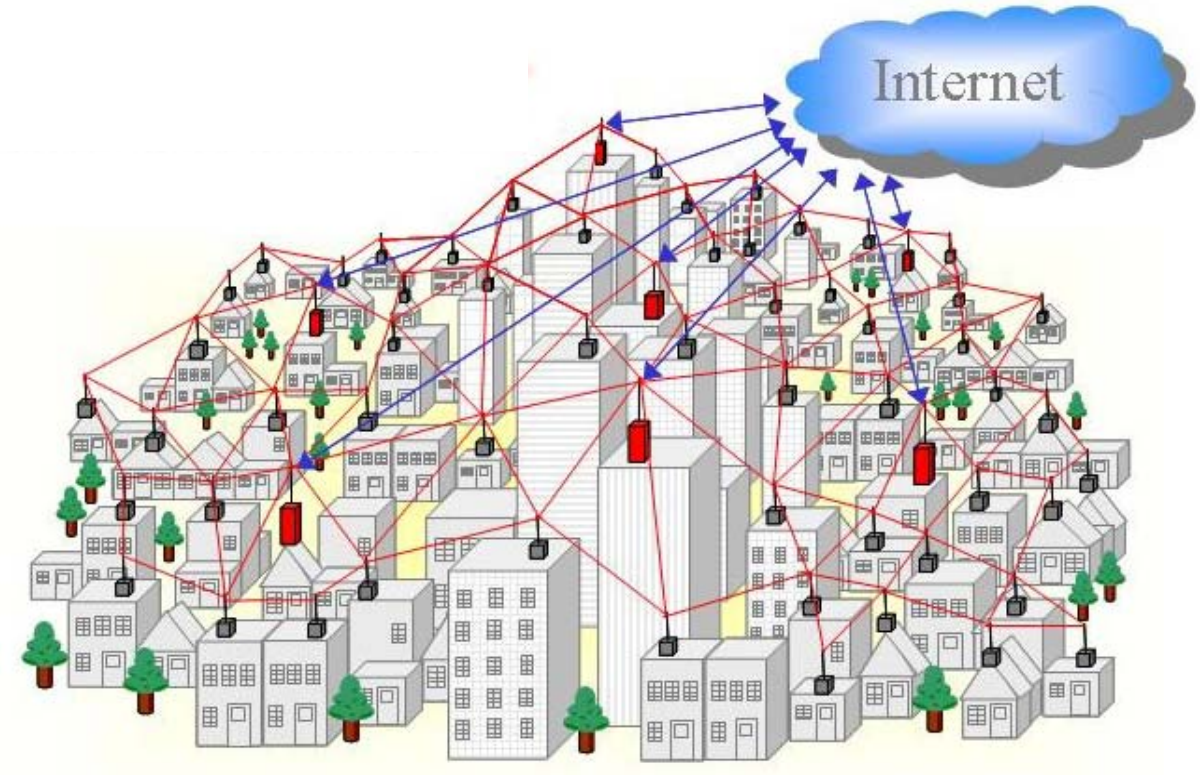
ANDRE Emmanuel,
DE RUGY Guillaume,
HERBIET Guillaume-Jean,
INCATASCIATO Benoit

RADIOCOMMUNICATION ET RADIODIFFUSION

Rapport d'électif

****



Réseaux mobiles maillés

Introduction

Les « réseaux maillés » sont-ils l'avenir des réseaux sans-fil ? Depuis mars dernier, le campus parisien de Jussieu construit un de ces réseaux sans fil d'un nouveau genre, voire d'une autre génération : les « réseaux maillés » ou « mesh networks ». Les premières applications sont prévues pour la fin de cette année.

Les supporters des réseaux maillés leur voient plusieurs avantages, par rapport aux autres réseaux fonctionnant par ondes radio, comme le désormais célèbre Wifi : cette technologie permet d'envisager 60 % d'économie de points d'accès, sans perte de qualité et avec de nouvelles applications en mode peer-to-peer.

Toute proportion gardée, les réseaux sans fil actuels sont monolithiques. Ils manquent d'abord de souplesse. Pour les étendre, il faut installer une nouvelle borne émettrice d'ondes radio et la relier par un fil au reste du réseau. De plus, la qualité du signal devient imprévisible au-delà d'une certaine limite. Deux raisons qui obligent à augmenter la puissance d'émission.

Les réseaux maillés adoptent une tout autre architecture. Au lieu augmenter l'intensité pour lui permettre de parcourir la distance, on la maintient quasiment à l'identique et on réduit la distance. Les différents nœuds du réseau, auparavant de simples points d'accès, relaient dorénavant le signal. En les faisant ainsi collaborer, le signal conserve sa qualité et le débit reste identique.

Table des matières

I. Rapide historique des réseaux maillés

A. Topologie des réseaux

1) Les réseaux en BUS

Dans les réseaux de ce type, l'information émise par une station est diffusée pour tout le réseau et y est accessible à tout le monde. Chaque station accédant directement au réseau sans hiérarchisation, il se pose des problèmes de conflits d'accès au BUS (contentions ou collision), ce qui nécessite l'élaboration d'un protocole d'accès plus complexe que la simple relation maître/esclave des liaisons multipoints.

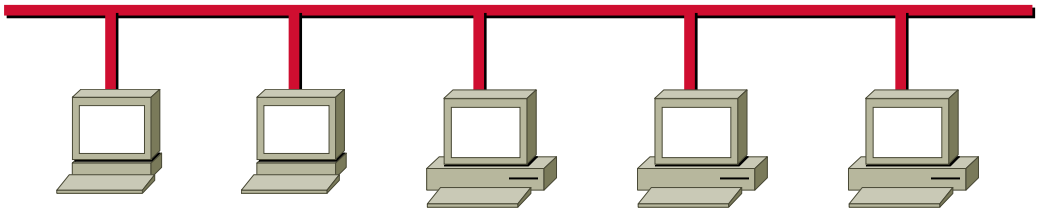


Figure 1 : Réseau en bus

L'avantage de ces réseaux réside dans leur bon rapport performance/prix. Il est par ailleurs très facile de rajouter une station supplémentaire sur le BUS (raccordement direct) sans perturber les communications en cours.

2) Les réseaux en étoile

Tous les nœuds du réseau sont ici reliés à un nœud central commun: le concentrateur. Tous les messages transitent par ce point central qui examine chaque message et ne le retransmet qu'à son destinataire.

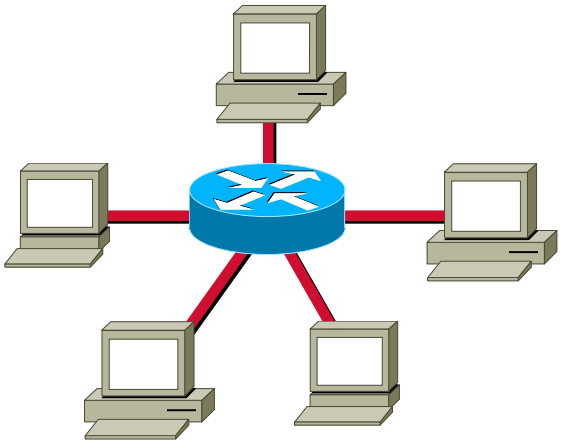


Figure 2 : Réseau en étoile

Ce genre d'architecture est utilisé pour les réseaux téléphoniques privés (type PABX par exemple). On peut ainsi obtenir des dialogues inter-nœuds très performants et la défaillance d'un poste n'entraîne pas celle du réseau. Le réseau reste toutefois très vulnérable à une panne du nœud central.

3) Les réseaux en anneaux

Dans ce type de configuration, est connecté au point suivant en point à point et l'information ne circule que dans un seul sens, chaque station recevant le message et le régénérant. Si le message lui est destiné, la station le recopie au vol.

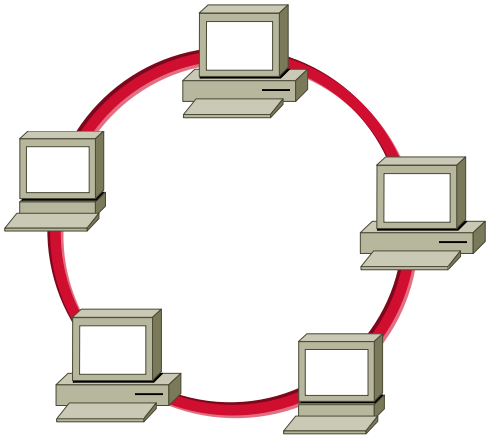


Figure 3 : Réseau en anneau

Grâce à ce type de réseau, on peut obtenir des débits élevés sur de grandes distances (grâce à la régénération du signal par chaque station). L'anneau est bien sûr sensible à la rupture de la boucle mais on peut palier à cet inconvénient en réalisant un double anneau autorisant la circulation de l'information en sens inverse. L'exemple le plus connu de tel type de réseau en France est le réseau Renater pour la recherche.

4) Les réseaux maillés

La structure de réseau maillé est la plus couramment utilisée aujourd'hui. C'est un réseau dans lequel deux stations de travail peuvent être mis en relation par différents chemins. Cette mise en relation s'effectue à l'aide de commutateurs, chaque commutateur constituant un nœud du réseau.

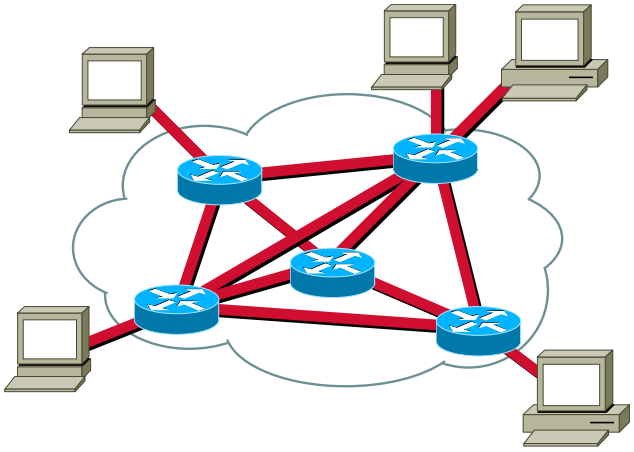


Figure 4 : Réseau maillé

Ce type de réseau est très résistant à la défaillance d'un noeud du fait que l'information a plusieurs chemins possibles pour aller d'un point à un autre. La défaillance d'un noeud peut donc être aisément contournée. Par ailleurs, cette architecture permet une optimisation de l'emploi des ressources en répartissant la charge entre les différents noeuds (voies).

Cette structure est la plus utilisée aujourd'hui dès qu'il s'agit de grands réseaux nationaux et internationaux et des variantes comme les réseaux ad-hoc (réseaux points à points étendus en maillage) pour les mobiles.

B. Rapide historique d'Internet

Internet est le premier grand réseau maillé à s'être développé après celui du téléphone. Aussi nous a-t-il semblé important d'en retracer succinctement l'histoire.

Après le succès scientifico-militaire remporté par les Soviétiques en octobre 1957 avec le lancement de Spoutnik en pleine guerre froide, le président Eisenhower demande au ministère de la Défense américain de créer l'ARPA (Advanced Research Project Agency), l'agence pour les projets de recherche avancée. Rassemblant les meilleurs scientifiques américains, l'ARPA est mise en place pour renforcer la recherche susceptible d'intéresser les militaires.

Le gouvernement américain cherche alors à créer un réseau de communication pouvant continuer à fonctionner après une attaque nucléaire. Paul Baran de la société RAND (Research ANd Development) est chargé par l'ARPA d'étudier ce problème. Deux ans plus tard, en 1964 il soumet à l'ARPA sa proposition: le réseau devra être décentralisé et présenter une structure maillée, chaque nœud (ordinateur) étant aussi bien capable d'envoyer que de recevoir des messages. Il introduit de plus la notion de transfert de données par paquets pour des raisons de sécurité et de fiabilité. Il s'agit là de la technologie dite du packet-switching ou de « commutation de paquets » dont Paul Baran est l'un des inventeurs, et dont la théorie avait été étudiée par Leonard Kleinrock au MIT (Massachussets Institute of Technology) en 1961.

Le modèle proposé par P. Baran est séduisant à maints égards. Tout d'abord, en raison de la structure maillée du réseau, les connexions entre ordinateurs sont redondantes, si bien que l'acheminement des messages est assuré même en cas de destruction partielle du réseau. Ensuite, tous les nœuds étant équivalents, il n'existe pas de point névralgique dont la destruction serait fatale au bon fonctionnement du réseau. Enfin, le packet-switching permet à plusieurs ordinateurs d'utiliser simultanément une même ligne et garantit la fiabilité, car l'interception d'un message secret, ou un incident, n'affecte qu'une petite partie du message. En effet, chaque paquet porte des informations relatives à son origine et à sa destination, si bien qu'en cas de perte d'un paquet lors de son acheminement vers le destinataire, seul ce paquet sera réexpédié par l'émetteur et non la totalité du message.

