

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
UNIVERSITE ABOU BEKR BELKAID TLEMEN
FACULTE DE TECHNOLOGIE

DEPARTEMENT DE TELECOMMUNICATIONS



MEMOIRE

Pour l'obtention du diplôme de
MASTER en

Réseaux mobiles et services de télécommunications

Réalisé par

Mlle. ABDERRAHIM Radjae
Mlle. ABDELLI Amel

THEME

Simulation d'un réseau MANET avec OPNET

Soutenu en 24 Mai 2015 devant le Jury :

Mr. ZERROUKI Hadj

M.C.B à l'Université de Tlemcen

Président

Mr. MERZOUGUI Rachid

M.C.A à l'Université de Tlemcen

Examineur

Mr. HADJILA Mourad

M.C.B à l'Université de Tlemcen

Encadreur

Mlle. SOUIKI Sihem

Doctorante à l'Université de Tlemcen

Co-encadreur

Année universitaire : 2014-2015



Remerciements

Avant tout on tient nos remerciements à notre dieu tout puissant de nous avoir donné la foi, la force et le courage.

*A travers ce modeste travail, nous tenons à remercier vivement notre encadreur « **Mr. HADJILA MOURAD** » qui a toujours été disponible malgré ses nombreuses occupations, et dont les encouragements et les conseils judicieux nous furent d'une très grande utilité.*

*Nos remerciements les plus vifs s'adressent aussi au monsieur le président « **Mr. ZERROUKI HADJ** » et l'examineur de jury « **Mr. MERZOUGUI RACHID** » d'avoir accepté d'évaluer notre travail.*

Nous exprimons également notre gratitude à tous les professeurs et enseignants qui ont collaboré à notre formation depuis notre premier cycle d'étude jusqu'à la fin de notre cycle universitaire.



Dédicaces

*Je tiens à remercier Dieu qui m'a donné la santé,
la possibilité ainsi que la volonté d'entamer
et de continuer mes études.*

*Je dédie ce modeste travail à:
A mes très chères parents qui ont beaucoup sacrifiés
pour me faire réussir et pour leur patience et encouragement.*

*A mes Très chères sœurs
et mes très chers frères.
A mon fiancé*

*A toute La famille 'ABDERRAHIM'
A ma copine 'AMEL'*

ABDERRAHIM Radjaa



Dédicaces

*Je rends grâce à dieu de m'avoir donné le courage et la volonté
ainsi que la conscience d'avoir pu terminer mes études.*

J'ai l'immense honneur de dédier ce mémoire :

*A mes très chers parents qui étaient présents pour moi
durant toute ma vie.*

*Je dédie ce travail aussi à mes très
chers frères : RAFIK & ABDELKADER sans oublier ma très
chère sœur IKRAM*

A ma copine RADJAA

A tous ceux qui me sont chères.

ABDELLI Amel



Table des matières

Glossaire.....	1
Introduction générale.....	3

Chapitre I : Généralités sur les réseaux *Ad hoc*

I.1 . Introduction.....	5
I.2. Définition des différents types de réseaux.....	5
I.2.1. Réseaux statiques.....	5
I.2.2. Réseaux <i>Ad hoc</i>	5
I.2.3. Réseaux <i>MANETs (Mobile Ad hoc Networks)</i>	6
I.3. Caractéristiques des réseaux <i>Ad hoc</i>.....	7
I.4. Atouts des réseaux <i>Ad hoc</i>	8
I.5. Inconvénients des réseaux <i>Ad hoc</i>	9
I.6. Applications des réseaux <i>Ad hoc</i>.....	10
I.6.1. Application militaire	11
I.6.2. Réseaux d'urgence	11
I.6.3. Réseaux de capteurs.....	12
I.6.4. Extension de réseaux dotés d'infrastructure	12
I.6.5. Applications commerciales.....	12
I.6.6. Autres applications	12
I.7. Modes de communication dans les réseaux mobile	12
I.7.1. Mode unicast	12
I.7.2. Mode multicast	13
I.7.3. Mode diffusion	13
I.8. Normes utilisés pour les réseaux <i>Ad hoc</i>	14
I.9. Conclusion.....	15

Chapitre II : Protocoles de routages dans les réseaux *Ad hoc*.

II.1. Introduction.....	17
II.2. Routage dans les réseaux <i>Ad hoc</i>	17
II.3. Contraintes du routage dans les réseaux <i>Ad hoc</i>	18
II.4. Différentes approches mises en œuvre	19
II.4.1. Protocoles proactifs.....	20
II.4.1.1. Protocole « <i>DSDV</i> ».....	20
II.4.1.2. Protocole « <i>OLSR</i> »	21

II.4.2. Protocoles réactifs.....	22
II.4.2.1. Protocole « DSR ».....	22
II.4.2.2. Protocole « AODV ».....	23
II.4.3. Protocoles hybrides.....	25
II.5. Comparaison entre les protocoles proactifs et réactifs.....	25
II.5.1. Spécificités <i>OLSR / AODV</i>	26
II.5.2. Synthèse de comparaison <i>OLSR / AODV</i>	26
II.6. Conclusion	26

Chapitre III : Simulation des différentes modèles.

III.1. Objectifs de projet.....	28
III.2. Modèles de tests et configuration de réseaux.....	28
III.3. Présentation du simulateur <i>OPNET (Optimum Network Performance)</i>	29
III.3.1. Installation du simulateur <i>OPNET</i>	30
III.3.2. Structure d' <i>OPNET</i>	32
III.3.3. Simulation sous <i>OPNET</i>	32
III.3.4. Ses avantages	32
III.3.5. Son inconvénient	33
III.4. Modèles de simulation <i>OPNET</i>.....	33
III.4.1. Modèle de Mobilité.....	33
III.4.2. Modèle de puissance de communication	34
III.4.3. Modèle de performances de routage <i>MANET</i>	35
III.5. Métriques de performance	36
III.6. Conclusion	38

Chapitre IV : Résultats et analyses.

IV.1 Introduction.....	39
IV.2 Résultats et discussions	39
IV.2.1. Modèle 1	39
IV.2.2. Modèle 2	42
IV.2.3. Modèle 3	43
IV.3. Conclusion	48

Conclusion générale.....	49
Perspectives.....	51
Références & Bibliographie.....	52

Liste des figures

Figure I.1. Exemple d'un réseau <i>Ad hoc</i>	6
Figure I.2. Quelques domaines d'application pour les réseaux <i>Ad hoc</i>	11
Figure I.3. Mode <i>Unicast</i>	13
Figure I.4. Mode <i>Multicast</i>	13
Figure I.5. Mode <i>Broadcast</i>	13
Figure II.1. Exemple d'un routage direct	18
Figure II.2. Taxonomie des protocoles de routages des réseaux <i>Ad hoc</i>	20
Figure II.3. Multipoints relais	21
Figure II.4. Etablissement d'une route sous <i>AODV</i>	24
Figure III.1. Lancement du simulateur <i>OPNET</i>	29
Figure III.2. Fichier pour mettre la licence	30
Figure III.3. Fenêtres d'installation de compilateur <i>C++</i>	31
Figure III.4. Message de la simulation complète	31
Figure III.5. Réseau <i>Ad hoc</i> simulé dans <i>OPNET</i>	33
Figure III.6. Animation du réseau <i>Ad hoc</i> simulé.....	34
Figure III.7. Réseau <i>Ad hoc</i> composé de 16 nœuds simulé dans <i>OPNET</i>	35
Figure III.8. Animation du réseau <i>Ad hoc</i> simulé	36
Figure IV.1. Trafic reçu par la destination	39
Figure IV.2. Trafic envoyé par la source.....	40
Figure IV.3. Métriques d'évaluation	40
Figure IV.4. Trafic envoyé des données et la charge	41
Figure IV.5. Variation de la puissance en fonction de la distance	42
Figure IV.6. Temps de découvert de la route pour <i>AODV</i> et <i>OLSR</i>	43
Figure IV.7. Acheminement du trafic reçu pour <i>AODV</i> et <i>OLSR</i>	44
Figure IV.8. Acheminement du trafic envoyé pour <i>AODV</i> et <i>OLSR</i>	44
Figure IV.9. Paquets de demande de route pour <i>AODV</i> et <i>OLSR</i>	45
Figure IV.10. Paquets de réponse de route pour <i>AODV</i> et <i>OLSR</i>	46
Figure IV.11. Paquets perdus pour <i>AODV</i> et <i>OLSR</i>	47

Liste des tableaux

Tableau II.1. Comparaison entre les protocoles proactifs et réactifs.....	25
Tableau II.2. Spécificités <i>OLSR / AODV</i>	26
Tableau III.1. Paramètres de générateur de trafic.....	34
Tableau III.2. Paramètres de puissances.....	35
Tableau III.3. Paramètres de générateur de trafic <i>MANET</i>	35
Tableau IV.1. Variation de la puissance en fonction de la distance	42

Glossaire

Glossaire

A

AODV: Ad Hoc **O**n-Demand **D**istance **V**ector.

D

DSDV: Destination **S**equence **D**istance **V**ector.

DSR: Routage à **S**ource **D**ynamique.

I

IDE: Integrated **D**evelopment **E**nvironment.

IEEE: Institute of **E**lectrical and **E**lectronics **E**ngineers.

IETF: Internet **E**ngineering **T**ask **F**orce.

IP: Internet **P**rotocol.

L

LAN: Local **A**rea **N**etwork.

M

MAC: Media **A**ccess **C**ontrol.

MANET: **M**obile **A**d hoc **N**ETwork.

MPR: **M**ulti**P**oint **R**elaying.

O

OLSR: Optimized **L**ink **S**tate **R**outing.

OPNET: Optimum **N**etwork **P**erformance.

R

RREP: Route **RE**ply.

RREQ: Route **RE**quest.

S

SN: Sequence Number.

W

WAN: Wide Area Network.

Web ASP.NET: Website Active Server Pages for **NET**work.

Web XML: Website *Extensible Markup Language*.

Wi-Fi: Wireless Fidelity.

WLAN: Wireless Local Area Network.

Introduction générale

Introduction Générale

On assiste ces dernières années à une importante évolution dans la société de l'information, conduite par la commercialisation et l'émergence des appareils de communications (tels que les téléphones cellulaires, les ordinateurs portables, les assistants personnels, etc.) et la convergence des réseaux fixes et mobiles. L'utilisateur passe ainsi de l'âge de l'ordinateur personnel à l'âge de l'ubiquité du traitement à travers plusieurs infrastructures. Il a accès à l'information n'importe où et n'importe quand.

Un utilisateur mobile peut consulter son courrier électronique, navigué sur Internet dans les aéroports, les gares ou dans d'autres lieux publics. Dans une conférence, les chercheurs peuvent transférer des fichiers et d'autres types d'information grâce à leurs appareils électroniques via des réseaux locaux sans fil; dans sa maison, une personne peut synchroniser des données et échanger des fichiers entre différents terminaux.

Les technologies de l'information n'ont jamais cessé d'améliorer le quotidien de l'homme. L'un de leurs plus grand succès est le pouvoir de communication. Un pouvoir obtenu grâce au concept de réseau. Le terme réseau, en informatique, désigne un ensemble de machines (appelées aussi nœuds) et de moyens matériels et logiciels leur permettant de communiquer.

Un réseau est dit sans fils si la communication entre ses composants se fait via un medium sans fils (onde radio ou infrarouge). Il existe deux catégories de réseaux sans fil : réseau avec infrastructure et réseaux sans infrastructure. La première catégorie se base sur une infrastructure fixe qui coordonne et assure la communication entre les différents mobiles. La deuxième catégorie ne repose sur aucune infrastructure et elle s'auto-organise.

Dans ce travail, nous nous intéressons au deuxième type de réseaux et particulièrement à ceux appelés réseaux sans fils "Ad hoc". Ces réseaux représentent littéralement des réseaux prêts à l'emploi. C'est une collection de nœuds souvent mobiles dans laquelle chaque nœud joue le rôle de source, destinataire et routeur. C'est au début des années 1970 que ces

réseaux font leur apparition dans le domaine militaire. Ce n'est que vers la fin des années 1990, avec l'arrivée des technologies radio bon marché (principalement *IEEE 802.11*), que ce domaine s'est révélé et a pris son essor dans le monde civil. Depuis, un très grand enthousiasme s'est créé autour de ces réseaux.

L'immense intérêt porté par la communauté de recherche à ces réseaux, se justifie par l'avenir glorieux et le succès auquel ces réseaux sont promis. En effet, plusieurs domaines d'applications leurs sont déjà favorables (allant du domaine militaire, cas d'urgence ou de catastrophe naturelle ou à un simple partage d'Internet dans une maison, ...). Leurs plus gros avantages reviennent à leur facilité, simplicité et rapidité de déploiement ainsi qu'à leur coût faible, mais aussi et surtout à leur autonomie et mobilité. Une autonomie est possible grâce à des batteries de durée de vie limitée. Cette durée de vie limitée influence considérablement la survie du réseau. Aujourd'hui encore, pour pouvoir profiter pleinement de ces réseaux, il faut résoudre un certain nombre de problèmes (qualité de service, sécurité, énergie, ...).

Notre travail entre dans le cadre de l'étude du problème de routage dans les réseaux mobiles Ad hoc (*MANET*). 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 est organisé comme suit : le premier chapitre est consacré aux réseaux *Ad hoc* de façon générale. Le deuxième chapitre abordera le fonctionnement des différents protocoles de routage dans les réseaux *Ad hoc*. C'est dans le troisième chapitre que nous décrirons les différents scénarios à simuler en mettant l'accent sur le principe de fonctionnement d'*OPNET (Optimum Network Performance)*. Enfin, les analyses des résultats couvrent le quatrième chapitre qui est prend fin par des conclusions et perspectives.



Chapitre I
Généralités sur les réseaux Ad hoc.

I.1. Introduction

Les environnements mobiles offrent aujourd'hui une grande flexibilité d'emploi. En particulier, ils permettent la mise en réseau des sites dont le câblage serait trop onéreux à réaliser dans leur totalité, voire même impossible.

Dans ce chapitre, nous présentons les caractéristiques des réseaux statiques, des réseaux *Ad hoc* et des *MANETs* ainsi que les problématiques spécifiques associées. Nous définissons la notion de service dans les réseaux *MANETs* et nous présentons un aperçu des solutions aux problèmes classiques.

I.2. Définition des différents types de réseaux

Un réseau est un ensemble de terminaux interconnectés par un moyen de communication. Selon leur méthode de constitution et d'administration, on distingue les réseaux statiques, les réseaux *Ad hoc* et les *MANETs* (*Mobile Ad hoc Networks*).

