

# Chapitre 2

## Les Réseaux Mobiles Ad Hoc & les Protocoles de Routage

### 2.1. Introduction

Les réseaux sans fil (*Wireless LAN ou WLAN ou IEEE 802.11*), offrent aujourd'hui de nouvelles perspectives dans le domaine des télécommunications. C'est un système de transmission des données, conçu pour assurer une liaison indépendante de l'emplacement des périphériques informatiques qui compose le réseau. Les réseaux sans fil sont principalement employés lorsqu'il s'agit d'interconnecter des utilisateurs nomades (par exemple des portables) entre eux.

Ce système ne pose aucune restriction sur la localisation des usagers. Il utilise des ondes radio plutôt qu'une infrastructure câblée pour communiquer. Ce nouveau mode de communication engendrent de nouvelles caractéristiques, propres à l'environnement mobile : de fréquentes déconnexions, un débit de communication et des ressources modestes, et des sources d'énergie limitées.

Les réseaux mobiles peuvent être classés en deux grandes classes :

- Réseau sans fil avec infrastructure (comme le GSM).
- Réseau sans fil sans infrastructure (comme les réseaux ad hoc).

Cette deuxième classe de réseaux sans fil constitue la base de notre sujet d'étude, et c'est ce que l'on va développer dans ce présent chapitre.

Dans le but de bien comprendre les stratégies et les approches utilisées dans la conception des protocoles permettant aux réseaux ad hoc de se relier à Internet, nous allons, tout d'abord, présenter le routage dans les réseaux ad hoc eux-mêmes. Après avoir décrit les réseaux ad hoc et leurs principales caractéristiques, nous présenterons les principes des protocoles de routage inter ad hoc les plus connus.

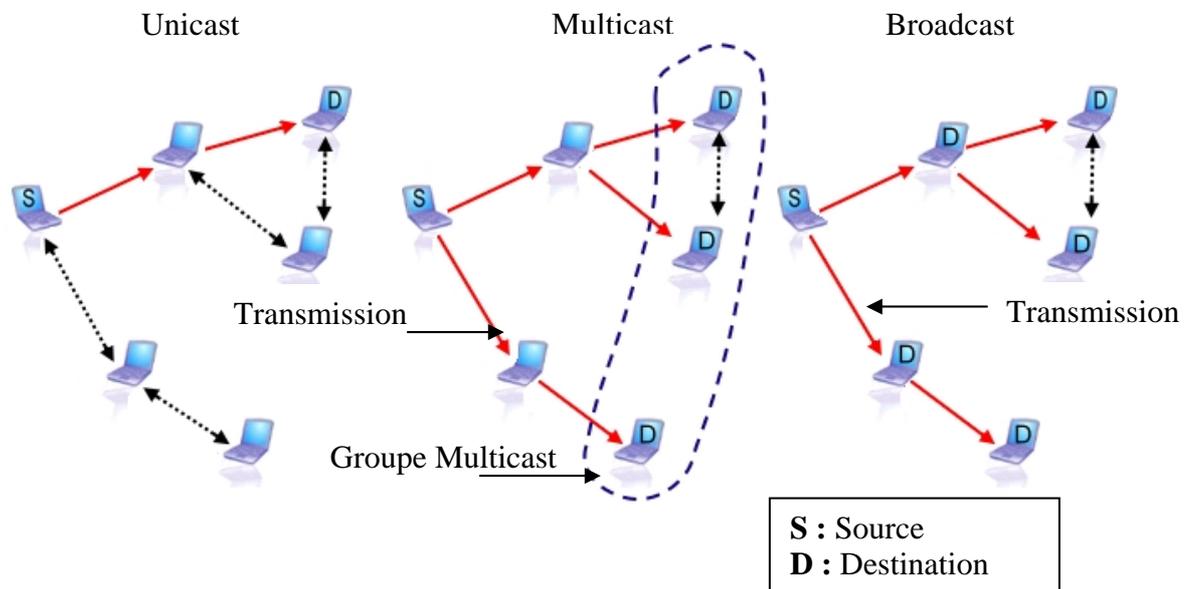
## 2.2. La transmission radio dans les environnements sans fil

La transmission radio utilisée dans la communication sans fil est basée sur le principe que l'accélération d'un électron crée un champ électromagnétique qui, à son tour accélère d'autres électrons et ainsi de suite. Il est alors possible de provoquer un déplacement électromagnétique [3]. Ce déplacement coordonné d'électrons peut alors servir pour le transfert d'information et constitue la base de la communication sans fil.

Deux signaux sur la même fréquence interfèrent et s'altèrent mutuellement. Pour y remédier, le spectre de fréquence est divisé en plusieurs parties (bandes de fréquence), chaque partie est dédiée à une utilisation spécifique. La taille limitée du spectre de fréquence impose donc le regroupement d'utilisateurs dans des bandes. Par exemple, la bande de 25 Mhz à 890 Mhz est réservée aux émissions de télévision et la bande supérieure à 890 Mhz pour la téléphonie cellulaire et la transmission par satellite [3].

## 2.3. Modes de communication dans les réseaux mobile

La communication dans les réseaux mobiles Ad Hoc utilise plusieurs modes dont : la communication « point à point » ou « Unicast », la communication « multipoint » ou « Multicast », et la diffusion « Broadcast ». Ces trois modes de communication peuvent être schématisés par la figure 2.1.



**Figure 2.1 :** Les différents modes de communication

## 2.4. Les classes de réseaux mobiles

Dans l'espace des réseaux mobiles, nous pouvons distinguer deux classes de réseaux, à savoir, les réseaux mobiles basés sur une infrastructure de communication (*modèle cellulaire*), et les réseaux mobiles sans infrastructure (*modèle ad hoc*).

