الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

UNIVERSITÉ BADJI MOKHTAR - ANNABA
BADJI MOKHTAR – ANNABA UNIVERSITY

جامعة باجي مختار – عنابـــة

Faculté : Science de l'ingéniorat

Département : Electronique

Domaine : Sciences et Technologie

Filière : Télécommunication

Spécialité : *Réseaux de télécommunication*

Mémoire

Présenté en vue de l'obtention du Diplôme de Master

Thème:

Simulation des protocoles des routages AODV et OLSR dans les réseaux ad-hoc via Opnet

Présenté par :

M^lle ZERDI Fatma Zohra

M^r KHOUALDIA Billel

Encadrant : *TAIBI Mahmoud* *Professeur* *Univ-Annaba*

Jury de Soutenance :

FEZARI Mourad	Professeur	Univ-Annaba	Président
TAIBI Mahmoud	Professeur	Univ-Annaba	Encadrant
BOUKARI Karima	MCA	Univ-Annaba	Examinateur

Année Universitaire : 2019/2020

Dédicace

A MA TRES CHERE MERE

« BOUROUHOU DALILA »

Source inépuisable de tendresse, de patience et de sacrifice. Ta prière et ta Bénédiction m'ont été d'un grand secours tout au long de ma vie.

Quoique je puisse dire et écrire, je ne pourrais exprimer ma grande affection et ma profonde reconnaissance. J'espère ne jamais te décevoir, ni trahir ta confiance et tes sacrifices.

Puisse Dieu tout puissant, te préserver et t'accorder Santé, longue vie et bonheur.

A LA MEMOIRE DE MON TRES CHER PERE
« MOHAMED 'HAMDI' »
De tous les pères, tu es le meilleur qui a été toujours avec moi
Que tu reposais dans le paradis du seigneur

ET EN DERNIER A MON FRERE

« ABD EL REZZEK »

Un Frère comme on ne peut trouver nulle part ailleurs,
Je ne saurai traduire sur du papier l'affection que j'ai pour Toi,
Tu as été à mes côtés pendant toutes les étapes de ma vie et tu resteras toujours.
Je n'oublierai jamais ces merveilleux moments passés ensemble
Je te souhaite tout le bonheur du monde
J'implore Allah de te réserver un avenir meilleur

RAOUIA

Dédicace

Je dédie ce modeste travail et ma profonde gratitude :

*A **MES TRES CHERS PARENTS***

« BENNACER ZOUBEIDA »** et **« KHOUALDIA SALIM »

Avec tous mes sentiments De respect, d'amour, de gratitude et de reconnaissance, pour tous leurs sacrifices, leur amour, leur tendresse, leur appui, leurs encouragements et leurs prières tout au long de mes études.

*A **MES TRES CHERES SŒURS***
***« CHAIMA » « NADIA » « CHAHRAZED »,** pour leurs encouragements permanents et leur appui moral.*

*A toute ma famille « **KHOUALDIA** » et « **BENNACER** ».*

À tous ceux qui me sont très chers.

A mes amis.

A tous mes professeurs qui m'ont enseigné.

BILLEL

REMERCIEMENT

Tout d'abord, nous remercions Dieu le tout Puissant qui nous a donné la force et la volonté pour réaliser ce modeste travail.

Nous tenons à exprimer nos remerciements à notre encadreur ***Mr TAIBI MAHMOUD****, pour avoir accepté de nous encadrer tout au long de ce travail, pour sa disponibilité, son amabilité, ses conseils et suggestions.*

Nous tenons à remercier les membres de jury d'avoir répondu présent à l'évaluation de notre travail de fin d'étude.

Nous exprimons également notre gratitude à tous les professeurs et enseignants qui ont collaboré à notre formation depuis notre premier cycle d'étude jusqu'à la fin de notre cycle universitaire « ***BOULMAIZ AMIRA, AMARA FETHI, K.BEDOUD, BOUCHAALA ALI, AFIFI SADEK, Mr FEZARI, Mme BOUKARI, Mme ZERMI*** *» et Notre chef de département «* ***GHEDJATI ABD EL GHANI*** *»*

Enfin, nous remercions Nos amis aussi.

Résumé :

Les réseaux mobiles Ad Hoc appelés généralement MANET (Mobile Ad Hoc Network) sont devenus de plus en plus populaires ces dernières années, en raison de l'importance des domaines d'application des réseaux Ad Hoc. Ils sont un nouveau type de réseaux basés sur la technologie sans fil. Les réseaux Ad Hoc sont des systèmes autonome communique avec des ondes radio sans infrastructure. La communication entre les nœuds de réseaux MANET nécessite des protocoles de routage à cause de topologie dynamique et l'absence d'administration centrale.

Parmi les protocoles de routage existants, le protocole AODV (Ad hoc On Demand Distance Vector Routing), et le protocole OLSR (Optimized Link State Routing) sont abordés dans ce travail.

Dans ce mémoire, nous avons analysé la performance de ces deux protocoles de routage basés sur les résultats obtenus après simulation à l'aide de simulateur OPNET pour trouver le meilleur Protocol parmi les deux proposés.

Mots clés : *Protocole de routage, MANET, AODV, OLSR, simulation, OPNET.*

Abstract:

Mobile Ad Hoc networks commonly referred to as MANET (Mobile Ad Hoc Network) have become increasingly popular in recent years, due to the importance of the application areas of Ad Hoc networks. They are a new type of networks based on wireless technology. Ad Hoc networks are autonomous systems communicating with radio waves without infrastructure. Communication between MANET network nodes requires routing protocols due to dynamic topology and lack of central administration.

Among the existing routing protocols, the AODV (Ad hoc On Demand Distance Vector Routing) and OLSR (Optimized Link State Routing) protocols are discussed in this work.

In this thesis, we analyzed the performance of these two routing protocols based on the results obtained after simulation using an OPNET simulator to find the best protocol among the two proposed.

Keywords: *routing protocol, MANET, AODV, OLSR, simulation, OPNET.*

ملخص:

Mobile Ad Hoc Network , يشار إليها عادة باسم MANET ,أصبحت شائعة بشكل متزايد في السنوات الأخيرة، نظرا لأهمية مجالات التطبيق لشبكات Ad Hoc، إنها نوع جديد من الشبكات التي تعتمد على التكنولوجيا اللاسلكية.

الشبكات المخصصة هي أنظمة مستقلة تتواصل مع موجات الراديو بدون بنية تحتية. يتطلب الاتصال بين عقد شبكة MANETبروتوكولات توجيه بسبب الهيكل الديناميكي ونقص الإدارة المركزية.

من بين بروتوكولات التوجيه الحالية، تمت مناقشة بروتوكولات AODV و OLSR في هذا العمل.

في هذه المذكرة، قمنا بتحليل أداء بروتوكولي التوجيه بناء على النتائج التي تم الحصول عليها بعد المحاكاة باستخدام المحاكي OPNETللعثور على أفضل بروتوكول بين البروتوكولين المقترحين.

الكلمات المفتاحية : *بروتوكول التوجيه، MANET, AODV, OLSR, المحاكاة, OPNET.*

Liste des acronymes:

AODV	*Ad hoc on Demand Distance Vector Routing*
MANET	*Mobile Ad hoc Network*
OLSR	*Optimized Link State Routing*
MPR	*Multipoint Relays*
TC	*Topology Control*
WLAN	*Wireless Local Area Networks*
FTP	*File Transfer Protocol*
OPNET	*Optimized Network Engineering Tool*
RREQ	*Route Request*
RREP	*Route Reply*
RERR	*Route Error*

Liste des figures:

Liste des tableaux

SOMMAIRE

INTRODUCTION GENERALE

Depuis l'apparition des réseaux informatiques, ce domaine a connu une évolution sans cesse notamment sur le plan physique et artistique. Avec le développement constant des technologies, l'utilisation des systèmes d'information s'est transformée. Elle s'exprime notamment par un besoin de mobilité des utilisateurs. Les réseaux sans fil sont en plein développement du fait de la flexibilité de leur interface, qui permet à un utilisateur de changer facilement de place.

Différentes catégories des réseaux sans fil existent suivant leur étendue (WPAN, WLAN, WMAN, WWAN). Ces dernières années, le développement de la technologie sans fil a ouvert de nouvelles perspectives dans le domaine des télécommunications. L'utilisation des terminaux mobiles impose l'emploi d'une infrastructure (points d'accès) parfois coûteuse ou difficile à implanter.

De fait, cette solution n'est pas toujours envisageable. Il existe deux types de réseaux mobiles, les réseaux mobiles avec infrastructure et les réseaux mobiles Ad Hoc. Les réseaux mobiles avec infrastructure sont basés sur un ensemble de sites fixes appelés stations de base, ces sites vont relier les différents nœuds mobiles pour former un réseau interconnecté. Par conséquent, des réseaux mobiles dépourvus d'infrastructure ont été déployés. Ces réseaux sont plus connus sous le nom de réseaux Ad Hoc mobiles ou MANETS (Mobile Area NETWORKS).

Un réseau Ad hoc mobile (MANET) est un système autonome constitué de nœuds mobiles reliés par des liens sans fils. Les nœuds du MANET jouent le rôle de routeurs, se déplaçant d'une façon aléatoire, et s'organisant arbitrairement. En conséquence, la topologie du réseau MANET peut changer rapidement et de manière imprévisible. Ce type de réseau est sans infrastructure et représente une option attractive pour connecter spontanément des terminaux mobiles. MANET est appliqué dans le domaine militaire ou dans des situations de secours parce qu'il permet l'établissement d'un réseau de transmission à très court terme et à un coût très bas. Cependant, le réseau MANET est limité par différentes contraintes telles que la largeur de bande, le délai, la mobilité, etc...

L'étude et la mise en œuvre de protocoles de routage pour assurer la connexion des réseaux ad hoc au sens classique du terme (tout sommet peut atteindre tout autre), est un problème très compliqué. Cela est dû essentiellement à la propriété qui caractérise les réseaux ad hoc et qui est l'absence d'infrastructure fixe et de toute administration centralisée.

Vu les limitations des réseaux ad hoc, la construction des routes doit être faite avec un minimum de contrôle et de consommation de la bande passante.

Suivant la manière de création et de maintenance de routes lors de l'acheminement des données, les protocoles de routage peuvent être séparés en deux catégories, les protocoles proactifs et les protocoles réactifs.

Les protocoles proactifs établissent les routes à l'avance en se basant sur l'échange périodique des tables de routage, alors que les protocoles réactifs cherchent les routes à la demande.

Un protocole de routage sert à déterminer la route optimale pour le transfert de données entre deux nœuds. Pour bien comprendre son comportement lors de routage, on propose une étude sur les protocoles de routage en se focalisant sur les deux protocoles OLSR et AODV suivie par des simulations afin de soulever des résultats et des analyses comparatives.

Notre mémoire qui est subdivisé en trois principaux chapitres :

- *Le premier chapitre introduit un état de l'art sur les réseaux ad hoc, les différents types et caractéristiques des réseaux ad hoc.*
- *Dans le second chapitre, nous avons présenté le simulateur OPNET*
- *Le troisième chapitre est consacré à la description des protocoles OLSR et AODV.*

CHAPITRE 1

I.1 LES RESEAUX AD HOC

I.1.1 Définition :

Les réseaux mobiles Ad Hoc appelés généralement MANET (Mobile Ad Hoc Network) sont devenus de plus en plus populaires ces dernières années, en raison de l'importance des domaines d'application des réseaux Ad Hoc. Ils sont un nouveau type de réseaux basés sur la technologie sans fil. Les réseaux Ad Hoc sont des systèmes autonomes qui communiquent avec des ondes radios qui se propagent entre les différents nœuds mobiles sans infrastructure. Il n'y a aucune limitation de taille dans un réseau Ad Hoc, il peut contenir des dizaines ou des milliers de nœuds. La communication entre les nœuds de réseaux MANET nécessite des protocoles de routage à cause de topologie dynamique et l'absence d'administration centrale [1].

Figure 1.1: Réseau sans fil sans infrastructure (Ad Hoc).

I.1.2 Caractéristique des réseaux Ad Hoc :

Les réseaux mobiles Ad Hoc sont caractérisés par ce qui suit:

- ***Sans infrastructure:***

Les réseaux ad hoc se distinguent des autres réseaux mobiles par la propriété d'absence d'infrastructures préexistantes et de tout genre d'administration centralisée.

Les hôtes mobiles sont responsables d'établir et de maintenir la connectivité du réseau d'une manière continue [2].

- ***Mobilité et topologie dynamique:***

Les unités mobiles du réseau se déplacent d'une façon libre et arbitraire, par conséquent la topologie du réseau peut changer à des instants imprévisibles, d'une manière rapide et aléatoire. Les liens de la topologie peuvent être mono ou bidirectionnels [3].

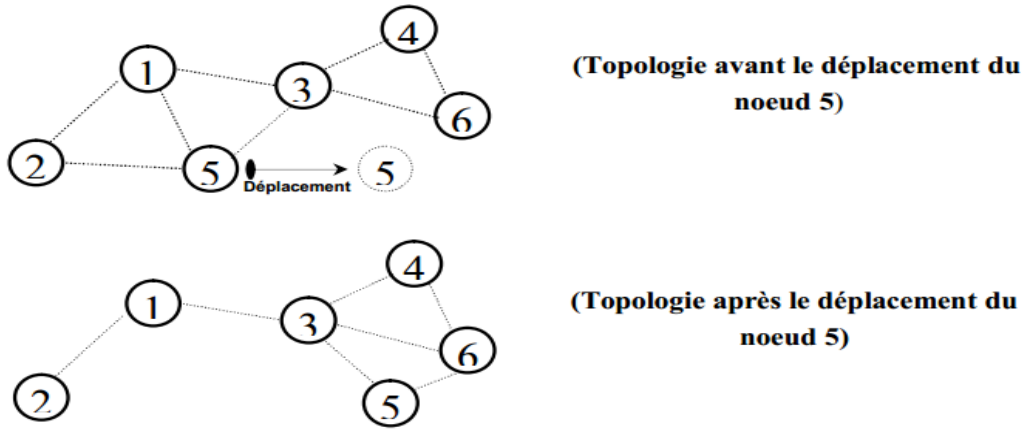


Figure 1.2: Changement de la topologie d'un réseau Ad Hoc.

- ***Contraintes de ressources:***

  Les nœuds disposent de ressources d'alimentation et de capacités de calcul et de stockage limités, d'où une gestion efficace est nécessaire pour avoir une longue durée de vie, le trafic de routage devrait être maintenu à un minimum [3].

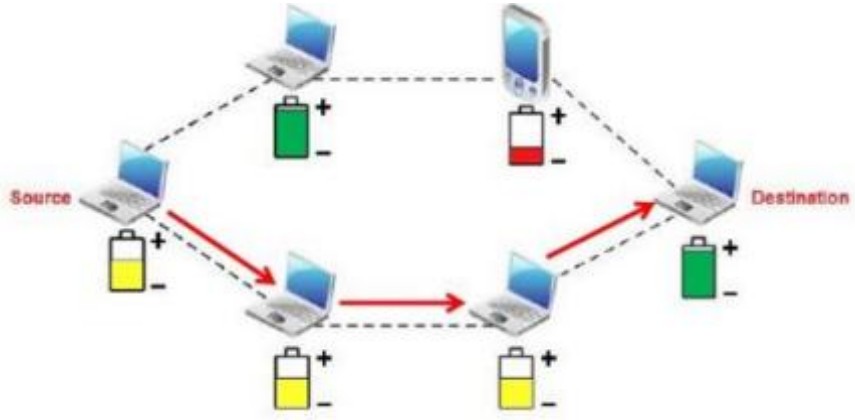


Figure 1.3: durée de vie de batterie des nœuds.

- ***Bande passante limitée:***

  La communication dans les réseaux Ad Hoc se base sur le partage d'un medium sans fil (onde radio). Ce qui induit une bande passante modeste, pour chaque hôte du réseau [3].

- ***Interférences:***

  Dans un réseau Ad Hoc, les liens radio ne sont pas isolés. Ceci peut impliquer que deux transmissions simultanées sur une même fréquence ou sur des fréquences proches peuvent interférer et provoquer des erreurs de transmission. Un grand nombre de paquets peuvent être endommagés et perdus lors du transfert [3].

- ***Sécurité physique limitée:***

Les terminaux ne sont pas protégés, ils sont menacés de vol ou de destruction, donc les nœuds d'un réseau Ad Hoc n'ont pas la même protection physique que les nœuds d'un réseau filaire. En effet, ceux d'un réseau Ad Hoc sont censés être mobiles et parfois complètement autonomes, c'est notamment le cas des réseaux de capteurs où les nœuds sont souvent lâchés, dans un environnement particulier et parfois hostile, sans aucune surveillance particulière [3].

Sécurité et Vulnérabilité:

Les réseaux sans fil sont par nature plus sensibles aux problèmes de sécurité que les réseaux filaires. Pour les réseaux Ad Hoc, le principal problème ne se situe pas tant au niveau du support physique mais principalement dans le fait que tous les nœuds sont équivalents et potentiellement nécessaires au fonctionnement du réseau [3].

I.1.3 les avantages des réseaux ad Hoc:

- ***Pas de câblages:*** *L'une des caractéristiques des réseaux Ad Hoc est l'absence d'un câblage, en effet, on élimine toutes les connexions filaires et on les remplace par des connexions radio [4][3].*
- ***Déploiement facile:*** *L'absence du câblage donne plus de souplesse et permet de déployer un réseau Ad Hoc facilement et rapidement, cette facilité peut être justifiée par l'absence d'une infrastructure préexistante permettant ainsi d'économiser tout le temps de déploiement et d'installation du matériel nécessaire [4][3].*
- ***Mobilité permise:*** *Comme l'indique leurs noms et à l'image des réseaux sans fils avec infrastructure, les réseaux mobiles Ad Hoc permettent une certaine mobilité à leurs nœud set de ce fait, ces derniers peuvent se déplacer librement à condition de ne pas s'éloigner trop les uns des autres pour garder leur connectivité [4][3].*
- ***Coût:*** *Le déploiement d'un réseau Ad Hoc ne nécessite pas d'installer des stations de base. Les mobiles sont les seules entités physiques nécessaires pour se déployer [5][3].*

I.1.4 Les inconvénient des réseaux ad Hoc:

- ***Topologie non prédictible :*** *L'activité permanant et les déplacements fréquents des nœuds d'un réseau Ad Hoc rendent son étude très difficile. La raison est bien connue le changement rapide de sa topologie du au déplacement des nœuds [6].*
- ***Capacités limitées*** *: Dans un tel réseau Ad Hoc la configuration de la portée de communication des nœuds est importante. En effet il faut qu'elle soit suffisante pour assurer la connectivité du réseau, mais plus on accroit la portée des mobiles plus les communications*

demandent de l'énergie. Il faut donc trouver un compromis entre la connectivité du réseau et la consommation énergétique [6].

