

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE  
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

N° d'ordre : ...

**UNIVERSITE DE MOHAMED BOUDIAF - M'SILA**

**FACULTE DES MATHEMATIQUES ET DE  
L'INFORMATIQUE**

**Département d'Informatique**

**MEMOIRE de fin d'étude**

***Présenté pour l'obtention du diplôme de MASTER***

**Domaine : Mathématiques et Informatique**

**Filière : Informatique**

**Spécialité : Systèmes d'Informations Avancés**

**Par: MERATATE Soumia**

**SUJET**

**Les protocoles de routage dans le  
reseau ad-hoc**

**Soutenu publiquement le :    /    /2015            devant le jury  
composé de :**

.....	Université de M'sila	Président
HAMAK	Université de M'sila	Rapporteur
.....	Université de M'sila	Examineur
.....	Université de M'sila	Examineur

**L'année universitaire : 2015/2016**

## **Dédicace et remerciements**

*Ce modeste travail n'est ni plus ni moins le fruit de parents qui ont su comment faire aboutir ce projet de MASTER. Ils m'ont toujours encouragé et orienté vers la réussite.*

*Je ne les remercierai jamais assez.*

*Je suis profondément reconnaissante à mon encadreur **DR. HAMAK** à l'université qui a toujours été présent pour M'éclairer le chemin ainsi que pour ses conseils et ses critiques.*

*Je remercie aussi les membres du jury d'avoir accepté de jurer ce mémoire.*

*A ma sœur DR.MERATATE.F, mon mari ben yahia Ahmed, et tous mes sœurs et frères*

*Je dédie le cœur de cette thèse de MASTER*

**Meratate soumia**

## Résumé

Un réseau ad-hoc sans fil est une collection de nœuds mobiles formant un réseau temporaire à topologie variable et fonctionnant sans station de base et sans administration centralisée, les communications multi sauts y sont possibles grâce à des protocoles de routage spécifiques..

Notre travail entre dans le cadre de l'étude du mécanisme de routage dans les réseaux mobiles Ad hoc. Notre étude repose principalement sur les travaux de recherche qui ont été fait, et qui se font à l'heure actuelle, dans le but de comprendre le principe d'acheminement de données entre les hôtes mobiles du réseau ad hoc

Nous présentons les environnements mobiles et les principaux concepts liés à ces environnements. Nous commençons par la définition de l'environnement et citer les deux classes qui le constituent, Nous donnons par la suite quelques notions importantes utilisées dans les systèmes mobiles et qui sont plus liées à la technologie sans fil qui représente le cœur de la télécommunication sans fil. Nous introduisons le concept de réseau ad hoc Après la description des principales applications et caractéristiques de l'environnement ad hoc, nous présentons les différents protocoles de routage existant dans le contexte des réseaux ad hoc. Nous décrivons les principales caractéristiques et fonctionnalités des stratégies de routage les plus connues permettant d'assurer l'acheminement des données entre les hôtes mobiles.

Notre objectif est de simuler des protocoles de routage ad hoc avec le simulateur de réseaux NS pour analyser leurs performances dans une multitude de scénarios, où des topologies et des flux sont à définir. Une fois les simulations

terminées et leurs traces<sup>2</sup> générées, nous les analyserons suivant différents critères et générerons des courbes qui présentent les synthèses finales.

## **Table de matières**

### **Chapitre 1. Les réseaux mobiles**

<b>1.1</b>	Définition des réseaux mobiles	<b>15</b>
<b>1.1.1</b>	Les réseaux mobiles avec infrastructure	<b>15</b>
<b>1.1.1.1</b>	Réseaux sans fil téléphonique	<b>16</b>
•	GSM (Global System for Mobile Communications)	<b>16</b>
•	GPRS (General Packet Radio Service)	<b>16</b>
•	UMTS (Universal Mobile Telecommunications System)	<b>16</b>
•	EDGE (Enhanced Data rate for GSM Evolution)	<b>16</b>
•	WAP (Wireless Application Protocol)	<b>16</b>
•	iMode (Internet Mode)	<b>17</b>
<b>1.1.1.2</b>	Réseaux sans fil informatiques	<b>17</b>
•	Bluetooth (Internet Mode)	<b>17</b>
•	HomeRF	<b>18</b>
•	HiperLAN	<b>19</b>
•	WiFi	<b>19</b>
<b>1.1.2.</b>	<b>Le réseau mobile sans infrastructure</b>	<b>20</b>
<b>1.1.2.1</b>	Les réseaux mobiles Ad Hoc	<b>20</b>
•	Définition	<b>20</b>
•	Modélisation	<b>21</b>
•	Les caractéristiques des réseaux ad hoc	<b>22</b>
•	Les applications des réseaux mobiles ad hoc	<b>23</b>
•	Communication dans les réseaux ad hoc	<b>24</b>

## **Chapitre 2. Les protocoles de routage dans les réseaux Ad- Hoc**

<b>2.1</b>	<b>Définition du routage</b>	<b>28</b>
<b>2.2</b>	<b>Le Routage dans les Réseaux Ad Hoc</b>	<b>29</b>
<b>2.3</b>	<b>La difficulté du routage dans les réseaux Ad hoc</b>	<b>30</b>
<b>2.4</b>	<b>Les contraintes de routages dans les réseaux ad hoc</b>	<b>30</b>
•	<b>Minimisation de la charge du réseau :</b>	<b>31</b>
•	<b>Offrir un support pour pouvoir effectuer des communications multi-points fiables</b>	<b>31</b>
•	<b>Assurer un routage optimal</b>	<b>31</b>
•	<b>Le temps de latence</b>	<b>31</b>
<b>2.5</b>	<b>Les protocoles de routage dans les réseaux ad – hoc</b>	<b>32</b>
<b>2.5.1</b>	<b>Les protocoles de routage proactifs</b>	<b>35</b>
	<i>Avantages et les inconvénients des protocoles proactifs</i>	
<b>2.5.1.1</b>	<b>LE PROTOCOLE DE ROUTAGE « DSDV »</b>	<b>35</b>
<b>2.5.1.2</b>	<b>Le protocole de routage FSR</b>	<b>36</b>
<b>2.5.1.3</b>	<b>Le protocole de routage CGSR (Clusterhead Gateway Switch Routing</b>	<b>39</b>
<b>2.5.2</b>	<b>Les protocoles de routage réactifs (à la demande)</b>	<b>40</b>
<b>2.5.2.1</b>	<b>Avantages et les inconvénients des protocoles réactifs</b>	
<b>2.5.2.2</b>	<b>Le protocole de routage AODV</b>	<b>41</b>
<b>2.5.2.3</b>	<b>Le protocole DSR</b>	<b>42</b>
<b>2.6</b>	<b>Propriétés ciblées par les protocoles de routage des réseaux ad hoc</b>	<b>43</b>

<b>2.6.1</b>	<b>Distribution des opérations</b>	<b>44</b>
<b>2.6.2</b>	<b>Routes sans cycle</b>	<b>44</b>
<b>2.6.3</b>	<b>Opération à la demande</b>	<b>44</b>
<b>2.6.4</b>	<b>Liens unidirectionnels</b>	<b>44</b>
<b>2.6.5</b>	<b>La sécurité</b>	<b>44</b>
<b>2.6.6</b>	<b>Conservation d'énergie</b>	<b>44</b>
<b>2.6.7</b>	<b>Multi-routes</b>	<b>45</b>
<b>2.6.8</b>	<b>Le support de la qualité de service</b>	<b>45</b>

## **Chapitre 3 : comparaison entre des protocoles de routage des réseaux adhoc**

	<b>INTRODUCTION</b>	<b>46</b>
<b>3.1.1</b>	<b>Métrieologie et modèle utilise</b>	<b>46</b>
<b>3.1.2</b>	<b>Résultats et analyse</b>	<b>50</b>
	<b>Conclusion</b>	<b>59</b>
	<b>RÉFÉRENCES</b>	<b>60</b>

## **Liste des acronymes**

- AODV : ad hoc On-Demande Distance-Vector

- BTS : Base Tranceiver Station
- Bluetooth : Technologie de réseau personnel sans fils (noté WPAN pour Wireless Personal Area Network),
- Broadcast Diffusion
- CGSR : Clusterhead Gateway Switch Routing
- CLR Clear packet
- CMU : Carnegie Mellon University
- CSMA/CA : Carrier Sense, Multiple Access/Collision Avoidance
- CSMA/CD : Carrier Sense Multiple Access / Collision Detect
- DAG : Graphe Dirigé Acyclique (Directed Acyclic Graph)
- DECT : Digital Enhanced Cordless Technology
- DSDV : Destination Sequenced Distance-Vector Routing
- DSR : Dynamic Source Routing

## Listes des figures

<b>Figure 1.1 :</b>	Le modèle des réseaux mobiles avec infrastructure	16
<b>Figure 1.2 :</b>	Simple réseau ad hoc	21
<b>Figure 1.3 :</b>	La modélisation d'un réseau ad hoc	21
<b>Figure 1.4:</b>	La topologie du réseau ad-hoc	22
<b>Figure 1.5 :</b>	Zones de communication et de détection de porteuse	26



<b>Figure 2.1 :</b>	Le chemin utilisé dan le routage entre la source et la destination.	29
<b>Figure 2.2 :</b>	: œil de poisson	38
<b>Figure 2.3 :</b>	Routage du 1 au noeud 8 par CGSR	40
<b>Figure 2.4:</b>	La requete (RREP)	43
<b>Figure 3.1 :</b>	coût de routage en fonction de la charge	49
<b>Figure 3.2:</b>	taux de paquets delivres,en fonction de la charge	49
<b>Figure 3.3 :</b>	Delai,en fonction de la charge	49
<b>Figure 3.4 :</b>	Gigue.en fonction de la charge	49
<b>Figure 3.5 :</b>	Concentration de l'activite ,en fonction de la charge	40
<b>Figure 3.6 :</b>	Consommation d'energie en fonction de la vitesse des nœuds	50
<b>Figure 3.7 :</b>	Consommation d'energie en fonction de nombre de nœuds	53
<b>Figure 3.8 :</b>	Consommation d'energie en fonction de la taille du reseau	54
<b>Figure 3.9:</b>	Consommation d'energie en fonction denombre de paquets	55
<b>Figure 3.10 :</b>	Consommation d'energie en fonction de nombre de sources	55



# INTRODUCTION

Les environnements mobiles offrent aujourd'hui des perspectives intéressantes dans le domaine des télécommunications. L'évolution récente des moyens de communication sans fil a permis la manipulation d'informations au travers d'unités de calcul portables aux caractéristiques bien particulières (faible capacité de stockage, source d'énergie autonomie, puissance limitée, etc.) qui accèdent au réseau par le biais d'une interface de communication sans fil.

Les réseaux mobiles sans fil, peuvent être classés en deux catégories : les réseaux avec infrastructure qui utilisent généralement le modèle de la communication cellulaire, et les réseaux sans infrastructure ou les réseaux ad hoc.

Plusieurs systèmes utilisent déjà le modèle cellulaire de réseaux sans fil, et connaissent une très forte expansion à l'heure actuelle : exemple les réseaux GSM, On cite aussi l'exemple du projet hollandais NAFIN ( Netherlands Armed Forces Integrated Network ), qui a visé d'améliorer les performances des forces militaires de l'air et marines, en intégrant la technologie des réseaux sans fil. L'inconvénient majeur du modèle cellulaire est qu'il requière une importante infrastructure logistique et matérielle fixe.

La contrepartie des réseaux cellulaires sont les réseaux mobiles ad hoc. Un réseau ad hoc est une collection d'entités mobiles interconnectées par une technologie sans fil formant un réseau temporaire sans l'aide de toute administration ou de tout support fixe.

Les applications des réseaux ad hoc sont nombreuses, on cite l'exemple classique de leur application dans le domaine militaire et les autres applications de tactique comme les opérations de secours et les missions d'exploration.

Notre travail entre dans le cadre de l'étude du problème de routage dans les réseaux mobiles ad hoc. Notre étude offre principalement une étude synthétique des travaux de recherche qui ont été fait, et qui se font à l'heure actuelle, dans le but de résoudre le problème d'acheminement de données entre les hôtes mobiles du réseau ad hoc. Comme nous allons voir le problème de routage est très compliqué, cela est dû essentiellement à la propriété qui caractérise les réseaux ad hoc et qui est l'absence d'infrastructure fixe et de toute administration centralisée.

Ce mémoire se divise en trois chapitres :

Dans le premier chapitre on présente les réseaux mobiles ad hoc, leurs caractéristiques, leurs applications et le problème de routage.

Au deuxième chapitre on présente une classification des différents protocoles de routage pour les réseaux ad hoc et on décrit en détail quelques protocoles tout en indiquant leurs avantages et leurs inconvénients.

Au troisième chapitre nous essayons d'évaluer et de comparer les performances de deux protocoles de routage Ad hoc. Les métriques d'évaluation de performances considérées dans cette étude sont : le coût de routage, le taux de paquets délivrés, le délai, la gigue, et la concentration de l'activité. La consommation d'énergie.

# **Chapitre 1.**

## **Les réseaux mobiles**

Dans ce chapitre nous allons présenter les environnements mobiles et les principaux concepts liés à ces environnements. Nous commençons par la définition de cet environnement et les deux classes qui le constituent (mode infrastructure et mode sans infrastructure). Nous introduisons ensuite le concept des réseaux ad hoc et les caractéristiques inhérentes à ces réseaux. Enfin nous définissons quelques domaines d'application d'un réseau ad hoc.

