GENERALITES SUR LES RESEAUX MOBILES SANS FIL

Introduction

Dans la seconde moitié des années 90, plusieurs normes pour les réseaux sans fil à portée limitée ont été développées. Leur arrivée a soulevé un engouement nouveau pour les réseaux radio multisauts, qui étaient le domaine exclusif des militaires.

Dans ce chapitre, nous présentons ces différentes normes, en particulier l'architecture, la position dans le modèle OSI et la méthode d'accès de la norme IEEE 802.11 plus particulièrement 802.11a, 802.11b et 802.11g, de Bluetooth (802.15) et d'HiperLAN qui sont désormais utilisées dans la plupart des travaux appliqués de la communauté ad hoc.

I. L'ARCHITECTURE SANS FIL 802.11

Cette technologie est conçue pour les réseaux locaux, en entreprise ou chez les particuliers. Elle permet de relier des équipements de type PC, PC portable ou PDA (Personal Digital Assistant) en utilisant des ondes radio[1]. Les performances atteintes (11 à 54 Mbits/s pour des portées de l'ordre d'une centaine de mètres) permettent d'envisager le remplacement partiel de réseaux filaires de type Ethernet et d'éviter ainsi les contraintes de câblage [32, 33].
La norme 802.11 implémente deux modes de fonctionnement :

- le mode « infrastructure » ou BSS (Basic Service Set) ;
- le mode « ad hoc ».

En mode « infrastructure » les stations de base reliées entre elles par un réseau filaire, assurent la couverture d'une zone et prennent en charge les mobiles dans leur voisinage. Les stations de base (SB) sont munies d'une interface de communication sans fil pour la communication directe avec les stations mobiles localisées dans une zone géographique limitée. Cette zone est appelée cellule et est contrôlée par un point d'accès (AP, Access Point), qui coordonne les transmissions et sert de pont entre le réseau câblé et le WLAN.

Le mode « ad hoc » permet à des stations de communiquer directement entre elles sans utiliser un point d'accès. Pour pouvoir fonctionner sur un réseau étendu, ce mode doit être associé à un protocole de routage permettant à des stations distantes de communiquer par l'intermédiaire d'autres stations faisant office de routeurs.

[1] Onde radio (onde radioélectrique) est une onde électromagnétique (déplacement d'électrons dans le vide) dont la fréquence est comprise entre 9 KHz à 3000 GHz.

1. La norme IEEE 802.11 dans le modèle IEEE

Cette norme concerne la couche MAC du modèle IEEE (Institute of Electrical and Electronics Engineers) associée à différentes normes de transmission physique (infrarouge : IR ou radio : FHSS/DSSS) [32, 33]. La figure 1.1 illustre la position de la norme IEEE 802.11 dans le modèle OSI.

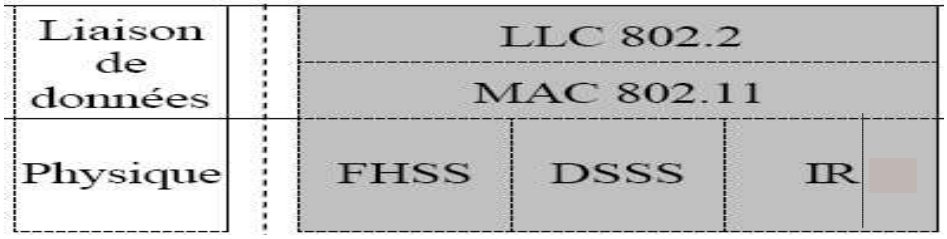

Figure 1. 1 : modèle de couches de la norme IEEE 802.11

a. La couche physique

Le standard définit actuellement une seule couche MAC qui interagit avec 3 couches physiques :

