unicast**) ou faire une diffusion (**broadcast**). Dans le cas d'une diffusion, les acquittements ne sont pas utilisés et les paquets peuvent être perdus de manière tout à fait silencieuse (car si chaque mobile ayant reçu le paquet

diffusé cherche à envoyer un acquittement au même moment, il y aura une série de collisions sur les acquittements).

Avec Ethernet, l'idée est d'observer l'état du canal avant d'émettre. Si le canal est libre, la trame peut être envoyée (et si à ce moment-là une collision est détectée, la trame sera réémise un peu plus tard, après une durée d'attente aléatoire). Or, dans un environnement radio, il n'est pas possible de détecter directement les collisions. Par conséquent, le mécanisme qui conditionne l'autorisation d'émettre sur le canal doit lui aussi être modifié par rapport à ce qui se fait en 802.3. En effet, si l'émetteur se contente d'attendre que le canal se libère pour émettre, alors si plusieurs nœuds mobiles étaient en attente d'émission, ils détecteraient tous le canal libre et émettraient au même moment. Dans ce cas là, il y aurait collision aux récepteurs et il faudrait attendre que le délai imparti pour le retour des acquittements soit écoulé pour s'en rendre compte, ceci pourrait être relativement long. L'idée dans le 802.11 est donc de faire en sorte que lorsque le canal devient libre, chaque nœud doit attendre une période de durée aléatoire supplémentaire appelée backoff avant de commencer l'émission des trames. Ainsi, si plusieurs nœuds veulent émettre, la probabilité est minime pour qu'ils aient choisi la même durée. Et celui qui a choisi la plus petite valeur de backoff va commencer à émettre. Les autres nœuds vont alors se rendre compte que le canal n'est pas libre et vont attendre. La figure 4.3 montre ce qui peut se passer lorsque deux nœuds à portée de communication tentent d'émettre vers un troisième nœud au moment où le canal devient libre. Dès que le canal devient libre, il doit rester dans cet état (libre) pour une période **DIFS** (*DCF Inter-Frame Space*). Après, s'il est resté libre durant toute cette période, chaque nœud voulant émettre choisira un backoff aléatoire exprimé par le nombre de time slots d'une durée fixe (20 µs).

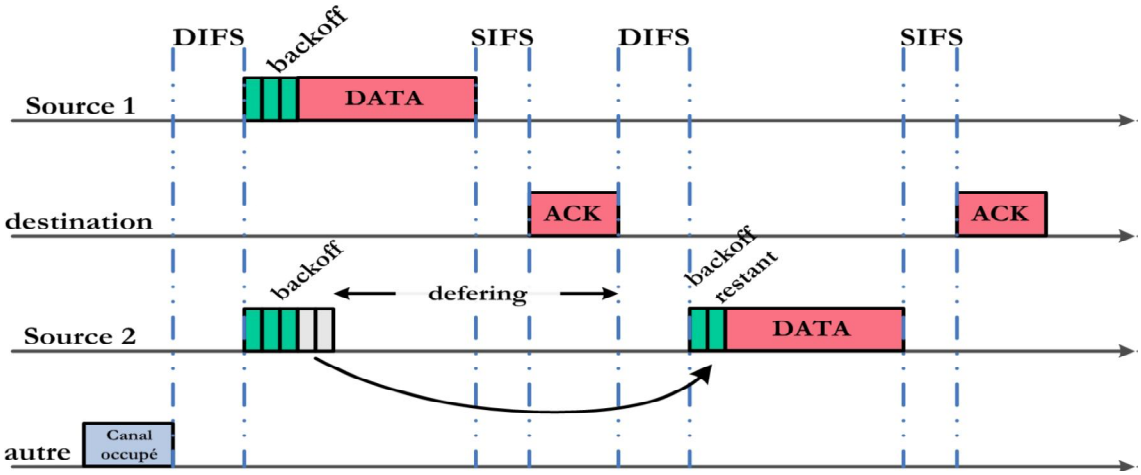


Fig. 3.3 – Les mécanismes du backoff et du defering

Dans l'exemple illustré par la figure 3.8, la valeur du backoff pour le nœud 1 est égale à 3 tandis que celle du nœud 2 est égale à 5. Une fois ces deux valeurs de backoff sont tirées par les deux nœuds, tant que le canal reste libre, les nœuds décrémentent leur *backoff*. Dès que l'un d'eux a terminé (ici

le nœud 1), il commence l'émission. Tandis que l'autre nœud, dès qu'il détecte le reprise d'activité sur le canal de communication, il arrête la décrémentation de son *backoff* et entre en période dite de report ou *defering*.
Il faut noter que le temps de pause appelé **SIFS** (*Short Inter-Frame Space*) et qui sépare un paquet de données et son acquittement est plus court que le DIFS. Chaque nœud en état de *deferring* ne pourra reprendre la décrémentation de son *backoff* que si le canal est libre à nouveau (pendant une durée équivalente à DIFS). SIFS est plus court et empêche que la décrémentation du backoff ne reprenne de manière inopportune entre les données et l'acquittement. Le nœud 2 ne peut reprendre la décrémentation de son backoff, que lorsque le nœud 1 reçoit l'acquittement de ses données et que le canal reste libre pendant une période DIFS. Dans ce cas, aucun autre nœud ne peut empêcher le nœud 2 d'envoyer finalement ses données.
En utilisant le mécanisme de *backoff* les risques de collision sont limités mais ne sont pas complètement supprimées. Cependant, si une collision se produit et afin de diminuer les chances que de telles collisions se répètent, une nouvelle valeur du *backoff* est tirée aléatoirement. Mais après chaque collision consécutive, la taille de la fenêtre de contention **CW** *(Contention Window*) sera doublée afin de diminuer les chances de tomber encore une fois en collision. La valeur de la fenêtre de contention CW est comprise entre zéro et une borne supérieure (calculée en puissances de 2 moins 1) qui évolue entre deux valeurs CWmin et CWmax définies par la norme 802.11. Cette borne supérieure de la fenêtre de contention est réinitialisée à CWmin chaque fois qu'un paquet a été correctement envoyé (ou lorsque les timers de réémission expirent).

– Le mécanisme EIFS

Dans la configuration illustrée par la figure 4.4, le nœud de gauche (appelé autre) détecte la porteuse de l'émetteur sans pour autant comprendre le message (signal trop faible pour être décodé, mais assez fort pour être reconnu). Les paquets envoyés par la destination ne sont quant à eux pas détectés par ce nœud. Dans cette situation, 802.11 impose l'utilisation d'un nouveau type de période appelé **EIFS** (*Extended Inter Frame Spacing*), afin d'éviter une éventuelle collision au niveau de l'émetteur au moment de la réception du **CTS** (*Clear To Send*) ou de l'acquittement ACK par la destination.

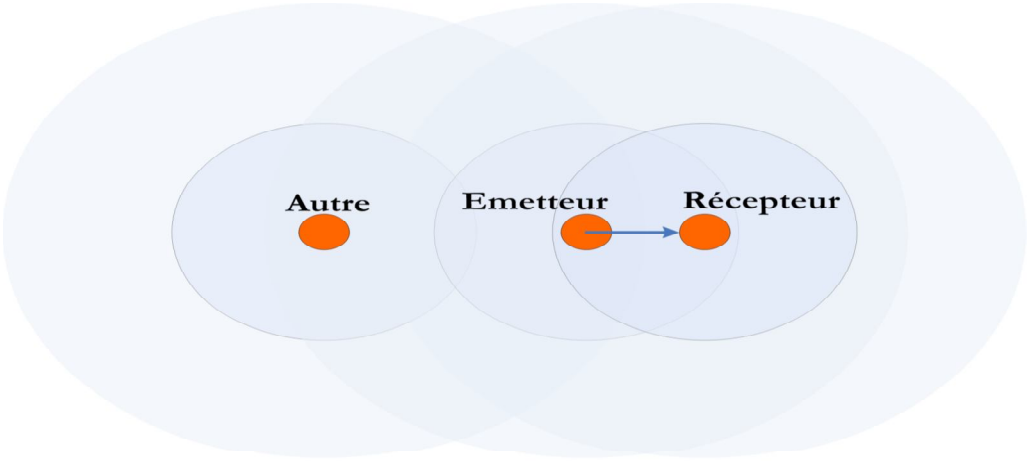


Fig. 3.4 – Une configuration où l'EIFS est nécessaire

Dans la figure 4.5, l'émetteur envoie un paquet de contrôle de type **RTS** (*Request To Send*). Ce paquet est reçu par le récepteur, qui va y répondre par un paquet de type CTS. A ce moment, le nœud autre, détecte de l'activité sur le canal lors du RTS mais sans comprendre le paquet. Le mécanisme de *defering* présenté précédemment l'empêche d'émettre pendant l'envoi du RTS (canal occupé) et pendant une période DIFS consécutive (attente obligatoire que le canal reste libre pendant DIFS). Mais la période DIFS est plus courte que SIFS + CTS. Si jamais le nœud autre avait terminé de décrémenter son backoff trop vite, il aurait pu émettre pendant le CTS provoquant une collision au niveau de l'émetteur. Pour éviter cela pour le CTS (et de manière similaire pour l'acquittement), 802.11 impose que le nœud attend pendant un temps EIFS lorsque le canal redevient libre mais que le paquet n'a pas été compris.

EIFS étant suffisamment long pour que l'envoi du CTS ou de l'ACK se déroule normalement.

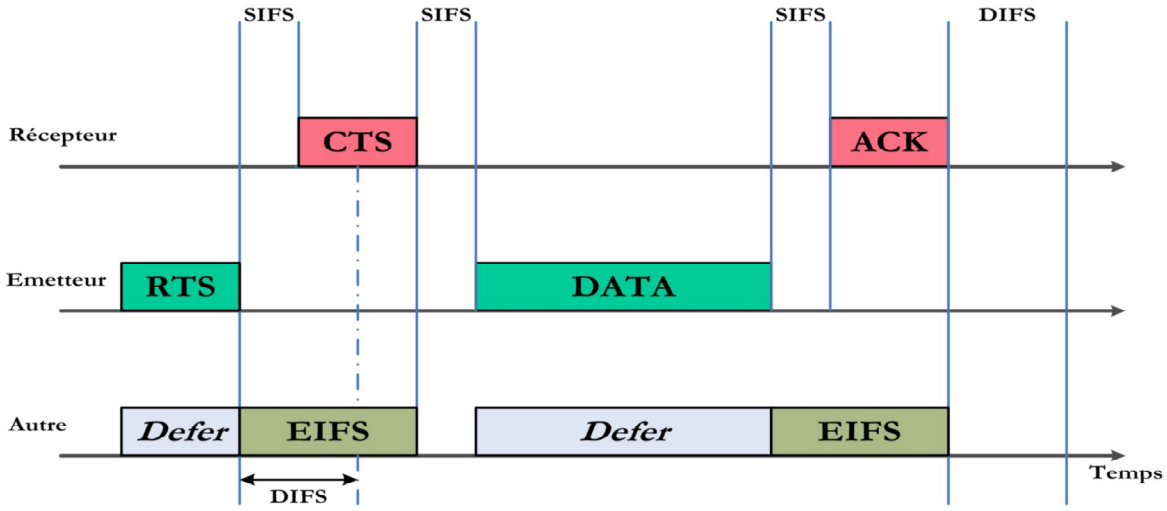


Fig.3.5 – L'Extended Inter Frame Spacing (EIFS)

3.2.5 Description de la fonction PCF

A l'opposé du DCF, où le contrôle d'accès au support est distribué sur toutes les stations, le mode PCF définit le point d'accès **AP** (*Access Point)* comme seul contrôleur d'accès au support. En effet, le point d'accès ordonne les transmissions et distribue le droit à la parole. La fonction DCF permet un fonctionnement totalement distribué de l'accès au canal. Afin de limiter le nombre des collisions, CSMA/CA a recours à une durée aléatoire avant chaque émission d'un paquet. Ce temps passé à attendre peut représenter autant de perte de débit effectif. Le modèle 802.11 propose en effet, un mécanisme (optionnel) centralisé qui permet une meilleure utilisation du canal. Ce mécanisme appelé **PCF** (*Point Coordination Function*) requiert l'utilisation de stations de base et de nœuds l'implémentant.

L'objectif de ce mécanisme (PCF) est de centraliser la gestion de l'accès au canal. C'est le point d'accès qui indiquera à chacun des nœuds mobiles qui lui sont rattachés le moment où il peut émettre ses paquets. Ainsi, le backoff aléatoire devient, en partie inutile car la station de base impose son ordre des transmissions et il n'y a pas de contention pour l'accès au médium (Contention Free Period). Cependant et afin de préserver la compatibilité, dans chaque cycle PCF, une période DCF est conservée pour permettre aux nœuds n'implémentant pas la PCF de continuer à accéder au canal, comme le montre la figure 4.6. La cohabitation entre les deux mécanismes est assurée grâce au temporisateur **PIFS** (*PCF Inter Frame Spacing*). Durant la période

PCF, les paquets ne sont en effet séparés que par des périodes PIFS ou SIFS (selon le cas) qui sont plus courtes que le DIFS.

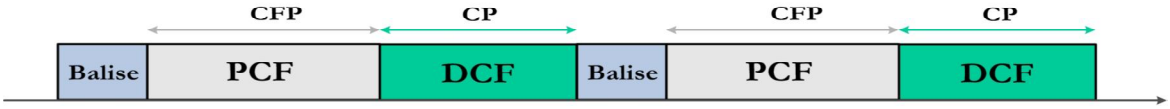


Fig. 3.6 – L'alternance des modes PCF et DCF

3.3 La qualité de service dans le standard 802.11

3.3.1 IEEE 802.11e

Le groupe IEEE 802.11e a proposé une nouvelle approche par priorité liée aux catégories de trafic [10] [29]. Cette solution nécessite une extension de la méthode d'accès DCF. Dans cette méthode, le calcul des fenêtres de contention est géré par un mécanisme spécifique qui permet une croissance exponentielle de ces fenêtres pour chaque catégorie de trafic. Dans le 802.11e, huit niveaux de priorité on été définis pour huit catégories de trafic avec pour chacune des valeurs pour la fenêtre de contention (valeur minimale et valeur maximale) et des délais inter-trame (*Inter Frame*) différents.

La valeur du backoff d'une station devient ainsi une fonction de ces paramètres :

$$back(TC_i) = f(AIF_i, CW\min_i, CW\max_i, PF_i) \qquad (4.3.1)$$

Où, *AIFi* est le délai *Inter Frame* de la catégorie de trafic i (*TCi*). $CWmin_i$ est la valeur minimale de la fenêtre de contention de cette catégorie de trafic. $CWmax_i$ est la valeur maximale de la fenêtre de TC_i et PF_i est le facteur de persistance (*Persistence Factor*) qui sert à réduire la probabilité de collision pour TC_i. Ainsi, en cas de collision, la nouvelle fenêtre est calculée par la formule suivante (pour chaque catégorie de trafic TC_i) :

$$CWnouvelle[TC_i] = ((CWancien[TC_i] + 1) \times PF[TC_i]) - 1 \qquad (4.3.2)$$

Avec :

$$CWnouvelle[TC_i] = \min(CWnouvelle[TC_i], CW\max[TC_i]) \quad (4.3.3)$$

3.3.2 La fonction EDCA (Enhanced Distributed Channel Access)

L'EDCA (offre un accès distribué différencié au médium en utilisant différentes priorités pour différentes catégories de trafic(TC).dans ce qui suit on présente les composants, la description et le fonctionnement de l'EDCA.