## **1.1 Définition des réseaux Mobiles**

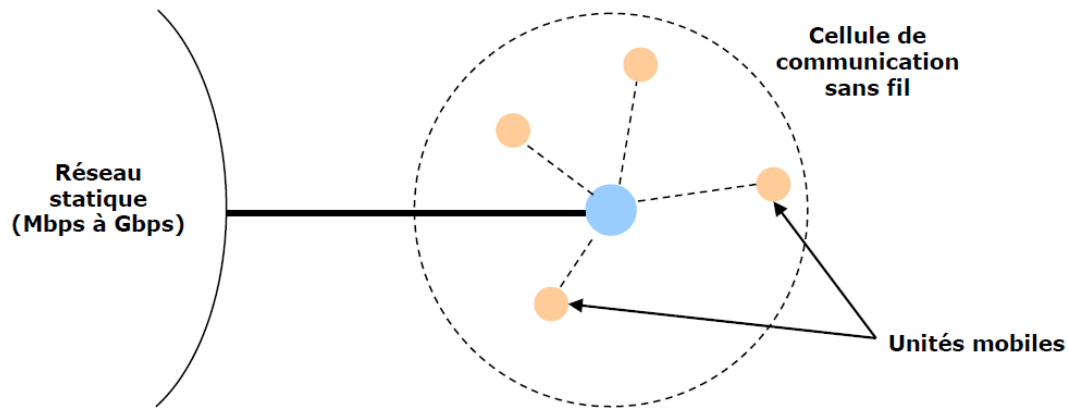
Un réseau est dit mobile s'il permet à ses utilisateurs d'accéder à l'information Indépendamment de leur position géographique. Pour communiquer entre eux les nœuds du réseau mobile utilisent une interface de communication sans fil (médium radio ou infrarouge) qui permet de propager les signaux sur une certaine distance. Les réseaux mobiles offrent une plus grande flexibilité d'emplois et un plus grand confort par rapport aux réseaux statiques.

Nous pouvons distinguer deux classes de réseaux mobiles, les réseaux mobiles avec infrastructure de communication, et les réseaux mobiles sans infrastructure de communication ou les réseaux Ad Hoc.

### **1.1.1 Les réseaux mobiles avec infrastructure**

Un réseau mobile avec infrastructure est basé sur un ensemble de sites fixes appelés stations de base qui sont interconnectés entre eux à travers un réseau de communication filaire, chaque station de base peut communiquer directement en

utilisant une interface sans fil avec les nœuds mobiles se trouvant dans une zone géographique limitée comme le montre la figure suivante



**Figure 1.1 :** Le modèle des réseaux mobiles avec infrastructure

### 1.1.1.1 Réseaux sans fil téléphonique

- **GSM (Global System for Mobile Communications)**

Norme mondiale la plus répandue de téléphonie cellulaire numérique qui exploite les fréquences 900 et 1800 Mhz dans plusieurs pays du monde et la 1900 Mhz en Amérique du Nord.

- **GPRS (General Packet Radio Service)**

Amélioration du GSM pour supporter les transferts de données.

- **UMTS (Universal Mobile Telecommunications System)**

La 3<sup>ème</sup> génération introduite comme la révolution des applications mobiles où elle assure aussi le transfert de sons, images et vidéos en haut débit (de 384 Kbps à 2Mbps)

- **EDGE (Enhanced Data rate for GSM Evolution)**

Proposé par l'opérateur téléphonique Bouygues Télécom alternative à l'UMTS avec un débit maximum de 384 Kbps. Les couches citées ci-dessus sont utilisées par quelques applications telles que WAP, iMode

- **WAP (Wireless Application Protocol)**

Introduit en 1997 dans le but de permettre aux téléphones portables de se connecter au Web par les collaborateurs NOKIA, ERICSSON, MOTOROLA et UNWIRED PLANET. Cette initiative devait permettre la consultation d'e-mails, l'accès aux réseaux locaux d'entreprises et beaucoup d'autres services. Mais les aspects techniques étaient limités et loin de l'image marketing annoncée pour ce protocole.

- **iMode (Internet Mode)**

Technologie développée par l'opérateur japonais NTT-DoCoMo et introduite en France par l'opérateur téléphonique Bouygues Télécom. iMode utilise la couche basse GPRS, et réalise de ce fait une économie considérable par rapport au WAP. Il garde la connexion juste au moment du transfert des paquets contrairement au WAP qui facture le temps de la consultation mais pas le volume des données transférées.

### **1.1.1.2 Réseaux sans fil informatiques**

Les autres réseaux qui nous intéressent particulièrement sont : Bluetooth, HomeRF, HiperLAN et WiFi

- **Bluetooth (Internet Mode)**

Cette technologie gère les connexions sans fil de type ondes radio utilisant les fréquences 2,4 Ghz d'un débit de 1Mbps et d'une portée de 10m à 30m. Cette technologie concurrence fortement l'infrarouge IrDA (InfraRed Data Association).

Le nom Bluetooth a été inspiré en 1994 par ses créateurs (ERICSSON, IBM, INTEL, NOKIA et TOSHIBA) du nom de Harald Blaatand (910-986), littéralement « Harald à la dent bleue » qui unifia le Danemark et la Norvège, dans une Europe divisée.



Le Bluetooth Special Interest Group (SIG) qui compte notamment Microsoft, IBM et Nokia comme membres vient d'adopter en novembre 2004, les spécifications de la norme Bluetooth 2.0+ Enhanced Data Rate. Offrant des débits théoriques de l'ordre du 3 Mbps, la future norme a fait son apparition début 2005 dans les magasins.

L'organisme a révélé quelques unes des principales nouveautés de son nouveau standard. Outre l'augmentation du débit qui va donc passer de 1 Mbps à 3 voire 10 Mbps dans certains cas, la consommation devrait diminuer de l'ordre de 50% environ.

Le taux d'erreurs sur bits, donnée caractérisant la fiabilité des communications, sera également en baisse. Ce lot d'innovation s'accompagne d'une compatibilité garantie avec les versions antérieures du Bluetooth.

- **HomeRF**

Norme qui devrait servir à banaliser la mise en place des réseaux locaux domestiques sans fil. Elle est inspirée des deux normes DECT (pour la transmission de la voix) et WLAN(pour la transmission de données TCP/IP)

HomeRF assure un traitement allant jusqu'à 127 noeuds et 6 liaisons voix.

Dans la pratique, la portée d'une base est de 50 mètres, ce qui est censé couvrir une maison moyenne avec son jardin. À l'opposé, un réseau Bluetooth définit un PAN(Personal Area Network), réseau radio de très courte portée, d'environ 10 mètres. Le débit brut radio d'une base HomeRF est de 1,6 Mbps et de 1 Mbps utile en IP, 800 Kbps en tenant compte des pertes et des interférences (une évolution vers un débit de 10 Mbps et 2 Mbps utiles est prévue, mais les matériels sont encore en phase de développement).

En matière de réseaux domestiques sans fil, HomeRF doit affronter la concurrence de Bluetooth.

La norme est en effet promue par plus de 1 000 industriels contre 90 pour

HomeRF. En outre, le groupe de travail 802. 15 de l'IEEE vient de se former pour standardiser une norme de réseau personnel PAN (Personal Area Network) sans fil reposant sur la technique Bluetooth. HomeRF a cependant pris de l'avance, puisque les premiers matériels sont déjà disponibles sur le marché. " Bluetooth possède un avantage marketing certain. Mais pour relier tous les appareils d'une maison, il est insuffisant en termes de portée. Bluetooth serait plutôt concurrent des liaisons infrarouges.

De plus, les premiers modèles d'appareils à la norme tardent à être Commercialisés. Il se pourrait que la première technologie sur le marché réussisse tout de même à l'emporter ", analyse le responsable des produits sans fil chez France Télécom R&D.

- **HiperLAN**

Spécifié par l'ETSI (European Telecommunications Standards Institute)

Mobilité supportée : piétonne (3m/s max i.e. 10km/h)

Hiperlan émet dans la bande des 5 GHz et permet d'atteindre un débit de 54 Mbps.

HiperLAN possède des avantages techniques, par exemple l'inclusion d'une classe de service lui permettant de gérer la voix et l'émission multimédia en continu. Elle intègre également une technique empêchant les interférences avec d'autres équipements radio.

- **WiFi**

La norme IEEE 80-2.11 [1A1](ISO/IEC 8802-11) est un standard international décrivant les caractéristiques d'un réseau local sans fil (WLAN). Le nom WiFi(contraction de Wireless Fidelity, parfois notée Wi-Fi) correspond initialement au nom donné à la certification délivrée par la Wi-Fi Alliance, anciennement WECA (Wireless Ethernet Compatibility Alliance), l'organisme chargé de maintenir l'interopérabilité entre les matériels répondant à la norme

802.11. Par abus de langage (et pour des raisons de marketing) le nom de la norme se confond aujourd'hui avec le nom de la certification.

Ainsi un réseau Wifi est en réalité un réseau répondant à la norme 802.11.

### **1.1.2 Le réseau mobile sans infrastructure :**

Le réseau mobile sans infrastructure également appelé réseau Ad hoc ou IBSS (Independent Basic Service Set) ne comporte pas l'entité « site fixe », tous les sites du réseau sont mobiles et se communiquent d'une manière directe en utilisant leurs interfaces de communication sans fil . L'absence de l'infrastructure ou du réseau filaire composé des stations de base, oblige les unités mobiles à se comporter comme des routeurs qui participent à la découverte et la maintenance des chemins pour les autres hôtes du réseau

#### **1.1.2.1 Les réseaux mobiles Ad Hoc**

##### **1. Définition**

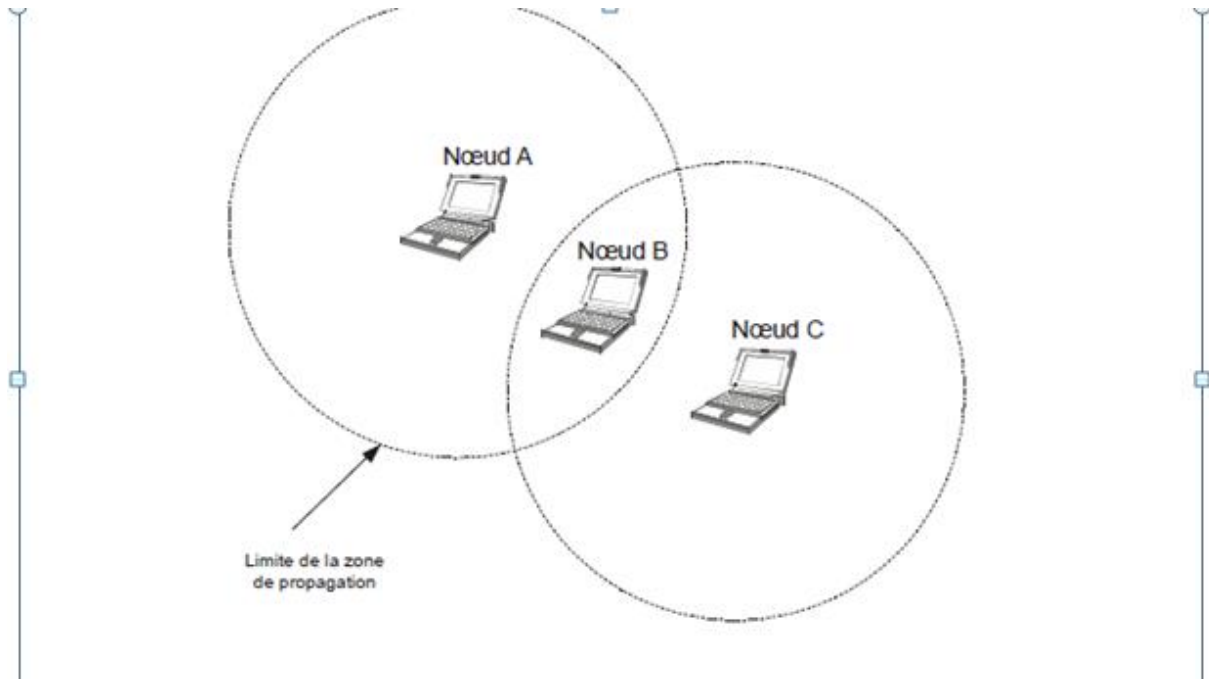
Un réseau mobile ad hoc, appelé généralement MANET (Mobile Ad hoc NETwork), consiste en une grande population relativement dense d'unités mobiles qui se déplacent dans un territoire quelconque et dont le seul moyen de communication est l'utilisation des interfaces sans fil, sans l'aide d'une infrastructure préexistante ou d'administration centralisée.

Le concept des réseaux mobiles ad hoc essaie d'étendre les notions de la mobilité à toutes les composantes de l'environnement. Ici, contrairement aux réseaux basés sur la communication cellulaire :

- Aucune administration centralisée n'est disponible

⇒ Ce sont les hôtes mobiles elles-mêmes qui forment, d'une manière ad hoc, une infrastructure du réseau.

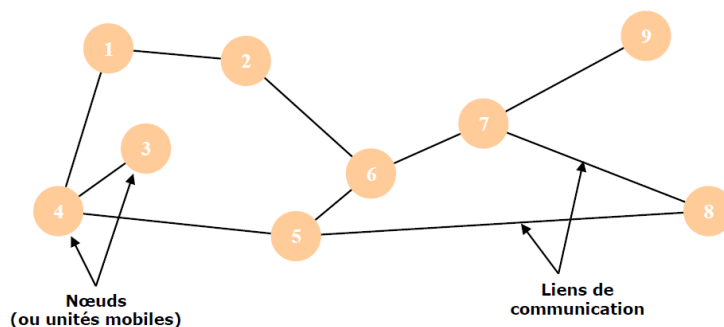
- Aucune supposition ou limitation n'est faite sur la taille du réseau ad hoc, le réseau peut contenir des centaines ou des milliers d'unités mobiles.