En 1968, le National Physical Laboratory en Grande-Bretagne met en place le premier réseau à commutation de paquets. Pendant ce temps, l'ARPA étudie un projet beaucoup plus ambitieux mettant en application la proposition de P. Baran avec les ordinateurs les plus puissants de l'époque.

En août 1969, le premier ordinateur du réseau étudié par l'ARPA est installé à UCLA (University of California Los Angeles). En octobre, novembre et décembre de la même année, trois autres ordinateurs du réseau sont installés respectivement à Stanford, à l'université de Santa Barbara (Californie) et à l'université de l'état d'Utah. Avec ces quatre ordinateurs interconnectés, chacun doté de la technologie du packet-switching le projet arrive à terme.

Après avoir résolu certains problèmes techniques, Arpanet devient réellement opérationnel, permettant aux quatre institutions de transférer des données et d'effectuer à distance certains calculs longs sur plusieurs ordinateurs afin d'aller plus vite. En 1971-72, apparaît le premier programme pour l'envoi et la réception de courrier électronique (SNDMSG et READMAIL). Le signe @ que nous utilisons encore aujourd'hui est introduit dans l'adresse de messagerie et on simule avec succès l'envoi et la réception du premier e-mail. Au même moment, on écrit le premier programme de gestion du courrier électronique (classer, répondre, enregistrer etc.). En 1973, le courrier électronique représente 75% du trafic total sur Arpanet!

Le nombre de machines connectées à Arpanet puis à Internet augmente rapidement, passant de 20 en 1971 à 30000 en 1990 pendant que le réseau s'étend d'abord en Grande Bretagne puis en Norvège et enfin au monde entier au fur et à mesure que se rattachent d'autres réseaux au réseau principal. En 1974, le protocole TCP/IP est créé et s'impose comme la norme en moins de 10 ans: ce protocole, toujours basé sur le mode de transmission par paquets définit en plus un mode d'adressage chargé d'assurer l'acheminement des paquets d'ordinateur en ordinateur jusqu'à destination.

Enfin, en 1991, au CERN, est inventé le World Wide Web permettant de créer un ensemble de documents rattachés les uns aux autres par des liens hypertextes, afin de faciliter la recherche d'informations pour les physiciens des particules: Internet tel que nous le connaissons actuellement était né.

En parallèle de ce gigantesque réseau qu'allait devenir Internet, on commence, à partir du début des années 80 pour la France, à voir l'apparition des premiers réseaux de téléphonies mobiles (Radiocom 2000 à partir de 1986 puis GSM à partir de 1992 puis 3G en 2004) qui sont bâtis eux aussi sur le principe d'un réseau maillé comprenant près de 35000 sites auxquels viennent se rajouter les satellites de radiocommunication.

Les principales évolutions d'Internet aujourd'hui se situent autour des nouvelles technologies sans fils, type Bluetooth, WiFi et WiMAX. La multiplication des terminaux mobiles oblige à faire évoluer le concept de réseau maillé à nœuds fixes que l'on a connu jusqu'à présent pour s'orienter de plus en plus vers des réseaux dits ad-hoc, ou à nœuds mobiles.

II. Réseaux maillés fixes

Un réseau maillé fixe est constitué par un ensemble de nœuds acheminant les messages à transmettre d'une ligne d'entrée vers une ligne de sortie. Sachant que les messages à transmettre par l'intermédiaire de ce réseau peuvent emprunter plusieurs chemins pour atteindre leurs destinataires, chaque nœud doit transférer ces messages de manière adéquate. On peut classifier ces derniers en deux catégories : les commutateurs et les routeurs.

A. Commutation et routage

Un nœud doit effectuer les opérations suivantes :

- récupérer la référence ou l'adresse du destinataire dans l'en-tête du message,
- commuter ou router le message,
- enfin multiplexer les différents messages sur le sortie déterminée.

Ces équipements doivent également être équipés de mémoires tampons afin de pouvoir stoker les messages à traiter lorsqu'ils doivent être redirigés vers une même ligne de sortie. Ces files d'attentes peuvent être situées sur les lignes d'entrées, sur les lignes de sorties ou encore le long de la chaîne de transfert.

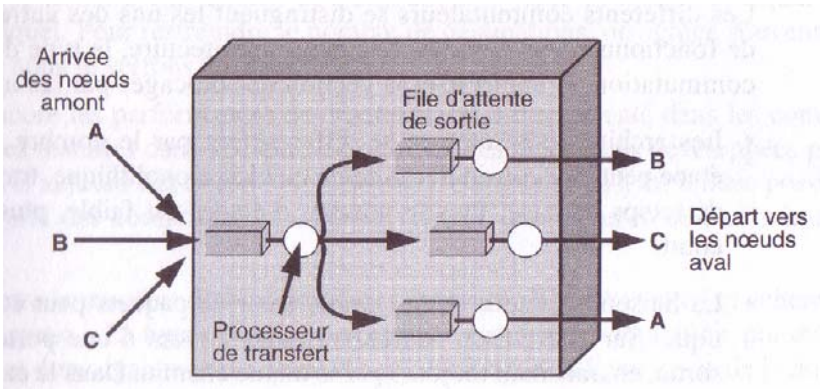


Figure 5 : Fonctionnement d'un nœud de transfert

Regardons maintenant le deuxième point, à savoir commutation ou routage.

1) Commutation

Les commutateurs utilisent des références afin de transmettre le message qu'ils reçoivent en entrée au récepteur, accessible directement ou non sur une de leur sortie. Ainsi, un message à destination d'un terminal, portant une référence. Ce message est émis par un autre terminal (extrémité) et atteint le premier commutateur. Les commutateurs disposent tous d'une table de commutation associant justement ces références à une de leurs lignes de sortie. Le premier commutateur constate alors que la référence correspond à tel sortie et y envoie le paquet. Le message arrive sur un second commutateur, qui associe à son tour cette référence à une de ses sorties et y envoie le message, et ainsi de suite jusqu'au récepteur. De fait, les messages (trames, paquets, etc.) portant une même référence seront tous dirigés vers la même sortie du commutateur. Remarquons que des messages spécifiques sont employés pour trouver le chemin adéquat au transfert d'un message, et que ces données particulières sont dirigées grâce à une table de routage : un commutateur possède donc une table de commutation mais aussi une table de routage ! Un message transite donc sur le réseau, passant de nœuds en nœuds en suivant un circuit qui n'est autre qu'une succession de références. Ce circuit est par ailleurs virtuel puisqu'il n'est pas réservé à un couple émetteur-récepteur particulier.

2) Routage

Un routeur utilise une table de routage pour diriger le message vers le destinataire. Un message est routé à l'entrée de chaque nœud grâce à l'adresse complète du destinataire (là où le commutateur utilise une seule référence). La ligne de sortie est indiquée dans une table de routage. Le routage est plus complexe et lent que la commutation car il faut traiter l'adresse complète de destination, et il faut maintenir à jour la table de routage. Hors la gestion des tables de routage est plus complexe que celle des tables de commutation car ces dernières sont généralement plus petites (seules les connexions actives sont prises en compte).

B. Technique de transfert

Il existe différentes techniques de transfert. Celles basées sur la commutation ne fonctionnent qu'avec des réseaux commutés tandis que les autres peuvent s'appliquer aussi bien pour ce type de réseau que dans le cas de routage.

1) Commutation de circuits

Il s'agit d'une technique historique, notamment utilisée avec le réseau téléphonique classique. Un circuit est crée entre l'émetteur et le récepteur, et leur est réservée. Il est établi lorsqu'un terminal veut échanger des informations avec un autre, et ne prend fin que lorsqu'un les de ces deux équipements interrompt la communication. Ainsi, si les deux équipements ne communiquent pas pendant un certain temps, cette ressource disponible est perdue puisqu'elle ne peut être utilisée par d'autres terminaux !

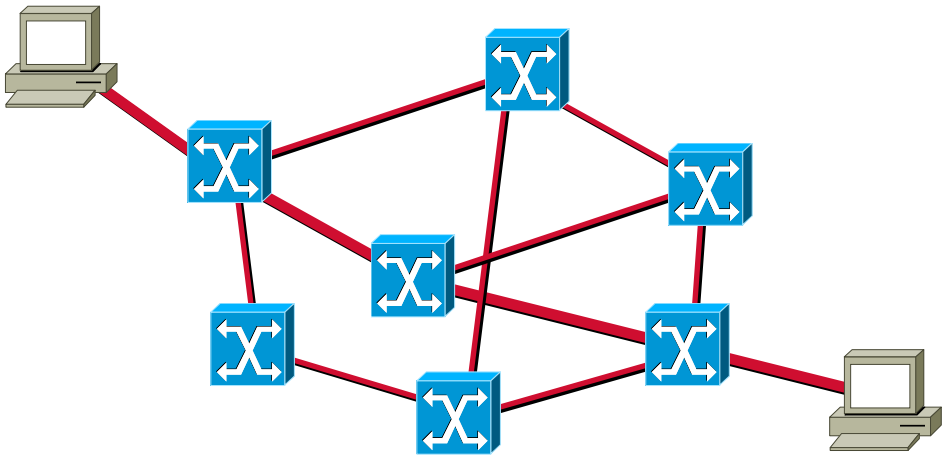


Figure 6 : Réseau à commutation de circuits

2) Transfert de messages

Le message (suite d'information formant un tout pour les terminaux) est envoyé de nœud en nœud, à chaque fois qu'un nœud donné l'a reçu en intégralité. Ce système pose plusieurs problèmes : d'une part il faut stocker les messages dans chaque nœud, leur longueur pouvant être variable et importante, d'autre part le temps de propagation est relativement important à cause justement de ces étapes. Ce temps sera également d'autant plus long si des erreurs surviennent en cours de route puisqu'il faudra réémettre dans le pire des cas le message.

3) Transfert de paquets

Afin de palier les inconvénients du transfert de message, les messages sont découpés en blocs dont la taille maximale est fixée, appelé paquets. Ainsi, chaque nœud n'est plus obligé d'attendre l'arrivé complète d'un message mais d'un paquet, beaucoup plus cours. De fait, le récepteur peut, suivant le cas, recevoir les premiers paquets alors que le destinataire n'a pas encore envoyé les derniers paquets, ce qui est impossible avec la technique précédente. De même, si des erreurs surviennent, il suffit juste de renvoyer les paquets incriminés. Au final, le temps de propagation est bien plus cours qu'avec un transfert de message. Enfin, les paquets d'un même message peuvent empruntés différentes routes, dans le cas d'un routage dynamique.

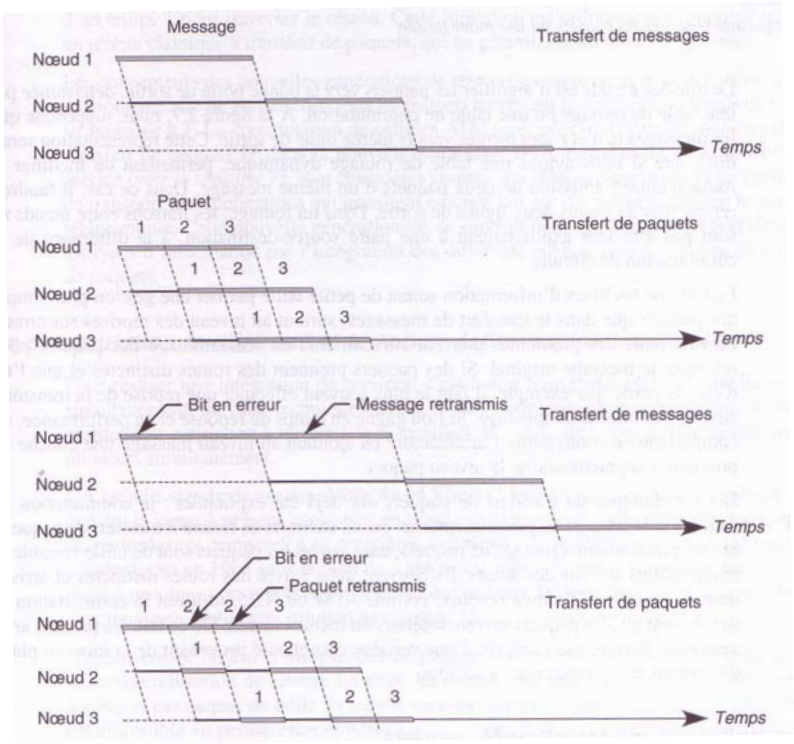


Figure 7 : Temps de réponse comparé entre commutation de paquets et commutation de messages

4) Transfert de trames

Le principe est le même que pour le transfert de paquets, excepté le fait qu'ici, le paquet est encapsulé dans une trame après des éléments binaires signalant qu'il s'agit du début du « message » (de la trame dans notre cas). En effet, les paquets ne peuvent être directement transmis de manière physique puisque rien n'indique le début et la fin des paquets. Dans le cas du transfert de paquets, chaque nœud doit donc décapsuler puis ré-encapsuler les paquets dans des trames au moment où il les reçoit et où il les envois. Dans le cas du transfert de trames, les nœuds sont simplifiés puisqu'ils n'ont plus à faire ces opérations. Celles-ci sont en effet effectuées au niveau de l'émetteur et du destinataire. Généralement, cette technique est utilisée avec la commutation, bien que théoriquement, on pourrait utiliser le routage.

