

## CHAPITRE 1 : TYPOLOGIE DES RESEAUX SANS FIL

### Introduction

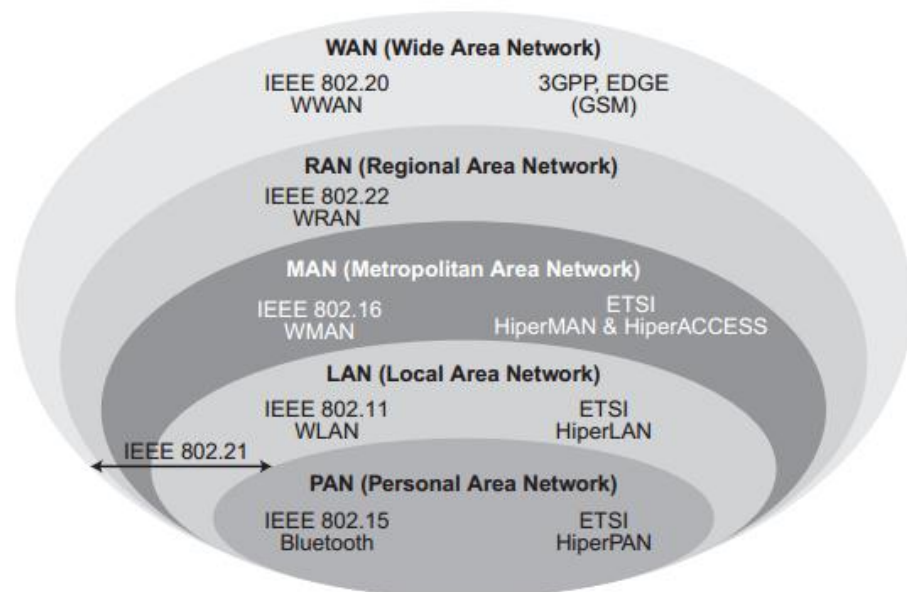
Les réseaux sans fil sont en plein développement du fait de la flexibilité de leur interface, qui permet à un utilisateur de changer de place tout en restant connecté. Les communications entre équipements terminaux peuvent s'effectuer directement ou par le biais de stations de base, appelées points d'accès, ou AP (Access Point). Les communications entre points d'accès peuvent être hertziennes ou par câble. Les débits de ces réseaux se comptent en dizaines de mégabits par seconde.

Plusieurs gammes de produits sont actuellement commercialisées, mais la normalisation pourrait encore modifier les choses. Les groupes de travail qui se chargent de cette normalisation proviennent de l'IEEE aux États-Unis et de l'ETSI sur le Vieux Continent.

La figure 21.1 décrit les différentes catégories de réseaux suivant leur étendue et la figure 21.2 les normes existantes.

)

**Figure 21.1**  
*Catégories de  
réseaux sans fil*



Les principales normes sont IEEE 802.15, pour les petits réseaux personnels d'une dizaine de mètres de portée, IEEE 802.11, ou Wi-Fi, pour les réseaux WLAN (Wireless Local Area Network), IEEE 802.16, pour les réseaux WMAN (Wireless Metropolitan Area Network) atteignant plus de dix kilomètres, IEEE 802.22, pour les WRAN (Wireless Regional Area Network), et IEEE 802.20, pour les réseaux WWAN (Wireless Wide Area Network), qui correspondent aux solutions cellulaires permettant de couvrir un pays. Pour cette catégorie

de réseaux, nous avons retenu la proposition IEEE 802.20, qui peut être considérée comme une des solutions multimédias à très haut débit concurrentes de la future quatrième génération de réseaux de mobiles.

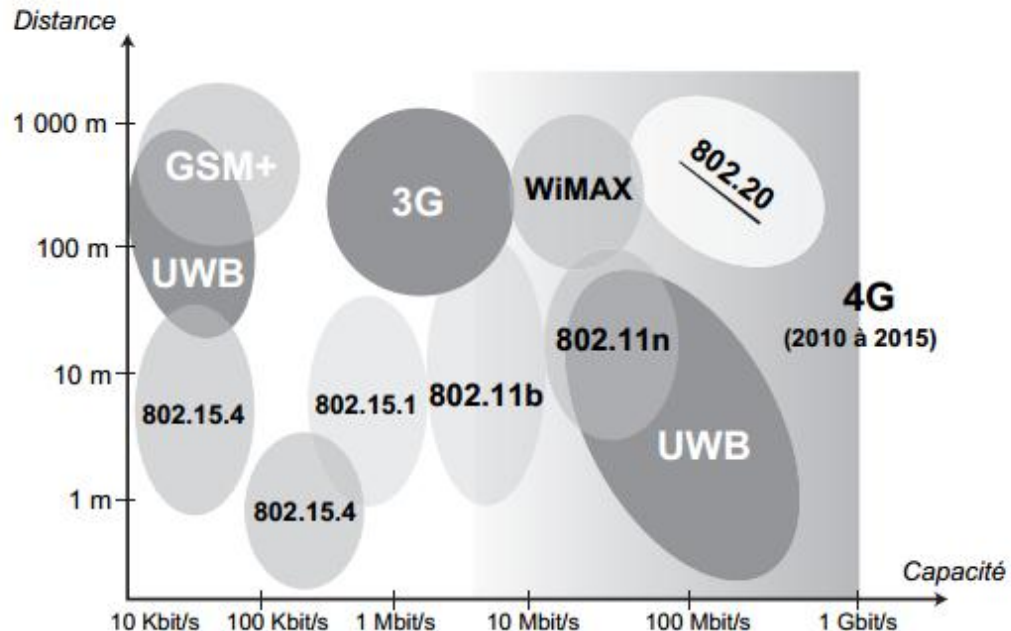


Figure 21.2

## I. Principales normes de réseaux sans fil

Dans le groupe IEEE 802.15, trois sous-groupes normalisent des gammes de produits en parallèle :

