

Aperçu sur les nouvelles communications sans fil et leurs applications dans l'industrie

■ Par Jean-Pierre HAUET
Associate Partner BEA Consulting

Mots clés

Réseaux,
Radiocommunications,
Étalement de spectre,
Haut débit,
Multiplexage,
Saut de fréquence,
Wi-Fi,
Bluetooth,
Zigbee,
Wi-Max

Le développement des réseaux locaux de radiocommunications sous leurs différentes formes : Wi-Fi, Bluetooth, Zigbee, Wi-Max etc. vient perturber considérablement l'évolution du monde des communications sans fil, qui reposait sur le passage des systèmes 2G (GSM) aux systèmes 3G (UMTS). L'impact sur les applications industrielles peut être considérable.

1. Introduction

L'histoire des télécommunications est marquée par de nombreux sauts technologiques qui, tous les 20 ou 30 ans, ont permis des avancées spectaculaires. Rappelons ici simplement l'invention du télégraphe optique par Chappe (1792), celle du téléphone par Graham Bell (1876), les premières expériences de radio par Marconi (1895), l'invention du transistor, du laser, des fibres optiques, des circuits intégrés (dans les années 1947 à 1970). Plus récemment vinrent les liaisons par satellites, la numérisation de l'information et la généralisation de l'Internet.

Le développement des radiotéléphones fait partie de ces grandes avancées technologiques, marqué par la percée du téléphone cellulaire analogique (1G) puis par le fantastique succès du GSM (2G). La progression paraissait tellement naturelle que les systèmes de 3^{ème} génération

(UMTS) connurent dans leur principe un engouement incroyable, au point que des licences furent vendues dans certains pays à des prix exorbitants, avant même que la technique ne soit stabilisée et que les besoins ne soient clairement identifiés.

Mais les choses ne se sont pas passées exactement comme prévu et les nouvelles communications sans fil, objet du présent Repères, sont brusquement intervenues dans le paysage et ont fortement « modifié la donne ».

Qui sait, le recours aux Qubits, décrit dans l'article invité de Yury MUKHARSKY, fondé sur l'intrication des états quantiques des systèmes, permettra-t-il un jour une révolution d'une tout autre ampleur dans le domaine du calcul et des communications, ouvrant la voie à des applications qui relevaient jusqu'ici de la science-fiction ?

L'ESSENTIEL

Jusqu'à une date récente, l'évolution prévisible des communications sans fil était censée se faire au travers du passage des systèmes dits de 2^{ème} génération (le GSM notamment) vers les systèmes de 3^{ème} génération (UMTS). Plusieurs facteurs, technologiques et réglementaires ont permis à de nouvelles solutions (essentiellement le Wi-Fi et le Bluetooth) de voir le jour et d'étendre progressivement leur domaine d'application.

Ces solutions et leurs extensions prévisibles (le Wi-Max) constituent de plus en plus, pour l'avenir, une alternative crédible aux solutions proposées par les opérateurs traditionnels. Les industriels doivent y veiller car le sans-fil permettra, dans les systèmes de contrôle, de réaliser de nouvelles économies et d'apporter davantage de flexibilité. Mais le choix des solutions à retenir reste aujourd'hui un point d'interrogation.

SYNOPSIS

Until recently, wireless communications evolution was supposed to be an evolution from 2G solutions (mainly GSM) to 3G solutions (namely UMTS). But several factors, either technical or legal, have permitted the emergence of entirely new solutions (mainly the Wi-Fi and the Bluetooth). These solutions are progressively expanding their field of application.

Together with their foreseeable extensions (such as the Wi-Max), they constitute a credible challenge vis-à-vis the solutions implemented by the historical operators. Industry managers must pay sufficient attention to this evolution because wireless solutions will allow new savings and more flexibility in the industrial control systems. But the selection of the right solutions remains an issue.

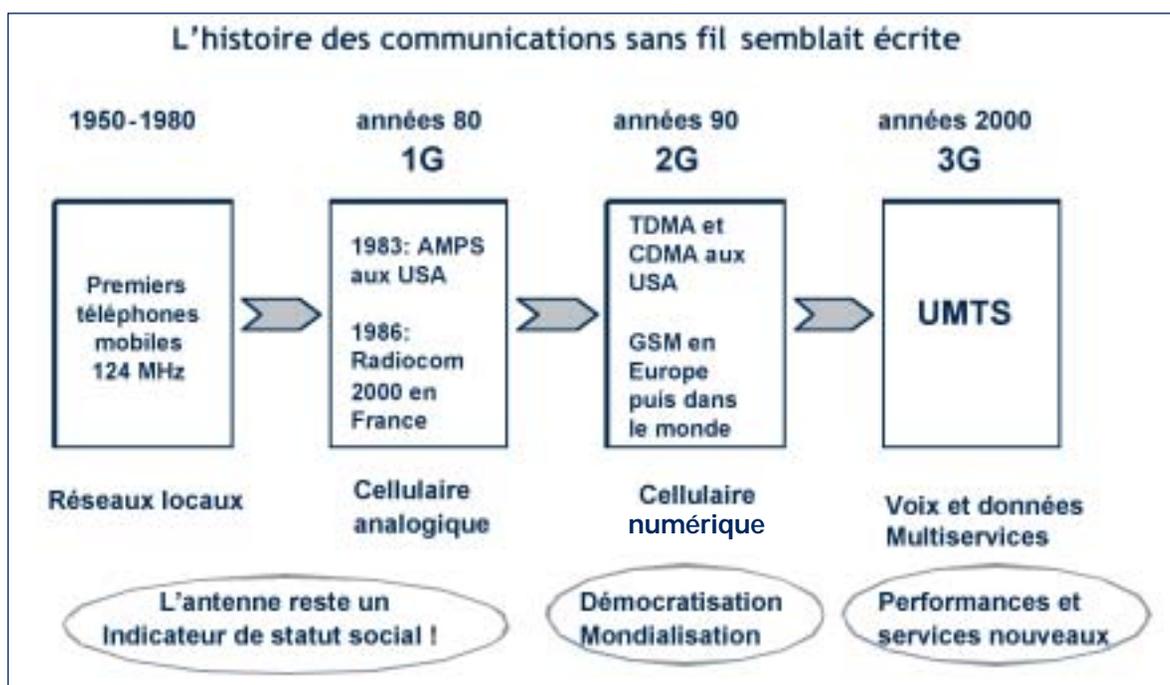


Figure 1. L'évolution programmée des radiocommunications.

2. L'histoire des communications sans fil semblait écrite

2.1. Les réseaux de première génération

Les réseaux de radiotéléphonie cellulaire de 1^{ère} génération (figure 1) connurent un très grand succès. En France, ce fut le Radiocom 2000 de Matra (1986), système analogique fonctionnant dans la bande des 400 MHz, qui marqua le début de l'itinérance et de l'universalité du numéro.

La qualité de transmission était bonne, mais l'équipement (3 000 € actuels) et les communications (0,70 € par minute) étaient chers. Le système restait réservé à une certaine élite dotée du « privilège de l'antenne ». Il répondait à une norme nationale et ne supportait pas la transmission des données. Sa sécurité était insuffisante.

Néanmoins le réseau, conçu initialement pour 300 000 abonnés, fut vite saturé : la demande de mobilité était intrinsèquement très forte.

2.2. Les réseaux de deuxième génération : le GSM

Dès 1985, les bases d'un nouveau standard étaient jetées au niveau européen par l'ETSI : celles GSM ou Groupe Spécial Mobile, devenu, succès oblige, Global System for Mobile communication en 1991. Adopté par l'ensemble des pays européens puis par 180 pays dans le monde, le GSM constitue l'une des réussites technologiques les plus marquantes de tous les temps, permettant aujourd'hui à plus d'un milliard d'êtres humains dans le

monde de converser au travers de 600 opérateurs unis par des accords de roaming.

Le GSM, comme les systèmes de 1^{ère} génération, est fondé sur une architecture cellulaire, mais c'est un système numérique reposant sur un mécanisme de multiplexage fréquentiel et temporel (FDM/TDMA) permettant d'accroître considérablement le débit utile transitant dans la bande de fréquence qui lui est allouée (900 MHz en Europe, complétée plus tard par celle des 1800 MHz).

