



REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE



MINISTRE DE L'ENSEIGNEMENT SUPERIEUR
ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE ABOU BAKR BELKAID-TLEMCEM
FACULTE DE TECHNOLOGIE
DEPARTEMENT DU GENIE ELECTRIQUE ET ELECTRONIQUE

MEMOIRE DE FIN D'ETUDE POUR L'OBTENTION DE DIPLOME DE MASTER
EN
TELECOMMUNICATIONS
OPTION
PHOTONIQUE ET RESEAUX OPTIQUES DE TELECOMMUNICATIONS

THEME

***ETUDE ET EVALUATION DES
PERFORMANCES DU RESEAU WIFI MESH
(802.11S)***

Soutenu le 01 juillet 2013

Présenté par :

Melle. BOUATIA Wassila
Melle. MEZIANE TANI Fadia Selma

Devant les membres du jury composés de :

Mr. BAHRI Sid Ahmed	Maitre de conférences classe «B »	Président
Mr. BORSALI Ahmed Riad	Maitre de conférences classe « A »	Examineur
Mr. MERZOUGUI Rachid	Maitre de conférences classe « A »	Examineur
Mr. BOUABDALLAH Réda	Maitre assistant classe « A »	Encadreur
Mr. BENMOUSSAT Chemseddine	doctorant	Co-Encadreur

Année universitaire : 2012– 2013

*A cœur vaillant rien d'impossible
A conscience tranquille tout est accessible*

*Quand il y a la soif d'apprendre
Tout vient à point à qui sait attendre*

*Quand il y a le souci de réaliser un dessein
Tout devient facile pour arriver à nos fins*

*Malgré les obstacles qui s'opposent
En dépit des difficultés qui s'interposent*

*Les études sont avant tout
Notre unique et seul atout*

*Ils représentent la lumière de notre existence
L'étoile brillante de notre réjouissance*

*Comme un vol de gerfauts hors du charnier natal
Nous partons ivres d'un rêve héroïque et brutal*

*Espérant des lendemains épiques
Un avenir glorieux et magique*

*Souhaitant que le fruit de nos efforts fournis
Jour et nuit, nous mènera vers le bonheur fleuri*

*Aujourd'hui, ici rassemblés auprès des jurys,
Nous prions dieu que cette soutenance
Fera signe de persévérance
Et que nous serions enchantés
Par notre travail honoré*



Remerciements



La rédaction de ce mémoire et sa soutenance marquent la fin d'une aventure à plusieurs facettes : aventure dans le monde des études, aventure humaine, aventure familiale. Différentes personnes nous ont accompagnées tout au long de ce parcours et nous tenons ici à remercier :

& En premier lieu notre DIEU le tout puissant, de nous avoir accordé vie, santé et paix de l'esprit sans quoi nous n'aurions pu achever ce modeste travail.

& Notre encadreur Mr BOUABDALLAH Réda maitre assistant classe « A » à l'université ABOU BAKR BELKAID, Tlemcen pour ses conseils et pour nous avoir honorés en acceptant de diriger ce travail.

& Notre Co-encadreur Mr BENMOUSSET Chemseddine doctorant à l'université ABOU BAKR BELKAID, Tlemcen d'avoir accepté de nous Co-encadrer et de nous avoir guidé.

& Mr BAHRI Sid Ahmed maitre de conférences classe «B » à l'université ABOU BAKR BELKAID, Tlemcen qui nous a honorés en acceptant de présider notre honorable jury.

& Mr BORSALI Ahmed Riad, Maitre de conférences classe « A » à l'université ABOU BAKR BELKAID, Tlemcen d'avoir eu l'amabilité d'accepter de juger notre travail.

Monsieur, nous avons toujours admiré vos qualités humaines et professionnelles ainsi que votre compétence et votre disponibilité chaque fois que vous étiez sollicités

Veillez accepter, cher Maître, l'assurance de notre estime et profond respect.

& Mr Merzougui Rachid, Maitre de conférences classe « A » à l'université ABOU BAKR BELKAID, Tlemcen de siéger parmi notre honorable jury. Vos qualités humaines et professionnelles ainsi que votre modestie qui restent exemplaires, ont suscité en nous une grande admiration et un profond respect Pour vous.

Nos plus sincères remerciements vont à tous ceux qui ont contribué à l'aboutissement de ce travail, nous citerons en l'occurrence tout le corps des enseignants et à leur tête notre professeur CHIKH BLED Mohammed responsable de la formation PROTONS (Photoniques et Réseaux Optiques de TélécommunicatiONS), sans le savoir que vous nous avez inculqués durant ces années universitaires nous n'aurions pu réaliser tout ceci.



Dédicaces



Par la grâce de dieu Je dédie ce travail . . . ✍

À MES CHERS PARENTS

Aucune dédicace ne saurait exprimer mon respect, ma reconnaissance, mon amour éternel et ma considération pour les sacrifices que vous avez consentis pour mon instruction et mon bien être, Votre joie et votre gaieté me comblent de bonheur.

A ma très chère mère Nadjet

Autant de phrases aussi expressives soient-elles ne sauraient montrer le degré d'amour et d'affection que j'éprouve pour toi.

Tu as fait plus qu'une mère puisse faire pour que ses enfants suivent le bon chemin dans leur vie et leurs études.

Tu m'as comblée avec ta tendresse et ton affection tout au long de mon parcours. Tu n'as cessé de me soutenir et de m'encourager durant toutes les années de mes études, tu as toujours été présente à mes côtés pour me consoler quand il fallait. Ta prière et ta bénédiction m'ont été d'un grand secours pour mener à bien mes études.

En ce jour mémorable, pour moi ainsi que pour toi, Je te dédie ce modeste travail en témoignage de mon profond amour. Puisse Dieu, le tout puissant te donner santé, bonheur et longue vie afin que je puisse te combler à mon tour

A mon très cher Père Ismail

Aucune dédicace ne saurait exprimer l'amour, l'estime, la gratitude, la reconnaissance et le respect que j'ai toujours eu pour toi.

Tu as su m'inculquer le sens de la responsabilité, de l'optimisme et de la confiance en soi face aux difficultés de la vie. Tes conseils ont toujours guidé mes pas vers la réussite. Ta patience sans fin, ta compréhension et ton encouragement sont pour moi le soutien indispensable que tu as toujours su m'apporter.

Toi, qui a cru en moi et qui m'a donné les moyens d'aller aussi loin, Je te dois ce que je suis aujourd'hui et ce que je serai demain et je ferai toujours de mon mieux pour rester ta fierté et ne jamais te décevoir. Que Dieu le tout puissant te préserve, t'accorde santé, bonheur, quiétude de l'esprit et te protège de tout mal.

A MON ADORABLE FRÈRE NADIR

En souvenir d'une enfance dont nous avons partagé les meilleurs et les plus agréables moments. Pour toute la complicité et l'entente qui nous unissent, Je te dédie ce travail avec tous mes vœux de bonheur, de santé et de réussite et que le dieu, le tout puissant, te protège et te garde.

A MA TRÈS CHÈRE GRAND MÈRE MATERNELLE

Malgré la distance, tu es toujours dans mon cœur. Je te remercie pour ton hospitalité sans égal et ton affection si sincère, pour tes prières qui m'ont accompagnée, pour ta douceur. Que Dieu te prête longue vie, santé et de beaucoup de bonheur.

A LA MÉMOIRE DE MES GRAND-PÈRES ET MA GRANDE MÈRE PATERNELLE

Qui ont été toujours dans mon esprit et dans mon cœur, je vous dédie aujourd'hui ma réussite. Que Dieu, le miséricordieux, vous accueille dans son éternel paradis.

À MES CHÈRES ONCLES, TANTES, A MES CHÈRES COUSINS COUSINES

Vous avez toujours été présents pour les bons conseils. Veuillez trouver dans ce modeste travail ma reconnaissance pour tous vos efforts.

A MA TRÈS CHÈRE COUSINE MANEL

Ma confidente, mon amie et ma sœur. Je t'aime tant

A MON TRÈS CHER BINÔME FADIA

Ma sœur, ma très chère amie, ma confidente, khbiza ta3i que j'adore et avec laquelle j'ai partagé beaucoup d'émotion, de complicité aussi bien dans notre travail scientifique et la vie quotidienne, mes sentiments restent éternels.

A MON INTIME DOUNIAZED

Amie fidèle, sœur, qui m'a assistée dans les moments difficiles et m'a prise doucement par la main pour traverser ensemble des épreuves pénible....Je te suis très reconnaissante, et je ne te remercierai jamais assez pour ton amabilité, ta générosité, ton aide précieuse.

À MES AMIS DE TOUJOURS :

Houria, Hanene, Khawla, Dounyazed, Yasmine, Imen, Samir et Hichem.

A TOUTE LA PROMOTION PROTONS

Wassila...

Par la grâce de dieu, je dédie ce modeste travail... ✍

À MES TRÈS CHERS PARENTS

Aucune dédicace ne saurait exprimer mon respect, mon amour éternel et ma considération pour les sacrifices que vous avez consenti et les efforts que vous avez fournis jour et nuit pour mon instruction, mon éducation et mon bien être.

MAMAN

Autant de phrases et d'expression aussi éloquente soient-elles ne sauraient montrer le degré d'amour et de reconnaissance que j'éprouve pour toi Ma maman chérie. Ma conseillère, et amie fidèle, qui m'a assistée dans les moments difficiles, Tu représentes pour moi le symbole de la bonté par excellence, tu m'as comblée avec ta tendresse et affection tout au long de ma vie. Tu n'as cessé de me soutenir, de m'encourager et de prier pour moi durant toutes les années de mes études, tu as toujours été présente à mes cotés pour me consoler quand il le fallait.

PAPA

Toutes les lettres ne sauraient trouver les mots qu'il faut, Tous les mots ne sauraient exprimer la gratitude, L'amour, le respect et la reconnaissance pour ton affection, pour tous les sacrifices consentis, pour l'éducation que tu m'as donnée et pour tous les efforts que tu ne cesse de fournir pour ma réussite.

Que ce modeste travail soit l'exaucement de vos vœux tant formulés, le fruit de vos innombrables sacrifices, bien que je ne vous en acquitterai jamais assez. Puisse Dieu, le Très Haut, vous accorder santé, bonheur et longue vie et faire en sorte que jamais je ne vous déçoive.

À Mon Adoré

Mon très cher frère NADIR, les mots ne me suffisent guère pour exprimer l'attachement, l'amour l'affection et la profonde tendresse que je te porte. Tes encouragements et ton soutien étaient la bouffée d'oxygène qui me ressourçait dans les moments difficiles. Je te souhaite une vie pleine de bonheur et de succès. Que dieu le tout puissant te garde et te protège.

À Ma très chère grand Mère maternelle

Qui n'a jamais cessé de prier pour moi, exemple de sagesse de douceur de générosité et de bonté sans égale. Elle a toujours fait passer notre bonheur avant le sien, puisse Dieu lui prêter santé et longue vie.

À LA MEMOIRE DE MES chers Grands-parents paternels, Mon cher Grand Père maternel ET Mon très cher Oncle Maternel

J'aurais tant aimé que vous soyez présents à mes cotés. Vous Me manquez Tant. Que Dieu ait vos âmes dans son vaste paradis.

À Mon cher oncle Mokhtar

À Toi khay Mokhtar, l'homme au grand cœur, je te souhaite un prompt rétablissement, et une longue vie. Tu mérites tout le bien du monde, tu es non seulement mon oncle mais aussi mon deuxième papa. Que dieu te garde.

À MES CHERS ONCLES, TANTES, COUSINS ET COUSINES

*En particulier mamans : **NACERA**, HAFEDA, NORIA et NABAHAT qui ont toujours su admirablement jouer le rôle d'une seconde mère pour moi. Je vous aime tant.*

Veillez tous trouver dans ce travail l'expression de mon respect le plus profond et mon affection la plus sincère.

À MES cousines chéries

*IKRAM, MIMI, SOUAD, MANEL, **YASMINA**, NESRINE, NARIMANE, INES.*

Que je porte profondément dans mon cœur vous êtes non seulement mes cousines mais aussi mes amies et mes sœurs. je vous aime.

À Mon cher binôme WASSILA

Plus qu'un binôme, tu es une sœur pour moi nous avons partagé ensemble les moments les plus difficiles toujours la pour moi pour partager mes joies et mes peines je t'adore ELBII. je te souhaite un avenir radieux ainsi qu'à toute la famille Bouatia.

*À MES chers AMIS : YASMINE, DOUNIA, ASMA.S, ESMA.L,
DOUNIA.B, IMANE, HOURLA, HICHAM, SAMIR,*

À toute la promotion PROTONS (Photoniques et Réseaux Optiques de Télécommunications).

FADIA M.T

Sommaire

Introduction générale	1
Chapitre I : La norme 802.11s	
I.1.Introduction	4
I.2.Définition	4
I.3.Architecture des réseaux maillés sans fil	5
I.3.1.Architecture client	5
I.3.2. Architecture en infrastructure « backbone »	6
I.3.3.Architecture Hybride	7
I.4. Les caractéristiques des réseaux aillés sans fil	8
I.5. Fonctionnement du Wifi maillé IEEE 802.11s	10
I.5.1. Couche physique	10
I.5.1.1La sous couche PLCP	10
I.5.1.2 La sous couche PMD	11
I.5.2. Couche liaison de données	13
I.5.2.1 La sous couche LLC	13
I.5.2.2 La sous couche MAC	13
I.5.3. Couche réseau	16
I.6. Les applications des réseaux maillés sans fil	17
I.7. Avantages des réseaux maillés sans fil	23
I.8. Inconvénients des réseaux maillés sans fil	23
I.9. Conclusion	24
Chapitre II : Routage et QOS dans les WMNs	
II.1. Introduction	26
II.2. Routage	26
II.2.1. Définition du routage	26

II.2.2. Problématique et contrainte du routage dans le réseau Wifi maillé	26
II.2.3. Les objectifs des protocoles de routage dans les réseaux maillés sans fil	27
II.2.4. notions sur le routage dans les réseaux maillés sans fil	28
II.2.4.1. L'inondation	28
II.2.4.2. Multihopping	28
II.2.4.3. Le concept de groupe	29
II.2.5. Les méthodes de routage	29
II.2.5.1. Routage à vecteur de distance	30
II.2.5.2. Routage à état des liens	30
II.2.5.3. Routage par la source	31
II.2.5.4. Routage Saut par saut	31
II.2.6. Classification des protocoles de routage	31
II.2.6.1. Selon le moment d'établissement de route	32
II.2.6.1.1. Les protocoles de routage proactifs	32
II.2.6.1.2. Les protocoles de routage réactifs	32
II.2.6.1.3. Les protocoles de routage hybrides	33
II.2.6.2. Selon la participation des nœuds dans le routage	34
II.2.6.2.1. Les protocoles uniformes	34
II.2.6.2.2. Les protocoles non uniformes	34
II.2.7. Exemples de protocoles de routage	35
II.2.7.1. Le protocole de routage proactif OLSR	35
II.2.7.2. Le protocole de routage proactif DSDV	36
II.2.7.3. Le protocole de routage réactif DSR	37
II.2.7.4. Le protocole de routage réactif AODV	38
II.2.7.5. Le protocole de routage hybride ZRP	39
II.3. Qualité de service	40
II.3.1. Définition de la qualité de service	40
II.3.2. Les classes de services	40

II.3.3. Niveaux de service	41
II.3.4. paramètres de la qualité de service	41
II.3.5. La QOS dans les réseaux maillés sans fil	42
II.4. Conclusion	43

Chapitre III : Etude comparative entre les protocoles AODV et DSR

III.1. Introduction	45
III.2. Motivation	45
III.3. Etude des Protocoles de routage	46
III.3.1. Le protocole AODV	46
III.3.1.1. Tables de routage et paquets de contrôle	47
III.3.1.2. Gestion des numéros de séquence	49
III.3.1.3. La découverte de route	50
III.3.1.4. La maintenance de route	52
III.3.1.5. Analyse du protocole AODV	53
III.3.2. Le protocole DSR	53
III.3.2.1. La découverte de route	54
III.3.2.2. La maintenance de route	56
III.3.2.3. Analyse du protocole DSR	57
III.3.3. Comparaison entre les protocoles AODV et DSR	58
III.4. Conclusion	60

Chapitre IV : Analyse et simulation

IV.1. Introduction	62
IV.2. Présentation du simulateur NS2	62
IV.2.1. Généralité	62
IV.2.2. Principe de base	63
IV.2.3. Visualisation des résultats	64

IV.2.3.1. Fichier trace	64
IV.2.3.2. Interface graphique NAM	65
IV.2.3.3. L'Interface XGRAPH	66
IV.2.4. Comment créer un scénario de simulation avec NS2.29	66
IV.2.5. Composition d'un modèle en NS	67
IV.2.6. Principaux composants disponible dans NS	68
IV.3. Simulation et interprétation des résultats	68
IV.3.1. Modèle de simulation	68
IV.3.2. Modèle de trafic	68
IV.3.3. Métrique	69
IV.3.3.1. Taux de perte des paquets	69
IV.3.3.2. Délai moyen de transfert des paquets	69
IV.3.3.3 Le débit	69
IV.3.4. Scénario de simulation	69
IV.3.5. Résultats et discussion	70
IV.4 proposition d'un protocole hybride entre AODV et DSR (ODSR)	76
IV.5 Problèmes rencontrés et perspectives :	78
IV.5. Conclusion	78
Conclusion générale	79

Liste des figures

Figure I.1. Réseau maillé sans fil (WMN)	5
Figure I.2. Architecture client d'un WMN	6
Figure I.3. Architecture en infrastructure d'un WMN	7
Figure I.4. Architecture hybride d'un WMN	8
Figure I.5 : Principe de la technique FHSS	11
Figure I.6 : principe de la technique DSSS	12
Figure I.7 : Principe de la technique OFDM	12
Figure I.8 : accès au support CSMA/CA	15
Figure I.9 : station cachée	15
Figure I.10 : réservation du support avec les trames RTC/CTC	16
Figure I.11 : réseau maillé sans fil domestique	17
Figure I.12 : réseau maillé sans fil de communauté	18
Figure I.13 : réseau maillé sans fil d'entreprise	19
Figure I.14 :réseau maillé sans fil pour une zone public	20
Figure I.15 : Infrastructure de connexion internet via wifi mesh	21
Figure I.16 : Les applications multimédia	22
Figure II.1. l'hôte S envoie des informations par inondation	28
Figure II.2. Le multihopping dans les réseaux maillés	29
Figure II.3. La décomposition du réseau en groupes	29
Figure II.4. Classification des protocoles de routage	34
Figure II.5. Exemple de routage dans le DSR	38
Figure II.6. Zone de routage	39
Figure III.1. Fonctionnement du protocole AODV	47
Figure III.2. Format général d'une route request (RREQ)	49
Figure III.3. Format général d'une route Reponce (RREP)	49
Figure III.4. Inondation de RREQ et renvoie du RREP dans AODV	51
Figure III.5. Coupure de route et envoie du RERR dans AODV	52

Figure III.6. Découverte de route dans le protocole DSR	55
Figure IV.1. Création de topologie sous NAM/NS2	65
Figure IV.2. Exemple d'un graphe obtenu grâce à l'interface XGRAH	66
Figure IV.3 : Le délai de transfert pour V=4Km/h	70
Figure IV.4 : Le délai de transfert pour V=30km/h	71
Figure IV.5 : Le taux de perte des paquets pour V=4Km/h	72
Figure IV.6 : Le taux de perte des paquets pour V=30Km/h	73
Figure IV.7 : Le débit pour V= 4 km/h	74
Figure IV.8 : Le débit pour V=30Km/h	75

Liste des tableaux

Tableau III.1. Tableau comparatif	59
Tableau III.2. résumé des avantages et des inconvénients	60
Tableau IV.1.Principaux composants actuellement disponible dans NS	68
Tableau IV.2. Le délai de transfert pour $V=4\text{km/h}$	70
Tableau IV.3 : Le délai de transfert pour $V=30\text{km/h}$	70
Tableau IV.4 : Le taux de perte des paquets pour $V=4\text{Km/h}$	72
Tableau IV.5 : Le taux de perte des paquets pour $V=30\text{Km/h}$	72
Tableau IV.6 : Le débit pour $V= 4\text{Km/h}$	74
Tableau IV.7 : Le débit pour $V=30\text{Km/h}$	75

Abréviations

A

AODV Ad-Hoc On Demand Distance Vector

C

CSMA/CA Carrier Sense Multiple Access with Collision Avoidance

CTS Clear To Send

D

DIFS Distributed Inter Frame Space

DSDV Destination Sequence Distance Vector

DSL Digital SubscriberLines

DSR Dynamic Source Routing

DSSS Direct Sequence Spread Spectrum

F

FAI Fournisseur d'Accès Internet

FHSS Frequency Hopping Spread Spectrum

I

IARP IntrazoneRouting Protocol

IERP Interzone Routing Protocol

L

LLC Logical Link Control

M

MAC Medium Access Control

MPR RelaisMultiPoint

N

Nam	Network Animator
NS2	Network Simulator 2
O	
OFDM	Orthogonal Frequency Division Multiplexing
OLSR	Optimized Link State Routing
P	
PCF	Physical Carrier Sense
PLCP	Physical Layer Convergence Protocol
PMD	Physical Medium Dependent
Q	
QOS	Quality Of Service
R	
RERR	Route Error
RMSF	Réseau Maillé Sans Fil
RREP	Route Reply
RREQ	Route Request
RTS	Ready To Send
S	
SN	Sequence Number
T	
TC	Topology Control
TCL	Tool Command Language
TTL	Time To Live
V	
VCS	Virtuel Carrier Sens

W

Wi-Fi

Wireless Fidelity

WLAN

Wireless Local Area Network

WMC

WirelessMesh client

WMN

WirelessMesh Network

WMR

WirelessMesh Router

Z

ZRP

Zone Routing Protocol

Introduction général :

Ces dernières années, les réseaux sans fils ont connus une grande évolution et une large utilisation dans notre vie quotidienne.

Les entreprises et les gouvernements déploient les réseaux sans fils qui, grâce à leurs simplicités et souplesse d'une part, ainsi que leur coût et leur débit d'autre part, rendent l'accès au réseau plus confortable aux utilisateurs. En effet, les équipements sans fil sont moins chers comparés au filaire et permettent d'économiser le coût de câblage dans les bâtiments.

Les WLAN offrent aux utilisateurs la possibilité de se déplacer tout en restant connecté pour peu qu'ils se trouvent dans la zone de couverture du point d'accès. Ces réseaux sont faciles et rapides à déployer et permettent, en plus de la transmission de données, d'autres applications telles que la voix, la vidéo et l'Internet.

Cependant, comme les utilisateurs sont de plus en plus exigeant en terme de mobilité, l'idée d'étendre la zone de couverture d'un réseau WLAN est récemment adressée par les chercheurs. Cette idée a donné naissance à un nouveau type de réseaux : les réseaux mesh sans fil.

En effet, dans un réseau mesh sans fil, le nœud mobile n'est plus obligé d'être à proximité d'un point d'accès, comme dans les réseaux WLAN, puisque son trafic peut être relayé par les nœuds intermédiaires situés entre lui et le routeur mesh. Par conséquent, il est possible de déployer un réseau à large zone de couverture avec un coût réduit.

Le réseau maillé sans fil est une solution prometteuse, vu ses caractéristiques telles que l'architecture, les technologies et les techniques utilisées, qui représentent les facteurs clés de sa réussite. Une partie importante de cette solution est le routage, qui est en cours de développement et de recherche pour trouver le protocole de routage le mieux adapté pour améliorer les performances du wifi mesh.

L'objectif de notre étude est de résoudre certaines limitations rencontrées à l'heure actuelle dans les WMN et d'améliorer la QOS (délai, perte de paquet, débit) des applications multimédia temps-réel en évaluant et en essayant de rendre plus performants les différents protocoles de routage, appliqués aux réseaux maillés sans fil, ainsi que tirer des conclusion et des propositions pour la solution idéal.

Pour cela notre travail a été effectué comme suit :

Le premier chapitre est consacré à une étude détaillée sur les WMN, (leurs architecture, caractéristiques, applications, fonctionnement).

Dans le second chapitre nous étudions les protocoles de routages utilisés dans les réseaux maillés ainsi que la qualité de service.

Dans le 3eme chapitre nous allons nous intéresser plus particulièrement aux deux protocoles de routages AODV et DSR.

Le dernier chapitre contient une présentation du simulateur NS2, avec une comparaison des protocoles AODV et DSR et nous concluons nos tests par un modèle que nous proposons et des perspectives.

CHAPITRE I :
LE RESEAU WIFI MESH
(802.11S)

I.1. Introduction :

Les technologies sans fil connaissent ces dernières années un essor prodigieux, ce qui a favorisé une utilisation massive d'appareils mobiles tels que les téléphones intelligents, les ordinateurs portables etc. Ces technologies ont permis la mise en place de réseaux de télécommunications sans fil à large bande avec une large couverture comme les réseaux maillés sans fil (RMSF). En phase de recherche depuis quelques années, les RMSF sont une nouvelle classe de réseau sans fil. Comme leurs noms l'indiquent, ce sont des réseaux basés sur une ou plusieurs technologies sans fil telles qu'IEEE 802.11 (WLAN) et IEEE 802.16 (WIMAX). Ces réseaux ont une architecture maillée où tous les routeurs sont connectés de proche en proche sans hiérarchie centrale et où chaque nœud peut jouer le rôle d'émetteur, de récepteur ou de relai. Ainsi, chaque communication entre une source et une destination se fait à travers un acheminement à plusieurs sauts.

Les RMSF conviennent à tout type d'environnement. Ils peuvent bien être déployés sur de petites surfaces comme des maisons ou sur de plus grandes surfaces telles que des campus, des entreprises, ou même des villes entières. L'un des plus grand avantage de l'utilisation des RMSF, est que ces technologies offrent des liaisons à hauts débits. De plus, ces environnements mobiles offrent une grande flexibilité d'emploi, en particulier ils permettent la mise en réseau de sites pour lesquels le câblage serait trop onéreux ou complexe à déployer, voire même impossible.

