Évolution des réseaux sans fil

Daniel Azuelos
Institut Pasteur
dan@pasteur.fr
03 octobre 2003

Résumé

L'utilisation de radiofréquences pour transporter de l'information n'est guère nouvelle. Grâce aux techniques récentes d'encodage l'accès multiple au medium, l'espace, est possible ; les portées et débits atteints se rapprochent de ceux de l'Ethernet partagé.

Cette famille de techniques de construction de réseaux sans fil initiée avec le 802.11 offre une possibilité économique, performante et souple à l'architecture de réseau.

Elle remet aussi sur le tapis des problèmes un peu oubliés, et leur donne ainsi une chance de trouver une solution correcte :

- *sécurité des personnes dans un environnement de plus en plus saturé en rayonnements électro-magnétiques (fours à micro-ondes, téléphones DECT, téléphones mobiles, radars...) ;*
- *cohabitation de diverses techniques utilisant des radiofréquences : 802.11b, 802.11a, 802.11g.*
- *sécurité des réseaux :*
  - *contrôle d'accès au medium (prises en libre service) : WEP, 802.11i, 802.1X ;*
  - *contrôle de ce qui est branché dans un réseau (répéteurs pirates) ;*
  - *périmètre de sécurité face à la mobilité (syndrome Maginot) ;*
  - *maîtrise des signaux compromettants (qu'est ce qu'ils écoutent dans la rue voisine ?).*

1 Introduction

La radio, la télévision, plus récemment la téléphonie, ont eu un déploiement dont le succès a tenu essentiellement à la maîtrise de techniques de transport de l'information sans fil. Toutes les autres techniques de transport utilisant un support conducteur électrique ou optique se sont trouvées un jour ou l'autre freinées par des problèmes techniques. Ces problèmes de travaux publics, ou de bâtiment font que les techniques utilisant le câble sont hautement discriminatoires dans la possibilité d'accès à l'information. Un câble n'amènera jamais le réseau à un coût uniforme que ce soit dans une entreprise, dans un pays ou dans le monde. L'explosion de la téléphonie mobile dans des pays où le téléphone filaire était très en retard est une démonstration flagrante de cette réalité.

Dans le domaine des réseaux informatiques nous sommes en train de vivre depuis 1997 la même mutation. Le signal qui transporte l'information est en train de s'affranchir de son support conducteur électrique ou optique, pour utiliser tout l'espace. En 1997, sous l'instigation de Lucent (ex Bell labs), l'IEEE éditait la première spécification des réseaux sans fil. En 1999 Apple intégrait correctement cette technique dans un ordinateur personnel, dans un ensemble de piles protocolaires et dans un équipement réseau (borne AirPort) qui fera date dans l'histoire des réseaux informatiques.

2 Terminologie

Les réseaux sans fil, ont depuis leur conception reçu diverses dénominations :

- WLAN : Wireless LAN ;
- RLAN : Radio LAN ;
- RLR : Réseau Local Radio ;
- AirPort : marque Apple ;
- Wi-Fi : Wireless Fidelity…

Tous ces noms, plus ou moins en adéquation avec la technique décrite, sont amenés à disparaître, sauf peut-être le plus simple qui risque de rester dans le grand public au même titre que HiFi. Un nom commun les décrit assez correctement : réseaux sans fil. AirPort est un nom propre qui au même titre qu'Ethernet en son temps à des chances de perdurer.

Ensuite, pour désigner précisément la technique utilisée il faut faire appel aux spécifications de l'IEEE de la famille 802.11. Ces spécifications couvrent les couches 1 et 2 du modèle OSI et sont en tout point comparables à la famille 802.3 de spécifications (Ethernet). Elles portent sur l'utilisation d'ondes hertziennes à large spectre comme porteuse, et précisent les méthodes d'accès au medium physique et de gestion de la liaison.

En 1997, l'IEEE publiait la spécification 802.11 qui permettait d'utiliser des radiofréquences à large spectre pour atteindre un débit physique maximal de 2 Mbit/s. En 1999, la spécification 802.11b voyait le jour et permettait d'atteindre un débit physique maximal de 11 Mbit/s. En 2000 Apple en adoptant cette technique permettait un véritable démarrage aussi bien dans le public que dans quelques entreprises.

Aujourd'hui 802.11 est mort, 802.11b bien que largement déployé est en sursis. Ces 2 étapes technologiques n'étaient que des lanceurs. Le standard ayant un avenir est, depuis bientôt un an, le 802.11g.

3 Fonctionnement

Un réseau sans fil utilise des radiofréquences (ondes électro-magnétiques) comme porteuse d'un signal. Chaque point d'une liaison est constitué d'une antenne utilisée en émission et réception, et d'un module de traitement (modulation - démodulation) du signal. Une onde électro-magnétique est caractérisée par sa fréquence ou sa longueur d'onde, les 2 étant liées : $\lambda \times f = c \approx 3 \times 10^8 m/s$. Sa longueur d'onde est une caractéristique à connaître car elle indique à quelle taille de structures elle va être sensible, c'est à dire absorbée ou bien transmise.

Pratiquement, l'électronique qui gère le codage de l'information et la modulation sur une porteuse (ainsi que les fonctions inverses) est intégrée dans une carte de format PCMCIA ou bien PCI. Ces cartes sont appelées selon les constructeurs Orinoco, AirPort, Wi-Fi ou 802.11b.