La question de savoir si le GSM est techniquement supérieur à ses concurrents américains ou japonais fondés sur d'autres solutions d'accès au réseau (TDMA ou CDMA) a donné lieu à débat. Mais le résultat est là : le fait d'être parvenu à un accord sur un standard commun a donné à la solution européenne un fantastique élan qui lui a permis de se répandre partout dans le monde, y compris en Chine, qui est aujourd'hui le premier marché mondial du téléphone portable et même à présent aux USA où le GSM, dans la bande des 1 900 MHz, finit par émerger face aux solutions concurrentes.

Pourtant le GSM n'est pas parfait : il nécessite, en solution de base, l'établissement d'un circuit (commutation de circuit) avec un temps de latence souvent assez long. Son débit en transmission de données est faible et limité à 9,6 kbits/s dans la solution GSM Data. Il offre des possibilités de connexion à Internet médiocres et le WAP n'a jamais réussi à s'imposer. La couverture du territoire, malgré le resserrement des cellules, n'est pas dénuée de lacunes et engendre des phénomènes de « trous noirs » ou

d'interruption brutale des communications. Enfin certains continuent à soulever le problème des risques potentiels des émissions électromagnétiques pour la santé, malgré l'absence de preuve dans ce domaine.

Dans le monde industriel, le GSM a connu peu d'applications propres aux procédés, compte tenu des exigences de fiabilité, de débit et de temps garanti généralement requis.

2.3. L'UMTS : un saut technologique préprogrammé

Le succès du GSM, et en même temps ses limitations, ne laissent aucun doute dans l'esprit des grands acteurs du monde des communications sur l'intérêt de passer rapidement à une 3^{ème} génération de systèmes de radiocommunications qui soit reconnue dès le début comme un véritable standard mondial, et qui viendrait pallier les insuffisances du GSM et des autres systèmes de 2^{ème} génération.

Ainsi est né, avec une hâte d'agir proche de la précipitation, l'UMTS (Universal Mobile Telecommunications System) qui devait être le nouvel eldorado des télécommunications en permettant, grâce à une combinaison du meilleur du GSM et de ses concurrents, une utilisation optimale de la bande des 2 GHz, en offrant de nouveaux services multimédia (notamment l'Internet nomade voire mobile, la vidéo à la demande, une amélioration de la qualité de service, le fonctionnement en mode paquet ou en mode circuit, le trafic voix et données), des débits accrus (jusqu'à 2,4 Mbits/s en mode stationnaire et 384 kbits/s en mobile), une consommation électrique plus faible, un véritable lien entre le monde des communications sans fil et le monde des ordinateurs et d'Internet, avec notamment le support d'Internet IPV6.

Tout cela reste dans l'ensemble exact. Toutefois, les choses ne se sont pas déroulées comme prévu.

3. Les choses n'ont pas évolué comme prévu

- Le GSM est devenu si compétitif que le 3G a eu de facto plus de mal que prévu à s'imposer (coût des licences, coût des équipements terminaux),
- Le 3G s'est de son côté révélé plus long et plus coûteux à développer,
- Les services nouveaux résultant de la bande passante offerte par le 3G sont devenus d'un intérêt moins évident,
- La liaison avec le monde IP est devenue un impératif essentiel, pour le transfert des données et pour la voix (VoIP),
- La continuité avec les réseaux filaires Ethernet 802.3 est devenue un must,
- La demande de transmission en mode paquet est devenue de plus en plus pressante (succès foudroyant des SMS),

- De nouveaux progrès techniques ont été réalisés dans les VLSI CMOS :
 - Aptitude à fonctionner à très haute fréquence (comme les composants AsGa),
 - Baisse continue des prix (effet « Centrino »),
- Avec la fin de la guerre froide, de nouvelles bandes de fréquences ont été libérées par les armées dans la plupart des grands pays industrialisés,
- De nouveaux standards internationaux, sur lesquels nous reviendrons, ont vu le jour sous l'égide de l'IEEE, au sein notamment du comité IEEE 802 (Local & Metropolitan Area Network Standard Committee),
- Un concept nouveau, celui des communications nomades, qui est venu s'intercaler entre ceux des communications fixes et des communications mobiles.

4. Les conséquences de l'évolution du contexte

Cette évolution du contexte a eu deux conséquences principales :

- Le développement de variantes du GSM (appelées souvent solutions 2,5 G)
- Le développement des réseaux locaux radioélectriques ou RLAN.

4.1. Les variantes du GSM

Elles sont essentiellement au nombre de deux : le GPRS et l'EDGE.

Le GPRS

Le GPRS (General Packet Radio Service) est la première application d'un système à commutation de paquets fondé sur le GSM. Son débit théorique est de 160 kbits/s, dans la pratique de 40 kbits/s. Il permet des connexions permanentes (« immediacy »), l'accès rapide à Internet, le paiement en fonction de la quantité de données transmises. En bref, il contourne des limitations du GSM Data (9,8 kbits/s) et des SMS (160 caractères maxi).

L'EDGE

L'EDGE (Enhanced Data rate for GSM Evolution) est un perfectionnement du GPRS qui améliore à la fois le mode paquet et le mode circuit. Il permet, grâce à une technique de modulation plus performante (8-PSK), d'atteindre un débit théorique de 473,6 kbits/s sur 8 canaux (dans la pratique 384 kbits/s, ce qui génère souvent certaines confusions avec l'UMTS).

Sommairement dit, l'EDGE multiplie les performances du GPRS par trois dans l'attente de l'UMTS qui multiplierà à nouveau les performances par trois.

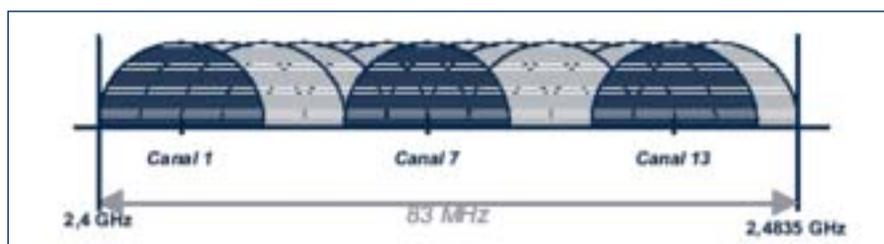


Figure 2. La bande ISM des 2,4 GHz.

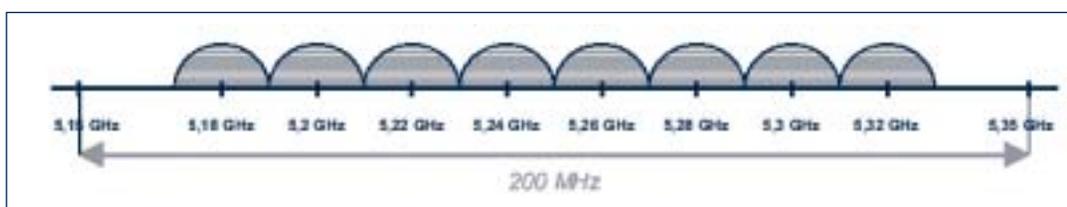


Figure 3. La bande UN-II des 5 GHz (bande inférieure).

4.2. Les réseaux locaux radioélectriques (RLAN)

Le développement des RLAN constitue la donnée véritablement nouvelle de ces toutes dernières années. Ces RLAN (appelée aussi WLAN, pour Wireless Local Area Networks) prennent différentes formes selon la nature des applications et en particulier la distance desservie :

- Personal Area Networks (PAN)
- Vehicle Area Networks (VAN)
- Local Area Networks (LAN)
- Metropolitan Area Networks (MAN)
- Wide Area Networks (WAN)

Le développement des RLAN s'explique par plusieurs considérations :

- L'intérêt pour la mobilité et/ou le nomadisme,
- Les fonctionnalités nouvelles offertes,
- La souplesse dans les architectures
 - réseaux d'infrastructure,
 - réseaux ad-hoc,
- Les progrès techniques, l'amélioration des performances, la diminution des coûts et de l'encombrement,
- Les nouvelles formes de concurrence vis-à-vis des réseaux en place, et la pression sur les prix qu'elles génèrent.

Mais quelles solutions techniques vont s'imposer pour supporter ces RLAN ? Quel marché vont-ils conquérir ? Quelles applications industrielles peuvent-ils avoir ? Comment vont-ils coopérer avec les réseaux traditionnels, et en particulier les réseaux de 3^{ème} génération ? Telles sont quelques-unes des questions auxquelles le présent Repères cherche à répondre.

5. Les nouvelles bandes de fréquence

Deux bandes de fréquence ont été libérées dans la plupart des pays industrialisés : la bande des 2,4 GHz et la bande des 5 GHz.

