République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Faculté des Sciences Exactes et Sciences de la Nature et de la Vie

Université de Tébessa

Département des mathématiques et informatique

MEMOIRE DE MASTER
Domaine: Informatique
Filière : Informatique
Option : Réseaux et sécurité informatique

Thème :

Une version optimisée de protocole de routage AODV dans les réseaux Ad Hoc

Réalisé par :

GUERRAD Abdelghani SELATNIA Zoubir

Devant le jury:

Président : M. TAG Samir	Université de Tébessa
Encadreur : M. MAHMOUDI Rachid	Université de Tébessa
Examinateur : M. AOUINE Mohamed	Université de Tébessa

Date de soutenance :

Note : Mention :

Promotion : 2016 – 2017

Remerciement

Nous remercions tout d'abord ALLAH tout-puissant de

Nous avoir armés de force et nous guider pour élaborer

Ce modeste travail.

Nous adressons nos remerciements à notre encadreur

M. Mahmoudi Rachid pour l'honneur qu'il nous fait en acceptant de guider

Cette mémoire avec ses conseils et son aide précieuse.

On tient à adresser notre profonde gratitude à toutes les personnes qui nous a

Aidés et encourager.

Nous remercions les membres du jury qui nous font le grand honneur d'évaluer

Notre travail.

Et en fin notre plus profonde et sincères remerciements à nos parents et nos familles qui nous Ont toujours soutenues, encouragé et aidé, ils ont su de nos données toutes les Chances pour réussir.

Résumé

Résumé : Le réseau ad hoc mobile (MANET) est une collection d'appareils mobiles, interconnectés entre eux avec les ondes radio, sont des réseaux sans infrastructure, auto-configuré, multi-saut, chaque périphérique en topologie de réseau servant de routeur. Les protocoles de routage sont nécessaires pour trouver des chemins d'accès pour atteindre un autre nœud. En raison de la mobilité des nœuds, le routage joue un rôle important dans la communication, La performance du protocole de routage dans le réseau ad hoc mobile (MANET) dépend de la valeur des paramètres utilisés. En raison de très grande combinaison de ces valeurs, il est difficile de trouver une combinaison optimale pour une meilleure optimisation dans MANET. Par conséquent, nous avons proposé une méthode comparative basée sur l'optimisation pour trouver une combinaison optimale dans le protocole de routage (AODV),à travers des scénarios réalisés par l'outil de simulation OPNET 14.5. Les résultats expérimentaux montrent une délai plus réduite, un moindre nombre de paquets perdus, une optimisation considérable de temps de découverte de route et un débit élevé (throughput) en utilisant une combinaison optimale de paramètres d'après cette méthode expérimentale comparative par rapport les paramètres de la version originale , nous concluons que des meilleures optimisations sont possibles avec la modification de certains paramètres du protocole, sans modifier l'algorithme (le code source). Les tests expérimentaux de nos valeurs optimaux des paramètres montrent une amélioration considérable du protocole (AODV).

Mot clés : réseaux, Ad Hoc, MANET, AODV, optimisation, simulation.

Abstract

Abstract: The mobile ad hoc network (MANET) is a collection of mobile devices, interconnected with radio waves, and are networks without infrastructure, self-configured, multi-hop, each device in network topology serving as a router. Routing protocols are needed to find paths to reach another node. Due to the mobility of the nodes, routing plays an important role in communication. The performance of the routing protocol in the mobile ad hoc network (MANET) depends on the value of the parameters used. Due to the very large combination of these values, it is difficult to find an optimal combination for better optimization in MANET. Therefore, we proposed a comparative method based on optimization to find an optimal combination in the routing protocol (AODV), through scenarios performed by the OPNET 14.5 simulation tool. The experimental results show a shorter delay, a lower number of lost packets, a considerable optimization of the road discovery time and a high throughput by using an optimal combination of parameters according to this comparative experimental method with respect to the parameters Of the original version, we conclude that optimization is possible with the modification of some parameters of the protocol, without altering the algorithm (the source code). Experimental tests of our optimal parameter values show a considerable improvement of the protocol (AODV).

Key words: networks, ad hoc, MANET, AODV, optimization, simulation.

ملخص

ملخص: الشبكات الديناميكية(MANET)ad hocهي عبارة عن مجموعة من الأجهزة النقالة المرتبطة مع بعضها البعض لاسلكيا بواسطة موجات مغناطيسية، وهي شبكات بدون بنية تحتية ،ذاتية الاعدادات الشبكية، متعددة القفزات، كل جهاز فيها يلعب دور جهاز توجيه، وهناك حاجة إلى بروتوكولات التوجيه للعثور على المسارات للوصول إلى جهاز أخر، وكون الأجهزة المشكلة للشبكة متحركة، فان التوجيه يلعب دور هام في عملية الاتصال، كما أن أداء بروتوكول التوجيه في شبكة (MANET)يعتمد على قيمة المعاملات المستخدمة، وبسبب صعوبة ملاءمة هذه القيم قصد العثور على التركيبة الأمثل من أجل الاستفادة بشكل أفضل في MANET، اقترحنا طريقة المقارنة من أجل إيجاد التركيبة المثلى لهذه القيم في بروتوكول التوجيه AODVعن طريق سيناريوهات منجزة باستعمال أداة المحاكاة OPNET 14.5 ، النتائج التجريبية بينت تحسن في الوقت الخاص بالشبكة ، عدد أقل في عدد الحزم الضائعة ، كذلك تحسن كبير في فترة اكتشاف الطريق المؤدي الى نقطة الوصول ، أيضا نسبة عالية في حجم المعلومات المتبادلة في الشبكة (throughput)، وذلك باستخدام المعاملات المثلى ، من خلال هذه الدراسة التجريبية المعتمدة أساسا على مبدأ المقارنة مع النسخة الأصلية لهذا البروتوكول ، استنتجنا أنه يمكن تحسين في أداء البروتوكول AODV بفضل إيجاد القيم المثلى لبعض المعاملات ، دون اللجوء الى التغيير في الخوارزمية الأصلية، الاختبارات التجريبية للقيم المثلى التي تحصلنا عليها أظهرت تحسننا معتبرا في البروتوكول AODV .

الكلمات المفتاحية :الشبكات(réseaux)، الشبكة المتحركة المخصصة (ad hoc)، مانيت MANET، أ ؤ د ف AODV،التحسينoptimisation، المحاكاةsimulation.

Liste des figures

Chapitre 01 : Généralité Sur Les Réseaux sans fils et les réseaux Ad Hoc

Chapitre 02 : Le routage dans les réseaux Ad Hoc

Chapitre 03 : Présentation de Protocole AODV

Chapitre 04 : Simulation et Simulateurs réseau

Chapitre 05 : Optimisation De Protocole De Routage AODV Basée sur la modification des paramètres

Chapitre 06 : Tests et résultats

Liste des tableaux

Chapitre 02 : Le routage dans les réseaux Ad Hoc

Chapitre 03 : Présentation de Protocole AODV

Chapitre 04 : Simulation et Simulateurs réseau

Chapitre 05 : Optimisation De Protocole De Routage AODV Basée sur la modification des paramètres

Chapitre 06 : Tests et résultats

Acronyme	Description
AODV	Ad Hoc On Demand Distance Vector
DSDV	Dynamic Destination-Sequenced Distance-Vector
DSR	Dynamic Source Routing
IARP	Intrazone Routing Protocol
IERP	Interzone Routing Protocol
MANET	Mobile Ad hoc NETWORK
OPNET	Optimized Network Engineering Tools.
RREQ	Route Request
RREP	Route Reply
RERR	Route Error
RREP-ACK	Reply_Acknowledgment
TTL	Time-To-Live.
WLAN	Wireless Local Area Networks
WMAN	Wireless Metropolitan Area Networks
WWAN	Wireless Wide Area Networks
WiFi	Wireless Fidelity.
VANET	Vehicular Ad-hoc NETwork
ZRP	Zone Routing Protocol

Table des matières

Chapitre 02 : Le routage dans les réseaux Ad Hoc

Chapitre 03 : Présentation de Protocole AODV

Chapitre 04 : Simulation et Simulateurs réseau

Introduction générale

Dans la terminologie informatique, Un réseau informatique est un ensemble de machines interconnectées qui permet l'échange ’informations et le partage des ressources, ce réseau est divisé en deux grandes catégories selon le moyen de connexion entre les machines : les réseaux filières et les réseaux sans fil, dans ces derniers réseaux, les terminaux sont interconnectes sans aucun moyen physique mais par les ondes radio.

Un environnement sans fil est un système composé de sites mobiles et qui permet à ses utilisateurs d’accéder à l’information indépendamment de leurs positions géographiques.

Nous pouvons distinguer deux classes de réseaux mobiles, les réseaux mobiles avec infrastructure qui utilisent généralement le modèle de la communication cellulaire, et les réseaux mobiles sans infrastructure ou les réseaux Ad Hoc, Un réseau mobile ad hoc appelé généralement MANET (*Mobile Ad hoc NETWORK*).

Les réseaux ad hoc représentent une nouvelle porte dans l'avenir des télécommunications, permettant d'interconnecter les périphériques sans fil, formant ainsi des réseaux de communication sans infrastructure, où chaque nouveau nœud fonctionne à la fois client et routeur, ce qui étend la portée du réseau. Sur la première considération, ce concept peut sembler inutile, mais la réalité est que l'utilisation de protocoles décentralisés permet de former des réseaux avec des nœuds mobiles (extrêmement difficiles pour les protocoles de routage classiques) qui changent de position en continu et donc modifient la topologie du réseau.

Ces réseaux sont flexibles et peuvent être utilisés dans des opérations de secours militaires, des conférences interactives, des informations sur les échanges commerciaux et des situations d'urgence.

Le routage est une fonction important dans les MANET où chaque entité mobile joue le rôle d’un routeur et participe activement dans la transmission des paquets de données.et pour faire la communication entre les nœuds directement si un nœud dans sa portée radio. Sinon elle utiliser la collaboration entre les voisins.

Plusieurs protocoles de routage ont été développés, chaque protocole essaye de maximiser les performances du réseau Ad Hoc, trois grandes familles de protocoles ont été définies : proactifs, réactifs et hybrides. L’étude de ces différentes approches nous a permis d’orienter nos travaux sur les protocoles de routage réactif. De fait, nous avons choisi de baser nos contributions sur l’optimisation du protocole de routage réactif AODV *(Ad Hoc On-Demand Distance Vector),* AODV est préféré car il minimise les charges d'acheminement par rapport aux autres protocoles et donc l'amélioration des performances du réseau.

Le protocole de routage avec vecteur de distance à la demande AODV *(Ad Hoc On-Demand Distance-Vector)* permet un routage dynamique, autonome et multi-saut entre les nœuds sans fil qui participent au réseau Ad hoc. Il permet des réseaux avec des centaines de nœuds et des taux de mobilité différents, ainsi qu'une grande variété de niveaux de trafique. Ce protocole, dans sa phase expérimentale, a montré dans des tests réels qu'il est capable de trouver des routes fiables en peu de temps, ainsi que de récupérer des liens perdus en raison de l'échec du nœud ou du mouvement du nœud. Ce protocole est devenu très connu et beaucoup de travaux ont déjà été réalisés à son propos.

Le cadre de notre travail est de modifier certains paramètres du protocole pour améliorer la performance du réseau, pour avoir une version optimisé d’AODV, en utilisant une méthode

expérimentale comparative. Le travail de simulation a été effectué en OPNET, sans modifier l'algorithme du protocole (le code source).

Problématique

Différents protocoles de routage ont été conçus mais non encore normalisés. Ils font l'objet d'un grand effort de tests, d'évaluations et d'améliorations. Nous avons essayé à travers ce travail d'optimiser l'un des protocoles ad hoc les plus connus : le protocole AODV.

Le problématique de ce travail est comment résoudre le problème de la détermination des valeurs optimaux des paramètres de protocole de routage AODV *(Ad Hoc On-Demand Distance-Vector)* Pour améliorer la performance, on peut le reformuler notre problématique par les sous problématique suivantes :

- Est-ce qu'en peut optimiser ce protocole et améliorer la performance sans modifier l'algorithme De protocole (le code source).
- Quel est la stratégie définie pour trouver les valeurs optimales des paramètres.
- Comment choisir l'outil et l'environnement de réalisation de cette optimisation.
- Comment créer un réseau ad hoc et activer le protocole AODV dans ce réseau.
- Quel sont les paramètres choisis pour chercher d'autres valeurs optimaux.
- Quel sont les aspects de performance évalués avec notre modification.
- Comment interpréter les résultats obtenus.

Objectifs

Notre objectif est l'optimisation de protocole de routage (AODV), avec une amélioration de la performance par la modification de certains valeurs des paramètres de la version originale, sans touché l'algorithme de protocole (le code source), avec une évaluation de quelque aspects de performances, on utilisant une approche comparative par l'outil de simulation OPNET.
Pour atteindre cet objectif, on peut le reformuler suivant les sous objectifs suivants :

- création d'une version optimisée du protocole AODV, basé sur la modification de certaines valeurs de paramètres d'algorithme de routage (le fonctionnement d'algorithme dépond de ses instructions et ses paramètres).
- conception d'une approche expérimentale (comparative) pour trouver les valeurs optimales des Paramètres.
- L'outil et l'environnement choisi sont : la simulation comme méthode de réalisation et de tests et l'outil OPNET 14.5 comme environnement de simulation.
- Réalisation d'un réseau ad hoc mobile (MANET) routé par le protocole de routage AODV par le simulateur OPNET 14.5.
- On choisit les paramètres suivants : ACTIVE_ROUTE_TIMEOUT, ALLOWED_HELLO_LOSS, NET_DIAMETER, RREQ_RETRIES et NODE_TRAVERSAL_TIME pour trouver d'autres valeurs qui améliore la performance de réseaux.

- Evaluation des performances de réseaux à travers les métriques suivants tel que : le temps de découverte de la route (route discovry Time), le totale des paquets perdus (total packets dropped), le débit du réseau (throughput), le Délai (Delay).
- A travers l'analyse des graphes de la simulation et les résultats obtenus et la comparaison entre la version originale et la version modifié dans chaque scenario et choisir les valeurs de paramètres comme des valeurs optimaux où les valeurs optimaux sont les valeurs des meilleures performances. .

Structure de mémoire

Ce mémoire est structuré en six (06) chapitres comme suit :

- Dans Le premier chapitre**,** nous avons présenté les différents concepts liés aux réseaux sans fil et réseaux mobiles Ad Hoc, en mettant la lumière sur ses caractéristiques et ses spécificités et le domaine d'application.

- Le deuxième chapitre**,** concentré sur le routage et nous présentons une classification des différentes classes de routage dans ce type de réseaux avec une présentation de quelque type de routage.

- Dans Le troisième chapitre, une description détaillé sur le protocole de routage AODV, et son principe de fonctionnement.

- La simulation, les différents types des simulateurs, et une présentation de L'environnement de notre outil de simulation OPNET 14.5sont abordés dans le quatrième chapitre.

- Dans Le cinquième chapitre**,** nous avons présenté notre contribution, ainsi la réalisation de ce dernier par simulation et une vue globale sur les recherches existent dans ce contexte (état de l'art).

- Le sixième chapitre**,** contient les tests et les résultats de simulation à travers des graphes contient des courbes représentent les métriques de réseaux, et une comparaison entre les deux protocoles : AODV (originale) et AODV (optimisé).

CHAPITRE I

GÉNÉRALITÉ SUR LES RÉSEAUX SANS FILS ET LES RÉSEAUX AD HOC

1- Introduction

Au début de l'utilisation de l'informatique, toutes les informations nécessaires aux traitements étaient centralisées sur la même machine. Les réseaux informatiques sont nés pour le but d'échanger les informations et communiquer de façon simple et rapide. Les réseaux informatiques sont divisés en deux grandes familles : les réseaux filaires et les réseaux sans fil voir la figure 1.1.

La majorité des ordinateurs et la quasi-totalité des appareils « mobiles » (tels que les téléphones portables) disposent de moyens de connexion à un ou plusieurs types de réseaux sans fil comme le Wifi, le Bluetooth ou l'infrarouge. Ainsi, il est très facile de créer en quelques minutes un réseau « sans fil » permettant à tous ces appareils de communiquer.

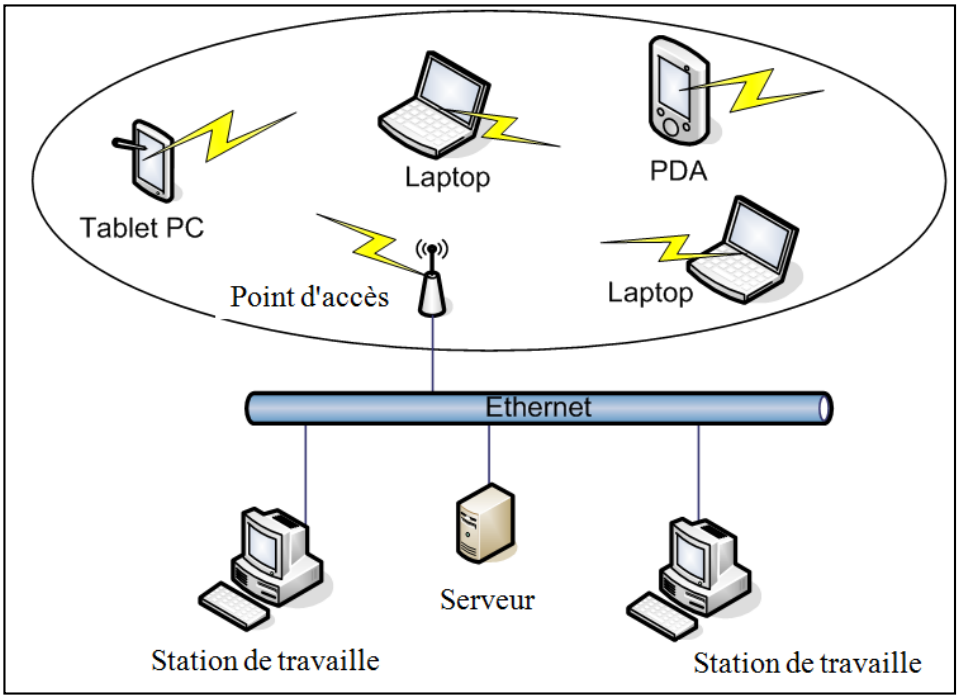


Figure 1.1 : Modèle du réseau filière et réseau sans fil

Le réseau filaire classique utilise des câbles pour relier des ordinateurs et des périphériques via un routeur ou un commutateur.