L'émetteur est cadencé sur une fréquence de base et va coder 2^n bits sur une porteuse sous la forme d'une modulation d'amplitude et phase. Lorsque le rapport signal sur bruit de la porteuse baisse, les valeurs de la grille d'amplitude phase utilisables vont être réduites et le nombre de bits pouvant être ainsi codés va passer à 2^{n-1} (ce qui correspond à une division du débit physique par 2).

Un ordinateur équipé d'une carte 802.11b détermine une zone spatiale dans laquelle il est possible d'établir une liaison avec un ordinateur. Cette zone spatiale est déterminée par la portée jusqu'à laquelle le rapport signal sur bruit est suffisant pour porter encore de l'information. La forme de cette zone de couverture spatiale dépend énormément de la qualité du dessin d'antenne et peut aller de quasi-sphérique (antenne omni-directionnelle) à un lobe allongé (antenne directionnelle).

3.1 802.11b

802.11b[3] utilise des radiofréquences à large spectre (Spread Spectrum) sur la **bande ISM** (Industrial Scientific and Medical) autour des 2,4 GHz. Au niveau bas, il existe 3 méthodes d'utilisation des ondes électro-magnétiques : par sélection de fréquence (DSSS : Direct Sequence Spread Spectrum), par saut de fréquence (FHSS : Frequency Hopping Spread Spectrum, technique utilisée dans BlueTooth), et par utilisation des infra-rouges. Ces 2 dernières méthodes ont été abandonnées au profit de la seule encore utilisée : DSSS.

Cette bande de fréquences est subdivisée en **14 canaux de 22 MHz** de bande passante se chevauchant (figure 1). Les canaux utilisables diffèrent selon les pays et les problèmes d'interférences avec les utilisations existantes. La bande ISM n'étant pas libre, 802.11b rencontre des problèmes de cohabitation pacifique avec les services qui utilisaient cette bande de fréquences.

Pour utiliser 802.11b en DSSS, tout poste équipé d'une telle carte doit ou bien être statiquement configuré sur un canal, ou bien sélectionner plus ou moins dynamiquement l'un des canaux qu'il reçoit.

Tout comme sur un réseau Ethernet, les émissions depuis plusieurs postes peuvent donner lieu à des collisions. Néanmoins, là où sur Ethernet une telle collision sera détectée de tous les postes, sur un réseau 802.11b une telle collision peut passer inaperçue d'un poste : Ethernet utilise un support à une dimension, 802.11b utilise l'espace. 2 postes qui ne sont pas à portée optique l'un de l'autre peuvent néanmoins provoquer une collision si leurs zones de couverture spatiale ont une intersection.

Pour pallier à ce phénomène de « **collision cachée** » 802.11b utilise une méthode d'accès au medium par « évitement de collision » : **CSMA/CA** (Carrier Sense Multiple Access with Collision Avoidance). Avant toute émission un poste envoie un RTS (Request To Send) et attend un CTS (Clear To Send) du destinataire. Il s'ensuit tout naturellement que le 802.11b s'approche beaucoup moins de son débit physique maximal qu'Ethernet.

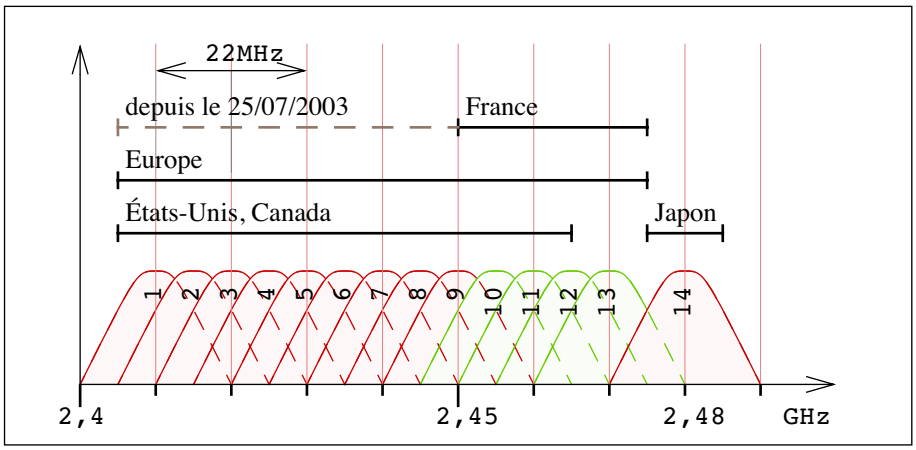

figure 1 : *canaux utilisables en 802.11b*

Le débit physique que fournit la porteuse en 802.11b est fonction du rapport signal sur bruit. Il peut prendre les valeurs de 11 Mbit/s, 5,5 Mbit/s, 2 ou bien 1 Mbit/s. Cette dernière valeur étant souvent dans une zone fluctuante, n'est pas utilisable en pratique.

3.2 Types de réseaux

Deux types de réseaux peuvent être aisément construits avec des cartes 802.11b :

- réseau multi-point ;
- réseau d'infrastructure.

Un **réseau multi-point** (« ad-hoc » en anglais, terminologie à proscrire car vide de sens) est monté à partir de postes équipés d'une carte 802.11b dont le 1er va définir le canal et le nom (SSID = Service Set Identifier, terme ronflant qui désigne simplement un identifiant de réseau). Dans la pratique un tel réseau peut être monté entre ordinateurs pas trop éloignés les uns des autres, comme par exemple lors d'une réunion improvisée entre collègues à l'occasion de leur rencontre à une conférence. Ce réseau permet essentiellement de faire du partage de fichiers très souplement.

