

République Algérienne Démocratique et Populaire.  
Ministère de L'Enseignement Supérieur et de la Recherche Scientifique.  
Université Mouloud Mammeri de Tizi Ouzou.  
Faculté de Génie Electrique et D'informatique.  
Département D'informatique.



Mémoire de fin d'études

En vue d'obtention du diplôme Master informatique.  
*Option : Conduite de projets informatiques.*

# Thème : Interactions des protocoles MAC, Routage et TCP pour une meilleure QoS dans un MANET

Réalisé par :

**M<sup>r</sup> SAFRI Madjid**

Membres du Jury :

1. Présidente : **M<sup>me</sup> F. AOUGHLIS**

2. Examineur 1 : **M<sup>r</sup> M. DAOUI**

3. Examinatrice 2 : **M<sup>elle</sup> L. CHAMEK**

4. Promoteur : **M<sup>r</sup> S. HAMRIOUI**

2010/2011

## **REMERCIEMENTS :**

**J**e tiens à exprimer mes remerciements à mon promoteur M<sup>r</sup> HAMRIOUI pour ses encouragements et son soutien tout au long de ce travail.

Je remercie également, les membres du jury pour m'avoir fait l'honneur d'évaluer mon travail.

Je tiens enfin à remercier, toute personne ayant contribué, de près ou de loin, à la réalisation de ce travail.

---

Introduction générale .....	10
-----------------------------	----

## **Chapitre I : les réseaux ad hoc mobiles (MANET)**

Introduction .....	13
1. Les réseaux sans fil et réseaux de mobiles .....	13
1.1. Les réseaux sans fil .....	14
1.2. Les réseaux de mobiles .....	14
2. les principes de transmission radioélectrique .....	14
3. les défauts de radioélectrique .....	14
3.1. Les environnements du signal .....	14
3.2. Les interférences .....	15
3.3. Les spécificités de la communication sans fil .....	15
3.3.1. Mobilité .....	15
3.3.2. Autonomie .....	15
3.3.4. Débit et portée faibles .....	15
3.3.5. Non sécurisé .....	16
4. Classification des réseaux sans fil .....	16
4.1. Classification suivant la portée des unités mobiles .....	17
4.1.1. Les réseaux personnels sans fil ou WPAN .....	17
4.1.2. Réseaux locaux sans fil ou WLAN (Wireless Local Area Network) .....	18
4.1.3. Réseaux métropolitains sans fil ou WLAN (Wireless Metropolitan Area Network) .....	19
4.2. Classification suivant l'infrastructure .....	20
4.2.1. Réseaux sans avec infrastructure .....	20
4.2.2. Réseaux sans fil sans infrastructure (ad hoc) .....	21
5. Les réseaux ad hoc mobiles (MANETs) .....	21
5.1. Définition .....	21
5.2. Domaines d'application des réseaux ad hoc .....	22
5.3. Modélisation .....	23
5.4. Caractéristiques des MANETs .....	24
5.5. Problèmes spécifiques posés par les MANETs .....	25

5.5.1. Canaux radio .....	25
5.5.1.1 Canal bruyant .....	25
5.5.2. Nœuds cachés et nœuds exposés .....	26
5.5.3. Mobilité des nœuds .....	27
5.5.3.1 Séparation du réseau .....	28
5.5.3.2 Faux routage .....	28
5.5.4. L'hétérogénéité des nœuds .....	28
5.5.5. La taille des réseaux ad hoc .....	28
5.5.6. Ressources limitées .....	29
5.5.7. L'absence d'une infrastructure centralisée .....	29
5.5.8. Incertitudes sur les liens .....	29
5.5.9. La contrainte d'énergie .....	29
Conclusion .....	29

## **Chapitre II : Protocoles MAC (Medium Acces Control) dans les MANETs**

Introduction .....	32
1. Etat de l'art .....	32
1.1. Protocoles MAC basés sur la contention .....	33
1.2. Protocoles MAC sans contention .....	36
1.2.1. Accès multiples par répartition dans le temps (TDMA) .....	37
1.2.2. Accès multiples par répartition en fréquences (FDMA) .....	37
1.2.3. Accès multiples par répartition de code (CDMA) .....	38
2. Description de la couche MAC IEEE 802.11 .....	39
Conclusion .....	41

## **Chapitre III : les protocoles de routage dans les MANETs**

Introduction .....	43
1. Définition du routage .....	43
2. Méthodes utilisées par les protocoles de routage Ad-hoc .....	44

---

2.1.	Distance Vector (DV) : vecteur de distance .....	44
2.2.	Link State (LS) : état de lien .....	45
2.3.	Distance Vector vs Link State .....	45
2.4.	Routage hiérarchique ou plat .....	46
2.4.1.	Les protocoles de routage à plat .....	46
2.4.2.	Les protocoles de routage hiérarchiques .....	46
2.5.	Le routage à la source et le routage saut par saut .....	46
2.5.1.	Le routage à la source .....	46
2.5.2.	Le routage saut par saut .....	47
3.	Les protocoles de routage pour les réseaux ad hoc .....	47
3.1.	Classification .....	47
3.2.	Les protocoles de routage proactifs .....	47
3.2.1.	Le protocole de routage « OLSR » .....	47
3.2.1.1.	Détection de voisinage .....	48
3.2.1.2.	Gestion de la topologie .....	50
3.2.1.3.	Calcul des routes .....	51
3.3.	Les protocoles de routage réactifs .....	51
3.3.1.	Le protocole de routage « DSR » .....	51
3.3.2.	Le protocole de routage « AODV » .....	53
	Conclusion .....	54

## **Chapitre IV : le protocole TCP dans les MANETs**

Introduction .....	57
1. Le protocole TCP .....	57
2. Conséquences des problèmes liés aux MANETs sur le protocole TCP.....	58
2.1. Canal bruyant .....	58
2.2. Nœuds cachées et exposés.....	59
2.3. Mobilités des nœuds.....	59
3. Caractéristiques du protocole TCP.....	59
3.1. Le transfert fiable des données.....	59
3.2. Le contrôle de congestion TCP .....	60

---

4. Les défis de TCP dans les MANETs.....	62
5. Solutions proposées.....	64
5.1. TCP-F TCP Feedback .....	64
5.2. TCP Split.....	65
Conclusion.....	66

## Chapitre V : la QoS (Quality of Service) dans les MANETs

Introduction.....	68
1. Principaux modèle de QoS dans les réseaux ad hoc .....	68
1.1. Les protocoles d'accès au médium avec QoS .....	70
1.1.1. IEEE 802.11 <sup>e</sup> .....	70
1.1.2. Différenciation de services pour 802.11 <sup>e</sup> .....	71
1.1.3. MACA / PR .....	72
1.2. Les protocoles de routage avec qualité de service.....	72
1.2.1. Routage avec QoS sur DSDV.....	73
1.2.2. Routage avec QoS sur AODV.....	73
2. Modèles de qualité de service dans les réseaux ad-hoc .....	74
2.1. Les modèles standards existants.....	75
2.1.1. IntServ .....	75
2.1.2. DiffServ.....	77
2.2. Les principaux modèles utilisés dans les MANETs.....	78
2.2.1. FQMM (Flexible quality of service model for MANETs).....	78
2.2.2. SWAN (Service differentiation in wireless ad hoc networks).....	78
2.2.3. QPART (QoS Protocol for Ad hoc Real-time Traffic).....	79
2.2.4. Modèle iMAQ (integrated MANET QoS).....	79
Conclusion.....	80

---

## Chapitre VI : Interactions entre les protocoles MAC, Routage et TCP

Introduction .....	83
1. Architecture de communications entre couches.....	84
1.1. Communication directe entre couches.....	85
1.2. Interactions vers une entité intermédiaire .....	85
1.3. Nouvelles abstractions .....	86
2. Interactions entre les protocoles .....	86
2.1. Interaction entre le protocole MAC et le protocole TCP .....	86
2.1.1. Etat de l'art.....	86
2.1.2. Notre contribution .....	93
2.2. Interaction entre le protocole MAC et le protocole de routage .....	94
2.2.1. Etat de l'art.....	94
2.2.2. Notre contribution .....	100
2.3. Interaction entre le protocole TCP et le protocole de routage .....	101
2.3.1. Etat de l'art.....	101
2.3.2. Notre contribution .....	107
Conclusion.....	108
Conclusion générale .....	110
Bibliographie.....	113

## Liste des figures

Figure 1.1 : Classification des réseaux sans fil .....	16
Figure 1.2 : Le modèle des réseaux mobiles avec infrastructure .....	20
Figure 1.3 : Réseau mobile ad hoc(MANET).....	22
Figure 1.4 : Modélisation d'un réseau ad hoc.....	23
Figure 1.5 : Le changement de la topologie des réseaux ad hoc .....	24
Figure 1.6 : Le multipath.....	26
Figure 1.7 : Le nœud caché .....	26
Figure 1.8: Le nœud exposé .....	27
Figure 1.9 : La séparation du réseau .....	28
Figure 2.1 : Sous-couche MAC dans le modèle OSI et TCP/IP .....	32
Figure 2.2 : Inter Frame Spacing dans 802.11 .....	36
Figure 2.3: architecture la norme IEEE 802.11.....	39
Figure 2.4 : Principe de la fonction DCF .....	40
Figure 2.5 : Méthode d'accès DCF .....	40
Figure 3.1 : le chemin optimal entre la source et la destination .....	47
Figure 3.2 : classification des protocoles de routage.....	51
Figure 3.3 : exemple d'information de voisinage maintenue par OLSR.....	53
Figure 3.4 : Optimisation de l'inondation par des relais multipoint.....	54
Figure 3.5 : exemple d'information de topologie maintenue par OLSR.....	54
Figure 3.6 : exemple de routage maintenu par OLSR.....	55

Figure 3.7 : la découverte de chemins dans le protocole DSR .....	56
Figure 4.1 : TCP Split .....	69
Figure 5.1 : Besoin du débit, gigue et délai pour le multimédia .....	73
Figure 5.2 : Besoin en délai et bande passante des applications .....	74
Figure 5.3 : Le principe d'AODV avec QoS .....	78
Figure 5.4 : principe de fonctionnement du protocole IntServ .....	80
Figure 6.1 : interaction entre couches (cross-layer) .....	84
Figure 6. 2: modèle d'architecture cross-layer .....	85

**V**u les avancées fulgurantes que connaît le monde informatique, nous assistons aujourd'hui à l'émergence de nouveaux appareils qui ont la particularité d'être mobiles, tels que les téléphones portables, les ordinateurs portables, les équipements GPS (Global Positioning System) et les PDAs (Personal Digital Assistant). Dans un souci d'établir des échanges d'information entre les utilisateurs possédant ces dispositifs mobiles, les réseaux sans fil voient le jour.

Un réseau ad hoc mobile (MANET) pour Mobile Ad hoc NETwork ; est un ensemble autonome et coopératif de nœuds mobiles qui se déplacent et communiquent par une transmission sans fil qui ne suppose pas d'infrastructure préexistante. Le réseau ad hoc se forme de manière spontanée et provisoire dès que plusieurs nœuds mobiles se trouvent à portée radio les uns des autres. Les nœuds communiquent, selon la distance qui les séparent, par deux modes de communication : soit les nœuds mobiles peuvent directement communiquer (en transmission ad hoc) car ils sont dans à portée de transmission, soit ils doivent utiliser d'autres nœuds mobiles comme des relais pour acheminer les paquets à destination (la transmission est multi-sauts).

Cette absence d'infrastructure fixe pose un certain nombre de problèmes. En particulier, afin d'assurer la transmission des informations d'un bout à l'autre du réseau, les terminaux mobiles doivent avoir la capacité de retransmettre des informations, jouant ainsi le rôle de routeurs. Cependant, les spécificités du lien radio ainsi que la mobilité potentielle des utilisateurs rendent les protocoles de routage, de transport et MAC utilisés dans les réseaux usuels peu performants. C'est pourquoi un groupe de travail de l'IETF travaille actuellement à la standardisation d'un ou plusieurs protocoles de ce type de réseaux.

Au delà de l'intérêt d'étudier le domaine des réseaux multi-sauts mobiles, qui ont suscité une activité intense de recherche protocolaire ces 10 dernières années en raison de leurs caractéristiques fort différentes des réseaux filaires traditionnels, nous nous intéressons à l'interaction protocolaire pour une meilleure Qualité de Service dans les MANETs .

La tendance de travaux de recherche sur la Qualité de Service dans les réseaux ad hoc mobiles (MANETs) se repose sur une approche dite cross-layer qui favorise l'interaction des couches de la pile OSI, et la coopération entre les mécanismes (protocoles) de QoS misent en œuvre au niveau des différentes couches. Bien que notre thèse se focalisera essentiellement sur les trois couches de la piles OSI à savoir ; la couche liaison de données (protocole MAC) ; la couche réseau (protocole de routage) ; la couche transport (protocole TCP ...).

Cette thèse est composée de chapitres suivants :

- Dans le premier chapitre nous présenterons les différents environnements mobiles, et réseaux sans fil ainsi que des généralités sur les réseaux ad hoc mobiles (MANET), les concepts fondamentaux, les définitions, les caractéristiques et les domaines d'applications, et ainsi que des problèmes causé par les caractéristiques de ce dernier.
- Le second chapitre sera consacré pour le protocole MAC (Medium Access Control), les différentes normes existantes. Ainsi q' un état de l'art sur l'évolution de la norme.
- Dans le troisième chapitre, nous allons présentés les protocoles de routages dans les MANETs, les différentes classifications de ces dernier, ainsi que certaines critiques vis-à-vis ces protocoles.
- Le chapitre quatre fera le tour sur le protocole TCP de la couche transport de la pile OSI dans les MANETs, et quelques algorithmes proposés dans la littérature pour remédier à certains problèmes de ce dernier.
- Comme cinquième chapitre, nous l'avons consacré à la qualité de service dans les MANETs, les différents modèles existants pour les réseaux filaires, et leurs homologues dans les MANETs.
- Et finalement le dernier chapitre sera consacré sur un état d'art des différents travaux de recherches fait et qui se font à l'heure actuelle en ce qui concerne l'approche dite cross-layer, et les différentes interactions les protocoles MAC, TCP et Routage comme suit
  - TCP/MAC.
  - TCP/Routage.
  - MAC/Routage.

Pour une meilleure QoS dans les MANETs. Et notre contribution

### Introduction :

L'évolution rapide de la technologie dans le domaine de la communication sans fil, a permis aux usagers munis d'unités de calcul portables d'accéder à l'information indépendamment des facteurs : temps et lieu. Ces unités, qui se communiquent à travers leurs interfaces sans fil, peuvent être de diverses configurations : avec ou sans disque, des capacités de sauvegarde et de traitement plus ou moins modestes et alimentés par des sources d'énergie autonomes (batteries). L'environnement de calcul résultant est appelé environnement mobile. Cet environnement n'astreint plus l'utilisateur à une localisation fixe, mais lui permet une libre mobilité tout en assurant sa connexion avec le réseau [BAD98].

Plusieurs systèmes utilisent déjà le modèle cellulaire et connaissent une très forte expansion à l'heure actuelle mais requièrent une importante infrastructure logistique et matérielle fixe. La contrepartie des réseaux cellulaires sont les réseaux mobiles Ad-hoc (MANET). Ce système peut fonctionner d'une manière isolée ou s'interfacer à des réseaux fixes au travers de passerelles». C'est la caractéristique qui distingue les réseaux mobiles Ad-hoc des réseaux sans fil plus traditionnels comme les réseaux cellulaires et les réseaux locaux sans fil. Aucune supposition ou limitation n'est faite sur la taille du réseau.

Ce chapitre a pour but de présenter l'environnement mobile, et les principaux concepts liés à ce nouvel environnement et par la suite, nous présenterons le concept du réseau ad hoc mobile (MANET), et les différentes caractéristiques et domaines d'application et ainsi que ses limitations qui sont dues généralement aux caractéristiques de ce type de réseau. Le chapitre introduit la technologie de communication sans fil utilisée par les réseaux mobiles; pour cela nous détaillons quelques principales notions nécessaires à la compréhension de ces systèmes.

### 1. réseaux sans fil et réseaux de mobiles :

Les termes mobile et sans fil sont souvent utilisés pour décrire les systèmes existants, tels que le GSM, IEEE 802.11, Bluetooth, etc. Toutefois, il est important de distinguer les deux catégories de réseaux que regroupent les concepts de mobile et de sans fil, de façon à éviter toute confusion [APV01].

**1.1. Les réseaux sans fil :** Le concept de sans fil est étroitement associé au support de transmission. Un système est dit sans fil s'il propose un service de communication totalement indépendant de prises murales. Dans cette configuration, d'autres moyens d'accès sont exploités, tels que l'infrarouge ou les ondes hertziennes. Ces différentes interfaces ne sont toutefois pas sans faire naître de nouvelles difficultés.

**1.2. Les réseaux de mobiles :** Un utilisateur mobile est défini théoriquement comme un utilisateur capable de communiquer à l'extérieur de son réseau d'abonnement tout en conservant une même adresse. Bien entendu, certains systèmes tels que le GSM offrent la mobilité et le sans-fil simultanément.

### **2. Le principe de transmission radioélectrique :**

Découvert par le physicien allemand Heinrich Hertz en 1887, les ondes radioélectriques, support capital de la transmission sans fil sont basés sur le principe suivant :

L'accélération d'un électron crée un champ électromagnétique qui à son tour accélère d'autres électrons et ainsi de suite. Il est alors possible de provoquer le déplacement électromagnétique. Plus le nombre d'électrons déplacés est important, plus le signal est fort et plus sera grande sa portée, avec une vitesse proche de celle de la lumière [TIS99]. Un déplacement coordonné d'électrons peut alors servir pour le transfert d'information et constitue la base de la communication sans fil. L'approche standard de la transmission radio est le déplacement des électrons à une fréquence donnée.

### **3. Les défauts de transmission radioélectrique :**

Les modes de transmissions filaires fournissent des supports de transmissions, pour lesquels la théorie définit des modèles qui permettent de prévoir les défauts, parce que l'on sait contrôler l'environnement. Cependant, la nature hertzienne et incontrôlable et des liens de transmission sans fil posent problème.

**3.1. L'environnement du signal :** Avec la transmission hertzienne, Les sources de perturbation du signal sont connues, leurs effets également. La transmission a lieu dans un milieu ouvert dans lequel les sources de perturbation se déplacent, chacune avec sa propre loi, à titre d'exemple les ondes créées par les orages peuvent brouiller le

signal, le vent le fait bouger. A ceci peut s'ajouter les différents obstacles sur lesquels réfléchissent les ondes radioélectriques, par exemple le sol, les voitures.

**3.2. Les interférences :** Dans la communication radiofréquence, une unité désirant entrer en communication utilise une fréquence radio. L'exploitation de la même fréquence radio, en même temps, par différentes unités conduit à une interférence, bien entendu, dans le cas où les unités se trouvent l'un à la portée de l'autre. Pour palier à ce problème, une solution facile serait d'attribuer à chaque unité une bande de fréquence différente. Par défaut de la ressource bande de fréquence, cette solution limite considérablement le nombre d'abonné du réseau, ce qui n'est pas économique pour les opérateurs. Une autre solution consiste, notamment dans le radio téléphone cellulaire, à attribuer la fréquence à la demande. Une unité mobile, avant d'entamer une communication, demande un canal qui lui sera attribué en fonction de la saturation du réseau, une fois la transmission finie, le canal sera libéré. Nous allons revoir toutes ces notions plus en détails par la suite.

**3.3. Les spécificités de la communication sans fil :** Après les problèmes dus à la nature radiofréquence du lien de communication, l'opportunité donnée à l'utilisateur, celle de pouvoir communiquer là où il veut et quant il veut, ne va pas sans solutionner ceux posés par la mobilité.

**3.3.1. Mobilité :** L'utilisateur des réseaux sans fil a la possibilité de se déplacer dans le réseau tout en gardant la même adresse, il peut accéder aux services offert par le réseau de n'importe où et à n'importe quel moment. Cela nécessite d'une part des mécanismes de localisation de l'utilisateur, et d'autre part une assurance de la continuité des communications en cours de déplacement.

**3.3.2. Autonomie :** Les unités mobiles ont une contrainte liée à la durée de vie des batteries, il faut économiser autant que possible les transmissions inutiles. Heureusement qu'actuellement les nouvelles technologies de mobiles présentent des durées plus importantes offrant aux mobiles une autonomie plus importante.

**3.3.3. Débit et portée faible :** L'une des limites de la communication sans fil vient de la relative faiblesse de la bande passante des technologies utilisées. Plusieurs facteurs

limitent la portée d'une transmission sans fil, comme la faible puissance du signal, les obstacles qui empêchent, atténuent, ou réfléchissent les signaux.

**3.3.4. Non sécurisé :** Les réseaux sans fil offrent de nouvelles failles aux pirates. De part la nature immatérielle du support physique, l'écoute clandestine sur un réseau sans fil est facile. Il faut donc protéger l'accès aux ressources sans fil et aux informations qui circulent dans les trames. Les systèmes mobiles sont généralement équipés de processeurs moins puissants que les machines fixes, et ne peuvent se permettre d'effectuer de longs calculs demandés par les systèmes de cryptographie. L'énergie de la batterie est une ressource rare et pose également des problèmes de sécurité.

**4. Classifications des réseaux sans fil :**

Plusieurs technologies de réseaux sans fil existent qui se distinguent par la fréquence d'émission utilisée, le débit, la portée des transmissions et même le mode de fonctionnement. Plusieurs classifications peuvent être définies suivant ces caractéristiques. Nous étudions deux de ces classifications à savoir : la classification selon la portée des sites et selon l'infrastructure utilisée. (figure 1.1)

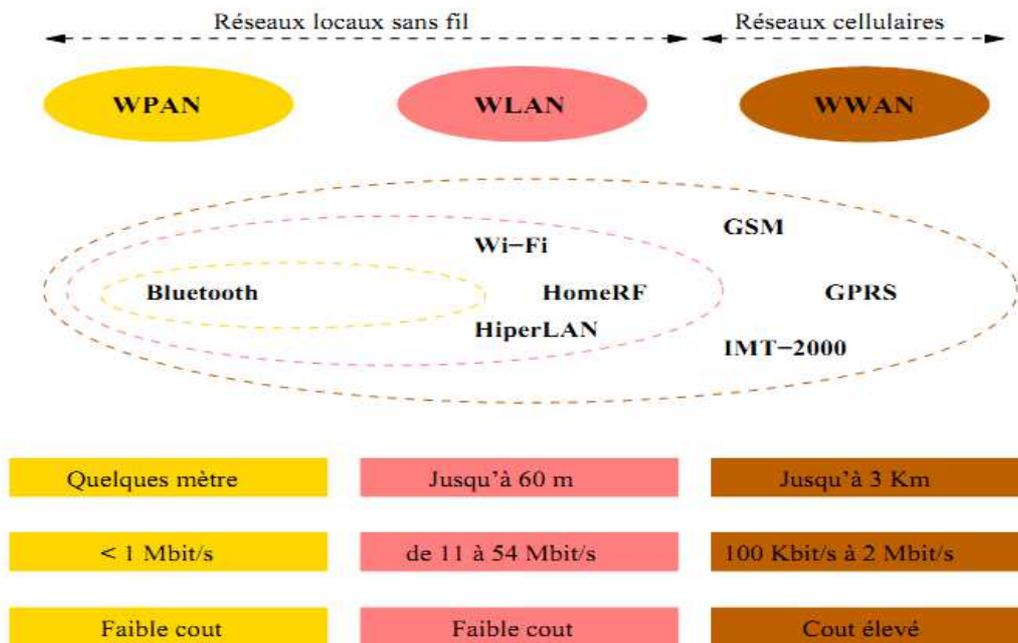


Figure 1.1 : Classification des réseaux sans fil.

### 4.1. Classifications suivant la portée des unités mobiles :

Il existe plusieurs technologies qui se distinguent d'une part par la fréquence d'émission utilisée mais également par le débit et la portée des transmissions. C'est d'ailleurs cette dernière caractéristique qui permet de classer les réseaux sans fil, à l'instar des réseaux filaires. Celles-ci sont donc définies en fonctions du périmètre géographique offrant une connectivité, plus communément appelées **zone de couverture** [DGA03].

**4.1.1. Les réseaux personnels sans fil ou WPAN :** Le réseau personnel sans fil, WPAN (*Wireless Personal Area Network*) concerne les réseaux sans fil d'une faible portée ; de l'ordre de quelques dizaines de mètres. Ce type de réseau sert généralement à relier des périphériques (imprimante, téléphone portable, appareils domestiques, ...) ou un assistant personnel (PDA) à un ordinateur sans liaison filaire ou bien à permettre la liaison sans fil entre deux machines très peu distantes [DGA03].

Il existe plusieurs technologies utilisées pour les WPAN :

- **Bluetooth :** Norme créée en 1994 par Ericsson et validé sous le nom de IEEE 802.15.1 (*IEEE : Institute of Electrical and Electronics Engineers*), un de ses points forts est l'utilisation de petits composants utilisant de faibles puissances ce qui la rend particulièrement adapté à une utilisation au sein de petits périphériques [APV01].
- **Zigbee :** Initiée par Motorola et ratifiée en août 2003 sous la norme IEEE 802.15.4 [IEE03]. Il Permet d'obtenir des liaisons sans fil à très bas prix et avec une très faible consommation d'énergie. Particulièrement adaptée pour être directement intégré dans de petits appareils électroniques, capables d'opérer plusieurs mois sur batterie et de se relier ensemble en réseau (appareils électroménagers, jouets, ...).
- **Infrared data Association :** IrDA (InfraRed Data Association) est un organisme à but non lucratif créé en 1993, fondé pour promouvoir les standards de communication point à point basés sur l'infrarouge. Il est utilisé principalement pour l'échange d'informations entre outils communicants tels

que les téléphones mobiles, les assistants personnels ou les ordinateurs portables.

**4.1.2. Réseaux locaux sans fil ou WLAN (Wireless Local Area Network) :** Le réseau local sans fil, WLAN (Wireless Local Area Network) est un réseau permettant de couvrir l'équivalent d'un réseau local d'entreprise, soit une portée d'environ une centaine de mètres. Il permet de relier entre eux les terminaux présents dans la zone de couverture. Il existe plusieurs technologies concurrentes [DGA03] :

- **Wifi [GER06] :** Norme publiée en juin 1997 par l'IEEE sous le nom d'IEEE 802.11, soutenue par l'alliance WECA (Wireless Ethernet Compatibility Alliance), elle est basée sur une topologie cellulaire (au même titre que GSM) et permet de répondre à deux catégories d'architecture : Le mode Ad Hoc (point à point) et le mode Infrastructure (architecturé autour d'un point d'accès).
- **HiperLan (High Performance Radio LAN, versions 1 et 2) :** HiperLAN (High Performance Radio LAN) est un standard européen initié par l'ETSI (European Telecommunications Standards Institute) en 1998, il est composé de 2 normes wireless de haut débit : HiperLAN1 [ETS98] et HiperLAN2 [ETS00]. Il a comme inconvénient de n'avoir aucun soutien pour le marché américain. Il a une transmission dans la Bande des 5 GHz. HiperLAN 1 est pour les réseaux en mode Ad Hoc uniquement, avec un débit de 20 Mbits/s théorique. HiperLAN 2 est pour les réseaux en mode Infrastructure uniquement, avec un débit de 54 Mbits/s théorique.
- **HomeRF :** Lancée en 1998 par le HomeRF [NSL00] (Home Radio Frequency) Working Group, formé notamment par les constructeurs Compaq, HP, Intel, Siemens, Motorola et Microsoft, Cette technologie met en avant ses petits prix et sa facilité de mise en œuvre, elle Utilise la norme DECT pour réaliser le transfert de la voix (protocole TDMA) et la norme 802.11 pour le transfert de données (CSMA/CA), elle permet de fournir de

multiples canaux de voix de bonne qualité. Elle utilise des architectures en modes Ad Hoc et Infrastructure.

**4.1.3. Réseaux métropolitains sans fil ou WMAN (Wireless Metropolitan Area Network) :** Ces réseaux sont connus sous le nom de Boucle Local Radio ou BLR [APV01]. En télécommunication, la boucle locale est la partie du réseau qui relie le terminal de l'utilisateur à un équipement de l'opérateur. La boucle locale radio n'est autre que la boucle locale dans laquelle le lien de communication entre l'utilisateur et le premier équipement de l'opérateur utilise des ondes radios. Dans ces systèmes, une antenne, qui couvre 3 à 15 km, est placée haut en vue directe avec des petites antennes installées chez les clients.

Parmi les technologies utilisées par les WMAN on peut citer :

- **LMDS (Local Multipoint Distribution Service) :** Le LMDS [APV01] est une technologie cellulaire "Point à multipoint": un émetteur central dessert un nombre élevé d'abonnés. Les systèmes LMDS modernes offrent une portée d'environ 5 à 6 km et utilisent des fréquences supérieures à 20 GHz. Ils autorisent des transmissions bidirectionnelles symétriques dotées de débits allant de 64 Kbits/s à plusieurs Mbits/s, ainsi que la transmission de la voix. L'émetteur se présente sous la forme d'une tour bardée d'antennes, assez similaires aux antennes GSM. L'équipement de l'abonné se résume à une petite antenne (environ 25 cm de diamètre). Selon les constructeurs (Alcatel, Lucent, Nortel...), cet équipement fournit un débit maximal de 8 à 10 Mbits/s en voie montante et descendante sous la forme d'un bouquet de service voix et données.
- **IEEE 802.16 :** [IEE03] Alias WiMax, nouvelle norme développée pour offrir des réseaux sans fil longue distance et haut-débits. Basée sur des fréquences allant de 2 à 10GHz, il pourra offrir un débit allant jusqu'à 130 Mbit/s. En pratique on pourra avoir un débit de 70 Mbit/s (par secteur radio et par canal de 20MHz) sur une couverture d'une dizaine de kilomètres. WiMax devrait permettre l'extension des connexions Internet haut-débit aux zones non couvertes par l'ADSL.