I.2. Définition :

Un réseau maillé sans fil(WMN pour Wirless Mesh Network en anglais) est un réseau de communication qui se distingue d'un réseau local sans fil (WLAN) par le fait que le réseau maillé possède des routeurs d'accès (appelés aussi routeurs maillé) au lieu que de simple points d'accès [1].

Il est constitué d'un ensemble d'équipement informatique sans fil interconnectés entre eux sans hiérarchie centralisée, formant une stucture de maillage. la topologie des WMN est constituée de trois éléments : des clients maillés, des routeurs maillés et des passerelles (voir figure I.1).

- Les clients sont les équipements mobiles (qui peuvent être des ordinateur portable, notebook, PDA, ...) qui se connectent au réseau maillé.

- Les routeurs maillés forment l'épine dorsale du réseau maillé; ils relaient le trafic entre les clients et la passerelle.
- La passerelle est l'élément de sortie du réseau, elle permet l'accès aux différentes technologies sans fil (internet, GSM, Wimax...etc) [2].

Les routeurs du réseau maillé sans fil sont capables de s'auto configurer et s'organiser dynamiquement avec la possibilité de l'établissement et du maintien automatique des connexions et la déconnexion de relais. Lorsqu'un routeur est activé, il scrute l'environnement radio et se connecte au routeur le plus proche.

La communication entre les nœuds est basée sur le principe de multi-saut, d'où plusieurs nœuds intermédiaires participent intelligemment dans la retransmission des informations jusqu'à destination [1].

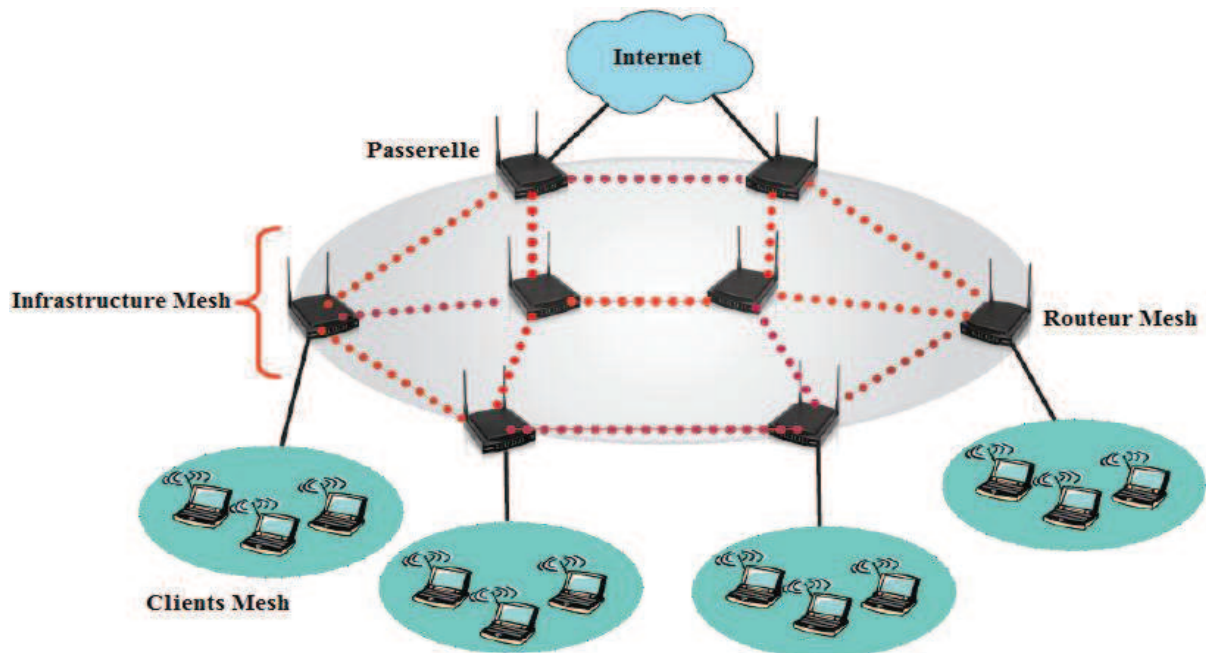


Figure I.1 : réseau maillé sans fil (WMN)

I.3. Architecture des réseaux maillés sans fil :

L'architecture des WMN est classifiée selon trois types : architecture client, architecture en infrastructure "backbone" et architecture hybride.

I.3.1. L'architecture client :

Elle est constituée des nœuds clients seulement. Ceux-ci jouent un double rôle : utilisateur final et routeur. Cette architecture permet une communication "Point à Point" à

travers tous les nœuds du réseau. Ce type de réseaux est plus similaire aux réseaux conventionnels ad hoc puisqu'une seule technologie radio est utilisée. Cependant, ces nœuds clients doivent être équipés par plus de logiciels et de matériels pour supporter le routage [3].

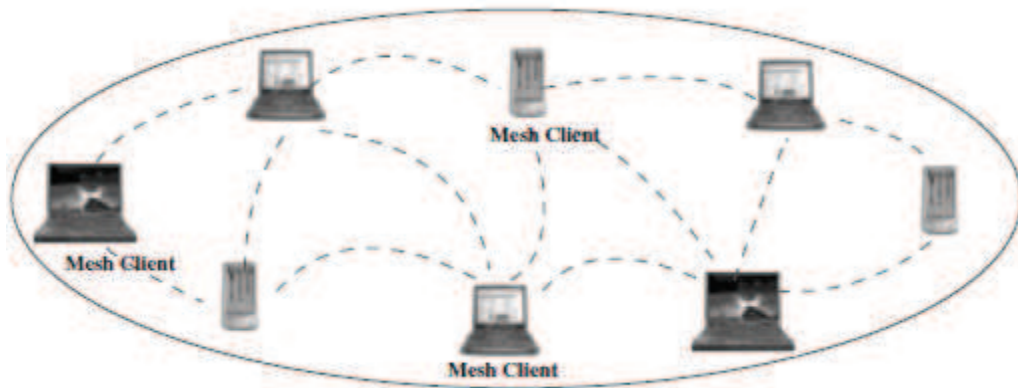


Figure I.2 : architecture client d'un WMN

1.3.2. l'architecture en infrastructure "backbone" :

Dans ce type d'architecture, nous trouvons deux niveaux, le premier niveau se compose des clients maillés et le second des routeurs maillés. En effet, le maillage se fait au niveau des routeurs, ces derniers forment l'épine dorsale (le backbone), vu qu'ils ont les caractéristiques d'être fixes ou d'une mobilité très réduite, qu'ils n'ont pas de contraintes énergétiques, et permettent aussi de maintenir la connectivité entre les différents clients. Un routeur maillé équipé d'une passerelle, peut intégrer des fonctionnalités d'accès à plusieurs réseaux assurant ainsi l'interconnexion entre eux .

En outre, les nœuds clients (WMC : Wireless Mesh Client) forment le maillage au niveau bas. N'importe quel équipement conventionnel peut être un client maillé. Ils peuvent être mobiles ou stationnaires, connectés de façon directe aux routeurs.

La particularité du réseau maillé au niveau de l'infrastructure résulte dans la connectivité de réseaux sans fil dans de vastes espaces, où le déploiement de points d'accès avec des réseaux filaires serait techniquement / économiquement impossible, comme par exemple dans une partie d'une ville, des ports de plaisance, des terrains de golf...etc.

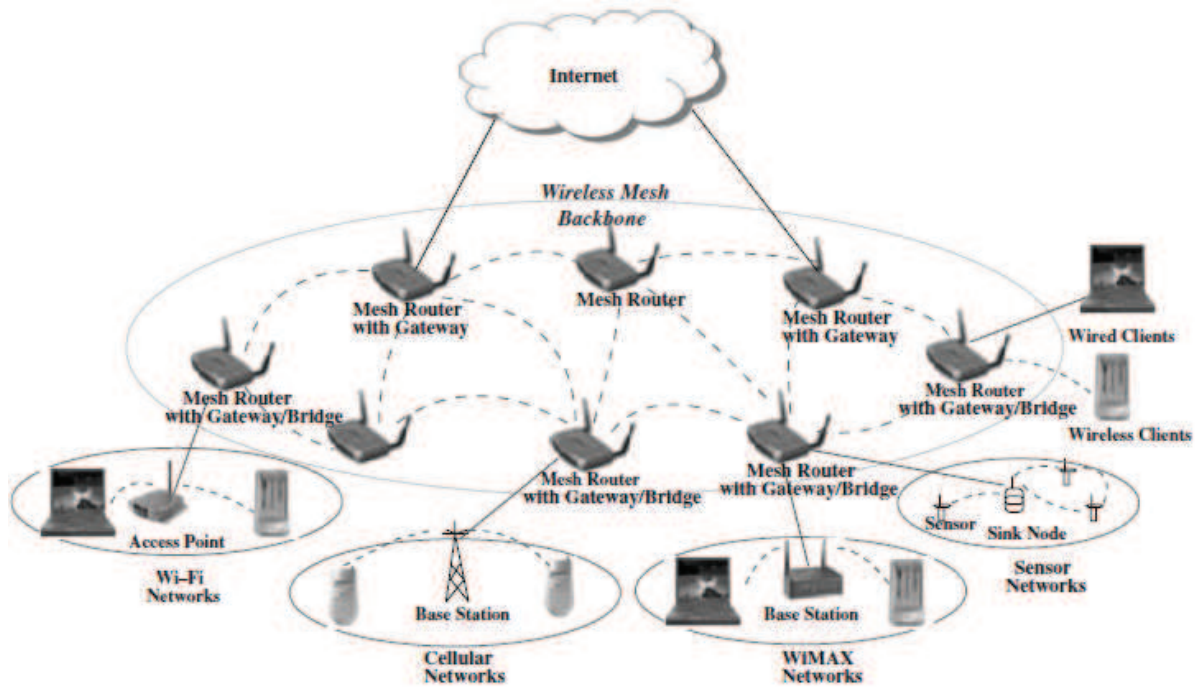


Figure I.3 : architecture en infrastructure d'un WMN

I.3.3. L'architecture hybride :

Cette architecture est la combinaison entre la première et la deuxième architecture (comme il est indiqué dans la figure I.4). Les clients maillés peuvent accéder au réseau par l'intermédiaire des routeurs ou bien directement avec d'autres clients, tandis que l'infrastructure fournit la connectivité à d'autres réseaux tels que le réseau internet, Wifi, WIMAX ou GSM [6].cette combinaison donne plus de solutions dans le calcul des routes, ce qui augmente les performances du réseau étudié.

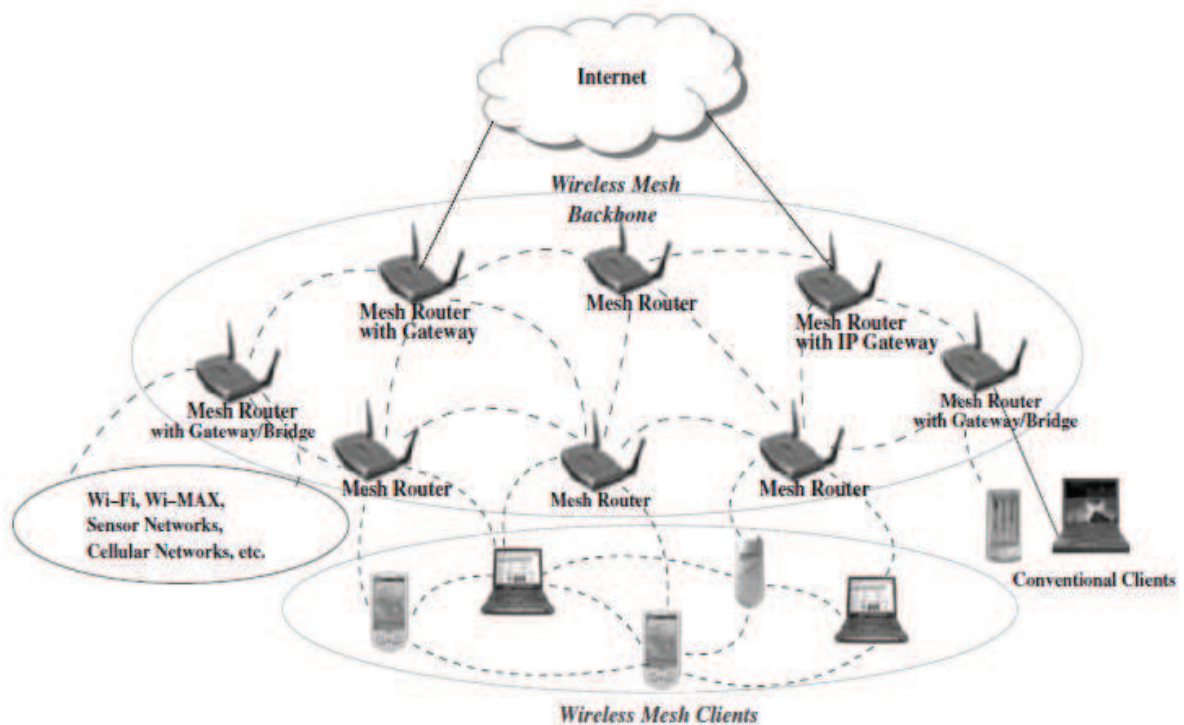


Figure I.4 : Architecture hybride d'un WMN

I.4 Les caractéristiques des réseaux maillés sans fil :

Les architectures sans fil maillées ont une approche différente des réseaux sans fil déjà existants. Elles portent de nombreuses caractéristiques :

- *Réseau multi sauts :*

L'objectif principal des réseaux maillés est d'élargir la zone de connectivité (couverture) offerte par les autres types de réseaux sans fil sans sacrifier la capacité du réseau.

Dans un réseau en multi sauts, deux nœuds qui ne sont pas liés directement peuvent communiquer par l'intermédiaire des nœuds qui assurent le routage saut par saut. Cette caractéristique permet à un nœud d'atteindre la totalité des nœuds du réseau [5].

Par conséquent, le multi saut est indispensable pour réaliser cet objectif, il offre un débit important en utilisant des liens de courtes distances et qui présentent moins d'interférence et en déployant des canaux de transmission différents [4].

- *Support des fonctionnalités des réseaux ad hoc :*

Les réseaux maillés améliorent les performances des réseaux ad hoc par la flexibilité de l'infrastructure, le déploiement facile, la tolérance à la rupture de lien, la connectivité et la

communication multipoint à multipoint. De ce fait, l'installation et l'extensibilité d'un réseau maillé sont faciles [4]. En plus de cela ils ont d'autres fonctionnalités essentielles comme, la capacité d'auto-configuration et d'auto-organisation.

- *La mobilité :*

La mobilité dans les réseaux maillés varie selon le type de nœud : les routeurs maillés ont généralement une mobilité très réduite, tandis que les clients peuvent être stationnaires ou mobiles.

- *La contrainte d'énergie dépend du type de nœuds :*

Le problème d'énergie n'est pas cruciale pour les réseaux maillés, vue que les routeurs qui forment le squelette du réseau sont branchés aux ressources énergétiques, par contre les clients mobiles souffrent toujours de ce problème [5].

- *Compatibilité et interopérabilité :*

Les réseaux maillés basés sur les technologies IEEE802.11 donnent la possibilité de supporter les clients conventionnels wifi. Ils doivent aussi inter-opérer avec d'autres technologies sans fil comme le wimax ou le zigbee.

Les WMN contiennent de nombreuses différences par rapport aux réseaux ad hoc. Toutefois, les réseaux ad hoc peuvent être considérés comme un sous-ensemble de WMN.

Plus précisément, les techniques existantes développées pour les réseaux Ad- hoc sont déjà applicables aux WMN, a titre d'exemple les protocoles de routages que nous allons détailler dans le chapitre II.

- *La qualité de service :*

Les réseaux maillés sans fil permettent d'intégrer plusieurs technologies sans fil et ont donc pour vocation de jouer le rôle d'un réseau d'accès vers l'Internet ou vers différents types de réseaux sans fil. Ils sont donc amenés à être le support de communication d'une grande diversité d'applications ayant des exigences différentes de qualité de service (QoS). Ces besoins peuvent être exprimés en termes de débit, délai ou taux de perte. Les réseaux ad hoc trouvent des difficultés pour garantir une QoS minimale à cause des problèmes de mobilité, partage de la bande passante et limitation des ressources. Par ailleurs, les réseaux Wifi souffrent aussi des problèmes de liaison filaire entre les points d'accès. De ce fait les réseaux maillés sans fil semblent plus adaptés pour offrir la QoS. En effet, les réseaux maillés sont

caractérisés par une infrastructure partiellement stable à l'inverse des réseaux ad hoc où les nœuds sont constamment mobiles.

- *Plusieurs interfaces de transmission radio :*

Les routeurs sont dotés de deux types d'interfaces de transmission : une pour les transmissions inter-mesh routeurs et l'autre pour les transmissions maillé routeur-clients, par contre les clients sont dotés d'une seule interface de transmission utilisée pour les transmissions inter client ou client-routeur [5].

- *Plusieurs fonctionnalités des routeurs :*

Certains routeurs sont chargés de fonctions supplémentaires (le rôle d'une passerelle, pont), en plus de leur tâche principale qui est le routage.

- *Le débit :*

Les réseaux maillés en générale et la norme 802.11s en particulier est actuellement en cours d'élaboration. Le débit de wifi mesh varie avec la technologie utilisé mais il atteint en moyenne 100Mo.

I.5. Fonctionnement du Wifi maillé IEEE 802.11s

Comme tous les standards de l'IEEE. L'IEEE 802.11b couvre les deux premières couches du modèle OSI (Open System Interconnexion).

Le fonctionnement du 802.11s est similaire à la norme 802.11b sauf que le 802.11s utilise les trois couches basses du modèle OSI.

Dans la section suivante nous allons détailler les trois niveaux de telle sorte que nous aurons une idée très précise du fonctionnement du réseau maillé.

I.5.1 Couche physique :

La couche physique définit la modulation des ondes radioélectrique et les caractéristiques de la signalisation pour la transmission de données. la couche physique est divisée en deux sous-couches : la couche PLCP (Physical Layer Convergence Protocol) et la couche PMD (Physical Medium Dependent).

I.5.1.1 La sous couche PLCP :

La couche PLCP permet la liaison entre la couche PMD et la couche MAC et a pour principal rôle la gestion des trames (encapsulation, décapsulation, etc.). Elle spécifie le type

de support de transmission, le type d'émetteur-récepteur, le type de connecteur et la technique de modulation et de démodulation.

Elle permet aussi d'envoyer à la couche MAC des rapports d'erreur ou encore de lui signifier si le support est libre ou non.

1.5.1.2 La sous couche PMD :

Elle s'occupe de la détection du support et fournit un signal appelé CCA (Clear Channel Assessment) à la sous couche MAC pour lui indiquer si le support est occupé ou non. La couche PMD définit les caractéristiques de la couche physique employée à savoir les techniques de transmissions utilisées (FHSS, DSSS ou OFDM).

- *FHSS (Frequency Hopping Spread Spectrum) :*

Le FHSS est un système à saut de fréquence ou la totalité disponible est divisée en 79 canaux de 1 MHz. Les transmissions se font sur l'ensemble des canaux selon une séquence de sauts prédéfinie, définissant ainsi le facteur d'étalement : le système passe d'un canal à un autre toute 300ms selon cette séquence. L'avantage de cette technique est toute personne écoutant la bande et ne connaissant pas la séquence de sauts ne pourra intercepter les données. D'autre part, étant donné que le système saute d'un canal à un autre, le FHSS possède une immunité contre des interférences locales. Son seul défaut réside dans la faible largeur de bande par canal ne lui permettant pas d'atteindre des vitesses de transmission élevées.

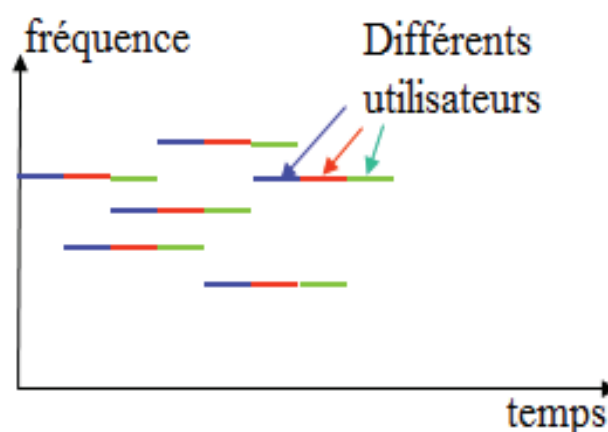


Figure 1.5 : Principe de la technique FHSS

- *DSSS (Direct Sequence Spread Spectrum)* :

Le DSSS utilise, quant à lui, comme facteur d'étalement une technique de chipping. Au lieu de découper la bande en canaux de 1MHz, la bande est découpée en quatorze canaux de 20 MHz mais un seul des canaux sera utilisé pour les transmissions. La technique de chipping consiste à envoyer un ensemble de bits (le chip) correspondant à un bit de données. L'étalement se fait donc au niveau de la quantité d'information envoyée.

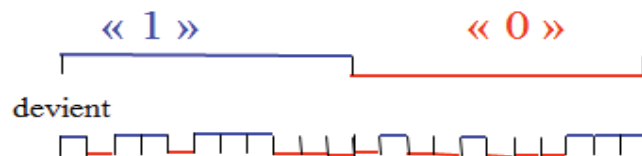


Figure I.6 : principe de la technique DSSS

- *OFDM (Orthogonal Frequency Division Multiplexing)*

La technique OFDM est une modulation multi porteuses, son principe est de diviser la bande passante en tranche appelé sous-canaux, tel que chaque sous-canal est utilisé comme un support de communication entre deux nœuds.

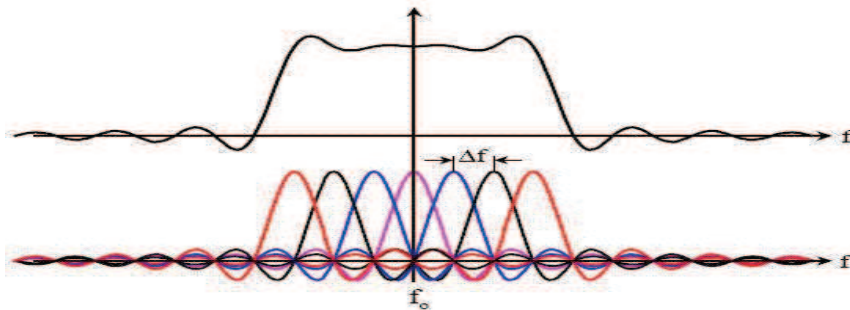


Figure I.7 : Principe de la technique OFDM

Cette technique est implémentée au niveau de points de maillage (mesh point) du réseau maillé .donc un mesh point équipé de plusieurs sous-canaux de transmission possède plusieurs interfaces logiques, ce qui diminue l'interférence et augmente la capacité d'un mesh point, et par conséquent il augmente la capacité du réseau. En plus, l'utilisation de la technique OFDM permet de créer des sous réseaux virtuels dont les nœuds utilisent le même sous canal, ce qui introduit la flexibilité au niveau de l'architecture du réseau.

I.5.2 Couche liaison de données :

Son rôle est un rôle de "liant" : elle va transformer la couche physique en une liaison a priori exempte d'erreurs de transmission pour la couche réseau.

La couche liaison de données doit être capable de renvoyer une trame lorsqu'il y a eu un problème sur la ligne de transmission. De manière générale, un rôle important de cette couche est la détection et la correction d'erreurs intervenues sur la couche physique. Cette couche intègre également une fonction de contrôle de flux pour éviter l'engorgement du récepteur.

La couche liaison de données est composée de deux sous-couches :

- ✓ La sous-couche de contrôle de liaison logique (LLC : Logical Link Control)
- ✓ La sous-couche de contrôle d'accès au support (MAC : Medium Access Control)

I.5.2.1 La sous couche LLC :

C'est une sous-couche de contrôle de la liaison logique (Logical Link Control) permet :

- Un transfert fiable (la détection et la correction des erreurs).
- Le contrôle de flux.
- D'établir un lien logique entre la couche MAC et la couche de niveau 3 du modèle OSI, la couche réseau par l'intermédiaire du *Logical Service Access Point*(LSAP).

I.5.2.2 La sous couche MAC :

C'est une sous-couche de contrôle d'accès au support (Media Access Control - MAC) utilisée dans le mode infrastructure et qui assure :

- La gestion d'accès de plusieurs stations à un support partagé dans lequel chaque station écoute le support avant d'émettre. (Contrôle d'accès au support).
 - L'adressage des paquets.
 - Le formatage des trames.
 - Le contrôle d'erreurs à partir d'un *CyclicRedundancy Check* (CRC).
 - Également la fragmentation et le réassemblage des trames.
 - Qualité de service (QoS - *Quality of Service*).
 - Gestion de l'énergie.
 - Gestion de la mobilité.
 - Sécurité.

En plus de ces fonctions habituellement rendues par la sous-couche MAC, la sous-couche MAC 802.11 offre d'autres fonctions qui sont normalement confiées aux protocoles supérieur, comme :

- ✓ La fragmentation et réassemblage.
- ✓ Les retransmissions de paquets.
- ✓ Les accusés de réception.

❖ *Méthode d'accès au support*

Dans un environnement sans fil le procédé de CSMA/CD n'est pas possible dans la mesure où deux stations communiquant avec un récepteur ne s'entendent pas forcément mutuellement en raison de leur rayon de portée. Ainsi la norme 802.11s propose une méthode similaire appelé CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). La méthode d'accès au média CSMA/CA utilise un mécanisme d'esquive de collision basé sur un principe d'accusés de réception réciproques entre l'émetteur et le récepteur : La station voulant émettre écoute le réseau. Si le réseau est encombré, la transmission est différée. Dans le cas contraire, si le média est libre pendant un temps donné (appelé DIFS pour Distributed Inter Frame Space), alors la station peut émettre.