Les réseaux sans fil sont basés sur une liaison utilisant des ondes radioélectriques (radio et infrarouges)

2. Classification des réseaux sans fil

Les réseaux informatiques peuvent être classés selon deux critères : [1] [2]

- Classification des réseaux en fonction de la taille
- Classification des réseaux suivant le mode opératoire

2.1 Classification des réseaux en fonction de la taille :

On distingue quatre catégories de classification des réseaux en fonction de leur taille.[3]

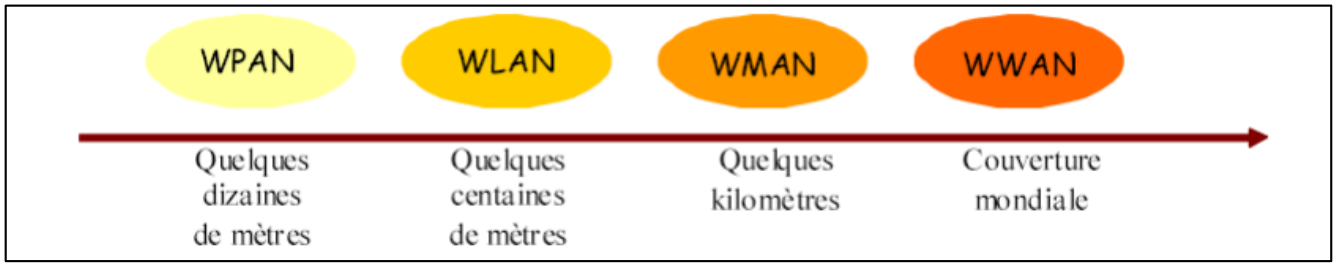


Figure 1.2 : Classification des réseaux sans fil suivant leur taille

2.1.1 Réseaux personnels sans fil WPAN (Wireless Personal Area Networks)

Dans cette catégorie, on retrouve les réseaux sans fil à l'échelle humaine dont la portée maximale est limitée à quelques dizaines de mètres autour de l'usager (bureaux, salles de conférence...). Cette catégorie concerne les réseaux sans fil utilisant des fréquences radio ou infrarouges, On y trouve les standards tels que le Bluetooth, ZIGBEE.

- ***La technologie Bluetooth (norme IEEE 802.15.1)*** **:** C'est la principale technologie WPAN est, lancée par Ericsson en 1994, proposant un débit théorique de 1 Mbps pour une portée maximale d'une trentaine de mètres via une liaison hertzienne. Elle possède l'avantage d'être très peu gourmande en énergie, ce qui la rend particulièrement adaptée à une utilisation au sein de petits périphériques.
- ***La technologie ZigBee (Norme IEEE 802.15.4) :*** Elle permet d'obtenir des liaisons sans fil à très bas prix et avec une très faible consommation d'énergie, ce qui la rend particulièrement adaptée pour être directement intégrée dans de petits appareils électroniques (appareils électroménagers, jouets,...)
- ***La technologie infrarouge :*** Enfin les liaisons infrarouges permettent de créer des liaisons sans fils de quelques mètres avec des débits pouvant monter à quelques mégabits par seconde. Cette technologie est largement utilisée pour la domotique (télécommandes).

2.1.2 Les Réseaux locaux sans fil WLAN (Wireless Local Area Networks)

C'est la catégorie des réseaux locaux sans fil dont la portée va jusqu'à 500 m, pour les applications couvrant un campus, un bâtiment, un aéroport, un hôpital, etc. On y trouve les standards tels que le Wi-Fi (Wireless Fidelity).

- ***La technologie Wifi (norme IEEE 802.11) :*** offre des débits allant jusqu'à 54Mbps sur une distance de plusieurs centaines de mètres. Elle est composée de plusieurs normes qui opèrent sur des fréquences radios différentes. Elle permet de monter un réseau sans fil entre les différents équipements informatiques (PC, Consoles de jeu, PDA, …).

2.1.3 Les réseaux métropolitains sans fil WMAN (Wireless Metropolitan Area Networks)

Plus connus sous le nom de Boucle Locale Radio (BLR), ce type de réseau utilise le même matériel que celui qui est nécessaire pour constituer un WLAN mais peut couvrir une plus grande zone de la taille d'une ville avec une portée pouvant aller jusqu'à 50 Km. C'est dans cette catégorie que l'on classe le WiMax.

2.1.4 Les réseaux sans fil étendus WWAN (Wireless Wide Area Networks)

C'est la catégorie de réseaux cellulaires mobiles dont la zone de couverture est très large, à l'échelle mondiale. Dans cette catégorie, on peut citer le GSM et ses évolutions (GPRS, EDGE).

2.2 Classification des réseaux suivant le mode opératoire

On distingue deux catégories de classification des réseaux en fonction de leur mode opératoire :

Les réseaux sans fil avec infrastructure et les réseaux mobile sans infrastructure. [4]

2.2.1. Le réseau mobile avec infrastructure (Réseaux cellulaires) : Le réseau mobile avec infrastructure intègre deux ensembles d'entités distinctes :

- Les « sites fixes » d'un réseau de communication filaire classique (wired network).
- Les sites mobiles (Wireless network).

Certains sites fixes, appelés stations support mobile (Mobile Support Station) ou station de base (SB) sont munis d'une interface de communication sans fil pour la communication directe avec les sites ou unités mobiles (UM), localisés dans une zone géographique limitée, appelée cellule (voir figure 1.3).

A chaque station de base correspond une cellule à partir de laquelle des unités mobiles peuvent émettre et recevoir des messages. Alors que les sites fixes sont interconnectés entre eux à travers un réseau de communication filaire, généralement fiable et d'un débit élevé. Les liaisons sans fil ont une bande passante limitée qui réduit sévèrement le volume des informations échangées. Dans ce modèle, une unité mobile ne peut être, à un instant donné, directement connectée qu'à une seule station de base [3].

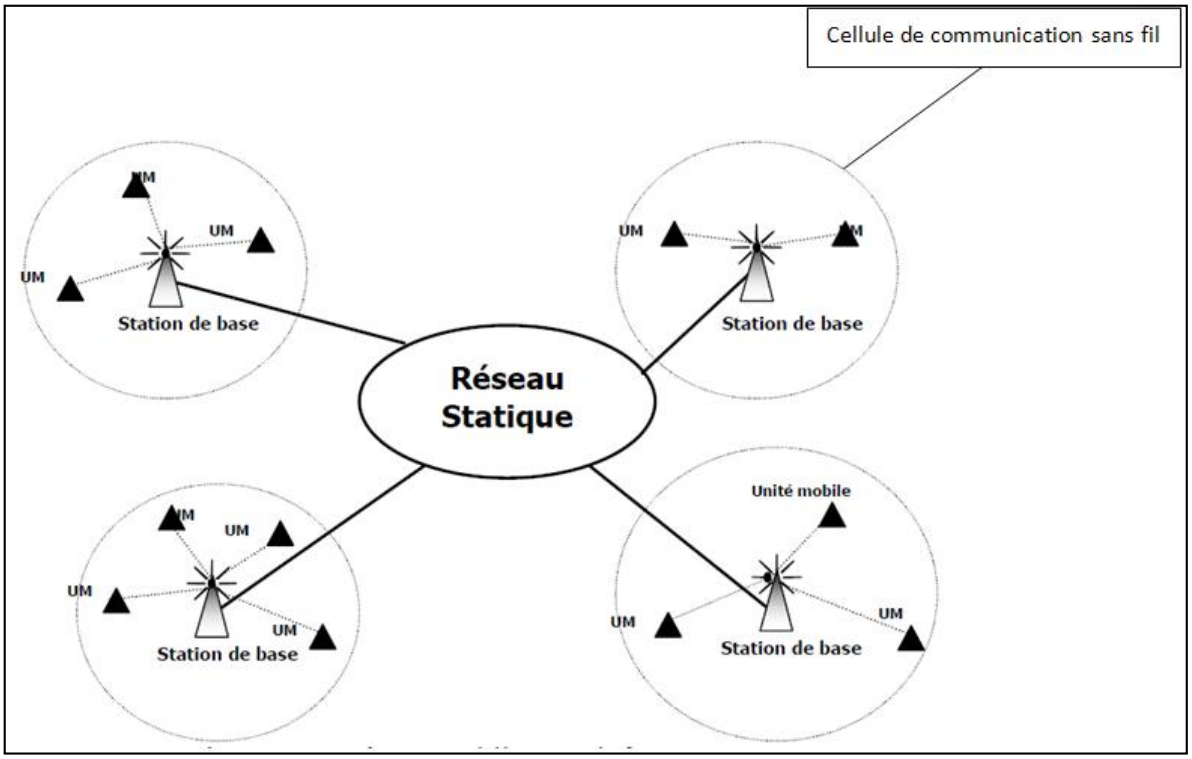


Figure 1.3 : Modèle du réseau mobile avec infrastructure [10]

2.2.2. Le réseau mobile sans infrastructure : Le modèle de réseau mobile sans infrastructure préexistante ne comporte pas l'entité « site fixe », tous les sites du réseau sont mobiles et se communiquent d'une manière directe en utilisant leurs interfaces de communication sans fil. L'absence de l'infrastructure ou du réseau filaire composé des stations de base, oblige les unités mobiles à se comporter comme des routeurs qui participent à la découverte et la maintenance des chemins pour les autres hôtes du réseau [3]. Ce modèle en appel le réseau mobile Ad hoc. [5]

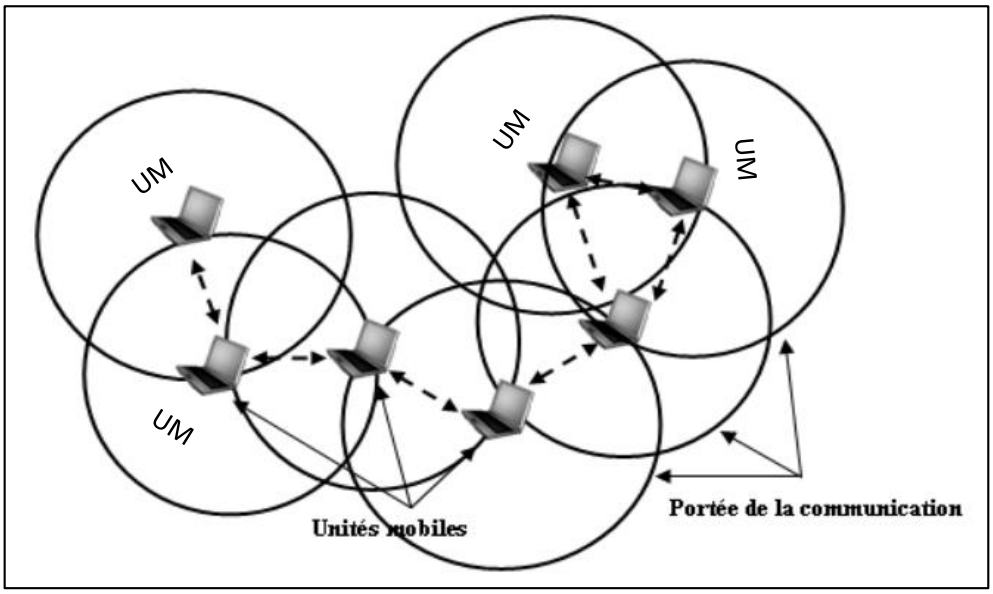


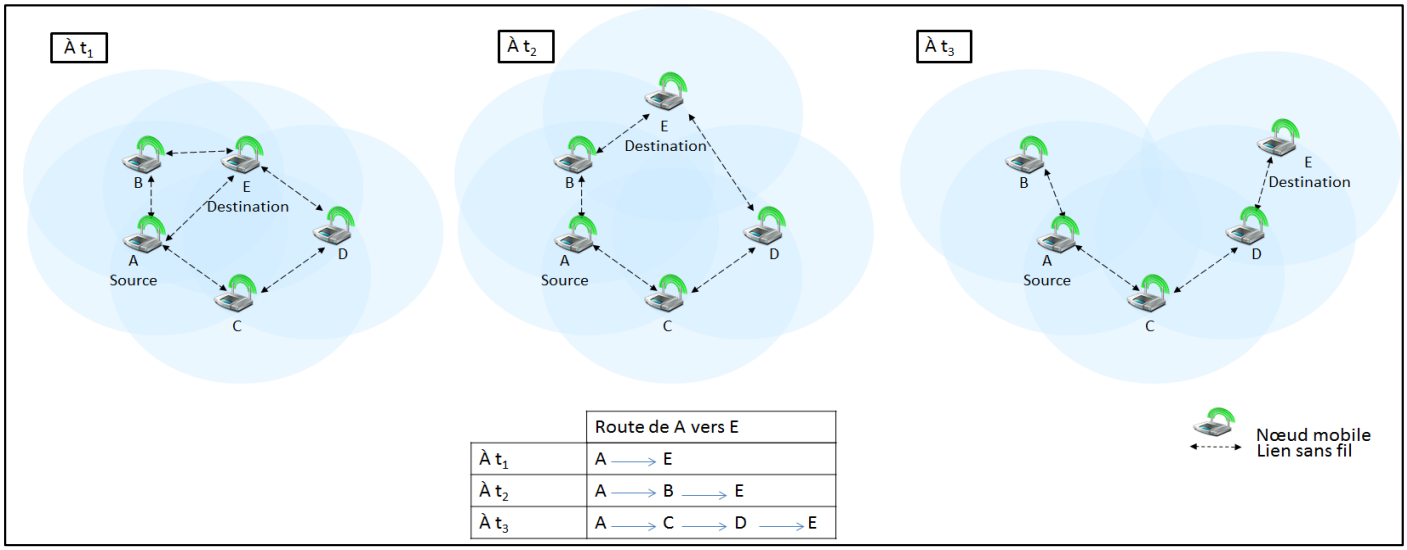
Figure 1.4 : Le modéle des reseaux mobiles sans infrastructure

3. Les réseaux mobiles Ad hoc

3.1 Définition

Un réseau mobile ad hoc est un environnement mobile sans infrastructure, appelé généralement MANET (Mobile Ad hoc NETWORK), est un ensemble de nœuds mobiles qui se déplacent dans un territoire quelconque d'une manière autonome et coopérative, sans l'utilisation d'une infrastructure préexistante ou d'une administration centralisée. Les "ondes radio" qui se propagent entre les différents nœuds mobiles sont le seul moyen de communication. Dès qu'un ensemble de nœuds mobiles se trouve à portée radio les uns des autres, alors le réseau se forme spontanément mais de manière provisoire. Il existe deux modes de communication entre deux nœuds mobiles qui dépendent de la distance qui les sépare : [6]

Dans le cas où les deux nœuds sont à portée radio et peuvent communiquer directement, ce mode est appelé transmission ad hoc. En revanche, dans le cas où les deux nœuds ne sont pas à Portée, ils doivent utiliser d'autres nœuds mobiles comme relais afin d'assurer la communication et d'acheminer les paquets à destination, ce mode est appelé transmission multi-sauts. [6]



	Route de A vers E
À t_1	A → E
À t_2	A → B → E
À t_3	A → C → D → E

Figure 1.5 : Changement de la topologie à cause de la mobilité

La Figure 1.5 montre un exemple de changement de la topologie à cause de la mobilité des nœuds sans fil. Chaque fois qu'un nœud bouge, les tables de routage doivent être recalculées pour prendre en compte les mises à jour. A t1 nous observons dans la Figure 1.5 que la route de A vers E est le lien direct A → E, si nous considérons le nombre de sauts comme métrique de routage. A t2 la topologie change : E n'est plus à portée radio avec A, alors le lien n'existe plus.

De ce fait, la route de A vers E change et devient : A →B →E. Les nœuds bougent encore à t3, E s'éloigne de B alors la route qui existe pour l'atteindre devient A →C →D →E.

La mobilité des terminaux est l'avantage indéniable des réseaux mobiles ad hoc. La topologie du réseau peut changer à tout moment d'une manière dynamique, rapide et aléatoire. Mais, les changements fréquents de la topologie peuvent engendrer la rupture des liens. En plus, l'utilisation des "ondes radio "pour communiquer limite la bande passante réservée à un nœud. Les erreurs de transmission radio sont plus fréquentes dans les réseaux mobiles ad hoc que dans les réseaux flaires. Une autre contrainte s'ajoutant aux contraintes des réseaux mobiles ad hoc est celle de l'interférence. Deux transmissions simultanées sur une même fréquence ou utilisant des fréquences proches peuvent interférer. Aussi, les contraintes et limitations physiques qui minimisent le contrôle des données transférées sont les causes d'une fiabilité limitée dans ce type de réseau.

3.2 L'évolution du réseau ad hoc

Historiquement, les réseaux mobiles Ad hoc ont été d'abord introduits pour l'amélioration des communications dans le domaine militaire. Dans ce contexte, il n'existe pas d'infrastructure existante pour relier les communications, vue la nature dynamique des opérations et des champs militaires.
Les premières applications dans les réseaux Ad hoc sont apparues avec le projet PRNet (Packet Radio Network) en 1972 [7]. Ce projet a été inspiré par l'efficacité la technologie par commutation de paquet, le partage de la bande passante, le routage 'store-and-forward', et ses applications dans l'environnement mobile sans fil.