### 4. 2. Classification suivant l'infrastructure :

Un environnement mobile est un système composé de sites mobiles et qui permet à ses utilisateurs d'accéder à l'information indépendamment de leurs positions géographiques. Les réseaux mobiles ou sans fil, peuvent être classés en deux classes : les réseaux avec infrastructure et les réseaux sans infrastructure.

**4.2.1. Réseaux sans fil avec infrastructure :** Dans ce mode de fonctionnement le réseau est obligatoirement composé d'un point d'accès appelé station de base (SB), munis d'une interface de communication sans fil pour la communication directe avec les sites ou unités mobiles (UM) (figure 1.2), une station de base couvre une zone géographique limitée, une unité mobile est rattachée à un moment donné qu'à une station de base lui offrant tous les services tant que l'UM est à l'intérieure de la zone de couverture de la SB. La SB fait office de pont entre réseau filaire et réseau sans fil, permettant de relier une UM à une unité connecté à un site fixe. La SB est aussi le point de passage de la transmission d'une UM à une autre UM. Si les deux UM dépendent de la même SB, la trame est simplement relayée par la SB. Si les deux UM sont à deux SB différentes, une trame échangée entre les deux UM doit être relayée par le réseau filaire qui relie les deux points d'accès. Les points d'accès peuvent être répartis sur tous le réseau filaire, agrandissant d'autant la couverture du réseau sans fil.

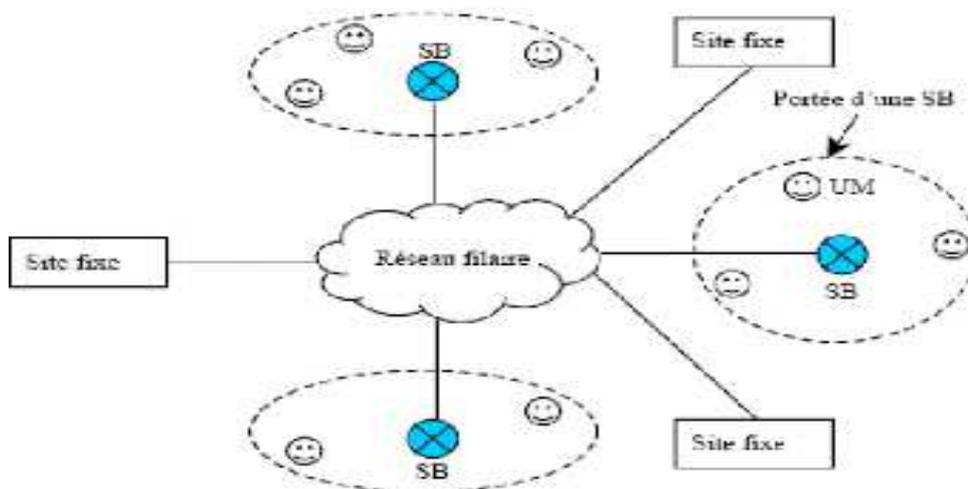


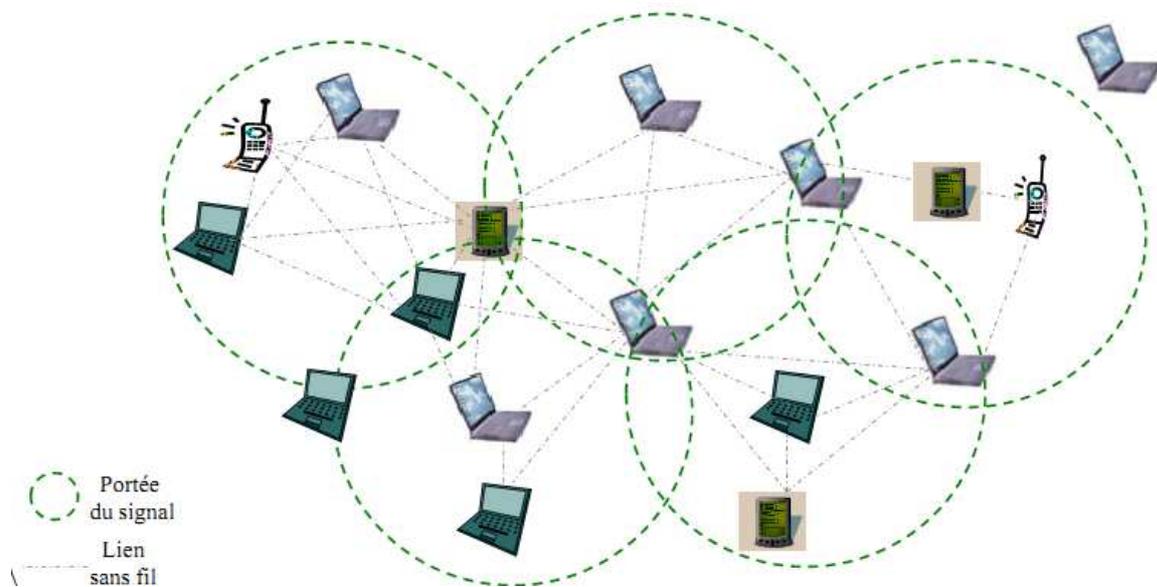
Figure 1.2 : Le modèle des réseaux mobiles avec infrastructure.

### 4.2.2. Réseaux sans fil sans infrastructure (ad hoc) :

Il s'agit d'un mode Point à Point, ne nécessitant pas de points d'accès. Il permet de connecter les stations quand aucun point d'accès n'est disponible. L'absence d'infrastructure oblige les UM à jouer le rôle de routeurs [CCL03]. Les réseaux ad hoc ont des typologies instables, ceci est dû aux déplacements fréquents des UM. D'autre part, la portée des transmissions radio étant limitée, le relaying est rendu obligatoire, et il faut donc que les UM forment ce réseau ad hoc et coopèrent pour transmettre les messages d'une source à une destination. Les chemins utilisés et les nœuds traversés sont déterminés par un protocole de routage dédié, c'est d'ailleurs la raison pour laquelle les réseaux ad hoc sont dits réseaux à routage interne ou aussi réseaux sans fil multi-saut (*multi-hop wireless ad hoc networks*) [CCL03]. Beaucoup de problèmes sont liés aux réseaux ad hoc : l'allocation des fréquences, problème des nœuds cachés et des nœuds exposés [BCG04].

### 5. les réseaux ad hoc mobiles (MANETs) :

**5.1. Définition :** Un réseau ad hoc mobile (MANET) peut être défini comme une collection d'entités mobiles interconnectées par une technologie sans fil formant un réseau temporaire sans l'aide de toute administration ou de tout support fixe (voir la Figure 1.3). Une définition de ces réseaux est donnée formellement dans RFC2501 [PEG]: « Un réseau mobile ad hoc comprend des nœuds qui sont libres de se déplacer sans contrainte. Un réseau mobile ad hoc est donc un système autonome de nœuds mobiles. Autrement dit, il consiste en une grande population, relativement dense, d'unités mobiles qui se déplacent dans un territoire quelconque et dont le seul moyen de communication est l'utilisation des interfaces sans fil, sans l'aide d'une infrastructure préexistante ou administration centralisée.



**Figure 1.3 : Réseau mobile ad hoc (MANET) [MAM].**

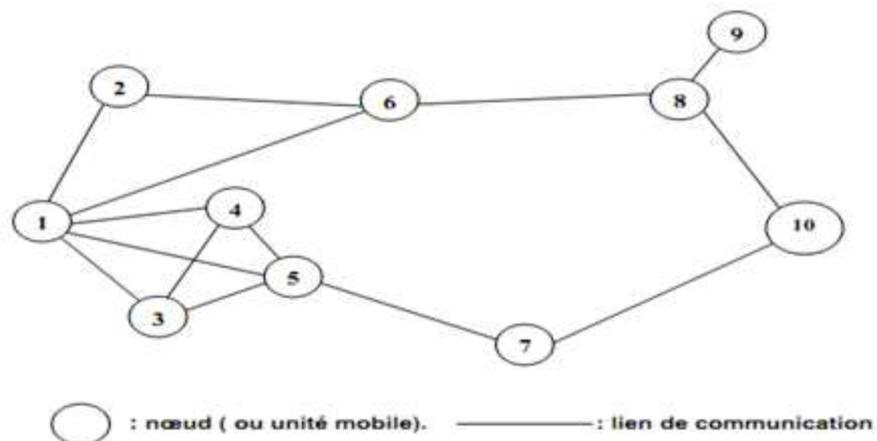
**5.2. Domaines d'application des réseaux ad hoc :** Les communications et les opérations dans le domaine militaire demeurent les toutes premières applications des réseaux ad hoc. Cependant, avec l'avancement des recherches dans le domaine des réseaux et l'émergence des technologies sans fil (ex : Bluetooth, IEEE 802.11 et Hiperlan) ; d'autres applications civiles sont apparues. On distingue [PUJ03]:

- Les services d'urgence : opération de recherche et de secours des personnes, tremblement de terre, feux, inondation, dans le but de remplacer l'infrastructure filaire.
- Le travail collaboratif et les communications dans des entreprises ou bâtiments dans le cadre d'une réunion ou d'une conférence par exemple.
- Home network : partage d'applications et communications des équipements mobiles.
- Applications commerciales : pour un paiement électronique distant (taxi) ou pour l'accès mobile à l'Internet, où service de guide en fonction de la position de l'utilisateur.

- Réseaux de capteurs : pour des applications environnementales (climat, activité de la terre, suivi des mouvements des animaux, ... etc.) ou domestiques (contrôle des équipements à distance).
- Réseaux en mouvement : informatique embarquée et véhicules communicants.

**5.3. Modélisation :** Un réseau ad hoc peut être modéliser par un graphe  $G_t=(V_t,E_t)$ . [BSA07] Où :  $V_t$  représente l'ensemble des nœuds (i.e. les unités ou les hôtes mobiles) du réseau et  $E_t$  modélise l'ensemble des connections qui existent entre ces nœuds. Si  $e = (u,v) \in E_t$ , cela veut dire que les nœuds  $u$  et  $v$  sont en mesure de communiquer directement à l'instant  $t$ .

La figure 1.4 suivante représente un réseau ad hoc de 10 unités mobiles sous forme d'un graphe :



**Figure 1.4 : Modélisation d'un réseau ad hoc.**

La topologie du réseau peut changer à tout moment, elle est donc dynamique et imprévisible ce qui fait que la déconnexion des unités soit très fréquente.

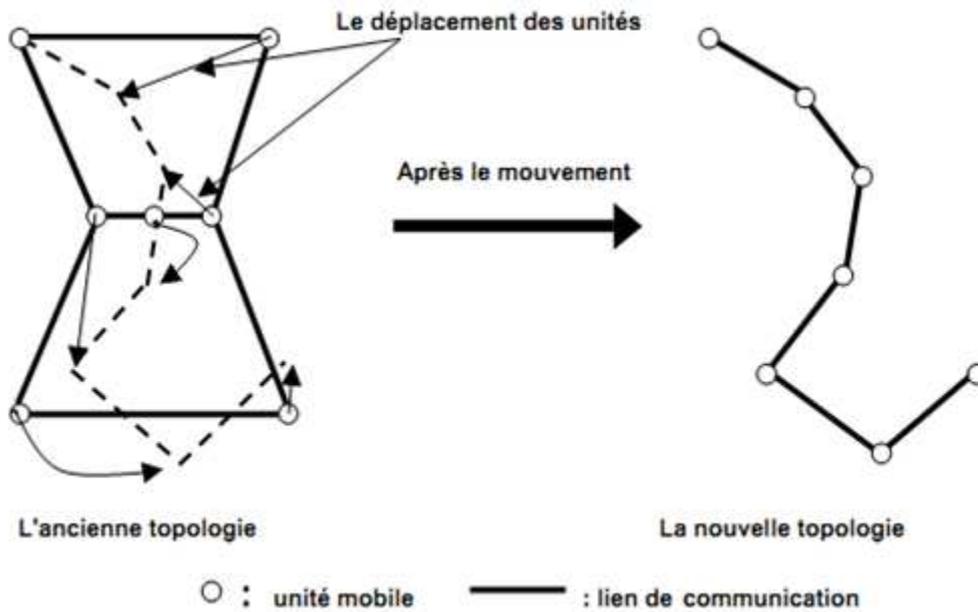


Figure 1.5 : Le changement de la topologie des réseaux ad hoc. [BSA07].

**5.4. Caractéristiques des MANETs:** Les réseaux mobiles ad hoc sont caractérisés par [APV01], [MUH02]:

- **Une topologie dynamique :** Les unités mobiles du réseau, se déplacent d'une façon libre et arbitraire. Par conséquent la topologie du réseau peut changer, à des instants imprévisibles, d'une manière rapide et aléatoire. Les liens de la topologie peuvent être unis ou bidirectionnels.
- **L'absence d'infrastructure :** Les réseaux Ad hoc se distinguent des autres réseaux mobiles par la propriété d'absence d'infrastructures préexistantes et de tout genre d'administration centralisée. Les hôtes mobiles sont responsables d'établir et de maintenir la connectivité du réseau d'une manière continue.
- **Un routage multi-sauts :** Cela signifie que des communications entre deux nœuds doivent pouvoir s'effectuer même si ceux-ci sont hors de portée de communication directe. La connaissance réciproque de leur existence et les échanges d'information doivent être possibles en traversant d'autres nœuds du réseau.

- **Chaque nœud du réseau est à la fois hôte et routeur** : Chaque nœud du réseau contribue au bon acheminement des informations dans le réseau. Pour ce faire, chaque nœud essaie de posséder une connaissance partielle du réseau la plus étendue possible pour jouer le rôle de routeur pour lui-même et pour tout autre nœud qui le lui demandera. Cette connaissance partielle se manifeste par la connaissance des voisins immédiats et leurs positions en fonction du temps.

D'une façon générale, les réseaux Ad hoc sont utilisés dans toute application où le déploiement d'une infrastructure réseau filaire est trop contraignant, soit parce que difficile à mettre en place, soit parce que la durée d'installation du réseau ne justifie pas de câblage à demeure. En plus, aucune supposition ou limitation n'est faite sur la taille du réseau Ad hoc, le réseau peut contenir des centaines ou des milliers d'unités mobiles.

**5.5. Problèmes spécifiques posés par les MANETs** : le canal radio n'est pas aussi stable et isolé comme le canal filaire, il existe plusieurs facteurs qui influencent sur la performance de la transmission des données. Parmi ces facteurs nous citons [CHE04] :

**5.5.1. Canaux radio** : Dans les réseaux ad hoc, tous les sauts partagent le même canal radio en même fréquence. Ça cause l'interférence du signal en transmettant [NGU09].

**5.5.1.1. Canal bruyant** : L'environnement de transmission dans les réseaux multi saut est le canal radio. Le canal radio n'est pas isolé, il existe plusieurs objets dans l'environnement qui déteignent sur la propagation de signal.

- **L'affaiblissement du signal** : l'affaiblissement est entraîné par la réduction de l'intensité d'énergie électromagnétique à côté du récepteur. Le récepteur peut détecter le signal que l'émetteur envoie, mais l'énergie de signal est très basse donc il ne peut pas recevoir les données. Ce problème provoque la déconnexion entre l'émetteur et le récepteur.
- **Le multipath** : c'est un phénomène (en télécommunication) qui est résulté lorsqu'un signal radio se propage par plusieurs chemins et est reçu sur une

antenne. La cause du multipath est la réflexion par des objets. Il va entraîner l'erreur de recevoir même paquet de données plusieurs fois.

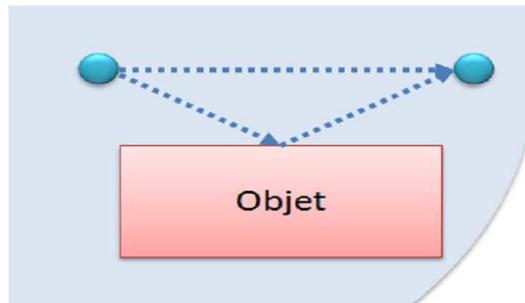


Figure 1.6 : Le multipath.

**5.5.2. Nœuds cachés et nœuds exposés :** La distance de transmission d'une antenne est limitée. La limite de la distance de transmission d'un signal radio d'un nœud est la portée (portée) de transmission de ce nœud dans lequel les autres nœuds peuvent recevoir le signal radio avec succès [NGU09]. Les nœuds cachés et exposés sont les nœuds qui ont des problèmes qu'ils sont dans la portée de transmission d'un autre nœud.

- **Le nœud caché** est décrit dans la figure 1.7. Le nœud A et C veulent transmettre les données vers le nœud B. avant d'envoyer les données, ils doivent vérifier que le canal est libre mais tous les deux reçoivent que le canal est libre parce que le nœud A ne peut pas détecter les signaux du nœud C et le nœud C en est à la même situation. Les nœuds A et C donc transmettent les paquets au nœud B en même temps.

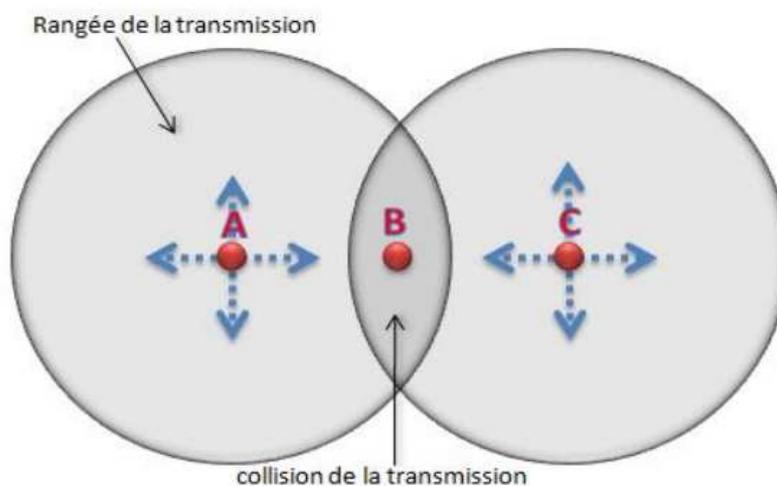
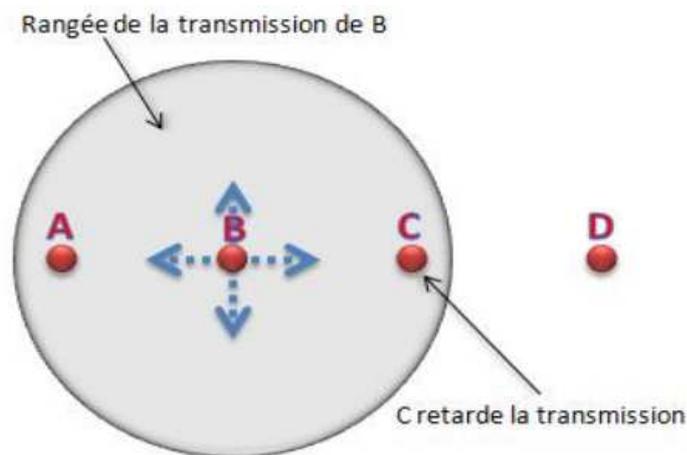


Figure 1.7 : Le nœud caché.

- **Le nœud exposé** est le nœud dans la situation où il se trouve dans la portée de transmission d'un autre nœud, et il veut lui aussi transmettre, mais il trouve son canal occupé. Il retarde donc la transmission. Dans l'exemple de figure 1.8, le nœud B transmet les données au nœud A mais le nœud C est dans la portée de la transmission de B, le canal est occupé, il ne peut pas donc transmettre au nœud D.

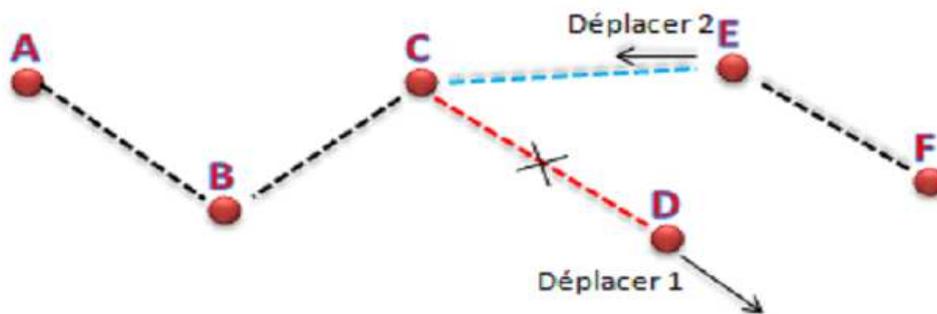


**Figure 1.8: Le nœud exposé.**

**5.5.3. Mobilité des nœuds :** [NGU09]. La mobilité des nœuds provoque des changements fréquents/dynamiques dans la topologie du réseau. Des routes peuvent se créer et disparaître très souvent. Ce déplacement a naturellement un impact sur la morphologie du réseau et peut modifier le comportement du canal de communication. Ajoutons à cela la nature des communications (longues et synchrones, courtes et asynchrones, . . .). Ces modifications doivent être prises en compte le plus rapidement possible par le protocole de routage afin de :

- maintenir une vision correcte de la topologie par les nœuds.
- supporter la maintenance.
- prendre en charge en un temps limité la reconstruction des routes tout en minimisant l'overhead généré par les messages de contrôle.

**5.5.3.1. Séparation du réseau :** Les éléments du réseau radio multi saut se déplacent par hasard et ce déplacement provoque la séparation du réseau. Après la séparation, les nœuds peuvent rejoindre, la topologie du réseau changée.



**Figure 1.9 : La séparation du réseau.**

Dans cet exemple (figure 1.9), le réseau est séparé quand le nœud D se déplace loin de nœud C et il est rejoint quand le nœud E va au nœud C.

**5.5.3.2. Faux routage :** Le faux routage est la situation fréquente dans les réseaux mobiles ad hoc. Cette situation est causée par la séparation ou le conflit des réseaux. Si un nœud détecte un faux routage, il va demander à rétablir le routage. La durée de rétablissement dépend du protocole de routage au-dessous, la mobilité du nœud.

**5.5.4. L'hétérogénéité des nœuds :** Un nœud mobile peut être équipé d'une ou plusieurs interfaces radio ayant des capacités de transmission variées et opérant dans des plages de fréquences différentes. Les nœuds peuvent avoir des différences en terme de capacité de traitement (CPU, mémoire), de logiciel, de taille (petit, grand) et de mobilité (lent, rapide). Dans ce cas, une adaptation dynamique des protocoles s'avère nécessaire pour supporter de telles situations.

**5.5.5. La taille des réseaux ad hoc :** Souvent de petite ou moyenne taille (une centaine de nœuds) ; le réseau est utilisé pour étendre temporairement un réseau filaire, comme pour une conférence ou des situations où le déploiement du réseau fixe n'est pas approprié (ex : catastrophes naturelles). Cependant, quelques applications des réseaux ad hoc nécessitent une utilisation allant jusqu'à des dizaines de milliers de nœuds, comme dans les réseaux de capteurs.

**5.5.6. Ressources limitées :** Il est important de rappeler que les réseaux ad-hoc obéissent à des contraintes très strictes en termes de ressources. Les terminaux mobiles sont par essence de petits terminaux, possédant des ressources limitées. La mobilité de ces terminaux impose une limitation sur leur capacité d'énergie qui a un impacte direct sur le rayon de transmission. D'autre part, les débits disponibles sont inférieurs à ceux que l'on peut observer dans les réseaux filaires.

**5.5.7. L'absence d'une infrastructure centralisée :** Chaque nœud travaille dans un environnement distribué, et agit en tant que routeur pour relayer des communications, ou génère ses propres données. La gestion du réseau est ainsi distribuée sur l'ensemble des éléments du réseau.

**5.5.8. Incertitudes sur les liens :** Dans ce type de réseau, on n'a aucune garantie sur le débit de chaque lien. De plus la puissance d'émission des terminaux peut varier dans le temps pour s'adapter aux ressources énergétiques du terminal par exemple.

**5.5.9. La contrainte d'énergie :** Les équipements mobiles disposent de batteries limitées, et dans certains cas très limitées tels que les PDA, et par conséquent d'une durée de traitement réduite. Sachant qu'une partie de l'énergie est déjà consommée par la fonctionnalité du routage. Cela limite les services et les applications supportées par chaque nœud.

### **Conclusion :**

**D**ans ce présent chapitre nous avons mis le point sur les environnement mobiles, leurs caractéristiques, ainsi que sur des façon de classifier des réseaux engendrés par ce genre d'environnements, et nous avons cité quelques exemples de ces classes, par la suite nous avons présenté les réseaux ad hoc mobiles dits « MANETs » pour Mobiles Ad hoc NETWORKs. Après l'avoir défini, nous avons recensé ses différents domaines d'application et ses avantages.

Une application très importante des réseaux Ad-hoc mobiles est celle de la mise en place rapide d'un réseau de communication dans le cas de catastrophe majeure sur des zones dépourvues d'infrastructures ou encore dans le cas où l'infrastructure existante est hors service, voire complètement détruite. Les exemples les plus réalistes sont ceux de zones soumises à des catastrophes

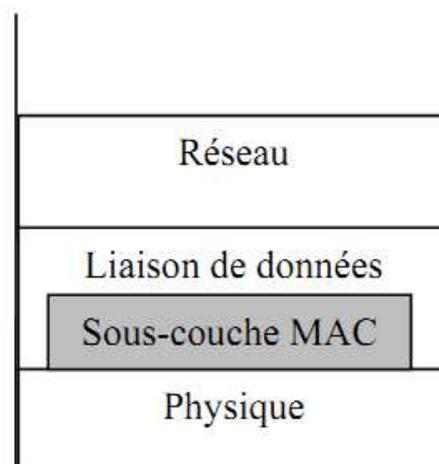
naturelles comme les tremblements de terre, les inondations, etc. Les équipes de secours ont besoin de mettre rapidement en place un réseau de communication pour coordonner les recherches.

Vu les caractéristiques et les limitations qu'engendre un réseau Ad-hoc mobiles(MANETs), plusieurs problèmes ont été posés pour ce type de réseaux : problème d'acheminement de l'information, problème de sources d'énergies (capacité des batteries), l'interopérabilité avec d'autres types de réseaux, l'effet de la mobilité des nœuds etc...

### Introduction :

Dans les télécommunications, les médiums de transmission peuvent être classés selon deux types de supports différents : filaire et sans fil. Les supports filaires sont les câbles électriques, des fibres optiques ; tandis que les supports sans fil sont les ondes radio, les ondes lumineuses, magnétiques.

Le but de ces supports est de transporter un flot de bits d'information d'une source vers une destination. Le médium de transmission est un dispositif commun pour tous les nœuds du réseau, il nécessite donc un mécanisme qui gère l'accès des nœuds pour déterminer le droit d'émettre de chacun d'entre eux dans le réseau. Dans le modèle OSI et TCP/IP [HHN06], cette tâche est gérée par la couche MAC, la sous-couche de la couche liaison de données (Figure2.1).



**Figure 2.1 - Sous-couche MAC dans le modèle OSI et TCP/IP**

#### 1. Etat de l'art :

Nous classons les protocoles d'accès au canal en deux familles principales: les protocoles MAC basés sur la contention et les protocoles MAC sans contention. Dans la première famille, tous les nœuds accèdent au canal en concurrence, il y a possibilité de collisions lorsque plus de deux nœuds accèdent au canal simultanément. Au contraire, dans la deuxième famille, chaque nœud possède son propre intervalle de temps ou sa propre fréquence de transmission. Les nœuds accèdent au canal sans concurrence et il n'y a jamais de collisions. Les travaux de

recherche des protocoles MAC sont très riches [HUN07], [HHN07], [HHV07] et le but de ce chapitre n'est pas de présenter une liste exhaustive de tous les protocoles MAC. Nous allons analyser plus en détail ces deux familles de protocoles MAC dans ce qui suit.

### 1.1. Protocoles MAC basés sur la contention :

Les protocoles MAC basés sur la contention sont apparus dès le début des communications sans fil. Ils continuent à être améliorés pour s'adapter aux différents types de réseaux. Dans cette partie, nous allons d'abord analyser les protocoles MAC pour les réseaux sans fil.