I.2.1. Les réseaux statiques

Les réseaux statiques [1] sont des réseaux qui ont vocation à être utilisés par des groupes humains dont la composition est connue à l'avance et évolue relativement peu rapidement, comme par exemple les collaborateurs d'une entreprise ou les membres d'un laboratoire de recherche. Ces réseaux, le plus souvent filaires, sont mis en œuvre grâce au matériel permettant de créer une infrastructure, comme des commutateurs, des routeurs ou dans certains cas des points d'accès sans fil. Les terminaux sont le plus souvent des postes fixes mais peuvent aussi être des postes nomades ayant accès à un relais sans fil. Les services fournis aux membres de ces réseaux sont le plus souvent localisés sur des serveurs qui connaissent *a priori* chacun des utilisateurs et leur apportent ainsi des services spécifiques : accès à un système de fichiers, serveur de courrier électronique, etc.

I.2.2. Les réseaux *Ad hoc*

Les réseaux *Ad hoc* [2] sont des réseaux souvent temporaires constitués le plus souvent lors d'un rassemblement, par exemple une conférence. Ils utilisent la plupart du temps une infrastructure proche de celle fournie par un réseau statique et à laquelle les terminaux

accèdent via des points d'accès sans fil. Ils peuvent aussi se former, et c'est en cela qu'ils se différencient, sans aucune infrastructure, en utilisant uniquement des connexions reliant les terminaux entre eux. Une fois constitué, un réseau *Ad hoc* a une composition relativement stable qui peut être conservée durant toute la durée de l'événement pour lequel il a été créé.

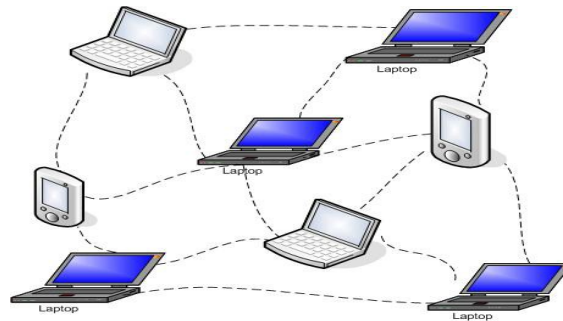


Figure I.1. Exemple d'un réseau Ad hoc.

En configuration *Ad hoc*, les services sont portés par les terminaux qui le constituent et permettent par exemple de partager des données qui ne sont portées que par un seul d'entre eux. Les périphériques utilisés sont le plus souvent des ordinateurs portables ou des assistants personnels équipés d'une connexion sans fil *WiFi* ou *Bluetooth*. La constitution et l'évolution des réseaux Ad hoc que nous définissons ici sont très proches de ce que l'on trouve avec les logiciels d'échange *peer-to-peer* (comme *Gnutella* [3]).

1.2.3. Les réseaux MANETs (*Mobile Ad hoc Networks*)

Les *MANETs* [4] sont le type de réseau le plus instable. Ils ne comportent pas d'infrastructure et les terminaux peuvent apparaître ou disparaître à tout moment suivant leurs capacités à communiquer ou leurs intérêts applicatifs ; ces changements peuvent donc être choisis ou subis. Par exemple, un réseau *MANET* peut-être constitué par les personnes à l'intérieur d'un commerce à un instant donné. Les terminaux utilisés sont très hétérogènes : ordinateurs portables, assistants personnels, téléphones ou même capteurs. Les services spécifiques aux réseaux *MANETs* ne peuvent pas reposer sur la supposition de la présence d'un terminal à un instant donné. L'accès à un service peut donc être discontinu, voire éphémère.

I.3. Caractéristiques des réseaux *Ad hoc*

On peut dégager six grandes caractéristiques :

➤ **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.

➤ **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.

➤ **Faible capacité en énergie**

Une partie des nœuds d'un réseau mobile *Ad hoc*, voire l'ensemble des nœuds, peut reposer sur des batteries ou un autre moyen limité pour épuiser leur énergie. Pour ces nœuds, le plus important est sans doute de mettre en place des critères d'optimisation pour la conservation d'énergie.

➤ **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.

➤ **Sécurité physique limitée**

Les réseaux mobiles *Ad hoc* sont plus touchés par le paramètre de sécurité, que les réseaux filaires classiques. Pour les réseaux *Ad hoc*, le principal problème ne se situe pas tant au niveau du support physique mais principalement dans le fait que tous les nœuds sont équivalents et potentiellement nécessaires au fonctionnement du réseau.

➤ **Les interférences**

Il y a de nombreuses interférences entre les hôtes du réseau. Elles accroissent le nombre d'erreurs sur la transmission et imposent un amoindrissement des performances.

I.4. Atouts des réseaux Ad hoc

Les réseaux Ad hoc offrent plusieurs avantages qui rendent leur utilisation, dans certains cas, indispensable voire préférable à tout autre type de réseaux (filaire ou mobile avec infrastructure), Ces principaux avantages sont :

➤ **La flexibilité**

La possibilité de travailler là où l'utilisateur le désire, là où il doit être, là où se trouve son travail.

➤ **Facilité et rapidité de construction**

Le déploiement d'un réseau *Ad hoc* ne requiert aucun câblage, ni présence d'une quelconque infrastructure. En effet, pour construire un réseau *Ad hoc*, il suffit de mettre des terminaux équipés de la technologie adéquate les uns à la portée d'émission des autres [5].

➤ **Réduction des coûts**

Les seules dépenses, dans ce genre de réseaux, sont pour l'achat des équipements le composant, dont le prix ne cesse de décroître.

➤ **Mobilité**

L'absence de câble apporte une certaine liberté de déplacement aux nœuds du réseau (éviter de sortir hors de la portée d'émission du réseau).

➤ **Evolutivité**

L'ajout (respectivement le retrait) d'un nœud à un réseau *Ad hoc* se fait en le rapprochant d'au moins l'un des nœuds du réseau (respectivement en l'éloignant de tout le réseau). Cet atout peut être perçu comme un inconvénient, en effet il peut poser des problèmes de sécurité, d'identification et d'adressage [6].

I.5. Inconvénients des réseaux Ad hoc

Parmi les inconvénients des réseaux *Ad hoc* qui existent :

➤ **Fiabilité**

La communication sans fil est moins fiable que la communication des réseaux filaires. La propagation du signal subit des perturbations (erreurs de transfert, microcoupures, timeout) dues à l'environnement, qui altère l'information transférée.

Il s'ensuit alors, un accroissement du délai de transit du message à cause de l'augmentation du nombre de retransmissions. La connexion peut aussi être interrompue ou altérée par la mobilité des sites.

➤ **vulnérabilité**

Les réseaux sans fil sont par nature plus sensibles aux problèmes de sécurité. Pour les réseaux *Ad hoc*, le principal problème ne se situe pas tant au niveau du support physique mais principalement dans le fait que tous les nœuds sont équivalents et potentiellement nécessaires au fonctionnement du réseau. Les possibilités de s'insérer dans le réseau sont plus grandes, la détection d'une intrusion plus délicate et l'absence de centralisation pose un problème de remontée de l'information et de détection d'intrusion.

➤ **Problème de réflexion de l'onde**

Un signal radio peut être réfléchi par des objets solides et risque par conséquent d'être reçu plusieurs fois (par différents chemins). Cette interférence porte le nom d'affaiblissement par trajets multiples (multipath fading).

➤ **Contraintes d'énergie**

Les hôtes mobiles sont alimentés par des sources d'énergie autonomes comme des batteries ou les autres sources consommables. Le paramètre d'énergie doit être pris en considération dans tout le contrôle fait par le système. Ce problème est d'autant plus important que chaque hôte mobile doit contribuer au routage d'où une dépense supplémentaire d'énergie.

➤ **Partage du medium radio**

Cela signifie que lorsqu'un mobile émet un signal, tous les mobiles dans un certain périmètre ne pourront pas transmettre de données simultanément, sous peine de provoquer des interférences à la réception.

I.6. Applications des réseaux *Ad hoc* [13]

Les nombreux avantages qu'offrent les réseaux *Ad hoc* ont donné naissance à plusieurs contextes d'applications, et cela dans divers domaines (militaire, publique, commerciale, etc.). Parmi ces applications, on peut citer :

I.6.1. Application militaire

Les premiers travaux sur les réseaux *Ad hoc* ont été militaires. En effet, ce type de réseaux représente le moyen idéal pour leurs communications (le déploiement d'une infrastructure dans un territoire ennemi étant impossible), en plus, leurs capacités à se reconfigurer et à rester opérationnel malgré la perte de nœuds qui se révèle très intéressante.

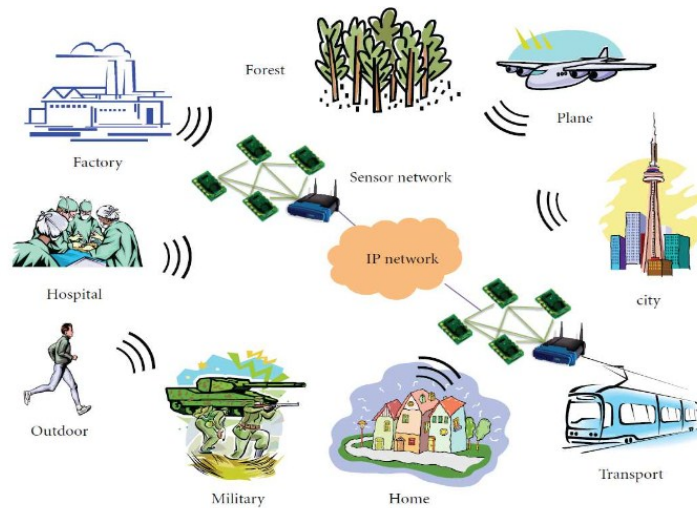


Figure I.2. Quelques domaines d'application pour les réseaux Ad hoc.

I.6.2. Réseaux d'urgence

Dans le cas de catastrophe naturelle (tremblement de terre, inondation, etc.), une mise en place rapide de réseau peut être indispensable que ce soit pour un réseau de communication entre les différentes équipes de secours (pour coordonner les recherches, échanger des informations ou encore offrir un moyen de communication aux victimes), ou pour remplacer des infrastructures détruites partiellement ou complètement.

I.6.3. Réseaux de capteurs

Il y a énormément d'applications utilisant ces réseaux, telles que les applications de contrôle de l'environnement (activité de la terre, détection de départ d'incendie, etc.), les applications militaires (détection de mouvement, détection de dangers chimiques, etc.), les applications industrielles (gestion de la circulation d'un objet, etc.) et bien d'autres.

I.6.4. Extension de réseaux dotés d'infrastructure

Un réseau *Ad hoc* peut être utilisé avec d'autres réseaux (filaires ou sans fils avec infrastructure). Cela ouvre plusieurs perspectives, l'une des plus intéressantes étant de faire une passerelle vers Internet et ainsi avoir l'accès à Internet dans des endroits tels que les transports en communs.

I.6.5. Applications commerciales

On trouve ce genre d'applications dans le paiement électronique distant (taxi), l'accès mobile à l'Internet, ou le service de guidage en fonction de la position de l'utilisateur.

I.6.6. Autres applications

Bien d'autres applications sont possibles, on peut citer une réunion de travail, connecter les appareils d'une même maison, des jeux en réseaux, diffusion d'informations sur les routes (pour éviter les embouteillages ou des accidents), etc.

I.7. Modes de communication dans les réseaux mobiles

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* » [14]. Ces trois modes de communication peuvent être schématisés par les figures suivantes :

I.7.1. Mode *unicast*

Le terme *unicast* définit une connexion réseau point à point, c'est un transfert d'un hôte à un autre hôte.

L'*unicast* est le fait de communiquer entre deux ordinateurs identifiés chacun par une adresse réseau unique. Les paquets de données sont routés sur le réseau suivant l'adresse du destinataire encapsulés dans la trame transmise. Seul le destinataire intercepte et décode le paquet qui lui est adressé.

Dans le protocole *IP*, les adresses doivent être uniques dans la mesure où les paquets sont routés au niveau du *LAN* ou du *WAN*.

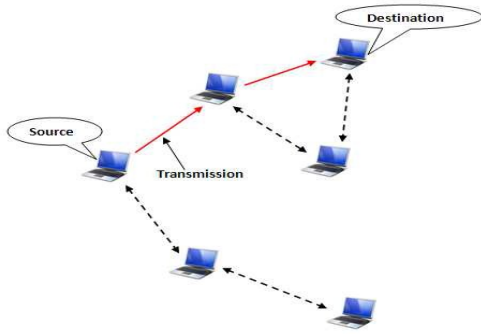


Figure I.3. Mode Unicast.

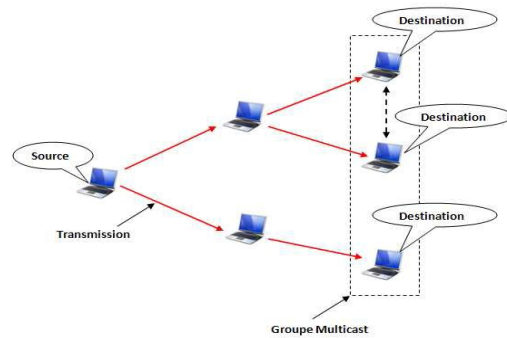


Figure I.4. Mode Multicast.

I.7.2. Mode multicast

Le terme multicast (multidiffusion) est utilisé pour désigner une méthode de diffusion efficace de l'information d'un émetteur (source unique) vers un groupe (plusieurs supports/médias). On dit aussi diffusion multipoint ou diffusion de groupe.

Les récepteurs intéressés par les messages adressés à ce groupe doivent joindre ce groupe au préalable. Le résultat de ces abonnements est de permettre aux commutateurs et routeurs intermédiaires d'établir une route depuis le ou les émetteurs de ce groupe vers le ou les récepteurs de ce groupe.

I.7.3. Mode diffusion

Les protocoles de communications réseau prévoient une méthode simple pour diffuser des données à plusieurs machines en même temps. Au contraire d'une communication point-à-point (*unicast*), il est possible d'adresser des paquets de données à un ensemble de machines d'un même réseau uniquement par des adresses spécifiques qui seront interceptées par toutes les machines du réseau ou du sous-réseau.

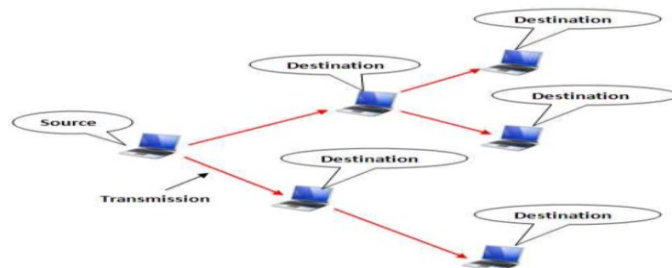


Figure I.5. Mode Broadcast.