**Figure 1.2 : SIMPLE RESEAU AD HOC**

## 2. Modélisation

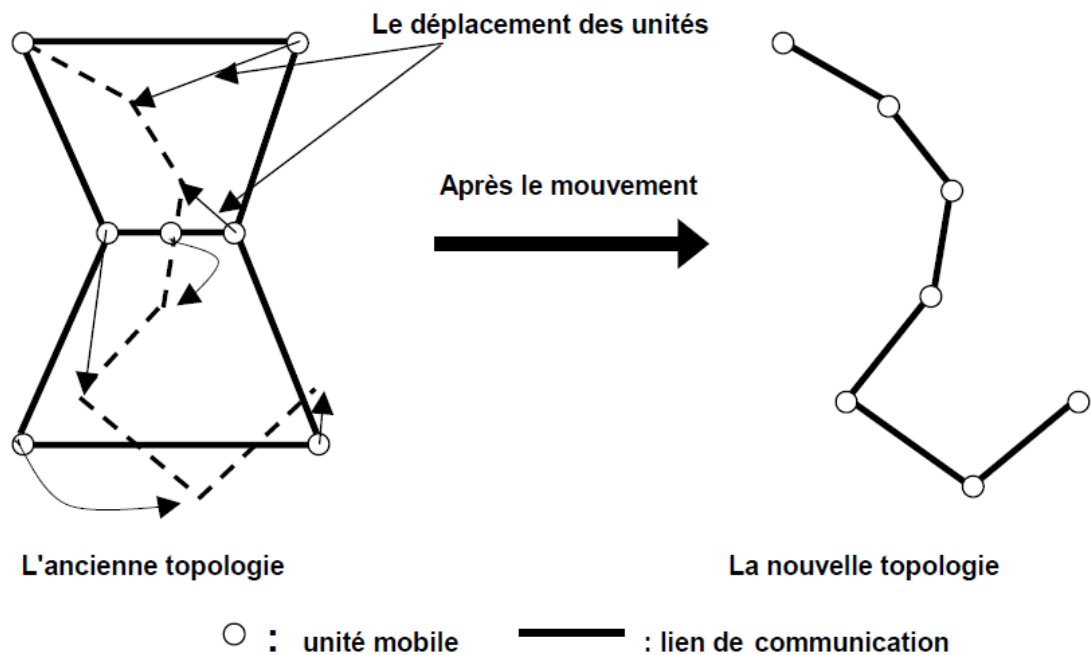
Un réseau ad hoc peut être modéliser par un graphe  $G_t = (V_t, E_t)$  où  $V_t$  représente l'ensemble des noeuds (i.e. les unités ou les hôtes mobiles) du réseau et modélise l'ensemble les connections qui existent entre ces noeuds (voir la figure 1.3). Si  $e = (u, v)$  appartient à  $E_t$ , cela veut dire que les noeuds  $u$  et  $v$  sont en mesure de communiquer directement à l'instant  $t$ .



**Figure 1.3 : La modélisation d'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.

### Exemple



**Figure 1.4 :** La topologie du réseau ad-hoc

## 3. Les caractéristiques des réseaux ad hoc

Les réseaux mobiles ad hoc sont caractérisés par ce qui suit :

**Une 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. Les liens de la topologie peuvent être unis ou bidirectionnels.

**Une bande passante limitée** : Une des caractéristiques primordiales des réseaux basés sur la communication sans fil est l'utilisation d'un médium de communication partagé. Ce partage fait que la bande passante réservée à un hôte soit modeste.

**Des 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.

**Une 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.

**L'absence d'infrastructure :** Les réseaux ad hoc se distinguent des autres réseaux mobiles par la propriété d'absence d'infrastructure 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.

**La notion de « multihop » :** un réseau ad hoc est qualifié par « multihop » car plusieurs noeuds mobiles peuvent participer au routage et servent comme routeurs intermédiaires.

#### **4. Les applications des réseaux mobiles ad hoc**

La particularité du réseau Ad hoc est qu'il n'a besoin d'aucune installation fixe, ceci lui permettant d'être rapide et facile à déployer. Les applications tactiques comme les opérations de secours, militaires ou d'explorations trouvent en Ad Hoc, le réseau idéal. La technologie Ad Hoc intéresse également la recherche, des applications civiles sont apparues. On distingue :

- Les services d'urgence : opération de recherche et de secours des personnes, tremblement de terre, feux, inondation, dans le but de remplacer l'infrastructure filaire.
- Le travail collaboratif et les communications dans des entreprises ou bâtiments : dans le cadre d'une réunion ou d'une conférence par exemple.

- Home network : partage d'applications et communications des équipements mobiles.
- Applications commerciales : pour un paiement électronique distant (taxi) ou pour l'accès mobile à l'Internet, où service de guide en fonction de la position de l'utilisateur.
- Réseaux de senseurs : pour des applications environnementales (climat, activité de la terre, suivi des mouvements des animaux, . . . etc.) ou domestiques (contrôle des équipements à distance).
- Réseaux en mouvement : informatique embarquée et véhicules communicants.
- Réseaux Mesh : c'est une technologie émergente qui permet d'étendre la portée d'un réseau ou de le densifier.

## **5. Communication dans les réseaux ad hoc**

Un réseau est dit sans fil lorsque les machines qui le composent ne sont pas reliées entre elles par des câbles, mais utilisent, pour communiquer, le médium radio ou infrarouge. Comme les signaux propagés sur ces media s'atténuent au fur et à mesure qu'ils s'éloignent de leur émetteur, un nœud ne peut pas communiquer avec un autre s'il est situé trop loin de lui. On définit alors l'ensemble des voisins d'un nœud comme étant l'ensemble des nœuds capables de recevoir et de comprendre les signaux émis par celui-ci.

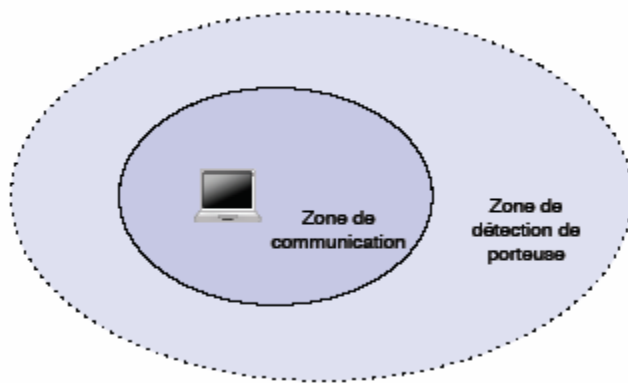
Avant tout, les conditions suivantes doivent être remplies pour qu'un paquet puisse être reçu :

- La puissance du signal reçu doit dépasser un certain seuil (seuil de communication).
- Le rapport signal sur bruit ambiant doit être suffisamment grand (le signal doit être clairement identifié, et non noyé dans le bruit).

Il existe un seuil de détection de porteuse. Si la puissance du signal est comprise entre ce seuil et le seuil de communication, alors le message n'est pas compris mais l'activité sur le canal est néanmoins détectée. Si le modèle de propagation radio utilisé «two-ray ground» (ou le modèle «free-space»), ces seuils définissent donc deux zones autour d'un nœud. Si le récepteur est placé au centre de la figure 1.3, alors un émetteur placé dans la zone interne (zone de communication) pourra lui envoyer des messages qui seront compris (en l'absence d'autres interférences). Si l'émetteur est placé dans la zone externe (zone de détection de porteuse), la communication ne sera pas possible mais l'autre mobile sera informé à chaque fois que l'émetteur accédera au canal. Si le modèle de propagation radio utilisé «shadowing», les deux zones sont également définies, mais leurs frontières sont "floues" du fait du caractère probabiliste du modèle.

<Le protocole 802.11 impose qu'un mobile qui veut émettre doit d'abord s'assurer qu'aucune autre communication n'est en cours dans son voisinage. Si une telle communication est en cours, et si l'émetteur est suffisamment proche (lui-même dans la zone de communication) du mobile qui voudrait lui aussi émettre, alors ce dernier a reçu l'en-tête du message et sait donc (par l'intermédiaire de son Network Allocation Vector) pour combien de temps le canal doit encore être occupé. Le nœud qui voulait émettre va donc attendre. Par contre, si le mobile qui veut aussi émettre est plus loin (dans la zone de détection de porteuse de l'émetteur) l'en-tête n'a pas pu être compris. Il est impossible dans ce cas de prévoir à l'avance quand on aura à nouveau le droit d'émettre, il faut attendre que l'activité sur le canal disparaisse. Dans ces contextes, les différents nœuds se gênent les uns les autres, et cela se traduit par un partage du canal entre eux.





**Figure 1.5 Zones de communication et de détection de porteuse**

Le réseau Ad hoc manifeste beaucoup de simplicités et assez d'avantages par rapport aux autres réseaux (filaires et cellulaires) par sa facilité de déploiement en cas d'urgence ou de travaux temporaires dont les autres réseaux engendrent des frais importants. Cependant de nouveaux problèmes apparaissent, en effet l'absence d'une infrastructure centralisée fait du routage dans les réseaux ad hoc un problème très compliqué. Dans la plupart des cas, le nœud destination ne se trouve pas obligatoirement dans la portée du nœud source ce qui implique que l'échange des données entre les deux nœuds doit être effectué par des stations intermédiaires. Par ailleurs, la topologie de ces réseaux qui peuvent être continuellement mobile oblige les protocoles de routage à réagir rapidement.

Après avoir présenté l'environnement mobile ad hoc, une étude sur le routage dans cet environnement sera faite dans le chapitre prochain.

# **Chapitre 2. Les protocoles de routage dans les réseaux Ad- Hoc**

Le routage est une méthode d'acheminement des informations vers la bonne destination à travers un réseau de connexion donnée, il consiste à assurer une stratégie qui garantit, à n'importe quel moment, un établissement de routes qui soient correctes et efficaces entre n'importe quelle paire de nœud appartenant au réseau, ce qui assure l'échange des messages d'une manière continue. Vu les limitations des réseaux ad hoc, la construction des routes doit être faite avec un minimum de contrôle et de consommation de la bande passante

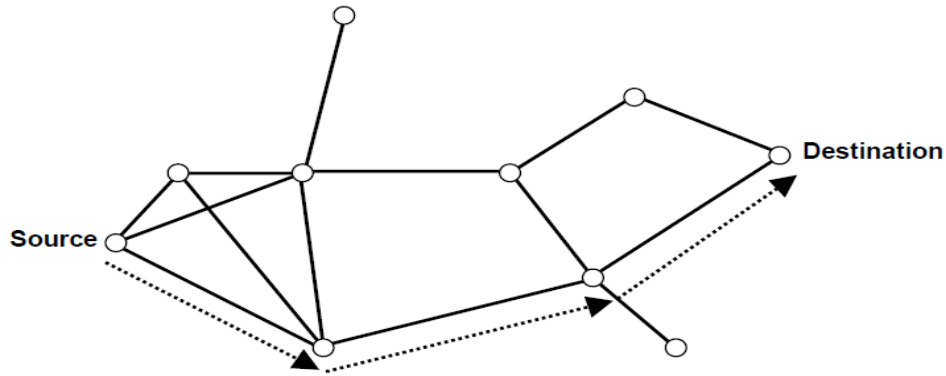
Dans ce qui suit, nous décrirons brièvement la difficulté de routage dans les réseaux ad hoc et les différents mécanismes de routages apparus pour la résolution de ce problème.

## **2.1 Définition du routage**

Le routage est une méthode d'acheminement des informations à la bonne destination à travers un réseau de connexion donné. Le problème de routage consiste à déterminer un acheminement optimal des paquets à travers le réseau au sens d'un certain critère de performance. Le problème consiste à trouver l'investissement de moindre coût en capacités nominales et de réserves qui assure le routage du trafic nominal et garantit sa survabilité en cas de n'importe quelle panne d'arc ou de nœud.

### **Exemple :**

Si on suppose que les coûts des liens sont identiques, le chemin indiqué dans la figure(3.1) suivante est le chemin optimal reliant la station source et la station destination. Une bonne stratégie de routage utilise ce chemin dans le transfert des données entre les deux stations.



**Figure 2.1 :Le chemin utilisé dan le routage entre la source et la destination.**

Le problème qui se pose dans le contexte des réseaux ad hoc est l'adaptation de la méthode d'acheminement utilisée avec le grand nombre d'unités existant dans un environnement caractérisé par de modestes capacités de calcul et de sauvegarde et de changements rapides de topologies.

Il semble donc important que toute conception de protocole de routage doive étudier les problèmes suivants :

- 1- La minimisation de la charge du réseau
- 2- Offrir un support pour pouvoir effectuer des communications multi-points fiables
- 3- Assurer un routage optimal
- 4- Offrir une bonne qualité concernant le temps de latence.

## **2.2 Le Routage dans les Réseaux Ad Hoc**

Les protocoles de routage peuvent être classés en différentes familles selon le moment auquel ils initient la découverte de route, selon la manière dont les nœuds d'un réseau se partagent le travail de routage et selon la manière dont les informations de routage sont échangées.

### **2.3 La difficulté du routage dans les réseaux Ad hoc**

De fait qu'un réseau ad hoc est un ensemble de nœuds mobiles qui sont dynamiquement et arbitrairement éparpillés d'une manière ou l'interconnexion entre les nœuds peut changer à tout moment. Il se peut qu'un hôte destination soit hors de la portée de communication d'un hôte source, ce qui nécessite l'emploi d'un routage interne par les nœuds intermédiaires afin de faire acheminer les paquets de message à la bonne destination.

En effet, la topologie évoluant constamment en fonction des mouvements des mobiles, Le problème qui se pose dans le contexte des réseaux ad hoc est l'adaptation de la méthode d'acheminement utilisée avec le grand nombre d'unités existant dans un environnement caractérisé par de modestes capacités de calcul et de sauvegarde.

D'ailleurs dans la pratique il est impossible qu'un hôte puisse garder les informations de routage concernant tous les autres nœuds, dans le cas où le réseau serait volumineux.