3.3.2.1 Catégories d'accès (ACs)

EDCA définie quatre catégories d'accès (ACs) pour les différents types de données, la différenciation de service est introduite par l'utilisation d'un groupe de paramètres différents pour chaque catégorie utilise pour chaque AC, ces paramètres, dites *paramètres d'EDCA*, sont décrites dans ce qui suit.

Les trames des différents flux de données sont classées en ACs suivant leurs trafics/applications exigences en QOS. Les catégories sont nommées **AC-BC** (*Background Access Category*), **AC-BE** (*Best Effort Access Category*), **AC-VI** (*Video traffic Access Category*) et **AC-VO** (*Voice traffic Access Category*).

Chaque trame arrive avec une valeur de priorité marquée par les couches les plus hautes, ces priorités sont dites priorités d'utilisateur (**UP** (*User Priority*)),il y'a huit UP allant de 0 à 7, l'affectation de ces priorités aux trames est une tâche des couches supérieures qui n'est pas décrite dans le standard 802.11e. Généralement ces priorités sont affectées par les utilisateurs des applications ou même par les applications conformément aux caractéristiques du trafic comme le débit, l'intervalle de paquet, la taille du paquet ...

Au niveau MAC les catégories d'accès (AC) seront dérivées des priorités d'utilisateurs (UP) comme le montre la Figure 4.7.

UP (User Priority)	Notation 802.1D	802.11e AC (Access Category)	type de Service
2	Not defined	0	Best Effort
1	Background (BK)	0	Best Effort
0	Best Effort (BE)	0	Best Effort
3	Excellent Effort (EE)	1	Video Probe
4	Controlled Load (CL)	2	Video
5	VI (Video <100ms latency and jitter)	2	Video
6	VO (Video <10ms latency and jitter)	3	Voice
7	Network Control (NC)	3	Voice

Fig.3.7 – Couplage de la priorité d'utilisateur(*UP)* aux catégories d'accès (*ACs)* de 802.11e.

3.3.2.2 EDCAF (Enhanced Distributed Channel Access Function)

Chaque station implémente quatre files d'attente; une pour chaque AC et quatre **EDCAF**s *(Enhanced Distributed Channel Access Function)* indépendantes comme illustré par la Figure 4.8, chaque EDCF est une version amélioré du DCF avec les mêmes principes d'accès au médium (CSMA/CA, *backoff*) mais basé sur des paramètres spécifiques pour chaque AC, la section suivante présente ces paramètres dites paramètres d'EDCA.

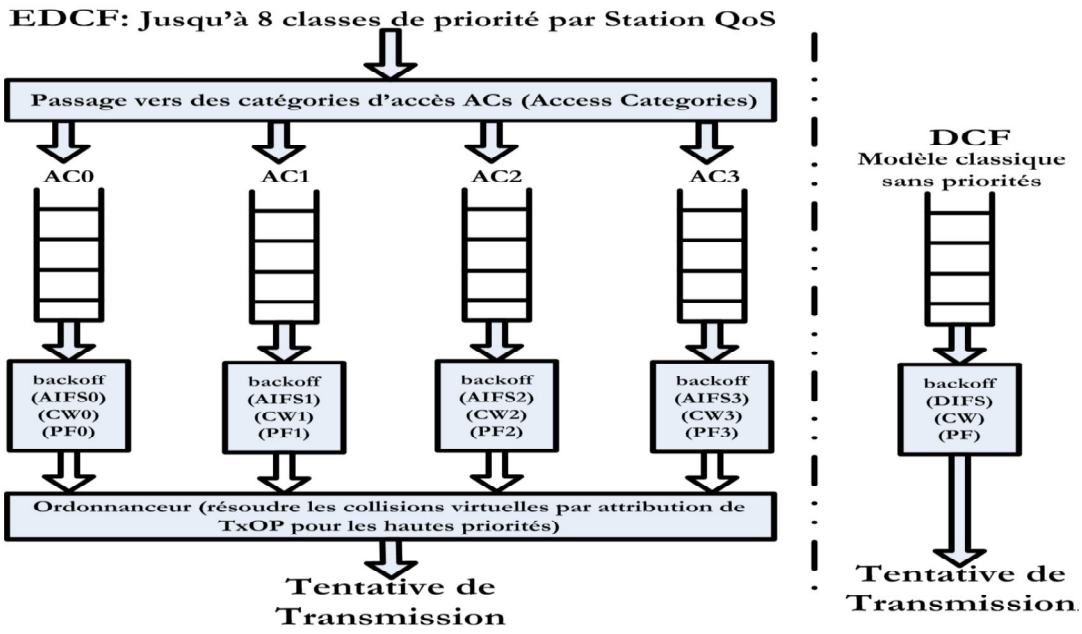


Fig. 3.8 – La fonction EDCF vs DCF

-EDCA Paramètres

Un EDCAF conteste pour l'accès au medium à base des paramètres suivant :

AIFS (*Arbitration Inter-Frame Space*) : la période du temps minimal durant laquelle le canal doit être libre avant une transmission ou un début d'un backoff. AIFS n'est pas une valeur constante comme le DIFS du DCF ; il dépend de la Catégorie d'accès pour laquelle il conteste .AIFS est calculée par la formule suivante :

$$AIFS[TC] = AIFSN[TC] \times aSlotTime + aSIFSTime \qquad (4.3.4)$$

Avec *SlotTime* est la durée d'un *slot*, *aSIFSTime* est le SIFS et *AIFSN[TC]* est le **AIFSN**(*Arbitration Inter-Frame Space Number*) de la catégorie TC qui représente le nombre des slots qui constituent en plus du SIFS le AIFS d'une TC. Différentes valeurs d'AIFSN sont utilisées pour les différents ACs selon leurs TC comme le montre la figure 4.9; ces valeurs par defaut peuvent être modifié par .....

CWmin,CWmax est la valeur minimale/maximale de la fenêtre de backoff d'une catégorie de trafic.les limites de la fenêtre de contention ne sont pas fixés comme en DCF mais dépendent du AC, ils sont petites pour les ACs de hautes priorité pour leurs permettre d'attendre moins que ceux de priorité inferieure comme le montre la figure 4.9.

TXOP limite: la durée maximale d'une transmission après l'acquisition du canal. Lorsqu'un EDCAF aille le canal, il pourra transmettre pendant une durée qui ne dépasse pas la limite du TXOP, la durée de transmission englobe toutes les trames échangées y compris les périodes SIFS, ACK, RTS et CTS, on appelle *Contention Free Bursting* (**CFB**) cette période de transmission d'une suite de trames de même AC sans interruption.si le mécanisme RTS/CTS est utilisé RTS est transmise une seule fois au début et CTS une seule fois à la fin du CFB. Si la limite de TXOP est à 0, cas d'AC_BK et AC_BE (figure 4.9) l'EDCAF n'a le droit qu'à transmettre une seule trame avec son RTS et ACK si le mode RTS/CTS est actif.CFB permet aux ACs de haute priorité saisissent le canal pour des durées de temps importante ce qui réduit d'une façon significatif la latence(*delay*). Cependant Une grande TXOP limite pénalisera les ACs de priorités faible par une longue latence.

AC	CWmin	CWmax	AIFSN	Limite du TXOP	
				FHSS	DSSS
AC_BK	CWmin	CWmax	7	0	0
AC_BE	CWmin	CWmax	3	0	0
AC_VI	(CWmin+1)/2-1	CWmin	2	6.016ms	3.008ms
AC_VO	(CWmin+1)/4-1	(CWmin+1)/2-1	2	3.264ms	1.504ms

Fig. 4.8 – Valeurs des paramètres par défaut d'EDCA

3.3.4 La fonction HCF

Le schéma de PCF a été prolongé dans 802.11e [25] en utilisant la fonction **HCF** (*Hybrid Coordination Function*). Dans ce schéma, il y a un coordonnateur hybride (HC) habituellement co-placé avec le point d'accès. Ce coordonnateur peut s'allouer des TXOPs pour transmettre après avoir attendu pendant PIFS (qui est plus court que DIFS et n'importe quel AIFS). Ainsi le coordonnateur hybride obtient la priorité par rapport aux autres nœuds pour transmettre des trames. Le HCF reste opérationnel pendant les périodes de contention (CP) et les périodes sans contention (CFP). Pendant la période de contention CP, chaque nœud obtient son TXOP aussi bien quand le canal est libre selon les règles EDCF, que lorsque le nœud reçoit une trame de QoS CF-Poll du HC. Pendant la période CFP selon les règles du **HCCA (***HCF controlled channel access***)**, le temps de départ ainsi que la durée maximale de chaque TXOP sont indiqués par le coordonnateur hybride en utilisant des trames de CF-Poll. Comme son nom l'indique (période sans

contention), les nœuds ne peuvent pas contester entre eux pour TXOP pendant la CFP. La CFP finit soit au temps indiqué dans la trame de balise (*becon*) soit par une trame de CF-End envoyée par le HC.

Le 802.11e utilise également un autre mécanisme par lequel les nœuds envoient l'information de mise à jour au coordonnateur hybride. Il inclut les nœuds qui doivent être sélectionnés, le temps de sélection et la durée de transmission. Le mécanisme utilisé est appelé contention contrôlée dans lequel le HC assigne un certain nombre d'opportunités de contentions contrôlées, séparées par des SIFS. Cela est fait de sorte que les stations avec des trafics prioritaires n'aient pas besoin de faire face à d'autre trafic de EDCF pour transmettre l'information requise. Le coordonnateur hybride envoie également un masque de filtrage contenant les TCs dans lesquelles des demandes de ressources peuvent être placées. Chaque nœud choisit un intervalle d'opportunité et transmet une trame de demande de ressources contenant la TC et la durée TXOP demandée. Le HC envoie également un acquittement de sorte que les nœuds demandés puissent détecter des collisions pendant la contention contrôlée. Habitué

3.4 Conclusion

Dans ce chapitre, nous avons présenté le standard IEEE 802.11, avant de détailler le nouveau modèle de support de qualité de service, IEEE 802.11e. Cette dernière norme vise à offrir une différenciation de service au niveau MAC afin de mieux servir des flux considérés de haute priorité tels que les flux multimédia ou les flux temps réel.

Dans le prochain chapitre, nous allons présenter un protocole MAC avec prise en charge de la différenciation de service qui se base sur une architecture distribué organisé sous forme d'un cluster construit par un algorithme que nous proposons pour résoudre les problèmes lié à la nature ad hoc du réseau (nœud caché, nœud exposé, problème des trois pairs ...) et au comportement égoïste(*selfish behavour)* par le polling distribué.

Chapitre 4
Protocole DCC-MAC (Distributed Clustering and Communication MAC protocol)

Sommaire

4.1 Introduction

On a essayé à partir de nos lectures de quelques protocoles existants pour les réseaux Ad Hoc (Chapitre 3) d'en extraire quelque inconvénients et avantages, on a essayé de proposer les meilleures solutions pour ces inconvénients en y décelons des avantages d'autres ce qui a donné naissance au *Distributed clustering and communication MAC protocol* (DDC**-MAC protocol**).

Nous avons vu dans le chapitre précédent que la norme ieee802.11e et malgré tous les avantages qu'elle présente (support de QOS) souffre encore de problème de non fiabilité en cas de surcharge de réseau et en augmentation de nombre des nœuds de réseau [25] comme elle souffre encore des problèmes de collisions interne et collisions externes . Pour faire face à ces problèmes on propose dans ce présent chapitre un nouveau protocole de communication distribué qui supporte la QOS via deux phase une pour le *clustering* qui a comme objectif principale de résoudre le problème de Nœud caché en offrant une architecture transparente à tous les nœuds et la deuxième de transmission par le biais de quartes sous phases, Sélection du TC prioritaire au niveau de chaque nœud en utilisant le même mécanisme de différenciation de service du protocole 802.11e[12],échange des candidatures pour avoir la TXOP suivant un protocole *robin round* suivant les identités des nœuds, polling distribué en utilisant les information issus des trames de candidature avec un algorithme que nous présenterons et finalement la transmission du rafale des *selected-node* pendant la TXOP désignée ;

Dans ce chapitre nous présenterons premièrement les idées principales de notre protocole et on détaille par la suite toutes les phases du protocole DCC-MAC et on finie par une présentation de son évaluation par le biais des résultats de son simulation avec le simulateur NS2 sur un réseau de nombre limité de nœuds.

4.2 Idées principales de protocole DCC-MAC

Comme on l'a déjà cité dans les précédents chapitres, les protocoles MAC des réseaux Ad Hoc et malgré le nombre important des travaux déjà réalisés et des protocoles proposés restent encore un champ très riche à exploiter car les protocoles réellement implémentés et standardisés ne dépassent pas le nombre du doit d'une seule main comme ils présentent encore plusieurs lacunes [30],[2], l'idée de départ était de proposer un protocole aussi simple et sans inconvénient mais en lisant sur le domaine les différentes problèmes spécifiques aux réseau Ad Hoc nous a mené successivement à arriver à notre proposition .

L'idée générale est d'avoir toute la transparence possible aux nœuds pour leurs permettre d'avoir un esprit de groupe, tuer le problème d'égoïsme (*selfish behaviour*)[15] entre les différentes nœuds d'un réseau , en leurs informant tous par ce qui se passe au niveaux de tout le réseau et en leurs offrir tous la même méthode de penser pour finir tous par la même décision et ne pas contester pour avoir la même opportunité de transmission ; pour se faire les nœuds doivent échanger des informations sur leurs statuts en toute transparence pour cela on a trouvé que communiquer leurs envies est la seule méthode et c'est ce qu'on fait dans la phase de **candidature** et pour que cette candidature n'aura pas de problème on a proposer un clustering qui permet à chaque nœud d'avoir les détailles de son voisinage(*neighborhood*) pour éviter les problèmes de collision et du nœuds cachés, pour le reste de protocole on s'est beaucoup inspiré des premiers standards au monde actuellement dans ce domaine (ieee802.11)[11] pour répondre au mieux au exigences de qualité de service (QOS) et ce en implémentant un mécanisme de différentiation (diffserv) similaire au 802.11e .

DDC-MAC comporte les phases présentées dans la figure suivante (figure 4.1), les détailles de chaque phase seront présentées dans les paragraphes suivantes.

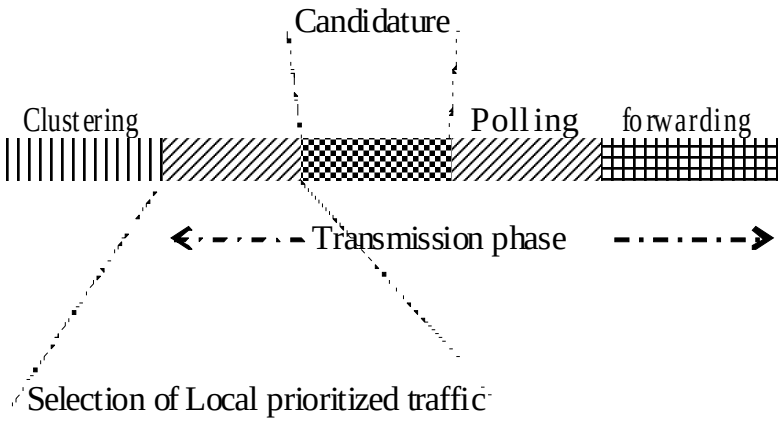


Fig. 4.1 – les phases du protocole DCC-MAC

4.3 Phase de Clustering

4.3.1 Clustering Vs trames de contrôle

On trouve dans la littérature deux approches pour faire face aux problèmes issus des difficultés d'évitement des collisions dû principalement au problèmes de perception du porteuse liés à la localisation des nœuds de réseaux Ad Hoc (*Location-Dependent Carrier Sensing*)[1]comme le problème du nœud caché ou exposé .