- En 1970, le protocole **ALOHA** est proposé comme le premier protocole de gestion d'accès au canal pour les réseaux sans fil. L'idée du protocole ALOHA est simple : un nœud accède au canal quand il a des données à transmettre. Si plusieurs nœuds accèdent au canal en même temps, les trames de données rentrent en collision ce qui engendre des retransmissions. Après une collision, les nœuds attendent un temps aléatoire avant de réessayer de transmettre à nouveau.
- Deux ans après, L.J Roberts a proposé une amélioration du protocole ALOHA qui s'appelle **ALOHA discrétisé**. Dans ce protocole, le temps est divisé en slots correspondant aux trames de données. Les nœuds se synchronisent entre eux et ils transmettent des trames de données au début de chaque slot. La collision se produit seulement quand deux nœuds émettent en même temps sur le même slot. ALOHA discrétisé génère de meilleures performances qu'ALOHA classique.
- Les protocoles ALOHA ne prennent pas en compte les transmissions des autres, ce qui augmente le nombre de collisions dans le réseau. Pour remédier à ce problème, le protocole d'accès multiple par écoute de porteuse (**Carrier Sense Multiple Access – CSMA**) a été proposé en 1975. Dans ce protocole, avant de transmettre des trames de données sur le réseau, un nœud écoute le médium de transmission pour voir ce qui se passe dans le canal. Si le canal est libre, il transmet les trames de données. Sinon, il attend un certain temps et il peut retenter de transmettre à nouveau.

- Selon la façon qu'un nœud attend le canal, les auteurs proposent 3 protocoles principaux CSMA : **CSMA 1-persistant**, **CSMA non persistant** et **CSMA p-persistant**. Dans le premier cas, si un nœud détecte que le canal est occupé, il continue à surveiller le canal jusqu'à ce qu'il soit libre. Ce nœud transmet ses trames dès que le canal est libre. Ce protocole est efficace en termes de temps d'attente. Pourtant, si plusieurs nœuds sont entrain d'attendre avant de transmettre, lorsque le canal est libre ils vont tous transmettre en même temps ce qui provoque une collision. Pour les nœuds qui sont moins pressés de transmettre, le protocole CSMA non persistant est plus adaptable. Dans ce protocole, une fois qu'un nœud détecte que le canal est occupé, il ne reste pas en écoute en permanence mais il attend un temps aléatoire avant de retenter de transmettre à nouveau. Cela évite le problème où différents nœuds attendent le canal et transmettent les trames de données en même temps lorsque le canal devient libre. Enfin, le protocole CSMA p-persistant semble être le protocole intermédiaire entre CSMA 1-persistant et CSMA non persistant. Après avoir détecté un canal occupé, les nœuds restent en écoute sur le canal. Cependant, une fois que le canal est libre, ils ne transmettent qu'avec une probabilité  $p$ .

Dans les trois protocoles CSMA présentés ci-dessus, les auteurs supposent que tous les nœuds sont dans la portée des ondes radio des autres. Pourtant, cela n'est pas toujours le cas, car dans les réseaux sans fil, il y a des nœuds qui ne sont pas dans la portée des autres. Un nœud ne peut pas communiquer avec un autre si ce dernier est à l'extérieur de sa portée. Cela est complètement différent par rapport aux réseaux filaires où les nœuds partagent le médium de transmission filaire.

Quand un nœud transmet, tous les autres nœuds dans le réseau sont immédiatement au courant (ou dans un très court intervalle de temps) de cette transmission. Dans les réseaux sans fil, comme la portée des ondes radio est limitée, il existe quelques problèmes avec l'utilisation de CSMA. Ces problèmes sont bien connus sous le nom des problèmes des nœuds cachés et exposés (voire le premier chapitre). Les deux nœuds voisins sont connectés et la portée des ondes radio est limitée entre les voisins.

- Pour éviter le problème de la station cachée, F.A Tobagi et Al ont proposé une extension de CSMA nommé **BTMA** (Busy Tone Multiple Access) la même année. L'idée de BTMA est d'utiliser deux canaux de communication : le premier pour la transmission des trames de données et le deuxième pour signaler qu'un nœud est en état de réception. Quand un nœud reçoit des données sur le premier canal, il émet un signal occupé sur le deuxième canal pour que les nœuds voisins n'émettent pas. Ainsi, le fait d'utiliser deux canaux de communication rend BTMA compliqué en termes de conception de matériel.
- Quelques extensions de BTMA ont été proposées dont le premier est MACA. Les nœuds utilisent un seul canal de communication. Afin d'éviter le problème de la station cachée, **MACA (Multiple Access Collision Avoidance)** utilise les paquets de contrôle RTS (Request To Send) et CTS (Clear To Send). Un nœud échange les paquets de contrôle avant d'émettre les trames de données. Une fois qu'un nœud reçoit CTS après avoir envoyé RTS, il commence à transmettre immédiatement sans utiliser l'écoute de porteuse. Lorsque les nœuds voisins reçoivent ces paquets de contrôle, ils savent qu'il y a une transmission dans le médium et n'essaient pas d'accéder au canal immédiatement. Le protocole MACA fonctionne bien dans le cas où il n'y a pas d'erreurs de transmission. Mais, dans un réseau sans fil, des erreurs de transmission sont inévitables à cause du bruit ou d'obstacle dans l'environnement.
- **MACAW (MACA for Wireless LANs)** ajoute les paquets d'acquittement ACK (Acknowledgement) à la fin de chaque trame de données envoyée pour garantir une bonne transmission dans le réseau. MACAW améliore MACA en augmentant le débit du réseau.
- Avec le développement rapide de différentes techniques d'accès au médium des réseaux locaux sans fil, l'organisation IEEE a standardisé une norme pour ce type de réseau local sans fil nommé **IEEE 802.11**. Cette norme propose deux protocoles MAC : Fonction de Coordination Distribuée (DCF - Distributed Coordination Function) et Fonction de Coordination du Point d'Accès (PCF – Point Coordination Function).

- Le mode **DCF** est un protocole d'accès au médium purement distribué et il se base sur MACAW en ajoutant l'écoute d'un canal virtuel. Ce dernier est une évaluation du temps de transmission lorsqu'un nœud reçoit des paquets RTS, CTS, ACK des autres. Pendant cette durée de temps, les nœuds savent que le canal est occupé et ils essaient d'accéder au canal lorsque cette durée du temps expire
- Le mode **PCF** est un protocole d'accès au médium centralisé où la station de base gère tous les droits d'accès au canal de tous les nœuds dans le réseau.

Afin de faire coopérer les différents modes d'accès au canal, IEEE 802.11 propose différents intervalles inter-trame pour distinguer les différents niveaux de priorité : Intervalle Inter-trame court (**SIFS – Short Inter-frame Spacing**), Intervalle Inter-trame PCF (**PIFS – PCF Inter-frame Spacing**), Intervalle Inter-trame DCF (**DIFS – DCF Inter-frame Spacing**). Un nœud doit attendre un intervalle inter-trame et un temps back-off avant d'accéder au canal. L'intervalle inter-trame court est réservé pour les paquets de contrôle (e.g RTS, CTS, ACK). Lorsqu'un nœud reçoit un RTS ou une trame, il est sûr de gagner le canal pour répondre au transmetteur. Le standard IEEE 802.11 donne plus de priorité au mode PCF qu'au mode DCF. Après l'expiration de PIFS, la station de base a le droit d'accéder au canal afin de diffuser l'ordonnancement du temps d'accès au canal à tous les nœuds. Après tous ces intervalles de temps, si aucun nœud n'accède au canal, tous les nœuds attendent la fin de DIFS pour commencer la contention afin de décider le droit d'accès au canal (figure.2). Nous allons revoir la norme IEEE 802.11 dans la suite de ce chapitre.

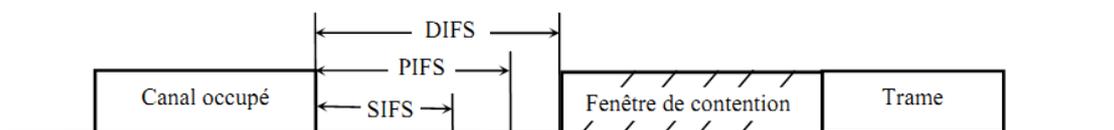


Figure 2.2 : Inter Frame Spacing dans 802.11

### 1.2. Protocoles MAC sans contention :

Dans cette famille de protocoles MAC, les nœuds accèdent au canal sans concurrence. Chaque nœud possède sa propre ressource pour accéder au canal et les

autres nœuds ne peuvent pas utiliser cette ressource. Les protocoles MAC sans contention sont divisés en trois catégories principales :

- Accès multiple par répartition dans le temps (Time Division Multiple Access TDMA).
- Accès multiple par répartition en fréquence (Frequency Division Multiple Access-FDMA).
- Accès multiple par répartition en code (Code Division Multiple Access - CDMA).

Nous allons analyser ces trois catégories en détail dans ce qui suit.

### 1.2.1. Accès multiple par répartition dans le temps (TDMA) :

Dans ce type de protocole MAC, chaque nœud a un intervalle de temps où il peut accéder au canal.

Un nœud ne peut pas accéder au canal pendant l'intervalle de temps réservé à un autre. De ce fait, il n'y a jamais de collision dans ce type de protocole MAC. Cependant, il faut toujours un ou plusieurs nœuds coordinateurs qui attribuent les intervalles de temps aux autres. Pour que TDMA puisse bien fonctionner, il faut un bon niveau de synchronisation entre les nœuds (quelques  $\mu$ s).

Quand la topologie du réseau change, il faut changer aussi les intervalles de temps attribués pour les nœuds. A première vue, on peut dire que TDMA est bien adapté aux MANETs en ce qui concerne la consommation d'énergie car il n'y a pas du tout de collisions. Cependant, l'attribution des intervalles de temps de TDMA est effectuée d'une manière statique. Si un nœud se voit attribuer un intervalle de temps et qu'il n'a pas de données à transmettre, il ne peut pas laisser cet intervalle de temps à quelqu'un d'autre. C'est aussi un gaspillage de bande passante et d'énergie. D'ailleurs, l'approche centralisée de TDMA semble moins adaptable aux réseaux ad hoc mobiles.

### 1.2.2. Accès multiples par répartition en fréquence (FDMA) :

Dans ce type de protocole MAC, chaque nœud possède plusieurs bandes de fréquence différentes.

Un nœud connaît la fréquence de ses voisins. Quand il veut transmettre des trames de données à un de ses voisins, il choisit la fréquence de ce voisin pour transmettre. Les nœuds peuvent faire plusieurs transmissions simultanément dans la portée des

autres sans les interférer. Nous pouvons imaginer ce type de protocole MAC comme le trafic sur une autoroute avec plusieurs voies dont chacune représente une bande de fréquence. Les véhicules représentent les trames de données et elles peuvent circuler chacune sur une voie sans perturber les autres. FDMA possède un gros avantage car il peut fonctionner sans interférence et avec un débit important. En effet, chaque transmission est réalisée sur une bande de fréquence différente. Cette technique est utilisée dans le domaine du téléphone mobile où la taille des terminaux est assez importante et il n'y a pas trop de contrainte de prix. FDMA requiert une conception complexe avec des circuits complémentaires, ce qui augmente le prix des dispositifs. De ce fait, FDMA n'est pas un bon candidat pour le protocole MAC des MANETs. Cela explique la raison pour laquelle il n'y a pas beaucoup de travaux sur le protocole MAC de ce type.

### 1.2.3. Accès multiple par répartition de code (CDMA) :

Dans ce type de protocole MAC, les nœuds ont seulement une bande de fréquence pour faire les transmissions. Ceci est pris comme une hypothèse des protocoles MAC basés sur la contention.

Dans les protocoles d'accès multiple par écoute de porteuse, quand plusieurs nœuds transmettent en même temps dans la même portée, il y a une collision et le récepteur reçoit seulement un bruit.

Ce n'est plus le cas dans CDMA où on considère que différentes trames de données peuvent se chevaucher de façon linéaire. Ainsi, chaque nœud possède un code différent. Il diffuse son code à ses voisins. Donc, un nœud garde aussi une liste des codes de tous ses voisins. Quand un nœud veut transmettre une trame de données, il code sa trame de données avec son propre code et l'envoie au récepteur. Plusieurs nœuds peuvent transmettre les données codées en même temps en utilisant leur propre code. Le récepteur utilise le code de son transmetteur pour recevoir les trames qui viennent du transmetteur. En utilisant le code de son transmetteur, tous les bruits créés par les autres transmetteurs sont détruits et le récepteur peut recevoir une bonne trame de données même si il y a des interférences.

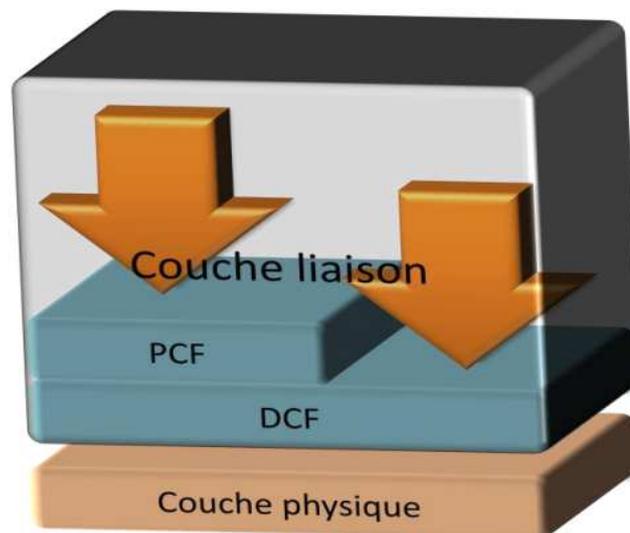
CDMA est avantageux car les nœuds utilisent la même bande de fréquence, sans collision, sans problème d'interférence avec une faible latence. Cette technique est beaucoup utilisée aux États-Unis dans le domaine des téléphones mobiles.

Cependant, la station de base est le seul nœud qui distribue les codes aux autres dans le réseau. C'est donc une approche centralisée qui n'est pas adaptable aux MANETs.

### 2. Description de la couche MAC IEEE 802.11 :

Le protocole d'accès au médium est en charge d'éviter les collisions, d'assurer le partage de la bande passante et de résoudre certains problèmes spécifiques aux transmissions hertziennes.

La couche MAC du standard 802.11 se base sur la méthode d'accès appelée « Distributed Coordination Function »(DCF) qui utilise CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) pour supporter des transmissions asynchrones de données. La deuxième fonction d'accès, optionnelle, est la PCF (Point Coordination Function) qui sert à supporter les trafics temps réel. La fonction DCF est employée pour les réseaux Ad hoc (figure 2.3).



**Figure 2.3: architecture la norme IEEE 802.11**

Le principe de la fonction DCF consiste à écouter le médium pour voir si un autre nœud est en train d'émettre, pour savoir si le médium est libre pour une certaine durée appelée (DIFS) avant d'émettre. Sinon, la transmission est différée d'un temps de Backoff, choisi aléatoirement entre 0 et une valeur maximale appelée Contention Window (CW). Cette dernière ne sera décrétementée que si le médium est libre.

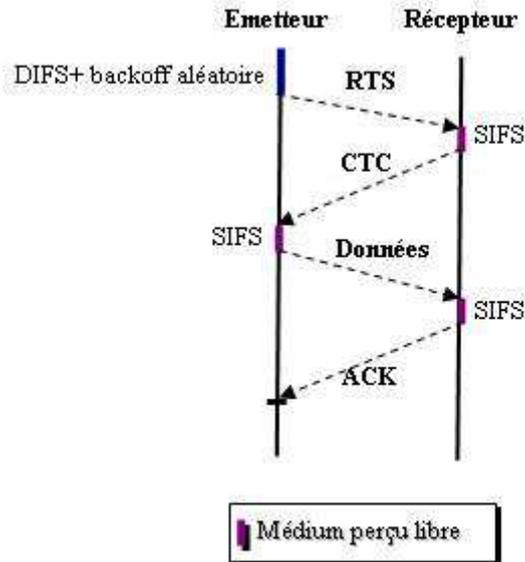


Figure 2.4 : Principe de la fonction DCF

Néanmoins, la détection de collision par une station qui est entrain d'émettre simultanément avec une autre n'est pas possible. Pour cela, un acquittement (ACK) est utilisé pour informer la station émettrice que la trame est reçue avec succès.

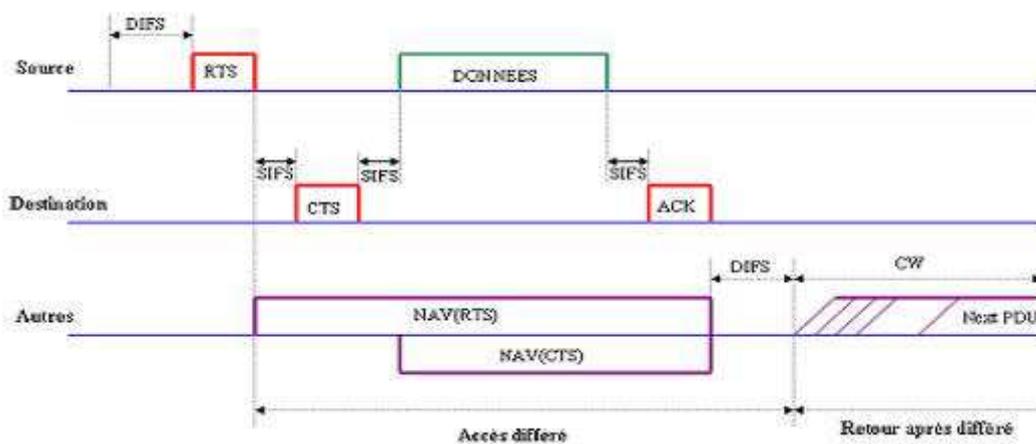


Figure 2.5 : Méthode d'accès DCF

Un principe RTS/CTS (Request To Send / Clear To Send) est utilisé pour résoudre le problème des stations cachées. Avant toute émission la station devra envoyer un message RTS pour réserver le canal, la destination répond donc par un message CTS pour dire si elle est prête à recevoir. Ainsi, le canal est réservé pour la durée de la transmission. Les messages RTS/CTS et ACK sont prioritaires à l'accès au médium,

car ils disposent d'un temps d'attente IFS (Inter Frame Space) inférieur à celui des paquets de données.

Dans la fonction DCF, les trames n'ont pas de priorités, ce qui est inadapté pour les applications temps réel. Un mécanisme de priorité pour la fonction DCF de la couche MAC 802.11 consiste à différencier les trafics, et introduire une priorité en modifiant les paramètres de la fonction d'accès DCF. Son principe consiste à associer des DIFS ou des temps de backoff plus court pour les flux prioritaires. Ainsi, les flux prioritaires auront une plus grande probabilité d'accéder au médium que les autres. D'autres paramètres de la fonction DCF peuvent aussi être utilisés pour différencier des services.

### **Conclusion :**

**L**es protocoles MAC sont divisés en deux familles principales : MAC basé sur la contention et MAC sans contention. Nous avons constaté que les travaux de recherche sur la première famille sont beaucoup plus riches que la deuxième famille. La raison est que la deuxième famille requiert soit une conception complexe, soit une synchronisation stricte entre les nœuds. Ces conditions ne s'adaptent pas à un environnement dynamique d'un réseau mobile ad hoc à large échelle.

**Introduction :**

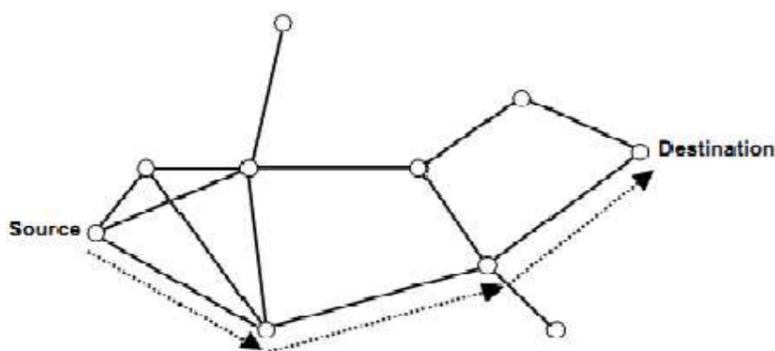
**U**n réseau ad hoc est une collection d'entités mobiles interconnectées par une technologie sans fil formant un réseau temporaire sans l'aide de toute administration ou de tout support fixe [BAC05].

Nous allons traiter le problème de routage dans les réseaux mobiles ad hoc. Nous allons étudier principalement quelques protocoles de routage qui ont été fait, et qui se font à l'heure actuelle, dans le but de résoudre le problème d'acheminement de données entre les hôtes mobiles du réseau ad hoc. Comme nous allons voir le problème de routage est très compliqué, cela est dû essentiellement à la propriété qui caractérise les réseaux ad hoc et qui est l'absence d'infrastructure fixe et de toute administration centralisée.

**1. Définition du routage :**

Le routage est une méthode d'acheminement des informations à la bonne destination à travers un réseau de connexion donné [LEM00]. Le problème de routage consiste à déterminer un acheminement optimal des paquets à travers le réseau au sens d'un certain critère de performance. Le problème consiste à trouver l'investissement de moindre coût en capacités nominales et de réserves qui assure le routage du trafic nominal et garantit sa serviabilité en cas de n'importe quelle panne d'arc ou de nœud.

**Exemple :** Si on suppose que les coûts des liens sont identiques, le chemin indiqué dans la figure suivante est le chemin optimal reliant la station source et la station destination. Une bonne stratégie de routage utilise ce chemin dans le transfert des données entre les deux stations.



**Figure 3.1 : le chemin optimal entre la source et la destination**

Le problème qui se pose dans le contexte des réseaux ad hoc est l'adaptation de la méthode d'acheminement utilisée avec le grand nombre d'unités existant dans un environnement caractérisé par de modestes capacités de calcul et de sauvegarde et de changements rapides de topologies.

Il semble donc important que toute conception de protocole de routage doive étudier les problèmes suivants [LEM00] :

- 1- La minimisation de la charge du réseau
- 2- Offrir un support pour pouvoir effectuer des communications multipoints fiables
- 3- Assurer un routage optimal
- 4- Offrir une bonne qualité concernant le temps de latence.

#### **2. Méthodes utilisées par les protocoles de routage Ad-hoc :**

Le protocole de routage doit garder la trace des changements sur le réseau et doit partager ces changements avec des nœuds dans le réseau. La plupart des protocoles de routage Ad-hoc utilise deux méthodes majeures : vecteur de distance (Distance Vector) et état de lien (Link State).

##### **2.1 Distance Vector (DV) : vecteur de distance [SOU03] :**

Les protocoles de routage à base de la méthode DV établissent une table de routage recensant le « coût » de chacune des routes du réseau puis transmettent cette table périodiquement aux nœuds voisins. Au début, chaque nœud détecte ses voisins directs et construit sa propre table de routage puis il la diffuse à ses voisins. Les tables sont mises à jour en fonction des informations reçues (ajout et modification d'une entrée) et convergent jusqu'à ce que la structure du réseau à travers ces tables se stabilise. Chaque entrée de la table de routage est un triplet (nœud destinataire, nœud suivant, métrique) où la métrique est le coût de la route pour atteindre le nœud destinataire en passant par le nœud suivant. La métrique utilisée peut être le nombre de sauts, le délai d'acheminement, le nombre total de paquets en file d'attente pour ce parcours, ou un critère semblable. Les mises à jour régulières entre les nœuds permettent de communiquer les modifications de topologie.

DSDV et AODV sont des protocoles de routage qui utilisent la méthode DV.

### 2.2. Link State (LS) : état de lien [SOU03] :

Les protocoles de routage utilisant la méthode LS écoutent le réseau en continu afin de recenser les différents éléments qui l'entourent. Chaque nœud a une vue globale du réseau représenté par un graphe. A partir de ces informations (temps, nombre de sauts, distance réelle, délai de transmission, fiabilité, etc.), chaque nœud calcule le plus court chemin (à l'aide de l'algorithme de Dijkstra [DIJ11]) vers les nœuds du réseau et diffuse cette information sous forme de paquets de mise à jour. Les protocoles à état de lien ont été conçus pour pallier les limitations des protocoles de routage utilisant le vecteur de distance. Ils ont pour avantage de répondre rapidement aux moindres changements sur le réseau en envoyant des mises à jour déclenchées uniquement après qu'une modification soit survenue.

Dès qu'un nœud détecte la modification d'une liaison ou d'une route, il crée une mise à jour de routage à état de lien (LSA, Link State Advertisement) concernant cette liaison. Cette mise à jour LSA est ensuite transmise à tous les nœuds voisins. Chacun d'eux en prend une copie, met à jour sa base de données (graphe) à état de lien et transmet la mise à jour LSA aux autres nœuds voisins. Cette diffusion de mises à jour LSA est nécessaire afin que tous les nœuds puissent créer des bases de données transcrivant de manière précise la topologie du réseau et mettre à jour leur table de routage.

OLSR est un protocole de routage basé sur LS.

### 2.3. Distance Vector vs Link State:

Il y a deux grandes différences entre DV et LS. La première est que DV échange les mises à jour de routage périodiquement même s'il n'y a pas de changements de topologie. Cela maximise le temps de convergence et augmente les risques de boucles de routage. D'autre part, LS ne déclenche pas d'envois de mises à jour de routage que lors du changement de topologie. Après la première inondation, des mises à jour d'état des liens seront envoyées à tous les autres nœuds. Ceci permet de minimiser le temps de convergence et c'est la raison pour laquelle il n'y a aucune chance de boucles de routage. La deuxième différence est que dans DV, un nœud se base sur les informations de ses voisins connectés directement afin de calculer et d'accumuler des informations sur les routes. Au contraire, dans LS, un

noeud ne se base pas uniquement sur l'information de ses voisins pour calculer l'information sur la route. LS a un système de bases de données qui est utilisé afin de calculer le meilleur chemin pour des destinations dans le réseau en utilisant l'algorithme de Dijkstra. Pour cela, DV nécessite très peu de chargements depuis la mémoire et de puissance du processeur par rapport à LS.

#### **2. 3. Routage hiérarchique ou plat :**

Le premier critère utilisé pour classifier les protocoles de routage dans les réseaux ad hoc concerne le type de vision qu'ils ont du réseau et les rôles qu'ils accordent aux différents mobiles.

**2.3.1. Les protocoles de routage à plat :** considèrent que les noeuds sont égaux. La décision d'un noeud de router des paquets pour un autre dépendra de sa position. Parmi les protocoles utilisant cette technique, on cite l'AODV (Ad hoc On Demand Distance Vector).

**2.3.2. Les protocoles de routage hiérarchiques :** fonctionnent en confiant aux mobiles des rôles qui varient de l'un à l'autre. Certains noeuds sont élus et assument des fonctions particulières qui conduisent à une vision en plusieurs niveaux de la topologie du réseau. Par exemple, un mobile pourra servir de passerelle pour certain nombre de noeuds qui se seront attachés à lui. Le routage en sera simplifié, puisqu'il se fera de passerelle à passerelle, jusqu'à celle directement attachée au destinataire. Dans ce type de protocole, les passerelles supportent la majeure partie de la charge de routage (les mobiles qui s'y rattachent savent que si le destinataire n'est pas dans leur voisinage direct, il suffit d'envoyer à la passerelle qui se débrouillera). Un exemple de protocole utilisant cette stratégie est l'OLSR (Optimized Link State Routing).

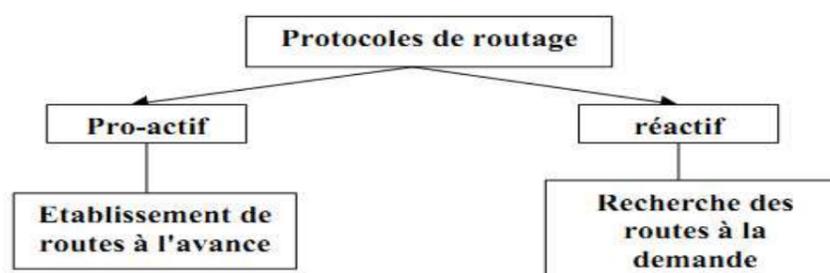
#### **2.4. Le routage à la source et le routage saut par saut :**

**2.4.1. Le routage à la source [BAC05] :** le routage à la source ou « source routing » consiste à indiquer dans le paquet routé l'intégralité du chemin que devra suivre le paquet pour atteindre sa destination. L'entête de paquet va donc contenir la liste des différents noeuds relayeur vers la destination. Le protocole le plus connu basant sur cette classe est DSR (Dynamic Source Routing).

**2.4.2. Le routage saut par saut [BAC05] :** le routage saut par saut ou « hop by hop » consiste à donner uniquement à un paquet l'adresse du prochain nœud vers la destination. AODV fait partie des protocoles qui utilisent cette technique.

### 3. Les protocoles de routage pour les réseaux ad hoc :

**3.1. Classification :** Suivant la manière de création et de maintenance de routes lors de l'acheminement des données, les protocoles de routage peuvent être séparés en deux catégories, les protocoles proactifs et les protocoles réactifs. Les protocoles proactifs établissent les routes à l'avance en se basant sur l'échange périodique des tables de routage, alors que les protocoles réactifs cherchent les routes à la demande [BAC05].



Classification des protocoles

Figure 3.2 : classification des protocoles de routage

**3.2. Les protocoles de routage proactifs :** Les protocoles de routage proactifs pour les réseaux mobiles ad-hoc (MANET), sont basés sur la même philosophie des protocoles de routage utilisés dans les réseaux filaires conventionnels. Les deux principales méthodes utilisées sont :

- La méthode Etat de Lien ("Link State").
- La méthode du Vecteur de Distance ("Distance Vector").

Les deux méthodes exigent une mise à jour périodique des données de routage qui doit être diffusée par les différents nœuds de routage du réseau.