La station transmet un message appelé Ready To Send (noté RTS signifiant prêt à émettre) contenant des informations sur le volume des données qu'elle souhaite émettre et sa vitesse de transmission. Le récepteur (généralement un point d'accès) répond un Clear To Send (CTS, signifiant Le champ est libre pour émettre), puis la station commence l'émission des données.

L'idée du 802.11s est de vérifier dans un premier temps lors de l'émission d'une donnée, si le canal est libre. Si c'est le cas, l'émetteur doit attendre une période de durée aléatoire appelée backoff avant d'émettre. Ce mécanisme s'applique lorsque le canal devient libre aussi bien après une de nos propres émissions qu'après toutes autres émissions. Ainsi, si plusieurs mobiles veulent émettre, il y a peu de chances pour qu'ils aient choisi la même durée. Celui qui a choisi le plus petit Backoff va commencer à émettre, et les autres vont alors se rendre compte qu'il y a à nouveau de l'activité sur le canal et vont attendre à nouveau.

La figure suivante schématise ce qui se passe lorsque deux mobiles veulent émettre et met en avant les mécanismes de temporisation [8].

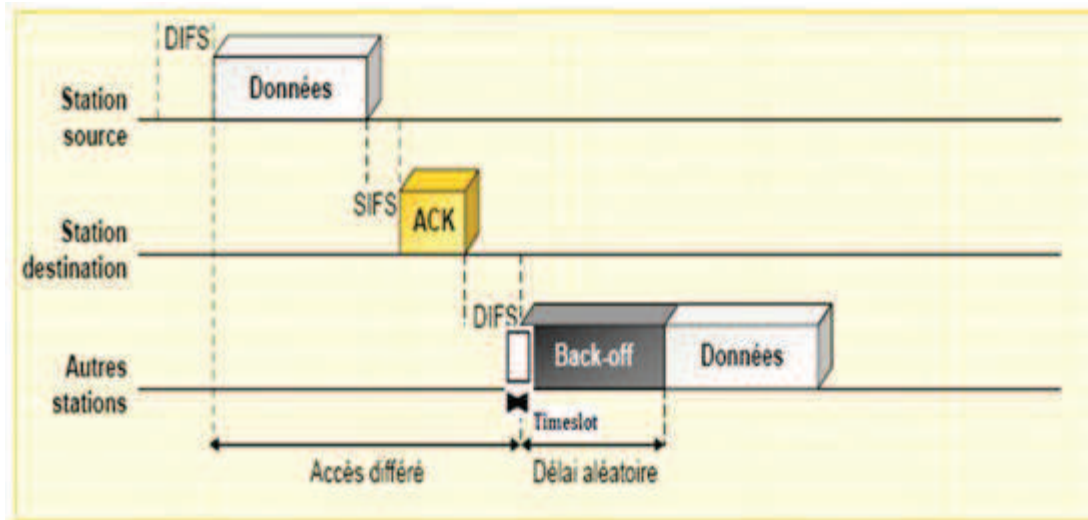


Figure I.8 : accès au support CSMA/CA

Le Backoff permet de tirer un nombre aléatoire entre 0 et X, où la valeur de X croît exponentiellement par rapport au nombre de tentatives de transmission. Le nombre tiré est multiplié par le timeslot. La station devra attendre le temps correspondant au résultat de l'algorithme avant de refaire une nouvelle tentative de rémission sur le support, tout en vérifiant qu'il soit libre. Après un certain nombre d'échec, on considère que l'émission a échoué.

Cette technique permet d'éviter au maximum les collisions en laissant, pour chaque station, la même probabilité d'accès au support.

❖ Cas de la station cachée

Une station A émet vers une station B ; une autre station C qui est hors de portée de la station B provoque une collision qui ne peut être évitée par la méthode CSMA/CA.

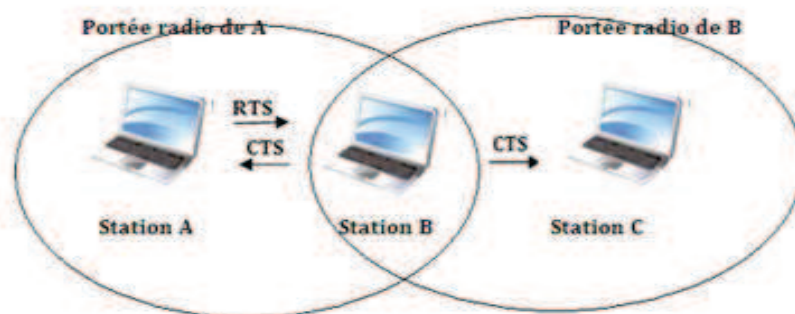


Figure I.9 : station cachée

Pour résoudre ce problème, la norme 802.11 a défini le mécanisme de VCS (Virtual Carrier Sense). Il est comparable à l'écoute du support effectué au niveau physique (PCF,

Physical Carrier Sense). Une station voulant émettre transmet d'abord une petite trame (30 octets) de contrôle RTS (Request To Send). Toutes les stations qui entendent le RTS mettent à jour leurs NAV en fonction du champ durée du RTS. La station destination concernée répond après l'attente d'un temps SIFS avec une trame courte CTS. (Clear To Send). La NAV est de nouveau mis à jour par la station entendant le CTS. Après réception du CTS par la station source, celle-ci est assurée que le support est réservé pour sa transmission pendant un temps au moins égal au NAV.

Par ailleurs, les stations cachées seront prévenues d'une émission en cours (dans l'exemple précédent, la station C qui aura entendu le CTS émis par B différera sa transmission). Ce mécanisme permet donc d'une part de réserver le support pendant un temps paramétrable et de résoudre le problème de la station cachée. Il n'évite cependant pas les collisions de RTS ou de CTS, mais celle-ci sont moins coûteuses que des collisions de longues trames de données.

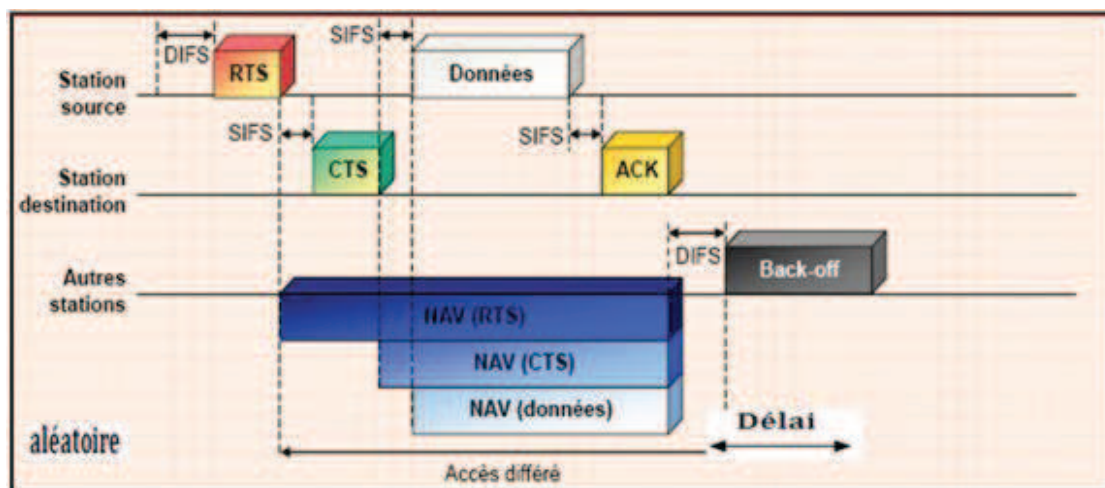


Figure I.10 : réservation du support avec les trames RTS/CTS

1.5.3 La couche réseau :

C'est la couche qui permet de gérer le sous-réseau, i.e. le routage des paquets sur ce sous-réseau et l'interconnexion des différents sous-réseaux entre eux. Au moment de sa conception, il faut bien déterminer le mécanisme de routage et de calcul des tables de routage (tables statiques ou dynamiques...). Les différents protocoles de routage utilisés dans les réseaux maillés en générale et en wifi maillé en particulier seront détaillés dans le chapitre II.

I.6. Les applications des réseaux maillés sans fil :

Contrairement aux réseaux ad hoc qui sont limités aux applications militaires et aux applications civiles spécifiques, les réseaux maillés satisfont le besoin de plusieurs applications.

- *Réseau domestique haut débit :*

Les réseaux domestiques classiques souffrent d'un problème de coût de déplacement et d'installation des points d'accès filaires d'où il faut faire une étude préalable de localisation des points d'accès pour assurer une bonne couverture et éviter par conséquent le déplacement des points d'accès, Mais cette étude ne résout pas le problème définitivement [5]. Les réseaux maillés peuvent le régler en remplaçant Les points d'accès par des routeurs maillés sans fil avec une connectivité réseau établie entre eux.

Les WMN permettent de créer à faible coût et avec une facilité de déploiement incomparable une excellente couverture sans fil dans toute la maison. La technologie des réseaux maillés permet d'éliminer les zones non couvertes ou les zones avec une qualité de couverture sans fil médiocre [7].

Ainsi, les nouvelles applications hauts débit comme la transmission et la diffusion de vidéo haute définition (~10Mb/s) seront facilement supportées dans les réseaux domestiques.



Figure I.11 : réseau maillé sans fil domestique

- *Réseau de communauté et de voisinage :*

Actuellement, la communication entre maisons se fait par l'intermédiaire du réseau internet, Un avantage de cette architecture est la couverture étendue du réseau.

Par contre elle possède des inconvénients :

- Même si l'information doit être partagée au sein d'une communauté ou d'un quartier, n'importe quelle communication entre deux utilisateurs passe obligatoirement par internet.

- La nécessité d'une passerelle pour chaque maison, ce qui peut augmenter le coût des services du réseau.

- Un grand pourcentage de zones entre les maisons ne sont pas couverts par les services sans fil.

La solution maillé peut faire face à ces problèmes par l'installation des routeurs pour chaque maison, ainsi que doter quelque maison par des passerelles pour permettre l'accès aux autres réseaux .comme le montre la figure qui va suivre. Les WMN peuvent également activer de nombreuses applications telles que le stockage de fichiers distribué, l'accès aux fichiers distribué, et le streaming vidéo.

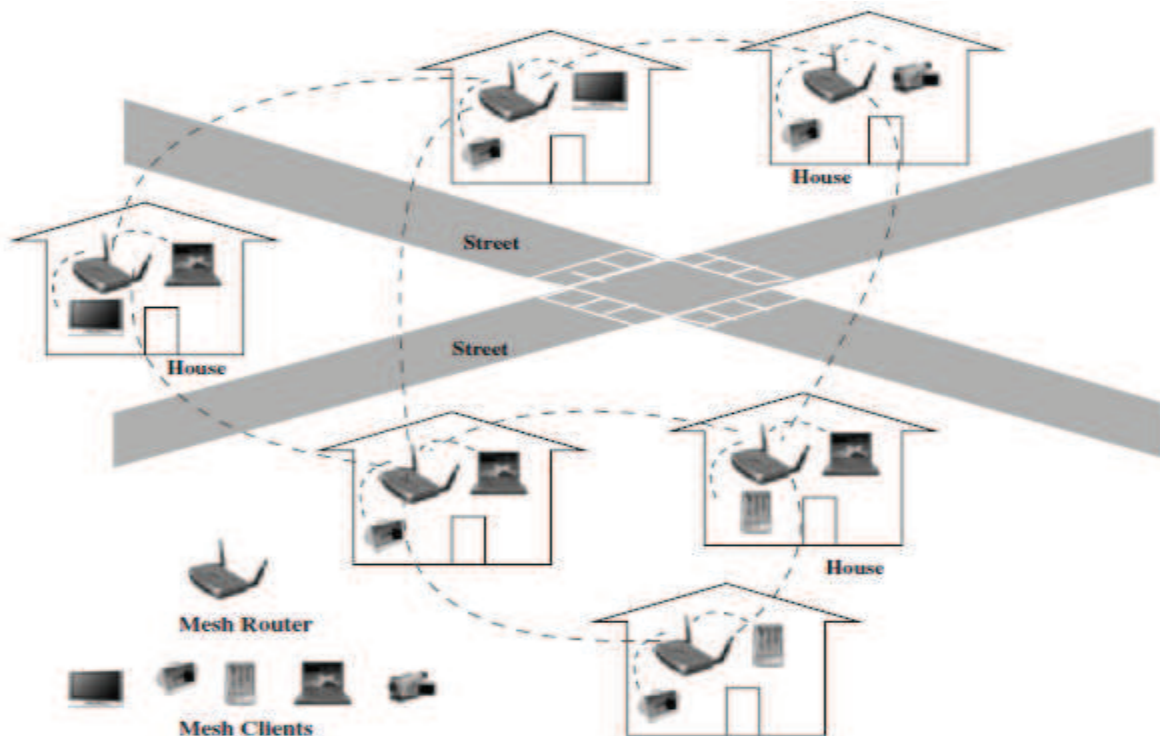


Figure I.12 : réseau maillé sans fil de communauté

- *Réseaux d'entreprises :*

La motivation principale derrière l'introduction des réseaux maillés est de fournir de la connectivité dans l'entreprise et d'utiliser des technologies sans fil performantes, fiables, peu chers, et faciles à déployer. Les entreprises peuvent ainsi maîtriser les coûts associés à l'installation du réseau et réduire le temps nécessaire pour le déploiement [7].

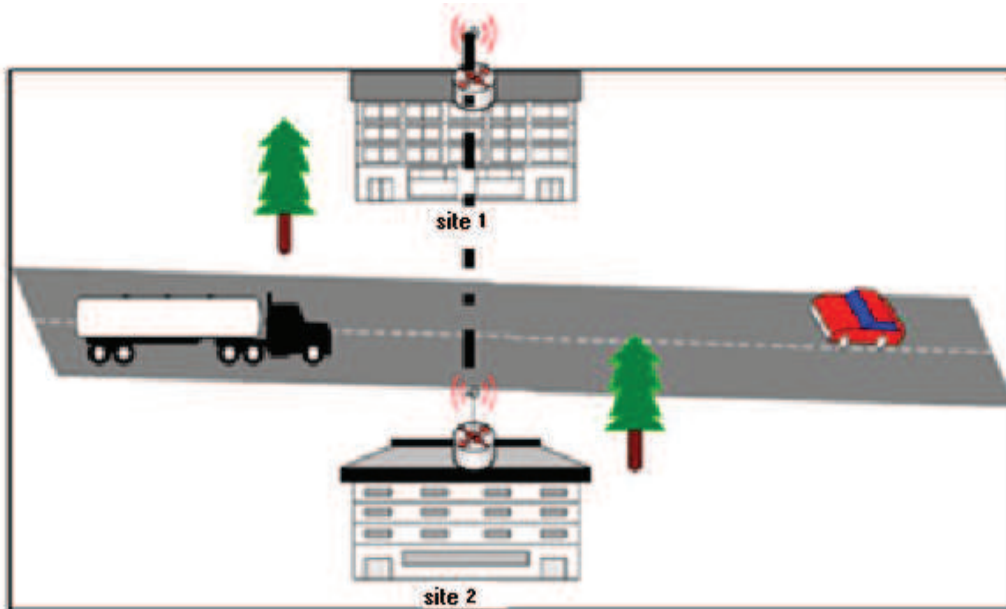


Figure I.13 : réseau maillé sans fil d'entreprise

- *ZONE PUBLIC (campus, communauté) :*

Les réseaux maillés peuvent être déployé dans les lieux publics (aéroport, restaurant, parc) pour offrir une connexion internet aux passagers et clients. Le choix du réseau maillé dans ces endroits peut se justifier par le besoin de mobilité et le coût réduit du déploiement. Les réseaux maillés peuvent aussi être déployé dans les universités et les campus pour permettre aux étudiants d'accéder aux ressources de l'université ou bien de vérifier leurs mails depuis n'importe quel endroit même en dehors de leur campus [1].

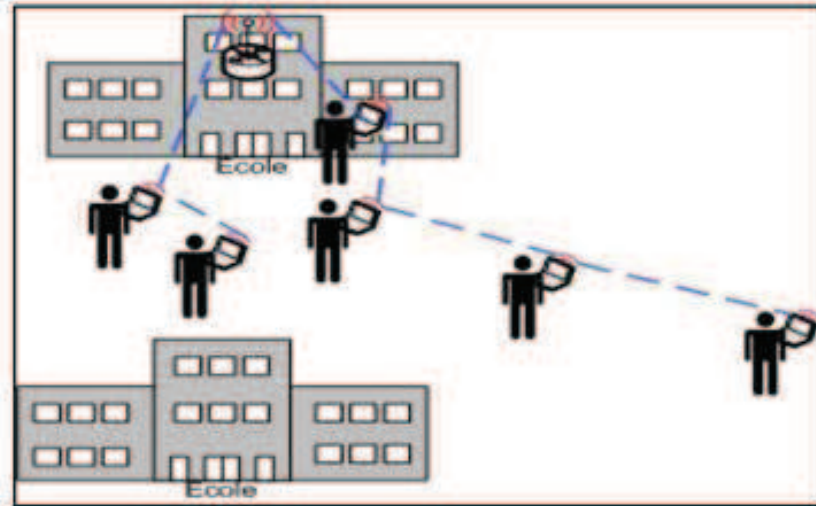


Figure I.14 :réseau maillé sans fil pour une zone public

- *Infrastructure de connexion internet :*

Les réseaux maillés présentent aussi une solution rentable pour un fournisseur d'accès internet (FAI) qui peut étendre sa zone de couverture grâce à la collaboration de ses abonnés. En effet, les FAI peuvent utiliser l'architecture maillés comme infrastructure pour distribuer la connexion internet dans un périmètre étendu [5].

Un seul nœud attaché à un routeur maillé peut servir plusieurs voisins qui sont trop éloignés pour joindre directement le réseau. Il faut noter que la solution maillé pour offrir une connexion internet est intéressante dans les milieux ruraux aussi bien qu'urbain. Dans les milieux ruraux, tirer des câbles ou des lignes DSL (Digital Subscriber Lines) pour les grandes distances est très onéreux.de plus cette solution n'est pas rentable puisque le nombre d'utilisateur est généralement limité. Par conséquent les routeurs maillés permettent d'éliminer le coup de câblage. Dans les milieux urbains ou la densité des nœuds connectés est élevée, la solution maillée peut être intéressante en termes de fiabilité et de qualité de service .en effet, la redondance de chemins peut augmenter la fiabilité et éliminer les congestions dans le réseau [1].

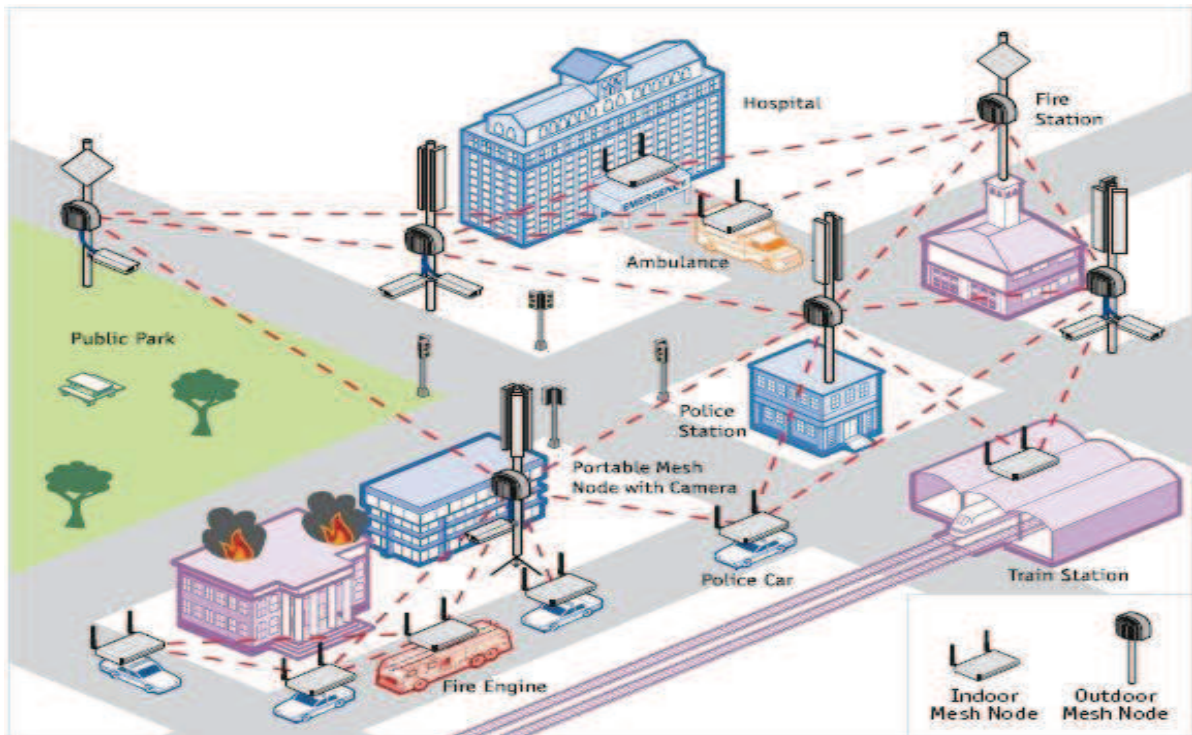


Figure I.15 : Infrastructure de connexion internet via wifi mesh

- *Les applications Multimédias :*

Les applications multimédias peuvent se positionner dans toutes les "sphères de la vie", publiques et privées. Elles s'adressent à un public toujours plus varié : simple citoyen, entreprises, administrations, professionnels, élèves et étudiants, consommateurs, touristes, journalistes, chercheurs, demandeurs d'emploi, passionnés de nouvelles technologies, etc.

Il serait bien difficile d'énumérer tous les produits existant sur le marché. Voici un inventaire, loin d'être exhaustif, d'applications pour quelques domaines d'activité montrant la diversité qui existe déjà :

- *Enseignement/Formation :*

Plateformes d'e-learning, cours accessibles en streaming ou en podcast, jeux éducatifs, portails administratifs en ligne pour les formalités scolaires des étudiants, formations personnalisées, sites Web d'établissements scolaires et universitaires, etc.

- *Divertissement/Loisirs :*

Vidéos interactives, applications de Web TV, jeux vidéo, sites Web de jeux en ligne, de musique et de vidéo, portails d'activités de loisirs, etc.

- *Communication/Echanges sociaux :*

Réseaux sociaux, groupes de discussion, forums de discussion, newsletters, annuaires électroniques, etc.

➤ *Commerce/Economie :*

Catalogues électroniques, netbanking, sites d'achat, de réservations et de paiement en ligne, organisateurs numériques, etc.

➤ *Culturel :*

Encyclopédies électroniques, livres électroniques, musées en ligne, bornes interactives de musée, portails culturels, etc.

➤ *Tourisme/Voyages :*

Villes virtuelles, sites de réservation d'hôtels et d'avions, applications en ligne de calculs d'itinéraires routiers, cartes et plans interactifs, systèmes de géo localisation par satellite, etc.

➤ *Santé :*

Portails d'information sur la santé, dossiers médicaux interactifs, plateformes d'échange de données sur la santé, etc.

➤ *Edition/Presse :*

Journaux en ligne, magazines sur CD-ROM ou DVD, dictionnaires et livres électroniques, encyclopédies interactives, etc.

Grace au WIFI maillé (802.11S) les utilisateurs peuvent bénéficier de ces applications à haut débit.



Figure I.16 : Les applications multimédia

I.7. Avantages des réseaux maillés sans fil :

Les Réseaux Maillés Sans Fil suscitent un grand intérêt dans la communauté des chercheurs en télécommunication grâce à leurs nombreux avantages.

- Tolérance aux pannes : si une route sur le réseau devient défaillante, le flux d'information n'est pas interrompu, le réseau va dynamiquement changer de route.
- Coût de déploiement réduit : les réseaux sans fils sont basés sur des routeurs maillé qui sont interconnectés par des liaisons radio. Cela minimise le nombre de câbles par la suite réduit le coût de déploiement du réseau.
- Facilité de déploiement : il est très simple de créer, configurer et déployer un nœud.
- Consommation énergétique : contrairement aux réseaux ad hoc ou le problème d'énergie représente un obstacle majeur pour le bon fonctionnement du réseau à cause des ressources énergétique limitées de la majorité des nœuds ainsi que les tâches supplémentaires accomplis par ces derniers (routage, auto configuration). Dans les WMN cet obstacle est diminué par les routeurs qui sont branchés aux ressources énergétiques, ce qui libère les nœuds clients.
- Capacité : les nœuds dans les réseaux ad hoc classiques utilisent une seule interface de communication ce qui limite la capacité du réseau, par contre les WMNs utilisent généralement deux interfaces : une pour les communications inter routeurs et l'autre pour les communications de type client-routeur ou client-client, ce qui augmente sensiblement la capacité du réseau.
- Couverture étendue.
- Réseau à haut débit, par rapport aux autres réseaux mobiles.
- Fiabilité : la redondance des chemins dans un réseau maillé augmente la fiabilité du réseau. en effet, lorsqu'un nœud intermédiaire quitte le réseau ou échoue dans le délayage du trafic, l'émetteur peut basculer vers un autre chemin.

I.8. Inconvénients des réseaux maillés sans fil :

Malgré tous les avantages que nous avons cité, les réseaux maillés sans fils ont aussi des inconvénients :

- Le déploiement de réseaux maillés nécessite bien entendu que l'opérateur qui l'installe soit capable de maintenir une qualité de service minimal.
- La taille du réseau influe sur les performances de la capacité. En effet, plus le nombre de nœuds augmente plus les performances se dégrade.

- la communication vers l'extérieur ne se fait que par les routeurs, le placement de ces derniers a une grande influence sur les performances du réseau.
- Assurer la sécurité des informations, sachant qu'elles sont susceptibles de passer par n'importe quel utilisateur, et assurer un routage optimal et robuste sont deux autres problèmes majeurs des réseaux maillés.