1-la solution à base des trames de contrôle (exemple : RTS/CTS, BB(Burst Black)...)qui a l'inconvénient d'encombrement du support commun du transmission et de consommation des ressources. Avec un nombre important de nœud [30],cette technique se complique et ne sera plus utile car les collisions entre ses trame de contrôle même seront très importants car rien n'assure que ces collisions ne parvient pas[17] mais l'idée est simplement que perdre du temps à retransmettre ces paquets courts est moins couteux que la retransmission des trames de données.

2-Par clustering [24], dans cette approche on essaye d'utiliser des informations issus d'autres couches pour avoir une topologie transparente du voisinage en constituant des groupes de nœuds similaires suivant un ensemble de caractères. Pour le niveau MAC les algorithmes de clustering ont chacun un objectif bien déterminé pour aider à accomplir une tâche bien spécifié au niveau MAC [9][15], cette approche a l'avantage de réutilisabilité soit des information de clustering pour le routage ou l'utilisation d'informations de routage au niveau MAC ou bien via une architecture inter-couche (*cross-layer)* [23] .pour notre protocole nous optons pour cette approche pour profiter de ses apport

prouver pour supporter la QOS[16], dans notre cas l'objectif principale du clustering est d'éliminer le phénomène du nœud caché, ça n'empêche que nos clusters ne souffrent théoriquement d'aucun des problèmes dépendant à la localisation des nœuds.

4.3.2 Algorithme de clustering

L'objectif principal de notre algorithme de clustering est d'éliminer le problème du nœud caché pour augmenter l'utilisation du canal en diminuant les pertes de temps causées par les collisions et les retransmissions qui en résultent.

Chaque session dans notre protocole commence par la classification des nœuds de réseau en clusters transparents, la transparence de la topologie résultante découle du fait que chaque nœud est conscient de tous les autres dans son cluster comme il peut détecter leurs signaux en toute clarté sans aucun problème (bien sure sans prendre en compte les problèmes d'altération de signale : atténuation, réflexion, interférence, réfraction, diffraction, L'absorption ...) .

Les clusters seront formés comme suit :

Premièrement chaque nœud construit la table de tous les nœuds qu'il peut entendre clairement mutuellement, cette table dite de voisinage (*neighborhood*).

La seconde étape est l'échange des tables de voisinage entre les nœuds figurant dans les tables de voisinage de chaque nœud ,

En recevant les tables de voisinage des autres nœuds , chaque nœud les compare au sien pour avoir une des résultat suivantes :

1-les tables sont similaires ce que veux dire que ces deux nœuds appartiennent au même cluster,

2-les tables sont différentes, mais l'ensemble de leur intersection ne peut être vide car ils s'entends au moins mutuellement ; les nœuds qui entendent à la fois des nœuds d'autre clusters seront les nœuds intermédiaires, il seront activer selon les secteurs auxquels ils appartiennent en excluant mutuellement les secteurs d'intersection non vide.

Pour chaque deux différents clusters nous avons au moins un nœud qui ne peut pas entendre tous les autres nœuds du cluster auquel

il n'appartient pas, un de ces nœuds sera choisi comme identificateur du cluster, nous choisissant celui avec l'identifiant minimal.

Algorithme de Clustering (au niveau du nœud I)

Notations:

Msg(I): message d'identité du ***I***
Nbh(I): la liste des nœuds voisin du nœud ***I***
Clst(I): cluster contenant ***I***
Ch: cluster head
dif(nbh(I),nbh(J)):différence entre ***nbh(I)*** et ***nbh(J)***
otherClst: ensemble des liste des nœuds d'autre clusters qui se chevauche avec ***Clst(I)***
ClstNmb: Nombre des clusters affectés par la transmission au sein du cluster ***I***
T1,T2: Temps nécessaire pour la transmission de **msg(ID)** et **nbh(I)**(respectivemet)

Formation des Cluster:

```
Begin
  Ch:= I;
  ClsNmb:=0;
  //Diffusion des messages d'identités
  While timer 'T1' is valid do
    Send msg(ID);
      //construction de table des nœuds que I peut entendre et qui peuvent
      clairement     l'entendre( table de voisinage)
    Build nbh(I);
  //Echange des tables de voisinage
  While 'T2' is valid do
    Send Nbh (I);
  For every J in Nbh(I) do

      If  Nbh(I)  < = Nbh(J) then
        Begin
          //ajout des nœuds qui ont la même table de voisinage au cluster de I
          Add J to Clst(I)
          //affecter au Ch la valeur de l'identité minimale des nœuds qui le
          composent
          If J< I then
            Ch: =J;
        End
      //si les Nbh sont différentes on décide suivant leurs différence
      Else
        Begin
          If dif(nbh(I),nbh(J)) not in OtherClst then
            Begin
              Add dif(nbh(I),nbh(J)),OtherClst)
              ClsNmb:= ClstNmb+1
            End
      Endif
End.
```

Le clustering permet aux nœuds d'être conscients du topologie dont ils sont membres et d'éliminer les problèmes lies au localisation des

nœuds [4], les résultat du clustering vont être utilisés dans les phases suivantes du protocole DCC-MAC.

EXEMPLES DE CLUSTERING

Si on prend le schéma présenté par la figure 4.2, nous aurons :

Paramètre / Nœud	Ch	Nbh	ClsNmb	otherClst
1	0 ,4	10,11, 0, 1, 2, 3	1	1, 2, 3, 4, 5, 6
10	0	11, 10,0, 1, 2, 3	0	Néant
12	12	13,14	0	Néant
3	0, 4, 7	3, 6, 9, 7, 8	2	11, 0, 10, 1, 2, 3 4, 5, 6, 1, 2, 3

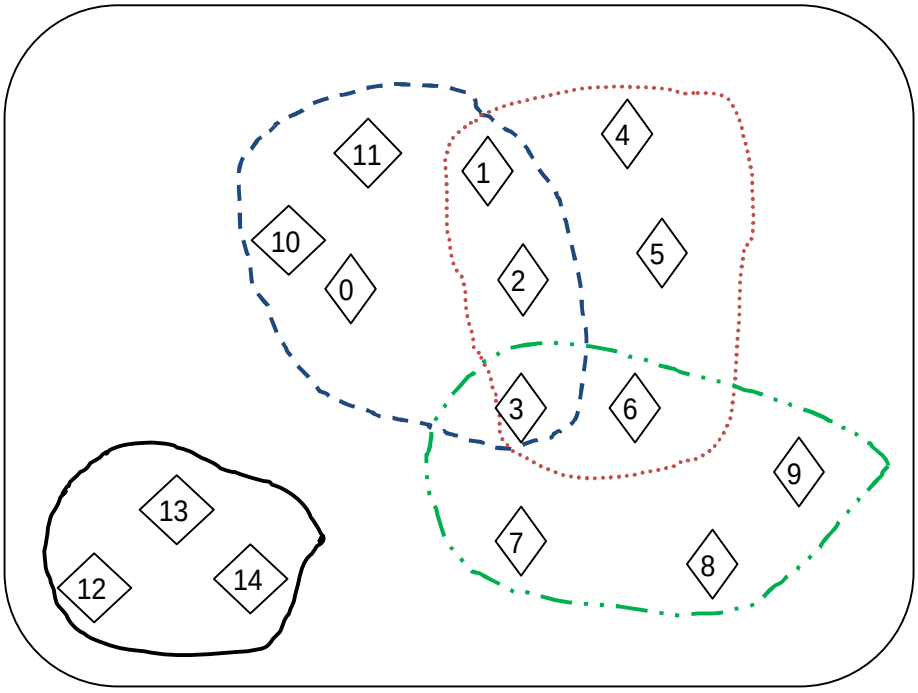


Fig. 4.2 – Exemple de clustering

4.4 Phase de transmission

Maintenant que nous avons une topologie transparente basée cluster par laquelle nous avons complètement résolu le problème du nœud caché et par conséquent celui de collision, nous devons trouver une politique d'accès au médium qui en profite et qui répond au maximum aux exigences de la qualité de service. A cette fin nous proposons à procéder par échange des besoins des nœuds pour donner à tout nœud au sein du même cluster une image claire sur les besoins exprimés par tous ses voisins et leurs permettre tous d'avoir la même décision et utiliser ce schéma claire de besoins au sein

d'un cluster pour accorder le nombre des slots répondants aux besoins exprimées au nœud prioritaire.

-Choix intra-nœud de l'AC prioritaire : utilisation des variables issues de la différenciation de service pour choisir l'AC prioritaire au niveau de chaque nœud.

-Candidature : transmission en robin round selon les identités des nœuds des trames issues de l'étape précédente du choix intra-nœud de l'AC prioritaire.

-Choix inter-nœud de l'AC prioritaire : en recevant toutes les trames de candidatures ; chaque nœud applique le même algorithme pour élire l'AC prioritaire parmi ceux désignés prioritaire au niveau de chaque nœud.

-Expédition : consiste à la diffusion des trames du nœud élu durant le TXOP spécifié et la mise en mode veille de tous les autres nœuds sauf nœud destinataire.

4.4.1 Mécanisme de différenciation de service

En utilisant le même principe de l'EDCA les priorités de l'utilisateur (UP) seront mappées aux catégories d'accès(AC) et nous aurons les mêmes quatre queues du QSTA du 802.11e (Fig. 4.8). Chaque nœud applique **l'algorithme de résolution de collision** inter-nœud qui n'est qu'une adaptation de l'EDCF (Enhanced Distributed Channel Access Function) de la norme ieee802.11e (paragraphe 4.3.2.2) pour avoir comme résultat l'**AC** prioritaire avec son **TXOP** qui forment ensemble la trame de candidature.

La différentiation de service (*diffserv*) au niveau de chaque nœud est accomplit à l'aide des *timers* de ***Backoff***, des **AIFS** et d'un compteur d'opportunités perdus (**Oprt)** ; on va essayer de garder le même schéma de *backOff* et de l'espace inter-trame pour implémenter la différentiation de service dans un environnement sans collision, pour ceci ces timeres ne vont pas induirent une transmission des donner en atteignant la valeur nulle mais juste une incrémentation du compteur d'opportunité perdu (Oprt) pour que l'ensemble sera transmis en candidature, la figure 4.3 illustre un tableau comparatif de l'EDCF du 802.11e et l'EDCF du DCC-MAC.

EDCF du 802.11e	EDCF du DDC-MAC
Collision externe	Tout droit de transmission perdu
Transmission avec succès	Candidature accepté
Emission de trames de données	Incrémentation du Oprt

Fig. 4.3 –Tableau comparatif de l'EDCF et du DCC-MAC

4.4.1.1 Acquisition du TXOP

La différentiation de service (*diffserv*) au niveau de chaque nœud est accomplit à l'aide du **backoff** et de l'espace inter-trame **AIFS** qui sera spécifique à chaque TC grâce au AIFSN :

$$AIFS[TC] = AIFSN[TC] \times aSlotTime + aSIFSTime \qquad (4.4.1)$$

Les valeurs des AIFSN seront ceux par défaut du 802.11e (Fig. 4.8), quand une TC aura **l'AIFS minimum** et le compteur d'opportunités perdu (**Oprt) maximum** au début d'une phase de candidature, ce nœud émettra sa demande de TXOP pour cette TC pour la prochaine phase de candidature ; en cas ou nous avons deux AC qui ont les mêmes valeurs pour le AIFS et le Oprt ; on choisira l'AC de priorité élevé

A chaque limite spécifique d'un slot [12], chaque EDCF détermine lesquelles des fonctions suivantes doit-elle performer :

— transmission de sa demande de candidature, Apres la phase de clusturing.

— Décrémentation du timer du backoff pour cette fonction d'accès, si le timer de backoff n'est pas nul après la période de l'AIFS qui n'est pas suivi par une candidature accepté

— Invocation de la procédure backoff à cause d'une collision interne ou à cause de la perte d'une opportunité de transmission qui va être considéré comme une collision externe

—incrémentation de la valeur du Oprt .après chaque perte d'une occasion de transmission à cause d'occupation de canal par une autre EDCF ou à cause d'utilisation du medium par des trames de contrôle d'autres phases

— ne rien faire pour cette fonction d'accès, si y'a pas de trame à transmettre dans la queue

Chaque EDCAF incrémente son compteur d'opportunités perdus (**Oprt)** si :

—y'a une trame prête à la transmission dans ce nœud, et

— Le timer du backoff pour cette EDCF a une valeur minimum dans le nœud pour cette phase de candidature, et

— l'initiation d'une séquence de transmission n'est pas permise à ce moment pour une EDCF de UP élevée

Chaque EDCAF invoque la procédure de backoff à cause d'une collision interne si :

— Y'a une trame en attente de transmission dans cet EDCAF, et

— la valeur du timer du backoff est nulle pour cette EDCAF, et

— l'initiation d'une transmission pour une EDCAF de Up plus élevés est permise à ce moment

4.4.1.2 Procédure du backoff

Chaque EDCAF doit maintenir l'état du variable CW[AC],qui sera initialisé à la valeur du paramètre CWmin[AC]. Après chaque transmission réussie, l' EDCAF reinitialize son CW[AC] à CWmin[AC]

La procédure du backoff sera lancée pour une EDCAF si une des évènements suivante se produit :

— une trame dans cette EDCAF doit être transmise mais elle n'en a pas le droit.

— la dernière tentative de transmission s'est bien passée The final transmission.

— la tentative de transmission entrée en collision avec une autre EDCAF d'un AC plus élevée.

4.4.2 Choix intra-nœud de l'AC prioritaire

Cette étape a comme objectif de déceler l'AC prioritaire de la phase de candidature suivante au niveau de chaque nœuds.

En appliquant l'algorithme de différentiation de service chaque nœud aura à chaque instant pour ces quatre AC les valeurs de *timers* de *Backoff* (**Tbkf[AC]**), des **AIFS[AC]** et des compteurs d'opportunités perdu (**Oprt[AC]**) . L'AC qui sera élu par le nœud pour émettre sa candidature est celle avec la valeur maximale du compteur d'opportunités perdu (**Oprt[AC]**) et en cas d'égalité de Oprt pour deux catégorie, on prendra celle avec le AIFS minimale si un des deux nœud et en état de décrémentation de son compteur de AIFS sinon on choisira celle avec le Tbkf minimale.

Par la fin de cet étape chaque nœud aura son AC candidate pour la phase de transmission suivante.

Algorithme intra-nœud de sélection de l'AC prioritaire du nœud

Tbkf[i] : timers de Backoff de l'AC numero i

AIFS[i]: valeur du timer de l'AIFS du Ac numero i

Oprt[i]) : compteur d'opportunités perdu du Ac numero i

Etat[i] : Etat du EDCAF du AC(I), 1 pour mode backoff ou 0 en décrémentation du AIFS

ACp: numero Ac candidate

```
Begin
ACp=: 3
For i= 0 to 2 do
//choix de l'AC avec le nombre maximum d'opportunités perdu
   If (Oprt[i] > Oprt[ACp]) then
     ACP:= i
   Else
       If (Oprt[i] = Oprt[ACp]) then
            //si nous avons deux AC avec la même valeur du Oprt, onchoisi celle en mode  décrémentation du AIFS.
          If ( Etat[i] > Etat[ACp] )then
            ACp:= i
          Else
             If ( Etat[i] = Etat[ACp]) then
                  //Si les deux AC sont en mode décrémentation du backoff, on choisi celle avec  le  Tbkf  minimal.
               If ( Etat[ACp] =1) then
                     begin
                      If (Tbkf[i] < Tbkf[ACp]) then
                         ACp:= i;
                     End
                //  si les deux AC sont en mode décrémentation du AIFS, on choisi celle avec le AIFS  minimale
                Else
                     if ( AIFS[i] < AIFS[ACp]) then
                        ACP:= I;
                Endif;
               Endif;
          Endif;
       Endif;
   Endif;
End.
```

4.4.3 Phase de Candidature

La candidature consiste à l'émission d'une demande d'allocation du medium pour un TXOP par un nœud pour une de ces TC (*Traffic Category*) qui sera choisi en se basant sur les résultat l'algorithme de différentiation de service.

