

CHAPITRE 1

LES RÉSEAUX SANS FIL

1.1 Introduction

Ces dernières années, les téléphonies sans fil et mobile ont connu un essor fulgurant. Cet essor est dû principalement à la commercialisation et l'émergence des appareils de communication (téléphone portable, ordinateurs portable, assistants personnel portable, etc.) et la convergence des réseaux fixes et mobiles. Le domaine des réseaux mobiles ne se limite pas à la communication téléphonique et aux réseaux cellulaires. Un utilisateur ne veut plus se limiter à un lieu ou un temps pour consulter son courrier électronique ou naviguer sur Internet. Actuellement, les applications mobiles les plus utilisées sont la connexion réseau et les services de données associés. Une telle application est généralement réalisée à l'aide d'un réseau sans fil basé sur une infrastructure fixe : le terminal sans fil se connecte à un point d'accès du réseau via une communication sans fil, puis le reste de la connexion s'effectue sur l'infrastructure filaire réseau. Un utilisateur doit se trouver dans la zone de communication (zone de couverture) du point d'accès pour qu'il puisse se connecter au réseau. Sur une géographie étendue, la mise en place d'une infrastructure fixe conséquente est nécessaire avec l'établissement d'un nombre important de points d'accès. Ce déploiement est coûteux en termes de réalisation et matériel, de configuration et de temps [Lassous (2004)].

Une solution pour remédier à ces limitations consiste à utiliser les réseaux sans infrastructure fixe. Dans ce genre de réseau la portée de transmission des terminaux sans fil détermine ceux qui peuvent communiquer directement les uns avec les autres. La communication ne doit pas se limiter entre les terminaux à portée directe mais elle doit

s'étendre entre les terminaux à portée non-directe, ce qui nécessite que les terminaux soient capables de relayer les paquets. Ce réseau est capable de s'auto-initialiser et s'auto-configurer quand la topologie du réseau change suite au mouvement des mobiles sans aucune intervention d'un opérateur. Un tel réseau est appelé un réseau *ad hoc*. Il est possible d'obtenir les services Internet dans un réseau *ad hoc* en lui ajoutant des points d'accès connectés à l'Internet. Les réseaux *ad hoc* présentent de nombreuses avantages : ils permettent une mobilité sans contrainte, ils ne nécessitent aucune installation et sont faciles à déployer, ils sont flexibles et faciles à utiliser. Les applications des réseaux *ad hoc* sont nombreuses dans les domaines militaire et civil.

Vers la fin des années 1980, la recherche pour les applications militaires a été intensivement déployée à travers la planète. Le besoin de créer des standards ouverts dans le domaine des communications entre ordinateurs s'est fait sentir et un groupe de travail au sein de l'IETF³, nommé MANET⁴, a été formé pour établir des standards sur les protocoles et les spécifications fonctionnelles des réseaux *ad hoc*. L'objectif principal de ce groupe de travail consistait à fournir une standardisation pour la fonctionnalité de routage afin qu'elle supporte une infrastructure de réseau mobile capable de s'auto-organiser.

1.2 Les réseaux *ad hoc*

Dans un réseau *ad hoc*, une communication entre source et destination est généralement acheminée par des nœuds (terminaux) intermédiaires. La source et la destination ne sont pas nécessairement accessibles directement, les nœuds intermédiaires devant relayer le trafic de la source vers la destination. Les terminaux doivent s'auto-organiser et collaborer pour acheminer le trafic, d'un nœud à un autre. Toutes les fonctions doivent

³ IETF : *Internet Engineering Task Force*, organisme de standardisation des protocoles d'Internet

⁴ MANET : *Mobile Ad hoc Network*

être déployées automatiquement sans paramétrages éventuels de l'utilisateur. À cet environnement multi saut à nœuds hétérogènes s'ajoute la mobilité potentielle de chaque nœud : chaque terminal est libre de se déplacer dans n'importe quelle direction et avec n'importe quelle vitesse, obligeant ainsi une adaptation dynamique du réseau.

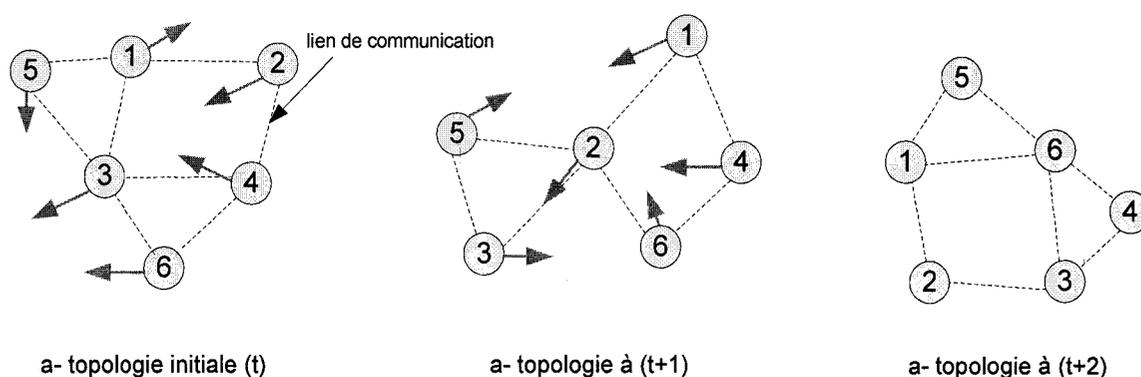


Figure 1 La topologie change dans un réseau *ad hoc*

La figure 1 illustre l'exemple d'une topologie dynamique pour un réseau sans fil *ad hoc*. Les liens radio entre les nœuds sont schématisés par des traits discontinus. Le sens de déplacement de chaque nœud est représenté par un vecteur. Au cours du temps, le déplacement des nœuds entraîne non seulement le changement de voisinage pour chaque nœud mais aussi la topologie globale du réseau.

