21

Les réseaux sans fil

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 mégabits par seconde, voire 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.

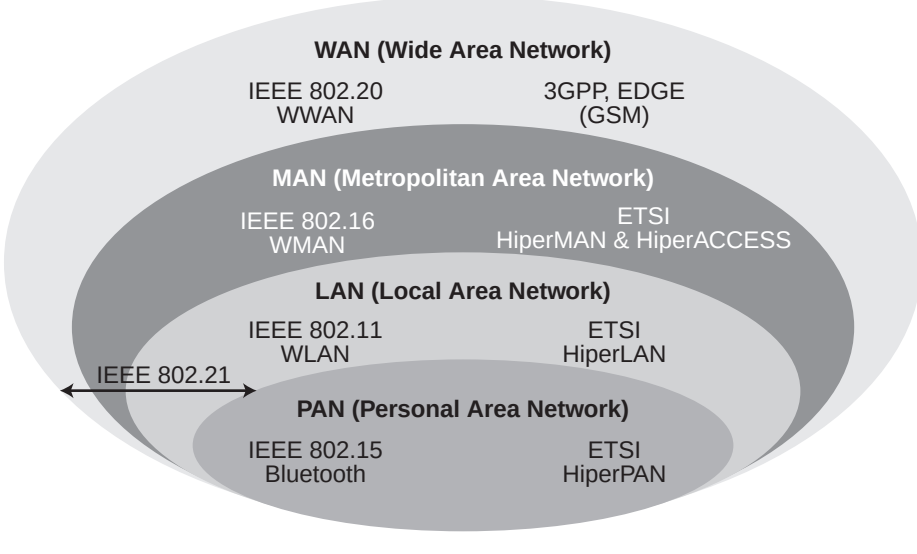


Figure 21.1

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, et IEEE 802.20, pour les réseaux WWAN (Wireless Wide Area Network), c'est-à-dire les très grands réseaux.

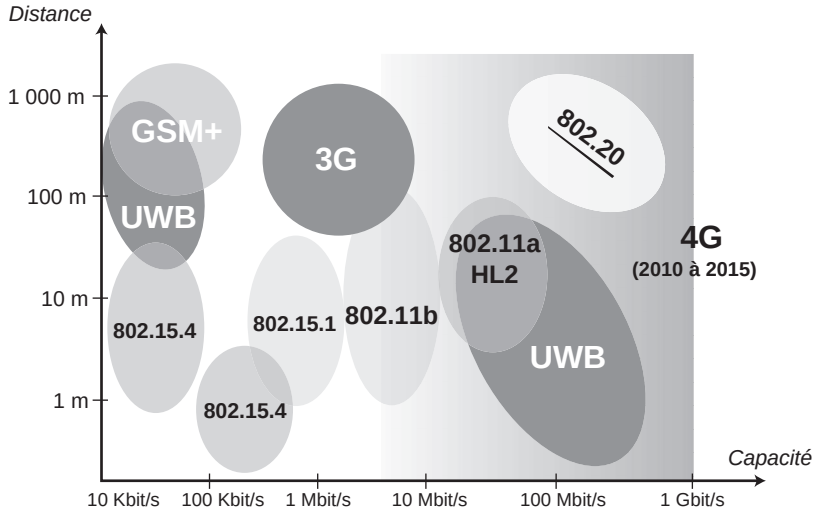


Figure 21.2

Principales normes des réseaux sans fil

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

- IEEE 802.15.1, le plus connu, prend en charge la norme Bluetooth, aujourd'hui largement commercialisée.
- 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). Les débits atteints sont de l'ordre du gigabit par seconde sur une distance de 10 mètres.
- 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.

Le groupe de travail HiperPAN de l'ETSI n'est pas assez avancé pour qu'on ait une idée précise de ce qui en sortira.

Du côté de la norme IEEE 802.11, dont les produits sont nommés Wi-Fi (Wireless-Fidelity), 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, devrait bientôt augmenter le débit, qui pourrait atteindre 320 Mbit/s. Les fréquences utilisées se placent dans la bande 2,4-2,483 5 MHz pour les extensions b et g et dans la bande 5,15-5,3 MHz pour 802.11a.

Pour HiperLAN (High Performance Local Area Network), les bandes de fréquences retenues se situent entre 5 150 et 5 300 MHz, auxquelles il faut ajouter une bande de 200 MHz dans les fréquences autour de 17 GHz. Les vitesses de transfert, qui atteignent une cinquantaine de mégabits par seconde, pourraient concurrencer le marché des réseaux locaux filaires les plus rapides du marché. La distance entre postes de travail et stations de base va de quelques dizaines de mètres jusqu'à une centaine de mètres.

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 importants pour du hertzien, 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. Les prochaines années devraient apporter la possibilité de se connecter de l'antenne de l'opérateur à des terminaux mobiles et non plus seulement à des fixes comme aujourd'hui, ce qui permettrait l'arrivée de jonctions ADSL vers les mobiles.

Les réseaux à grande étendue se sont principalement développés sous l'égide d'organismes internationaux tels que l'UIT. Les principaux standards sont le GSM, le GPRS, Edge, l'UMTS et le cdma2000. La norme concurrente provenant de l'IEEE est IEEE 802.20, ou MBWA (Mobile Broadband Wireless Access), dont l'objectif est de concurrencer les standards des opérateurs de téléphonie mobile par un coût très avantageux. Le nom commercial des produits provenant de cette norme sera Wi-Mobile.

WPAN et IEEE 802.15

Le groupe IEEE 802.15 a été mis en place en mars 1999 dans le but de réfléchir aux réseaux hertziens d'une portée d'une dizaine de mètres, ou WPAN (Wireless Personal Area Network), avec pour objectif de réaliser des connexions entre les différents portables d'un même utilisateur ou de plusieurs utilisateurs. Ce réseau peut interconnecter un PC portable (laptop), un téléphone portable, un PDA ou tout autre terminal de ce type. Trois groupes de services ont été définis, A, B et C.

Le groupe A utilise la bande du spectre sans licence d'utilisation (2,4 GHz) en visant un faible coût de mise en place et d'utilisation. La taille de la cellule autour du point d'émission est de l'ordre du mètre. La consommation électrique doit être particulièrement faible pour permettre au terminal de tenir plusieurs mois sans recharge électrique. Le mode de transmission choisi est sans connexion. Le réseau doit pouvoir travailler en parallèle d'un réseau IEEE 802.11. Sur un même emplacement physique, il peut donc y avoir en même temps un réseau de chaque type, les deux pouvant fonctionner, éventuellement de façon dégradée.

Le groupe B affiche des performances en augmentation, avec un niveau MAC pouvant atteindre un débit de 100 Kbit/s. Le réseau de base doit pouvoir interconnecter au moins seize machines et proposer un algorithme de QoS, ou qualité de service, pour autoriser le fonctionnement de certaines applications, comme la parole téléphonique, qui demande une qualité de service assez stricte. La portée entre l'émetteur et le récepteur atteint une dizaine de mètres, et le temps maximal pour se raccorder au réseau ne doit pas dépasser la seconde. Enfin, cette catégorie de réseau doit posséder des passerelles avec les autres catégories de réseaux 802.15.

Le groupe C introduit de nouvelles fonctionnalités importantes pour particuliers ou entreprises, comme la sécurité de la communication, la transmission de la vidéo et la possibilité de roaming, ou itinérance, entre réseaux hertziens.

Pour répondre à ces objectifs, des groupements industriels se sont mis en place, comme Bluetooth ou HomeRF. Bluetooth regroupe plus de 800 sociétés qui ont réalisé une spécification ouverte de connexion sans fil entre équipements personnels. Bluetooth est fondé sur une liaison radio entre deux équipements, tandis que HomeRF s'intéresse à la connexion des PC avec toutes les machines domestiques sur une portée de 50 m.

Le groupe de travail IEEE 802.15 s'est scindé en quatre sous-groupes :

- IEEE 802.15.1, pour les réseaux de catégorie C ;
- IEEE 802.15.3 pour les réseaux de catégorie B ;
- IEEE 802.15.4 pour les réseaux de catégorie A ;
- IEEE 802.15.2 pour s'occuper des problèmes d'interférences avec les autres réseaux utilisant la bande des 2,4 GHz.

Le choix du premier groupe, le plus avancé, s'est tourné vers Bluetooth, présenté en détail à la section suivante. Le second réseau intéressant est celui du groupe 802.15.4, qui a défini un réseau à très faible portée, de l'ordre du mètre, pour interconnecter tous les capteurs et actionneurs que l'on peut trouver un peu partout, dans les jouets par exemple.

Bluetooth

Le Bluetooth Special Interest Group, constitué au départ par Ericsson, IBM, Intel, Nokia, et Toshiba et rejoint par plus de 2 500 sociétés, définit les spécifications de Bluetooth.

C'est une technologie peu onéreuse, grâce à sa forte intégration sur une puce unique de 9 mm sur 9 mm. Les fréquences utilisées sont comprises entre 2 400 et 2 483,5 MHz. On retrouve la même gamme de fréquences dans la plupart des réseaux sans fil utilisés dans un environnement privé, que ce dernier soit personnel ou d'entreprise. Cette bande ne demande pas de licence d'exploitation.

Schémas de connexion

Plusieurs schémas de connexion ont été définis par les normalisateurs. Le premier d'entre eux correspond à un réseau unique, appelé piconet, qui peut prendre en charge jusqu'à huit terminaux, avec un maître et huit esclaves. Le terminal maître gère les communications avec les différents esclaves. La communication entre deux terminaux esclaves transite obligatoirement par le terminal maître. Dans un même piconet, tous les terminaux utilisent la même séquence de saut de fréquence.

Un autre schéma de communication consiste à interconnecter des piconets pour former un scatternet, d'après le mot anglais *scatter*, dispersion. Comme les communications se font toujours sous la forme maître-esclave, le maître d'un piconet peut devenir l'esclave du maître d'un autre piconet. De son côté, un esclave peut être l'esclave de plusieurs maîtres. Un esclave peut se détacher provisoirement d'un maître pour se raccrocher à un autre piconet puis revenir vers le premier maître, une fois sa communication terminée avec le second.

La figure 21.3 illustre des connexions de terminaux Bluetooth dans lesquelles un maître d'un piconet est esclave du maître d'un autre piconet et un esclave est esclave de deux maîtres. Globalement, trois piconets sont interconnectés par un maître pour former un scatternet.

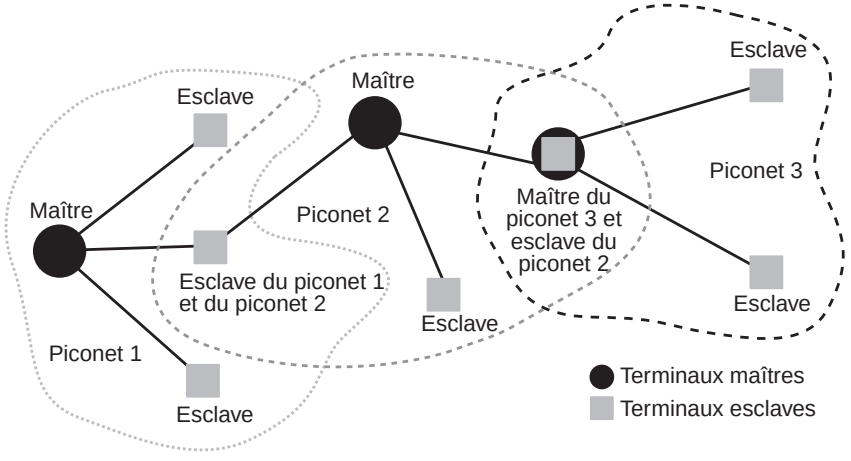


Figure 21.3
Schéma de connexion de terminaux Bluetooth

La communication à l'intérieur d'un piconet peut atteindre près de 1 Mbit/s. Comme il peut y avoir jusqu'à huit terminaux, la vitesse effective diminue rapidement en fonction du nombre de terminaux connectés dans une même picocellule. Un maître peut cependant accélérer sa communication en travaillant avec deux esclaves en utilisant des fréquences différentes.

Les communications

La communication sur une liaison Bluetooth entre deux machines peut atteindre un débit de 433,9 Kbit/s dans une communication bidirectionnelle (full-duplex). Les débits sont égaux à 723,2 Kbit/s dans un sens et 57,6 Kbit/s dans l'autre en cas de communication déséquilibrée.

Les communications peuvent être de deux types : asynchrone ou synchrone. Une communication synchrone, ou SCO (Synchronous Connection-Oriented link), permet un débit synchrone de 64 Kbit/s. Ce type de connexion autorise le passage de la parole téléphonique avec une garantie de service. Une communication asynchrone, ou ACL (Asynchronous Connectionless Link), permet des trafics asynchrones avec plus ou moins de protection. Le débit peut atteindre 723,2 Kbit/s.

Plusieurs catégories de communications peuvent être définies sur une connexion Bluetooth : une seule communication asynchrone, trois communications simultanées en SCO ou une SCO avec une ACL symétrique de 433,9 Kbit/s. Cela donne un débit total de la liaison de presque 1 Mbit/s dans le dernier cas. Un terminal esclave ne peut prendre en charge, au maximum, que deux canaux SCO provenant de deux terminaux distincts.

De façon plus précise, le temps est découpé en tranches, ou slots, à raison de 1 600 slots par seconde. Un slot fait donc 625 µs de long, comme illustré à la figure 21.4. Un terminal utilise une fréquence sur un slot puis, par un saut de fréquence (Frequency Hop), il change de fréquence sur la tranche de temps suivante, et ainsi de suite.

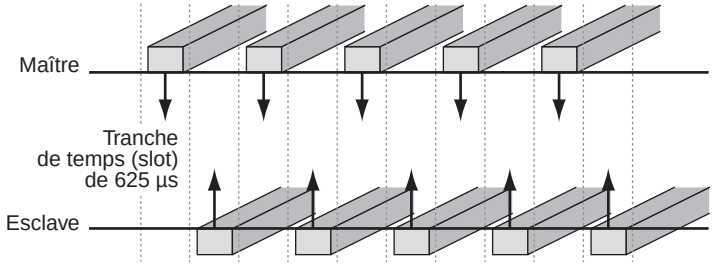


Figure 21.4
Découpage en slots

Un client Bluetooth utilise de façon cyclique toutes les bandes de fréquences. Les clients d'un même piconet possèdent la même suite de sauts de fréquence, et, lorsqu'un nouveau terminal veut se connecter, il doit commencer par reconnaître l'ensemble des sauts de fréquence pour pouvoir les respecter. Une communication s'exerce par paquet. En règle générale, un paquet tient sur un slot, mais il peut s'étendre sur trois ou cinq slots *(voir figure 21.5)*. Le saut de fréquence à lieu à la fin de la communication d'un paquet.