### **2.4 Les contraintes de routages dans les réseaux ad hoc**

L'étude et la mise en œuvre d'algorithmes de routage pour assurer la connexion des réseaux ad hoc au sens classique du terme (tout sommet peut atteindre tout autre), est un problème complexe. L'environnement est dynamique et évolue donc au cours du temps, la topologie du réseau peut changer fréquemment. Il semble donc important que toute conception de protocole de routage doive étudier les problèmes suivants :

- **Minimisation de la charge du réseau :**

L'optimisation des ressources du réseau renferme deux autres sous problèmes qui sont l'évitement des boucles de routage, et l'empêchement de la concentration du trafic autour de certains nœuds ou liens.

- **Offrir un support pour pouvoir effectuer des communications multi-points fiables :**

Le fait que les chemins utilisés pour router les paquets de données puissent évoluer, ne doit pas avoir d'incident sur le bon acheminement des données. L'élimination d'un lien, pour cause de panne ou pour cause de mobilité devrait, idéalement, augmenter le moins possible les temps de latence.

- **Assurer un routage optimal :**

La stratégie de routage doit créer des chemins optimaux et pouvoir prendre en compte différentes métriques de coûts (bande passante, nombre de liens, ressources du réseau,... etc.). Si la construction des chemins optimaux est un problème dur, la maintenance de tels chemins peut devenir encore plus complexe, la stratégie de routage doit assurer une maintenance efficace de routes avec le moindre coût possible.

- **Le temps de latence :**

La qualité des temps de latence et de chemins doit augmenter dans le cas où la connectivité du réseau augmente

### **3.1 Les protocoles de routage dans les réseaux ad – hoc**

Comme nous avons déjà vu, un réseau ad hoc est un ensemble de nœuds mobiles qui sont dynamiquement et arbitrairement éparpillés d'une manière où l'interconnexion entre les nœuds peut changer à tout moment. Dans la plupart des cas, l'unité destination ne se trouve pas obligatoirement dans la portée de l'unité source ce qui implique que l'échange des données entre deux nœuds quelconques, doit être effectué par des stations intermédiaires.

La stratégie de routage est utilisée dans le but de découvrir les chemins qui existent entre les nœuds. Le but principal d'une telle stratégie est l'établissement de routes qui soient correctes et efficaces entre une paire quelconque d'unités, ce qui assure l'échange des messages d'une manière continue. Vu les limitations des réseaux ad hoc, la construction des routes doit être faite avec un minimum de contrôle et de consommation de la bande passante.

Il existe deux grandes familles de protocoles de routage : les protocoles basés sur l'état des liens, et ceux basés sur le vecteur de distance.

Les deux méthodes exigent une mise à jour périodique des données de routage qui doivent être diffusées par les différents nœuds de routage du réseau. Les algorithmes de routage basés sur ces deux méthodes, utilisent la même technique qui est la technique des plus courts chemins, et permettent à un hôte donné, de trouver le prochain hôte pour atteindre la destination en utilisant le trajet le plus court existant dans le réseau.

La famille des protocoles à état de liens se base sur les informations rassemblées sur l'état des liens dans le réseau. Ces informations sont disséminées dans le réseau périodiquement ce qui permet ainsi aux nœuds de construire une carte complète du réseau. Un nœud qui reçoit les informations concernant l'état des liens, met à jour sa vision de la topologie du réseau et applique un algorithme de calcul des chemins optimaux afin de choisir le nœud suivant pour une destination donnée. Un exemple des algorithmes les plus connus appliqué dans le calcul des plus courts chemins, est celui de Dijkstra.

Les protocoles à vecteur de distance se basent sur un échange, entre voisins, des informations de distances des destinations connues. Chaque nœud envoie à ses voisins la liste des destinations qui lui sont accessibles et le coût correspondant. Le nœud récepteur met à jour sa liste locale des destinations avec les coûts minimums. 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).

Un problème de performance de cet algorithme est dû à l'absence de coordination entre nœuds, dans les modifications des tables de routage qui peuvent être faites en se basant

sur des données erronées (le problème de « *boucles de routage* »). En plus de cela, le DBF ne possède pas de mécanisme précis qui peut déterminer quand est ce que le réseau doit arrêter l'incrément de la distance qui correspond à une destination donnée, ce problème est appelé : « *comptage à l'infini* ».

La circulation inutile des paquets de messages, qui peut arriver avec le DBF, est intolérable dans les réseaux mobiles ad hoc, caractérisés par une bande passante limitée et des ressources modestes. En plus de cela, la mobilité fréquente des nœuds met que la convergence du DBF prend beaucoup de temps, ce qui pénalise le routage dans de tels environnements.

Les principaux protocoles de routage dans les réseaux sans fil ad hoc sont les suivants :

- DSR, Dynamic Source Routing.
- DSDV, Destination-Sequenced Distance Vector.
- AODV, Ad-hoc On Demand Distance Vector[4].
- TORA, Temporally-Ordered Routing Algorithm.
- OLSR Optimized Link State Routing Protocol.
- TBRPF, Topology Broadcast Based on Reverse-Path Forwarding.



Le classement de ces protocoles suivant les deux familles de protocoles est le suivant :

- État des liens : TORA[6], OLSR et TBRPF.
- Vecteur de distance : DSR, DSDV et AODV.

Suivant la manière de création et de maintenance de routes lors de l'acheminement des données, les protocoles de routage peuvent être séparés en :

- **Proactif** : DSDV, OLSR et TBRPF adoptent ce comportement. Les protocoles proactifs établissent les routes à l'avance en se basant sur l'échange périodique des tables de routage.
- **Réactif** (on demand) : TORA et AODV adoptent ce comportement. Les protocoles réactifs cherchent les routes à la demande. AODV est en fait une version réactive de DSDV.
- **Hybride** : les protocoles hybrides définissent deux zones où ils combinent le comportement proactif à l'intérieur d'une zone et le comportement réactif entre les zones. Par exemple DSR, qui est réactif à la base mais qui peut être optimisé s'il adopte un comportement proactif.

### 3.1.1 Les protocoles de routage proactifs

Les protocoles de routage proactifs essaient de maintenir les meilleurs chemins existants vers toutes les destinations possibles (qui peuvent représenter l'ensemble de tous les nœuds du réseau) au niveau de chaque nœud du réseau. Les routes sont sauvegardées mêmes si elles ne sont pas utilisées. La sauvegarde permanente des chemins de routage, est assuré par un échange continu des messages de mise à jour des chemins, ce qui induit un contrôle excessif surtout dans le cas des réseaux de grande taille.

### **3.1.1 Avantages et les inconvénients des protocoles proactifs :**

Avec un protocole proactif, les routes sont disponibles immédiatement, ainsi l'avantage d'un tel protocole est le gain de temps lors d'une demande de route. Le problème est que, les changement de routes peuvent être plus fréquents que la demande de la route et le trafic induit par les messages de contrôle et de mise à jour des tables de routage peut être important et partiellement inutile, ce qui gaspille la capacité du réseau sans fin. De plus, la taille des tables de routage croît linéairement en fonction du nombre de nœud.

#### **3.1.1.2 LE PROTOCOLE DE ROUTAGE « DSDV » [7]**

- Basé sur l'idée classique de l'algorithme distribué de Bellman-Ford en rajoutant quelques améliorations.
- Chaque station mobile maintient une table de routage qui contient :
  - Toutes les destinations possibles.
    - Le nombre de nœud (ou de sauts) nécessaire pour atteindre la destination.
    - Le numéro de séquences (SN : sequence number) qui correspond à un nœud destination.
  - Le NS est utilisé pour faire la distinction entre les anciennes et les nouvelles routes, ce qui évite la formation des boucles de routage.
  - La mise à jour dépend donc de deux paramètres : Le temps, c'est à dire la période de transmission, et Les événements
- Un paquet de mise à jour contient :

1- Le nouveau numéro de séquence incrémenté, du noeud émetteur.

Et pour chaque nouvelle route :

2- L'adresse de la destination.

3- Le nombre de noeuds (ou de sauts) séparant le noeud de la destination.

4- Le numéro de séquence (des données reçues de la destination) tel qu'il a été estampillé par la destination

.

- Le DSDV élimine les deux problèmes de boucle de routage "routing loop", et celui du "counting to infinity".

Cependant :

- Dans ce protocole, une unité mobile doit attendre jusqu'à ce qu'elle reçoive la prochaine mise à jour initiée par la destination, afin de mettre à jour l'entrée associée à cette destination, dans la table de distance. Ce qui fait que le DSDV est lent.
- Le DSDV utilise une mise à jour périodique et basée sur les événements, ce qui cause un contrôle excessif dans la communication.

### **3.1.1.3 Le protocole de routage FSR**

Le protocole "Routage à Etat de l'œil du Poisson" FSR, (Fisheye State Routing) peut être vu comme une amélioration du protocole GSR précédent. Le nombre élevé des messages de mise à jour échangés implique une grande consommation de la bande passante, ce qui a un effet négatif dans les réseaux ad hoc caractérisés par une bande passante limitée. Le protocole FSR est basé sur l'utilisation de la technique "œil de poisson" (fisheye), proposée par Kleinrock et

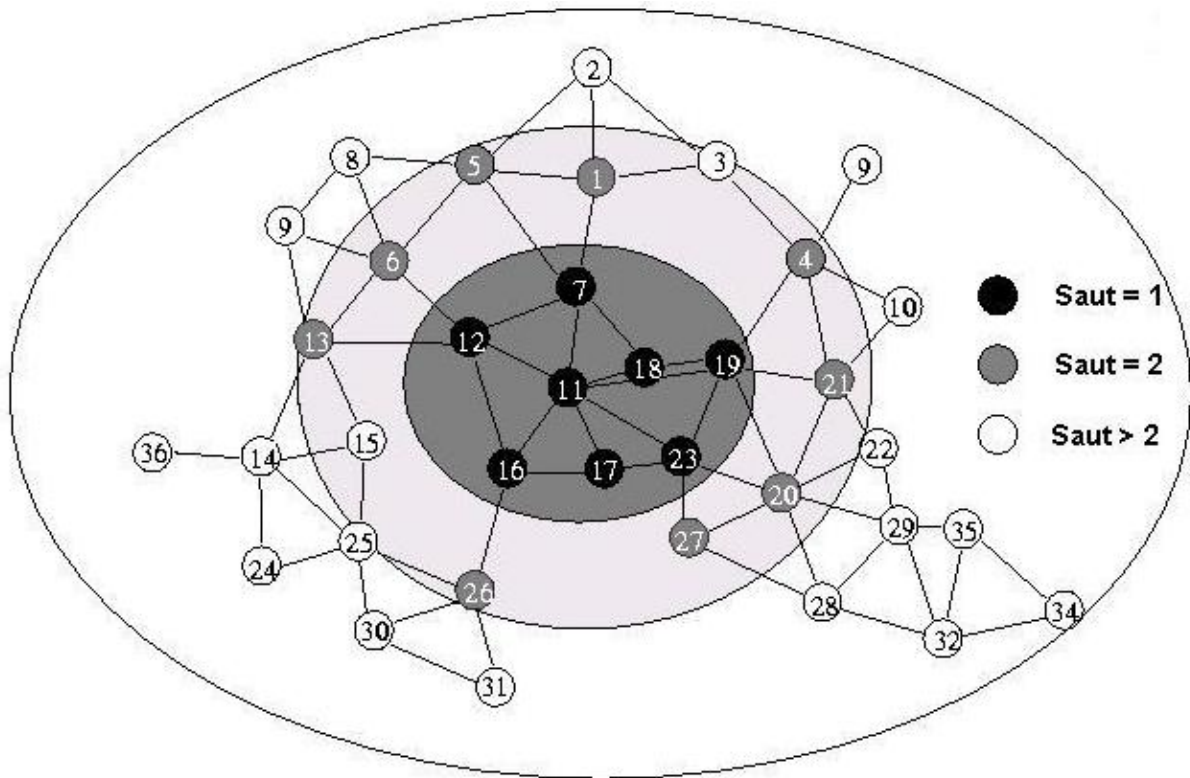
Stevens, qui l'ont utilisé dans le but de réduire le volume d'information nécessaire pour représenter les données graphiques.

L'œil d'un poisson capture avec précision les points proches du point focal. La précision diminue quand la distance, séparant le point vu et le point focal augmente. Dans le contexte du routage, l'approche du "fish-eye" matérialise, pour un nœud, le maintien des données concernant la précision de la distance et la qualité du chemin d'un voisin direct, avec une diminution progressive du détail et de précision quand la distance augmente.

Le protocole FSR est similaire au protocole LS dans sa sauvegarde de la topologie au niveau de chaque nœud. La différence principale réside dans la manière dont les informations de routage circulent. Dans le FSR, la diffusion par inondation de messages n'existe pas : l'échange se fait uniquement avec les voisins directs. Les données de mise à jour échangées périodiquement dans le FSR ressemblent au vecteur échangé dans le protocole DSDV, où les distances sont modifiées suivant l'estampille du temps ou le numéro de séquence associé au nœud qui a été l'origine de la mise à jour.

Dans le FSR les états de liens sont échangés, l'image complète de la topologie du réseau est gardée au niveau de chaque nœud, et les meilleurs chemins sont échangés en utilisant cette image. Comme nous l'avons déjà dit, l'état des liens change fréquemment dans les réseaux ad hoc. Le FSR effectue la mise à jour de ces changements de la même manière que le protocole GSR, ce qui résout les problèmes du protocole LS concernant le volume des données de contrôle.

Avec le GSR, quand la taille du réseau devient très grande, les messages de mise à jour peuvent consommer considérablement de bande passante. Afin de réduire le volume de messages échangés sans toucher à la consistance et la précision des données de routage, le FSR utilise la technique "œil de poisson".