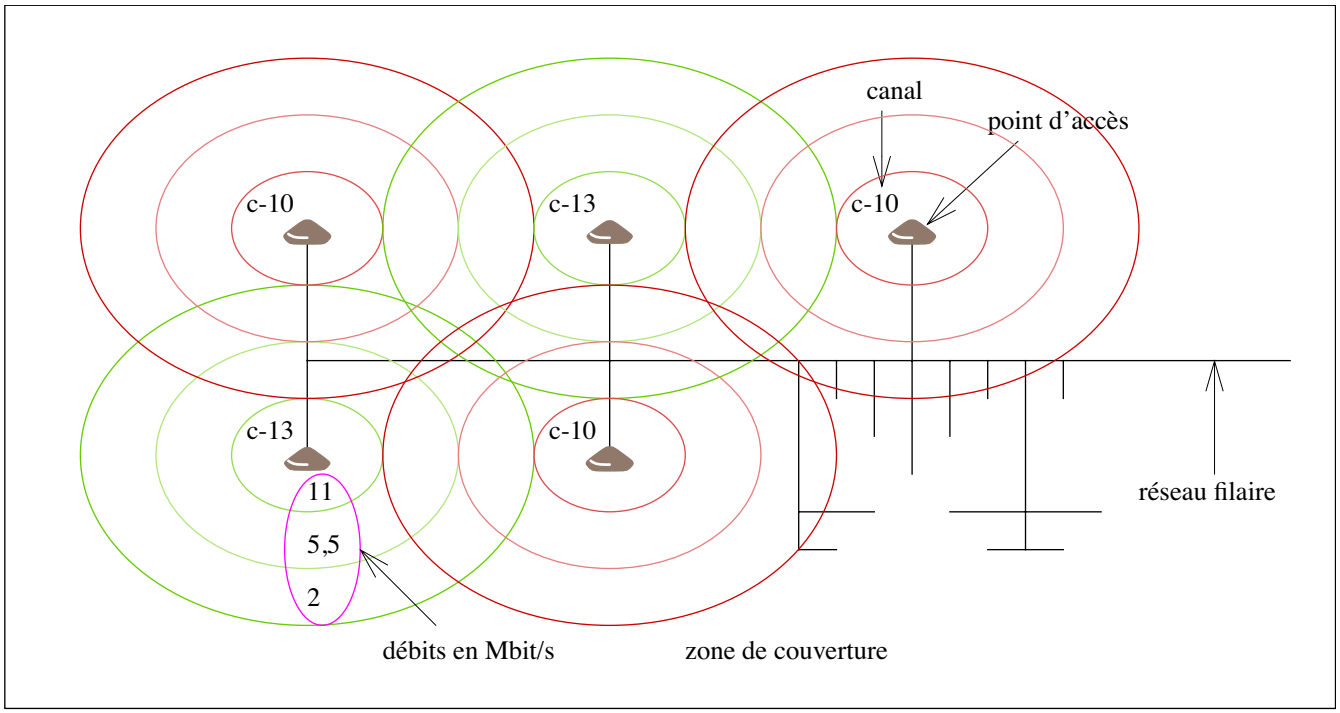

figure 2 : *réseau d'infrastructure*

Dans ce type de montage « improvisé », le réseau sans fil offre un avantage décisif sur le réseau Ethernet point à point : on peut être largement à plus de 2 sur ce réseau, et on peut bouger.

Toutefois l'authentification d'accès à ce réseau, la confidentialité des données échangées sont liées à la qualité du plus médiocre des systèmes d'exploitation participant à ce réseau multi-point.

Un **réseau d'infrastructure**, bâti à partir d'un ou plusieurs « points d'accès » fait le lien entre l'accès sans fil et l'infrastructure de réseau Ethernet traditionnelle (figure 2). Un point d'accès étant un équipement réseau plus ou moins intelligent et ayant 2 interfaces réseau : l'une du côté avec fil et l'autre du côté sans.

L'utilisation de radiofréquences permet la mobilité à l'intérieur de la zone spatiale de couverture d'un point d'accès. Si chacune des zones de couvertures est correctement mise en œuvre, alors la couverture intégrale d'un bâtiment peut être réalisée et permettre la mobilité à l'intérieur d'un unique réseau sans fil (identifié par son nom).

3.3 Réglementation

La réglementation qui s'applique en France, définie par l'ART[1], vient d'être largement assouplie le 25 juillet 2003. Dans tous les départements métropolitains, en intérieur, tous les canaux de 1 à 13 peuvent être utilisés jusqu'à une puissance (PIRE[1]) de 100mW. En extérieur, les canaux 1 à 7 peuvent être utilisés jusqu'à 100mW, et les canaux 8 à 13 ne peuvent être utilisés que jusqu'à 10mW (cette limitation correspondant plutôt à ce qui est utilisé en BlueTooth et n'ayant qu'une applicabilité pratique limitée : aucune carte « sans fil » n'est capable de baisser sa puissance lorsqu'on la sort dehors).

Rien n'est prévu pour arbitrer les conflits entre particuliers, entreprises, et fournisseurs d'accès. C'est pour l'instant la loi de la jungle. Pour éviter le pire, il va de soi qu'il vaut mieux d'ores et déjà être sur le terrain et définir sur son domaine de responsabilité comment seront arbitrés les conflits de couverture. Il coule donc de source que sur le campus d'une université, d'un centre de recherche, ou d'une entreprise, c'est un réseau d'infrastructure qui doit être déployé, accompagné d'information et de règles d'usage.