- **FSSH** (Frequency Hopping Spread Spectrum): la plupart des interférences nuisibles aux transmissions radio n'agissent en fait que sur des bandes de fréquences assez étroites. Si par malchance de telles interférences ont lieu où l'on transmet, alors le signal sera fortement brouillé. Cette technique consiste à transmettre sur toute la largeur de la bande avec un saut de fréquence (un changement de canal) toutes les 20 ms suivant une séquence commune d'une BSS. Elle utilise la bande sans licence ISM (Industrie, Science, Médecine) des 2.4 GHz (2.4000- 2.4835 GHz), divisée en 79 canaux de 1 MHz chacun. Cette technique accroît l'immunité au bruit et permet une co-localisation ;
- **DSSS** (Direct Sequence Spread Spectrum) : pour lutter contre les interférences importantes agissant sur des plages de fréquences assez étroites, il existe la technique de l'étalement de spectre. Elle consiste à ne transmettre que sur un seul canal par BSS. La technique de la séquence directe divise la bande des 2.4 GHz en 14 canaux de 20 MHz chacun. Pour compenser le bruit il est utilisé une technique de chipping qui consiste à convertir chaque bit de données en une séquence de 11 bits ;
- **IR** (Infrarouge) : le standard IEEE 802.11 prévoit également une alternative à l'utilisation des ondes radio qui est la lumière infrarouge. La technologie infrarouge a pour caractéristique principale d'utiliser une onde lumineuse pour la transmission de données. Ainsi les transmissions se font de façon unidirectionnelle, soit en "vue directe", soit par réflexion. Le caractère non dissipatif des ondes lumineuses offre un niveau de sécurité plus élevé. Il est possible grâce à la technologie infrarouge d'obtenir des débits

allant de 1 à 2 Mbit/s en utilisant une modulation appelée PPM (pulse position modulation) ;

- Une autre technique est aussi intégrée au niveau de cette couche : c'est le **OFDM** (Orthogonal Frequency Division Multiplexing). Les systèmes OFDM [36, 37] subdivisent le canal (ici un canal de 22 MHz) en N sous canaux (appelés également porteuses : 52 sous porteuses dont 48 pour les données et 4 pour la synchronisation) dont les fréquences centrales sont espacées d'un multiple de l'inverse de la période symbole 1/T. Chacune des porteuses peut être considérée comme un émetteur à part entière, c'est donc une parallèlisation des flux.

b. La sous-couche MAC

Elle définit deux modes de fonctionnement sur la coordination des échanges correspondant à deux méthodes d'accès différentes [32, 33] :

- **PCP** (Point Coordination Function): ce mode est basé sur l'interrogation à tour de rôle des terminaux par l'AP (méthode déterministe), dont le but est la gestion de l'accès au canal. C'est le point d'accès qui indiquera à chacun des mobiles qui lui sont rattachés quand ils devront émettre leurs paquets en imposant l'ordre des transmissions ;
- **DCF** (Distributed Coordination Function): ce mode n'est pas fondé sur une gestion centralisée. Les liaisons radio ne sont pas full duplex, la méthode de détection de collision de type CSMA/CD (Carrier Sense Multiple Access with Collision Detection) ne peut être utilisée dans la mesure où la station ne peut pas être à l'écoute pendant son émission. C'est pourquoi un mécanisme d'écoute de porteuse avec évitement de collision et acquittement est donc utilisé dans le DCF. Il s'agit de la méthode d'accès CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). Un MANET utilise uniquement le DCF. Le mode CSMA/CA est illustré par la figure 1.2.