Les identifiants des nœuds d'un cluster sont connus dans tous le cluster (présence de la table du nœud voisin issue de la phase de *clustering* au niveau de chaque nœud), ces identifiants vont être utilisés pour organiser l'émission des trames de candidature dans l'ordre de ces identités, la connaissance de l'ordre des identités de tous les nœuds de son cluster, va être utiliser pour réduire la taille du trame de candidature par élimination de l'identité de l'émetteur de cet trame. La trame de candidature doit contenir toutes les informations nécessaires pour élire le nœud le plus prioritaire ; ces informations sont :

-la catégorie d'accès candidate **AC**,

-le timers de Backoff de l'AC candidate (**Tbkf[AC]**) ;

-valeur du timer de l'AIFS du AC candidate (**AIFS[AC]**)

-compteur d'opportunités perdu du AC candidate (**Oprt[AC]**)

-Etat du EDCAF du AC candidate (**Etat[AC]**)

-le **TXOP** demandé.

-identité du nœud destinateur (**Dest**)

La figure 4.4 présente la forme de la trame de candidature.

AC	Oprt	Etat	AIFS	Tbkf	TXOP	Dest

Fig. 4.4 –format de la trame de candidature

À la fin de cette étape tous les nœuds du cluster auront un schéma détaillé des besoins de tout le cluster, ce schéma global va être utilisé d'une façon distribué pour allouer les ressources du cluster au nœud prioritaire

4.4.4 Choix inter-nœud de l'AC prioritaire

Les étapes précédentes nous ont permis d'avoir les même données sur l'état des besoins dans le cluster au niveau de chaque nœuds .Dans cette étape tous les nœuds du cluster appliquent un algorithme similaire à celui du choix de AC prioritaire intra-nœuds pour désigner le nœud prioritaire qui va émettre durant le TXOP demander les trame de l'AC indiqué dans sa candidature.

L'algorithme de choix de cette phase implémente les mêmes principes que celui du choix de AC prioritaire intra-nœuds, nous n'avons qu'a changer le AC prioritaire par le nœud prioritaire et à modifier le nombre d'itération au niveau de chaque cluster pour qu'il soit égale au cardinale de ce cluster.

En exécutant l'algorithme du Choix inter-nœud de l'AC prioritaire tous les nœuds du cluster sauront à qui sera consacré le médium et pour combien de temps pour l'étape d'émission suivante.

Nous présentons ci-dessous l'Algorithme inter-nœud de sélection du nœud prioritaire dans le cluster :

Algorithme inter-nœud de sélection du noeud prioritaire dans le cluster

Tbkf[i] : timers de Backoff du nœud numéro i

AIFS[i]: valeur du timer de l'AIFS du nœud numéro i

Oprt[i]) : compteur d'opportunités perdu du nœud numéro i

Etat[i] : Etat du EDCAF du AC(I), 1 pour mode backoff ou 0 en décrémentation du AIFS

Ndp: numéro du nœud prioritaire

Card(cluster): le nombre de noeud dans le cluster

```
Begin
Ndp=: card(cluster)
For i= 0 to card(cluster)-1 do
//choix du nœud avec le nombre maximum d'opportunités perdu
    If (Oprt[i] > Oprt[Ndp]) then
      NDP:= i
    Else
        If (Oprt[i] = Oprt[Ndp]) then
            //si nous avons deux AC avec la même valeur du Oprt, onchoisi celle en mode  décrémentation du AIFS.
          If ( Etat[i] > Etat[Ndp] )then
            Ndp:= i
          Else
             If ( Etat[i] = Etat[Ndp]) then
                  //Si les deux AC sont en mode décrémentation du backoff, on choisi celle avec  le  Tbkf  minimal.
               If ( Etat[Ndp] =1) then
                      begin
                       If (Tbkf[i] < Tbkf[Ndp]) then
                          Ndp:= i;
                      End
                 // si les deux AC sont en mode décrémentation du AIFS, on choisi celle avec le AIFS  minimale
                Else
                      if ( AIFS[i] < AIFS[Ndp]) then
                         NDP:= I;
                Endif;
             Endif;
          Endif;
        Endif;
    Endif;
End.
```

4.4.5 Étape d'Expédition

Dans cette étape le nœud élu se met en mode transmission et diffuse ses trames pendant le TXOP spécifié et la destination se met en mode réception, le reste des nœuds du cluster seront en mode veille pour économiser leurs énergie.

Si les nœuds appartenant à plus d'un cluster (nœud se trouvant à l'intersection des clusters) ne sont ni émetteur ni récepteur pour le cluster en cours durant cette étape, ils peuvent activer d'autre clusters auquel ils appartiennent comme ceci ne va pas causer de collision.

4.5 Conclusion

Nous avons présenté dans ce chapitre l'idée principale de notre protocole ainsi que les détails de toutes ses phases avec une argumentation de chaque proposition.

Dans ce qui suit nous allons simuler notre proposition pour pouvoir analyser ces apports et ses inconvénients.

Chapitre 5 : Évaluation des Performances

Sommaire

5.1- Introduction

Nous avons utilisé le simulateur NS2 (Network Simulator 2) [18, 37] pour l'évaluation des performances da la phase transmission de DCC-MAC dans un cluster supposé généré par l'algorithme de clustering que nous venons de proposer. Ce simulateur permet de créer différents types de topologies. Nous avons fait l'évaluation en comparant les performances de du DCC-MAC proposé par rapport à la fonction de de qualité de service EDCF définie par la norme 802.11e et réalisée par le laboratoire TKN [48].

Le choix de cette comparaison vient du fait que cette solution représente une amélioration du protocole 802.11e et du fait que 802.11e représente une référence de la qualité de service au niveau MAC.

5.2- Environnement et contexte de la simulation

5.2.1- Modèle de simulation

Le programme de simulation utilise Network Simulator dans sa version ns-3.33 [44] sous la version UBUNTU 10.4 de Linux,(Annex I) à Laquelle j'ai ajouté le module d'extension réalisée par le laboratoire de recherche TKN[48] pour pouvoir implémenter EDCF et lui apporter les changements nécessaire afin d'avoir notre protocole DCC-MAC.

La simulation de DDC-MAC s'est basé sur l'implémentation du ieee802.11e EDCAF du TKN [48] auquel on a fait du reverse ingeeniring (manuel) pour comprendre le rôle de chaque classe et variable, méthode et appel à fin de pouvoir faire les ajouts et les modifications appropriés pour avoir le DCC-MAC, à cette fin le site de Joshua Robinson [36] nous a été très utile et surtout le graphe des classes présenté par la figure 5.2 [38]ainsi que les travaux de Georg Lukas présenté sur son site web [50]

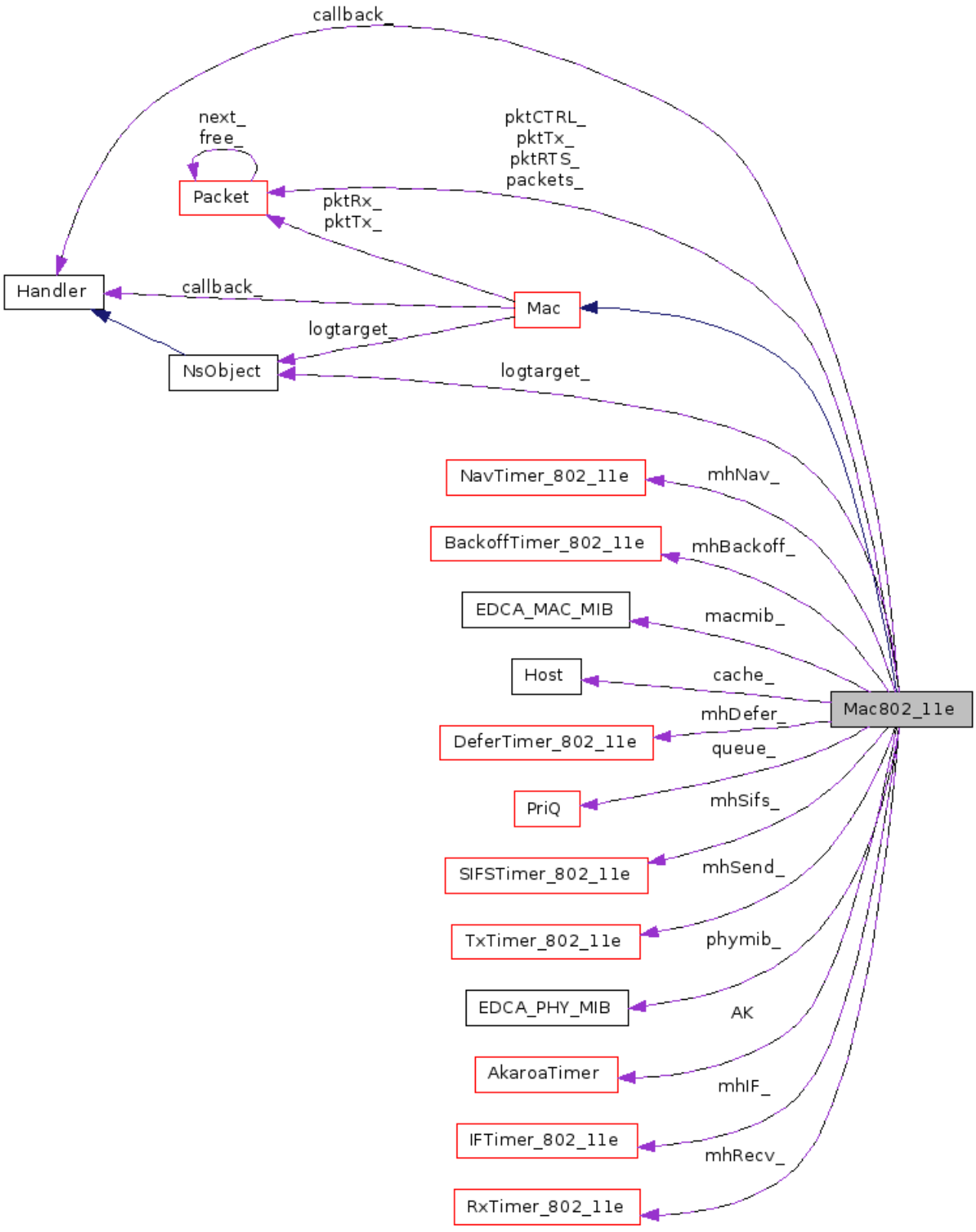


Fig. 5.1 – Graphe du classe du protocole 802.11e sous ns-2

5.2.2 Architecture simulée :

Comme le montre la figure suivante nous avons simulé un réseau Ad Hoc de sept Nœuds qui a toute les caractéristiques d'un cluster résultant de l'application de notre algorithme de clustering,

Le réseau simulé se compose de Sept Nœuds déposé comme le montre la Figure 5.2, la distance entre chaque deux nœuds est moins que 250 mètres qui représente le rang de propagation.