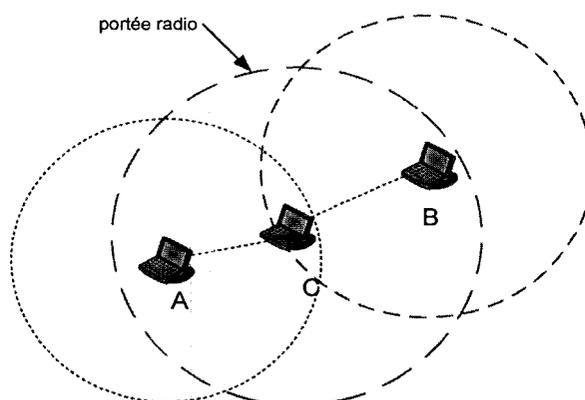


Figure 2 Principe de relayage dans un réseau *ad hoc* sans fil

Un réseau *ad hoc* utilise un médium radio avec des communications partagées. La portée des transmissions radio étant limitée, le relayage est alors obligatoire. Comme illustré dans la figure 2, le nœud *A* doit passer par *C* pour communiquer avec *B*. Dû aux évanouissements locaux du signal, le médium physique change et par conséquent la topologie change rapidement. Cet effet s'ajoute à la mobilité des nœuds.

Dans un réseau *ad hoc*, les nœuds sont équipés d'émetteurs et de récepteurs sans fil utilisant des antennes qui peuvent être omnidirectionnelles (*broadcast*), fortement directionnelles (point-à-point), probablement orientables, ou une combinaison de tout cela. Il y a une connectivité sans fil qui existe entre les nœuds sous forme de graphe multi saut aléatoire⁵ qui dépend de la position des nœuds, de la configuration de leur émetteur-récepteur, des niveaux de puissance de transmission et de l'interférence entre les canaux.

1.2.1 Caractéristiques des réseaux *ad hoc*

Comme nous venons de le voir, les réseaux *ad hoc* possèdent des caractéristiques très spécifiques. Ces caractéristiques sont différentes de celles des réseaux filaires et des réseaux cellulaires avec station de base. Les principales caractéristiques sont les suivantes :

- **Absence d'infrastructure** : à l'opposé des réseaux cellulaires où une station de base est chargée de la gestion et de l'acheminement des appels, les terminaux dans les réseaux *ad hoc* sont eux-mêmes chargés par ces fonctionnalités. Pour que le réseau fonctionne, il faut que chaque nœud soit volontaire pour relayer le trafic des autres participants.

⁵ RFC 2501 : www.ietf.org/rfc/rfc2501.txt

- **Communication multi saut** : une source et sa destination peuvent ne pas se retrouver à l'intérieur de la même portée radio. Dans ce cas, la communication source-destination nécessite le support des autres nœuds intermédiaires pour pouvoir véhiculer les paquets de données.
- **Liaisons à débit variable et à bande passante limitée** : les liaisons sans fil auront toujours une capacité inférieure à leurs homologues câblés. De plus, le débit réel des communications sans fil, après avoir déduit les effets des accès multiples, du *fading*, du bruit, des interférences, etc., est souvent inférieur aux taux de transfert maximum de la radio. Un système de communication radio se caractérise par un taux de perte assez élevé⁶. Ainsi, il est nécessaire que le trafic de gestion du réseau occupe le minimum de la bande passante possible afin de préserver le reste pour le trafic de données.
- **Topologie dynamique** : les nœuds sont libres de se déplacer arbitrairement, de telle sorte que la topologie du réseau, typiquement multi saut, peut changer aléatoirement et rapidement, et peut être constituée à la fois de liaisons unidirectionnelles et bidirectionnelles. Une infrastructure temporaire peut se former à n'importe quel moment et sous n'importe quelle forme. Un lien actif entre deux nœuds peut devenir brusquement non valide dû aux phénomènes d'évanouissement multi-chemin (*multipath fading*), à l'accès multiple, au bruit et à l'interférence d'autres transmissions. Un tel lien de communication est considéré non fiable, et on peut avoir recours à la retransmission pour avoir des services fiables.

⁶ Dans un environnement sans fil on parle d'un taux d'erreur de l'ordre de 10^{-3} alors qu'il est normalement de l'ordre de 10^{-9}

- **Utilisation limitée d'énergie** : une partie des nœuds d'un réseau *ad hoc*, ou encore l'ensemble des nœuds, peut dépendre des batteries ou d'une autre source d'énergie limitée qui peut s'épuiser rapidement. Pour ces nœuds, le plus important est sans doute de mettre en place des mécanismes capables de limiter la consommation de l'énergie.
- **La qualité de service** : la qualité de service (QoS) définit un ensemble de règles permettant, entre autres, le transport de trafic isochrone ou temps réel tels que la téléphonie ou la vidéo. Les modèles proposés dans les réseaux filaires ne sont pas viables dans un environnement comme celui des réseaux *ad hoc*.
- **Sécurité physique limitée** : les réseaux sans fil mobiles sont généralement plus sensibles aux menaces physiques que ceux qui sont câblés et fixes. La possibilité accrue d'attaques par écoute du canal est réelle. Les techniques existantes pour la sécurité des liaisons sont souvent appliquées au sein des réseaux sans fil pour réduire les risques d'attaques. Il est donc indispensable de définir pour les réseaux *ad hoc* une politique qui assure une sécurité stricte basée sur des mécanismes tels que l'authentification, le contrôle d'intégrité, le chiffrement, etc.

1.2.2 Principe d'auto configuration

Afin d'assurer une auto configuration, chaque nœud doit être capable de collecter et de maintenir suffisamment d'information sur la topologie du réseau [Murthy et Manoj (2004)]. Ces informations sont alors stockées dans deux types de tables :

- **Table des voisins** : chaque nœud maintient une liste de ses voisins à un saut obtenu grâce à l'envoi périodique d'un paquet de contrôle appelé *hello* par chaque nœud amorçant son existence. Seuls les voisins avec lesquels le nœud a un lien radio (les nœuds se trouvant dans la portée de transmission) seront retenus dans la table des voisins; la qualité d'un lien sera calculée en fonction du nombre de paquets reçus d'un voisin sur un intervalle de temps donné; cette métrique permet de garder tous les voisins pour lesquels le lien radio est stable.