I.8. Normes utilisés pour les réseaux Ad hoc

Les caractéristiques principales d'un réseau *Ad hoc* sont la facilité d'installation et de désinstallation et la mobilité. Pour assurer une connexion entre les éléments mobiles, le réseau *Ad hoc* se base sur quelques standards où on cite les plus utilisés :

➤ **Standard IEEE 802.11**

IEEE 802.11 est une norme établie par l'*IEEE (Institute of Electrical and Electronic Engineers)*. Elle décrit les couches physiques et *MAC* d'interfaces réseau radio et infra-rouge. Les débits possibles varient entre 1 et 54 *Mbit/s* suivant les techniques et les éventuelles extensions de la norme employées. Ce standard définit deux modes de configuration (avec et sans infrastructure). D'autres améliorations en été publiées par la suite, on cite entre autres :

- ***IEEE 802.11b***

Elle est apparue en 1999, elle est la plus répandue. Elle permet un débit théorique de 11 *Mbps* et peut atteindre 22 *Mbps* pour une fréquence de 2,4 *GHz* et dispose d'un rayon d'action de 100 *m* à ciel ouvert.

- ***IEEE 802.11g***

Elle est finalisée et standardisée au mois de juin 2002. Elle est donc la dernière en date. Elle garantit des débits de 54 *Mbps* théoriques (voire 72 ou 100 *Mbps*) et fonctionne à la même fréquence que la première (*IEEE 802.11b*) tout en restant compatible avec celle-ci. On trouve déjà sur le marché des équipements *IEEE 802.11g*.

- ***IEEE 802.11a***

Elle est aussi appelé *Wi-Fi5* offre pour sa part une bande passante de 54 *Mbps* à une fréquence de 5 *GHz*. Elle n'est pas compatible avec les deux autres. Malgré ses performances et sa bonne résistance aux interférences, elle reste très coûteuse.

I.10. Conclusion

Les travaux actuels ne se limitent pas à la conception d'une technologie sans fil adaptée aux réseaux *Ad hoc* et à un protocole de routage extensible. Bien que d'autres recherches soient en cours dans ce domaine, il n'est pas possible de décrire dans ce chapitre les voies de recherche en cours. Néanmoins, ce chapitre va se conclure sur une énumération des travaux les plus actifs actuellement.

Les voies de recherche sont multiples et il reste encore beaucoup de travail avant que les réseaux *Ad hoc* présentent un fonctionnement avancé. Néanmoins, avec les protocoles élaborés jusqu'ici, il est possible de construire de tels réseaux permettant la communication simple (sans qualité particulière) entre tous les mobiles. Il existe d'ailleurs certaines solutions commerciales qui sont soit des logiciels de routages, soit des cartes sans fil combinant une technologie sans fil et un protocole de routage.

Actuellement, le domaine militaire et le domaine académique sont probablement les principaux utilisateurs de ces réseaux. Pour que ces derniers puissent entrer dans la sphère du privé, il sera alors nécessaire d'identifier des applications-clés et un modèle économique pertinent.

Dans le chapitre qui suit, nous traitons les différents protocoles de routages dans les réseaux *Ad hoc*.

Chapitre II
Protocole de routage dans les
réseaux Ad hoc

.

II.1. Introduction

Même si aucune technologie sans fil n'a été conçue spécialement pour les réseaux *Ad hoc*, il est possible d'utiliser les technologies sans fil actuelles en leur ajoutant les protocoles adéquats pour faire fonctionner un réseau *Ad hoc*. Par exemple, avec le standard *IEEE 802.11* qui ne permet que la communication entre mobile à portée de communication, il est nécessaire d'ajouter, au-dessus de cette technologie, un protocole de routage qui rendra la communication possible entre tous les mobiles du réseau. Les protocoles de routage élaborés et utilisés dans les réseaux filaires sont difficilement utilisables tels qu'ils sont dans les réseaux *Ad hoc*. En effet, ces derniers sont mobiles donc avec une topologie hautement dynamique et une grande partie des ressources (comme par exemple la bande passante et l'énergie) sont très limitées. Des solutions adaptées aux caractéristiques des réseaux *Ad hoc* sont donc nécessaires, des solutions peu coûteuses en termes de bande passante et qui acheminent, si possible rapidement, les paquets à destination, quelle que soit la dynamique du réseau. Le principe de diffusion est une technique de routage très simple : chaque mobile, s'il n'a pas déjà reçu le paquet, il le réémet. Or, ce principe est très coûteux en bande passante. Il faut donc trouver des solutions plus intelligentes. La conception d'un protocole de routage a été la tâche principale du groupe de travail *MANET* à l'*IETF*. Ce groupe, fondé en 1995, est seulement en train de choisir non pas un protocole de routage mais plusieurs protocoles, ceci laisse penser que la tâche n'est pas si simple. En effet, ce n'est pas la conception d'un protocole de routage pour les réseaux *Ad hoc* qui est insurmontable, ce sont les différentes approches des protocoles proposés qui ont longuement animé le débat et ralenti le cours de la standardisation. Deux des approches ont des points de vue diamétralement opposés, alors que chacune a des avantages et des inconvénients. L'une des approches est appelée réactive alors que l'autre est considérée comme proactive.

II.2. Routage dans les réseaux *Ad hoc*

Le routage est l'élément primordial d'un réseau *Ad hoc*. Il faut un logiciel de routage dans chaque nœud du réseau pour gérer le transfert des paquets. La solution la plus simple est évidemment d'avoir un routage direct comme celui illustré à la figure suivante, dans lequel

chaque station du réseau peut atteindre directement une autre station, sans passer par un intermédiaire. Ce cas le plus simple correspond à une petite cellule, d'un diamètre inférieur à 100 mètres, comme dans un réseau IEEE 802.11 en mode Ad hoc.

Le cas classique du routage dans un réseau Ad hoc consiste à transiter par des nœuds intermédiaires. Ces derniers doivent posséder une table de routage apte à diriger le paquet vers le destinataire. Toute la stratégie d'un réseau Ad hoc consiste à optimiser les tables de routage par des mises à jour plus ou moins régulières. Si les mises à jour sont trop régulières, cela risque de surcharger le réseau. Cette solution présente toutefois l'avantage de maintenir des tables à jour et donc de permettre un routage rapide des paquets. Une mise à jour uniquement lors de l'arrivée nouveau flot restreint la charge circulant dans le réseau mais décharge le réseau de nombreux flots de supervision. Il faut arriver dans ce cas à mettre en place des tables de routage susceptible d'effectuer l'acheminement dans des temps acceptables.

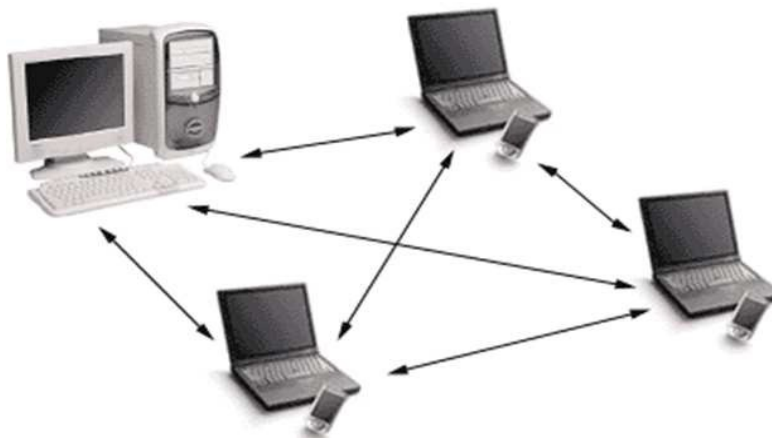


Figure II.1. Exemple d'un routage direct.

II.3. Les contraintes du routage 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 doit 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 multipoints 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.

II.4. Différentes approches mises en œuvre

Beaucoup de travaux de recherche ont été réalisés et se développent encore à l'heure actuelle dans le but de résoudre le problème d'acheminement des données entre les nœuds mobiles d'un réseau *Ad hoc*.

Le routage au sein des réseaux *Ad hoc* comporte quelques spécificités dues notamment à la mobilité des stations. Il est ainsi possible de distinguer différents types de protocoles de routage en fonction de la nature des flux transitant, des stations, des impératifs de communication *etc.*

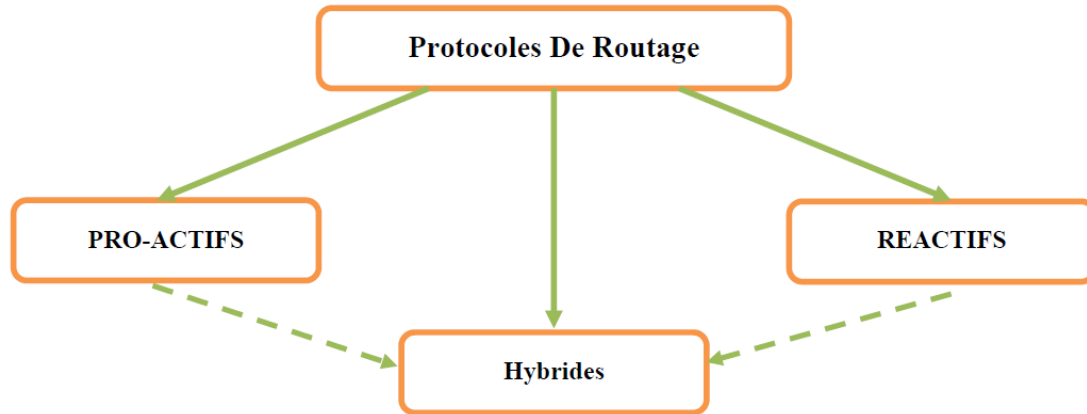


Figure II.2. Taxonomie des protocoles de routages des réseaux Ad hoc.

II.4.1. Protocoles proactifs

Dans les protocoles proactifs, les routes sont créées à l'avance dans une phase d'initialisation. Chaque nœud du réseau maintient une table de routage pour toutes les destinations indépendamment de l'utilité des routes. Si un changement de topologie survient, la modification des tables de routage doit être diffusée. Ce type de protocole est adapté aux applications qui nécessitent un prélèvement périodique des données (*application time driven*). Et par conséquent, les capteurs peuvent se mettre en veille pendant les périodes d'inactivité et n'enclencher leur dispositif de capture qu'à des instants particuliers [15].

II.4.1.1. Protocole «DSDV»

DSDV (Destination Sequence Distance Vector) est un protocole proactif unicast mobile Ad hoc qui est basé sur l'algorithme de *Bellman-Ford* [16]. Dans les tables de routage de *DSDV*, on trouve:

- ❖ Toutes les destinations possibles.
- ❖ Le nombre de nœuds (ou de sauts) nécessaire pour atteindre la destination.
- ❖ Le numéro de séquences (*SN : sequence number*) qui correspond à un nœud destination.

Les numéros de séquence sont utilisés dans *DSDV* pour distinguer les anciennes et nouvelles routes et pour éviter la formation de boucles de parcours. Chaque nœud transmet périodiquement des mises à jour, y compris des informations de routage à ses voisins immédiats.

II.4.1.2. Protocole «*OLSR*»

OLSR (Optimized Link State Routing Protocol) est un protocole de routage proactif au niveau IP destiné aux réseaux mobiles. Ce protocole est défini dans la *RFC 3626* de l'*IETF*. Comme son nom l'indique, il s'agit d'un protocole à état de lien optimisé. Le but d'*OLSR* est d'optimiser la diffusion des paquets d'information dans le réseau. Pour cela, le protocole se base sur la notion de relai multipoint. Un relai multipoint d'un mobile est un voisin à un saut et seuls les relais multipoints de ce mobile vont transmettre les informations émises par relai celui-ci. Pour que tous les voisins à deux sauts de ce mobile reçoivent les informations qu'il envoie, il faut que l'ensemble de ces relais multipoints soient voisins de tous les voisins à deux sauts du mobile. Par exemple sur la figure suivante, les mobiles A et B peuvent être des relais multipoints du mobile central : les mobiles à un saut du mobile central sont les mobiles dans les cercles bleus alors que les mobiles à deux sauts sont les mobiles dans les cadres noirs ; l'ensemble constitué de A et B est relié à tous les mobiles à deux sauts du mobile central, c'est donc un ensemble de relais multipoints du mobile central. Ainsi, si A et B retransmettent les informations envoyées par le mobile central, tous les voisins à deux sauts recevront ces informations.

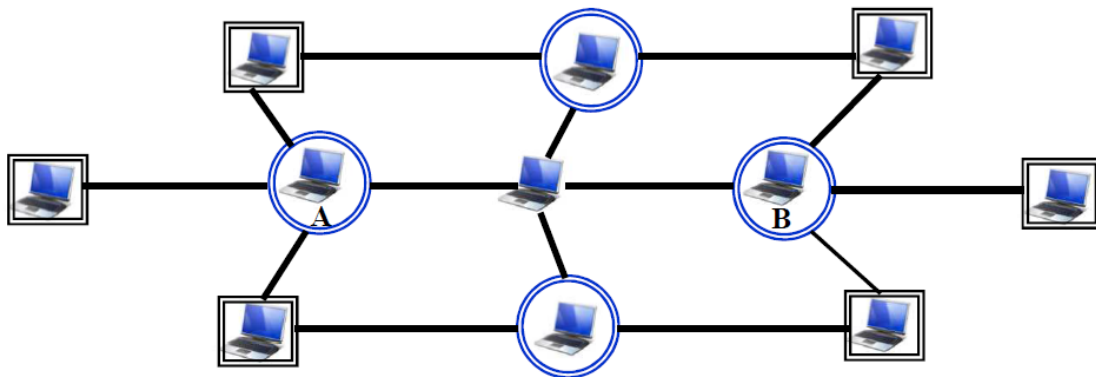


Figure II.3. Relais multipoints.

La diffusion d'information va donc se faire via les relais multipoints puisque seuls ces relais vont retransmettre les informations et non plus tous les mobiles du réseau comme dans une simple diffusion. Pour que la diffusion soit optimale en nombre de retransmissions, il faut que chaque mobile choisisse un nombre minimal de relais multipoint. Afin d'établir sa liste de relais multipoints, chaque mobile envoie régulièrement son identité et sa liste des voisins à un saut. Avec cette information, chaque mobile va connaître la topologie du réseau dans son voisinage à deux sauts. Ainsi, il va pouvoir déterminer une liste de relais multipoints qui couvrira tous les voisins à deux sauts, le but étant d'essayer de minimiser le nombre de relais multipoints choisis. Chaque terminal informe ses relais multipoints de son choix, ce qui permet à chaque mobile du réseau de savoir s'il est en mesure de retransmettre les informations qu'il reçoit d'un mobile donné. Chacun va donc diffuser dans le réseau, via les relais multipoints, cette information, qui l'a choisi comme relai multipoint. Grâce à cette diffusion, chacun peut construire une table de routage en déterminant, pour chaque mobile du réseau, le mobile voisin à atteindre.

II.4.2. Protocoles réactifs

Les protocoles réactifs créent et maintiennent des routes à la demande. Lorsque le réseau a besoin d'une route, une procédure de découverte de route est lancée. Ce type de protocole est pratique pour des applications temps réel (*event driven application*) où les capteurs doivent réagir immédiatement à des changements soudains des valeurs captées.