- ***Taux d'erreur important :*** *Les risques de collision augmente avec le nombre de nœud qui partagent le même médium par conséquent plus la portée augmente plus le risque de collision n'est important [6].*
- ***Sécurité :*** *Un autre choix des réseaux Ad Hoc et qui attire la curiosité des chercheurs et des spécialistes de ce domaine est la notion de sécurité un réseau Ad Hoc tel que définit précédemment ne permet pas d'assurer la confidentialité de l'information échanger entre les nœuds contrairement en réseau filaire [7].*

I.1.5 Domaines d'applications

- *Les réseaux Ad Hoc sont utilisés dans toutes les applications où le déploiement d'une architecture centralisée est contraignant, voire impossible. En effet, la robustesse, le coût réduit et le déploiement rapide qu'ils présentent leur confèrent un accès à une large palette d'applications dont :*
- ***Les applications militaires:*** *Les réseaux Ad Hoc ont été utilisés la première fois par l'armée. En effet ce type de réseaux est la solution idéale pour maintenir une communication sur un champ de bataille entre les différentes troupes unités d'une armée [8][9].*

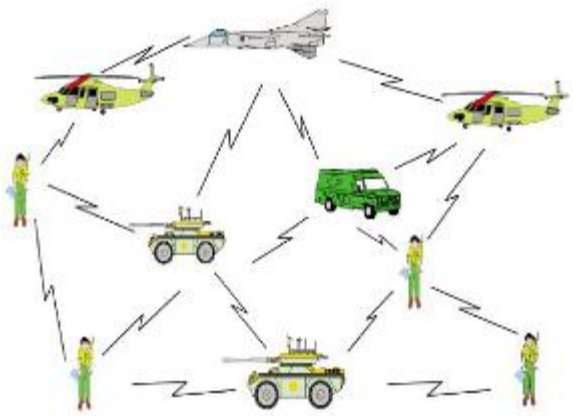


Figure 1.4 : Les applications militaires de réseau Ad Hoc.

- ***Les opérations de secours:*** *Dans les zones touchées par les catastrophes naturelles (cyclone, séisme, etc.), le déploiement d'un réseau Ad Hoc est indispensable pour permettre eux unités de secours de communiquer [8][9].*

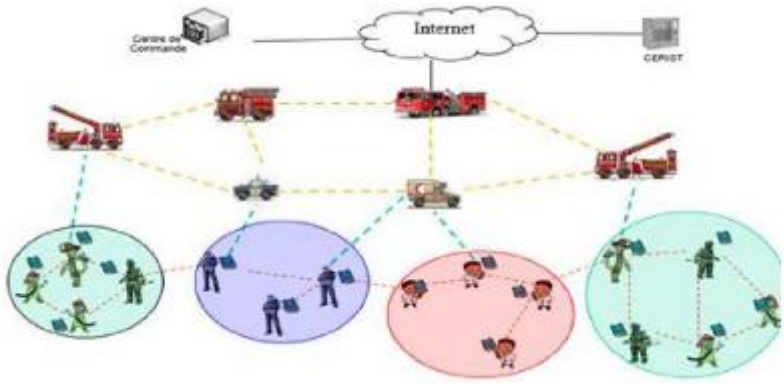


Figure 1.5: applications de secours des réseaux Ad Hoc.

- ***L'utilisation à des fins éducatives:*** *Le déploiement d'un réseau Ad Hoc lors d'une conférence ou d'une séance de cours est très judicieux car cela permet aux chercheurs et étudiants de partager des ressources (fichiers, accès à internet…etc.) et de communiquer sans avoir besoin d'une quelconque infrastructure [10].*
- ***Applications industrielles:*** *Des scénarios plus complexes dans le domaine industriel appelés réseaux de capteurs peuvent former un MANET pour s'adapter à différents environnements. Un exemple d'une telle application est la formation d'un MANET pour la surveillance médicale, la détection des Feux de forêt, la surveillance des volcans…etc [8].*
- ***Mise en œuvre des réseaux véhiculaires:*** *Sur un réseau routier les véhicules peuvent avoir besoin de communiquer entre eux ou avec leur environnement afin de partager des informations dans le but de gérer et réguler le trafic routier. Les réseaux Ad Hoc sont alors la solution idéale [8].*

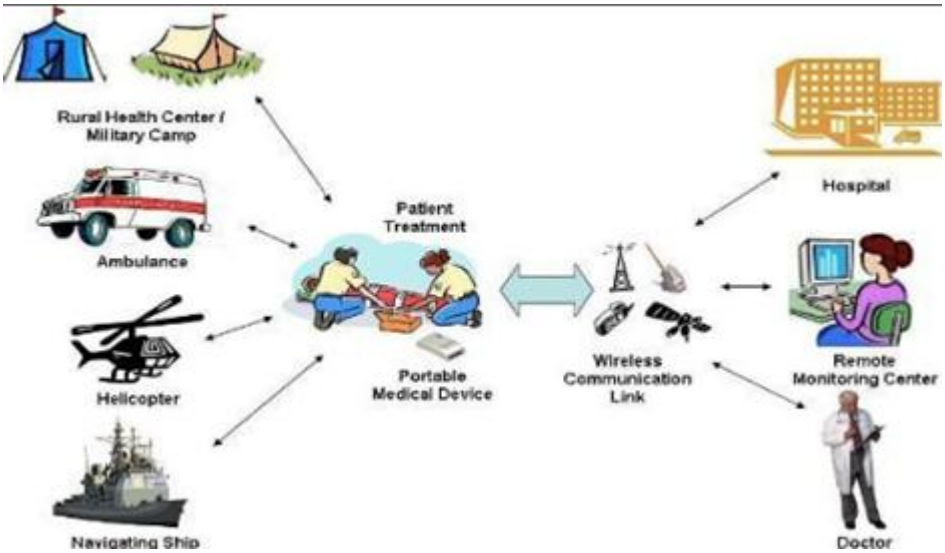


Figure 1.6: domaine d'application des réseaux Ad Hoc.

I.2 LE ROUTAGE

I.2.1 DEFINITION

Le routage est une m´méthode d'acheminement des informations vers la bonne destination à travers un réseau de connexion donnée, il consiste à assurer une stratégie qui garantit, à n'importe quel moment, un établissement de routes qui soient correctes et efficaces entre n'importe quelle paire de nœuds appartenant au réseau, ce qui assure l'échange des messages d'une manière continue [11].

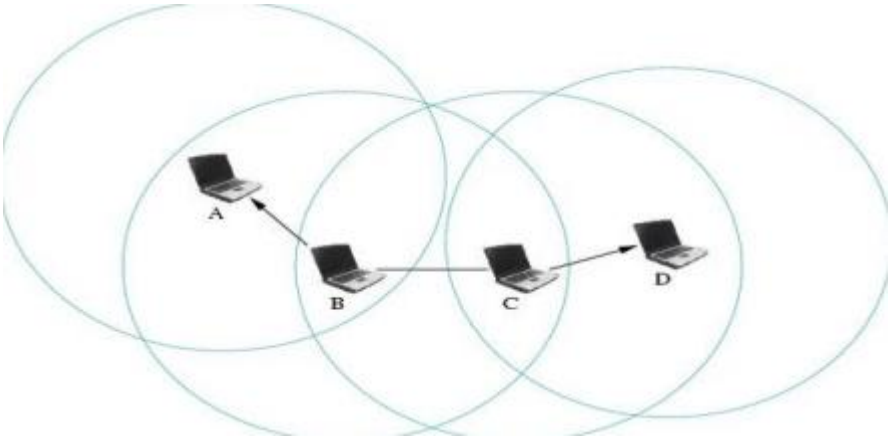


Figure 1.7: Le chemin utilisé dans le routage entre la source et la destination.

I.2.2 LE ROUTAGE DANS LES MANETS

Le routage joue un rôle très important dans les MANET puisque tous les services supportés, unicast ou multicast, se basent sur des communications multi-sauts pour l'acheminement des données. Pour réaliser les échanges, les protocoles de routage utilisent des informations locales, sur le voisinage immédiat, ou globales, concernant tout le réseau, pour déterminer les nœuds qui participent à l'acheminement des données de communications, les protocoles de routage peuvent être séparés en Proactif, Réactif et Hybride [12].

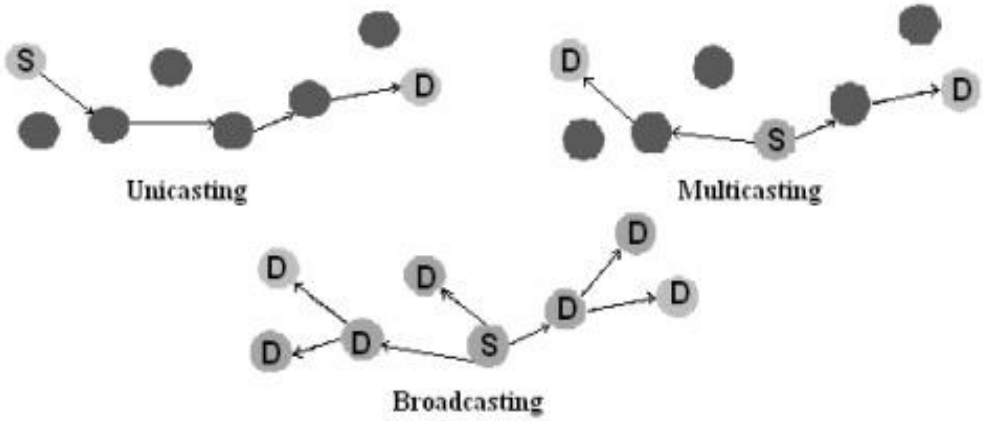


Figure 1.8: Illustration du routage unicast, multicast et broadcast.

L'objectif principal des protocoles de routage est l'établissement et la maintenance des chemins, pour que les données soient correctement délivrées dans le réseau [13]. La conception des protocoles de routage pour les MANETS est loin d'être un problème simple. Des nouvelles approches de routage sont nécessaires pour effectuer un routage de données sûr et efficace. L'instabilité du médium de communication sans fil, la limitation d'énergie et de la bande passante, ainsi que la mobilité des nœuds introduisent plus de difficulté et de complexité à la conception des protocoles de routage pour les MANETS. Nous expliquerons, dans la section suivante, les propriétés requises pour les protocoles de routage dans les MANETS.

I.2.3 Propriétés requises pour les protocoles de routage dans les réseaux Ad Hoc

Les propriétés que doivent vérifier les protocoles de routage pour les MANETS peuvent être résumés dans les points suivant:

- ***Implémentation distribuée:*** *les MANETS sont des systèmes autonomes et auto organisés. Les protocoles de routage doivent être distribués en ne reposant plus sur une administration centralisée [4].*
- ***Utilisation efficace de la bande passante:*** *la bande passante est une ressource limitée dans les MANETS. Un protocole de routage doit générer le moindre possible de paquets de contrôle [4.]*
- ***Optimisation de la consommation d'énergie:*** *dans un réseau Ad Hoc les nœuds ont besoin que leurs données soient acheminées par plusieurs nœuds intermédiaires pour qu'ils arrivent à leurs destinations. Une réduction en nombre de nœuds dégrade les performances du réseau comme elle peut aussi causer son partitionnement. Pour prolonger la durée de vie de chaque nœud et donc du réseau complet, la consommation d'énergie doit être prise en considération dans la conception des protocoles de routage [4].*
- ***Robustesse :*** *les pertes des paquets sont fréquentes dans les MANETS et elles sont dues aux collisions, à la mobilité des nœuds et à leurs durées de vie limitées. De ce fait, les protocoles de routage doivent être conçus pour continuer à fonctionner correctement même en présence des pertes [4].*
- ***Convergence rapide:*** *après la rupture d'un chemin, un protocole de routage doit rétablir un nouveau chemin le plutôt possible [4].*
- ***Elimination des boucles de routage:*** *comme les chemins sont maintenus de manière distribuée, la possibilité de création de boucles dans un chemin reste un problème sérieux.*

Le bouclage des paquets provoque une perte considérable en bande passante et en énergie. Les protocoles de routage doivent éviter/détecter la formation de boucles [4].

- ***Support des liens unidirectionnels:*** *dans les MANETS, il y a certains facteurs comme l'hétérogénéité des capacités de transmission des nœuds qui engendrent des liens unidirectionnels. Un protocole de routage doit pouvoir fonctionner même en présence de liens unidirectionnels [4].*
- ***Sociabilité:*** *les protocoles de routage doivent fonctionner efficacement même si la taille du réseau grandisse. Cela n'est pas facile à réaliser, car établir un chemin entre deux nœuds mobiles devient couteux en termes du temps requis, nombre d'opérations, et bande passante dissipée, quand le nombre de nœuds augmente [4].*
- ***Optimisation des métriques:*** *parmi les métriques qui méritent d'être considérées lors de la conception des protocoles de routage pour les MANETS, on peut citer: -Taux de délivrance maximal. -Plus court chemin. -Consommation d'énergie minimale.*
-Minimum de charge de routage (bande passante). -Stabilité des chemins [4].

I.2.4 Services de routage dans les réseaux Ad Hoc

Les réseaux Ad Hoc étant de nature multi-sauts, le protocole de routage détermine une route entre un nœud source et un nœud destination. De par la faible bande passante offerte par les réseaux Ad Hoc et du fait de la diffusion des données, les protocoles de routage actuellement utilisés dans les réseaux filaires ne peuvent être utilisés, sans modifications, dans les réseaux MANETS. De fait, des nouveaux protocoles de routage ont dû être développés [1].

Pour être réellement opérationnel dans un environnement mobile, le protocole de routage prend en compte trois phases :

- ***Dissémination de l'information de routage:*** *elle permet de connaître suffisamment d'éléments sur la topologie pour choisir un chemin atteignant le nœud de destination. Suivant la quantité d'informations échangées, les nœuds obtiennent une vue plus ou moins précise de la topologie du réseau. Le protocole de routage se voit dans l'obligation d'optimiser l'envoi de ces informations, car elles sont fortement consommatrices en bande passante [1].*
- ***Sélection du chemin:*** *une fois les informations de routage obtenues, le protocole de routage peut sélectionner une route parmi l'ensemble obtenu en fonction de certains critères. Pour les protocoles Meilleur effort (« Best Effort »), le critère est de minimiser le nombre de sauts du chemin. Ainsi, parmi l'ensemble des routes qui lui sont proposées, le protocole choisit celle traversant le plus faible nombre de nœuds. Les routes choisies doivent être dépourvues de boucles. La présence de boucles rend inefficace le chemin sélectionné puisque le paquet ne pourra pas atteindre la destination consommant inutilement de la bande passante. En effet, un*

paquet de données transitant sur un chemin, possédant une boucle, va tourner en rond tant que la boucle est présente. Pour éviter qu'un paquet de données tourne indéfiniment, le paquet est détruit lorsqu'il atteint la limite imposée par le champ TTL présent dans le protocole IP. Un protocole de routage peut créer deux sortes de boucles: les boucles temporaires et les boucles permanentes [1]. Les premières ont lieu pendant le transfert d'un message de routage. Durant ce temps, des stations peuvent être mises à jour et d'autres non, d'où la possible apparition d'une boucle. Elle dure au maximum la durée de traversée du réseau par un message de routage.

Les boucles permanentes, quant à elles, sont dues au phénomène du bouclage à l'infini [1]. Ces boucles peuvent consommer énormément de bande passante.

- ***Maintenance des routes:*** *dans un environnement mobile, la topologie du réseau ne cesse d'évoluer avec le temps. De fait, les routes sont amenées à changer avec le déplacement des nœuds. Une route doit éviter de rester longtemps interrompue, car les paquets ne pourraient atteindre leur destination. Le protocole de routage doit donc tenir compte de ces changements et mettre à jour les routes qui viennent à être coupées [1].*

I.2.5 Les contraintes de routages dans les réseaux Ad Hoc

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

- ***Minimisation de la charge du réseau:*** *l'optimisation des ressources du réseau renferme deux autres sous problèmes qui sont l'évitement des boucles de routage, et l'empêchement de la concentration du trafic autour de certains nœuds ou liens [2].*
- ***Bon acheminement des données:*** *le fait que les chemins utilisés pour router les paquets de données puissent évoluer, ne doit pas avoir d'incident sur le bon acheminement des données. L'élimination d'un lien, pour cause de panne ou pour cause de mobilité devrait, idéalement, augmenter le moins possible les temps de latence [2].*
- ***Assurer un routage optimal:*** *la stratégie de routage doit créer des chemins optimaux et pouvoir prendre en compte différentes métriques de coûts (bande passante, nombre de liens, ressources du réseau,... etc.). Si la construction des chemins optimaux est un problème dur, la maintenance de tels chemins peut devenir encore plus complexe, la stratégie de routage doit assurer une maintenance efficace de routes avec le moindre coût possible [2].*

- ***Le temps de latence:*** *la qualité des temps de latence et de chemins doit augmenter dans le cas où la connectivité du réseau augmente [2].*

I.3 CLASSIFICATION DES PROTOCOLES DE ROUTAGE

Ce sont principalement des régimes à base topologique qui utilisent une approche réactive, proactive ou hybride pour créer des itinéraires [3]. Comme il est illustré dans la figure 1.9.

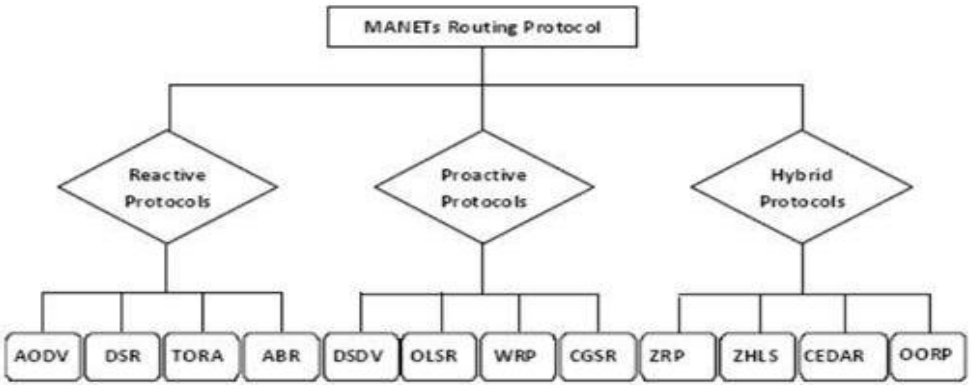


Figure 1.9 : la classification des protocoles de routage.

I.3.1 Les protocoles à vecteur de distance

Dans les protocoles à vecteur de distances, la table de routage d'un nœud est calculée en fonction des tables reçues par ses voisins, comme son nom l'indique, ce protocole fonctionne selon une notion de distance. Chaque nœud enregistre dans sa table de routage les next-hops et les distances nécessaires pour atteindre toutes les destinations du réseau. Selon le protocole, cette distance peut être le nombre de hop, la bande passante, etc. À chaque modification de sa table de routage, le nœud broadcaste celle-ci. Cette table peut être modifiée lorsqu'une autre table a été reçue d'un voisin, ou lorsque le nœud a détecté un changement de topologie dans son voisinage. Lorsqu'un nœud reçoit une table de routage d'un de ses voisins, il recalcule les routes les plus courtes pour chaque destination. Ces calculs sont effectués via l'équation de Bellman-Ford. Les vecteurs de distances sont des messages utilisés pour distribuer les informations à propos du réseau. À la création du réseau, chaque nœud crée une table de routage contenant son propre identifiant comme destination et next-hop et un coût associé nul. À intervalles réguliers, chaque nœud envoie sa table de routage à ses voisins via des vecteurs de distances [1]. Le nom de ces messages est issu du fait qu'ils peuvent être vus comme des vecteurs où la direction est le voisin à contacter et la distance est le nombre de hops à effectuer pour atteindre la destination. Lorsqu'un nœud réceptionne un tel message, il utilise l'équation de Bellman-Ford pour déterminer si la table de routage actuelle doit être mise à jour avec celle reçue de son voisin. Si la table est mise à jour, le nœud envoie sa nouvelle table à ses voisins. Ce processus continue

tant que des mises à jour sont à réaliser par les nœuds. Une fois que tous les nœuds ont obtenu les informations sur les meilleures routes, le réseau est stabilisé. Si un nœud détecte un changement de topologie, c'est-à-dire que l'un de ses voisins n'est plus accessible, le nœud indique son voisin comme inaccessible dans sa table de routage, partage celle-ci à son voisinage et l'information est transmise sur l'ensemble du réseau [1].