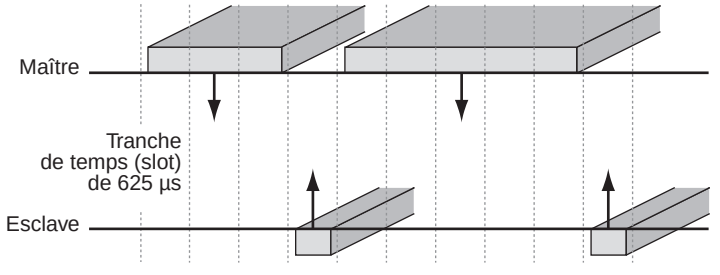


Figure 21.5
Transmission sur plusieurs slots

Fonctionnement de Bluetooth

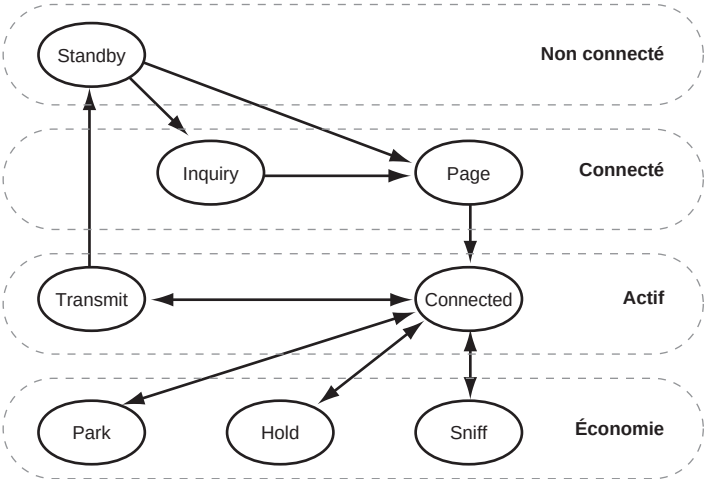
Comme indiqué précédemment, Bluetooth permet la réalisation de petits réseaux personnels de quelques mètres carrés, les piconets. Les terminaux se connectent entre eux par l'intermédiaire d'un maître. La puissance de transmission peut atteindre 100 mW (milliwatt), ce qui permet une émission sur plusieurs dizaines de mètres. Il est possible de réduire cette puissance à 2,5 et 1 mW pour atteindre une portée de quelques mètres.

À une puissance de 100 mW, une batterie peut tenir assez longtemps, à condition d'utiliser des options d'économie d'énergie. Pour cette raison, des états de basse consommation ont été introduits dans la norme Bluetooth, qui autorisent une autonomie de plusieurs jours.

États des terminaux Bluetooth

Les terminaux Bluetooth autorisent des états spécifiques permettant au terminal de dépenser moins d'énergie et donc de prolonger la durée d'utilisation de la batterie. La figure 21.6 illustre les états possibles d'un terminal Bluetooth.

Figure 21.6
États d'un terminal Bluetooth



Dans l'état parqué (Park), le terminal ne peut ni recevoir ni émettre. Il peut seulement se réveiller de temps en temps pour consulter les messages émis par le maître. Utilisant le minimum d'énergie, il n'est pas comptabilisé dans une picocellule et peut donc être remplacé par un autre terminal dans les sept connexions que peut recevoir un maître.

L'état suspendu (Hold) indique que le terminal ne peut que recevoir des communications synchrones de type SCO. Le terminal se met en veille entre les instants synchrones de réception des paquets. L'état de repos actif (Sniff) permet au terminal de décider des slots pendant lesquels il travaille et de ceux pendant lesquels il se met à l'état de repos.

Dans un état de marche normal, le terminal maître doit être dans l'état Inquiry et l'esclave dans l'état Inquiry Scan. Le maître émet une signalisation pour initialiser la communication. Dans ce cas, si l'esclave reçoit les messages, il passe dans un état Inquiry Response, qui lui permet d'envoyer un message au maître lui précisant son adresse et l'état de son horloge. Il passe ensuite dans un nouvel état, Page Scan, dans lequel il attend de recevoir un paquet contenant son adresse sur l'une des neuf fréquences disponibles.

À réception du message, le maître passe à l'état Page, dans lequel il met à jour ses tables de connexion puis envoie un message vers l'esclave. Lorsque l'esclave détecte ce message, il se place dans l'état Slave Response puis répond au maître en indiquant son code d'accès. Le maître se met alors dans l'état Master Response et envoie un paquet Frequency Hopping Synchronization, qui permet à l'esclave de se synchroniser sur l'horloge du maître, puis passe à l'état connecté (Connected). De même, lorsque l'esclave reçoit ce message, il passe à l'état connecté (Connected). Le maître n'a plus qu'à effectuer une interrogation, ou polling, vers l'esclave pour vérifier qu'il y a bien eu connexion.

Techniques d'accès

Bluetooth met en œuvre une technique temporelle synchronisée dans laquelle le temps est divisé en tranches de longueur égale, appelées slots. Un slot correspond au temps élémentaire de transmission d'un paquet. Un paquet peut demander un temps de transmission plus ou moins long, qui ne peut pas accéder cinq slots.

Le format standard d'un paquet Bluetooth est illustré à la figure 21.7.

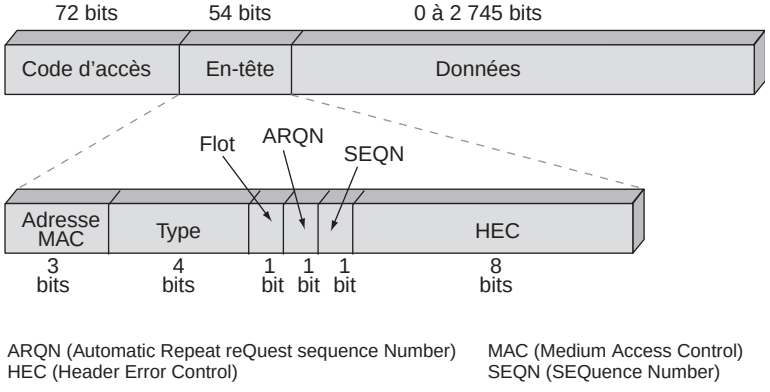


Figure 21.7
Format d'un paquet Bluetooth

Les 72 premiers bits du paquet permettent de transporter le code d'accès tout en effectuant une synchronisation entre les composants Bluetooth. Cette zone se compose de 4 bits, de préambule 0101 ou 1010, permettant de détecter le début de la trame, puis de 64 ou 68 bits pour le code et enfin de 4 bits de terminaison — lorsque le corps fait 64 bits — permettant de détecter la fin de la synchronisation en utilisant les séries 0101 ou 1010. Les 54 bits suivants consistent en trois fois une même séquence de six champs de longueur 3, 4, 1, 1, 1 et 8 bits. Ces champs servent à indiquer l'adresse d'un membre actif du piconet, ainsi qu'un numéro de code, un contrôle de flux piconet, une demande d'acquittement et un contrôle d'erreur des transmissions. Le champ de 18 bits est répété trois fois de suite pour s'assurer de sa réception correcte au récepteur. La zone de données qui s'étend ensuite de 0 à 2 745 bits contient une zone de détection d'erreur sur un ou deux octets.

Trois grands types de paquets sont définis dans Bluetooth, les paquets de contrôle, les paquets SCO et les paquets ACL. Les paquets de contrôle permettent de gérer les connexions des terminaux Bluetooth entre eux. Les paquets SCO correspondent aux communications synchrones de type SCO, et les paquets ACL aux transferts de données asynchrones.

Dans chacun de ces types de paquets, plusieurs sous-catégories peuvent être distinguées :

- Les paquets DV (Data-Voice), qui portent à la fois des données et de la parole.
- Les paquets DMx (Data-Medium) pour les paquets ACL en mode asynchrone avec un encodage permettant la correction des erreurs en ligne. La valeur *x*, qui vaut 1, 3 ou 5, indique la longueur du paquet en nombre de slots.

- Les paquets DHx (Data-High) pour les paquets ACL en mode asynchrone mais sans correction d'erreur, permettant ainsi un débit effectif plus élevé. De même que précédemment, *x* indique la longueur du paquet.
- Les paquets HVy (High-quality-Voice) pour les paquets SCO en mode synchrone sans correction d'erreur. La valeur *y* indique le type de contrôle d'erreur dans le paquet. Si *y* = 1, un FEC (Forward Error Correction) de 1/3 est utilisé. Dans ce cas, le corps du paquet contient une redondance par l'émission de trois fois la même information. Si *y* = 2, un FEC de 2/3 est utilisé. Dans ce cas, on transforme à l'aide d'un code la suite d'éléments binaires à transmettre de façon à détecter et corriger les erreurs. Si *y* = 3, aucune protection n'est utilisée.

Sécurité et fonctions de gestion

Trois niveaux de sécurité ont été définis dans Bluetooth. Le premier niveau n'a pas de gestion de sécurité. Le deuxième niveau instaure une sécurité à l'échelon applicatif en introduisant un processus d'identification lors de l'accès au service. Le troisième niveau introduit une sécurité plus importante en travaillant sur la liaison Bluetooth. Un processus d'authentification est mis en place, qui peut être suivi par un chiffrement à l'aide de clés privées pouvant atteindre 64 bits — la norme cite 128 bits comme future extension.

La sécurité est un élément important dans les systèmes de liaison radio puisque l'émission est diffusée et peut potentiellement être captée par les récepteurs environnants. Dans Bluetooth, deux équipements, par exemple deux PDA situés dans les poches de deux utilisateurs du métro, pourraient très bien entrer en communication par hasard. Pour éviter cela, Bluetooth offre des mécanismes d'authentification et de chiffrement au niveau MAC.

La principale technique d'authentification provient d'un programme automatique mis en place dans les terminaux Bluetooth, qui permet l'authentification et le chiffrement par une génération de clés par session. Chaque connexion peut utiliser ou non le mécanisme de chiffrement dans un sens seulement ou dans les deux sens simultanément. Seules des clés de 40 ou 64 bits peuvent être utilisées, ce qui confère une sécurité relativement faible, quoique suffisante pour le type de communication transitant entre deux terminaux Bluetooth. Si une sécurité supplémentaire doit être obtenue, il est nécessaire d'utiliser un chiffrement au niveau de l'application.

L'algorithme de sécurité utilise le numéro d'identité du terminal, ainsi qu'une clé privée et un générateur aléatoire interne à la puce Bluetooth. Pour chaque transaction, un nouveau numéro aléatoire est tiré pour chiffrer les données à transmettre. La gestion des clés est prise en charge par l'utilisateur sur les terminaux qui doivent s'interconnecter.

En utilisant le même procédé pour réaliser le chiffrement dans un scatternet, il est nécessaire de procéder, au début de la mise en relation, à un échange de clés privées entre les possesseurs de piconets indépendants.

Dans un piconet, un système de gestion est nécessaire pour réaliser les fonctions classiques de mise en œuvre des communications. Le processus de gestion des liaisons prend en charge les procédures classiques d'identification ainsi que la négociation des paramètres d'authentification. Il prend également à sa charge la configuration de la liaison, c'est-à-dire la définition des paramètres de fonctionnement. Ce processus de gestion s'effectue par un échange de requêtes-réponses entre les deux extrémités de la liaison.

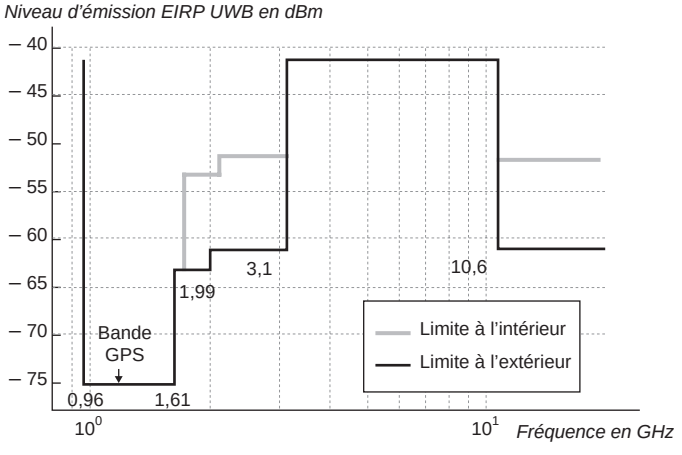
Les réseaux WiMedia, UWB et WUSB

WiMedia est une initiative visant à réaliser un environnement sans fil à très haut débit (480 Mbit/s) pour un réseau personnel. L'objectif est d'éliminer tous les fils connectant les équipements vidéo, audio et de données que l'on peut rencontrer dans un bureau ou un salon. Cette solution prend comme base la normalisation des réseaux personnels de l'IEEE, et plus particulièrement d'IEEE 802.15.3 UWB.

Une solution matérielle sera apportée par l'interface WUSB (Wireless USB), dont l'objectif est de remplacer les interfaces métalliques USB 2 par une interface sans fil à la même vitesse de 480 Mbit/s.

Dans le groupe de travail IEEE 802.15.3, deux solutions ont été développées, une sur la bande classique des 2,4 GHz, qui atteindra une vitesse de 54 Mbit/s effective, et une qui utilise l'ensemble de la bande passante entre 3,1 et 10,7 GHz, mais à une puissance très faible, en dessous du bruit ambiant. De la sorte, cette solution ne gênera pas les applications civiles et militaires utilisant ces bandes. Le spectre visé par cette technologie est illustré à la figure 21.8.

Figure 21.8
Partie du spectre pouvant être utilisée par l'UWB



En dépit de la très faible puissance utilisée, la bande passante de plus de 7 GHz permet d'obtenir une vitesse située entre 110 et 480 Mbit/s en fonction des perturbations externes. Si l'UWB ne perturbe pas les autres applications, les autres applications peuvent en effet perturber le réseau personnel.

Une des propriétés de l'UWB est de pouvoir prendre en charge des communications avec des équipements qui se déplacent à relativement faible vitesse. L'objectif est de connecter et déconnecter ces équipements en des temps extrêmement courts, de l'ordre de la seconde.

La topologie du réseau UWB est en tout point similaire à celle des réseaux Bluetooth, avec des piconets et des scatternets. Les connexions et déconnexions d'une machine à l'intérieur d'un piconet ou d'un piconet à l'intérieur d'un scatternet proviendront essentiellement du déplacement des machines terminales.

Les réseaux UWB pourront fonctionner en mode ad-hoc, et une qualité de service sera assurée par une utilisation simple d'une technique TDMA par découpage dans le temps et l'utilisation de slots déterministes pour les différentes connexions simultanées.

Plusieurs niveaux de gestion de l'alimentation seront également disponibles sur l'interface UWB.

La figure 21.9 illustre différents appareils susceptibles de faire partie d'un réseau UWB.

Figure 21.9
Réseau UWB

L'initiative WiMedia prend en compte plus de couches protocolaires que la simple interface physique. Au-dessus de la couche de communication, deux grandes fonctionnalités devraient être disponibles, l'une concernant la définition de profils applicatifs, comme les applications de streaming, d'imprimante, etc., l'autre pour la découverte de service.

Les réseaux UWB ont de nombreuses propriétés intéressantes, qui déboucheront sur des produits nouveaux. Tout d'abord la faible complexité du système et sa très faible consommation en font un produit bon marché pour communiquer à haut débit. La plupart des cartes mères des ordinateurs personnels devraient, par exemple, embarquer un composant WUSB (Wireless USB), qui n'est autre qu'un réseau UWB.