SURAN (Survivable Radio Networks) [8] a été développé par la DARPA en 1983 pour dresser les principaux problèmes du projet PRNet dans le domaine de la stabilité, la sécurité, la capacité de traitement et gestion d'énergie. Les objectifs étaient de proposer des algorithmes qui peuvent supporter jusqu'à une dizaine de milliers de nœuds, tout en utilisant des mécanismes radio simples, avec une faible consommation d'énergie, et un faible coût. Ce travail a amené à la conception de la technologie LPR (Low-cost Packet Radio) [7] en 1987, dotée d'une couche radio DSSS (Direct Sequence Spread-Spectrum) avec un processeur pour la commutation de paquets intégré (Intel 8086). De plus, une famille de protocoles pour la gestion du réseau a été développée, et une topologie hiérarchique du réseau basée sur un clustering dynamique est utilisée pour remédier au problème de la stabilité. Des améliorations pour l'adaptabilité de la couche radio, la sécurité et l'augmentation de la capacité ont été proposées.

L'évolution des infrastructures du réseau Internet et la révolution de la micro-informatique ont permis de rendre faisables et applicables les idées initiales des réseaux radio de paquets. Le programme GloMo (Global Mobile) [7] initié par la DARPA en 1994 avait comme objectif de supporter les communications multimédia n'importe quand et n'importe où à travers des équipements sans fil.

Tactical Internet (IT)[7] est l'une des implémentations des réseaux sans fil Ad hoc grandeur nature développée par l'armée américaine en 1997, utilisant des débits de plusieurs dizaines de kilobits par seconde.

Un autre déploiement a été réalisé en 1999, avec ELB ACTD (Extending the Littoral Battle-space Advanced Concept Technology Demonstration) [7] qui permet de démontrer la faisabilité de concepts militaires pour les communications des bateaux en mer aux soldats sur la terre par l'intermédiaire d'un relais aérien. 20 nœuds dans le réseau ont été considérés.

3.3 Caractéristiques

Les réseaux mobiles Ad hoc possèdent non seulement les mêmes caractéristiques que les réseaux mobiles avec infrastructure, mais aussi un certain nombre de caractéristiques qui leur sont propres et qui les différencient des autres. Nous pouvons citer quelques caractéristiques principales :

- **Bande passante limitée** : Comme tous les réseaux sans fil, les réseaux ad hoc mobiles disposent d'une bande passante limitée. En effet, la capacité des liaisons sans fil est beaucoup plus faible que la capacité des liaisons filaires. De plus, la capacité réelle utilisable par chaque nœud est généralement beaucoup plus faible que la capacité maximum théorique de la liaison. En effet, les liaisons sans fil sont soumises à de nombreux phénomènes qui en diminuent les performances : bruit, accès multiples, interférences. On a donc un taux d'erreur élevé. Dans le cadre des réseaux ad hoc mobiles, on doit donc minimiser l'échange d'informations de signalisation pour favoriser les données utiles pour l'utilisateur final. [9]
- **Contraintes d'énergie** : Les hôtes mobiles sont alimentés par des sources d'énergie autonomes comme les batteries ou les autres sources consommables. Le paramètre d'énergie doit être pris en considération dans tout contrôle fait par le système. [10]
- **Sécurité physique limitée** : Les réseaux sans fil sont généralement plus sensibles aux menaces physiques que les réseaux câblés. Les techniques existantes pour la sécurité des liaisons sont souvent appliquées au sein des réseaux sans fil pour réduire les risques d'attaques. Cela se justifie par les contraintes et limitations physiques qui font que le contrôle des données transférées doit être minimisé. [11]
- **Erreur de transmission** : Les erreurs de transmission radio sont plus fréquentes que dans les réseaux filaires. [14]
- **Absence d'infrastructure** : pas de station de base ou de point d'accès, tous les nœuds du réseau se déplace dans un environnement distribué sans point d'accès ou un point de rattachement à l'ensemble du réseau. Un nœud joue le rôle aussi bien d'un acteur actif dans le réseau émetteur

et récepteur mais aussi de routeur pour relayer la communication des autres nœuds du réseau. [12]

- **Interférences** : Les liens radios ne sont pas isolés, Les interférences peuvent être de natures diverses. Par exemple, deux transmissions simultanées sur une même fréquence ou, utilisant des fréquences proches peuvent interférer. L'environnement lui-même peut également produire des bruits parasites (certains équipements électriques, certains moteurs, ...) qui interfèrent avec les communications. [13]
- **Topologie du réseau dynamique** : Les nœuds du réseau sont autonomes et capables de se déplacent de manière arbitraire. Cette mobilité fait que la topologie réseau est dynamique car elle peut changer à tout instant de façon rapide et aléatoire. Ce changement de topologie a un impact sur les connexions ou les liens unidirectionnels et bidirectionnels des nœuds. Comme exemple, un nœud (routeur) peut à chaque moment quitter ou rejoindre le réseau. [12]

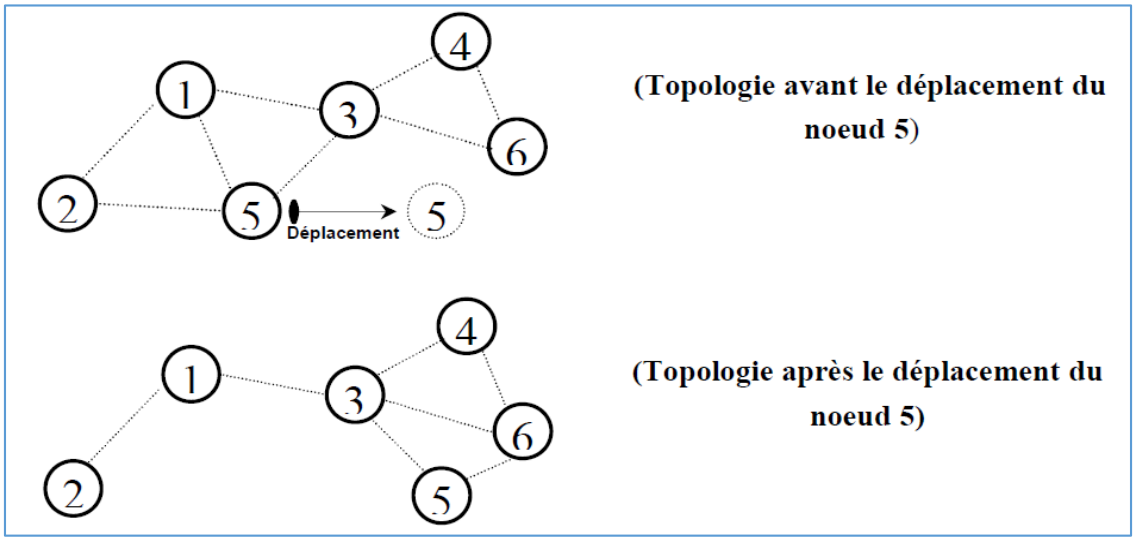


Figure 1.6 : Changement de la topologie d'un réseau ad hoc.

- **Nœuds cachés** : Ce phénomène est très particulier à l'environnement sans fil. Un exemple est illustré par la figure 1.7. Dans cet exemple, les nœuds B et C ne s'entendent pas, à cause d'un obstacle qui empêche la propagation des ondes. Les mécanismes d'accès au canal vont permettre alors à ces nœuds de commencer leurs émissions simultanément. Ce qui provoque des collisions au niveau du nœud A. [10]

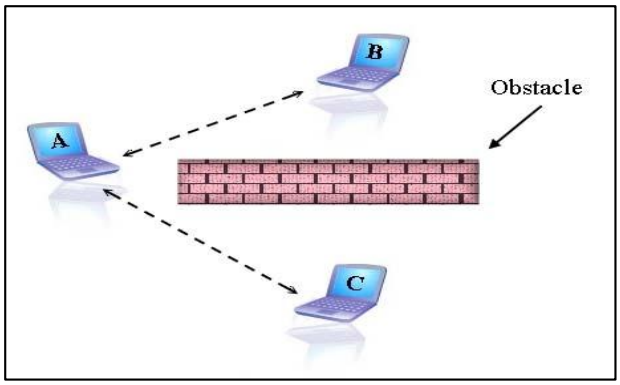


Figure 1.7 : Les nœuds cachés [4]

3.4 Différentes techniques de communication

Dans les réseaux ad hoc, il existe plusieurs techniques de communication : le broadcast, le multicast ou l'unicast. Dans le broadcast, encore dit de technique de la diffusion, un message envoyé par un nœud est reçu par tous ses voisins. Dans une communication en multicast, un message envoyé par un nœud est reçu par un groupe de nœuds parmi ses voisins. Et dans la technique de unicast, encore dite communication point à point, un message envoyé par un nœud est destiné à un seul de ses voisins. Cependant, dans chacune de ces différentes techniques, les communications entre les nœuds ne nécessitent aucune infrastructure fixe. De ce fait, les réseaux ad hoc représentent une alternative aux réseaux avec infrastructure, notamment pour des applications qui requièrent un déploiement dynamique du réseau. Ces trois modes de communication peuvent être schématisés par la figure 1.8. [15]

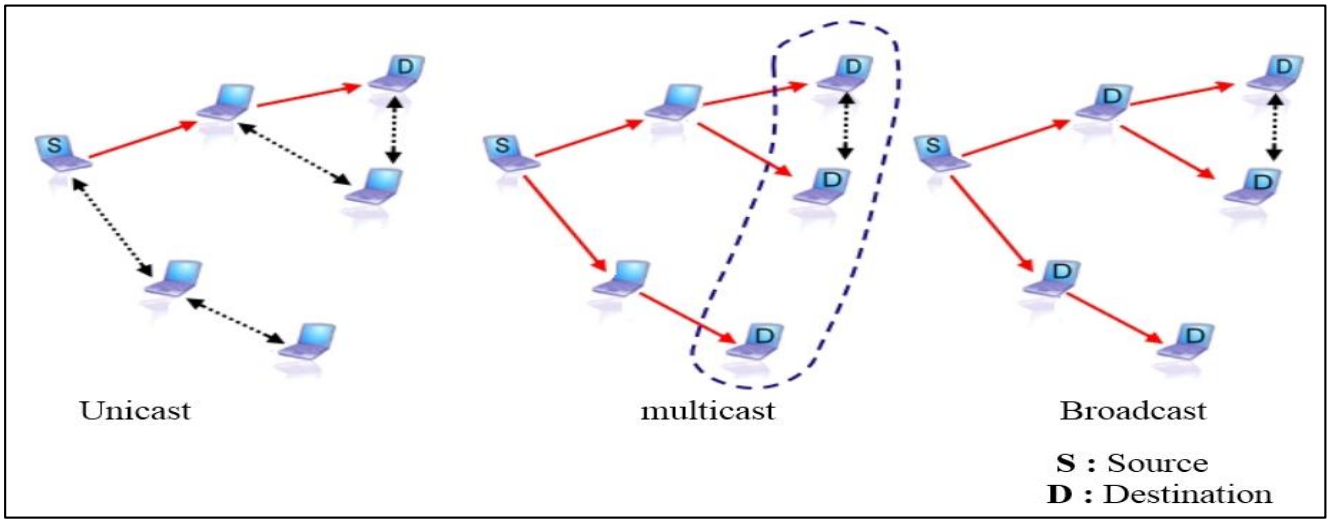


Figure 1.8 : Les différentes techniques de communication

3.5 Domaines d'applications des réseaux ad hoc (MANET)

Les réseaux ad hoc sont idéals pour les applications caractérisées par une absence (ou la non fiabilité) d'une infrastructure préexistante ; telles que les applications militaires et les autres applications de tactique

comme les opérations de secours (incendies, tremblement de terre, etc.) et les missions d'exploration. Les applications ayant recours aux réseaux ad hoc, couvrent un très large spectre, incluant les bases de données parallèles, l'enseignement à distance, etc.

D'une façon générale, les réseaux ad hoc sont utilisés dans toute application où le déploiement d'une infrastructure réseau filaire est trop contraignant; soit parce que difficile à mettre en place, soit parce que la durée d'installation du réseau ne justifie pas un câblage à demeure. [16]

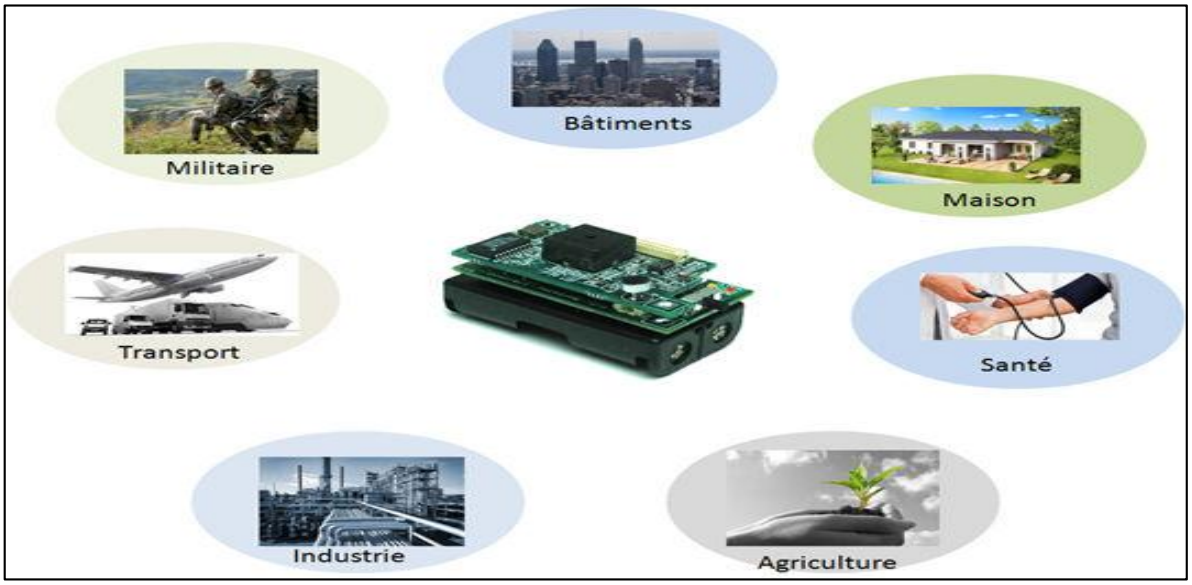


Figure 1.9 : Domaines d'applications.

3.5.1 Applications militaires.

La transmission sécurisée est un des aspects principaux de toutes opérations militaires réussies [16]. En outre, beaucoup d'opérations de la défense ont lieu dans des endroits où l'infrastructure de transmission n'est pas disponible. Les nœuds mobiles de ce type de réseau peuvent être des soldats, des chars, des avions de chasse, etc. L'utilisation des réseaux sans fil ad hoc dans de telles situations devient très utile. Les différentes unités (armée terrestre, marine, et l'armée de l'Air) impliquées dans des opérations militaires doivent également garder la transmission entre eux. Les avions de l'armée de l'air volant dans un groupe peuvent établir un réseau sans fil ad hoc pour communiquer entre eux et échanger des images et des données. Les groupes d'armée en mouvement peuvent également utiliser les réseaux sans fil ad hoc pour communiquer entre eux-mêmes. La même chose s'applique à la marine.

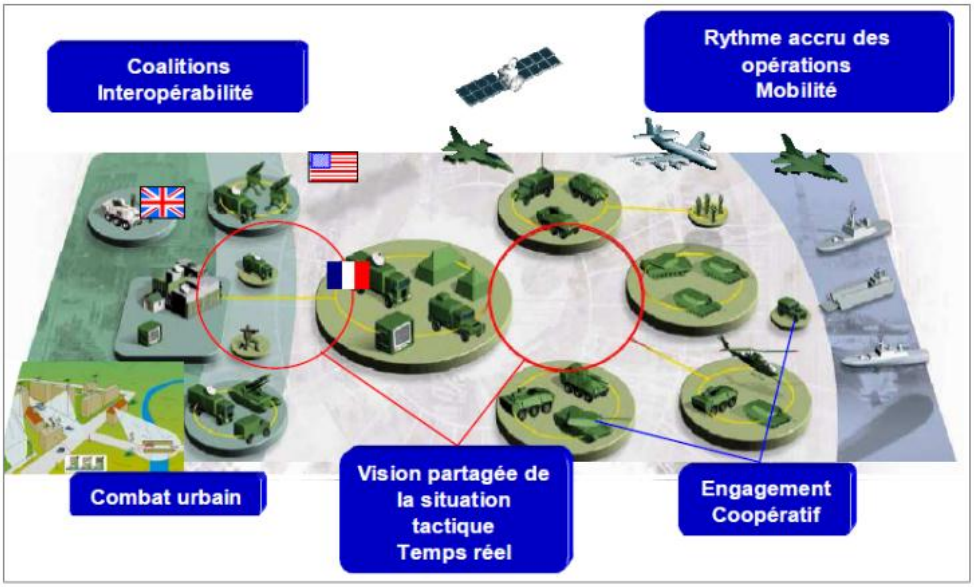


Figure 1.10 : Application des réseaux Ad-Hoc dans le domaine militaire [17]

La figure 1.10 montre les possibilités d'interaction entre les différentes unités (soldat, char et avion) que pourrait offrir une structure de communication basée sur la technologie Ad-Hoc.