I.3.2 Les protocoles à état de liens

Dans les protocoles à état de liens, chaque nœud connaît à tout moment la topologie complète du réseau, c'est-à-dire l'état des liens existant entre chaque couple de nœuds du réseau. L'ensemble du réseau peut être comparé à une carte routière. À chaque intersection (c.-à-d. les nœuds du réseau), il faut déterminer quelle est la meilleure direction à prendre (c.-à-d. la liaison vers un nœud voisin) pour atteindre une certaine destination. Pour ce faire, chaque nœud envoie à l'ensemble du réseau tous les nœuds auxquels il est relié. Sur base de ces informations, chaque nœud peut calculer indépendamment le meilleur next-hop pour atteindre chaque destination. Il est possible que certaines routes changent, apparaissent ou disparaissent. Dans ce cas, il faut en informer l'ensemble du réseau. Voici comment se déroulent les communications au sein de ce type de protocole, comme expliqué par J. Doyle [1]. On peut distinguer trois phases :

- ✓ *La découverte du voisinage.*
- ✓ *La distribution de la topologie.*
- ✓ *La détermination des meilleures routes.*

a. ***Découverte du voisinage :*** *Les messages HELLO sont utilisés pour gérer le voisinage sur le réseau. À intervalles réguliers, chaque nœud broadcaste un message HELLO pour avertir de sa présence. Une fois que deux nœuds se sont découverts mutuellement, ils se considèrent chacun comme voisins. Ces messages servent aussi à détecter la disparition de nœuds et les défaillances de liens: si un nœud n'a pas reçu de message HELLO d'un de ses voisins endéans un certain temps, le lien avec ce voisin est considéré comme rompu [1].*

b. ***Distribution de la topologie :*** *Pour distribuer les informations sur l'état du réseau, chaque nœud broadcaste un message LSA (Link State Advertisement) à intervalles réguliers. Ce type de message contient l'identifiant du nœud originaire du paquet, une liste de tous les voisins de ce nœud et un numéro de séquence incrémenté à chaque nouvel envoi. Lorsqu'un nœud reçoit un LSA, il sauvegarde les informations sur le nœud d'origine du message ainsi que sur l'ensemble de ses voisins. Ensuite, il broadcaste le message LSA à son tour. Il peut arriver qu'un même nœud reçoive plusieurs messages LSA d'une même origine. Dans ce cas, le numéro de séquence présent dans le message est utilisé pour déterminer si celui-ci a déjà été traité ou non. Pour ce*

faire, chaque nœud enregistre dans une table l'identifiant du nœud ayant envoyé le message et le plus grand numéro de séquence reçu. Si un paquet est reçu avec un numéro de séquence inférieur à celui enregistré, c'est qu'il a déjà été traité. Par la suite, à partir de toutes les informations récupérées, chaque nœud est capable de générer une carte du réseau comprenant l'ensemble des nœuds connus et leurs interconnexions. Cette carte doit être mise à jour à chaque réception d'un nouveau message TC contenant des modifications de topologie [1].

c. Détermination des meilleures routes : *Une fois la carte du réseau générée, chaque nœud peut déterminer les meilleurs next-hops pour atteindre chaque destination. Pour ce faire, des algorithmes de calcul de plus court chemin sont utilisés tel que l'algorithme de Dijkstra. Une table de routage contenant les next-hops pour chaque destination du réseau est maintenue et mise à jour à chaque modification de la carte du réseau. Il s'agit là de l'intuition de base pour tout protocole de routage à état de liens. Énormément de protocoles sont basés sur ce modèle, les plus utilisés étant IS-IS et OSPF [1]. Le principal avantage de ce type de protocole est qu'à tout moment, le meilleur next-hop pour atteindre tout nœud du réseau est connu. On a donc une propagation très rapide des paquets au sein du réseau. Par contre, ce type de protocole a une réaction assez lente aux changements de topologie, étant donné qu'il faut attendre la réception de nouveaux messages LSA pour connaître les mises à jour à effectuer. De plus, la quantité d'informations à maintenir à propos du réseau peut être très importante. Au niveau des réseaux sans fil, ce protocole a d'autres défauts. Dans le cas des réseaux sans fil mobiles, les changements très fréquents de topologie mènent à l'utilisation de routes rapidement périmées. De plus, les broadcastes de messages peuvent vite provoquer de la congestion sur le réseau et encouragent les risques d'interférences de signal. C'est pourquoi d'autres protocoles ont du être inventés afin de remédier à ces problèmes. Les protocoles OLSR et B.A.T.M.A.N. sont basés sur le protocole LSR et proposent certaines optimisations propres aux réseaux mobiles sans fil.*

I.3.3 Les protocoles de routage proactifs

I.3.3.1/Définition

Les protocoles de cette catégorie sont basés sur les algorithmes classiques d'état de liens et de vecteur de distance. Les protocoles de routage proactifs essaient de maintenir les meilleurs chemins existants, vers toutes les destinations possibles au niveau de chaque nœud du réseau. Les routes sont sauvegardées même si elles ne sont pas utilisées [14].

I.3.3.2 Avantages

- ✓ *Pas de temps de réaction.*
- ✓ *Adaptés aux réseaux denses de taille moyenne.*
- ✓ *Adaptés aux réseaux à forte mobilité.*

I.3.3.3 Inconvénients

- ✓ *Trafic de contrôle important.*
- ✓ *Capacité d'échange du réseau limitée.*

I.3.4 Protocole de routage réactif

I.3.4.1 Définition

Les protocoles réactifs adoptent des algorithmes classiques tels que le routage par vecteur de distance. Les routes sont établies uniquement sur demande et seules les routes en cours d'utilisation sont maintenues.
Lorsqu'un nœud veut envoyer des paquets, une étape de découverte de route est initiée par la diffusion d'un message de recherche de route. Tout nœud qui reçoit ce message et qui ne dispose pas d'informations à propos de la destination, il diffuse à son tour le message. Ce mécanisme est appelé mécanisme d'inondation [15].

I.3.4.2 Avantages

- ✓ *Trafic de contrôle faible.*
- ✓ *Adaptés aux grands réseaux.*
- ✓ *Consommation énergétique réduite.*

I.3.4.3 Inconvénients

- ✓ *Temps de réaction long.*
- ✓ *Problème en cas de forte mobilité des nœuds.*

I.3.5 Les protocoles de routage hybrides (les zones)

I.3.5.1 Définition

Les protocoles de routage hybrides combinent les deux approches de routage réactif et proactif. Dans ce type de protocole, on peut garder la connaissance locale de la topologie jusqu'une certaine distance (nombre prédéfini de sauts) par un échange périodique de trame de contrôle, autrement dit par une technique proactive. Les routes vers des nœuds plus lointains sont obtenues par schéma réactif, c'est-à-dire par l'utilisation de paquets de requête en diffusion. Avec ce système, on dispose immédiatement des routes dans notre voisinage proche, et lorsque la recherche doit être étendue plus loin, elle en est optimisée [16].

I.3.5.2 Avantages et inconvénients des protocoles hybrides

Le protocole hybride est un protocole qui se veut comme une solution mettant en commun les avantages des deux approches précédentes en utilisant une notion de découpage du réseau. Cependant, il rassemble toujours quelques inconvénients des deux approches proactives et réactives [5].

I.4 Le protocole de routage OLSR (Optimized Link State Routing)

I.4.1 Définition :

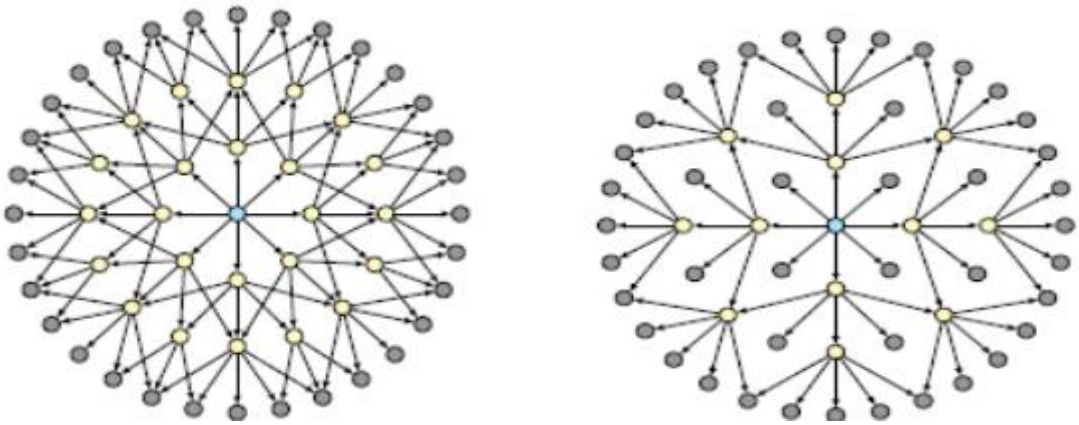
OLSR est un protocole proactif qui repose sur l'échange régulier d'informations sur la topologie du réseau et aussi un protocole à état de liens qui construit des routes du plus court chemin.

L'algorithme est optimisé par la réduction de la taille et du nombre des messages échangés. Seuls des nœuds particuliers, les MPR (Multi Point Relay) diffusent des messages de contrôle sur la totalité du réseau. Le MPR est le nœud sélectionné par un de ses voisins immédiats pour retransmettre ses messages à travers le réseau. L'ensemble des MPRs d'un nœud est choisi parmi les voisins immédiats, de manière à permettre d'atteindre tous les nœuds situés exactement à 2 sauts.

Tous les nœuds envoient périodiquement des messages HELLO à leurs voisins immédiats sur chacune de leurs interfaces. Ces messages permettent à chaque nœud de maintenir à jour toutes les informations nécessaires au choix des relais multipoints et effectuer le calcul des tables de routage.

Le routage vers les stations éloignées de plus d'un saut se fait grâce aux MPR, qui diffusent périodiquement des messages de contrôle de la topologie TC (Topology Control) contenant la liste de leurs MPRs. Ces messages servent à maintenir dans chaque station une table de la topologie du réseau. La table de routage est construite et mise à jour à partir des informations contenues dans la table des interfaces voisines et la table de la topologie, en utilisant un algorithme du plus court chemin.

La métrique prise en compte est le nombre de sauts [18].



a. Routage par inondation (24 transmissions pour atteindre tous les nœuds à 3 sauts).

b. Routage avec les nœuds MPR (12 transmissions pour atteindre tous les nœuds à 3 sauts).

Figure 1.10: Avantage de l'utilisation des MPR.

OLSR étant proactif, chaque nœud construit en permanence une vision de la topologie du réseau sous forme d'un graphe où les arcs constituent les liens entre les nœuds. La cohérence de cette vision est assurée grâce à des diffusions périodiques des liens sortants. Ainsi, un nœud recevant ces informations met à jour sa vision de la topologie et applique l'algorithme du plus court chemin pour choisir le prochain saut en direction de chaque destination. Nous présentons maintenant les étapes permettant la construction de la topologie:

- ***Écoute des voisins (neighbors ensing):*** *Il s'agit du processus de découverte du voisinage direct et symétrique qui est effectué grâce à la diffusion périodique de messages de type HELLO contenant des informations sur le voisinage ainsi que l'état des liens (link state) le reliant à cet ensemble de nœuds. Ce message de contrôle est destiné exclusivement aux voisins à un saut et n'est donc pas retransmis. De cette manière, un nœud construit la liste des voisins à un saut (Neighbor Set) tout en marquant les liens symétriques et puisqu'il voit aussi la liste des voisins de ceux-ci, il construit la liste des voisins à deux sauts (2-Hops Neighbor Set) [17].*
- ***Sélection des relais multi-point****: Cette sélection est faite de façon indépendante par chaque nœud. Elle passe par le choix du sous ensemble des nœuds à un saut qui permettent d'atteindre l'intégralité de voisins à deux sauts. Dans la figure 1.8, le nœud 1 choisit 2 comme MPR parce que c'est le seul nœud qui lui permet d'atteindre 5. Ensuite, il choisit le nœud 3 lui permettant d'atteindre 6, 7 et 8. De cette manière il couvre la totalité des voisins à deux sauts. Le sous ensemble obtenu est annoncé à tous les voisins dans des messages HELLO ultérieurs [7].*

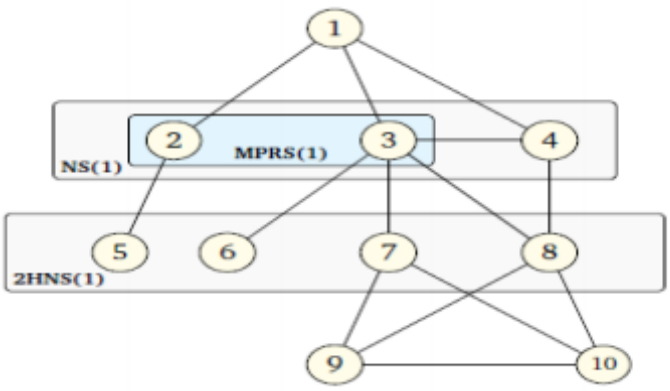


Figure 1.11: Choix des relais multi-point pour le nœud 1.

- ***Déclaration des relais multi-point****: Les nœuds MPR diffusent des paquets de contrôle spécifiques appelés TC (Topology Control) pour construire une base d'informations sur la topologie du réseau. Les messages TC sont transmis à intervalles réguliers et déclarent l'ensemble MPRSS (Multi Point Relay Selector Set), c'est-à-dire l'ensemble contenant les voisins ayant choisit le nœud origine de ce message comme MPR. Les informations sur la*

topologie du réseau reçues dans les messages TC sont enregistrées dans la table de topologie (topology table) [7].

- ***Calcul de la table de routage**: La table des voisins (neighbor table) ainsi que la table de topologie (topology table) sont utilisées pour le calcul de la table de routage qui se base sur l'algorithme du plus court chemin.*

  Toute modification de l'une de ces tables entraine la modification de la table de routage. Cette amélioration à base de relais multi-point fournit des routes optimales en nombre de sauts tout en diminuant le nombre de messages de contrôles qui circulent lors d'une diffusion. Il convient ainsi aux grands réseaux Ad Hoc mais semble être moins efficace pour des petits réseaux [17].

I.4.2 Différents mécanisme utilisé dans le fonctionnement de ce protocole

a. ***Découverte de voisinage***

Chaque nœud émet périodiquement des messages appelés HELLO qui contiennent essentiellement la liste des liens connus vers les voisins directs. La fonction de ces messages est multiple. Ils servent tout d'abord à détecter les voisins directs et la qualité des liens vers ceux-ci, à savoir s'ils sont symétriques ou asymétriques. Comme chaque nœud y publie la liste de ses voisins, il est possible pour un nœud d'acquérir des informations sur son voisinage à deux sauts. Par ailleurs, une fois qu'un nœud a effectué la sélection de ses MPRs, il indique dans ses messages HELLO lesquels de ses voisins sont ses MPRs. Ceci permet à un nœud de savoir quels voisins l'ont choisi comme MPR, autrement dit de constituer son ensemble de ***MPR-selectors*** *[2.]*

b. ***Diffusion optimisée***

Lorsque qu'un nœud reçoit un message de contrôle OLSR, il le traite et ne le transmet que si l'émetteur du message (l'adresse source du message, qui peut être différente de l'adresse de l'émetteur si le message a été généré par un nœud distant) appartient à l'ensemble des MPR selectors. Cette technique permet de diffuser des messages dans tout le réseau en évitant la saturation [2].

c. ***Les messages topologiques***

Les messages topologiques, appelés ***TC*** *(topology control) ne sont émis par un nœud qu'à condition que son ensemble de MPR-selectors n'est pas vide, c'est-à-dire qu'il est MPR d'un de ses voisins. Les messages contiennent la liste des MPR-selectors du nœud. Les nœuds du réseau reconstituent donc une topologie globale mais partielle, puisque tous les nœuds atteignables sont connus, mais pas tous les liens. Cette topologie partielle est néanmoins suffisante pour calculer des chemins minimaux en nombre de sauts vers toute destination.*

Le fait de ne permettre qu'aux MPRs de générer des messages TC permet de limiter la quantité de messages diffusés dans le réseau et le fait de ne diffuser que la liste des MPR selectors permet de limiter la taille des messages [2].

d. ***Les changements topologiques***

À chaque changement de topologie, le calcul des routes vers toutes les destinations est déclenché pour mettre à jour les tables de routage. Par ailleurs, lorsque son ensemble de voisins directs ou à deux sauts change, un nœud doit effectuer la sélection de ses MPRs à nouveau [2].

e. ***Calcul des routes***

Une fois que les nœuds auraient envoyé les TC (les liens qui leur lie aux MPRs), chaque nœud constitue sa matrice des coûts et utilise un Algorithme de recherche de plus court chemin dans un graphe pour tracez sa cartographie du réseau (méthode à état des liens).

Dans ce protocole, seuls les nœuds, pour lesquels le MPRs-selector est non vide, ont droit à diffuser les messages topologiques. Si bien que la quantité de message de contrôle générer par le réseau est limité. La convergence des tables de routage est rapide dans la mesure où chaque nœud constitue sa cartographie du réseau au lieu d'attendre que leur voisin le leur communique. Pour ce qui est le délai de transmission, il est efficace vu la nature proactive du protocole. En fin, ce protocole montre tous ces avantages mais il n'y a aucun algorithme de recherche de plus court chemin qui résout complètement le problème de boucle de routage temporaire, aussi, les fonctions de calcules qui permettent à un nœud de sélectionner ses MPRs sont très complexes [2].

I.5 Le protocole de routage AODV (Ad Hoc On demand Distance Vector)

I.5.1 PRESENTATION :

*AODV (Ad-hoc On-demand Distance Vector), qui a été normalisé dans la RFC 3561**.** AODV a fait l'objet de nombreux travaux. Comme DSR, il s'agit d'un protocole réactif, et donc il existe des similitudes importantes entre les deux protocoles. Néanmoins, AODV n'utilise pas de routage par la source, et utilise des numéros de séquence afin de déterminer si un message est plus récent ou ancien que l'information déjà connue. En outre, une métrique est utilisée afin de pouvoir utiliser une meilleure route si elle devient disponible, il s'agit d'une métrique comptant simplement le nombre de sauts [2].*

I.5.2 TABLE DE ROUTAGE

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.*
- ✓ *Le nœud suivant.*
- ✓ *La distance en nombre de nœud (i.e. le nombre de nœud nécessaire pour atteindre la destination).*
- ✓ *Le numéro de séquence destination qui garantit qu'aucune boucle ne peut se former.*
- ✓ *Liste des voisins actifs (origine ou relais d'au moins un paquet pour la destination pendant un temps donné).*
- ✓ *Le temps d'expiration de l'entrée de la table.*
- ✓ *Un tampon de requête afin qu'une seule réponse soit envoyée par requête. A chaque utilisation d'une entrée, son temps d'expiration est remis à jour (temps courant + active route time) [2].*

I.5.3 LES MESSAGES DE CONTROLE DE PROTOCOLE AODV

Les mécanismes de découverte et de maintenance de routes peuvent s'effectuer par le biais des messages de contrôles suivants:

RREQ (Route Request): *Message de demande de route.*

RREP (Route Reply): *Message de réponse à un RREQ.*

RERR (Route Error): *Message qui signale la perte d'une route.*

Le format des paquets est donné ci-dessous:

I.5.3.1 Message de demande de route RREQ

Il contient essentiellement les champs suivants: [2]

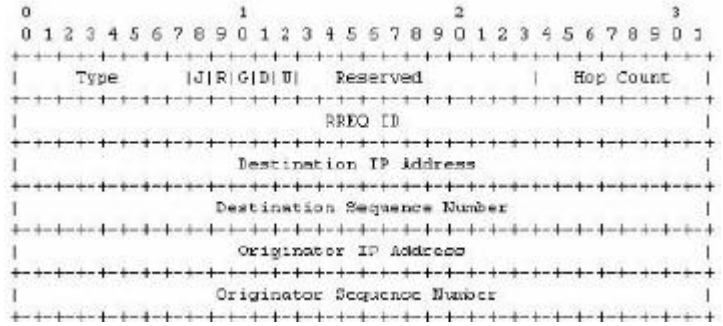


Figure (1.12) : Format du message RREQ.