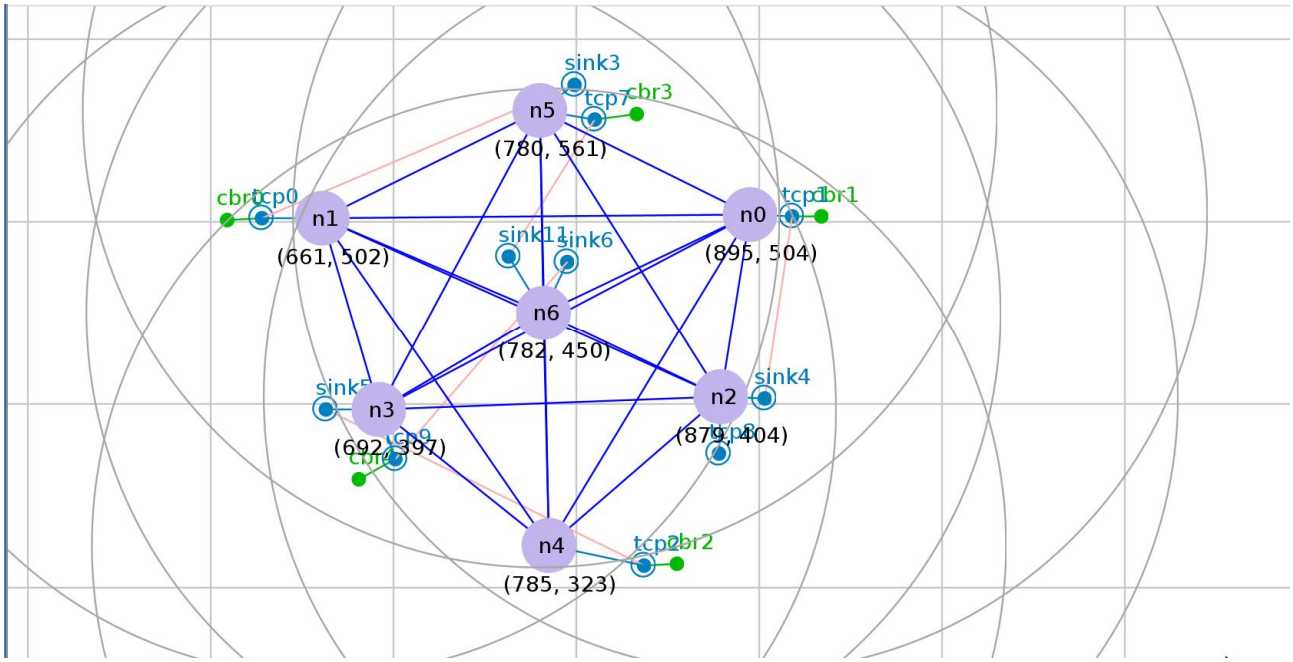


Fig. 5.2 – Architecture simulée

Pour créer le schéma de la figure précédente on a utilisé le code OTCL/TCL suivant sous NS2.33 :

```
#================================
# Prameters de simulation
#================================
set val(chan)   Channel/WirelessChannel    ;
set val(prop)   Propagation/TwoRayGround
; set val(netif)  Phy/WirelessPhy          ;
 set val(mac)    Mac/802_11e      ;
set val(ifq)    Queue/DTail/PriQ    ;
set val(ll)     LL                  ;
set val(ant)    Antenna/OmniAntenna  ;
set val(ifqlen) 50                   ;
 set val(nn)     7                   ;
 set val(rp)     DSDV                ;
set val(x)      545                 ;
set val(y)      545                 ;
set val(stop)   10.0                ;
Mac/802_11e set RTSThreshold_ 000
#================================
#       Initialization
#================================
#Définition d'un objet ns
set ns [new Simulator]
set topo       [new Topography]
$topo load_flatgrid $val(x) $val(y)
create-god $val(nn)
# Ouverture de fichier de suivi de trace
set tracefile [open out.tr w]
$ns trace-all $tracefile
#Overture de NAM trace file
set namfile [open out.nam w]
$ns namtrace-all $namfile
$ns namtrace-all-wireless $namfile $val(x)
$val(y)
set chan [new $val(chan)];#Create wireless
channel
#================================#
Paramètres des noeuds
#================================
$ns node-config -adhocRouting  $val(rp) \
            -llType        $val(ll) \
            -macType       $val(mac) \
            -ifqType       $val(ifq) \
            -ifqLen        $val(ifqlen) \
            -antType       $val(ant) \
            -propType      $val(prop) \
            -phyType       $val(netif) \
            -channel       $chan \
            -topoInstance  $topo \
            -agentTrace    ON \
            -routerTrace   ON \
            -macTrace      ON \
            -movementTrace OFF
#================================
#       Définition  des Noeuds
#================================
set n0 [$ns node]
$n0 set X_ 895
$n0 set Y_ 504
$n0 set Z_ 0.0
$ns initial_node_pos $n0 20
set n1 [$ns node]
$n1 set X_ 661
$n1 set Y_ 502
$n1 set Z_ 0.0
$ns initial_node_pos $n1 20
set n2 [$ns node]
$n2 set X_ 879
$n2 set Y_ 404
$n2 set Z_ 0.0
$ns initial_node_pos $n2 20
set n3 [$ns node]
$n3 set X_ 692
$n3 set Y_ 397
$n3 set Z_ 0.0
$ns initial_node_pos $n3 20
set n4 [$ns node]
$n4 set X_ 785
$n4 set Y_ 323
$n4 set Z_ 0.0
$ns initial_node_pos $n4 20
set n5 [$ns node]
$n5 set X_ 780
$n5 set Y_ 561
$n5 set Z_ 0.0
$ns initial_node_pos $n5 20
set n6 [$ns node]
$n6 set X_ 782
$n6 set Y_ 450
$n6 set Z_ 0.0
$ns initial_node_pos $n6 20
#================================
#       Définition des Agents
#================================
set tcp0 [new Agent/TCP]
$tcp0 set class_ 1
$tcp0 set prio_ 3
$ns attach-agent $n1 $tcp0
set sink3 [new Agent/TCPSink]
$ns attach-agent $n5 $sink3
$ns connect $tcp0 $sink3
set tcp1 [new Agent/TCP]
$tcp1 set class_ 0
$tcp1 set prio_ 2
$ns attach-agent $n0 $tcp1
set sink4 [new Agent/TCPSink]
$ns attach-agent $n2 $sink4
$ns connect $tcp1 $sink4
set tcp2 [new Agent/TCP]
$tcp2 set class_ 4
$tcp2 set prio_ 1
$ns attach-agent $n4 $tcp2
set sink5 [new Agent/TCPSink]
$ns attach-agent $n3 $sink5
$ns connect $tcp2 $sink5
set tcp7 [new Agent/TCP]
$tcp7 set class_ 5
$tcp7 set prio_ O
$ns attach-agent $n5 $tcp7
set sink11 [new Agent/TCPSink]
$ns attach-agent $n6 $sink11
$ns connect $tcp7 $sink11
set tcp9 [new Agent/TCP]
$tcp9 set class_ 3
$tcp9 set prio_ 3
$ns attach-agent $n3 $tcp9
set sink6 [new Agent/TCPSink]
$ns attach-agent $n6 $sink6
$ns connect $tcp9 $sink6
$ns color 1 black
$ns color 2 yellow
$ns color 7 yellow
$ns color 0 Red
$ns color 9 black
$tcp1 set fid_ 1;
$tcp1 set fid_ 2;
$tcp7 set fid_ 7;
$tcp9 set fid_ 9;
$tcp0 set fid_ 0;
#================================
#       Définition des Applications
#================================
set cbr0 [new Application/Traffic/CBR]
$cbr0 attach-agent $tcp0
$cbr0 set packetSize_ 1000
$cbr0 set rate_ 1.0Mb
$cbr0 set random_ null
$ns at 1.0 "$cbr0 start"
$ns at 10.0 "$cbr0 stop"
set cbr1 [new Application/Traffic/CBR]
$cbr1 attach-agent $tcp1
$cbr1 set packetSize_ 1000
$cbr1 set rate_ 1.0Mb
$cbr1 set random_ null
$ns at 1.0 "$cbr1 start"
$ns at 10.0 "$cbr1 stop"
set cbr2 [new Application/Traffic/CBR]
$cbr2 attach-agent $tcp2
$cbr2 set packetSize_ 1000
$cbr2 set rate_ 1.0Mb
$cbr2 set random_ null
$ns at 1.0 "$cbr2 start"
$ns at 10.0 "$cbr2 stop"
set cbr3 [new Application/Traffic/CBR]
$cbr3 attach-agent $tcp7
$cbr3 set packetSize_ 1000
$cbr3 set rate_ 1.0Mb
$cbr3 set random_ null
$ns at 1.0 "$cbr3 start"
$ns at 10.0 "$cbr3 stop"
#Définition des applications CBR Application
over TCP connection
set cbr4 [new Application/Traffic/CBR]
$cbr4 attach-agent $tcp9
$cbr4 set packetSize_ 1000
$cbr4 set rate_ 1.0Mb
$cbr4 set random_ null
$ns at 1.0 "$cbr4 start"
$ns at 10.0 "$cbr4 stop"
#================================
#       Termination
#================================
#définition de la procedure  'finish'
proc finish {} {
   global ns tracefile namfile
   $ns flush-trace
   close $tracefile
   close $namfile
   exec nam out.nam &
   exit 0
}
for {set i 0} {$i < $val(nn) } { incr i } {
   $ns at $val(stop) "\$n$i reset"
}
$ns at $val(stop) "$ns nam-end-wireless
$val(stop)"
$ns at $val(stop) "finish"
$ns at $val(stop) "puts \"done\" ; $ns halt"
$ns run
```

5.2.3- Paramètres de simulation

Les valeurs de DIFS, PIFS, SIFS et SlotTime sont:

SlotTime	20µs
SIFS	10µs
PIFS	30µs
DIFS	50µs

Les valeurs utilisées dans la simulation sont d'après [27] et on les a gardé sans modification pour DCC-MAC :

TC	**0**	**1**	**2**	**3**
AIFSN	2	2	3	7
CWmin	7	15	31	31
CWmax	15	31	1023	1023
TXOPlimit	3.008ms	6.016 ms	0	0

Les paramètres de configuration de DCC- MAC sont comme suit :

Paramètres de simulation	**Taille/ Valeur**
RTS (Trame de candidature pour DCC-MAC)	20 bytes
CTS (éliminé pour DCC-MAC)	14 bytes
DATA	512 bytes
ACK	14 bytes
Propagation delay	5µs
Transmission Range	250m
Data rate of control and data packets	1Mb
SIFS	8µs
DIFS	16µs

5. 3- Résultats de simulation

Après avoir exécuté les simulations avec différents nombres de flux, nous avons eu un certain nombre de résultats sur lesquelles on a appliqué les scripts AWK [35] approprié sur les fichiers out.tr résultants pour en extraire les données ciblés et on a utilisé par la suite le logiciel gratuit de génération des graphes Gnuplot [48] dans ça version 4.4.0 pour représenter nos résultats sous forme de graphes comme le montre les figures que nous allons présenter et analyser.

5.3.1- Pourcentage des paquets perdus

La figure 5.3 présente le pourcentage des paquets de haute (*TC numéro 0*) et de basse priorité (TC numéro 3) perdus en utilisant DCC-MAC ainsi que l'EDCF.

Ceci permet de montrer que le pourcentage des paquets de haute priorité ainsi que celui des paquets de basse priorité, est plus faible dans le cas du DCC-MAC par rapport à celui de la fonction EDCF.

Ce résultat peut être interprété par l'absence des collisions et du l'algorithme de choix de AC prioritaire Intra-nœud. En effet, des valeurs plus grandes de **Oprt** (*compteur d'opportunités perdu du AC candidate*) sont attribuées aux trames dans les files d'attente suivant la priorité d'utilisateur et le temps d'attente dans la file.

Le cas de la fonction EDCF, les files d'attente sont toujours en compétition pour avoir l'accès au canal, ce qui augmente le nombre de collision et par conséquent le taux de perte de paquets.

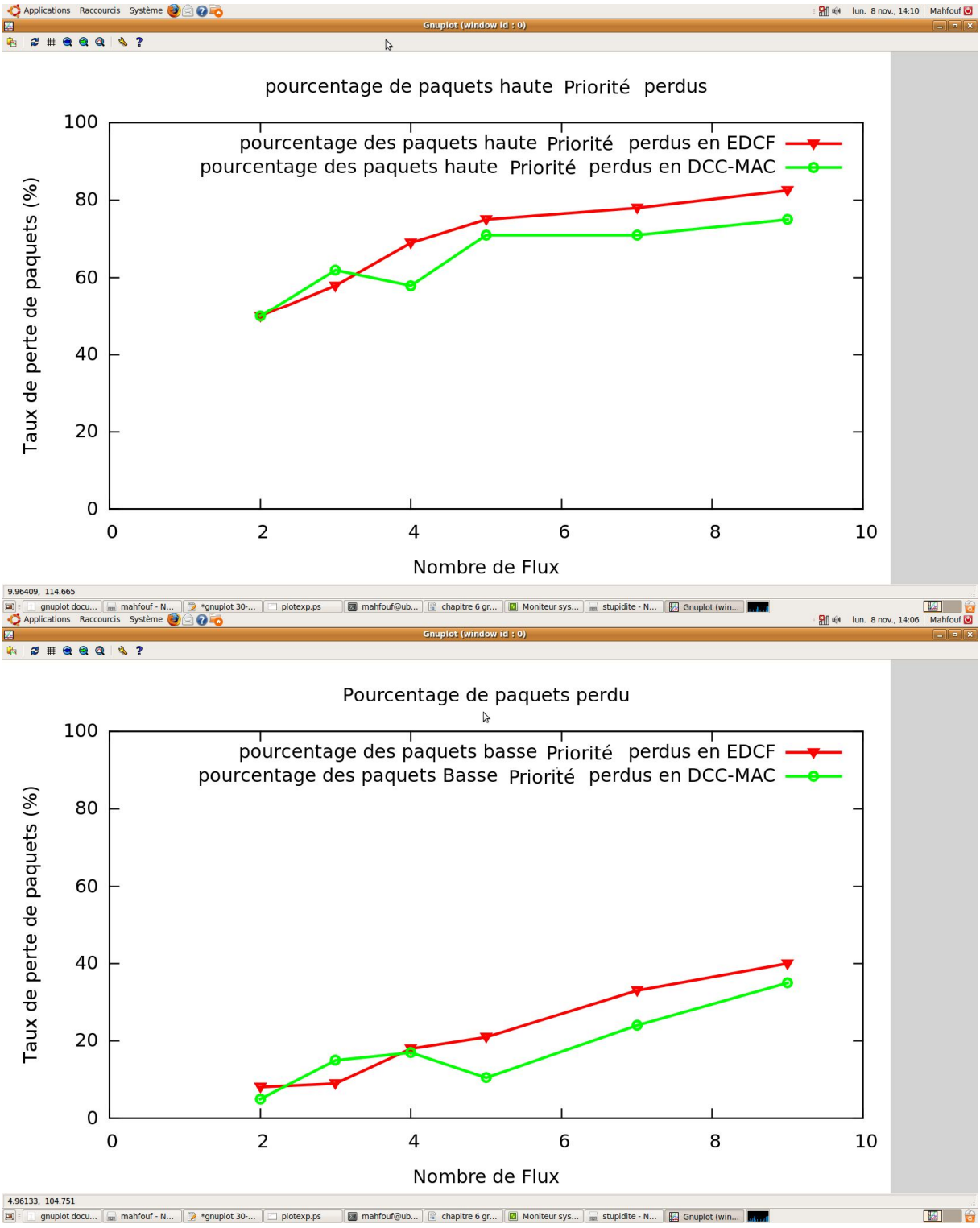


Fig. 5.3 – Pourcentage de paquets perdu

5.3.2-Nombre de paquets reçus

En terme de gain, la figure 5.4 donne le nombre de paquets de haute et de basse priorité reçus dans les deux protocoles : DCC-MAC et la fonction EDCF. Cette figure montre d'une part, que le protocole DDC-MAC donne de meilleurs résultats pour l'architecture simulé en ce qui concerne le nombre de paquets de haute priorité reçus. A titre d'exemple, lorsqu'on active neuf flux, le gain est de 26% par rapport à celui de la fonction EDCF. D'une autre part, le nombre de paquets de basse priorité reçus, est lui aussi meilleur avec DCC-MAC. Ainsi, nous pouvons constater deux phases dans les graphes représentés par la figure 5.4, la première phase concerne le nombre de flux inferieure à 6 et la deuxième phase concerne le cas où nous avons plus de six flux.

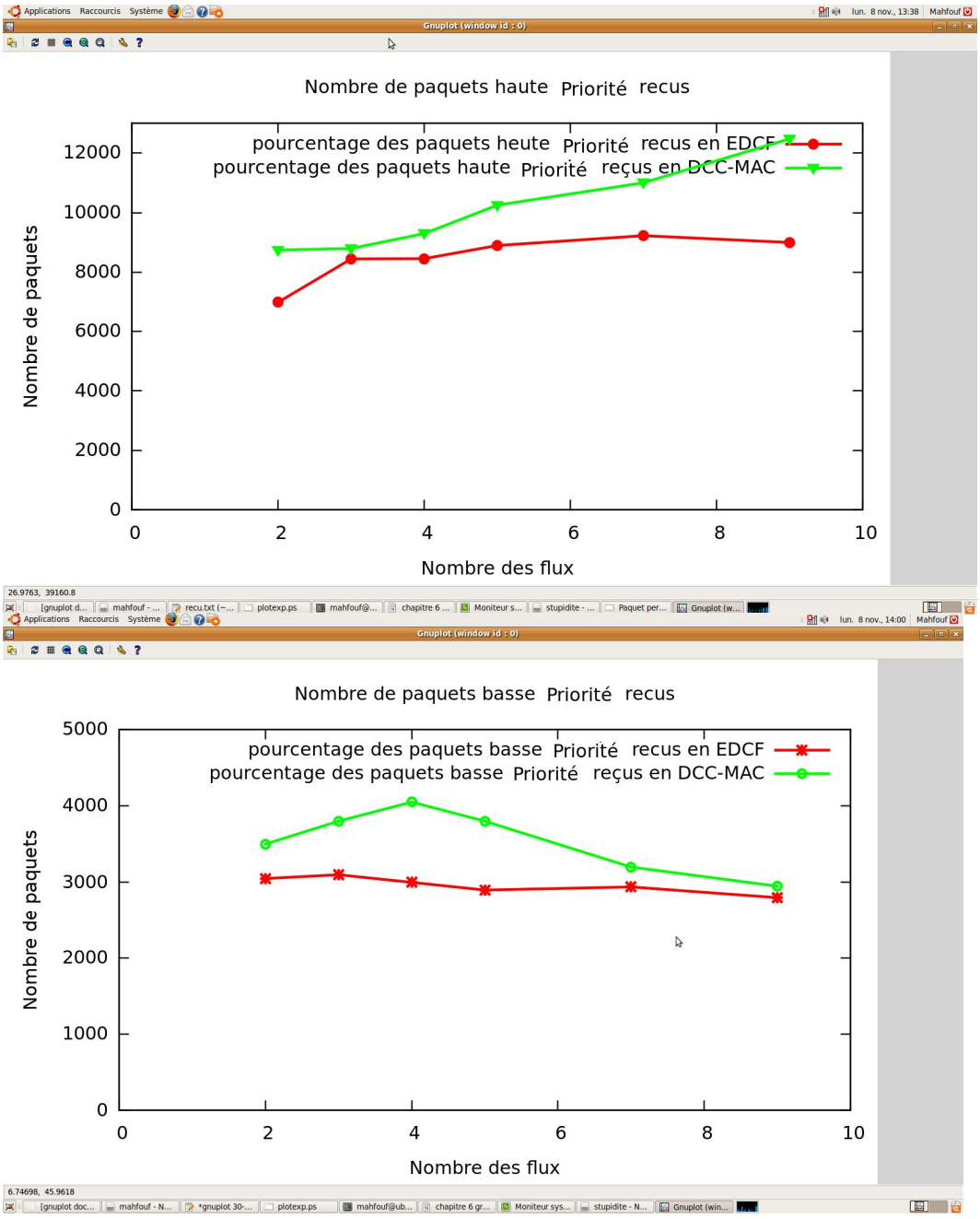


Fig. 5.4 –Nombre de paquets HP et BP reçus

Dans la première phase, le nombre de paquet Basse Priorité reçus est un petit peu plus élevé dans le cas de DCC-MAC, cependant cette différence commence à diminuer au fur et à mesure après l'activation de 6 flux. Cela est dû au fait, qu'après cette valeur (seconde phase), le nombre de paquets dans les files d'attente Haute Priorité augmente. Ainsi, DCC-MAC accorde plus de TXOP au paquet des catégories 0 (de plus haute priorité), ce qui ralentit par conséquent les paquets de basse priorité, qui seront moins servis.