4 Mise en œuvre

Le déploiement d'un réseau d'infrastructure apporte une solution économique là où le réseau filaire bute, soit qu'il implique des coûts prohibitifs, soit qu'il soulève des risques inacceptables.

- Prise à plus de 100m d'un équipement réseau.
- Prises dans de grands espaces où le mobilier est régulièrement déplacé.
- Dans des bâtiments classés.
- Lorsqu'il faut ponctuellement beaucoup d'accès réseau, alors qu'en temps normal un petit nombre peut suffire. Par exemple pour un accès en libre service, une salle de réunion, une salle de conférence, une bibliothèque.
- Dans des laboratoires à hautes normes de sécurité, dans des passages non contrôlés et exposés à de l'écoute ou de la destruction.

Le réseau sans fil impose pas mal de contraintes nouvelles par rapport au câblage Ethernet.

- Il s'agit de couvrir un espace au moyen de sphères en minimisant les interférences entre réseaux sur le même canal.
- La sécurité des personnes et des communications doivent être analysées.
- Enfin les points d'accès doivent être raccordés aux réseaux électrique et Ethernet.

4.1 Propagation

Les radiofréquences se propagent en ligne droite à la vitesse de la lumière, et comme toutes les ondes électro-magnétiques ont divers types de comportement face aux matériaux rencontrés : elles peuvent être complètement absorbées, ou bien être plus ou moins déviées par réfraction, réflexion ou diffraction. La transparence des matériaux (figure 3) dans le spectre des radiofréquences n'est pas visible, il faut donc avoir recours à des outils simples permettant de mesurer la qualité du signal dans l'environnement à couvrir.

1. PIRE : Puissance Isotrope Rayonnée Équivalente, puissance qu'il faudrait fournir à une antenne isotrope (omni-directionnelle) pour qu'elle fournisse la même puissance dans la direction considérée.

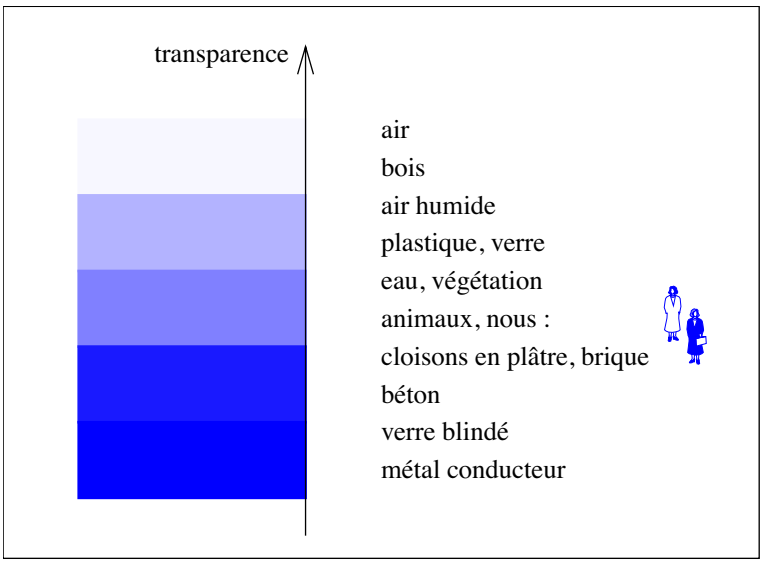

figure 3 : *transparence aux radiofréquences*

4.2 Interférences

En environnement de bureau ou de laboratoire, les diverses réflexions des ondes électro-magnétiques peuvent donner lieu à interférence entre 2 signaux du même émetteur mais ayant suivi des chemins optiques différents. Cette caractéristique de multiplicité de chemin optique est à la fois un avantage et un inconvénient des réseaux sans fil. Elle leur permet d'atteindre des points inaccessibles en ligne directe, mais leur rend aussi inaccessibles des points proches par excès d'interférences (figure 4).