5.1. La bande ISM (Industrial, Scientific, Medical) des 2,4 GHz

14 canaux de 20 MHz de 2 400 à 2 483,5 kHz.

Attention :

- seuls trois canaux sont sans recouvrement,
- les canaux ouverts ne sont pas les mêmes dans tous les pays.

5.2. La bande UN-II (Unlicensed National Information Infrastructure) des 5 GHz

Cette bande, au régime voisin de celui de l'ISM, se décompose en fait en plusieurs bandes dont les statuts varient encore selon les pays, y compris en Europe, nonobstant une recommandation de la Commission européenne du 20 mars 2003.

La partie basse de la bande (5 150 à 5 350 MHz) est la plus largement ouverte. Elle est divisée en 8 canaux de 20 MHz qui, à la différence de ceux délimités dans la bande des 2,4 GHz, sont indépendants. C'est elle qui, on le verra plus loin, supporte la norme 802.11a.

La partie haute (5 470 à 5 725 MHz) est destinée à être ouverte dans la plupart des pays, mais ne l'est pas encore en France.

La décision de l'autorité de régulation (ART) du 25 juillet 2003 conduit à la situation suivante pour la France métropolitaine (tableau 1).

Puissances maximales autorisée en France		
	Fréquence centrale (MHz)	Fréquence centrale (MHz)
2400-2454 MHz	100 mW	100 mW
2454-2483,5 MHz		10 mW
5150-5250 MHz	200 mW	Impossible
5250-5350 MHz	200 mW avec DFS/TPC (*) 100 mW avec DFS seul	Impossible
5470-5725 MHz	Impossible	Impossible
5725-5825 MHz	Impossible	Impossible

Tableau 1 : Puissances maximales autorisées en France métropolitaine pour les RLAN selon la décision de l'ART du 25 juillet 2003.
(*) DFS : Dynamic Frequency Selection – TPC : Transmit Power Control

- Encombrement des fréquences → étalement de spectre et multiplexage- brevet Hedy Lamarr¹ et George Antheil (pianiste) de 1941 (US patent 2.2292.387),
- Problèmes de propagation, fading, interférences, trajets multiples, trous noirs etc. → techniques FHSS, DSSS, OFDM,
- Amélioration des débits → nouvelles techniques de modulation,
- Conflits d'accès → CSMA/CA (au lieu de CSMA/CD - Avoidance au lieu de détection) - ALOHA - Slotted ALOHA - TDMA,
- Nomadisme et mobilité → l'itinérance reste un point faible par rapport aux réseaux administrés. Le nomadisme est beaucoup plus facile à réaliser que la mobilité pure.
- Sécurité : intrusion, interception des données, brouillage, dénis de service → des progrès restent à accomplir. L'adoption de la norme 802.11.i en juin 2004 marque une étape importante mais il faut d'abord utiliser les techniques existantes.
- Multiplication des standards → c'est un peu la jungle. Une nouvelle guerre des « fieldbus » est possible mais l'IEEE jouit d'une autorité reconnue.

Tableau 2 : Quelques-uns des problèmes soulevés par les RLAN.

La situation est en fait très évolutive et dans tout projet de RLAN, il y a lieu de s'enquérir soigneusement des règles applicables dans le pays considéré. On notera par exemple qu'aux Etats-Unis la puissance autorisée dans la bande ISM 2,4 GHz atteint 1 W (contre 100 mW) en France) et que la bande des 5 GHz y est largement ouverte alors qu'en France elle s'entrouvre à peine. L'ouverture d'une troisième bande en Unlicensed Band de 3 650 à 3 700 MHz donne en outre lieu actuellement à une enquête préliminaire aux USA.

5.3. Les problèmes à résoudre

Malgré les progrès accomplis, les RLAN posent des problèmes sérieux dans leur mise en œuvre. Les réponses techniques apportées font que les limites d'utilisation sont continuellement reculées, mais il faut garder présent à l'esprit que les liaisons sans fil présentent des aléas de mise en œuvre, qui semblent parfois échapper à toute rationalité, et que les performances réelles, notamment en termes de portée, sont souvent très inférieures à celles qui

sont annoncées pour des conditions de propagation optimales (notamment en vision directe ou LOS : Line Of Sight).

Le tableau 2 liste quelques-uns de ces problèmes avec les réponses qui peuvent être apportées.

6. Les solutions en présence

Le tableau 3 rassemble les principales solutions actuellement commercialisées et qui sont industriellement validées. Le tableau 4 regroupe quant à lui celles qui sont aujourd'hui au stade du développement, et susceptibles d'apporter des améliorations significatives en termes de performances.

Il conviendrait en outre de mentionner les solutions « en extinction », parfois avant d'avoir vu le jour comme Home-RF (supplannée par 802.11.b et Bluetooth) et l'Hiperlan/2, projet de l'ETSI qui a de facto convergé avec 802.11.a.

¹ Hedy Lamarr fut une actrice célèbre des années 30. Elle fut la première actrice à jouer nue dans un film (Extase -1933). Elle fut mariée six fois et épousa notamment un fabricant de torpilles dont le guidage posait problème. Hedy Lamarr apporta la solution après discussion avec son voisin, le pianiste-compositeur George Antheil, qu'elle avait consulté en raison de ses connaissances en endocrinologie, étant désireuse de donner davantage d'ampleur à sa poitrine... Ni l'un ni l'autre ne touchèrent jamais aucune royauté sur leur invention qui reste au cœur des télécommunications modernes.

	WI-FI IEEE 802.11	Bluetooth IEEE 802.15.1	IEEE 802.15.4
Bande des 2,4 GHz	802.11.b 802.11.g 802.11.g turbo (non standardisée)	Bluetooth 1.1	Zigbee
Bande des 5 GHz	802.11.a (surtout aux USA)		
Perfectionnements	802.11.i		
Applications	LAN	PAN et VAN	PAN et LAN

Tableau 3. Les solutions RLAN disponibles industriellement.

	WI-FI IEEE 802.11	Bluetooth IEEE 802.11	IEEE 802.15.3	IEEE 802.16-2004 802.16. e	WI-FI IEEE 802.11
Bande des 2,4 GHz	Perfectionnements:	Bluetooth 1.2	Wi-Media		
Bande des 5 GHz	802.11.e 802.11.f 802.11.h			2 à 11 GHz Wi-Max	
Bande des 3,1 à 10,6 GHz					ULB
Applications	LAN		PAN et LAN	MAN et LAN	PAN et LAN

Tableau 4. Les solutions RLAN en cours de développement.

Le choix entre ces diverses solutions n'est pas toujours évident ; plusieurs critères doivent être pris en compte parmi lesquels :

- La bande de fréquence (la bande des 2,4 GHz est très encombrée),
- La technique de codage (DSSS, FHSS, OFDM),
- La technique d'accès (CSMA/CA, ALOHA, TDMA),
- L'aptitude à s'organiser spontanément en réseau,
- La consommation d'énergie des terminaux,
- La sensibilité aux interférences et autres perturbations,
- Le niveau de sécurité (résistance à la malveillance) et la fiabilité,
- L'existence de couches supérieures à TCP (couche OSI 4) permettant d'assurer l'interopérabilité,

et bien entendu :

- Le débit,
- La portée.

Ces critères ne sont pas indépendants et doivent eux-mêmes donner lieu à approfondissement. Ainsi le débit généralement annoncé pour la solution Wi-Fi de base est-il de 11 Mbits/s, mais ce débit est un débit maximal et, en fonction de la qualité de la transmission, le système se repositionne de lui-même sur des niveaux plus bas (5,5, 2 ou même 1 Mbits/s) par changement de technique de modulation.

En outre, pour les solutions en développement, il ne faut pas confondre standard ou projet de standard avec solution industriellement éprouvée. On a bien vu avec les systèmes 3G la distance qui sépare un standard adopté dans l'euphorie générale d'un succès industriel et commercial.