La sécurité des communications est assurée par une authentification et un chiffrement de l'information. L'authentification utilisera sûrement le protocole EAP-TLS (Extensible Authentication Protocol-Transport Layer Security), que nous examinons plus en détail à la section dédiée à la sécurité. L'utilisation de l'algorithme AES (Advanced Encryption Standard) avec une clé de 128 bits doit garantir la sécurité du transport de l'information.

Étant donné les très hauts débits disponibles, la qualité de service est assurée de façon très simple par un multiplexage temporel du support physique entre les différentes machines qui communiquent.

En conclusion, les réseaux UWB ont un avenir assuré permettant le remplacement des câbles par des connexions hertziennes.

Les réseaux ZigBee

Les réseaux ZigBee sont l'inverse des réseaux UWB. Leur objectif est de consommer extrêmement peu d'énergie, de telle sorte qu'une petite batterie puisse tenir presque toute la durée de vie de l'interface, mais avec une vitesse extrêmement faible.

Deux types de transfert sont privilégiés dans ZigBee : la signalisation et la transmission de données basse vitesse. La figure 21.10 illustre un environnement ZigBee pour la domotique.

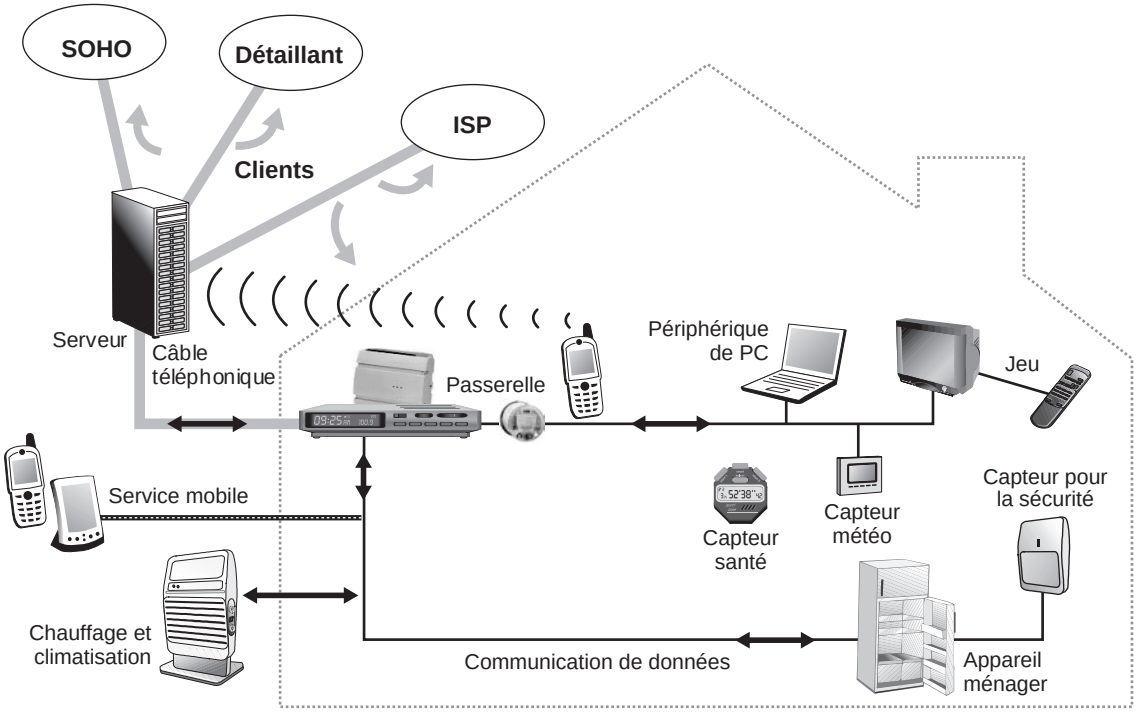


Figure 21.10
Réseau ZigBee

Dans la normalisation, ZigBee peut avoir trois vitesses possibles :

- 250 Kbit/s avec la bande classique des 2,4 GHz ;
- 20 Kbit/s avec la bande des 868 MHz disponible en Europe ;
- 40 Kbit/s avec la bande des 915 MHz disponible en Amérique du Nord.

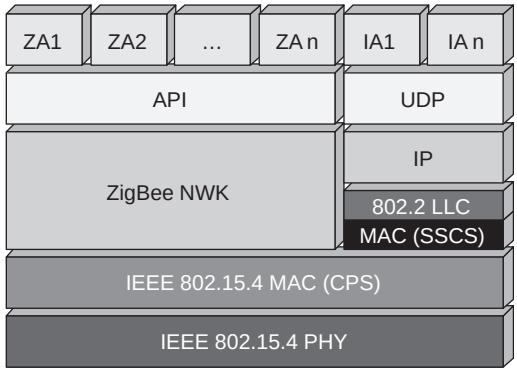
Ces différentes possibilités sont illustrées à la figure 21.11.

Figure 21.11
Bandes de fréquence et débits de ZigBee

	Bande	Couverture	Débit données	Numéro de canal
2,4 GHz	ISM	Mondiale	250 Kbit/s	16
868 MHz		Europe	20 Kbit/s	1
915 MHz	ISM	Amerique	40 Kbit/s	10

Les réseaux ZigBee devraient arriver en force sur le marché de la commande et des bas débits dans les domaines de la domotique, de la bureautique et de l'automatisme.

Figure 21.12
Architecture d'un réseau ZigBee



ZA (ZigBee Application)
IA (Industrial Application)
NWK (Network Wireless Key)
LLC (Logical Link Control)
SSCS (Service Specific Convergence Sublayer)
CPS (Common Part Sublayer)

Comme illustré à la figure 21.12, l'architecture d'un réseau ZigBee contient cinq grandes couches. En partant du sommet, on trouve la couche applicative, qui utilise des profils applicatifs prédéterminés. La couche sous-jacente correspond à l'interface applicative ou au protocole UDP si l'application est à distance. Puis nous trouvons la couche ZigBee proprement dite, qui gère la topologie, le routage, la découverte de protocole et la sécurité. En dessous se trouvent la couche MAC et la couche physique.

Les réseaux Wi-Fi

La norme IEEE 802.11 a donné lieu à deux types de réseaux sans fil, ceux qui travaillent à la vitesse de 11 Mbit/s et ceux qui montent à 54 Mbit/s. Les premiers se fondent sur la norme IEEE 802.11b et les seconds sur les normes IEEE 802.11a et g.

Pour le premier type, les fréquences choisies se situent dans la gamme des 2,4 GHz. Dans cette solution de réseau local par voie hertzienne, les communications peuvent se faire soit directement de station à station, mais sans qu'une station puisse relayer les paquets vers une autre station terminale, soit en passant par une borne de concentration, que l'on appelle point d'accès, ou AP (Access Point).

L'accès au support physique s'effectue par le biais du protocole MAC, interne au niveau MAC, pour tous les types de réseau Wi-Fi. De nombreuses options rendent toutefois sa mise en œuvre assez complexe. Le protocole MAC se fonde sur la technique d'accès CSMA/CD, déjà utilisée dans les réseaux Ethernet métalliques. La différence entre le protocole hertzien et le protocole terrestre provient de la façon de détecter les collisions. Dans la version terrestre, on détecte les collisions en écoutant la porteuse. Lorsque deux stations veulent émettre pendant qu'une troisième est en train de transmettre sa trame, cela mène automatiquement à une collision *(voir le chapitre 16)*. Dans le cas hertzien, le protocole d'accès permet d'éviter la collision en obligeant les deux stations à attendre un temps différent avant de transmettre. Comme la différence entre les deux temps d'attente

est supérieure au temps de propagation sur le support de transmission, la station qui a le temps d'attente le plus long trouve le support physique déjà occupé et évite ainsi la collision. Cette nouvelle technique s'appelle le CSMA/CA (Collision Avoidance).

Comme nous venons de le voir, pour éviter les collisions, chaque station possède un temporisateur avec une valeur spécifique. Lorsqu'une station écoute la porteuse et que le canal est vide, elle transmet. Le risque qu'une collision se produise est extrêmement faible, puisque la probabilité que deux stations démarrent leur émission dans une même microseconde est quasiment nulle. En revanche, lorsqu'une transmission a lieu et que d'autres stations se mettent à l'écoute et persistent à écouter, la collision devient inévitable. Pour empêcher la collision, il faut que les stations attendent avant de transmettre un temps permettant de séparer leurs instants d'émission respectifs. On ajoute pour cela un premier temporisateur très petit, qui permet au récepteur d'envoyer immédiatement un acquittement. Un deuxième temporisateur permet de donner une forte priorité à une application temps réel. Enfin, le temporisateur le plus long, dévolu aux paquets asynchrones, détermine l'instant d'émission pour les trames asynchrones.

La norme IEEE 802.11

Les réseaux Wi-Fi proviennent de la norme IEEE 802.11, qui définit une architecture cellulaire. Un groupe de terminaux munis d'une carte d'interface réseau 802.11 s'associent pour établir des communications directes. Elles forment alors un BSS (Basic Service Set), à ne pas confondre avec le BSS (Base Station Subsystem) des réseaux GSM. La zone occupée par les terminaux d'un BSS peut être une BSA (Basic Set Area) ou une cellule.

Comme illustré à la figure 21.13, la norme 802.11 offre deux modes de fonctionnement, le mode infrastructure et le mode ad-hoc. Le mode infrastructure est défini pour fournir aux différentes stations des services spécifiques, sur une zone de couverture déterminée par la taille du réseau. Les réseaux d'infrastructure sont établis en utilisant des points d'accès, qui jouent le rôle de station de base pour un BSS.

Lorsque le réseau est composé de plusieurs BSS, chacun d'eux est relié à un système de distribution, ou DS (Distribution System), par l'intermédiaire de leur point d'accès (AP) respectif. Un système de distribution correspond en règle générale à un réseau Ethernet filaire. Un groupe de BSS interconnectés par un système de distribution forme un ESS (Extented Service Set), qui n'est pas très différent d'un sous-système radio de réseau de mobiles.

Le système de distribution est responsable du transfert des paquets entre différents BSS d'un même ESS. Dans les spécifications du standard, il est implémenté de manière indépendante de la structure hertzienne de la partie sans fil. C'est la raison pour laquelle le système de distribution correspond presque toujours à un réseau Ethernet mais rien n'empêcherait d'utiliser un réseau Token-Ring ou FDDI. Une autre solution est d'utiliser le réseau Wi-Fi lui-même, ce qui donne les « meshed network », ou réseaux mesh, que nous étudions en fin de chapitre.

L'ESS peut fournir aux différentes stations mobiles une passerelle d'accès vers un réseau fixe, tel qu'Internet. Cette passerelle permet de connecter le réseau 802.11 à un autre réseau. Si ce réseau est de type IEEE 802.x, la passerelle incorpore des fonctions similaires à celles d'un pont.

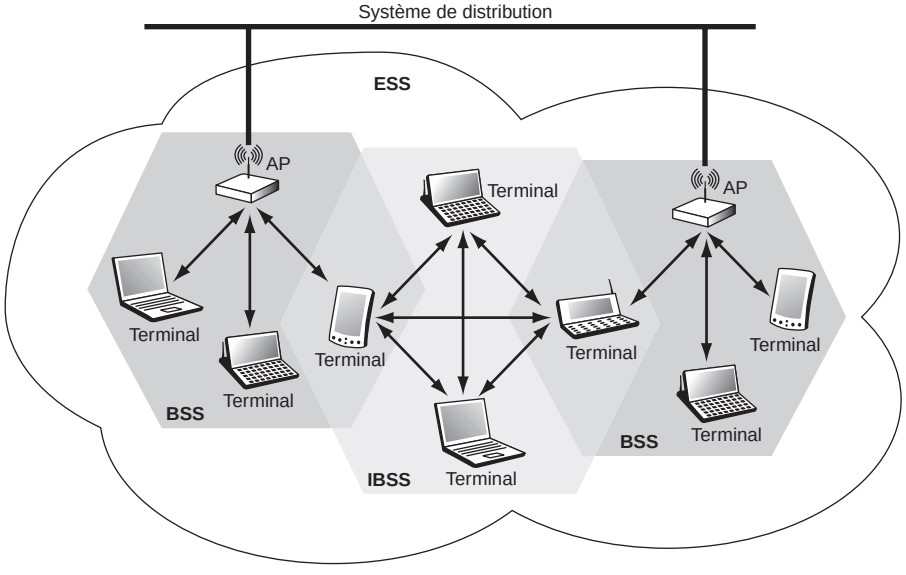


Figure 21.13
Architecture d'un réseau Wi-Fi

Un réseau en mode ad-hoc est un groupe de terminaux formant un IBSS (Independent Basic Service Set), dont le rôle consiste à permettre aux stations de communiquer sans l'aide d'une quelconque infrastructure, telle qu'un point d'accès ou une connexion au système de distribution. Chaque station peut établir une communication avec n'importe quelle autre station dans l'IBSS, sans être obligée de passer par un point d'accès. Comme il n'y a pas de point d'accès, les stations n'intègrent qu'un certain nombre de fonctionnalités, telles les trames utilisées pour la synchronisation.

Ce mode de fonctionnement se révèle très utile pour mettre en place facilement un réseau sans fil lorsqu'une infrastructure sans fil ou fixe fait défaut.

L'architecture Wi-Fi

Comme tous les standards de l'IEEE, 802.11 couvre les deux premières couches du modèle de référence OSI. L'une de ses caractéristiques essentielles est qu'il définit une couche MAC commune à toutes les couches physiques. De la sorte, de futures couches physiques pourront être ajoutées sans qu'il soit nécessaire de modifier la couche MAC.

La couche physique

La couche physique a pour rôle de transporter correctement la suite de signaux 0 ou 1 que l'émetteur souhaite envoyer au récepteur. Elle est divisée en deux sous-couches, PLCP (Physical Layer Convergence Protocol) et PMD (Physical Medium Dependent).

La sous-couche PMD s'occupe de l'encodage des données, tandis que la sous-couche PLCP prend en charge l'écoute du support. Elle fournit pour cela un CCA (Clear Channel Assessment), qui est le signal utilisé par la couche MAC pour savoir si le support est occupé ou non.

IEEE 802.11 définit quatre couches physiques différentes :

- FHSS (Frequency Hopping Spread Spectrum)
- DSSS (Direct Sequence Spread Spectrum)
- IR (Infrarouge)
- OFDM (Orthogonal Frequency Division Multiplexing)

Le FHSS et le DSSS utilisent la bande des 2,4 GHz de l'ISM (Industrial, Scientific, and Medical). Nous reviendrons sur cette bande sans licence. L'infrarouge n'est utilisé que dans les cas où les distances entre les différentes stations sont faibles.

La quatrième couche physique a été définie dans la bande des 5,2 GHz. Grâce au codage OFDM, des débits compris entre 6 et 54 Mbit/s peuvent être atteints. 802.11 est le premier standard à utiliser un codage OFDM pour une communication de type paquet. Cette technologie était jusqu'à présent utilisée pour des systèmes de transmission de données continue, tels que DVB (Digital Video Broadcasting) ou DAB (Digital Audio Broadcasting).