3.5.2 Applications médicales

L'échange de l'information multimédia (audio, vidéo, et données) entre le patient et les équipements est très utile dans des situations critiques et d'urgences. Un individu qui est transporté à l'hôpital dans une ambulance peut envoyer de l'information en utilisant les réseaux ad hoc. Un docteur, dans beaucoup de situations, est en bonne position pour diagnostiquer et préparer un traitement pour un patient s'il a une vidéo plutôt que juste des données. Par exemple, la vidéo peut être utile en évaluant les réflexes et en visualisant la capacité de coordination d'un patient. De même, la gravité des blessures d'un patient peut être établie mieux avec l'information visuelle qu'avec information sonore ou juste autre information. L'échographie des reins d'un patient, du cœur, ou d'autres organes, en temps réel, peut être très utile en préparant un traitement pour un patient qui est transporté à l'hôpital, avant son arrivée. Une telle information peut être communiquée par les réseaux sans fil, d'une ambulance à un hôpital ou à des chirurgiens qui sont dispersés dans différents endroits mais ils convergent vers l'hôpital pour traiter le patient.

3.5.3 Recherche et sauvetage

Quand nous sommes en face d'un tremblement de terre, un ouragan ou bien n'importe quel désastre, les réseaux sans fil ad hoc peuvent s'avérer très utiles dans les opérations de la recherche et sauvetage. En général, les désastres laissent une grande population sans électricité et moyens de communication. Les réseaux sans fil ad hoc peuvent être établis sans de telles infrastructures et peuvent fournir des

transmissions entre les diverses équipes de recherche pour coordonner leurs opérations de sauvetage. [13]

3.5.4 Applications commerciales

Utilisés pour un paiement électronique distant (taxi, boutiques) ou pour un accès Internet mobile, etc. [13]

3.5.5 Réseaux de capteurs

Les réseaux de capteurs généralement exploités pour des applications environnementales (météo, activité terrestre, suivi animale, etc.). Leur usage permet l'analyse et la gestion de phénomènes complexes sur une longue période de temps et sur une large zone géographique tel que : la température, l'humidité, la pression, le bruit, etc. [13]

3.5.6 Réseau d'entreprise

La facilité à déployer ces réseaux et leur coût réduit intéressent de plus en plus les entreprises. Cela permet d'assurer une grande mobilité des agents, le partage des données et les conférences. Par exemple, lors d'une réunion ou conférence, l'intervenant peut communiquer avec tous les participants et créer un débat interactif. [18]

3.5.7 Applications transports

La technologie VANET (Vehicular Ad-hoc NETwork) a été proposée comme une variante de réseaux MANET appliquée au domaine du transport. Cette application est considérée comme l'une des applications les plus prometteuses de la technologie Ad-Hoc. Elle pourrait révolutionner la communication inter-véhiculaire avec des systèmes intelligents (régulation de trafic, prévention d'accident,...) et aussi avec l'avènement des ordinateurs embarqués à l'intérieur des véhicules. [16]

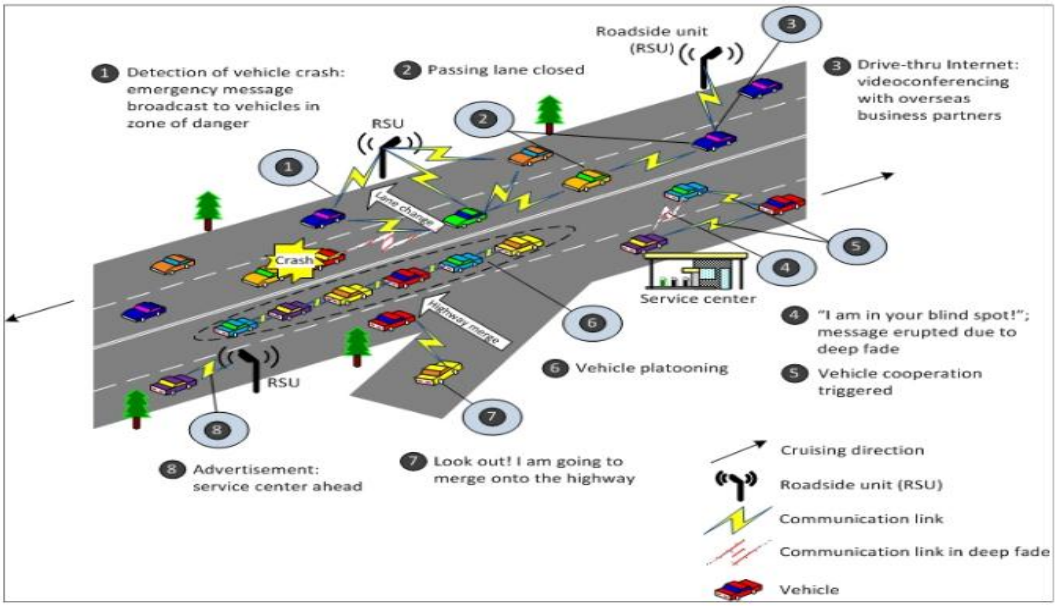


Figure 1.11 : Application des réseaux Ad-Hoc dans le domaine du transport [17]

La figure 1.11 montre l'utilisation des MANET dans le domaine du transport. Les VANET seront sans doute une brique essentielle dans les projets ITS (Intelligent Transportation System) (Chen et al. 2010) [17] visant à créer des applications de communication pour gérer dynamiquement le trafic et la signalisation routière.

3.6 Les avantage et les Inconvénients

3.6.1 Avantage [19]

- **Pas de câblages:** L'une des caractéristiques des réseaux Ad Hoc est l'absence d'un câblage et ce en éliminant toute les connexions filaires qui remplacées par des connexions radio.
- **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 justifié par l'absence d'une infrastructure préexistante permettant ainsi d'économiser tout le temps de déploiement et d'installation du matériel nécessaire.
- **Mobilité permise:** Comme l'indique leur nom et à l'image des réseaux sans fils avec infrastructure les Réseaux mobiles Ad Hoc permettent une certaine mobilité à leurs nœud .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.
- **Cout:** Le déploiement d'un réseau Ad Hoc ne nécessite pas d'installer des stations de base. Les mobiles sont les seules entités physique nécessite Pour déployer.

3.6.2 Inconvénients

- **Débit faible**: Les ondes radio ne permettent qu'un débit faible comparé aux réseaux filaires puisque, l'air étant un support moins fiable et soumis aux bruits parasites, le taux d'erreur sur l'interface air est nettement plus important que sur les liens filaires [19].
- **Connectivité limité:** Ce qui réduit les possibilités de communication [19]. Ainsi deux stations ne sont joignables que s'il existe un ensemble de stations pouvant assumer la fonction de routeur afin de faire suivre les paquets de données échangées entre les deux stations. Dans l'architecture filaire, les possibilités de communication sont prévisibles avant sa mise en place et les bornes d'accès d'une architecture sans fil de type GSM ou UMTS permettent de manière similaire de connaître avec exactitude les zones de couverture (sous réserve d'absence de panne et d'une bande passante suffisante bien sûr). Ce n'est plus le cas avec Les réseaux Ad Hoc où une communication n'est possible que si la collaboration entre stations est suffisante pour lier l'émetteur jusqu' au récepteur.
- **Pollution du voisinage**: Les liens entre les stations, ne sont plus isolés les uns des autres et polluent le voisinage par diffusion lors de chaque émission ou réception de données [19]. Par conséquent, tout paquet de diffusion émis vers une station réceptrice en cours de communication (à qui le

paquet est ou n'est pas destiné) va altérer la communication, et rendre celle-ci inexploitable pour la station réceptrice. En fait, les diffusions sont un facteur qui alourdissent aussi d'autres paramètres : en effet, la diffusion d'un paquet engendre une diminution des batteries de l'ensemble des récepteurs dans la portée de l'émetteur et non pas seulement du récepteur concerné par le paquet émis (si tant est qu'il y est un récepteur concerné, ce qui n'est pas toujours le cas, par exemple dans une découverte de route). Les diffusions, étant constituées de paquets plus ou moins grands, vont entraîner également une baisse illégitime de la bande passante.

- **Sécurité difficile:** Ce qui est difficile à contrôler, notamment parce que sur l'interface air l'écoute clandestine constitue une faille de sécurité importante et très simple à réaliser [19].
- **Difficulté d'adopter des politiques de gestion globale du réseau:** L'absence de centralisation rend les stations toutes semblables à un revers ce qui rend difficile de mettre en place un système de facturation est techniquement délicat, et offrir des qualités de service différentes aux utilisateurs est difficilement contrôlable dans ce contexte.
- **Utilisation courte du terminal:** enfin, la faible autonomie des batteries constitue un frein à une utilisation longue du terminal et à la mise en place de nouveaux services. C'est une contrainte qui existe certes dans la problématique des réseaux de type GSM ou UMTS, mais qui est plus forte ici puisque les ressources y sont mises en commun pour les besoins du routage. L'autonomie est particulièrement limitative pour la mise en place de systèmes de cryptographie, par exemple, qui requièrent des calculs longs et complexes, ce qui complexifie davantage le problème de la sécurité dans les réseaux Ad Hoc qui est déjà délicat avec l'interface air.

4. Conclusion

Ce chapitre a été axé sur l'étude de concept des environnements mobiles et les domaines d'application de la technologie de communication Ad Hoc. Le réseau Ad Hoc offre beaucoup de simplicité et assez d'avantages par rapport aux autres réseaux (filaires) par sa facilité de déploiement et son coût réduit. Une des contraintes des réseaux MANET est le problème d'acheminement des données entres les nœuds mobiles du réseau. Dans le chapitre qui suit, on détaille le routage dans les réseaux Ad Hoc.

CHAPITRE II

LE ROUTAGE DANS LES RÉSEAUX AD HOC

1. Introduction

Lors de la transmission d'un paquet de données d'une source vers une destination, il est nécessaire de faire appel à un protocole de routage qui acheminera correctement le paquet par le meilleur chemin.
Comme nous avons déjà vu, un réseau Ad Hoc est un ensemble de nœuds mobiles qui se déplacent dans un territoire quelconque d'une manière autonome et coopérative, sans l'utilisation d'une infrastructure préexistante ou d'une administration centralisée. Dans la plupart des cas, l'unité destination ne se trouve pas obligatoirement dans la portée de l'unité source ce qui implique que l'échange des données entre deux nœuds quelconques, doit être effectué par des stations intermédiaires.
Pour cela le réseau doit donc s'organiser automatiquement et réagir rapidement aux différents mouvements des nœuds. Chaque unité devient donc un nœud susceptible d'être mis à contribution pour participer au routage. Pour pallier ce type de problème, de nombreux protocoles ont été proposés, ils peuvent être classés 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 de tables de routage alors que les protocoles réactifs recherchent les routes à la demande du réseau. Il existe une troisième approche, dite hybride, qui combine les deux approches précédentes.

Dans ce chapitre, nous allons décrire un certain nombre de protocole de routage.

2. Définition du routage

Généralement, le routage est une méthode d'acheminement des informations à la bonne destination à travers un réseau de connexion donné, 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. Si une seule destination est impliquée dans la communication, alors il s'agit d'un "routage unicast" ; si encore tous les nœuds du réseau ou juste un sous ensemble sont concernés par la réception des données alors on parle du "broadcast" et du "routage multicast", respectivement.

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. [20]

3. Les protocoles de routage dans MANET

3.1. Définition d'un protocole de routage

Le protocole de routage est un programme ou bien algorithme qui sert à déterminer la route optimal pour le transfert de données entre deux nœuds. 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.

3.2. Propriétés requises pour les protocoles de routage dans les MANETs

Les propriétés que doivent vérifier les protocoles de routage pour les MANETs peuvent être résumés dans les points suivant [10] [21] [22] :

- **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 s'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.
- **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.
- **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.
- **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.
- **Convergence rapide**: après la rupture d'un chemin, un protocole de routage doit rétablir un nouveau chemin le plutôt possible.
- **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.
- **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.
- **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.

3.3. Notions fondamentales sur le routage

3.3.1. Routage à plat

Le routage à plat [23] Considèrent que tous les nœuds sont égaux (figure 2.1). La décision d'un nœud de router des paquets pour un autre dépendra de sa position. Permis les protocoles utilisant cette technique, on cite l'**AODV** (Ad Hoc On Demand Distance Vector).

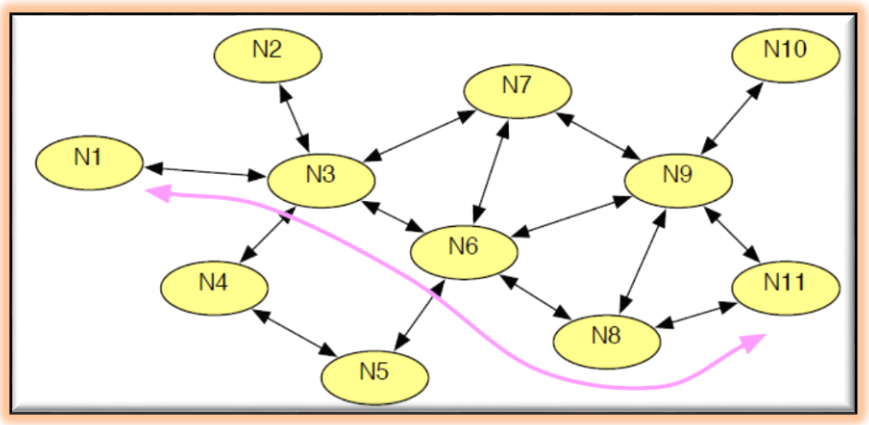


Figure 2.1 Routage à plat

3.3.2. Routage hiérarchique

Le routage hiérarchique [24] fonctionne en confiant aux mobiles des rôles qui varient de l'un à l'autre. Certains nœuds sont élus et assument des fonctions particulières qui conduisent à une vision en plusieurs niveaux de la topologie du réseau. Un mobile pourra servir de passerelle pour un certain nombre de nœuds qui se seront attachés à lui. Le routage en sera simplifié, puisqu'il se fera de passerelle à passerelle, jusqu'à celle directement attachée au destinataire. Un exemple est donné sur la figure 2.2, ou le nœud N3 passe par les passerelles P1, P2 et P3 pour atteindre N7. L'un du protocole utilisant cette stratégie est l'OLSR (Optimized Link State Routing).

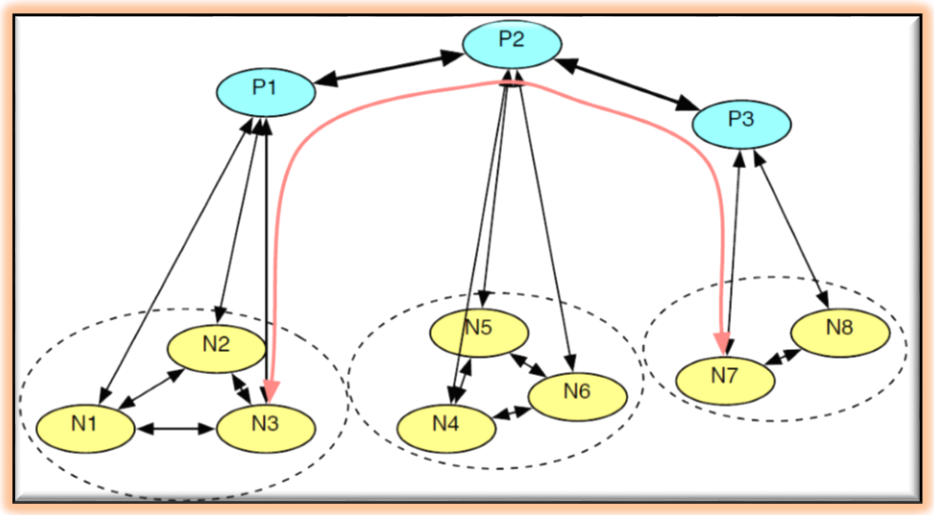


Figure 2.2 Routage hiérarchique

3.3.3. L'inondation

L'inondation [25] ou la diffusion pure, consiste à faire propager un paquet (de données ou de contrôle) dans le réseau entier. Un nœud qui initie l'inondation envoie le paquet à tous ses voisins directs. De même, si un nœud quelconque du réseau reçoit le paquet, il le rediffuse à tous ses voisins. Ce comportement se répète jusqu'à ce que le paquet atteigne tous les nœuds du réseau. Notons que les nœuds peuvent être amenés à appliquer - durant l'inondation - certains traitements de contrôle dans le but d'éviter certains problèmes tel que le bouclage et la duplication des messages.

3.3.4. Etat de lien (Link state)

L'état de lien [13] consiste que chaque nœud maintient une vision globale de la topologie du réseau. La mise à jour de cette vision se fait par diffusion périodique (par inondation) des requêtes par chaque nœud déclarant l'état des liens de ses voisins à tous les nœuds du réseau. L'opération de mise à jour peut se faire aussi dans le cas de changement d'un état des liens. Une fois que la mise à jour est effectuée, chaque nœud change sa vision de la topologie en se basant sur l'image complète du réseau formé des liens les plus récents. Ensuite, il applique un algorithme de calcul de route optimale pour calculer la distance qui le sépare d'une destination donnée. Cette technique est basée sur l'algorithme Dijkstra c'est un algorithme les plus couramment appliqués dans le calcul de plus court chemin.

3.3.5. Vecteur de distance

Le vecteur de distance [26] consiste que chaque nœud diffuse à ses nœuds voisins, sa vision des distances qui le séparent de tous les hôtes du réseau. En se basant sur les informations reçues par tous ses voisins, chaque nœud de routage fait un certain calcul pour trouver le chemin le plus court vers n'importe quelle destination. Le processus de calcul se répète, s'il y a un changement de la distance minimale séparant deux nœuds, jusqu'à ce que le réseau atteigne un état stable. Cette technique est basée sur l'algorithme distribué de Bellman Ford.

3.4. Classification des protocoles de routage

Le principal but de toute stratégie de routage est de mettre en œuvre une bonne gestion d'acheminement qui est robuste et efficace. D'une manière générale, toute stratégie de routage repose sur des méthodes et des mécanismes que l'on peut regrouper en trois grandes classes : les protocoles de routage proactifs, les protocoles de routage réactifs et les protocoles de routage hybrides.