II.4.2.1. Protocole « DSR »

Le protocole *DSR (Routage à Source Dynamique)* [17] est basé sur l'utilisation de la technique "routage source". Dans cette technique, la source des données détermine la séquence complète des nœuds à travers lesquelles les paquets de données seront envoyés.

Un site initiateur de l'opération de « découverte de routes » diffuse un paquet requête de route. Si l'opération de découverte est réussite, l'initiateur reçoit un paquet réponse de route qui liste la séquence de nœuds à travers lesquels la destination peut être atteinte. Le paquet requête de route contient donc un champ enregistrement de route dans lequel sera accumulée la séquence des nœuds visités durant la propagation de la requête dans le réseau.

L'utilisation de la technique "routage source" fait que les nœuds de transit n'aient pas besoin de maintenir les informations de mise à jour pour envoyer les paquets de données puisque ces derniers contiennent toutes les décisions de routage.

Dans ce protocole, il y a une absence totale de boucle de routage car le chemin source-destination fait partie des paquets de données envoyées.

II.4.2.2. Protocole « AODV »

AODV (Ad hoc On-Demand Distance Vector) appartient à la famille des protocoles de routage à vecteur de distance, comme *DSDV*. Dans ces protocoles, les mobiles vont connaître pour certaines destinations, la meilleure distance en nombre de sauts et le mobile suivant à atteindre. *DSDV* est proactif, donc, chaque mobile maintiendra ses informations pour tous les autres mobiles du réseau tandis que dans *AODV*, les mobiles ne conservent ces informations que pour certains mobiles (ceux à qui ils ont des paquets par le passé).

Lorsqu'un mobile désire envoyer des paquets à une destination donnée avec *AODV*, il commence par vérifier qu'il n'a pas de route disponible dans sa table de routage. Si ce n'est pas le cas, il va initier une recherche de route grâce à un paquet *Route Request (RREQ)* pour localiser le mobile destinataire. Ce paquet est diffusé à ses voisins. Les mobiles qui reçoivent ce paquet *RREQ* regardent s'ils ont une route disponible vers le destinataire dans leur table de routage. Si ce n'est pas le cas, ils rediffusent à leur tour le paquet *RREQ* à leurs propres voisins et en gardent une trace. Grâce à l'utilisation de numéros de séquence sur les paquets, ceci permet d'éviter les problèmes de bouclage à l'infini. Les paquets *RREQ* se diffusent ainsi dans tout le réseau. Lorsqu'un tel paquet atteint le mobile destinataire ou un mobile qui dispose d'une route vers ce destinataire, alors un paquet de réponse (*RREP*) est généré par ce mobile et envoyé par le chemin inverse, grâce aux informations gardées dans les caches des mobiles traversés par les *RREQ*. Lors du passage du paquet *RREP*, chaque mobile touché va mettre à jour sa table de routage en gardant l'identité du mobile suivant dans la route construite pour le destinataire concerné. Par exemple sur la figure suivante, le mobile A, qui n'a pas de route vers le mobile B, initie une requête de recherche de route. *RREQ (i)* correspond au i-ème paquet *RREQ* envoyé dans le réseau.

Cette notation illustre seulement, pour l'exemple, l'ordre d'envoi des *RREQ* dans le protocole. Il faut noter que, suivant le protocole *MAC* utilisé, il est tout à fait possible que différents mobiles transmettent en même temps des paquets *RREQ*. A chaque transmission d'un paquet *RREQ*, chaque mobile garde en mémoire l'identité du mobile qui lui a envoyé précédemment un *RREQ*. Par exemple, lorsque le mobile 2 transmet un *RREQ*, il garde en mémoire l'identité de 1. De même, le mobile 4 garde l'identité de 2. Sur cette exemple, on voit d'ailleurs que lorsque 4 reçoit un *RREQ* de 3, il ne le retransmet pas car il a déjà émis un *RREQ* pour B venant de A. aucun mobile dans cet exemple n'a une route vers B dans son cache, donc, seul B atteint par *RREQ* va initier un paquet de réponse. Ce paquet va suivre le chemin inverse qui a été emprunté par le *RREQ* pour atteindre B : 4 sait que c'est 2 qu'il a été touché et c'est donc à 2 qu'il va envoyer le *RREP* ; 2 sait que c'est par 1 qu'il a été touché et c'est donc par 1 qu'il va envoyer le *RREP*, etc.

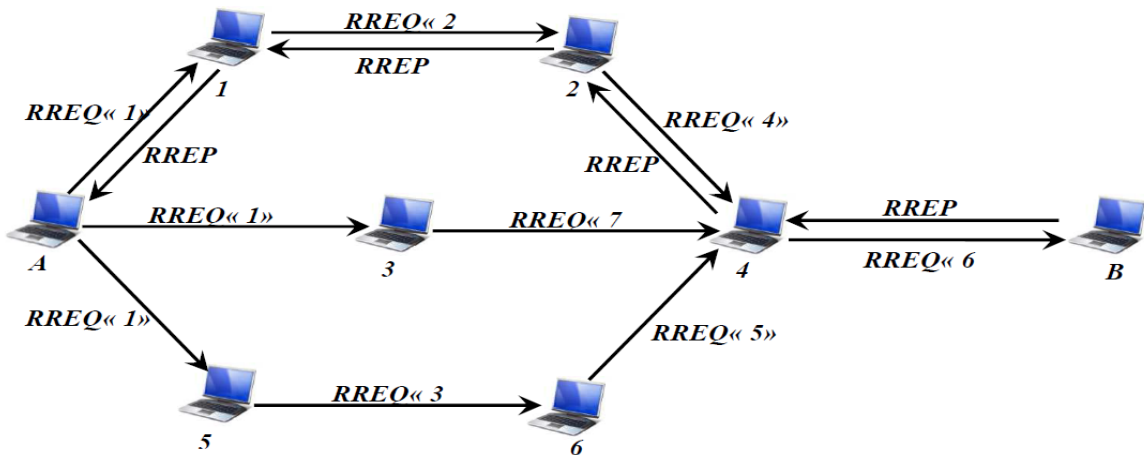


Figure II.4. Etablissement d'une route sous AODV.

Si une route n'est pas utilisée pendant un certain temps, chaque mobile concerné par cette route va l'enlever de sa table de routage. Lorsque le mobile source d'un message se déplace, il réinitie alors la recherche de route afin de trouver une nouvelle route vers son destinataire. Si c'est un mobile intermédiaire dans la route qui bouge, le mobile précédant sur le chemin se rend compte de sa disparition et envoie donc une notification de coupure de lien qui sera propagé jusqu'au mobile source qui peut choisir de rechercher une nouvelle route ou non.

II.4.3. Protocoles hybrides

Les protocoles hybrides utilisent une combinaison des deux principes. Par exemple, ils utilisent le principe des protocoles proactifs pour apprendre le proche voisinage, ainsi, ils disposent de routes immédiatement dans le voisinage. Au-delà du voisinage, le protocole hybride fait appel aux principes des protocoles réactifs pour chercher des routes.

II.5. Comparaison entre les protocoles proactifs et réactifs

Il est difficile de comparer les protocoles proactifs et les protocoles réactifs. En général, les protocoles réactifs sont moins coûteux en termes de signalisation et d'énergie, puisqu'ils établissent les routes que lorsqu'ils en ont besoin. En revanche, l'établissement d'une route est beaucoup plus rapide avec les protocoles proactifs puisque les mobiles ont les informations de routage à jour. Les analyses de performance sur ces différents protocoles montrent notamment que les protocoles proactifs comme *OLSR* sont efficaces dans le cadre des réseaux denses avec une mobilité relativement élevée, tandis que les protocoles réactifs comme *DSR* sont plus efficaces sur des réseaux creux avec une mobilité réduite. Le tableau suivant illustre les compromis faits :

Proactifs	Réactifs
maintiennent toujours les routes	un surcoût minimal parce que les routes ne sont déterminées qu'à la demande
peu ou pas de délai pour déterminer une route	un délai important lors de la détermination d'une route
consomme de la bande passante pour maintenir à jour les routes	emploie des systèmes d'inondations (flooding) pour réaliser une recherche globale
maintiennent des routes qui peuvent ne jamais servir	le contrôle des échanges peut être difficile

Tableau II.1. Comparaison entre les protocoles proactifs et réactifs.

On a pris l'exemple de comparaison d'un protocole de routage proactif, qui est *OLSR* et un protocole de routage réactif, qui est *AODV* :

II.5.1. Spécificités *OLSR* / *AODV* :

	<i>AODV</i>	<i>OLSR</i>
Sans boucle	Oui	Oui
Plusieurs routes possibles	Non	Non
Distribué	Oui	Oui
Type	Oui	Oui
Sécurité	Non	Non
Messages de contrôles périodiques	Non	Oui
Liens unidirectionnels	Non	Oui
Multicast	Oui	oui

Tableau II.2. Spécificités *OLSR* / *AODV*.

II.5.2. Synthèse de comparaison *OLSR* / *AODV*

AODV est utile pour des connections spontanées sur des réseaux citoyens. On n'a pas besoin de connaître la topologie du réseau. En revanche, son gros point faible est son temps de latence. En effet, la découverte des routes induit un temps de latence important. Le point faible d'*OLSR* est le taux d'overhead plus important qu'*AODV*. En revanche, sa connaissance totale de la topologie lui permet d'avoir un temps de latence beaucoup faible. De plus, *OLSR* a l'avantage d'être implémenté sur différentes plateformes (*Windows, Linux, MacOS, etc.*).

II.6. Conclusion

Bien que d'autres protocoles de routage aient été proposés pour les réseaux *Ad hoc*, les principales approches ont néanmoins été décrites et il est important de retenir qu'aucun des protocoles élaborés n'a tous les avantages et les performances ultimes. Le choix d'un protocole de routage sera fortement conditionné par les applications que l'on cherche à mettre en œuvre

et le type de réseau utilisé. Même si le groupe *MANET* est en train de standardiser plusieurs protocoles de routage, les recherches dans ce domaine ne vont pas s'arrêter dès demain.

Deux voies de recherche semblent se dégager principalement. La première concerne l'utilisation des réseaux Ad hoc qui seront rarement des réseaux isolés mais plutôt une composante de réseaux plus étendus comprenant différents sous-réseaux de technologies et architectures variées. Quels protocoles de routage proposer dans ce cas ? La deuxième voie de recherche est motivée par les mêmes raisons de facteur d'échelle qui ont poussé les chercheurs à repenser les protocoles proposés pour les réseaux radio par paquets.

Les protocoles proposés jusqu'ici fonctionnent pour des réseaux comprenant plusieurs milliers de mobiles, mais présentent de mauvaises performances pour des réseaux de plus grande échelle avec plusieurs dizaines ou centaines de milliers de mobiles.

Dans le chapitre qui suit, nous décrivons les différents scénarios à simuler en mettant l'accent sur le principe de fonctionnement d'*OPNET (Optimum Network Performance)*.

Chapitre III

Simulation des différents modèles.

III.1. Objectifs de projet

Même si aucune technologie sans fil n'a été conçue spécialement pour les réseaux *Ad hoc*, il est possible d'utiliser les technologies sans fil actuelles en leur ajoutant les protocoles adéquats pour faire fonctionner un réseau *Ad hoc*. Par exemple, avec le standard *IEEE 802.11* qui ne permet que la communication entre mobile à portée de communication, il est nécessaire d'ajouter, au-dessus de cette technologie, un protocole de routage qui rendra la communication possible entre tous les mobiles du réseau.

Notre objectif est d'examiner l'influence de la puissance sur la distance de communication, et même de comparer les performances des protocoles de routages des réseaux *MANETs*.

III.2. Modèles de tests et configuration de réseaux

La communication dans les réseaux *MANETs* rencontre plusieurs problèmes tels que ceux reliés au routage, à la congestion, à la puissance réduite dans *MANET*. Ces problèmes peuvent être causés par la mobilité des réseaux *MANETs* ou par les besoins des applications multimédia.

Pour atteindre nos objectifs, il faut tout d'abord constituer un réseau *MANET*, composé de plusieurs stations. Celles-ci seront générées par des différents scénarios dans le réseau. Cette approche va nous permettre de savoir la distance de communication d'une part et de connaître les performances de protocoles de routage d'autre part.

➤ Modèles de tests

Afin de voir l'effet de la portée sur la puissance de communication et les performances de routages, maintes situations seront créées dans le réseau *MANET*. Pour ce faire, plusieurs scénarios peuvent être exécutés:

❖ Scénario de puissance de communication

Ce scénario consiste à examiner la puissance de transmission des stations du réseau *MANET*. La puissance de transmission détermine la portée dans laquelle le signal peut être

reçu. Elle est cruciale en déterminant la performance du réseau en termes de trafic reçu, trafic envoyé, et taux d'envoi.

❖ Scénario de comparaison entre AODV et OLSR

Ce scénario consiste à comparer les performances des deux protocoles de routages *AODV* et *OLSR*. En les déterminant en termes de trafic émis, nombre de paquets routé, temps de découverte de la route etc.

III.3. Présentation du simulateur *OPNET (Optimum Network Performance)*

OPNET est un outil de modélisation et de simulation de réseaux très puissant et très complet s'adressant à différent public (entreprises, opérateurs, chercheurs, etc.), Basé sur une interface graphique intuitive, son utilisation et sa prise en main est relativement aisée.

Ce simulateur fournit une bibliothèque de plus de 400 fonctions propriétaires spécifiques à l'usage des réseaux (création, envoi et réception de paquets, extraction de valeurs contenues dans les différents champs d'un entête, etc.). Il permet de gérer plusieurs types d'objets relatifs aux réseaux parmi eux : les liens, les formats de paquets [18].

La librairie d'*OPNET* est riche de protocoles réseaux, apprentissage long, description de modèles à l'aide d'une interface graphique.

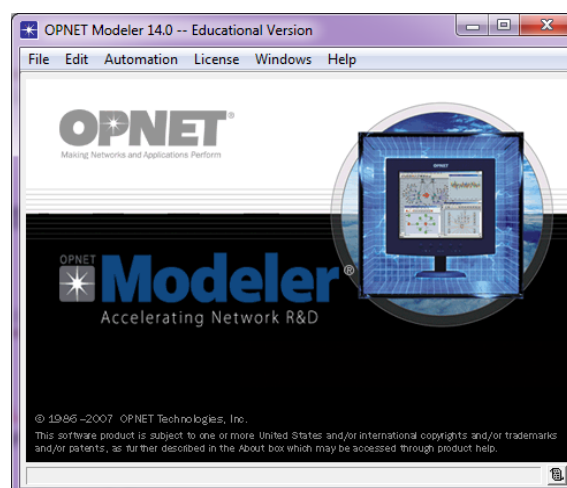


Figure III.1. Lancement du simulateur *OPNET*.