**La figure 2.2 : œil de poisson.**

Dans cette figure, on définit la portée, ou le champ de vision, de l'œil de poisson pour le nœud du centre, d'identificateur 5. La portée est définie en termes de nœuds qui peuvent être atteints en passant par un certain nombre de sauts. Le nœud du centre (le nœud 11), maintient les données les plus précises des nœuds appartenant au cercle, et cette précision diminue progressivement pour les cercles moins proches du centre.

### **La technique "œil de poisson".**

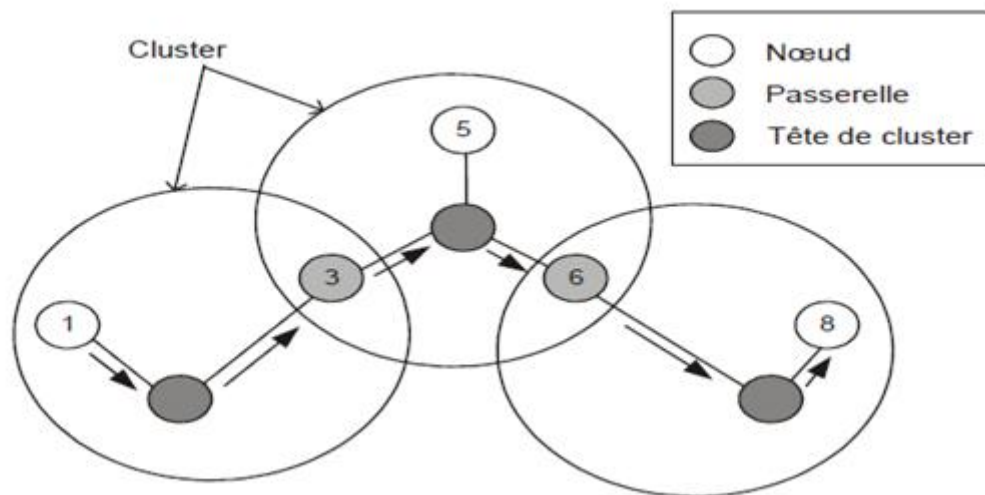
- Dans le contexte du routage, l'approche du "fish-eye" matérialise, pour un nœud, le maintien des données concernant la précision de la distance et la qualité du chemin d'un voisin direct, avec une diminution progressive, du détail et de précision, quand la distance augmente.
- La diminution de fréquence est assurée en changeant les fréquences de mise à jour, et cela en utilisant des périodes d'échanges différentes pour les

différentes entrées de la table de routage. Les entrées qui correspondent aux nœuds les plus proches, sont envoyés aux voisins avec une fréquence élevée (donc avec une période d'échange relativement petite).

#### **3.1.1.4 Le protocole de routage CGSR (Clusterhead Gateway Switch Routing )**

Ce protocole décompose la topologie en un groupe de clusters où dans chaque cluster un algorithme distribué est chargé d'élire un leader qui prend la responsabilité de tout le cluster (voir Figure 1.7). Plusieurs schémas de routage sont acceptés. L'allocation de la bande passante est aussi possible. CGSR utilise DSDV comme protocole de routage fondamental, mais ici l'approche est hiérarchique où pour le routage il faut passer par les têtes de cluster. La gestion de ce système de têtes de cluster peut réduire les temps d'acheminements des paquets utiles. Une passerelle *Gateway* est le nœud chargé de router les paquets entre deux têtes de cluster. Le routage s'effectue dans l'ordre : Source - Tête de cluster - Gateway - ..... - Tête de cluster - Gateway -

Destination. Chaque nœud garde une table de membres de clusters et une autre table de routage. Elles sont mises à jour en utilisant DSDV. Avec ces deux tables chaque nœud sera en mesure de déterminer la tête de cluster le plus proche de sa destination. Sur la figure 3.2, nous remarquons que le nœud 1 pour envoyer au nœud 8, il doit s'adresser à la tête de cluster auquel il appartient puis c'est elle qui prend en charge le reste du routage en passant par les *Gateways* et même d'autres têtes de clusters.



**Figure 2.3 ROUTAGE DU 1 AU NŒUD 8 PAR CGSR**

### 3.1.2 Les protocoles de routage réactifs (à la demande)

Les protocoles de routage réactifs (dits aussi : protocoles de routage à la demande), représentent les protocoles les plus récents proposés dans le but d'assurer le service du routage dans les réseaux sans fil.

La majorité des solutions proposées pour résoudre le problème de routage dans les réseaux ad hoc, et qui sont évaluées actuellement par le groupe de travail MANET (Mobile Ad Hoc Networking Working Groupe[2]) de l'IETF (Internet Engineering Task Force[3]), appartiennent à cette classe de protocoles de routage.

Les protocoles de routage appartenant à cette catégorie, créent et maintiennent les routes selon les besoins. Lorsque le réseau a besoin d'une route, une procédure de découverte globale de routes est lancée, et cela dans le but d'obtenir une information. Le routage à la demande induit une lenteur à cause de la recherche des chemins, ce qui peut dégrader les performances des applications interactives (exemple les applications des bases de données distribuées). En outre, il est impossible de connaître au préalable la qualité du chemin (en termes de bande passante, délais,... etc.). Une telle connaissance est importante dans les applications multimédias.

### **3.1.2.1 Avantages et les inconvénients des protocoles réactifs:**

A l'opposé des protocoles proactifs, dans le cas d'un protocole réactif, aucun message de contrôle ne charge le réseau pour des routes inutilisées ce qui permet de ne pas gaspiller les ressources du réseau. Mais la mise en place d'une route par inondation peut être coûteuse et provoquer des délais importants avant l'ouverture de la route et les retards dépassent bien souvent les délais moyens admis par les logiciels, aboutissant à une impossibilité de se connecter alors que le destinataire est bien là.

### **3.1.2.2 Le protocole de routage AODV**

- Le protocole "Routage avec Vecteur de Distance à la Demande" (AODV : Ad hoc Ondemand Distance Vector), représente essentiellement une amélioration de l'algorithme DSDV discuté dans la section 3.2.1. Il réduit le nombre de diffusions de messages en créant les routes au besoin, contrairement au DSDV qui maintient la totalité des routes.
- L'AODV est basé sur l'utilisation des deux mécanismes "Découverte de route" et "Maintenance de route" (utilisés par le DSR), en plus du routage nœud-par-nœud, du principe des numéros de séquence et de l'échange périodique du DSDV.
- A cause de la mobilité des nœuds dans les réseaux ad hoc, les routes changent fréquemment ce qui fait que les routes maintenues par certains nœuds, deviennent invalides. Les numéros de séquence permettent d'utiliser les routes les plus nouvelles (fresh routes).



## PRINCIPE

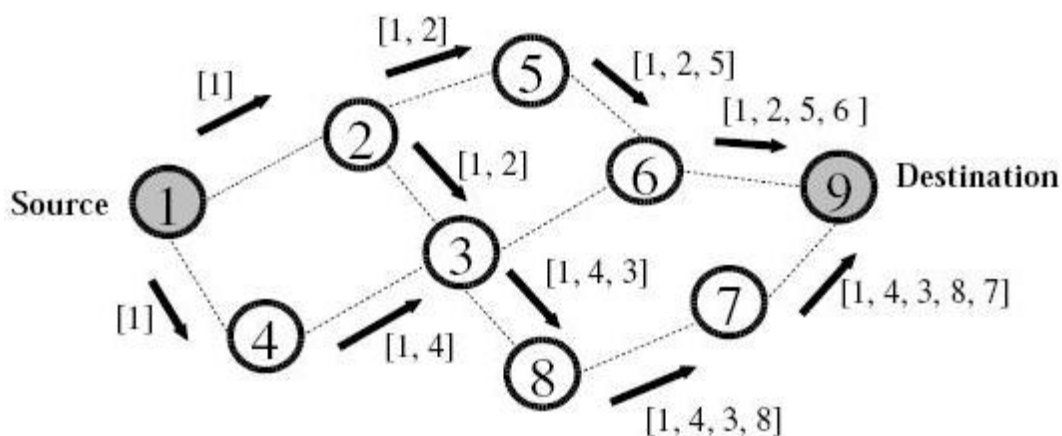
- De la même manière que dans le DSR, l'AODV utilise une requête de route dans le but de créer un chemin vers une certaine destination. Cependant, l'AODV maintient les chemins d'une façon distribuée en gardant une table de routage, au niveau de chaque nœud de transit appartenant au chemin cherché.
  - Un nœud diffuse une requête de route dans le cas où il aurait besoin de connaître une route vers une certaine destination et qu'une telle route n'est pas disponible. Cela peut arriver :
    - → si la destination n'est pas connue au préalable, ou
    - → si le chemin existant vers la destination a expiré sa durée de vie ou il
    - est devenu défaillant
  - Le champ numéro de séquence destination du paquet RREQ, contient la dernière valeur connue du numéro de séquence, associé au nœud destination. Cette valeur est recopiée de la table de routage. Si le numéro de séquence n'est pas connu, la valeur nulle sera prise par défaut. Le numéro de séquence source du paquet RREQ contient la valeur du numéro de séquence du nœud source.
  - Afin de maintenir des routes consistantes, une transmission périodique du message "HELLO" est effectuée. Si trois messages "HELLO" ne sont pas reçus consécutivement à partir d'un nœud voisin, le lien en question est considéré défaillant.
  - Le protocole AODV ne présente pas de boucle de routage, en outre il évite le problème "counting to infinity" de Bellman-Ford, ce qui offre une convergence rapide quand la topologie du réseau ad hoc change.

### 3.1.2.3 Le protocole DSR

DSR (*Dynamic Source Routing*) [5] est un protocole On-demand semblable au protocole AODV, il utilise une technique appelé « Source Routing » dans laquelle l'émetteur (la source) indique la route complète par laquelle un paquet doit passer pour atteindre sa destination, cette route est insérée dans l'entête du paquet. Les nœuds intermédiaires entre le nœud source et le nœud destination n'ont pas besoins de maintenir à jour les informations sur la route traversée puisque la route complète est insérée dans l'entête du paquet.

Si un nœud dans DSR veut communiquer avec une destination à laquelle il ne possède pas de route, il inonde le réseau avec un paquet de requête (RREQ) similaire a celui de AODV. Chaque nœud qui reçoit la requête et qui ne possède pas de route à la destination demandée insère son adresse dans le paquet RREQ et le diffuse à ses voisins. La réponse à la requête (RREP) est retournée par la destination ou par un autre nœud qui possède une route à la destination (figure 3.4).

(Inondation de la requête)



(Renvoi de la réponse)

**figure 2.4 la requête (RREP)**

## **2.6 Propriétés ciblées par les protocoles de routage des réseaux ad hoc**

Les protocoles ad hoc vérifient des propriétés que d'autres n'ont pas, mais il reste encore d'autres dignes d'intérêt. Nous citons certaines propriétés pour les deux cas :

### **2.6.1 Distribution des opérations**

Il faut que chacun des nœuds agisse tout seul suite à un événement et il ne doit dépendre d'aucun autre nœud. Tous les nœuds sont au même niveau et il n'existe aucune hiérarchie ni de structure centralisée pour la supervision, seuls les trois états sont accessibles récepteur, émetteur ou routeur.

### **2.6.2 Routes sans cycle**

Le protocole doit générer des routes sans cycle « *loop-free* » ce qui nous évite les pertes sur la bande passante ainsi que la consommation de ressources CPU ou d'énergie.

### **2.6.3 Opération à la demande**

La réaction à la demande permet d'économiser de l'énergie. Parce qu'avec les messages périodiques, non seulement la bande passante est mal exploitée mais en plus l'énergie est utilisée inutilement dans la plupart des cas.

### **2.6.4 Liens unidirectionnels**

L'usage de la technologie radio provoque des liaisons unidirectionnelles surtout si des obstacles physiques se trouvent dans l'environnement, où nous trouvons un nœud qui peut atteindre un autre par contre la réciproque ne peut se faire. L'acceptation des liens unidirectionnels améliore considérablement les performances du protocole

### **2.6.5 La sécurité**

Les réseaux ad hoc sont très sensibles aux attaques. Des mesures de sécurité sont appelées à être mis en place et l'usage de l'authentification, du tatouage de

l'information et la cryptographie semblent nécessaires. Il y a même des discussions sur IP-sec qui introduit les tunnels pour le transport des paquets.

### **2.6.6 Conservation d'énergie**

Étant donné que l'énergie emmagasinée dans les batteries des nœuds mobiles est réduite et très limitée, il serait nécessaire que les protocoles proposés supportent le mode veille au niveau de chacun des nœuds.

### **2.6.7 Multi-routes**

Si chaque nœud peut stocker plusieurs routes vers la même destination, les changements fréquents de la topologie influenceront peu sur le trafic où nous trouvons moins de congestions et peu de paquets de contrôles issues des découvertes de routes.

### **2.6.8 Le support de la qualité de service**

Plusieurs modèles de qualité de service sont envisageables pour les protocoles ad hoc et beaucoup d'applications verront le succès, comme le support du trafic temps réel et la réservation de la bande passante pour la vidéo conférence à titre d'exemple. Nous avons présent une classification de protocole de routage dans les environnements mobiles, avec quelques exemples pour les protocoles de routage proactif et réactif qui ont été conçu pour les réseaux Ad hoc.

Dans notre dernier chapitre nous allons nous détailler sur le fonctionnement de ces deux protocoles OLSR et AODV qui sont les plus avancés sur la voie d'une normalisation. Nous présenterons en outre leur impacts dans le routage d'un réseau sans en mode Ad-hoc.