- a) IEEE 802.15.1, le plus connu, prend en charge la norme Bluetooth, aujourd'hui largement commercialisée. La version 3.0 utilise l'interface radio décrite dans IEEE 802.15.3, ce qui procure à Bluetooth une nouvelle jeunesse, avec un débit de 480 Mbit/s.
- b) IEEE 802.15.3 définit la norme UWB (Ultra-Wide Band), qui met en œuvre une technologie très spéciale, caractérisée par l'émission à une puissance extrêmement faible, sous le bruit ambiant, mais sur pratiquement l'ensemble du spectre radio (entre 3,1 et 10,6 GHz). Le débit est de 480 Mbit/s sur une portée de 3 m et décroît à environ

120 Mbit/s à une dizaine de mètres.

- a) IEEE 802.15.4 s'occupe de la norme ZigBee, qui a pour objectif de promouvoir une puce offrant un débit relativement faible mais à un coût très bas. ZigBee est avant tout normalisé pour le passage des commandes plutôt que des données. Cependant, une

version sortie en 2007 propose d'utiliser l'UWB et offre donc malgré tout un débit important.

Du côté de la norme IEEE 802.11, dont les produits sont nommés Wi-Fi (WirelessFidelity), il existe aujourd'hui trois propositions, dont les débits sont de 11 Mbit/s (IEEE 802.11b) et 54 Mbit/s (IEEE 802.11a et g). Une quatrième proposition, provenant des travaux du groupe IEEE 802.11n, permet d'augmenter fortement le débit, avec une centaine de mégabits par seconde au mieux en débit réel. Les fréquences utilisées se placent dans la bande 2,4-2,483 5 MHz pour les extensions b et g et dans la bande 5,15-5,35 MHz pour 802.11a. Les réseaux hertziens IEEE 802.16 visent à remplacer les modems ADSL, que l'on trouve sur les réseaux téléphoniques fixes, pour donner à l'utilisateur final des débits du même ordre de grandeur que l'ADSL, jusqu'à plusieurs mégabits par seconde. Ces réseaux forment ce que l'on appelle la boucle locale radio. Plusieurs normes sont proposées suivant la fréquence utilisée. Un consortium s'est mis en place pour développer les applications de cette norme sous le nom de WiMAX. Deux versions sont commercialisées, l'une fixe, dont l'objectif est clairement de remplacer l'ADSL dans les zones rurales, l'autre mobile, permettant d'avoir un modem ADSL dans sa poche et toujours connecté.

Les réseaux régionaux sont étudiés par l'IEEE 802.22. Le rayon de la cellule peut atteindre 50 kilomètres pour les gammes de fréquences en dessous de 1 GHz. La distance potentielle du terminal étant importante, le débit montant est assez limité. En revanche, sur la bande descendante, 4 Mbit/s sont disponibles. L'application de base est la télévision interactive ou les jeux vidéo interactifs.

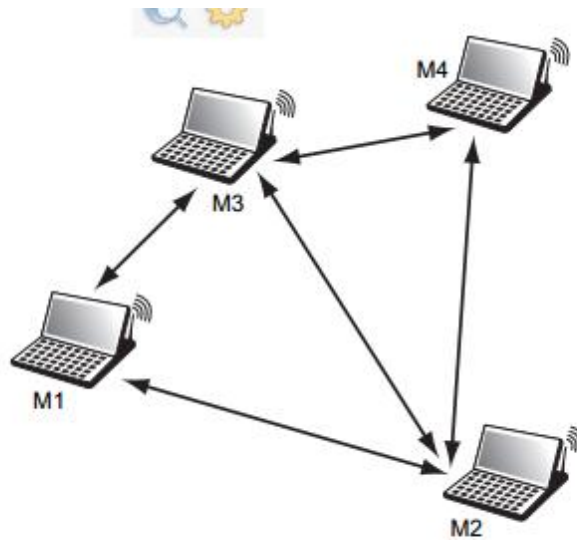
En ce qui concerne les WAN (Wide Area Network), c'est plutôt l'interconnexion des réseaux précédents qui les supporte. Pour cela, il fallait définir une norme d'interconnexion, qui a été apportée par les spécifications du groupe IEEE 802.21. On peut aussi classer dans cette catégorie la norme IEEE 802.20, qui correspond à des cellules cohérentes et permet les accès large bande.

## **II. LES RESEAUX AD-HOC**

Une autre grande catégorie de réseaux sans fil est constituée par les réseaux ad-hoc, dans lesquels l'infrastructure n'est composée que des stations elles-mêmes. Ces dernières acceptent de jouer le rôle de routeur pour permettre le passage de l'information d'un terminal vers un autre, sans que ces terminaux soient reliés directement.

Un réseau ad-hoc est illustré à la figure 21.3.

**Figure 21.3**  
*Réseau ad-hoc*



Contrairement aux apparences, les réseaux ad-hoc datent de plusieurs dizaines d'années. Ils visent à réaliser un environnement de communication qui se déploie sans autre infrastructure que les mobiles eux-mêmes. En d'autres termes, les mobiles peuvent jouer le rôle de passerelle pour permettre une communication d'un mobile à un autre. Deux mobiles trop éloignés l'un de l'autre pour communiquer directement peuvent trouver un mobile intermédiaire capable de jouer le rôle de relais.

La difficulté majeure engendrée par ce type de réseau provient de la définition même de la topologie du réseau : comment déterminer quels sont les nœuds voisins et comment aller d'un nœud vers un autre nœud ? Deux solutions extrêmes peuvent être comparées.

La première est celle d'un réseau ad-hoc dans lequel tous les nœuds peuvent communiquer avec tous les autres, impliquant une longue portée des émetteurs. Dans la seconde solution, au contraire, la portée hertzienne est la plus courte possible : pour effectuer une communication entre deux nœuds, il faut généralement passer par plusieurs machines intermédiaires. L'avantage de la première solution est la sécurité de la transmission, puisqu'on peut aller directement de l'émetteur au récepteur, sans dépendre d'un équipement intermédiaire. Le débit du réseau est minimal, les fréquences ne pouvant être réutilisées. Dans le second cas, si un terminal tombe en panne ou est éteint, le réseau peut se couper en deux sous-réseaux

distincts, sans communication de l'un à l'autre. Bien évidemment, dans ce cas, le débit global est optimisé, puisqu'il peut y avoir une forte réutilisation des fréquences.