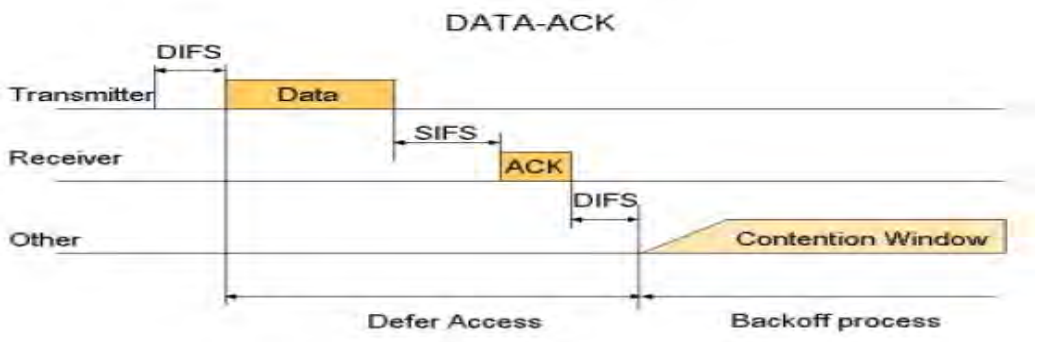

Figure 1. 2 : mode CSMA/CA

Le mode CSMA/CA présente des limites. Par exemple une station peut écouter le canal et à chaque fois qu'il est occupé, elle émet pour provoquer un déni de service par l'envoi d'un **Jam** (rupture de la communication), car les paquets Jam sont prioritaires. Un attaquant peut aussi monopoliser le médium pour une longue période à cause du faible débit qu'il utilise. Il pénalise ainsi les autres nœuds qui ont un débit supérieur, puisque tous les nœuds ont la même probabilité d'accéder au canal.

Par ailleurs, un autre problème spécifique au sans fil est celui du "nœud caché", où deux stations situées de chaque côté d'un point d'accès peuvent entendre toutes les deux une activité du point d'accès, mais pas de l'autre station. Ce problème est généralement lié aux distances ou à la présence d'un obstacle. Pour résoudre ce problème, le standard 802.11 définit sur la couche MAC un mécanisme optionnel de type **RTS/CTS** (Request to Send/Clear to Send) appelé mécanisme de Virtual Carrier Sense (sensation virtuelle de porteuse).

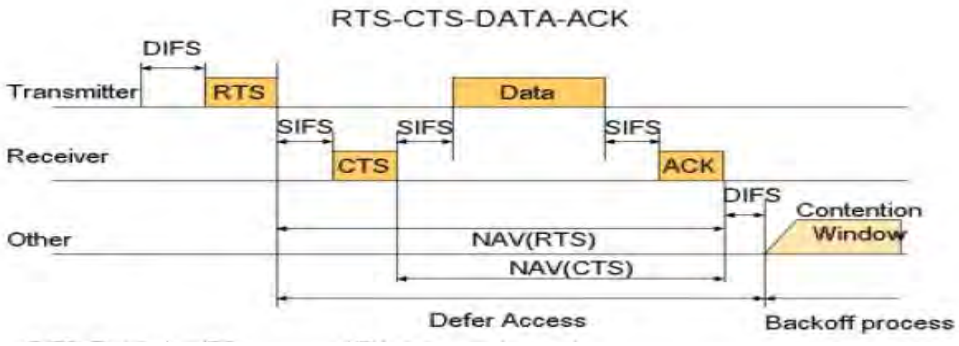

Figure 1. 3 : mode RTS/CTS

Le RTS/CTS présente des inconvénients. Un attaquant peut envoyer un grand nombre de **RTS** ou **CTS** aux autres stations, ces derniers lui réservent le canal et il peut nier la transmission empêchant une station qui voulait émettre d'émettre, provoquant ainsi un déni de service.

La couche LLC (Logical Link Control) normalisée 802.2 permet de relier un WLAN 802.11 à tout autre réseau respectant l'une des normes de la famille 802.*x*. La norme IEEE 802.11 est en réalité la norme initiale offrant des débits de 1 ou 2 Mbps. Des révisions ont été apportées à la norme originelle afin d'optimiser le débit [28, 29, 30]. Ces normes sont représentées dans le tableau 1.

Tableau 1 : Tableau récapitulatif des normes 802.11

Norme	Fréquence	débit	Portée	Mode d'accès	Technique de transmission
802.11a	5 GHz.	54 Mbit/s en théorie et 30 Mbit/s réels	~25 m à 75m	CSMA/CA RTS/CTS	OFDM un canal de 22 MHz en 52 sous canaux
802.11b	2.4 GHz	11 Mbit/s, 6.5 Mbit/s	~50 m à 300m	CSMA/CA RTS/CTS	DSSS 14 canaux de 20 MHz
802.11g	2.4 GHz	54 Mbit/s en théorie et 30 Mbit/s réels	~25 m à 75m	CSMA/CA RTS/CTS	OFDM. un canal de 22 MHz en 52 sous canaux

II. La norme HiperLAN (High performance LAN)

L'ETSI propose une normalisation des WLAN (Wireless LAN) haut débit appelée HiperLAN. On distingue en général deux grands types d'HiperLAN [28, 30, 32] :