- **Table de routage :** Cette table indique, pour chaque nœud, une destination possible dans le réseau et l'identité du nœud vers lequel les paquets doivent être relayés ainsi que le nombre de sauts restant avant d'atteindre la destination; une telle table sera construite à l'aide des paquets *hello* : au lieu d'indiquer sa seule identité dans ces paquets, comme indiqué précédemment, chaque nœud ajoute à son identité la liste de ses voisins à un saut; les nœuds recevant de tels paquets vont donc connaître leurs voisins à un saut et leurs voisins à deux sauts; en répétant ce principe, chaque nœud va connaître sa distance en nombre de sauts et l'identité du nœud voisin à qui il doit transmettre les paquets. Le but de la table de routage est de choisir la meilleure route jusqu'à la destination.

1.2.3 Accès au médium radio

Dans un réseau sans fil, deux mobiles peuvent communiquer en émettant des ondes radio. Ils se partagent un médium unique mais ne peuvent pas émettre en même temps. En effet, deux émissions simultanées sur le même canal entraînent une perte d'information à l'intersection des deux zones de communication (on parle alors de collision).

Pour pouvoir construire les tables de routage et réaliser le routage, il est indispensable de s'assurer que chaque nœud dans le réseau est capable d'accéder au canal radio afin de pouvoir émettre ses paquets. En effet, le canal est partagé entre les différentes entités et par conséquent un protocole d'accès au médium radio est nécessaire. Le protocole utilisé dans les réseaux radio par paquets (PRNet)⁷ est basé sur la technique CSMA (*Carrier Sense Multiple Access*). Cette technique assure qu'un nœud ne pourra commencer une émission si un autre nœud, dans son voisinage, est en train d'émettre sur le canal. Pour ce faire, chaque nœud va écouter le médium avant son émission potentielle. Si ce

⁷ Packet Radio Network

médium est occupé par une transmission en cours, alors la radio n'envoie pas son paquet et attend que le médium devienne libre. Cependant, avec cette technique, on ne peut pas empêcher deux transmissions de commencer en même temps. Afin de réduire la probabilité de transmission concurrente, un temps d'attente aléatoire est ajouté à la technique CSMA. Une fois que le médium est libre, le nœud qui cherche à émettre devrait attendre pendant un temps choisi aléatoirement. Si au bout de ce temps, le canal est toujours libre, alors il peut émettre sinon il recommence le processus (attendre que le médium soit libre puis choisir un temps d'attente aléatoire). Toutefois, des transmissions concurrentes peuvent avoir lieu dans le cas de nœuds cachés. Dans ce genre de situation, deux nœuds indépendants (non à la portée de communication) cherchent à communiquer avec le même destinataire. Par exemple, la figure 3 nous montre que les nœuds *A* et *B* veulent communiquer avec le même nœud *C*. Comme *A* et *B* ne sont pas à portée de communication, ils ne détectent pas leur activité réciproque sur le canal radio, et par conséquent, ils considèrent que le médium est libre et ils peuvent émettre leurs paquets. Ainsi, il y aura une collision au niveau du récepteur qui ne comprendra aucune des deux communications.

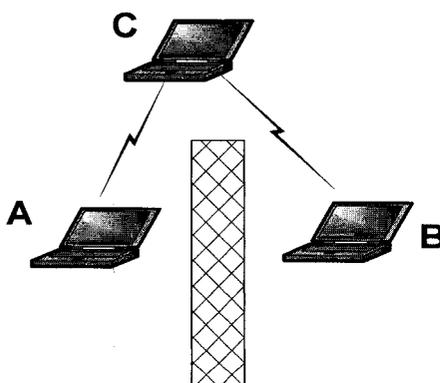


Figure 3 La collision se produit en *C* si *A* et *B* transmettent en même temps

La technique CSMA combinée à un temps d'attente aléatoire ne règle pas tous les problèmes. En effet, elle permet un accès simple au médium radio : aucune information ne peut être collectée ni mise à jour, et elle ne permet que la détection d'un signal sur le canal, le mécanisme étant complètement distribué (on n'a pas besoin d'une connaissance globale de tout le réseau). L'environnement voisin à lui seul suffit pour prendre la décision d'accès ou non au canal.

1.3 Classification des réseaux *ad hoc*

Les réseaux *ad hoc* peuvent être classés suivant deux catégories : les réseaux *ad hoc* statiques et les réseaux *ad hoc* dynamiques. Bien que la mobilité d'un terminal soit une des caractéristiques des réseaux *ad hoc* sans fil, il existe des situations où l'environnement du réseau est considéré comme statique. Dans un réseau statique, tous les terminaux ne se déplacent pas ou ils se déplacent rarement par rapport à leurs positions physiques. Alors que dans un réseau mobile la totalité ou la plupart des nœuds se déplacent d'une position à une autre de telle sorte que la topologie change. Un exemple de réseau *ad hoc* statique est le réseau de capteurs où les capteurs sont déployés sur des objets fixes. Un réseau *ad hoc* mobile peut être formé par des dispositifs (PDA, *laptop*, téléphone, etc.) qui sont utilisés par l'être humain et par conséquent ils ne sont pas fixes.

1.3.1 Les réseaux de capteurs sans fil

Les réseaux de capteurs sans fil (*Wireless Sensor Networks*) sont généralement formés pour surveiller un environnement éloigné ou inhospitalier comme par exemple : contrôle environnemental, mesure ou surveillance en climatologie, contrôle de processus, défense, etc. Un réseau de capteurs est caractérisé par :

- un emplacement non-déterministe des nœuds capteurs,
- un grand nombre de nœuds,
- une énergie limitée pour chaque nœud.

Une fois que les nœuds capteurs sont déployés, ils doivent réaliser la fonction de détection ainsi que la communication en utilisant leur propre énergie qui est généralement une batterie de faible autonomie. Ceci engendre un réseau avec une durée de vie limitée.