- ***Type (8 bits):*** *ce champ indique le type de paquet, dans ce cas il prend la valeur 1.*
- ***Flags (drapeaux) (5 bits):*** *ce champ contient cinq flags (J, R, G, D, U) tel que:*

- ✓ ***J (Join flag) et R (Repair flag):*** *sont réservés pour le multicast.*
- ✓ ***G (Gratuitous RREP flag):*** *indique si un message RREP spécifique doit être envoyé à la destination dans le cas ou un nœud intermédiaire possède un chemin à la destination.*
- ✓ ***D (Destination only flag):*** *ce drapeau indique si seulement la destination qui doit répondre à la requête ou pas.*
- ✓ ***U (Unknownsequencenumber)****: indique le numéro de séquence de la destination est inconnu.*

- ***Reserved (11 bits):*** *initialisé à la valeur 0 et ignoré à la réception du message.*
- ***Hop Count (8 bits):*** *il contient le nombre de sauts parcourus par RREQ.*
- ***RREQ ID:*** *il identifie la requête parmi les requêtes envoyées par la même source.*
- ***Destination IP Address:*** *l'adresse IP de destination pour laquelle une route est désirée.*
- ***Destination Séquence Number:*** *Le dernier numéro de séquence reçu dans le passé par le créateur pour n'importe quelle route vers la destination.*
- ***Originator IP Adress:*** *l'adresse IP de la source de la requête.*
- ***OriginatorSequenceNumber:*** *Le nombre de séquence courant de la source contenue dans la table de routage de ce nœud* ***s****.*

I.5.3.2 Message de réponse à un RREQ par RREP

Il contient essentiellement les champs suivants: [2]

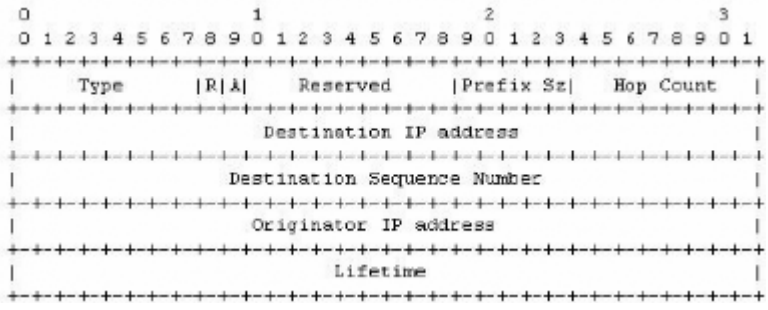


Figure (1.13): Format du message RREP.

- ***Type (8 bits):*** *ce champ indique le type de paquet, dans ce cas il prend la valeur 2.*
- ***Flags (drapeaux) (2 bits):*** *ce champ contient deux flags:*
  - ✓ ***R (Repair flag):*** *utilisé pour le multicast.*
  - ✓ ***A (Acknowledgmentrequired):*** *indique si la source doit envoyer un acquittement pout les messages RREP.*
- ***Reserved (9 bits):*** *initialisé à la valeur 0 et ignoré à la réception du message.*
- ***Préfix Sz (5 bits):*** *si la valeur de ce champs est différente de zéro, ce dernier indique que le nœud prochain peut être utilisé pour chaque nœud demandant cette destination et qui possède la même valeur de Préfix Sz.*

- ***Hop Count (8 bits):*** *il contient le nombre de sauts entre la source jusqu'à la destination.*
- ***Destination IP Address:*** *l'adresse IP de la destination du paquet RREQ.*
- ***Destination SequenceNumber:*** *le numéro de séquence de la destination associé à cette route.*
- ***Originator IP Adress:*** *l'adresse IP du nœud qui crée la requête.*
- ***Lifetime:*** *le temps pour lequel chaque nœud qui reçoit RREP considère que la route est valide.*

I.5.3.3 Message de perte de route RERR

Un message d'erreur de route contient essentiellement les champs suivants: [2]

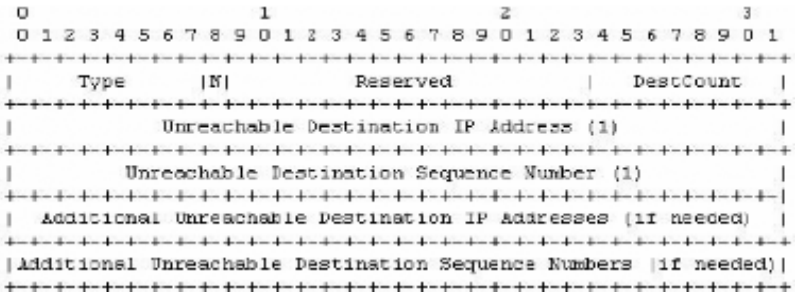


Figure (1.14) : Format du message RERR.

- ***Type (8 bits):*** *la valeur de ce champ prend 3 dans le message RRER.*
- ***Flag (1 bits):*** *il contient un drapeau (N: No delete flag), celui-ci est indicatif lorsqu'un nœud est capable de réparer le lien, et informe les nœuds suivants qu'ils ne doivent pas supprimer le chemin.*
- ***Reserved (15 bits):*** *initialisé à la valeur 0 et ignoré à la réception du message.*
- ***DestCount (8 bits):*** *il indique le nombre de destinations inaccessibles incluses dans ce message, ce champ doit être supérieur ou égal à un.*
- ***Unreachable Destination IP Address:*** *l'adresse IP des destinations inaccessibles pour la raison de cassure de lien.*
- ***Unreachable Destination SequenceNumber:*** *le nombre de séquence de la liste des destinations inaccessibles qui se trouve dans le champ Unreachable Destination IP Address.*

I.5.4 LE PRINCIPE DE NUMERO DE SEQUENCE

La circulation inutile des paquets de messages, qui peut arriver avec le DBF (Distribution de Bellman Ford), est intolérable dans les réseaux mobiles Ad Hoc, caractérisés par une bande passante limitée et des ressources modestes. L'AODV utilise les principes de numéro de séquence afin d'éviter le problème des boucles infinie et des transmissions inutiles de changent fréquemment ce qui fait que les routes maintenus par certains nœuds, deviennent invalide. Les numéros de séquence permettent d'utiliser les routes les plus nouvelles ou autrement dit les plus fraiches (fresh routes), un nœud les mis à jour chaque fois qu'une nouvelle information provenant d'un message RREQ, RREP ou RERR, il incrémente son propre numéro de séquence dans les circonstances suivantes:

- ✓ *Il est lui-même le nœud destination et offre une nouvelle route pour l'atteindre.*
- ✓ *Il reçoit un message AODV (RREQ, RREP, RERR) contenant de nouvelles informations sur le numéro de séquence d'un nœud destination.*
- ✓ *Le chemin vers une destination n'est plus valide [2].*

I.5.5 FONCTIONNEMENT DU PROTOCOLE AODV

AODV, est un protocole de routage réactif à vecteur de distance qui s'inspire de DSDV. Contrairement à celui-ci, il ne construit pas a priori la table de routage mais réagit à la demande et essaie de trouver un chemin avant de router les informations. Tant que la route reste active entre la source et la destination, le protocole de routage n'intervient pas, ce qui diminue le nombre de paquets de routage échangés entre les nœuds constituant le réseau [1].

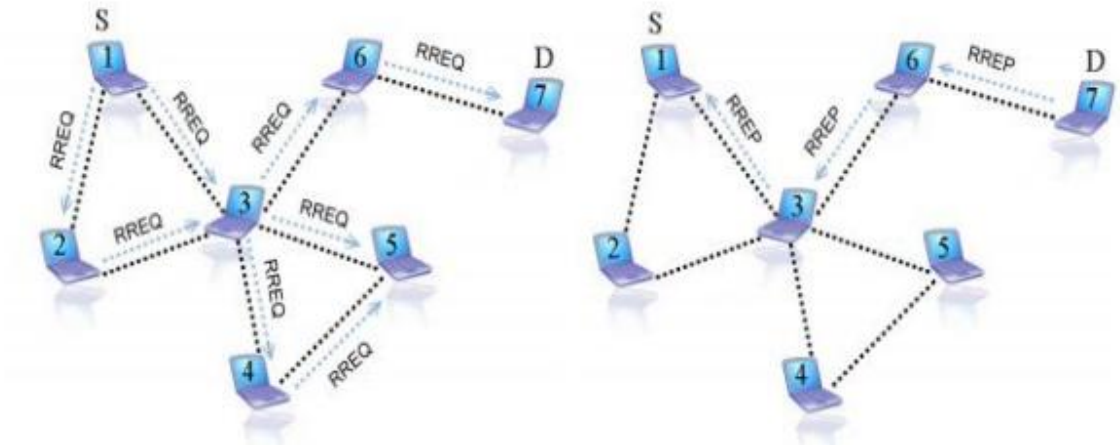


Figure 1.15: les deux requêtes RREQ et RREP utilisées dans le protocole AODV.

*Lorsqu'un nœud **S** essaie de communiquer avec un nœud **D**, l'échange de messages se fait en plusieurs étapes décrites ci-dessous à l'aide de l'exemple de la figure 1.16.*

I.5.5.1 Découverte de route

Lorsqu'un nœud source a besoin d'une route vers une certaine destination (e.g: le nœud 1 dans la figure 1.16 désire envoyer des données au nœud 5) et qu'aucune route n'est disponible (la route peut être non existante, avoir expiré ou être défaillante), la source 1 diffuse en broadcast (voir figure 1.16a) un message de demande de route RREQ (Route REQUEST), ce message contient un identifiant (RREQ_ID) associé à l'adresse de la source (@SRC) qui servira à identifier de façon unique une demande de route. Le nœud 1 enregistre cet identifiant de paquet RREQ ([RREQ_ID, @SRC]) dans son historique (buffer) et l'associe à un time qui décomptera sa durée de vie au delà de laquelle cette entrée sera effacée. Quand un nœud intermédiaire (cas des nœuds 2 et 4 dans la figure 1.16b) qui n'a pas de chemin valide vers la destination reçoit le message RREQ, il ajoute ou met à jour le voisin duquel le paquet a été reçu. Il vérifie ensuite qu'il ne l'a pas déjà traité en consultant son historique des messages traités. Si le nœud s'aperçoit que la RREQ est déjà traitée, il l'abandonne et ne la rediffuse pas Sinon, il met à jour sa table de routage à l'aide des informations contenues dans la requête afin de pouvoir reconstruire ultérieurement le chemin inverse vers la source, il incrémente ensuite le nombre de sauts HC (Hop Count) dans la demande de route et la rediffuse. Il est à noter qu'AODV utilise le principe des numéros de séquence pour pouvoir maintenir la cohérence des informations de routage. Ce numéro, noté SN (SequenceNumber), est un champ qui a été introduit pour indiquer la fraicheur de l'information de routage et garantir l'absence de boucles de routages. À la réception d'un paquet RREQ (figure 1.16c), la destination 5 ajoute ou met à jour dans sa table de routage un chemin vers le nœud voisin duquel il a reçu le paquet (nœud 4) ainsi qu'un chemin vers la source 1. La destination 5 génère ensuite une réponse de route RREP qu'elle envoie en unicast vers le prochain saut en direction de la source (voir figure 1.16c). Notons qu'un nœud intermédiaire peut aussi générer un RREP si la requête l'autorise à le faire (bit destination only de la RREQ mis à 0) et qu'il dispose déjà dans sa table de routage d'un chemin valide vers la destination 5. Les nœuds intermédiaires qui reçoivent la RREP (cas du nœud 4 dans la figure 1.16d) vont mettre à jour le chemin qui mène à la destination dans leur table de routage et retransmettre en unicast le message (après avoir incrémenté le nombre de sauts) vers le nœud suivant en direction de la source sachant que cette information a été obtenue lors du passage de la RREQ. Lorsque la réponse de route atteint la source (nœud 1 dans l'exemple), un chemin

bidirectionnel est établi entre la source et la destination (voir figure 1.5) et la transmission de paquets de données peut débuter [1].

I.5.5.2 Maintenance des routes

Afin de maintenir les routes, une transmission de messages HELLO est effectuée. Ces messages sont en fait des réponses de route (RREP) diffusés aux voisins avec un nombre de sauts égal à un. Si au bout d'un certain temps, aucun message n'est reçu d'un nœud voisin, le lien en question est considéré défaillant. Alors, un message d'erreur RERR (Route ERROR) se propage vers la source et tous les nœuds intermédiaires vont marquer la route comme invalide et au bout d'un certain temps, l'entrée correspondante est effacée de leur table de routage. Le message d'erreur RERR peut être diffusé ou envoyé en unicast en fonction du nombre de nœuds à avertir de la rupture de liaison détectée. Ainsi, s'il y en a un seul, le message est envoyé en unicast sinon, il est diffusé.

AODV à l'avantage de réduire le nombre de paquets de routage échangés étant donné que les routes sont créées à la demande et utilise le principe du numéro de séquence pour éviter les boucles de routage et garder la route la plus fraîche. Cependant, l'exécution du processus de création de route occasionne des délais importants avant la transmission de données [1].

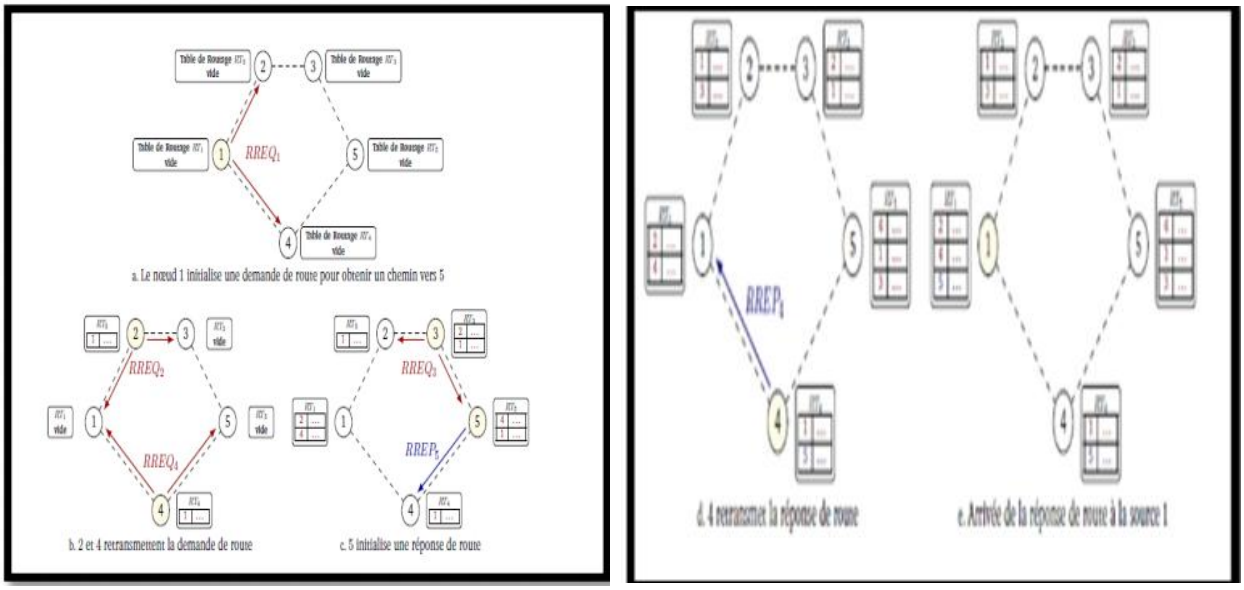


Figure. 1.16 (a,b,c,d,e): Exemple d'établissement de route entre 1 et 5.

I.5.5.3 Gestion des numéros de séquence

Il n'y a pas de numéro de séquence unique pour le réseau car il serait impossible de déterminer en permanence sa valeur de manière distribuée. Chaque nœud possède donc son propre numéro de séquence permettant de dater les informations provenant de lui seul. Un numéro de séquence est incrémenté dans les cas suivants: [1]

- *avant de commencer une découverte de route, un nœud incrémente son numéro de séquence.*
- *avant d'envoyer une réponse RREP, le nœud met à jour son numéro de séquence en utilisant le plus grand entre le numéro de séquence actuel et de celui indiqué comme numéro de séquence destination dans la requête RREQ reçue.*
- *En cas de rupture d'un lien, pour chaque route passant par le lien, le numéro de séquence associé à la destination de la route est incrémenté avant d'envoyer la réponse RREP informant de la rupture du lien.*

I.5.6 ÉVALUATION

Comme tout protocole réactif, AODV souffre d'un délai lors de l'envoi des premiers paquets vers une destination non connue. L'utilisation des numéros de séquence crée aussi une certaine complexité, mais a l'avantage de permettre de fortement limiter les retransmissions inutiles. Ajouté au fait que l'approche réactive du protocole ne pèse que peu sur la charge du réseau, il en résulte qu'AODV n'a que peu d'impact sur celle-ci. Les messages HELLO périodiques restent cependant nécessaires. Une différence majeure d'AODV par rapport à DSR est le fait qu'un nœud intermédiaire sur une route peut modifier la route d'une source à une destination. C'est notamment le cas si un lien est rompu et que le nœud intermédiaire parvient à trouver une route alternative ou si une meilleure route devient disponible entre le nœud intermédiaire et la destination. On peut parler de réparation locale du lien et d'optimisation locale de la route car ces informations n'ont pas à être remontées jusqu'à la source. Cette différence fait qu'AODV est plus adapté que DSR dans le cas d'une importante mobilité des nœuds, cela permet notamment à chaque source de choisir une route en fonction de critères qui lui sont propres, comme une métrique particulière ou encore le choix d'éviter certains nœuds ou liens. Le routage par la source de DSR reste néanmoins intéressant de par le fait qu'il permet à la source de contrôler exactement quelle route est utilisée [1].

I.5.7 LIMITATION DU PROTOCOLE AODV

Dans le protocole AODV, les routes sont établies en fonction du « nombre minimal des sauts » (le plus court chemin), cependant, si le nombre des communications augmente le principe du plus court chemin n'est plus le critère optimal du choix des routes, il est préférable alors d'utiliser d'autres métriques qui ont un effet significatif sur la connectivité et la durée de vie du réseau [1].