Nous allons décrire dans ce qui suit, l'un des protocoles qui est OLSR.

**3.2.1. Le protocole de routage « OLSR » :** Le protocole OLSR (Optimized Link State Routing protocol) [ABD09], [BAC05] est un protocole proactif. Il applique dans un contexte ad hoc les règles de routage, cette fois centrées sur l'état du lien. Dans un protocole de routage par état de lien, tous les liens avec les nœuds voisins

sont déclarés et inondés dans le réseau. Cette technique permet à chaque nœud de connaître parfaitement une vision globale sur la topologie du réseau. En utilisant cette carte topologique, un nœud source peut choisir le chemin le plus court vers une destination en appelant l'algorithme Dijkstra [DIJ11], couramment utilisé dans les techniques de découverte de routes d'une source vers une destination. Le protocole OLSR, est une optimisation de l'algorithme d'état de lien pure pour les réseaux Ad hoc : il réduit la taille des messages de contrôle, au lieu de tous les liens, il déclare un sous ensemble de liens avec ses voisins qui sont les relais multipoints (MPR) ; il minimise le coût d'inondation du trafic de contrôle par l'utilisation seulement des nœuds relais multipoint pour diffuser ses messages. Seuls les MPRs retransmettent les messages diffusés. La technique des relais multipoints réduit significativement le nombre des retransmissions redondantes lors de diffusion.

Les nœuds OLSR échangent périodiquement des messages de contrôle et maintiennent des routes pour atteindre tout nœud OLSR du réseau. Le protocole OLSR réalise principalement deux fonctionnalités : Détection de voisinage et Gestion de la topologie.

**3.2.1.1. Détection de voisinage [ABD09] :** Chaque nœud doit détecter toutes les interfaces de ses voisins ayant un lien direct et symétrique avec l'une de ses interfaces. En raison de l'incertitude de la propagation radio, le lien entre deux nœuds voisins peut être unidirectionnel. Les liens doivent donc être vérifiés dans les deux sens avant de les considérer comme valides. Alors, chaque nœud doit diffuser périodiquement un message *Hello* dans son voisinage direct (TTL=1). Ce message contient les informations relatives aux interfaces entendues par ce nœud : la liste des adresses des interfaces des nœuds voisins avec leurs états de lien. Un lien entre les interfaces d'un nœud et son voisin peut avoir l'un des quatre états suivant : « symétrique », « asymétrique », «MPR» ou « perdu ». Symétrique signifie que le lien est validé comme bidirectionnel est qu'il est possible de transmettre des données dans les deux sens. Asymétrique signifie que le nœud entend cette interface de voisin mais le lien n'est pas encore validé dans l'autre sens. MPR indique que ce nœud a sélectionné ce voisin comme relais multipoint et cela implique que le lien est symétrique. Perdu indique le lien avec cette interface de voisin n'est plus valide.

Les informations de voisinage sont maintenues dans une base d'information concernant les voisins directs et leurs interfaces multiples, les voisins à deux sauts, les relais multipoints et les sélecteurs de relais multipoint. La figure montre un exemple

de détection de voisinage. Chacun des nœuds possède une seule interface sans fil. Il est nécessaire qu'un nœud possédant plusieurs interfaces, choisisse l'adresse d'une de ses interfaces comme son adresse principale.

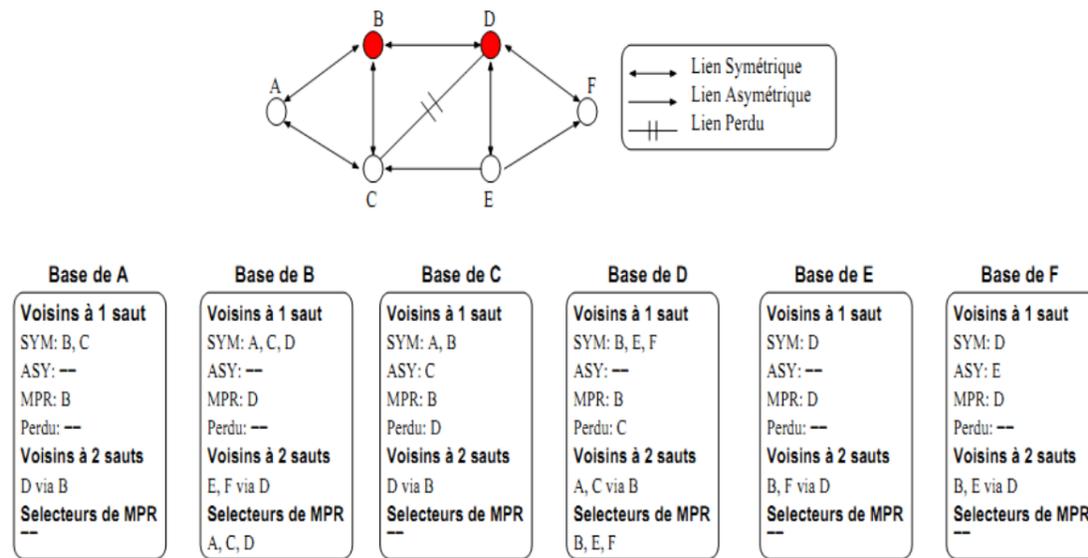


Figure 3.3 : exemple d'information de voisinage maintenue par OLSR [ABD09].

➤ **Le concept des relais multipoint [ABD09]** : Le concept de relais multipoint vise à diffuser efficacement les messages destinés à tous les nœuds du réseau ad hoc (par exemple, les messages TC : Topology Control). La transmission radio étant par défaut une inondation à tous les voisins directs. Les nœuds à deux sauts d'une source peuvent être joints par une retransmission d'un ou plusieurs voisins directs. L'idée de base est de désigner un nombre suffisant de voisins appelés relais multipoint permettant de réduire le nombre de retransmissions redondantes dans la même région du réseau.

En se basant sur l'information de voisinage, chaque nœud  $s$  sélectionne indépendamment un sous-ensemble minimal de nœuds parmi ses voisins directs pour retransmettre ses paquets. Ces nœuds possèdent des liens symétriques avec  $s$  et leur ensemble est noté  $MPR(s)$ . Les nœuds voisins de  $s$  qui ne sont pas des relais multipoints de ce nœud, reçoivent et traitent les messages diffusés par  $s$ , mais ne les retransmettent pas. Chaque nœud MPR maintient l'ensemble de ses sélecteurs de relais multipoint, noté Multipoint relay Selector (MS) et ne retransmet que les paquets reçu pour la première fois de ses sélecteurs de relais multipoint (voir figure). Cette technique réduit d'une façon significative le nombre de retransmissions lors du processus de diffusion. Les relais multipoint sont calculés suite à la détection d'un

changement de voisinage direct ou à deux sauts. La figure .a montre un exemple où un paquet de  $s$  est diffusé au voisinage à trois sauts par 24 retransmissions. Dans la figure .b seuls les relais multipoint retransmettent le paquet (12 retransmissions).

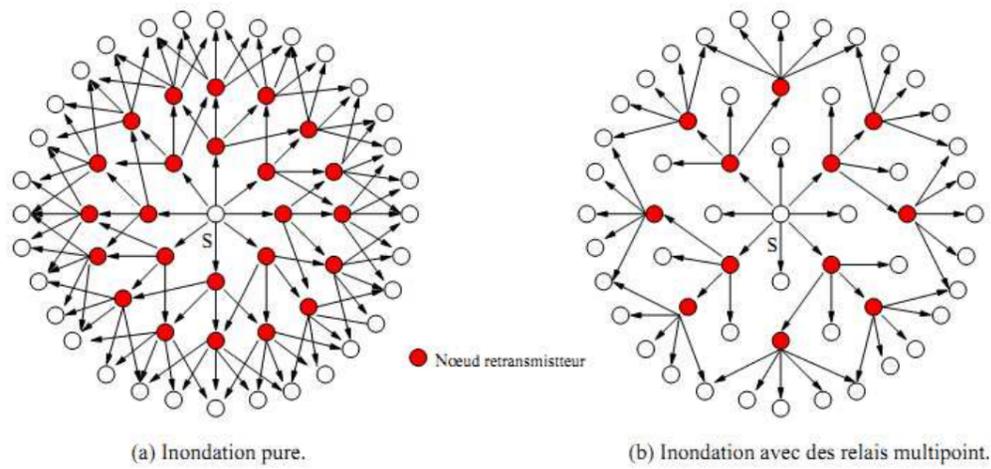


Figure 3.4 : Optimisation de l'inondation par des relais multipoint.

**3.2.1.2. Gestion de la topologie [ABD09] :** Chaque nœud sélectionné comme MPR dans le réseau diffuse périodiquement à tous les nœuds du réseau des messages de topologie, appelés Topology Control (*TC*) avec une fréquence déterminée par l'intervalle *TC\_Interval*. Un message *TC* contient les nœuds ayant sélectionné le nœud  $s$  origine du *TC* comme relais multipoint et un numéro de séquence associé à l'ensemble des sélecteurs de relais multipoint qui sera incrémenté à chaque changement de cet ensemble. Uniquement les nœuds MPRs ont le droit de rediffuser les *TCs*. La réception de ces messages *TCs*, permet à chaque nœud dans le réseau de maintenir une base contenant les informations topologiques du réseau qui donne une vision globale (mais non pas entière) de la topologie du réseau.

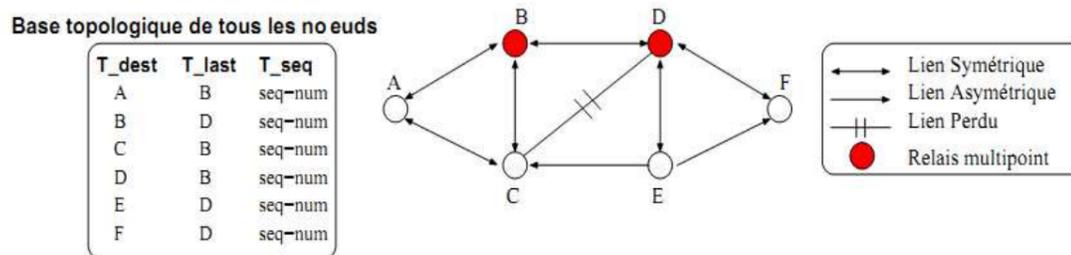


Figure 3.5 : exemple d'information de topologie maintenue par OLSR.

**3.2.1.3. Calcul des routes :** Le routage se fait saut par saut. Chaque nœud dans le réseau calcule sa table de routage pour atteindre tout autre nœud présent dans le réseau. Ce calcul est basé sur les informations de voisinage et de topologie rafraîchies périodiquement. Un nœud  $s$  utilise l'algorithme de Dijkstra, un algorithme du plus court chemin, sur le graphe de topologie partiel construit à partir des paires suivantes:

- Les liens  $(m, v)$  existants dans la table de voisinage, tels que  $v$  est un voisin symétrique de  $m$ ;
- Les liens  $(last, dest)$  existants dans la table de topologie.

Les routes trouvées sont optimales en nombre de sauts, sans boucles et les nœuds intermédiaires sont des relais multipoint. La table de routage est mise à jour chaque fois qu'il y a un changement dans la base de voisinage ou de la topologie. C'est-à-dire, quand on détecte l'apparition ou la perte d'un voisin ou lors de l'ajout ou la suppression d'un tuple de topologie.

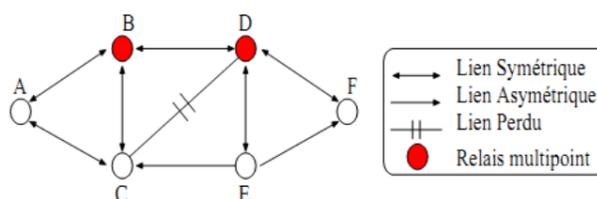


Table de routage de A			Table de routage de B			Table de routage de C			Table de routage de D			Table de routage de E			Table de routage de F		
R_dest	R_next	R_dist															
B	B	1	A	A	1	A	A	1	A	B	2	A	D	3	A	D	3
C	C	1	C	C	1	B	B	1	B	B	1	B	D	2	B	D	2
D	B	2	D	D	1	D	B	2	C	B	2	C	D	3	C	D	3
E	B	3	E	D	2	E	B	3	E	E	1	D	D	1	D	D	1
F	B	3	F	D	2	F	B	3	F	E	1	F	D	2	E	D	2

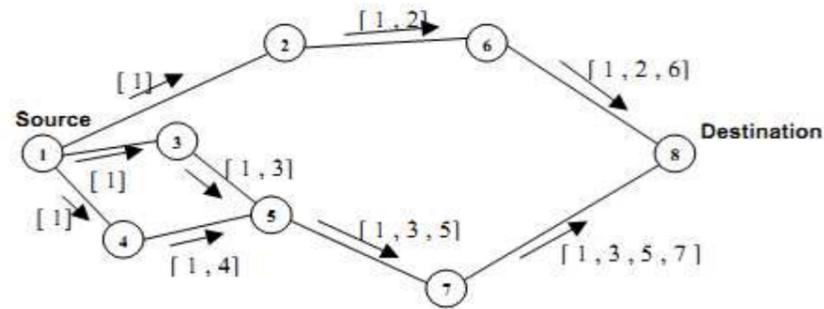
Figure 3.6 : exemple de routage maintenu par OLSR

**3.3. Les protocoles de routage réactifs [HAB08] :** Les protocoles de routage appartenant à cette catégorie, créent et maintiennent les routes selon les besoins. Lorsque le réseau a besoin d'une route, une procédure de découverte globale de routes est lancée, et cela dans le but d'obtenir une information spécifiée, inconnue au préalable.

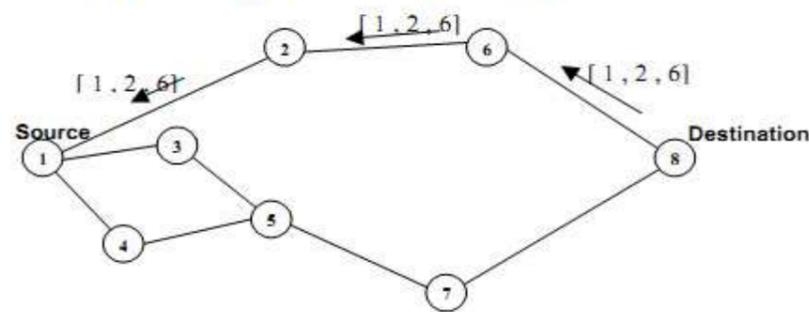
**3.3.1. Le protocole de routage « DSR » :**

- Le protocole "Routage à Source Dynamique" (DSR) [VDM06], est basé sur l'utilisation de la technique "routage source". Dans cette technique : la source des données détermine la séquence complète des nœuds à travers lesquelles, les paquets de données seront envoyés.

- Un nœud initiateur de l'opération de « découverte de routes », diffuse un paquet requête de route. Si l'opération de découverte est réussie, l'initiateur reçoit un paquet réponse de route qui liste la séquence de nœuds à travers lesquels la destination peut être atteinte. Le paquet requête de route contient donc un champ enregistrement de route, dans lequel sera accumulée la séquence des nœuds visités durant la propagation de la requête dans le réseau, comme le montre la figure suivante :



(a) Construction de l'enregistrement de route.



(b) Le renvoi du chemin.

La découverte de chemins dans le DSR.

Figure 3.7 : la découverte de chemins dans le protocole DSR

Afin d'assurer la validité des chemins utilisés, le DSR exécute une procédure de maintenance de routes :

- Quand un nœud détecte un problème fatal de transmission, à l'aide de sa couche de liaison, un message erreur de route (route error) est envoyé à l'émetteur original du paquet.
- Le message d'erreur contient l'adresse du nœud qui a détecté l'erreur et celle du nœud qui le suit dans le chemin.

- Lors de la réception du paquet erreur de route par l'hôte source, le nœud concerné par l'erreur est supprimé du chemin sauvegardé, et tous les chemins qui contiennent ce nœud sont tronqués à ce point là. Par la suite, une nouvelle opération de découverte de routes vers la destination, est initiée par l'émetteur.
- L'utilisation de la technique "routage source", fait que les nœuds de transit n'aient pas besoin de maintenir les informations de mise à jour pour envoyer les paquets de données, puisque ces derniers contiennent toutes les décisions de routage.
- Dans ce protocole, il y a une absence totale de boucle de routage, car le chemin source-destination fait partie des paquets de données envoyés.

### 3.3.2. Le protocole de routage « AODV » (Ad hoc On demand Distance Vector) :

- Le protocole AODV [HAB08], [VDM06] réduit le nombre de diffusions de messages, et cela en créant les routes lors du besoin, contrairement au DSDV, qui maintient la totalité des routes.
- L'AODV utilise les principes des numéros de séquence à fin de maintenir la consistance des informations de routage.
- A cause de la mobilité des nœuds dans les réseaux ad hoc, les routes changent fréquemment ce qui fait que les routes maintenues par certains nœuds, deviennent invalides. Les numéros de séquence permettent d'utiliser les routes les plus nouvelles (fresh routes).

De la même manière que dans le DSR, l'AODV [BAC05] utilise une requête de route RREQ dans le but de créer un chemin vers une certaine destination. Cependant, l'AODV maintient les chemins d'une façon distribuée en gardant une table de routage, au niveau de chaque nœud de transit appartenant au chemin cherché.

- Un nœud diffuse une requête de route dans le cas où il aurait besoin de connaître une route vers une certaine destination et qu'une telle route n'est pas disponible. Cela peut arriver :
  - Si la destination n'est pas connue au préalable, ou
  - Si le chemin existant vers la destination a expiré sa durée de vie ou il est devenu défaillant

- Le champ numéro de séquence destination du paquet RREQ, contient la dernière valeur connue du numéro de séquence, associé au nœud destination. Cette valeur est copiée de la table de routage. Si le numéro de séquence n'est pas connu, la valeur nulle sera prise par défaut. Le numéro de séquence source du paquet RREQ contient la valeur du numéro de séquence du nœud source.
- Afin de maintenir des routes consistantes, une transmission périodique du message "HELLO" est effectuée. Si trois messages "HELLO" ne sont pas reçus consécutivement à partir d'un nœud voisin, le lien en question est considéré défaillant.

Le protocole AODV ne présente pas de boucle de routage, en outre il évite le problème "counting to infinity", ce qui offre une convergence rapide quand la topologie du réseau ad hoc change.

#### Conclusion

**D**ans ce chapitre nous avons traité, le problème de routage dans les MANETs dit « Best effort », vu sa complexité dans ce genre de réseaux. Nous l'avons entamé par mettre en évidence les différents modèles de classification en se basant sur la manière d'acheminer les paquets de données ainsi que l'architecture de réseaux. Par la suite nous avons présenté quelques protocoles de routage du groupe MANET qui ont été proposés pour assurer le service de routage dans les réseaux ad hoc mobiles. Il existe d'autres protocoles qui ont été développés dans la littérature. Le groupe MANET a pour mission de normaliser des travaux qui sont effectués sur les réseaux ad hoc, s'efforce de trouver des protocoles adéquats et standards. Nous avons décrit leurs principales caractéristiques et fonctionnalités afin de comprendre les stratégies utilisées dans l'acheminement des données entre les différents nœuds.

Les protocoles proposés sont généralement classés en deux catégories : les protocoles proactifs et les protocoles réactifs. Les protocoles des deux catégories essaient de s'adapter aux contraintes imposées par les réseaux ad hoc, et cela en proposant une méthode qui soit de moindre cout en capacités et ressources, et qui garantit la disponibilité du routage en cas de panne de lien ou de nœuds. Les protocoles de

routage étudiés offrent différents avantages qui sont en réalité complémentaires et préférables pour différents types d'applications.

### Introduction :

**L**es MANETs sont les systèmes distribués complexes, se composent des appareils libres et dynamiques qui se communiquent via des canaux radio sans infrastructure. Pour transmettre les données dans les réseaux ad hoc, il faut utiliser le protocole TCP ou UDP dans la couche transport [EBQ05].

Le TCP est le protocole de la couche transport qui fournit une connexion fiable et orientée entre terminaux sur un réseau non fiable. En théorie, le protocole TCP est indépendant de la technologie dans les couches au-dessous. Malheureusement, le réseau sans fil et le réseau filaire sont différents en termes de la bande passante, de délai de propagation et de la fiabilité de lien. C'est pourquoi en pratique, la performance du TCP sur le réseau ad hoc est basse.

Actuellement, il existe déjà des algorithmes pour améliorer la performance de TCP dans les réseaux ad hoc, mais ils ne peuvent pas résoudre tous les problèmes et sont en train de développer. Alors le but est de faire une synthèse sur la réalité d'évaluer la performance de TCP sur les MANETs.

La couche transport, comme toutes les autres couches, constitue un défi à résoudre pour les MANETs. TCP, qui a été conçu pour les réseaux filaires, présente des limites quand il est appliqué aux réseaux sans fils multi-sauts. Dans ce chapitre, on va présenter brièvement le protocole TCP et son mécanisme de contrôle de congestion, expliquer pourquoi le TCP standard n'est pas efficace quand il est appliqué dans les MANETs en faisant le lien avec les propriétés et les caractéristiques de ces réseaux[NGU09].

### 1. Le protocole TCP :

TCP est la technologie prédominante utilisée sur l'Internet. Il s'agit d'un protocole de transport orienté connexion, fiable et qui permet le contrôle de congestion. Il est utilisé pour transporter différents types de trafic Internet : HTTP, FTP, SMTP et TELNET [EBQ05].

Le protocole TCP est un protocole de la couche transport. TCP est l'acronyme de « Transfert Control Protocol ». Il est décrit dans la RFC 793. Le protocole TCP permet

un transport fiable et en ordre des données de bout en bout grâce à son mécanisme d'acquittement et de l'utilisation de numéros de séquence. TCP est un protocole orienté connexion, les applications communiquent alors entre elles comme si elles étaient physiquement connectées. Avant que les deux applications puissent s'échanger des informations, elles doivent établir une connexion entre elles. Cette phase d'établissement permet aux deux applications d'échanger et d'initialiser plusieurs paramètres du protocole. Une fois la connexion établie, les deux applications peuvent commencer à envoyer leurs données.

TCP fournit un service de contrôle de flux afin de s'assurer que le transmetteur n'envoie pas à un taux que le récepteur ne peut pas supporter et cause ainsi un dépassement de mémoire au niveau du tampon. Pour assurer ce contrôle de flux, TCP utilise une variable nommée « *receive window* » qui indique au transmetteur l'espace disponible dans le tampon du récepteur.

- **Définition de la congestion :** La congestion est un phénomène causé par la saturation d'un ou plusieurs nœuds de commutations de paquets. Ceci entraîne une augmentation des délais et une possibilité de pertes de paquets. Les techniques de temporisation puis de retransmission aggravent le phénomène de congestion, jusqu'à ce que le réseau devienne inutilisable.

### 2. Conséquences des problèmes liés aux MANETs sur le protocole TCP : [NGU09] :

#### 2.1. Canal bruyant :

Le canal bruyant provoque quelque problème pour transmettre les données entre nœuds généralement, pas seulement pour TCP.

- l'affaiblissement du signal : quand la distance est longue entre deux nœuds ou il existe les objets au milieu des nœuds (un mur, un bâtiment, etc.). C'est la déconnexion des nœuds, elle entraîne la perte des paquets envoyés. Les nœuds déconnectés doivent reconnecter pour continuer à transmettre les données. Le temps de reconnexion doit être plus petit que le délai d'attente possible des protocoles de transmission (TCP, UDP) et des applications dans les couches supérieures.

- le multipath du signal à la destination cause le reçu d'un paquet plusieurs fois. Dans le protocole TCP, quand le récepteur reçoit plusieurs segments avec la même

séquence, il va répondre par « dupACK » à l'émetteur. L'émetteur reçoit plus de trois « dupACK », il va exécuter le mécanisme de contrôle de congestion (diminuer la fenêtre de la congestion).

### 2.2. Nœuds cachés et exposés :

Les problèmes des nœuds cachés et exposés existent si deux nœuds transmettent en même temps. Ce problème dégrade la performance du TCP parce qu'un nœud ne peut pas recevoir les segments de deux autres nœuds en même temps, ou il ne peut aussi recevoir un segment et expédie ce segment à un autre nœud immédiatement comme dans le réseau filaire [NGU09].

### 2.3. Mobilités des nœuds :

La mobilité des nœuds peut changer la topologie de réseau par la séparation et la réunion des nœuds. Pendant la séparation et la réunion des nœuds, la connexion TCP établit entre deux nœuds peut être en panne temporellement. Ce problème provoque la perte des paquets, cette perte est différente que celle causée par la congestion, mais le TCP original ne peut pas les distinguer. Le TCP se comporte comme la situation de la congestion pour les deux cas de pertes. Il va diminuer la valeur de la fenêtre de congestion pour limiter le nombre de segments envoyés. Cette action est adéquate pour le contrôle de la congestion, mais elle n'est pas nécessaire pour la perte causée par le changement de la topologie du réseau. Après le rétablissement de la connexion, la source peut envoyer les données avec la valeur de la fenêtre de congestion comme avant la déconnexion. Le faux routage et la séparation du réseau existent souvent dans les réseaux radio multi sauts, donc ils influencent sur la performance du TCP.

## 3. Caractéristiques du protocole TCP :

### 3.1. Le transfert fiable des données [NAA10] :

TCP fournit un transfert de données fiable. Un transfert fiable assure que les données envoyées arrivent au destinataire sans erreurs, non dupliqués et en séquence. Pour assurer ce transfert fiable, TCP utilise essentiellement les deux notions suivantes : les temporisateurs et les acquittements (ACK). Au moment où le segment est émis, TCP déclenche un temporisateur. Si le transmetteur ne reçoit pas un acquittement relatif

au segment émis avant l'expiration du temporisateur, le segment sera considéré comme perdu et le segment devra être retransmis. La question qui se pose à ce niveau est la valeur à assigner au temporisateur. Normalement, la valeur du temporisateur doit être supérieure au temps nécessaire à la transmission du segment jusqu'à la réception de son acquittement, soit le délai aller-retour, ou RTT (*Round Trip Time*). En effet la valeur du RTT est variable, et par suite si la valeur du temporisateur est inférieure au RTT alors on aura un *timeout* prématuré et une retransmission non nécessaire. Dans le cas où la valeur du temporisateur est beaucoup plus grande que le RTT, il y aura une lente réaction à la perte du segment.

### 3.2. Le contrôle de congestion TCP [NAA10] :

Une autre composante clé du protocole TCP, et qui peut être classifiée comme le plus grand avantage que TCP a apporté à Internet est son mécanisme de contrôle de congestion. TCP utilise un contrôle de congestion de bout en bout. Le principe de base est que chaque source TCP limite son débit de transmission en fonction de l'état de congestion tout au long du chemin vers la destination. Si aucune congestion n'a été détectée alors la source TCP peut augmenter son débit de transmission. Dans le cas de perception de congestion en détectant une perte de paquets, la source TCP doit réduire son débit de transmission pour ne pas aggraver encore la situation. Pour le contrôle de congestion, TCP utilise une variable appelée fenêtre de congestion et notée *CWnd*. Cette fenêtre constitue une limite pour le taux d'envoi pour la source TCP. Elle constitue le nombre maximal de paquets que l'émetteur peut envoyer sans recevoir d'accusé de réception. Comment la source TCP règle-t-elle son débit de transmission ? Comment TCP détecte-t-il ou s'aperçoit-il de la congestion? C'est le rôle de l'algorithme de congestion de TCP.

La RFC 2581 a défini quatre algorithmes qui globalement réalisent le contrôle de congestion :

- **Slow Start (démarrage lent)** : quand une connexion TCP commence, TCP ne sait rien de l'état et de la charge du réseau. La phase de démarrage consiste alors à tester la bande passante disponible. Au démarrage d'une connexion, cet algorithme initialise la valeur de la fenêtre de congestion *CWnd* à 1. Après la réception de l'acquittement, TCP transmet deux segments. Ainsi le transmetteur TCP augmente le taux d'envoi exponentiellement en doublant la

valeur de la fenêtre de congestion  $CW_{nd}$  à chaque RTT. Ce processus continue jusqu'à la détection d'une première perte soit à travers le déclenchement d'un timeout, soit suite à la réception de plus de 2 acquittements dupliqués. Dans ce cas l'algorithme *congestion avoidance* prend la relève. Le seuil de détection de congestion est déterminé à la détection d'une perte d'un segment et correspond à la moitié de la taille de la fenêtre  $CW_{nd}$ .