Parmi toutes ces techniques, outre le choix de la bande de fréquence, l'un des facteurs-clés de différenciation

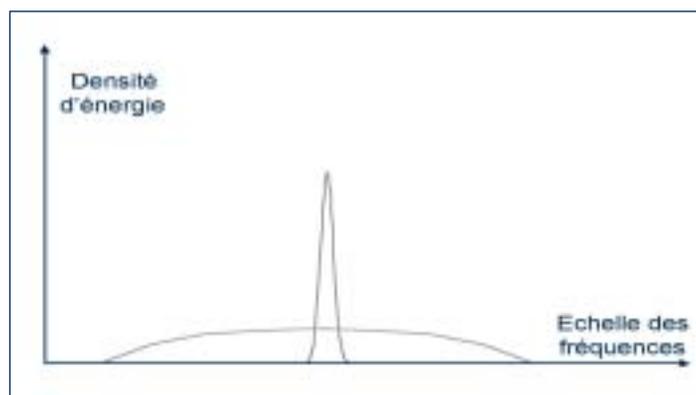


Figure 4. Principe de l'étalement de spectre.

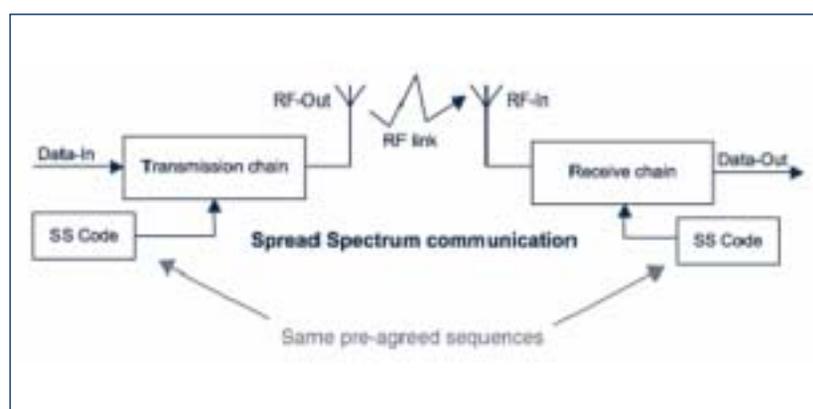


Figure 5. Codage et décodage par séquence pseudo-aléatoire

réside dans la solution utilisée pour utiliser au mieux cette bande de fréquence, c'est-à-dire le choix de la technique d'étalement de spectre ; ces techniques d'étalement de spectre, nées de l'invention Lamarr-Antheil, relèvent de la couche physique, mais reposent sur les mêmes principes que ceux qui différencient, au niveau de la couche 2, les différents systèmes de communication mobile passés rapidement en revue précédemment (TDMA, FDMA, CDMA).

7. Aperçu sur les techniques de codage

Les fréquences sont une denrée rare. Mais, paradoxalement, c'est en étalant les fréquences que l'on tire le meilleur parti du spectre. Les transmissions en bande étroite conduisent à un gaspillage des ressources et sont sensibles aux perturbations de toute nature (bruit et réflexions notamment).

Le théorème de Shannon-Hartley :

$C = B \times \log_2(1 + S/N)$ où C est la capacité de transmission du canal en bits/s, B la largeur du canal et S/N le rapport signal/bruit, conduit à étaler le signal sur une bande de fréquences plus large, dans des conditions permettant :

- 1- de séparer à la réception le signal pertinent du bruit, quelle qu'en soit l'origine,
- 2- de multiplexer plusieurs utilisateurs sur la même bande.

L'étalement (figure 4) se fait en conditionnant le signal à transmettre par un autre signal pseudo-aléatoire (mais connu du récepteur) de fréquence plus élevée. À la réception, l'opération inverse permet de récupérer le signal à l'exclusion des signaux parasites introduits en cours de route qui n'ont pas été codés par le code pseudo-aléatoire (PRN).

Selon le niveau où se fait l'étalement de spectre dans la chaîne de transmission, on distingue :

- le Direct Sequence Spread Spectrum (DSSS),
- le Frequency Hopping Spread Spectrum (FHSS),

DSSS et FHSS sont voisines dans leurs principes des méthodes d'accès CSMA et FDMA.

DSSS

En DSSS, l'étalement se fait en appliquant en entrée à chaque bit une séquence pseudo-aléatoire de Barker, de

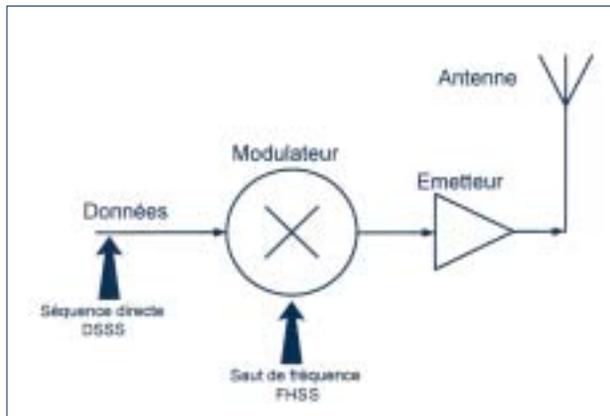


Figure 6. Différentes méthodes d'étalement de spectre.

Gold, d'Hadamard-Wallsh etc. (figure 7) qui permet de redonder l'information dans un « chip » ou « pattern » composé de n bits élémentaires.

En sortie, le « désétalement » se fait en appliquant le même vecteur. Les vecteurs utilisés sont orthogonaux, ce qui permet de séparer en sortie les informations propres à chaque utilisateur. La modulation se fait en restant à l'intérieur du même canal.

Le DSSS permet un débit élevé, une durée d'établissement courte, mais nécessite des composants rapides.

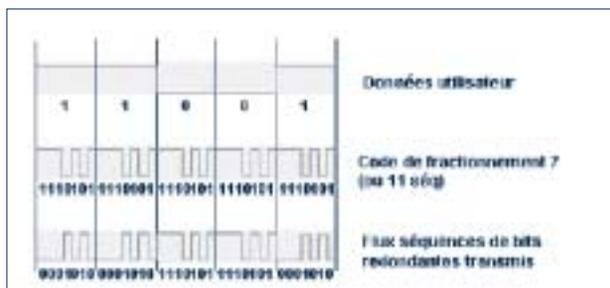


Figure 7. Étalement par un vecteur de longueur 7.

FHSS

Le FHSS (Figure 8) utilise un signal à bande étroite mais qui change continuellement et rapidement de canal (sauts de fréquence). Les sauts de fréquence s'accompagnent généralement d'un multiplexage temporel (TDMA) pour permettre la coexistence de plusieurs utilisateurs.

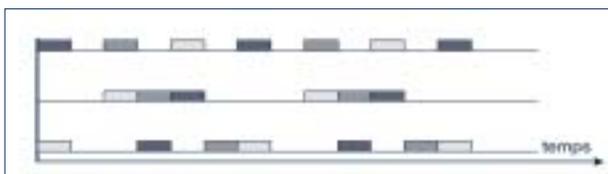


Figure 8. Sauts de fréquence accompagnés d'un multiplexage temporel.

Plus simple, de meilleure portée et moins sensible aux interférences que le DSSS mais de débit moindre, le saut de fréquence requiert une synchronisation émission-réception très fine.

OFDM (Orthogonal Frequency Multiplexing)

L'OFDM est une forme évoluée de multiplexage par division de fréquence, dans laquelle chaque canal est divisé en un grand nombre de sous-canaux, avec des porteuses de fréquences rapprochées (typiquement 300 kHz) mais orthogonales.

Les signaux rectangulaires d'entrée sont modulés par une IDFT (Inverse Discrete Fourier Transform) qui les transforme en onde de forme $\sin x/x$.

OFDM présente deux avantages essentiels :

- L'orthogonalité des sous-porteuses et l'usage d'IDFT permettent de discriminer les canaux beaucoup mieux qu'en FHSS classique (figure 10).
- L'utilisation de pulses rectangulaires permet d'ajouter un intervalle de garde ζ compensant l'étalement ζ dû aux multitrajets si $\zeta < \Delta$.

Découverte dans les années 50, l'OFDM est utilisée dans les standards 802.11.a et 802.11.g, dans l'ADSL et dans les techniques nouvelles de courants porteurs. Le W-OFDM est un perfectionnement de l'OFDM incluant des mécanismes de correction d'erreurs.

8. Les solutions IEEE 802.11

8.1. Le standard originel (1997)

Le standard initial 802.11, publié en 1997, prévoyait 3 couches physiques, infra-rouge, DSSS et FHSS, et une vitesse de transfert de 2 Mbits/s pour les couches physiques DSSS et FHSS dans la bande ISM des 2,4 GHz (figure 12).