Pour qu'un signal soit reçu correctement, sa portée ne peut dépasser 150 m dans un environnement de bureau, 600 m sans obstacle et 1,5 km avec une antenne extérieure. En règle générale, les stations ont une portée maximale de 50 m. Lorsqu'il y a traversée de murs, cette distance est souvent plus restrictive.

La couche liaison de données

La couche liaison de données est composée essentiellement de deux sous-couches, LLC (Logical Link Control) et MAC. La couche LLC utilise les mêmes propriétés que la couche LLC 802.2. Il est de ce fait possible de relier un WLAN à tout autre réseau local appartenant à un standard de l'IEEE. La couche MAC, quant à elle, est spécifique de 802.11.

Le rôle de la couche MAC 802.11 est assez similaire à celui de la couche MAC 802.3 du réseau Ethernet terrestre, puisque les terminaux écoutent la porteuse avant d'émettre. Si la porteuse est libre, le terminal émet, sinon il se met en attente. Cependant, la couche MAC 802.11 intègre un grand nombre de fonctionnalités que l'on ne trouve pas dans la version terrestre.

Les fonctionnalités nécessaires pour réaliser un accès sur une interface radio sont les suivantes :

- procédures d'allocation du support ;
- adressage des paquets ;
- formatage des trames ;
- contrôle d'erreur CRC (Cyclic Redundancy Check) ;
- fragmentation-réassemblage.

L'une des particularités du standard est qu'il définit deux méthodes d'accès fondamentalement différentes au niveau de la couche MAC. La première est le DCF (Distributed Coordination Function), qui correspond à une méthode d'accès assez similaire à celle des réseaux traditionnels supportant le best-effort. Le DCF a été conçu pour prendre en charge le transport de données asynchrones, dans lequel tous les utilisateurs qui veulent transmettre des données ont une chance égale d'accéder au support.

La seconde méthode d'accès est le PCF (Point Coordination Function). Fondée sur l'interrogation à tour de rôle des terminaux, ou polling, sous le contrôle du point d'accès, la méthode PCF est conçue essentiellement pour la transmission de données sensibles, qui demandent une gestion du délai utilisé pour les applications temps réel, telles que la voix ou la vidéo.

Un réseau en mode ad-hoc utilise uniquement le DCF, tandis qu'un réseau en mode infrastructure avec point d'accès utilise à la fois le DCF et le PCF.

Les techniques d'accès

Comme expliqué précédemment, le DCF est la technique d'accès générale utilisée pour permettre des transferts de données asynchrones en best-effort. D'après le standard, toutes les stations doivent la supporter. Le DCF s'appuie sur le CSMA/CA.

Dans Ethernet, le protocole qui implémente la technique d'accès CSMA/CD contrôle l'accès de chaque station au support et détecte et traite les collisions qui se produisent lorsque deux stations ou davantage transmettent simultanément. Dans les réseaux Wi-Fi, la détection des collisions n'est pas possible. Pour détecter une collision, une station doit être capable d'écouter et de transmettre en même temps. Dans les systèmes radio, la transmission couvre la réception de signaux sur la même fréquence et ne permet pas à la station d'entendre la collision : les liaisons radio ne sont jamais full-duplex. Comme une station ne peut écouter sa propre transmission, si une collision se produit, la station continue à transmettre la trame complète, ce qui entraîne une perte de performance du réseau. La technique d'accès de Wi-Fi doit tenir compte de ce phénomène.

Le protocole CSMA/CA

Le CSMA/CA évite les collisions en utilisant des trames d'acquittement, ou ACK (Acknowledgement). Un ACK est envoyé par la station destination pour confirmer que les données sont reçues de manière intacte.

L'accès au support est contrôlé par l'utilisation d'espaces intertrames, ou IFS (Inter-Frame Spacing), qui correspondent à l'intervalle de temps entre la transmission de deux trames. Les intervalles IFS sont des périodes d'inactivité sur le support de transmission. Les valeurs des différents IFS sont calculées par la couche physique.

Le standard définit trois types d'IFS :

- SIFS (Short Inter-Frame Spacing), le plus petit des IFS, est utilisé pour séparer les transmissions au sein d'un même dialogue (envoi de données, ACK, etc.). Il y a toujours une seule station pour transmettre à cet instant, ayant donc la priorité sur toutes les autres stations. La valeur du SIFS est de 28 µs.

- PIFS (PCF IFS), utilisé par le point d'accès pour accéder avec priorité au support. Le PIFS correspond à la valeur du SIFS, auquel on ajoute un temps, ou timeslot, défini dans l'algorithme de back-off, de 78 µs.
- DIFS (DCF IFS), utilisé lorsqu'une station veut commencer une nouvelle transmission. Le DIFS correspond à la valeur du PIFS, à laquelle on ajoute un temps de 128 µs.

Les terminaux d'un même BSS peuvent écouter l'activité de toutes les stations qui s'y trouvent. Lorsqu'une station envoie une trame, les autres stations l'entendent et, pour éviter une collision, mettent à jour un timer, appelé NAV (Network Allocation Vector), permettant de retarder toutes les transmissions prévues. Le NAV est calculé par rapport à l'information située dans le champ durée de vie, ou TTL, contenu dans les trames qui ont été envoyées. Les autres stations n'ont la capacité de transmettre qu'après la fin du NAV.

Lors d'un dialogue entre deux stations, le NAV est calculé par rapport au champ TTL des différentes trames qui sont envoyées (données, ACK, etc.). Le NAV est en fait un temporisateur, qui détermine l'instant auquel la trame peut être transmise avec succès. Une station source voulant transmettre des données écoute le support. Si aucune activité n'est détectée pendant une période de temps correspondant à un DIFS, elle transmet ses données immédiatement. Si le support est encore occupé, elle continue de l'écouter jusqu'à ce qu'il soit libre. Quand le support devient disponible, elle retarde encore sa transmission en utilisant l'algorithme de back-off avant de transmettre ses données.

Si les données envoyées sont reçues intactes, la station destination attend pendant un temps équivalent à un SIFS et émet un ACK pour confirmer leur bonne réception. Si l'ACK n'est pas détecté par la station source ou si les données ne sont pas reçues correctement ou encore si l'ACK n'est pas reçu correctement, on suppose qu'une collision s'est produite, et la trame est retransmise.

Lorsque la station source transmet ses données, les autres stations mettent à jour leur NAV, en incluant le temps de transmission de la trame de données, le SIFS et l'ACK.

La figure 21.14 illustre le processus de transmission des trames à partir d'un émetteur. Ce processus reprend les différentes attentes que nous venons de détailler.

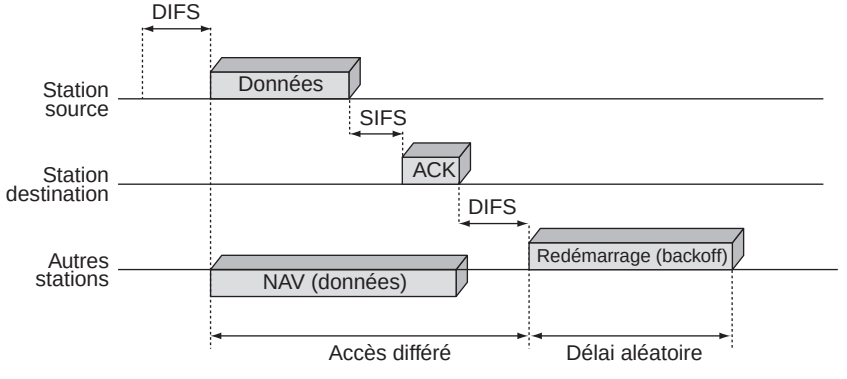


Figure 21.14

Processus de transmission des trames

L'algorithme de back-off permet de résoudre le problème de l'accès au support lorsque plusieurs stations veulent transmettre des données en même temps. Dans Wi-Fi, le temps est découpé en tranches, qui correspondent chacune à un timeslot. Contrairement au timeslot utilisé dans l'aloha, qui correspond à la durée minimale de transmission d'une trame, le timeslot utilisé dans Wi-Fi est un peu plus petit que la durée de transmission minimale d'une trame. Il est utilisé pour définir les intervalles IFS ainsi que les temporisateurs pour les différentes stations. Son implémentation est différente pour chaque couche physique.

Initialement, une station calcule la valeur d'un temporisateur, appelé timer de back-off, compris entre 0 et 7 et correspondant à un certain nombre de timeslots. Lorsque le support est libre, les stations décrémentent leur temporisateur jusqu'à ce que le support soit occupé ou que le temporisateur atteigne la valeur 0. Si le temporisateur n'a pas atteint la valeur 0 et que le support soit de nouveau occupé, la station bloque le temporisateur. Dès que le temporisateur atteint la valeur 0, la station transmet sa trame. Si deux ou plusieurs stations atteignent la valeur 0 au même instant, une collision se produit, et chaque station doit générer un nouveau temporisateur, compris cette fois entre 0 et 15.

Pour chaque tentative de retransmission, le temporisateur croît de la façon suivante :

$[2^{2+i} \times \text{ranf}()] \times \text{timeslot}$

i correspond au nombre de tentatives consécutives d'une station pour l'envoi d'une trame, et ranf() à une variable aléatoire uniforme comprise entre 0 et 1.

Grâce à cet algorithme, les stations ont la même probabilité d'accéder au support. Son seul inconvénient est de ne pas garantir un délai minimal et donc de compliquer la prise en charge d'applications temps réel telles que la voix ou la vidéo.

La réservation RTS/CTS et le problème de la station cachée

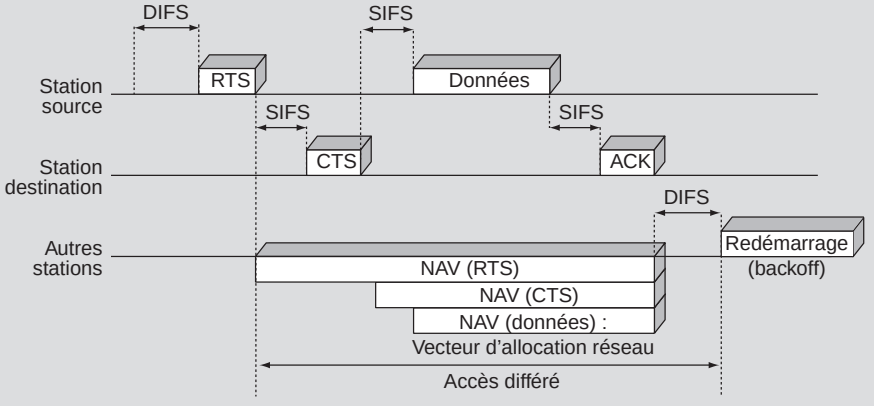
Dans Wi-Fi, l'écoute du support se fait à la fois au niveau de la couche physique, avec le PCS (Physical Carrier Sense), et au niveau de la couche MAC, avec le VCS (Virtual Carrier Sense). Le PCS détecte la présence d'autres stations Wi-Fi en analysant toutes les trames passant sur le support hertzien et en détectant l'activité sur le support grâce à la puissance relative du signal des autres stations.

Le VCS est un mécanisme de réservation fondé sur l'envoi de trames RTS/CTS (Request to Send/Clear to Send) entre une station source et une station destination avant tout envoi de données. Une station source qui veut transmettre des données envoie un RTS. Toutes les stations du BSS entendant le RTS lisent le champ TTL du RTS et mettent à jour leur NAV. La station destination ayant reçu le RTS répond, après avoir attendu pendant un SIFS, en envoyant un CTS. Les autres stations entendant le CTS lisent le champ de durée du CTS et mettent à nouveau à jour leur NAV. Après réception du CTS par la station source, cette dernière est assurée que le support est stable et réservé pour sa transmission de données.

Cela permet à la station source de transmettre ses données ainsi que de recevoir l'ACK sans collision. Comme les trames RTS/CTS réservent le support pour la transmission d'une station, ce mécanisme est habituellement utilisé pour envoyer de grosses trames pour lesquelles une retransmission serait trop coûteuse en terme de bande passante.

La réservation RTS/CTS et le problème de la station cachée *(suite)*

La figure 21.15 illustre le processus d'émission d'une trame lorsque la station destination est cachée.



ACK (ACKnowledgement)
CTS (Clear to Send)
DCF (Distributed Coordination Function)
DIFS (DCF Inter-Frame Spacing)
NAV (Network Allocation Vector)
RTS (Request to Send)
SIFS (Short Inter-Frame Spacing)

Figure 21.15
Transmission en utilisant les trames RTS/CTS

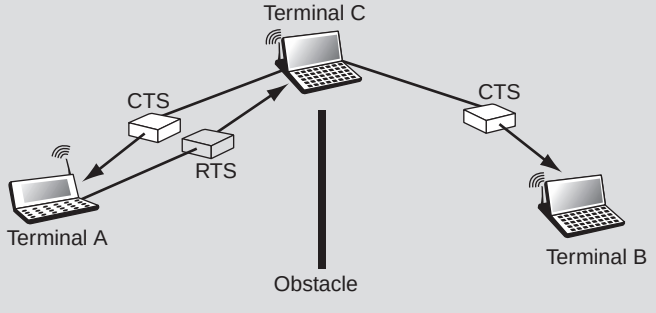
Les stations peuvent choisir d'utiliser le mécanisme RTS/CTS ou de ne l'utiliser que lorsque la trame à envoyer excède une variable RTS_Threshold ou encore de ne jamais l'utiliser.

Le problème de la station cachée

Un problème spécifique du monde sans fil est le problème de la station cachée. Deux stations situées chacune à l'opposé d'un point d'accès (AP) ou d'une autre station peuvent entendre l'activité de cet AP mais ne pas s'entendre l'une l'autre du fait que la distance entre les deux est trop grande ou qu'un obstacle les empêche de communiquer entre elles. Le mécanisme de réservation RTS/CTS permet de résoudre ce problème.

La figure 21.16 illustre une station B cachée de la station A mais pas de la station C. La station A transmet des données à la station C, mais la station B ne détecte pas l'activité de la station A. Dans ce cas, la station B peut transmettre librement, sans interférer avec la transmission de la station A. Toutefois, si A et C s'échangent des RTS et des CTS, la station B, bien que n'écoutant pas directement la station A, est informée par l'envoi par la station C d'un CTS que le support est occupé. Elle n'essaie donc pas de transmettre durant la transmission entre A et C. Ce mécanisme ne permet pas d'éviter les collisions, puisque des RTS peuvent être envoyés simultanément par A et par B, mais une collision de RTS ou de CTS ne gaspille pas autant de bande passante qu'une collision de données, étant donné que les trames RTS et CTS sont relativement petites.

Figure 21.16
Problème de la station cachée



CTS (Clear to Send) RTS (Request to Send)

En conclusion, le CSMA/CA permet de partager l'accès. Le mécanisme d'acquittement supporte en outre de manière efficace les problèmes liés aux interférences et, d'une manière générale, tous les problèmes liés à l'environnement radio. Le mécanisme de réservation RTS/CTS évite les problèmes de la station cachée. Tous ces mécanismes entraînent toutefois l'ajout aux trames Wi-Fi d'en-têtes, que les trames Ethernet ne possèdent pas. C'est pourquoi les réseaux Wi-Fi montrent toujours des performances plus faibles que les réseaux locaux Ethernet.