Les techniques d'accès sont du même type que dans les réseaux de mobiles. Cependant, du fait que tous les portables jouent le rôle de BSS et qu'ils sont eux-mêmes mobiles, de nouvelles propriétés doivent être apportées à la gestion des adresses des utilisateurs et au contrôle du routage.

La solution développée pour les réseaux ad-hoc prend pour fondement l'environnement IP. Les mobiles qui jouent le rôle de passerelles — le plus souvent l'ensemble des mobiles — implémentent un routeur dans leurs circuits, de telle sorte que les problèmes posés reviennent essentiellement à des problèmes de routage dans Internet, la mobilité étant gérée par le protocole IP Mobile.

Les avantages des réseaux ad-hoc sont leurs extensions très simples, leur couverture physique et leur coût. Toutefois, pour en bénéficier pleinement, un certain nombre d'écueils sont à surmonter, telles la qualité de service et la sécurité, du fait de la mobilité des nœuds.

MANET (Mobile Ad-hoc NETwork) est le groupe de travail de l'IETF qui se préoccupe de la normalisation des protocoles ad-hoc fonctionnant sous IP. Ce groupe s'est appuyé sur les protocoles classiques d'Internet et les a perfectionnés pour qu'ils puissent fonctionner avec des routeurs mobiles.

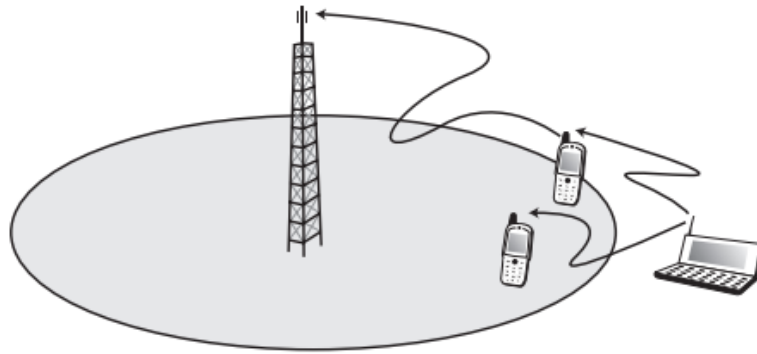
Deux grandes familles de protocoles ont été définies : les protocoles réactifs et les protocoles proactifs :

1. **Protocoles proactifs.** Les mobiles cherchent à maintenir une table de routage cohérente, même en l'absence de communication.

Les réseaux ad-hoc sont utiles dans de nombreux cas de figure. Ils permettent de mettre en place des réseaux dans un laps de temps restreint, en cas, par exemple, de tremblement de terre ou pour un meeting avec un très grand nombre de participants. Une autre possibilité est d'étendre l'accès à une cellule d'un réseau sans fil comme Wi-Fi. Comme illustré à la figure 21.4, un terminal situé hors d'une cellule peut se connecter à une machine d'un autre utilisateur se trouvant dans la zone de couverture de la cellule. Ce dernier sert de routeur intermédiaire pour accéder à l'antenne de la cellule.

Les réseaux ad-hoc posent de nombreux problèmes du fait de la mobilité de tous les équipements. Le principal d'entre eux est le routage nécessaire pour transférer les paquets d'un point à un autre point du réseau. L'un des objectifs du groupe MANET est de proposer une solution à ce problème. Pour le moment, quatre grandes propositions ont vu le jour, deux de type réactif et deux de type proactif. Parmi les autres problèmes, nous retrouvons la sécurité, la qualité de service et la gestion de la mobilité en cours de communication.

**Figure 21.4**  
*Extension de couverture  
par un réseau ad-hoc*



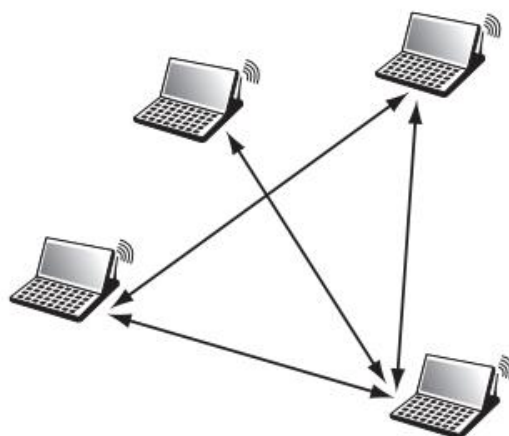
## 2. Le routage

Le routage est l'élément primordial d'un réseau ad-hoc. Il faut un logiciel de routage dans chaque nœud du réseau pour gérer le transfert des paquets IP. La solution la plus simple est évidemment d'avoir un routage direct, comme celui illustré à la figure 21.5, dans lequel chaque station du réseau peut atteindre directement une autre station, sans passer par un intermédiaire. Ce cas le plus simple correspond à une petite cellule, d'un diamètre inférieur à 100 m, comme dans un réseau 802.11 en mode ad-hoc.

Le cas classique du routage dans un réseau ad-hoc consiste à transiter par des nœuds intermédiaires. Ces derniers doivent posséder une table de routage apte à diriger le paquet vers le destinataire. Toute la stratégie d'un réseau ad-hoc consiste à optimiser les tables de routage par des mises à jour plus ou moins régulières. Si les mises à jour sont trop régulières, cela risque de surcharger le réseau. Cette solution présente toutefois l'avantage de maintenir des tables à jour et donc de permettre un routage rapide des paquets. Une mise à jour uniquement lors de l'arrivée d'un nouveau flot restreint la charge circulant dans le réseau mais décharge le réseau de nombreux flots de supervision.