5) Commutation de cellules

Il s'agit d'un transfert de trames où les trames ont une taille fixe immuable et très petite (53 octets) : si les données à transportées sont plus grandes, elles sont découpés. Elle a pour but de remplacer à la fois la commutation de circuit et le transfert de paquets. Cette solution est très employée depuis les années 80 car elle est simple et peut facilement monter en charge.

C. Algorithmes de routage

Ces algorithmes permettent de déterminer la route que doivent emprunter les messages dans un nœud. Pour cela, ils gèrent les tables de routage de chaque nœud, en veillant notamment à ne pas créer de boucle dans le réseau (message qui tournerait en rond en passant toujours par les mêmes nœuds, sans jamais atteindre leur destination). Cette table associe à chaque destination une ligne de sortie de l'équipement. Dans ce paragraphe ne seront considérés que les réseaux IP.

Comme les réseaux peuvent être très vastes (par exemple le réseau Internet), ils ont été scindé en systèmes autonomes (ensemble de routeurs et de réseaux reliés entre eux) pour en faciliter la gestion. Le protocole de routage utilisé dans un système autonome est dit protocole de routage intérieur. Le protocole de routage extérieur permet quant à lui de router les informations entre les différents systèmes autonomes.

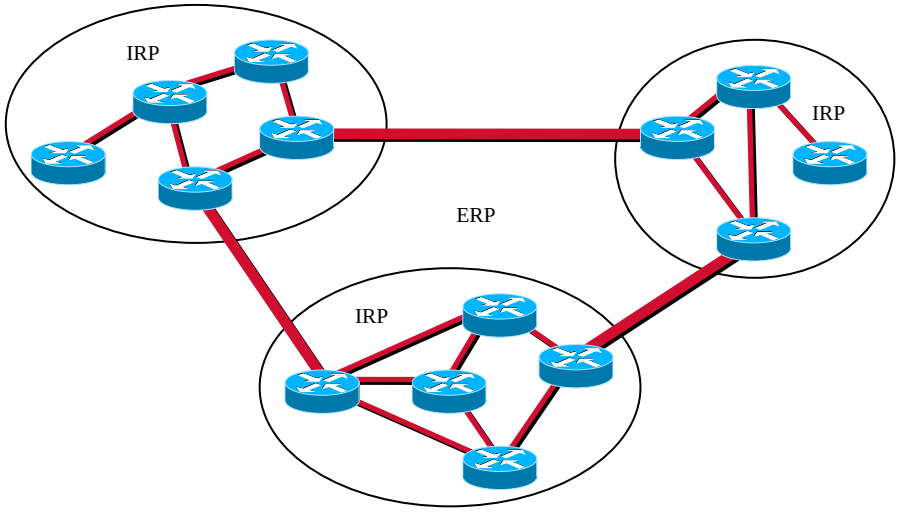


Figure 8 : Protocoles de routage intérieur et extérieur

Il existe trois grands types d'algorithmes de routage que nous allons maintenant voir.

1) Routage à vecteur de distance

Chaque nœud communique avec les nœuds voisins : il leurs transmet un vecteur contenant l'ensemble des réseaux qu'il peut atteindre avec la métrique associée. Ainsi la table de routage de ce nœud est établie avec les informations transmises par ces voisins, mais ne connaît pas les identités des routeurs qui se trouvent après ses voisins. Il s'agit du premier protocole utilisé avec ARPAnet, ancêtre de l'Internet. Néanmoins, cette technique est lourde lorsque le nombre de nœuds est important à cause des transferts d'informations de nœuds en nœuds : elle est difficilement envisageable pour les protocoles de routage extérieurs. De plus, comme un routeur ne connaît que ses voisins, il ne sait pas quel est le chemin global emprunté par un message, ce qui peut poser des problèmes de sécurité…

Le protocole RIP en est un exemple. Il est le plus utilisé en TCP/IP pour router les paquets entre les passerelles du réseau Internet. Il permet de trouver le chemin (nombre de nœuds à traverser) le plus court. Les informations avec les voisins sont échangées toutes les 30 secondes environ. Par ailleurs, il n'accepte pas de chemin de plus de 16 sauts. Si un message RIP (Routing Information Protocol) n'est pas reçu par un routeur au bout de 3 minutes, il considère que la liaison est tombée.

2) Routage à état des liens

Ce protocole devait initialement pallier le défaut du routage à vecteur de distance. Lorsqu'un routeur est initialisé, il calcule un coût vers chaque nœud auquel il est connecté, puis il transmet ces coûts à l'ensemble des nœuds du système autonome (et non uniquement aux voisins). Ainsi les tables de routages contiennent toutes les liaisons vers chacune des destinations possibles, avec leurs coûts associés. Dès qu'une modification survient, le routeur qui la détecte en informe tous les autres qu'il connaît afin que chacun mette à jour de manière adéquate leur table de routage. Ce type d'algorithme résout le problème d'utilisation avec un réseau extérieur, mais en introduit d'autres, notamment lorsque les métriques des systèmes autonomes ne sont pas les mêmes, ou que des restrictions ont lieu dans certains d'entre eux : le routage n'est plus alors cohérent. Enfin, la diffusion des informations peut éventuellement saturer un réseau.

Le protocole OSPF (Open Shortest Path First) est un exemple de routage à état des liens. Il utilise une base de données distribuée qui garde en mémoire l'état des liens : on a ainsi la topologie du réseau et l'état des liens ; on peut ainsi calculer les chemins les plus courts.

3) Routage à vecteur de chemin

Ces algorithmes remédient aux problèmes soulevés par ceux des deux types précédents : ils ne prennent pas en compte les distances ou coûts des chemins, mais permet de connaître les différents réseaux atteignables, en précisant par quels nœuds et quels systèmes autonomes ils le sont. Ce type de routage est de fait plutôt destiné aux routages extérieurs.

Le protocole BGP (Border Gateway Protocol) appartient à cette catégorie.

III. Réseaux maillés avec nœuds mobiles

Ainsi que nous l'avons vu, l'utilisation d'une topologie maillée permet à un réseau beaucoup plus de souplesse, une plus forte tolérance aux pannes et une qualité de service bien meilleure. Ces performances s'obtiennent au prix de la complexification de la gestion du réseau, notamment du routage, et d'une hausse substantielle du coût des infrastructures, liée notamment à la pose et à l'entretien des câbles liant les différents nœuds du réseau.

Avec le développement des réseaux sans fil, ce dernier inconvénient se voit réduit car la topologie maillée réduit le câblage à néant, tout en fournissant de manière inhérente une forte tolérance aux pannes et une grande évolutivité.

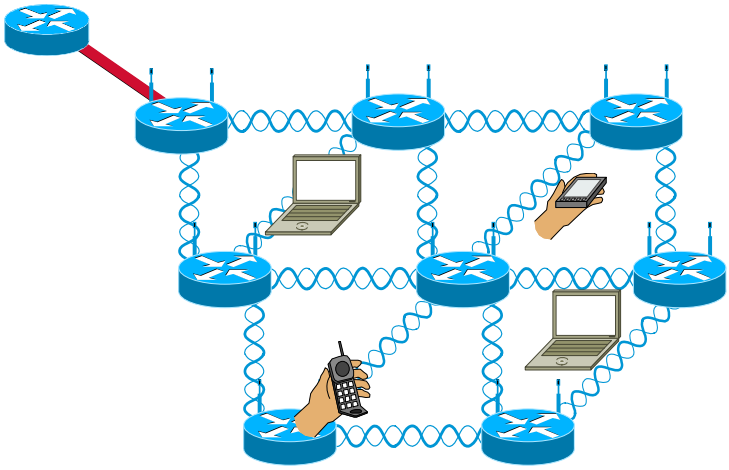


Figure 9 : Réseau wifi maillé : un réseau de mobiles

Comme le suggère la Figure 9, l'utilisation d'un maillage permet non seulement de rendre le réseau plus robuste (même si l'une des bornes émettrices subit un dysfonctionnement, comme chaque récepteur est en vue de plusieurs bornes, il est toujours en mesure de recevoir des informations du réseau), plus performant (en augmentant la qualité de réception et la portée du réseau).

A. Introduction à la mobilité

Pour autant, liaison sans fil, ne veut pas dire mobilité. En effet, dans la plupart des cas, seuls les nœuds terminaux du réseau, représentant souvent un utilisateur équipé d'un ordinateur ou d'un téléphone portable, possèdent une certaine mobilité.

En effet, pour arriver à une notion de réseau à nœuds mobiles, il faut également prendre en compte de nombreuses fonctions qui sont autant de challenges technologiques, notamment en ce qui concerne l'acheminement des données au travers d'un tel réseau et le routage, avec comme double objectif une qualité de service suffisante et une sécurisation des données transmises par voie hertzienne.

1) Réseau mobile et réseaux de mobiles

Une des principales différences à faire dans le domaine de la mobilité est la distinction entre ce que nous appellerons des « réseaux de mobiles » (qui concernent par exemple l'implantation actuelle de la téléphonie cellulaire de deuxième ou troisième génération) et de véritables « réseaux mobiles » (dans lequel les nœuds du réseau ne sont ni fixes ni persistants à la différence, par exemple, des antennes relais des réseaux GSM et UMTS).

En effet, dans le cas des réseaux de téléphonie cellulaire, les stations de bases, les commutateurs qui composent le cœur de réseau sont des équipements fixes, le plus souvent

interconnectés par des équipements filaires et seuls les terminaux et les antennes-relais (qui composent le dernier échelon de l'infrastructure du réseau de télécommunication) sont reliés de manière hertzienne et proposent des services inhérents à la mobilité : hand-over et roaming.

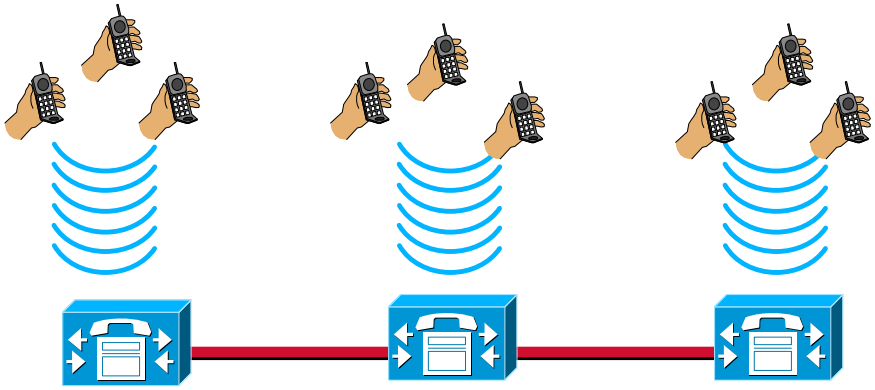


Figure 10 : Réseau à station de bases interconnectées : un autre réseau de mobiles

De même, le réseau wifi maillé représenté en Figure 9 n'est pas à proprement parler un « réseau mobile » puisque, là encore, les nœuds du réseau sont des bornes fixes et persistantes.

Un autre point permettant d'effectuer la distinction entre ces deux notions repose sur la notion d'architecture du réseau.

En effet, dans le cas du réseau de téléphonie cellulaire comme dans celui des bornes wifi présentées en Figure 9, l'architecture du réseau est, dans une certaine mesure, pyramidale que ce soit avec…

2) Les grands principes des réseaux mobiles

A la différence des « réseaux de mobiles », les « réseaux mobiles » présentent une architecture à la fois spontanée et anarchique (au sens où la hiérarchie entre les équipements du réseau est beaucoup moins marquée).

Les nombreux développements actuels autour des technologies sans fil, comme le wifi par exemple, s'articulent en effet essentiellement autour du mode sans infrastructure : le mode Ad-Hoc.

On utilise surtout ce mode pour connecter deux équipements entre eux (connexion dite « d'égal à égal » ou « point à point ») permettant des partages de données.

Ici, il s'agit de connecter des hôtes de proche en proche pour établir un réseau, permettant à tous les hôtes de communiquer entre eux.

Parmi la quantité de termes décrivant les réseaux sans fil de type ad-hoc, on regroupe souvent les termes « Mesh, Ad-hoc, Wifi » pour décrire les réseaux non filaires et sans structure centralisée.