I.6 CONCLUSION

Dans ce chapitre nous avons présentés les réseaux ad hoc ainsi le routage et la classification du routage dans les réseaux ad hoc.

Finalement on a présenté le fonctionnement et le comportement de chacun des protocoles AODV et OLSR dans les réseaux ad hoc.

AODV est un protocole de routage à la demande, il est utilisé principalement pour les réseaux sans fil. Ce protocole est le plus populaire des protocoles réactifs, son fonctionnement est basé sur la découverte de route et la maintenance de ces routes en utilisant des paquets de contrôle.

CHAPITRE 2

II.1 Présentation du simulateur OPNET

OPNET Modeler (Optimized Network Engineering Tool) d'OPNET Technologies INC. est un outil de développement permettant la conception et l'étude des réseaux numériques, et des protocoles de communication avec une grande flexibilité. Son approche est orienté objet et il possède une interface graphique simple dans laquelle on place les différents composants du réseau à étudier. Il comprend plusieurs protocoles, technologies et applications incluant WLAN (IEEE 802.11). Nous avons utilisé la version 17.5 dans notre simulation [19][20].

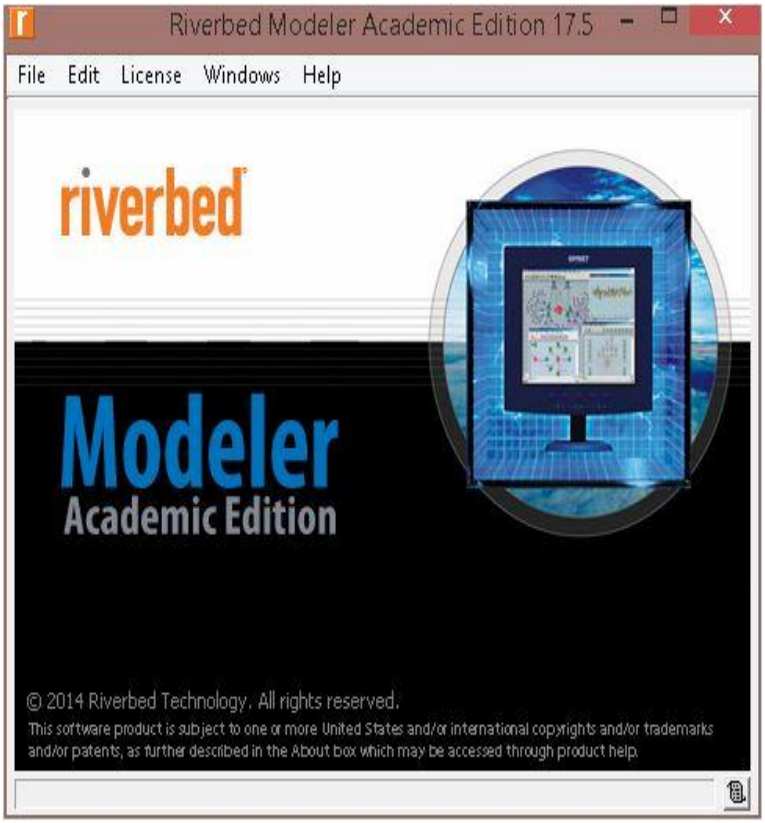


Figure (2.1) ***:*** *la fenêtre principale du simulateur OPNET.*

II.2 PRINCIPALES INTERFACES

Parmi les nombreuses interfaces que propose OPNET au démarrage, on distingue les interfaces suivantes [20] :

- *Project Editor*
- *Network Model Editor*
- *Node Model Editor*
- *Process Model Editor*

II.2.1 Project Editor

C'est l'interface principale du logiciel. Elle permet d'implanter des modèles issus des bibliothèques OPNET ainsi que des modèles créés par l'utilisateur. C'est aussi à partir du Project Editor que les simulations peuvent être configurées puis lancées et que les résultats issus de ces simulations peuvent être affichés. Les principales fonctions de cette interface sont disponibles sous formes d'icônes [20].

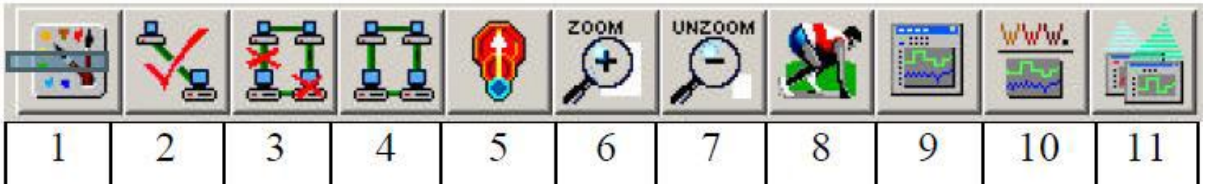


Figure (2.2) : project editor.

1 ➔Ouvrir la palette d'objet
2 ➔Vérification des liens
3 ➔Mise en panne d'un appareil ou d'un lien
4 ➔Remise en marche d'un appareil ou d'un lien
5 ➔Retour au réseau supérieur
6 / 7 ➔ Zoom + / -
8 ➔ Lancer la simulation
9 ➔ Visualiser les graphiques et statistiques collectés
10 ➔ Visualiser le rapport le plus récent
11 ➔Visualiser tous les graphiques

II.2.2/Network Model Editor

Permet de représenter la topologie d'un réseau de communication constitué de nœuds et de liens par l'intermédiaire de boîtes de dialogues (palettes et glisser/poser). Cette interface tient compte du contexte géographique (caractéristique physique pour la modélisation [20].

II.2.3 Node Model Editor

Affiche une représentation modulaire d'un élément de la bibliothèque on d'un élément créé par l'utilisateur. Chaque module envoie et reçoit des paquets vers d'autres modules. Les modules représentent des applications, des couches protocolaires ou des ressources physiques [20].

II.2.4 Process Model Editor

C'est l'interface donne une représentation d'un module par des machines à états finis, chaque état est liés à un autre état par des transitions conditionnelles ou non conditionnelles [20].

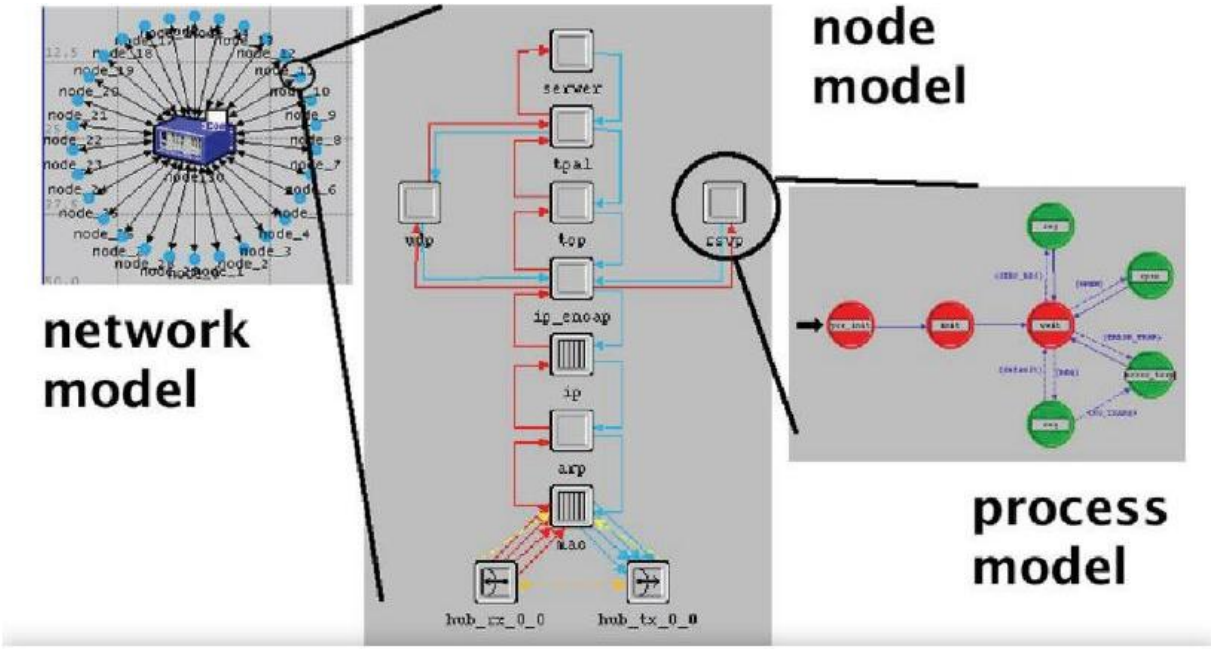


Figure (2.3): OPNET Graphic Editors for Network, Node, and Process Models.

II.3 Modélisation et simulation avec OPNET

OPNET Modeler utilise une approche par projet et par scénario pour modéliser les réseaux.

Projet *- un ensemble de scénarios liés au réseau, chacun d'eux explorant un aspect particulier de la conception du réseau [20].*

- *Tous les projets contiennent au moins 1 scénario*

Scénario *- une seule instance d'un réseau*

- *Typiquement, un scénario présente une configuration unique pour le réseau*
- *Le terme "configuration" peut se référer à différents aspects tels que la topologie, les protocoles, les applications, le trafic et les paramètres de simulation [20].*

II.3.1 La simulation sous OPNET :

1. ***Créer un projet***
2. ***Créer un scénario de référence***
   - *Importer ou créer une topologie réseau Importer ou créer du trafic*
   - *Choisir les statistiques à collecter Exécuter la simulation*
   - *Voir les résultats*
3. ***Dupliquer le scénario***
   - *Apporter des modifications*
   - *Ré-exécuter la simulation*
   - *Comparez les résultats obtenus*
4. ***Répéter l'étape 3 si nécessaire***

II.3.2 Etapes à suivre :

- ***New project***

Figure (2.4) : nouveau projet.

- ***Project Editor :*** *permet de construire et d'éditer la topologie d'un modèle de réseau*

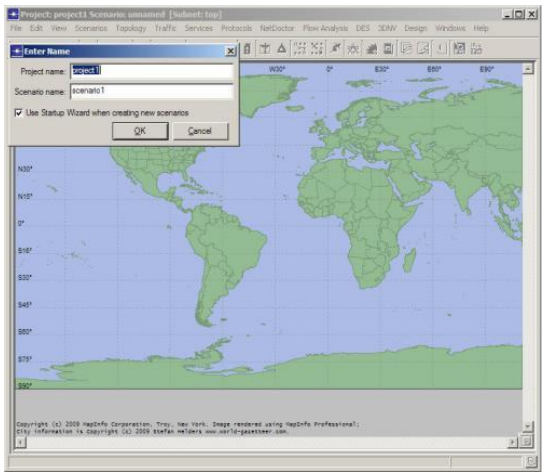


Figure (2.5) : la topologie.

- ***Project Editor window***

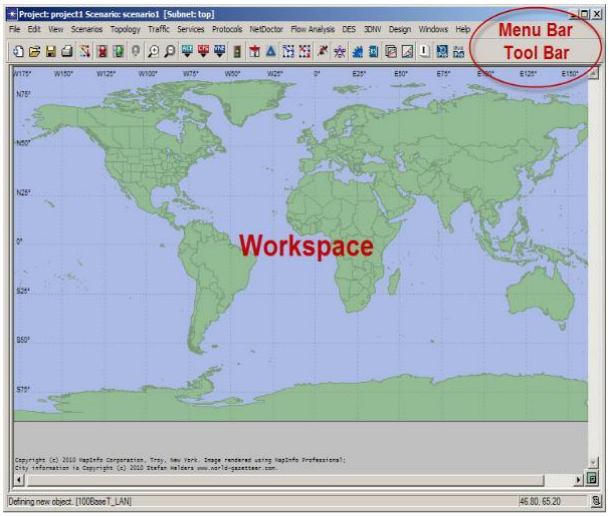


Figure (2.6) : Project editor Window.

- ***Initialisation de la topologie***

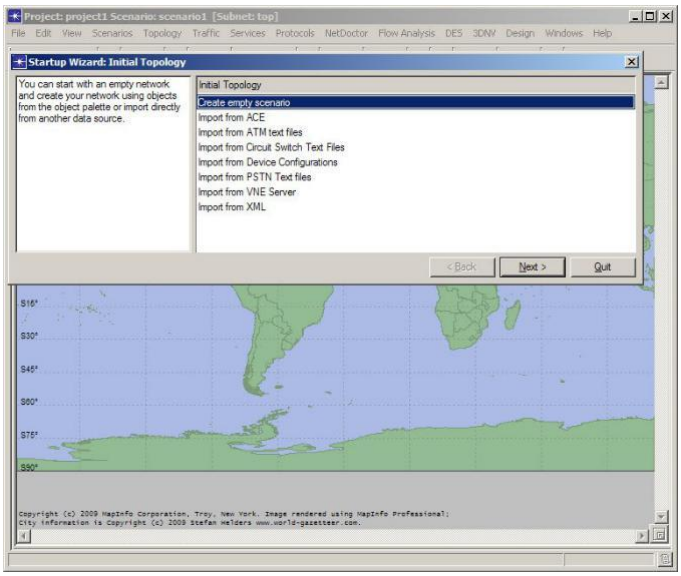


Figure (2.7) : initialisation de topologie.

Il existe plusieurs méthodes pour créer une topologie de réseau :

- *Manuellement, par glisser-déposer d'objets à partir d'une palette d'objets (**ObjectPalette**) à l'espace de travail de l'éditeur de projet*
- *Manuellement, en utilisant la commande Topology➔**Rapid Configuration**... de la barre de menu pour spécifier et construire rapidement une topologie réseau complète.*
- *Automatiquement, en **important** le modèle de réseau à partir d'une source de données externe - soit un système qui surveille votre réseau ou un ou plusieurs fichiers de données qui décrivent le réseau [20].*

L'importation d'une topologie garantit que le modèle de réseau que vous construisez correspond exactement au réseau existant.

- ***Network scale (Echelle du réseau)***

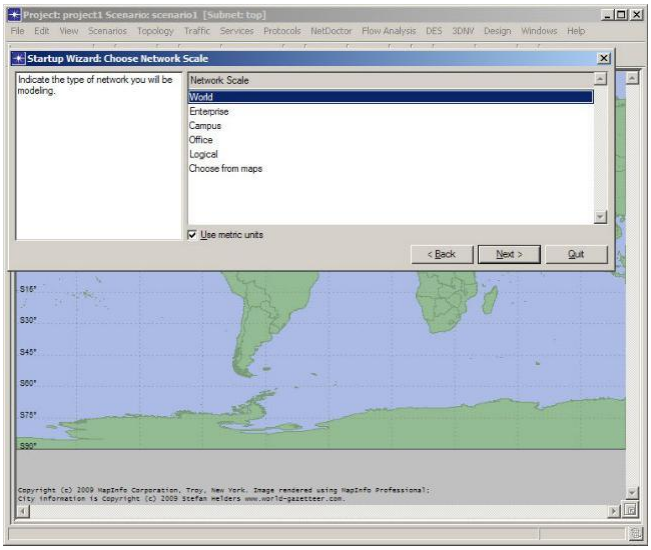


Figure (2.8) : network scale.

- ***Background maps (Cartes de fond)***

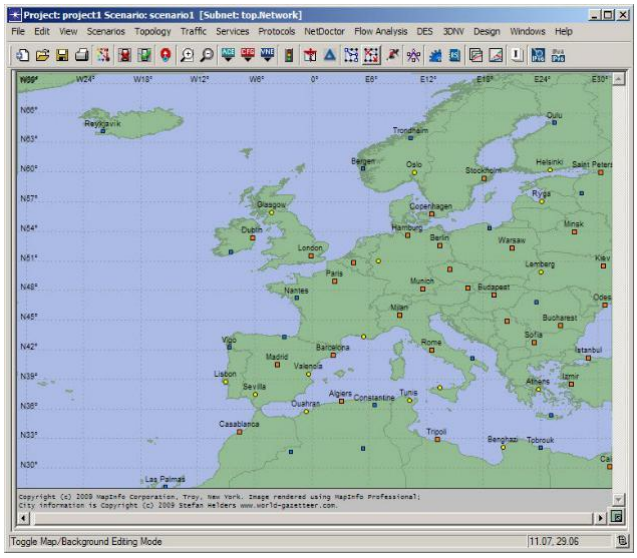


Figure (2.9) : background maps.

- ***Zooming***

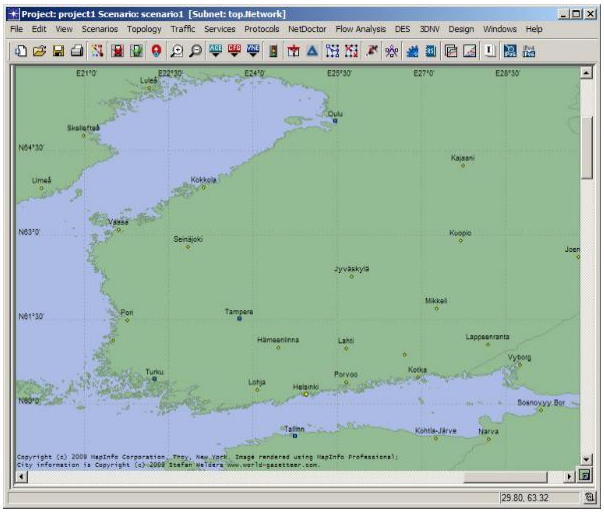


Figure (2.10) : zooming.

- ***Glisser-déposer des objets d'une palette d'objets dans l'espace de travail de l'éditeur de projet***

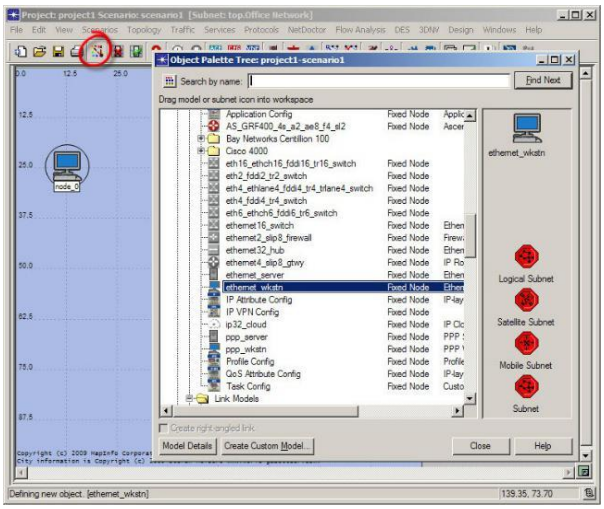


Figure (2.11) : espace de travail /palette d'objet.

- ***En utilisant la commande Topology Rapid Configuration. De la barre de menu pour déployer rapidement des topologies communes de réseau.***

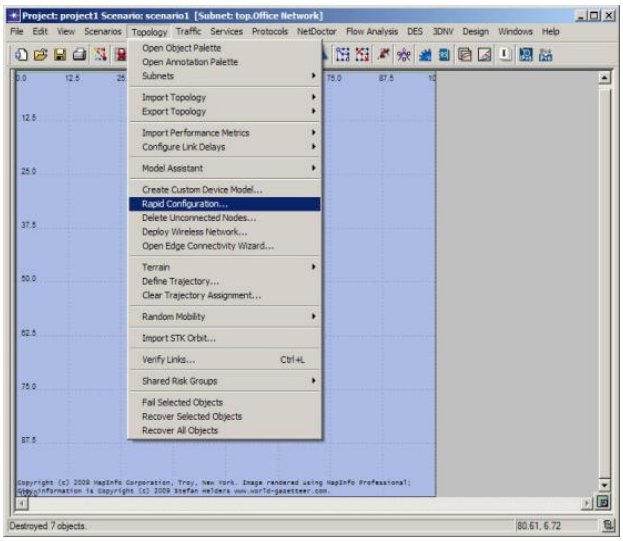


Figure (2.12) : la configuration de topologie.