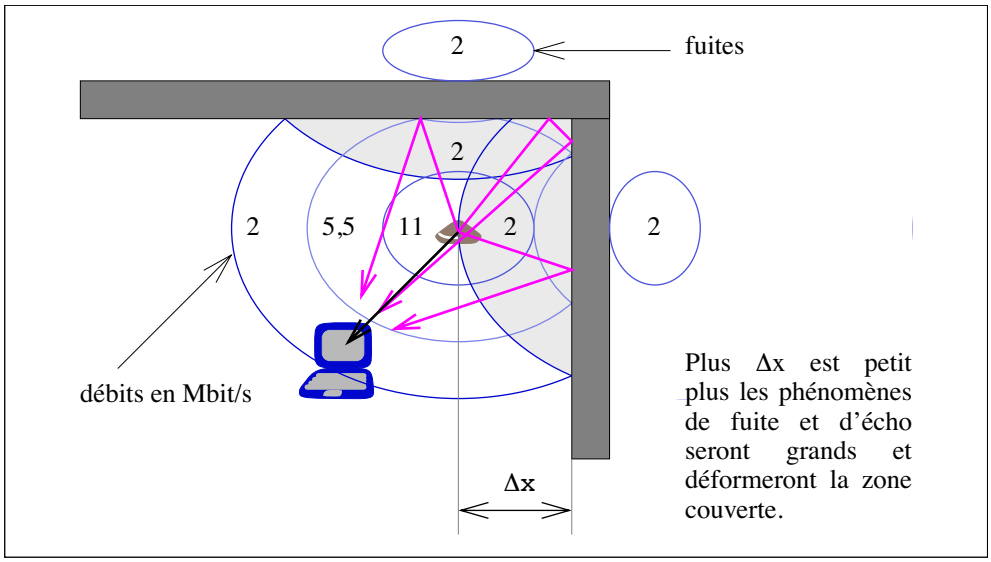

figure 4 : *interférences au voisinage d'un mur*

Au tout début des déploiements des réseaux sans fil, les constructeurs ont tenté de résoudre ce problème par 2 méthodes : l'amplification du signal émis et l'utilisation d'antennes directionnelles. L'amplification du signal ne fait qu'aggraver proportionnellement les distorsions de la zone couverte car plus d'obstacles sont atteints ou franchis. Le choix d'antennes directionnelles limite à un secteur angulaire la problématique de multiplicité de chemin optique, mais apporte le problème de réglage de la direction de l'antenne et les problèmes de diffraction en bordure du secteur angulaire couvert. Ces antennes doivent donc être fixées à un support fixe (mur ou plafond) créent sur celui-ci fuites et échos, et ramènent donc souvent aux problèmes soulevés par les prises Ethernet. Tout compte fait, ces 2 solutions sont largement pires que le problème qu'elles visaient à régler.

Le meilleur choix pour couvrir correctement un grand espace consiste à utiliser des points d'accès de puissance faible et réglable, munis d'une antenne quasi omni-directionnelle, donc totalement banalisés, mobiles et interchangeables à volonté.

4.3 Réglages

Le déploiement de réseaux sans fil nécessite quelques outils de mesure indiquant le rapport signal sur bruit de façon assez précise et entre autres sa variabilité au cours du temps. Notre choix du matériel Apple, en 2000, a été essentiellement déterminé par la qualité de leur logiciel de gestion qui décelait tout réseau et surtout permettait un suivi graphique du rapport signal sur bruit de tous les postes « raccordés ».

Dans un environnement amené à accueillir du monde, des réglages en présence et en absence de personnes doivent être effectués afin d'éviter des surprises désagréables les jours de réunion. En effet, malgré la multiplicité de trajectoire, le corps humain étant relativement opaque aux radiofréquences un réseau sans fil rétrécit en fonction de la densité de population. Le même phénomène se produit aussi avec l'hygrométrie de l'air : un réseau sans fil rétrécit à l'humidité.

5 Sécurité

La technique 802.11b très similaire à 802.3 souffre des mêmes problèmes de sécurité à tous les niveaux. Les 2 reposent sur l'utilisation d'ondes électro-magnétiques, dans un cas dans l'espace, dans l'autre sur un conducteur. Les 2 sont donc hautement sensibles aux parasites dans les hautes fréquences, et peuvent être écoutés. L'aspect qui les distingue est la taille de leur zone d'accès : en 802.3, il fait quelques mètres (câble autour d'une prise RJ45), alors qu'en 802.11b elle peut faire jusqu'à quelques centaines de mètres. 802.11b a l'heureux effet de nous rappeler que toute utilisation de champ électro-magnétique peut être écoutée, brouillée et soulever des problèmes de santé.

5.1 Sécurité des personnes

Compte-tenu du fait que la fréquence utilisée par le 802.11b (2,4 GHz) est proche d'une des fréquences d'absorption de l'eau[1], on est en droit de se demander quel peut être l'impact de l'utilisation généralisée de ces radiofréquences sur notre santé.

Avant d'envisager le déploiement de cette technique sur notre campus, nous avons analysé les études faites sur les conséquences sur la santé de l'utilisation des radiofréquences[2]. Dans l'ensemble, il ressort que pour l'instant s'il existe un risque pour la santé dans l'usage de diverses ondes électro-magnétiques, celui-ci serait plutôt du côté de l'usage des GSM ou des émetteurs puissants placés en hauteur. Les GSM (900 MHz) qui émettent tous à fond leurs 600 mW dans un wagon de métro parisien, ou le rayonnement continue des 6 MW de l'émetteur de la tour Eiffel sont loin devant (d'un ordre de grandeur >1000) en terme de puissance rayonnée. Pour obtenir la même quantité de rayonnement qu'un téléphone mobile GSM (≈ 600 mW), il faudrait se coller à la tête **10 portables du type iBook** avec une carte AirPort (≈ 60 mW) ou 1000 à une distance de l'ordre du décimètre, ou bien **équiper une salle de cours de 100 000 postes**. En effet tout champ électro-magnétique décroît en $\frac{1}{r^2}$ (60 mW à 1 cm devient 6 µW à 1 m et $100000 \times 6\ \mu W = 600\ mW$).

À la suite de cette analyse, nous avons consulté notre service hygiène et sécurité afin d'avoir leur autorisation pour procéder au déploiement de réseaux sans fil sur notre campus.

5.2 Sécurité des systèmes d'information

Les réseaux Ethernet supportent mal la cohabitation avec les courants forts et peuvent être aisément écoutés dès lors que les chemins de câbles ne sont pas intégralement protégés ou qu'il existe des prises accessibles.

Les réseaux sans fil ne font pas mieux sur ces 2 aspects : comme toute forme de transport d'information à base d'ondes électro-magnétique, ils sont sensibles aux interférences et peuvent être écoutés. Des réseaux sans fil doivent donc être déployés avec différentes protections.