8.2. Le 802.11.b

Le succès du Wi-Fi (802.11.b) tient à l'amélioration de ses performances et à la continuité d'acheminement qu'il permet par rapport à l'Ethernet conventionnel (802.3), d'où son appellation commune « d'Ethernet sans fil ».

Le 802.11. b opère dans la bande des 2,4 GHz en DSSS. Son débit maximal est de 11 Mbits/s mais celui-ci est ramené automatiquement à 5,5, 2 ou 1 Mbits/s, selon la qualité de l'environnement radio (murs, interférences, reliefs, chemins multiples etc.), par adaptation du type de modulation.

L'un des inconvénients de ce mécanisme est que l'ensemble du réseau s'aligne sur la « cadence » imposée par l'abonné dont les conditions d'émission et de réception sont les plus médiocres. Il faut donc veiller dans la

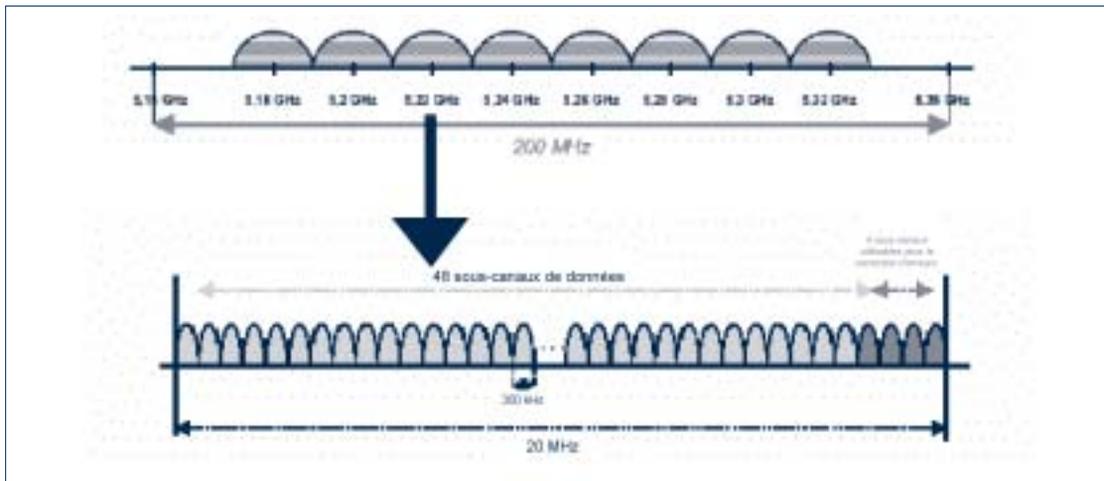


Figure 9. Utilisation des canaux en OFDM.

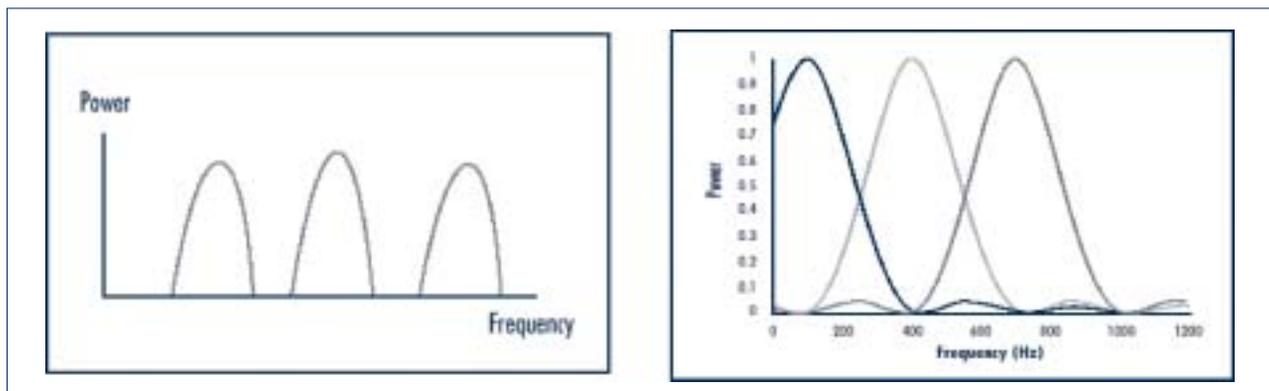


Figure 10. Discrimination des signaux de sortie en multiplexage de fréquences (à gauche) et en OFDM (à droite).

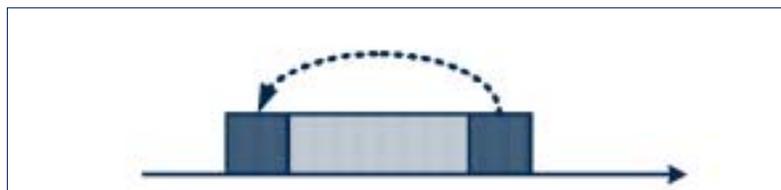


Figure 11. Introduction d'un intervalle de garde pour prendre en compte les trajets réfléchis.

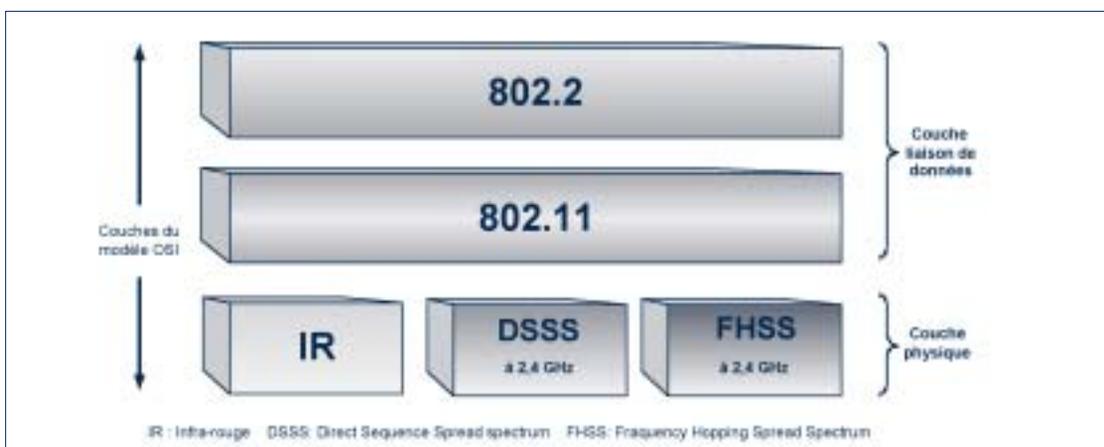


Figure 12. Structure du standard originel 802.11.

À l'intérieur		À l'extérieur	
Vitesse Mbits/s	Portée (en m)	Vitesse Mbits/s	Portée (en m)
11 Mbits/s	50 m	11 Mbits/s	200 m
5,5 Mbits/s	75 m	5,5 Mbits/s	300 m
2 Mbits/s	100 m	2 Mbits/s	400 m
1 Mbits/s	150 m	1 Mbits/s	500 m

Tableau 5. Zone de couverture du 802.11.b.

conception d'un réseau à ce que chaque abonné soit placé dans des conditions relativement similaires si l'on veut atteindre les performances escomptées.

Celles-ci demeurent très aléatoires. On trouve dans la littérature les données du tableau 5.

Dans la pratique, les distances sont souvent très inférieures et des zones d'ombre très locales peuvent apparaître. Il faut aussi se rappeler que la puissance d'émission autorisée en France est le dixième de celle permise aux USA.

Les avantages du 802.11.b tiennent au fait qu'il s'agit d'une technologie mature, de faible coût (un point d'accès coûte environ 65 €, une carte PCM-CIA 27 €, une clé USB 40 €).

Les inconvénients du 802.11.b résident dans la qualité de services incertaine (problèmes de propagation, d'interférences, faiblesses de la couche MAC CSMA/CA, qui entraîne un alignement sur le débit imposé par la station la plus éloignée), le niveau de sécurité médiocre (algorithme de codage WEP en version de base), la consommation d'énergie, l'itinérance limitée, l'encombrement de la bande des 2,4 GHz, l'absence de couches supérieures normalisées.