- « Mesh », terme anglais signifiant maille ou filet, s'applique à la topologie (architecture) d'un réseau, où tous les hôtes de ce réseau (filaire ou non) sont connectés de proche en proche, sans hiérarchie centrale, formant ainsi une structure en forme de filet ;
- Ad-Hoc, prend ici le sens de « spontané » et s'applique au type de connexion. C'est-à-dire qu'un PC qui se connecte à un réseau de type ad-hoc, fait parti instantanément du réseau ;
- Wifi, indique le type de connexion radio, mais d'autre technologie pourrait être utilisée.

Ce type de réseau ne nécessite pas de point d'accès, pas de routeur dédié et gère dynamiquement les associations et dé-associations des hôtes.

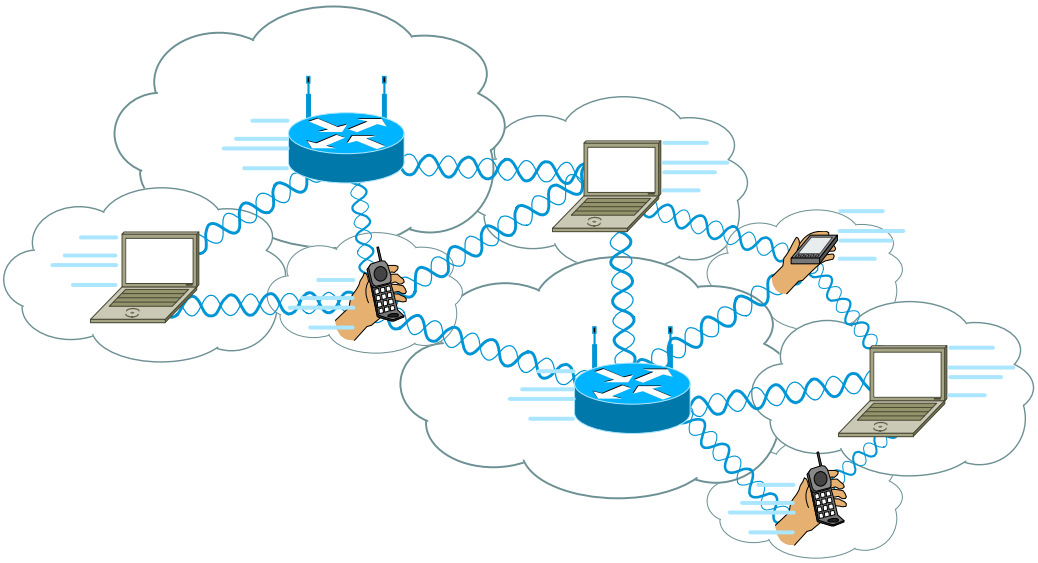


Figure 11 : Réseau mobile maillé

En résumé, pour un réseau ad-hoc maillé, tout les nœuds sont mobiles et exercent à la fois la fonction de nœud terminal du réseau (téléphonie, navigation, …) et de routeur. Ils organisent de manière dynamique la topologie du réseau qui ne présente, stricto sensu, aucune architecture rémanente.

Ces principes sont résumés le plus souvent dans la locution anglaise « Self-creating, self organizing, self-administrating » et ils visent à donner une couverture maximale avec une disponibilité sans faille (« Anytime, anywhere »).

Les principaux points forts de ce type de réseau sont bien évidemment la rapidité de mise en place, le coût réduit, indépendance vis à vis des point d'accès (que ce soit d'ordre commercial ou technique).

Le revers de la médaille est la nécessité d'un maillage important. Si un poste veut se connecter, il doit « accrocher » un voisin. Bien entendu il faut augmenter la portée des antennes, et faire en sorte que les postes soient en activité permanente, car chaque utilisateur est aussi un relai pour les suivants.

De plus, l'efficacité des liaisons est limitée par leur caractère asymétrique (différence de puissance d'émission entre, par exemple, un téléphone mobile et une station-relai) et par les nombreuses interférences qui viennent créer un phénomène de fading, même si différentes solutions sont à l'étude pour ne plus subir mais tirer pleinement partie de ce phénomène.

Des solutions sont en cours de test notamment au MIT (Massasuchet Institut of Technologie) de Cambridge (US). Des universités, des centres de recherche (tel l'Inria), des sociétés (Ozone) ainsi que de nombreuses associations travaillent et développent des réseaux wifi sans points d'accès (hot spot), c'est-à-dire en mode ad-hoc.

Les futures applications sont nombreuses : dans le domaine militaire, dans le domaine des secours et des services d'urgence et dans le domaine civil (connexion internet haut débit, réseaux citoyens…), de nombreuses villes développent des réseaux wifi ad-hoc. Même la NASA développe un système de communication wifi ad-hoc pour des véhicules d'exploration de Mars.

3) Les normes et protocoles utilisés

Le début des recherches sur des réseaux « Ad-Hoc multisauts » (« Ad-Hoc Multihop Network ») date des années 60 par la DARPA (Defense Advanced Reseach Project Agency), agence américaine de recherche dépendant de l'armée américaine.

Aujourd'hui la plupart des protocoles de routage spécifiques aux connexions Ad-Hoc et mobiles proviennent du groupe MANET (Mobile Ad-hoc NETwork), créé par l'IETF (Internet Engineering Task Force) en 1997.

Un réseau MANET se défini par des nœuds mobiles, possédant une ou plusieurs interfaces sans fil et disposant de fonction de routage. Cette fonction de routage permet à un paquet d'atteindre sa destination de nœud en nœud sans qu'il y ait de routeur désigné. D'autre part, le réseau est dynamique car les nœuds peuvent se déplacer et modifier constamment la topologie.

Les briques de base qui composent un protocole de routage MANET sont :

- une vue (partielle ou complète) de la topologie du réseau, par un échange de paquets de contrôle entre voisins ;
- un algorithme de calcul de route (MRCA : Mathematical Route Calculation Algorithm) permettant de trouver le meilleur chemin ;
- le temps de calcul de route, pour déterminer les nouvelles routes le plus en avance possible.

Ces protocoles sont donc une extension des protocoles de routage de l'IP fixe pou tenir compte de la mobilité des nœuds, ce qui est essentiel pour permettre aux réseaux ad-hoc maillés d'offrir les mêmes services qu'un réseau avec infrastructure.

B. Les techniques de routage

Pour offrir une connectivité plus étendue au sein d'un réseau mobile et auto-organisé, comme le sont les réseaux ad-hoc, il faut créer dynamiquement une connectivité multi sauts entre un ensemble de nœuds sans fil qui peuvent être en mouvement.

Ce besoin d'un protocole de routage pour trouver ces routes « multi sauts » est un véritable challenge face aux interférences et aux limitations de puissance.

La normalisation MANET fait apparaitre plus de 45 protocoles de routage différents, répartis en deux grandes familles :

- les protocoles réactifs, basés sur l'« inondation » du réseau ;
- les protocoles proactifs, basés sur une découverte topologique du réseau

Technique de routage utilisée	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)	
Etat du lien		OLSR (Optimized Link State Routing)

Tableau 1 : Principales techniques de routage

Ces différents protocoles sont en fait différents moyens adaptés à une situation de topologie dynamique d'effectuer une « distribution des chemins » en limitant les sauts (chemin optimal), en évitant les boucles (très néfastes car causant des pertes de paquets au

sein du réseau) et en minimisant l'« overhead » (données supplémentaires liées au contrôle de transfert et à la correction d'erreur).

Toutes ces solutions présentent des profils différents avec chacune leurs avantages et leurs inconvénients suivant le profil des réseaux et leur utilisation.

1) Les techniques réactives

Ces techniques, d'un fonctionnement assez simple, reposent sur une inondation du réseau et permettent de limiter au maximum l'échange de paquets de contrôle pour construire des tables de routage. Ceci s'effectue au prix de la consommation d'une grande quantité de ressources pour découvrir une simple route entre différents points du réseau.

AODV (Ad-hoc On-demand Distance Vector)

Ce protocole développé par la firme Nokia est particulièrement adapté aux réseaux qui affichent une topologie fortement dynamique.

La découverte de la route de fait par inondation : une route entre deux nœuds est envoyés suite à l'envoi d'une « Route Request ». Un signal de réponse « Route Response » est alors envoyé par un nœud voisin s'il est possible de se joindre à une route existante et il met à jour sa table de routage, puis par la destination lorsque celle-ci est atteinte.

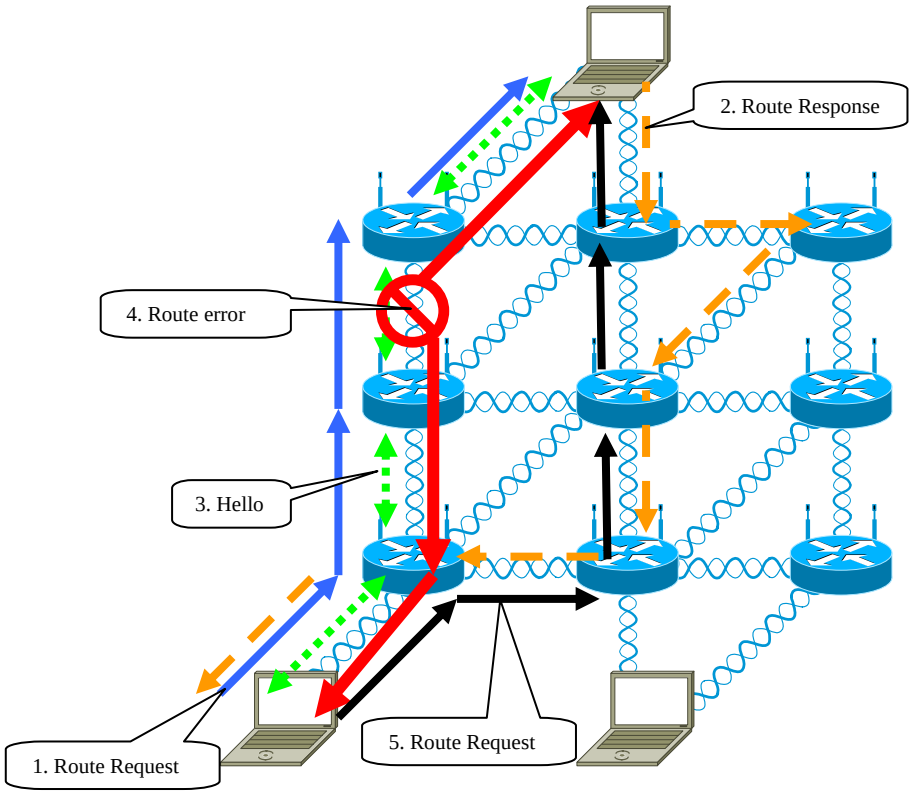


Figure 12 : Fonctionnement du routage AODV

Puis, les nœuds s'échangent des réponses périodiques, que l'on appelle parfois des messages « hello », pour installer et renouveler la validité de la route.

Quand elle n'est pas régulièrement mise à jour, une route expire (ceci correspond à un dysfonctionnement ou un « départ » du nœud qui quitte le réseau). Les nœuds restants qui ont une table de log avec les derniers utilisateurs de la route notifient ceux-ci pour enlever cette route (message de « Route Error ») et déclencher une nouvelle procédure de « Route Request ».

Les principaux défauts de ce mode de routage viennent de l'énorme overhead engendré par l'échange permanent des signaux « Hello » permettant de maintenir la validité de la route et du fait que le chemin suivi n'est pas garanti comme étant optimal, il s'agit en fait d'une route choisie aléatoirement parmi toutes les routes possibles.

DSR (Dynamic source routing)

Ce protocole à la particularité de ne pas nécessiter la présence de tables de routage sur les différents nœuds du réseau, puisqu'il repose sur le principe du routage par la source.

Pour initier un flux vers une destination, la source envoi une « Route Request » à tous les prochains nœuds, le message se propage de nœud en nœud jusque la destination.

Le destinataire reçoit donc plusieurs « Route Request » qui lui parviennent de différents nœuds voisins et choisit, selon un algorithme qui tient compte du nombre de « sauts » (algorithme dit de « shortest path ») minimisant le nombre de nœuds traversés et/ou de la qualité et de la rapidité des liaisons entre les nœuds. On espère ainsi arriver à l'établissement d'une route optimale.

La destination envoie alors un signal « Route Reply » vers la source en suivant le même chemin, mais dans le sens inverse. Ce qui permet à la source de disposer de l'ordre des nœuds à traverser, information que la source retranscrit dans tous ses paquets de données envoyés selon cette route.