- ***Configurations disponibles : Bus, maillage (complet ou aléatoire), anneau, étoile, arbre et filet non connecté.***

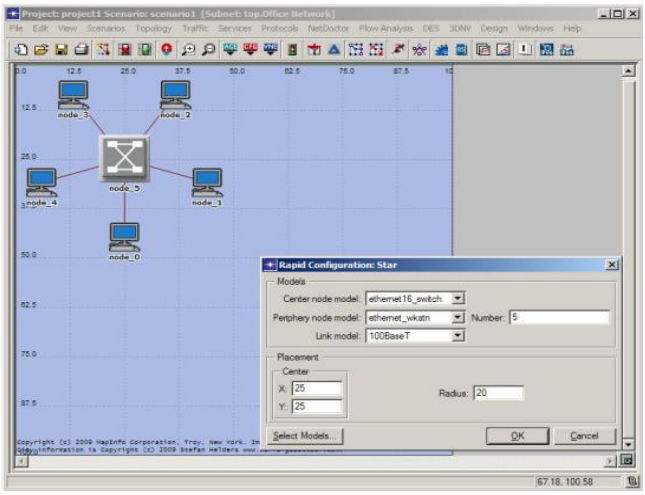


Figure (2.13) : les configurations disponibles.

II.3.3. La librairie du modèle:

OPNET Modeler fournit une bibliothèque étendue de modèles que vous pouvez utiliser pour construire des réseaux.

Ces modèles sont appelés modèles standard parce que les utilisateurs peuvent aussi développer leurs propres modèles.

Ces modèles peuvent ensuite être partagés avec d'autres utilisateurs OPNET si désiré.

Certains modèles répondent aux besoins des utilisateurs qui s'intéressent particulièrement aux technologies émergentes ou propres à un fournisseur (modèles spécialisés).

Une licence supplémentaire est nécessaire pour utiliser ces modèles dans une simulation [20].

La bibliothèque de modèles standard se compose des types d'objets suivants [20] :

- *Sous-réseaux*
- *Nœuds (ou dispositifs)*
- *Liens*
- *LANs et clouds Objets utilitaires*

♦ ***Model Family:*** *internet toolbox*

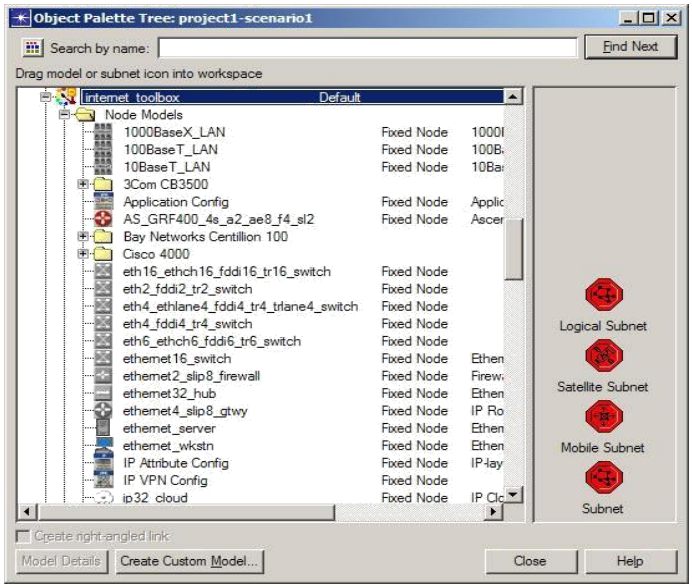


Figure (2.14) : object palette : internet toolbox.

♦ ***Sous-réseaux***

- *Les sous-réseaux sont essentiellement des conteneurs qui rassemblent les composants réseau spécifiés dans un seul objet.*
- *Un réseau partiel peut également contenir d'autres réseaux partiels.*
- *Un réseau partiel spécial appelé réseau partiel de niveau supérieur ou réseau partiel global est le réseau partiel supérieur dans la hiérarchie de réseau.*

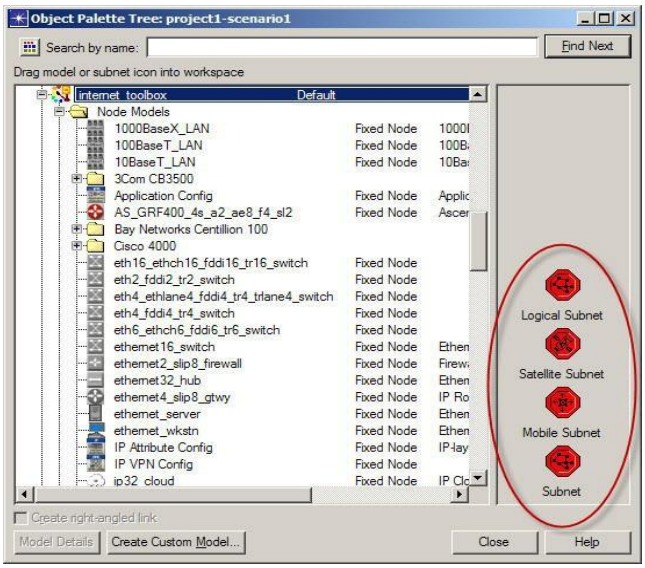


Figure (2.15) : object palette : les sous réseaux.

♦ ***Nœuds***

- *Un nœud représente un périphérique réseau avec un large éventail de capacités possibles (routeur, commutateur, concentrateur, station de travail, serveur, pare-feu, etc.)*
- *La fonction et le comportement réels d'un nœud sont déterminés par son modèle de nœud.*

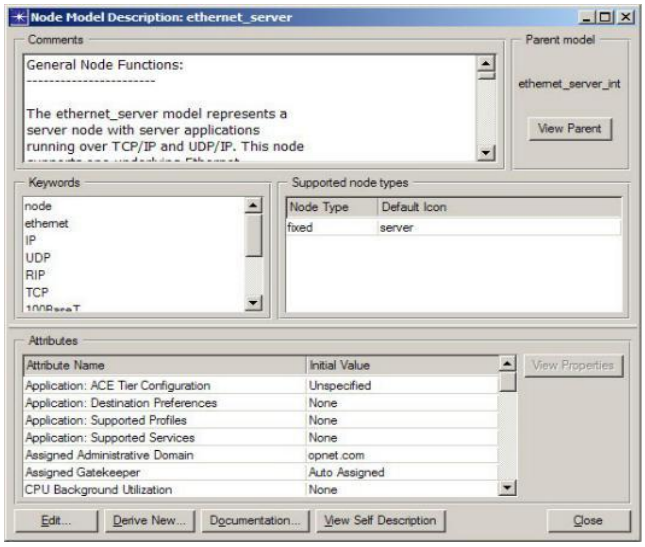


Figure (2.16) : Node Model diagnostic.

♦ ***Liens***

- *Les liens représentent les supports physiques et les propriétés (débit en bits par seconde, délai, probabilité de corruption des données, etc.)*
- *Les liens sont représentés sous forme de segments de ligne ou d'une série de segments de ligne avec des pointes de flèche.*

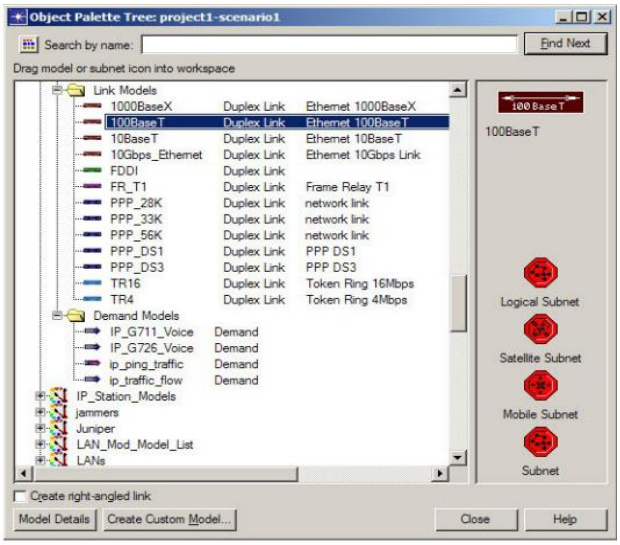


Figure (2.17) : object palette : linkModels.

- ***Réseaux locaux (LAN)***

- *Un objet LAN résume l'infrastructure LAN en un seul objet.*
- *Les objets LAN réduisent considérablement la quantité de configuration nécessaire pour représenter un réseau de LAN et la quantité de mémoire nécessaire pour exécuter la simulation.*

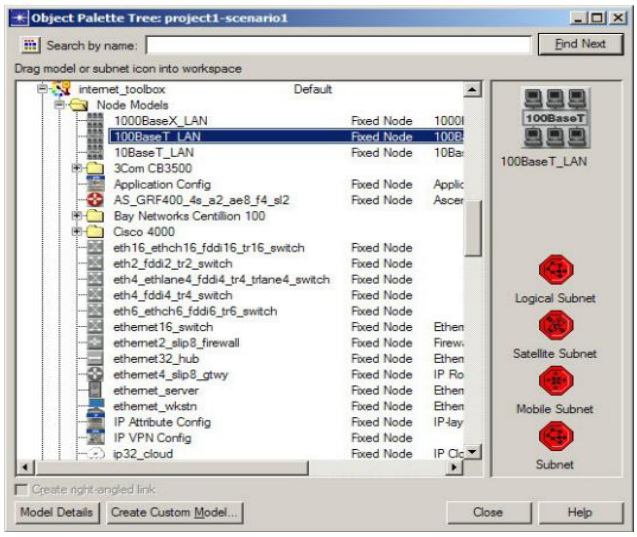


Figure (2.18) : object palette :Node Models (LAN).

- ***Clouds***

- *Un objet nuage (Cloud) résume l'infrastructure WAN en un seul objet.*
- *Les objets nuage fournissent des caractéristiques de haut niveau (latence des paquets et taux de rejet) utilisées pour simuler le comportement des réseaux WAN ATM, Frame Relay, et IP.*

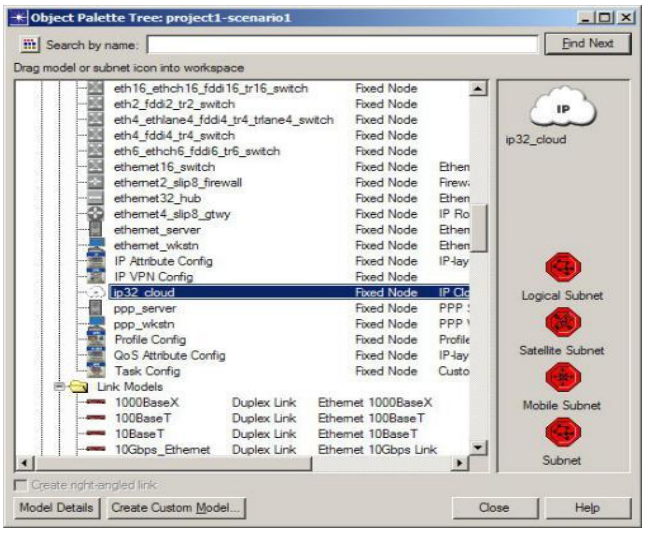


Figure (2.19) : Clouds.

♦ ***Objets utilitaires***

- *Les objets utilitaires ne correspondent pas à l'infrastructure physique réelle.*
- *Au lieu de cela, ils exécutent des fonctions logiques dans le réseau (configuration des ressources réseau, planification des événements spéciaux, etc.)*

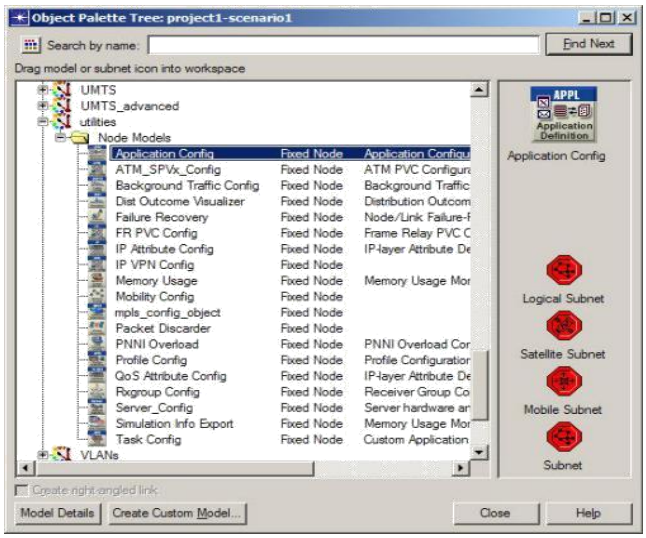


Figure (2.20) : objects utilitaires.

II.3.4 Applications et trafic :

La première étape consiste à glisser-déposer les objets Application Config et Profile Config de la palette des objets dans l'espace de travail de l'éditeur de projet.

- ***Application Config*** *spécifie l'application standard et personnalisées utilisées dans la simulation, y compris les paramètres de trafic et de QoS.*

- *Applications standard (Léger/Lourd) : Base de données, Courriel, FTP, HTTP, Imprimer, Connexion à distance, Vidéoconférence, Voix*

- ***Profil Config*** *spécifie les modèles d'activité d'un utilisateur ou d'un groupe d'utilisateurs en termes d'applications utilisées sur une période donnée.*

  - *Vous pouvez avoir plusieurs profils différents s'exécutant sur un poste de travail donné ou sur un réseau local.*

  - *Ces profils peuvent représenter différents groupes d'utilisateurs et modèles de comportement [20].*

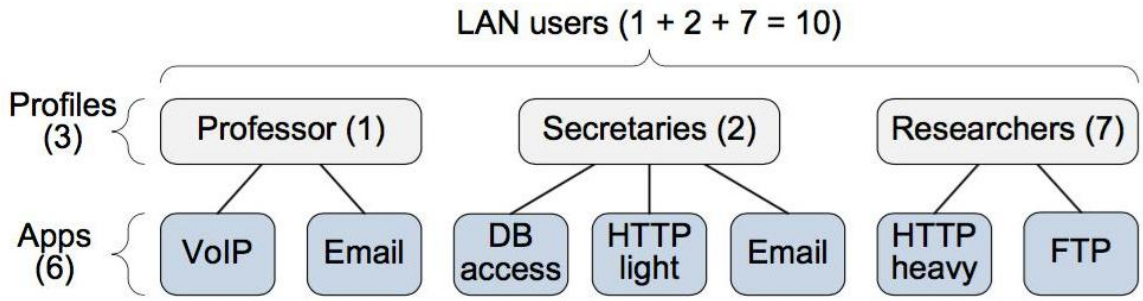


Figure (2.21) : LAN users.

II.3.5 Choisir les statistiques :

- ***Choisissez les statistiques à collecter***

  - *Barre de menu DES Choisissez Statistiques individuelles.....*
    −Ou cliquez avec le bouton droit de la souris dans l'éditeur de projet choisissez Statistiques DES individuelles.
  - *La liste des statistiques apparaît*

  - ***Types de statistiques***
    - ***Globale :*** *recueillie sur l'ensemble du réseau (p. ex., temps de réponse des applications).*
    - ***Nœud :*** *recueilli sur des nœuds individuels (p. ex., retard, variation de retard).*
    - ***Lien :*** *recueilli sur des liens individuels (p. ex., utilisation, débit, délai de file d'attente).*
  - ***Sélectionner résultats*** *Boîte de dialogue [20].*

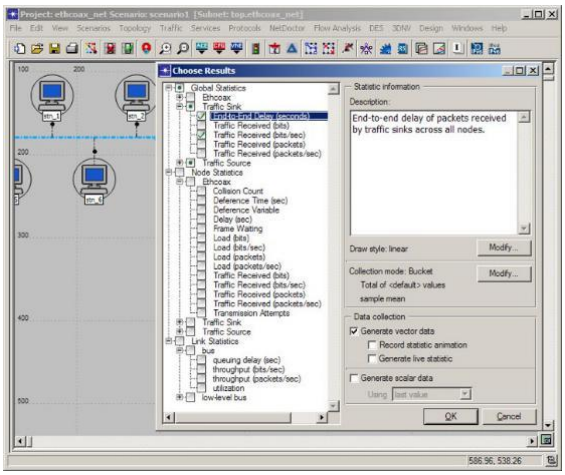


Figure (2.22) : boite de dialogue.

II.3.6 Exécution de la simulation :

Barre de menu DES Configure/RunDiscrete Event Simulation.... Définissez les options de simulation et cliquez sur Exécuter [20].

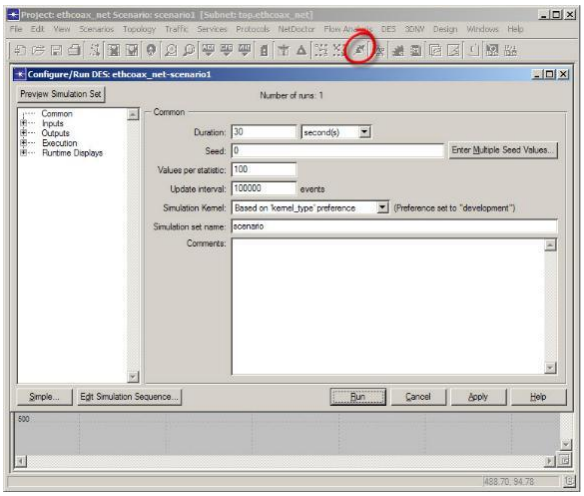


Figure (2.23) : exécuter la simulation

II.3.7 Visualisation des résultats :

Barre de menu DES Résultats Afficher les résultats.....

Ou cliquez avec le bouton droit de la souris dans l'éditeur de projet Voir les résultats [20].

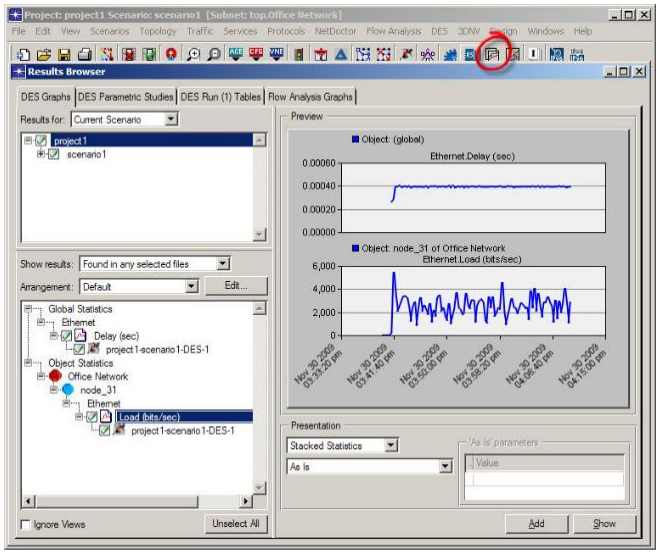


Figure (2.24) : visualiser les résultats

II.4 Conclusion

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

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

CHAPITRE 3

III.1 Simulation :

Les simulations sont effectuées à l'aide du modeleur OPNET 17.5 avec les nœuds répartis sur une zone carrée de 100 m x 100 m, Les simulations sont divisées en scénarios initialement avec 20 nœuds puis en augmentant le nombre de 50 et 100. Les détails sont représentés dans le tableau 1.