Maximiser la durée de vie d'un réseau est l'un des principaux objectifs des réseaux capteurs sans fil. Pour atteindre cet objectif, l'énergie provenant de la batterie doit être suffisante pour réaliser les tâches de détection, de routage et de communication. Une étude réalisée par Benini *et al.* [Benini *et al.* (2000)] a montré que les batteries ont approximativement deux fois plus d'autonomie si elles sont déchargées pendant une courte durée avec une période assez longue de repos. Les résultats de cette étude ont révélé que la durée de vie d'un réseau peut croître si on arrive à trouver de multiples ensembles exclusifs de nœuds actifs où chaque ensemble contient des nœuds capteurs qui couvrent la zone de surveillance. Slijepcevic et Potkonjak ont proposé [Slijepcevic et Potkonjak (2001)] une heuristique pour déterminer des ensembles mutuellement exclusifs des nœuds capteurs où chaque ensemble couvre une zone entière de surveillance. Ce problème est connu sous le nom *Set K-Cover Problem*. Leurs résultats démontrent qu'on peut économiser l'énergie d'une manière significative en maximisant le nombre des ensembles disjoints.

Dans [Zhao *et al.* (2002)], les auteurs ont développé une technique permettant de balayer l'énergie résiduelle dans un réseau capteur qui détermine approximativement la distribution de l'énergie restante dans le réseau. Cette technique utilise des algorithmes de localisation qui sont par la suite agrégés pour construire un système de balayage composite. Cette technique peut être utilisée pour informer les utilisateurs sur les régions ayant une faible énergie, ceux-ci pouvant décider d'ajouter le nouveau capteur dans cette région ou de prévoir de nouvelles stratégies pour aviser le niveau de puissance résiduelle. D'autre part, les auteurs ont montré aussi qu'une grande partie de l'énergie

dissipée pour la communication, utilisée par l'interface radio, est beaucoup plus importante que celle utilisée pour le traitement.

Dans un réseau capteur les nœuds possèdent un rayon de couverture limitée (R) et par conséquent le routage se fait par multi saut et le relayage se fait au moyen des nœuds intermédiaires. Par la suite, les informations recueillies par chaque nœud doivent être envoyées à la station de base et amalgamées pour obtenir des informations globales et significatives. Cependant, la minimisation de l'énergie pour le routage constitue un autre problème dans les réseaux de capteurs sans fil.

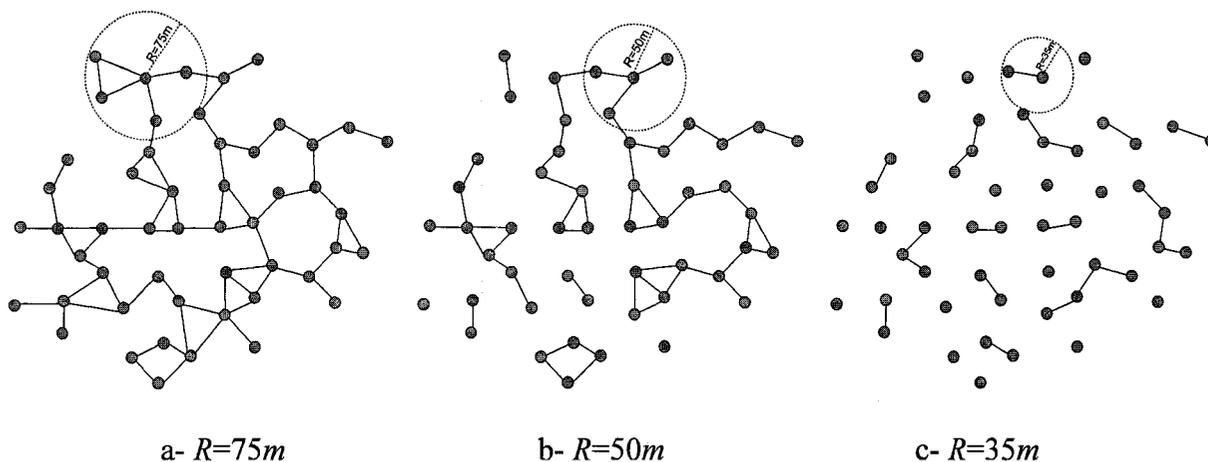


Figure 4 Un réseau avec 50 nœuds

La figure 4 illustre la connectivité d'un réseau comprenant 50 nœuds pour différents rayons de couverture R est égale à respectivement $75m$, $50m$ et $35m$. Dans cet exemple, les nœuds sont statiques et possèdent le même rayon de transmission. Nous remarquons que si le rayon de couverture passe de $75m$ à $35m$, nous obtenons un réseau non-connecté.

1.4 Les réseaux sans fil sans routage

1.4.1 Les réseaux cellulaires

Les réseaux de téléphonie cellulaire ont été conçus pour établir des communications téléphonie sans fil. Toutefois, ils offrent également des services de transmission de données très intéressants pour l'échange de message courts SMS (*Short Message Service*) ou de données en mode circuit (9,6 ou 14,4 kbps pour le GSM). De plus, L'évolution de la norme GSM a permis de définir un nouveau réseau : le GPRS (*General Packet Radio Service*) qui fonctionne en mode paquet jusqu'à un débit de 171,2 kbps. Enfin, la standardisation d'une nouvelle modulation (8PSK) a donné naissance à EDGE (*Enhanced Data for GSM Evolution*) permettant d'atteindre plus de 300 kbps [Vivier E. (2004)].

La norme GSM (*Global System for Mobile communication*) est largement utilisée en Europe et en Asie et elle ne constitue pas la seule norme pour les réseaux cellulaires. D'autres normes de téléphonie numérique existent comme l'IS-95 (*Interim Standard*) en Amérique du nord et le PDC (*Personal Digital Cellular*) au Japon.

La topologie utilisée est la topologie avec stations de base BS (*Base Station*). Une station de base est un ensemble d'émetteurs récepteurs munis d'une ou plusieurs antennes. Chaque station de base couvre une cellule indépendante. Un réseau cellulaire est formé d'une multitude de stations de base. Les BTS sont gérées par un contrôleur de stations de base BSC (*Base Station Controller*) qui assure également la concentration du trafic. Chaque BSC est connecté à un TCU (*TransCoder Unit*) qui rend compatible le réseau GSM avec les réseaux numériques fixes publiques par une adaptation du débit des circuits de parole. Les cellules adjacentes doivent utiliser des fréquences différentes afin d'éviter les interférences entre les communications. Les terminaux mobiles ne peuvent pas communiquer entre eux directement, ils doivent passer par la station de base même s'ils sont proches physiquement.