### 2.4.1. Les réseaux avec infrastructure (cellulaires)

Dans ce mode, le réseau sans fil est composé de deux ensembles d'entités distinctes : les « sites fixes » d'un réseau de communication filaire classique, et les « sites mobiles ». Certains sites fixes, appelés stations de bases (SB) sont munis d'une interface de communication sans fil pour la communication directe avec les sites ou les unités mobiles (UM) localisés dans une zone géographique limitée, appelée cellule.

Chaque station de base délimite une cellule à partir de laquelle des unités mobiles peuvent émettre et recevoir des messages. Alors que les sites fixes sont interconnectés entre eux à travers un réseau de communication filaire, généralement fiable et d'un débit élevé. Les liaisons sans fil ont une bande passante limitée qui réduit sévèrement le volume des informations échangées.

Dans ce modèle, une unité mobile ne peut être, à un instant donné, directement connectée qu'à une seule station de base. Elle peut communiquer avec les autres sites à travers la station à laquelle elle est directement rattachée. L'autonomie réduite de sa source d'énergie, lui occasionne de fréquentes déconnexions du réseau; sa reconnexion peut alors se faire dans un environnement nouveau voire dans une nouvelle localisation.

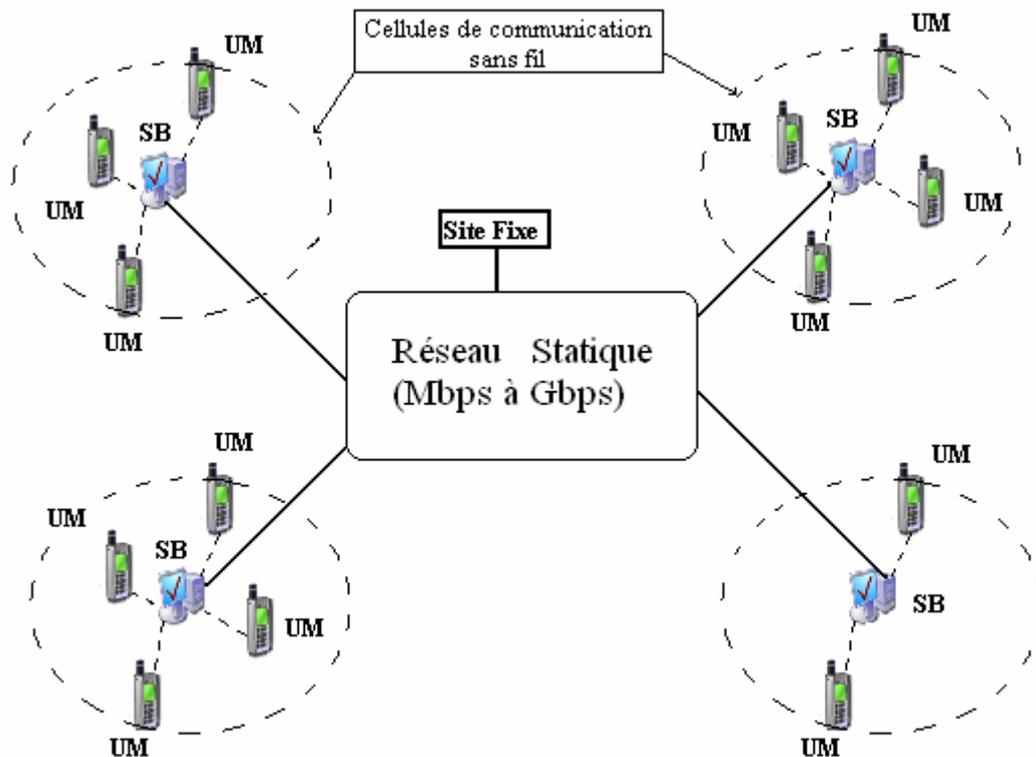


Figure 2.2 : Le réseau cellulaire (GSM)

A fin d'agrandir la surface de couverture, plusieurs points d'accès<sup>1</sup> peuvent être installés pour un même 'groupe de travail'<sup>2</sup>. Dans le cas d'utilisateurs mobiles, il y'a possibilité de passer d'un point d'accès à un autre sans perte de lien réseau (comme pour un réseau GSM schématiser dans la figure 2.2). Cette fonctionnalité s'appelle "Roaming".

## 2.4.2. Les réseaux sans infrastructure (AD HOC)

### 2.4.2.1. Définition d'un réseau ad hoc

Un réseau mobile Ad Hoc (figure 2.3), appelé généralement MANET (*Mobile Ad hoc NETWORK*), consiste en une grande population, relativement dense, d'unités mobiles qui se déplacent dans un territoire quelconque. Le seul moyen de communication est l'utilisation « des ondes radio » qui se propagent entre les différents nœuds mobiles, sans l'aide d'une infrastructure préexistante ou administration centralisée.

<sup>1</sup> Points d'accès sont les stations de base.

<sup>2</sup> Groupe de travail est un ensemble d'unités mobiles connectées à une même station de base.

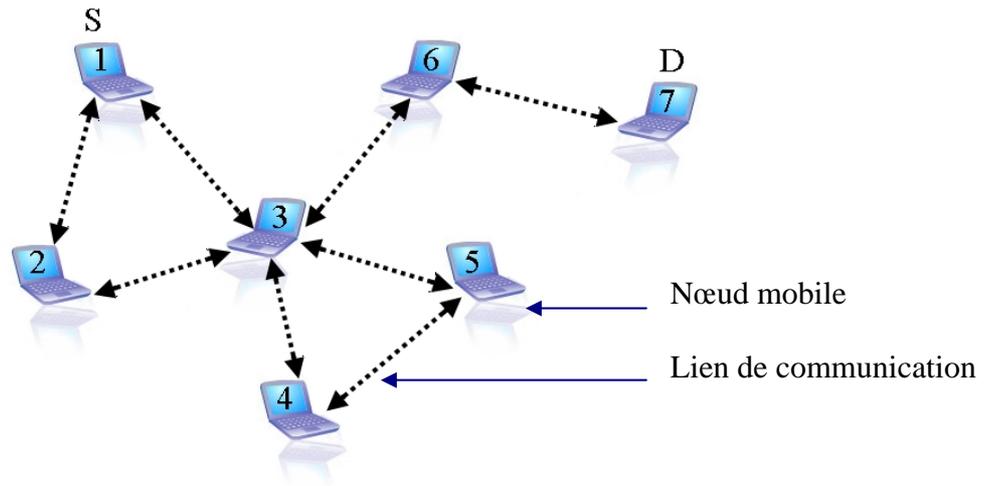


Figure 2.3 : un réseau Ad Hoc.