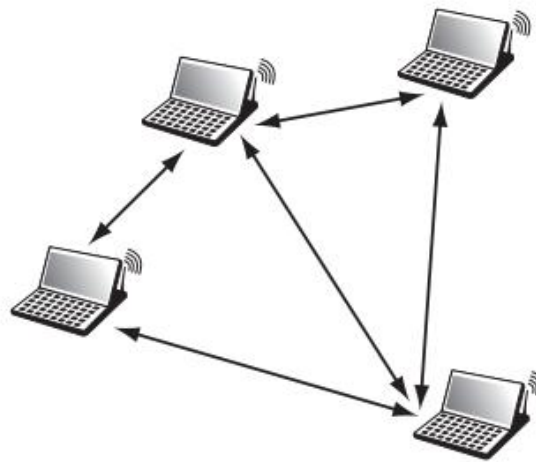
Il faut dans ce cas arriver à mettre en place des tables de routage susceptibles d'effectuer l'acheminement dans des temps acceptables.

**Figure 21.5**  
*Communication directe entre  
machines d'un réseau ad-hoc*



La figure 21.6 illustre le cas d'un réseau ad-hoc dans lequel, pour aller d'un nœud à un autre, il peut être nécessaire de traverser des nœuds intermédiaires. De nombreux écueils peuvent se trouver sur le chemin de la construction de la table de routage. Par exemple, en matière de transmission de signaux, il est possible que la liaison ne soit pas symétrique, un sens de la communication étant acceptable et pas l'autre. La table de routage doit en tenir compte. Les signaux radio étant sensibles aux interférences, l'asymétrie des liens peut par ailleurs se compliquer par l'évanouissement possible des liaisons.

**Figure 21.6**  
*Routage par le biais de nœuds intermédiaires*



Pour toutes ces raisons, les routes du réseau doivent être sans cesse modifiées, d'où l'éternelle question débattue à l'IETF : faut-il maintenir les tables de routage dans les nœuds mobiles d'un réseau ad-hoc ? En d'autres termes, vaut-il la peine de maintenir à jour des tables de routage qui changent sans arrêt ou n'est-il pas plus judicieux de déterminer la table de routage au dernier moment ?

Comme expliqué précédemment, les protocoles réactifs travaillent par inondation pour déterminer la meilleure route lorsqu'un flot de paquets est prêt à être émis. Il n'y a donc pas d'échange de paquets de contrôle en dehors de la supervision pour déterminer le chemin du flot. Le paquet de supervision qui est diffusé vers tous les nœuds voisins est de nouveau diffusé par les nœuds voisins jusqu'à atteindre le récepteur. Suivant la technique choisie, on peut se servir de la route déterminée par le premier paquet de supervision qui arrive au récepteur ou prévoir plusieurs routes en cas de problème sur la route principale.

Les protocoles proactifs se comportent totalement différemment. Les paquets de supervision sont émis sans arrêt dans le but de maintenir à jour la table de routage en ajoutant de nouvelles lignes et en supprimant certaines. Les tables de routage sont donc dynamiques et varient en fonction des paquets de supervision parvenant aux différents nœuds. Une difficulté consiste dans ce cas à calculer une table de routage qui soit compatible avec les tables de routage des différents nœuds de telle sorte qu'il n'y ait pas de boucle.

Une autre possibilité consiste à trouver un compromis entre les deux systèmes. Cela revient à calculer régulièrement des tables de routage tant que le réseau est peu chargé.

De la sorte, les performances des flots utilisateur en transit ne sont pas trop modifiées. Lorsque le trafic augmente, les mises à jour sont ralenties. Cette méthode simplifie la mise en place d'une table de routage réactive lorsqu'une demande parvient au réseau.

Les protocoles proposés à la normalisation du groupe MANET sont récapitulés au tableau 21.1. Différentes métriques peuvent être utilisées pour calculer la meilleure route :

- **Les vecteurs de distance** donnent un poids à chaque lien et additionnent les poids pour déterminer la meilleure route, qui correspond à celle du poids le plus faible.
- **Le routage à la source** permet de déterminer la meilleure route comme étant celle qui permet au paquet de supervision d'arriver le premier au destinataire.
- **Les états des liens indiquent** les liens qui sont intéressants à prendre et ceux qui le sont moins.

Métrique	Réactif	Proactif
Vecteur de distance	AODV (Ad-hoc On demand Distance Vector)	DSDV (Destination Sequence Distance Vector)
Routage à la source	DSR (Dynamic Source Routing)	
État du lien		OLSR (Optimized Link State Routing Protocol)

**TABLEAU 21.1 • Protocoles ad-hoc**

### 3. OLSR

Le protocole OLSR (Optimized Link State Routing) est certainement le plus utilisé des protocoles de routage ad-hoc. Il est de type proactif.

Pour éviter de transporter trop de paquets de supervision, OLSR s'appuie sur le concept de relais multipoint, ou MPR (MultiPoint Relay). Les MPR sont des nœuds importants qui ont la particularité d'être les meilleurs points de passage pour atteindre l'ensemble des nœuds lors d'un processus d'inondation sans diffuser tous azimuts. L'état des liens n'étant envoyé que par les MPR, cela réduit d'autant les messages de supervision.

La connaissance de ses voisins est obtenue par les messages Hello qui sont émis en diffusion. Cela permet de déterminer quels sont les voisins et d'envoyer les informations



0										1										2										3				
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0				
Reserved															Htime										Willingness									
Link Code					Reserved										Link Message Size																			
Neighbor Interface Address																																		
Neighbor Interface Address																																		
Link Code					Reserved										Link Message Size																			
Neighbor Interface Address																																		
Neighbor Interface Address																																		

**Figure 21.7**

*Structure du paquet Hello*

Le champ Reserved ne contient que des 0, le champ Htime indique l'intervalle de temps entre Hello, le champ Willingness demande à un nœud de devenir un MPR, le champ Link Code permet de faire passer les informations d'état de lien entre l'émetteur et les récepteurs indiqués dans la liste des « Neighbor Interface Address ».