# **Chapitre 3 : comparaison entre des protocoles de routage des réseaux adhoc**

## **INTRODUCTION**

La majorité des recherches effectuées pour comparer les protocoles de routage des réseaux ad hoc se fondent sur des études de performance qui permettent d'évaluer, par la mise en place de simulations, des paramètres tels que, classiquement, le délai d'acheminement, le taux de perte, la bande passante, la longueur de la route suivie, le taux de paquets envoyés et la consommation d'énergie.

Notre travail entre dans le cadre de l'étude théorique du mécanisme de routage dans les réseaux mobiles Ad hoc à travers les travaux de recherche qui ont été fait , dans le but de comprendre le principe d'acheminement de données entre les hôtes mobiles du réseau ad hoc et essayer de comparer entre les protocoles réactifs et proactifs à travers leur résultats trouvés et conclusion obtenue

### **I. Métrologie et modèle utilisé**

Pour analyser les métriques de performances des protocoles de routage AODV et OLSR, on a les critères suivantes [13] :

**I.1.Selon les métriques suivantes :** Le coût de routage, Le taux de paquets délivrés ou PDR (Packet Delivery Ratio), Le délai de bout en bout, La gigue et La concentration de l'activité ; nous avons choisi les paramètres suivants :

#### **I.1.1.Modèle de trafic**

Paramètre	Valeur
Type du trafic	CBR/UDP
Nombre de connexions	10, 20, 30, 40 et 50 connexions
Taux de transmission	8 paquets/seconde
Taille des paquets	512 octets

**Table 3.1 Paramètres utilisés pour le modèle de trafic**

#### **I.1.2. Modèle de mobilité**

Paramètre	Valeur
Temps de simulation	100 seconds
Aire du réseau Ad hoc	1000m x 1000m
Nombre de nœuds	20, 40, 60, 80 et 100 nœuds
Temps de pause	0, 20, 40, 60, 80 et 100 seconds
Vitesse maximale des nœuds	20 m/s
Modèle de mobilité	Random Waypoint

Table 3.2.Paramètres utilisés pour le modèle de mobilité

### **I.1.3. Caractéristiques physiques des nœuds mobiles**

Paramètre	Valeur
Protocole MAC	IEEE 802.11
Modèle de réflexion	Two-ray ground
Portée de communication	250 m
Débit	2 Mbps
Taille max des files d'attend	50 paquets

Table 3.3.Paramètres utilisés pour la couche physique

## **I.2. Selon La consommation d'énergie [14] :**

Ils définissent le réseau ad-hoc comme une surface de 600x600 mètres, avec 20 nœuds aléatoirement dispersés dans la surface du réseau et qui se déplacent pendant une durée de 1000seconds, avec une vitesse maximum de 2m/s et un temps de pause des nœuds de 35s. Les nœuds communiquent ensemble en générant chaque seconde 4 paquet CBR de 512 bytes chaque. Pour produire un modèle de trafic et de mouvement aléatoire, ils ont utilisé des générateurs aléatoires, en indiquant simplement les attributs de vitesse, de mouvement et de trafic; le générateur du trafic est appelé cbrgen.tcl et le programme de générateur de mouvement est appelé setdest (tous les deux disponibles sous NS).

## **I.3. Selon Le taux de perte et l'énergie et La perte des paquets [15]**

### I.3.1. Le taux de perte et l'énergie:

#### Contexte de simulation

Critère	valeur
Nombre de nœuds	5
Topologie réseau	2200x950
Temps de simulation	1200s
Taille des paquets	512 octets
L'interval de transmission	0.4s
Trasmissions effectuées	Ttransmission entre 0 et 2
Type de mouvement	Aléatoire
Temps de transmission	De 0.5 jusqu'à 1150s
Le paramètre simulé	Le taux de perte
L'énergie initiale	50 J
L'énergie moyenne de transmission d'1 paque	0.8 W
L'énergie moyenne de réception d'1 paquet	0.4 W

### I.3.2 La perte des paquets sous la contrainte de mobilité (Forte et Faible):

- Contexte de simulation

Critère	valeur
Nombre de nœuds	15
Topologie réseau	1200x1200
Temps de simulation	1200s
Taille du buffer	50 paquets
Taille des paquets	512
L'interval de transmission	0.4s
Trasmissions effectuées	Transmission entre les nœuds 0 et 4
Temps de transmission	De 0.5 jusqu'à 1150s
Le paramètre simulé	la perte des paquets sous TCP et UDP



### I.3.3 La perte des paquets, sous la contrainte de densité (nombre de Nœuds par espace):

- Contexte de simulation

Critère	valeur
Nombre de nœuds	10, 50, 100, 150 nœuds
Topologie réseau	2200x950
Temps de simulation	1200s
Taille du buffer	50 paquets
Taille des paquets	512
L'interval de transmission	0.4 s
Trasmissions effectuées	Transmission entre les nœuds 0 et 2
Temps de transmission	De 0.5 jusqu'à 1150s
Le paramètre simulé	Variation du nombre des noeuds

### I.3.4.La perte des paquets, sous la contrainte d'échelle (différente Valeurs de l'espace) :

- Contexte de simulation

Critère	valeur
Nombre de nœuds	35
Topologie réseau	500x500
Temps de simulation	1200s
Taille des paquets	512 octets
L'interval de transmission	0.4s
Trasmissions effectuées	Transmission entre les nœuds 0 et 2
Type de mouvement	Aléatoire
Temps de transmission	De 0.5 jusqu'à 1150s
Le paramètre simulé	Le taux de perte selon la topologie

## Résultats et analyse

- selon : Le taux, Le délai, La gigue, La concentration de l'activité :

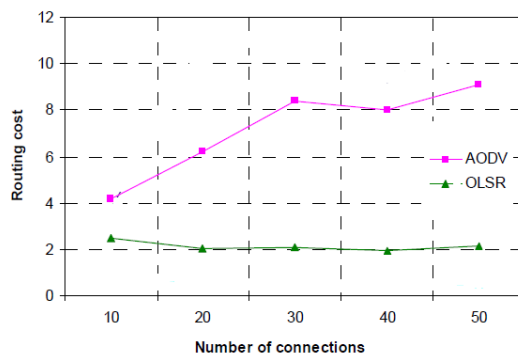


Figure 1. Coût du routage, en fonction de la charge

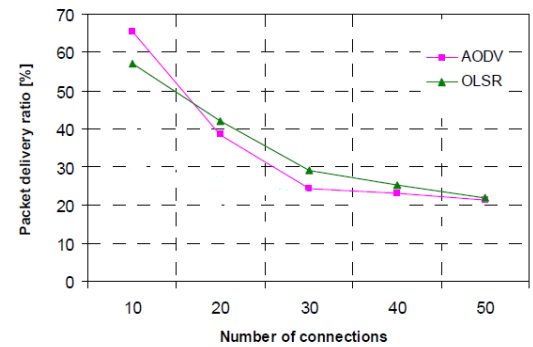


Figure 2. Taux de paquets délivrés, en fonction de la charge

- dans la figure 1 les chercheurs trouvent que le coût de routage est élevé pour AODV (classe réactive) et il s'accroît avec l'augmentation de la charge de trafic. Par contre il est stable pour OLSR (classe proactive), mais ils trouvent dans La figure 2 qui montre que le taux de paquets délivrés est influencé par l'augmentation de la charge de trafic. le plus élevé taux est celui de OLSR en particulier à partir de la charge 20 connexions.

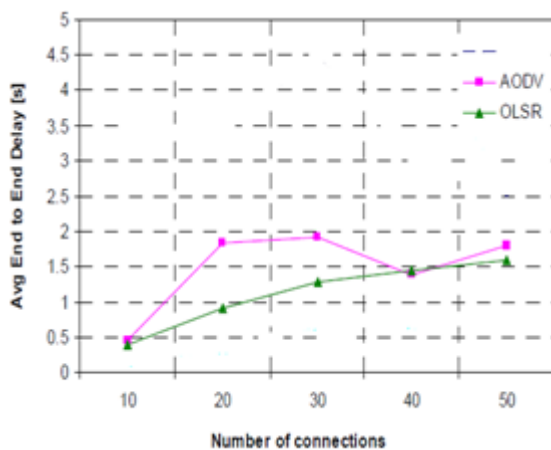


Figure 3.3 Délai, en fonction de la charge [13]

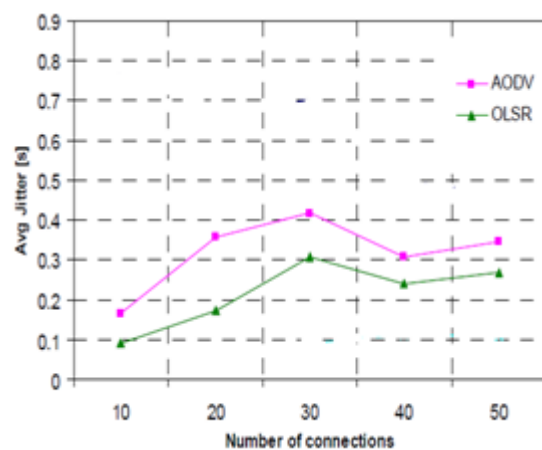
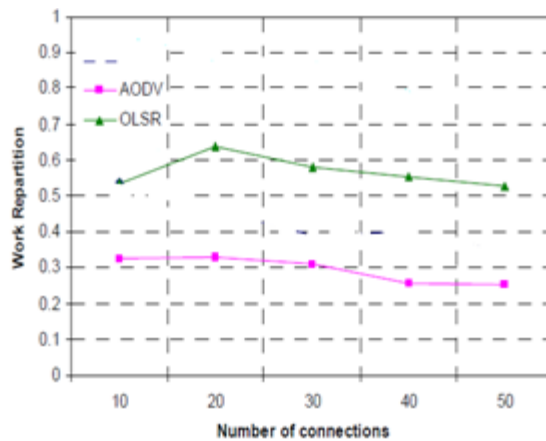


Figure 3.4 Gigue, en fonction de la charge [14]

Les chercheurs observent dans Les figures 3.3 et 3.4 qui ont montrent qu'en termes de délai et de gigue, OLSR (classe proactive) et AODV (classe réactive) sont dans l'ordre efficace. OLSR et AODV tend à augmenter lorsque la charge du trafic augmente. La nature proactive de OLSR permet à ce protocole de découvrir rapidement la route optimale et par la suite le temps de

transmission des paquets prend moins de temps par rapport au protocole réactif AODV ce qui explique des meilleures performances d'OLSR en termes de délai et de gigue.



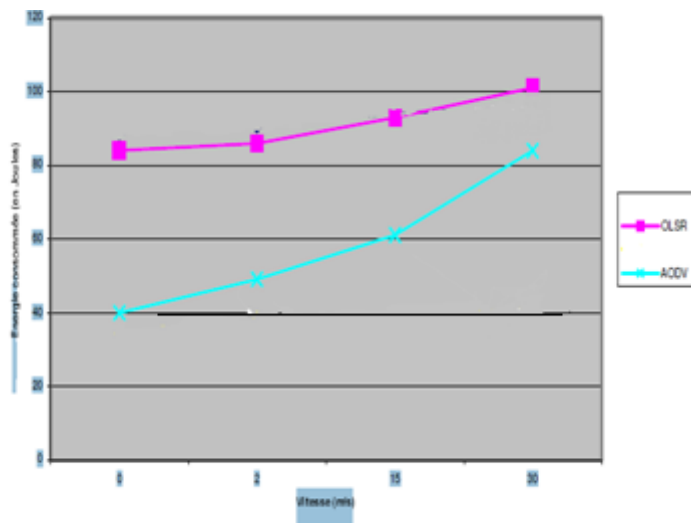
**Figure 3.5** Concentration de l'activité  
En fonction de la charge

Pour le 4ème paramètre « La concentration de l'activité », l'auteur trouve qu'elle reste cependant plus au moins stable pour la plupart des protocoles de routage, elle est moins importante pour AODV et plus importante pour OLSR.

- **Selon la consommation d'énergie**

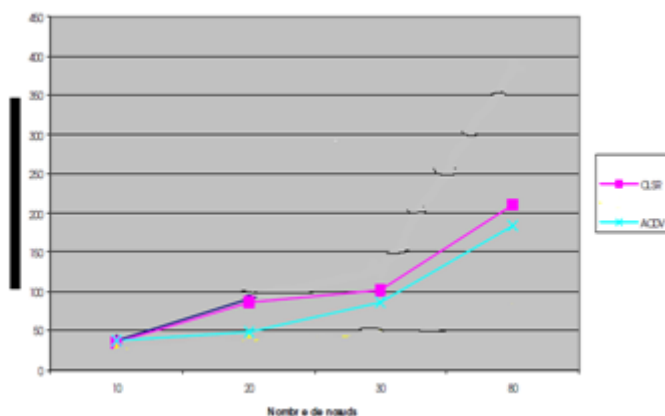
Les chercheurs trouvent que la consommation d'énergie des protocoles de routage lorsque la vitesse des nœuds change est montrée dans la figure 3.6. Ces résultats indiquent que les protocoles réactifs tels que AODV consomment moins d'énergie que les protocoles proactifs.

En effet, les protocoles réactifs ne font aucune consommation lorsqu'il n'y a aucun trafic dans le réseau, tandis que les protocoles proactifs consomment constamment de l'énergie par les calculs d'itinéraires même si aucun paquet ne sera envoyé. Les protocoles réactifs sont donc moins sensibles au déplacement des nœuds. En outre, la mise en place de nouveaux relais multipoint lorsque la Topologie du réseau change, rend OLSR (classe proactive) un peu plus consommateur que AODV (classe réactive).