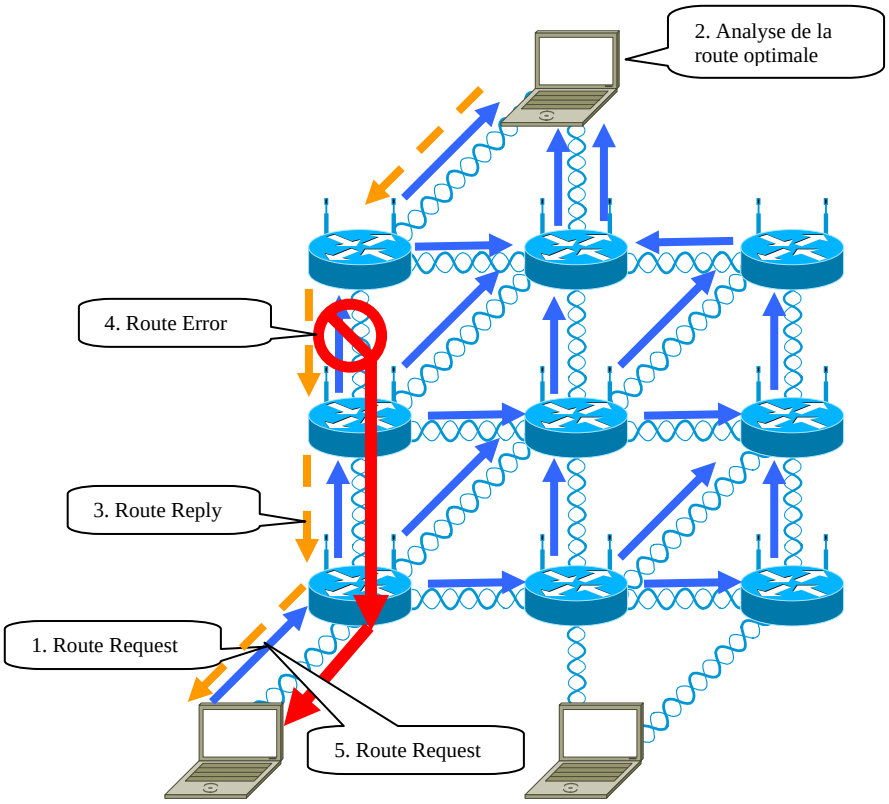


Figure 13 : Fonctionnement du routage DSR

En cas de dysfonctionnement ou de départ du $n^{ième}$ nœud de la route, le nœud n-1 ne parvient pas à joindre son voisin, il envoie alors un signal « Route Error » en remontant les nœuds du chemin. Quand ce message arrive à la source, celle-ci recommence une procédure de « Route Request ».

Ce protocole évite l'encombrement du réseau et la monopolisation des ressources en limitant l'échange d'informations de contrôle (messages « Hello » du protocole AODV) mais

on voit que chaque nouvel établissement de route se fait par l'envoi d'un flot de données assez significatif sur l'ensemble du réseau. De plus, ce protocole fait l'hypothèse de la symétrie des liaisons qui, dans de nombreux cas, n'est pas assurée : par exemple un téléphone cellulaire ou un PDA a beaucoup plus de capacité en réception depuis une borne émettrice que d'émission.

2) Les techniques proactives

Afin de limiter le flot de données lors des modifications de routes, qui doivent être mises à jour très régulièrement dans un réseau mobile, les techniques proactives reposent sur une découverte topologique du réseau préalable à l'établissement d'un chemin pour les données transmises.

DSDV (Destination Sequence Distance Vector)

C'est l'un des premiers protocoles mis au point par le groupe MANET et il s'inspire grandement du protocole RIP (Routing Information Protocol) utilisé dans le monde de l'IP filaire. On y a aujourd'hui pratiquement renoncé au profit l'AODV (des mêmes concepteurs) et le l'OSLR.

Ce protocole repose sur un vecteur de distance : chaque nœud possède une table (ou vecteur) de routage où chacune des lignes doit identifier :

- l'une des destinations possibles ;
- le nombre de sauts pour y parvenir ;
- le nœud voisin à traverser.

Le principal problème de ce type de protocole est la convergence des tables de routage qui n'est pas garantie, notamment à cause de la mobilité des nœuds au sein du réseau.

De plus, ce type de protocole génère encore un flot assez important de données, assez important, même pour les nœuds les moins mobiles.

OLSR (Optimized Link State Routing)

Ce protocole, l'un des plus récents et des plus performants, repose sur le concept d'« état du lien » : chaque nœud connait parfaitement la position des autres dans le réseau. Pour le routage, on choisit le chemin le moins coûteux (à la fois en nombre de sauts et en qualité/rapidité de liaison) en utilisant l'algorithme de Dijkstra sur un graphe étiqueté représentant la topologie du réseau.

Pour éviter l'inondation du réseau par messages de contrôles et la redondance, chaque nœud élit dynamiquement et périodiquement parmi ses proches un « représentant », appelé « Relais multipoint » ou MPR (Multi-Protocol Router, en anglais), dont l'ensemble va former un « backbone » (colonne vertébrale) de routage.

Peuvent devenir MPR les nœuds pouvant atteindre tous les autres nœuds se situant à une distance d'un ou deux sauts avec un lien symétrique.

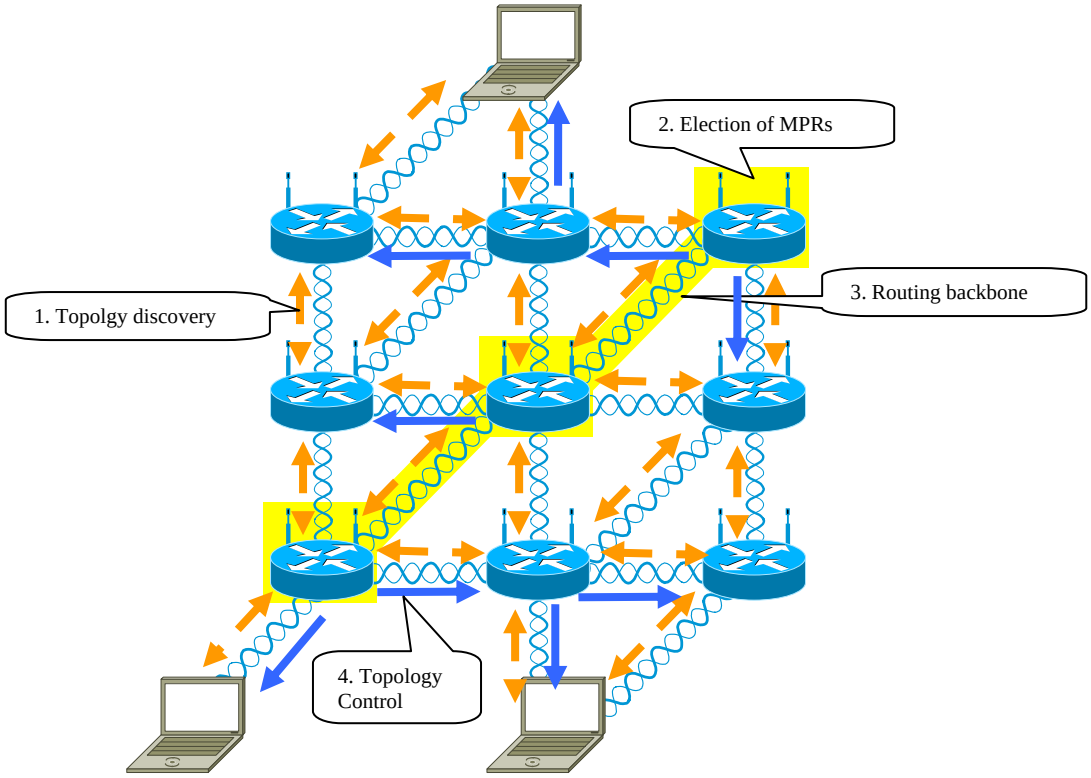


Figure 14 : Fonctionnement du routage OLSR

Par la suite, les MPR sont communiqués à tout le réseau par des messages nommés « Topology Control » qui permettent à tous les nœuds de mettre à jour leur table de routage. La suite du routage des paquets s'effectue comme dans la technologie IP filaire.

OLSR semble aujourd'hui être une des solutions retenues pour les réseaux tactiques par plusieurs nations : USA, Canada, Pays-Bas, Allemagne, etc... En France, le CELAR (département TEC/RX), appartenant au Ministère de la Défense (DGA), travaille depuis 3 ans, en partenariat avec l'INRIA de Rocquencourt (à l'origine du protocole de routage

OLSR), à l'évaluation de ce protocole (qualité de service, routage,…), et possède une plateforme expérimentale de 18 nœuds OLSR.

3) Comparaison de performances

Les performances de ces algorithmes sont dépendantes de différents paramètres du réseau, tels que le nombre de nœud (taille du réseau), le nombre de liens reliant chaque nœud (densité du réseau) et la disponibilité du réseau (probabilité qu'un lien connu soit en effet fonctionnel).

D'une manière générale, on peut constater que les protocoles réactifs, basés sur l'inondation, comme AODV et DSR ne garantissent pas une route optimale. D'un autre côté, les protocoles proactifs, utilisant une découverte de la topologie du réseau, comme le protocole OLSR, garantissent une route optimale et offrent la possibilité de changer de route « à chaud » en cas de défaillance, c'est-à-dire sans pour autant avoir à relancer une nouvelle « Route request ».

Au vu de ces conclusions, on pourrait conclure de la plus grande efficacité des protocoles proactifs. Pourtant, la réalité n'est pas aussi tranchée et dépend bien souvent de la structure du réseau.

Pour nuancer ce jugement, et mieux comprendre l'intérêt de ces différentes méthodes de routage, il faut mener des simulations ou effectuer des mesures exprérimentales.

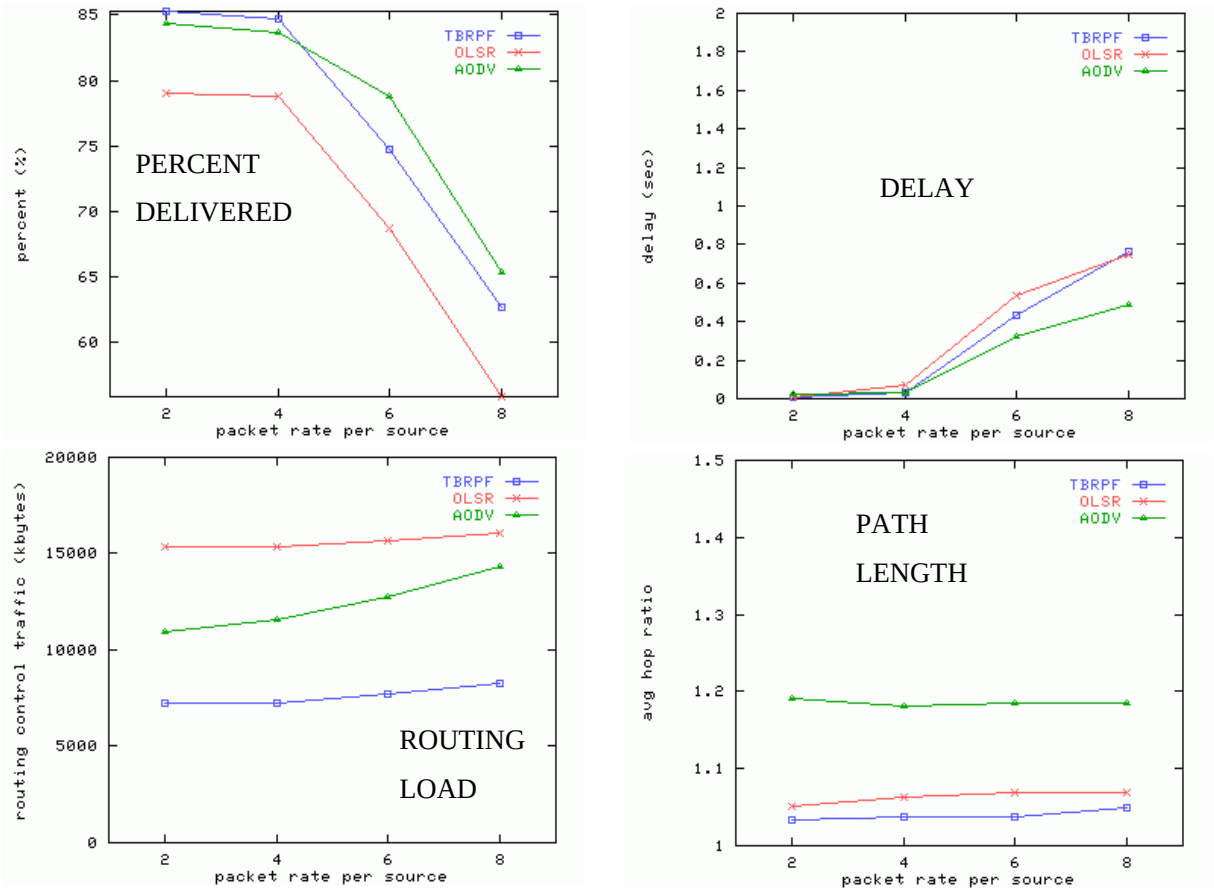


Figure 15 : Comparaison de performance des algorithmes de routage

C. Les enjeux

1) La qualité de service

Les protocoles étudiés plus haut s'inscrivent dans un contexte de routage au mieux.