Les paquets TC (Topology Control) sont émis uniquement par les MPR, avec toujours une adresse de broadcast. L'information émise indique la liste de tous les voisins qui ont choisi ce nœud comme MPR et permet, par la connaissance de tous les MPR et l'état des liens, d'en déduire la table de routage. Ces messages sont diffusés sur tout le réseau avec une valeur de 255 dans le champ TTL. La structure du paquet TC est illustrée à la figure 21.8.

0										1										2										3	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
ANSN															Reserved																
Advertised Neighbor Main Address																															
Advertised Neighbor Main Address																															

**Figure 21.8**

*Structure du paquet TC*

Le champ Reserved est toujours rempli de 0. Le champ ANSN (Advertised Neighbor Sequence Number) transporte un entier incrémenté à chaque changement de topologie.

Cette astuce permet de ne pas prendre en compte des informations qui seraient trop anciennes. Les champs Advertised Neighbor Main Address transportent les adresses IP des nœuds à un saut.

Les paquets MID (Multiple Interface Declaration) sont utilisés lorsque les nœuds ont plusieurs interfaces et qu'il faut signaler l'ensemble des interfaces disponibles.

L'algorithme de sélection des MPR est le suivant. Grâce aux messages Hello, les nœuds peuvent déterminer s'ils sont reliés en full-duplex à leurs voisins. La détermination des MPR ne tient compte que des liens symétriques. Par rapport à un nœud donné, un premier ensemble est déterminé, celui de ses voisins à un saut, l'ensemble A. Pour déterminer les MPR, les messages Hello sont reroutés, ce qui permet de déterminer les nœuds à deux sauts, qui forment un autre ensemble bien déterminé, l'ensemble B. Chaque nœud détermine les liens symétriques avec ses voisins. Pour tous les nœuds de B qui n'ont qu'un et un seul lien symétrique avec un nœud de A, on définit ce nœud de A comme MPR, et on ne tient plus compte des nœuds de B reliés par ce MPR. On réitère le processus jusqu'à ce qu'il n'y ait plus de nœud non relié dans B. Les nœuds MPR sont alors tous déterminés.

#### **4. AODV**

AODV (Ad-hoc On-demand Distance Vector) a été le premier protocole normalisé par le groupe MANET, juste avant OLSR. Il est du type réactif. Ce protocole peut gérer à la fois les routages unicast et multicast.

Lorsqu'un flot de paquets est émis par un nœud, la première action est de déterminer la route par une technique d'inondation. Pour cela, le paquet de requête de connexion mémorise les nœuds traversés lors de la diffusion. Lorsqu'un nœud intermédiaire reçoit une requête de connexion, il vérifie qu'il n'a pas déjà reçu une telle requête. Si la réponse est positive, un message est renvoyé vers l'émetteur pour indiquer l'abandon de cette route.

Le premier message qui arrive au destinataire détermine la route à suivre. La complexité du processus de détermination de la route doit être simplifiée au maximum en évitant les diffusions inutiles. Pour cela, chaque requête de demande d'ouverture d'une route est numérotée, afin d'éviter les duplications, et possède un TTL qui limite le nombre de transmissions dans le réseau.

L'avantage d'AODV est de ne pas créer de trafic lorsqu'il n'y a pas de message à transmettre. La détermination de la route est assez simple et n'implique que peu de calcul dans chaque nœud. Il est évident que les deux inconvénients majeurs résident dans le temps de mise en place de la route et de l'important trafic suscité pour mettre en place les route

### **III. LES RESEAUX MESH**

Les réseaux mesh (meshed networks) sont des réseaux ad-hoc dans lesquels les points de routage sont immobiles. Les clients sont rattachés par un réseau sans fil sur les points d'accès, et les points d'accès sont reliés entre eux par des liaisons sans fil.

L'avantage de ces réseaux est qu'ils peuvent couvrir une zone géographique importante, sans nécessiter de pose de câbles. Par exemple, sur un grand campus, les points d'accès peuvent se mettre sur les toits des différents bâtiments sans que l'architecte du réseau ait à se préoccuper de relier les points d'accès à un système câblé de type Ethernet.

Plusieurs possibilités se font jour pour réaliser un réseau mesh :

- Utiliser la même fréquence que les terminaux, en considérant que les points d'accès sont traités comme des machines terminales. L'inconvénient est bien sûr d'utiliser de la bande passante enlevée aux autres machines terminales. De plus, il faut faire attention que les deux points d'accès ne soient pas trop éloignés et n'obligent l'émetteur et le récepteur à baisser leur vitesse. Cette solution est considérée comme la première génération de réseaux mesh.
- Utiliser des fréquences différentes. Par exemple, un réseau Wi-Fi 802.11b comportant trois fréquences disponibles, il est possible d'utiliser deux cartes de communication avec des fréquences différentes. L'inconvénient est bien sûr de perturber le plan de fréquences, surtout si le réseau est important et possède de nombreux points d'accès. Cette solution fait partie de la seconde génération de réseaux mesh.
- Toujours dans la deuxième génération, le réseau mesh fait appel à une norme différente pour relier les points d'accès entre eux. Par exemple, un réseau mesh 802.11g peut utiliser la norme IEEE 802.11a pour interconnecter les points d'accès.
- On considère que la troisième génération utilise trois fréquences au total. Une pour connecter les clients, et deux pour interconnecter les points d'accès. Dans ce cas, les connexions amont et aval d'un même nœud utilisent des fréquences différentes. Il faut généralement utiliser 802.11a qui possède jusqu'à huit fréquences différentes.