1.4.1.1 Les réseaux *ad hoc* versus les réseaux cellulaires

La figure 5-a illustre la topologie d'un réseau cellulaire ayant une infrastructure dépendante, alors que la figure 5-b montre un réseau *ad hoc* sans fil basé sur le multi saut. L'établissement d'un chemin entre la source *S* et la destination *D* doit passer par les stations de base dans un réseau cellulaire. Alors que dans un réseau *ad hoc*, le chemin entre *S* et *D* s'établit par l'intermédiaire de nœuds mobiles.

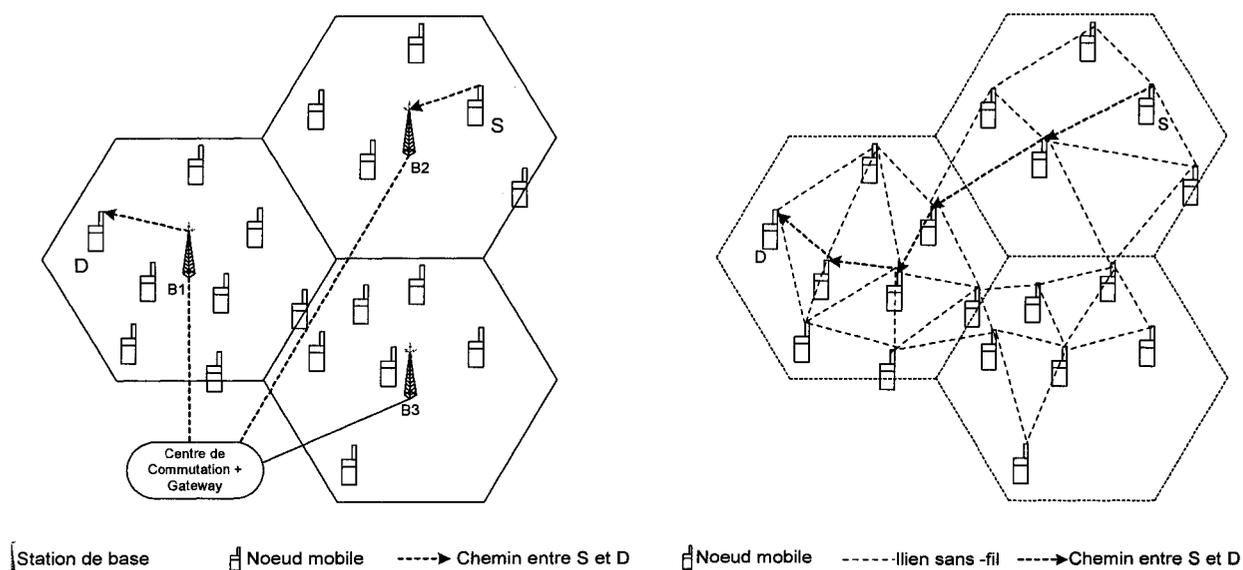


Figure 5 a- réseau cellulaire

b- réseau *ad hoc* sans fil

Les différences majeures entre les réseaux cellulaires et *ad hoc* sont résumées dans le Tableau I. L'existence d'une station de base simplifie le routage et la gestion de ressources dans un réseau cellulaire. Dans un réseau cellulaire, la décision de routage est réalisée de manière centralisée. Alors que dans un réseau *ad hoc* sans fil, le routage et la gestion de ressources sont réalisés de manière distribuée dans laquelle tous les nœuds se coordonnent pour établir une communication. Ceci demande à ce que chaque nœud soit plus intelligent alors qu'il doit fonctionner comme un hôte pour transmettre et recevoir les données et comme un routeur pour acheminer les paquets entre les nœuds. Dans un

réseau *ad hoc* les nœuds sont plus complexes que ceux des réseaux cellulaires [Murthy et Manoj (2004)].

Tableau I

Différence entre les réseaux cellulaires et les réseaux *ad hoc*

	Réseaux cellulaires	Réseaux <i>ad hoc</i>
Caractéristiques physiques	Basé sur une infrastructure fixe	Sans infrastructure
	Domaine d'application inclut civil et commercial	Urgence, opération de sauvetage, champs de bataille, travail de collaboration
	Coût élevé et temps de déploiement	Rapide et coût d'installation faible
	Coût élevé pour la maintenance (<i>backup, staffing, etc.</i>)	Fonctions d'auto-organisation et maintenance sont incluses dans le réseau
Gestion et routage	Lien à simple saut	Lien à multiple saut
	Routage centralisé	Routage distribué
	Commutation de circuit	Commutation de paquets
	Largeur de bande garantie (désignée pour le trafic de voix)	Canal radio partagé (plus convenable pour le trafic de données Best Effort)
	Facile pour employer la réservation de la bande passante	La réservation de la bande passante demande des protocoles de contrôle d'accès assez complexes
Déploiement	Hôte mobile ne sont pas trop complexe	Hôte mobile demande plus d'intelligence (doit être capable d'acheminer les paquets)
	Principaux objectifs du routage et l'admission d'appel sont de maximiser le taux d'acceptation d'appel et de minimiser le taux d'appel perdu	Principal objectif est de trouver les chemins avec un minimum d' <i>overhead</i> et une reconfiguration rapide en cas de chemins brisés.
	Largement déployé et actuellement dans la 3 ^{ème} génération	Plusieurs problèmes restent à investiguer pour un déploiement commercial bien qu'ils soient très utilisés en militaire.

1.4.2 Les technologies sans fil

La fin des années 90 a été marquée par la popularité des réseaux locaux informatiques. D'une part, l'utilisation courante du réseau local chez les particuliers, due en grande partie à Internet et, d'autre part, l'arrivée en masse des ordinateurs et autres matériels mobiles. Pour cela il faut trouver une technologie permettant de simplifier le câblage du réseau chez un particulier et de préserver la mobilité des produits portables. Un seul principe permet de concilier les deux; le sans fil. La solution peut paraître simple, autant elle est complexe à mettre en place pour plusieurs raisons. En effet, il faut tout d'abord développer une technologie proposant le plus d'avantages possibles comme une longue portée, le franchissement d'obstacles (murs) et surtout un prix bas.