- **Congestion avoidance (évitement de congestion)** : pendant la phase *Slow Start*, la fenêtre de congestion augmente exponentiellement d'où le risque d'une saturation rapide du réseau. Le but de cet algorithme est alors de réduire la cadence d'envoi après avoir atteint un certain seuil. Cette phase commence au moment où  $CW_{nd} > \text{seuil de détection de congestion}$ . Pendant cette phase la fenêtre de congestion  $CW_{nd}$  augmente linéairement. La valeur de  $CW_{nd}$  est incrémentée de 1 à chaque RTT indépendamment du nombre d'acquittements reçus durant ce RTT. S'il y a eu une détection de perte, suite à un timeout ou bien suite à la réception de plus de deux acquittements dupliqués, le seuil est réduit à sa moitié. Si la perte a été détectée suite à un timeout,  $CW_{nd}$  est mis à 1 et on reprend avec la phase *Slow Start*, mais si elle a été détectée suite à la réception de trois acquittements dupliqués ou plus TCP exécute les algorithmes *Fast Retransmit* et *Fast Recovery* qu'on va présenter ci-dessous.
- **Fast Retransmit (retransmission rapide)** : lorsqu'un accusé de réception porte le même numéro qu'un accusé de réception précédemment envoyé pour le dernier segment ordonné reçu, on dit que ces accusés de réception sont dupliqués. Cet algorithme considère que la réception de plus de deux accusés de réception dupliqués est une indication qu'au moins un segment a été perdu. La source TCP ne va pas attendre le déclenchement du timeout pour retransmettre le segment perdu : il va le retransmettre immédiatement, réduire sa fenêtre de congestion de moitié et passer à l'algorithme *Fast Recovery*.
- **Fast Recovery (recouvrement rapide)** : cet algorithme part du principe que la réception de trois accusés de réception ou plus n'est pas un signe d'une

congestion sévère. En conséquence, au lieu de passer à la phase de *slow start*, cet algorithme reprend la transmission avec une large fenêtre et l'incrémente comme dans la phase d'évitement de congestion.

#### 4. Les défis de TCP dans les MANETs :

Initialement conçu pour les réseaux filaires où les erreurs de transmissions et donc les pertes de paquets sont rares, le protocole TCP fait face à plusieurs défis quand il est déployé dans les MANETs [NAA10].

Dans la littérature, les auteurs observent à partir de leurs simulations que le débit de TCP est, approximativement, inversement proportionnel au nombre de sauts du chemin de transmission sans fil. Les problèmes des nœuds cachés et exposés peuvent être à l'origine de la dégradation de performance de TCP. Il est à noter que dans cette étude on utilise une seule radio. Le mécanisme RTS/CTS et ACK ait été proposé pour résoudre le problème des nœuds cachés dans les WLANs. Toutefois, il existe encore une grande probabilité que le problème se produise lors de la transmission des paquets de données. La perte des messages RTS constitue la majorité des pertes dues aux problèmes des nœuds cachés (73% des pertes). Puisque la transmission avec succès d'un paquet TCP nécessite la transmission avec succès d'un RTS, la performance de TCP se voit alors dégradée suite à ces pertes.

Dans les réseaux sans fils multi-sauts mobiles, l'accès au canal se produit à chaque nœud dans le chemin. Ces erreurs de transmission dues aux nœuds cachés vont augmenter le délai d'accès au canal pour les paquets TCP ce qui conduit à une ouverture plus lente de la fenêtre de congestion et par conséquent une diminution du débit TCP.

D'autre part, le problème du nœud exposé qu'on a déjà expliqué conduit à une utilisation inefficace du canal entre les nœuds adjacents puisqu'il arrive qu'un nœud diffère inutilement ses transmissions.

Autres que les problèmes qu'on vient de citer et d'une manière générale, TCP connaît les défis suivants quand il est déployé dans les MANETs [NAA10], [NGU09] :

- **Les erreurs de transmission, la détection et le contrôle imprécis de congestion** : la perte de paquets due aux erreurs de transmission est très fréquente dans le contexte des MANETs. Ces pertes de paquets sont considérées par TCP comme des signes de

congestion. TCP va alors diminuer la taille de sa fenêtre de congestion et par suite le débit sera atténué. Donc le TCP classique ne différencie pas les pertes liées aux congestions et celles liées aux erreurs de transmission. D'autre part, dans les MANETs, les coupures de liens sont fréquentes. Ces coupures de liens engendrent un calcul de nouveaux chemins. Puisque tous les chemins ont des RTTs différents, la mesure du RTT sur les différentes routes résulte en une large variance de son estimation ce qui donne une grande valeur pour le temporisateur de retransmission.

- **Le rétablissement des routes** : suite aux coupures de liens, les nœuds procèdent à un nouveau calcul de route. Une fois la route recalculée, TCP entre dans la phase du départ lent pour chercher la bande passante disponible. Cette entrée dans cette phase engendre une dégradation du débit.

- **L'ordonnement des paquets TCP à la réception** : dans les MANETs, les paquets peuvent suivre des chemins différents et arriver à la destination d'une manière désordonnée. S'ils ne sont pas traités parfaitement, des retransmissions de paquet sont nécessaires.

- **Asymétrie des réseaux** : on parle de réseaux asymétriques quand le chemin de l'aller ou de transfert est différent du chemin du retour en termes de débit, de latence et de taux de perte. Ce phénomène est plus important dans les réseaux multi-sauts pour différentes raisons. Les paquets et les ACKs peuvent prendre des chemins différents et ainsi ils auront une bande passante, un débit, et un taux de perte différents. Même dans le cas où ils prennent le même chemin, le problème peut toujours exister puisque la condition de canal et la bande passante changent au cours du temps. Puisque le contrôle d'erreur de TCP se base sur la temporisation des ACKs, une perturbation au niveau du feedback peut diminuer la performance. La bande passante des liens de retour peut changer et augmenter l'inter-espacement original entre les ACKs arrivant à l'émetteur, ce qui va causer un ralentissement de l'évolution de la fenêtre de congestion. D'autre part, si des données sont envoyées dans le chemin de retour, les ACKs vont trouver le chemin chargé et vont être enfilés derrière les paquets ce qui augmente le délai et la probabilité de ces ACKs et par suite il y aura une dégradation de la performance de TCP.

### 5. Solutions proposées :

Pour résoudre ces problèmes, plusieurs solutions ont été proposées. Nous allons énumérer quelques unes :

#### 5.1. TCP-F (TCP Feedback):

##### Algorithme proposé:

L'algorithme TCP-F [NGU09], [EBQ05] est proposé pour résoudre le problème suivant :

- le TCP dans les réseaux ad hoc ne peut pas distinguer la perte due à la congestion et la perte due à la déconnexion. Ce problème influence sur l'algorithme de contrôle de la congestion. Le TCP se comporte d'une manière semblable dans les deux cas de perte, il va diminuer la fenêtre d'émission. Le TCP-F est utilisé pour distinguer les deux cas de perte.

- ✓ Deux types de messages de notification :
  - RFN : Route Failure Notification : un nœud va envoyer cette notification à la source quand il détecte l'interruption à cause de la mobilité du prochain nœud.
  - RRN : Route Re-establishment Notification : quand un nœud qui reçoit RFN trouve un routage à la destination, il va envoyer RRN à la source.
- ✓ L'algorithme :
  - Un nœud détecte l'interruption de la connexion au prochain nœud, il envoie RFN à la source.
  - En recevant RFN, la source procède :
    - Arrêter d'envoyer les paquets proches.
    - Être en congélation et commencer à compter le temps de faux routage.
    - Rétablir la connexion et transporter les données quand elle reçoit RRN ou le temps de faux routage est assez long.

### 5.2. TCP Split [EBQ05] :

L'algorithme n'est pas proposé pour résoudre le problème de cas de perte comme TCP-F, il est proposé pour améliorer la performance du TCP. L'idée principale de cet algorithme est de séparer une longue route en plusieurs segments par deux « proxy » aux deux bouts de segments. Ces « proxy » sont comme les entrepôts temporels, ils interceptent les segments de la source, stockent temporairement dans la mémoire tampon, expédient les segments à la destination. A chaque fois qu'une destination demande de retransmettre un segment, le « proxy » le plus proche qui a ce segment va le retransmettre à la destination à la place de la source.

#### Algorithme proposé :

- Séparer une longue route en plusieurs segments.
- Mettre deux « proxy » aux deux bouts de segments.
- Les fonctions de « proxy » sont :
  - Intercepter les paquets.
  - Stocker temporairement les paquets.
  - Retransmettre les paquets au « proxy » prochain ou à la destination.
  - Envoyer le « LACK message » au « proxy » préalable ou à la source.
  - Supprimer les paquets en recevant « LACK message ».

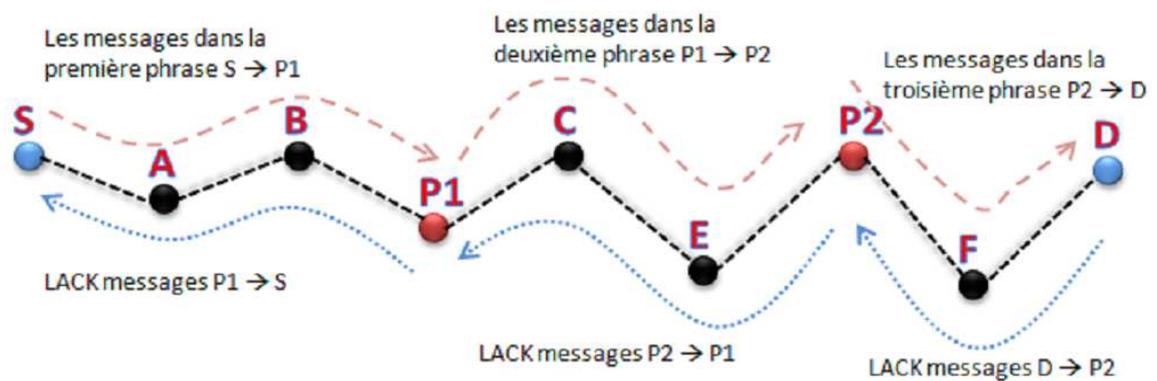


Figure 4.1 : TCP Split

### Conclusion :

**D**ans cette section, nous avons étudié l'un des protocoles responsables de transmettre les données au sein des réseaux ad hoc mobiles (MANETs), qui est le protocole TCP (Transfert Control Protocol) dans la couche transport de la pile OSI (Open Systems Interconnect).

Nous avons présenter brièvement le protocole TCP et son mécanisme de contrôle de congestion, expliquer pourquoi le TCP standard n'est pas efficace quand il est appliqué dans les MANETs en faisant le lien avec les propriétés et les caractéristiques et leurs conséquences pour ces réseaux. Par la suite nous avons traité des caractéristiques de ce protocole, tels que le transfert des données et le contrôle de la congestion.

Nous avons exposées quelques solutions et algorithmes proposés pour remédier à certains problèmes.

### Introduction :

**P**lein d'avenir et très prometteur, tel est le visage des réseaux ad hoc mobiles (MANET) aujourd'hui qui se distinguent des autres formes de réseaux sans fil par une absence totale d'infrastructure fixe. Un nombre quelconque de mobiles équipés de cartes d'interface radio et des couches protocolaires adéquates suffisent pour former un réseau ad-hoc mobiles. Les débits atteints aujourd'hui sur ce type de réseaux rendent possible le transfert de flux multimédia soumis à de fortes contraintes. Dès lors, il est légitime de chercher à fournir aux applications des garanties sur le délai, sur les taux de pertes ou encore sur la bande passante. Les solutions utilisées dans le monde filaire sont inadaptées aux contraintes liées à l'utilisation du médium radio et à l'absence d'administration centralisée.

La QoS (Quality of Service) est maintenant un point important dans tous les réseaux (informatique et Telecom). Il semble intéressant d'étudier les moyens permettant d'introduire cette notion dans les réseaux ad hoc et en particulier dans les réseaux ad hoc mobiles (MANETs) où les terminaux sont en mouvement les uns par rapport aux autres. En effet, les applications multimédia que l'on connaît aujourd'hui nécessitent des garanties de QoS plus ou moins importantes qu'il serait bon de pouvoir proposer dans ce type de réseaux encore expérimentaux.

### 1. Principaux modèles de QoS dans les réseaux Ad Hoc :

Dans les réseaux de télécommunication, l'objectif de la qualité de service est d'atteindre un meilleur comportement de la communication, pour que le contenu de cette dernière soit correctement acheminé, et les ressources du réseau utilisées d'une façon optimale. La qualité de service QoS (Quality of Service) peut être définie comme le degré de satisfaction d'un utilisateur des services fournis par un système de communication.

La QoS est définie comme la capacité d'un élément du réseau (ex : routeur, nœud ou une application) de fournir un niveau de garantie pour un acheminement des données. Le RFC 2386 caractérise la QoS comme un ensemble de besoins à assurer par le réseau pour le transport d'un trafic d'une source à une destination. Ces besoins

peuvent être traduits en un ensemble d'attributs pré-spécifiés et mesurables en terme de :

- Délai de bout en bout,
- Variance de délai, temps de réponse (gigue),
- Bande passante,
- Pertes de paquets.

Application	Caractéristiques du multimédia			
	Débit	Sensible a		
		Délai	Gigue	Perte
Voix sur IP	Faible	Important	Important	Moyen
Visioconférence	Important	Important	Important	Moyen
Streaming Vidéo à la demande	Important	Moyen	Moyen	Moyen
Streaming Audio	Faible	Moyen	Moyen	Important
Commerce Electronique	Moyen	Moyen	Faible	Important
Courier Electronique	Faible	Faible	Faible	Important
Transfert de fichiers	Moyen	Faible	Faible	Important

**Figure 5.1 : Besoin du débit, gigue et délai pour le multimédia**

Suivant le type de l'application, les besoins de QoS sont différents. Par exemple, pour les applications temps réel, comme la voix et la vidéo, le délai de bout en bout d'un paquet doit être limité, autrement le paquet est inutile. Les applications non temps réel, comme le transfert de fichier ou la messagerie, quand à elles se focalisent sur la fiabilité des communications.

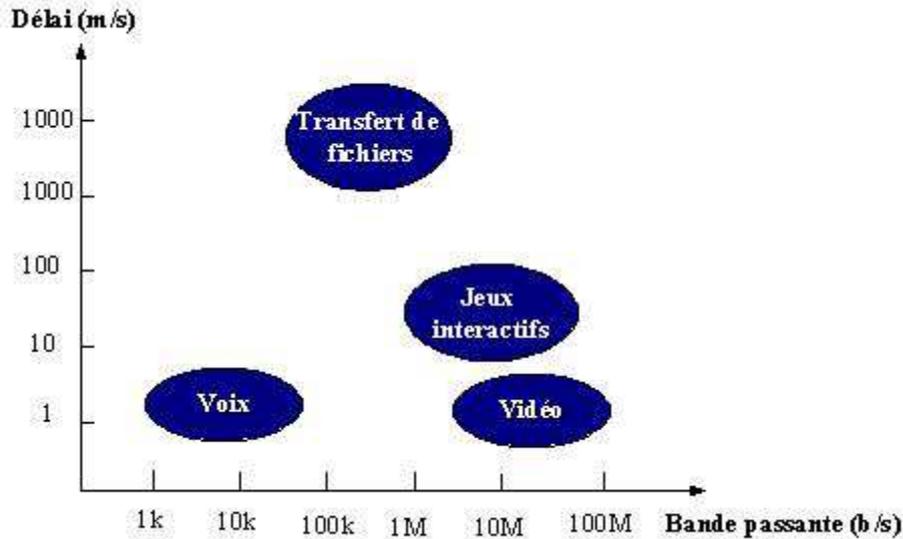


Figure 5.2 : Besoin en délai et bande passante des applications

Les recherches concernant la qualité de service dans les réseaux ad hoc sont souvent classées en catégories :

- les protocoles d'accès au medium cherchent à ajouter des fonctionnalités aux couches basses du modèle OSI afin de pouvoir offrir des garanties.
- les protocoles de routage avec qualité de service recherchent les routes ayant suffisamment de ressources disponibles pour satisfaire une requête.
- les modèles de qualité de service définissent des architectures globales dans lesquelles des garanties peuvent être fournies.

### 1.1. Les protocoles d'accès au medium avec QoS :

#### 1.1.1. IEEE 802.11e:

La spécification du IEEE 802.11e est qu'elle propose le support de la QoS dans les réseaux sans fil avec une nouvelle fonction de contrôle EDCA (Enhanced Distributed Channel Access), considérée comme la nouvelle version de la fonction DCF, et une fonction de coordination hybride (HCF). EDCA introduit quatre catégories de trafics. Les priorités sont contrôlées par les stations en modifiant le schéma d'accès de base (DCF). Plus flexible que la fonction PCF, HCF est utilisée par les points d'accès pendant la période d'accès contrôlée, qui peut commencer à n'importe quel moment durant *la superframe*. Autrement dit, ça lui permet d'avoir accès au médium pour faire passer un trafic ayant des contraintes de QoS.

Cette norme ré implémente la couche MAC (Medium Access Control) en ajoutant un mécanisme de réservation de la bande passante au niveau matériel. Elle est compatible avec les normes 802.11a, 802.11b (Wi-Fi) et 802.11g. Cependant, il est clair que tant qu'on n'aura pas amélioré le fonctionnement du cœur d'un réseau Infrastructure, c'est-à-dire la borne d'accès et plus précisément le protocole qui la gère, on ne pourra pas avoir une amélioration de la QoS. Il faut pour cela se rappeler que tous les paquets envoyés dans l'air doivent passer à travers la borne d'accès pour être routé vers leur destination. Un autre problème sensible affectant la QoS dans le lien air est la façon dont est partagée la bande passante en fonction des utilisateurs, mais là encore, comment partager différemment la bande passante si on n'a aucun moyen de différencier les différents flux de données arrivant à la borne d'accès.

C'est pourquoi l'arrivée de la norme 802.11e a été attendue avec impatience par tous les utilisateurs de réseau WLAN voulant faire de la VoIP ou d'autres applications temps réel.

### **1.1.2. Différenciation de services pour 802.11e :**

Afin de concevoir des mécanismes de différenciation de services efficaces, un mécanisme de priorités entre les trames est déployé. Pour ce faire, il faut adapter certains paramètres de la fonction de coordination distribuée (DCF) du protocole selon la priorité des paquets. Cette dernière repose sur la détection de porteuse (CSMA). Avant d'émettre, tout nœud doit s'assurer que le canal est libre depuis un certain temps (DIFS). Certains paquets de signalisation peuvent être plus privilégiés en leur accordant un temps SIFS (Short Inter Frame Spacing) plus court que le DIFS.

Dans le but d'améliorer la méthode d'accès DCF du protocole 802.11, les techniques suivantes ont été proposées :

1. La fonction de backoff différente: Consiste à attribuer des valeurs de fenêtres de contention (CW) supérieures pour les stations les moins prioritaires et inversement, permettant ainsi de donner plus de chance à une station prioritaire d'accéder au canal.
2. Les différents DIFS: Dans le standard IEEE 802.11 les trames ACK ont une priorité sur les trames RTS, en attendant un temps SIFS qui est inférieur à

DIFS. Dans cette technique de différenciation chaque station mobile dispose de sa propre valeur de DIFS qui définit son niveau de priorité pour l'accès au médium.

3. Un délai supplémentaire, constant, aléatoire est ajouté au DIFS, permettant ainsi en cas de collision de réinitialiser le processus et d'allonger le délai supplémentaire.

### 1.1.3. MACA / PR :

Le protocole MACA/PR (Multiple Access Collision Avoidance with Piggyback Reservation) propose de différencier la politique d'accès au médium selon la nature des flux. Il propose une bande passante garantie dans le réseau via une réservation pour les trafics temps réel. Les flux non privilégiés bénéficient du service « Best Effort ».

Les paquets des flux non privilégiés sont traités de façon standard. Pour les flux temps réel, une unique demande d'autorisation à transmettre (échange RTS-CTS) est effectuée en début de flux.

Dès qu'un paquet n'est pas acquitté, une nouvelle demande d'autorisation est émise. Afin de traiter les réservations de bande passante, l'émetteur inclut des informations dans chaque paquet sur l'ordonnancement du paquet suivant. Tous les voisins du nœud récepteur, en écoutant l'acquittement d'un paquet de données, possèdent des informations sur la date d'arrivée du prochain paquet et peuvent différer leurs transmissions. Ce mécanisme permet de résoudre le problème des stations cachées sans avoir recours à des paquets de signalisation particuliers.

### 1.2. Les protocoles de routage avec qualité de service :

Le routage avec QoS est un élément clé pour réaliser une architecture de QoS pour les MANETs. Il est important de définir les objectifs visés par le routage avec QoS. Le routage au mieux (sans QoS) ou « best effort » consiste en général à trouver le plus court chemin en termes de distance ou de délais entre une source et une destination. Dans le cas du routage avec QoS, l'objectif n'est pas seulement de trouver le meilleur chemin selon un critère précis, mais de trouver un chemin "admissible" satisfaisant certaines contraintes. Plusieurs paramètres peuvent être utilisés tels que le délai, la bande passante, la disponibilité en terme de QoS ou encore le coût de transmission.

On voit apparaître donc des spécificités où les routes doivent être calculées par flux et non par destination. En effet, un flux peut avoir des besoins de QoS alors qu'un autre flux entre ces mêmes nœuds en aura d'autres.

### 1.2.1. Routage avec QoS sur DSDV :

DSDV (Dynamic Destination Sequenced distance-Vector) ou vecteur de distance à destination dynamique séquencée est un protocole de routage proactif implémenté avec la qualité de service afin de résoudre les problèmes liés aux stations cachées. En effet, Lors d'une demande de réservation, DSDV évalue la quantité de bande passante disponible sur la route principale. Tout en évaluant le nombre d'unités TDMA (Division du temps en unités) appelées slots, disponible sur chaque lien tout au long de la route.

Il est nécessaire de ne pas utiliser les mêmes unités pour les transmissions entre deux liens adjacents. Dès que le destinataire reçoit la demande de route, il renvoie à l'émetteur une confirmation indiquant la politique d'allocation des unités choisie sur la route empruntée, la réservation de ressources se fait parallèlement à cette réponse. Pour pallier aux problèmes liés à la mobilité, une route secondaire non optimale en termes de nombre de sauts est maintenue. Bien que ce protocole évalue bien la bande passante disponible sur un chemin et offre le calcul de la probabilité de rejet des appels lors des simulations, il est incapable de résoudre les problèmes d'interférences, en particulier lorsque deux nœuds utilisant les mêmes unités TDMA se rapprochent et arrivent à portée d'émission l'un de l'autre.

### 1.2.2. Routage avec QoS sur AODV:

Le protocole de routage AODV avec QoS a pour objectif de :

- Introduire une métrique plus appropriée que la distance (nombre de sauts).
- Faire face aux changements fréquents de la topologie due à la mobilité des nœuds.

AODV se base sur un algorithme « à la demande » cela veut dire qu'il ne construit des routes entre nœuds que lorsqu'ils sont demandés par des nœuds sources. L'ajout dans les paquets de contrôle d'un champ « route réponse » RREP associé au paramètre délai ou au paramètre bande passante, À la réception d'un message « route

request » RREQ ajouté également. Du fait que les informations suivantes sont ajoutées dans la table de routage: bande passante minimale, délai maximum, et la liste des sources qui ont demandé des garanties de délai ou de bande passante.

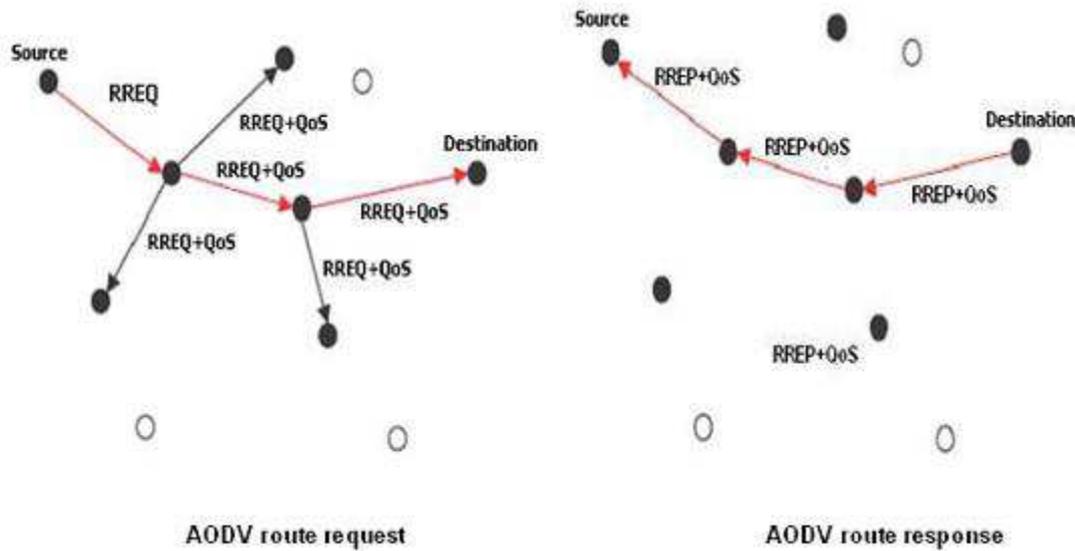


Figure 5.3 : le principe de AODV avec QoS.

Chaque mobile vérifie s'il est en mesure d'honorer le service demandé, avant de retransmettre le message. Si un nœud détecte que la QoS demandée n'est pas satisfaite alors il envoie un message à la source ayant initiée cette demande de QoS, pour l'informer.

## 2. Modèles de qualité de service dans les réseaux ad-hoc :

Actuellement les travaux qui ont été réalisés pour offrir une meilleure qualité de service pour les applications multimédia reposent sur certains aspects liés aux réseaux ad hoc qui sont, les modèles de qualité de service pour les MANETs en plus de l'introduction de la différenciation de service au niveau de la couche MAC. Ces travaux se sont inspirés de ce qui a été réalisé pour les réseaux filaires pour intégrer les aspects tels que :

- L'adaptation de la puissance d'émission en maximisant cette puissance pour les trafics prioritaires ; Le partage de charge entre les différents nœuds du réseau ;
- L'économie de batterie en essayant de trouver le chemin le plus court afin d'économiser l'énergie consommée.

- **Définition d'un modèle de qualité de service :**

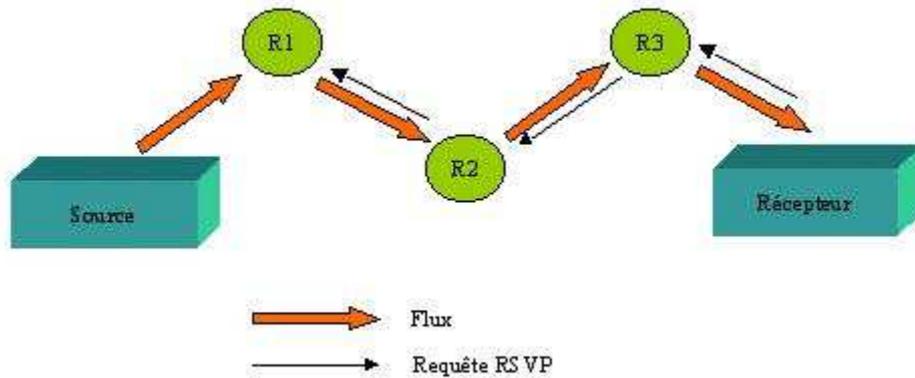
Un modèle de qualité de service décrit un ensemble de services bout-en-bout, qui permettent aux clients de sélectionner un nombre de garanties qui gouvernent des propriétés telles que le temps, l'ordonnancement et la fiabilité. Le modèle de qualité de service spécifie l'architecture qui va nous permettre d'offrir un service meilleur que celui offert par le modèle best-effort traditionnel. Cette architecture doit prendre en considération les défis imposés par les réseaux ad hoc, comme le changement de la topologie et les contraintes de délai et de fiabilité. Cependant, des modèles tels que Intserv/RSVP, proposés pour les réseaux filaires, ne prennent pas en compte les contraintes de limitation de ressources imposées par les réseaux ad hoc.

### **2.1. Les modèles standards existants :**

#### **2.1.1. IntServ :**

Le premier modèle s'appelle " Services Intégrés " ou IntServ. Il utilise un concept basé sur la réservation où chaque application transmet ses conditions à tous les nœuds de réseau traversés jusqu'au nœud de destination. Quand tous les nœuds ont acceptés les conditions, l'application commence l'acheminement de ses données. IntServ aborde la qualité de service en reprenant le concept du " meilleur effort " et en y rajoutant le support du trafic en temps réel. Le modèle IntServ est donc un modèle incluant le concept du " best effort ", un service en temps réel, et un partage de lien contrôlé. Le modèle de service gère deux sortes de trafic en temps réel : garanti et prévisible.

Cependant, IntServ, en rendant possible la réservation de ressources, permet des requêtes très précises en termes de qualité de service. Les clients obtiennent donc soit exactement ce qu'ils ont demandé soit leur requête échoue. La réservation de ressources est demandée par le récepteur, il émet une requête de QoS correspondant à ses besoins. Celle-ci parvient à l'émetteur sous forme d'un message RSVP(Resource ReserVation Protocol). Ce mode d'attribution de ressources à l'avantage d'être effectué par le récepteur qui, ainsi, peut demander une QoS adaptée à ses besoins et à la consommation désirée.



**Figure 5.4 : principe de fonctionnement du protocole IntServ**

Pour assurer un chemin unique au cours d'une communication, il faut que les systèmes terminaux fonctionnent en mode connecté. Cependant, RSVP n'assure pas un mode connecté avec les routeurs et une mise à jour dynamique de la réservation est nécessaire. Les récepteurs sont donc obligés d'envoyer périodiquement des messages RSVP aux routeurs assurant le chemin. Les requêtes RSVP sont des messages de différentes natures permettant à l'émetteur comme au récepteur d'avoir un chemin dédié au transfert.