III.2 Paramètres de simulation :

Tableau (3.1) : Les paramètres de simulations

Paramètres de simulation	***Valeur***
Nombre de nœuds	*20, 50,100*
Temps de simulation	*10 min*
Zone de simulation	*100m*100m*
Protocoles de routage	*AODV, OLSR*
Modèle de mobilité	*Randomway point*
Nom de l'application	*FTP*
Simulateur	*OPNET Modeler 17.5*

Les performances de la simulation sont analysées en fonction des différents critères des paramètres. Cette quantitative mesure est utiles pour évoluer la performance du réseau en utilisant les deux protocoles AODV et OLSR. Les mesures des performances suivantes sont employées dans cette étude :

Throughput (débit) : *c'est le rapport de la quantité totale de données que e récepteur reçoit à partir d'un expéditeur en un temps donné nécessaire pour que le récepteur obtienne le dernier paquet.*

Delay (retard) : *délai est le temps de génération d'un paquet de la source jusqu'à la destination. C'est donc le temps qu'un paquet pour aller sur le réseau.*

Load (la charge) : *est représentée en bit/s et c'est la charge totale soumise à WLAN couches par toutes les couches supérieurs dans tous les WALN nœuds du réseau.*

RandomWayPoint (RWP) *: Tous les nœuds sont uniformément répartis dans l'espace de mobilité. Les nœuds alternent successivement les temps de pause et de déplacement. Un nœud immobile, durant une certaine période fixée, détermine une destination et une vitesse aléatoire.*

III.3 But de la simulation

Dans cette partie, nous analysons la performance de deux protocoles de routage basé sur les résultats obtenue après simulation de ces protocoles.

Le principal objectif de cette étude est d'évaluer les performances et les comportements de protocoles AODV et OLSR à l'égard de l'effet de variation du nombre ne nœuds de l'application FTP. Les résultats sont basés sur l'évaluation des mesures de délai, la charge, débit et les données supprimées. Nous avons divisé notre études en trois ensembles de scénarios : la première série des études des performance des 2 protocoles sur un petit nombre de nœuds (20 nœuds) suivie par l'augmentation de nombre de nœuds à 50 en deuxième série , 100 nœuds dans le troisième scénario . Tous les trois ensembles montrent les résultats pour FTP.

III.4 Les scénarios :

A) Scénario 1

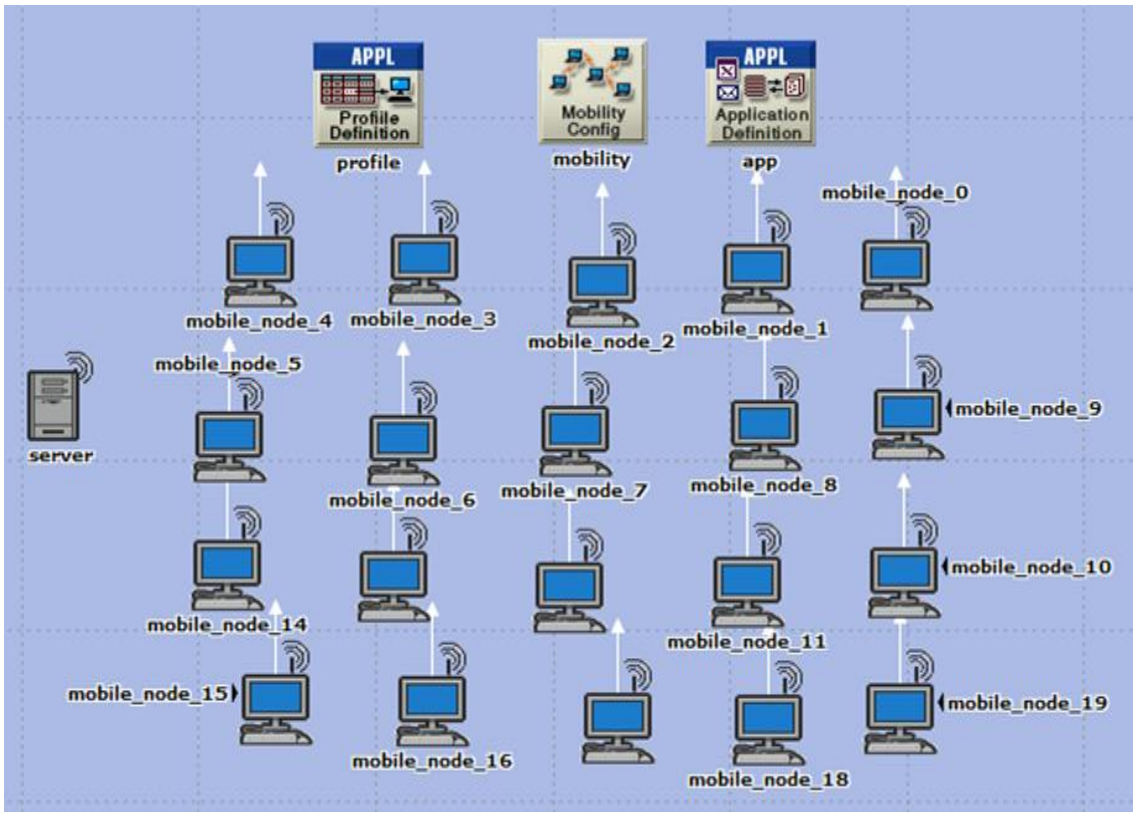


Figure (3.1) : la topologie d'un réseau Ad hoc avec 20 nœuds.

B) Scénario 2

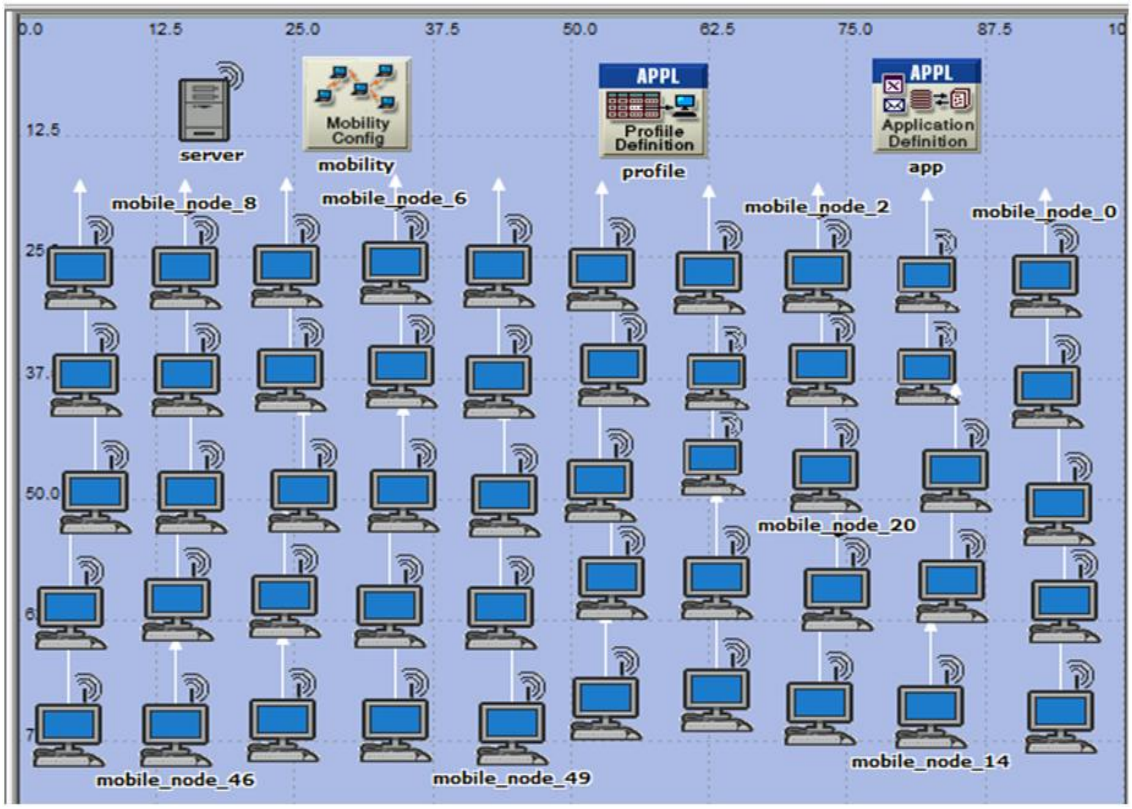


Figure (3.2) : la topologie d'un réseau Ad hoc avec 50 nœuds.

C) Scénario 3

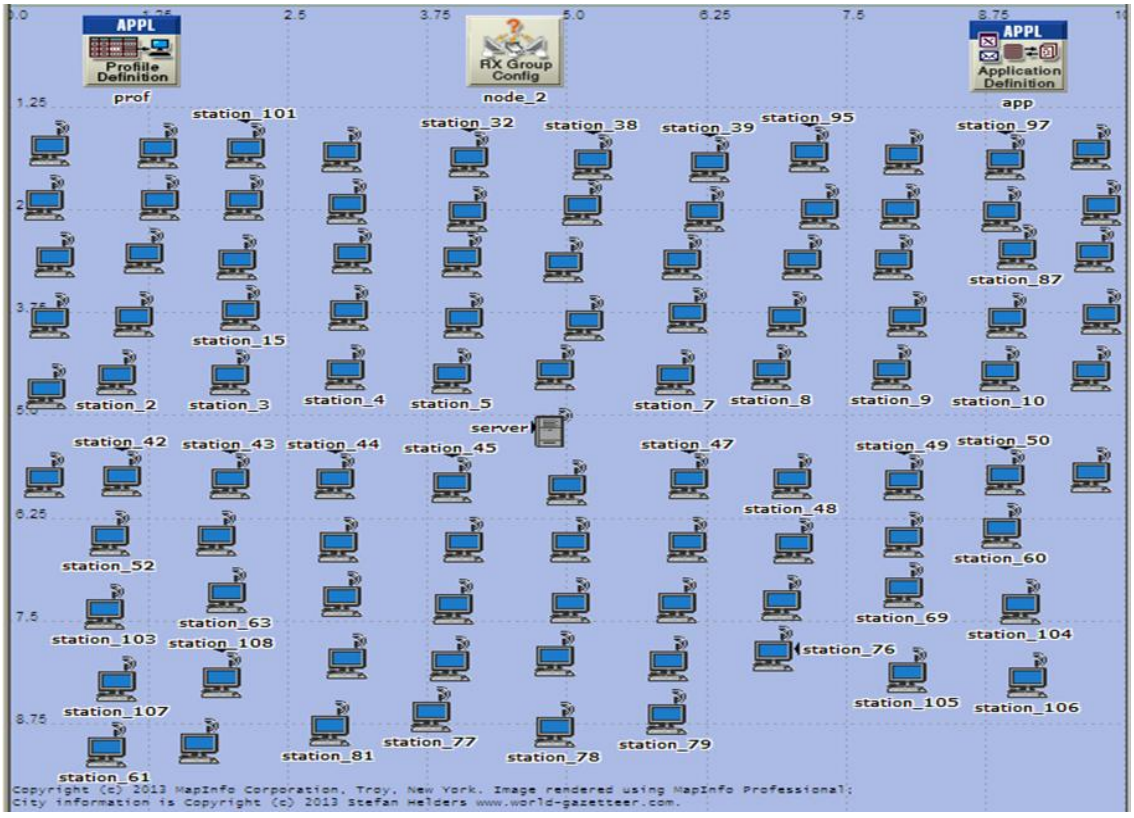


Figure (3.3) : la topologie d'un réseau Ad hoc avec 100 nœuds.

III.5 Les résultats de simulation :

A) Retard (Delay)

*-La Figure **(3.4)** montre la totalité de la période de retard de 20 nœuds en utilisant FTP*

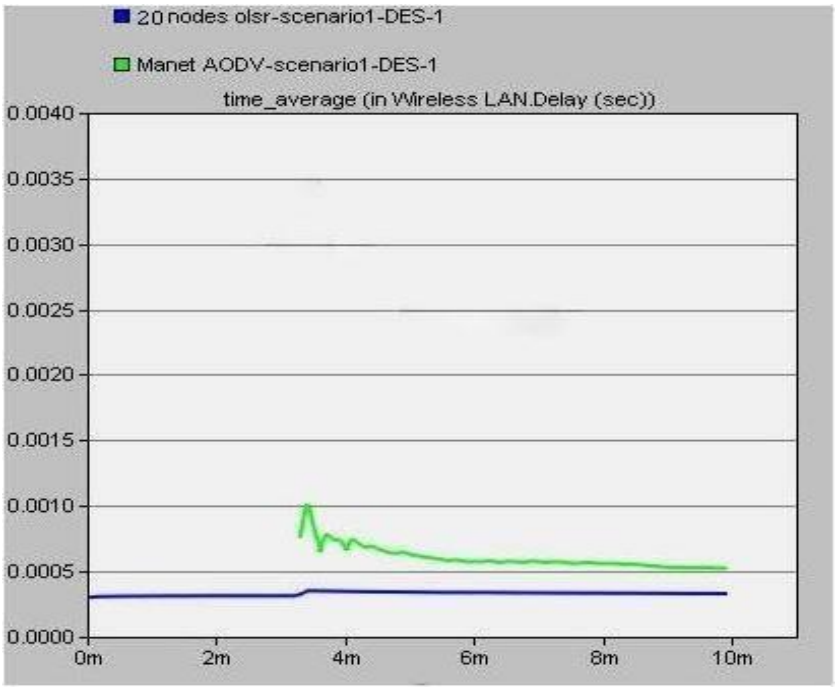


Figure (3.4) : le retard pour 20 nœuds en utilisant FTP.

***Remarque :** Le protocole OLSR enregistre moins de retard. Le protocole AODV enregistre un retard plus élevé allant jusqu'à la fin de simulation.*

-La Figure (3.5) montre le retard pour 50 nœuds en utilisant FTP

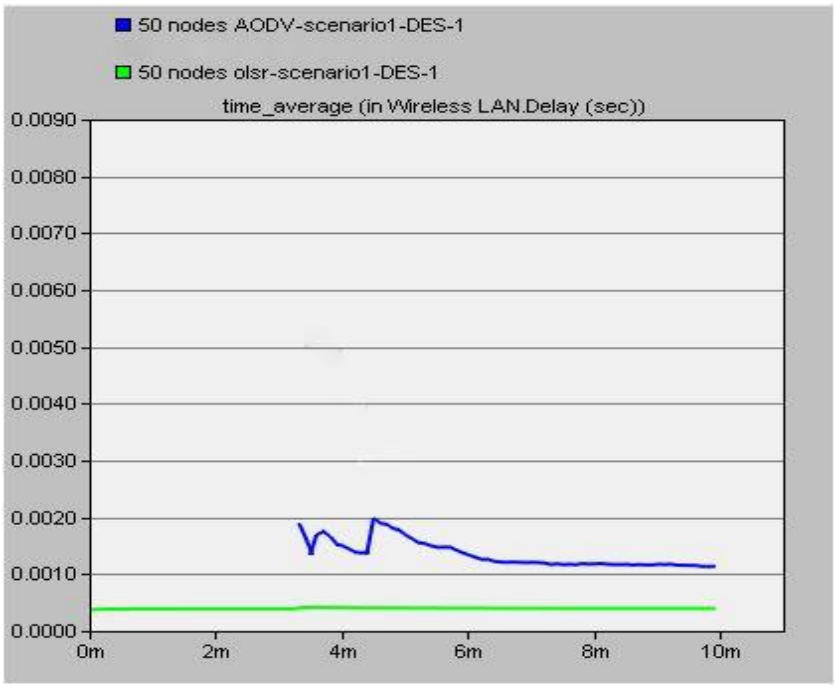


Figure (3.5) : le retard pour 50 nœuds en utilisant FTP.

***Remarque :** on remarque que le protocole OLSR diminue un peu mais reste constant, pour AODV c'est inchangé comme indiqué en figure précédente.*

-La Figure (3.6) montre le retard pour 100 nœuds en utilisant FTP

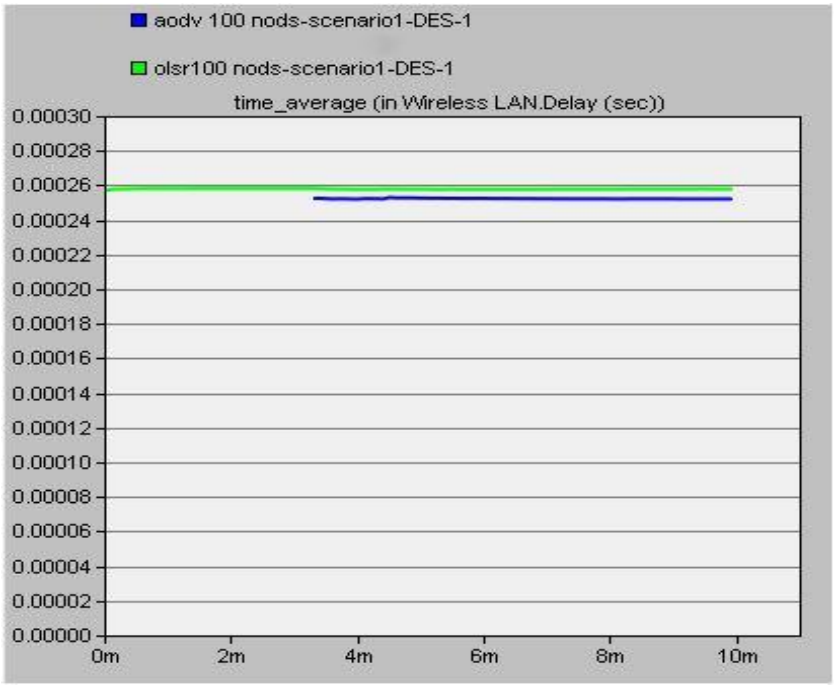


Figure (3.6) : le retard pour 100 nœuds en utilisant FTP.

B) Charge (Load)

-La Figure (3.7) montre la charge pour 20 nœuds en utilisant FTP

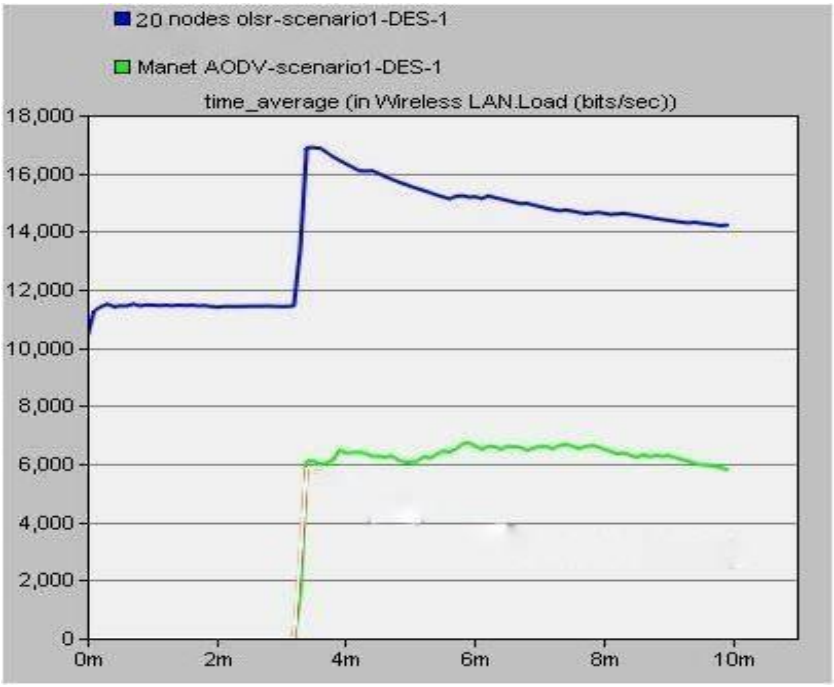


Figure (3.7) : la charge pour 20 nœuds en utilisant FTP.