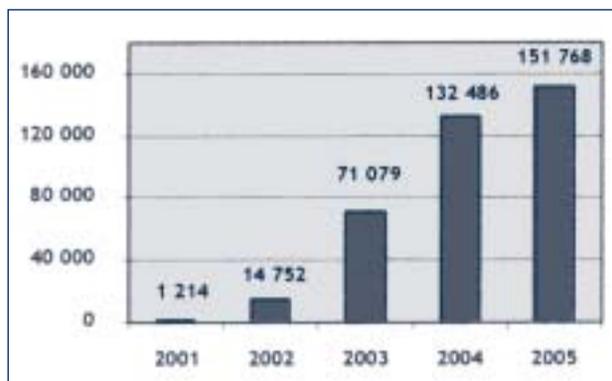


Figure 13. Evolution du nombre de bornes Wi-Fi dans le monde selon le Gartner Group.

Toutefois les « hot-spots » se sont développés très rapidement (figure 13) et le Wi-Fi, à défaut d'être une solution industrielle, permet de se familiariser avec les technologies sans fil, et peut être considéré dans toutes les applications où la qualité de service n'est pas un facteur critique.

8.3. Le 802.11.g

Le 802.11.g est le plus récent des standards 802.11 (2003) mais déjà le plus répandu. Il s'agit d'un « upgrade » du 802.11.b en mode OFDM, toujours dans la bande ISM 2,4 GHz. Il permet un débit allant de 6 à 54 kbits/s. La compatibilité avec le 802.11.b est assurée grâce à la fonction « request to sent/clear to send » du CSMA/CA.

Les avantages du 802.11.g résident dans le fait qu'il s'agit d'une technologie elle aussi mature et à faible coût. Les produits mixtes b/g sont à peine plus chers que les produits b. La technique de codage est plus robuste, le débit de données plus élevé et le standard est reconnu et adopté en particulier par Apple dans son offre « Airport Extreme ».

Mais le 802.11.g reste tributaire de la bande des 2,4 GHz et présente les mêmes limites que le 802.11.b en ce qui concerne la sécurité.

8.4. Le 802.11.a

Le 802.11.a est parfois appelé Wi-Fi 5. Il fonctionne dans la bande des 5 GHz (aux USA, dans les trois sous-bandes ouvertes soit sur 600 MHz – en France dans la sous-bande inférieure de 5 150 à 5 350 MHz). Le codage est en OFDM. Les débits théoriques sont de 6, 9, 12, 18, 24, 36, 48 et 54 kbits/s.

Historiquement, le concept est né avant le 802.11.b. Son développement a été freiné par le succès de ce dernier. Mais le 802.11.a a retrouvé de l'intérêt du fait de la saturation de la bande des 2,4 GHz et des performances offertes par l'OFDM. La technologie est disponible et

Vitesse Mbits/s	802.11b	802.11a	802.11g
Débit max en Mbits/s	11	54	54
Type de modulation	Barker et CCK	OFDM	CCK et OFDM
Débits supportés	1, 2, 5.5, 11 Mbits/s	6, 9, 12, 18, 24, 36, 48, 54 Mbits/s	OFDM: 6, 9, 12, 18, 24, 36, 48, 54 Mbits/s Barker et CCK: 1, 2, 5.5, 11 Mbits/s
Bandes de fréquence	2.4–2.497 GHz	5.15–5.35 GHz 5.425–5.675 GHz 5.725–5.875 GHz	2.4–2.497 GHz

Tableau 6. Comparaison des technologies 802.11 (valide aux USA seulement).

des produits « tribandes » (a, b, g) apparaissent sur le marché. La solution 802.11.a est attractive aux USA où les bandes de fréquence ouvertes sont beaucoup plus larges qu'en Europe et où la FCC autorise une puissance d'émission de 800 mW en bande inférieure. Du fait de la combinaison « 5 GHz + OFDM », la solution est plus industrielle et moins grand public. Toutefois son avenir reste incertain en Europe où son marché demeure limité.

Le tableau 6 récapitule les principales données relatives aux solutions 802.11, sachant que les données demeurent fortement évolutives et diffèrent d'un pays à l'autre.

8.5. Les améliorations sur le 802.11

De nombreux groupes de standardisation travaillent actuellement sur les améliorations à apporter aux solutions 802.11. Il est impossible ici d'en donner une vision exhaustive.

Un point essentiel concerne la sécurité, longtemps considérée comme le maillon faible des solutions Wi-Fi. L'article de M. Laurent BUTTI développe ce sujet et montre les progrès rendus possibles par l'adoption en juin 2004 du standard 802.11.i.

Le 802.11.i remplace le WEP (Wired Equivalent Privacy) par l'AES (Advanced Encryption Standard) ou le TKIP (Temporal Key Integrity Protocol). Dans le cadre du 802.11.i, la solution vise à intégrer dans les trames Internet le protocole d'authentification EAP (Extensible Authentication Protocol) permettant d'utiliser des serveurs d'authentification (Radius, Kerberos). Sans attendre l'application intégrale du standard 802.11.i, depuis septembre 2003, les produits certifiés Wi-Fi doivent répondre aux spécifications WPA (Wi-Fi Protected Access).

Les autres améliorations en cours portent principalement sur :

- **La qualité de service** : la couche MAC actuelle (CSMA/CA) n'assure pas de qualité de service. 802.11.e

visé à compléter CSMA/CA pour permettre des transmissions synchrones (voix sur IP).

- **Le roaming** : 802.11.f définira les règles de dialogue entre bornes d'accès pour permettre les changements de points d'accès (itinérance).

9. Bluetooth

Bluetooth est une solution initiée par le Bluetooth Special Interest Group (plus de 2 000 membres) afin d'éliminer les liaisons filaires dans les téléphones portables et se substituer aux liaisons infra-rouges. Les couches basses (physiques et liaisons de données) sont à présent normalisées par l'IEEE sous la référence IEEE 802.15.1.

Les couches supérieures demeurent propres au SIG mais constituent l'un des points forts de Bluetooth, qui est un système de communication complet conçu pour l'interopérabilité entre équipements, supportant voix et données.

- Couche physique : bande ISM 2,4 GHz en FHSS : 1 600 sauts de fréquence par seconde sur 79 canaux de 1 MHz (protection contre les interférences),
- Débit : 723 kbps,
- Portée standard: 10 m en solution de base mais la norme prévoit 3 classes:
 - PC space: 10 mètres et +
 - Office: 25 mètres et +
 - Entreprise: 100 mètres et +

Les architectures de réseau Bluetooth sont de deux types : les « piconets » et les « scatternets ».

Les « piconets » sont des microréseaux qui se forment spontanément autour d'une station qui prend le rôle de maître. Un « piconet » comprend 8 stations au plus. Toutes les communications passent par le maître qui assure la synchronisation de l'ensemble (figure 14).

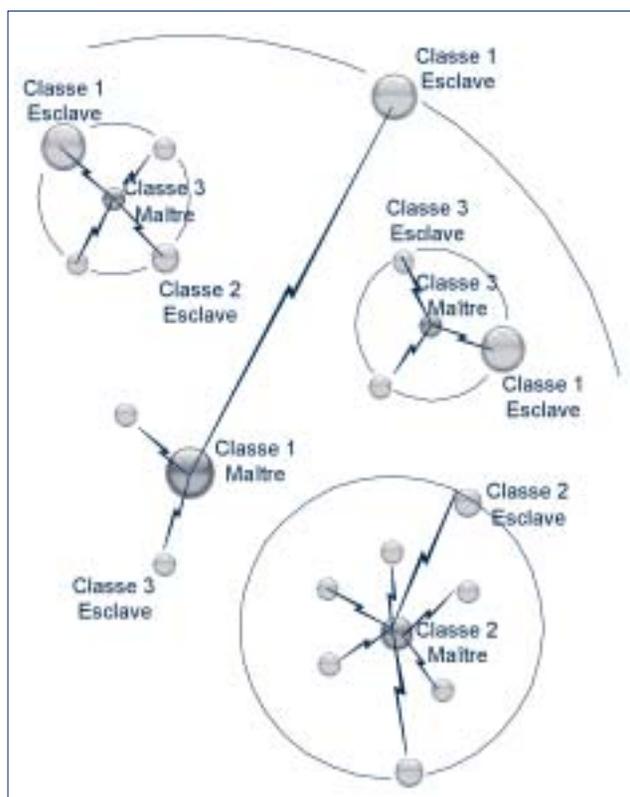


Figure 14. Architectures Piconet Bluetooth.