III.3.1. Installation du simulateur *OPNET*

L'installation d'*OPNET* se fait en différentes étapes suivant une procédure décrite dans le package téléchargé selon le système d'exploitation installé. Les éléments installés sur l'ordinateur seront les suivants :

- * Une bibliothèque de simulation interne.
- * Un compilateur du langage *C++*.
- * Un exécutable *OPNET*.
- * Une interface graphique de simulation.
- * Un outil de documentation de modèle (op_models).
- * Autres utilitaires (l'outil de création de projets, etc.).
- * Une documentation, des simulations types, etc.

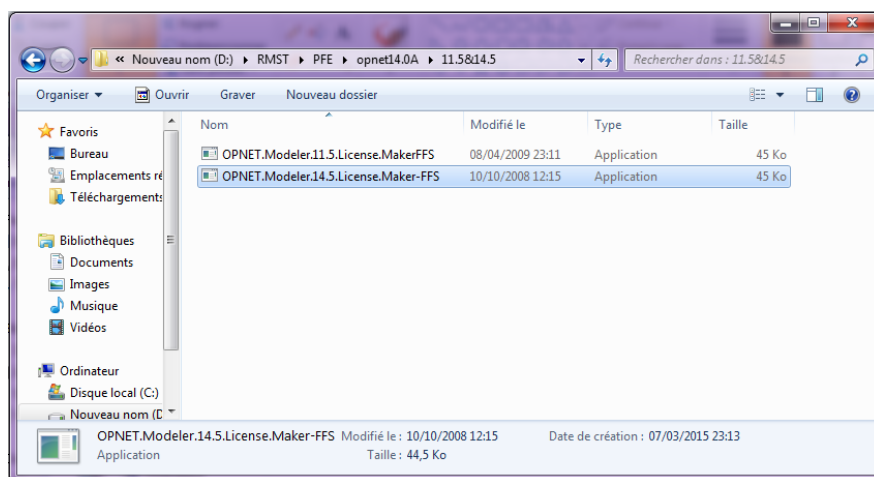


Figure III.2. Fichier pour mettre la licence.

Pour installer le simulateur *OPNET*, il faut déjà avoir installé sur l'ordinateur un compilateur *C++* (*Microsoft visual studio 2010*) afin d'avoir les animations des projets effectués.

❖ C'est quoi un visual studio ?

Visual Studio est un ensemble complet d'outils de développement permettant de générer des applications *Web ASP.NET*, des Services *Web XML*, des applications bureautiques et des

applications mobiles. Visual Basic, Visual C++, Visual C# et Visual J# utilisent tous le même environnement de développement intégré (*IDE, Integrated Development Environment*), qui leur permet de partager des outils et facilite la création de solutions faisant appel à plusieurs langages. Par ailleurs, ces langages permettent de mieux tirer parti des fonctionnalités du *Framework .NET*, qui fournit un accès à des technologies clés simplifiant le développement d'applications *Web ASP* et de *Services Web XML* grâce à *Visual Web Developer* [18].

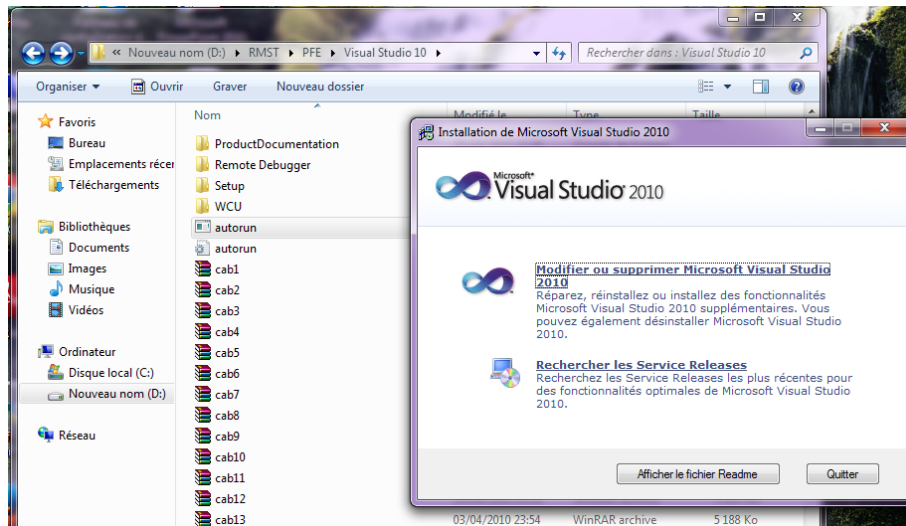


Figure III.3. Fenêtres d'installation de compilateur C++.

Ensuite, on va introduire les variables d'environnements dans le système des paramètres avancés d'ordinateur.

Enfin, on va mettre une licence pour pouvoir accéder au simulateur *OPNET* (voir la figure III.2), on peut tester ce simulateur d'après les exemples qui existent dans les modèles d'*OPNET* comme il est présenté sur la figure ci-après :

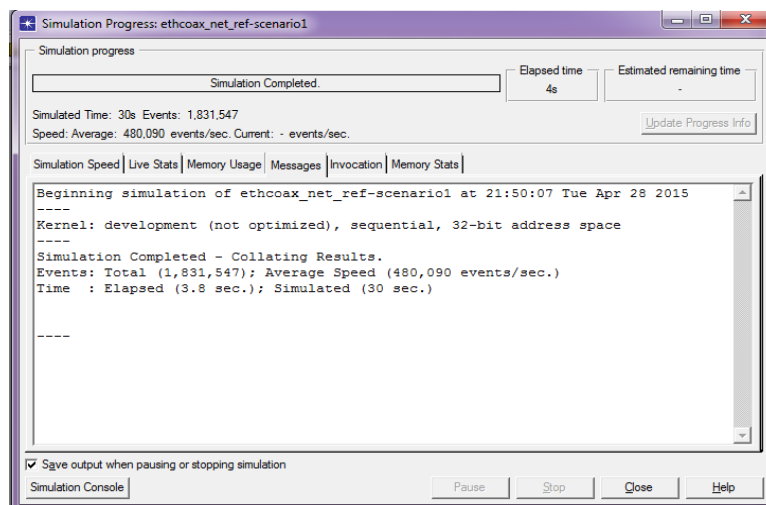


Figure III.4. Message de la simulation complète.

Pour vérifier si l'installation d'*OPNET* a réussi, vous devez avoir une fenêtre qui apparaît sur la figure précédente.

III.3.2. Structure d'*OPNET*

OPNET dispose de trois niveaux hiérarchiques imbriqués :

➤ **Network domain**

C'est le niveau le plus élevé de la hiérarchie d'*OPNET*. Il permet de définir la topologie du réseau en y installant des routeurs, des hôtes, des équipements tels que des switches, reliés entre eux par des liens. Chaque entité de communication (appelée nœud) est entièrement configurable et est définie par son modèle.

➤ **Node domain**

Le node domain permet de définir la constitution des nœuds (routeurs, stations de travail, hub, etc.). Le modèle est défini à l'aide de blocs appelés modules. Certains modules sont non programmables, les autres modules sont entièrement programmables.

➤ **Process domain**

La définition de chaque module programmable se fait à ce niveau.

III.3.3. Simulation sous *OPNET*

La simulation sous *OPNET* est basée principalement sur deux méthodes :

- utilisation des nœuds préprogrammés fournis par la librairie d'*OPNET*.
- définition d'un modèle de lien, des process models décrivant des routeurs et des hôtes...

III.3.4. Ses avantages

Il permet de concevoir et d'étudier des réseaux de communications, des nouvelles technologies, des protocoles et des applications avec facilité et évolutivité.

III.3.5. Son inconvénient

Parmi les problèmes d'*OPNET* :

- il est payant mais ce problème est résolu avec la version académique.
- apprentissage long.

III.4. Modèles de simulation *OPNET*

Afin de mieux présenter l'effet de la portée sur la puissance de communication et les performances de routages, des simulations d'un réseau *MANET* et avec différentes conditions ont été effectuées. Nous avons classé les simulations dans trois modèles différents, le premier est simple et a pour but de déterminer la portée de communication, le deuxième est fait pour calculer la puissance de communication et le dernier est réservé à la comparaison entre les protocoles de routage.

III.4.1. Modèle de mobilité

La simulation a été faite à l'aide du logiciel *OPNET* version 14.0. Tout d'abord, nous avons créé un réseau *Ad hoc* mobile. Ce réseau *Ad hoc* mobile est constitué de deux stations *WLAN* (*Workstation LAN*) qui sont distribuées dans une aire de la forme d'un carré (*grid*) (figure III.5). La topologie de carré a été utilisée afin d'augmenter les chances de trouver les différentes routes entre la source et la destination.

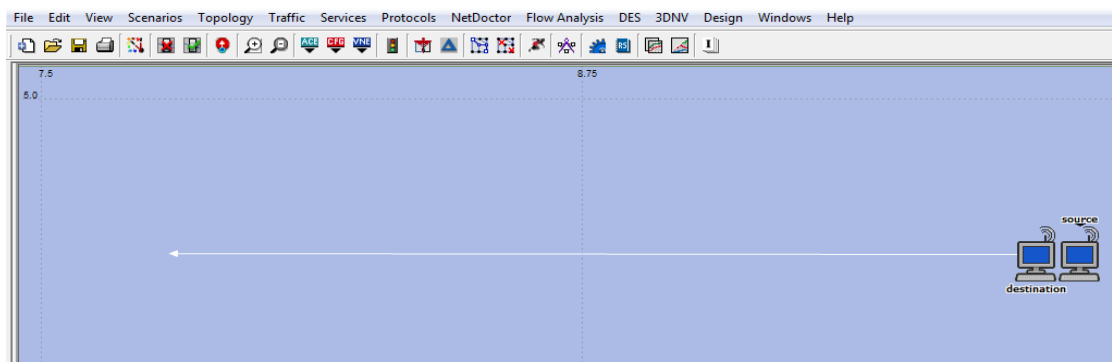


Figure III.5. Le réseau *Ad hoc* simulé dans *OPNET*.

La source et la destination sont présentées sur la figure III.5, et elles ont été choisies de façon que la distance entre les deux soit de 100 mètres. Nous avons définies une trajectoire de longueur 2000 mètres. Le temps de simulation est de 18 minutes. La vitesse de déplacement de destination est de 2m/s.

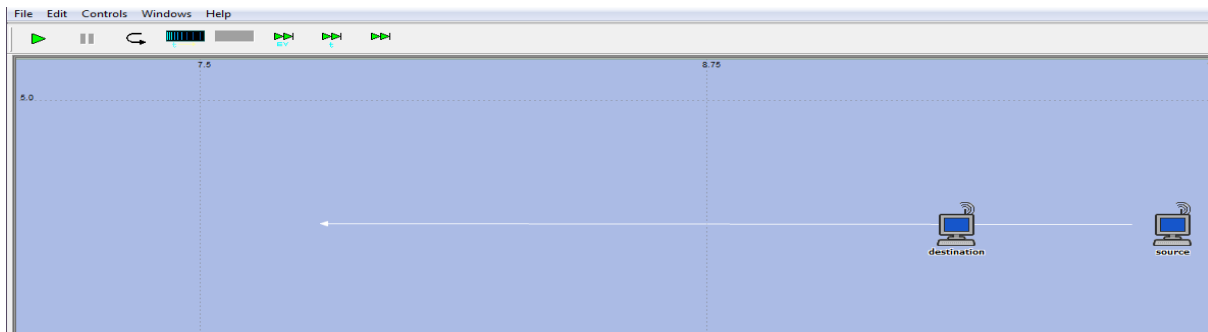


Figure III.6. Animation du réseau Ad hoc simulé.

Nous avons utilisé les paramètres de générateur de trafic comme il est présenté sur le tableau suivant :

Nom de la source	Source
Nom de la destination	Destination
Temps de départ	5 secondes
Etat ON	2000 secondes
Etat OFF	0 secondes

Tableau III.1. Paramètres de générateur de trafic.

III.4.2. Modèle de puissance de communication

Dans ce modèle, nous avons simulé le même réseau décrit précédemment mais maintenant on va introduire des variations dans les paramètres de générateur de trafic de la source (la source a besoin beaucoup plus de puissance pour atteindre la destination).

Puissance 1	0.001 W
Puissance 2	0.002 W
Puissance 3	0.005 W
Puissance 4	0.010 W

Tableau III.2. Paramètres de puissances.

III.4.3. Modèle de performances de routage *MANET*

Nous avons créé un réseau *Ad hoc* mobile à multi-sauts. Ce réseau *MANET* est constitué de 16 stations *WLAN (Ad hoc)* qui sont distribuées dans une aire de la forme d'un carré (*grid*) de 9 000 000 m² (figure III.7). La topologie de carré a été utilisée afin d'augmenter les chances de trouver les différentes routes entre la source et la destination. Les protocoles de routage utilisés sont *AODV* et *OLSR*. Le temps de simulation est de 200 secondes.

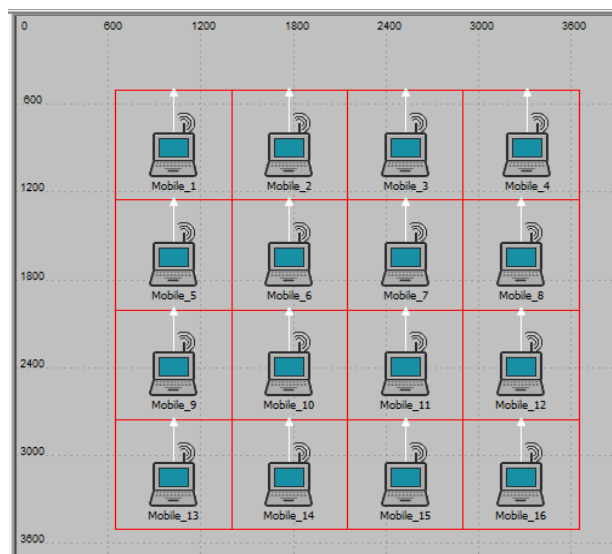


Figure III.7. Réseau *Ad hoc* simulé dans *OPNET*.

Le tableau III.3 représente les paramètres de génération de trafic *MANET*.

Temps de départ de génération de trafic	100 secondes
Type de communication	Aléatoire (<i>Random</i>)
Taille de paquets	1024 octet/s

Tableau III.3. Paramètres de générateur de trafic *MANET*.

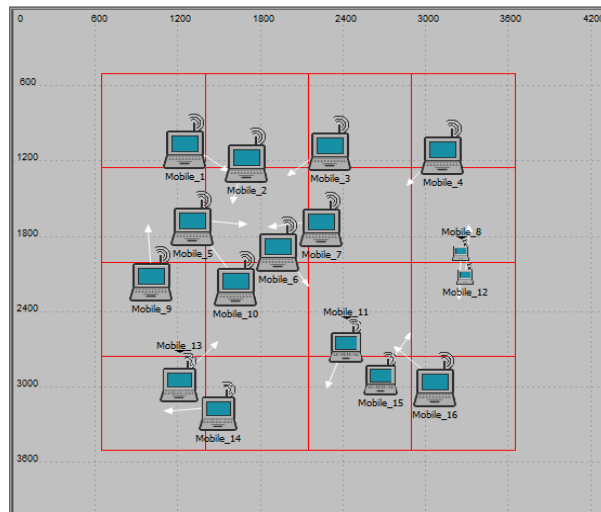


Figure III.8. Animation du réseau Ad hoc simulé.