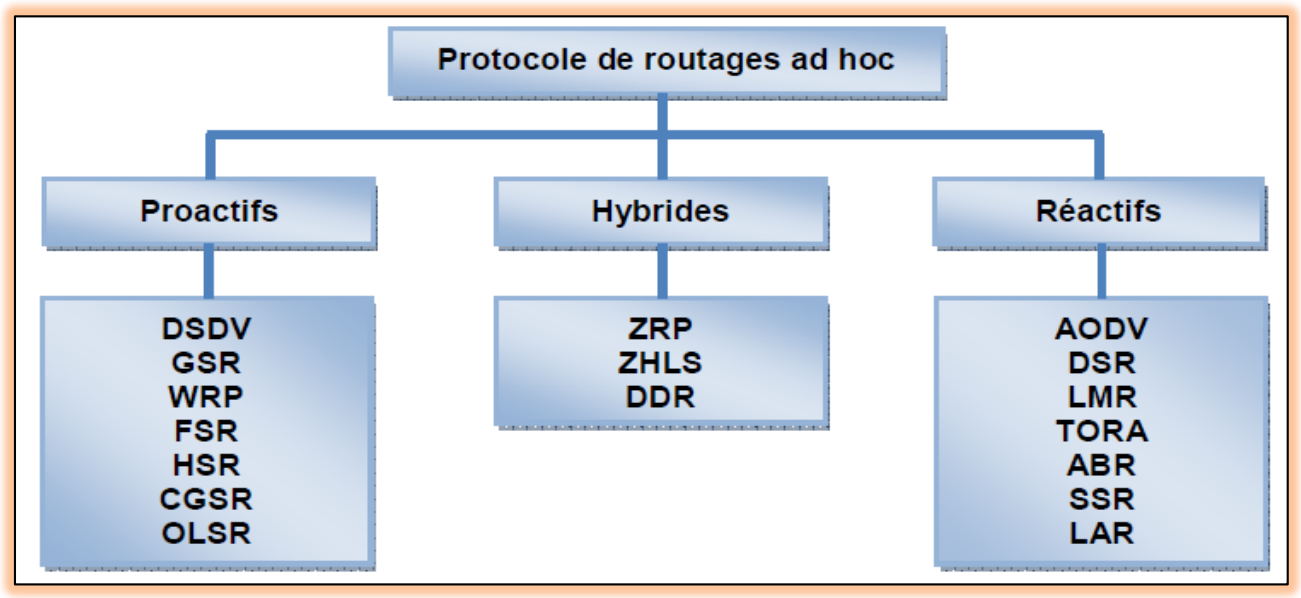


Figure 2.3 : Classification des protocoles de routage ad hoc

3.4.1. Les protocoles de routage proactifs

Un protocole de routage est dit proactif [27] si les procédures de création et de maintenance des routes, durant la transmission des paquets de données, sont contrôlées périodiquement. Cette maintenance reste toujours active même s'il n'y a pas de trafic circulant dans le réseau. Le but de cette stratégie est de fournir instantanément une route déjà stockée entre la source et la destination aussitôt que le besoin se présente. La famille de protocoles proactifs se divise en deux catégories. La technique utilisée pour la découverte et le maintien des liens différencie ces deux catégories. La première catégorie est appelée ***protocoles avec vecteur distance*** où la métrique pour le calcul des routes est le nombre de sauts séparant la source à la destination. La deuxième catégorie est appelée ***protocoles à état de lien*** utilisant l'état des liens pour le calcul de routes. La mise à jour des routes est faite par des techniques de l'inondation (Broadcast). Les protocoles DSDV (protocole avec vecteur distance) et OLSR (protocole avec état de lien) sont des exemples de ces deux catégories.

3.4.1.1. Le protocole DSDV (Dynamic Destination-Sequenced Distance-Vector)

Le DSDV (Dynamic Destination-Sequenced Distance-Vector) [31] est principalement inspiré de l'algorithme distribué de Bellman Ford (DBF : Distributed Bellman-Ford). Toutefois, chaque station mobile se voit maintenir une table de Routage contenant :

• Toutes les destinations possibles dans le réseau.

• Le nombre de nœuds (ou de sauts) nécessaire pour atteindre chacune de ces destinations.

• Le numéro de séquences (**SN**: Séquence Number) qui correspond à un nœud destination.

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

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

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

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

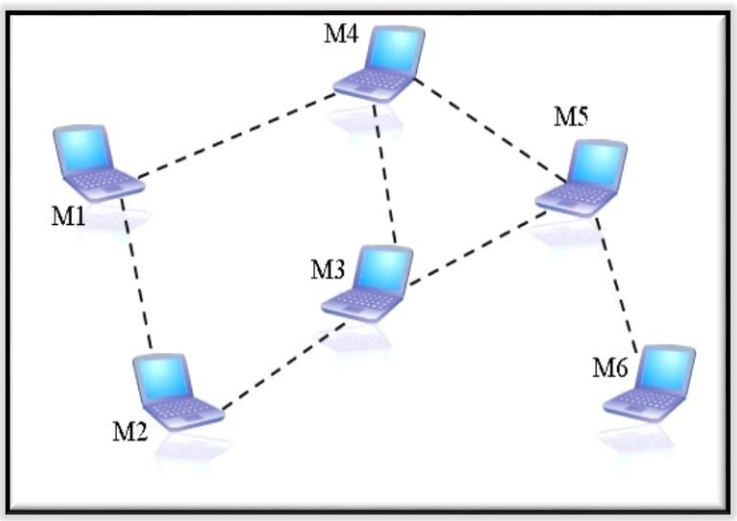


Figure 2.4 : Exemple d'un réseau Ad Hoc

Si l'on considère que le DSDV est le protocole de routage utilisé dans la figure 2.4, la table de routage correspondante au nœud M1 ressemblera à la suivante :

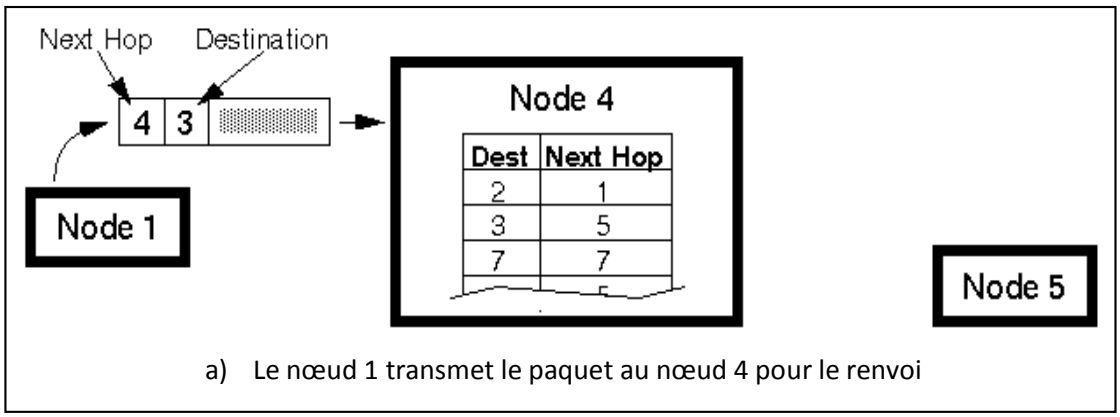
DESTINATION	*NOMBRE DE SAUTS*	*PROCHAIN NŒUD*	*NUMERO DE SEQUANCE*
M1	*0*	*M1*	*NS1*
M2	*1*	*M2*	*NS2*
M3	*2*	*M2*	*NS3*
M4	*1*	*M4*	*NS4*
M5	*2*	*M4*	*NS5*
M6	*3*	*M4*	*NS6*

Tableau 2.1 : Table de routage du nœud M1 du graphe 2.4

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

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

- **Procédure de routage dans DSDV :**



a) Le nœud 1 transmet le paquet au nœud 4 pour le renvoi

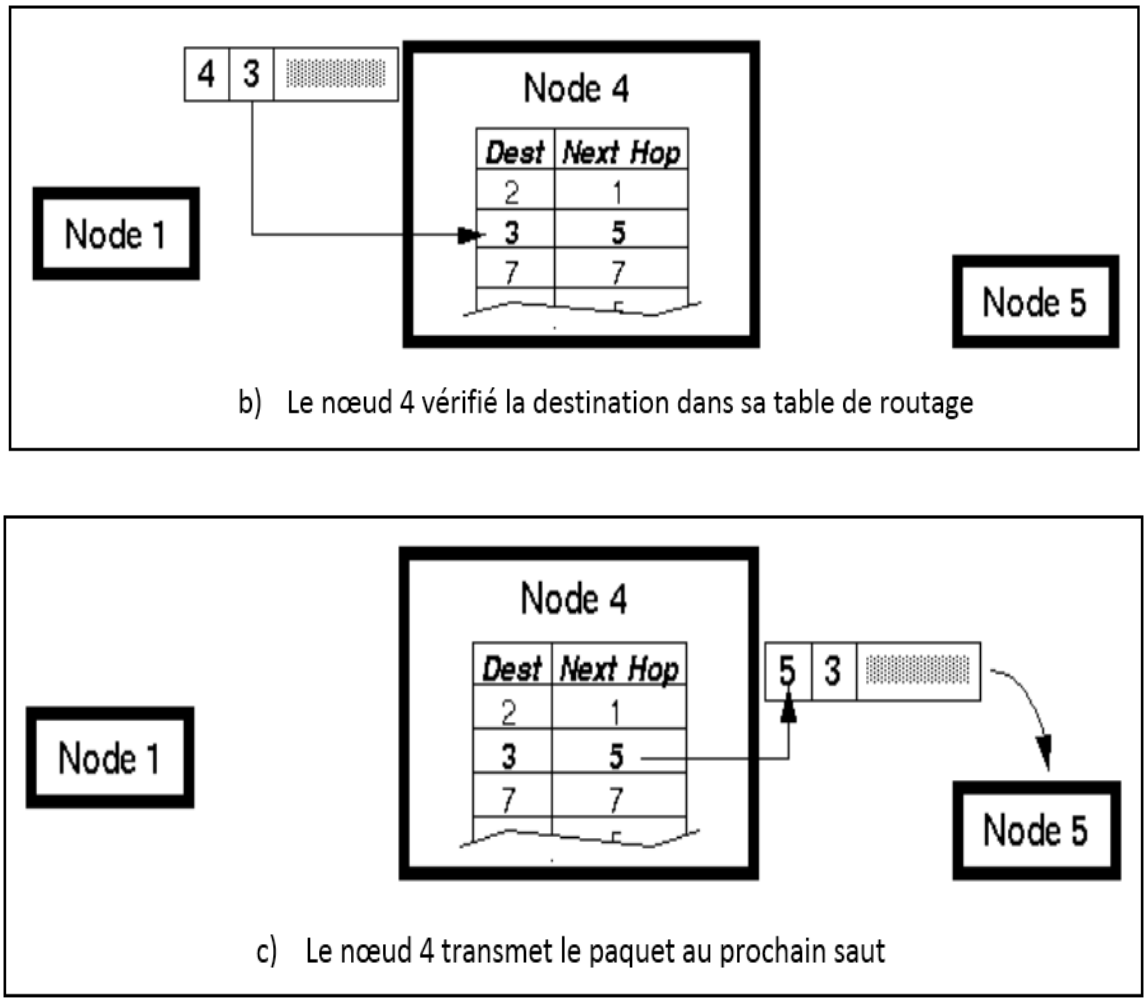


Figure 2.5: exemple de la procédure de routage dans DSDV.

La figure 2.5 illustre la procédure de routage dans DSDV [32]. Dans cet exemple, un paquet est envoyé du nœud 1 au nœud 3 (le nœud 3 n'est pas à la portée de nœud 1). Dans la table de routage de nœud 1, le prochain saut du paquet est le nœud 4 (Figure 2.5 a).Lorsque le nœud 4 reçoit le paquet, il recherche l'adresse de destination (nœud 3) dans sa table de routage (Figure 2.5 b). Le nœud 4 transmet ensuite le paquet au saut suivant comme spécifié dans le tableau, dans ce cas le nœud 5 (figure 2.5 c). Cette procédure est répétée jusqu'à ce que le paquet arrive à sa destination.

- **Gestion de la table de routage**

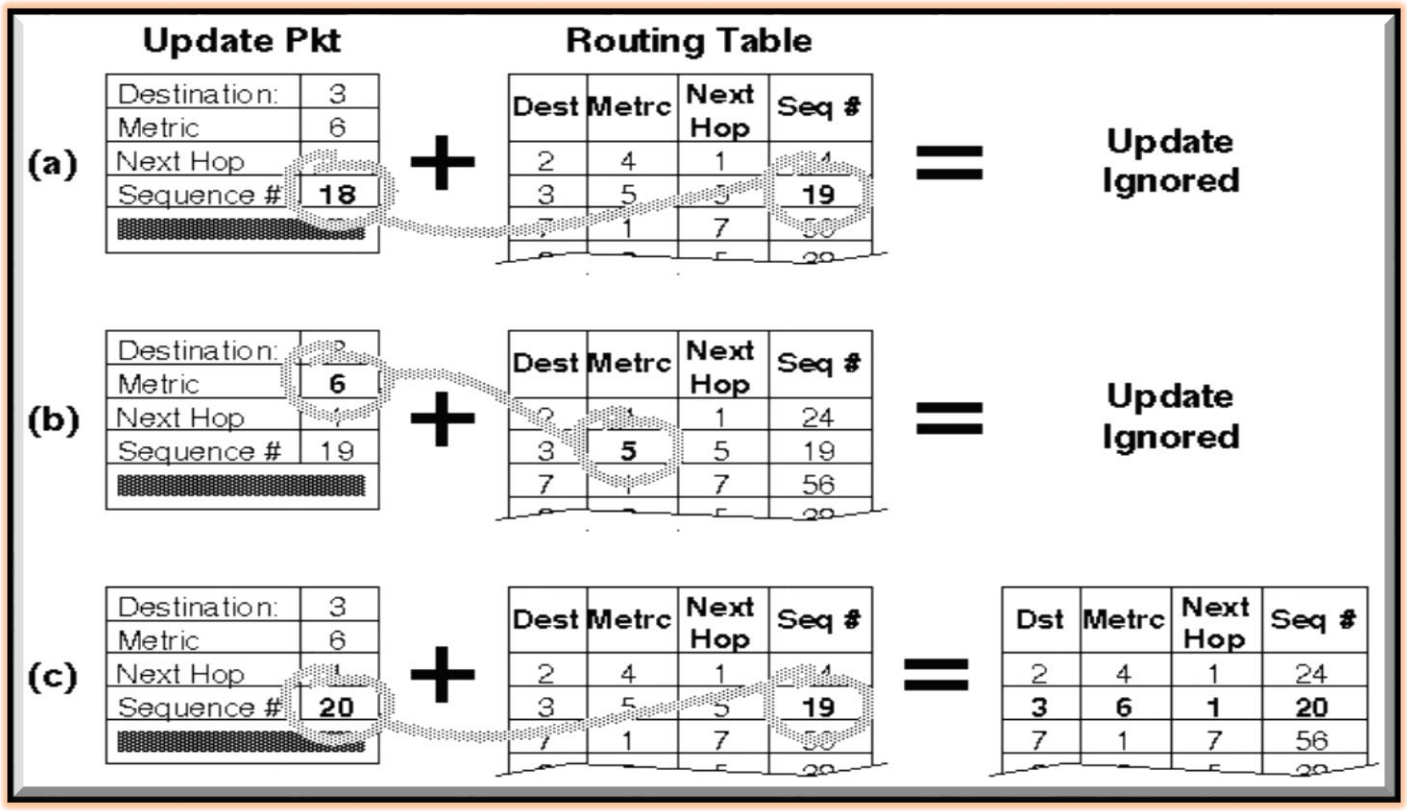


Figure 2.6: Un nœud recevant trois paquets de mise à jour. [32]

Chaque fois qu'un paquet de mise à jour est transmis, le paquet contient non seulement l'adresse de la destination éventuelle, mais contient également l'adresse du nœud expéditeur. L'adresse du nœud expéditeur est entrée dans la table de routage comme le prochain saut (sauf si le paquet est ignoré, bien sûr).

La figure 2.6 illustre comment un nœud traite un paquet de mise à jour dans des conditions variables. Pour que les paquets de mise à jour soient toujours entrés dans la table de routage il doit :

- le nombre de séquence plus élevés.
- le nombre de séquence du paquet égale le nombre de séquence dans la table de routage et la métrique du paquet plus petit que la métrique dans la table de routage.

3.4.2. Les protocoles de routage réactifs (à la demande)

Les protocoles de routage réactifs [27] sont des protocoles dans lesquels la mise à jour ou le contrôle des routes se fait à la demande, c'est-à-dire lorsqu'une source veut transmettre des paquets de données vers une destination. L'avantage de cette approche consiste à éliminer le coût de maintenance des tables de routage ainsi que la surcharge du réseau (pas de mise à jour de route requise). Toutefois, cette approche souffre de problèmes de délais de transmission de paquets engendrés par le processus de découverte de route lui-même. L'envoi des messages est retardé jusqu'au moment de trouver une route

vers la destination. Le protocole DSR et AODV est un exemple de ce type de protocole. Dans le cadre à la demande plusieurs politiques peuvent être adoptées, les plus importantes sont :

- **La Technique d'apprentissage en arrière**

Le mécanisme d'apprentissage en arrière [33] ou le **backward learning** est basé sur le fait que lorsqu'un nœud source veut transmettre un message à une destination précise, il procède tout d'abord à l'opération d'inondation de sa requête sur tout le réseau. Ainsi chaque nœud intermédiaire dit de transit (appartenant au chemin par lequel va passer le message), indique le chemin au nœud source lors de la réception de la requête.