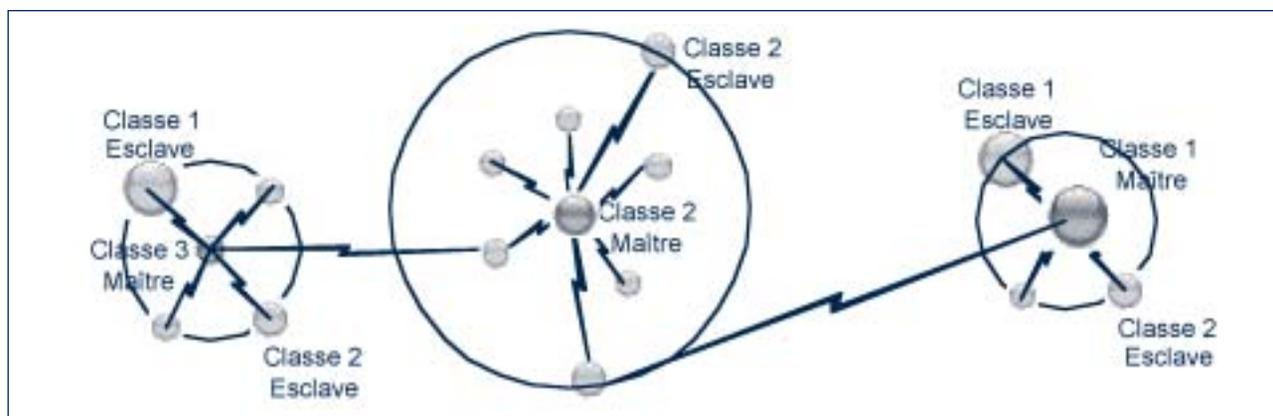


Figure 15. Architecture Scatternet Bluetooth.

Lorsqu'une station ne peut s'insérer dans un « piconet » existant du fait de sa saturation ou de son éloignement, elle peut négocier avec la station la plus proche la formation d'un « scatternet » formé de plusieurs « piconets », non synchronisés entre eux (figure 15).

Les avantages de Bluetooth sont nombreux :

- Technologie mature et bon marché (clé USB 15 mètres à 25 €),
- Des composants disponibles à bas prix,
- Faible consommation,
- Bonne résistance aux interférences (mais il y a nécessairement des interférences possibles avec les signaux Wi-Fi dans la bande des 2,4 GHz),
- Adopté par le monde des télécoms et de l'automobile,
- Souplesse dans les architectures,
- Fonctionne par circuit et par paquet,
- Meilleure sécurité que Wi-Fi (avant WPA) au niveau de l'authentification et de l'interception des données (utilisation de l'algorithme E0 au lieu de RC4, dans le WEP).

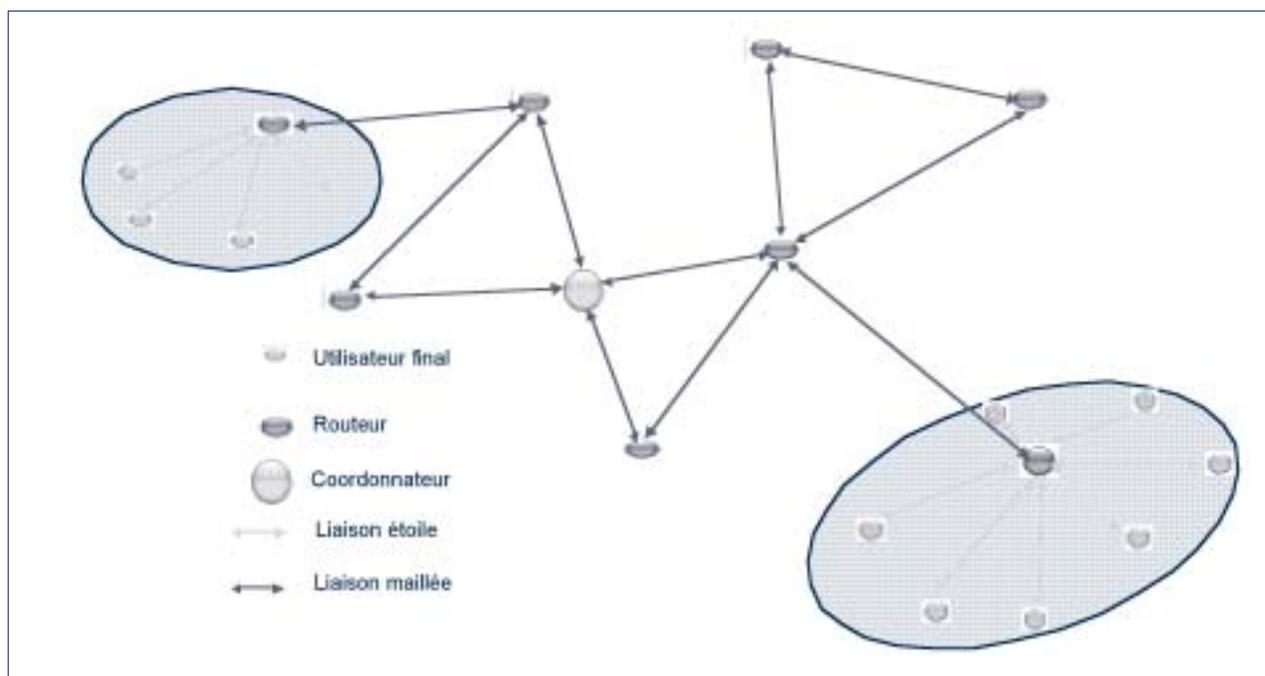


Figure 16. Exemple d'architecture ZigBee

Bluetooth reste très orienté vers les mondes télécom, informatique, médical, jeux, mais un sous-groupe « Industrial Automation » existe au sein du Bluetooth SIG et des applications industrielles pour la lecture des codes barres et le contrôle de position (via GPS et des PDA) se développent. Toutefois le positionnement sur la bande ISM des 2,4 GHz est une faiblesse, du fait notamment des interférences possibles avec Wi-Fi, malgré les avantages procurés par le saut de fréquence. Par ailleurs, le volume de mémoire requis est relativement important.

Mais Bluetooth évolue, la version 1.2 offrira :

- Un saut de fréquence adaptatif qui réduit les interférences,
- Une accélération des procédures de reconnaissance et de couplage.

Enfin, une évolution est prévue vers 2 et 3 Mbits/s .

10. ZigBee

Bénéficiant de l'héritage d'Home-RF, ZigBee est une solution nouvelle, encore assez peu connue, mais soutenue par un consortium regroupant de puissants industriels (Motorola, Honeywell, Invensys, Mitsubishi, Philips etc.).

Les couches 1 et 2 ont été standardisées par l'IEEE sous la référence 802.15.4. Mais, comme Bluetooth, il s'agit d'une solution complète, visant à bâtir des architectures interopérables, notamment pour les applications domestiques et les secteurs des automatismes industriels.

L'article de M. Cyril Zarader décrit en détail cette

solution et ses applications potentielles. On se contentera de souligner à ce stade quelques caractéristiques-clés :

- Fonctionnement essentiellement dans la bande ISM 2,4 GHz (16 canaux de 5 MHz) mais aussi à 915 MHz (USA) et à 868,3 MHz (Europe),
- Vitesse de 255 kbits/s sur 30 mètres.
- Très faible consommation d'énergie, les stations étant en sommeil plus de 97% du temps,
- Accès CSMA/CA, mais avec un slot périodique réservé au trafic garanti,
- Temps de latence très court,
- Architectures « peer to peer », « tree » ou « mesh » pilotée par un maître (figure 16).

Les avantages de ZigBee résident dans sa très faible consommation (hormis celle du coordonnateur de réseau), son orientation industrielle, la diversité des architectures possibles. Mais le fonctionnement à 2,4 GHz reste un inconvénient et, dans le domaine de l'automatisation industrielle, se pose la question du raccordement de cette solution avec les nombreux réseaux de terrain qui coexistent actuellement sur le marché (Profibus, Fieldbus Foundation, etc.). Le futur de ZigBee n'est donc pas acquis et en particulier l'évolution de son positionnement par rapport à Bluetooth est à suivre.