La figure III.8 présente l'animation du réseau simulé dans le modèle de performance de routage *MANET*.

III.5. Les métriques de performance

Avant de présenter les résultats et les analyses des simulations réalisées, nous définirons quelques termes quand peut les évalués sous l'outil *OPNET*. Ces définitions, tirées de la documentation d'*OPNET*, sont:

➤ **Paquets de contrôle**

Cette métrique détermine le nombre de paquets émis par un nœud dans le but de gérer le réseau (identification, recherche de route, maintien de la table de routage, maintenance des liens rompus, etc.). Comme chaque protocole a son propre algorithme de routage, nous espérons avec cette métrique, trouver lequel d'entre eux utilise le minimum de paquets de contrôle pour un meilleur acheminement de paquets et une meilleure visibilité de la topologie de réseau à n'importe quel instant.

➤ **Paquets perdus (Packets dropped)**

Cette métrique détermine le nombre de paquets de contrôle ou de données perdues physiquement dans le réseau. Ces pertes sont issues de trafic important ou de temps d'attente assez élevé. Les nœuds routeurs perdent des paquets de données utiles ou même de contrôle quand les liaisons sont perdues à cause du déplacement des nœuds récepteurs ou ils sortent du rayon de propagation de leurs émetteurs. Un bon algorithme génère plusieurs chemins pour éviter les pertes dans des cas pareils.

➤ **Trafic émis (Sent traffic)**

Ce trafic détermine le volume des paquets de données effectives émises par un nœud source au profit d'un nœud destinataire. Un nœud source peut ne pas avoir suffisamment de temps pour envoyer toutes les données qu'il souhaite envoyer. Les principales raisons sont soit le medium est très occupé par les nœuds voisins, soit le nœud même est trop chargé par le routage des données d'autres nœuds source. Un bon algorithme essaie de tendre vers un bon équilibre et trouver la meilleure combinaison de chemins qui optimise les flux sortants et routés.

➤ **Trafic routé (Routing traffic)**

Ce trafic détermine le volume des paquets de données effectives routées par un nœud routeur. Un nœud peut être source, routeur ou destination. Alors l'idéal serait, que chacune des sources envoie directement à sa destination sans déléguer sa charge à des nœuds intermédiaires (routeurs). Cette situation est loin d'être la réalité, mais en choisissant des chemins plus courts, le routage sera diminué en conséquence.

➤ **Temps d'attente (Backoff)**

C'est un temps aléatoire qu'un nœud peut attendre avant de tenter la retransmission. Les temps *backoff* sont ajustés pour augmenter ou diminuer la probabilité d'accès au medium afin de favoriser ou défavoriser la transmission de données aux flux de données de priorités faibles ou élevées.

➤ **Nombre de paquets routés (Load)**

C'est le nombre de paquets routés transmis par paquets de données livré à la destination. Chaque transmission *hop-wise* d'un paquet de routage est comptée comme une seule transmission. La mesure du paramètre *load* est importante pour le trafic *best-effort*. La mesure de la charge de routage évalue l'efficacité du protocole de routage.

➤ **Essai de retransmissions (Retransmission Attempts)**

C'est un mécanisme de retransmission en cas de collision. Le nombre de tentatives de retransmission peut être choisi.

➤ **Taille de file d'attente (Queue Size)**

C'est la taille des files d'attente.

III.6. Conclusion

Dans ce chapitre, nous avons présenté le simulateur *OPNET* pour les réseaux *MANETs*, notre choix a été fixé sur ce simulateur essentiellement à cause de sa construction modulaire et sa flexibilité. Ensuite, nous avons présenté les différents scénarios simulés sans oublier de décrire les métriques de performances de notre simulation.

Dans le chapitre suivant, on analysera les résultats de simulation des réseaux *MANETs* suivant plusieurs modèles.



Chapitre IV
Résultats et analyses.

IV.1. Introduction

Dans ce chapitre, nous présenterons les résultats et les analyses des simulations relatives à notre travail, qui est effectué avec logiciel *OPNET 14.0*.

IV.2 Résultats et discussions

Dans cette section, nous allons présenter les résultats que nous avons obtenus jusqu'à maintenant. Ces résultats valident le modèle de simulation que nous avons conçu.

IV.2.1. Modèle 1 (Modèle de mobilité)

Dans ce scénario, la source et la destination sont en mouvement suivant une trajectoire, on va définir la distance maximale de communication entre les deux stations.

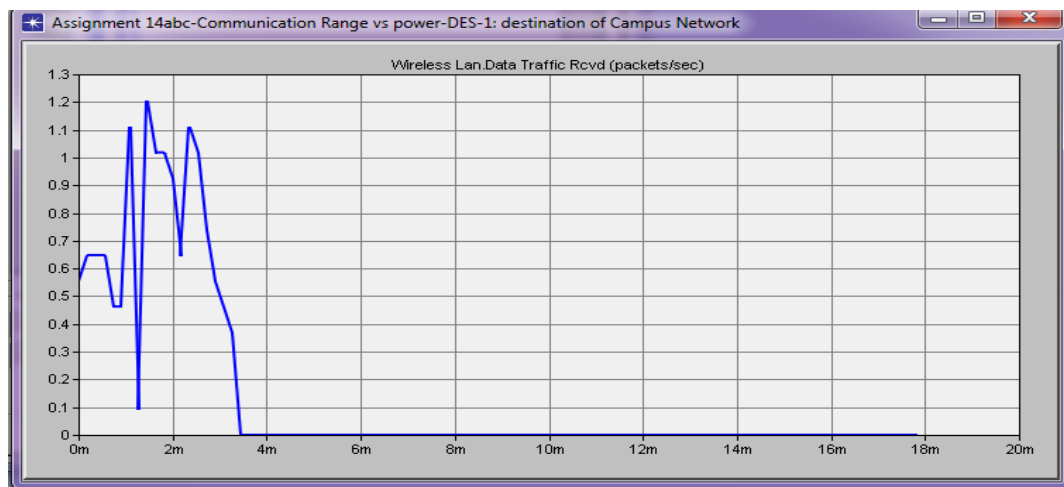


Figure IV.1. *Trafic reçu par la destination.*

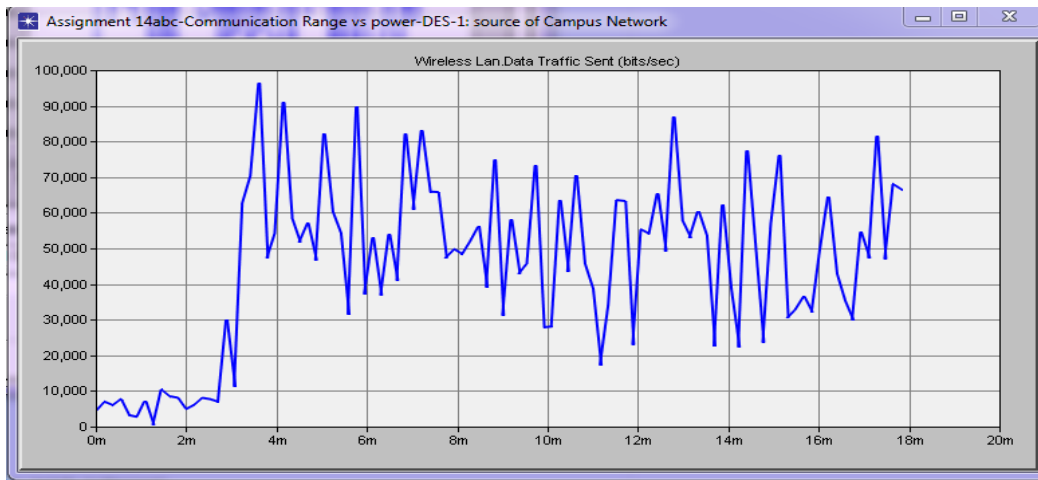


Figure IV.2. Trafic envoyé par la source.

D'après les deux figures précédentes, le temps où la destination arrête de recevoir le trafic est de : $3\text{min}25\text{s}$, à partir de cette valeur, la distance maximale calculée entre les deux nœuds est de : 410 m .

A l'instant $3\text{min}25\text{s}$ la destination arrête de recevoir le trafic et le taux d'envoi augmente car la source ne peut pas atteindre la destination, donc comme la distance est supérieure à 410 m le taux d'envoi augmente.

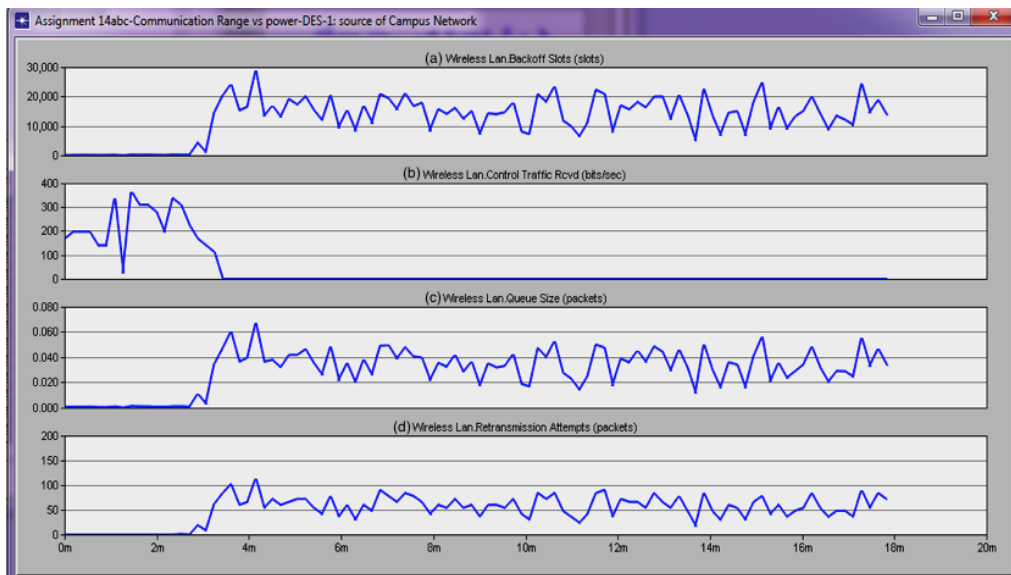


Figure IV.3. (a) Temps d'attente (b) Contrôle de trafic reçu. (c) La taille des files d'attente. (d) Les essais de retransmission.

A partir des résultats de simulation illustrés sur la figure IV.3 précédente, puisque le destinataire arrête de recevoir les données, on remarque que le mécanisme de retransmission de trafic ainsi que le temps nécessaire pour tenter cette retransmission déclenchent dès que les paquets de control responsables de la gestion du réseau établies le bon chemin pour renvoyer les paquets à l'instant *3min25s*.

Nous remarquons encore que la variation de ces deux premiers métriques reste presque similaire au cours du temps.

Concernant le troisième graphe dans la figure IV.3, on remarque que les files d'attentes sont vides jusqu'à l'établissement des chemins de transmission de données, les paquets arrivent aux ces fils d'attentes pour être routés vers le destinataire.

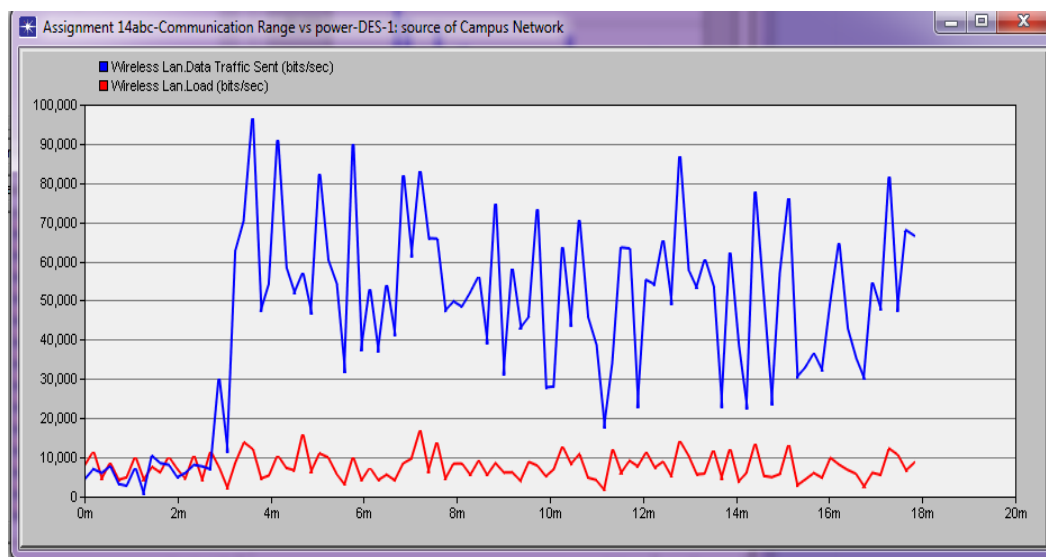


Figure IV.4. *Trafic envoyé des données et la charge.*

La figure IV.4 montre l'évolution du taux de trafic émis (bits/sec) et la charge des paquets envoyés vers le nœud destinataire variantes en fonction du temps, ces deux valeurs changent parallèlement environ 10.000 bits/sec jusqu'à l'instant où la transmission se bloque (*3min25s*).

Après cet instant le taux de trafic émis subit une augmentation importante (de 10.000 à 100.000 bits/sec) dans le but d'atteindre le destinataire alors que la charge reste dans le même niveau.

IV.2.2. Modèle 2 (Modèle de puissance de communication)

Dans ce scénario, le même modèle mais on va examiner l'influence de la distance sur la puissance de transmission.

Puissance (W)	0.001	0.002	0.005	0.01
Distance (m)	410	626	1058	1532

Tableau IV.1. Variation de la puissance en fonction de la distance.

On va introduire des variations sur la valeur de puissance de transmission de la source puis on va calculer la distance convenable à cette puissance comme illustre le tableau précédent.

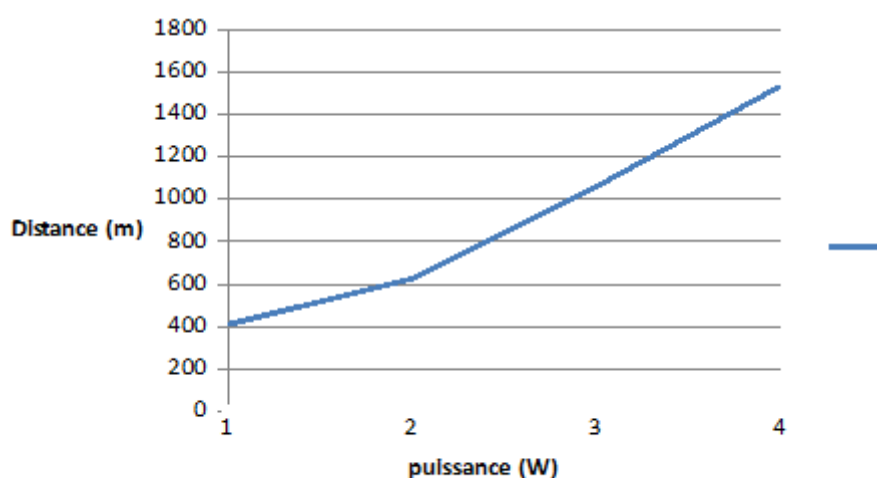


Figure IV.5. Variation de la puissance en fonction de la distance.