Fragmentation-réassemblage

Nous venons d'introduire le protocole CSMA/CA, qui permet à une station d'accéder au support hertzien pour émettre sa trame. Une question en suspens concerne la taille de la trame. Plus la taille d'une trame est importante, plus elle a de chance d'être corrompue. La fragmentation d'une trame en plusieurs trames de taille inférieure accroît la fiabilité de la transmission. Cette solution a pour effet de réduire le besoin de retransmettre des données dans de nombreux cas et d'augmenter ainsi les performances globales du réseau. La fragmentation est utilisée notamment dans les liaisons radio, dans lesquelles le taux d'erreur est important.

Wi-Fi utilise un système à saut de fréquence (Frequency Hop), dans lequel le support s'interrompt toutes les 20 ms pour changer de fréquence. Si la trame est petite, la probabilité pour que la transmission soit interrompue est faible. Pour savoir si une trame doit être fragmentée, on compare sa taille à une valeur seuil, appelée Fragmentation_Threshold. Si la taille de la trame est plus grande que ce seuil, la trame est fragmentée. Les fragments ont une taille équivalente à la valeur du seuil Fragmentation_Threshold, sauf pour le dernier, qui peut avoir une taille plus petite.

Quand une trame est fragmentée, tous les fragments sont transmis de manière séquentielle. Le support n'est libéré qu'une fois tous les fragments transmis avec succès ou lorsque la station source ne réussit pas à recevoir l'acquittement d'un fragment transmis. La station destination acquitte chaque fragment reçu avec succès en envoyant un ACK à la station source. La station source garde le contrôle du support pendant toute la durée de la transmission d'une trame en attendant un temps SIFS après la réception d'un ACK ou après la transmission d'un fragment. Si un ACK n'est pas correctement reçu, la station source arrête la transmission et essaie d'accéder de nouveau au support. Lorsque la station source accède au support, elle commence à transmettre à partir du dernier fragment non acquitté.

Si les stations utilisent le mécanisme RTS/CTS, seul le premier fragment envoyé utilise les trames RTS/CTS pour réserver le support. Les autres stations dans le BSS maintiennent leur NAV en extrayant l'information de durée de vie dans les différents fragments et ACK.

La figure 21.17 illustre le processus suivi par l'émetteur pour transmettre une suite de fragments provenant d'une même trame.

La trame est assemblée lorsque la station destination a reçu tous les fragments de la station source.

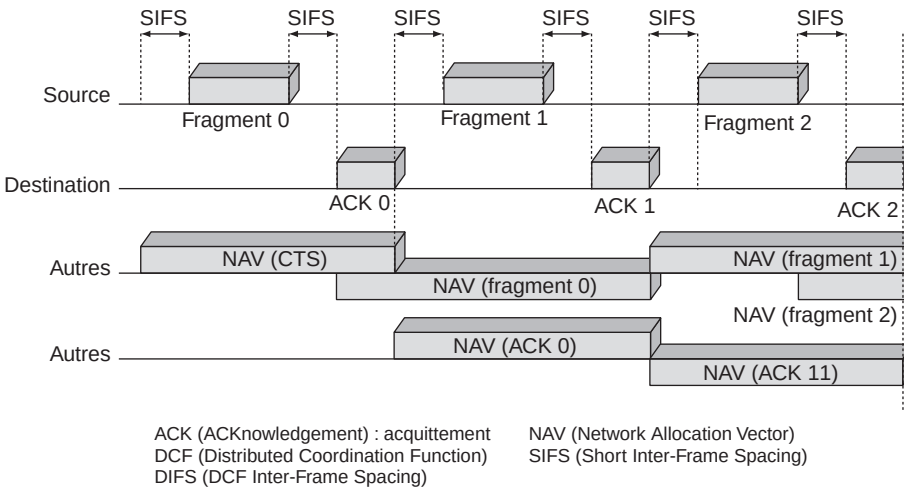


Figure 21.17
Transmission d'une trame fragmentée

Fonctionnalités

La norme Wi-Fi induit un fonctionnement qui, pour être classique dans les réseaux sans fil, est souvent négligé dans les réseaux de mobiles. Par exemple, le passage d'une cellule à une autre sans interruption de la communication n'a pas été prévu dans les premières versions, si bien que le handover a dû être introduit dans les nouvelles.

De même, la sécurité a été renforcée pour éviter qu'un client ne prenne la place d'un autre ou qu'il n'écoute les communications d'autres utilisateurs.

Les handovers

Dans les réseaux sans fil, les handovers interviennent lorsqu'un terminal souhaite se déplacer d'une cellule à une autre sans interrompre sa communication. Ils se font à peu près de la même manière que dans la téléphonie mobile, à quelques nuances près. Dans les réseaux sans fil, le handover s'effectue entre deux transmissions de données et non pas au milieu d'un dialogue. Les déconnexions temporaires ne perturbent pas la conversation dans la téléphonie mobile, tandis que, dans les réseaux sans fil, elles peuvent entraîner une perte de performance du réseau.

Le standard ne fournit pas de mécanisme de handover à part entière mais définit certaines règles, telles que la synchronisation, l'écoute passive et active ou encore l'association et la réassociation, qui permettent aux stations de choisir le point d'accès auquel elles veulent s'associer.

Lorsque les terminaux se déplacent, c'est-à-dire lorsqu'ils changent de cellule ou qu'ils sont en mode d'économie d'énergie, ils doivent rester synchronisés pour pouvoir communiquer. Au niveau d'un BSS, les stations synchronisent leur horloge avec l'horloge du point d'accès. Pour conserver la synchronisation, le point d'accès envoie

périodiquement des trames balises, ou Beacon Frames, qui contiennent la valeur d'horloge du point d'accès. Lors de la réception de ces trames, les stations mettent à jour leurs horloges pour rester synchronisées avec le point d'accès.

Quand un terminal veut accéder — après allumage ou retour d'un mode veille ou d'un handover — à un BSS ou à un ESS contrôlé par un ou plusieurs point d'accès, il choisit un point d'accès, auquel il s'associe, selon un certain nombre de critères, tels que la puissance du signal, le taux d'erreur des paquets ou la charge du réseau. Si la puissance du signal du point d'accès est trop faible, la station cherche un autre point d'accès plus approprié.

Cette recherche du meilleur point d'accès passe par l'écoute du support. Cette dernière peut se faire de deux manières différentes, passive ou active, selon des critères tels que les performances ou la consommation d'énergie :

- **Écoute passive.** La station attend de recevoir une trame balise venant du point d'accès.
- **Écoute active.** Lorsque que la station a trouvé le point d'accès le plus approprié, elle lui envoie une requête d'association par l'intermédiaire d'une trame appelée Probe Request Frame et attend que le point d'accès lui réponde pour s'associer.

Dès que le terminal est accepté par le point d'accès, il se règle sur le canal radio le plus approprié. Périodiquement, le terminal surveille tous les canaux du réseau pour évaluer si un point d'accès possède de meilleures performances. Si tel est le cas, il s'associe à ce nouveau point d'accès et règle son canal radio en conséquence.

Les réassociations s'effectuent lorsqu'une station se déplace physiquement par rapport à son point d'accès d'origine, entraînant une diminution de la puissance du signal. Dans d'autres cas, les réassociations sont dues à des changements de caractéristiques de l'environnement radio ou à cause d'un trafic réseau trop élevé sur le point d'accès d'origine. Dans ce cas, le standard fournit une fonction d'équilibrage de charge, ou Load Balancing, qui permet de répartir la charge de manière efficace au sein du BSS ou de l'ESS et ainsi d'éviter les réassociations.

La sécurité

Dans les réseaux sans fil, le support est partagé. Tout ce qui est transmis et envoyé peut donc être intercepté. Pour permettre aux réseaux sans fil d'avoir un trafic aussi sécurisé que dans les réseaux fixes, le groupe de travail 802.11 a mis au point le protocole WEP (Wired Equivalent Privacy), dont les mécanismes s'appuient sur le chiffrage des données et l'authentification des stations.

D'après le standard, WEP est optionnel, et les terminaux ainsi que les points d'accès ne sont pas obligés de l'implémenter. Comme nous allons le voir, la sécurité n'est pas garantie avec le WEP, et un attaquant peut casser les clés de chiffrement sans trop de difficulté. La Wi-Fi Alliance, l'organisme en charge de la promotion de Wi-Fi, a développé un deuxième mode de protection, le WPA (Wi-Fi Protected Access), qui résout ces problèmes, au moins pour quelques années. Enfin, le groupe de travail 802 .11 a créé un groupe spécifique, IEEE 802.11i, qui propose une solution pérenne, normalisée en juin 2004.

Avant de présenter ces trois protocoles de sécurité, rappelons deux règles de protection élémentaires :

- Cacher le nom du réseau, ou SSID, de telle sorte qu'un utilisateur ne voie pas le réseau et ne puisse donc pas s'y connecter. Cette mesure de sécurité n'est hélas que provisoire. Si un attaquant écoute le réseau suffisamment longtemps, il finira bien par voir passer le nom du réseau puisqu'un utilisateur qui souhaite se connecter doit donner ce SSID.
- N'autoriser que les communications contrôlées par une liste d'adresses MAC, ou ACL (Access Control List). Cela permet de ne fournir l'accès qu'aux stations dont l'adresse MAC est spécifiée dans la liste.

Le WEP

Comme expliqué précédemment, la solution de gestion de la confidentialité et l'authentification commercialisée avec les équipements Wi-Fi est le WEP.

Les trames transmises sur les réseaux sans fil sont protégées par un chiffrement. Seul un déchiffrement avec la bonne clé WEP statique, partagée entre le terminal et le réseau, est autorisé. Cette clé est obtenue par la concaténation d'une clé secrète de 40 ou 104 bits et d'un vecteur d'initialisation IV (Initialization Vector) de 24 bits. Celui-ci est changé dynamiquement pour chaque trame. La taille de la clé finale est de 64 ou 128 bits.

À partir de la clé obtenue, l'algorithme RC4 (Ron's Code 4) réalise le chiffrement des données en mode flux (stream cipher). Une clé RC4 a une longueur comprise entre 8 et 2 048 bits. La clé est placée dans un générateur de nombres pseudo-aléatoires, ou PRNG (Pseudo-Random Number Generator), issu des laboratoires RSA (Rivest, Shamir, Adleman). Ce générateur détermine une séquence d'octets pseudo-aléatoire, ou keystream. Cette série d'octets, appelée Ksi, est utilisée pour chiffrer un message en clair (Mi) à l'aide d'un classique protocole de Vernam, réalisant un ou exclusif XOR entre Ksi et Mi :

$Ci = Ksi \oplus Mi$.

Le message Mi est composé des données qui sont concaténées à leur ICV (Integrity Check Value). La trame chiffrée est ensuite envoyée avec son IV en clair. L'IV est un index qui sert à retrouver le keystream et donc de déchiffrer les données.

Le processus de chiffrement WEP est illustré à la figure 21.18.

Deux techniques d'authentification sont associées au WEP :

- Open System Authentication
- Shared Key Authentication

Dans la première, qui est le système d'authentification par défaut. l'authentification est explicite. Un terminal peut donc s'associer avec n'importe quel point d'accès et écouter toutes les données qui transitent au sein du BSS. La seconde est nettement meilleure car elle utilise un mécanisme de clé secrète partagée.

Le mécanisme Shared Key Authentication se déroule en quatre étapes :

1. Une station voulant s'associer avec un point d'accès lui envoie une trame d'authentification.
2. Lorsque le point d'accès reçoit cette trame, il envoie à la station une trame contenant 128 bits d'un texte aléatoire généré par l'algorithme WEP.

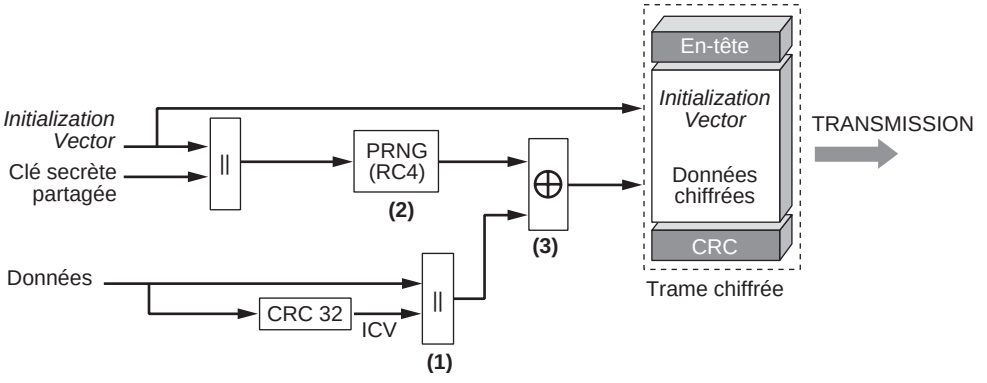
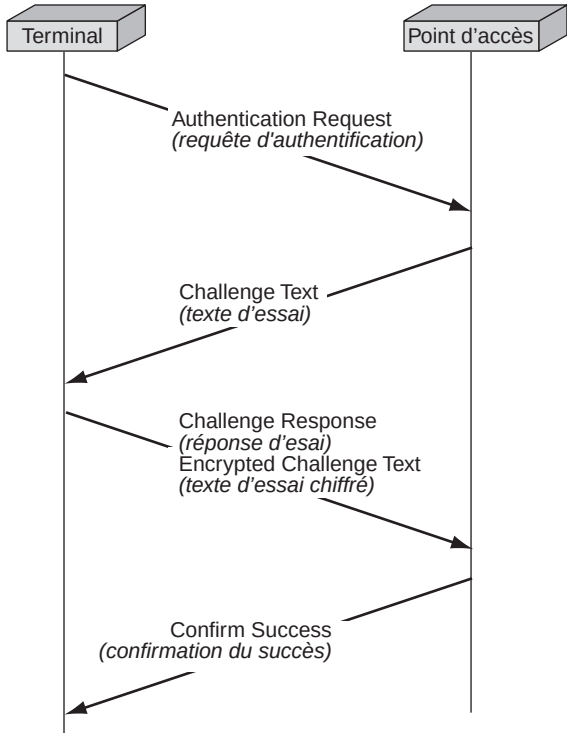


Figure 21.18
Chiffrement d'un paquet WEP

3. Après avoir reçu la trame contenant le texte, la station la copie dans une trame d'authentification et la chiffre avec la clé secrète partagée avant d'envoyer le tout au point d'accès.
4. Le point d'accès déchiffre le texte chiffré à l'aide de la même clé secrète partagée et le compare avec celui qui a été envoyé plus tôt. Si le texte est identique, le point d'accès lui confirme son authentification, sinon il envoie une trame d'authentification négative.

La figure 21.19 illustre ces étapes.