La topologie du réseau peut changer à tout moment, elle est donc dynamique et imprévisible ce qui fait que la déconnexion des unités soit très fréquente (figure 2.4).

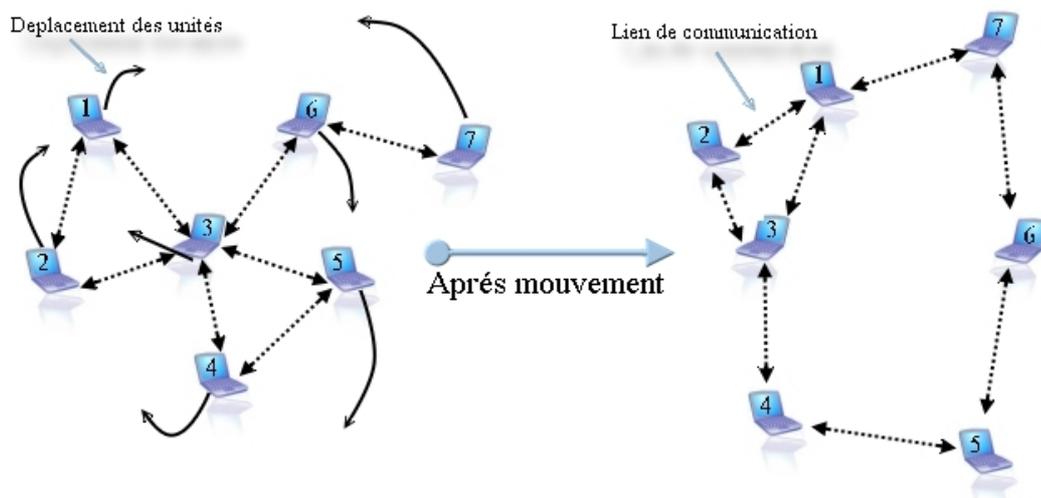


Figure 2.4 : Le changement de la topologie des réseaux Ad Hoc

#### 2.4.2.2. Les caractéristiques des réseaux Ad Hoc

Les réseaux sans fil ad hoc se caractérisent principalement par :

- **Bande passante limitée** : Une des caractéristiques primordiales des réseaux basés sur la communication sans fil est l'utilisation d'un médium de communication partagé (ondes radio). Ce partage fait que la bande passante réservée à un hôte soit modeste.
- **Contraintes d'énergie** : Les hôtes mobiles sont alimentés par des sources d'énergie autonomes comme les batteries ou les autres sources consommables. Le paramètre d'énergie doit être pris en considération dans tout contrôle fait par le système.

- **Sécurité physique limitée** : Les réseaux mobiles Ad Hoc sont plus touchés par le paramètre de sécurité que les réseaux filaires classiques. Cela se justifie par les contraintes et limitations physiques qui font que le contrôle des données transférées doit être minimisé.
- **Erreur de transmission** : Les erreurs de transmission radio sont plus fréquentes que dans les réseaux filaires.
- **Interférences** : Les liens radios ne sont pas isolés, deux transmissions simultanées sur une même fréquence ou, utilisant des fréquences proches peuvent interférer [5].
- **Absence d'infrastructure** : Les réseaux ad hoc se distinguent des autres réseaux mobiles par la propriété d'absence d'infrastructures préexistante et de tout genre d'administration centralisée. Les hôtes mobiles sont responsables d'établir et de maintenir la connectivité du réseau d'une manière continue.
- **Topologie dynamique** : Les unités mobiles du réseau se déplacent d'une façon libre et arbitraire. Par conséquent, la topologie du réseau peut changer à des instants imprévisibles, d'une manière rapide et aléatoire.
- **Nœuds cachés** : Ce phénomène est très particulier à l'environnement sans fil. Un exemple est illustré par la figure 2.5. Dans cet exemple, les nœuds B et C ne s'entendent pas, à cause d'un obstacle qui empêche la propagation des ondes. Les mécanismes d'accès au canal vont permettre alors à ces nœuds de commencer leurs émissions simultanément. Ce qui provoque des collisions au niveau du nœud A [5].

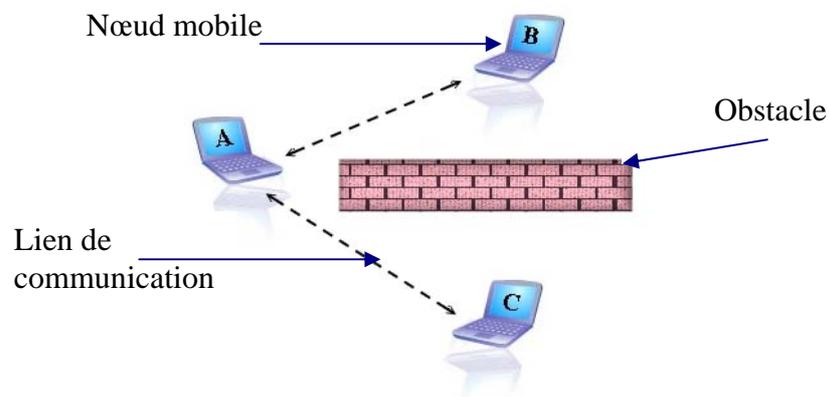


Figure 2.5 : Les nœuds cachés

#### 2.4.2.3. Les applications des réseaux mobiles Ad Hoc :

Les applications ayant recours aux réseaux ad hoc couvrent un très large spectre, incluant les applications militaires et de tactique, l'enseignement à distance, les opérations de secours...etc.