- **HiperLAN 1 :** est un standard de l'ETSI (European Telecommunications Standards Institute). L'architecture est totalement décentralisée, il n y a pas de notion de point d'accès et les nœuds HiperLAN 1 peuvent jouer des rôles de passerelles. Il utilise le mécanisme d'accès au médium **EY-NPMA** (Elimination Yield-Non Preemptive Multiple Access) qui gère les priorités et fonctionne en trois phases [30];
- **HiperLAN 2 :** est basé sur une centralisation poussée. Les points d'accès appelés Access Points (AP) sont reliés entre eux par une infrastructure réseau filaire ou non-filaire. HiperLAN 2 peut fonctionner en mode sans infrastructure fixe. Dans ce cas, un mobile est élu pour jouer le rôle de contrôleur central et les autres vont s'attacher à lui. Les deux normes sont représentées dans le tableau 2.

Tableau 2 : Tableau récapitulatif des normes HiperLAN

Norme	Fréquence	débit	Portée	Mode d'accès	Technique de transmission
HiperLAN1	5.15-5.30 GHz	23.5 Mbit/s	~50 m	EY-NPMA	OFDM un canal de 22 MHz en 52 sous canaux
HiperLAN2	5.15-5.30 GHz	23.5 Mbit/s	~200 m	Maître/ESclave	OFDM un canal de 22 MHz en 52 sous canaux

1. Les couches d'HiperLAN

Au niveau des couches, HiperLAN se décompose ainsi :

- la couche CAC (Channel Access Control) prend en charge la partie technique de l'accès au support, selon qu'il soit libre ou non. C'est elle qui définit le niveau de priorité lors de la transmission des paquets ;
- la couche MAC (Medium Access Control) : c'est elle qui prend en charge la partie logique c'est-à-dire la mise en forme de la trame, le routage interne, la gestion de priorité, l'insertion et le retrait des stations ;
- la couche physique HiperLAN utilise les mêmes techniques de transmission que la couche physique de la norme 802.11 a.

La figure 1.4 montre les couches d'HiperLAN.

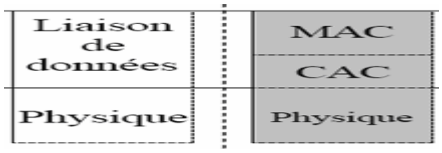

Figure 1. 4 : les couches d'HiperLAN

2. Méthodes d'accès d'HiperLAN

L'HiperLAN utilise la méthode d'accès au médium **EY-NPMA** (Elimination Yield-Non Preemptive Multiple Access). C'est lui qui permet en particulier de contrôler la gestion des priorités. Le fonctionnement de **EY-NPMA** est particulièrement intéressant puisqu'il est prévu pour fonctionner dans un contexte ad hoc. Il fonctionne en trois phases [30] :

- **la phase de priorité** : Cinq niveaux de priorité sont définis par la norme (de 0 pour le plus prioritaire à 4) et la phase de priorité est donc divisée en cinq slots. Au début d'un nouveau cycle de transmission, tous les nœuds qui veulent accéder au canal vont envoyer un burst de signalement (signal de demande d'accès au canal), dont la date de début dépend de la priorité du paquet. Plus la priorité est élevée, plus le burst commence tôt ;
- **La phase d'élimination :** Il se peut que plusieurs nœuds veuillent émettre en même temps des paquets de priorités identiques, donc il faut les départager. Pour cela, chaque nœud va poursuivre l'envoi de son burst de signalement pendant un nombre aléatoire de slots. Ce sera celui qui aura tiré le plus grand nombre qui l'emportera. Dès que l'émission de notre burst est terminée, nous écoutons le canal. Si nous y détectons de l'activité, c'est qu'un autre nœud a tiré un plus grand nombre que nous et nous abandonnons pour ce cycle ;

- **La phase d'écoute :** Si toutefois il reste plusieurs nœuds en lice alors l'élimination va se terminer dans la troisième phase. Un nombre aléatoire de slots est choisi. C'est celui qui a tiré le plus petit qui pourra transmettre. Chaque nœud attend la durée qu'il a déterminé, en écoutant le canal. S'il détecte de l'activité alors qu'il n'a pas fini d'attendre, il sait que quelqu'un a tiré un plus petit nombre que lui et il n'émettra pas durant ce cycle. Si son attente se termine alors que le canal est toujours libre, alors il émet. Il faut noter que si le paquet est envoyé en point à point, il sera acquitté par son récepteur.