Figure 21.19
Fonctionnement du mécanisme Shared Key Authentication



Une première amélioration de ces mécanismes a été apportée par l'introduction d'une authentification forte avec le protocole IEEE 802.1x. Nous décrivons ce dernier en détail au chapitre 34, consacré à la sécurité. Retenons pour l'immédiat que ce mécanisme est semblable à celui illustré à la figure 21.19.

WPA et IEEE 802.11i

Nous avons déjà souligné les faiblesses du protocole WEP. Le groupe de travail IEEE 802.11i a finalisé en juin 2004 une architecture destinée à combler ces lacunes. En attendant que ce standard arrive sur le marché sous le nom de WPA2, un comité industriel, la Wi-Fi Alliance (anciennement WECA) a édité une recommandation sous le nom de WPA (Wi-Fi Protected Access). Fondé sur un sous-ensemble de 802.11i, WPA utilise le matériel existant (AP, carte réseau sans fil).

Les apports de la norme IEEE 802.11i peuvent être classés en trois catégories :

- définition de multiples protocoles de sécurité radio ;
- éléments d'information permettant de choisir l'un d'entre eux ;
- nouvelle méthode de distribution des clés.

Le standard utilise 802.1x pour l'authentification et le calcul d'une clé maître, nommée PMK (Pairwise Master Key). Dans mode ad-hoc, cette clé est appelée PSK (Pre-Shared Key) et est distribuée manuellement.

Un RSN (Robust Security Network) 802.11i, ou réseau sécurisé, utilise donc 802.1x pour les services d'authentification et de gestion des clés. Le contrôle d'accès s'appuie sur une authentification forte des couches supérieures. Le RSN doit garantir sécurité et mobilité, intégrité et confidentialité, ainsi que passage à l'échelle et flexibilité.

Sécurité et mobilité

L'architecture sécuritaire doit fournir une authentification du client, indépendamment du fait qu'il se trouve dans son réseau de domiciliation ou dans un réseau étranger. Une architecture avec serveur d'authentification centralisé de type RADIUS (Remote Authentication Dial-In User Server) peut satisfaire à cette exigence. Le client n'a plus à se préoccuper du point d'accès auquel il est associé.

Intégrité et confidentialité

Dans l'architecture 802.1x, un réseau comporte trois éléments en communication : un « supplicant », qui est la station 802.1x demandant à être authentifiée, un « authenticator », le point d'accès, et un serveur d'authentification, ou AS (Authentication Server), le plus souvent RADIUS.

Chaque authenticator partage un secret avec le serveur RADIUS avec lequel il communique. Ce secret est utilisé pour calculer un résumé HMAC-MD5 sur les paquets RADIUS échangés. Chaque paquet RADIUS contient un champ Request Authenticator, qui est un résumé HMAC-MD5 du paquet, calculé avec ce secret. Ce champ est inséré par le serveur RADIUS et vérifié par le point d'accès. Dans l'autre sens de communication, le serveur RADIUS vérifie l'attribut EAP Authenticator présent avec l'attribut EAP

Message**.** Ces deux attributs offrent la possibilité d'une authentification mutuelle par paquet et préservent l'intégrité de la communication entre le serveur RADIUS et le point d'accès.

Puisqu'il est assez facile pour un attaquant équipé d'un outil de réception convenable d'écouter le trafic entre les stations sur le lien sans fil, l'architecture de sécurité proposée vise à fournir des garanties de confidentialité forte. Elle définit en outre un mécanisme de distribution dynamique de clés.

Passage à l'échelle et flexibilité

L'architecture 802.11i est extensible quant au nombre d'utilisateurs pris en charge et à la mobilité. Un utilisateur se déplaçant d'un point d'accès à un autre pourra être réauthentifié rapidement et de façon sécurisée.

De plus, pour répondre aux besoins de déploiement des réseaux sans fil dans les entreprises et les lieux publics, cette architecture de sécurité se veut flexible, afin d'en faciliter l'administration et de prendre en compte l'environnement de déploiement existant.

En séparant l'authenticator du processus d'authentification lui-même, le RSN permet le passage à l'échelle du nombre de points d'accès. La flexibilité est apportée par le fait que le message optionnel EAPoW-Key peut être désactivé pour un déploiement particulier, où la confidentialité des données n'est pas nécessaire.

Le modèle 802.11i précise comment le RSN interagit avec 802.1x. Deux types de protocoles assurent la sécurité au niveau MAC :

- TKIP (Temporal Key Integrity Protocol)
- CCMP (Counter with Cipher Block Chaining Message Authentication Code Protocol)

Un TSN (Transition Security Network) supporte les architectures pré-RSN, en particulier les mécanismes suivants hérités de la norme 802.11 :

- Open Authentication
- Shared Key Authentication
- WEP

Un réseau RSN doit supporter le protocole CCMP. Un TSN peut cependant assurer la transition avec les réseaux antérieurs en implémentant le protocole TKIP.

La figure 21.20 illustre les différents niveaux de sécurité qui doivent être pris en charge pour avoir une architecture sécurisée globale.

L'authenticator (le point d'accès) et le serveur d'authentification (AS) réalisent une authentification mutuelle et établissent un canal sécurisé. Le modèle 802.11i ne décrivant pas les méthodes utilisées pour mener à bien cette opération, des protocoles tels que RADIUS, IPsec ou TLS/SSL peuvent être mis en œuvre.

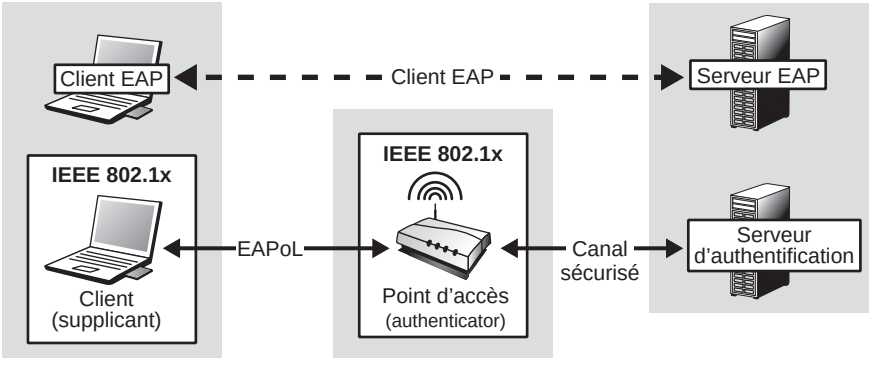


Figure 21.20
Niveaux de sécurité dans l'architecture 802.1x

Le client 802.1x, ou supplicant, et le serveur d'authentification s'authentifient mutuellement à l'aide du protocole EAP (Extensible Authentication Protocol) et gênèrent une clé maître PMK. Les éléments de cette procédure sont transportés par le canal sécurisé, dont les paramètres cryptographiques doivent être différents pour chaque client 802.1x. La clé PMK est partagée entre le client 802.1x et le point d'accès. Ceux-ci utilisent un protocole à quatre passes, ou 4-ways handshake, et des messages EAPoL-Key pour réaliser les opérations suivantes :

1. Confirmation de l'existence de la PMK.
2. Confirmation de la mise en service de la PMK.
3. Calcul de la clé PTK (Pairwise Transient Key) à partir de la PMK.
4. Mise en place des clés de chiffrement et d'intégrité des trames 802.11.
5. Confirmation de la mise en fonction des clés 802.11.

Ce processus est illustré à la figure 21.21.

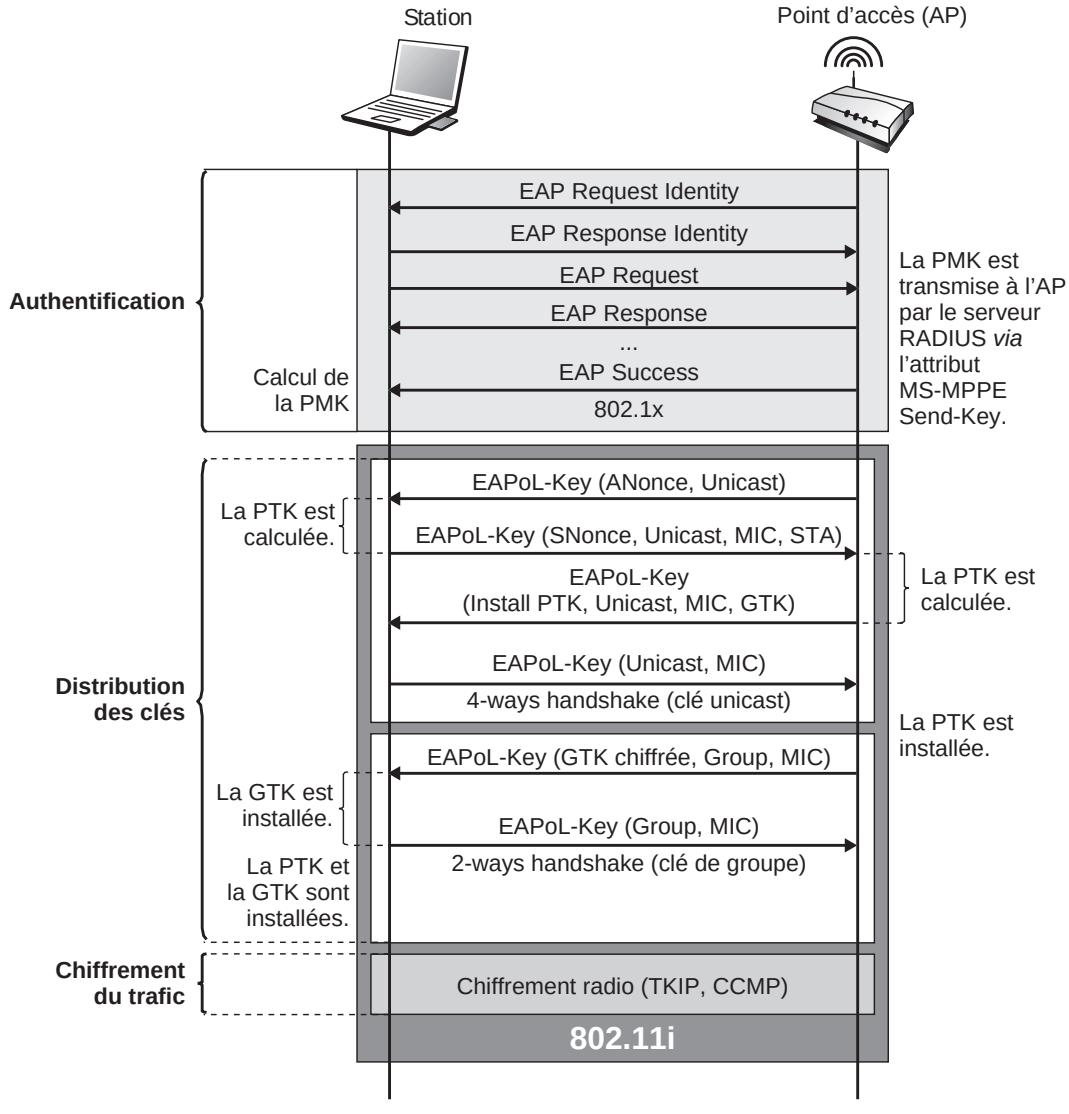
Une clé GTK (Group Transient Key), transmise *via* des paquets EAPoL-Key depuis le point d'accès vers le client 802.1x, permet à ce dernier d'échanger des messages en mode broadcast et optionnellement en mode unicast. Dans le cas du mode dit Pre-Shared Key, la clé PMK est préinstallée entre le client 802.1x et le point d'accès.

Négociation de la politique de sécurité

Un point d'accès diffuse dans ses trames beacon ou probe des éléments d'information, ou IE (Information Element), afin de notifier au client 802.1x les indications suivantes :

- liste des infrastructures d'authentification supportées (typiquement 802.1x) ;
- liste des protocoles de sécurité disponibles (TKIP, CCMP, etc.) ;
- méthode de chiffrement pour la distribution d'une clé de groupe (GTK).

Une station 802.11 notifie son choix par un élément d'information inséré dans sa demande d'association. Cette démarche est illustrée à la figure 21.22.



PMK (Pairwise Master Key)
PTK (Pairwise Temporal Key)
GTK (Group Transient Key)
MS-MPPE Send-Key (Microsoft Point-to-Point Encryption) : clé de Microsoft utilisée comme la clé Unicast par défaut
ANonce : nombre aléatoire
SNonce : nombre aléatoire
MIC (Message Integrity Code)
STA : adresse de la station
Group : adresse du groupe
TKIP (Temporal Key Integrity Protocol) : correspond à WPA
CCMP (Counter-mode/CBC-MAC Protocol) : correspond à WPA2

Figure 21.21

Fonctionnement du protocole à quatre passes 802.11i

La sécurité des réseaux Wi-Fi a démarré sous de mauvais auspices. Aujourd'hui, les problèmes de départ sont résolus, et même en dehors de WPA et WPA2 (IEEE 802.11i) il existe de nombreuses solutions très fiables, comme l'utilisation de réseaux privés virtuels ou de technologies fondées sur la carte à puce.

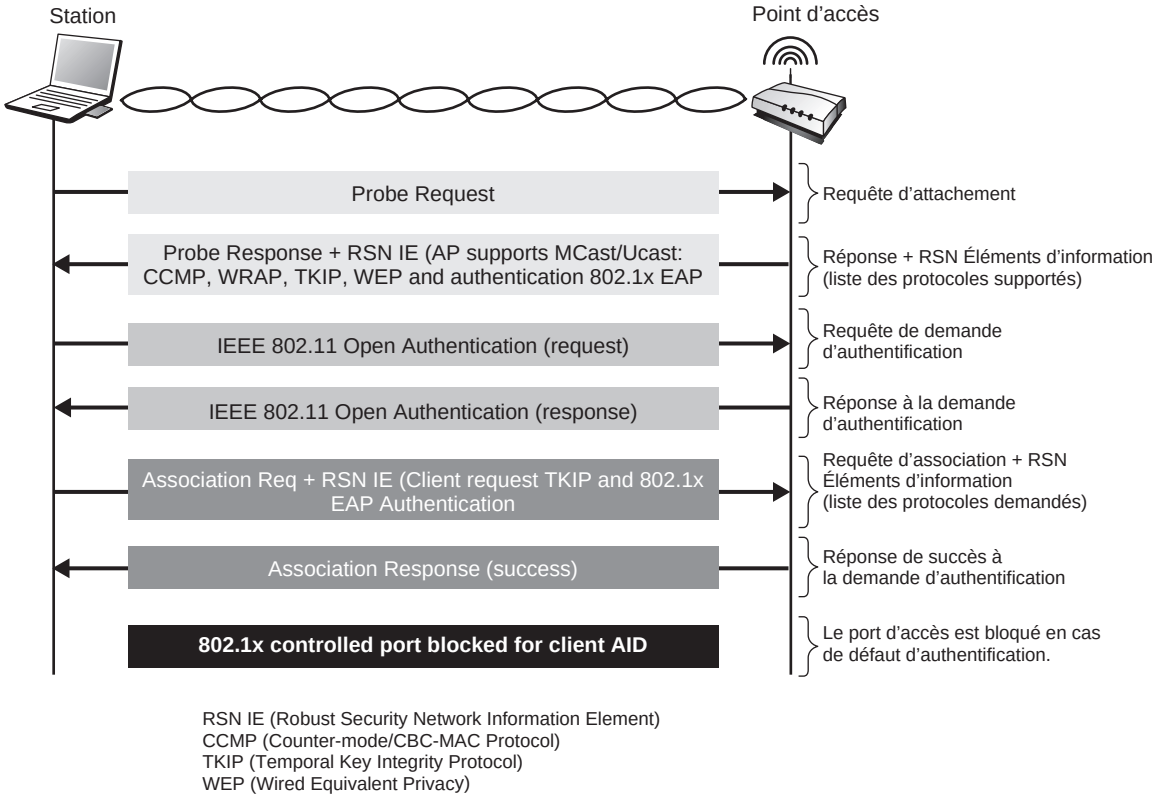


Figure 21.22
Négociation de la politique de sécurité

Économie d'énergie

Les terminaux sans fil peuvent être fixes ou mobiles. Le problème principal des terminaux mobiles concerne leur batterie, qui n'a généralement que peu d'autonomie. Pour augmenter le temps d'activité des terminaux, le standard IEEE 802.11 prévoit un mode d'économie d'énergie. Plus précisément, il existe deux modes de fonctionnement d'un terminal :

- Continuous Aware Mode
- Power Save Polling Mode

Le premier correspond au fonctionnement par défaut, dans lequel la station est tout le temps allumée et écoute constamment le support. Le second permet une économie d'énergie. Dans ce cas, le point d'accès tient à jour un enregistrement de toutes les stations qui sont en mode d'économie d'énergie et stocke les données qui leur sont adressées. Les stations qui sont en veille s'activent à des périodes de temps régulières pour recevoir une trame particulière, la trame TIM (Traffic Information Map), envoyée par le point d'accès.