D'une façon générale, les réseaux ad hoc sont utilisés dans toutes applications où le déploiement d'une infrastructure réseau filaire est trop contraignant, soit parce

qu'il est difficile le mettre en place, soit parce que la durée d'exploitation du réseau ne justifie pas de câblage à demeure [3].

## 2.5. Le routage dans les réseaux ad hoc

Pour mieux comprendre les stratégies et les approches utilisées dans la conception des protocoles permettant aux réseaux ad hoc de se relier à Internet, nous allons, tout d'abord, parler du routage à l'intérieur des réseaux ad hoc. Dans ce qui suit nous allons présenter les principes des protocoles de routages inter ad hoc les plus connus.

### 2.5.1. Définition du routage

Le routage est une méthode à travers laquelle on fait transiter une information donnée depuis un certain émetteur vers un destinataire bien précis. Le problème du routage ne se résume pas seulement à trouver un chemin entre les deux nœuds du réseau, mais encore à trouver un acheminement optimal et de qualité des paquets de données.

### 2.5.2. Difficulté de routage dans les réseaux Ad Hoc

Afin de palier aux problèmes dues aux différents mouvements des nœuds mobiles qui pourront modifier le trafic, un réseau ad hoc doit donc pouvoir s'ordonner automatiquement de tel sorte à être déployable rapidement, et de pouvoir s'accommoder aux conditions de propagation. Dans le cas où le nœud destinataire se trouve dans la portée du nœud émetteur nous n'aurons pas besoin de routage proprement dit, malheureusement ce n'est pas toujours le cas, en effet, chaque nœud sera donc susceptible de jouer un rôle dans l'acheminement du paquet vers sa destination finale. Ce qui nous pousse à dire qu'il se peut que plusieurs nœuds puisse participer au routage. Nous parlons alors d'un environnement dit "**multihop**"<sup>3</sup>. Autrement dit, chaque nœud participera au processus de routage du paquet.

Vu les modestes capacités de calcul et de sauvegarde dont est caractérisé un réseau ad hoc, et la taille du réseau, il est très important de signaler que les méthodes et les approches utilisés pour l'acheminement des paquets dans le réseau sont évidemment différentes et plus complexes à mettre en œuvre par rapport à celles utilisées dans les réseaux classiques (statique). Ce qui nous pousse à dire que la gestion du routage dans un environnement ad hoc diffère de loin à celle utilisée dans les réseaux filaires. [3]

## 2.6. Classification des protocoles de routage

Le principal but de toute stratégie de routage est de mettre en œuvre une bonne gestion d'acheminement qui soit robuste et efficace. D'une manière générale, toute

---

<sup>3</sup>Le nombre de stations mobiles qui peuvent être utilisées comme routeurs intermédiaires peut dépasser le un

stratégie de routage repose sur des méthodes et des mécanismes que l'on peut regrouper en trois grandes classes : les protocoles de routage proactifs, les protocoles de routage réactifs et les protocoles de routage hybrides.

### 2.6.1. Les protocoles de routage proactifs

Un protocole de routage est dit proactif si les procédures de création et de maintenance des routes, durant la transmission des paquets de données, sont contrôlées périodiquement. Cette maintenance reste toujours active même s'il n'y a pas de trafic circulant dans le réseau.

Deux principales méthodes sont utilisées dans cette classe de protocoles proactifs : la méthode *Link state* et la méthode *Distance Vector*. Ces méthodes sont utilisées aussi dans les réseaux filaires. Parmi les protocoles de routages proactifs les plus connus on citera le DSDV, FSR, OLSR ...

#### a- Link Stat

Dans cette méthode, chaque nœud garde une vision de toute la topologie du réseau et ce par l'intermédiaire des requêtes périodiques portant sur l'état des liaisons avec les nœuds voisins. En effet la mise à jour dans cette méthode se fait pour chaque nœud diffusant l'état des liens des nœuds voisins dans le réseau. Cette opération est aussi faite en cas de changement dans l'état des liens [3] [64] [65] [66].

#### b- Distance Vector

Dans cette méthode par contre, chaque nœud diffuse à ses nœuds voisins sa vision des distances qui le séparent de tous les hôtes du réseau. En se basant sur les informations reçues par tous ses voisins, chaque nœud de routage fait un certain calcul pour trouver le chemin le plus court vers n'importe quelle destination. Le processus de calcul se répète, s'il y a un changement de la distance minimale séparant deux nœuds, et cela jusqu'à ce que le réseau atteigne un état stable. Cette technique est basée sur l'algorithme distribué de Bellman Ford (*DBF*) [67] [68] [69] [70] [71].

### 2.6.2. Les protocoles de routage réactifs (à la demande)

Ce sont des protocoles dans lesquels la mise à jour ou le contrôle des routes se fait à la demande, c'est-à-dire lorsqu'une source veut transmettre des paquets de données vers une destination. Dans ce cadre plusieurs politiques peuvent être adoptées, les plus importantes sont :

#### a. La Technique d'apprentissage en arrière

Le mécanisme d'apprentissage en arrière ou le **backward learning** [20] est basé sur le fait que lorsqu'un nœud source veut transmettre un message à une destination précise, il procède tout d'abord à l'opération d'inondation de sa requête sur tout le

réseau. Ainsi chaque nœud intermédiaire dit de transit (appartenant au chemin par lequel va passer le message), indique le chemin au nœud source lors de la réception de la requête.