I.9. Conclusion :

La facilité de déploiement et l'absence de gestion centralisée des communications dans les RMSF en font une solution présentant plusieurs avantages. Les RMSF essaient de répondre à l'augmentation croissante du nombre d'utilisateurs et de leurs applications qui demandent de plus en plus de ressources.

Ce chapitre a présenté un aperçu général sur le standard 802.11s qui a comme objectif d'introduire les fonctionnalités nécessaires dans le standard 802.11 pour supporter les architectures et les protocoles multi-saut maillés et qui est considéré comme l'un des réseaux maillés sans fil.

Les réseaux maillés représentent une technologie prometteuse en pleine essor permettant d'étendre rapidement et facilement la couverture d'un réseau WLAN classique. Ils permettent également la mise en place de solutions abordables et économiquement viables en comparaison aux réseaux filaires pour ramener de la connectivité dans les zones où le coût du câblage est élevé ou impossible. Les pays en cours de développement seront certainement intéressés par une telle technologie qui permettra de combler la fracture numérique entre pays développés et ceux qui sont en voie de développement.

CHAPITRE II :
ROUTAGE ET QOS DANS
LE WIFI MESH

II.1. Introduction :

Les performances des réseaux multi-sauts tels que les Réseaux Maillés Sans Fil dépendent pour une grande part des protocoles de routage et de leur manière de choisir les routes. Ces protocoles devraient être en mesure de gérer le trafic et de garantir la QOS pour tout type de trafic, mais cela demeure un défi dans le domaine de la recherche.

Le choix de route se fait selon un ou plusieurs protocole qui permettent de différencier les "bonnes" des "mauvaises" routes. [9] Un protocole de routage permet de quantifier la qualité d'un lien ou un chemin selon certains critères tels que le taux de perte, l'interférence, la longueur des routes, le délai etc. Selon les applications, on peut avoir différentes contraintes, pour la voix par exemple on devrait donner un meilleur coût aux chemins avec moins de délai quitte à accepter un léger taux de perte.

Suivant la manière de création et de maintenance de routes lors de l'acheminement des données, les protocoles de routage peuvent être séparés en trois catégories (Proactif, Réactif, Hybride) [10].

Dans ce chapitre, nous allons présenter les trois classes des protocoles de routage dans les réseaux maillés en étudiant, dans chaque cas, quelques protocoles ; nous décrirons leurs principales caractéristiques et fonctionnalités qui permettent d'assurer l'acheminement des données entre les différentes unités mobiles, nous verrons aussi quelques notions sur la qualité de service.

II.2. Routage :*II.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 du routage ne se résume pas seulement à trouver un chemin entre les deux nœuds du réseau, mais encore à trouver un acheminement optimal des paquets à travers le réseau au sens d'un certain critère de performance.

II.2.2. Problématiques et contraintes du routage dans les réseaux maillés sans fil :

Contrairement aux réseaux filaires classiques où les nœuds sont fixes ce qui donne une stabilité des routes, la mobilité fréquente des nœuds dans les réseaux Ad-Hoc et la nature des liens sans fil impliquent la modification, la disparition des routes, et l'apparition des nouvelles routes, Ainsi que l'absence d'une infrastructure chargée de routage augmente sa complexité. Ce qui change complètement l'approche de routage par rapport aux approches classiques.

D'où la nécessité de trouver des protocoles de routage plus performants pour s'adapter à cet environnement. Ces protocoles exigent des ressources importantes : mémoires, processeurs, bande passante et énergie, mais ces ressources sont rares dans les Ad-Hoc vu ses caractéristiques, ce qui complique la conception de ces protocoles, ainsi que la participation des nœuds dans le calcul des routes nécessite l'utilisation des algorithmes de routage distribués [5].

Dans le réseau Wifi maillé, les mêmes caractéristiques s'applique que les réseaux Ad-hoc mais vue que le réseau 802.11s est divisé en deux parties (routeurs et clients) et que les routeurs forme l'épine dorsale du réseau qui est déjà alimenté et fixe en générale, donc y'a pas de problème d'énergie ni de mobilité. Par contre au niveau des clients maillés, la mobilité varie selon l'utilisateur, et l'énergie dépend du terminal utilisé. Donc principalement l'objectif du routage dans le 802.11s et d'améliorer la QoS d'une manière intelligente pour satisfaire les exigences des utilisateurs [6].

II.2.3. Les objectifs des protocoles de routage dans les réseaux maillés sans fil :

l'objectif principal d'un protocole de routage est de trouver et de maintenir le chemin optimal à multi- sauts pour une communication quelconque, le sens du mot optimal dépend de la nature du réseau , la nature de l'application, la nature des informations échangées et la nature des utilisateurs, on distingue plusieurs points de vue :

- Chemin qui consomme le minimum de ressources (bande passante, mémoire, processeur, énergie).
- Chemin qui utilise le minimum de sauts.
- Chemin qui est le plus court chemin (distance).
- Chemin qui est le plus sûr.
- Chemin qui assure la meilleure qualité de service. [5].

Cet objectif peut être atteint par les points suivants :

- Eviter les boucles de routage.
- Réduire le nombre et la taille des messages de contrôle.
- Maintenir la topologie d'une manière dynamique.
- Réduire et simplifier les traitements [4].

II.2.4. notions sur le routage dans les réseaux maillés sans fil :

Nous allons présenter dans cette section quelques notions sur le routage dans les réseaux maillés sans fil :

II.2.4.1. L'inondation :

L'inondation ou la diffusion pure, est une technique de routage fréquemment utilisée qui consiste à faire parvenir un paquet à tous les nœuds du réseau. Un nœud qui initie l'inondation envoie le paquet à tous ses voisins directs, de même si un nœud quelconque du réseau reçoit le paquet pour la première fois, il le rediffuse à tous les voisins, Ainsi de proche en proche le paquet inonde le réseau. Le mécanisme d'inondation est utilisé généralement dans la première phase du routage plus exactement dans la procédure de découverte des routes, et cela dans le cas où le nœud source ne connaît pas la localisation exacte de la destination.

Ce type de routage entraîne une charge importante sur le réseau et engendre des problèmes tels que le bouclage et la duplication des messages [11].

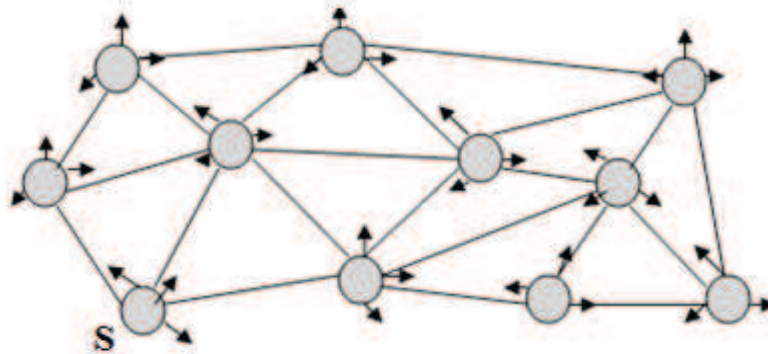


Figure II.1 : L'hôte S envoie des informations par inondation.

II.2.4.2. Multihopping :

Les stratégies de routage dans les réseaux ad hoc utilisent le principe de multihopping (multi sauts). Un paquet est acheminé à sa destination en sautant d'un nœud à un autre sans qu'il y ait besoin d'une station de base comme dans les réseaux cellulaires ou réseaux sans fil avec infrastructure [6].

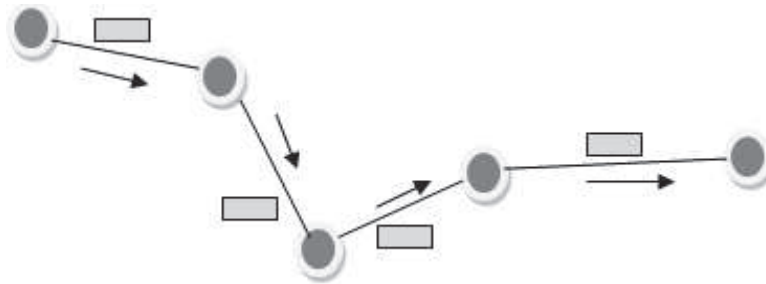


Figure II.2 : Le multihopping dans les réseaux maillés

II.2.4.3. Le concept de groupe :

Dans la communication de groupe, les messages sont transmis à des entités abstraites ou groupes, les émetteurs n'ont pas besoin de connaître les membres du groupe destinataire. La gestion des membres d'un groupe permet à un élément de se joindre à un groupe, de quitter ce groupe, se déplacer ailleurs puis rejoindre le même groupe. C'est en ce sens que la communication de groupe assure une indépendance de la localisation, ce qui la rend parfaitement basée sur les groupes [15]. Le concept de groupe facilite les tâches de la gestion du routage (telles que les transmissions des paquets et l'allocation de la bande passante) et cela en décomposant le réseau en un ensemble de groupes connectés.

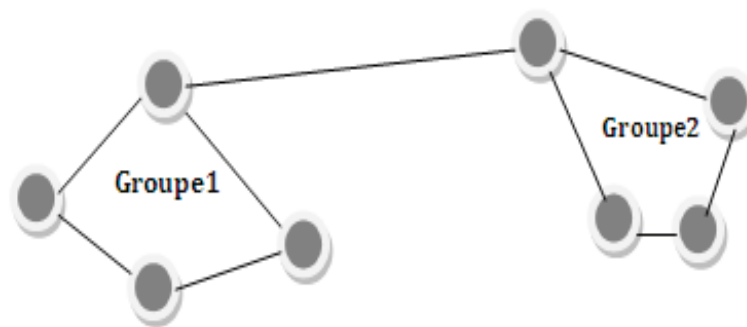


Figure II.3 : La décomposition du réseau en groupes

II.2.5. Les méthodes de routage :

Les méthodes de routage représente l'approche suivie pour déterminer le chemin optimal pour une transmission donnée, elles permettent de déterminer la route que doivent emprunter les messages dans un réseau. Pour cela, ils gèrent les tables de routage de chaque nœud, en veillant notamment à ne pas créer de boucle dans le réseau (message qui tournerait en rond en passant toujours par les mêmes nœuds, sans jamais atteindre leur destination).

il existe plusieurs méthodes : routage par vecteur de distance, routage par état des liens, routage à la source .

II.2.5.1. Routage à vecteur de distance :

Dans cette méthode chaque élément qui participe au routage diffuse à ses voisins directs sa table de routage, à chaque modification de celle-ci et à des intervalles de temps réguliers. Cette diffusion périodique permet de diminuer le nombre de boucles de routage. Si un nœud ne reçoit pas la table d'un de ses voisins pendant une période de temps fixée à l'origine il considérera ce nœud comme défaillant. A chaque fois qu'une des stations reçoit une table de la part de son voisin, elle rajoute les entrées qu'elle n'avait pas, et s'il existe des routes à moindre coût, elle les adopte.

Cette méthode impose de fixer une métrique commune à chaque nœud, basée par exemple sur :

- Le nombre de sauts, c'est à dire le nombre de nœuds intermédiaires que le paquet devra traverser avant d'atteindre sa destination finale. Dans ce cas, la distance entre deux nœuds voisins est une constante fixée à 1.
- Le nombre de paquets dans la file d'attente de l'interface choisie, ce qui permet d'avoir une idée de l'état de congestion d'un lien particulier.
- Le temps mis pour atteindre le prochain nœud.
- Le coût financier du lien.

Néanmoins, cette technique est lourde lorsque le nombre de nœuds est important à cause des transferts d'informations de nœuds en nœuds. De plus, comme un routeur ne connaît que ses voisins, il ne sait pas quel est le chemin global emprunté par un message, ce qui peut poser des problèmes de sécurité.

Les protocoles de routage basés sur le vecteur de distance les plus connus sont : DSR, DSDV et AODV.

II.2.5.2. Routage à état des liens :

Contrairement au routage par vecteur de distance, la distance pour atteindre une destination n'est pas calculée au fur et à mesure. Dans cette méthode, chaque nœud tient à jour une base de données décrivant la topologie entière du réseau, c'est à dire l'ensemble des nœuds, et leurs interconnexions, pour calculer la distance qui le sépare d'une destination, chaque nœud construit un arbre dont il est la racine, et suit au fur et à mesure toutes les ramifications du réseau tant qu'il n'a pas atteint la destination finale.

Le calcul de cet arbre permet de connaître le chemin complet (c'est à dire tous les nœuds intermédiaires que le paquet devra traverser), cependant seule l'adresse du prochain saut est conservée par le nœud puisque de son point de vue, c'est la seule information utile.

Lorsqu'un lien change d'état, le nœud qui le détecte transmet cette information à tous ses voisins par un mécanisme d'inondation. Chaque nœud recevant cette information met à jour sa base de données, et s'il s'agit d'une information nouvelle (en d'autres termes, s'il n'a pas déjà reçu cette information), il réémet le message d'information à tous ses voisins.

Ce mécanisme permet à tous les nœuds d'être informés rapidement de toute modification, tout en assurant que le message soit détruit dès que tous l'ont reçu. Le principal problème de cet algorithme est le coût, en termes de capacité de calcul et de mémoire demandée par l'élaboration de l'arbre. En effet, à chaque changement de topologie, chaque nœud doit à nouveau dérouler le même algorithme, et calculer le plus court chemin pour atteindre chaque destination présente dans sa base de données. De plus, tout ce calcul paraît fastidieux quand on sait que seule l'adresse du prochain saut est conservée.

II.2.5.3. Routage par la source :

Le routage par la source permet à l'émetteur de préciser le chemin par lequel devra transiter le paquet pour joindre le destinataire. L'entête de paquet va donc contenir la liste des différents nœuds relayeur vers la destination.

Il existe deux modes de fonctionnement :

- ✓ Mode strict où la liste exhaustive des routeurs doit être fournie.
- ✓ Mode libéral (*loose*) où seulement l'adresse de certains routeurs sur le chemin est précisée [9].

Le protocole le plus connu basant sur cette classe est : DSR

II.2.5.4. Routage saut par saut :

Dans le routage saut-par saut chaque paquet de données porte uniquement l'adresse de la destination et celle du saut prochain. De ce fait, chaque nœud intermédiaire utilise sa table de routage pour acheminer chaque paquet de données.

II.2.6. Classification des protocoles de routage :

Il existe plusieurs critères pour classer les protocoles de routage :

II.2.6.1. Selon le moment d'établissement des routes :

II.2.6.1.1. Les protocoles de routages proactifs :

Le principe de cette classe est que les routes sont préparées à l'avance. Les protocoles de routage proactifs utilisent une ou plusieurs tables de routage dans chaque nœud, Ils essaient de maintenir les meilleurs chemins existants vers toutes les destinations possibles au niveau de chaque nœud du réseau, pour le faire ils utilisent l'échange régulier des messages de contrôle pour mettre à jour les tables de routage vers toute destination atteignable depuis celui-ci. Cette approche permet de disposer d'une route vers chaque destination immédiatement au moment où un paquet doit être envoyé. Les tables de routage sont modifiées à chaque changement de la topologie du réseau. Les deux principales méthodes utilisées sont : les méthodes Etat de Lien "*Link State*" et la méthode du Vecteur de Distance "*Distance Vector*" [5].

Les célèbres protocoles basés sur ce principe sont : DSDV,WRP,TBRPF,GSR,FSR, ZHLS, CGSR, DREAM, LSR et OLSR .

✧ *Avantages et 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 fil. De plus, la taille des tables de routage croît linéairement en fonction du nombre de nœud.

II.2.6.1.2. Les protocoles de routages réactifs :

Le principe de cette classe est que les routes sont établies à la demande. Ces protocoles se basent sur la découverte et le maintien des routes. Suite à un besoin, une procédure de découverte globale de route est lancée, ce processus s'arrête une fois la route trouvée ou toutes les possibilités sont examinées, dès que la communication est établie, cette route est maintenue jusqu'à ce que la destination devienne inaccessible ou jusqu'à ce que la route ne soit plus désirée [5]. Les protocoles de routage réactifs peuvent être classifiés en deux catégories : à routage source ou à routage saut-par-saut.

Parmi les protocoles basés sur Ce principe on cite : DSR, CEDAR, TORA, ABR, SSR, LAR, RDMAR, EARP et AODV.

✧ *Avantages et les inconvénients des protocoles réactifs :*

Ce type de routage minimise l'échange des messages de contrôle ce qui libère la bande passante, il permet aussi une meilleure adaptabilité aux changements fréquents de topologie, car chaque nœud utilise les informations les plus fraîches dans le routage.

Cependant, L'efficacité de l'approche réactive commence à diminuer quand le trafic et la mobilité deviennent plus importants. De plus, les protocoles de routage réactifs possèdent un temps de réponse plus élevé que celui des protocoles de routage proactifs ce qui peut influencer sur les performances des applications interactives.

II.2.6.1.3. *Les protocoles de routage hybrides :*

Cette classe combine les deux concepts proactif et réactif, afin de profiter de leurs avantages, et limiter leurs inconvénients.

Les protocoles hybrides utilisent un protocole proactif, pour apprendre le proche voisinage par exemple voisinage à deux sauts ou trois sauts. Ainsi ils disposent des routes immédiatement dans le voisinage. Au-delà de cette zone prédéfinie, le protocole hybride fait appel aux techniques des protocoles réactifs pour chercher des routes. Avec ce découpage, le réseau est partagé en plusieurs zones, et la recherche de route en mode réactif peut être améliorée. Ce type de protocole s'adapte bien aux grands réseaux [5].

✧ *Avantages et inconvénient des protocoles hybrides :*

Les protocoles de routage hybrides ont l'avantage de scalabilité, car la taille des tables de routage est réduite à la taille des zones. De plus, ils permettent un temps de réponse plus court que les protocoles de routage purement réactifs.

Cependant, il rassemble toujours quelques inconvénients des deux approches proactives et réactives.

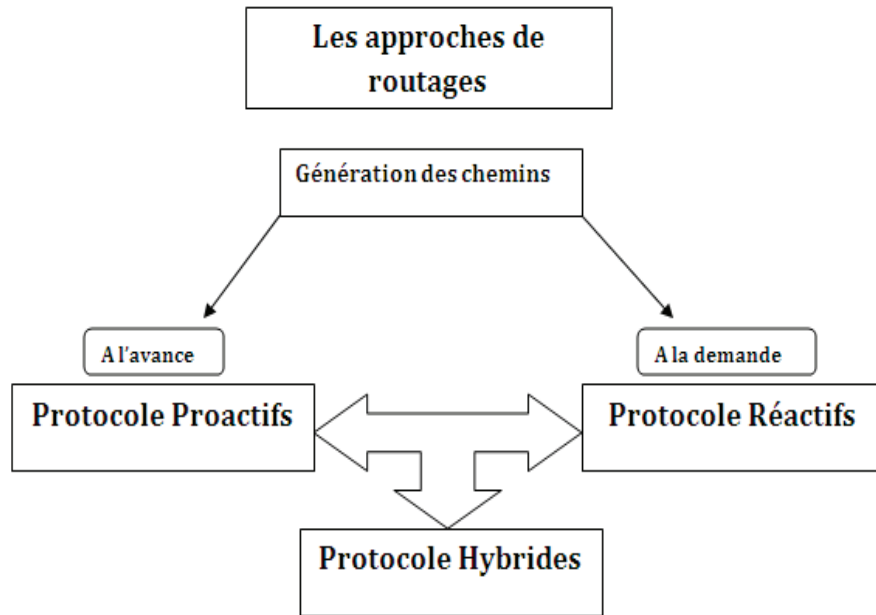


Figure II.4 : Classification des protocoles de routage

II.2.6.2. Selon la participation des nœuds dans le routage :

II.2.6.2.1. Les protocoles uniformes :

Dans cette classe de protocoles, les nœuds ont le même niveau et les mêmes fonctionnalités en point de vue de la responsabilité de participer dans le routage. La décision qu'un nœud peut router des paquets dépend de sa position. Ainsi que chaque nœud envoie et reçoit des messages de contrôle de routage. Donc la charge est répartie de façon uniforme dans le réseau. Ce type de routage est simple et efficace dans les réseaux de petites tailles, par contre dans le cas des réseaux denses ou de grande dimension, le volume d'information de routage devenant important.

II.2.6.2.2. Les protocoles non uniformes :

Le but de ce type de protocole est de limiter la complexité du routage en réduisant le nombre de nœuds qui contribuent à la détermination des routes. Donc les nœuds n'ont pas la même responsabilité dans le routage. Cette classe de protocoles est composée de deux familles :

- Protocoles à sélection des voisins : chaque nœud sélectionne un sous-ensemble de ses voisins qui prend un rôle distinct dans l'opération de routage. Chaque nœud fait sa sélection tout seul (indépendamment des autres).

- Protocoles à partitionnement (hiérarchique) : les nœuds négocient un partitionnement sur la topologie, Cette opération est effectuée de manière distribuée car il n'Ya pas de nœud qui fait office de gestionnaire de topologie. Généralement, les nœuds sont partitionnés en groupe (clusters) dont l'appartenance d'un nœud varie suivant les changements de connectivité. Quelques nœuds sont élus pour prendre un certain rôle dans le routage (leader du groupe [cluster Head], ou bien passerelle entre deux groupes [Gateway] [5].

Cette classe de protocoles donne de bons résultats dans les réseaux denses ou de grande taille.

II.2.7. Exemples de protocoles de routage :

Nous allons citer dans cette section quelques protocoles de routage

II.2.7.1. Le protocole de routage proactif OLSR (Optimized Link State Routing) :

OLSR est un protocole de routage proactif à état de liens. Son innovation réside dans sa façon à économiser la consommation de la bande passante lors des broadcast. Ceci est réalisé grâce à l'utilisation du concept des "relais multipoints " (MPR) dans lequel chaque nœud choisit un sous-ensemble de ses voisins pour retransmettre ses paquets en cas de broadcast.

En se basant sur le broadcast en utilisant les MPR, tous les nœuds du réseau sont atteints avec un nombre réduit de répétitions. Un ensemble de MPR d'un nœud N est l'ensemble minimal de ses premiers sauts voisins qui couvrent (dans le sens de la portée de communication) ses deuxièmes sauts voisins.

Dans OLSR, chaque nœud broadcast périodiquement des messages Hello qui contient l'état de ses liens avec ses premiers sauts voisins (unidirectionnel, bidirectionnel ou MPR pour dire que ce voisin est un MPR). Grâce aux messages Hello, un nœud construit sa table des voisins ainsi que la liste des voisins qui l'ont choisi comme MPR dits "MPR-sélecteurs". De plus, un nœud broadcast périodiquement des messages TC (*Topology Control*) qui contient la liste de ses MPR-sélecteurs. En exploitant ces messages, chaque nœud remplit les deux champs nommés "destination" (correspond aux MPR-sélecteurs dans le message TC) et "dernier saut" (prend comme valeur l'identificateur du nœud émetteur du message TC) d'une table dite de topologie. Les tables de topologie et des voisins sont exploitées pour construire la table de routage [6].

Il est à noter que le protocole OLSR est adapté aux réseaux à une haute densité. Dans un réseau à faible densité, chaque voisin devient MPR et OLSR se réduit à un protocole à état de liens pur.

II.2.7.2. Le Protocol de routage proactif DSDV (Destination Sequence Distance Vector) :

DSDV est un protocole de routage proactif basé sur l'algorithme *Bellman-Ford*. Il a été proposé par Charles Perkins et Pravin Bhagwat en 1994.

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

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

Chaque station mobile maintient une table de routage qui contient : toutes les destinations possibles, le nombre de nœuds (ou de sauts) nécessaire pour atteindre la destination et le numéro de séquences (SN : Séquence Number) qui correspond à un nœud destination. La contribution principale du protocole DSDV est l'utilisation des SN, qui permettent de faire la distinction entre les anciennes et les nouvelles routes, ce qui évite la formation des boucles de routage [3].

La mise à jour dépend de deux paramètres : Le temps, c'est-à-dire la période de transmission, et les événements. Un paquet de mise à jour contient : le nouveau numéro de séquence incrémenté du nœud émetteur et, pour chaque nouvelle route, l'adresse de la destination, le nombre de nœuds (ou de sauts) séparant le nœud de la destination et le numéro de séquence (des données reçues de la destination) tel qu'il a été estampillé par la destination [3].

Quand un nœud reçoit plusieurs paquets de mise à jour au sujet d'un même nœud destination, il choisit celui avec le numéro de séquence le plus haut. Un nœud qui détecte la rupture d'un lien, génère un paquet de mise à jour dont le numéro de séquence possède une valeur infini. En recevant ce paquet, chaque nœud retire l'entrée correspondante de sa table de routage. Pour assurer la consistance des tables de routage, les mises à jour de ces derniers s'effectuent périodiquement et immédiatement après un changement de topologie. Pour réduire la quantité du trafic que génèrent ces mises à jour, deux types de paquets sont utilisés.

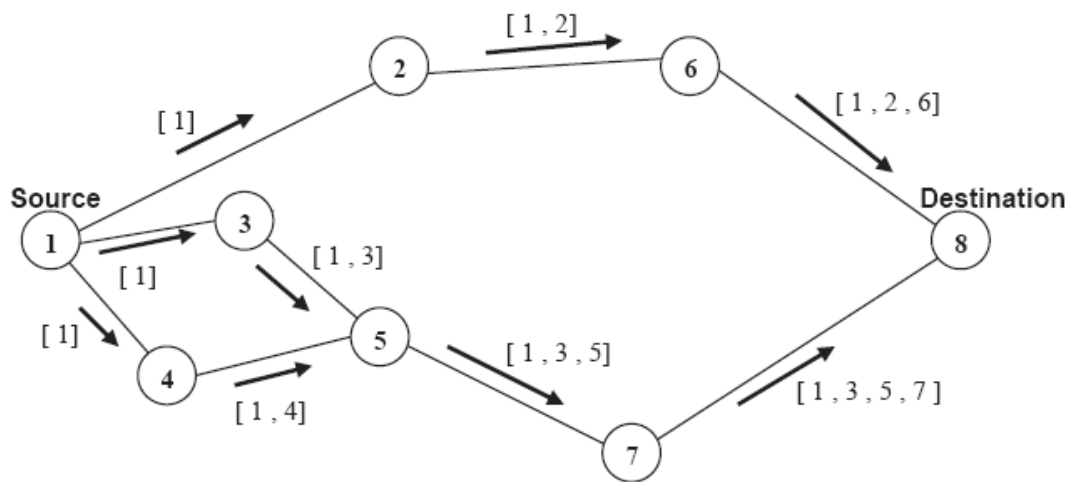
Le premier est appelé " *full dump* " et il contient toutes les informations de routage. Dans le cas d'une basse mobilité, des paquets plus petits dits " *incrémental* ", qui contiennent juste les informations de routage qui ont changé depuis la dernière mise à jour complète, sont utilisés. Une autre solution pour réduire le trafic dans le réseau est que les nœuds reportent les mises à jour par un laps de temps qui vaut le temps moyen que nécessite la découverte du chemin le plus court vers une destination donnée [18].