Entre les trames TIM, les terminaux retournent en mode veille. Toutes les stations partagent le même intervalle de temps pour recevoir les trames TIM, de sorte à s'activer au même moment pour les recevoir. Les trames TIM font savoir aux terminaux mobiles si elles ont ou non des données stockées dans le point d'accès. Lorsqu'un terminal s'active pour recevoir une trame TIM et s'aperçoit que le point d'accès contient des données qui lui sont destinées, il envoie au point d'accès une requête, appelée Polling Request Frame, pour mettre en place le transfert des données. Une fois le transfert terminé, il retourne en mode veille jusqu'à réception de la prochaine trame TIM.

Pour des trafics de type broadcast ou multicast, le point d'accès envoie aux terminaux une trame DTIM (Delivery Traffic Information Map).

Les trames Wi-Fi

Les paquets IP composés dans les terminaux du réseau sans fil doivent être transmis sur le support hertzien. Pour cela, ils doivent être placés dans une trame Ethernet. De plus, pour contrôler et gérer la liaison, il est nécessaire d'avoir des trames spécifiques.

Les trois types de trames disponibles dans Wi-Fi sont les suivantes :

- trame de données, pour la transmission des données utilisateur ;
- trame de contrôle, pour contrôler l'accès au support (RTS, CTS, ACK) ;
- trame de gestion, pour les associations ou les désassociations d'une station avec un point d'accès, ainsi que pour la synchronisation et l'authentification.

Toutes les trames Wi-Fi sont composées de la manière illustrée à la figure 21.23.

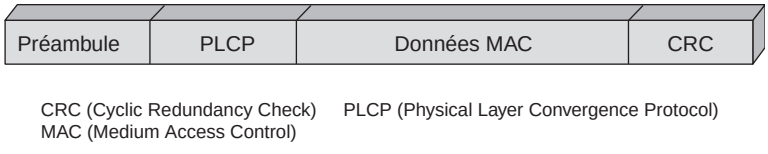


Figure 21.23
Structure d'une trame Wi-Fi

Le préambule est dépendant de la couche physique et contient les deux séquences suivantes :

- Synch, de 80 bits alternant 0 et 1, qui est utilisée par le circuit physique pour sélectionner l'antenne à laquelle se raccorder.
- SFD (Start Frame Delimiter), une suite de 16 bits, 0000 1100 1011 1101, utilisée pour définir le début de la trame.

L'en-tête PLCP (Physical Layer Convergence Protocol) contient les informations logiques suivantes utilisées par la couche physique pour décoder la trame :

- Longueur de mot du PLCP_PDU : représente le nombre d'octets que contient le paquet, ce qui permet à la couche physique de détecter correctement la fin du paquet.

- Fanion de signalisation PLCP : contient l'information concernant la vitesse de transmission entre la carte coupleur et le point d'accès.
- Champ d'en-tête du contrôle d'erreur : champ de détection d'erreur CRC sur 16 bits.

La zone MAC transporte le protocole de niveau sous-jacent, comme illustré à la figure 21.24.

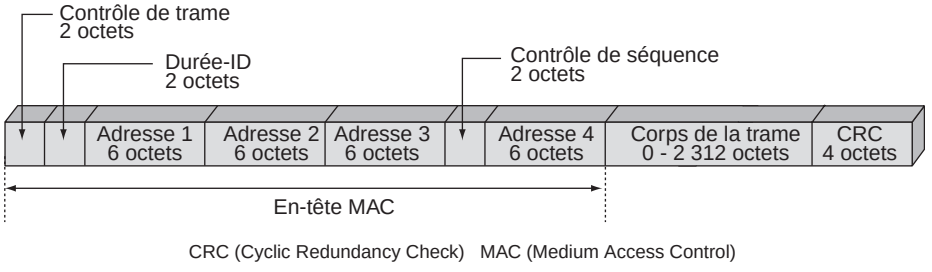


Figure 21.24
Zone MAC

IEEE 802.11a, b et g

Les réseaux Wi-Fi de base proviennent de la normalisation IEEE 802.11b sur la bande des 2,4 GHz. Comme expliqué précédemment, cette norme a pour origine des études effectuées dans le cadre général du groupe 802.11.

En ce début des années 2000, 802.11b s'est imposé comme standard, et plusieurs millions de cartes d'accès Wi-Fi ont été vendues. D'abord déployé dans les campus, les aéroports, les gares et les grandes administrations publiques ou privées, il s'est ensuite imposé dans les réseaux des entreprises pour permettre la connexion de PC portables et d'équipements de type PDA.

Les réseaux 802.11 travaillent avec des points d'accès dont la vitesse de transmission est de 11 Mbit/s et la portée de quelques dizaines de mètres. Pour obtenir cette valeur maximale de la porteuse, il faut que le terminal soit assez près du point d'accès, à moins d'une vingtaine de mètres. Il faut donc, au moment de l'ingénierie du réseau, bien calculer le positionnement des différents points d'accès.

Treize fréquences sont disponibles aux États-Unis dans la bande des 83,5 MHz et quatorze en Europe. Un point d'accès ne peut utiliser que trois fréquences au maximum, car l'émission demande une bande passante qui recouvre quatre fréquences.

Les fréquences peuvent être réutilisées régulièrement. De la sorte, dans une entreprise, le nombre de machines que l'on peut raccorder est très important et permet à chaque station terminale de se raccorder à haut débit à son serveur ou à un client distant.

Des extensions des réseaux Wi-Fi ont été apportées par les normalisations IEEE 802.11g, dans la bande des 2,4 GHz, et IEEE 802.11a, dans celle des 5 GHz. Ces normes ont pour origine des études effectuées dans le cadre de la normalisation HiperLAN (High Performance Local Area Network) de l'ETSI en ce qui concerne la couche physique.

La couche MAC de 802.11b est conservée et est donc différente de la couche équivalente d'HiperLAN, qui est fondée sur ATM. Les réseaux 802.11b et 802.11g sont compatibles dans le sens ascendant. Une carte 802.11g peut donc se connecter à un réseau 802.11b à la vitesse de 11 Mbit/s, mais l'inverse est impossible. On considère que 802.11g est le successeur de 802.11b, et la plupart des équipementiers l'ont adopté. En revanche, les fréquences des réseaux 802.11b et 802.11a étant totalement différentes, il n'y a aucune compatibilité entre eux. Si l'équipement qui souhaite accéder aux deux réseaux comporte deux cartes d'accès, les fréquences peuvent toutefois se superposer.

Pour la partie physique, les propositions suivantes ont été retenues pour les réseaux 802.11a :

- Fréquence de 5 GHz dans la bande de fréquences sans licence U-NII (Unlicensed-National Information Infrastructure), qui ne nécessite pas de licence d'utilisation.
- Modulation OFDM (Orthogonal Frequency Division Multiplexing) avec 52 porteuses, autorisant d'excellentes performances en cas de chemins multiples.
- Huit débits, échelonnées de 6 à 54 Mbit/s. Le débit sélectionné par la carte d'accès dépend de la puissance de réception.

La distance maximale entre la carte et le point d'accès peut dépasser 100 m, mais la chute du débit de la communication est fortement liée à la distance. Pour le débit de 54 Mbit/s, la station mobile contenant la carte Wi-Fi ne peut s'éloigner que de quelques mètres du point d'accès. Au-delà, le débit chute très vite pour être approximativement équivalent à celui qui serait obtenu avec la norme 802.11b à 100 m de distance.

En réalisant de petites cellules, de façon que les fréquences soient fortement réutilisables, un réseau 802.11a permet à plusieurs dizaines de clients par 100 m^2 de se partager entre 100 et 200 Mbit/s. Un tel réseau est dès lors capable de prendre en charge des flux vidéo de bonne qualité.

Les niveaux supérieurs au niveau MAC, c'est-à-dire à la couche gérant l'algorithme d'accès CSMA/CD, correspondent à ceux que l'on rencontre dans les réseaux Ethernet.

IEEE 802.11e et f

Le groupe de travail IEEE 802.11e définit une norme ayant pour objectif d'améliorer les diverses normes 802.11 en introduisant de la qualité de service et de nouvelles fonctionnalités de sécurité et d'authentification. Un autre groupe de travail, IEEE 802.11f, se penche sur les problèmes liés aux changements intercellulaires, ou handovers.

Ces ajouts visent à faire transiter dans les réseaux Wi-Fi des applications possédant des contraintes temporelles, comme la parole téléphonique ou les applications multimédias. Pour cela, il a fallu définir des classes de services et permettre aux terminaux de choisir la bonne priorité en fonction de la nature de l'application transportée.

La gestion des priorités s'effectue au niveau du terminal par l'intermédiaire d'une technique d'accès au support physique modifiée par rapport à celle utilisée dans la norme de base 802.11. Les stations prioritaires ont des temporisateurs d'émission beaucoup plus courts que ceux des stations non prioritaires, ce qui leur permet de prendre l'avantage lorsque deux stations de niveaux différents essayent d'accéder au support.

IEEE 802.11f a une tout autre ambition puisqu'il vise à permettre les handovers pour les clients qui changent de cellules en se déplaçant. La norme commune qui a été choisie correspond aux implémentations d'Orinoco.

Avant de terminer cette section, l'encadré suivant introduit rapidement la norme HiperLAN et en particulier HiperLAN2, qui ont été en grande partie à la base de la norme IEEE 802.11 et plus spécifiquement de la norme IEEE 802.11a. Malheureusement, la norme européenne n'a jamais vu le jour industriellement.

HiperLAN (High Performance Local Area Network)

La normalisation des réseaux locaux sans fil, ou WLAN (Wireless Local Area Network), est assurée aux États-Unis par le groupe de travail IEEE 802.11 et en Europe par le groupe ETSI RES10, encore appelé HiperLAN.

Dans HiperLAN, les bandes de fréquences se situent entre 5 150 et 5 300 MHz, auxquelles il faut ajouter une bande de 200 MHz dans les fréquences autour de 17 GHz. Les vitesses de transfert vont de 19 à 25 Mbit/s. La distance entre les postes de travail et un point d'accès peut atteindre plusieurs centaines de mètres, mais une restriction de ces distances garantit plus facilement la qualité du service demandée par l'utilisateur. La communication peut se faire directement de station à station ou par l'intermédiaire d'un nœud central comme dans le modèle 802.11.

Sur la bande passante affectée au réseau HiperLAN, cinq canaux indépendants autorisent cinq porteuses en parallèle. La puissance d'émission est d'environ 1 watt. La modulation est de type GMSK (Gaussian Minimum Shift Keying). La redondance nécessaire pour obtenir une qualité classique dans un réseau local s'effectue *via* un code BCH (Bose-Chaudhuri-Hocquenghem). La technique d'accès au réseau local hertzien est un peu plus sophistiquée. Il s'agit d'une adaptation du CSMA/CD, appelée EY-NPMA (Elimination Yield-None Preemptive Priority Multiple Access), qui utilise les cinq canaux avec des ordres de priorité. Dans un premier temps, la station essaie d'accéder aux canaux selon un ordre dépendant de leur priorité. Une fois le problème de priorité résolu, les collisions potentielles sont annihilées par une technique de contention sur des tranches de temps préétablies. En cas de succès, la transmission s'effectue.

La couche MAC se subdivise en deux parties, la sous-couche CAC (Channel Access Control), qui correspond à la partie physique de la technique d'accès, et la sous-couche MAC, qui correspond à la partie logique. La sous-couche CAC contient toute la partie transmission et réception, qui gère les problèmes liés au canal hertzien. La partie MAC comprend la mise en forme de la trame, le routage interne, les algorithmes de confidentialité, la gestion de priorités pour assurer une qualité de service, l'insertion et le retrait des stations.

La famille HiperLAN inclut plusieurs propositions, notamment HiperLAN Type 1, destinée à une utilisation à l'intérieur des bâtiments sur des distances de l'ordre de 50 m par borne, et HiperLAN Type 2, qui étend la distance à 200 m et le débit à 25 Mbit/s au lieu de 19. Autre membre de la famille, la norme HiperAccess est beaucoup plus proche de la boucle locale classique, avec une portée maximale de 5 km et un débit de 25 Mbit/s. Cette solution devait satisfaire les entreprises de grande taille et les campus. Enfin, la norme HiperLink avait pour objectif de relier entre elles deux machines à très haut débit (155 Mbit/s) situées à une distance de 150 m avec une fréquence de 17 GHz.

Les réseaux WiMax

L'initiative WiMax est partie de l'idée de développer des liaisons hertziennes concurrentes des techniques *x*DSL terrestres. Après de longues années d'hésitation, le vrai démarrage de cette technologie a été favorisé par l'arrivée de la norme IEEE 802.16.

Avant de décrire brièvement cette norme, nous avons représenté un exemple de son utilisation à la figure 21.25.