On dit qu'il apprend le chemin au nœud source, tout en sauvegardant la route dans la table transmise. Enfin, lorsque la requête arrive à bon port, le nœud destinataire, et suivant le même chemin, transmet sa réponse sous forme de requête. Notons que le chemin établi entre les nœuds est un chemin Full duplex. Signalant aussi que la source garde trace du chemin tant qu'il restera en cours d'utilisation une fois que le chemin sera calculé.

### b. Technique du routage source

Dans cette technique, le nœud source détermine toute la liste des nœuds par lesquels doit transiter le message, ainsi le nœud émetteur inclut dans l'entête du paquet une route source. En effet, afin de construire la route, le nœud source doit préciser les adresses exactes des nœuds par lesquels le message transitera jusqu'à atteindre le

destinataire. Ainsi, le nœud source transmet le paquet au premier nœud spécifié dans la route. Notons que chaque nœud par lequel le paquet transit, supprime son adresse de l'entête du paquet avant de le retransmettre. Une fois que le paquet arrive à sa destination, il sera délivré à la couche réseau du dernier hôte.

Plusieurs protocoles de routage réactifs existent dont l'AODV, TORA, DSR...etc.

### 2.6.3. Les protocoles de routages Hybrides

Les protocoles hybrides combinent les deux idées : celle des protocoles proactifs et celle des protocoles réactifs. Ils utilisent un protocole proactif pour avoir des informations sur les voisins les plus proches (au maximum les voisins à deux sauts). Au-delà de cette zone prédéfinie, le protocole hybride fait appel aux techniques des protocoles réactifs pour chercher des routes.

Ce type de protocoles s'adapte bien aux grands réseaux, cependant, il cumule aussi les inconvénients des protocoles réactifs et proactifs en même temps (*messages de contrôle périodique, le coût d'ouverture d'une nouvelle route*). Plusieurs protocoles hybride existent dont le **CBRP** et le **ZRP** (*Zone Routing Protocol*) [13].

### 2.7. Quelques protocoles de routages unicast

Dans ce qui suit, on va décrire trois protocoles de routages, conçus pour les réseaux ad hoc :

- Le protocole DSDV.
- Le protocole AODV.
- Le protocole ZRP.

Nous avons choisit ces trois protocoles, suivant les trois grandes classes de protocoles de routages cités ci-avant.

### 2.7.1. Le protocole DSDV

Le **DSDV** (*Dynamic Destination-Sequenced Distance-Vector*) [17] est principalement inspiré de l'algorithme distribué de Bellman Ford (*DBF : Distributed Bellman-Ford*) [17]. Toute fois, chaque station mobile se voit maintenir une table de routage contenant :

- Toutes les destinations possibles dans le réseau.
- Le nombre de nœuds (ou de sauts) nécessaire pour atteindre chacune de ces destinations.
- Le numéro de séquences (**SN** : *Séquence Number*) qui correspond à un nœud destination [3].

Afin de conserver la consistance des tables de routages dans un réseau, souvent connue par la forte variation de la topologie, à chaque nœud est attribué un numéro de séquence **NS** qui permet de distinguer les nouvelles routes des anciennes. Ce qui permet de remédier au problème de *boucle de routage*. Ainsi chaque nœud transmet à son voisin direct sa table de routage périodiquement ou en cas de changement imprévu de la table. Donc, la mise à jour se fait selon deux facteurs : le temps et les événements qui peuvent surgir (déplacement de nœuds, apparition d'un nouveau voisin ...etc). Vu ces deux facteurs, on peut distinguer deux types de mise à jour [19] :

- **Mise à jour complète** : qui n'est rien autre que la mise à jour périodique, c'est-à-dire que le nœud transmet la totalité de sa table de routage vers ses voisins.
- **Mise à jour incrémentale** : cette mise à jour n'est faite qu'en cas d'événements (Apparition d'un nouveau voisin, disparition d'un nœud ...etc.), et dans ce cas il n'y a que l'entrée concernant le nœud en question dans la table de routage qui change. Cette mise à jour est aussi dite mise à jour partielle.

Notons que la mise à jour se fait à travers la transmission d'un paquet généralement contenant :

- Le nouveau numéro de séquence, incrémenté, du nœud émetteur.
- L'adresse de la destination.
- Le nombre de sauts séparant le nœud de la destination.
- Le numéro de séquence (des données reçues de la destination) tel qu'il a été estampillé par la destination.

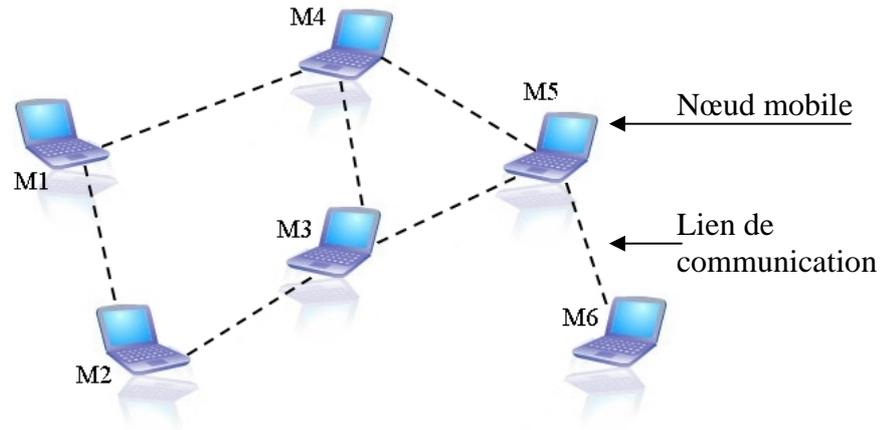


Figure 2.6 : Exemple d'un réseau Ad Hoc

Si l'on considère que le DSDV est le protocole de routage utilisé dans la figure 3.2, la table de routage correspondante au nœud M1 ressemblera à la suivante :

Destination	Nombre de sauts	Prochain nœud	Numéro de séquence
M1	0	M1	NS1
M2	1	M2	NS2
M3	2	M2	NS3
M4	1	M4	NS4
M5	2	M4	NS5
M6	3	M4	NS6

Figure 2.7 : Table de routage du nœud M1 du graphe 2.6.