Les réseaux mesh posent des problèmes inédits aux réseaux sans fil, notamment les suivants : comment optimiser les batteries des points d'accès si ceux-ci ne sont pas reliés au courant électrique ? comment optimiser le routage pour ne pas perturber le trafic utilisateur aux points d'accès, surtout s'ils sont déjà saturés ? quelle densité de points d'accès faut-il utiliser, ce qui revient à se poser la question de la puissance des points d'accès ?

L'avantage de cette technologie est d'être capable de se reconfigurer facilement lorsqu'un point d'accès tombe en panne. Les clients peuvent se connecter à un autre point d'accès, quitte à augmenter légèrement la puissance des points d'accès voisins de celui en panne.

Le problème principal est de gérer le routage. Ce dernier est traité dans les points d'accès qui ne sont pas des machines très puissantes, et il faut de ce fait éviter les points d'accès qui supportent beaucoup de trafic provenant des clients raccordés. De nombreuses propositions sont en discussion, en premier lieu celles provenant des réseaux ad-hoc.

Le groupe de travail IEEE 802.11s a également cet objectif. À la suite d'une quinzaine de propositions, le groupe a retenu deux propositions le SEE-Mesh et le Wi-Mesh, qui se sont regroupés pour former une proposition unique. Cette proposition est devenue un standard en avril 2007, après de nombreuses discussions d'implémentation. Les points d'accès et les stations qui possèdent l'algorithme de routage 802.11s sont nommés Mesh Points (MP). Les liaisons radio permettent de les interconnecter. Le protocole par défaut est le HWMP (Hybrid Wireless Mesh Protocol). Ce protocole hybride provient d'une combinaison d'un protocole provenant d'AODV, le RM-AODV (Radio Metric-AODV) et d'un algorithme fondé sur les arbres. Un second protocole peut être utilisé lorsque les MP l'acceptent : le protocole RA-OLSR (Radio Aware-OLSR).

Le groupe IEEE 802.11s définit également des solutions de sécurité pour les réseaux mesh. Pour cela, il faut définir une authentification mutuelle des MP, générer et contrôler les clés de session, permettre le chiffrement des données sur les lignes du réseau ad-hoc et détecter les attaques. Pour cela, il faut effectuer des authentifications avec le protocole IEEE 802.1x que nous détaillons au chapitre 23. Les clés de session sont gérées par une PKI (Public Key Infrastructure), dont nous verrons les détails au chapitre 38, dédié à la sécurité. La confidentialité est assurée par la norme IEEE 802.11i, décrite au chapitre 23.

#### **IV. LES RESEAUX DE CAPTEURS**

Un réseau de capteurs se définit comme un ensemble de capteurs connectés entre eux, chaque capteur étant muni d'un émetteur-récepteur. Les réseaux de capteurs forment une nouvelle génération de réseaux aux propriétés spécifiques, qui n'entrent pas dans le cadre des architectures classiques.

La miniaturisation des capteurs pose des problèmes de communication et de ressources d'énergie. Il faut que le capteur soit suffisamment intelligent pour rassembler l'information requise et l'émettre à bon escient. De plus, le processeur du capteur ne doit pas être utilisé trop intensivement afin de consommer le moins d'énergie possible. Il doit donc incorporer des éléments réactifs plutôt que cognitifs. Enfin, pour assurer un bon débit, la portée des

émetteurs-récepteurs doit être nécessairement faible, de l'ordre d'une dizaine de mètres. La mise en place d'un réseau de capteurs pose donc des problèmes de routage, de contrôle des erreurs et de gestion de l'alimentation.

Du point de vue de la communication, l'environnement des protocoles IP est trop lourd et engendre un débit trop important et une surconsommation. Les solutions qui ont été dérivées des réseaux de terrain, ou réseaux industriels temps réel, présentent un meilleur compromis entre efficacité et énergie consommée. Comme les capteurs peuvent être diffusés par centaine au mètre carré, l'adressage IPv6 semble le plus probable. Dans le futur, il faudra sûrement utiliser un environnement de paquets IP encapsulés dans des trames spécifiques à déterminer. Pour le moment, les problèmes de sécurité et de qualité de service sont mis au second plan par rapport aux problèmes de consommation. Un champ de recherche important est en tout cas ouvert pour rendre les réseaux de capteurs efficaces et résistants.

Les principaux standards radio concernent ZigBee, que nous examinons en détail au chapitre suivant. WiBree et 6LowPAN forment d'autres solutions. Wibree est une technologie très basse consommation d'une portée de 10 m et d'un débit de 1 Mbit/s.

Cette solution a été développée par Nokia pour concurrencer à la fois ZigBee et Bluetooth.

Les réseaux 6LowPAN (IPv6 over Low power Wireless Personal Area Networks) proviennent d'un groupe de travail de l'IETF. L'objectif est clairement de permettre la continuité du protocole IP vers des machines peu puissantes et avec une puissance électrique limitée. L'utilisation de la norme IPv6 pour obtenir un très grand nombre d'adresses pour les immenses réseaux de capteurs pose problème. En effet, les seize octets d'adresse de l'émetteur et les seize octets d'adresse du récepteur plus les champs obligatoires impliquent une mauvaise utilisation de la liaison radio pour transporter ces informations de supervision. Cela devient réellement problématique avec le peu d'énergie du capteur. ZigBee, au contraire, limite la longueur de sa trame à 127 octets, ce qui peut aussi poser des problèmes si l'information à transporter venant d'un capteur est longue. Les réseaux de capteurs forment des réseaux mesh, et il leur faut un protocole de routage.

L'utilisation d'un protocole comme IEEE 802.11s associé à des adresses IPv6 serait catastrophique pour la longévité de la batterie des capteurs. Pour cette raison, les propositions actuelles sont beaucoup plus simples, avec des protocoles comme LOAD (6LowPAN Ad-hoc Routing Protocol), une simplification d'AODV, DyMO-Low (Dynamic MANET On-demand for 6LowPAN), une simplification de DyMO du groupe de travail MANET, et Hi-Low (Hierarchical Routing over 6LowPAN), qui comporte un adressage hiérarchique. Ces

différents protocoles proviennent de proposition de l'IETF et donc de la normalisation des réseaux ad-hoc, mais en ne prenant pas en compte tout ce qui est optionnel.