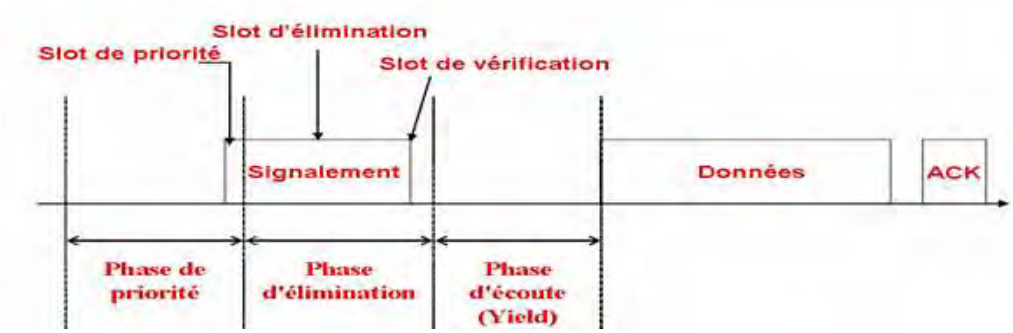

Figure 1. 5 : Procédure de EY-NPMA

Le mode EY-NPMA présente des insuffisances. Un attaquant peut créer un déni de service en envoyant un grand nombre de bust de signalement lors de la demande de priorité. Il peut aussi empêcher les nœuds légitimes d'accéder au canal car s'ils y détectent de l'activité, c'est qu'un autre nœud a tiré un plus grand nombre qu'eux et ils abandonnent pour ce cycle, l'attaquant peut le faire indéfiniment créant ainsi des boucles.

III. L'Architecture sans fil 802.15 (Bluetooth)

C'est le suédois Ericsson qui en 1994 est l'initiateur de Bluetooth (BT). Par la suite BT est devenue la norme **IEEE 802.15** après la création d'un consortium : le Bluetooth **S**pecial **I**nterest **G**roup (**SIG**) formé en mai 1998 à l'initiative de plusieurs gros constructeurs dont Nokia, Intel, IBM, Toshiba et Ericsson. Le Bluetooth est une liaison radio faible portée (10 mètres) et qui opère dans la bande **ISM** (réservée aux applications **I**ndustrielles, **S**cientifiques et **M**édicales) de 2.4 GHz et qui offre un débit d'environ 1 Mbits/s. Cette technologie est destinée à relier par onde radio des équipements légers de type téléphone portable, PDA, lecteurs audio, appareils domestiques, ou encore PC portables. La bande ISM est mondiale donc Bluetooth est internationalement interopérable [27, 28, 29, 30].

1. Les couches de la norme IEEE 802.15

La norme IEEE 802.15 concerne la couche MAC du modèle IEEE associée à une transmission physique par ondes radio [32, 33] :

- **la couche physique** : comme pour Wifi, les transmissions utilisent la bande sans licence ISM des 2.4 GHz. Celle-ci est divisée en 79 canaux de 1 MHz chacun avec la même technique de saut de fréquence FSSS ;
- **La sous-couche MAC** : contrairement aux méthodes d'accès type CSMA des normes 802.3 et 802.11, la méthode est déterministe et les échanges sont réglés par la station maîtresse du piconet qui alloue au esclave demandeur un temps de parole. Lors de la transmission, le temps est découpé en tranches ou slot time. Chaque slot correspond à une durée de 625 µs.

Conclusion

Cette partie a permis de sortir de nombreuses technologies sans fil standardisées et de les caractériser. Les caractéristiques de ces technologies permettent de nombreuses variations de topologies, de débits, et autorisent une connectivité de plus en plus importante. Cependant, cette diversité entraîne par elle même de nombreux trous de sécurité pour l'intégrateur de solutions. Chacune d'elles représente un compromis entre différents facteurs tels que la portée, le débit, les contraintes temporelles, le mode fonctionnement...