Ainsi tout nœud, qui a subi une mise à jour, compare les données de routage reçus avec les siennes, et la route la plus récente (celle avec la plus grande valeur du numéro de séquence) sera utilisée. Si deux routes ont le même numéro de séquence, alors la route qui possède la meilleure métrique est celle qui sera utilisée. La métrique utilisée dans le calcul des plus courts chemins est, tout simplement, le nombre de nœuds intermédiaires existants sur ce chemin. Un lien rompu est matérialisé par une valeur infinie de sa métrique, i.e. une valeur plus grande que la valeur maximale permise par la métrique [3].

Parmi les inconvénients du protocole DSDV, est qu'il est très lent, du fait qu'il doit attendre la mise à jour transmise par le destinataire pour modifier l'entrée adéquate dans la table de distance. Bien qu'il remédie au problème de boucle de routage « **Routing Loop** » et du **Counting to Infinity** (*du DBF*) [17].

### 2.7.2. Le protocole AODV

L'AODV (*Ad hoc On Demand Distance Vector*) [17, 8] ou bien le routage avec vecteur de distance à la demande adopte en réalité deux politiques présentées comme optimisation du protocole DSDV. Le protocole AODV minimise sensiblement le nombre de diffusions de messages en créant le chemin à la demande en plus du routage nœud à nœud et le principe des numéros de séquence. AODV utilise aussi l'échange

périodique d'une part, d'autre part, il a hérité des deux mécanismes qui caractérisent le DSR et qui sont : *la découverte et la maintenance des routes*

Comme dans le DSDV, l'AODV utilise le principe des numéros de séquence, il permet aux nœuds d'utiliser les routes les plus fraîches suivant leurs numéros de séquence.

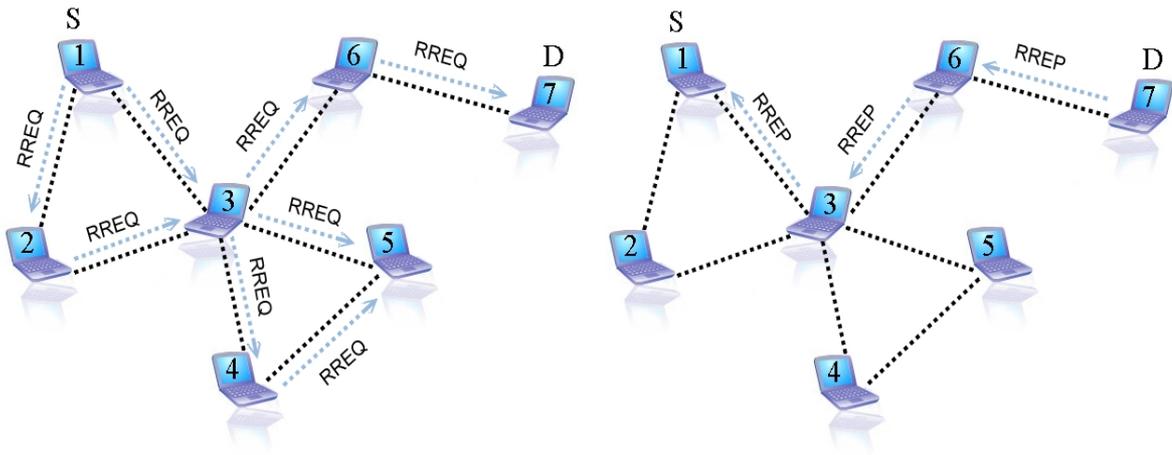
Le concept du paquet *Route Request* et aussi bien utilisé dans l'AODV. En effet dans une table de routage propre à l'AODV, les chemins sont maintenus d'une manière distribuée au niveau de chaque nœud.

Une entrée de la table de routage contient essentiellement [31] :

- 1) *L'adresse de la destination.*
- 2) *Adresse du nœud suivant.*
- 3) *La distance en nombre de sauts (i.e. le nombre de nœuds nécessaires pour atteindre la destination).*
- 4) *Le numéro de séquence destination.*
- 5) *Le temps d'expiration de chaque entrée dans la table.*

Précisons que le protocole AODV ne supporte que les liens symétriques dans la construction des chemins inverses; c'est-à-dire que lorsqu'un nœud intermédiaire transmet le paquet *Route Request* à un voisin, il procède la à sauvegarde de l'identificateur du nœud à partir duquel la première copie de la requête est reçue. Ce chemin inverse sera traversé par le paquet *Route Reply*, et de cette façon tous les nœuds appartenant au chemin retour modifieront leurs tables de routage en fonction du paquet réponse de route.

Dans le cas où les routes ne sont pas déterminés à l'avance, ou bien la durée de vie du chemin vers la destination à expirée ou encore une défaillance surgit pour un chemin donné, le nœud diffuse un paquet *Route Request (RREQ)* (figure 2.8). Le champ NS destination de ce dernier nous indiquera le dernier numéro de séquence associé au nœud destination. En effet si le NS n'est pas connu, la valeur zéro lui sera attribuée par défaut. Si après un certain temps le nœud émetteur ne reçoit pas le paquet *Route Reply (RREP)*, le nœud source rediffuse une nouvelle fois le *RREQ*. Ainsi, et à chaque fois que *RREQ* est rediffusé, le champ « *Broadcast ID* » [31] du paquet *RREQ* est incrémenté. Un message d'erreur est délivré si au bout d'un certain nombre de rediffusions du *RREQ*, le *RREP* n'est pas réceptionné.