On dit qu'il apprend le chemin au nœud source, tout en sauvegardant la route dans la table transmise. Enfin, lorsque la requête arrive à bon port, le nœud destinataire, et suivant le même chemin, transmet sa réponse sous forme de requête.

- **Technique du routage source**

Dans la technique du routage source [33], le nœud source détermine toute la liste des nœuds par lesquels doit transiter le message, ainsi le nœud émetteur inclut dans l'entête du paquet une route source. En effet, afin de construire la route, le nœud source doit préciser les adresses exactes des nœuds par lesquels le message transitera jusqu'à atteindre le destinataire. Ainsi, le nœud source transmet le paquet au premier nœud spécifié dans la route. Notons que chaque nœud par lequel le paquet transit, supprime son adresse de l'entête du paquet avant de le retransmettre. Une fois que le paquet arrive à sa destination, il sera délivré à la couche réseau du dernier hôte.

3.4.2.1. Le protocole DSR (Dynamic Source Routing)

Le protocole « routage par la source » DSR [35] (Dynamic Source Routing) est un protocole de routage ad hoc réactif à état de lien. Les routes sont construites à la demande en utilisant la technique de routage source. Chaque nœud inclut son adresse dans l'entête de telle sorte qu'en arrivant à la destination, le paquet contient une liste complète et ordonnée de nœuds par lesquels le paquet a transité de la source à la destination (figure 2.7a, b, c). Cette liste est renvoyée à la source dans un paquet de réponse de route (figure 2.7d). Nous donnons plus de détails sur le processus de découverte de route dans ce qui suit. DSR définit deux opérations : la découverte des routes et la maintenance de route.

- **Découverte de route.** [36]

Lorsqu'un nœud source désire envoyer des données à une destination et qu'il ne trouve pas de route disponible pour cette destination dans son cache (route cache), il initialise une demande de route RREQ (Route Request). C'est le cas du nœud **S** dans la figure 2.7a. La RREQ contient un identifiant unique (route request identifier), la destination à atteindre et une liste d'adresses de nœuds qui contient

initialement uniquement l'adresse de la source (cette liste constituera le chemin entre la source et la destination à la fin du processus de découverte).

Lorsqu'un nœud intermédiaire reçoit la demande de route RREQ, il commence par vérifier s'il ne s'agit pas d'une requête déjà traitée en cherchant dans l'historique l'existence du couple ([identifiant de la requête, adresse de la source]) identifiant cette RREQ. Si c'est le cas, le paquet est ignoré sinon, le nœud rajoute son adresse dans la liste du paquet et rediffuse ce paquet à son tour après l'avoir ajouté dans son historique.

Lorsque le paquet RREQ arrive à la destination, la liste contenue dans le paquet constitue le chemin complet pour l'atteindre (cas du nœud D dans la figure 2.7c). La destination crée alors une réponse de route RREP (Route Reply) en y copiant la liste contenue dans la RREQ reçue et en insérant son adresse à la fin de cette liste. Une fois envoyée, cette réponse de route suivra le chemin contenu dans la liste jusqu'à atteindre la source. Ainsi, le chemin est établi entre la source et la destination et la transmission de données peut débuter.

Dans certains cas, un nœud intermédiaire peut avoir une route qui mène à la destination dans son route cache. Dans cette situation, le nœud intermédiaire peut générer une réponse de route en concaténant le chemin qu'il a reçu dans le paquet RREQ avec celui qui se trouve dans son route cache en s'assurant qu'il n'y a pas de nœud qui figure dans les deux parties auquel cas il devra renoncer à la création de la RREP pour éviter la création des boucles de routage.

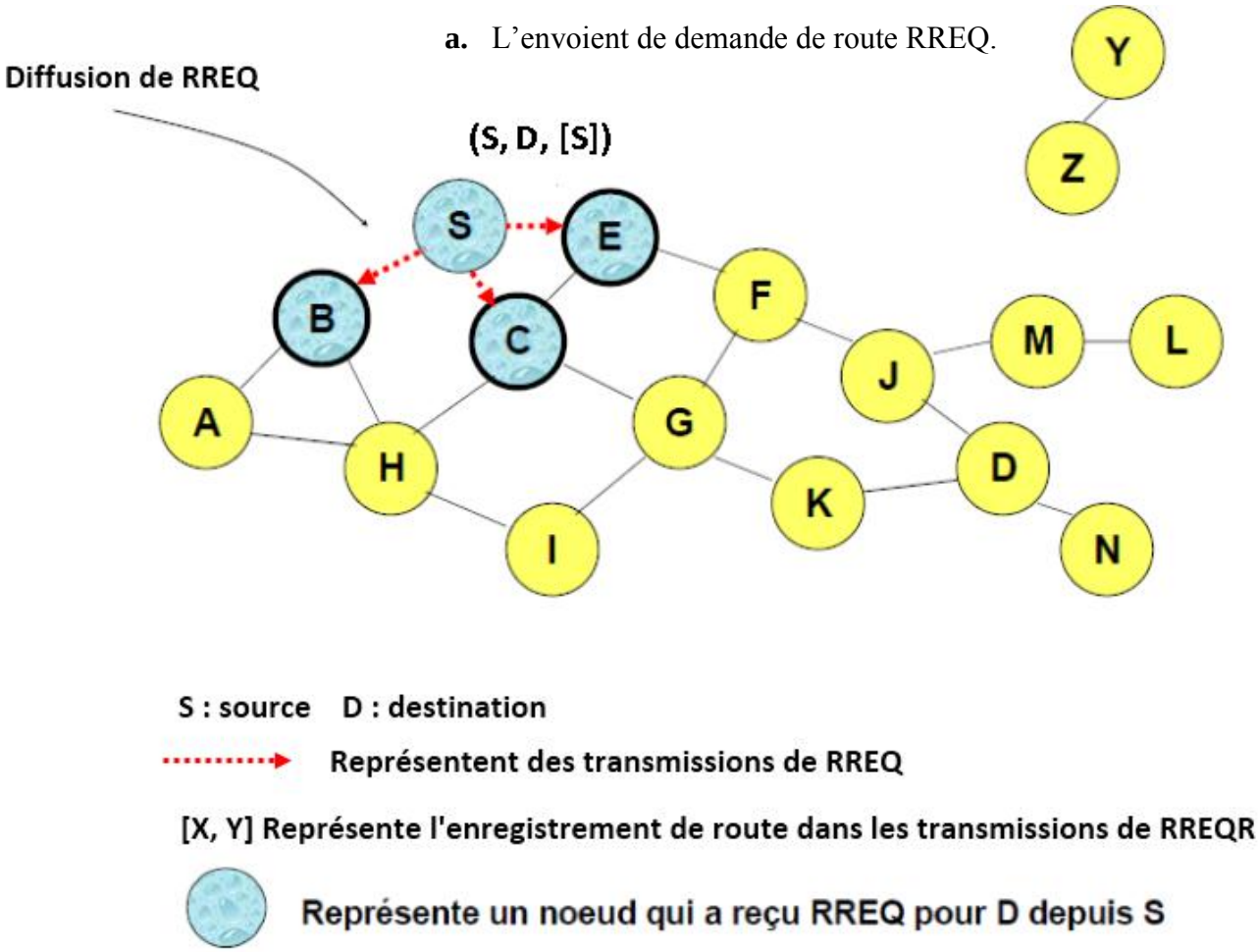
À la fin du processus de découverte de route, un nœud peut avoir dans son cache plus d'une route pour certaines destinations auquel cas il devra choisir une route en se basant sur le plus court chemin ou en utilisant une autre métrique (e.g. rapidité d'établissement du chemin).

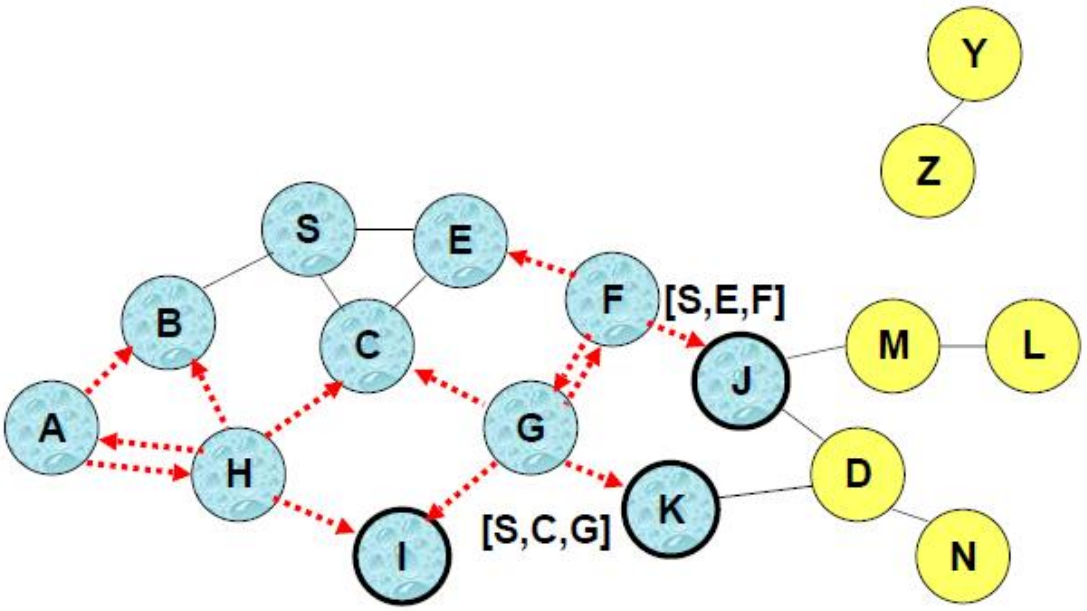
- **Maintenance des routes.** [36]

Un paquet erreur de route RERR (Route Error) est émis quand une route est inutilisable. Ce paquet, contenant l'adresse du nœud qui a détecté l'erreur et celle du nœud qui le suit dans le chemin, est envoyé à l'émetteur original du paquet, dont la "non transmission" a déclenché la détection de panne. Quand la source reçoit le paquet RERR, le nœud concerné par l'erreur est supprimé du chemin sauf gardé et tous les chemins qui contiennent ce nœud sont tronqués à ce point-là. Par la suite, une nouvelle opération de découverte de route vers la destination est initiée par l'émetteur.

DSR optimise ses algorithmes par un mécanisme de cache. Le cache est utilisé à la source pour mémoriser plusieurs routes vers une destination. En cas de panne la source n'initie pas de nouvelle recherche de route, elle utilise la route mémorisée dans le cache (figure 2.7). Le mécanisme de cache est également utilisable sur les nœuds intermédiaires.

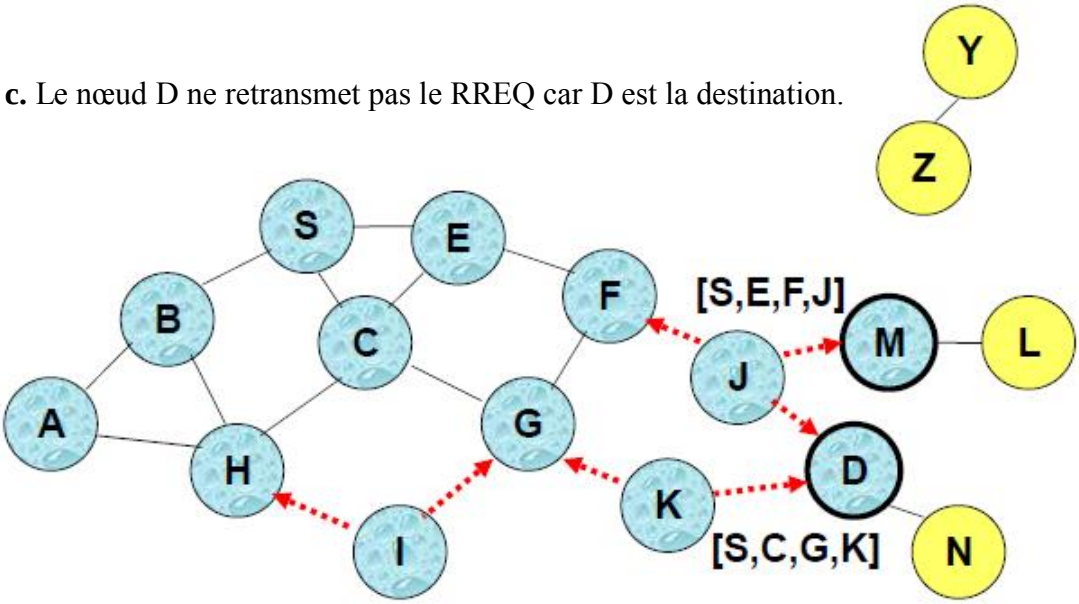
a. L'envoient de demande de route RREQ.





b. Les nœuds J et K retransmettent tous les deux le RREQ avec une possibilité de collision.

c. Le nœud D ne retransmet pas le RREQ car D est la destination.



d. L'envoient de repense de route RREP.

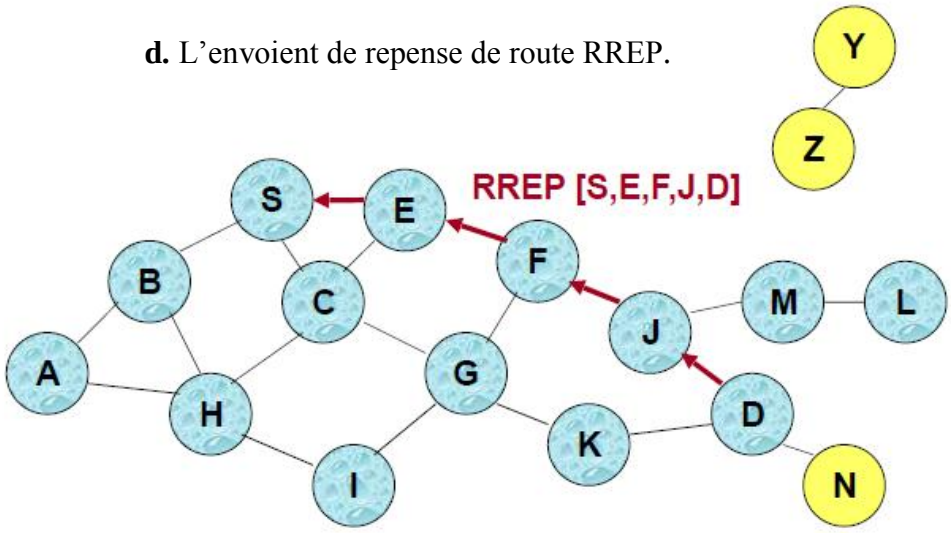


Figure 2.7 : Exemple de découverte de route dans le protocole DSR

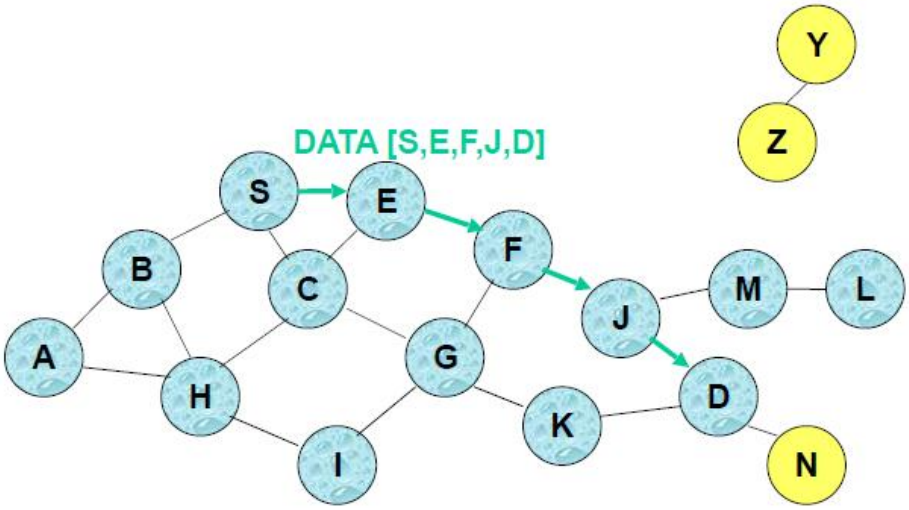


Figure 2.8 : L'acheminement de données dans le protocole DSR

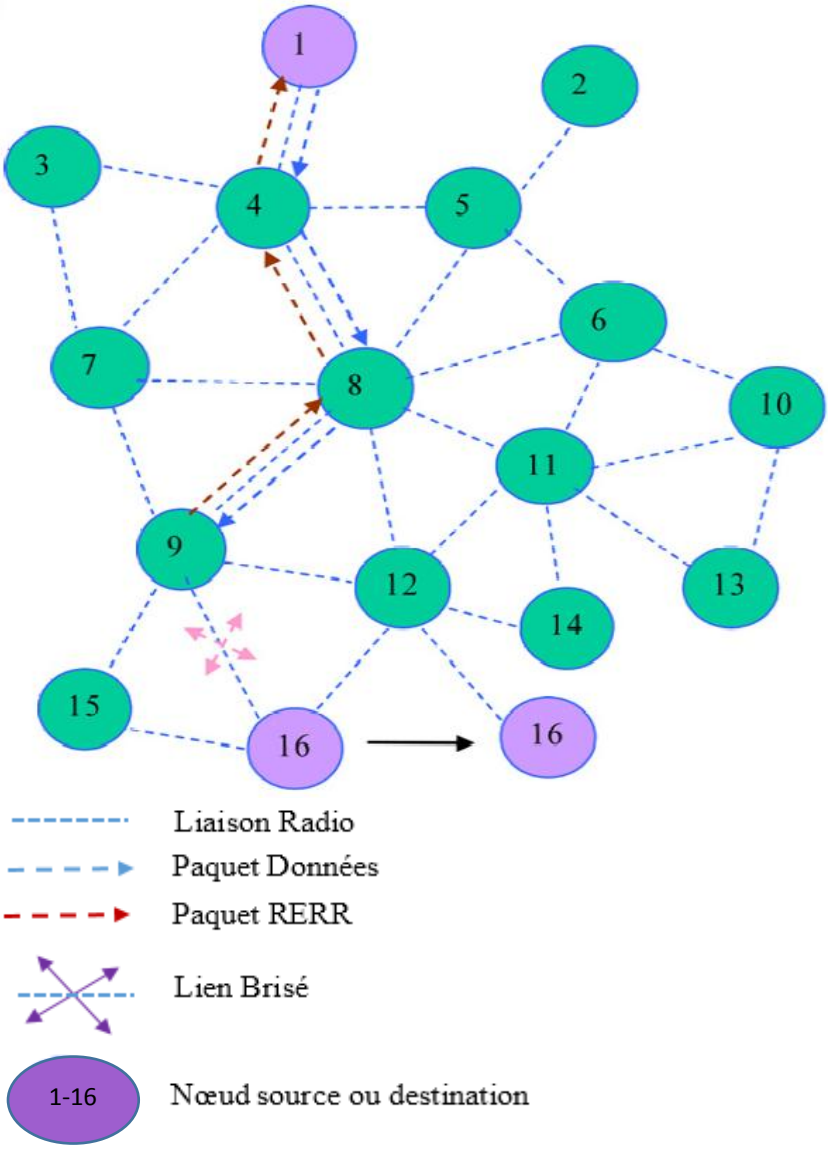


Table de routage de Nœud 1

Destination	Route
2	4-5
3	4-8-9-7
	4-8-12-9-7
.	.
.	.
.	.
.	.
.	.
.	.
.	.
.	.
.	.
.	.
16	4-3-7-9
	4-3-7-9-12
	4-3-7-9-15
	4-8-9
	4-8-9-15
	4-8-12
	4-5-6-11-12

Figure 2.9 : Exemple Maintenance des routes dans le protocole DSR

3.4.3. Les protocoles de routages Hybrides

Une troisième catégorie appelée les protocoles hybrides permet de combiner les deux concepts: celui des protocoles proactifs et celui des protocoles réactifs. Généralement, le réseau est divisé en deux zones et le principe est d'utiliser une approche proactive pour avoir des informations sur les voisins les plus proches, qui se trouvent au maximum à deux sauts du nœud mobile. Une approche réactive est utilisée au-delà de cette zone prédéfinie afin de chercher des routes.