Une autre caractéristique importante des protocoles des réseaux de capteurs concerne la découverte de service, qui doit permettre la mise en marche du réseau de façon automatique. L'IETF joue également un rôle important dans ce domaine, en proposant plusieurs solutions, dont une orientée vers les capteurs : LowPAN Neighbor Discovery Extension. Ce protocole est une réduction de la norme Neighbor Discovery concernant tous les éléments consommateurs d'énergie, comme les broadcast et la gestion des multicast.

Un réseau de capteurs particulier est proposé par les poussières intelligentes (Smart Dust), dont l'objectif est de développer des capteurs en nanotechnologie et de les relier entre eux par un réseau de type ad-hoc ou mesh. La poussière intelligente tient dans un cube inférieur au millimètre cube, d'où son nom de poussière. Dans cette poussière, se trouvent tous les composants nécessaires pour réaliser un ordinateur communiquant : un processeur, de la mémoire, de la radio, une batterie, etc.

La problématique principale est ici encore la sauvegarde de l'énergie lors de l'exécution des fonctions du capteur. En particulier, la partie réseau doit mener à des communications dépensant très peu d'énergie. L'Université de Berkeley a ainsi conçu un système d'exploitation et des protocoles spécifiques nommés TinyOS et Tiny protocol. Le TinyOS a été écrit dans un langage C simplifié, appelé nesC, qui est une sorte de dialecte destiné à optimiser l'utilisation de la mémoire.

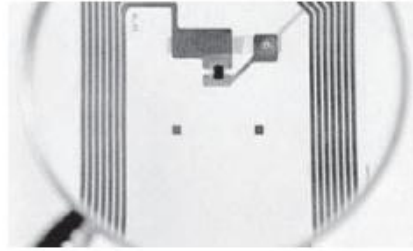
- i. **La RFID** (Radio-Frequency Identification) a été introduite pour réaliser une identification des objets, d'où son autre nom d'étiquette électronique.

Les étiquettes électroniques sont interrogées par un lecteur, qui permet de récupérer l'information d'identification. Les étiquettes électroniques sont utilisées dans de nombreuses applications, allant du suivi d'animaux à des étiquettes pour magasin.

Il existe deux grands types d'étiquettes électroniques : les étiquettes passives et les étiquettes actives. Les étiquettes passives ne possèdent aucune ressource d'énergie. Elles sont allumées par un lecteur qui procure un champ électromagnétique suffisant pour générer un courant électrique permettant l'émission par une onde radio des éléments binaires stockés dans une mémoire EEPROM constituant l'identification RFID. Une étiquette passive est illustrée à la

figure 21.9. L'antenne doit être architecturée de sorte à recevoir le champ électromagnétique du lecteur et émettre son identité.

**Figure 21.9**  
*RFID passif*



Un RFID passif peut être très petit. Les équipements nécessaires étant limités, des tailles d'un dixième de millimètre sur un dixième de millimètre sont suffisantes. Le prix d'une étiquette électronique dépend du nombre d'éléments fabriqués dans une même passe.

Les étiquettes électroniques actives disposent d'une source d'alimentation électrique dans le composant. Le premier avantage très important de ces étiquettes tient à la qualité de la transmission. Une session peut être ouverte entre le lecteur et le RFID de telle sorte qu'une retransmission puisse être réalisée automatiquement en cas de problème. Un autre avantage est la transmission avec une portée de plusieurs mètres entre le RFID et le lecteur, au lieu de quelques centimètres. Un inconvénient pourrait être la durée de vie de la batterie. Cependant, pour une utilisation standard de quelques lectures par jour, il est possible de dépasser la dizaine d'années.

Le RFID actif peut posséder une mémoire plus importante pour le stockage d'attributs associés à la valeur de l'identité.

Un RFID actif est illustré à la figure 21.10.

**Figure 21.10**  
*RFID actif*



## **ii. Utilisation des RFID**

Une application très connue des RFID est le passeport électronique. Le passeport électronique est défini dans le texte ICAO (International Civil Aviation Organization), Document 9303, Part 1, Volumes 1 et 2 (6<sup>e</sup> édition, 2006). Le composant de l'étiquette électronique contient les informations qui sont imprimées sur le passeport lui-même, ainsi qu'une photo numérisée du propriétaire du passeport.

Les titres de transport forment une seconde application des RFID. Par exemple, les tickets du métro parisien contiennent une étiquette électronique qui mémorise un ensemble d'informations comprenant la date et l'endroit de l'achat. Des solutions plus sophistiquées sont mises en œuvre dans les transports publics de Séoul, où l'étiquette devient active et contient de l'argent pour permettre l'utilisation d'un même ticket plusieurs fois.

Des barrières de péage pour autoroute utilisent également cette solution de RFID actif, avec des portées de quelques mètres. L'étiquette active permet de soustraire le prix du péage de la somme d'argent stockée dans la mémoire. De même, des barrières de péage pour des remontées mécaniques dans de nombreuses stations de ski françaises utilisent des RFID actifs.


Une autre application assez immédiate est le suivi des voitures pour détecter les voitures volées lors du passage près d'un lecteur.

Enfin, une des applications les plus connues concerne les inventaires et les achats dans les magasins. Les inventaires peuvent s'effectuer plus souvent et avec moins d'erreurs.

Les achats posés dans un caddy peuvent de la même façon être lus par le lecteur et apporter une grande simplification à la procédure de paiement des achats dans un magasin .

### iii. La technologie RFID

Les fréquences de transmissions du RFID sont indiquées au tableau 21.2. Elles sont déterminées par les organismes de normalisation locaux ou régionaux.