11. UWB (Ultra Wide Band)

Parmi les solutions en développement, les techniques à très large bande figurent en bonne position. Elles ont

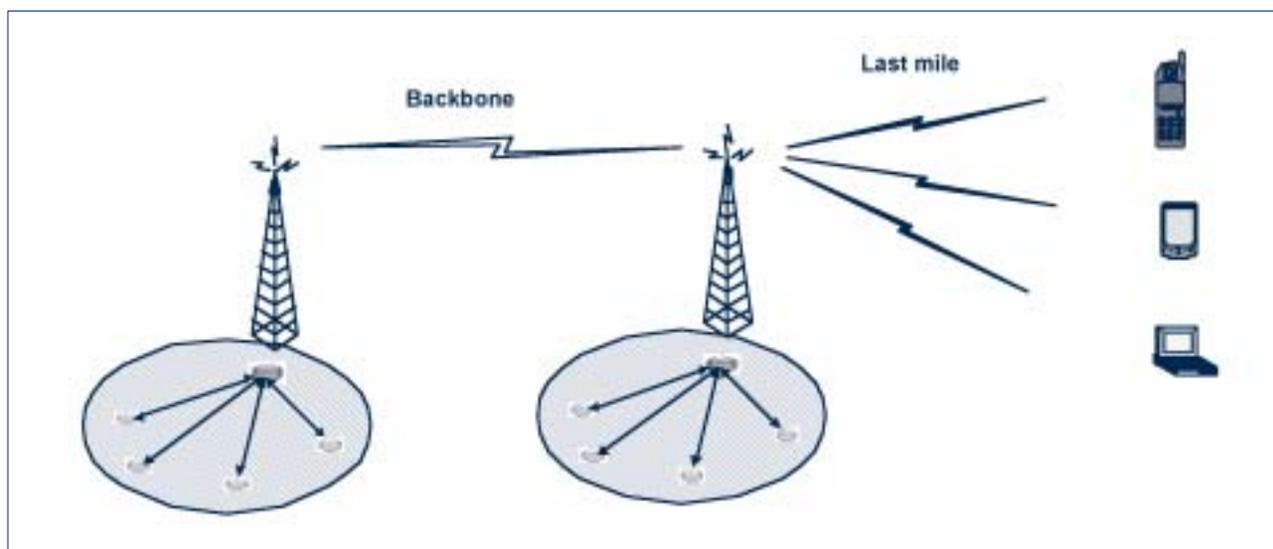


Figure 17. Architecture Wi-Max.

donné lieu à une série de publications dans le numéro de la REE de n° 4 / 2004.

On se limitera donc à rappeler ici quelques caractéristiques :

- Il s'agit d'une nouvelle forme de radiocommunications par impulsions dans une bande très large : 3,1 à 10,6 GHz, voire au-delà, en monobande ou multibandes (>500 MHz),
- Les impulsions sont très courtes en monobande (de l'ordre de la centaine de picosecondes) et peuvent se superposer aux solutions plus conventionnelles sans interférer avec elles d'où nécessité d'avoir des horloges très précises,
- Les impulsions sont plus longues (2,5 nanosecondes) en multibandes à porteuse unique ou modulation de type OFDM en multibandes à sous-porteuses multiples (IEEE 802.15.3.a).

Ces techniques ne sont pas encore stabilisées mais ouvrent la voie à des débits importants (100 Mbits/s), au moins sur courtes distances, avec une très bonne capacité de pénétration (murs et autres obstacles).

12. Wi-Max

Le Wi-Max ((Worldwide Interoperability for Microwave Access) constitue, parmi les techniques nouvelles, le sujet le plus "chaud" actuellement. Le Wi-Max est souvent présenté comme le Wi-Fi de deuxième génération. Mais les ambitions sont plus larges :

- d'une part, il s'agit de permettre la connexion entre elles de cellules de type Wi-Fi par des systèmes

plus économiques et plus efficaces que les communications satellitaires (objectif : 268 Mbits/s),

- d'autre part, l'objectif serait également de s'affranchir des réseaux en place, et donc des opérateurs historiques, pour fournir des liaisons à haut débit sur le First et le Last mile (objectif : 2 Mbits/s).

On le devine, l'enjeu économique est considérable. L'initiative est soutenue par un consortium regroupant des sociétés traditionnelles du monde des communications (Intel, Alcatel, Fujitsu, Siemens, etc.) mais aussi de nombreux « new comers » (Alvarion, Wi-Lan, Aperto Networks etc.).

Du succès de Wi-Max dépendra pour une large part l'avenir des systèmes 3G en cours de mise en œuvre et décrit en première partie de cet article. La collision sera-t-elle frontale ou bien une complémentarité sera-t-elle possible ? Il est encore trop tôt pour le dire.

Aujourd'hui Wi-Max est un défi technique mais c'est déjà un enjeu marketing. Un nouveau standard vient d'être publié au 1^{er} octobre 2004 : le 802.16-2004 (remplaçant notamment le 802.16a-2003 traitant des communications fixes dans la bande de 2 à 11 GHz - vitesse max : 70 Mbits/s – portée : 20 à 30 km) mais, même si beaucoup de sociétés se réclament dès à présent de la compatibilité Wi-Max, les premiers équipements certifiés Wi-Max ne sont pas attendus avant mi-2005. La mobilité n'est pas oubliée et devrait être traitée dans le 802.16e. Il faut attendre encore au moins un an avant de pouvoir juger de la capacité du monde industriel à répondre à des spécifications de plus en plus ambitieuses. En France, une période de tests techniques du Wi-Max,

dans la bande 3,4-3,8 GHz, est ouverte jusqu'au 31 août 2005.

À plus long terme, le groupe de travail 802.20 pourrait déboucher sur la définition de liaisons longues distances encore plus performantes.

13. Les applications industrielles

Le monde industriel est un monde exigeant, qui se méfie des effets de mode et où les technologies nouvelles ne sont acceptées que progressivement. Les applications industrielles requièrent :

- Fiabilité,
- Sécurité,
- Compétitivité,
- Performances,
- Standardisation,
- Interopérabilité (non dépendance d'un seul fournisseur).

Ces conditions ne sont que partiellement remplies actuellement. Toutefois, le sans-fil est une technologie de rupture et nous pensons que l'avenir est au sans-fil.

La question reste cependant ouverte de savoir quelle solution l'emportera. La route 2G, 2,5G, 3G est solidement balisée. Mais l'irruption des RLAN, par leur flexibilité et leurs perspectives de baisse de coûts, est à coup sûr à prendre au sérieux. Des briques technologiques existent pour la plupart des solutions évoquées précédemment :

- Composants et « chip sets » pour quelques €,
- Cartes de connexion et points d'accès (hubs et switches),
- Antennes, directionnelles ou non.

Il existe, il est vrai, assez peu de produits véritablement industriels : des lecteurs de code-barres, des systèmes de GPS, certains capteurs sans fil mais utilisant pour la plupart des solutions radio propriétaires. Le marché du sans-fil dans l'industrie reste donc pour l'instant un marché de niches :

- Contrôle d'installations distantes (réservoirs, pipelines, distribution d'eau, réseaux électriques),
- Relevé de compteurs,
- Extension de réseaux locaux sur un même site,
- Gestion de flottes,
- Logistique, transitique, convoyage, magasinage,
- Liaisons avec du matériel en mouvement (machines tournantes, robots de manutention),
- Applications dans les transports (liaisons entre les trains, les métros, les autobus et les installations au sol).

Mais la liste de ces applications s'allonge et les industriels auront tôt ou tard des choix à faire :

- Quelle solution au niveau du terrain : ZigBee, Bluetooth, 802-11 ?
- Quelle solution au niveau du système : 3G, 802-11 (a, b ou g) voire Bluetooth ?
- Quelle solution au niveau du site ou de l'entreprise : 3G, Wi-Max ou Internet ?
- Quelles couches supérieures ?
- Quelles exigences en matière de sécurité et quelles solutions ?
- Quelles sources d'alimentation ?

Après la guerre du fieldbus, la guerre du wireless est-elle déclarée?

L ' a u t e u r

Jean-Pierre Hauet est né en 1945. Il est ancien élève de l'École polytechnique et Ingénieur du corps des mines. Après quelques années passées dans l'Administration, il a rejoint le groupe Alcatel Alsthom (à l'époque Compagnie générale d'électricité) où il a occupé diverses fonctions, notamment celles de président directeur général des Laboratoires de Marcoussis (centre de recherches d'Alcatel), de directeur général de la branche Produits et techniques de Cégélec et, jusqu'à fin 2001, celle de Chief Technology Officer d'ALSTOM. Il est actuellement Associate Partner de BEA Consulting (www.beaconsulting.com). Il est président d'ISA-France, section française de l'ISA (Instrumentation, Systems and Automation society) : www.isa-france.org et est délégué général adjoint du Forum mondial du développement durable : www.equitable-forum.org.