Cependant, l'attrait suscité par les applications multimédia laisse penser que certaines applications pourraient tirer parti de certaines garanties qui pourraient être offertes par le réseau. Par exemple, garantir une borne sur le délai de transmission des paquets peut être profitable aux applications de téléphonie ; garantir un débit peut être nécessaire pour les applications de vidéo à la demande, etc. C'est pourquoi il semble important de s'interroger sur la meilleure façon d'assurer une certaine qualité de service aux stations d'un tel réseau. Le terme « qualité de service » regroupe un grand nombre de concepts et de techniques complémentaires.

Nous pouvons maintenant proposer une définition du routage avec qualité de service : il s'agit du processus d'établissement et de maintenance de routes optimales satisfaisant un certain critère sur la qualité de la transmission de données. Si l'on peut considérer que cet objectif sera bientôt atteint dans les réseaux locaux filaires, les réseaux ad hoc présentent un grand nombre de spécificités qui rendent la conception d'un tel algorithme difficile.

Nous avons vu que les protocoles classiques étaient assez gourmands en bande passante notamment les protocoles réactifs (AODV, DSR), or assurer une bande passante est un critère important en terme de qualité de service. Quant aux protocoles proactifs, ils mettent sérieusement en cause le délai d'attente avant la transmission.

Par conséquent, on s'aperçoit que les spécificités techniques dues au support de transmission engendrent des contraintes fortes pour la qualité de service en comparaison avec

les réseaux filaires. Cependant, des études sont en cours pour essayer de définir des protocoles intégrant cette qualité de service et reposant sur les méthodes de routage au mieux développées spécifiquement pour les réseaux ad-hoc.

Des études récentes tendent à montrer qu'à l'opposé des réseaux filaires où l'état des liens renseigne sur les capacités du réseau, dans un réseau ad hoc il vaut mieux considérer l'état des nœuds du voisinage. En effet, on a vu, dans les problèmes relatifs aux nœuds cachés ou exposés, que les voisins peuvent perturber l'état des transmissions. Le problème revient donc à considérer des hyperliens entre des ensembles de nœuds proches de la source et proches de la destination (théorie basée sur l'étude des hypercubes). Un hyperlien renseigne alors le protocole sur son utilisation globale des ressources du réseau, en termes d'accès au support et de consommation d'énergie. Un protocole a été proposé qui est basé sur le protocole réactif AODV.

2) La sécurité

Les réseaux ad hoc posent des problèmes spécifiques de sécurité : chaque nœud peut être un routeur et les protocoles de routage proposés partent du principe, par défaut, que tous les nœuds sont dignes de confiance. Les travaux sur OLSR précédemment menés à Supélec ont montré comment un nœud malicieux pouvait perturber le fonctionnement d'un réseau ad hoc. Des solutions adaptées pour l'authentification et la détection des intrusions ont été proposées dans le cadre de ces travaux.

Les travaux déjà réalisés ont fait l'objet de validations dans des contextes d'utilisation civils ; des études complémentaires doivent être menées pour prendre en compte les spécificités du domaine militaire.

OLSR est en effet à l'origine un protocole coopératif conçu pour fonctionner dans un environnement de confiance. Dans un contexte différent, dans lequel la capture d'éléments du réseau est possible, il faut mettre en œuvre des mécanismes permettant la neutralisation de ces équipements (bannissement).

Dans des scénarios de type CLAN (*Coalition LAN*), une politique de sécurité adaptée devrait permettre le partage de ressources pour le routage (afin d'étendre la zone de couverture et la densité du réseau) tout en conservant si nécessaire la confidentialité des communications de chaque groupe.

De plus, les solutions proposées doivent prendre en compte la géométrie particulière d'un réseau mobile. En particulier, les contraintes d'alimentation en énergie et la puissance de calcul disponible (pour la mise en œuvre de fonctions cryptographiques) sont des paramètres qui influent sur les choix possibles en fonction de la nature des équipements.

La cryptographie à clef publique qui est utile à l'établissement de clefs partagées entre nœuds n'est pas réaliste aujourd'hui. La demande en temps de calcul et en mémoire est si forte que le nœud n'est plus réactif pendant de longues périodes. Ce problème l'expose aux dénis de service. Les éléments sont également vulnérables à la capture physique. En effet, les nœuds sont fréquemment déployés en très grand nombre dans des milieux publics ou des environnements hostiles. Cela implique un coût aussi bas que possible et, de ce fait, force les fabricants à minimiser les questions d'inviolabilité de leurs dispositifs. Les protocoles de sécurité des réseaux classiques peuvent bénéficier d'une étape de configuration de chaque dispositif installé. Dans le cas des réseaux mobiles, leur déploiement massif nécessite au contraire des protocoles auto-configurables et un faible travail de préparation.

IV. Panorama des solutions pour étendre les réseaux actuels avec des solutions maillées

A. Introduction

Historiquement, les réseaux « mesh » ont été conçus pour les champs de bataille et les opérations de crise. Pour répondre aux attentes d'une armée américaine éparpillée et en mouvement, ces réseaux se devaient de présenter une architecture « dynamique et modulaire ». En clair, leur maillage peut se déformer, accueillir de nouveaux nœuds ou en abandonner, sans interruption du service.

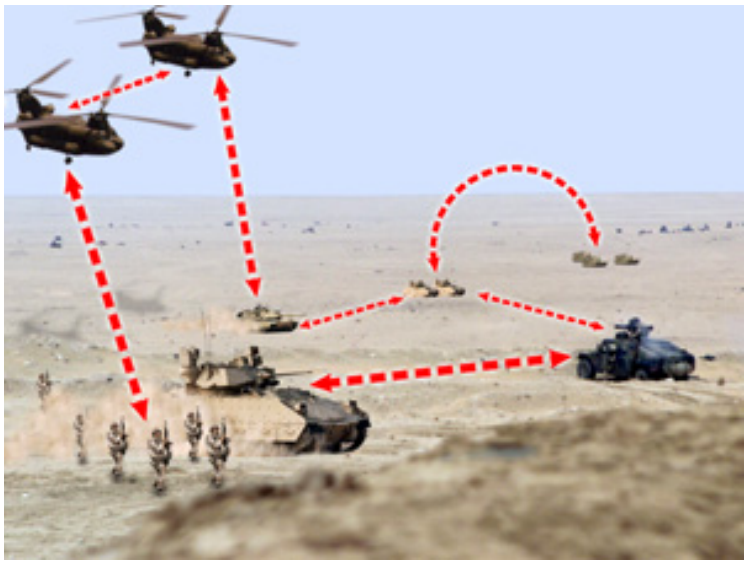


Figure 16 : L'armée américaine en terre étrangère n'a aucune infrastructure de communication. Les besoins de communication sont immenses et mettre en place une infrastructure serait trop long et très coûteux. Ils avaient besoin de communiquer efficacement sans déployer des infrastructures et pouvoir transférer des données à haute vitesse. Seule la solution mesh convient à ce genre de situation.

Cette caractéristique devient particulièrement intéressante dans un environnement urbain. Le signal se propage comme pour les systèmes d'échange « peer-to-peer » sur différents réseaux, privés ou publics. A mesure que progressera « l'urbanisation radio » des villes, qui accueillent de plus en plus de bornes et de relais émetteurs, on comprend que ce fonctionnement donnera lieu à des économies.

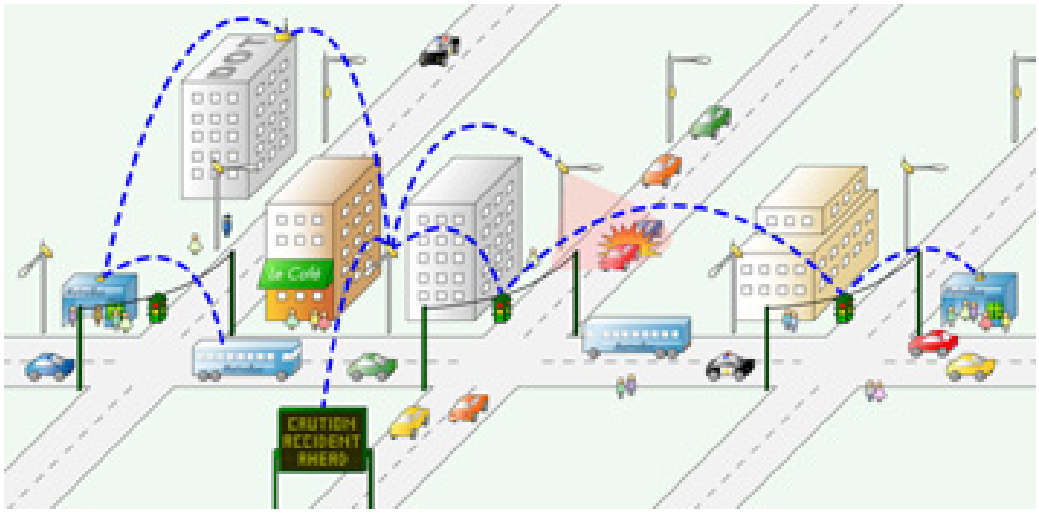


Figure 17 : Exemple d'implantation de réseau mobile maillé en milieu urbain

B. Applications courantes

Il existe de nombreuses applications pratiques pour un réseau maillé, la plupart ayant déjà été mises en place aujourd'hui :

- Couverture géographique étendue du Haut débit : campus, ville, village, parc etc.
- WISP commercial : vendre des accès haut début sans fil : (réseau à tolérance de panne, QOS etc.)
- Secteur public, administration, éducation, hôpitaux, universités, écoles etc.
- Projets sans fil coopératifs, communautaires : Village on-line, partage de bande passante entre voisins etc.
- Domotique : vers la maison intelligente ou « vivre dans le réseau »

On peut distinguer 3 grands types d'organisation d'un tel réseau, du plus pragmatique au plus idéaliste :

- propriétaire : dans une grande entreprise, on dispose des répéteurs pour couvrir une vaste zone de trafic modéré (un entrepôt, par exemple), ou des bâtiments où le câblage n'est pas envisagé (bâtiments historiques, temporaires...).
- collectif : A l'image de l'ancien réseau BiBop, on peut imaginer un réseau maillé urbain permettant aux utilisateurs, aux services de secours.... de se connecter n'importe où, même en roulant. Ce système serait un concurrent direct de l'UMTS (dans l'état où on le connaît actuellement), mais ne nécessitant pas l'ajout d'un nouveau protocole dans les machines.
- collaboratif : chaque utilisateur peut devenir un relais transparent pour la transmission de ses voisins. Si l'on suppose que les utilisateurs sont suffisamment nombreux pour constituer un réseau maillé dense dans un endroit, alors, les communications peuvent ainsi sauter de proche en proche jusqu'à leur destinataire ou, plus vraisemblablement, jusqu'à un point de concentration fixe.

Etendre la portée d'un réseau, améliorer la qualité de service, ajouter de la redondance et la stabilité à un réseau maillé est aussi simple que d'ajouter des noeuds !

Un noeud mesh ne requiert qu'un faible voltage et peut être alimenté par une batterie et un panneau solaire. Ainsi en diminuant la distance entre les noeuds, le signal s'en trouvera amélioré et par conséquent, la qualité des liens également.

L'inventeur d'Ethernet, Bob Metcalfe a déclaré que "la valeur d'un réseau augmente proportionnellement à son nombre de points de connections."

1) InfRadio : le champ de bataille de Jussieu

La faculté de Jussieu, actuellement en travaux pour cause de désamiantage, correspond à une configuration de "champ de bataille" telle que l'ont pensée les inventeurs des réseaux maillés : la topologie physique du campus varie dans le temps et il accueille beaucoup de passage. Dans le projet Infradio, chaque point d'accès sera transformé en routeur. Ce maillage radio relaiera les informations tout en conservant un nombre limité de points d'accès.

De ces problèmes d'urbanisation radio, la densité des routeurs constitue un paramètre crucial. L'intérêt de l'approche «Mesh » est que l'infrastructure est réduite car un équipement privé peut être utilisé à ce titre, évitant la location de locaux techniques pour les héberger. De plus, cette architecture est dynamique et modulaire dans le sens où il est simple d'insérer un nouveau routeur radio dans l'infrastructure, où, de les déplacer sans arrêt du service. Cette

caractéristique est particulièrement intéressante dans des environnements à dimension variable dans le temps ou l'espace (par exemple, réseaux de champs de bataille spontanés, réseaux en situation de crise, etc.)

InfRadio offre une connectivité au travers de 15 points d'accès déployés sur le campus de Jussieu. Dans la seconde phase du projet, le réseau sera étendu par des routeurs maillés sans-fil. Globalement, la couverture du campus de Jussieu est assurée dans les 6 zones représentées sur le plan suivant.