On remarque à partir du graphe que la puissance de la source augmente avec la distance de transmission car la source a une puissance suffisante pour atteindre la destination, donc la puissance est directement proportionnelle à la distance.

IV.2.3. Modèle 3 (Modèle de performances de routage MANET)

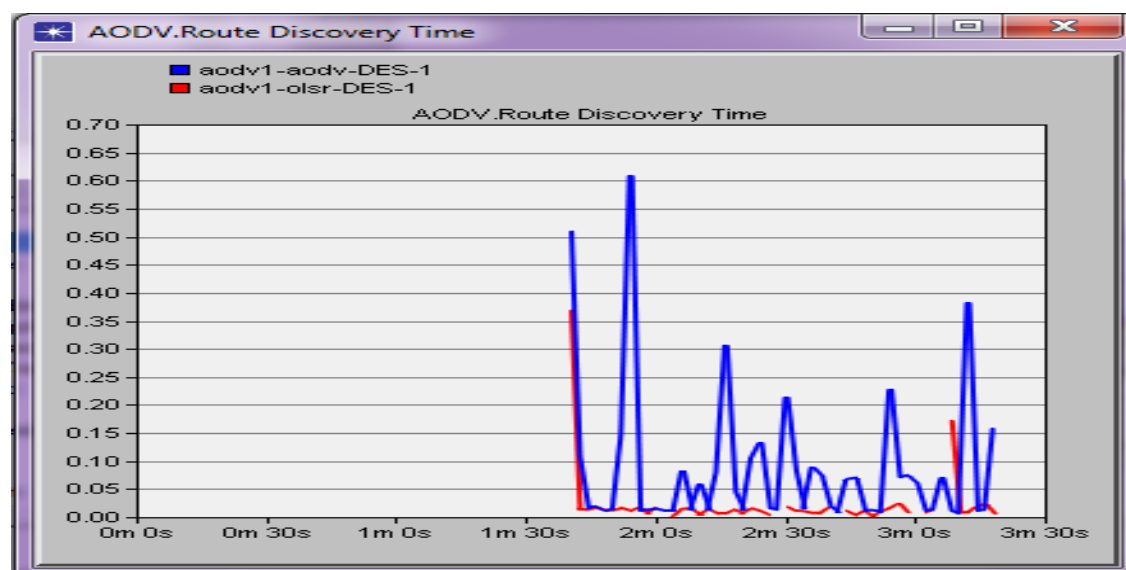


Figure IV.6. Temps de découvert de la route pour l'AODV et OLSR.

A partir de la figure IV.6, on remarque que la découverte de la route pour l'AODV est continue tandis qu'elle est discrète pour l'OLSR, on remarque aussi une variation importante pour le premier protocole (entre 0.01 et 0.60) alors que pour le deuxième elle est presque négligeable sauf à deux instants 1min40s et 3min10s, elle augmente respectivement jusqu'à 0.36 et 0.17.

Cela est due au principe de fonctionnement de ces deux protocoles : lorsqu'un nœud dans un réseau exécutant le protocole OLSR souhaite trouver une route vers un hôte, tout ce qu'elle a à faire est déclencher une recherche dans la table de routage, alors que dans un réseau d'AODV, un processus de découverte de route doit être initialisé.

Il est évident qu'une simple consultation de la table de routage prend moins de temps que d'inonder le réseau, ce qui rend la performance de protocole OLSR mieux dans les réseaux sensibles au retard.

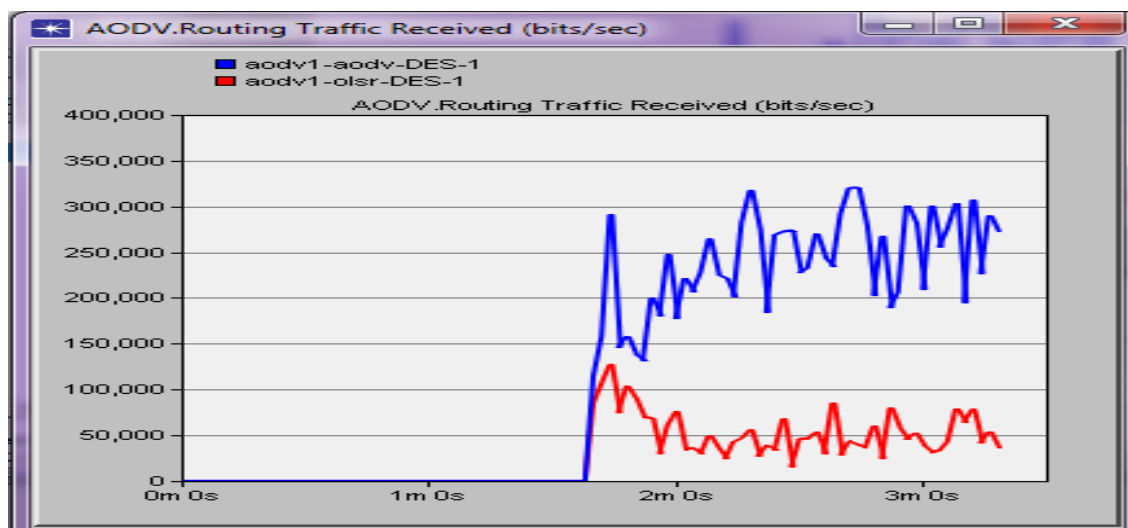


Figure IV.7. Acheminement du trafic reçu pour l'AODV et OLSR.

Cette figure montre l'acheminement de trafic reçu (bits/sec) on utilisant les deux protocoles AODV et OLSR, pour 16 nœuds, le trafic reçu par l'AODV montre une augmentation jusqu'à 300.000 bits/sec à l'instant 1min30s, par ailleurs la valeur d'OLSR accoisent jusqu'à la moitié de la valeur d'AODV au même instant.

Après ce changement, la variation des paquets de réception d'OLSR est beaucoup plus faible que celle d'AODV, ils varient de 275.000 à 120.000 bits/sec pour AODV tandis qu'elles restent entre 130.000 et 25.000 bits/sec, donc en générale, on observe que pour l'OLSR la variation des paquets reçus et quasiment stable avec le temps de simulation qu'AODV.

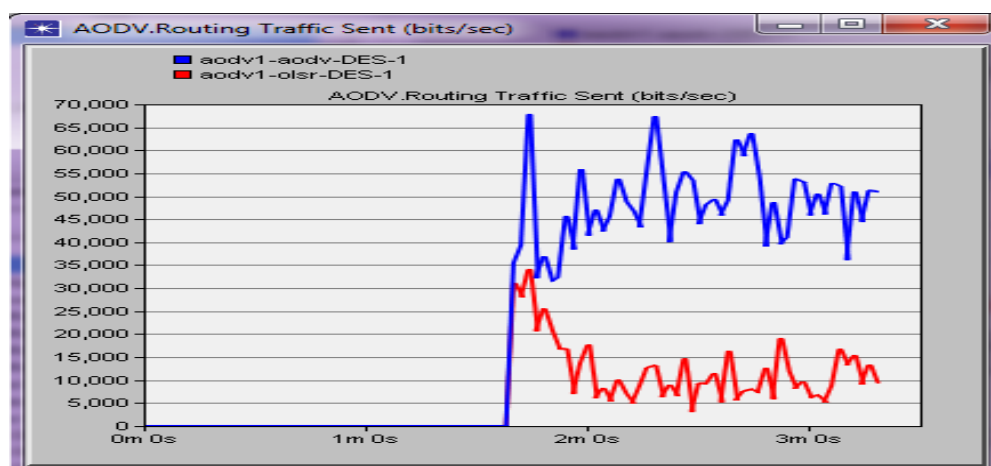


Figure IV.8. Acheminement du trafic envoyé pour l'AODV et OLSR.

La figure IV.8 illustre le comportement de l'acheminement du trafic envoyé par rapport au temps, la taille des paquets de trafic envoyés est plus basse que celle de trafic reçus, on remarque une augmentation de trafic envoyé pour l'AODV à un certain seuil (70.000 bits/sec) où il commence à diminuer jusqu'à 32.000 bits/sec qui va être la plus basse valeur concernant ce protocole. Cependant le trafic d'OLSR augmente de 35.000 bits/sec à l'instant 1min40s (même instant qu'AODV), ensuite décline jusqu'à 7.000 bits/sec et reste en variation entre 4.000 et 20.000 bits/sec cela se traduit par la faible quantité des messages de contrôle qui jouent un rôle important sur le nombre collisions dans la couche MAC, bien que le nombre de collisions reste inférieur pour OLSR. Quand les nœuds sont stabilisés, les routes établis sont maintenus plus long, ce qui entraîne une meilleure réutilisation des routes préalablement établis et la construction de nouvelles routes devient moins gourmand et par conséquent les paquets de contrôle se diminuent donc l'acheminement du trafic envoyé est rarement utilisé.

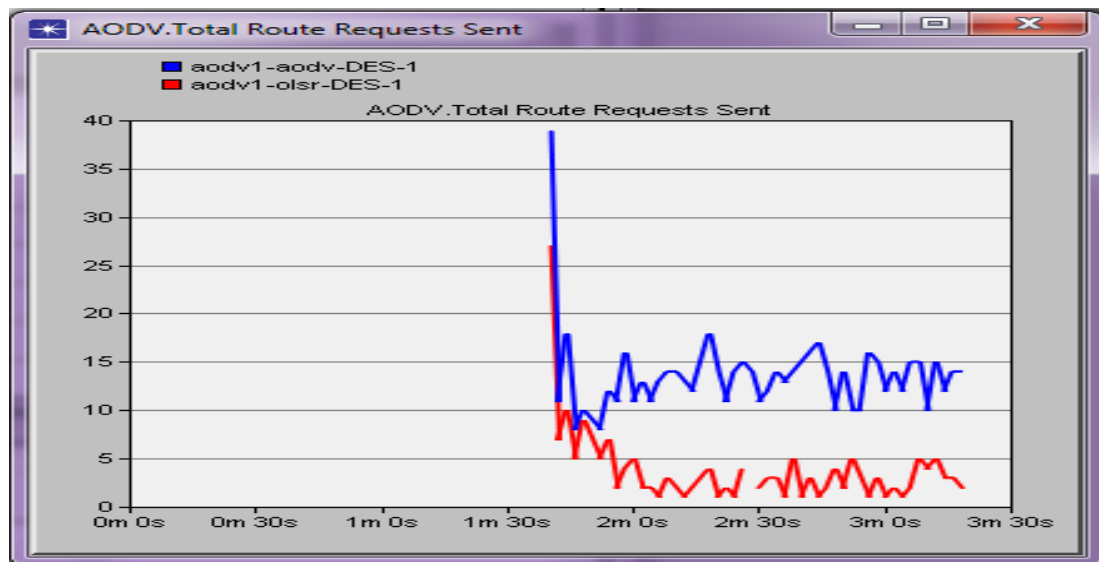


Figure IV.9. Paquets de demande de route pour l'AODV et OLSR.

La figure IV.9 ci-dessus décrit le taux de paquets envoyés de demande d'une route, on observe que les graphes des deux protocoles augmentent au même instant (1min40s) jusqu'à 39 paquets pour l'AODV et 26 paquets pour l'OLSR puis

commencent à décliner jusqu'à 10 paquets ou les demandes de route envoyés pour l'AODV restent entre l'intervalle de 8 et 17 paquets tandis que pour l'OLSR ils varient entre 0 et 5 paquets.

Cette différence est à cause de type de protocole, comme l'AODV est un protocole réactif, il établit les chemins pour la transmission des données à la demande donc il utilise plusieurs types de messages de contrôle de route (*RREQ*, *RREP*, *RERR*) contenant des nouvelles informations sur le numéro de séquence d'un nœud destination, par contre l'OLSR est un protocole proactif son concept des relais multipoint vise à réduire le nombre de messages de contrôle inutiles lors de l'inondation dans le réseau.

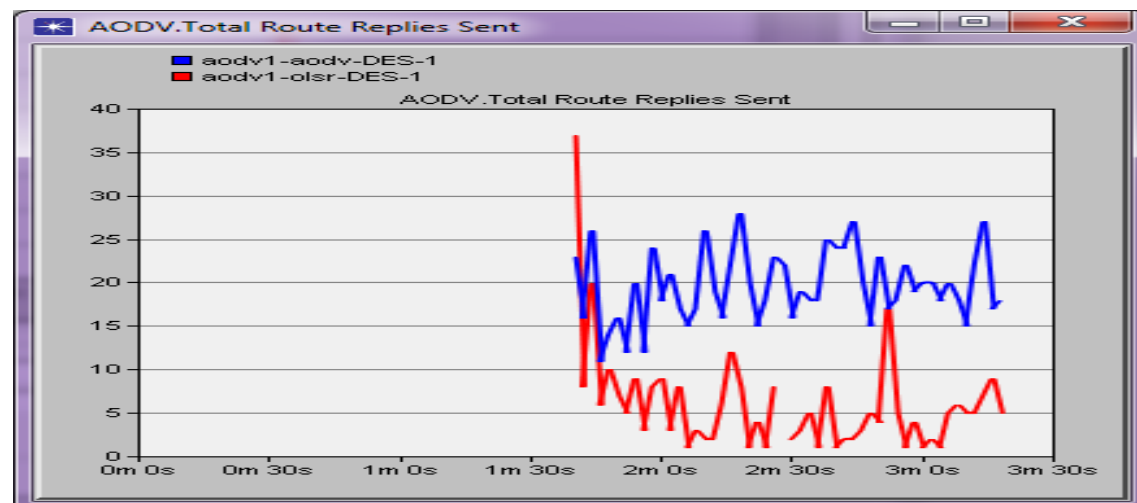


Figure IV.10. Paquets de réponse de route pour l'AODV et OLSR.

La figure IV.10 montre la variation des paquets de réponse de route pour l'AODV et OLSR, les deux graphes subissent la même variation que celles des paquets de demande de route, concernant l'AODV le taux des paquets *RREP* varie entre 10 et 27 paquets alors que pour l'OLSR départ par une valeur supérieure (37 paquets) et commence à diminuer jusqu'à 0 (presque nulle), cela résulte de mode de fonctionnement des protocoles proactifs où les nœuds possèdent déjà les routes vers les autres nœuds voisins dans leurs tables de routages et donc la destination reprend plus vite que dans AODV.