Partie II :
LES RESEAUX MOBILES AD HOC

CHAPITRE 2 : GENERALITES SUR LES RESEAUX MOBILES AD HOC

I. Définition des réseaux mobiles ad hoc

Un réseau **Ad Hoc** est généralement appelé **MANET** (**M**obile **A**d hoc **NET**work). Ce nom a été attribué à un groupe de travail à l'**IETF** ((**I**nternet **E**ngineering **T**ask **F**orce). Les membres de ce groupe soumettent régulièrement des propositions de protocoles de routage adaptés aux réseaux mobiles Ad hoc [24, 25].

Un réseau **Ad Hoc** consiste en un regroupement d'une grande population d'unités mobiles se déplaçant dans un territoire quelconque, avec leur interface sans fil pour seul moyen de communication. Le tout ne repose sur aucune infrastructure préexistante ou administration centralisée. L'architecture d'un réseau ad hoc est représentée par la figure 2.1.

Figure 2. 1 : Architecture d'un réseau mobile ad hoc

II. Caractéristiques des réseaux mobiles ad hoc

Les réseaux mobiles ad hoc sont caractérisés dans la plupart du temps par les éléments suivants :

- **Une topologie dynamique :** les nœuds du réseau se déplacent de façon libre et arbitraire. Par conséquent, la topologie du réseau peut changer rapidement, de façon aléatoire et non prédictible;

- **Absence d'infrastructure** : les réseaux ad hoc se distinguent des autres réseaux mobiles par la propriété d'absence d'infrastructure préexistante et de toute d'administration centralisée. Les hôtes mobiles sont responsables d'établir et de maintenir la connectivité du réseau de manière continue;

- **Une bande passante limitée** : l'utilisation d'un médium de communication partagé par utilisateurs fait que la bande passante soit modeste puisque les nœuds cachés qui ne sont pas autorisés d'émettre peuvent émettre;

- **Des contraintes d'énergie** : les hôtes mobiles sont alimentés par des sources d'énergie autonomes comme les batteries. Les hôtes, pour transmettre des informations, utilisent leurs voisins pour échanger les données. Que l'on soit actif ou passif, l'hôte reçoit des informations qu'il retransmet consommant ainsi de l'énergie. Le paramètre d'énergie doit être pris en considération dans tout contrôle fait par le système;

- **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. Cette hétérogénéité de capacité peut engendrer des liens asymétriques dans le réseau. De plus, les nœuds peuvent avoir des différences en terme de capacité de traitement (CPU, mémoire), de logiciel et de mobilité (lente, rapide). Dans ce cas, une adaptation dynamique des protocoles s'avère nécessaire pour supporter de telles situations;

- **L'auto configuration :** permet aux nœuds de s'intégrer facilement dans un réseau. Elle facilite la gestion du réseau car l'interconnexion des éléments ne nécessite qu'un minimum d'intervention technique externe. Cette fonctionnalité est de plus en plus nécessaire pour un déploiement à grande échelle des réseaux sans fil ad hoc;

- **Une sécurité physique limitée :** les réseaux sans fil sont plus touchés par le paramètre de sécurité, que les réseaux filaires classiques. Cela se justifie par les contraintes et limitations physiques c'est-à-dire la propagation des ondes dans l'espace qui fait que la sécurité des données transférées doit être assurée. Dans les MANETs, le problème réside dans le fait que tous les nœuds sont équivalents et potentiellement nécessaires au bon fonctionnement du réseau. Les possibilités de s'insérer dans le réseau sont plus grandes, la détection d'une intrusion ou d'un déni de service plus délicate et l'absence de centralisation pose un problème de remontée de l'information de détection d'une intrusion. La sécurité des informations transitant sur le réseau est limitée étant donné que le média est partagé par tout le monde, y compris les personnes qui n'appartiennent pas au réseau. En effet, rien n'empêche des personnes malintentionnées d'écouter ce qui se passe sur le média, c'est-à-dire les ondes électromagnétiques.