- La maîtrise de la portée spatiale du réseau en utilisant les obstacles, la puissance d'émission des points d'accès de

1. Une des fréquences de résonnance de l'eau est autour des 900 MHz (utilisée par les GSM), mais les four à micro-ondes utilisent une fréquence plus élevée de 2,4 GHz pour que le rayonnement ne soit pas intégralement absorbé dès la surface. Contrairement à une idée reçue, la fréquence de 2,4 GHz n'est absolument pas la plus dangereuse du spectre d'absorption de l'eau : elle ne provoque qu'une oscillation d'ensemble de la molécule.

façon à ne jamais sortir des espaces à couvrir.

- La résistance aux interférences en déployant les réseaux de façon à partitionner complètement mais sans recouvrement excessif un espace donné. L'utilisation de points d'accès permettant de régler leur « robustesse anti-interférence ».
- Le filtrage d'association entre poste client et point d'accès basé sur l'adresse MAC (sur 6 octets exactement comme en 802.3).
- Le chiffrement des données échangées directement dans le protocole.
- Enfin un filtrage d'accès au reste du réseau pour les cas souhaités et délimités d'accès en libre service.

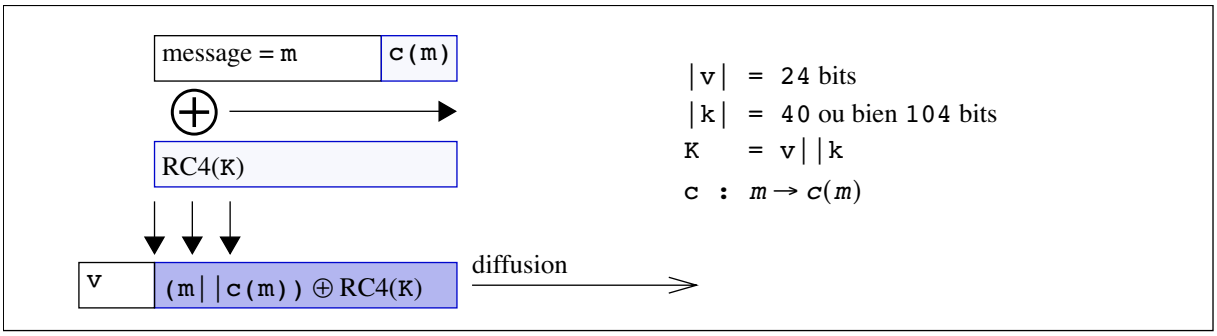

figure 5 : *fonctionnement de WEP*

WEP : Wired Equivalent Privacy

Bien conscient que l'absence de confidentialité des échanges nuirait à l'utilisation du 802.11b, l'IEEE y a intégré une fonction optionnelle permettant d'amener ce réseau à un niveau de sécurité « équivalent » à celui d'Ethernet : WEP (figure 5).

Cette fonction utilise le protocole de chiffrement à clé symétrique partagée RC4, qui en terme d'algorithme de chiffrement est excellent. Mais dans ce jugement, il est fait abstraction de « toutes » les limites de cet algorithme de chiffrement.

Au niveau de l'émetteur un message `m` est tout d'abord prolongé d'un code de vérification d'intégrité `c(m)`. La clé de RC4 est la concaténation d'un vecteur d'initialisation pseudo-aléatoire `v` de 24 bits, et de la clé secrète `k` de 40 ou bien 104 bits.

Le message diffusé est la concaténation de `v` et de `(m||c(m))` ⊕ RC4(K)[1].

Les limites d'utilisation de RC4 qui le rendent attaquable par diverses techniques de cryptanalyse sont :

- diffusion de `v` en clair ;
- `m` est prévisible (en-tête TCP/IP) et peut être généré par l'attaquant (utilisation de `ping(1)`).

Ces vulnérabilités de mise en œuvre de RC4 sont utilisables avec des outils publiquement disponibles comme AirSnort[5]. Bien que plusieurs travaux[4] aient stigmatisé ces problèmes de mise en œuvre, le pire est hors de la technique de chiffrement et ceci aussi grande soit la clé de chiffrement utilisée :

- génération de `k` (par l'administrateur réseau ou bien par M. X) ;
- rien n'est prévu pour limiter la diffusion de `k`, ni son changement à chaque compromission ;
- stockage de `k` (sur un poste client dans quel état : combien a-t-il de BackOrifice ?).

Pour toutes ces déficiences WEP est un protocole qui est dans la catégorie de ce que l'on peut faire de pire en sécurité : l'« **extincteur vid**e ». **WEP est donc à proscrire dans tout réseau sans fil**.

Filtrage par adresse MAC

Le filtrage par adresse MAC ne fait pas partie de la norme 802.11b, mais c'est une fonction que l'on trouve sur tout équipement réseau moderne Ethernet ou 802.11b. Ce filtrage ne protège que l'établissement de la liaison et n'apporte rien au niveau confidentialité des données échangées. Il présente l'avantage de n'être à configurer que sur les points d'accès.

Ce filtrage est évidemment très facile à contourner exactement comme sur Ethernet. Il suffit d'utiliser une carte Ethernet ou 802.11b qui permette la modification de son adresse MAC.

1. || = opérateur de concaténation, ⊕ = ou exclusif.

Toutefois il ne faudrait pas dramatiser la faiblesse de cette protection sans prétention. Sur un réseau typique d'entreprise où cette possibilité d'établissement de connexion frauduleuse existe de longue date en Ethernet c'est paradoxalement plutôt de ce côté que se produisent les accès indésirables allant de l'écoute passive (sur répéteur pirate) à l'établissement de liaison (sur prise libre avec usurpation d'adresse MAC).