II.2.7.3. Le protocole de routage réactif DSR (Dynamic Source Routing)

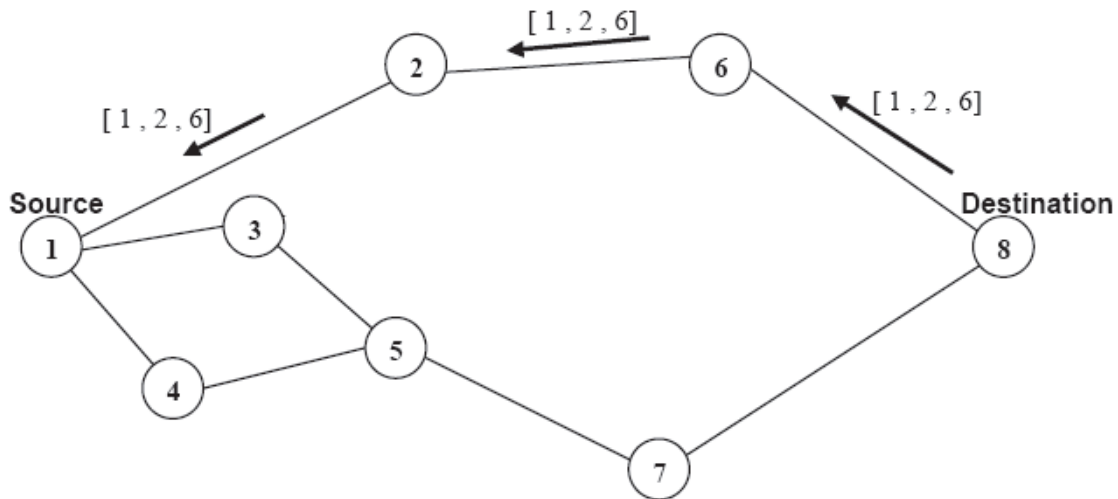
Ce protocole a la particularité de ne pas nécessiter la présence de tables de routage sur les différents nœuds du réseau, puisqu'il repose sur le principe du routage par la source.

Il est composé de deux mécanismes : la découverte des chemins et la maintenance des chemins. Dans cette technique la source détermine la séquence complète des nœuds à travers lesquels les paquets de données seront envoyés. Avant d'envoyer un paquet de données vers un autre nœud, l'émetteur diffuse un paquet "route request" vers tous ses voisins. Si l'opération de découverte de routes est réussie, l'émetteur reçoit un paquet "route réponse" qui contient une séquence de nœuds à travers laquelle la destination peut être atteinte. Le paquet "route request" contient un champ d'enregistrement de routes, dans lequel sera accumulée la séquence des nœuds visités durant la propagation de la requête dans le réseau. [17].

L'utilisation de la technique de routage par la source, fait que les nœuds de transit n'ont pas besoin de maintenir les informations de mise à jour pour envoyer les paquets de données.



Paquet de découverte de route



Renvoi du chemin par la destination

Figure II.5 : Exemple de routage dans le DSR

II.2.7.4. Le Protocole de routage réactif AODV (Ad-hoc On Demand Distance Vector)

Le protocole de routage AODV, tout comme DSR, repose sur le mécanisme de découverte de chemins à la demande mais il n'utilise pas le routage source. Il est basé sur le principe, vecteur à distance. Il ne construit de routes entre les nœuds que lorsqu'elles sont demandées par les nœuds sources afin de réduire le nombre de diffusions de messages. La découverte de la route se fait par inondation : une route entre deux nœuds est envoyée suite à l'envoi d'une « Route Request » (RREQ). Un signal de réponse « Route Reponse » (RREP) est alors envoyé par un nœud voisin s'il est possible de se joindre à une route existante et il met à jour sa table de routage, puis par la destination lorsque celle-ci est atteinte.

AODV s'appuie sur le routage saut par saut. Chaque nœud dans AODV, maintient une table de routage et utilise les numéros de séquence comme DSDV pour éviter le problème des boucles de routage. Les numéros de séquences permettent d'utiliser les routes les plus récentes.

Toutefois, si la destination n'est pas connue au préalable, si le chemin existant vers la destination a expiré, ou s'il est devenu défaillant, la route peut ne pas exister. Néanmoins, AODV garde une table de routage, au niveau de chaque nœud de transit tout en maintenant les chemins d'une façon distribuée.

La maintenance des chemins dans AODV est basée sur l'échange périodique des paquets Hello qui sont effectués dans le but de maintenir des routes cohérentes. Quoique, si

on ne reçoit aucun message "Hello" après un laps de temps bien déterminé à partir d'un nœud voisin, le lien est considéré comme défaillant. Par ailleurs, quand la topologie du réseau change, AODV ne présente pas de boucles de routage et offre une convergence rapide.

✧ *Avantages et Inconvénients :*

L'un des avantages d'AODV est l'utilisation de numéro de séquence dans les messages. Ces numéros de séquences permettent d'éviter les problèmes de boucles infinies et sont essentiels au processus de mise à jour de la table de routage.

Un autre avantage est le rappel de l'adresse IP du nœud origine dans chaque message. Ceci permet de ne pas perdre la trace du nœud à l'origine de l'envoi du message lors des différents relais.

Un inconvénient d'AODV est qu'il n'existe pas de format générique des messages. Chaque message a son propre format : RREQ, RREP, RERR.

II.2.7.5. Le protocole de routage hybride ZRP (Zone Routing Protocol) :

ZRP est un protocole de routage dit hybride. Il met en place, simultanément, un routage proactif et un routage réactif, afin de combiner les avantages des deux approches.

Dans le ZRP le réseau est décomposé en plusieurs zones de routages chevauchées. Appelées « zone de routage ». La zone de routage d'un nœud est définie comme l'ensemble des nœuds qui se trouvent à une distance inférieure ou égale au rayon de la zone. Ce rayon correspond au nombre de sauts maximum qu'il peut y avoir entre deux nœuds.

Les nœuds qui se trouvent exactement à une distance égale au rayon de la zone sont appelés "nœuds périphériques".



Figure II.6 : Zone de routage dans le protocole ZRP

Le routage au sein d'une zone se fait de manière proactive, via le protocole IARP (Intrazone Routing Protocol) et le routage vers les nœuds extérieurs de la zone se fait de façon réactive, grâce au protocole IERP (Interzone Routing Protocol).

Le routage intrazone peut être assuré par n'importe quel protocole de routage proactif, à condition qu'il soit modifié pour que la portée des mises à jour soit restreinte au rayon de la zone de routage. Le routage interzone est assuré par un cycle RREQs- RREPs. Quand un nœud reçoit un paquet RREQ s'il n'est pas destination et si encore la destination ne réside pas dans sa zone, il renvoie le RREQ uniquement vers les nœuds périphériques. Cela limite considérablement le nombre des RREQs propagés dans le réseau. Les performances de ZRP dépendent de la valeur choisie pour le rayon des zones. Pour des grandes valeurs, ZRP se comporte comme un protocole de routage purement proactif tandis que pour des petites valeurs, il se comporte comme un protocole de routage purement réactif.

II.3. Qualité de service :

II.3.1. Définition de la Qualité de service :

Le terme QoS (acronyme de « Quality of Service », en français « Qualité de Service ») désigne la capacité à fournir un service (notamment un support de communication) conforme à des exigences en matière de temps de réponse et de bande passante.

Appliquée aux réseaux à commutation de paquets (réseaux basés sur l'utilisation de routeurs) la QoS désigne l'aptitude à pouvoir garantir un niveau acceptable de perte de paquets, défini contractuellement, pour un usage donné (voix sur IP, vidéo-conférence, etc.).

II.3.2. Les classes de services :

Une classification des principales applications est présentée comme suit :

- Voix : Regroupe toutes les applications du type conversationnel (Voix, Visio Conférence, ...) ayant pour contrainte forte des objectifs sur le délai et la gigue. Elles sont également sensibles au taux de perte bien qu'il ne soit pas possible de retransmettre les données et requièrent des débits assez faibles,

- Vidéo : Regroupe toutes les applications multimédia diffusées ou non (Vidéo à la Demande – VoD, la télévision sur IP – IP TV, ...) ayant pour contrainte forte le taux de perte et le débit et dans une moindre mesure le délai et la gigue,

- Donnée : Regroupe toutes les applications de transfert de données ayant pour seule contrainte un taux de perte nul et qui s'accommodent d'un délai et d'une gigue quelconque. Un débit garanti caractérise cette classe sans toutefois en faire une contrainte stricte,

II.3.3. Niveaux de service :

Le terme « niveau de service » (en anglais *Service level*) définit le niveau d'exigence pour la capacité d'un réseau à fournir un service point à point ou de bout en bout avec un trafic donné. On définit généralement trois niveaux de QoS :

- Meilleur effort (en anglais *best effort*) : ne fournissant aucune différenciation entre plusieurs flux réseaux et ne permettant aucune garantie. Ce niveau de service est ainsi parfois appelé *lack of QoS*.
- Service différencié (en anglais *differentiated service* ou *soft QoS*) : permettant de définir des niveaux de priorité aux différents flux réseau sans toutefois fournir une garantie stricte.
- Service garanti (en anglais *guaranteed service* ou *hard QoS*) : consistant à réserver des ressources réseau pour certains types de flux. Le principal mécanisme utilisé pour obtenir un tel niveau de service est RSVP (*Resource reSerVation Protocol*, traduisez *Protocole de réservation de ressources*).

II.3.4. Paramètres de la qualité de service :

Pour qu'une conversation audio puisse être comprise par les interlocuteurs, la qualité de celle-ci est importante. Cependant, cette qualité est dépendante de plusieurs paramètres.

Les principaux paramètres sont les suivants :

- Débit :

En anglais *bandwidth*, parfois appelé *bande passante* par abus de langage, il définit le volume maximal d'information (bits) par unité de temps. Il existe deux modes de disponibilité de la bande passante, en fonction du type de besoin exprimé par l'application. Le mode "burst" est un mode immédiat, qui monopolise toute la bande passante disponible (lors d'un transfert de fichier par exemple). Le mode "Stream" est un mode constant, plus adapté aux fonctions audio/vidéo ou aux applications interactives.

- Le délai de transit (latence) :

C'est le délai de traversée du réseau, d'un bout à l'autre, par un paquet. Les différentes applications présentes sur ce réseau n'auront pas le même degré d'exigence en fonction de leur nature : faible, s'il s'agit d'une messagerie électronique ou de fichiers échangés, ce degré d'exigence sera fort s'il s'agit de données "voix". La latence dépend du temps de propagation (fonction du type de média de transmission), du temps de traitement (fonction du nombre d'équipements traversés) et de la taille des paquets (temps de sérialisation).

- La gigue :

Désigne les variations de latence des paquets. La présence de gigue dans les flux peut provenir des changements d'intensité de trafic sur les liens de sorties des commutateurs. Plus globalement, elle dépend du volume de trafic et du nombre d'équipements sur le réseau.

- Perte de paquet :

En anglais *packet loss*, Correspond aux octets perdus lors de la transmission d'un paquet de données, la plupart du temps due à un encombrement du réseau. S'exprime en taux de perte.

II.3.5. La QOS dans les réseaux maillés sans fil :

Depuis 2005, l'annexe 802.11e ajoute à la norme Wifi une gestion de QoS sur la couche MAC. Ceci est nécessaire pour les applications à temps critiques comme la téléphonie, ou le transport de vidéo (streaming).

Les besoins de la QoS sont différents selon le type de l'application. Par exemple, pour les applications temps-réel, comme la voix et la vidéo, le délai de bout en bout d'un paquet doit être limité, autrement le paquet est inutile. Les applications qui ne sont pas en temps-réel, comme le transfert de fichier ou la messagerie, se focalisent quant à elles sur la fiabilité des communications.

Il est très difficile de garantir une QoS prédéterminée à une application temps-réel dans un WMN, car il faut prendre en considération les spécificités de ces réseaux, à savoir: la bande passante limitée, le changement dynamique de la topologie dans le temps ainsi que le manque d'information complète sur l'état du réseau. En outre, la communication entre les stations mobiles, étant effectuée par voie radio, la qualité du lien sans fil reste peu fiable, et sujette à des variations selon la configuration et l'état du réseau.

II.4. conclusion :

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

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

Des études sont en cours pour essayer de définir des protocoles intégrant cette qualité de service et reposant sur les méthodes de routage au mieux développées spécifiquement pour les réseaux maillés sans fil.

CHAPITRE III :
ETUDE COMPARATIVE
ENTRE LES
PROTOCOLES AODV ET
DSR

III.1. Introduction :

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

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

Comme nous l'avons vu précédemment le routage est une méthode d'acheminement des informations à la bonne destination à travers un réseau de connexion donné. Lors de la transmission d'un paquet de données d'une source vers une destination, il est nécessaire de faire appel à un des protocoles de routage qui acheminera correctement le paquet par le meilleur chemin.

Ces différents protocoles sont en fait différents moyens adaptés à une situation de topologie dynamique, capables d'effectuer une « distribution des chemins » en limitant les sauts (chemin optimal), en évitant les boucles (très néfastes car causant des pertes de paquets au sein du réseau) et en minimisant l'« overhead » (données supplémentaires liées au contrôle de transfert et à la correction d'erreur).

Dans le chapitre précédant nous avons présenté un certain nombre de protocoles de routage mais dans ce qui va suivre nous allons-nous intéressés plus particulièrement à deux d'entre eux. Il s'agit des deux protocoles de routage réactifs : AODV et DSR.

III.2. Motivation :

D'après l'analyse effectuée dans le chapitre II et littérature existante, les protocoles de 1ère génération AODV et DSR offrent de très bonnes performances, en ce qui concernent le débit et le délai de bout en bout, sur des réseaux de petite taille (de l'ordre de la centaine de nœuds) et des charges de réseau faibles.

L'une des raisons qui nous a poussé à tester le DSR est le fait qu'il offre la possibilité d'avoir plusieurs routes dans son cache et que seuls : l'ajout des types de nœuds ainsi que la modification de la procédure de sélection de route, sont nécessaires pour arriver à montrer l'intérêt de la différenciation de terminaux. Dans ce cas, aucun ajout de nouveaux messages, ou modification dans le fonctionnement du protocole lui-même ne sont effectués.

Le protocole AODV représente essentiellement une amélioration de l'algorithme DSR, Il a pour avantage de réduire le nombre de diffusions de messages et cela en créant les routes

lors du besoin, ceci peut être très intéressant lorsqu'un réseau est très grand et composé de nombreux nœuds, Il est capable de s'adapter aux changements de topologie du réseau en trouvant très rapidement un chemin alternatif sans devoir reconstruire la route dans son entièreté.

III.3. Etude des protocoles de routage :

III.3.1. le protocole AODV :

Le protocole AODV (*Ad hoc On-demand Distance Vector*) appartient à la famille des protocoles à la Demande, il est considéré comme la combinaison de DSR et de DSDV. Il combine les mécanismes de découverte et de maintenance de routes de DSR en y associant le numéro de séquence (pour le maintien de la consistance des informations de routage) de DSDV.

La découverte de route permet de trouver une route pour atteindre une destination et cela en inondant un paquet de requête dans tout le réseau, tandis que La maintenance de route permet de détecter et signaler les coupures de routes provoquées éventuellement par la mobilité des nœuds.

Pour créer et maintenir ces routes, AODV utilise trois types de messages le RREQ (Route Request) pour demander une route, le RREP (Route Reply) pour répondre à une requête de demande de route, et le RERR (Route Error) pour signaler une coupure de route.

En plus du routage nœud-par-nœud et l'échange périodique, L'AODV utilise le principe des numéros de séquence À fin de maintenir la consistance des informations de routage, ce qui Permet aux nœuds d'utiliser les routes les plus fraîches suivant leurs numéros de séquence.

AODV n'utilise pas des mises à jour périodiques, les routes sont découvertes et maintenues selon les besoins ce qui réduit le nombre de diffusions de messages [16].

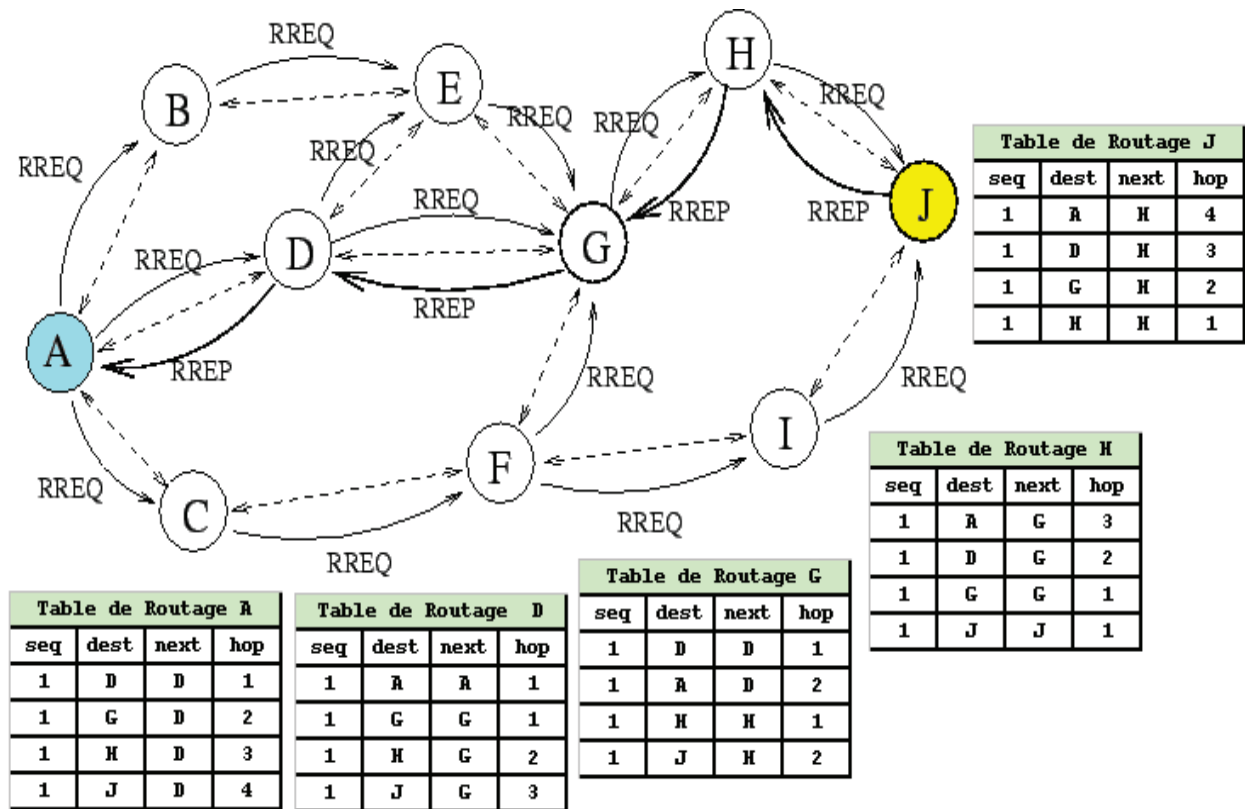


Figure III.1 : fonctionnement du protocole AODV

La figure ci-dessus illustre une recherche de route à l'initiative du nœud A et en direction de J et les différentes tables de routages constituées. La diffusion du message RREQ à partir de A se fait en broadcast vers tous ses voisins. Lorsque que J reçoit le message il retourne un message RREP à A en passant par H, G et D.

III.3.1.1. Table de routage et paquets de contrôle :

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.

Une entrée de la table de routage contient essentiellement :

- L'adresse IP de la destination.
- Next Hop : Adresse IP du prochain nœud en direction de la destination (Le nœud suivant).
- Hop count : Le nombre de saut nécessaire pour atteindre la destination.

- La distance en nombre de nœud (i.e. le nombre de nœud nécessaire pour atteindre la destination).
- Le numéro de séquence de la destination : Il permet de faire la distinction entre une ancienne information de routage se propageant dans le réseau et une nouvelle due par exemple à un changement de topologie.
- Life time : Durée de vie d'une route. Pour une route active ce champ indique l'instant où elle deviendra invalide. Pour une route invalide, ce champ indique l'instant de suppression de la route.
- Le temps d'expiration de l'entrée de la table : C'est le temps au bout duquel l'entrée est valide.
- Liste des voisins actifs (origine ou relais d'au moins un paquet pour la destination pendant un temps donné).
- Flags : Indique l'état de la route. Elle peut être valide (en cours d'utilisation), invalide (le timer a expiré, elle sera bientôt supprimée) ou en cours de réparation (la route a été brisée, une réparation est en cours a fin de la rétablir).
- Liste des précurseurs : Cette liste est constituée des adresses IP des nœuds précédents qui utilisent le nœud courant pour atteindre la destination. Ils font office de "Previous Hops" et permettent, lors d'une cassure, d'informer les nœuds de sa réparation.

Une entrée de la table est mise à jour lorsque le nœud reçoit un message contenant :

- ✓ un numéro de séquence plus élevé pour la destination.
- ✓ le même numéro de séquence mais un Hop Count plus petit.
- ✓ le même numéro de séquence mais que la route avait été marquée comme invalide ou en cours de réparation.

La mise à jour de ces tables s'effectue par l'échange de trois types de messages entre les nœuds :

- RREQ Route Request, un message de demande de route.
- RREP Route Reply, un message de réponse à un RREQ.
- RERR Route Error, un message qui signale la perte d'une route.

❖ *Format général d'une RREQ :*

@source	Num.seq.Source	Broadcast ID	@Destination	Num. Seq. Destination	Nombre de sauts
---------	----------------	--------------	--------------	--------------------------	-----------------

Figure III.2 : format général d'une route request

- Broadcast ID : Cet identifiant permet à chaque nœud recevant le paquet de faire la distinction entre un nouveau RREQ et un RREQ déjà reçu par un autre chemin. Le nœud source incrémente l'identifiant avant l'émission d'une nouvelle requête.
- L'adresse IP de la source et du destinataire.
- Le numéro de séquence de la source et du destinataire.
- Le nombre de sauts (Hop Count) initialisé à 0.

❖ *Format général d'une RREP :*

@source	@Destination	Num.seq. destination	Nombre de sauts	Life Time
---------	--------------	-------------------------	-----------------	-----------

Figure III.3 : format général d'une route réponse

- L'adresse IP et le numéro de séquence du destinataire (qui est la source du RREQ)
- L'adresse IP et numéro de séquence de la source (qui est le destinataire du RREQ).
- Nombre de sauts séparant le nœud courant de la destination du RREQ.
- Life time : les nœuds recevant le RREP doivent considérer la route comme étant valide à partir de cet instant.

III.3.1.2. Gestion des numéros de séquence :

Les protocoles à vecteur de distance sont en général sujets au problème de boucles de routage et de comptage à l'infini de l'algorithme de Bellman-Ford qu'ils utilisent, C'est un algorithme qui trouve le plus court chemin entre deux nœuds, Ce qui peut causer un phénomène de bouclage dans lequel les nœuds injoignables se voient attribuer des distances de plus en plus grandes.

Dans le cas d'AODV, ces problèmes sont résolus par l'utilisation de numéros de séquence pour les messages de contrôle [12].

Les numéros de séquence sont un moyen simple et efficace Pour éviter le problème des boucles infinies et des transmissions inutiles de messages sur le réseau. Ils permettent d'utiliser les routes les plus nouvelles ou autrement dit les plus fraîches (fresh routes).

Chaque nœud du réseau possède un numéro de séquence dont il est chargé à le maintenir à jour en l'incrémentant dans deux circonstances :

- Avant d'initier un processus de découverte de route, ce qui permet d'éviter les conflits avec les routes précédemment construites par ce même nœud.
- Avant l'émission d'un RREP par le destinataire, ce qui permet de mettre à jour les informations de routage des nœuds traversés par le paquet.

Chaque nœud maintient également un numéro de séquence dans sa table de routage pour chaque destinataire d'une route active. Ce numéro de séquence est mis à jour dans deux situations :

- Lors de l'expiration d'une route ou d'une cassure sur le chemin. Un nœud peut alors incrémenter le numéro de séquence du destinataire et invalider la route au prêt des autres nœuds.
- A la réception d'un message contenant un numéro de séquence plus élevé pour le même destinataire, le paquet contient alors des informations plus fraîches quant à la route.

III.3.1.3. La Découverte de route :

Le processus de découverte de la route dans le cas d'AODV consiste à construire des routes par l'emploi d'un cycle de requêtes « route request / route reply ».

Un nœud diffuse une requête de route (RREQ : Route REQuest), 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.

Après la réception de cette requête les nœuds mettent à jour leurs informations relatives à la source. Outre l'IP de la source, le numéro de séquence courant et l'identifiant de diffusion, le paquet RREQ contient également la dernière valeur du numéro de séquence, associée au nœud destination, connue par la source.

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.

Un nœud recevant un paquet RREQ émettra alors un paquet « route reply » (RREP) s'il est la destination ou s'il possède une route vers la destination avec un numéro de séquence supérieur ou égal à celui repris dans le paquet RREQ. Si tel est le cas, il envoie un paquet RREP vers la source.

Les tables de routage des différents nœuds sont mises à jours après chaque retransmission de ces messages RREQ et RREP.