Fréquence pour les RFID	Commentaire
125 kHz (LF)	Première solution permettant une portée relativement importante pour les RFID passifs
13,56 MHz (HF)	Une des fréquences standardisées très utilisée pour les RFID passifs
400 MHz	Quelques utilisations spécifiques, comme la détection des voitures volées
865-868 MHz (UHF)	Bande de fréquences normalisées en Europe pour une utilisation intensive des RFID
902-928 MHz (UHF)	Bande de fréquences normalisée pour l'Amérique du Nord
2,4-2,483 5 GHz	Bande libre ISM dans laquelle devraient se développer de nombreuses applications RFID.

**TABEAU 21.2 • Fréquences de transmission des RFID**



## EPCglobal

Les RFID ont pour objectif de donner l'identité des objets auxquels ils sont adossés. La normalisation de cette identification a été réalisée par le consortium EPCglobal. Deux générations sont disponibles : EPC Gen1 et EPC Gen2. Nous nous intéresserons surtout à cette deuxième génération, sortie mi-2006, qui a permis au RFID de devenir une technique industrielle.

EPC Gen2 est l'acronyme d'EPCglobal UHF Class1 Generation 2. Cette spécification est sortie dans sa version 1.1 en mai 2006. Elle prend en charge le protocole entre le lecteur, d'une part, et le RFID et l'identification, d'autre part. L'objectif du protocole est de lire, écrire et tuer un RFID, de telle sorte que les lecteurs vendus par n'importe quel équipementier soient interchangeables.

La procédure de lecture est définie en utilisant un système à base de tranches temporelles (slots) muni d'un système anticollision. En effet, un lecteur pouvant allumer simultanément un grand nombre de RFID, des lectures simultanées des différentes étiquettes entraîneraient des collisions. Une signalisation permet de définir la fréquence, le codage utilisé (entre DSB-ASK, SSB-ASK et PR-ASK) et le débit du canal. Le système anticollision permet à chaque lecture simultanée que seulement la moitié des objets qui ont pu transmettre puisse transmettre de nouveau dans la lecture suivante. Au bout d'un certain nombre de collisions, un seul RFID transmet avec succès. L'algorithme est conçu de telle sorte que chaque RFID passe ensuite à tour de rôle. La vitesse de lecture peut atteindre 640 Kbit/s.

L'identité de l'objet est déterminée par l'EPCglobal Electronic Product Code. La Gen1 utilise 96 bits tandis que la Gen2 passe à 256 bits de longueur. Un exemple de cette identification pour la Gen1 est illustré à la figure 21.11. La figure 21.12 indique les champs de l'identification dans la Gen2. Cette solution est beaucoup plus complexe, car elle fait appel à des filtres intermédiaires qui déterminent les longueurs des champs suivants. Il est à noter que le numéro de série passe de 36 à 140 bits, ce qui permet, pour un article donné, de ne jamais repasser par la valeur 0.

### **iv. Sécurité des RFID**

La sécurité est un problème épineux dans le monde des RFID. En effet, la lecture d'un RFID passif peut se faire facilement à l'aide d'un lecteur d'une personne tierce. De même, la vie privée peut être mise à mal par le suivi et la traçabilité de tout ce qui concerne un individu.

Des solutions sont disponibles, comme le chiffrement de l'identifiant dans l'étiquette ou le changement de la valeur de l'étiquette après chaque lecture. Ces solutions reposent sur un middleware capable d'interpréter les valeurs des étiquettes ou de suivre les changements de valeur.

Les étiquettes actives peuvent ouvrir une session d'authentification permettant un échange avec le lecteur, qui joue alors le rôle de serveur d'authentification. Il faut dans ce cas un circuit électronique dans l'étiquette capable de chiffrer un texte émis par le serveur d'authentification. Cependant, la longueur des clés est si faible que la possibilité de les casser après une suite de tentatives d'authentification n'est pas négligeable. De nombreuses propositions ont été effectuées en utilisant l'algorithme anticollision, qui permet de sérialiser la lecture des étiquettes, pour l'authentification.

## **Conclusion**

Les réseaux sans fil sont devenus un marché porteur au XXI<sup>e</sup> siècle. Les terminaux téléphoniques mobiles ont été les grands gagnants de la fin du XX<sup>e</sup>, mais ils ne sont dévolus qu'aux communications téléphoniques. Les tentatives d'introduire les données par le biais du WAP (Wireless Application Protocol) ont été un échec, essentiellement du fait des médiocres débits offerts par les réseaux de mobiles. Le GPRS apporte un peu plus de débit mais plafonne à 40 Kbit/s. L'UMTS devrait encore augmenter le débit pour les données mais part avec beaucoup de retard sur les réseaux sans fil. En effet, les réseaux sans fil apportent des débits élevés, qui permettent à un PC ou à un PDA de se connecter sans se soucier du câblage et même de se déplacer lentement, à condition de ne pas sortir de sa cellule. La diffusion massive de stations de travail de poche, telles que Pocket PC, d'une puissance comparable aux PC de bureau, va démultiplier le développement de ces réseaux sans fil, qui se présenteront comme l'entrée du réseau Internet. On donne parfois à un tel réseau, auquel on peut accéder de partout, à tout moment et à haut débit, le nom d'Internet ambiant.

Dans un avenir proche, le changement intercellulaire sera possible dans les réseaux sans fil, permettant un déplacement plus important de l'équipement mobile. De surcroît, la téléphonie ne deviendra qu'une application particulière de cette nouvelle génération. On peut donc s'attendre à une diversification des stations terminales de poche capables de se connecter à des réseaux Internet ambiants disponibles dans tous les lieux de passage fréquentés, comme le cœur des villes, les gares, les aéroports, le métro, etc.

Les réseaux de mobiles ont cependant une sérieuse carte à jouer avec la gamme UMTS

–HSDPA, HSUPA et HSOPA –, qui permet de concurrencer les réseaux sans fil avec des débits similaires. La qualité des équipements, la sécurité et les prix devraient départager ces deux grandes solutions que sont les réseaux de mobiles et les réseaux sans fil, avec plus certainement un partage du marché.