**Figure 2.8 :** Les deux requêtes *RREQ* et *RREP* utilisées dans le protocole AODV.

Comme nous l'avons déjà dit, le protocole AODV exécute lui aussi une procédure de maintenance des routes, cette procédure se fait par l'émission périodique d'un message "*HELLO*". Le lien entre deux nœuds voisins sera considéré comme défaillant dans le cas où trois messages "*HELLO*" ne sont pas reçus respectivement.

Les défaillances des liens sont généralement dues à la mobilité du réseau ad hoc. Les mouvements des nœuds qui ne participent pas dans le chemin actif n'affectent pas la consistance des données de routage. Quand un lien, reliant un nœud  $p$  avec le nœud qui le suit sur le chemin de routage, devient défaillant, le nœud  $p$  diffuse un paquet *UNSOLICITED RREP* avec une valeur de numéro de séquence égale à l'ancienne valeur du paquet *RREP* incrémentée de un, et une valeur *infinie* de la distance. Le paquet *UNSOLICITED RREP* est diffusé aux voisins actifs jusqu'à ce qu'il arrive à la source. Une fois le paquet est reçu, la source peut initier le processus de la découverte de routes.

L'AODV maintient les adresses des voisins à travers lesquels les paquets destinés à un certain nœud arrivent. Un voisin est considéré actif, pour une destination donnée, s'il délivre au moins un paquet de donnée sans dépasser une certaine période (appelée : *active time out period*). Une entrée de la table du routage est active, si elle est utilisée par un voisin actif. Le chemin reliant la source et la destination, en passant par les entrées actives des tables de routage, est dit un *chemin actif*. Dans le cas des défaillances des liens, toutes les entrées des tables de routage participantes dans le chemin actif, et qui sont concernées par la défaillance, sont supprimées. Cela est accompli par la diffusion d'un message d'erreur entre les nœuds actifs.

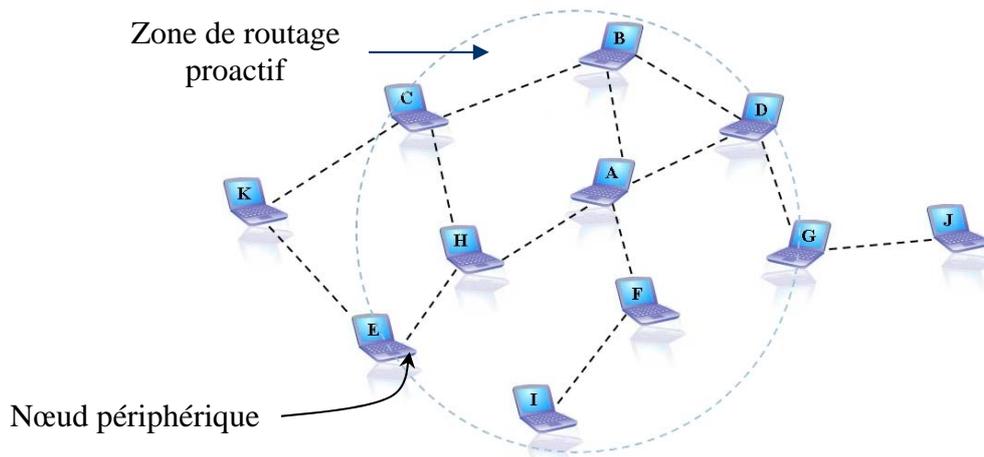
Le protocole de routage AODV (et même le protocole DSR), n'assure pas l'utilisation du meilleur chemin existant entre la source et la destination. Cependant, des évaluations de performances récentes ont montré qu'il n'y a pas de grandes différences (en terme d'optimisation) entre les chemins utilisés par le protocole AODV et ceux utilisés par les protocoles basés sur les algorithmes de recherche des plus courts chemins [10].

En plus de cela, le protocole AODV ne présente pas de boucle de routage, et évite le problème "*Counting to Infinity*" de Bellman-Ford [17], ce qui offre une convergence rapide quand la topologie du réseau ad hoc change.

### 2.7.3. Le protocole ZRP

Le protocole de routage ZRP (*Zone Routing Protocol*) utilise les deux approches (*Proactif et Réactif*), il limite la procédure proactive uniquement aux nœuds voisins (*les changements de la topologie doivent avoir un impact local*) et, bien que de nature global, offre une recherche rapide et efficace dans le réseau. Contrairement à une recherche sur tout le réseau [13], dans ce protocole, la détection des boucles de routage est possible grâce à la connaissance de la topologie du réseau.

Une Zone de routage est alors définie pour chaque nœud, elle inclut les nœuds qui sont à une distance minimale (*en terme de nombre de sauts*), du nœud en question, inférieure ou égale au rayon  $\delta$  de la zone [13]. L'exemple ci-dessous illustre la zone associée au nœud **A** avec un rayon égal à 2 sauts.



**Figure 2.9** : la zone de routage A avec  $\delta=2$ .

Dans l'exemple de la figure 2.9, les nœuds B, D, H, et F appartiennent à la zone de routage de **A**, ils sont considérés comme nœuds internes (*la distance qui les séparent du nœud A est strictement inférieure au rayon  $\delta$* ). Les nœuds C, E, I, et G qui sont distant du nœud **A** d'une distance égale au rayon ( $\delta=2$ ) sont dit nœuds périphériques. Pour ce qui est des nœuds J et K, ils ne sont pas inclus dans la zone de **A**.