Deux solutions sont proposées. La première consiste à utiliser l'infrarouge. Malgré son coût faible, l'infrarouge présente deux inconvénients majeurs : un temps de réaction très lent et l'obligation de maintenir l'émetteur dans la zone de réception sans obstacle en chemin. La deuxième est la transmission par radio, qui ne possède pas les inconvénients rencontrés avec la transmission infrarouge et dont les coûts de production ne cessent de baisser. Deux normes utilisant la technologie de transmission par radio sont déjà sur le marché, soit le *Bluetooth* et l'IEEE 802.11.

Ces standards n'ont pas été conçus dans l'objectif d'une utilisation complètement *ad hoc*. Ces technologies ne permettent que la communication entre terminaux à portée radio directe. Afin de pouvoir communiquer entre n'importe quelle paire de mobiles dans le réseau, il est indispensable de mettre en place un protocole de routage dédié. Un protocole de routage assure le relayage multi saut.

1.4.2.1 *Bluetooth*

Bluetooth est le premier standard pour une communication point-à-point à simple saut capable d'échanger les données et la voie. *Bluetooth* a pour objectif de faire disparaître les câbles entre les divers équipements numériques (périphériques d'ordinateurs tels que clavier, imprimante, modem, ou encore appareil photo numérique, PDA, walkman, etc.). Les équipements *Bluetooth* ont donc des portées et des débits assez limités, ainsi qu'une consommation électrique en rapport.

Un réseau *Bluetooth* forme des *piconets* composés par un groupe de nœuds dans une petite région géographique où chaque nœud est capable de rejoindre à un saut n'importe quel autre nœud dans son groupe. Le groupe de travail *Bluetooth SIG (Bluetooth Special Interest Group)* en a élaboré les spécifications. Ce réseau permet des communications ayant une portée d'une dizaine de mètres. Le *Bluetooth* opère dans la bande de fréquences des 2.4 GHz.

Les réseaux *Bluetooth* sont construits de manière centralisée. Un maître élu peut prendre en charge jusqu'à huit esclaves et forme ainsi un piconet. Dans un piconet, c'est le maître qui contrôle toutes les transmissions. Les esclaves ne peuvent émettre des paquets que s'ils ont été invités par le maître. L'accès au médium est un protocole de type jeton sans collision.

Le débit maximum dans un piconet est de 1 Mbits/s et une communication bidirectionnelle entre deux terminaux est d'au plus 433kbits/s. Un tel piconet peut constituer un réseau *ad hoc* à deux sauts dans lequel un terminal est à un saut de tous les autres. Pour construire un réseau multi saut, il est possible d'interconnecter plusieurs piconets, donnant lieu à un *scatternet*. La figure 6 donne un exemple de *scatternet*. Un esclave alterne entre les piconets 1 et 2 afin d'en assurer la liaison et le mobile esclave du piconet 2 est aussi maître dans le piconet 3 (le processus d'association est réversible,

il est possible de quitter temporairement un piconet puis de le rejoindre à nouveau et de revenir à la situation initiale).

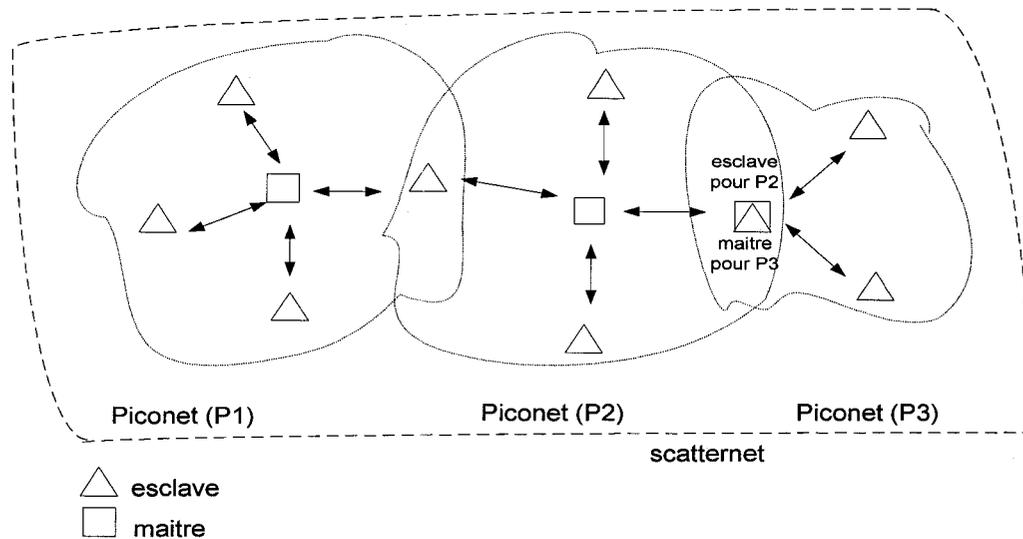


Figure 6 Un *scatternet* piconet nuage [Pujolle (2003)]

Bluetooth présente bel et bien une forme de réseau *ad hoc* multi saut. Mais du fait de l'utilisation ciblée pour un usage personnel, ces réseaux restent assez statiques et leur étendue reste limitée.

1.4.2.2 IEEE 802.11

Dans cette section, nous présentons les caractéristiques du standard IEEE 802.11 utilisées dans les réseaux *ad hoc* et ses performances dans un tel contexte. IEEE 802.11 a été développé en 1997 pour définir une couche physique et une couche accès au médium pour les réseaux locaux sans fil. En 1999, une extension de 802.11 a donné lieu aux standards 802.11a et 802.11b. Le 802.11a utilise la technique de modulation OFDM. Il fonctionne dans la bande de fréquence de 5 GHz et offre un débit de 6 Mbits/s. Alors que le 802.11b utilise la technique de modulation DSSS, il fonctionne dans la bande de

fréquence de 2,4 GHz et offre un débit jusqu'à 11 Mbits/s. Par la suite, un autre standard 802.11g⁸ a été créé pour atteindre un débit de 54 Mbits/s. Un nouveau standard 802.11n est en cours de standardisation pour atteindre un débit de l'ordre de quelques centaines de Mbits/s [Stallings (2005)].