Ce modèle n'est pas applicable aux MANETs car:

- Les informations sur les flux augmentent proportionnellement au nombre de flux gérés. ce problème n'est pas spécifique au MANETs, on le retrouve aussi dans l'internet. La maintenance de cette quantité d'information par des terminaux mobiles dont les ressources sont limitées n'est pas envisageable. Même si aujourd'hui les MANETs restent de petite taille et ne sont destinés à gérer qu'un nombre restreint de flux, cette solution n'est pas viable à long terme, puisqu'il est probable que les MANETs vont être amenés à se développer.
- Les paquets de signalisation RSVP utilisent une quantité non négligeable de bande passante sur des liens déjà limités.
- Chaque nœud doit se charger de gérer le contrôle d'accès, la classification et l'ordonnancement des flux. C'est une charge trop importante pour des terminaux aux ressources limitées.

### 2.1.2. DiffServ

Le deuxième modèle, " Services Différenciés " ou DiffServ, utilise une technique de marquage des paquets (chaque paquet est tagué d'un code dans son entête IP pour indiquer à quelle classe de trafic il appartient. Les commutateurs traversés sur le chemin manipulent donc les paquets différemment en fonction de la classe de service à laquelle ils appartiennent. Le comportement à chaque nœud du réseau est en effet choisi en se basant sur la classe de chaque paquet. Diffserv emploie le champ ToS dans l'en-tête d'IP pour déterminer à quelle classe un paquet spécifique appartient.

L'émetteur de flux spécialisé, au travers du champ "Type Of Service", spécifie une classe de service qu'il souhaite donner à ses paquets. Au cours de son voyage dans le réseau, ce paquet traverse des modules (routeurs) qui, équipés d'algorithmes (Packet Classifier), lisent le champ TOS. Ensuite un répartiteur de paquet (Packet Scheduler) met en œuvre le traitement différencié en lui affectant une discipline de service adaptée (file d'attente spécialisée). Rappelons que les routeurs sont soumis à de grands nombres de demandes qui les obligent à gérer des files d'attente. La stratégie des services différenciés (Diffserv) est apparue pour faire face à la complexité et au coût de l'approche " Services Intégrés ". Cette approche est différente d'IntServ par son concept de classification des flux.

L'avantage de ce modèle est qu'il offre des classes de QoS sans modifications en termes de gestion du trafic et il fournit des solutions de continuité par rapport au service au mieux (best effort) traditionnel. Par rapport à IntServ, on perd en termes de flexibilité et de fermeté des garanties. Le problème du plan de contrôle reste entier. Dans le cas du multicast, les choses se compliquent davantage, en effet aucune approche n'a été proposée sur la façon de dimensionner le réseau et de conditionner un trafic de multicast.

Malheureusement, ce modèle ne convient pas aux MANETs car la question de la définition des routeurs de bord et des routeurs de cœur reste très ambiguë dans ces réseaux. Intuitivement, la source fait parti des routeurs de bords et les nœuds du chemin font parti des routeurs de cœur. Mais dans les MANETs, chaque nœud doit pouvoir jouer les deux rôles à la fois, puisqu'il peut être source d'une communication

et relais pour une autre. Cela engendrerait donc une charge trop importante sur tous les nœuds du réseau.

### **2.2. Les principaux modèles utilisés dans les MANETs :**

#### **2.2.1. FQMM (Flexible quality of service model for MANETs) :**

Les concepteurs du modèle FQMM prennent en compte le fait que les réseaux ad hoc pourraient, à terme, être connectés à des réseaux filaires de type Internet. Il apparaît dès lors nécessaire d'offrir un mécanisme de qualité de service suffisamment proche des protocoles filaires afin de s'interfacer avec ces derniers. Le modèle repose sur une architecture réseau plate (non hiérarchique), constituée d'une cinquantaine de nœuds mobiles. Il combine les propriétés des modèles filaires IntServ et DiffServ, en offrant une méthode d'approvisionnement hybride :

- Par flux, pour les trafics prioritaires.
- Par classe, pour les autres trafics.

Afin d'obtenir les deux types de granularité (par flux ou par classe) des modèles filaires, FQMM définit plusieurs classes de service dont la plus haute permet à chaque flux de spécifier les contraintes qui lui sont propres. A l'image de DiffServ, FQMM définit trois types de nœuds :

- Les nœuds d'entrée (émetteurs)
- Les nœuds intermédiaires.
- Les nœuds de sortie (récepteurs).

Les nœuds d'entrée permettent de marquer et classifier les paquets, qui seront ensuite relayés par les nœuds intermédiaires jusqu'à arriver au nœud destinataire.

#### **2.2.2. SWAN (Service differentiation in wireless ad hoc networks):**

Ce modèle fait partie de ces protocoles mythiques cités dans presque tous les articles traitant de la qualité de service dans les réseaux ad hoc, La philosophie du protocole est de ne pas garder d'état dans les nœuds mais se base sur des algorithmes de contrôle distribués dans le but d'assurer une différenciation de services dans les réseaux ad hoc.

Ce modèle offre la priorité (au niveau paquet) aux trafics temps réel en contrôlant la quantité de trafics best effort acceptée par nœud. Pour accepter un nouveau trafic temps réel, le contrôle d'admission sonde la bande passante minimale disponible sur la route (valide et obtenu par un protocole de routage). Une prise de décision est alors faite à la source suivant la bande passante obtenue. Dans le but de maintenir la qualité de service des trafics déjà acceptés, le débit des trafics best effort est régulé en utilisant comme paramètre, les mesures de délais au niveau MAC. Face à une congestion, les bits ECN (Explicit Congestion Notification) de l'entête des paquets IP sont positionnés pour permettre à la source de re-initier le contrôle d'admission. Si la route ne dispose pas d'assez de bande passante, le trafic est supprimé. Plusieurs solutions sont proposées pour le choix des flux à ré-établir. L'idée est d'introduire un mécanisme aléatoire dans le choix des flux à stopper afin de ne pas arrêter trop de flux en même temps dans les endroits congestionnés. Si cette approche est assez simple, le fait d'être indépendant d'un protocole de routage avec qualité de service peut conduire à un rejet de certains flux, puisque les routes reconstruites seront très probablement les mêmes qu'avant la congestion et que par conséquent il ne sera pas possible d'acheminer sur ces mêmes routes tous les flux qui ont provoqué précédemment une congestion.

### **2.2.3. QPART (QoS Protocol for Ad hoc Real-time Traffic):**

Ce modèle se situe dans le même état d'esprit que SWAN ceci par rapport à la différenciation de services entre différents types de trafic et garanties pour certains trafics sans garder d'états dans les nœuds.

QPART considère trois types de trafic : le trafic sensible au délai, le trafic sensible à la bande passante et le trafic Best Effort. La garantie des contraintes et celle de la différenciation sont réalisées par des modifications des tailles des fenêtres de contention pour les différents types de trafic. En ce qui concerne les trafics sensibles au délai, la taille de la fenêtre de contention sur chaque nœud dépend du délai connu par le paquet sur le lien précédent et de celui qu'il aurait dû avoir.

### **2.2.4. Modèle iMAQ (integrated MANET QoS):**

Ce modèle fournit le support des transmissions des données multimédia dans un MANET. Il inclut une couche ad hoc de routage et une couche de service logiciel

(Middleware). Dans chaque nœud, ces deux couches partagent les informations et communiquent afin de fournir les garanties de QoS aux trafics multimédia. Le modèle est basé sur la prédiction de la position des nœuds (predictive location-based) et orienté QoS. La couche Middleware communique également avec la couche application et la couche réseau et essaye de prévoir le partitionnement du réseau. Pour fournir une meilleure accessibilité aux données, il réplique les données entre les différents groupes du réseau avant d'effectuer le partitionnement.

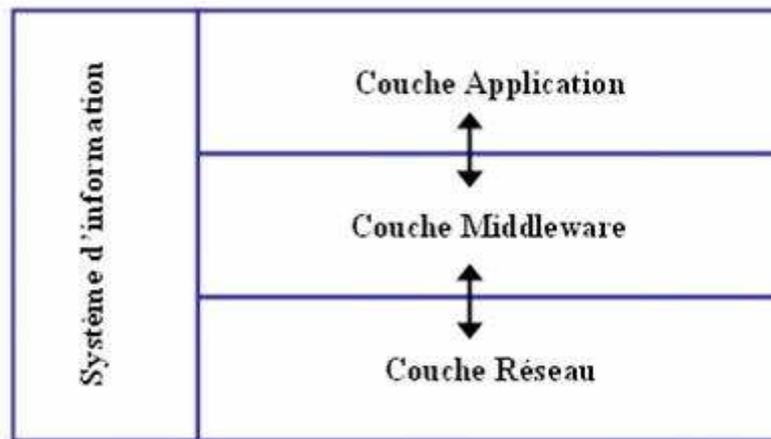


Figure 5.5 : le modèle iMAQ

**Conclusion :**

**P**lusieurs contraintes sont liées au mode Ad Hoc et au médium sans fil, dont notamment la peu fiabilité du médium, bande passante limitée, routage plus complexe, beaucoup de contraintes physiques (interférences...)

Néanmoins, il existe toujours un compromis entre le volume d'informations échangées (volumes et profils de trafics au niveau de chaque nœud, mobilité des nœuds, etc.) et précision des garanties. Plus les nœuds sont au courant de l'état du réseau, plus ils seront capables d'évaluer la capacité résiduelle de ce dernier. Nous avons en outre présenté les architectures proposées par les groupes de travail IntServ et DiffServ et qui se sont montrés inadaptés aux MANETs. Nous avons explicité par la suite l'émergence de nouvelles techniques telle FQMM qui combine les propriétés

des modèles filaires IntServ et DiffServ, en offrant une méthode d'approvisionnement hybride: par flux (pour les trafics prioritaires) et par classes (pour les autres flux), la technique SWAN qui se base sur des algorithmes de contrôle distribués, la QPART qui rejoint le même état d'esprit que la SWAN, ceci par rapport à la différenciation de services entre différents types de trafic et aussi par rapport à la garantie offerte pour certains trafics sans se soucier de l'état des nœuds tout en considérant trois types de trafic: le trafic sensible au délai, le trafic sensible à la bande passante et le trafic Best Effort. Le dernier modèle traité iMAQ fait la transmission des données multimédia dans un MANET en incluant une couche Ad Hoc de routage et une couche de service logiciel.

Un travail important serait de fournir une base d'évaluation standard des différentes solutions définissant les scénarios, les outils et les paramètres de simulations possibles.

Dans un futur proche, un grand nombre de travaux devront être menés pour aboutir à une connaissance suffisante des spécificités de ces réseaux.

### Introduction :

L'architecture actuelle des protocoles réseaux, que ce soit le modèle OSI ou le modèle TCP/IP, repose sur un ensemble de modules devant chacun fournir un service précis et ce de façon autonome. Ces modules ont été organisés hiérarchiquement dans une pile, chaque module se trouvant au dessus du service dont il a besoin pour fournir le sien.

De façon à assurer la maintenabilité des systèmes de communication face aux évolutions technologiques, les interfaces entre modules sont limitées : seules les interactions de services entre modules directement adjacents sont autorisées, chacun gérant son propre espace de données. Cependant, dès l'apparition d'influences entre deux couches, l'envie est forte que ces couches puissent se communiquer un ensemble de variables statistiques, qui aideront à la résolution d'un problème. C'est ce que proposent les architectures cross layer [RSL06].

Un exemple de retour particulièrement intéressant dans les réseaux ad hoc mobiles, qui permet d'optimiser des protocoles de différents niveaux, concerne la qualité de la liaison. Cette information, déterminée par un ensemble de paramètres de la couche physique, est utilisable par la couche MAC/LLC (Logical Link Control) pour décider d'utiliser ou non des mécanismes de contrôle d'erreur ou encore pour adapter la portée de la transmission.

Cette information peut également être utilisée par le routage pour sélectionner les nœuds qui constituent un chemin. Un grand nombre de protocoles cherchant à améliorer TCP utilisent des mécanismes cross-layer. Ceux-ci peuvent demander une coopération importante de la part des nœuds de routage et nécessitent souvent l'utilisation de messages, ou de champs de messages, spécifiques.

Nous présentons à la suite deux mécanismes typiques de cross-layer, et différentes interactions entre des protocoles des couches : Transport (TCP), Réseau (Routage) et liaisons de données (MAC).

Et pour conclure, nous allons faire un état de l'art sur différents travaux qui ont été fait sur les différentes interactions protocolaires dans différentes couches. Afin de proposer des améliorations pour une meilleure QoS dans un réseau ad hoc mobiles.

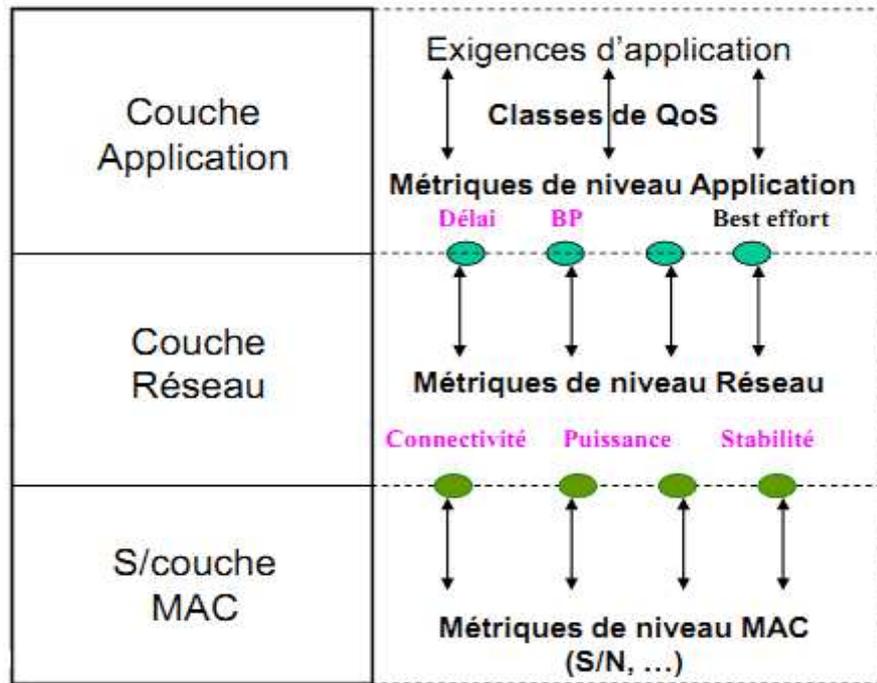


Figure 6.1 : interaction entre couches (cross-layer).

### 1. Architecture de communications entre couches :

Dans l'approche cross layer, les échanges d'informations se font entre des couches qui ne sont pas forcément adjacentes : la performance globale est optimisée en adaptant chaque niveau en fonction de l'information disponible. Les architectures protocolaires, pour mettre en œuvre les mécanismes d'adaptation, s'inspirent de trois modèles :

- communication directe entre couches ;
- interactions vers une entité intermédiaire ;
- nouvelles abstractions.

Ces trois modèles, exposés par Srivastava et Motani [VSM05], sont représentés sur la Figure 2.

- communication directe entre couches ;
- interactions vers une entité intermédiaire ;
- nouvelles abstractions.

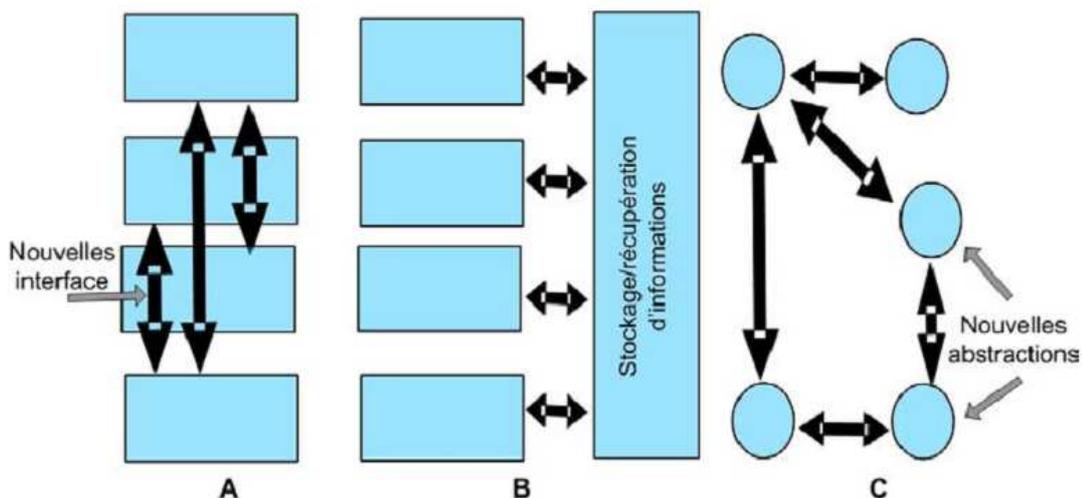


Figure 6. 2: modèle d'architecture cross-layer.

### 1.1. Communication directe entre couches:

Une façon pour un protocole de s'adapter est de permettre des communications directes entre les couches qu'elles soient ou non adjacentes, comme indiqué sur la Figure 2-A. De nouvelles interfaces sont utilisées pour partager les informations entre les couches.

Par cette méthode, des flux d'informations peuvent être redirigés d'une (de) couche(s) inférieure(s) vers une (des) couche(s) supérieure(s), ou du(e) niveau(x) supérieur(s) vers un (des) niveau(x) inférieurs. Un problème inhérent à cette méthode est la complexité de gestion des espaces de mémoire partagée entre les niveaux, qui peut poser un problème d'implantation dès lors que les ressources des équipements sont limitées. De plus, ce type d'architecture pose des problèmes de maintenance dans la mesure où l'ajout, le retrait ou l'évolution d'éléments, influe sur de nombreuses interactions [VKK05].

### 1.2. Interactions vers une entité intermédiaire :

Ce modèle introduit un point de synchronisation qui facilite la communication entre les couches (voir la Figure2-B). Il s'agit de spécifier les interactions des différentes couches vers une entité intermédiaire. Le partage de données s'effectue par un service de stockage/récupération d'informations sur toutes les couches ainsi que par la possibilité de positionner dans une couche spécifique des variables optimisées par une autre couche.

Un exemple de cette approche est l'interface Xian qui permet à un réseau local de type WiFi 802.11 de propager ses informations vers tous les niveaux protocolaires [ACL06], [ACL08].

### 1.3. Nouvelles abstractions :

La Figure 2-C présente une autre façon d'organiser les protocoles. Ceux-ci ne sont plus considérés comme des modules organisés hiérarchiquement avec des interactions récursives, mais comme des ensembles de composants fournissant un service spécifié par un graphe. Cette méthode, qui remet en cause le principe de structuration en couches, par une approche fonctionnelle, au bénéfice d'une structuration service, par une approche composants, a comme avantage d'offrir une grande flexibilité d'évaluation tout en minimisant les problèmes d'interactions et donc de maintenance.

## 2. Interactions entre les protocoles :

### 2.1. Interaction entre le protocole MAC et le protocole TCP :

#### 2.1.1 Etat de l'art :

L'information disponible à la couche liaison de données (MAC), concerne le mécanisme de contrôle d'accès au canal et éviter les collisions, ainsi ; la couche liaison de données peut adapter son schéma de contrôle selon le délai et les pertes de paquets de la couche transport (TCP).

Dans la suite, nous allons présenter quelques travaux de recherche faits en ce sens :

- La popularité de l'internet au cours des dernières décennies a entraîné un avancement rapide des applications exigeantes. Le Transfert Control Protocol / Internet Protocol (TCP / IP) est un protocole bien connu dans le développement de l'Internet d'aujourd'hui. Fondamentalement, TCP fournit une livraison de données orienté connexion et fiable de bout en bout entre deux hôtes de réseaux filaires traditionnels. Comme TCP est bien réglé et en raison de sa large acceptation dans Internet, il est souhaitable d'étendre et d'adopter ses fonctionnalités aux réseaux sans fil. D'autre part, des

caractéristiques uniques et l'utilisation de réseaux multi-sauts sans fil requièrent une conception robuste, fiable et évolutive. Ceci peut être réalisé [FSJ11] en tenant compte de l'interaction des différentes couches de répondre aux exigences croissantes de ces réseaux. La fiabilité de TCP est réalisée en retransmettant les paquets perdus et l'acquittement (ACK) de confirmation. Si l'expéditeur ne reçoit aucun accusé de réception dans un intervalle de temps ou reçoit ACK dupliqués, le paquet sera retransmis. Toute perte de paquets est supposée qu'elle est due à la congestion dans les réseaux filaires. Quand une perte de paquet est détectée, le protocole TCP qui invoque son mécanisme de contrôle de congestion pour ralentir le taux d'envoi afin de réduire la congestion. Toutefois, [FSJ11] les pertes de paquets ne sont pas principalement dues à la congestion dans les réseaux sans fil. Il pourrait être dû à certaines propriétés sans fil spécifiques telles que l'accès au médium, faux routage et un taux élevé d'erreur d'envoi. Le principal défi du protocole TCP est son utilisation de bande passante et la performance médiocre quand il fonctionne sur les réseaux 802.11 sans fil multi-sauts. La raison est peut être expliquée en le vaste nombre d'accès au médium réalisé par TCP. Fondamentalement, le protocole TCP expéditeur sera informé si la transmission est réussie en recevant l'acquittement de l'hôte destinataire. Les overheads MAC peuvent être causés par les paquets ACK redondants qui se disputent le même parcours avec des paquets de données pour les médias. Bien que les paquets TCP et ACK sont petits, ils peuvent causer la surcharge comme des paquets de données dans la couche MAC résultant en un gaspillage de ressources sans fil. En fait, les courtes trames RTS / CTS mises en œuvre par 802,11 protocole MAC, ne peuvent pas éliminer l'interférence dans les grandes topologies. Comme la charge augmente, les effets bien connus de terminal cachés causés par des interférences entre les paquets ACK et les données peuvent influencer sur les performances TCP de façon spectaculaire dans de longs chemins, si TCP reconnaît tous les paquets de données entrants. Une façon d'améliorer les performances TCP sur 802,11 en réseaux ad-hoc mobiles est de soulager la contention d'accès au médium en réduisant le nombre d'ACK générés, tout simplement appelé ACK retardé. Cela peut être fait par la fusion de plusieurs acquittements dans un ACK qui

est possible grâce au régime ACK cumulatif utilisé dans TCP. Se référant aux approches déjà proposées pour réduire le nombre d'ACK générés, les performances TCP sont toujours affectées par une limitation d'une méthode qui sélectionne dynamiquement le nombre d'ACK retardé basée sur l'état de canal. Ce qui motive les auteurs dans [FSJ11] à étudier les performances de TCP-ACK en interaction avec 802.11 sur les réseaux ad-hoc mobiles et de développer une dynamique stratégie ACK retardé pour ajuster le protocole TCP à ces types de réseaux.

- Le document [YCX10] montre d'abord que le mécanisme de contrôle de congestion TCP basé sur la perte de paquets ne s'adapte pas bien dans les réseaux ad hoc multi-sauts. Puis après la modélisation du protocole MAC, il s'est basé sur l'interaction entre le protocole MAC et TCP, la fonction de la couche MAC est d'essayer de son mieux de rechercher un groupe de planification des tâches mutuellement exclusives pour le trafic chargé, alors que la fonction de la couche de transport est d'ajuster son trafic pour assurer l'existence d'un ordonnancement faisable pour que la couche MAC puisse le trouver. En construisant le protocole MAC optimale selon le graphe de contention, on gagne le taux de transmission maximal d'expéditeurs TCP qui peut assurer l'équité TCP.
- L'article [PBA09] évalue le rendement de l'interaction entre les protocoles de transport et la couche MAC dans un réseau mobile ad hoc (MANET). Dans un réseau ad hoc, certains paramètres de QoS comme le taux d'erreur, le retard et la perte de paquets sont augmentés, et certains paramètres comme le débit et la bande passante sont diminués dans la couche de transport, et ça est due à des problèmes de la couche MAC, et la déconnexion qui est due à la mobilité des nœuds ou panne de courant. Ainsi, combiner les mécanismes de ces deux couches pour améliorer la qualité de service de façon significative afin que les gens puissent concevoir le réseau en fonction de leurs exigences. Les auteurs ont examiné les effets de deux protocoles MAC ; IEEE-802.11 et IEEE802.11e avec démarrage lent qui est un mécanisme de TCP. Et l'IEEE802.11e utilise la fonction de coordination distribuée améliorée : Enhanced Distributed Coordination Function (EDCF). Plus précisément, ils

ont étudié l'impact de plusieurs sauts sans fil et la mobilité des nœuds sur la performance de débit de TCP sur chaque protocole MAC.

Les résultats montrent que dans tous les cas, les paramètres de la QoS ont 15-20% d'amélioration du débit, 40-45% d'amélioration du produit délai-bande passante, la perte de paquets est réduite de façon significative à 40-50% en IEEE802.11e avec démarrage lent par rapport à IEEE802.11 sans démarrage lent. Les résultats montrent aussi que les paramètres de la QoS s'améliorent tels que : le débit de 35-40%, 25 - 30% d'amélioration du produit de délai-bande passante.

- Dans les MANETs [MRH09] les nœuds agissent à la fois comme des hôtes et comme routeurs intermédiaires. Lorsque la communication se produit, ces nœuds forment des chaînes entre les différentes sources et les destinations. Les chercheurs ont étudié comment ces chaînes se comportent, en découvrant que les interactions niveau MAC joue un rôle majeur dans la détermination de leur performance. Dans l'article [MRH09], les auteurs ont étendu cette analyse pour étudier comment les connexions TCP, qui impliquent des flux bidirectionnels, de se comporter sur les chaînes sans fil. D'abord, ils ont examiné les types de chaînes qui se produisent plus fréquemment dans les configurations TCP, et les classer par la nature des interactions au niveau MAC qui se posent dans chacun. Ils ont montré alors que le débit de TCP sur une chaîne sans fil est grandement affecté par le type d'interactions au sein de la chaîne. Enfin, ils ont montré les implications des interactions niveau MAC sur la performance du réseau: en particulier, l'instabilité des chemins et le nombre de retransmissions.
- Un nœud candidat à la congestion devrait refléter l'état de discorde MAC, et en raison de collision pour le fait que l'affirmation de MAC est étroitement associé à la congestion TCP. Ensuite, le candidat doit préciser la bande passante disponible pour exploiter pleinement le canal partagé sans causer une congestion TCP sévère et la collision des paquets. Dans les travaux de [KSR09], ils ont proposé de développer une inter-couche à base de protocole MAC pour utiliser complètement la bande passante de canal et d'augmenter

l'équité de chaque flux sans provoquer d'embouteillages. Dans ce protocole, la bande passante disponible le long de chaque chemin de la source à la destination, est estimée à partir d'une technique de sondage. Le nœud de destination envoie des paquets de sonde vers le nœud source de sorte que le nœud source peut estimer la bande passante disponible et la discorde entre eux.

Ensuite, la source sélectionne la voie qui a assez de bande passante, en utilisant un protocole de routage multi-chemins. En plus de cela, un flux centralisés ordonnanceur est conçu pour surmonter les overheads et les inconvénients de la norme IEEE 802.11. Ce calendrier planificateur des flux au lieu de nœuds. Grâce à des résultats de simulation, ils ont montré que le protocole proposé atteint un débit et équité élevés.

- Dans [FSJ08] ils ont constatés que la stratégie des acquittements (ACK) a un grand potentiel pour augmenter le débit TCP quand il fonctionne sur le protocole MAC 802.11. En particulier, les acquittements TCP sont nombreux à accéder au medium pour prendre le même chemin que les paquets de données pour les médias. Comme la charge augmente, les effets bien connus de terminal cachés causés par des interférences entre les paquets ACK et les données dans la couche MAC peut dégrader les performances TCP considérablement si TCP reconnaît tous les paquets de données entrants. Dans cette étude ; une stratégie d'interaction dynamique TCP/MAC a été proposée qui tente de réduire le nombre d'ACK induite par le suivi de l'état du canal. Pour ce faire, la probabilité de collision totale collectée sur le chemin de l'expéditeur au récepteur dans la couche MAC a été utilisée pour définir correctement le nombre d'ACK retardé (DA) en TCP. Basé sur la probabilité de collision mesurée, TCP ajuste dynamiquement l'expéditeur lui-même à l'état du canal en retardant moins de ACK dans des conditions de trafic élevé, et en retardant plus dans des conditions de faible trafic. Les résultats des simulations montrent une amélioration du débit allant jusqu'à 15% sur la méthode existante appelée Dynamic Adaptive Acknowledgment (TCP-DAA) et beaucoup plus sur le protocole TCP réguliers dans les scénarios traitant avec un taux de perte dynamique.