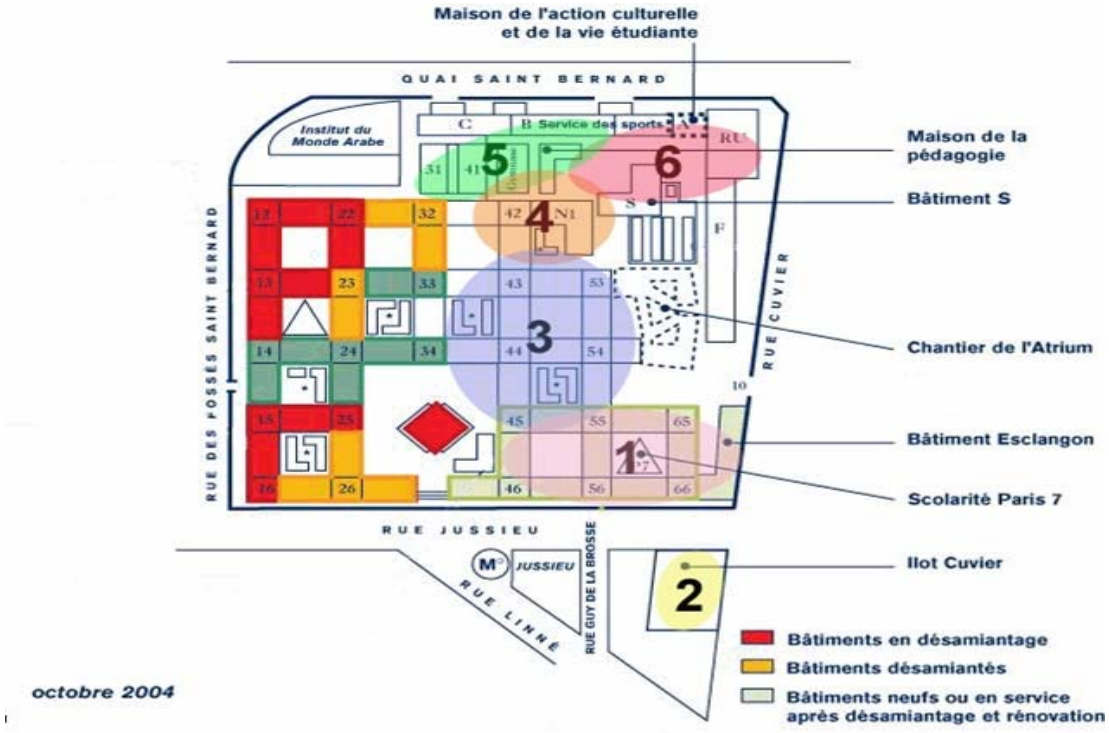


Figure 18 : Plan des zones de couverture du réseau sans fil sur le campus de Jussieu

2) La couverture du « Last Mile »

Un état des lieux

Zones blanches, zones grises, zones noires : ces cartes géographiques, qui indiquent les territoires auxquels l'espoir d'un raccordement à haut débit est plus ou moins permis, nous deviennent familières. Les petites communes enclavées sont mal parties face aux quartiers d'affaires, et les opérateurs téméraires qui ont cru, à grands renforts de discours et de levées de fonds ambitieuses, présenter une alternative viable, quittent silencieux et dévastés, le champ de bataille. La révolution numérique attendra, les vieux modems ne sont pas si lents, de toutes façons les sites eux-mêmes ne sont pas si rapides… Une ombre de résignation s'étend sur nos villages, qui resteront reliés par des chemins vicinaux au « Village global ».

Nous avons intériorisé ces contraintes. Même ce que nous faisons pour les contrer va dans leur sens : qui va assurer la collecte et la desserte ? Qui va payer pour le « dernier kilomètre », pour la liaison entre le dernier poste avancé du monde civilisé (un central téléphonique, généralement) et les habitants des contrées reculées ? L'aménagement numérique du territoire est généralement coercitif, trop souvent curatif, parfois même palliatif. Notre vocabulaire est imprégné de cette vision, produite par les grands opérateurs de télécommunication, et si proche d'une conception autoroutière des échanges. Mais peut-être est-il temps de quitter cette approche bloquante et verticale, de prendre les autoroutes de l'information à contresens.

Les réseaux maillés métropolitains

La topologie à nœuds métropolitains utilise les deux types de réseaux maillés. On les nomme « Backhaul » et « Last Mile »

Les « backhaul » sont soit des topologies point-à-point, soit des topologies point-à-multipoints. Leur conception vise à fournir un backbone aux nœuds « uplink » (voir la configuration des MeshAP). Les nœuds utilisent deux antennes, une étant directionnelle vers l'uplink, l'autre fournissant la connection au dernier kilomètre (last mile). Cette dernière antenne est souvent omni-directionnelle. La configuration des Backhaul par le WIANA utilise 2 realms, canaux et ESSID différents. Les clients n'utilisent pas le backhaul en tant que point d'accès. Sa mission principale est d'amener de la bande passante à différentes parties du « Last Mile ».Les nœuds « uplink » dans le backhaul fournissent des connection muti-redondantes à l'Internet filaire et ont plus de capacité que les 11Mbps radio. En fonction de la zone à couvrir, un certain nombre de backhaul peuvent d'avérer indispensable pour couvrir une grande ville.

« Last Mile » (le dernier kilomètre) est une topologie multipoints-à-multipoints. Ses nœuds ont une seule carte radio reliée à une antenne omni et sont reliées à l'antenne omni du backhaul. La différence entre les topologies « Last Mile » et « Multipoints-à-multipoints » est que la connection Internet ne vient pas d'un routeur filaire mais du maillage backhaul via un point central.

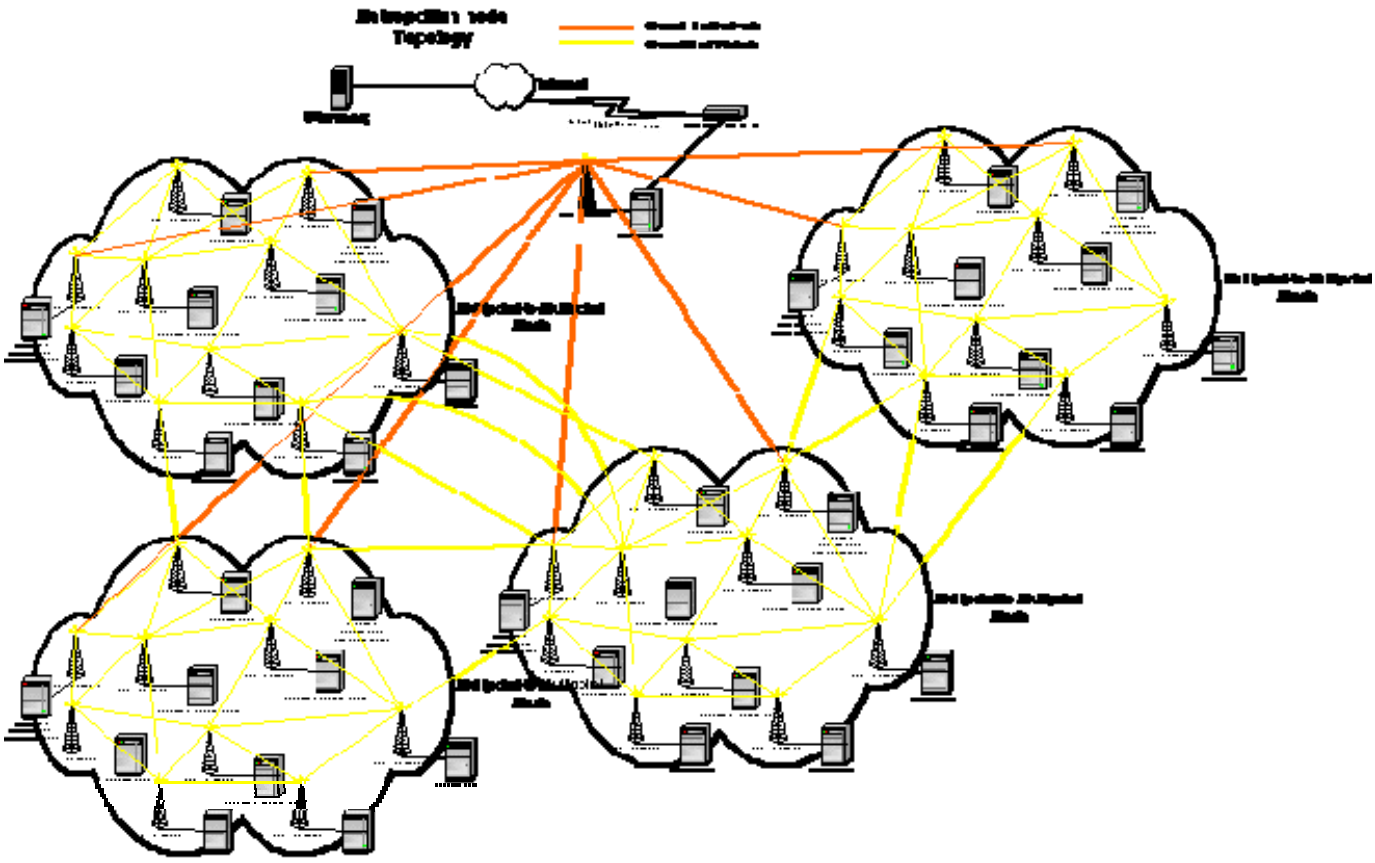


Figure 19 : Réseau maillé métropolitain

Ozone : le réseau métropolitain parisien

Les hot-spots pullulent dans les grandes villes, les gares et les aéroports. A ces bulles locales disjointes, Ozone oppose le « réseau omniprésent » (pervasive network). Objectif : vendre un accès Internet haut-débit par Wi-Fi, opérationnel chez soi comme à l'extérieur.

Ozone n'est pas le seul opérateur à s'intéresser au sans-fil pour la fourniture d'accès Internet, mais son approche diffère *radicalement. Ozone oppose aux hot spots de ses concurrents - pour lesquels les problèmes de connexion, de roaming et de facturation* se cumulent - un réseau dense et continu où l'accès à Internet s'effectue en Wi-Fi, chez soi comme à l'extérieur et sans changer d'appareil.

Pour l'instant, la plate-forme technique se rode dans le treizième arrondissement parisien (avant le quinzième) avec une centaine d'utilisateurs. Quatorze points d'implantation des antennes suffisent pour couvrir le secteur Est à un débit compris en moyenne entre 2 et 6 Mbit/s.

Ozone crée des MAN de dorsales sans fil métropolitains (les oBones) dans des agglomérations grandes et moyennes. La première des villes concernées est Paris. Ces MAN sont connectés à l'Internet par Ozone. Si ces MAN utilisent aujourd'hui la technologie Wi-Fi, ils pourraient à terme utiliser toute autre technologie.

Ces dorsales ont une double vocation :

- acheminer le trafic depuis/vers les différentes zones locales de couverture (oZones) mises en place par Ozone (voir ci-dessous)
- interconnecter entre eux les différents autres réseaux locaux sans-fil issus de l'initiative d'associations, d'organismes publics, d'entreprises, ou de particuliers.

Autour des points de présence créés sur le parcours de son MAN, Ozone crée des zones locales de couverture. A l'intérieur de ces zones, les utilisateurs ont la possibilité de se connecter au réseau d'Ozone et d'accéder à l'Internet. Cet accès est utilisable tant pour un usage domestique permanent, qu'en situation de mobilité.

Ozone fournira aux utilisateurs qui le souhaitent un équipement spécial, l'Ombrelle, construit par Ozone, qui leur permettra :

- D'isoler leur réseau privé du réseau public d'Ozone.
- De réémettre le signal d'Ozone en constituant un réseau ad-hoc selon un système de Mesh Network. Le réseau local devrait par conséquent s'étendre au fur et à mesure de la connexion de nouveaux utilisateurs.

Le RéseauCitoyen

Imaginez alors une ville où les habitants peuvent communiquer grâce à un réseau libre d'accès, sans obligation de contrôle et de gestion par un organe centralisateur, sans restriction géographique ni zone d'exclusion, sans frais d'usage (mis à part l'électricité), sans abonnement... Or le coût pour rejoindre un tel réseau est comparable à celui d'un GSM milieu de gamme.

Pour y arriver, des individus déploient spontanément chez eux un PC (souvent récupéré dans les poubelles de grosses corporates) équipé d'une carte WiFi à laquelle on raccorde éventuellement une antenne HomeMade (bricolée maison). Avec ce type d'équipement, ReseauCitoyen a réalisé des connexions entre des ordinateurs distants d'une vingtaine de kilomètres. Une ou plusieurs cartes Ethernet classiques peuvent alors assurer une

interconnexion entre les parties filaires et sans fil. L'utilisation d'un système d'exploitation libre et gratuit permet d'atteindre ces objectifs de liberté de diverses manières.