5.3.3- Délais de Latence

Les délais de latence offerts par DCC-MAC et EDCF sont présentés par la figure 5.5. Cette figure trace les graphes des délais de bout en bout pour les paquets de haute et de basse priorité et montre que le délai de latence pour les paquets de haute priorité dépend essentiellement du nombre de flux dans le réseau. Cependant, la fonction EDCF offre de meilleurs résultats au fur et à mesure que le nombre de flux augmente .

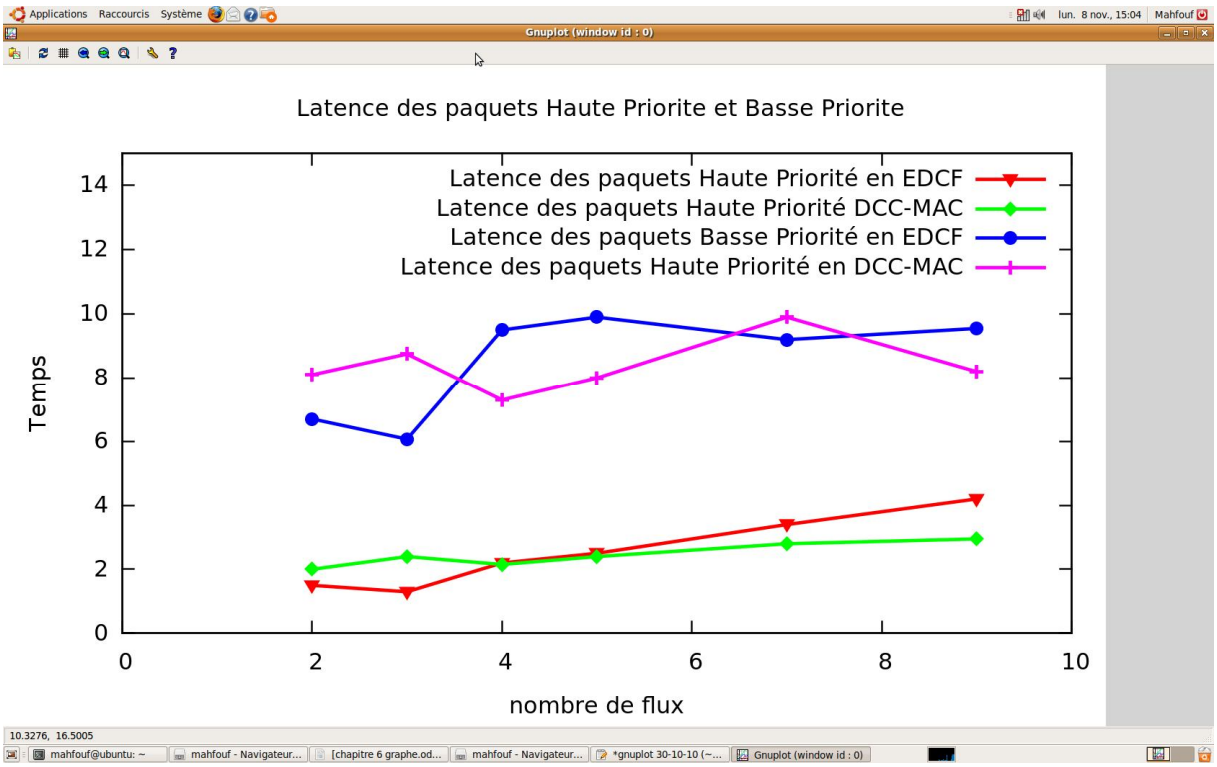


Fig. 5.5– Latence des paquets Haute Priorité et Basse Priorité

5.3.3- Débit et Paquets perdus

Les nombre de paquet perdu par DCC-MAC et EDCF sont présentés par la figure 5.6. Cette figure trace les graphes de nombre total des paquets perdu par seconde pour une simulation de 5 flux et avec des débit changeants et montre que la perte des paquets dépends du débit et que DCC-MAC donne des résultats insatisfaisant, et sont de plus en plus mauvaise en augmentant le débit. Cependant, la fonction EDCF offre de meilleurs résultats au fur et à mesure que le débit augmente .

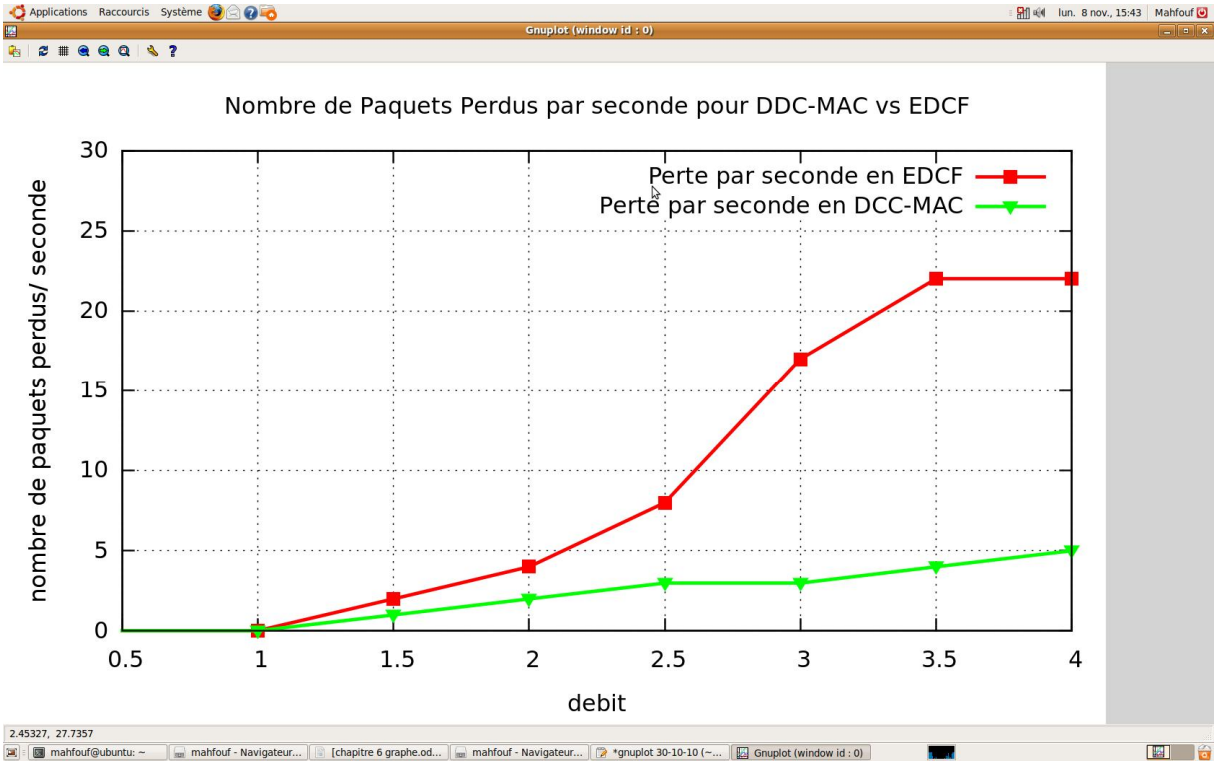


Fig. 5.6– Nombre de Paquets perdus suivant le débit

5.4- Conclusion

Notre évaluation était faite sur le simulateur NS-2 et le module EDCF de TKN [50], et d'après les documents qu'on a consulter sur les simulateurs et les résultats de simulation [20]; personnellement je ne fait vraiment pas confiance au résultats de simulation car un petit omis d'un petit facteur dont on a pas d'information sur sa valeur par défaut peut conduire à des résultats complètement divergente du réel,

Mais voyons les résultats qu'on a eu et qui s'accorde logiquement avec ce qu'on attend de notre protocole, on peut dire que DCC-MAC améliore les performances de QOS et ce pour l'architecture et avec les paramètres proposés,

Mais on a remarqué et ça reste sous test que DCC-MAC avec d'autre circonstance réduit d'une manière très importante le throughput ce qui fait qu'il n'est utile que dans des circonstance bien spécifié là ou la perte de paquet est non tolérée mais le throughput n'est pas critique.

On doit aussi mentionner que la partie clustering de notre protocole n'a pas été simulée ni modulée , c'est juste une proposition qui parait logique et on a basé la phase transmission sur l'existence d'une architecture résultante de notre algorithme de clustering , mais ça ne déni pas l'existence d'es architecture similaire dans l'industrie comme y'a aussi les problèmes de QOS dans ce domaine mais pas en se basant sur les priorité d'utilisateur mais sur l'importance de l'information issue des transmetteurs .

ANNEXE I: Simulation des Protocoles Ad Hoc

Sommaire

I.1 Introduction

En raison des exigences demandées par les protocoles *ad hoc* (en performances et en temps), de la complexité de mise en œuvre et de la réduction des coûts d'un tel système, il est judicieux d'étudier son comportement avant son déploiement sur le terrain afin de comprendre, régler et ajuster les éventuels paramètres influents du système. La simulation est une méthode flexible et efficace et souvent la seule disponible pour effectuer des études comparatives et d'optimisation et pour établir les spécifications détaillées [20]. Elle permet donc de tester à moindre coût les nouveaux protocoles et d'anticiper les problèmes qui pourront se poser ultérieurement afin d'implémenter la technologie la mieux adaptée aux besoins. Elle joue un rôle très important durant toutes les phases d'ingénierie et de conception d'un tel système, qu'il soit de communication ou autre (aéronautique, mécanique....) :

- la phase d'étude des protocoles et algorithmes,

- la phase de mise en en œuvre, de prototypage virtuel et d'implémentation,

- la phase de réalisation et de test.

La simulation joue également un rôle important dans la phase d'établissement des spécifications détaillées des sous-systèmes, et de la vérification de différents paramètres indépendamment les uns des autres ou l'influence des uns sur les autres. Elle permet aussi de visualiser les résultats sous la forme de valeurs numériques ou de graphes pour faciliter l'analyse et l'interprétation.

I.2 Méthodes et outils de simulation des protocoles ad hoc

Les performances d'un système de communication peuvent être évaluées en utilisant l'une des trois principales méthodes [20]:

- La méthode de modélisation analytique basée sur les formules mathématiques pour créer et simplifier le modèle traduisant le comportement et intégrant les paramètres du système. Avec ces méthodes (chaînes de Markov pour les accès aux ressources, files d'attente pour les commutateurs, réseaux de files d'attente pour les réseaux, réseau de Pétri pour la synchronisation et le temps réel,...), il est extrêmement difficile d'évaluer les performances d'un système de communication complexe.

- La méthode de prototypage physique et de mesure. Cette méthode est précise et utile, mais coûteuse et obligatoire avant chaque commercialisation d'un système.

- La méthode de simulation permet de modéliser le système avec un niveau de granularité variable. C'est la seule alternative technologique lorsque le système à étudier est difficile à déployer physiquement.

Cette classification n'implique pas que les trois méthodes soient mutuellement exclusives. En effet, une meilleure approche est souvent une combinaison entre chacune des trois méthodes. L'avantage de l'utilisation des techniques de simulation pour évaluer un tel système de communication par rapport à l'utilisation des deux autres méthodes est de traduire d'une manière plus réaliste et plus rapide le comportement du système à évaluer, car il est obtenu à partir d'une modélisation exécutable permettant une simulation de l'architecture opérationnelle considérée. Le système réel est modélisé comme un ensemble d'activités parallèles indépendantes mais dont le déroulement est synchronisé. Chaque activité (*flot de contrôle*) peut manipuler des données (*flot de données*) et les transférer à une autre activité qui en prend le contrôle. La modélisation des activités et les données sont propres à chaque outil.

La méthode de modélisation, qu'elle soit analytique ou par simulation, constitue l'outil de base pour résoudre les problèmes dans toutes les disciplines de la science et de l'ingénierie.

De nombreux outils de simulation à évènements discrets sont utilisés pour l'évaluation de performances des systèmes communicants (

NS2, GloMoSim, OMNeT++, JavaSim, SSFNet-Java and SSFNet-C++)

, [18].

I.3 Les différents processus de la simulation

Les premières simulations (simulation des niveaux d'ondes) ont débuté avec l'invention des ordinateurs à usage civil (fin des années 1940), qui ont été premièrement utilisés pour simuler le comportement des systèmes de contrôle dans les armes et les avions. Même si quelques 'supers ordinateurs' demeurent obligatoires pour des simulations très importantes, le développement et la progression des ordinateurs personnels en terme de vitesse et de capacité mémoire, et l'abaissement des coûts ont permis leurs utilisations dans des applications de simulations numériques.

Dans le cas d'un simulateur à évènements discrets (système décrit par des variables d'états discrètes), plus les intervalles de temps entre évènements sont petits et plus d'évènements seront générés sur l'échéancier[1] donc plus la simulation sera précise. Néanmoins, le temps de calcul sera d'autant plus long. La figure 7.1 illustre le processus complet de la simulation d'un système : la précision et l'exhaustivité des résultats de simulation dépendent des paramètres d'entrée/sortie du simulateur et par conséquent du choix du simulateur le plus adapté. Par contre, la pertinence des résultats dépend du choix des paramètres de la simulation (nombre de paquets, files d'attentes, temps, nombre de nœuds,..).

[1] File d'évènement, chaque évènement possède une date plus un certain nombre d'attributs. Lorsqu'il est traité, un nouvel événement est éventuellement inséré plus tard dans l'échéancier.