Deux modes d'opération ont été décrits dans ce standard : le premier est le mode infrastructure et le deuxième est le mode *ad hoc*. Le mode infrastructure requiert une station de base alors que le mode *ad hoc* ne requiert pas de station de base. Par conséquent, deux mobiles à portée de transmission l'un de l'autre pourront communiquer sous ce dernier mode sans passer par l'intermédiaire d'une station de base. Le mode infrastructure utilise la fonction d'accès PCF (*Point Coordination Function*) qui sert pour supporter les trafics synchrones, c'est-à-dire les trafics temps réel. Le mode *ad hoc* utilise le service DCF (*Distributed Coordination Function*). Avec DCF, si un mobile détecte une activité sur le canal, le mobile va tirer une valeur aléatoire (*backoff*) dans une fenêtre de contention CW (*Contention Window*) puis il va décrémenter cette valeur, tant que le canal est libre. Une fois que le *backoff* atteint la valeur zéro, le mobile envoie son paquet. Durant la décrémentation du *backoff*, si le mobile détecte encore de l'activité sur le canal, il va arrêter cette décrémentation et continuer à utiliser ce *backoff* lors de la tentative d'émission suivante jusqu'à ce que le canal redevienne libre [Pujolle (2003)].

La spécification adoptée IEEE 802.11e⁹ propose le support de la QoS dans les réseaux sans fil avec une nouvelle fonction de contrôle EDCA (*Enhanced Distributed Channel Access*), considérée comme la nouvelle version de la fonction DCF, et une fonction de coordination hybride HCF (*Hybrid Coordination Function*). EDCA décrit quatre catégories de trafics TC (*Traffic Categories*). Les priorités sont contrôlées par les

⁸ Approuvé le 12 juin 2003

⁹ http://en.wikipedia.org/wiki/IEEE_802.11e

stations en modifiant le schéma d'accès de base (DCF). HCF est plus flexible que la fonction PCF. Il est utilisé par les points d'accès pendant la période d'accès contrôlée CAP (*Control Access Period*), qui peut commencer à n'importe quel moment durant la "*superframe*". Autrement dit, il permet d'accéder au médium pour faire passer un trafic ayant des contraintes de QoS.

Pour pallier au problème des nœuds cachés, décrit dans la section 1.2.3, le standard IEEE 802.11 donne la possibilité d'ajouter des paquets de contrôle avant d'échanger un paquet de données. Avant de transmettre son paquet, un émetteur envoie un paquet de contrôle appelé RTS (*Request To Send*). Ce paquet a pour rôle de réserver le lien radio en empêchant les voisins de transmettre suite à la réception de ce paquet. Un récepteur qui reçoit le RTS répond par un paquet de contrôle CTS (*Clear To Send*) s'il est en mesure d'accepter la communication. Le paquet CTS a le même effet que le paquet RTS, c'est-à-dire qu'il va réserver le lien médium et empêcher tous les nœuds voisins du récepteur d'émettre. À la réception du paquet CTS, l'émetteur sait que la communication va être préservée et qu'il peut transmettre ses paquets de données. En utilisant ce mécanisme, deux nœuds cachés désirant transmettre à la même destination seront alors au courant de leurs transmissions concurrentes. Dans le cas des nœuds cachés, s'il y a collision, elle se fera au niveau des paquets de contrôle et non pas au niveau des paquets de données; moins de bande passante sera consommée étant donné que les paquets de contrôle ont une taille beaucoup plus petite que les paquets de données.

Ce mécanisme est très efficace dans le cas des réseaux sans fil avec station de base, mais pas autant dans le cas des réseaux *ad hoc*. En effet, des collisions peuvent se produire même au niveau des paquets de données. Dans l'exemple de la figure 7, considérons le scénario suivant : *A* veut communiquer avec *B* et *C* avec *D*; *A* envoie un RTS; *B* reçoit ce RTS et pendant que *B* envoie un CTS, *C* envoie un RTS; comme *B* et *C* sont en train d'émettre, ils ne se rendent pas compte de leur émission respective; *D* reçoit le RTS de *C* et envoie un CTS; pendant ce temps *A* a déjà reçu le CTS de *B* et suppose que les liens

sont réservés, il va donc envoyer des paquets de données. En même temps, *C* reçoit le CTS de *D* et pense que les liens sont réservés; il envoie alors les données à *D*. Or ses données vont rentrer en collisions avec les données provenant de *A* au niveau du nœud *B* et ainsi *B* ne sera pas en mesure de comprendre la communication de *A*.

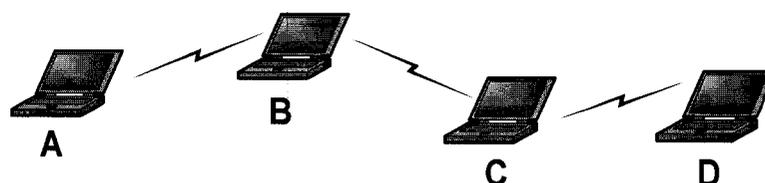


Figure 7 Méthode d'accès DCF

Un autre problème se pose très souvent dans le cadre des réseaux *ad hoc*. C'est le problème des stations exposées. Ce problème, à l'opposé des stations cachées qui se traduit en termes de sur-utilisation du médium, correspond à une sous-utilisation du médium radio. Considérant le même réseau de la figure 7, si *B* veut communiquer avec *A* et *C* veut communiquer avec *D*, *B* va accéder en premier au canal radio. *C*, situé dans la portée de transmission de *B*, va détecter de l'activité sur le canal et va donc s'empêcher d'émettre d'après le fonctionnement de DCF. Or, *C* aurait pu communiquer en même temps que *B*, dans le cas où les nœuds destinataires sont suffisamment éloignés des émetteurs de transmissions concurrentes, *A* de *C* et *D* de *B*.