Chacun de ces PC devient alors un « nœud » (node) du réseau en gestation. Tant que le réseau n'est pas connexe, il n'est pas... Pourtant il faut passer par là. Au début, les nœuds sont éloignés les uns des autres et ils ne se voient pas (c'est une contrainte technologique, les antennes doivent « se voir ») et donc ne communiquent pas. Puis, au fur et à mesure que de nouveaux nœuds s'allument, les premières connexions intermittentes surviennent. Ensuite la première connexion "permanente" s'établit. Suivie d'une autre, dans un autre quartier de la ville. Puis d'une autre, et d'une autre encore et d'un "brin" à plusieurs... Des segments qui peu à peu fusionnent en une pelote autogérée.

Techniquement, le routage des paquets d'information (au sens TCP/IP) se fait grâce à l'utilisation du protocole AODV. C'est un protocole de routage conçu pour des réseaux sans fil Multi-Hop en mode Ad-Hoc. Multi-Hop signifie que les paquets transitent par des routeurs intermédiaires avant d'atteindre leur destination. Ad-Hoc indique que le réseau est exclusivement composé de routeurs égaux entre eux. Une particularité de tels réseaux est la possible réutilisation du même spectre simultanément en deux zones du réseau pour transmettre de l'information différente. Un tel réseau est l'exemple parfait de ce que pourrait être fait avec cette technologie du « Mesh Network ».

ReseauCitoyen est en train de prouver que ce rêve peut être une réalité.

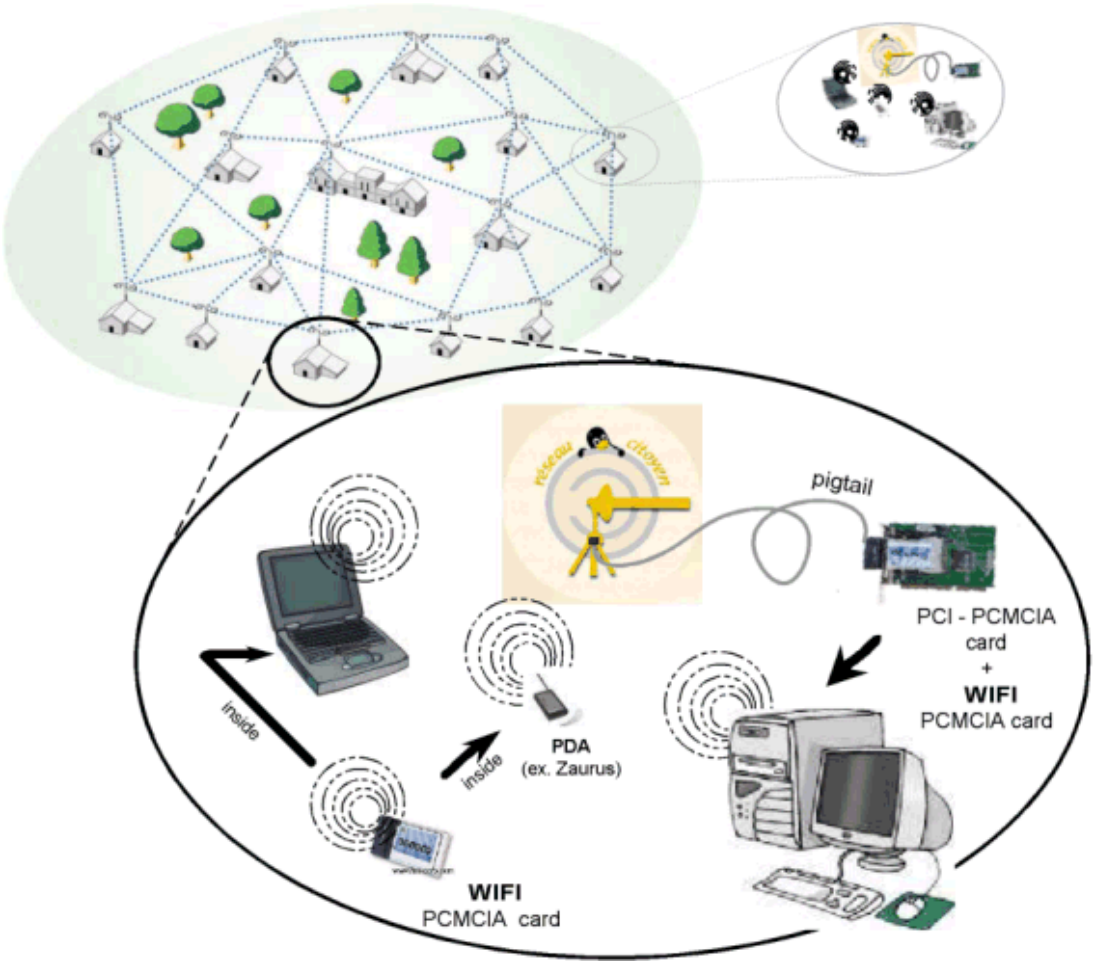


Figure 20 : Réalisation du RéseauCitoyen

Conclusion

Le développement des technologies radio force les cités à les considérer comme une solution à la connexion des derniers mètres. L'implantation dans les équipements des normes pour les réseaux métropolitains sans fil (comme le 802.16) et la commodité des appareils sans fil rendent les réseaux métropolitains sans fil moins cher et plus facile à déployer.

Aujourd'hui, la première raison pour construire de tels réseaux est de fournir des connexions à l'Internet à haut débit, lorsque seules des connexions téléphoniques sont disponibles. Ils se trouvent principalement dans les zones rurales ignorées par les câblo-opérateurs et les fournisseurs DSL.

Mais, dans un futur proche, les raisons pour construire de tels réseaux seront :

- Réduire les coûts de télécommunications des villes, tout en satisfaisant des objectifs socio-économiques
- Créer une infrastructure à ultra-haut débit qui ne sera pas l'otage d'une seule entité commerciale, mais ouverte à une diversité de fournisseurs (l'idée est qu'une telle infrastructure conduise le développement économique).

Des matériels bon marché et une politique de liberté pour l'allocation des fréquences radio pourront ensemble permettre la réalisation de réseaux métropolitains comme solution de connexion des derniers mètres, très attractive pour les villes.

3) La ville intelligente ou « vivre dans le réseau »

Le service public interconnecté

- Des véhicules de police très branchés.
- La compagnie Mesh Networks est capable de transformer tout véhicule de police, équipé d'un portable, en un bureau mobile assez performant. En déplacement, les policiers ont accès à des bases de données, à des caméras de surveillance ou à des outils de reporting qui leur permettent d'éclairer leurs décisions.
- Des véhicules secours très communicants.
- Lors d'un incident, l'efficacité des secours repose souvent sur la qualité des communications qui peuvent être établies entre les différentes unités. Les réseaux de Mesh Network peuvent aider des équipes en déplacement à se synchroniser ou à surveiller à l'aide de caméras l'évolution d'un phénomène.
- Des transports publics reliés en permanence à Internet.
- Avec la technologie de Mesh Networks, les hot spots peuvent être rendus mobiles : autrement dit une ligne complète d'autobus, voire de métro, pourrait être connectée à Internet sur toute la durée du trajet. Ainsi le concept de "hot route" est en train de supplanter celui de "hot spot".

Z-Wave : La technologie sans fil des petites structures

Commercialisée par une compagnie appelée Zensys, la technologie Z-Wave™ représente un important progrès technologique. Elle fonctionne à partir de radio fréquences (RF) sur un réseau maillé utilisant un protocole de communications bidirectionnelles. Cette technologie sans fil permet le contrôle et la surveillance des appareils courants de la maison.

La technologie Z-Wave™ a été conçue pour le contrôle des résidences et des petits édifices commerciaux ainsi que pour les applications telles que relevés de compteur, contrôle de luminaires et d'appareils ménagers, système CVCA, contrôle d'accès, détection d'intrus, détection d'incendie, etc.

Un nombre croissant de sociétés travaillent présentement à la conception de produits utilisant le protocole de communications Z-Wave™. Advanced Control Technologies (ACT) ont été les premiers à utiliser la technologie Z-Wave™. Ils fabriquent le système de contrôle de lumières et d'appareils HomePro ainsi que l'interface PC (USB) à Z-Wave™. D'autres produits seront bientôt disponibles : détecteurs de mouvements, détecteurs de fumée, détecteurs d'humidité, détecteurs pour porte et fenêtres.

La technologie Z-Wave™ permet aux produits de différents manufacturiers d'interagir au moyen d'une plateforme commune. Zensys est d'avis que les consommateurs apprécieront de plus en plus les avantages d'un système de domotique permettant l'interaction de différents produits.

Par exemple, un système de contrôle d'accès possède une valeur accrue en association avec un système d'alarme et un système de contrôle de luminaires. L'avenir du domaine de la domotique donnera l'opportunité à plusieurs sociétés de coopérer afin d'offrir aux consommateurs des solutions intéressantes et attrayantes.

Figure 21 : Produits à base de puces Z-Wave

- Starter Pack (2 Modules pour prises + 1 télécommande)

- Module USB pour diriger tous les équipements depuis un PC

ZigBee

Beaucoup moins connue que Bluetooth, ZigBee est une norme de transmission de données sans fil permettant la communication de machine à machine. Sa très faible consommation électrique et ses coûts de production très bas en font une candidate idéale pour la domotique ou les matériels de type capteur, télécommande ou équipement de contrôle dans le secteur industriel.

Zigbee (également connue sous le nom IEEE 802.15.4) n'est pas issue de nulle part puisque c'est le prolongement de la norme HomeRF (Home Radio Frequency) qui a, depuis son lancement en 1998, été dépassée par le Wi-Fi.

Les débits autorisés sont relativement faibles, entre 20 et 250 Kbits/s, mais c'est véritablement sa très faible consommation électrique qui en fait son atout principal. Zigbee fonctionne sur la bande de fréquences des 2,4 GHz et sur 16 canaux. Sa portée était au début d'une dizaine de mètres, elle est désormais de 100 mètres.

De nombreux industriels - parmi lesquels Honeywell, Mitsubishi, Motorola, Philips et Samsung - sont partie prenante dans l'élaboration et la diffusion de la norme. Ils appartiennent d'ailleurs tous à la ZigBee Alliance, association visant à promouvoir la technologie.

Les débouchés dans le secteur de la domotique sont importants, vu la prolifération - par exemple - des télécommandes. ZigBee a notamment été créée pour répondre au besoin exprimé par le marché de voir se créer une technologie de réseau sans fil domestique (Home Area Network - HAN) qui soit bon marché, basée sur des standards et capable de supporter de faibles échanges de données, en consommant peu, de manière sécurisée et fiable.

Figure 22 : Produits Ember à base de puces ZigBee

Conclusion

En dehors de ces applications commerciales, et à l'instar du peer-to-peer, ces nouvelles architectures de réseau incluent également une dimension politique qu'il ne faut pas négliger. Outre les solutions techniques qu'elles proposent, plusieurs sociétés du domaine donnent également naissance à des associations destinées à la promotion de réseaux sans fil citoyens, incitant fortement les utilisateurs à s'emparer du concept. On parle d'internet « organique », de « renaissance », ou d'internet « tel qu'il devrait être ». Et on évoque de multiples applications potentielles, comme des serveurs de jeu mis à disposition de la communauté, du peer-to-peer de voisinage, de la télévision et des radios en accès libre et local, ou du contenu accessible à haut débit sur des mobiles. En somme, on décrit un réseau « libéré des limites du corporatisme et des stratégies commerciales, qui cesserait de privilégier la recherche de profit au détriment de la performance, et serait géré par les utilisateurs, pour les utilisateurs" »

C'est bien aussi de cela dont il s'agit ici. Le « Mesh networking » pourrait réussir là où Wifi seul a partiellement échoué, en devenant une technologie privilégiée, bon marché et « plug and play », pour créer des réseaux métropolitains sans-fil efficaces et autogérés et, probablement, donner naissance à de nouveaux usages, voire définir le visage d'une nouvelle citoyenneté urbaine. Bien que de multiples associations s'y emploient, de tels réseaux Wifi ne sont pas encore très répandus, en France notamment, et l'utilisation du Mesh pourrait accélérer l'appropriation de Wifi par les citoyens.

Bibliographie

Les Réseaux Edition 2005, **Guy Pujolle** (Eyrolles)

Initiation aux réseaux : cours et exercices, **Guy Pujolle** (Eyrolles)

Réseaux de mobiles et réseaux sans fil, **Khaldoum Al Agha, Guy Pujolle et Guillaume Vivier** (Eyrolles)

Télécoms 1 : De la transmission à l'architecture des réseaux, **Claude Servin** (Dunod)

Boucles d'accès hauts débits, **Maurice Gagnaire** (Dunod)

Introduction aux réseaux, **Xavier Lagrange et Dominique Seret** (Hermes)

Détection d'intrusions dans les réseaux ad-hoc, **Jean-Marc Percher et Bernanrd Jouga** (Supélec)

Cours de réseau, **Bénédicte Le Grand** (http://www-rp.lip6.fr/~blegrand/)