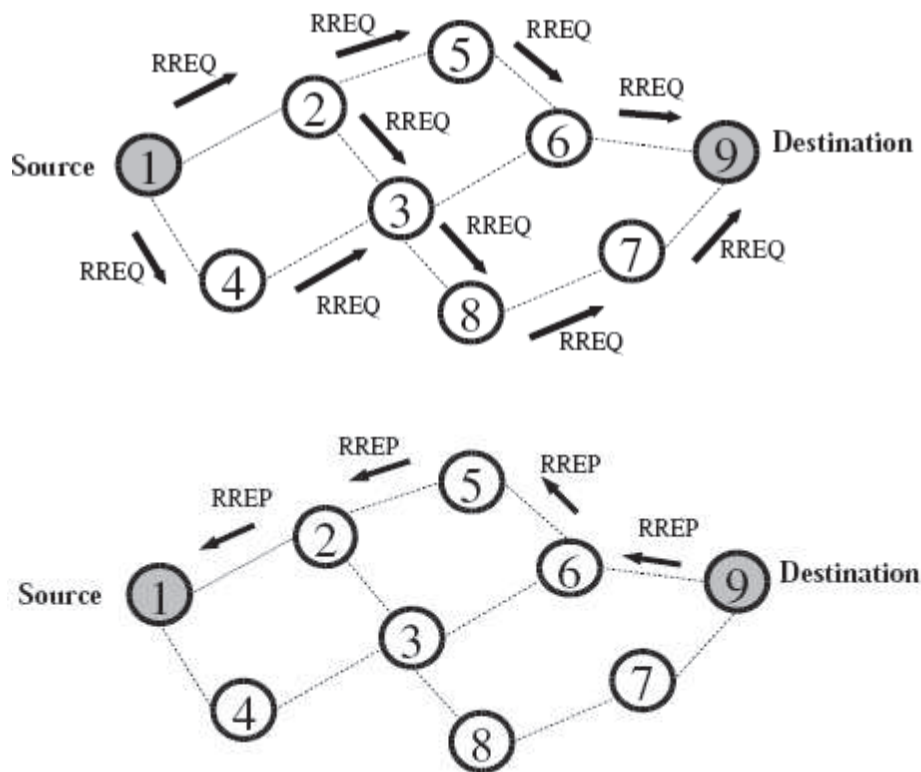


Figure III.4 : Inondation de RREQ et renvoi du RREP dans AODV

Si le nœud émetteur de la requête ne reçoit pas de réponse RREP pendant une certaine période il rediffuse une nouvelle requête. Si la requête RREQ est rediffusée un certain nombre de fois sans recevoir de réponse une erreur est déclenchée.

Un nœud intermédiaire (se trouvant entre un nœud source et un nœud destination) qui rediffuse une requête de route), sauvegarde l'adresse du nœud source qui a envoyé la requête

la première fois et l'adresse du nœud voisin qui lui a transmis la requête, cette information est utilisée pour reconstruire la route inverse qui sera traversée par la réponse de route (RREP).

III.3.1.4. La maintenance de route :

Comme nous l'avons déjà dit, le protocole AODV exécute lui aussi une procédure de maintenance de routes, cette procédure se fait par l'émission périodique d'un message "HELLO" (qui est un RREP avec un TTL (Time To Live) de 1), Le lien entre deux nœuds voisins sera considéré comme défaillant dans le cas où trois messages "HELLO" ne sont pas reçus respectivement.

L'AODV maintient les adresses des voisins à travers lesquels les paquets destinés à un certain nœud arrivent. Un voisin est considéré actif, pour une destination donnée, s'il délivre au moins un paquet de donnée sans dépasser une certaine période.

Une entrée de la table du routage est active, si elle est utilisée par un voisin actif. Le chemin reliant la source et la destination, en passant par les entrées actives des tables de routage, est dit un chemin actif. Les mouvements des nœuds qui ne participent pas dans ce chemin n'affectent pas la consistance des données de routage.

Si un lien entre deux nœuds est invalide (à cause de la mobilité ou la défaillance d'un nœud), les nœuds utilisant ce lien sont prévenus par un message d'erreur (RERR), ils vont alors diffusés une autre requête. La figure suivante illustre la coupure d'un lien entre deux nœuds et l'envoi du RERR dans AODV.

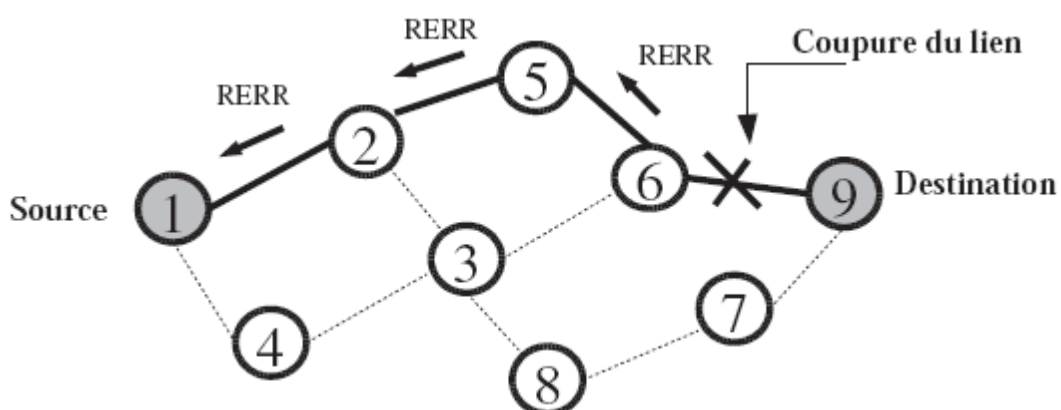


Figure III.5 : Coupure de route et envoi du RERR dans AODV.

Dans le cas des défaillances des liens, toutes les entrées des tables de routage participantes dans le chemin actif, et qui sont concernées par la défaillance, sont supprimées.

III.3.1.5. Analyse du protocole AODV :

Le protocole AODV (Ad-hoc On-demand Distance Vector) est un protocole de routage réactif ce qui signifie qu'une route vers une destination n'est construite que lorsqu'elle est nécessaire, il combine des mécanismes de découverte et de maintenance de routes avec le routage par sauts, l'utilisation de numéros de séquence et la transmission périodique de paquets Hello.

AODV emprunte l'utilisation des numéros de séquence de DSDV afin de dater les différentes routes pour avoir des routes à jour et se prémunir des boucles, tandis que sa procédure de découverte des routes est dérivée de celle adoptée par DSR

En raison de la mobilité des nœuds dans les réseaux maillés sans fils, les routes changent fréquemment ce qui fait que les routes maintenues par certains nœuds deviennent invalides, AODV possède des procédures de réparation locale de la route a son point de cassure. Par conséquent, il est capable de s'adapter aux changements de topologie du réseau en trouvant très rapidement un chemin alternatif sans devoir reconstruire la route dans son entièreté.

AODV utilise des tables de routage distribuées. Cela diminue l'overhead par paquet car chaque paquet est routé uniquement selon le champ adresse destination (routage par saut). De plus, les nœuds doivent périodiquement émettre des paquets Hello afin de maintenir la fraîcheur des informations de routage.

Le protocole de routage AODV n'assure pas l'utilisation du meilleur chemin existant entre la source et la destination mais il ne présente pas de boucle de routage et évite le problème "counting to infinity" de Bellman-Ford

Ce protocole a pour avantage de ne pas avoir un temps de réaction et Il est Adapté aux réseaux denses de taille moyenne et à forte mobilité, cependant il a une capacité d'échange du réseau limitée et un Trafic de contrôle important.

III.3.2.le protocole DSR :

DSR est un protocole de routage réactif qui utilise le routage de source afin d'envoyer des paquets de données. Il est composé principalement de deux mécanismes : découverte de route et Maintenance de route. Le premier permet de déterminer automatiquement les routes nécessaires à la communication entre nœuds, tandis que le second permet de s'assurer de la correction des routes tout au long de leur utilisation [13].

Comme dans AODV, la demande d'une route dans DSR exige une inondation avec des paquets *Route Request*.

Le protocole DSR n'intègre pas l'opération de découverte de routes avec celle de la maintenance. Quand un nœud détecte un problème de transmission, un message erreur de route est envoyé à l'émetteur original du paquet. Le message d'erreur contient l'adresse du nœud qui a détecté l'erreur et celle du nœud qui le suit dans le chemin. Lors de la réception du paquet erreur de route par l'hôte source, tous les chemins qui contiennent ce nœud sont supprimés. Ensuite, une nouvelle opération de découverte de routes vers la destination est initiée par l'émetteur [14].

Nous allons décrire les deux mécanismes dans les sous sections suivantes.

III.3.2.1. Découverte de route :

DSR étant un protocole réactif, un nœud source va rechercher une route uniquement s'il veut émettre un paquet vers un nœud destinataire, et qu'il ne possède aucune route vers celui-ci dans son cache.

Pour trouver la route depuis le nœud source, DSR initie une *Route Discovery* en émettant un paquet d'en-tête *Route Request* (RReq), qui va inonder le réseau comme dans le protocole AODV que nous avons vu précédemment. Ce paquet va donc être reçu par tous les nœuds intermédiaires du réseau.

Le destinataire reçoit plusieurs « *Route Request* » qui lui parvient de différents nœuds voisins et choisit, selon un algorithme qui tient compte du nombre de « sauts » minimisant le nombre de nœuds traversés et/ou de la qualité et de la rapidité des liaisons entre les nœuds [18].

Afin d'éviter des inondations inutiles du réseau, la procédure de demande de route commence d'abord à questionner les nœuds voisins s'ils ont une route disponible dans le voisinage direct. Ceci est fait en envoyant le premier paquet *Route Request* avec une limite de sauts égale à zéro, afin que celui-ci ne soit pas transféré ensuite aux voisins. S'il n'y a pas de réponses obtenues lors de cette demande initiale, un nouveau paquet *Route Request* est diffusé dans le réseau entier [17].

La *Route Request* contient :

- la source S et la destination D de la *Route Discovery*.
- un numéro unique de la requête (le ID).
- un enregistrement qui liste les adresses de chaque nœud intermédiaire à travers lesquels la copie de cette *Route Request* a été transmise.

Quand le destinataire D reçoit cette *Route Request*, il retourne à la source un paquet d'en-tête *Route Reply* (RRep) qui liste la séquence de nœuds à travers lesquels la destination peut être atteinte.

En outre, Dans le réseau, les nœuds peuvent enregistrer dans leur cache des informations de routage obtenues au travers des différents paquets *Route Discovery* reçus et des paquets de données. De plus, si un nœud intermédiaire qui reçoit un message *Route Request* possède en cache une route vers la destination, alors il envoie un *Route Reply* à la source en ajoutant la route connue, Si un nœud recevant un message *Route Request* a récemment vu un autre message *Route Request* contenant le même ID et la même adresse de destination, ou si la propre adresse du nœud est déjà listée dans la *Route Request*, alors le nœud supprime la requête.

Finalement, le nœud source obtient plusieurs routes pour atteindre le destinataire. Une fois ces routes connues, le nœud va pouvoir envoyer des paquets d'option *Source Route* (SrcR) contenant les données à échanger

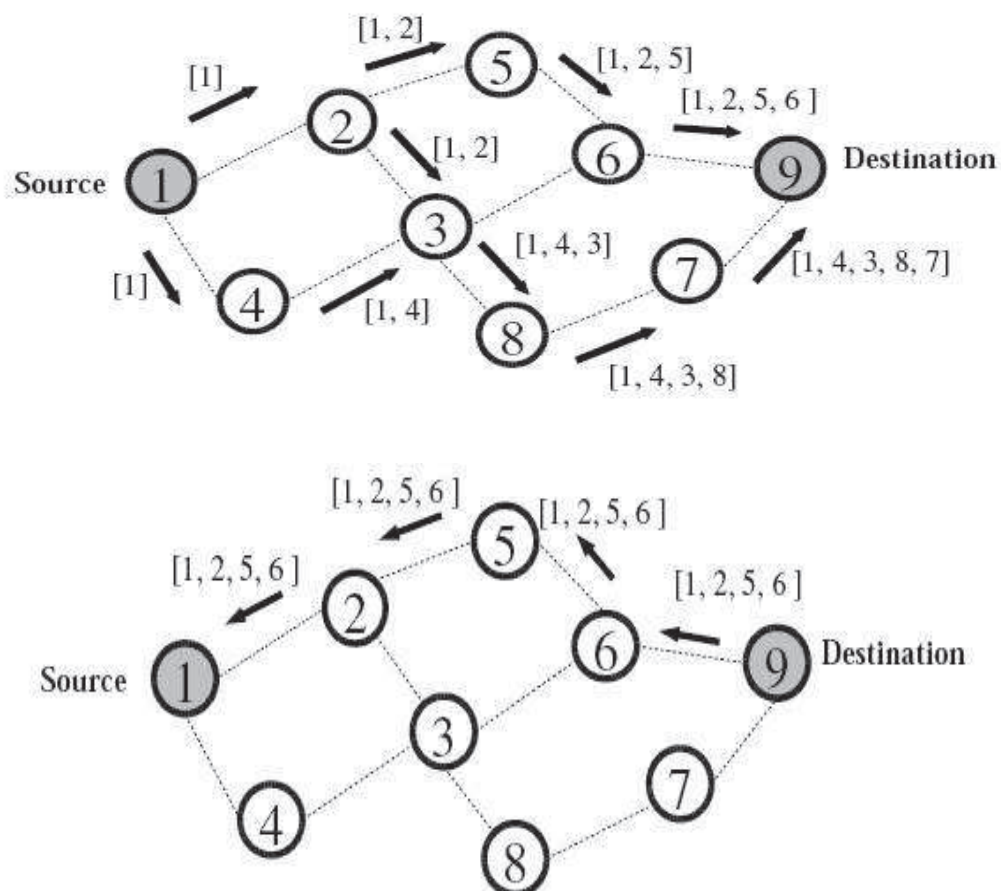


Figure III.6 : Découverte de route dans le protocole DSR

- *Quelques notions sur la découverte de route :*

- écoute active (Snooping) : lorsqu'un nœud transmet un paquet de données ou qu'il écoute le support, il peut enregistrer dans sa table de routage le chemin présent dans le paquet.

- réponse du cache (Replying from Cache) : si un nœud reçoit une requête de route pour laquelle il possède un chemin dans son cache, il renvoie directement une réponse à la source et ne rediffuse pas la requête. Ainsi, la découverte de routes est accélérée.

- limitation de la portée des requêtes : cette optimisation consiste à ajuster le TTL du paquet IP qui contient la requête de route. Le but est d'éviter l'inondation du réseau avec des paquets de requête. Deux techniques de découverte de route en découlent :

- Réponse des voisins (Non-propagating Route Request) : quand un nœud entreprend une découverte de routes, il envoie en premier lieu une requête en positionnant le TTL (du paquet IP qui la contient) à 1, afin qu'elle ne soit pas rediffusée par ses voisins. Si aucune réponse n'a été reçue après expiration d'un timer, la source déclenche une requête avec un TTL égal à la taille maximale d'une route. Cette optimisation prévient l'inondation inutile du réseau quand un des voisins est la destination recherchée ou qu'il possède la route adéquate.
- recherche incrémentale (Expanding Ring Search) : le nœud commence par envoyer une requête de route "Non-propagating" avec un TTL égal à 1. Si le nœud ne reçoit pas de réponse, il double la valeur du TTL lors de sa requête suivante. Il poursuit ce processus jusqu'à ce qu'il reçoive une réponse de route. Avec cette technique, le nœud explore progressivement le réseau pour ne pas inonder systématiquement le réseau.

Les techniques visant à limiter la portée des requêtes de route peuvent également être utilisées dans le protocole AODV.

III.3.2.2. Maintenance de routes :

Le nœud initie ou relaie un paquet de données, il doit s'assurer que le nœud suivant dans le chemin a effectivement reçu le paquet.

Le contrôle de la réception du paquet par le nœud suivant se fait au niveau MAC (par exemple, grâce au mécanisme d'acquiescement du 802.11). Un nœud qui transmet un paquet en utilisant un chemin source est responsable de confirmer la bonne réception de ce dernier ; le paquet est retransmis jusqu'à la réception d'une confirmation ou jusqu'à ce que le nombre maximal de retransmission soit atteint.

Si les tentatives de retransmission s'avèrent impossible ou le nombre maximal de retransmissions est atteint, le mobile qui a détecté la défaillance envoie un paquet d'erreur (Route Error) vers la source, indiquant quel nœud est à l'origine du problème. La source tronque alors les routes de son cache contenant le lien erroné. Si la source dispose d'une autre route vers la même destination (grâce à des réponses de routes supplémentaires issues de sa découverte de routes ou bien via un chemin obtenu par écoute des autres paquets), elle poursuit l'émission avec sa nouvelle route. Dans le cas contraire, elle effectue une nouvelle découverte de routes.

- *Quelque notion sur la maintenance de route :*

- récupération de route (Salvaging) : le nœud détectant l'inaccessibilité d'un nœud suivant consulte son cache à la recherche d'un autre chemin menant à la destination. S'il possède une route, il renvoie un message d'erreur vers la source en précisant les modifications apportées au chemin et il transmet le paquet de données avec la nouvelle route. Sinon, le nœud peut lancer une découverte de route ciblée vers le nœud destinataire. Ainsi, on évite de repartir de la source.

- annonce de route erronée (Gratuitous Route Errors) : lorsqu'une source reçoit un message d'erreur de route, elle le joint à sa nouvelle requête de route. Ainsi, elle ne recevra pas de réponse contenant le chemin erroné.

III.3.2.3. Analyse du protocole DSR :

Le protocole DSR (Dynamic Source Routing) est un protocole de routage pour les réseaux mailles sans fils, il est basé sur l'utilisation de la technique "routage à la source" c'est-à-dire c'est à la source de déterminer la séquence complète des nœuds selon lesquelles, les paquets de données seront envoyés. Les nœuds n'ont pas besoin de tables de routage. Les deux opérations de base de DSR sont : la découverte de routes (route discovery) et la maintenance de routes (route maintenance).

Il est similaire à AODV dans le sens où la demande d'une route dans DSR exige une inondation avec des paquets Route Request. Quand un nœud veut transmettre,

Afin de réduire le coût et la fréquence de la découverte de routes, chaque nœud garde trace des chemins trouvés à l'aide des paquets de réponses. Ces chemins sont utilisés jusqu'à ce qu'ils soient invalides.

L'un des principaux avantages du DSR réside dans son fonctionnement purement réactif car les mécanismes de routage ne sont déployés qu'en cas de besoin, réduisant ainsi la

consommation de bande passante. Ceci, couplé avec le routage par la source permet d'éviter les boucles et élimine le besoin d'envois périodiques de message de mise à jour.

De plus, de cette façon, seule la source doit maintenir une route cohérente vers la destination et aucune mémorisation n'est nécessaire sur les nœuds intermédiaires.

Cependant, l'utilisation du routage source implique un overhead important par paquet de données car la route est incluse dans chaque en-tête. De nombreuses optimisations ont été apportées à l'algorithme initial du DSR.

Le protocole DSR n'est pas très efficace dans les grands réseaux étant donné que chaque source doit avoir la vision du réseau. Mais pour les petits et moyens réseaux, il prend un avantage sur AODV.

III.3.3. Comparaison entre les protocoles AODV et DSR

Dans notre mémoire et pour mieux exposer notre étude approfondie sur les deux protocoles étudiés, deux tableaux seront définies : le premier tableau expose les différences entre les deux protocoles en terme de fonctionnement, et le deuxième tableau va résumer les avantages et les inconvénients de chaque protocoles, afin d'exploiter notre étude théorique lors de nos simulations qui vont suivre dans le prochain chapitre.

AODV	DSR
Utilise une table de routage	N'utilise pas de table de routage
La maintenance de route se fait au niveau de la table de routage	La maintenance de route se fait dans le cache de route
la Découverte de route s'effectue par une inondation	la Découverte de route s'effectue par une inondation
Utilise des messages « HELLO » mais avec les voisins actifs seulement	N'utilise pas des messages « HELLO »
La route découverte est stockée à chaque nœud	La route découverte est insérée dans l'entête du paquet
Utilise un numéro de séquence	N'utilise pas de numéro de séquence, il maintient la totalité des routes aussi longtemps que cela est nécessaire.

Utilise des temporisateurs de route	N'utilise pas des temporisateurs de route
Une seule route disponible	Multiple routes disponibles
Pas besoin de mise à jour périodique	Pas besoin de mise à jour périodique

Tableau III.1 : Tableau comparatif

	AODV	DSR
Avantages	le rappel de l'adresse IP du nœud origine dans chaque message. Ceci permet de ne pas perdre la trace du nœud à l'origine de l'envoi du message lors des différents relais.	Chaque nœud garde trace des chemins trouvés ce qui réduit le coût et la fréquence de la découverte de routes.
	possède des procédures de réparation locale de la route à son point de cassure.	les mécanismes de routage ne sont déployés qu'en cas de besoin ce qui réduit la consommation de bande passante.
	ne présente pas de boucle de routage et évite le problème "counting to infinity" de Bellman-Ford.	permet d'éviter les boucles et élimine le besoin d'envois périodiques de message de mise à jour.
	utilise des tables de routage distribuées. Cela diminue l'overhead par paquet.	aucune mémorisation n'est nécessaire sur les nœuds intermédiaires.
	Adapté aux réseaux denses de taille moyenne et à forte mobilité.	Efficace pour les petits et moyens réseaux.

	Utilise les numéros de séquences qui permettent d'éviter les problèmes de boucles infinies et qui sont essentiels au processus de mise à jour de la table de routage.	Connaissance totale par un nœud de la route empruntée.
Inconvénients	n'assure pas l'utilisation du meilleur chemin existant entre la source et la destination.	un overhead important par paquet de données car la route est incluse dans chaque en-tête.
	a une capacité d'échange du réseau limitée et un Trafic de contrôle important.	Le protocole DSR n'est pas très efficace dans les grands réseaux
	il n'existe pas de format générique des messages. Chaque message a son propre format : RREQ, RREP, RERR.	il n'existe pas de format générique des messages. Chaque message a son propre format : RREQ, RREP, RERR.

Tableau III.2 : résumé des avantages et des inconvénients

III.4. Conclusion :

Dans ce chapitre nous avons présenté deux protocoles de routages réactifs (AODV et DSR) qui ont été proposés pour assurer le service de routage dans les réseaux maillés sans fil. Nous avons décrit leurs principales caractéristiques et fonctionnalités afin de comprendre les stratégies utilisées dans l'acheminement des données entre les différentes unités mobiles.

Assurer la connexion de tous les nœuds d'un réseau maillés sans fil est un problème très complexe vu la dynamique et l'évolution rapide de la topologie, en effet les unités mobiles sont dynamiquement et arbitrairement éparpillés d'une manière ou l'interconnexion peut changer à tout moment. Le but d'un protocole de routage est donc, l'établissement de routes qui soient correctes et efficaces entre une paire quelconque d'unités. Les protocoles de routage étudiés offrent différents avantages qui sont en réalité complémentaires et préférables pour différents types d'applications.

CHAPITRE IV :
ANALYSE ET
SIMULATION

IV.1. Introduction :

Après l'analyse et la comparaison des deux protocoles de routage (AODV et DSR) effectué dans le troisième chapitre nous allons procéder à la simulation.

Cette dernière permet à l'utilisateur de définir un réseau et de simuler des communications entre les nœuds de ce réseau, de tester à moindre coût les nouveaux protocoles, d'anticiper les problèmes qui pourront se poser dans le futur et d'implémenter la technologie la mieux adaptée aux besoins.

Nous avons choisi le logiciel NS2 car c'est un très bon outil dans le domaine de la recherche, et du développement de nouveaux protocoles pour différents types de réseaux.

Ce chapitre est composé de trois parties :

Dans la première partie nous allons présenter le simulateur utilisé pour cette simulation, qui est le NETWORK SIMULATOR2 ou NS2.

Dans la deuxième partie nous allons faire une comparaison entre les deux protocoles de routage réactif (AODV et DSR) qui sont déjà intégré dans le simulateur NS2.

Dans la dernière partie nous allons proposer une combinaison entre ces deux protocoles de routage.

IV.2. Présentation du simulateur NS2 :*IV.2.1. Généralité :*

NS2, Network Simulator, est aujourd'hui le simulateur de réseau probablement le plus utilisé par la communauté scientifique des réseaux. Il s'agit d'un simulateur à événements discrets, fruit de la collaboration entre l'université de Berkeley, USC (University of Southern California) et le centre de recherche Xerox PARC (Palo Alto Research Center) dans le cadre du projet VINT2 (Virtual Inter Network Testbed). Ce projet est soutenu par DARPA3 (Defense Advanced Projects Agency) Ou (agence avancée de projets de la défense).

NS est un outil de recherche très utile pour la compréhension des protocoles. Il sert aussi bien dans l'étude des protocoles de routage qu'à l'étude des réseaux mobiles ou les communications par satellites. Il permet à l'utilisateur de définir un réseau et de simuler les communications entre nœuds. Le simulateur utilise le langage orienté objet OTCL pour la description des conditions de simulation sous forme de script. Dans le script l'utilisateur fournit la topologie du réseau, les caractéristiques des liens physiques, les protocoles utilisés, le type de trafic généré par les sources, les événements,...etc.

Si le script écrit en OTCL permet une utilisation (édition, modification des simulations) facilitée du simulateur, Les protocoles sont codés avec le C++ pour avoir une plus grande puissance de calculs. La simulation doit d'abord être saisie sous forme de fichier texte que NS va utiliser pour produire un fichier trace contenant les événements qui se sont déroulés durant la simulation à chaque instant. Un traitement ultérieur de ce fichier permet d'en soustraire l'information souhaitée.

Par ailleurs le simulateur permet la création d'un fichier d'animation (d'extension.tr), permettant de visualiser la simulation sur l'interface graphique NAM. Ce visualisateur fournit une représentation du graphe du réseau sur laquelle on peut voir les paquets circuler, suivre le niveau des files d'attente et observer le débit courant des liaisons.