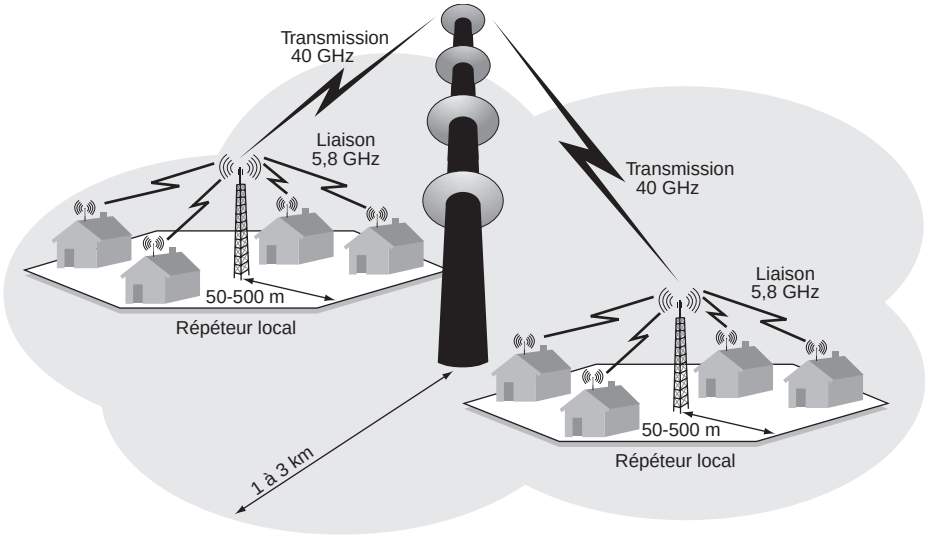


Figure 21.25
Réseau WiMax

À partir d'une antenne d'opérateur, plusieurs répéteurs propagent les signaux vers des maisons individuelles, leur donnant accès à la téléphonie et à l'équivalent d'une connexion *x*DSL. Sur la figure, la connexion à l'utilisateur se fait en deux temps, en passant par un répéteur. Il est tout à fait possible d'avoir une liaison directe entre l'utilisateur et l'antenne de l'opérateur.

Le groupe de travail 802.16 a mis en place des sous-groupes pour s'attaquer à des problèmes distincts. Le groupe de travail de base a normalisé un accès métropolitain dans la bande des 10-66 GHz, avec une vue directe entre les antennes et un protocole point-à-point. Finalisée en 2001, cette norme a été complétée par les extensions 802.16c, en 2002, qui introduit les profils système WiMax, et 802.16d, en 2004, qui apporte des correctifs, ainsi que les éléments nécessaires à une compatibilité avec la future extension 802.16e.

Une autre extension, 802.16a, sortie en 2003, concerne la bande de 2 à 11 GHz et la possibilité d'utiliser des protocoles multipoint en plus de l'environnement point-à-point de base.

802.16e a pour objectif d'étendre WiMax à des machines terminales mobiles, impliquant donc la possibilité de réaliser des connexions *x*DSL vers des mobiles. Les fréquences utilisées se situeront entre 2 et 6 GHz.

Les différences entre ces normes et extensions et 802.11 sont nombreuses. D'abord, la portée est beaucoup plus grande, puisqu'elle peut dépasser 10 km, contre quelques dizaines ou centaines de mètres pour Wi-Fi. La technologie 802.16 est en outre moins sensible aux effets multitrajet et pénètre mieux à l'intérieur des bâtiments. Elle est de surcroît mieux conçue pour assurer le passage à l'échelle sur de grandes surfaces. Pour un canal

de 20 MHz, WiMax permet enfin de faire passer un peu plus de débit, avec une meilleure qualité de service.

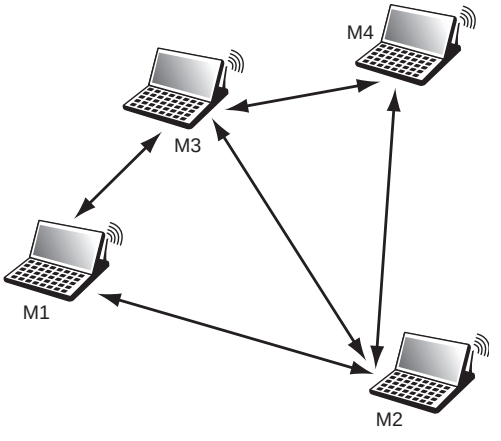
En contre-partie, les avantages de Wi-Fi résident dans son faible prix de revient, la forte réutilisation des fréquences qu'il permet et sa reconnaissance à peu près partout dans le monde.

Les réseaux ad-hoc

Une autre grande catégorie de réseaux 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 21.26.

Figure 21.26
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 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 tout 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 :

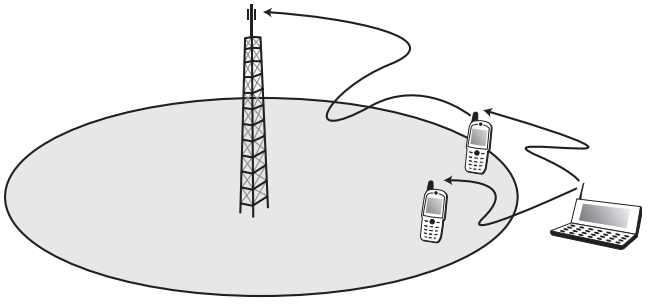
- **Protocoles réactifs.** Les terminaux ne maintiennent pas de table de routage mais s'en préoccupent lorsqu'une émission est à effectuer. Dans ce cas, on se sert essentiellement de techniques d'inondation pour répertorier les mobiles pouvant participer à la transmission.
- **Protocoles proactifs.** 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 21.27, 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 21.27
Extension de couverture par un réseau ad-hoc

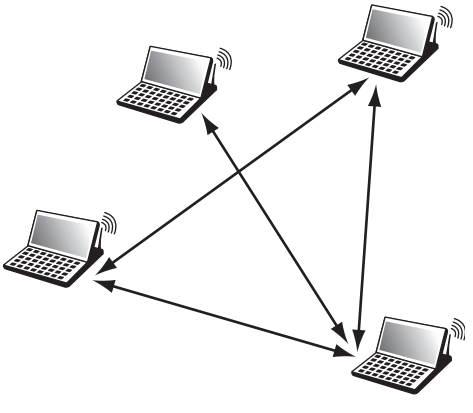


Le routage

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 21.28, 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 21.28
Communication directe entre machines d'un réseau ad-hoc

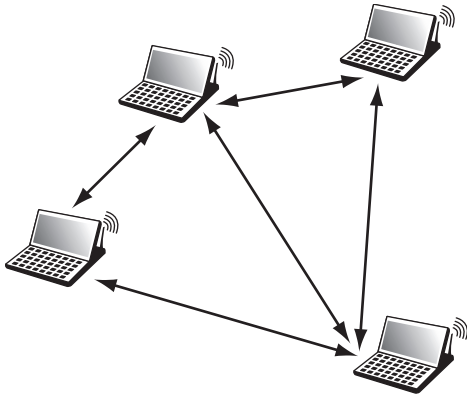


La figure 21.29 illustre le cas d'un réseau ad-hoc dans lequel, pour aller d'un nœud à un autre, il peut être nécessaire de traverser des nœuds intermédiaires. De nombreux écueils peuvent se trouver sur le chemin de la construction de la table de routage. Par exemple,

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 21.29

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 denier 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

En conclusion, si les études du groupe MANET sont assez avancées en ce qui concerne le routage, tout ou presque reste à faire pour la qualité de service, la sécurité et la consommation électrique.

Réseaux de capteurs et réseaux mesh

Cette section décrit brièvement deux environnements qui se développent rapidement, les réseaux de capteurs et les réseaux mesh (meshed networks).

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 ressource 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 est 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 et de contrôle des erreurs.

La recherche semble se diriger vers des réseaux hybrides, mêlant IP à d'autres technologies à déterminer.

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 réseaux mesh utilisent des points d'accès fixes, reliés entre eux par le même médium hertzien que les machines terminales. L'avantage de ces réseaux est de pouvoir couvrir une zone géographique importante sans avoir à poser de câble. Par exemple, sur un campus industriel, 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 obligent l'émetteur et le récepteur à baisser leur vitesse.
- 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.
- Faire appel à une norme différente pour relier les points d'accès entre eux. Par exemple, un réseau mesh 802.11b peut utiliser la norme IEEE 802.11a pour interconnecter les points d'accès.

Les réseaux mesh comme les réseaux de capteurs 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 ? faut-il émettre un peu plus fortement pour qu'un nœud ait beaucoup plus de choix pour travailler avec ces voisins ?

Des réponses à ces questions et à bien d'autres dépendront le succès ou l'échec de ces nouveaux environnements hertziens à fort potentiel.

Conclusion

Les réseaux sans fil sont devenus un marché porteur en ce début de XXI^{e} siècle. Les terminaux téléphoniques mobiles ont été les grands gagnants de la fin du XX^{e}, 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.

Références

Livre complet sur les réseaux de mobiles et les réseaux sans fil :

K. AL AGHA, G. PUJOLLE, G. VIVIER – *Réseaux de mobiles et réseaux sans fil*, 2e édition, Eyrolles, 2005

Un livre dévolu aux applications dans les réseaux sans fil :

H. P. ALESSO, C. F. SMITH – *The Intelligent Wireless Web*, Addison Wesley, 2001

Les réseaux de capteurs posent de nouveaux problèmes architecturaux et protocolaires. Le livre suivant en dresse l'inventaire :

E. H. CALLAWAY – *Wireless Sensor Networks: Architectures and Protocols*, Auerbach Publications, 2003

La sécurité est le point faible des réseaux Wi-Fi avec la qualité de service. Le livre de J. Davies fait le point sur ces questions dans l'environnement Windows :

J. DAVIES – *Deploying Secure 802.11 Wireless Networks with Microsoft Windows*, Microsoft Press, 2003

Livre intéressant par sa présentation très pédagogique du réseau Wi-Fi :

H. DAVIS, R. MANSFIELD – *The Wi-Fi Experience: Everyone's Guide to 802.11b Wireless Networking*, Que, 2001

Un excellent livre sur les applications que l'on peut mettre en place dans les réseaux sans fil :

A. DORMAN – *The Essential Guide to Wireless Communications Applications*, Prentice Hall, 2002

Un livre qui se démarque par la façon de présenter les réseaux sans fil en examinant le problème de leur mise en place dans une communauté d'intérêt :

R. FLICKENGER – *Building Wireless Community Networks*, O'Reilly, 2001

Un livre très didactique sur les réseaux 802.11 :

M. S. GAST – *802.11 Wireless Networks: The Definitive Guide*, O'Reilly, 2002

Un excellent livre sur les réseaux de capteurs :

A. HAC – *Wireless Sensor Network Designs*, Wiley, 2003

Les réseaux sans fil forment une excellente solution pour l'accès à un modem ADSL ou un modem câble dans l'environnement domotique :

P. HELTZEL – *Complete Wireless Home Networking*, Prentice Hall, 2003

Les réseaux sans fil sont souvent difficiles à architecturer, et des analyses de performance sont les bienvenues. Le livre suivant donne la plupart des outils qui peuvent être utilisés pour réaliser une étude de performance :

T. JANEVSKI – *Traffic Analysis and Design of Wireless IP Networks,* Artech House, 2003

Un bon livre technique sur la sécurité dans les réseaux d'entreprise de type Wi-Fi :

J. KHAN, A. KHWAJA – *Building Secure Wireless Networks with 802.11,* Wiley, 2003

Excellente introduction aux réseaux Wi-Fi :

J. LA ROCCA – *802.11 Demystified: Wi-Fi Made Easy,* McGraw-Hill, 2002

Un livre détaillé sur les réseaux Wi-Fi et leur ingénierie :

D. MALES, G. PUJOLLE – *Wi-Fi par la pratique, deuxième édition,* Eyrolles, 2004

L'ingénierie des réseaux Wi-Fi paraît simple. En réalité, selon la taille du réseau, la complexité augmente vite. Les règles élémentaires à mettre en œuvre sont très bien expliquées dans ce livre :

M. MALLICK – *Mobile and Wireless Design Essentials,* Wiley, 2003

La sécurité est un problème capital. Pour un lecteur intéressé plus spécifiquement par ce domaine dans les réseaux sans fil, ce livre devrait être bien perçu :

M. MAXIM, D. POLLINO – *Wireless Security,* McGraw-Hill, 2002

Un livre complet sur les réseaux ad-hoc :

C. S. R. MURTHY, B. S. MANOJ – *Ad Hoc Wireless Networks: Architectures and Protocols*, Prentice Hall, 2004

Un autre excellent livre sur la sécurité dans les réseaux sans fil :

R. K. NICHOLS, P. C. LEKKAS – *Wireless Security: Models, Threats, and Solutions,* McGraw-Hill, 2001

L'IEEE, qui gère les groupes de travail sur la normalisation du sans-fil, publie un bon livre technique sur le 802.11 :

B. O'HARA, A. PETRICK – *The IEEE 802.11 Handbook: a Designer's Companion,* IEEE Press, 1999

Un livre pour bien comprendre Wi-Fi et son installation dans l'entreprise :

F. OHRTMAN, K. ROEDER – *Wi-Fi Handbook: Building 802.11b Wireless Networks,* McGraw-Hill, 2003

Excellente approche, présentant les grands principes des technologies sans fil :

K. PAHLAVAN, P. KRISHNAMURTHY – *Principles of Wireless Networks: a Unified Approach*, Prentice Hall, 2001

Le livre de référence sur les réseaux ad-hoc :

C. PERKINS – *Ad-hoc Networking*, Addison Wesley, 2000

Un livre consacré aux communications personnelles dans un environnement sans fil :

R. PRASAD – *Universal Wireless Personal Communications,* Artech House, 1998

Très bon livre d'introduction aux réseaux sans fil :

T. S. RAPPAPORT – *Wireless Communications Principles and Practice*, Prentice Hall, 2001

Un livre orienté vers les solutions Wi-Fi Cisco :

P. ROSHAN, J. Leary – *Wireless Local-Area Network Fundamentals*, Cisco Press, 2003

Un livre d'introduction sur les réseaux sans fil, aujourd'hui un peu dépassé par le nombre de nouveaux standards arrivés sur le marché depuis sa parution :

A. SANTAMARIA, *et al.* – *Wireless LAN Systems*, Artech House, 1994

Un livre pour ceux qui veulent creuser les détails des réseaux sans fil :

C. W. SAYRE – *Complete Wireless Design*, McGraw-Hill, 2001

Un des nombreux livres de Stallings, toujours très pédagogique et complet :

W. STALLINGS – *Wireless Communications & Networks*, Prentice Hall, 2001

Un livre pratique sur WiMax. À conseiller sur cette technologie :

D. SWEENEY – *WiMax Operator's Manual: Building 802.16 Wireless Networks*, Apress, 2004

Livre complet sur les réseaux ad-hoc. Pour tous ceux qui souhaitent entrer dans les détails des protocoles de routage :

C. K. TOH – *Ad-hoc Mobile Wireless Networks: Protocols and Systems*, Prentice Hall, 2001

Pour ceux qui veulent aller plus loin sur la couche physique des réseaux Wi-Fi :

X. WANG, H. V. POOR – *Wireless Communication Systems: Advanced Techniques for Signal Reception*, Prentice Hall, 2003

Excellent livre, qui introduit surtout les réseaux sans fil de la boucle locale :

W. WEBB – *Introduction to Wireless Local Loop*, Artech House, 2000

Un très bon livre sur les réseaux de capteurs :

F. ZHAO, L. GUIBAS – *Wireless Sensor Networks*, Morgan Kaufmann Publishers, 2004