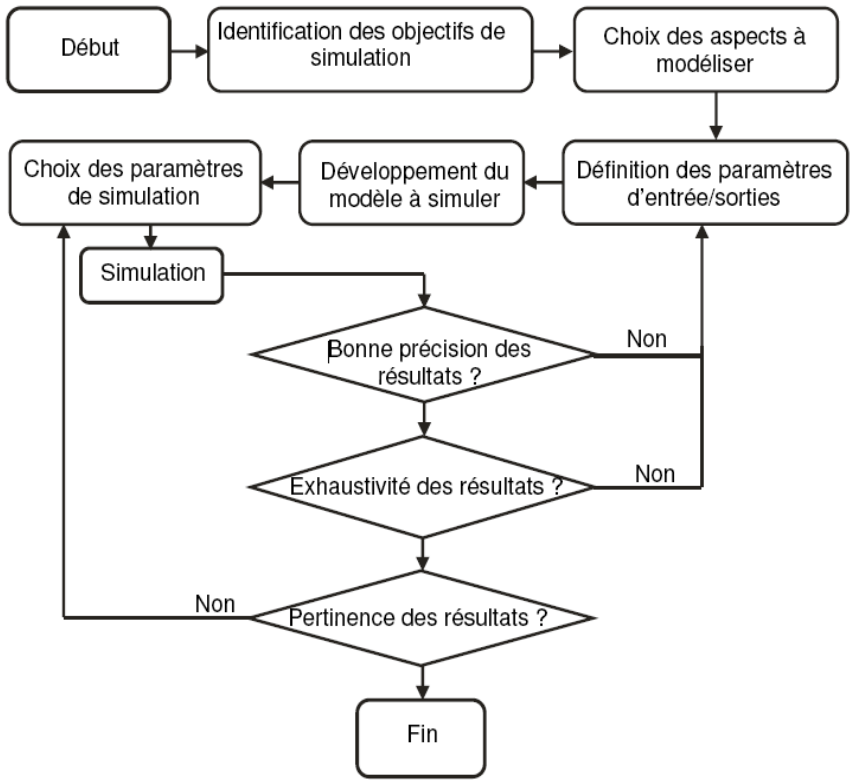


Fig. I.1 Processus d'une simulation.

Après avoir vu les différentes méthodes utilisées pour l'étude de performances, ainsi que les étapes utiles à la simulation d'un réseau sans fil, nous allons présenter le simulateur **NS-2**, que nous avons utilisé pour étudier notre proposition

I.4 Logiciel Network Simulator NS-2

I.4.1 Introduction

NS-2 [45] est un outil logiciel de simulation libre à code source ouvert et à évènements discrets permettant l'étude, la conception et la gestion des protocoles pour les réseaux informatiques. Il a été développé à partir de méthodes de conception orientées objets dans le projet *VINT* [46] associant plusieurs centres de recherche comme *AT&T research institute* à *Berckeley (ACIRI), Xerox PARC* et *Sun Microsystems*. ***NS-2*** contient des librairies pour la génération des fonctions (topologie, trafic, routage, *MAC, LLC*,...) et des outils graphiques pour faciliter l'interprétation (***Xgraph***) [44] et la visualisation (*network animator NAM*) [39] des résultats.

Le simulateur ***NS-2*** dans sa version actuelle est particulièrement bien adapté aux réseaux à commutation de paquets et à la réalisation de simulations de réseaux de petite taille. Il contient les fonctionnalités nécessaires pour l'étude des méthodes d'accès au médium, des algorithmes de routage point à point ou multipoint, des protocoles de transport, de session, de réservation de ressources, des protocoles d'application comme *HTTP* (*HyperText Transfer Protocol*). Cependant, il ne contient pas toutes les fonctionnalités nécessaires de la couche physique telles que les modèles de propagation (seuls les modèles de propagation dans l'air sont prévus) et les supports de transmission (seuls les liens filaires et les liens radio sont prévus). Le Tableau 5 donne les principaux composants disponibles pour chaque couche et par catégorie disponible dans ***NS-2***. L'ensemble de ces capacités utilisées conjointement ont permis l'étude des différents mécanismes au niveau de différentes couches de l'architecture réseau et font de NS-2 un standard reconnu par la communauté scientifique pour échanger les résultats et scripts de simulation entre les chercheurs [40].

Application	Web, FTP, Telnet, Générateur de Trafic (Constant Bit Rate CBR,Exponentiel, Pareto, Real Audio).
Couche Transport	Unicast TCP (Transmission Control Protocol) et UDP (User Datagram Protocol), Multicast SRM (Scalable Reliable Multicast), RTP (Real-time Transfer Protocol)
Couche Réseau	Routage statique et dynamique unicast et multicast (vecteur de distance DSR, AODV)
Couche Liaison de Donnée	CSMA/CD, CSMA/CA, liaisons point à point, MAC 802.11. LLC(ARP).
Couche Physique	Médium Filaire, Sans Fil et Satellite (Trafic, topologie du réseau, mobilité, model de propagation).
Gestion des files d'attente	RED, DropTail, Token bucke

Fig I.2 : Principaux protocoles et modèles disponibles sous NS-2

I.4.2 Concepts de base

Le simulateur ***NS-2*** permet à l'utilisateur de définir un réseau et de simuler des communications entre les nœuds de ce réseau. Il est écrit en **C++** et interfacé via une interface textuelle (interpréteur) qui utilise le langage de commande ***OTCL*** (*Object Tools Command Language*) dérivé du langage ***TCL*** (*Tools Command Language*) [41]. C++ sert à décrire le fonctionnement interne des composants de la simulation (définir les classes). L'outil *OTCL* fournit les moyens nécessaires (fonctionnalités orientées objet) pour contrôler les conditions et le scénario de la simulation. *OTCL* permet également de décrire le comportement de chaque composant du réseau à simuler tel que les caractéristiques physiques du réseau (la topologie par exemple), les protocoles, les communications qui peuvent avoir lieu entre les nœuds du réseau, le scénario temporel de la simulation, les dimensions du réseau. A chaque exécution d'une simulation, l'interpréteur *TCL* effectue l'analyse syntaxique du script de simulation et appelle ensuite la fonction C++ correspondant à chaque commande *TCL*. Notons également que le *TCLCL* permet aux objets et variables d'apparaître et d'être utilisés par les deux langages C++ et *OTCL*. Le rôle du script textuel de simulation (*script.tcl*) est d'indiquer la topologie du réseau, d'activer les traces aux endroits spécifiés et de provoquer des évènements particuliers à des instants donnés.

Pour définir l'architecture et la topologie du réseau à simuler, les classes ***Node***, ***Link*** et ***Packet/Header*** sont utilisées pour modéliser les nœuds qui constituent le réseau et les arcs d'un graphe pour relier ces différents nœuds entre eux (liens entre nœuds) et les systèmes de transmission. Dans le langage ***OTCL***, la classe ***Node*** est composée d'une collection de classificateurs (***classifier***) et d'agents (***agent***). Les classificateurs servent pour le démultiplexage et la redirection des paquets (*Adress classifier* et *Port classifier*) comme le montre la figure I.2. Par contre, les agents représentent des comportements, par exemple des applications ou des protocoles pour la génération et le traitement des paquets, l'adresse locale et de destination. La classe ***Packet/Header*** est utilisée pour la gestion des paquets. Lorsqu'un paquet arrive sur un nœud, le classificateur examine et vérifie les champs du paquet (y compris l'adresse de destination). Si le paquet est destiné à ce nœud, il passe ensuite au classificateur de port qui va le diriger vers le bon agent. Les paquets qui ne sont pas destinés au nœud en question sont soit supprimés soit transférés vers la bonne interface de sortie en utilisant les agents de routage.

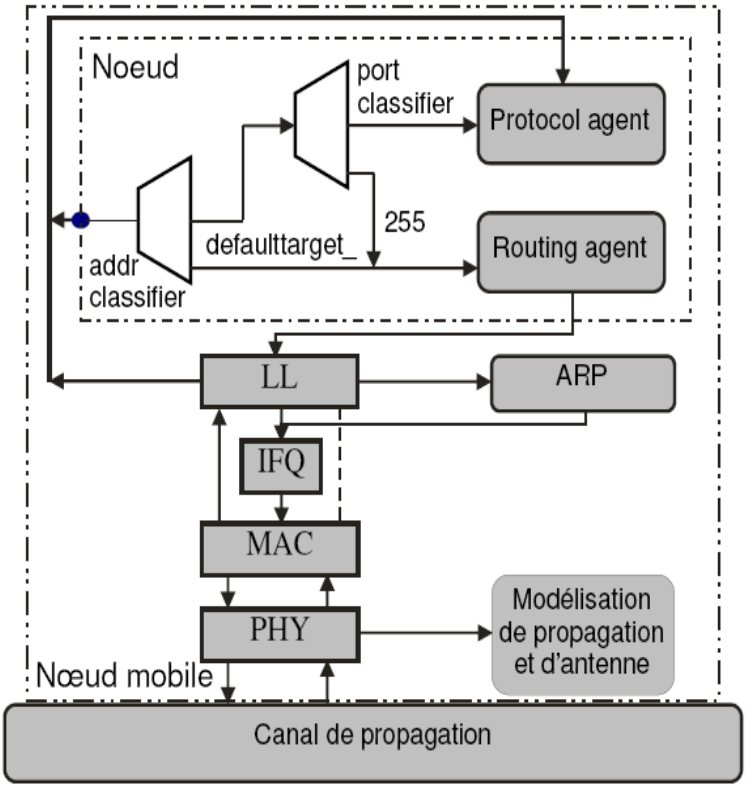


Fig. I.3 : Structure d'une liaison sans fil dans NS-2.

Une application *NS-2* se compose de deux éléments fonctionnels : un interpréteur et un moteur de simulation :

– Le moteur de simulation effectue les calculs qui sont applicables au modèle préalablement construit par l'utilisateur via l'interpréteur. Pour la création des objets de modèle de simulation *NS*, l'utilisateur crée un nouvel objet via *OTCL* qui va être interprété et cloné en un objet compilé correspondant dans le simulateur.

–L'interpréteur des résultats de simulation, est utilisé pour l'exploitation et l'interprétation des résultats de simulation *NS-2* et prévoit deux procédés pour extraire les données de la simulation :

- la **trace** qui est un fichier texte structuré en lignes et qui enregistre les changements d'états d'un paquet. Les changements des valeurs des variables peuvent être également tracés dans des fichiers de traçage *TacedInt* et *TracedDouble* dérivés de la classe de base *TracedVar*.

- Le **moniteur** qui insère des sondes (*snoop*) dans la topologie du réseau pour faire remonter les informations d'état du réseau au point d'assemblage des informations qui est le moniteur. Ce dernier peut également faire des calculs sur différentes grandeurs relatives au lien tel que le nombre de paquets ou d'octets arrivés.

I.4.3 Utilitaire NAM

Pour visualiser, animer et interpréter les données fournies à travers le fichier *trace* et donner un compte-rendu graphique, *NS-2* emploie l'outil d'animation ***NAM*** (*Network AaniMator*) basé sur le langage ***TCL/TK*** (*Tool Command Language/ToolKit*) qui est une extension du langage *TCL* pour la gestion graphique [42]. *NAM* permet également de donner une représentation graphique du réseau décrit dans le fichier de simulation TCL tout en animant les liens entre les nœuds et la circulation des données et les informations de la gestion du réseau entre les différents nœuds du réseau. Le modèle théorique du *NAM* a été non seulement créé pour lire un large ensemble de données d'animation, mais aussi suffisamment extensible pour être utilisé quelque soit le type de réseau simulé (fixe ou mobile ou mixte), ce qui permet de visualiser tout type de situation possible.

I.4.4 Utilitaire Xgraph

Xgraph est un autre utilitaire utilisé par *NS-2* et qui permet lui aussi de fournir un compte rendu graphique, mais cette fois-ci sous forme de courbes statistiques. Les formats de données acceptés en entrée sont de type deux dimensions (x et y). Les valeurs dans chaque ligne sont séparées par des espaces ou des colonnes, et les données peuvent être à deux ou à plusieurs colonnes.

I.4.5 Classes C++ du Simulateur

Comme nous l'avons précisé précédemment, *NS-2* est composé de plusieurs classes structurées sous une forme arborescente. Ces classes sont utilisées par le simulateur pour le fonctionnement de ses composantes. Les classes visibles au niveau de l'interpréteur comprennent une déclaration dans la classe *TclClass* qui est la racine de toutes les autres classes à la fois dans l'arborescence compilée et interprétée. Le nom de chaque classe correspond toujours à celui utilisé dans le code source *C++* de *NS-2*. La

figure I.4 , montre l'arborescence de dérivation des classes compilées *C++* du simulateur[45].

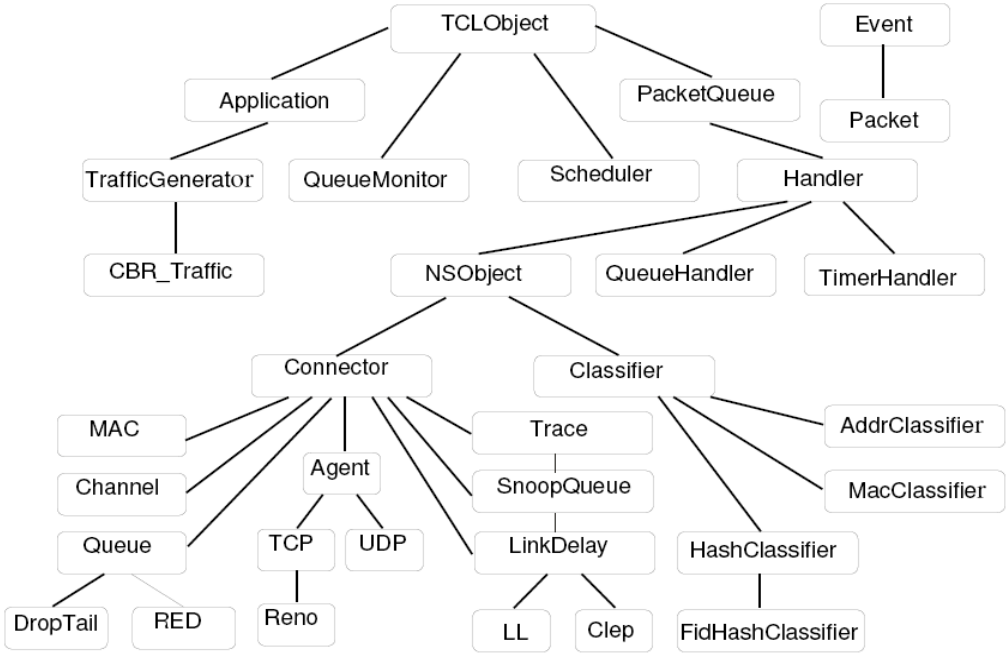


Fig. I.4 : Arborescence des classes du simulateur NS-2.

I.4.6 Ajout d'éléments et modification de NS-2

Comme nous l'avons déjà annoncé, *NS-2* est un simulateur dont le code source est libre et par conséquent extensible (possibilité de modifier la source et de la recompiler). Pour modifier le comportement d'objets existants ou rajouter des nouveaux objets, il est donc nécessaire de modifier le code source *C++* qui réalise l'implantation de l'objet en question ou d'étendre les fonctionnalités de l'interpréteur *OTCL* (fichier *API OTCL* dans *NS-2* : *ns-lib.tcl*).

Le tutorial *NS-2* de Marc Greis [43] donne la méthodologie avec un exemple d'ajout de nouveaux protocoles à *NS-2*. La méthode utilisée pour ajouter des fonctionnalités à NS-2 dépend du niveau protocolaire du protocole à implémenter. Lorsque le protocole est de niveau IP ou au-dessus, il est codé sous forme d'un agent (classe dérivée de la classe agent). Si le nouveau protocole est de niveau inférieur à IP, il doit être codé comme une classe dérivée de la classe racine (la classe *NsObjec*t). D'une manière plus générale, ajouter un nouvel élément à *NS-2* nous conduit aux étapes suivantes :

– définir les nouveaux fichiers d'entête (*fichier.h*) pour la déclaration de la structure de données,

– déclarer la classe du protocole,

– définir la liaison entre le code source *C++* et le code *OTCL,*

– modifier le fichier *makefile* par l'ajout du ficher rajouté à la liste des fichiers de NS-2,

Chapitre 6
Conclusion et perspectives

Sommaire

6.1 Conclusion Générale

Nous avons tenté à travers ce mémoire de bien comprendre les protocoles d'accès au medium de la couche MAC et de présenter un nouveau protocole pour une architecture distribué qui répond au mieux aux exigences de qualité de service. Pour se faire notre travail à comporter les étapes suivantes :

-Comprendre les caractéristiques et les contraintes et les difficultés spécifiques aux réseaux sans fil et précisément au type ad hoc de ces réseaux.