Le standard 802.11b utilise différents débits de transmission. Les paquets en mode diffusion, comme les paquets de contrôle (RTS, CTS, etc.), sont envoyés à un ou deux Mbits/s alors que les paquets *unicast* peuvent être envoyés à 11 Mbits/s. Toutefois, si le débit augmente la portée diminue; un paquet envoyé à deux Mbits/s va être reçu par des nœuds plus éloignés que le même paquet envoyé à 11Mbits/s. Cependant, les routes construites avec les paquets diffusés ne sont pas directement exploitables à des débits

plus élevés. Ce problème est connu sous le nom de problème de la zone grise [Lundgren *et al.* (2002)].

Le problème de la zone grise n'est pas l'unique problème issu de l'utilisation de débits différents dans 802.11. Un autre problème a été mentionné dans [Heuse *et al.* (2003)]. Si plusieurs flux sont en contention pour l'accès au médium, la technique DCF cherche à donner à chaque paquet les mêmes chances pour y accéder. Ceci n'est possible que si tous les mobiles se trouvent dans la même zone de communication. Or, dans un réseau *ad hoc*, les nœuds peuvent être étendus géographiquement et certains mobiles sont indépendants et non à la portée de communication. Ces mobiles indépendants peuvent réduire fortement l'égalité des chances dans l'accès au canal ou l'égalité de transmissions réussies. Par exemple dans la figure 7, les nœuds *A* et *C* sont indépendants et n'ont pas conscience de leur transmission réciproque. Le nœud *B* est alors sujet à des collisions, et il n'est pas en mesure de comprendre la communication provenant de *A*, par conséquent le débit entre *A* et *B* est beaucoup plus faible qu'entre *C* et *D*.

1.5 Les protocoles de routage

Dans un réseau *ad hoc*, un protocole de routage a pour rôle d'établir et de maintenir une route d'une source vers une destination. Les caractéristiques des réseaux *ad hoc* rendent l'utilisation des protocoles filaires classiques non-utilisable. En effet, ces protocoles ont été conçus pour des réseaux ayant des topologies statiques et les nœuds possèdent suffisamment de ressources ce qui n'est pas le cas pour les réseaux *ad hoc*.

Les protocoles de routage dans les réseaux *ad hoc* sans fil sont classés en deux catégories : proactif (*table-driven*) et réactif (à la demande). Dans le routage proactif, chaque nœud doit maintenir une table de routage pour toutes les destinations et cette table doit être mise à jour de façon périodique. Dans le routage réactif, les nœuds n'ont pas de table de routage, c'est uniquement quand la source désire communiquer avec la destination qu'une route est déterminée. Ceci permet de réduire la taille des tables de

routage maintenues par les nœuds. Il existe une troisième classe : hybride. Cette classe est la combinaison des deux autres classes.

Tableau II

Protocoles de routage pour les réseaux *ad hoc*

Catégorie	Exemple de protocole de routage	Type
Proactif	OLSR, DSDV	plat
Réactif	AODV, ABR, DSR, TORA	plat
Hybride	ZRP	hiérarchique

Pour des raisons de mise à l'échelle, les protocoles de routage réactifs gagnent plus de terrain et attirent plus d'attention que les protocoles proactifs. Généralement, les protocoles réactifs utilisent l'inondation (*flooding*) pour trouver une route de la source vers la destination et l'inondation peut engendrer le phénomène d'orage de diffusion (*Broadcast Storm Problem*) tel que décrit dans [Tseng *et al.* (2002)].

L'économie d'énergie de la batterie est un autre problème pour les réseaux *ad hoc* sans fil. Plusieurs travaux de recherche ont été menés pour minimiser l'énergie totale consommée [Wan *et al.* (2001); Wieselther *et al.* (2000)]. Si l'énergie diminue dans un nœud critique le fonctionnement de tout le réseau sera alors perturbé. Pour augmenter la durée de vie du réseau, il est nécessaire d'étudier aussi bien l'énergie totale consommée que la consommation de l'énergie [Stallings (2005)].

D'autres protocoles de routage ont été proposés et leur application dépend de l'utilisation d'un système de positionnement tel le système GPS (*Global Positioning System*). Pour pouvoir utiliser ces protocoles, chaque terminal mobile doit être équipé d'un tel système

ce qui n'est pas toujours le cas. La plupart des terminaux actuels ne sont pas équipés de GPS et l'intégration de ce système engendre un coût additionnel. Aussi, ce système n'est efficace que pour les applications en plein air (pour des applications *indoor* le signal GPS est faible et n'est pas efficace). Le tableau III donne des exemples de protocole de routage basés sur l'utilisation du GPS.

Tableau III

Protocole de routage pour les réseaux dynamiques

Catégorie	Exemple de protocole de routage	Type
Proactif	GeoCast, DREAM, GPSR	géographique
Réactif	LAR	géographique

1.6 Conclusion

Dans ce chapitre, nous avons présenté un aperçu général sur les réseaux *ad hoc* mobiles, leurs caractéristiques, leurs applications, leurs types etc. Nous avons aussi présenté les technologies sans fil qui peuvent être utilisées comme infrastructure pour assurer la communication entre les mobiles dans le réseau. En effet, les différentes technologies proposées offrent différentes portées de communication et seuls les terminaux à portée de communication les unes des autres vont pouvoir échanger directement les messages. L'absence d'infrastructure et la nature dynamique de la topologie dans le réseau nécessitent l'existence d'un protocole de routage qui rendra la communication possible entre tous les nœuds du réseau. Un protocole de routage dans un réseau *ad hoc* doit réagir rapidement pour permettre la continuation de la communication.

Dans le chapitre suivant, nous allons effectuer une revue plus détaillée sur les protocoles de routage proposés dans littérature. Par la suite, nous allons discuter les approches

proposées pour la configuration et l'adressage dans un réseau *ad hoc*. Finalement, nous allons discuter les différentes approches pour effectuer le contrôle de la topologie dans les réseaux *ad hoc*.