- *Les langages utilisés par NS2 :*

Network Simulator NS-2 utilise les deux langages suivants :

- TCL (Tool Command Language) est un langage de commande qui sert à contrôler les applications.

TCL offre des structures de programmation telles que les boucles, les procédures ou les notions de variables. Il y a deux principales façons de se servir de TCL :

- Comme un langage autonome interprété.
- Comme une interface applicative d'un programme classique écrit en C ou C++.

D'autre part, l'utilisateur souhaite changer rapidement ses scénarios de simulation, dans ce cas l'orienté objet OTCL offre une bonne solution.

- Le C++ offre une création rapide et efficace des objets et variables manipulés lors de la simulation.

IV.2.2.Principe de base :

L'application NS se compose de deux éléments fonctionnels :

- Un interpréteur : au moyen de l'interpréteur l'utilisation est capable de créer le modèle De simulation ce qui revient à assembler les différents composants nécessaires à l'étude. Les composants du modèle de simulation sont appelés (objets) ou encore (instances de classe).
- Le moteur de simulation : effectue les calculs applicables au modèle préalablement construit par l'utilisateur via l'interpréteur.

NS bénéficie de toutes les possibilités qu'offrent les techniques objets comme l'héritage, le polymorphisme, la surcharge,... etc. l'héritage permet d'élaborer des arborescences de classes.

IV.2.3. Visualisation des résultats :

IV.2.3.1. fichier trace :

On va demander à NS de récolter un certain nombre de données statistiques relatif au déroulement de la simulation et de les sauvegarder dans un fichier « trace ». La commande qui permet d'obtenir un tel fichier (dans cet exemple nommé out.all) est la suivante :

```
Set trace [open out.all]
$ns trace-all $trace proc finish {} {global trace
Close $trace}
```

Ce fichier va contenir tous les événements survenus de la simulation :

L'arrivée d'un paquet à un nœud, départ d'un paquet d'un nœud, perte d'un paquet ou encore réception d'un paquet par un agent. Chaque paquet peut donc être suivi tout au long de son parcours.

En traitant ce fichier de très grande taille on va pouvoir en extraire l'information souhaitée : calcul de débit aux nœuds, évaluation des pertes, ...etc. voici un extrait d'un tel fichier.

+	8.5623	0	1	tcp	1000	----- 0	2.0	3.0	4562	102
-	8.5789	0	1	ack	40	----- 1	2.0	3.0	4586	103
D	8.8789	2	3	tcp	1000	----- 1	2.0	3.0	4586	99
R	8.9789	2	3	tcp	1000	----- 1	2.0	3.0	4596	253

Chacune des lignes correspond à un évènement survenu à un paquet.

Voici le détail de ce que contiennent ces colonnes. En commençant par la colonne de gauche.

1. Action effectuée sur le paquet. Un « + » signifie que le paquet est reçu dans une file, un « - » signifie que le paquet quitte la file, un « d » signifie que le paquet est jeté et un « r » signifie que le paquet est réceptionné par un agent.
2. Instant ou l'action est effectuée.
3. Nœud de départ du lien concerné.

4. Nœud d'arrivée du lien concerné.
5. Type de paquet.
6. Taille du paquet en bytes.
7. Flags
8. Identificateur de flux.
9. Agent de départ.
10. Agent d'arrivée.
11. Numéro de séquence.
12. Identificateur unique pour chaque paquet.

IV.2.3.2. Interface graphique Nam (Network Animator):

NS-2 ne permet pas de visualiser le résultat des expérimentations. Il permet uniquement de stocker une trace de la simulation, de sorte qu'elle puisse être exploitée par un autre logiciel, comme NAM.

Le Nam est un outil d'animation basé sur Tcl/Tk, utilisé dans NS afin de visualiser le tracé de simulation des réseaux, ainsi que les tracés de données. Le modèle théorique du NAM a été non seulement créer pour lire un large ensemble de données d'animation, mais aussi suffisamment extensible pour être utilisé quel que soit le type de réseau simulé (fixe, mobile ou mixte). Ce qui permet de visualiser tout type de situation possible. Par exemple, il est capable de représenter des paquets TCP ou UDP, la rupture d'un lien entre noeuds, ou encore de représenter les paquets rejetés d'une file d'attente pleine.

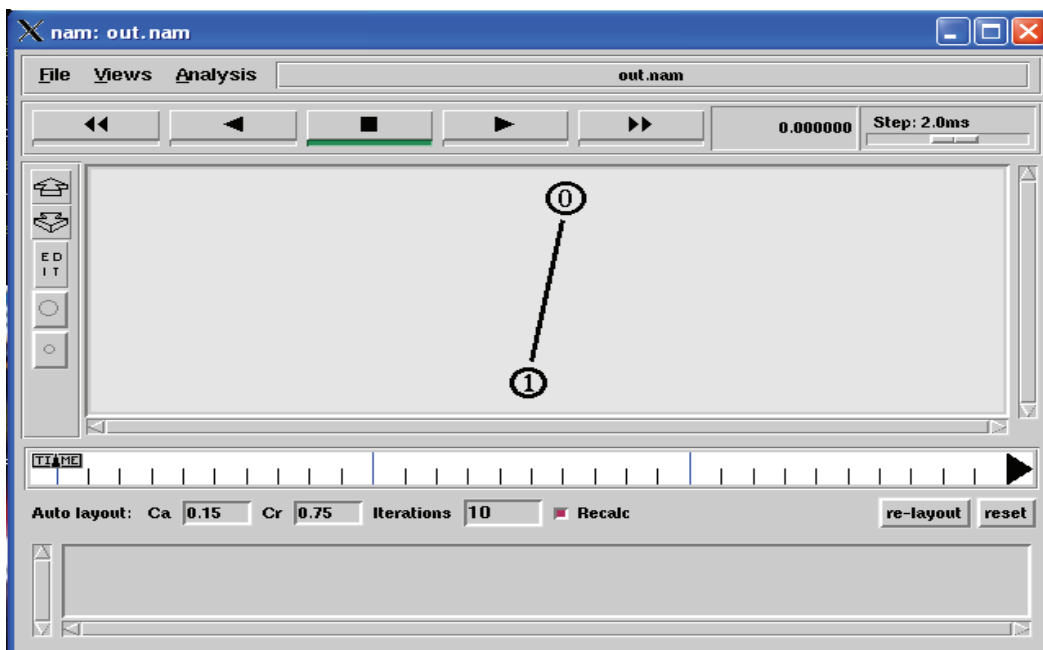


Figure IV.1. Création de topologie sous NAM/NS2

IV.2.3.3. L'interface XGRAPH :

C'est un outil qui fait la visualisation des données contenue dans les fichiers TRACE sous forme de graphes.

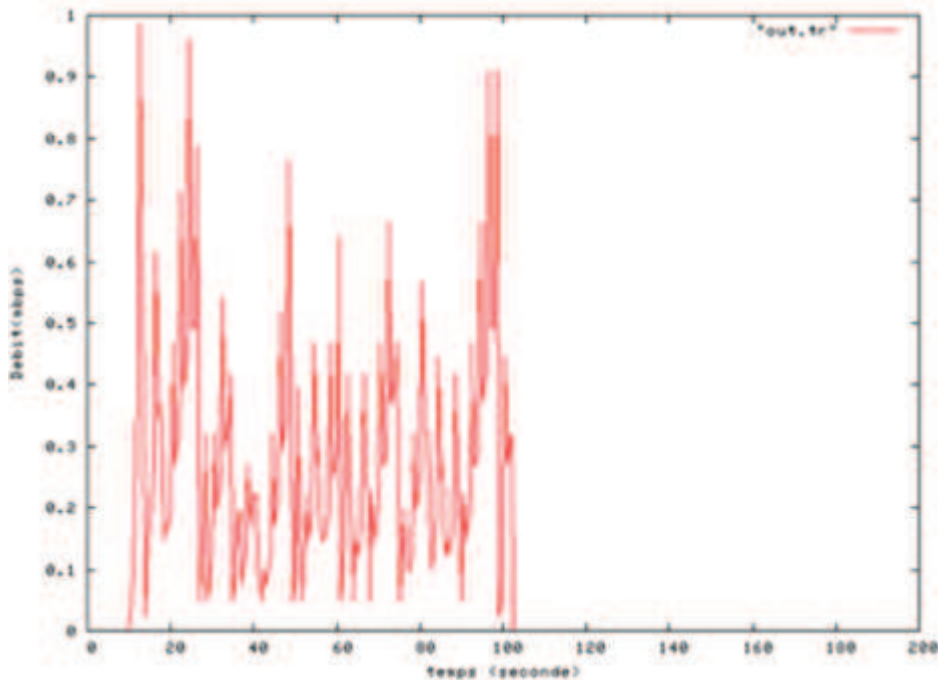


Figure IV.2. Exemple d'un graphe obtenu grâce à l'interface XGRAPH

IV.2.4 Comment crée un scénario de simulation avec NS2.29 ?

Dans la terminologie NS, ce que nous appelons machine s'appelle un nœud. Un nœud peut contenir des agents (tcp, udp...etc.) qui représentent des comportements, par exemple des applications (ftp, cbr...etc.). Une bibliothèque assez complète de composants existe de façon standard. Une propriété intéressante de ce système est son extensibilité. En effet, il est assez facile d'étendre la bibliothèque des composants, des types de liens, ou de tout autre élément du système en programmant ses propres extensions qui deviennent alors intégrées au système. Les commentaires (introduits par le caractère#) expliquent le rôle de chaque instruction ou partie de programme. Mais il nécessaire de commencer chaque simulation avec la commande :

```
Set ns [new Simulator]
```

Déclaration de base :

- Ouvrir un fichier trace :

```
Set tracefile1 [open out]
```

```
Set trace -all $tracefile1
```

- Ouvrir un fichier NAM trace :

```
Set namfile [open out .nam w]
$ nsnamtrace -all $namfile
```

IV.2.5 Composition d'un modèle NS :

Un modèle de réseau en **ns** est constitué de :

- Les Nœuds :

Le nœud est un des premiers éléments de description de la topologie d'un réseau sous NS.

Un nœud est une collection de classifieur et d'agents. Le classifieur a pour objectif de retrouver une référence à un autre objet de la simulation à partir d'une comparaison sur un critère dont la valeur est contenue dans le paquet, Il a un rôle de démultiplexeur en quelque sorte. L'agent est habituellement l'entité d'un protocole.

Création d'un nœud n0

```
Set n0 [$ns node]
```

- Les liens :

Les liens servent à connecter les nœuds entre eux, sans eux il n'y a de réseau .ils sont principalement caractérisés par un délai de propagation et une bande passante.

La déclaration d'un lien duplex entre les nœuds n0 et n1 avec un temps de propagation de 10 ms et un débit 10Mb/s se fait de la manière suivante :

```
$ns duplex -link $n0 $n1 10Mb 10ms DropTail
```

- Les agents:

Les agents font partie de la collection d'un nœud, Ce sont les points terminaux du réseau qui reçoivent ou délivrent les paquets des applications. Il Ya plusieurs types d'agents (TCP, UDP... etc.)

Voyons comment créer un agent et l'attacher à un nœud. Voici la commande qui permet de créer un agent. Ci-dessous nous créons un agent « TCP source » et un agent « TCP récepteur ».

```
Set source [new Agent/TCP]
Set destination [new Agent/TCP Sink]
```

IV.2.6. Principaux composants disponibles dans NS :

La liste des principaux composants actuellement disponible dans NS par catégorie est représentée dans le tableau suivant :

Application	Web, ftp, Telnet, générateur de trafic (CBR,...)
Transport	TCP, UDP, RTP, SRM
Routage	Statique, dynamique (vecteur de distance) et Routage multipoint (DVMRP, PIM)
Gestion de la Fille d'attente	RED, DropTail, Tokenbucket
Discipline de Service	CBQ, SFQ, DRR, Fairqueueing
Système de Transmission	CSMA/CD, CSMA/CA, lien point à point

Tableau IV.1 : principaux composants actuellement disponible dans NS

IV.3.Simulation et interprétation des résultats :

Dans cette section, nous présentons une comparaison entre les deux protocoles de routage AODV et DSR. Les simulations de ces deux protocoles ont été faites sur le même modèle de simulation (les mêmes valeurs des paramètres et les mêmes modèles de trafic).

IV.3.1.Modèle de simulation :

Afin d'étudier et d'analyser le fonctionnement et le comportement des deux protocoles de routage dans un réseau maillé (AODV et DSR). Nous avons choisi le simulateur Network Simulator (NS2) présenté ci-dessus qui est devenu un standard de référence dans le domaine de la recherche, et du développement de nouveaux protocoles pour différents types de réseaux.

Les paramètres standards pour la simulation (medium, la propagation radio ... etc) sont utilisés. Le protocole IEEE 802.11 est utilisé comme protocole d'accès au médium. Le type gestion de la file ou queue en chaque nœud est « PriQueue».

IV.3.2. Modèle de trafic :

Nous avons utilisé des applications qui sont des sources de trafic de type CBR (Constant Bit Rate) et qui émettent des paquets à intervalles réguliers. Ces sources de trafic

modélisent la couche application sur des agents de transport UDP. L'utilisation de ce protocole permet d'éviter d'avoir à gérer le contrôle de flux.

IV.3.3. Métrique :

Trois métriques sont utilisées afin d'évaluer notre approche :

IV.3.3.1 Taux de perte des paquets :

Ce nombre représente l'efficacité d'un protocole dans l'envoi des données aux récepteurs prévus à travers le réseau.

On peut extraire cette métrique en exploitant le fichier trace et en utilisant ces formules :

$$\text{Taux de perte de paquets} = \frac{\text{Nombre des paquets perdus}}{\text{Nombre des paquets envoyé}} \times 100$$

$$\text{Nombre des paquets perdus} = \text{nombre des paquets envoyé} - \text{nombre des paquets reçus}$$

IV.3.3.2 délai moyen de transfert des paquets :

Cette métrique mesure le temps moyen mis pour qu'un paquet arrive à sa destination. Elle montre donc à quel point un protocole est rapide à l'envoi des paquets de données.

IV.3.3.3 Le débit :

C'est une Unité mesurant la vitesse de transmission des données dans une voie de communication. Pour une liaison numérique, il s'agit du nombre de bits transférés en un temps donné. Pour une connexion Internet, le débit s'exprime en kbps (kilobits par seconde).

IV.3.4 Scénarios des simulations :

Pour notre simulation nous avons utilisé le simulateur NS version 2.29. Le réseau considéré est composé de 60 nœuds wifi maillé.

Dans notre modèle, nous avons choisi une topologie qui reflète le réseau wifi maillé. Dans notre topologie nous avons deux types de nœuds, des nœuds fixes qui vont jouer le rôle de routeurs maillé et au même temps d'être élu directement comme passerelles, Et des nœuds mobiles, en utilisant une mobilité aléatoire, qui vont être considérés comme les clients maillés.

Trois métriques sont utilisées afin d'évaluer notre approche, comme il est mentionné en dessus, Le choix de ces métriques est basé sur le fait que ce sont les critères les plus pertinents et les plus utilisés pour évaluer les performances d'un réseau exigeant en QoS.

IV.3.5 Résultats et discussion :

Dans la partie simulation, nous avons étudié l'effet de la vitesse des nœuds sur les trois métriques (délai de transfert des paquets taux de perte et le débit) pour cela nous avons fixé la vitesse des nœuds à 4km/h ensuite à 30 km/h.

A. Le délai de transfert des paquets :

- Pour la vitesse= 4 km/h

	0	30	60	90	120	150	180	210	240	270	300
AODV	0	0,12	0,13	0,15	0,14	0,14	0,11	0,11	0,13	0,09	0,10
DSR	0	0,15	0,18	0,18	0,17	0,19	0,19	0,18	0,13	0,15	0,18

Tableau IV.2. Le délai de transfert pour V=4km/h

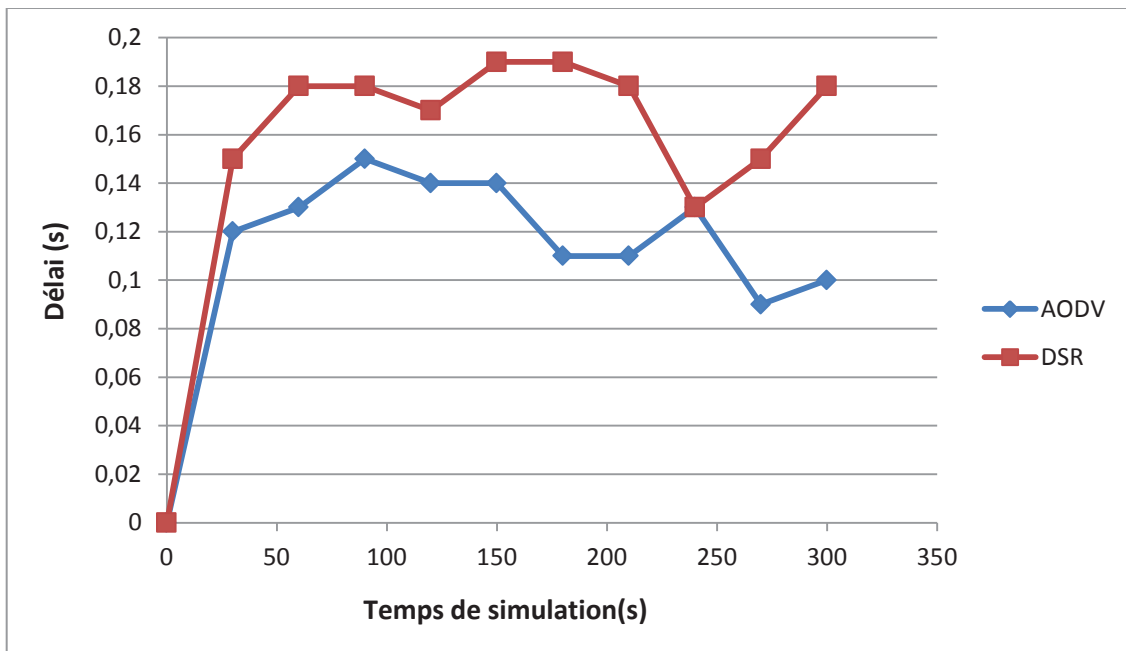


Figure IV.3 : Le délai de transfert pour V=4Km/h

- Pour la vitesse= 30 km/h

	0	30	60	90	120	150	180	210	240	270	300
AODV	0	0,16	0,15	0,20	0,19	0,18	0,22	0,21	0,19	0,18	0,17
DSR	0	0,68	0,69	0,65	0,61	0,72	0,68	0,67	0,73	0,65	0,64

Tableau IV.3 : Le délai de transfert pour V=30km/h

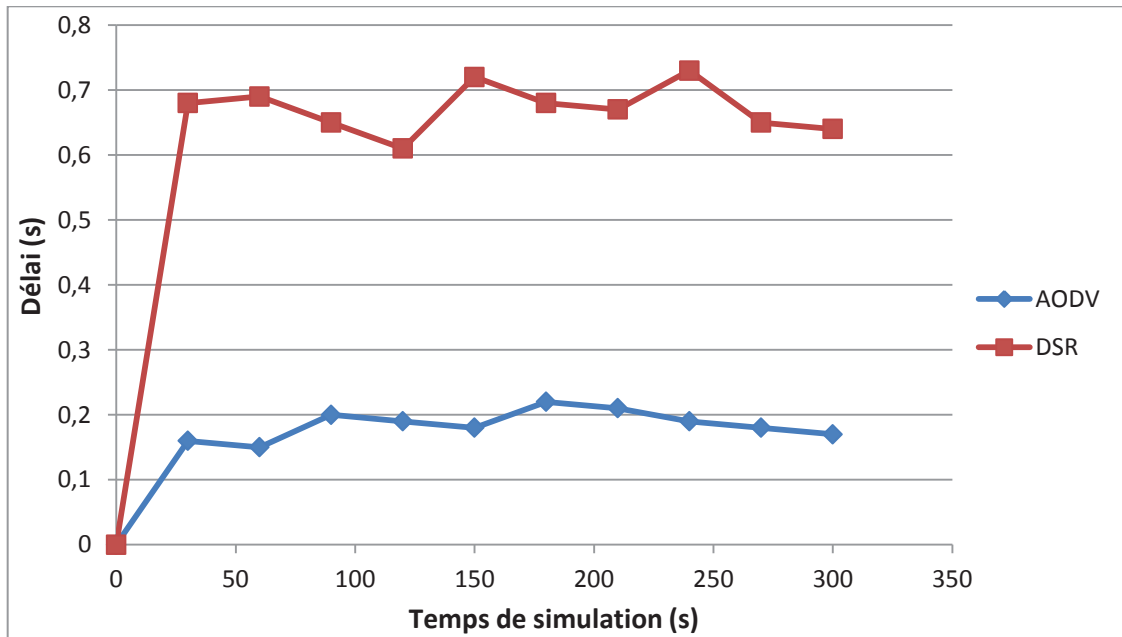


Figure IV.4 : Le délai de transfert pour $V=30\text{km/h}$

Discussion :

D’après les deux figures ci-dessus, nous remarquons qu’en général, le protocole de routage AODV offre un délai moyen de transfert des paquets nettement meilleur que le protocole de routage DSR surtout dans les réseaux à forte mobilité ($V=30\text{km/h}$) et ils se rapprochent dans les réseaux à faible mobilité ($V=4\text{km/h}$).

Nous remarquons que dans les deux protocoles le délai augmente avec la vitesse des nœuds. Par exemple : dans le cas d’une vitesse de 4km/h le protocole AODV offre un délai moyen maximale de 0.15 seconde, celui-ci augmente jusqu’à 0.22 seconde pour le cas d’une vitesse de 30km/h , la même chose pour DSR qui offre un délai moyen maximale de 0.19 seconde dans un réseau à faible mobilité et 0.73 seconde dans un réseau à forte mobilité.

Le protocole de routage AODV possède une table de routage dans chaque nœud du réseau dans laquelle il sauvegarde un ensemble d’information telle que l’adresse IP de la destination, l’adresse IP du prochain nœud en direction de la destination, le nombre de saut et le numéro de séquence de la destination.

Dans le protocole de routage DSR, Avant d’envoyer un paquet de données vers un autre nœud, l’émetteur diffuse un paquet “route request” vers tous ses voisins. Si l’opération de découverte de routes est réussie, l’émetteur reçoit un paquet “route réponse” qui contient une séquence de nœuds à travers laquelle la destination peut être atteinte, il n’utilise pas les

tables de routage contrairement au protocole AODV ce qui explique la rapidité de transfert de paquets du protocole AODV par rapport au DSR.

B. Le taux de perte des paquets :

- Pour la vitesse = 4 km/h :

	0	30	60	90	120	150	180	210	240	270	300
AODV	0	3.2	3.3	3.6	4.3	6.1	6.6	4.21	4.52	4.29	4.94
DSR	0	3,6	3,3	3,39	4,41	7,45	8,1	5,72	5,9	5,2	5,67

Tableau IV.4 : Le taux de perte des paquets pour $V=4Km/h$

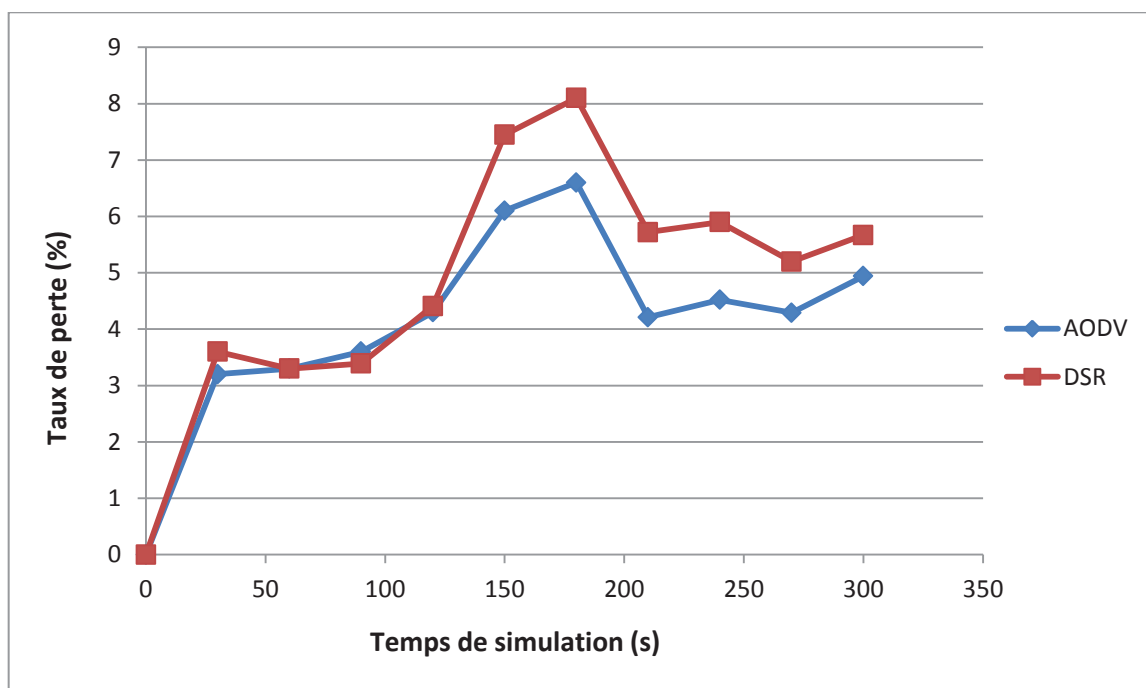


Figure IV.5 : Le taux de perte des paquets pour $V=4Km/h$

- Pour la vitesse = 30 km/h

	0	30	60	90	120	150	180	210	240	270	300
AODV	0	10	12,2	12,6	12,8	16,5	17,2	14,9	12,2	12	13.5
DSR	0	35	38	36,2	35	48,1	52,3	36	35	34,3	37

Tableau IV.5 : Le taux de perte des paquets pour $V=30Km/h$

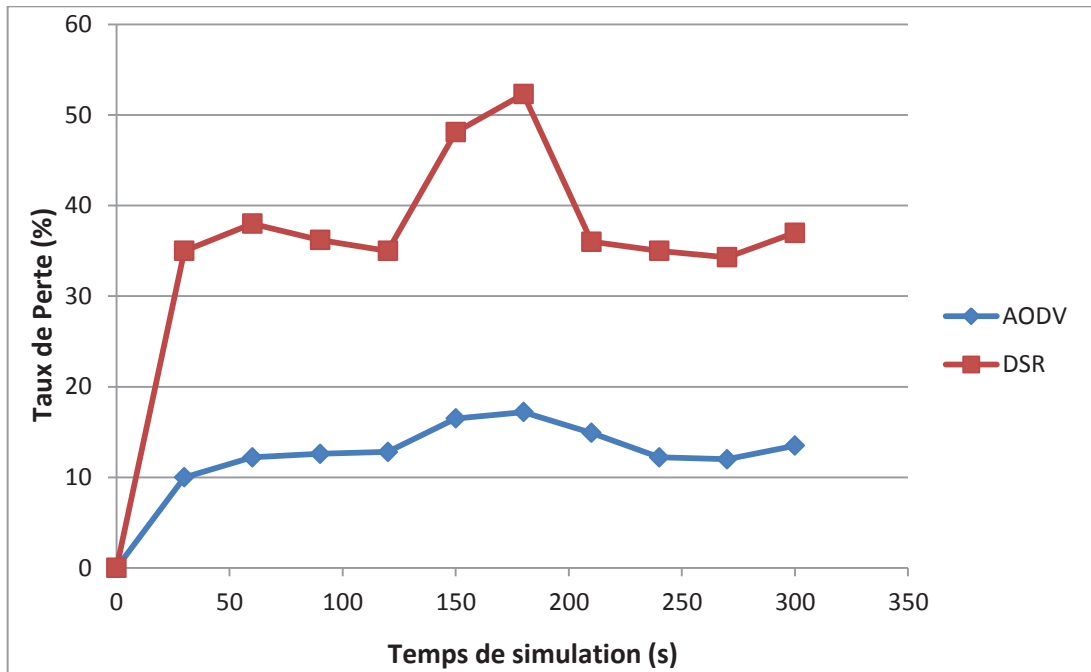


Figure IV.6 : Le taux de perte des paquets pour $V=30\text{Km/h}$

Discussion :

Nous remarquons dans les figures ci-dessus que les pertes de paquets de données avec le protocole DSR sont plus élevées que celles du protocole AODV. Ces pertes augmentent avec l'augmentation de la vitesse de la mobilité, Par exemple : dans le cas d'une vitesse de 4km/h le protocole AODV à un taux de perte maximale de 6,6%, celui-ci augmente jusqu'à 17.2% pour le cas d'une vitesse de 30km/h, la même chose pour DSR qui a un taux de perte maximale de 8.1% dans un réseau à faible mobilité et 52.3% dans un réseau à forte mobilité.