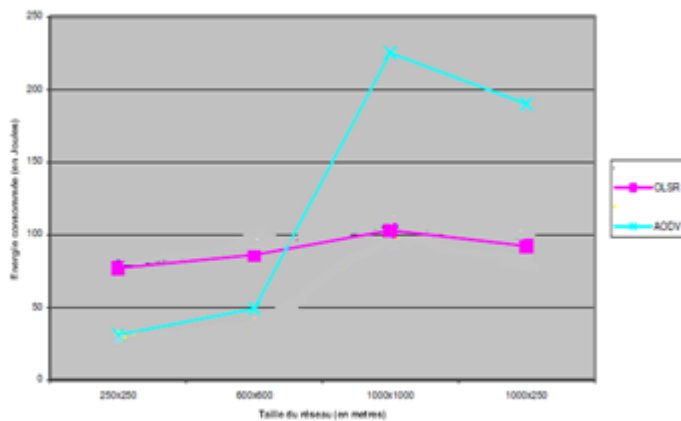
**Figure 3.6 consommation d'énergie en fonction  
De la vitesse des nœuds**

Dans la figure 3.7, les chercheurs remarquent que les protocoles réactifs surpassent encore les protocoles proactifs lorsque le nombre de nœuds se développent même si AODV est moins stable. Mais OLSR consomme beaucoup davantage et de manière irrégulière. Plus le nombre de nœuds est grand, plus les protocoles proactifs souffrent de leur mise à jour et comme OLSR réduit le nombre de diffusion aux seuls nœuds multipoints. Globalement, les protocoles Proactifs posent ici le problème de la sociabilité dans un grand réseau.



**Figure 3.7 consommation d'énergie en fonction  
Du nombre des nœuds**

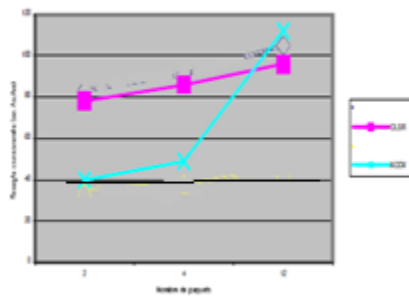
Sur la figure 3.8, la distinction entre les protocoles proactifs et réactifs disparaît lorsqu'ils ont fait varier la taille du réseau. Même si OLSR présente toujours un comportement régulier, AODV ne consomme davantage que les deux autres protocoles proactifs. En fait, les nœuds étant plus espacés le routage est plus important.



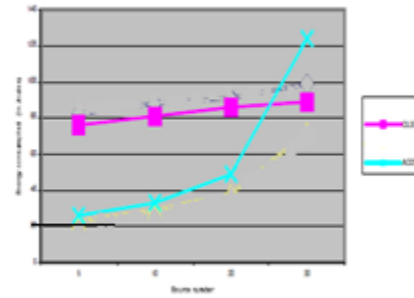
**Figure 3.8 consommation d'énergie en fonction de la taille du réseau**

Finalement, les schémas 3.9 et 3.10 montrent un comportement similaire des protocoles de routage puisque les paramètres qu'ils font varier concernent le trafic et que les résultats obtenus sont semblables. À mesure que le trafic augmente, OLSR (classe proactive) voient leur énergie décroître de manière régulière, avec un net avantage. Ils rentabilisent en quelque sorte le travail de leur mise en place de la table de routage puisque les découvertes de routes ont déjà été faites de manière globale.

Le même problème apparaît avec AODV (classe réactive) puisque AODV montre aussi ses faiblesses lorsque le trafic croît et de manière encore plus flagrante. En fait, sanctionné pour deux de ces caractéristiques : les messages «hello », périodiquement envoyer aux voisins actifs dans les communications ainsi que les redécouvertes de route forcées par un temporisateur qui permet de purger les entrées de la table.



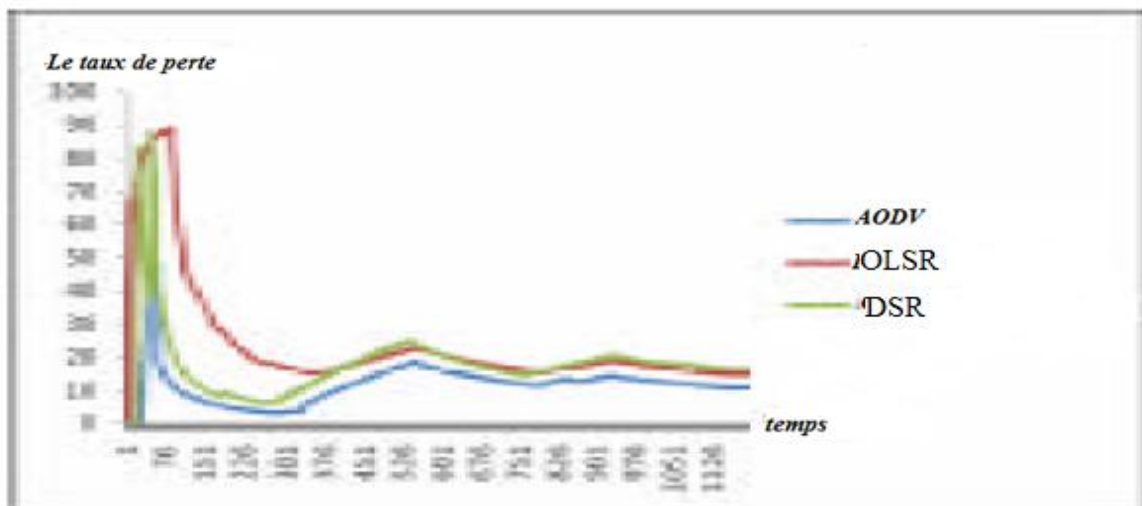
**Figure 3.9** Consommation d'énergie  
En fonction du nombre de paquets



**Figure 3.10** Consommation d'énergie  
en fonction du nombre de sources

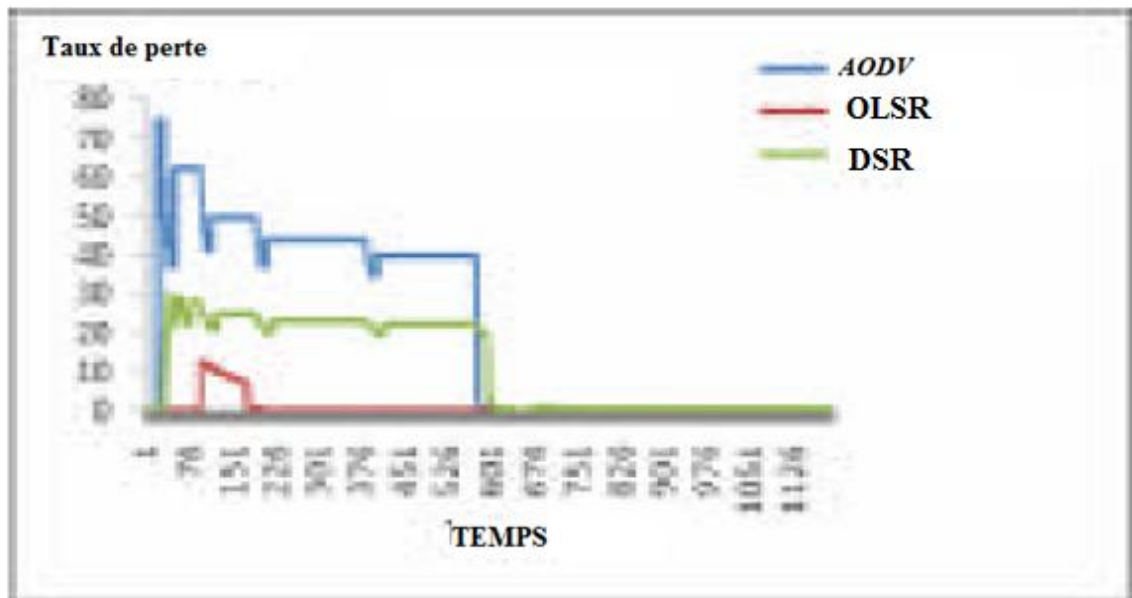
- Selon le taux de perte et l'énergie et la perte des paquets

**Scénarios 1 :** Une énergie initiale de 50 j avec l'énergie de transmission supérieure à celle de la réception



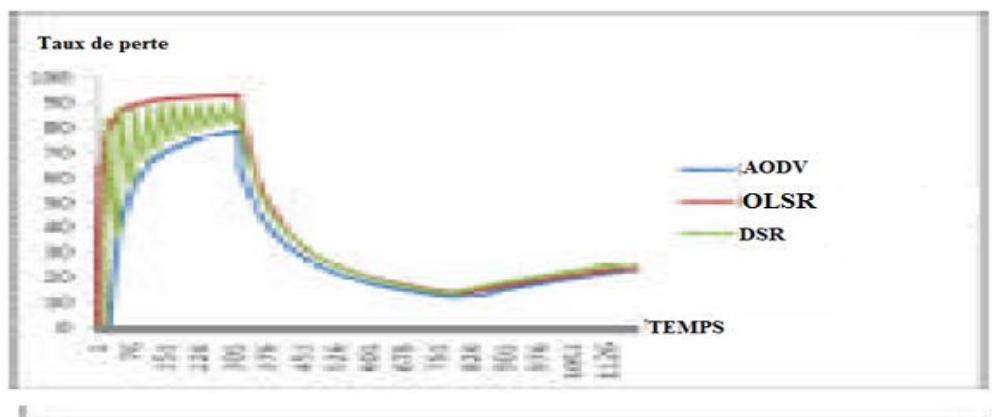
	Transmis	Perdus	Taux
OLSR	9867	2551	25,85 %
AODV	4291	2251	59,45 %
DSR	6805	1786	26,24 %

- **Scénarios 2 :** La forte mobilité



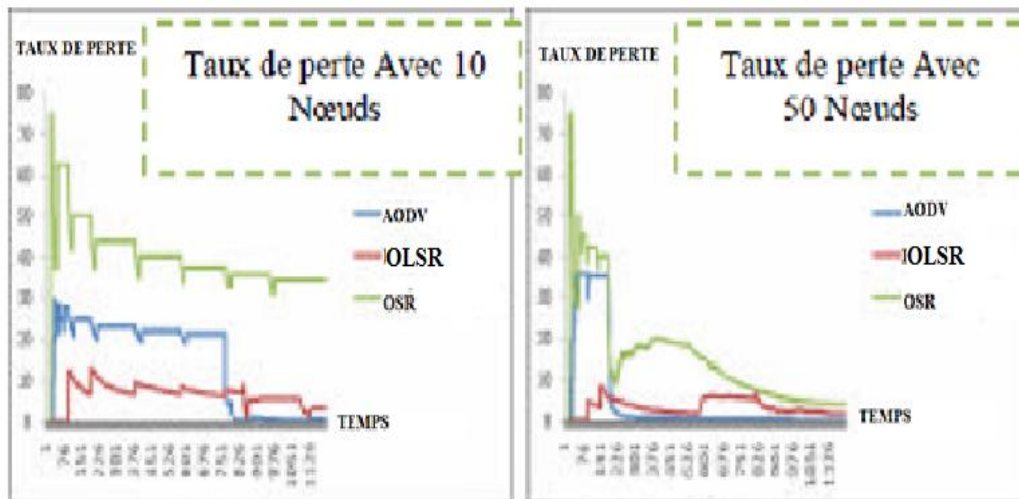
	Transmis	Perdus	Taux de perte
OLSR	10800	1599	14,8%
AODV	8185	1325	16,1%
DSR	9564	1042	10,8%

### Scénarios 3 : La faible mobilité

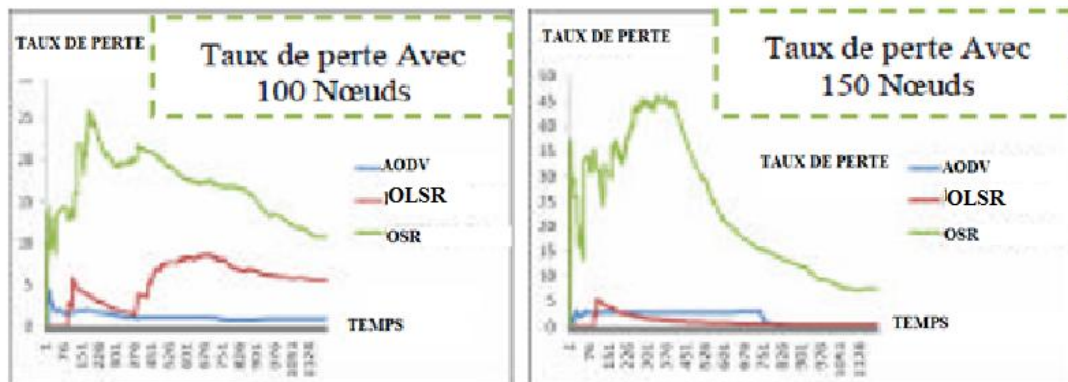


	Transmis	Perdus	Taux
OLSR	10483	1177	11.22%
AODV	9244	830	8.97%
DSR	9767	715	7.32%