- Etablir un état de l'art sur les protocoles MAC des réseaux sans fil et mettre le point sur ceux développer pour les architectures sans infrastructures et qui vise d'améliorer la qualité de service, pour finir cette étape en détaillant les derniers (selon notre modeste recherche) qui implémente la topologie basé cluster.

-chercher une solution pour les problèmes de perception des porteuses liés à la localisation des nœuds de réseaux Ad Hoc (Location - Dependent *Carrier Sensing*) ; pour cela on a proposé un algorithme de clustering.

-Comprendre les standard 802.11 et essentiellement la version 802.11e et son EDCAF (*Enhanced Distributed Channel Access Function*) du quelle on a essayé d'inspirer notre mécanisme de différenciation de service.

-Et finalement proposition d'un nouveau protocole d'accès au médium pour une architecture basé cluster qui répond au mieux aux exigences de qualité de service pour les réseaux ad hoc. Pour évaluer les apports réels de notre proposition On l'a simulé à l'aide de simulateur **NS-2** (*Network simulator*).

6.2 Perspectives

Si les contributions apportées dans le cadre de ce mémoire ont résolu un certain nombre de problèmes, de nombreux autres points restent à discuter :

-Utiliser la meilleure EDCA [28] adapté à notre schéma.

-Prendre en considération le délai d'expiration des trames pour améliorer la gigue.

-finaliser l'algorithme de clustering qu'on a proposé par la maintenance et le test dans des circonstances réels

-Adapter les différents protocoles des routeurs appelés PHB (Per Hop Behaviors) pour les implémenter comme algorithme de résolution de collision inter nœud.

_ profiter de l'architecture basé cluster et du nœuds en intersection pour proposer un protocole cross-layer pour les deux ; routage et contrôle d'accès pour mieux répondre aux exigences de mobilité et de qualité de service.

-Améliorer le mécanisme de calcule de TXOP pour qu'il répond au mieux aux exigences de la QOS .

-Enfin, les études que nous avons menées, ont été effectuées à l'aide du simulateur NS2 et il serait intéressant de réaliser ces études dans des conditions réelles de manière à comparer les vraies performances avec celles offertes par des simulations.

Table des figures

Liste des acronymes

AP	Access Point
BSS	Basic Service Set
BSSID	Basic Service Set Identifier
DS	Distribution System
ESS	Extended Service Set
ESSID	Service Set Identifier
IBSS	Independent Basic Service Set
IEEE	Institute of Electrical Electronic Engineers
DCF	Distributed Coordination Function
PCF	Point Coordination Function
QoS	Quality Of service
DIFS	*DCF Inter-Frame Space*
SIFS	*Short Inter-Frame Space*
EIFS	*Extended Inter Frame Spacing*
CTS	*Clear To Send*
RTS	*Request To Send*
PIFS	*PCF Inter Frame Spacing*
DiffServ	*Differentiation of Service*
EDCA	Enhanced Distributed Channel Access
AC	Access Category
AC-BC	*Background access category*
AC-BE	*Best Effort Access Category*
AC-VI	Video Traffic Access Category
AC-VO	*Voice Traffic Access Category*
UP	*User Priority*
EDCAF	Enhanced Distributed Channel Access Function
AIFS	Arbitration Inter Frame Spacing).
AIFSN	*Arbitration Inter-Frame Space Number*
TXOP	transmission opportunity
CFB	*Contention Free Bursting*
HCF	*Hybrid Coordination Function*
PCF	Point Coordination Function
CF-Poll	Contention Free – Poll
PCF	Point Coordination Function
DCF	Distributed Coordination function
HCCA	HCF controlled channel access
FCS	frame check sequence

OFDM	*Orthogonal Frequency Division Multiplexing*
DSSS	Direct Sequence Spread Spectrum
FHSS	Frequency-hopping spread spectrum
TDMA	*Time Division Multiple Access*
FDMA	Frequency Division Multiple Access
CDMA	Code Division Multiple Access
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
Oprt	compteur d'opportunités perdus

Bibliographie

[1] **Ajay Chandra, V. Gummalla and John O. Limb** *" Wireless medium Access control Protocols*", IEEE Communications Surveys & Tutorials, Second Quarter:2–15, 2000.

[2] **Anni Matinlauri**,"*Fairness and Transmission Opportunity Limit in IEEE 802.11e Enhanced Distributed Channel Access*",Master's Thesis Espoo, March 14, 2008, HELSINKI UNIVERSITY OF TECHNOLOGY Faculty of Electronics, Communications and Automation Networking Laboratory

[3] **ANSI/IEEE ,802.11**,"*Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*", 1999 Edition (R2003)

[4] **Bai Xiang Mao Yu-Ming** ," *The Impact of Hidden Nodes on MAC Layer Performance of Multi-Hop Wireless Networks Using IEEE802.11e Protocol*", This paper appears in: Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007. International Conference on Publication Date: 21-25 Sept. 2007

[5] **R. Rollet, C. Mangin**, "*IEEE 802.11a, 802.11e and HiperLAN/2 Goodput Performance Comparison in Real Radio Conditions*," GLOBECOM, pp. 724-728, Dec 2003.

[6 **Chunhung Richard Lin and Mario Gerla**, "*Adaptive Clustering for Mobile Wireless Networks*",Selected Areas in Communications-IEEE Journal, Volume 15,Issue 7,pages 1265-1275,Sep 1997

[7] **D. Goderis, H. De Neve, Y. T. Joens, J. De Vriendt, and T. Soetens**. "*Towards an Integrated Solution for Multimedia over IP*". Alcatel Telecommunications Review, pages 97–104, 2001. 2ème trimestre 2001.

[8] **ETSI TS-101 761-1**. "*Technical Specification Broadband Radio Access Networks HIPERLAN Type 2*". Avril 2000. Data Link Control Layer Part 1 : Basic Data Transport Functions.

[9] **Gerla M, and Tsai JTC,** "*Multicluster mobile multimedia radio networks*", ACM-Baltzer Journal of Wireless Networks,1(3):255-256, 1995.

[10] **IEEE 802.1:** "*local and metropolitan area networks. Media Access Control (MAC) bridges*", IEEE 802.1D Std., 2004

[11] **IEEE 802.11 WG**. "*Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*". 1999. Reference number ISO/IEC 8802- 11 : 1999(E) IEEE Std 802.11, 1999 edition. International Standard for Information Technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific Requirements. Part 11.

[12] **IEEE 802.11e WG**. "*Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications : Medium Access Control (MAC) Enhancements for Quality of Service (QoS)*". Novembre 2002. Draft Supplement to standard for Telecommunications and Information Exchange between Systems - LAN/MAN specific Requirements, IEEE 802.11e/D4.0. Part 11.

[13] **J. Freebersyser, B. Leiner**, "*A DoD Perspective on Mobile Ad Hoc*

Networks", In "Ad Hoc Networking", edited by Charles E. Perkins, chapter 2, pp. 29-51, Addison-Wesley, 2001.

[14] **J. Jubin and J.D. Tornow**, *''The DARPA packet radio network protocols,''* Proceedings of the IEEE, January, 1987.

[15] **Jin, Tao; Chigan, Chunxiao**,"*A Security-Enabled Wireless Token Cluster MAC Protocol with Intelligent Token Policy*", Military Communications Conference, 2007. MILCOM 2007. IEEE,Volume , Issue , 29-31 Oct. 2007 Page(s):1 – 7

[16] **Johansson, T., Carr-Motyckova, L.**, "*On Clustering in Ad Hoc Networks*", Proc. Vehicular Tech. Conf. Fall , Swedish National Computer Networking Workshop 2003, (2003).

[17] **Kosek, K.; Natkaniec, M.; Vollero, L.; Pach, A.R**."*Performance Analysis of 802.11e Networks with Hidden Nodes in a Star Topology*" Consumer Communications and Networking Conference, 2008. CCNC 2008. 5th IEEE, Volume , Issue , 10-12 Jan. 2008 Page(s):440 – 441

[18] **Lessmann, J.; Janacik, P.; Lachev, L.; Orfanus, D.,** "*Comparative Study of Wireless Network Simulators*", Networking, 2008. ICN 2008, Seventh International Conference on Volume , Issue , 13-18 April 2008 Page(s):517 - 523

[19] **M. Brahma, A. Abouaissa, and P. Lorenz**. "*A Service Differentiation and Traffic Engineering Scheme for Mobile Ad-Hoc Networks*". International Journal of Sensor Networks (IJSNET), Septembre 2006

[20] **M. C. Jeruchim., P. Balaban., K.S. Shanmugan**. "*Simulation of Communication Systems*". Plenum Publishing Corporation. 1992, ISBN 0-306-43989-1, pp.723.

[21] **M.Brahma,** Rapport de Thèse: « *Étude de la QoS dans les Réseaux Ad hoc : Intégration du Concept de l'Ingénierie du Trafic* », UNIVERSITÉ DE HAUTE ALSACE-UFR DES SCIENCES ET TECHNIQUES, 2007

[22] **Miquel Oliver, Ana Escudero**, "*Study of different CSMA/CA IEEE 802.11-based implementations*", MoMM '08 Proceedings of the 6th International Conference on Advances in Mobile Computing and Multimedia,2008

[23] **Nauman Aslam, W. Phillips and W. Robertson**, *"A Unified Clustering and Communication Protocol for Wireless Sensor Networks*", International Journal of Computer Science (IJCS), Volume 35, Issue 3, 2008, Page(s): 249 - 258.

[24] **P. Popovski, F. Fitzek, H. Yomo, T. Madsen, and R. Prasad**, "*MAC-layer*

[25] *Approach for Cluster-Based Aggregation in Sensor Networks*", Proceedings of International Workshop on Wireless Ad-hoc Networks (IWWAN), pp. 89-93, Oulu, Finland, June, 2004.

[26] **S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss**. "*An Architecture for Differentiated Services*", Décembre 1998. RFC 2475.

[27] **S. Choi et al**., "*IEEE 802.11e Contention-Based Channel Access (EDCF) Performance Evaluation*", in Proc. IEEE ICC'03, May 2003.

[28] **S. Choi, J. D. Prado, S. Shankar, and S. Mangold**, *"IEEE 802.11e contention-based channel access (EDCF) performance evaluation,*" in Proc. of IEEE ICC, Anchorage, Alaska, May 2003, pp. 1151–1156.

[29] **Stefan Mangold, Sunghyun Choi, Peter May, Ole Klein,Guido Hiertz, and Lothar Stibor,** "*IEEE 802.11e Wireless LAN for Quality of Service*", Proceeding of the European Wireless '02, Florence, Italy, February 2002.

[30] **Sunil Kumar , Vineet S. Raghavan and Jing Deng** , "*Medium Access Control protocols for ad hoc wireless networks: A survey*", Ad Hoc Networks,

Volume 4, Issue 3, May 2006, Pages 326-358

[31] **W. Z. Song, Y. Wang, X. Y. Li, and O. Frieder**. "*Localized Algorithms for Energy Efficient Topology in Wireless Ad Hoc Networks*". pages 98–108, Mai 2004. In Proceedings of the 5th ACM international symposium on Mobile ad hoc networking and computing, Roppongi Hills, Tokyo, Japan.

[32] **Wonchang Choi, Miae Woo**, "*A Distributed Weighted Clustering Algorithm for Mobile Ad Hoc Networks*," aict-iciw, pp.73, Advanced International Conference on Telecommunications and International Conference on Internet and Web Applications and Services (AICT-ICIW'06), 2006

[33] **Y. P. Chen, A. L. Liestman, and J. Liu,** "*Clustering algorithms for ad hoc wireless networks*", Ad Hoc and Sensor Networks, vol. 28, 2004.

[34] **Z. J. Haas, M. R. Pearlman, and P. Samar.** "*The Zone Routing Protocol (ZRP) for Ad hoc Networks*". Juillet 2002. IETF MANET Internet Draft draft-ietfmanet

REFERENCES INTERNET

[35] Site de AWK http://www.chemie.fu-berlin.de/chemnet/use/info/gawk/gawk_toc.html

[36] Site de http://www.joshuarobinson.net/docs/802_11.html

[37] Site de NS-2 simulator. http://www.isi.edu/nsnam/ns/

[38] SITE WEB http://www.auto-nomos.de/ns2doku/class_mac802__11.html

[39] Site de NSnam : http://www.isi.edu/nsnam/nam/index.html

[40] SITE DE http://nile.wpi.edu/NS/

[41] Site de Otcl : ftp://ftp.tns.lcs.mit.edu/pub/otcl/doc/

[42] Site de Tcltk : http://www.tcl.tk/

[43] Site de tutorial NS : http://www.isi.edu/nsnam/ns/tutorial/

[44] Site de Xgraph : http://www.isi.edu/nsnam/xgraph/

[45] Site du Manuel de Network Simulator : http://www.isi.edu/nsnam/ns/doc/

[46] site du Projet VINT : http://netweb.usc.edu/vint/.

[47] Site http://celadas.unizar.es/ns-2/html/d9/dbd/classMac802__11e.html

[48] SITE WEB DE GNUPLOT http://sourceforge.net/projects/gnuplot

[49] SITE WEB http://www.tkn.tu-berlin.de / research / 802.11e_ns.

[50] Site de http://www-ivs.cs.uni-magdeburg.de/EuK/forschung/projekte/gea/index.shtml

DCC-MAC (Distributed Clustering and Communication MAC protocol)

Many technological factors, such as cheaper hardware, smaller transceivers, and faster processors, are fueling the increased interest in wireless ad hoc networks. The main goal of wireless ad hoc networks is to allow a group of communication nodes to set up and maintain a network among themselves, without the support of a base station or a central controller. From the applications perspective, wireless ad hoc networks are useful for situations that require quick or infrastructureless local network deployment, such as crisis response, conference meetings, sensor networks, military applications, and possibly home and office networks. Ad hoc networks could, for instance, empower medical personnel and civil servants to better coordinate their efforts during large-scale emergencies that bring infrastructure networks down, such as flood, earthquake...

In the OSI reference model, medium access is a function of the layer 2 sub-layer called the Medium Access Control (MAC) layer. MAC protocols for wireless networks must address the hidden node problem and must exercise power control. Accessing the wireless medium thus requires a more elaborate mechanism than what is required by wired networks to regulate user access to the channel. Ad hoc wireless networks present even greater challenges than infrastructure wireless networks at the MAC layer. The absence of a centralized controller creates the need for distributed management protocols at the MAC layer, and possibly at higher layers of the network stack.

In this thesis we present specific issue of ad hoc wireless networks than we conduct a study of some existing MAC protocols for wireless ad hoc networks, We than propose a novel distributed MAC protocol with quality of service support for a cluster based topology. Our protocol enclose five phases, clustering (using our loosely centralised Algorithm to avoid exposed and hidden node problems), intra-node traffic category election using service differentiation mechanism, candidature phase to exchange nodes need, inter-nodes distributed selection of the current high priority node and finally data transmission of the designed node

***Keywords**: Ad hoc networks; Wireless networks; MAC; Medium Access Control; Quality of Service (QoS);clustering, diffserv, 802.11e.*