Nous remarquons aussi que pour une vitesse de 4km/h les taux de pertes de paquet des deux protocoles se rapprochent alors que pour une vitesse de 30km/h, le protocole DSR à un taux de perte nettement supérieure à celui du protocole AODV.

Le taux de perte de paquets augmente subitement puis diminue entre 100s et 200s, surtout pour le protocole DSR, cela est dû à un trafic plus important.

Dans une topologie mobile la manière de trouver une route pour atteindre une destination est très importante, la majorité du temps lorsqu'un nœud veut émettre il cherche sa destination puisque la topologie est mobile il ne va pas la trouver facilement donc nous aurons des paquets qui tournent dans le réseau dans le vide.

Dans les deux protocoles utilisés la découverte de route se fait par inondation. Cette dernière provoque une congestion ce qui entraîne des pertes de paquets.

Le protocole AODV est plus souple que le protocole DSR, son fonctionnement est plus réduit vu qu'il fait sa maintenance en utilisant les messages hello qui ont une taille plus réduite par rapport aux paquets RREQ qui sont utilisés en abondance dans le protocole DSR (Découverte et maintenance).

Donc les échanges sont plus importants dans le protocole DSR que dans le protocole AODV.

C. Le Débit

- Pour la vitesse = 4 km/h

	0	30	60	90	120	150	180	210	240	270	300
AODV	0	9,5	9,3	9,4	9,4	7,35	5,1	8,4	9,8	9,5	9.6
DSR	0	6,8	6,7	6,78	6,9	4,3	4,0	5,9	6,2	6,5	6,8

Tableau IV.6 : Le débit pour $V= 4\text{Km/h}$

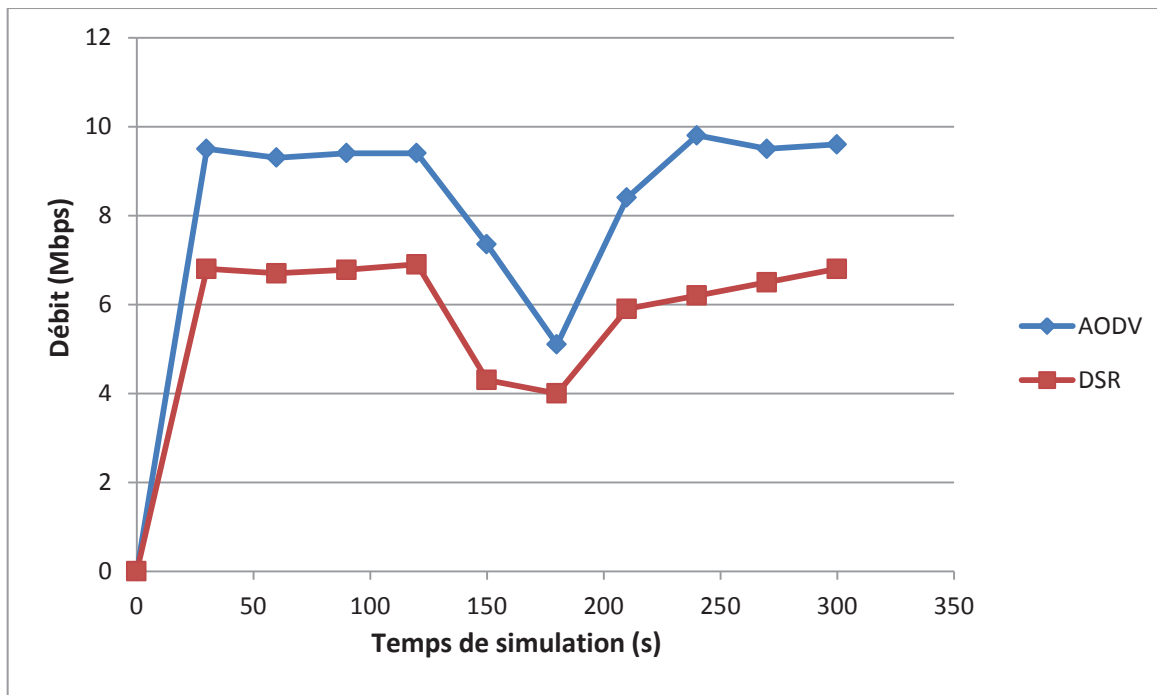


Figure IV.7 : Le débit pour $V= 4 \text{ km/h}$

- Pour la vitesse =30km/h

	0	30	60	90	120	150	180	210	240	270	300
AODV	0	7,2	7,3	7,8	7,5	6,2	4,9	6,9	7,02	7,1	7,4
DSR	0	3,21	3,28	3,33	3,0	2,8	2,5	3,6	4,2	4,1	3,9

Tableau IV.7 : Le débit pour V=30Km/h

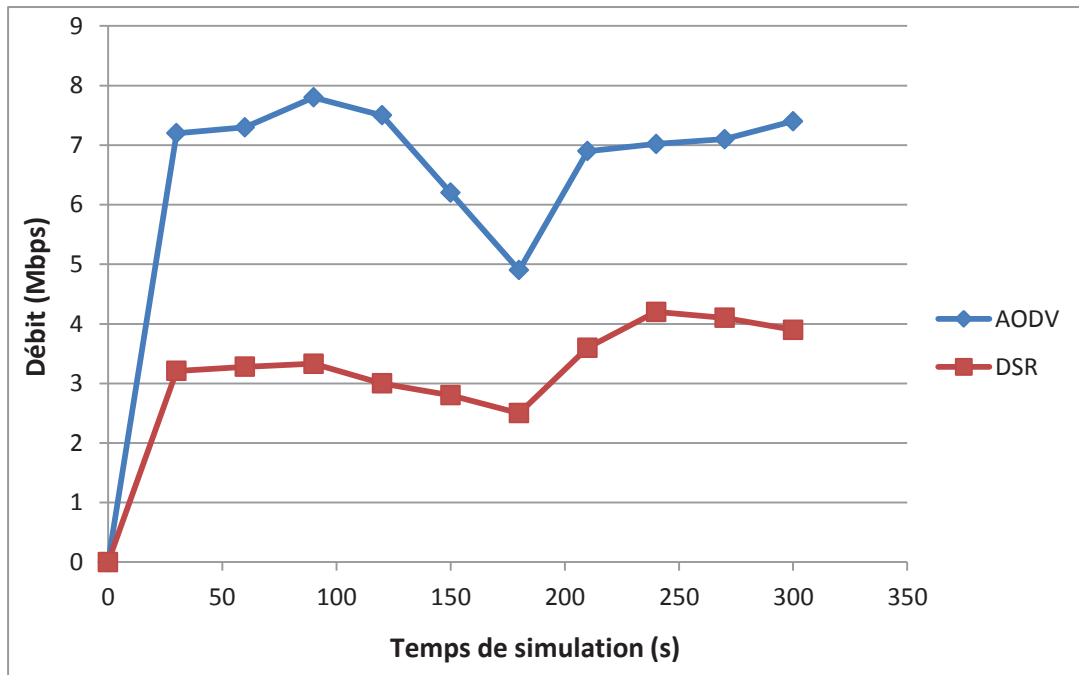


Figure IV.8 : Le débit pour V=30Km/h

Discussion :

D’après les deux figures ci-dessus, nous remarquons que le protocole de routage AODV offre un Débit meilleur que le protocole de routage DSR surtout dans les réseaux à faible mobilité par exemple : pour une vitesse de 4km/h le protocole AODV offre un débit maximal de 9.8 Mbps qui diminue jusqu’à 7.8 Mbps pour une vitesse de 30km/h, la même chose pour DSR.

Le débit diminue subitement puis augmente entre 100s et 200s, surtout pour le protocole AODV, cela est dû à un trafic plus important.

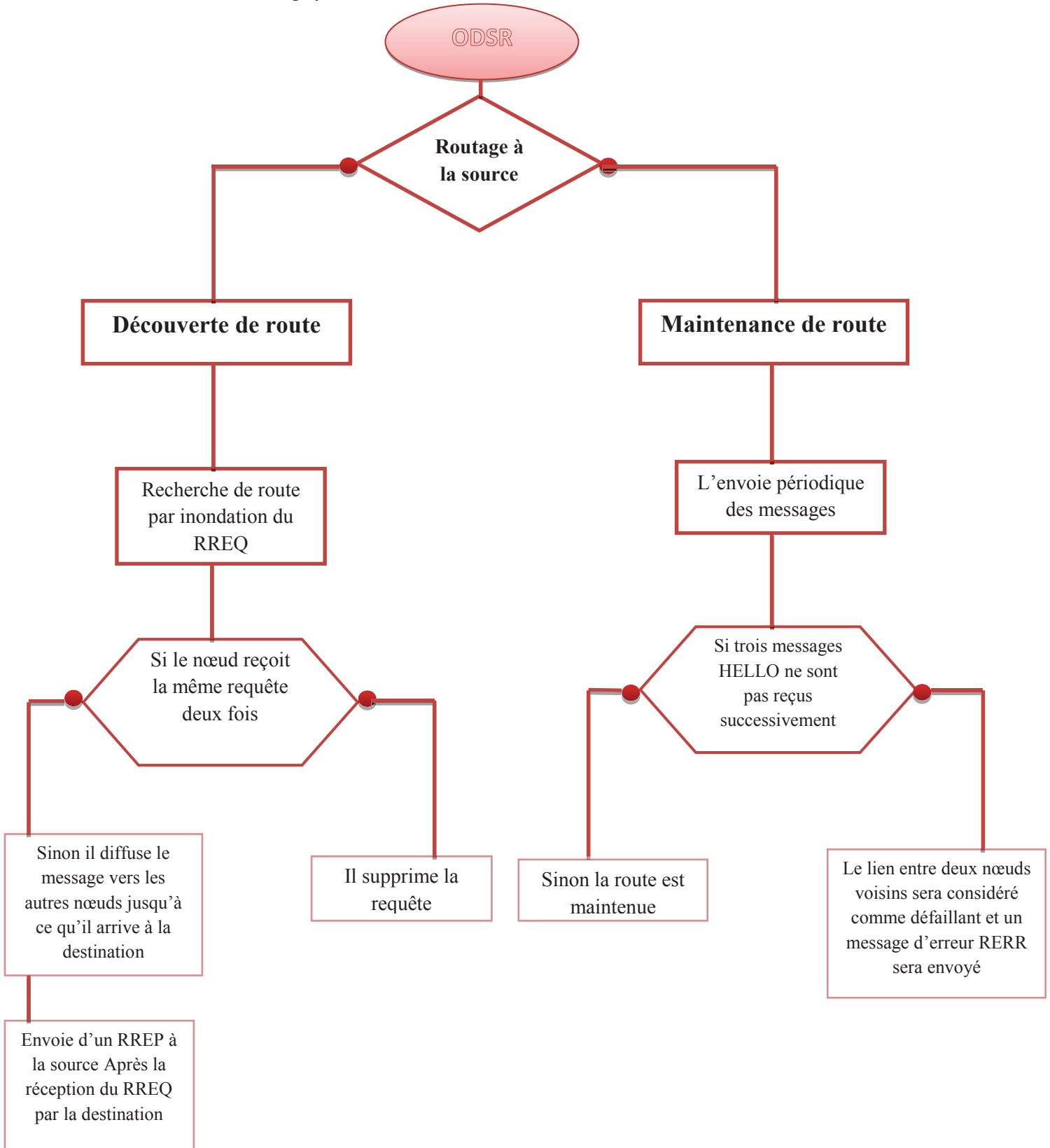
Le protocole AODV utilise des messages de contrôle qui ont une petite taille cela permet au nœud de les lire très rapidement sans avoir de congestion.

De plus, les résultats de notre simulation, nous ont montré que le protocole AODV offre un meilleur délai que le protocole DSR, Et un protocole qui offre un meilleur délai offre un

meilleur débit c'est pour cela que le protocole AODV a un débit plus élevé que le protocole DSR.

IV.4 proposition d'un protocole hybride entre AODV et DSR (ODSR) :

- schéma descriptif :



L'AODV est un protocole de routage réactif tout comme DSR sauf que l'AODV utilise le routage à vecteur de distance alors que le DSR utilise le routage à la source.

D'après les résultats de notre simulation nous avons déduit que le protocole AODV est plus performant que le protocole DSR c'est la raison pour laquelle nous avons choisis d'améliorer le protocole DSR en utilisant un des avantages du protocole AODV.

Nous avons vu lors du chapitre III que le protocole AODV a un Overhead minime par rapport au protocole DSR et c'est le point que nous avons traité en proposant un algorithme qui minimise l'Overhead dans le protocole DSR.

Comme cité dans [19] DSR est un protocole standardisé et il possède un mécanisme d'options qui facilite l'ajout de nouveaux paquets au protocole.

Nous savons aussi que l'overhead est nul quand aucun nœud n'effectue de requêtes de route.

En se basant sur ces deux points nous avons pensé à ajouter au protocole DSR des paquets de contrôles qui sont des messages HELLO existant dans le protocole AODV afin de minimiser l'Overhead car Dans le DSR lors de la maintenance de route un paquet est retransmis jusqu'à la réception d'une confirmation ou jusqu'à ce que le nombre maximal de retransmission soit atteint ce qui cause une surcharge du réseau.

En faisant une combinaison entre les protocoles AODV et DSR, nous avons défini un protocole que nous appelons ODSR (On Demand Source Routing) qui a les mêmes fonctionnalités que le protocole DSR sauf que la maintenance se fait avec l'envoi périodique des messages HELLO comme dans le protocole AODV.

Donc la découverte de route s'effectue comme suit :

Lorsqu'une source veut atteindre une destination et qu'elle ne possède aucune route vers celle-ci dans son cache elle envoie une Route Request « RREQ » à tous les prochains nœuds, le message se propage de nœud en nœud jusque la destination.

Si un nœud recevant un message *RREQ* a récemment vu un autre message *RREQ* contenant le même identifiant et la même adresse de destination, ou si la propre adresse du nœud est déjà listée dans la *Route Request*, alors le nœud supprime la requête, sinon le message RREQ sera diffusé jusqu'à atteindre la destination.

Quand La destination reçoit le paquet RREQ elle envoie alors un signal Route Reply « RREP » vers la source en suivant le même chemin, mais dans le sens inverse.

En ce qui concerne la maintenance de route :

Elle se fait par l'émission périodique d'un message *HELLO* (qui est un RREP avec un TTL (*Time To Live*) de 1), Le lien entre deux nœuds voisins sera considéré comme défaillant dans le cas où trois messages "*HELLO*" ne sont pas reçus respectivement.

Si un lien entre deux nœuds est invalide les nœuds utilisant ce lien sont prévenus par un message d'erreur (RERR), ils vont Alors diffusés une autre requête.

Donc le protocole ODSR garde tous les avantages du protocole DSR en éliminant l'inconvénient d'Overhead vu que le nombre de requête lors de la maintenance a diminué.

IV.5 Problèmes rencontrés et perspectives :

- *Problèmes :*

Durant la réalisation de notre travail nous avons rencontré beaucoup de problèmes, parmi eux nous citons :

- L'installation complexe du NS2 sous Windows.
- Les résultats de simulation ne sont pas bien précisés.

- *Perspectives :*

Nous proposons comme perspectives :

- valider le protocole proposé qui est ODSR en l'intégrant dans NS2 et en effectuant des simulations, ensuite le comparer avec les autres protocoles existants.
- Intégrer d'autre protocoles dans NS2 et les comparés ensemble.

IV.6. Conclusion :

Dans ce chapitre nous avons comparé les deux protocoles de routage AODV et DSR en utilisant le simulateur NS2 ou le but a été d'étudier les performances avec différentes vitesses. Nous avons utilisé trois métriques qui sont le taux de perte de paquets, le délai moyen, et le débit.

Les résultats de simulation ont été récupérés, traités puis représentés sur des graphes et interprétés pour distinguer la différence et comprendre le comportement de chaque protocole.

Nous avons proposé aussi d'améliorer le protocole DSR en lui intégrant un des avantages du protocole AODV.

Ce chapitre contient aussi une représentation du Network Simulator (NS2).

Conclusion générale :

Les réseaux maillés sans fil apparaissent comme une nouvelle technologie évolutive et prometteuse. En effet, ils bénéficient de caractéristiques avantageuses comme La facilité de déploiement et l'absence de gestion centralisée des communications. Les réseaux maillés sans fil essaient de répondre à l'augmentation croissante du nombre d'utilisateurs et de leurs applications qui demandent de plus en plus de ressources.

L'objectif de ce mémoire est d'évaluer les performances du réseau wifi mesh, pour cela nous avons procédé en premier temps à détaillé les réseaux maillés sans fil en mettant l'accent sur leurs caractéristiques leurs architecture ainsi que leur mode de fonctionnement et leurs applications.

Après cela nous nous sommes intéressés aux protocoles de routages utilisés dans cette catégorie du réseau.

Par la suite nous nous sommes focalisés sur les deux protocoles réactifs AODV et DSR en faisant une analyse et une comparaison théorique.

Cette étude a été conclue par des simulations où nous avons simulé les deux protocoles étudiés précédemment sous NS2, ce qui nous permis de soulevé des résultats et des analyses comparatives qui nous ont montré que le protocole AODV est plus performant que le protocole DSR en termes de délai , de taux de perte de paquets et de débit .

Ces résultats nous ont poussé à proposer une combinaison entre les deux protocoles AODV et DSR afin d'amélioré ce dernier.

Notons que les portes restent ouvertes pour les autres pour valider cette combinaison en tenant compte d'autres critères et contraintes.

Références bibliographique :

- [1] : Omar chikhrouhou. « Sécurité des réseaux mesh sans fils » ,Ecole national d'ingénieur de Sfax, mai 2006 .
- [2] : Stephane davy . « performances des réseaux maillés multiradio sur banc de test », Ecole de technologie supérieure université du Québec, aout 2010 .
- [3] : Jihene Rezgui. « Gestion adaptative des ressources dans les réseaux maillés sans fil à multiples-radios multiples-canaux », Université de Montréal, Août 2010.
- [4] : « routage dans les réseaux locaux maillés sans fils », cours.
- [5] : Mohammed mehseur.« Routage dans les réseaux maillés sans fils », Université m'hamed Bouguara Boumerdés, 2011.
- [6] : Chemsddine benmoussat. « Contribution à l'étude du trafic multimédia sur wifi mesh (IEEE 802.11s) », université abou bakr belkaid-tlemcen, 2013.
- [7] : http://www.senouci.net/download/Publications/Book- Chapters/Senouci_IC2-2008_3.pdf.
- [8]: Mohamed reda ouled el bali et asmaa boumeddine. «Routage collaboratif dans un réseau Mesh », ingénierie du logiciel, des systèmes d'informations et du multimédia Université d'avignon.
- [9] : Yaye Sarr, « Métriques de routage dans les réseaux maillés sans fil », Université de Montréal, Avril 2011.
- [10] : Tayeb lemlouma, « Le Routage dans les Réseaux Mobiles Ad Hoc », Université des sciences et des technologies, houari boumediene, alger, algérie, 2000.
- [11] : Hagggar bachar Salim, « Les protocoles de routage dans les réseaux ad hoc », Université de Reims - UFR Sciences, juin 2007.
- [12]: David elorrieta, « Protocoles de routage pour l'interconnexion des réseaux Ad-Hoc et UMTS », l'académie universitaire wallonie- bruxelles,2007.
- [13] : S.Maag, C.Grepet, A.Cavalli, « Un Modèle de validation pour le protocole de routage DSR », Institut National des Télécommunications CNRS UMR 5157, janvier 2005.
- [14] : Rabah meraihi, « Gestion de la qualité de service et contrôle de topologie dans les réseaux ad hoc », Ecole nationale supérieure des télécommunications.
- [15] :http://www.memoireonline.com/05/12/5873/m_Etude-sur-les-protocoles-de-routage-dun-reseau-sans-fil-en-mode-Ad-Hoc-et-leurs-impacts-cas-de28.html
- [16] :<http://wapiti.telecomlille1.eu/commun/ens/peda/options/ST/RIO/pub/exposes/exposesrio2007/bousmina-beaurin/>

[17] : Kamal beydoun, « conception d'un protocole de routage hiérarchique pour les réseaux de capteurs », l'U.F.R des sciences et techniques de l'université de franche -comte, décembre 2009.

[18] : Seloua chettibi, « Protocole de routage avec prise en compte de la consommation d'énergie pour les réseaux mobiles ad-hoc », Université Mentouri Constantine, Décembre 2008

[19] : Farid JADDI, « CSR : une extension hiérarchique adaptative du protocole de routage ad hoc DSR », institut national polytechnique de toulouse, octobre 2006.

Résumé :

Ces dernières années, les technologies sans fil ont connu un essor fulgurant. Elles ont permis la mise en place de réseaux sans fil à hautes performances. Les réseaux maillés sans fil (en anglais "Wireless Mesh Network (WMN)") sont une nouvelle génération de réseaux sans fil qui offrent des débits élevés par rapport aux réseaux Wi-Fi classiques et aux réseaux ad-hoc.

La recherche dans le domaine des réseaux maillés sans fil suscite un grand intérêt auprès de la communauté des chercheurs en télécommunications. Ceci est dû aux nombreux avantages que la technologie WMN offre, telles que l'installation facile et peu coûteuse, la forte tolérance aux pannes, la connectivité fiable et l'interopérabilité flexible avec d'autres réseaux existants. Cependant plusieurs problèmes subsistent et doivent être résolus notamment celui du routage qui demeure un défi majeur dans les WMN.

Le but des protocoles de routage est de trouver les meilleures routes c.-à-d. des routes qui maximisent les débits et minimisent les délais, lors de l'acheminement du trafic.

Dans notre étude, après avoir présenté les WMN, nous avons donné une description détaillée de plusieurs protocoles de routage suivi d'une étude comparative entre les protocoles AODV et DSR. Pour terminer nous avons exploité notre étude théorique avec des simulations sous NS-2, afin d'avoir le meilleur protocole en termes de QoS et proposé un modèle hybride entre les deux protocoles étudiés.

Mot-clé : Réseau maillé sans fil, routage, AODV, DSR, NS2.

ABSTRACT:

These last years, wireless technologies made fulgurating great strides. They allowed the installation of wireless networkings high efficiencies. The ring main systems without wire ("Wireless Mesh Network (WMN)" in English) are a new generation of wireless networkings which offer flows raised compared to the traditional Wi-Fi networks and with the ad hoc networks.

Research in the field of the mesh networks without wire arouses a great interest near the community of the researchers in telecommunications. This is due to the many advantages which technology WMN offers, such as the easy and inexpensive installation, the strong fault-tolerance, reliable connectivity and flexible interworking with other existing networks. However several problems remain and must be solved in particular that of the routing which remains a major challenge in the WMN. The goal of the protocols of routing is to find the best roads i.e roads which maximize the flows and minimize the deadlines, at the time of the routing of the traffic.

In our study, after having presented the WMN, we gave a description detailed of several protocols of routing followed by studies comparative between protocols AODV and DSR, to finish we exploited our studies theoretical with simulations under NS-2, in order to have the best protocol in term of QoS and proposed a hybrid model between the two studied protocols.

Key word: Mesh network without wire, routing, AODV, DSR, NS2.