- **Scénarios 4 :** Cas de TCP avec 10, 50, 100 et 150 nœuds



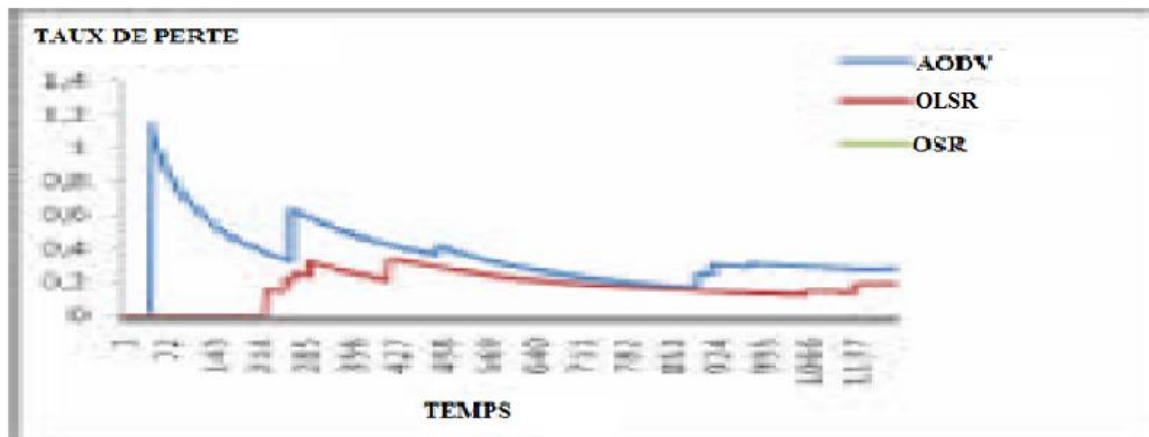
Taux de perte avec 10 nœuds				Taux de perte avec 50 nœuds		
	Transmis	Perdus	Taux	Transmis	Perdus	Taux
OLSR	2700	85	34,3%	14538	223	1,5%
AODV	32	11	3,1%	34691	1395	4,0%
DSR	19057	98	0,5%	23772	24	0,10%



Taux de perte avec 100 nœuds				Taux de perte avec 150 nœuds		
	Transmis	Perdus	Taux	Transmis	Perdus	Taux
OLSR	5449	302	5,5%	1063	3	0,28%
AODV	17983	1947	10,8%	34389	2522	7,3%
DSR	7670	60	0,7%	28172	24	0,08%

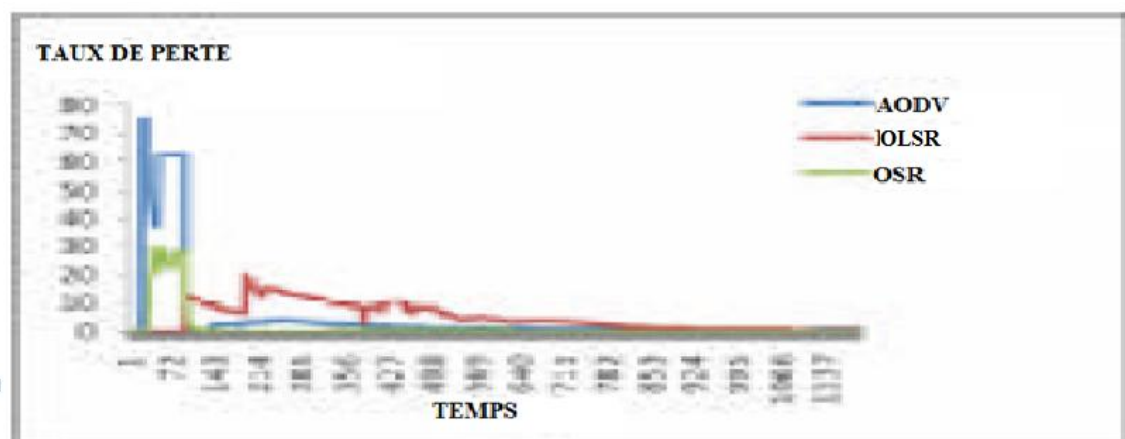
- **Scénarios 6 :** Une échelle de 500x500





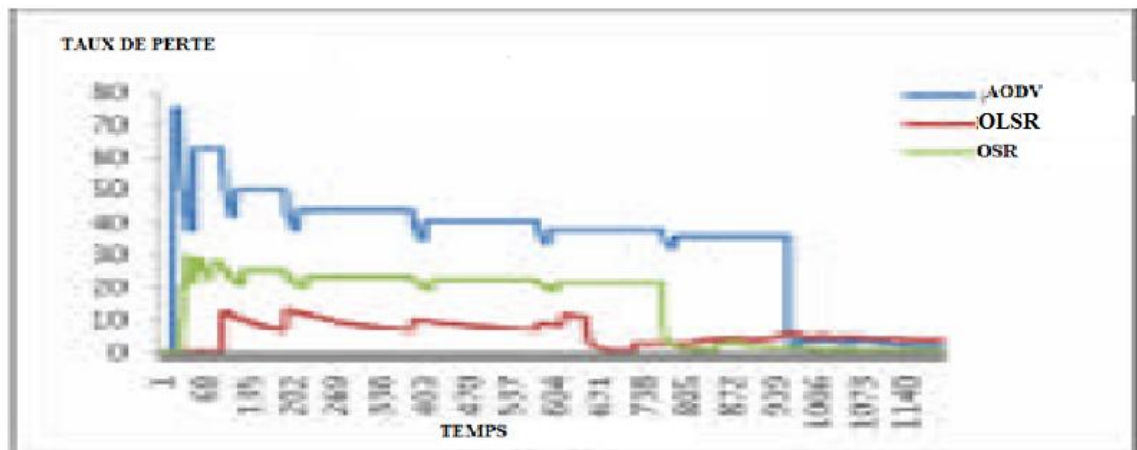
	Transmis	Perdus	Taux
OLSR	11536	6	0,05 %
AODV	11949	54	0,45 %
DSR	11570	0	0 %

- **Scénarios 7** : Une échelle de 1500x1500



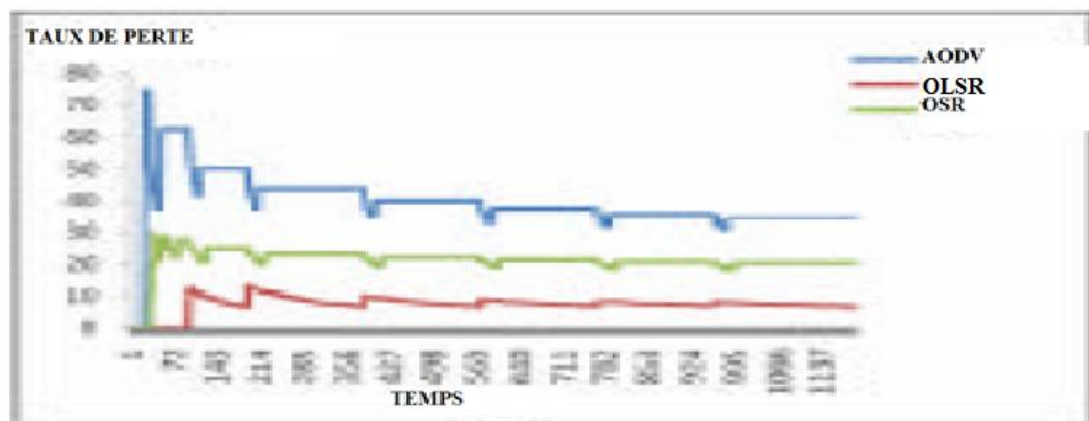
	Transmis	Perdus	Taux
OLSR	10219	510	4,99 %
AODV	11582	266	2,29 %
DSR	11879	139	1,17 %

- **Scénarios 8** : Une échelle de 3000x3000



	Transmis	Perdus	Taux
OLSR	7304	1535	21,01 %
AODV	7002	1925	27,49 %
DSR	8751	989	11,30 %

- **Scénarios 9 :** Une échelle de 6000x6000



	Transmis	Perdus	Taux
OLSR	3191	2857	89,53 %
AODV	3045	2858	93,85 %
DSR	3335	2844	85,27 %

**INTERPRETATION DES RESULTATS:**

- **Energie** : En générale la consommation d'énergie est proportionnelle au nombre de paquets traités et au type du traitement effectué (émission/réception) il est a noté que l'émission d'un paquet demande plus d'énergie que la Réception. La quantité d'énergie consommée est moyenne pour OLSR (classe proactive) et importante pour l'AODV (classe réactive).

- **Mobilité** : Pour une forte mobilité et en tenant compte des valeurs du tableau récapitulatif, on constate que le protocole DSR (classe réactive) minimise au maximum la perte des Paquets puis c'est le protocole OLSR (classe proactive) Et enfin le protocole AODV (classe réactive) reste le moins performant, et la perte des paquets est importante. AODV est loin d'être comparer à DSR Ou OLSR, peut être par ce qu'il supporte moins la mobilité que les deux autres. Pour une faible mobilité, DSR donne toujours de meilleurs résultats en termes de perte de paquets par rapport à AODV et OLSR comme protocole de transport. En conclusion et en toutes circonstances, on constate que le protocole DSR est celui qui minimise beaucoup plus la perte des paquets qu'OLSR et AODV, alors on peut dire que les protocoles réactive sont donne des meilleurs résultats en termes de perte de paquets par rapport à les protocoles proactifs.

- **Nombre de nœuds (densité)** : un taux de perte plus élevé en implémentant un routage OLSR (classe proactive) ou AODV (classe réactive), et moins élevé avec DSR (classe réactive). On conclut que dans de telles conditions, c'est DSR qui donne de bons résultats suivi d'OLSR et l'AODV .alors dans ce cas on peut dire que les protocoles réactive sont donne des meilleurs résultats en termes de densité par rapport à le protocole proactives.

- **Échelle** : On ne constate que le protocole DSR (classe réactive). Reste le plus performant en toutes circonstances. Par contre le protocole OLSR (classe proactive). Perd ces performances devant L'AODV (classe réactive).pour une échelle moyenne. Il y'a une sorte de rivalité entre OLSR et AODV, l'un est plus performant que l'autre dans une situation donnée. Mais pour déterminer le bon protocole à implémenter, cela dépend du réseau à mettre en œuvre. Alors on peut dire que les protocoles réactive sont donne des meilleurs résultats en termes de petites valeurs de l'espace par rapport à le protocole proactives

## Conclusion

Après avoir étudié les résultats obtenus, nous avons constaté que tous les tests effectués par les chercheurs de comparer les protocoles de recherche proactif et réactif, nous constatons qu'il n'y a pas un protocole qui est favori par rapport aux autres dans tous les scénarios et les critères d'évaluation. Quelque soit la charge du réseau, la mobilité des nœuds et la densité.

Notre projet repose principalement sur l'étude théorique des plusieurs recherches menées par des chercheurs dans ce domaine, on comparant les résultats obtenus pour aider l'utilisateur à choisir le bon type de protocole. Dans le réseau Ad hoc.

, OLSR (classe proactive).et AODV(classe réactive)., bien que de nature très différentes, sont très similaires en termes de performances. Dans un réseau très mobile, avec de fréquent changement de topologie, AODV a un petit avantage sur OLSR car les routes sont mises à jours plus rapidement. OLSR doit attendre plusieurs paquets Hello perdus avant de modifier l'état du lien et envoyer des informations de mise à jour. Par contre, dans un réseau plus statique, OLSR encombre moins le réseau qu'AODV qui émet beaucoup plus de messages à chaque découverte de route. En effet dans ce cas OLSR n'émet presque pas de message de mises à jour de la topologie.

Dans un réseau très dense, OLSR charge moins le réseau qu'AODV. Dans des réseaux moyens, OLSR et AODV sont équivalent. Lors de communications courtes, OLSR à un énorme avantages sur AODV car les routes sont disponible immédiatement. Dans la plupart des cas, les messages de contrôles d'AODV sont légèrement plus nombreux que ceux d'OLSR. AODV émet d'autant plus de paquets que le réseau est grand.

Enfin, toutes les recherches effectuées indiquent que le choix de l'algorithme de routage dépend de plusieurs contraintes, et la comparaison entre les protocoles de routage réactives et proactives dépend aussi a ces contraintes

## RÉFÉRENCES

- [1] Daniel L. Lough, T. Keith Blankenship, Kevin J. Krizman. "A Short Tutorial on Wireless LANs and IEEE 802.11". Summer 1997.
- [2] <http://www.ietf.org/>
- [3] [http://www.ee.surrey.ac.uk/Personal/G.Aggelou/MANET\\_PUBLICATIONS.htm](http://www.ee.surrey.ac.uk/Personal/G.Aggelou/MANET_PUBLICATIONS.htm)
- [4] Charles E. Perkins, Elizabeth M. Royer, Samir R. Das. "Ad hoc On-Demand Distance Vector (AODV) Routing". Internet Draft, 2 March 2001
- [5] David B. Johnson, David A. Maltz, Yih-Chun Hu, Jorjeta G. Jetcheva. "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks". Internet Draft, 2 March 2001.
- [6] V. Park, S. Corson. "Temporally-Ordered Routing Algorithm (TORA) Version 1". Internet Draft, 20 July 2001
- [7] Charles Perkins, Pravin Bhagwat. "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers ". 1994
- [8] <http://www.isi.edu/nsnam/ns/>
- [9] Charles E. Perkins, Elizabeth M. Belding-Royer, et Samir Das. "Ad hoc On-Demand Distance Vector (AODV) Routing". Internet Request For Comments RFC 3561, Internet Engineering Task Force, Juillet 2003.
- [10] Eddy Cizeron, "Routage Multichemins et Codage à Description Multiple dans les Réseaux Ad Hoc" , Thèse de Doctorat de l'Université de Nantes, septembre 2009
- [11] Abdelali Boushaba, Mohammed Oumsis "Rachid Benabbou3Evaluation des performances des protocoles de routage Ad hoc"
- [12] laurent ouakil DEA Reseaux \_ lip6.septembre 2002  
laurent.oaukil@rp.lip6.fr

[13] Abdelali Boushaba<sup>1</sup>, Mohammed Oumsis<sup>2</sup>, Rachid Benabbou<sup>3</sup>  
Laboratoire LISQ, Département de Mathématiques et Informatique, Faculté des  
Sciences Dhar Mahraz  
Fès, Maroc

[14] laurent ouakil. Dea reseaux\_lip6.septembre 2002.  
[laurent.ouakil@rp.lip6.fr](mailto:laurent.ouakil@rp.lip6.fr)

[15] Sedrati Maamar, Aouragh Lamia, Guettala Leila, Bilami Azeddine  
Département d'informatique, Faculté des sciences de l'ingénieur, Université El  
Hadj Lakhdar - Batna.