En résumé, ZRP définit donc deux types de protocoles : l'un fonctionnant localement et le deuxième fonctionnant entre zones. Ces deux protocoles sont :

- **IARP** [14] (*IntraZone Routing Protocol*) offrant les routes optimales vers les destinations qui se trouvent à l'intérieur de la zone à une distance déterminée, et tout changement est répercuté uniquement à l'intérieur de la zone .

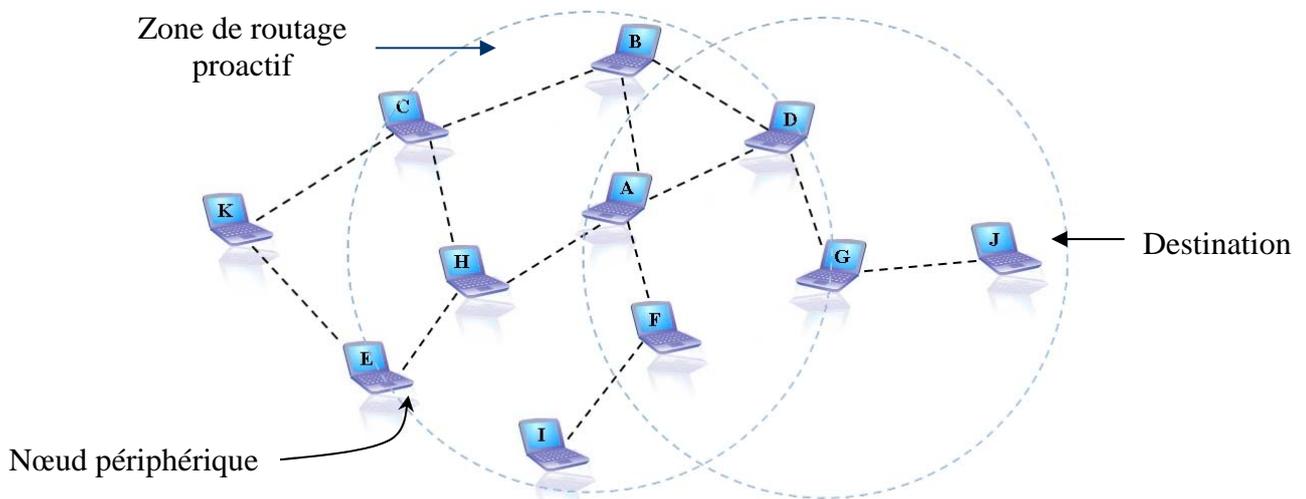
- **IERP** [15] (*IntErzone Routing Protocol*) quant à lui s'occupe de rechercher les routes à la demande pour des destinations en dehors d'une zone.

En plus de ces deux protocoles, le ZRP utilise le protocole BRP (*Bordercast routing protocol*) [16]. Ce dernier utilise les données de la topologie fournies par le protocole IARP afin de construire sa liste des nœuds de périphérie et la façon de les atteindre. Il est utilisé pour guider la propagation des requêtes de recherche de route de l'IERP dans le réseau.

La recherche des chemins est effectuée en vérifiant tout d'abord si le nœud destinataire ne se trouve pas dans la zone du nœud source (*la procédure IERP suppose que chaque nœud connaît le contenu de sa zone*), auquel cas, le chemin est déjà connu.

Autrement, une demande d'établissement de route « RREQ » est initiée vers tous les nœuds périphériques, ces derniers vérifient, à leur tour, si la destination spécifiée par la source existe dans leurs zones. Dans le cas positif, la source recevra alors un paquet « RREP » contenant le chemin menant à la destination, sinon, les nœuds périphériques diffusent la requête de demande à leurs propres nœuds périphériques, qui à leurs tours, effectuent le même traitement.

Dans la Figure 2.10, le nœud **A** veut envoyer un paquet au nœud **J**, puisque ce dernier n'est pas dans la zone de routage de **A**, une requête « RREQ » est envoyée par **A** aux nœuds périphériques qui sont **C**, **E**, **I**, et **G**. Ces derniers vérifient l'existence du nœud **J** dans sa zone de routage et, par conséquent, l'envoi d'un message « RREP », contenant le chemin établi, du nœud **G**.



**Figure 2.10** : Demande de route A --- J ( $\delta=2$ )

Les erreurs de route sont également prévues par l'IERP en utilisant un mécanisme de réponse réactif. Lors d'une propagation d'un paquet, si une erreur survient au niveau du prochain nœud (*le nœud devient inaccessible*), un message « RERR » est délivré à la source.

En résumé, le ZRP combine plusieurs sous protocoles, à savoir, IARP (à l'intérieur de la zone), IERP (à l'extérieur de la zone), et d'autres (ICMP et BRP ...etc.).

## 2.8. Conclusion

L'étude effectuée sur les réseaux mobiles ad hoc nous a permis de connaître leurs différentes caractéristiques (absence d'infrastructure, topologie dynamique, bandes passantes limitées, sécurité physique limitée, contraintes d'énergie, ...etc.), et ainsi constater que leur apparition a, certes, facilité la mise en œuvre d'applications mobiles et ne supportant pas d'infrastructure préexistante (telles que les applications militaires), mais en revanche, a laissé émerger un bon nombre de problèmes dont celui du routage.

Dans l'étude des protocoles de routage, on a commencé par présenter les trois classes de protocoles de routages : Proactifs, Réactifs et hybrides, ainsi que les politiques et les méthodes d'acheminement sur lesquelles ils reposent. Par la suite on a donné un exemple de protocole pour chacune des trois classes : DSDV, AODV, ZRP. D'autres protocoles existent évidemment, mais, dans le cadre de notre travail, on se contente de ce peu, car le plus important pour nous est de choisir un protocole de routage unicast qui semble plus flexible, afin de l'étendre pour une nouvelle application qui est : la connexion des réseaux ad hoc à Internet. Pour cela, le chapitre suivant vient pour mettre en évidence cette nouvelle technologie.