- Dans [LGP] ils se sont intéressés à l'amélioration des performances des flux TCP lorsqu'une courte rupture de signal 802.11 conduit à la perte de segments. Une courte étude analytique met en évidence les deux niveaux distincts de recouvrement MAC et TCP et l'absence d'interactions entre ceux-ci. Cette étude montre de plus l'intérêt d'adapter dynamiquement, dans certains cas de perte, le paramètre MAC *Retry Limit* pour réduire la baisse de performance due au déclenchement inapproprié du mécanisme de contrôle de congestion TCP. Un algorithme de type LDA (*Loss Differentiation Algorithm*) intervenant au niveau MAC et permettant de différencier les pertes dues aux déplacements et aux obstacles, et d'agir en conséquence est ainsi proposé. Son évaluation montre le gain en performance obtenu par rapport à une solution sans LDA.
- L'article [DPH] évalue la performance et l'interaction entre le TCP et l'exploitation de protocole de la couche MAC dans un réseau mobile ad hoc (MANET). Les auteurs ont examiné les effets de deux protocoles MAC : CSMA et IEEE 802.11. Plus précisément, ils ont étudié l'impact de multi sauts sans fil, la mobilité des nœuds, et l'intensité du trafic sur les performances de débit de TCP pour chaque protocole MAC. L'équité des protocoles MAC par rapport à un partage égal de la bande passante entre les flux TCP multiples est également étudiée. En outre, une approche de conception est utilisée pour quantifier les effets de trois facteurs - vitesse nœud, l'intensité du trafic, et le protocole MAC utilisé - sur le débit TCP. Les résultats montrent que dans certains cas, l'équité du réseau est très inégale entre les flux TCP simultanées, ce qui entraîne l'envoi de plusieurs stations à un débit très faible. La constatation la plus significative est obtenue lorsque la mobilité est introduite dans le modèle. Quand une topologie statique est utilisée, le rendement de CSMA est plus bas que le débit de 802.11, principalement en raison de collisions de paquets. Toutefois, lorsque les nœuds sont mobiles, CSMA surpasse constamment 802.11. Les premières expériences suggèrent que les fréquents changements topologiques donnent un

nombre élevé de clair to send (CTS) lorsqu'on utilise le protocole MAC 802.11, ce qui réduit le débit global.

- Le nombre des terminaux qui ne cesse d'augmenter et l'expansion des réseaux sans fil témoignent de la demande croissante des utilisateurs pour un accès à des ressources telles que des données ou des services applicatifs, à tout moment et n'importe où. Dans ce contexte [HBL07], les MANET (Mobile Ad hoc Networks) peuvent jouer un rôle important puisqu'ils peuvent être utilisés lorsque le déploiement d'infrastructures est coûteux ou sans objet, ou encore pour accroître la portée des réseaux à base d'infrastructure. Toutefois, des contraintes spécifiques aux MANET existent qui demeurent des freins majeurs au développement d'applications pour les MANET. L'une de ces contraintes est la dégradation de la performance du protocole TCP (Transfer Control Protocol) due essentiellement aux nœuds exposés et nœuds cachés qui agissent négativement sur le comportement du protocole MAC (Medium Acces Control) vis-à-vis du protocole TCP surtout si ces deux protocoles ne les prennent pas en compte et ne procèdent pas à l'adaptation de leurs comportements en faveur des flux TCP. Dans le cadre de ces travaux, les auteurs présenteront une optimisation de l'algorithme de backoff du protocole MAC pour une meilleure performance du protocole TCP. Cette dernière se base sur l'ajustement de ses paramètres en fonction du nombre de nœuds que constitue le MANET.
  
- Le mécanisme traditionnel de contrôle de congestion de TCP rencontre un certain nombre de nouveaux problèmes et souffre d'une mauvaise performance lors de la norme IEEE 802.11 du protocole MAC, qui est utilisé dans les réseaux ad hoc mobiles. Dans [HXY07], les auteurs ont d'abord constaté que l'accès au médium et la congestion sont intimement couplés, et l'algorithme de contrôle de congestion TCP devient trop important dans sa granularité, entraînant une instabilité de débit et un retard excessif. De plus, le problème d'équité de TCP due à la contention du médium et le compromis entre le débit global et d'équité. Dans ce travail, Ils ont proposé un nouveau protocole de contrôle de congestion sans fil ; Wireless Congestion Control

Protocol (WCCP) pour soutenir efficacement et équitablement les services de transport dans les réseaux ad hoc multi-sauts. Dans ce protocole, chaque nœud transfère le long d'un flux de circulation, des informations concernant la répartition des ressources entre nœud d'une manière équitable et détermine les réactions de la couche MAC.

Des simulations approfondies montrent que WCCP surpasse de manière significative TCP traditionnelle en termes d'utilisation de canaux, de retard, et d'équité, et élimine le problème de la famine.

### 2.1.2. Notre contribution :

Comme nous venons de le voir précédemment, le mécanisme de contrôle de congestion TCP traditionnel dans les réseaux filaires, souffre d'une mauvaise performance lors de la norme IEEE 802.11 du protocole MAC. Et inversement le protocole MAC influence négativement sur le protocole TCP par son mécanisme de contrôle d'accès, entraînant des timeouts multiples, l'algorithme de contrôle de congestion devient trop important et entraîne une instabilité et un retard excessif du délai de bout en bout. Parfois, les courtes ruptures du signal 802.11 conduisent à un déclenchement inapproprié du mécanisme de contrôle de congestion TCP, et il dégrade ses performances.

- Pour remédier à cette situation, nous proposons une approche entre les deux couches transport et liaison de données. Il s'agit d'adapter le protocole MAC pour pouvoir identifier dynamiquement les types de pertes, s'il s'agit d'une courte rupture due à un obstacle ou un petit déplacement, il n'est pas nécessaire de faire appel au mécanisme de contrôle de congestion TCP qui est coûteux en termes de délai et débit global...

Ce mécanisme est un paramètre temporel qui détermine à quel moment on doit faire appel au contrôle de congestion TCP, il s'agit d'une variable échangée entre les deux couches sous-jacentes (MAC et TCP), et elle doit être paramétrable selon la mobilité et la taille du réseau (plus ces derniers augmentent, plus les défaillances du signal augmentent). Cette approche théorique résout à la fois les deux influences l'un sur l'autre, pour le TCP, il va diminuer son mécanisme de contrôle de congestion dans les cas où il n'est pas

nécessaire, et puisque les paquets vont diminuer et par conséquent le nombre de paquets à accéder au médium va diminuer et bien sur le mécanisme de contrôle d'accès au médium de MAC va être soulagé.

### 2.2. Interaction entre le protocole MAC et le protocole de routage :

#### 2.2.1. Etat de l'art :

Minimiser la consommation d'énergie est plus qu'importante dans les MANET. L'interface radio des nœuds mobiles peut être à vide (ne transmet pas et ne reçoit pas), alors cette dernière doit s'éteindre (mise en veille du nœud) lorsque elle n'est pas utilisée. En réalité, cette politique n'est pas vraiment pratique car le nœud mis en veille doit se réveiller périodiquement non seulement pour récupérer des paquets à sa destination, mais aussi pour participer dans le fonctionnement des couches hautes notamment la couche routage. La coopération entre le mécanisme de routage, supporté par les protocoles de routage, et le mécanisme de sauvegarde de l'énergie, supporté par le protocole MAC, n'est pas une tâche aisée et nécessite de bien étudier les interactions entre ces deux protocoles.

Dans ce qui suit nous présenterons quelques travaux de recherches sur ce genre d'interaction entre ces deux couches :

- Une des tendances les plus visibles dans le marché actuel de la communication commerciale est l'adoption de la technologie sans fil. Les réseaux sans fil sont attendus pour transporter le trafic qui sera un mélange de trafic en temps réel comme la voix, les conférences multimédias, les jeux et le trafic de données telles que la navigation web, de messagerie et de transfert de fichier. Toutes ces applications nécessitent des flux de données très variables et la garantie de qualité de service (QoS). Dans des travaux de recherches pour améliorer les performances des réseaux sans fil, il ya eu un intérêt accru dans les protocoles qui s'appuient sur des interactions entre les différentes couches. Cross-Layer Design est devenu la nouvelle architecture dans les systèmes de communication sans fil, elle cherche à renforcer la capacité des réseaux sans fil de manière significative, grâce à l'optimisation conjointe de plusieurs couches dans le réseau. Les réseaux ad-hoc mobiles ont généré beaucoup d'intérêt dans un passé récent à cause de leurs nombreuses

applications potentielles. Multi-sauts implique l'existence de nombreux appareils répartis géographiquement qui partagent le médium sans fil qui crée le besoin d'efficacité MAC, et les protocoles de routage afin d'atténuer les interférences et de profiter pleinement de la réutilisation spatiale. Cross-Layer Design est une proposition à soutenir des approches émergentes flexibles pour réseaux ad-hoc mobiles (MANET). Dans ce papier [BSM11], les auteurs ont présenté quelques propositions de conception par l'analyse des activités de recherche en cours dans ce domaine pour optimiser les performances des protocoles de routage et ceux de MAC dans MANET.

- les réseaux mobiles ad hoc (MANET) adoptent généralement une architecture peer-to-peer. La déconnexion entre une paires de nœuds, induite par la mobilité, ce qui rend l'entretien des routes difficiles et dégrade la capacité du réseau. Dans le papier [AKN11], ils ont présenté un schéma de routage pour la gestion proactive des déconnexions, par la fusion de l'information provenant s'appuyant sur de multiples niveaux de la pile de protocoles réseau en utilisant l'approche d'interaction entre couches. Un défi majeur dans les MANET est d'élaborer des méthodes efficaces pour assurer la disponibilité des routes tout en contrôlant la surcharge. les techniques de routage peuvent être divisées en deux types de protocoles : proactifs et réactifs. les protocoles proactifs souffrent souvent de surcharge de contrôle excessif associé au maintien de routes vers les destinations, même quand il n'est pas nécessaire; les protocoles réactifs retardent les paquets de bout en bout par rapport à des protocoles proactifs, car les routes doivent être réformées pendant la communication. Le plus souhaitable protocole de routage est celui qui offre un minimum de retards de paquets de bout en bout pour le trafic en temps réel et moins de contrôle pour les trafics en non temps réel. Ceci peut être réalisé que par l'exploitation des informations d'état de lien (tels que la durée de vie lien) qui est généralement ignoré dans les environnements ad hoc, les protocoles de routage: même les protocoles hybrides, existants n'utilisent pas les informations d'état de liaison, et donc n'offrent pas un avantage énorme sur les performances actuelles. La durée de vie d'un lien (LLT) est l'une des informations d'état de liaison la plus importante, principalement contrôlée par

déconnexion due à la mobilité et la défaillance d'un nœud en raison du manque de puissance.

- Comme les réseaux mobiles ad hoc (MANET) gagnent en popularité, la nécessité de disposer d'un protocole MAC et des protocoles de routage adéquats va continuer à croître. Cross layer est une proposition à soutenir des approches émergentes couche flexible de MANET. L'algorithme LEMO (Less remaining hop More Opportunity) a été proposé pour améliorer le taux de livraison des paquets et l'équité entre les flux de réseaux mobiles ad hoc par le biais de l'interaction entre la couche MAC et la couche de routage. Les informations de routage concernant le total des sauts restants requis par un paquet pour atteindre sa destination est exploitée par la couche MAC afin de donner la priorité aux paquets qui sont plus proches de leur destination. Ce document [MKC10] compare les performances de l'algorithme de LEMO en utilisant les protocoles DSR et AODV de la couche de routage et de varier la mobilité et les conditions de charge. Avec l'aide d'indicateurs de performance tels que taux de livraison de paquets, le délai de bout en bout retard et normalisé la charge de routage, il est démontré que la superposition entre les DSR et IEEE 802.11 DCF fonctionne mieux que la superposition entre AODV et IEEE 802.11 DCF.
- L'un des problèmes très sérieux auxquels est confronté un MANET (Mobile Ad hoc Network) est la durée de vie très limitée de ses nœuds mobiles. Cette contrainte est considérée comme conséquence de l'absence d'échange d'informations sur l'état des mobiles entre le protocole MAC, supportant généralement un mécanisme de sauvegarde de l'énergie, et le protocole de routage. Cette absence d'informations conduira le protocole de routage à solliciter souvent des nœuds à faible énergie qui s'épuisera rapidement ainsi causera la rupture d'activité du réseau. Ces problèmes nécessitent de considérer les interactions entre les protocoles en question et de bien les étudier afin de dégager des solutions qui les optimisent. Dans [HAL09], ils ont étudié, en premier lieu, les interactions entre les protocoles MAC et routage pour une meilleure QoS (Quality of Service) dans les MANET, et

terminé leurs travail par proposer deux solutions pour ces interactions, dont l'implémentation et la simulation fera l'objet de leurs futurs travaux. Et comme solutions proposées après cette analyse de problème, la performance du mécanisme de sauvegarde de l'énergie supporté par le protocole MAC, notamment 802.11 DCF, dépend fortement de ce dernier (le protocole MAC) et du protocole de routage les quels il faut interagir d'une manière coopérative pour cette finalité à savoir une meilleure et équitable consommation d'énergie entre les différents nœuds du réseau. A travers cette étude d'interactions, il semble important de fonder la conception de solutions sur les interactions entre protocoles et viser une meilleure consommation d'énergie qui prend en compte les points suivants : Certains ou tous les nœuds ayant une énergie faible, doivent être évités dans le routage afin de maintenir des valeurs d'énergie pareilles pour tous les nœuds mobiles, ainsi garantir une plus longue vie du réseau. Les nœuds mobiles n'opteront pas pour le mode de sauvegarde de l'énergie si cela provoquera une rupture de connectivité dans le réseau.

- Ce travail [ROF06] se concentre sur la conception, le développement, et l'évaluation des mécanismes cross-layer basés sur le protocole 802.11 et qui visent à améliorer la qualité de service dans ce type de réseaux.

Avant d'étudier les approches cross-layer, ils ont exploré l'idée d'améliorer, séparément, le fonctionnement d'une couche de communication ; à savoir le protocole MAC 802.11 e qui est conçu pour la différenciation de service. Bien qu'on ait aboutit à des améliorations en utilisant un nouveau mécanisme adaptatif de la couche MAC, les résultats des études de performance montrent les limitations de l'architecture en couches qui a, par ailleurs, démontré ses bons résultats dans les réseaux filaires.

Il y a de nombreuses possibilités d'interaction inter-couche. Dans [ROF06] ils intéressent au partage de paramètres entre la couche MAC et la couche routage. Ils estiment que la coopération entre ces deux couches fournit une meilleure amélioration de performance que la coopération entre d'autres couches. En particulier, ils se concentrent sur le problème de l'acheminement des paquets de données d'une manière qui prend en compte le niveau de congestion du canal, les caractéristiques de réseau, et les besoins de protocoles

de couches hautes. Les auteurs proposent un routage optimal en ce qui concerne la stabilité des liens, le délai de bout-en-bout, et la conservation d'énergie, avec et sans assistance/initiation de réseau. Ils proposent plusieurs mécanismes cross-layer qui visent à résoudre le problème de routage dans MANETs tout en augmentant la performance des importantes métriques de qualité de service tels que ; la stabilité du chemin, la consommation d'énergie, le délai de bout-en-bout. A cet effet, ils identifient les paramètres adéquats à partir de la couche MAC et la couche réseau et ils les adaptent pour fournir de la qualité de service basé sur de nouveaux algorithmes de coopération inter-couches. En outre, ils identifient les avantages et les inconvénients des architectures inter-couches par rapport à l'architecture en couche traditionnelle pour améliorer la performance de protocoles de communication dans un environnement sans fil.

- La prochaine norme IEEE 802.11e a été développée pour offrir des capacités QoS pour le WLAN, offrant des améliorations significatives au trafic multimédia. MANET bénéficieront également de cette nouvelle technologie depuis les interfaces sans fil les plus largement déployées et utilisées IEEE 802.11 sont basées. Dans cet article **[CMM]** ; ils ont exposé les résultats relatifs à l'interaction des protocoles de routage réactifs pour les MANET et de la technologie IEEE 802.11e. Ils ont constaté que des améliorations très substantielles en termes de débit et de routage sont atteints en raison de la réactivité de routage. Ils ont détaillé la relation entre le comportement expérimentés dans chaque cas et les mécanismes internes du protocole de routage utilisé, offrant une vue des phénomènes.
- Dans ce document **[BDM02]**, ils ont étudié l'effet de la mobilité et l'interaction entre divers paramètres sur les performances des protocoles conçus pour les réseaux ad hoc sans fil. Un objectif important est d'étudier l'interaction du routage et des protocoles de couche MAC dans les paramètres de mobilité différente. Ils ont utilisé trois modèles de mobilité de base: modèle de mobilité de grille, modèle waypoint aléatoire, et exponentielle du modèle corrélé au hasard. Les performances des protocoles sont mesurées en

termes de qualité de service diverses, y compris la latence, le débit, le nombre de paquets reçus et l'équité à long terme. Trois différents protocoles de routage couramment étudiés sont utilisés: AODV, DSR et LAR. De même des protocoles MAC sont utilisés: la MACA, 802.11 et CSMA. Leur principale contribution est basée sur la simulation d'expériences couplées à une analyse statistique rigoureuse pour caractériser l'interaction entre les paramètres ci-dessus indiqué. A partir des résultats, ils ont conclu qu'en général, il n'est pas significatif pour parler d'un MAC ou un protocole de routage dans l'isolement. Présence d'interaction conduit à des arbitrages entre la quantité de paquets de contrôle générés par chaque couche. Les résultats soulèvent la possibilité d'améliorer les performances d'un protocole de couche MAC notamment en utilisant un protocole de routage intelligemment conçu, ou vice-versa.

- Le protocole MAC IEEE 802.11, utilisé dans les réseaux mobiles ad hoc (MANET), souffre du problème bien connue qui est l'équité. Dans ce papier [ZSA03], en utilisant le routage statique, ils ont d'abord étudié l'équité MAC en considérant trois facteurs, notamment la station cachée, qui est liés à la propriété d'atténuation du signal des réseaux sans fil. Depuis le protocole MAC et le protocole de routage interagissent les uns avec les autres, ils ont ensuite étudié l'interaction entre l'équité MAC et mécanisme routage en remplaçant le routage statique avec AODV et DSDV. Les principaux enseignements tirés de ces études sont: (i) la distinction entre l'équité MAC et l'équité globale du système, (ii) dans l'étude de l'équité MAC, on doit isoler les facteurs (par exemple, le protocole de routage) qui ne sont pas directement liés à la couche MAC, et (iii) d'étudier l'équité globale du système, en plus de l'étude de l'équité MAC, on doit aussi examiner les effets de nombreux autres facteurs tels que le mécanisme de routage, modèle de trafic, modèle de mobilité etc.
- Pour les réseaux sans fil multi-sauts, la performance de chaque nœud est une fonction complexe des facteurs suivants: - les signaux utilisés dans la couche physique; - la topologie du réseau de radio, - l'ordonnancement de transmission établi à la couche MAC, - les résultats de sélection du tracé de la couche réseau. L'entrée de tout composant ci-dessus est partiellement décidé

par la sortie des autres composantes, par exemple le choix du chemin qui relie les nœuds décide quels seront utilisés pour les transmissions, puisque les paquets de contrôle de routage sont transmis comme des paquets de données à la couche MAC, le calendrier de transmission décide comment les informations de routage seront propagées à travers le réseau. Par conséquent, l'analyse des performances des piles de protocoles dans un réseau sans fil doit prendre en compte les interactions entre les différentes couches. En fait, une perspective inter-couche à l'analyse du rendement et la conception du protocole porté à l'attention des avancées récentes dans les réseaux sans fil. Il est essentiel de traiter l'ensemble de la pile de protocole comme une seule structure algorithmique, afin d'améliorer la performance et, en général, il n'est pas significatif pour parler d'un MAC ou un protocole de routage dans l'isolement. Ce travail [XGS] présente un cadre de modélisation pour la performance obtenue avec un protocole MAC en collaboration avec les différentes disciplines de transmission de paquets sur le dessus d'une couche physique réaliste.

### 2.2.2. Notre contribution :

Les changements fréquents de topologie et la contrainte de batterie entraînent généralement des ruptures des liens et qui rendent le maintien des routes assez compliqué. Dans les protocoles de routage, la solution la plus évidente est de créer des routes avec un minimum de sauts possible. Cette approche est intéressante dans la mesure où elle est bien étudiée et minimise les délais. Une autre préoccupation très importante est l'économie de l'énergie au niveau MAC, mais la politique de minimiser le nombre de nœuds pour une route n'est pas vraiment idéale pour l'économie de l'énergie, vu que les nœuds diffèrent dans leurs quantité d'énergie disponible. Les travaux de recherche faits en ce sens visent à concevoir des protocoles de routage qui minimisent la consommation d'énergie au sein des nœuds. La majorité de ces solutions vise à utiliser dans le routage des nœuds avec une quantité assez suffisante d'énergie et éviter au maximum les nœuds avec une quantité minimale. Le principe de cette stratégie est d'éviter une courte vie des nœuds (ainsi celle du réseau), ainsi éviter les ruptures de routes et une utilisation non équitable de l'énergie. La majorité des protocoles MAC (exemple de 802.11 DCF) proposés dernièrement

dans cette optique optent pour la méthode de mise en veille des nœuds lorsqu'ils ne sont pas actifs (pas de réception et pas d'émission).

Un nœud non actif peut être mis en veille même s'il dispose d'une grande quantité d'énergie. Du fait de cette grande quantité, le nœud sera plus probable d'être sélectionné par le protocole de routage afin de participer au routage et dire que ce nœud est en phase d'économie d'énergie (mode veille).

Ce problème s'accroît si le nœud passé en mode veille a créé une rupture de connectivité du réseau, alors cela perturbera tout le réseau et conduira à retarder la procédure de découverte de nouvelle route et regagner la connectivité du réseau (si il y a d'autres nœuds plus adéquats pour participer dans le routage, sinon, attendre la réveil du ou des nœuds qui sont en mode veille). Tous ces processus encombreront le réseau avec le trafic manipulé (message de contrôle et les overheads). Donc, le protocole MAC, dans sa gestion de l'énergie, influence négativement sur le bon fonctionnement du protocole de routage et cela parce que les interactions entre ces deux protocoles ne sont pas prises en compte.

- Nous proposons un mécanisme qui va prendre en compte cette interaction entre ces deux protocoles, qui permet le réveil des nœuds mis en veille et susceptible d'avoir une grande quantité d'énergie, par la stratégie d'économie d'énergie dans la couche MAC (citée plus haut). Il s'agit d'un message de contrôle (message de réveil) de catégorie d'accès prioritaire dans MAC, émet par le nœud source ; pour ce faire nous proposons l'intégration de l'information de quantité d'énergie disponible dans les tables de routage des nœuds ; ainsi cette information sera échangée périodiquement dans les protocoles de routage proactifs, et peut aider à sélectionner la route dans les protocoles réactifs. Et dans ces derniers (protocoles réactifs) avant l'envoi la demande de route, il doit être précédé par le message de réveil.

### **2.3. Interaction entre le protocole TCP et le protocole de routage :**

#### **2.3.1. Etat de l'art :**

Les principales raisons qui entraînent une dégradation de performance dans les réseaux ad hoc proviennent, de la qualité du lien sans fil, mais également, de la qualité du chemin donc le protocole de routage. Plus précisément, une raison à la

dégradation de performance provient du comportement erroné de TCP ; le protocole déduit à tort un état de congestion du réseau et diminue inutilement son débit d'émission. Cette mauvaise interprétation de l'état du réseau est provoquée par des pertes de données qui ne sont pas dues à de la congestion mais plutôt à un routage erroné.

Dans la suite, nous allons présenter quelques travaux de recherche faits en ce sens, et l'interaction entre TCP et routage :

- Le routage échoue fréquemment à cause de la mobilité des nœuds dans un MANET. Le protocole TCP fonctionne mal généralement dans les MANET, car l'algorithme de contrôle de congestion prend tous les problèmes dans les MANET (déconnexions, des changements d'itinéraire, etc.). Pour améliorer l'efficacité de la transmission de bout en bout, ce document [SGU10] propose un protocole de transmission inter-couches de contrôle qui interagit avec le lien fiable des protocoles de routage, qui est appelé TCP-PLRT (Transmission Control Protocol basé sur la probabilité de durée de vie résiduelle du lien). TCP-PLRT juge de la stabilité de bout en bout grâce à des informations de connexion sur la probabilité de la durée de vie résiduelle d'un lien que sur la rétroaction de la couche de routage. Trois mécanismes complémentaires ont été proposées: Routing Switch, si le lien n'est pas assez stable, SAVE puis vers l'avant, si le lien est sur le point de casser, et reconfirmer ACK, si l'acheminement a été reconstruit. Par conséquent, le protocole TCP-PLRT peut faire de prédiction avant un routage échoué. Il a été démontré par simulation sur ordinateur que les résultats du protocole TCP-PLRT ont considérablement amélioré la perte de paquets, causée par l'échec de routage, et ont augmenté le débit beaucoup plus.
- Les réseaux ad hoc mobiles (MANET) est un réseau sans fil, sans infrastructure ni centralisation et disposent d'un déploiement facile et abouti à de nombreuses applications dans l'ère moderne. Dans [YSK10], les auteurs ont examiné des aspects différents des protocoles de routage tels que l'évolutivité, la mobilité de la charge du réseau, et retarder le protocole TCP pour analyser la performance des protocoles de routage DSR, OLSR et AODV. Le trafic HTTP est utilisé sur le réseau conçu. Des métriques sont

utilisées pour l'analyse des performances. Dans les résultats de simulation, aucun des protocoles qu'ils ont sélectionné, n'a montré dans tous les différents aspects pris en considération, des meilleures performances. Ils ont conclu que l'efficacité d'un réseau peut être réalisée en choisissant les meilleurs protocoles appropriés fondée sur l'exigence du réseau.

- Dans [TAA09], ils ont examiné l'impact du retard moyen d'acheminement Average Path Delay Routing (APDR) pour TCP, dans les réseaux ad hoc. L'algorithme de découverte de route est basé sur le plus faible temps moyen (Time Average) du chemin, ainsi que sur OLSR. Bien qu'une telle approche puisse sembler évidente pour les performances de TCP, son étude de simulation sur des scénarios réalistes sur MANET permet de tirer des conclusions intéressantes. Premièrement, le chemin choisi par le protocole OLSR n'est pas toujours le meilleur du point de vue temps aller-retour ; Round-Trip Time (RTT) de TCP, de sorte que le plus court chemin ne garantit pas nécessairement le plus bas retard. Par conséquent, une diminution de temps moyen de bout en bout est souvent faite au détriment d'un plus long chemin. Même si la probabilité de collision n'augmente pas en raison de l'augmentation de nombre de sauts, les résultats APDR dans la réduction du débit global. Comme le montre, les événements d'oscillations du chemin régulier provoque le ré ordonnancement des paquets, et dans le contexte du protocole TCP, évoquent la reproduction des acquittements (ACK) et les retransmissions. Les oscillations se produisent parce que la route d'un nœud ne peut pas distinguer le retard qu'il induit à la chaîne, du retard total. Deuxièmement, le retard seul n'est pas suffisant comme une métrique de routage, sans l'invocation d'un régime de réservation de chemin, pour éviter l'instabilité des routes. Dans les réseaux ad hoc sans mobilité, nous appliquons APDR utilisant le routage source, sans changer le chemin pendant le flux de TCP. Avec la réservation de chemin, APDR surpasse OLSR standard et améliore le débit. L'étude APDR aide à comprendre plus profondément le comportement TCP par rapport à la densité et la mobilité, et les rendements pour le routage source, afin d'éviter les chemins multiples.

- Dans cette recherche [NHJ08], ils ont d'abord étudié l'interaction inter-couche entre TCP et les protocoles de routage dans la norme IEEE 802.11 des réseaux ad hoc. Les protocoles de routage réagissent aux événements de réseau tels que le bruit du canal, la mobilité, et la congestion, ce qui, en association avec le protocole TCP, détériore la qualité de la connexion de bout en bout. La mauvaise connectivité de bout en bout détériore les performances de TCP à son tour. Basé sur la célèbre équation TCP-friendly, dans cette recherche, ils ont procédé à une étude quantitative sur la plage de fonctionnement de protocole TCP en utilisant un routage statique et les flux TCP montrent que Additive-Increase, Multiplicative-Decrease (AIMD) et le comportement du mécanisme de la fenêtre TCP est agressif pour une norme IEEE 802.11 multi-sauts typiques réseau avec un faible produit bande passante-retard. Ensuite, pour répondre à ces problèmes, ils ont proposé deux mécanismes complémentaires, qui sont, l'incrémentaire fractionnaire de la fenêtre TCP (FEW), le régime et la notification Route-échec à l'aide de la politique en vrac de perte de déclenchement BULK-loss Trigger (ROBUST). Le protocole TCP est un peu une solution préventive pour réduire la perte de congestion pour liaison sans fil. La politique ROBUST est une solution corrective qui permet des protocoles de routage à la demande pour supprimer la sur-réaction induite par le comportement agressif du TCP. Il est démontré par simulation sur ordinateur que ces deux mécanismes se traduisent par une amélioration significative du débit TCP, sans modifier la fenêtre de base TCP ou les mécanismes MAC sans fil.
- TCP, le protocole de transport utilisé pour transporter la majeure partie du trafic Internet, fonctionne mal dans les réseaux mobiles ad hoc (MANET) ; aussi largement rapportés dans la littérature. Ceci est principalement dû aux interactions entre TCP et protocoles des couches inférieures. Parmi ces derniers, les protocoles de routage ont peut-être le plus grand impact sur les performances de TCP. Dans ce papier [MSL07], par simulation extensive, les auteurs ont démontré comment TCP interagit avec certains des protocoles de routage standardisés par IETF ; réactifs (AODV, DSR) et proactif (OLSR) dans des conditions différentes de réseau tels que la charge, la taille et la

mobilité. Contrairement à la plupart des études antérieures, qui ont compté uniquement sur le trafic TCP, ils considèrent un trafic plus réaliste transportant un mélange de Constant Bit Rate (CBR) et TCP.