La protection par filtrage d'adresse MAC n'apporte rien face à un attaquant compétent, mais protège plutôt des erreurs d'utilisateurs bien intentionnés dans des réseaux voisins.

Le successeur de ce filtrage est aujourd'hui disponible chez quelques constructeurs qui mettent en œuvre le standard **802.1X** de l'IEEE qui permet l'authentification de l'accès basé sur l'adresse MAC ou bien sur un couple (compte, mot de passe) voire sur des méthodes d'authentification plus sophistiquées.

Filtrage d'accès au réseau : extranet

La sécurité des réseaux sans fil est en pleine gestation, et pour l'instant n'offre pas de solution simple permettant de garantir à tous les ordinateurs sur un réseau sans fil qu'il n'y a ni écoute, ni modification des échanges. Partant de là, une sage mesure de précaution consiste à traiter ces accès comme des accès « externes » au réseau de l'entreprise.

Ces réseaux peuvent être déployés derrière un coupe-feu. Dans notre cas nous avons choisi une interface virtuelle sur un routeur de cœur de réseau, cette interface étant configurée avec une ACL en tout point semblable à celle que nous avons en entrée de site par l'Internet. Cette ACL fait fonction de diode :

- passant tout vers les réseaux sans fil ;
- bloquant presque tout vers les réseaux internes ;
- passant presque tout vers l'Internet.

Plus précisément ce filtrage (sur le trafic venant du réseau d'accueil des réseaux sans fil) est définit par les règles suivantes (la première applicable dans l'ordre est appliquée) :

protocole	source	destination	passage	journalisation
IP	*[1]	équipements actifs	interdit	oui
DHCP	*	serveurs DHCP	autorisé	
IP	hors de notre réseau	*	interdit	oui
DNS	*	serveurs DNS	autorisé	
TCP	*	serveurs publics	autorisé	
IP	*	réseaux internes	interdit	oui
IP	*	*	autorisé	

1. * = n'importe quelle adresse.

Confidentialité des échanges

En l'état actuel de la technique le chiffrement sur les réseaux sans fil au niveau liaison n'est pas pratiquement utilisable. Il est donc nécessaire d'en informer correctement les utilisateurs et de les inciter à utiliser des protocoles de chiffrement de plus haut niveau (tunnel chiffré sur IPSEC, SSH, SSL).

Audit

Le réseau filaire ne poussant jamais assez vite pour les urgences des utilisateurs, ceux-ci ont la fâcheuse tendance à vouloir l'aider à pousser au moyen de répéteurs de supermarché, ou aujourd'hui au moyen de points d'accès sans-fil. Et il ont bien raison, puisque le coût et le temps d'installation sont bien moindre qu'en passant par le maître d'œuvre du réseau. Malheureusement, installés comme dit dans la publicité, c'est à dire sans le mode d'emploi, ces équipements font de notre périmètre de sécurité une vraie passoire.

Afin de ne pas tomber dans ce « **syndrome Maginot** » qui consiste à croire qu'une fois un coupe-feu installé nous sommes à l'abri de notre périmètre de sécurité, quelques précautions sont à entretenir. Les adresses IP privées ou plus généralement hors plan d'adressage doivent être détectées (routeurs internes filtrants et journalisants). Il est indispensable de procéder à des

audits en bordure physique de campus afin de détecter les réseaux sans fil pirates qui peuvent nuire aux voisins comme à nous, et inversement détecter tôt les réseaux sans fil de voisins naïfs sur lesquels nos utilisateurs pourraient tomber à leur insu, raccordant ainsi à l'intérieur de notre campus le réseau du voisin.

Risques

Dans cette démarche de recherche exhaustive de signaux compromettants il est intéressant de noter que la couverture totale par des réseaux sans fil est un avantage. Occuper le terrain ne laisse guère de place aux intrus ni aux apprentis ingénieur réseau et permet d'éviter les problèmes d'arbitrage d'attribution de canaux et d'espaces couverts. Mieux, lorsque un bâtiment est couvert par plusieurs réseaux sur le même canal sans chevauchement à l'intérieur du bâtiment, les possibilités d'écoute passive tombent très vite dès que l'on s'en éloigne puisque tous les signaux interfèrent sur le même canal et sont donc difficiles à séparer quel que soit le gain de l'antenne du récepteur.

Des mesures de champs électro-magnétiques faites sur notre campus ont mis en évidence qu'encore aujourd'hui c'est la THT d'un bon vieux tube cathodique qui rayonne le plus fort et le plus loin.

6 Évolutions

Le 802.11b avec un débit physique maximum de 11 Mbit/s et un débit pratique en TCP/IP de 6 Mbit/s normalisé en 1999 a commencé son déclin avec l'avénement du 802.11a et du 802.11g en 2002. On peut estimer qu'il sera totalement remplacé dans les parcs déployés d'ici 2005.

802.11a publié en 2002, permet d'atteindre un débit physique maximum de 54 Mbit/s sur la bande de fréquence UNII (Unlicensed National Information Infrastructure) située autour des 5,5 GHz. Il est incompatible avec le 802.11b.

802.11g publié en 2003 permet d'atteindre le même débit physique maximum de 54 Mbit/s sur la bande de fréquence ISM. Il est compatible avec le 802.11b.