En général, le taux des paquets de réponse de route dans l'AODV est plus important qu'OLSR.

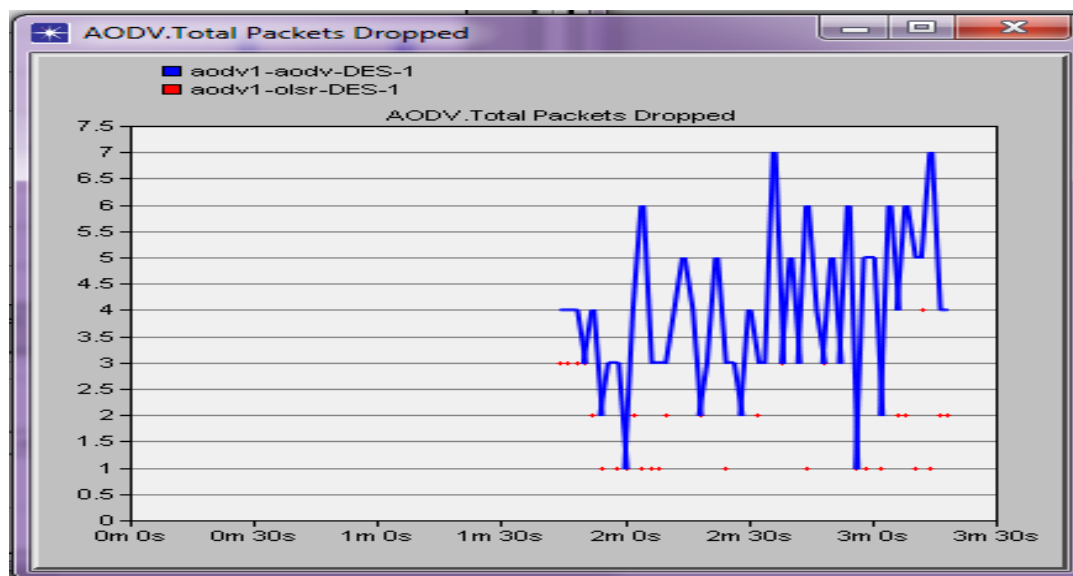


Figure IV.11. Paquets perdus pour l'AODV et OLSR.

La figure IV.11 illustre la fluctuation du taux des paquets perdus en utilisant le protocole AODV et OLSR, la différence est bien visible sur les deux courbes. Pour l'AODV, on remarque plusieurs fluctuations continues entre 1 et 7 paquets à l'intervalle [1min40s - 3min10s], par contre pour l'OLSR les paquets sont perdus d'une manière périodique par exemple à l'instant 2min0s, il y a un taux de perte égale à 1, l'OLSR a une perte presque négligeable donc il assure moyennement la préservation des paquets. AODV perd plus en plus de paquets avec le temps de simulation à cause des chemins qui ne restent plus valides en raison de la mobilité des nœuds.

En générale, l'AODV enregistre une perte de paquet considérable, tandis que dans l'OLSR la quasi-totalité des paquets arrivent à la destination même dans les fortes mobilités.

IV.3. Conclusion

Notre but, à travers les simulations effectuées était de tester les performances de notre approche "Simulation d'un réseau *MANET* avec *OPNET*" en spécifiant deux protocoles à comparer l'*AODV* et l'*OLSR*.

Dans ce chapitre nous avons pu déceler quelques écarts entre les deux protocoles simulés *AODV* et *OLSR* ainsi que d'autres entre les types de protocoles proactifs et réactifs. Ces écarts sont loin d'être exhaustifs par rapport à la réalité de ces protocoles divers et variés.

Toutefois, dans tous les scénarios simulés, nous observons la différence entre le mode de fonctionnement de ces protocoles. Cependant, nous remarquons toujours la performance de certains résultats par rapport aux autres.

Le protocole proactif *OLSR* se distingue par rapport à l'autre par sa particularité de garder à jour une table de routage. Nous avons noté qu'il commence à émettre réellement très vite après la demande, il utilise rarement le mécanisme découverte de la route. Ces routes sont toujours à disposition même dans les fortes mobilités. Par rapport aux taux d'acheminement des paquets il assure une très bonne stabilité, la pluparts des paquets arrivent à destination.

Le protocole réactif *AODV* est un peu moins performant, il craint les fortes mobilités ainsi que les flux de données importants ou il enregistre une perte de paquets considérable, il utilise beaucoup les paquets de contrôle pour établir les chemins ce qui résulte une surcharge sur le réseau.

Conclusion générale

Conclusion générale

Ces dernières années, le besoin en mobilité ne cesse d'augmenter. Les réseaux *MANETs* permettent aux usagers de communiquer et avoir accès au multimédia et aux applications temps réel tout en se déplaçant librement. Ces réseaux doivent pouvoir supporter les mêmes applications que les réseaux filaires et cela de façon transparente.

Cependant, ces réseaux souffrent d'inconvénients à la fois liés aux liens de partage du canal de transmission qui engendre un faible débit, mais également aux protocoles de routage. Notre étude est essentiellement basée sur les protocoles de routage qui sont élément indispensable pour la sélection des routes et le transfert de données ainsi ils jouent un rôle important dans l'amélioration de la qualité de service et le partage de la bande passante.

Les réseaux *MANET* doivent s'organiser automatiquement de façon à être déployables rapidement et pouvoir s'adapter aux conditions de propagation, au trafic et aux différents mouvements pouvant intervenir au sein des unités mobiles. Dans le but d'assurer la connectivité du réseau malgré l'absence d'infrastructure et la mobilité des stations, chaque nœud est susceptible d'être mis à contribution pour participer au routage et pour retransmettre les paquets d'un nœud qui n'est pas en mesure d'atteindre sa destination, tout nœud joue ainsi le rôle de station et de routeur. Chaque nœud participe donc à une stratégie de routage qui lui permet de découvrir les chemins existants, afin d'atteindre les autres nœuds du réseau.

Ce travail entre dans le cadre de l'étude du problème de routage dans les environnements mobiles caractérisés par l'absence d'infrastructure. Différentes stratégies de routage conçues pour les réseaux *MANETs* ont été étudiées. Selon la

manière de construction de chemins entre les stations sources et les stations destination, les stratégies (ou les protocoles) de routage sont divisées en trois classes : les protocoles proactifs, les protocoles réactifs et les protocoles hybrides. Les protocoles proactifs cherchent à maintenir une vue globale du réseau au niveau de chaque station afin que celle-ci puissent router les paquets de messages, alors que dans l'approche réactive une station cherche à découvrir une route avant de pouvoir communiquer. Les protocoles hybrides combinent entre ces deux approches.

A travers notre étude des différents protocoles de routage qui existent, en précisant le réactif *AODV* et le proactif *OLSR*, nous avons vu que ces protocoles utilisent une variété de techniques afin de résoudre le problème de routage dans l'environnement des réseaux *MANETs* à l'aide du simulateur *OPNET 14.0* qui nous a permis de comparer entre ces deux protocoles en se basant sur des paramètres d'évaluation. Parmi ces paramètres, on cite : la découverte de la route, les paquets de contrôle de trafic, l'acheminement des paquets envoyés et reçus, le taux des paquets perdus.

L'étude que nous avons fait nous a permis de conclure que le protocole *OLSR* est plus performant qu'*AODV* à cause de ces efficaces techniques d'acheminer les données jusqu'à la destination, chaque nœud possède une table de routage contenant des informations sur les routes disponibles à ce nœud pour transmettre ses données, ces informations sont périodiquement mises à jour ce qui réduit l'utilisation de la technique de découverte de la route ainsi que la diffusion des paquets de contrôle qui conduit à une inondation du réseau et par conséquent un taux élevé des paquets perdus, c'est le cas de l'*AODV*.

Perspectives

Durant les deux phases de notre étude théorique et pratique, nous nous sommes vite rendu compte que le domaine de recherche dans les réseaux sans fils est tout jeune et qu'il a un long chemin à parcourir. Plusieurs groupes scientifiques s'intéressent à ce type de réseaux qui promet beaucoup pour l'avenir. Plus spécialement les protocoles de routage attirent de plus en plus les simulateurs afin de combiner les meilleurs atouts de chacun d'eux en un seul. Après notre étude théorique nous avons sélectionné des propriétés afin de les simuler et trouver les écarts entre les algorithmes de routage.

Ce travail de préparation des simulations nécessite beaucoup de recherche et de développements. Notre modeste contribution a besoin d'être élargie avec des simulations sur d'autres paramètres. De nouvelles métriques de comparaisons sont à envisager pour mieux accentuer les différences. Les études de simulations sur un seul protocole auquel on apporte des changements sur son algorithme de routage pourraient nous révéler de nouvelles particularités. Ainsi, nous allons permettre aux algorithmes de progresser et les réseaux sans fils de voir de nouveaux terrains d'applications. La téléphonie sur *IP*, la visiophonie et les applications multimédias sont tous à l'attente de tels types de réseaux sans fils mais avec des bandes passantes beaucoup plus larges et des temps de réponses très courts. La majorité des applications actuelles exigent le maintien d'une qualité de service minimale.

Bibliographie & Références

Références & Bibliographie

- [1] **A. Tanenbaum**. Computer Networks. Prentice Hall PTR, 2003. ISBN : 0130661023.
- [2] **Charles E. Perkins**. *Ad Hoc* Networking. Addison-Wesley, 2001. ISBN : 0201309769.
- [3] **M. Ripeanu**. Peer-to-Peer Architecture Case Study : Gnutella Network. Technical report, University of Chicago, 2001.
- [4] IETF MANET group.
[Http : //www.ietf.org/html.charters/manet-charter.html](http://www.ietf.org/html.charters/manet-charter.html).
- [5] **Dr. N. Badache, D. Djenouri, A. Derhab, T. Lemlouma**. « Les protocoles de routage dans les réseaux mobiles Ad Hoc ».
- [6] **K. Salhi, S.Taazibt**, « Protocoles de routages pour les réseaux Ad hoc », Projet de Fin d'étude pour l'obtention du Diplôme d'ingénieur d'état en Télécommunications soutenus à l'institut National des Télécommunications et des Technologies de l'Information et de la Communication, Algérie, juin 2009.
- [7] <http://mahieus.no-ip.org/articles/print.php?id=4>
- [8] **K.Medjani, S.Bellali, Y.Mahmoud, Y.Dai**. « Les réseaux *MANETs* », Mini projet soutenus à l'université des Sciences et de la Technologie de Houari Boumediene, Algérie.
- [9] **S.J.NouhoNoutat**, «Problématique de normalisation des données de configuration dans les réseaux de capteurs sans fil : cas des protocoles de routage», Mémoire présenté en vue de l'obtention du Diplôme de Master II en informatique en l'université de Yaoundé I, Cameroun, 2011.
<http://www.lirima.uninet.cm/index.php/mediatheque/archives/telechargeables/fun-c-startdown/33/>
- [10] **R. Bellman**, «On a Routing Problem, in Quarterly of Applied Mathematics». 16(1), 1958, pp.87-90.

[11] **G. Jolly, Mustafa C.Kuşçu, PallaviKokate et M.Younis**, «A Low-Energy Key Management Protocol for Wireless Sensor Networks», Proceedings of the Eighth IEEE International Symposium on Computers and Communication ,(ISCC'03), IEEE COMPUTER SOCIETY,2003.

[12] **P.A. Bisgambiglia** , « Pourquoi modéliser un réseau ? Comment évaluer ses performances ? Présentation d'outils de modélisation », Support de Cours à Université de Corse, Pasquale PAOLI, 2008 – 2009.

[13] **A. Munaretto, H. Badis, K. Al Agha, et G. Pujolle**, «QoS-enhanced OLSR Protocol for Mobile Ad Hoc Networks». In the Proceedings of The ANWIRE 1st International Workshop, Glasgow, Ecosse, April 2003, pp 171–183.

[14] **D. B. Johnson, D. A. Maltz, et J. Broch**, «DSR The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks». In Ad Hoc Networking, edited by Charles E. Perkins, chapter 5, Addison-Wesley, pp. 139–172, 2010.

[15] **I.F. Akyildiz, W. Su, Y.Sankarasubramaniam et E.Cayirci**, «Wireless sensor networks: a survey», Computer Networks. Vol. 38(4). - pp. 393-422, 2002.

[16] **B.Sahraoui**, «Etude d'un protocole de routage basé sur les colonies de Fourmis dans les réseaux de capteurs sans fil », Mémoire de fin d'études pour l'obtention du diplôme de Master en Informatique de l'université Abou Bekr Belkaid, Tlemcen, Algérie, 2013.

<http://dspace.univ-tlemcen.dz/bitstream/112/4643/1/MEMOIRE-SAHRAOUI.pdf>

[17] **M. Erwan Ermel**, « Localisation et Routage géographique dans les réseaux sans fil hétérogènes », Université Pierre et Marie CURIE, 21 Juin 2004.

[18] **K.Chebira**, « Etude et analyse de la stabilité des protocoles de routage dans les réseaux *Ad hoc* », Mémoire présenté en vue de l'obtention du Diplôme de Magister en Informatique à l'université Hadj Lakhdar, Batna, 2007.

Résumé

Les réseaux *MANETs* (*Mobile Ad Hoc NETWORKs*) constituent une catégorie de réseaux sans fil pouvant être déployés rapidement, multi-sauts et sans infrastructure. Ces réseaux permettent la communication entre utilisateurs d'applications mobiles diverses (applications collaboratives, urgences, militaires, embarquées, *etc.*). Les travaux actuels ne se limitent pas à la conception d'une technologie sans fil adaptée aux réseaux *MANETs* et un protocole de routage extensible. Bien que d'autres recherches soient en cours dans ce domaine, il n'est pas possible de décrire dans le présent document toutes les voies de recherche en cours.

Notre travail est essentiellement basé sur les protocoles de routage dans les réseaux *MANETs* ainsi qu'une comparaison entre le protocole réactif *AODV* et le protocole proactif *OLSR* simulé avec l'outil *OPNET 14.0*, qui nous a aidés à mieux étudier les performances de ces deux protocoles.

Mots clés : *MANET*, protocoles de routage, *AODV*, *OLSR*, *OPNET 14.0*.

Abstract

MANETs (*Mobile Ad Hoc NETWORKs*) are a category of wireless networks to deploy rapidly, multihop and without infrastructure. These networks allow communication between users of various mobile applications (collaborative applications, emergency, military, embedded ...). The current work is not limited to the design of a wireless technology suitable for *MANETs* and expandable routing protocol. Since research is under constant development in this field, it is not possible to mention in this paper all the related literature avenues (*paths*).

Our work is mainly based on the routing protocols in *MANETs* as well as a comparison between the reactive protocol *AODV* and proactive protocol *OLSR* simulated with *OPNET 14.0* tool that has helped us to better study the performance of these two protocols.

Keywords: *MANET*, routing protocols, *AODV*, *OLSR*, *OPNET 14.0*.