L'avantage de cette troisième catégorie de protocoles est le fait qu'elle s'adapte bien aux réseaux de grandes tailles. Cependant, cette approche a comme inconvénient de cumuler les points faibles des protocoles réactifs et ceux des protocoles proactifs, tels que les messages de contrôle périodique et le coût d'établissement d'une nouvelle route. Il existe plusieurs protocoles connus appartenant à cette catégorie de protocoles hybride, citons ZRP (Zone Routing Protocol) et CBRP (Cluster Based Routing Protocol).

a. Le Protocole ZRP (Zone Routing Protocol)

Le protocole de routage hybride le plus répandu est le protocole ZRP (Zone Routing Protocol) [37] est un protocole de routage hybride. Ce protocole est basé sur la notion de découpage du réseau en deux zones. Chaque nœud définit autour de lui une zone de routage qui regroupe un ensemble de nœuds situés à distance limitée en nombre de sauts par rapport à ce nœud est appelée Intrazone. Les nœuds situés à la frontière de l'Inrazone (c.-à-d. ayant exactement la distance limite par la zone) sont appelés nœuds périphérique. La seconde zone est la zone extérieure à un nœud, appelée Interzone.

Pour déterminer le chemin pour joindre une destination, deux protocoles de routage vont être employés suivant la zone dans laquelle se trouve la destination. Ainsi, si la destination se situe dans l'Intrazone, le protocole de routage proactif **IARP** (Intrazone Routing Protocol) [38] est utilisé. Si la destination est extérieure à cette zone, le protocole de routage réactif **IERP** (Interzone Routing Protocol) [39] est employé.

Le protocole de routage IARP est basé sur un protocole à état de liens. Chaque nœud diffuse, périodiquement, sa connaissance de ses voisins. A l'aide des informations diffusées, les nœuds construisent la topologie et déterminent les routes vers les nœuds situés à proximité. Pour éviter que la diffusion des paquets de contrôle se propage sur la totalité du réseau, la source met le champ TTL à la valeur de H le nombre de saut maximum auquel se limite l'Intrazone. Chaque fois qu'un nœud reçoit un tel paquet, il met à jour sa table de routage puis décrémente de 1 le champ TTL du paquet. Si ce champ est égal à 0 le paquet est supprimé sinon il est propagé.

Le protocole IERP est un protocole de routage réactif, ce protocole est responsable uniquement des communications entre les différentes zones. La source détermine un ensemble de nœuds frontières à son

Intrazone. Elle utilise ces nœuds pour déterminer un chemin jusqu'à la destination, tout en réduisant le délai et le surcoût pris par la recherche. Lors de la réception de la requête de demande de création de route, les nœuds frontières ajoutent leur identifiant dans l'entête de la requête.
La recherche des chemins dans ZRP s'effectue de la manière suivante :

- Lorsqu'un nœud souhaite transmettre des paquets, il vérifie si le nœud destination se trouve dans sa « zone ».
- Si le nœud destination se trouve dans sa table de routage, alors les paquets sont transmis lance le protocole IARP.
- Sinon (le nœud destination est située en dehors de la « zone » du nœud source), il lance le protocole IERP. Ce dernier envoie une demande d'établissement de route « Route Request » à l'ensemble des nœuds périphériques de la zone.
- Si un nœud périphérique a connaissance de la route demandée, alors le nœud demandeur recevra de ce nœud un paquet « Route Replay » contenant le chemin menant à la destination. Dans le cas contraire, le protocole ce poursuit récursivement jusqu'à obtention d'une raiponce.

La figure 2.10 illustre le fonctionnement du protocole ZRP avec une zone de routage limitée à deux sauts

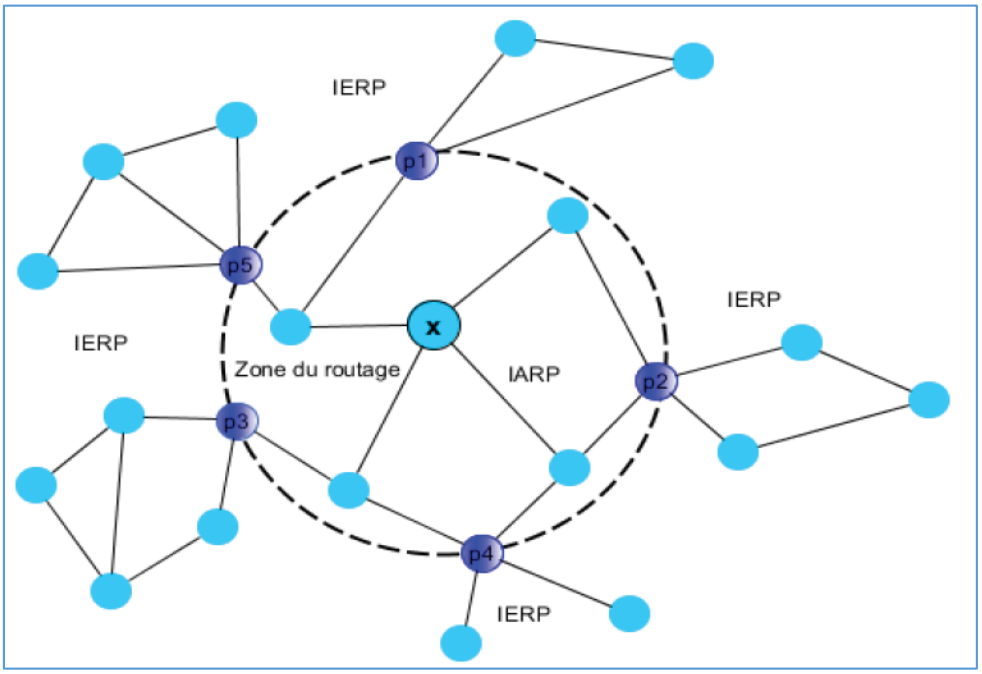


Figure 2.10 : Le principe de fonctionnement de ZRP

ZRP possède un troisième protocole interne appelé BRP (Bordercast Routing Protocol) [40] et dont le rôle est de définir les frontière des différentes « zones » et de construire des listes des nœuds périphériques aux différentes « zones » de routage.

L'avantage du protocole ZRP est qu'il réduit de manière significative le temps de transmission des paquets par rapport aux protocoles proactifs et réactifs purs. En effet, chaque nœud ne connait que la topologie de sa propre « zone » et non pas la totalité du réseau comme le cas des protocoles proactifs. En outre, l'emploi des nœuds périphérique facilite et optimise les opérations de découverte de routes mieux que dans les protocoles réactifs puisque chaque nœud périphérique qui reçoit une requête de recherche réactive peut indiquer immédiatement si la destination est dans son voisinage ou non, et par conséquent savoir s'il faut aiguiller la dite requête vers les autres zones sans « perturber » les nœuds de sa propre zone. L'inconvénient principal du protocole ZRP réside d'une part au niveau du calcul difficile des distances qui limite les zones, et d'autre part il doit supporter plusieurs types de protocoles internes et externes pour assurer la communication et l'envoi de paquets.

4. Conclusion

Le réseau Ad Hoc manifeste beaucoup de simplicité et assez d'avantages par rapport aux autres réseaux (filaires) par sa facilité de déploiement et son coût réduit.

L'étude effectuée sur les réseaux mobiles Ad Hoc nous permis de connaître leurs différentes caractéristiques (absence d'infrastructure, topologie dynamique, bandes passantes limitées…). Les MANETS exigent des contraintes additionnelles à celles des réseaux filaires.

Afin de satisfaire les besoins de toutes ces applications, de nouvelles fonctionnalités doivent être réalisées, plus particulièrement au niveau du routage de données et l'établissement de chemins corrects et efficaces soit un objectif important dans la conception des protocoles de routage pour les MANETS.

Dans le chapitre suivant, nous allons présenter le protocole de routage réactif (AODV) dans les réseaux MANETS.

CHAPITRE III

PRÉSENTATION DE PROTOCOLE AODV

1. Introduction

La performance d'un réseau est un élément fondamental et nécessaire pour une utilisation efficace d'applications, Le déploiement de telles applications dans les MANETS représente de nombreux intérêts.

Le routage dans les MANETS s'effectue en mode multi-sauts, des nœuds intermédiaires sont indispensables pour assurer la communication entre les nœuds sources et destinations qui ne résident pas dans la zone de transmission les uns des autres .Cependant on doit faire face à plusieurs défis et difficultés, et trouver des solutions fiables qui aident à trouver le chemin optimal entre deux nœud source et destination.

Dans ce chapitre, nous présentons les structures maintenues par chaque nœud exécutant AODV. Nous nous intéressons aussi à la structure des messages échangées entre les nœuds lors du processus de création et de maintien des routes.

2. Présentation de protocole AODV

Le protocole AODV (Ad Hoc On-Demand Distance-Vector) ou bien le routage avec vecteur de distance à la demande qui a été normalisé dans la RFC 3561[45], est un protocole réactif basé sur le principe des protocoles de routage à vecteur de distance. Il est à la fois capable de routage unicast et broadcast [46]. Il est pour l'essentiel une combinaison de DSDV [47] et de DSR [48]. Le protocole AODV minimise sensiblement le nombre de diffusions de messages en créant le chemin à la demande en plus du routage nœud à nœud et le principe des numéros de séquence comme dans le protocole de routage DSDV et emprunte, à DSR ses mécanismes de découverte et de maintenance des routes (Route Discovery et Route Maintenance). AODV il est libre de boucle, auto-démarrant et s'accommode d'un grand nombre de nœuds mobiles. Ce protocole de routage est peu gourmand en énergie et ne nécessite pas de grande puissance de calcul, il est donc facile à installer sur de petits équipements mobiles [49].

Le protocole AODV définit cinq types de messages distincts, ces messages sont la Route Request (RREQ), Route Reply (RREP), Route Error (RERR), le message Hello et le Data. Les quatre premiers messages sont reçus via le port UDP [50].

3. Table de routage et paquets de contrôle

3.1. Table de routage

La gestion d'une table de routage [51] [52] [53] [54] s'impose puisqu'il s'agit d'un protocole de routage. Les informations sur les routes doivent être conservées même pour les liaisons de courtes durées. La structure de cette table est présentée dans la Tableau 3.1.

@D	#SN	Valid_SN	State	Interface	#HC	@NH	PL	LT

Tableau 3.1 : Format de la table de routage

- @D : L'adresse IP de la destination.
- #SN (Sequence Number of destination) : Numéro de séquence de la destination.
- Valid_SND : Drapeau indiquant la validité du numéro de séquence.
- State : Drapeau indiquant l'état de l'entrée (par exemple : Valid, Invalid, repairable, being repaired).
- Interface : Interface réseau.
- #HC (Hop Count) : Nombre de saut nécessaires pour atteindre la destination.
- @NH (Next Hop) : Prochain saut en direction de la destination.
- PL (Precursor List) : Liste des précurseurs : c'est la liste des voisins auxquels une réponse de route est générée ou transféré.
- LT (Life Time) : Temps au-delà duquel la route expire ou est effacée.

3.2. Table d'historique (buffer)

Pour diminuer le nombre de messages qui circulent dans le réseau, AODV ne traite qu'une seule fois un message de demande de route. Ainsi, il garde trace des demandes de route déjà traitées en les stockant dans une structure appelée table d'historique (buffer) [55]. Donc, si un nœud reçoit de nouveau la même demande de route une seconde fois (ou une n^{énième} fois), il la jette.

Chaque entrée de la table d'historique est composé de :

- #ID : Identifiant de la demande de route RREQ.
- @S : Adresse de de source.
- LT : Temps au-delà duquel l'entrée sera effacée.

#ID	@S	LT

Tableau 3.2 : Format de la table d'historique (buffer)

3.3. Format de message demande de route *(RREQ Route Request)*

Le message demande de route RREQ [55] est diffusé lorsqu'un nœud détermine qu'il a besoin d'une route vers une destination et ne dispose pas d'une route disponible. C'est le cas lorsque la destination est inconnue ou lorsque une route précédemment valide dans sa table de routage expire ou est marquée invalide. Le nœud créé le paquet présenté dans le tableau 3.3. Il est constitué d'une trame de 24 octets :

Les quatre premiers octets sont constitués du champ Type sur 8 bits forcé à 1 indiquant qu'il s'agit d'un message RREQ. Les bits suivants : J, R, G, D, U décrits plus bas indiquent les différentes utilisations du message. Un champ Réservé sur 11 bits mis à 0 laisse la possibilité d'évolution ultérieure. Puis un champ de 8 bits indique le Nombre de Sauts.

Les quatre octets suivants portent l'Identification du Message RREQ. Les quatre suivants l'Adresse IP de la Destination. Les quatre suivants le Numéro de Séquence de la Destination. Les deux suivants l'Adresse IP de la Source. Les quatre derniers le Numéro de Séquence actuelle de la Source.

<table>
<tr><td colspan="8">1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 2122 23 24 25 26 27 28 29 30 31</td></tr>
<tr><td>Type =1</td><td>J</td><td>R</td><td>G</td><td>D</td><td>U</td><td>Reserved</td><td>Hop count</td></tr>
<tr><td colspan="8">RREQ ID</td></tr>
<tr><td colspan="8">Destination IP Address</td></tr>
<tr><td colspan="8">Destination Sequence Number</td></tr>
<tr><td colspan="8">Originator IP Address</td></tr>
<tr><td colspan="8">Originator Sequence Number</td></tr>
</table>

Tableau 3.3 : Format de trame de message de la demande de route (RREQ Route Request).

Le format du message de demande de route ***RREQ*** est illustré ci-dessus et contient les champs suivants :

Le champ Type : est identifié le Type du paquet de contrôle, qui est toujours 1 pour les messages RREQ.

- Le champ Type : 1.
- Le bit J : est positionné à 1 sur le message sortant en cas d'utilisation de multicast.
- Le bit R : est positionné à 1 sur le message retour en cas d'utilisation de multicast.
- Le bit G : Drapeau RREP gratuite, indique la nécessité de générer une réponse de route vers la destination. Une RREP de ce genre (*gratuitous*) est généré seulement lorsqu'il s'agit d'un nœud intermédiaire qui répond.
- Le bit D : Drapeau de destination seulement, indique que la destination seule peut répondre à cette demande de route RREQ.

- Le bit U : Numéro de séquence inconnue, indique que le numéro de séquence de la destination est inconnu.
- Reserved : mis à zéro lors de l'envoi et ignorés à la réception.
- Hop count : Le nombre de sauts à partir de l'adresse IP origine jusqu'au nœud de traitement de la demande (initialement mis à zéro au niveau du nœud source et incrémenté à chaque saut).
- RREQ ID : Un numéro de séquence identifiant de manière unique une demande de route (RREQ) lorsqu'il est associé à l'adresse de la source.
- Destination IP Address : Adresse IP de la destination à laquelle une route est demandée.
- Destination Sequence Number : Le dernier numéro de séquence connu pour la destination.
- Originator IP Address : Adresse IP de la source (nœud qui a initialisé la demande de route).
- Originator Sequence Number : Numéro de séquence actuel de la source qui sera associé à l'entrée de la table de routage dans les nœuds traitant le message RREQ.