Les normes 802.11a et 802.11g utilisent comme technique de modulation du signal l'OFDM (Orthogonal Frequency Division Multiplexing). Cette technique consiste en l'utilisation de 52 porteuses distinctes sans chevauchement de leurs bandes passantes, de façon à ce que ces porteuses soient toutes des harmoniques d'une même fréquence $f = n \times 312{,}5\ kHz$. Ces porteuses ayant toutes leurs nœuds synchronisés dans le temps et dans l'espace n'interfèrent que peu entre elles. Les bits sont codés en parallèles sur toutes ces porteuses, ce qui permet de maintenir relativement bas le débit en bit/s sur chacune d'entre elles.

6.1 802.11a

Le 802.11a a été défini sur une bande de fréquence libre, mais sur des plages différentes entre les États-Unis, l'Europe et le Japon (exactement comme ce fut le cas pour 802.11b jusqu'à tout récemment). Le fait que cette bande de fréquence UNII soit libre signifie que si son usage rencontre le succès alors les problèmes de cohabitation et d'arbitrages sont des problèmes auxquels le 802.11a sera alors immanquablement confronté.

Le 802.11a utilise une fréquence double du 802.11b et par conséquent transporte une énergie double : $E = h \times f$. De ce fait son absorption est plus élevée, et pour une puissance d'émission identique à une carte 802.11b, une carte 802.11a va avoir une couverture approximativement 2 fois plus courte dans une direction donnée. Pour couvrir à puissance identique un même volume qu'avec du 802.11b, il faudrait 8 fois plus de points d'accès 802.11a. Cette densité importante de déploiement des points d'accès fait perdre beaucoup de son intérêt au réseau sans fil.

6.2 802.11g

Le 802.11g utilise la même plage de fréquence que le 802.11b où les problèmes de cohabitation avec les autres utilisations sont en passe d'être aplanis. Il utilise simultanément les 2 techniques DSSS et OFDM. Il permet l'établissement d'une liaison conjointement avec un poste équipé d'une carte 802.11b et un autre équipé d'une carte 802.11g. Cependant, dans ce mode, c'est le plus lent qui va définir le débit pratique utilisable. Le 802.11g est aujourd'hui la technique à utiliser pour gérer l'accès au parc des postes équipés en 802.11b et assurer la transition vers le futur.

6.3 802.11i

Le standard 802.11i qui devrait bientôt être publié a pour objectif de traiter correctement la confidentialité des données transportées sur un réseau sans fil, et l'authentification d'accès. À cette fin, il devra intégrer une gestion de clé correcte, contrairement à ce qui était fait dans WEP.

Le chiffrement adopté par 802.11i est l'AES en lieu et place de RC4.

Pour l'aspect authentification d'accès, c'est le standard 802.1X[6] qui sera adopté (et amélioré) et qui permet l'authentification d'accès sur tout type de réseau (avec ou sans fil). C'est la méthode d'authentification qui est utilisée de longue date pour les accès PPP via un serveur RADIUS.

Cependant cette authentification d'accès et ce chiffrement des données ne nous affranchissent toujours pas du risque lié aux portables ayant un système d'exploitation de mauvaise qualité. Quand bien même ils ne sont raccordés qu'en Ethernet voire même par un tunnel chiffré, sitôt le dernier ver Windows attrapé ils en feront joyeusement profiter tous leurs voisins d'infortune à l'abris du coupe-feu : syndrome Maginot.

7 Conclusion

Les réseaux sans fil mettent en évidence pas mal de problèmes et sont générateurs de solutions. Ils doivent être déployés maintenant car c'est là que se font les avancées en terme de maîtrise du périmètre de sécurité de l'entreprise.

Ces avancées (comme 802.1X) gagneront à être appliquées aussi à Ethernet. L'idée selon laquelle un réseau Ethernet est sûr puisque tous les bouts en sont visibles est on ne peut plus trompeuse. À la base les réseaux avec ou sans fil s'appuient sur les mêmes phénomènes électro-magnétiques, sur les mêmes adresses MAC et transportent les mêmes piles protocolaires. Ces similitudes fondamentales sont là pour nous rappeler qu'ils peuvent souffrir des mêmes maux et des mêmes remèdes :

« Benjamin Franklin was undoubtedly thinking of 802.11b when he famously said those who would sacrifice freedom for security deserve neither. »[7].

Références

[1] ART : Autorité de Régulation des Télécommunications, http://www.art-telecom.fr
« *Les réseaux locaux radioélectriques ou RLAN / Wi-Fi* »,
http://www.art-telecom.fr/dossiers/rlan/menu-gal.htm

[2] Ministère de la santé, « *Téléphones mobiles et santé* » :
http://www.sante.gouv.fr/htm/dossiers/telephon_mobil/

[3] 802.11b, standard IEEE (http://standards.ieee.org/), « *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications* » :
http://standards.ieee.org/getieee802/download/802.11-1999.pdf
http://standards.ieee.org/getieee802/download/802.11b-1999.pdf

[4] Nikita Borisov, Ian Goldberg, David Wagner « *Intercepting Mobile Communications: The Insecurity of 802.11* ».
Dans Proceedings of the 7th annual international conference on Mobile computing and networking, pp. 180-189, Rome Italy, 16-21/07/2001 :
http://doi.acm.org/10.1145/381677.381695

[5] Page web d'AirSnort :
http://airsnort.shmoo.com

[6] 802.1X, standard IEEE « *Local and Metropolitan Area Networks: Port-Based Network Access Control* » :
http://standards.ieee.org/getieee802/download/802.1X-2001.pdf

[7] Rupert Goodwins, « 802.11i - designed to integrate ». Dans ZDNet UK, 10/04/2003 :
http://insight.zdnet.co.uk/communications/wireless/0,39020430,2133239,00.htm