- Des recherches récentes dans les réseaux mobiles ad hoc (MANET) ont souligné l'effet néfaste des temporisations de retransmission multiples timeouts (RTO) sur le débit TCP. Cependant, l'effet de la stratégie de mise en mémoire tampon du protocole de routage sur ce phénomène n'a pas été explicitement démontré ou étudié. Dans [TAA06], ils présentent et analysent par des simulations en utilisant banc d'essai fonctionnel de routage des agents, des performances de débit TCP. Les résultats de l'analyse sur trois populaires protocoles de routage, à savoir AODV, DSR et OLSR, produit un aperçu des différents modèles de comportement de TCP au cours de cette manifestation, et met en évidence les mécanismes de chaque protocole de routage qui l'affectent. Par ailleurs, les arbitrages dans le choix des paramètres de routage à l'égard de la performance TCP sont discutés.
- Le groupe de travail IETF MANET (Mobile Ad hoc Network) a standardisé le protocole AODV (Ad Hoc Distance Vector On demand) et le protocole OLSR (Optimized Link State Routing) comme réactif et proactif des protocoles de routage, respectivement. En outre, du point de vue de la couche transport, TCP (Transmission Control Protocol) est toujours nécessaire pour MANET, car il est largement utilisé dans l'Internet actuel et adapté à une intégration harmonieuse avec l'Internet fixe. Particulièrement, le TCP et ses variantes, à savoir le protocole TCP-Reno et TCP-Vegas. Cependant, il n'y a pas eu de travaux de recherche sur la comparaison des performances étendues de TCP-TCP-Reno et Las Vegas au cours de AODV et OLSR. Ce document [DHJ05] est le premier essai pour effectuer des recherches en utilisant le simulateur NS-2. Grâce à des simulations approfondies, les auteurs ont constaté que : choisir parmi les protocoles de routage est plus important de choisir parmi les variantes TCP, car la différence de performance entre TCP-Reno et TCP-Vegas sur n'importe quel protocole de routage sélectionnée n'est pas tellement exceptionnel.

- Le débit obtenu dans un réseau ad hoc est affectée par plusieurs facteurs, y compris les interférences radio, la capacité du protocole de routage à réagir aux changements de topologie, et d'une interaction complexe entre les applications et protocoles sous-jacents. Cet article [RNG] étudie expérimentalement l'impact de ces facteurs sur les protocoles UDP et TCP. En outre, lorsque les protocoles TCP et UDP font quelques sauts dans un réseau ad hoc il ya une interaction complexe entre les protocoles de transport, ainsi qu'avec le protocole de routage. Les résultats montrent que cette interaction entraîne une gigue UDP significative, les liaisons instables affaiblie nettement le débit TCP. Ils ont utilisé un banc d'essai contrôlé réel pour les expériences et un outil graphique qui capture les interactions.
- TCP a été principalement développé pour être déployée dans les réseaux filaires. Récemment, de nombreuses recherches ont étudié ses performances au sein de réseaux mobiles ad hoc (MANET). Les résultats de recherche ont constaté que les performances de protocole TCP sont fortement influencées par les caractéristiques de ces réseaux. Cela est dû à la manière que le protocole TCP utilise pour mettre en œuvre la fiabilité et de son incapacité à distinguer entre les différentes raisons de perte de paquets. En effet, contrairement aux réseaux câblés, où la perte de paquets est principalement causée par la congestion du réseau, dans les MANET nous pourrions avoir de nombreuses autres raisons pour perdre un paquet de données. Toutefois, le protocole TCP considère que toutes les pertes de paquets sont dues à la congestion du réseau. Ceci impose à TCP d'être agressif en face de certains types de perte de paquets. Les pertes de paquets dans les MANET peuvent être soit liés à l'environnement de communication sans fil (à savoir les interférences, multi-chemin de routage, etc.) ou de la nature dynamique de ces réseaux (défaillances de liaison, le partitionnement de réseau). Ce dernier pourrait être dû à la mobilité des nœuds ou à l'épuisement de la batterie d'un nœud. Cela pourrait conduire à un recalcul fréquent d'une route au sein du réseau. Dans ce travail [SGS], les auteurs ont l'intention d'étudier l'effet des protocoles de routage ad hoc sur les performances du protocole TCP dans les

MANET. Ils considèrent dans leur étude différents types de protocoles de routage ad hoc ayant des caractéristiques différentes: réactive vs proactif, vecteur de distance par rapport à l'état des liens, et le routage source. Les résultats de l'étude montrent que le protocole de routage proactif DSDV conduit à des résultats plus acceptables des performances de TCP et cela est confirmé au niveau de mobilité différente.

- TCP/IP est le protocole réseau standard sur Internet et est également le plus largement utilisé. Pour ces raisons, son utilisation sur Mobile Ad-Hoc Networks est une certitude. Les réseaux ad hoc sont sujets aux défaillances des liens dues à la mobilité. TCP est incapable de distinguer entre les pertes dues aux défaillances d'acheminement et les pertes dues à la congestion. En conséquence, le débit se dégrade de manière significative lorsque les nœuds se déplacent. Il est donc essentiel d'étudier comment le protocole TCP s'effectue plus dans les réseaux ad-hoc. Dans [AAS00], ils ont utilisé des simulations dans ns pour analyser les performances de TCP Tahoe sur un ensemble de protocoles de routage, y compris la stabilité du signal adaptatif du protocole de routage qu'ils ont mis en œuvre dans NS-2. Ils identifient les caractéristiques de chacun de ces protocoles de routage qui déterminent le comportement de TCP sur eux.

### 2.3.2. Notre contribution :

Dans les travaux vus précédemment, il a été prouvé que les performances TCP sont fortement influencées par la nature dynamique des réseaux mobiles ad hoc, en raison de la mobilité des nœuds. Aussi, le choix du protocole de routage ad hoc à mettre en œuvre au sein du réseau affecte le comportement TCP au sein de ce réseau. En effet, d'une part, la surcharge de messages de contrôle provoquée par le protocole de routage pourrait conduire à la congestion du réseau. Ainsi, on applique le protocole TCP pour déclencher son algorithme de contrôle de congestion. D'autre part, l'approche de recouvrement de route utilisée par le protocole de routage peut avoir un bon ou un mauvais effet sur le comportement TCP. Par conséquent, si le temps de récupération fait par le protocole de routage pour rétablir un lien rompu est plus court que le timer RTO de TCP, TCP ne connaîtra pas de perte de paquets. Sinon,

TCP émetteur reconnaît la perte de paquets par le timer RTO. Cette dernière mènera TCP à réagir de façon inadéquate aux pertes de paquets en déclenchant son algorithme de contrôle de congestion.

- Nous avons constatés que la mobilité des nœuds n'est pas toujours un facteur de dégradation des performances TCP. Parfois, la mobilité peut aider les protocoles de routage ad hoc de rétablir les liens brisés rapidement. Cela empêche l'algorithme TCP expéditeur contrôle de congestion pour commencer. L'importance est de choisir le taux de mobilité. Comme un résultat général, nous avons constaté que DSDV pourrait être le meilleur choix pour être mis en œuvre lorsqu'on utilise TCP dans les réseaux mobiles ad hoc. En effet, il s'est avéré être le meilleur protocole de routage performants avec toutes les variantes TCP dans l'environnement ad hoc mobiles. DSDV, comme un protocole de routage proactif à vecteur de distance, comprend toutes les routes disponibles vers n'importe quelle destination dans le réseau dans sa table de routage.

### Conclusion :

**D**ans ce chapitre, nous avons exposés une approche qui se base non seulement sur l'étude des couches séparément, mais sur leurs interactions pour le bon fonctionnement dans un MANET, en premier lieu nous avons présentés l'approche cross-layer ainsi que ses différents modèles, et par la suite nous avons faits un état de l'art sur les différentes interactions sur les couches liaison de données, réseau et transport entre leurs protocoles respectivement :

- TCP/MAC.
- TCP/Routage.
- MAC/Routage.

Et nous avons proposés notre contribution sur ces différentes interactions pour une meilleure QoS dans les MANETs.

L'évolution rapide et la popularité des technologies sans fil auprès des consommateurs a conduit à l'omniprésence d'appareils numériques sans fil dans le contexte quotidien d'une personne. Ces technologies sans fil et les réseaux ad hoc peuvent être exploités dans différents types de scénarios allant d'une simple visite guidée d'un site historique, à une opération militaire d'une grande envergure.

Dans les réseaux mobiles ad hoc, les nœuds peuvent être en mobilité permanente rendant ainsi la topologie du réseau dynamique. Ce sont des systèmes totalement distribués qui offrent beaucoup d'avantage à leur utilisation, mais qui posent beaucoup de difficultés quand à leur développement et normalisation.

Les réseaux ad hoc utilisent une transmission sans fil directe entre les équipements sans passer par des stations de base : ils n'ont pas d'architecture. La transmission entre les nœuds adjacents est gérée par un protocole d'accès au médium et un protocole de routage lorsque la source doit utiliser des relais pour joindre la destination. Les protocoles d'accès et de routage ont fait l'objet de nombreuses recherches qui ont abouti à la standardisation de solutions spécifiques. Cependant l'utilisation de ces solutions ne résout pas les problèmes de performances au niveau des protocoles supérieurs. Les réseaux ad hoc, outre la transmission sans fil et la capacité de routage, sont également caractérisés par la mobilité de leurs éléments. Les protocoles de transport qui sont chargés de fiabiliser la communication sur des réseaux à pertes sont affectés par ce type de comportement. Alors qu'ils ont été conçus pour s'adapter aux problèmes de congestion dans les réseaux filaires, il s'agit à présent pour eux de s'adapter à la mobilité en utilisant au mieux les ressources limitées du système.

La plupart des approches visant à offrir une QoS dans les réseaux sans fil sont limitées à un niveau particulier et les interactions avec les couches adjacentes sont souvent négligées. L'approche de communication inter-couches (cross layer) mise en œuvre pour optimiser les performances d'un protocole d'un niveau donné, en fonction de ses dépendances à d'autres niveaux. L'adaptation des protocoles de transport, routage et accès au médium par une communication inter-couches est l'approche utilisée dans cette thèse.

Contrairement à ce qui a été étudié auparavant, où les protocoles sont conçus séparément ; les protocoles dans l'approche dite cross-layer, conçus ou utilisés en

exploitant les dépendances ou les interactions entre les couches dans le but d'améliorer les performances. Cross layer utile pour les réseaux sans fil :

- Ajustement dynamique des paramètres TCP suivant la qualité du signal.
- Choix des routes dans un réseau ad hoc suivant la qualité des liens.
- Adaptations des temps d'accès au support suivant les contraintes des applications temps réel....

Violation de l'architecture de référence :

- Communications directe entre protocoles non adjacents ;
- Echange de variables entre couches sans passer par un service ;
- Fusion des protocoles de 2 couches adjacentes ;
- Ajustement successif des paramètres des couches inférieures pour améliorer les performances au niveau application.

Les interactions entre les couches peuvent être directes :

Exemple 1 : une indication de perte non résolue au niveau MAC est transmise à la couche TCP pour son mécanisme de recouvrement.

Exemple 2 : des mesures de métrique au niveau MAC peuvent servir des décisions de routage dans un contexte ad hoc.

Notre contribution, s'agit d'un état de l'art et un recueil bibliographiques des différents travaux de recherche faits en ce sens et proposer quelques ajustements pour une adaptation à une interaction entre couches (protocoles) ; pour une meilleure QoS dans un MANET.

## **Bibliographie :**

**[BOU10]** : Nadir BOUCHAMA, Qualité de service dans les réseaux mobiles ad hoc. Conférence donnée à l'occasion du 25 ème anniversaire du CERIST. Ben Aknoun. Algérie. Juin 2010.

**[CGL06]** : Claude Chaudet, Isabelle Guérin Lassous. Etat des lieux sur la qualité de service dans les réseaux ad hoc. 2006.

**[WIK11]**: [http://fr.wikipedia.org/wiki/Qualite\\_de\\_service](http://fr.wikipedia.org/wiki/Qualite_de_service).

**[PSO10]** : Patrick SONDI OBWANG, Docteur de l'Université de Valenciennes et du Hainaut-Cambrésis, Le Routage à Qualité de Service dans les Réseaux Mobiles Ad Hoc, 2010.

**[BAD05]** : HAKIM BADIS, Étude et conception d'algorithmes pour les réseaux mobiles et ad hoc, thèse doctorat de l'université paris-sud, 2005.

**[XSL00]**: H. Xiao, W.K.G Seah, A. Lo, and K.C. Chua. A flexible quality of service model for mobile ad hoc networks. In IEEE vehicular Technology Conference, Tokyo, Japan, Mai 2000.

**[CGL03]** : Claude Chaudet, Isabelle Guérin Lassous. Routage QoS et réseaux ad hoc : de l'état de lien à l'état de nœud. 2003.

**[APV01]** : K. Al Agha, G. Pujolle and G. Vivier, Réseaux de mobiles & Réseaux sans fil. No. ISBN 2-212-11018-9, Eyrolles, 2001.

**[GER06]**: A. GERON. WIFI deployment et sécurité. Edition : DUNOD. 2006.

**[DGA03]** : F. DI GALIO. WiFi L'essentiel qu'il faut savoir... 2003.

**[BAD98]** : Nadjib BADACHE, la mobilité dans les systèmes répartis, 98.

**[IEE03]**: IEEE Standard Information Technology. Telecommunications and Information Exchange Between Systems. Local and Metropolitan Area Networks. Specific requirements. Part 11 : Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. Juin 2003.

**[ETS98]**: ETSI. Broadband radio Access Networks (BRAN) ; High Performance Radio Local Area Network (HIPERLAN) Type1 ; Functional specification. Juillet 1998.

**[ETS00]**: ETSI. Broadband radio Access Networks (BRAN) ; High Performance Radio Local Area Network (HIPERLAN) Type2 ; System Overview.

**[TIS99]** : J. Tisal. Le réseau GSM, l'évolution GPRS : une étape vers l'UMTS. 3 éditions DUNOD 1999.

**[NSL00]**: K. J. Negus, A. P. Stephens, J. Lansford. HomeFR : Wireless Networking for the Connected Home. IEEE Personal Communications. Février 2000.

**[CCL03]** : I. Chlamtac, M. Conti, J.-N et liu. Mobile ad hoc networking : imperatives and challenges. 2003.

**[BCG04]**: S. Basangi, M. Conti et S. Giordano. Ad hoc Networking. IEEE Press, wiley-Interscience, A John wiley and Sons. Publication. 2004.

**[PEJ]** : J.M Percher, B. Jouga. Détection d'intrusions dans les réseaux ad hoc. Ecole supérieure d'électronique de l'ouest, Angers, France.

**[CHE04]** : Guillaume CHELIUS. Architectures et communications dans les réseaux spontanés sans-fil. Doctorat en Informatique de l'INSA de Lyon. 2004.

**[NGU09]** : NGUYEN Van Thiep. Le protocole TCP sur les réseaux radio multi saut. Hanoï, Juin 2009.

**[MAM]** : Z. MAMMERI, Routage à QoS dans les réseaux ad hoc mobiles.

**[PUJ03]** : G. PUJOLLE, Les réseaux. Edition : EYROLLES. 2003.

**[BSA07]** : R. BELAID, B. SI AHMED ; Une nouvelle approche pour l'économie de l'énergie dans les MANETs. 2007.

**[MUH02]** : P. MUHLETHALER. 802.11 et les réseaux sans fil. Editions : EYROLLES 2002.

**[HHN06]**: Hung-Cuong Le, Herve Guyennet and Noureddine Zerhouni. Over-hearing for Energy Efficient in Event-Driven Wireless Sensor Network. In First IEEE International Workshop on Intelligent System Techniques for Wireless Sensor Networks (IST-WSN), Vancouver Canada, Oct, 2006.

**[BOU11]** : Mohamed BOUHARRAS, ordonnancement équitable dans la couche mac avec détection multi-usagers dans les réseaux ad hoc, montréal, 2011.

**[HUN07]**: Hung-Cuong Le. A Clustered Data-Centric Storage for Wireless Sensor Networks. In the Third International Workshop on Distributed Framework for Multimedia Applications (DFMA), Paris, France, 5-6 July 2007.

**[HHN07]**: Hung-Cuong LE, Hervé Guyennet and Noureddine Zerhouni. Mobile Effect Reduction in Data-Centric Storage for Wireless Sensor Networks. The Third IET International Conference on Intelligent Environments (IE'07), Ulm, Gemany, September 2007.

**[HHV07]**: Hung-Cuong LE, Hervé Guyennet and Violeta FELEA. OBMAC: An Overhearing Based MAC Protocol for Wireless Sensor Networks. The International Conference on Sensor Technologies and Applications (SENSORCOMM), Valencia, Spain, October 2007.

**[LOR05]** : Jean LORCHAT. Amélioration du protocole MAC dans 802.11 dans 802.11 Définition d'un protocole de remplacement conservant la couche PHY, 2005.

**[DHO03]** : D. Dhoutaut. Etude du standard IEEE 802.11 dans le cadre des réseaux ad hoc : de la simulation à l'expérimentation. PhD thesis, Insa de Lyon, December 2003.

**[BLU]**: <http://www.bluetooth.org>.

**[BJG01]** : L. Bao and J.J. Garcia-Luna-Aceves, A New Approach To Channel Access Scheduling For Ad Hoc Networks, *Seventh Annual International Conference on Mobile Computing and Networking*, 2001.

**[ROG03]** : V. Rajendran, K. Obraczka, and J. Garcia-Luna-Aceves, Energy-efficient, collision-free medium access control for wireless sensor networks, *in 1st ACM Conf. on Embedded Networked Sensor Systems*, Los Angeles, CA, November 2003.

**[SCI01]**: E. Shih, S.-H. Cho, N. Ickes, R. Min, A. Sinha, A. Wang, and A. Chandrakasan, Physical layer driven protocol and algorithm design for energy-efficient wireless sensor networks, *in International Conference on Mobile Computing and Networking*, Rome, Italy, 2001.

**[NAA10]** : Zied NAAS. Étude de l'équité du protocole tcp dans les réseaux multi-saut. Montréal, 2010.

**[EBQ05]**: h. M. El-sayed, o. Bazan,u. Qureshi, m. Jaseemuddin. Performance evaluation of tcp in mobile ad-hoc networks college of information technology, uae university, uae 2005.

**[ABD09]** : ABDELLAOUI, Rachid. Su-olsr une nouvelle solution pour la sécurité du protocole olsr. Montréal, le 05 mai 2009.

**[BAC05]** : Nouha BACCOUR. Etude comparative de deux simulateurs pour les réseaux sans fil Ad-hoc. Ecole Nationale d'Ingénieurs de Sfax. 2005.

**[DIJ11]** : <http://fr.wikipedia.org/w/index.php?oldid=64297583>.

**[SOU03]** : Mohsen SOUISSI. Routage IP. ENSTA Réseaux informatiques et protocoles de communication. 2003.

**[HAB08]** : Loïc Habermacher. Routage réactif dans les réseaux mobiles ad hoc. 2008.

**[VDM06]**: VAN DER MEERSCHEN Jérôme. Hybridation entre les modes ad-hoc et infrastructure dans les réseaux de type Wi-Fi. 2006.

**[LEM00]** : Tayeb Lemlouma Mastère de thèse sur le routage dans les réseaux ad-hoc : le routage dans les réseaux ad-hoc , USTHB , Septembre 2000.

**[BSM11]**: P.K.Alima Beebi, Sulava Singha, Ranjit Mane, A Study on Cross Layer MAC design for performance optimization of routing protocols in MANETs. (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No.2, February 2011.

**[AKN11]:** Awadhesh Kumar, Dr. Neeraj Tyagi. Cross-layer self organized routing protocol for MANET. International Conference on Computer Communication and Management Proc .of CSIT vol.5 IACSIT Press, Singapore.2011.

**[FSJ11]:** Farzaneh R. Armaghani<sup>1</sup> and Sudhanshu S. Jamuar<sup>2</sup>, TCP-MAC Interaction in Multi-hop Ad-hoc Networks. 1.Monash University, GSIT, 2.Department of Electrical Engineering, University of Malaya,1.Australia, 2.Malaysia. 2011.

**[MKC10]:** Manjul Walia, Rama Krishna Challa, Performance Analysis of Cross-Layer MAC and Routing Protocols in MANETs, ICCNT '10 Proceedings of the 2010 Second International Conference on Computer and Network Technology IEEE Computer Society Washington, DC, USA. 2010.

**[YCX10] :** Yongkang Xiao; Cuiling Ji; Xiaoyan Hu; Bo Sun; Research of Interaction between TCP and MAC Protocol in Multihop Ad Hoc Networks. Sch. of Inf. Sci. & Technol., Beijing Normal Univ., Beijing, China. 2010.

**[HAL09] :** Sofiane HAMRIOUI, Mustapha LALAM, Interactions entre le Protocole MAC et le protocole de Routage pour l'Optimisation de la performance dans un MANET. Département d'Informatique, Université des Sciences et de la Technologie Houari Boumediene, Alger, ALGÉRIE ; Laboratoire de Recherche en Informatique (LARI), Université Mouloud Mammeri, Tizi ouzou, ALGÉRIE. 2009.

**[ACL06]:** H. Aiache, V. Conan, J. Leguay and M. Levy, "XIAN : Cross-Layer Interface for Wireless Ad hoc Networks", Mediterranean Ad Hoc Networking Workshop (MedHoc), Lipari Italy, June 2006.

**[ACL08] :** H. Aiache, V. Conan, L. Lebrun, J. Leguay, S. Rousseau and D. Thoumin, "XIAN Automated Management and Nano-Protocol to Design Cross-Layer Metrics for Ad hoc Networking", The International Federation for Information Processing Networking (IFIP Networking), Singapore, May 2008.

**[VKK05]:** V. Kawadia and P. R. Kumar, "A cautionary perspective on cross-layer design", IEEE Wireless Communications, pp. 3-11, February 2005.

**[VSM05] :** V. Srivastava and M. Motani, "Cross-layer design : a survey and the road ahead", IEEE Communications Magazine, vol. 43, no. 12, pp. 112-119, December 2005.

**[RSL06]:** V.T. Raisinghani and S. Iyer, “Cross Layer Feedback Architecture for Mobile Device Protocol Stacks”, IEEE Communications Magazine, Special Issue of Cross-Layer Protocol Engineering, January 2006.

**[HBL07] :** HAMRIOUI Sofiane, BOUAMRA Siham et LALAM Mustapha, Optimisation de l’algorithme de Backoff du protocole MAC pour une meilleure performance du protocole TCP dans les MANET. Laboratoire de Recherche en Informatique (LARI), Université Mouloud Mammeri de Tizi Ouzou, Algérie, 2007.

**[HXY07]:** Hongqiang Zhai, Xiang Chen, and Yuguang Fang, Improving Transport Layer Performance in Multihop Ad Hoc Networks by Exploiting MAC Layer Information, 2007.

**[ZSA03]:** Zhifei Li, Sukumar Nandi, and Anil K. Gupta; Study of IEEE 802.11 Fairness and its Interaction with Routing Mechanism. School of Computer Engineering, Nanyang Technological University, Singapore. In the Fifth IFIP International Conference on Mobile and Wireless Communications Networks (MWCN), Singapore, Oct. 2003.

**[XGS]:** XinWang, J.J. Garcia-Luna-Aceves, Hamid R. Sadjadpour; Performance Modeling of MAC and Multipath Routing Interactions in Multi-hop Wireless Networks. University of California, Santa Cruz. USA.

**[BDM02]:** Chris Barrett, Martin Drozda, Achla Marathe, Madhav V. Marathe, Characterizing the Interaction Between Routing and MAC Protocols in Adhoc Networks. Los Alamos National Laboratory. 2002.

**[MRD04] :** Mahesh K. Marina, Samir R. Das, Impact of caching and MAC overheads on routing performance in ad hoc networks. Department of Computer Science, State University of New York at Stony Brook, Stony Brook, NY. 2004.

**[CMM]:** Carlos T. Calafate, Pietro Manzoni, and Manuel P. On the interaction between IEEE 802.11e and routing protocols in Mobile Department of Computer Engineering Polytechnic University of Valencia (UPV), Valencia, Spain.

**[ROF06]:** LAMIA ROMDHANI-FILLALI, Cross-Layer Design Of IEEE 802.11 Based Mobile Ad Hoc Networks For QoS Provisioning. Paris, 2006.

**[LGP]** : Stephane Lohier, Yacine Ghamri Doudane, and Guy Pujolle, MAC-layer Adaptation to Improve TCP Flow Performance in 802.11 Wireless Networks Institut Universitaire de Technologie (IUT) de Marne la vallée.

**[MRH09]** : Adnan Majeed, Saquib Razak, Nael B. Abu-Ghazaleh, Khaled A. Harras, TCP over Multi-Hop Wireless Networks: The Impact of MAC Level Interactions. State University of New York at Binghamton

**[PBA09]**: J.premalatha, p.balasubramanie, Simulation Analysis of QoS parameters by combining MAC and TCP in MANETSAsst. Professor, department of computer science and engineering Kongu engineering college, erode, tamilnadu, india, 2009.

**[DPH]** : Dmitri D. Perkins and Herman D. Hughes, The Interaction of Medium Access Control and TCP in Ad Hoc Networks, Department of Computer Science and Engineering, Michigan State University,

**[LGP]** : Stéphane Lohier, Yacine Ghamri Doudane et Guy Pujolle, Adaptation de la couche MAC pour améliorer les performances des flux TCP dans les réseaux 802.11 LIP6 - Université de Paris VI, Institut d'Informatique d'Entreprise,

**[FSJ08]** : Farzaneh R. Armaghani, Sudhanshu S. Jamuar, Sabira Khatun, Mohd F. A. Rashid, An Adaptive TCP Delayed Acknowledgment Strategy in Interaction with MAC Layer over Multi-hop Ad-hoc Networks. Department of Computer and Communication System Engineering, Department of Electrical and Electronic Engineering, University Putra Malaysia. 2008.

**[RVC03]**: Rui Jiang, Vikram Gupta, Chinya V. Ravishankar, Interactions Between TCP and the IEEE 802.11 MAC Protocol. Computer Science and Engineering Department, University of California, Riverside, 2003.

**[KSR09]**: A Cross-Layer Based High Throughput MAC Protocol for 802.11 Multihop Adhoc Networks, 2009. K. Saravanan ,Paavai College of Technology, Salem, Tamilnadu, India  
T. Ravichandran, Principal, Hindustan Institute of Technology, Coimbatore, Tamilnadu, India.

**[YSK10]**: Yamsani Ravikumar, Sarath Kumar Chittamuru ; A Case Study on MANET Routing Protocols Performance over TCP and HTTP, School of Engineering

Blekinge Institute of Technology, Box 520, SE-372 25 Ronneby , Sweden. 2010.

**[SGU10]:** SUN Jie , GUO Wei ; Cross Layer Transmission Control Protocol Interacting with Link Reliable Routing in MANET. National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China, Chengdu, 611731, China. 2010.

**[SGS]:** Alaa Seddik-Ghaleb, Yacine Ghamri-Doudane, Sidi-Mohammed Senouci, Effect of Ad Hoc Routing Protocols on TCP Performance within MANETS Networks & Multimedia Systems Research Group (LRSM), Institut d'Informatique d'Entreprise (IIE) Evry.

**[RNG]:** Christian Rohner, Erik Nordstrom, Per Gunningberg, Christian Tschudin; Interactions between TCP, UDP and Routing Protocols in Wireless Multi-hop Ad hoc Networks. Uppsala University, Sweden and University of Basel, Switzerland.

**[MSL07] :** Consolee Mbarushimana, Ali Shahrabi, Hadi Larijani ; The effect of routing protocol dynamics on TCP performance in mobile ad hoc networks; School of Computing and Mathematical Sciences, Glasgow Caledonian University, Glasgow, UK, NBIS'07 Proceedings of the 1st international conference on Network-based information systems. 2007.

**[TAA06]:** Despina Triantafyllidou, Khaldoun Al Agha, on the interaction of TCP and Routing Protocols in MANETs. AICT/ICIW. 2006.

**[DHJ05] :** Dongkyun Kim, Hanseok Bae, Jeomki Song, Analysis of the Interaction between TCP Variants and Routing Protocols in MANETs, Kyungpook National University, ICPPW '05 Proceedings of the 2005 International Conference on Parallel Processing Workshops. 2005.

**[NHJ08]:** Kitae Nahm, Ahmed Helmy, and C.-C. Jay Kuo, Cross-Layer Interaction of TCP and Ad Hoc Routing Protocols in Multihop IEEE 802.11 Networks. IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 7, NO. 4, APRIL 2008.

**[TAA09]:** TRIANTAFYLLIDOU D / AL AGHA K. Improve TCP Performance In Ad Hoc Networks, With Delay Routing Andpath Reservation. Unité Mixte De Recherche 8623 CNRS-Université Paris Sud –Lri 03/2009.

**[AAS00]** : Ashish Ahuja, Sulabh Agarwal, Jatinder Pal Singh, Rajeev Shorey,  
Performance of TCP over Different Routing Protocols in Mobile Ad-Hoc Networks.  
IBM India Research Labs, Block I, Indian Institute of Technology,  
Hauz Khas, New Delhi 110016, India. 2000.