Remarque : *la figure montre l'augmentation pour AODV pour la charge à partir de 3.4m jusqu'à 6 bits/s, ce dernier reste constant à 6 bits/s jusqu'à la fin de simulation. En revanche l'OSLR commence par la valeur 10.4 bits/s et reste constant jusqu'à 3.4 m, après il augmente à 17.2bits/s.*

A partir de 4 m, l'OLSR commence la diminution jusqu'à la fin de simulation.

Le protocole AODV représente moins de charge par rapport à OLSR.

-La Figure (3.8) montre la charge pour 50 nœuds en utilisant FTP.

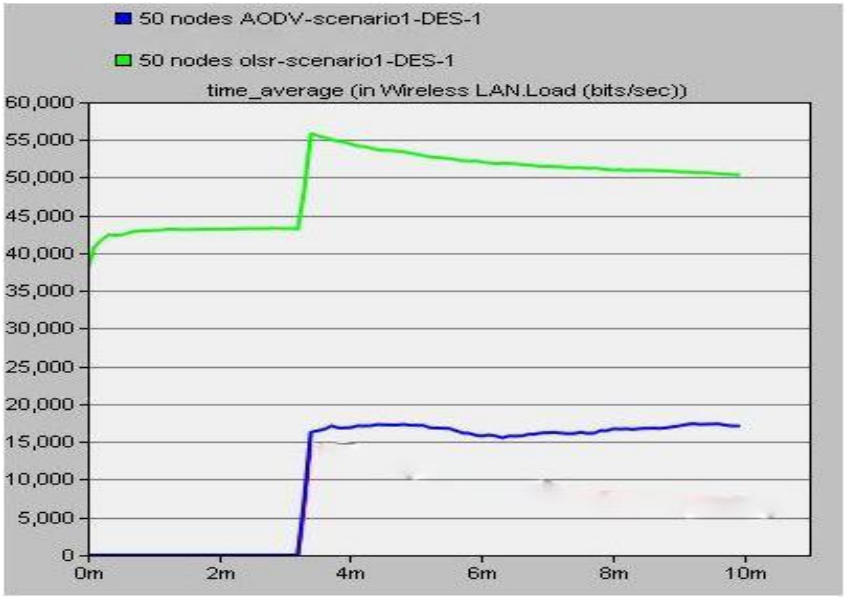


Figure (3.8) : la charge pour 50 nœuds en utilisant FTP.

Remarque : *on remarque presque la même figure précédente sauf que la charge augmente par exemple, OLSR commence par la valeur 40 bits/s et l'AODV commence à peu près à 15 bits/s.*

-La Figure (3.9) montre la charge pour 100 nœuds en utilisant FTP

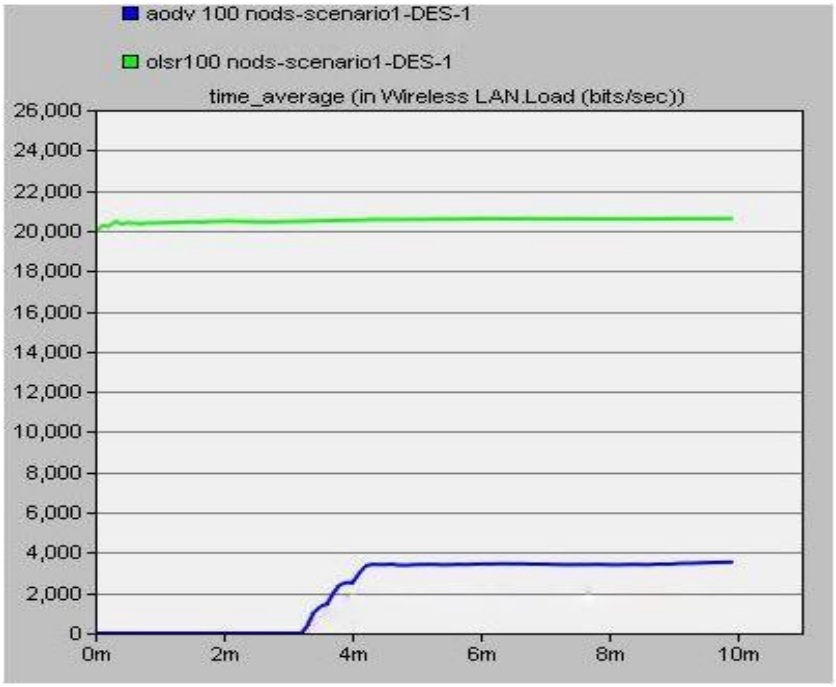


Figure (3.9) : la charge pour 100 nœuds en utilisant FTP.

Remarque : *le protocole OLSR constant à 20.1bits/s jusqu'à la fin de simulation; mais AODV et commence à 3.1 m et augmentent jusqu'à 4 bits/s pour AODV. Et à 4.2 m ce dernier reste constant jusqu'à la fin de la simulation.*

Explication :

OLSR est un protocole d'état de lien qui utilise une technique optimisée pour la diffusion des messages topologiques. Donc il produit plus de communication et prend plus de temps de maintenance qui ajoute à la charge totale de réseau.

D'autre part, AODV limite la communication pour augmenter l'utilisation de bande passante. C'est pour ça la charge est élevée dans les résultats, l'augmentation de nombre des nœuds faire une réduire de la charge des deux protocoles.

C) Débit (Throughput)

-La Figure (3.10) montre le débit e pour 20 nœuds en utilisant FTP

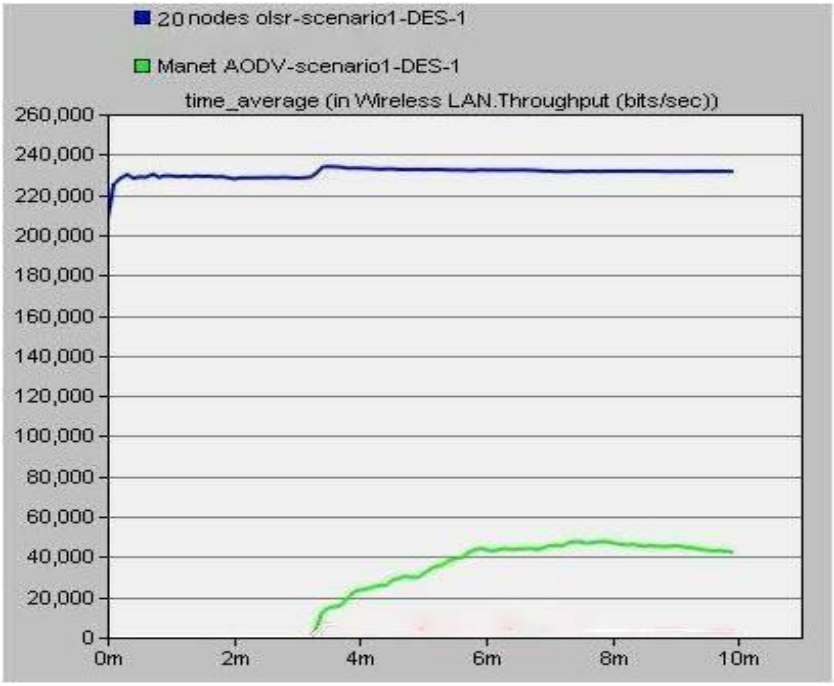


Figure (3.10) : le débit pour 20 nœuds en utilisant FTP.

Remarque : *Le protocole OLSR montre un haut débit par rapport au protocole AODV.*

-La Figure (3.11) montre le débit e pour 50 nœuds en utilisant FTP.

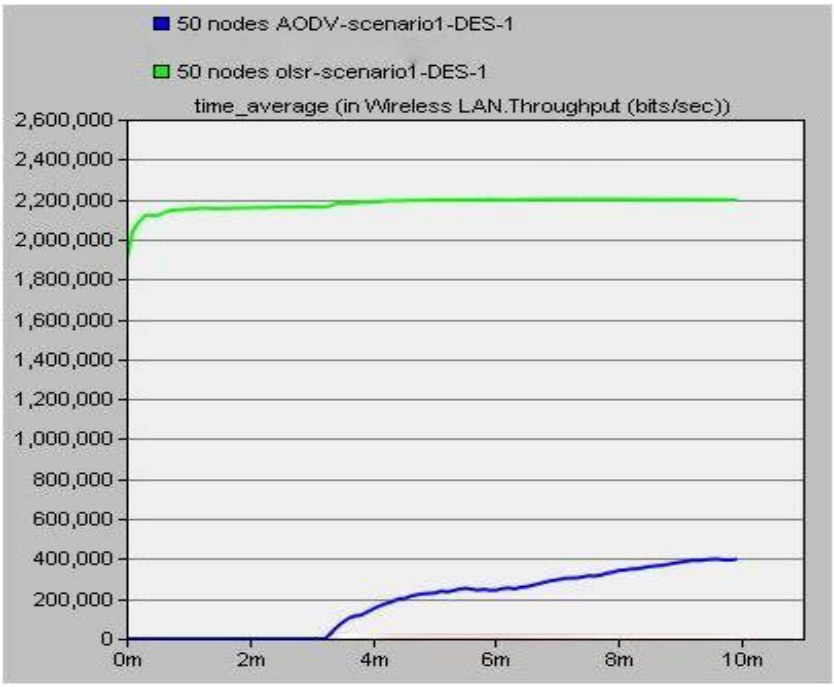


Figure (3.11) : le débit pour 50 nœuds en utilisant FTP.

Remarque :

- *Le protocole AODV montre un faible débit, la valeur la plus élevée d'exposition de protocole OLSR du débit qui est1.890.000. Bit/sec à la fin de simulation.*
- *Le protocole AODV a une diminution par rapport à l'OLSR.*

-La Figure (3.12) montre le débit e pour 100 nœuds en utilisant FTP.

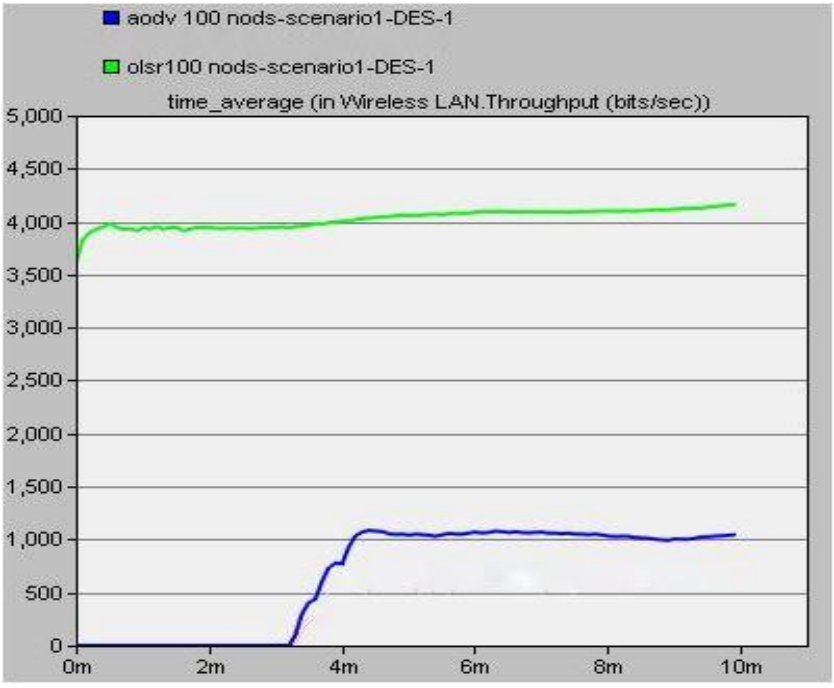


Figure (3.12) : le débit pour 100 nœuds en utilisant FTP.

Remarque : *La Figure montre les mêmes résultats, le protocole OLSR prend un débit élevé et le protocole AODV a un faible débit.*

Explication :

OLSR a le débit max dans chaque scénario. AODV représente le pire des cas. Une des raisons pour le débit inférieur par AODV est qu'il efface ses routes quand elles ne sont pas dans l'utilisation.

OLSR a un débit mieux qu'AODV. C'est en raison de proactive nature d'OLSR. Il réduit le contrôle du MPRs à propager les mises à jour d'états des liens, mais quand le nombre des hôtes mobiles augmentent, alors l'aérien de contrôle des messages augmentent aussi.

III.6 Conclusion :

- ✓ *Dans cette étude de simulation, un essai est fait pour évaluer la performance de deux protocoles de routage tels qu'AODV et OLSR et un effort est également senti pour comparer les résultats de ces protocoles en utilisant MANET.*
- ✓ *Dans le délai d'évaluation des performances, la charge et le débit sont adoptés pour l'ensemble des scénarios envisagés.*
- ✓ *La simulation à l'aide d'OPNET envisage différents scénarios qui tentent de couvrir tous les aspects nécessaires à l'évaluation du réseau.*
- ✓ *Les résultats expérimentaux ont démontré que le retard en utilisant le protocole AODV est le plus élevé et par OLSR, il est le plus bas.*
- ✓ *Dans le cas de débit, l'OLSR a relativement un bon débit.*
- ✓ *De l'autre côté de la charge l'OLSR fonctionne relativement mieux par rapport au protocole AODV.*
- ✓ *On a conclu parmi les résultats globaux que le protocole de routage proactif OLSR fait mieux que le protocole de routage réactifs AODV.*
- ✓ *L'une des principales raisons de la bonne performance de OLSR car :*
  - *OLSR a une forte probabilité que le protocole n'obtienne de routes assez rapidement, ainsi que son temps de convergence augmente. Dans le cas où le nombre de nœuds augmente, il recherche constamment des itinéraires pour toutes les destinations possibles dans le réseau.*

CONCLUSION GENERALE

Les Réseaux Manet est un sujet très vaste et le centre d'intérêt pour les chercheurs parce que c'est devenue une chose essentielle dans notre vie surtout avec la révolution technologique ou on cherche à optimisée les choses pour la vie réelle des humains.

Au cours de ce mémoire, notre objectif était d'étudier le comportement des

Deux protocoles de routages, AODV et OLSR dans les réseaux Ad hoc, après avoir décrit les types de ces derniers et la différence entre eux, ainsi leur caractéristiques (topologie dynamique, bande passante limitée, contraintes d'énergie, etc...)

Avec certaines de ses domaines d'applications : des applications militaires, ils peuvent être déployés à bon escient dans des situations d'urgence telles que les missions de secourisme en cas d'incendies ou de catastrophes naturelles (inondations, tremblements de terre, etc.). En outre, ils peuvent être utilisés dans tout groupement d'usagers liés par un intérêt commun, c'est le cas notamment des étudiants dans une classe, des chercheurs dans une conférence, etc. On a aussi présenté les classes des protocoles de routage existants, de plus on a cité quelques protocoles associes a chacune d'elles.

Par la suite, on a parlé sur le simulateur OPNET avec ses principales interfaces.

Dans cette étude nous avons montré les avantages, les inconvénients et les performances de chaque protocole.

D'après les résultats de simulation, on a pu déterminer et conclure que le protocole OLSR est plus performant qu'AODV et que l'OLSR fonctionne le mieux dans l'application requise.

Références

[1]*Hemaizia Zineb, Aissaoui Bouthaina." Un protocole de routage optimisé dans les réseaux Ad Hoc" Mai 2016.*

[2]*Fatima AMEZA."Les technologies sans fil: Le routage dans les réseaux ad hoc (OLSR et AODV)", Licence 2007.*

[3]*Nadjette & Hanane MOUICI & BOUKHALFA. "L'impact des attaques sur la fiabilité des réseaux ad hoc", Master 2-2015.*

[4]*Melle. Saloua CHETTIBI ; "Protocole de routage avec prise en compte de la consommation d'énergie pour les réseaux mobile Ad Hoc". Université Mentouri Constantine, 2008.*

[5] *Nadhir BOUKHECHEM, « Routage dans les réseaux mobiles Ad Hoc par une approche à base d'agents ». Promotion 2007-2008.*

[6]*Ameza Fatima, Assam Nassima, Atmani Mouloud, Le routage dans les réseaux Ad Hoc (OLSR et AODV), Licence en informatique, Université Abderrahmane Mira BÉJAÏA, 2007.*

[7]*Mohamed Ali AYACHI, Contributions à la détection des comportements malhonnêtes dans les réseaux Ad Hoc AODV par analyse de la confiance implicite, Thèse de doctorat : Université de Rennes 1, 24/02/2011.*

[8]*Ahizoune Ahmed, Un protocole de diffusion des messages dans les réseaux véhiculaires, Thèse de Maîtrise ès sciences (M. Sc.) de l'Université de Montréal, Avril 2011.*

[9]*Nadir BOUCHAMA, Qualité de Service dans les Réseaux Mobiles Ad Hoc, Centre de Recherche sur l'Information Scientifique & Technique, Division Théorie & Ingénierie des Systèmes Informatiques (DTISI), 08/06/2010.*

[10]*Nabila LABRAOUI, La sécurité dans les réseaux sans Fil Ad Hoc, Thèse de DOCTORAT, Université de Tlemcen, 2012.*

[11]*M elle BESSAIH Aldja M me BOUCHAKEL Siham."Routage et simulation dans les réseaux mobiles ad hoc", 2017, Université A/Mira de Béjaia.*

[12]*Ait Ali Kahina, Modélisation Et Etude De Performances Dans Les Réseaux VANET. Thèse de doctorat de l'Université de Technologie de Belfort-Montbéliard, 16 /10/ 2012.*

[13]*R. Meraihi ; "Gestion de la qualité de service et contrôle de topologie dans les réseaux ad hoc" ; Thèse de doctorat, École nationale supérieure des télécommunications, Paris, 2004.*

[14]*Khadidja AYAD, Sécurité du routage dans les réseaux Ad Hoc mobile, Thème de MAGISTER Option : Informatique Répartie et Mobile, 14 /11/ 2012.*

[15]*Amadou Adama Ba. , Protocole de routage basé sur des passerelles mobiles pour un accès Internet dans les réseaux véhiculaires, Thèse de doctorat, l'université de Montréal, Avril 2011.*

[16]*Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, A Survey on Attacks and Countermeasures inMobile Ad Hoc Networks, 2006 Springer.*

[17]*T. Clausen and P. Jacquet. Optimized Link State Routing Protocol OLSR. http://tools.ietf.org/html/rfc3626, October 2003. RFC3626.*

[18]*Abderrezak Rachedi, Contributions à la sécurité dans les réseaux mobiles Ad Hoc. Spécialité : Networking and Internet Architecture, Université d'Avignon France, 2012.*

[19] *SIDI YKHLEF asma et KEBIR khadidja "Modélisation et simulation d'un réseau en utilisant opnet modeler" memoire licence 2014-2015.*

[20] *Mme BOULMAIZ « Introduction et familiarisation avec Le logiciel OPNET » Master 2 Réseaux et Télécommunications / Systèmes de Télécommunications, 2020, Université BADJI MOKHTAR ANNABA.*