3.4. Format de message réponse de route (RREP Route Reply)

Lorsqu'une demande de route atteint la destination ou un nœud ayant un chemin valide vers la destination, celui-ci génère une réponse de route RREP [55] qui sera envoyé en unicast d'un nœud à un autre jusqu'à atteindre la source. Le paquet de réponse de route est représenté par le tableau 3.4.

Le message RREP constitué d'une trame de 20 octets :

Les quatre premiers octets sont constitués du champ Type sur 8 bits forcé à 2 indiquant qu'il s'agit d'un message RREP. Les deux bits R et A décrits plus bas indiquent pour le premier qu'une route défectueuse est réparée, le deuxième pour sa part indique que ce message sera suivi d'un RREP-ACK. Puis 12 bits réservés pour évolution mis à 0 puis 5 bits de préfixe référençant le nœud pour les routages. Puis un champ de 8 bits indique le nombre de saut.

Les quatre octets suivants l'identification du message.

Les quatre suivants l'adresse IP de la destination.

Les quatre suivants le numéro de séquence de la destination. Les deux suivants l'adresse IP d'origine.

Les quatre derniers sont destinés à l'identification de la transaction par la source IP.

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31					
Type =2	J	R	Reserved	PrefixSz	Hop count
Destination IP Address					
Destination Sequence Number					
Originator IP Address					
Lifetime					

Tableau 3.4 : Format de trame de message de la réponse de route RREP (Route Reply**).**

Le format du message Réponse de route RREP est illustré ci-dessus et contient les champs suivants :

Le champ Type : est identifié le Type du paquet de contrôle, qui est toujours 2 pour les messages RREP.

- Le champ Type : 2.
- Le bit R : Utilisée pour le multicast.
- Le bit A : Accusé de réception requis.
- Reserved : mis à zéro lors de l'envoi et ignorés à la réception.
- Prefix Size : Si c'est différent de zéro, cela signifie que le prochain saut peut être utilisé pour n'importe quel nœud avec le même préfixe.
- Hop Count : Nombre de sauts de la destination de la RREQ au nœud en cours de traitement.
- Destination IP : Adresse IP de la destination à laquelle une route est demandée.
- Destination Sequence Number : Numéro de séquence de la destination.
- Originator IP Address : Adresse IP de la source, nœud qui a initialisé la demande de route RREQ.
- Lifetime : Temps en milli-secondes pour lequel les nœuds recevant la RREP considèrent la route valide.

3.5. Format de message Bonjour (HELLO)

Les messages HELLO [55] offrent des informations sur la connectivité. Ils sont utilisés par seulement les nœuds faisant partie d'une route active pour valider les connexions avec les voisins. Ainsi, à chaque intervalle (Hello_Interval), le nœud vérifie qu'il a diffusé au moins un message et s'il ne l'a pas fait, il envoie une réponse de route avec un TTL (Time To Live) égal à 1 : Il s'agit du message HELLO.

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31					
Type =2	J	R	Reserved	PrefixSz	Hop count = 0
Destination IP Address					
Destination SequenceNumber					
Originator IP Address					
Lifetime					

Tableau 3.5 : Format de trame de message Bonjour (HELLO***).***

À chaque fois qu'un nœud reçoit un message (HELLO ou autre) de son voisin X, il remet à zéro le compteur (delete_period). Mais, s'il ne reçoit rien et la période est écoulée, le nœud suppose que le lien avec ce voisin X est perdu.

3.6. Format de message erreur de route (RERR Route Error)

Une erreur de route [55] est envoyée à chaque fois que la rupture d'un lien rend inaccessible l'accès à une ou plusieurs destinations. Il est constitué d'une trame de 20 octets :

Les quatre premiers octets sont constitués du champ Type sur 8 bits forcé à 3 indiquant qu'il s'agit d'un message erreur de route RERR. Le bit N décrit plus bas indique qu'une route défectueuse est réparée.

Puis 15 bits réservés pour évolution mis à 0. Les 8 bits suivants indiquent le numéro de destination inaccessible.

Puis sur quatre octets l'adresse IP de destination inaccessible.

Les huit suivants indiquent si besoin le complément d'adresse.

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31			
Type =3	N	Reserved	Destination Count
Unreachable Destination IP Address (1)			
Unreachable Destination Sequence Number (1)			
Additional Unreachable Destination IP Address (if needed)			
Additional Unreachable Destination Sequence Number (if needed)			

Tableau 3.6 : Format de trame de message de de l'erreur de route (RERR Route Error)

Le format du message Route Error est illustré ci-dessus et contient les champs suivants :

- Le champ Type : est identifié le Type du paquet de contrôle, qui est toujours 3 pour les messages RERR.
- le bit N : Indicateur de non-suppression. Quand un nœud a effectué une réparation locale d'un lien. Les nœuds amont ne doivent pas supprimer la route.
- Reserved : Envoyé à 0, ignoré à la réception.
- Dest Count : Le nombre des destinations non joignables incluses dans le message. Cette valeur doit être au minimum 1.
- Unreachable Destination IP Address : L'adresse IP de la destination qui n'est plus accessible.
- Unreachable Destination Sequence Number : Le numéro de séquence de la destination (pris de la table de routage) dont l'adresse IP est juste au-dessus.

Le message RERR est envoyé chaque fois qu'une rupture de liaison provoque une ou plusieurs destinations à devenir inaccessible à partir de certains des voisins du nœud.

3.7. Format de message Accusé de réponse de route *(RREP-ACK Reply_Acknowledgment)*

L'accusé de réception (ACKnowledgment) doit être envoyé en réponse à une RREP dont le bit "A" est à 1. Ceci est utilisé lorsque le nœud craint l'existence d'un lien unidirectionnel empêchant l'achèvement du processus de découverte de route.

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15	
Type = 4	Reserved

Tableau 3.7 : Trame de message Accusé de réponse de route (RREP-ACK)

- Le champ Type : forcé à 4.
- Reserved : forcé à 0 ignoré à la réception.

4. Le maintien du numéro de séquence

Chaque table de routage doit inclure la dernière information sur le numéro de séquence pour l'adresse IP de la destination pour laquelle la table de routage est maintenue. Cette information est remise-à-jour si le nœud reçoit une nouvelle indication de changement du numéro de la séquence de la destination. L'indication se fait à travers les paquets reçus (RREQ, RREP et RRER). Une destination incrémente son propre numéro de séquence dans les deux cas suivants:

- Juste avant qu'un nœud ait entrepris une découverte de route.
- Juste avant qu'une destination ait généré une RREP en réponse à une RREQ. Le nœud doit remettre-à-jour son propre numéro de séquence au maximum entre le numéro de séquence actuel et celui contenu dans le paquet RREQ.

Un nœud peut changer le numéro de séquence dans la table d'entrée de la destination dans les cas suivants :

- Si ce nœud est la destination elle-même, ou
- si ce nœud reçoit un message AODV avec de nouvelles informations sur le numéro de séquence de la destination, ou
- si le chemin menant à cette destination arrive à expiration ou est rompu.

5. Principe de fonctionnement

Deux étapes sont observées : le premier est la découverte d'une route, et la deuxième est la maintenance des routes : [27] [55] [56]

5.1. Découverte de route [57]

Lorsqu'un nœud source veut établir une route vers une destination pour laquelle il ne possède pas encore de chemin, il diffuse en broadcast un paquet RREQ (Route Request). Cela peut arriver si la destination n'est pas connue au préalable, ou si le chemin existant vers la destination a expiré sa durée de vie ou il est devenu défaillant (i.e. la métrique qui lui est associée est infinie). Le champ numéro de séquence destination du paquet RREQ, contient la dernière valeur connue du numéro de séquence, associé au nœud destination. Cette valeur est recopiée de la table de routage. Si le numéro de séquence n'est pas connu, la valeur nulle sera prise par défaut. Le numéro de séquence source du paquet RREQ contient la valeur du numéro de séquence du nœud source. Après la diffusion du RREQ, la source attend le paquet réponse de route (RREP : Route Reply). Si ce dernier n'est pas reçu durant une certaine période (appelée RREP_WAIT_TIME), la source rediffuse le message RREQ et attend une période supérieure à la première. En l'absence de réponse RREP, ce processus peut être répété jusqu'à RREQ_RETRIES fois (par défaut RREQ_RETRIES = 5).A chaque nouvelle diffusion, le champ RREQ ID du paquet RREQ est incrémenté pour identifier une requête de route particulière associée à une adresse source. S'il n'y a toujours pas de réponse au bout des six tentatives, le processus de recherche de route est abandonné.

Un nœud recevant un paquet RREQ émettra alors un paquet réponse de route RREP s'il est la destination ou s'il possède une route vers la destination avec un numéro de séquence supérieur ou égal à celui du paquet RREQ sinon (nœud intermédiaire) il rediffuse le paquet RREQ. Quand un nœud intermédiaire envoie le paquet de la requête à un voisin, il sauvegarde aussi l'identificateur du nœud à

partir duquel la première copie de la requête est reçue. Cette information est utilisée pour construire le chemin inverse, qui sera traversé par le paquet réponse de route de manière unicast aussi bien que le cas où ils reçoivent un paquet RREQ qu'ils ont déjà traité, ils le suppriment. Puisque le paquet réponse de route RREP va être envoyé à la source, les nœuds appartenant au chemin de retour vont modifier leurs tables de routage suivant le chemin contenu dans le paquet de réponse (temps d'expiration, numéro de séquence et prochain saut). Afin de limiter le coût dans le réseau.

La destination renvoie un message RREP, ce message peut donc être acheminé vers la source. Chaque nœud traversé incrémentera le nombre de sauts. Et ajoutera une entrée à sa table pour la destination. Une réponse adéquate peut aussi être donnée par un nœud situé entre la source et la destination. Dans ce cas l'obtention de routes bidirectionnelles est néanmoins possible grâce au drapeau "Gratuitous RREP". Le nœud intermédiaire enverra alors en plus un RREP vers la destination. Les nœuds entre le nœud intermédiaire et la destination ajouteront donc à leur table une entrée vers la source du RREQ. Cette disposition permettra à la destination d'envoyer directement des paquets `à la source sans devoir procéder à la recherche d'une route. C'est utile lors de l'établissement de communications TCP pour l'envoi du premier RREP-ACK (accusé de réception de réponse à la route).

Une fois que la source a reçu les paquets RREP, elle peut commencer à émettre des paquets de données vers la destination. Si, ultérieurement, la source reçoit un RREP contenant un numéro de séquence supérieur ou égal, mais avec un nombre de sauts plus petits, elle mettra à jour son information de routage vers cette destination et commencera à utiliser la meilleure route.

5.2 Maintenance des routes [58]

Afin de maintenir des routes consistantes, une transmission périodique du message « HELLO » (qui est un RREP avec un TTL = 1) est effectuée aux voisins. Si trois messages « HELLO » ne sont pas reçus consécutivement à partir d'un nœud voisin, le lien en question est considéré défaillant. Les défaillances des liens sont, généralement, dues à la mobilité du réseau ad hoc. Quand un lien, reliant un nœud N avec le nœud qui le suit dans le chemin de routage, devient défaillant, le nœud N diffuse un paquet RERR, avec une valeur de numéro de séquence égale à l'ancienne valeur du paquet RREP incrémentée d'une, et une valeur infinie de la distance. Le paquet RERR est diffusé aux voisins actifs, jusqu'à ce qu'il arrive à la source. Une fois le paquet est reçu, la source peut initier le processus de la découverte de routes. L'AODV maintient les adresses des voisins à travers lesquels les paquets destinés à un certain nœud arrivent. Un voisin est considéré actif, pour une destination donnée, s'il délivre au moins un paquet de données sans dépasser une certaine période (appelée active timeout period). Une entrée de la table du routage est active, si elle est utilisée par un voisin actif. Le chemin reliant la source et la destination en passant par les entrées actives des tables de routage, est dit un chemin actif. Dans le cas de défaillances

de liens, toutes les entrées des tables de routage participantes dans le chemin actif et qui sont concernées par la défaillance sont supprimées. Cela est accompli par la diffusion d'un message d'erreur entre les nœuds actifs.

6. Avantages et inconvénients

6.1. Les avantage [59]

- il demande moins de bande passante,
- il performe mieux pour les réseaux de grande taille,
- il offre une convergence rapide quand la topologie du réseau change, car il évite la boucle de routage et il évite le problème de *«counting to infinity»* de Bellman Ford.

6.2. Les inconvénients [59]

- une seule requête *RREQ* peut générer plusieurs paquets *RREP* qui peuvent engendrer un nombre important de message de contrôle,
- les nœuds intermédiaires peuvent mener à des chemins incohérents; c'est le cas où le *SN* de la source n'a pas été mis à jour et que les nœuds intermédiaires possèdent des *SN* plus grands mais plus petits que le *SN* de la dernière destination.

7. Exemple de fonctionnement d'AODV

Puisque le nœud 1 ne sait pas où transmettre un message pour le nœud 4, il diffuse un paquet RREQ.

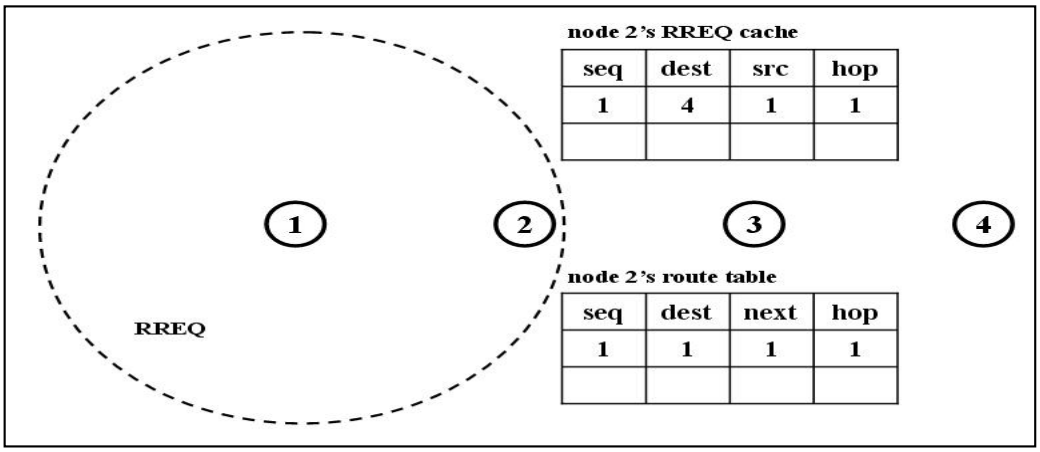


Figure 3.1 : Diffusion de message RREQ

Lors de la réception du paquet RREQ, le nœud 2 décode l'en-tête RREQ et stocke, dans la table cache RREQ, les informations telles que la séquence, la destination et l'adresse source. Ces informations sont utilisées pour empêcher la retransmission du même paquet RREQ.

Le nœud 2 insère les informations (séquence, destination, nœud de saut suivant, saut) de l'émetteur et la source du RREQ dans la table de route.

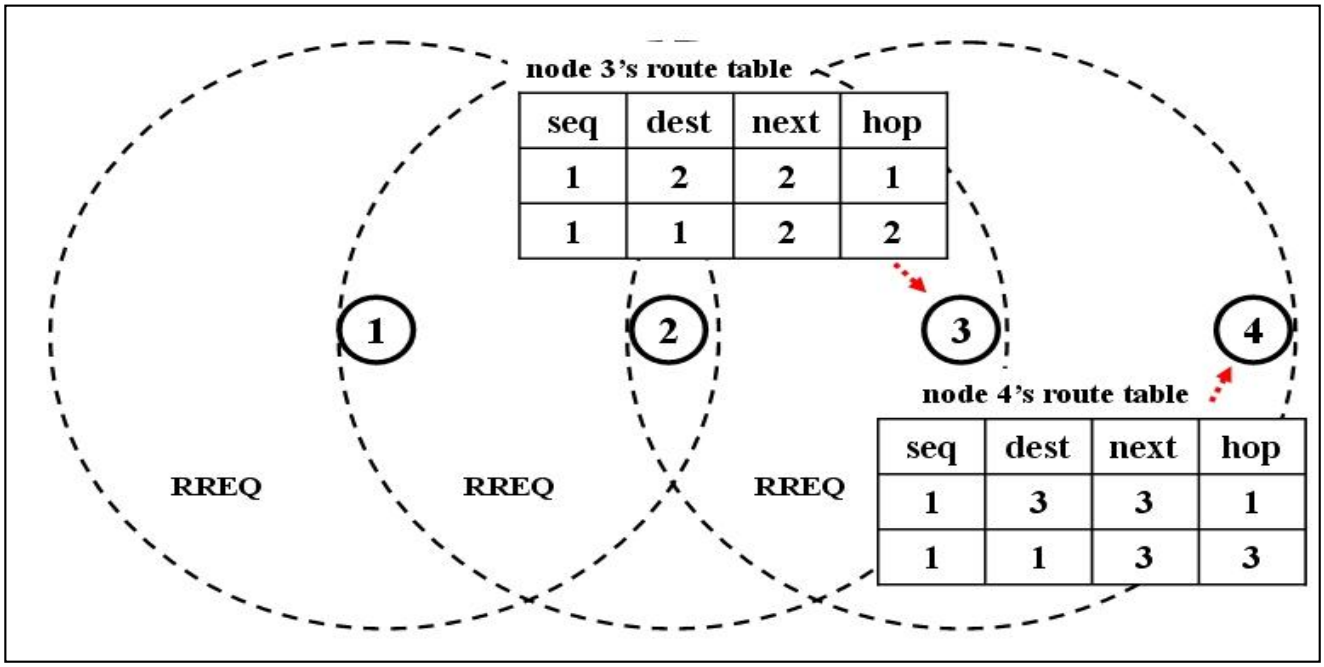


Figure 3.2 : Le RREQ est inondé dans tout le réseau.

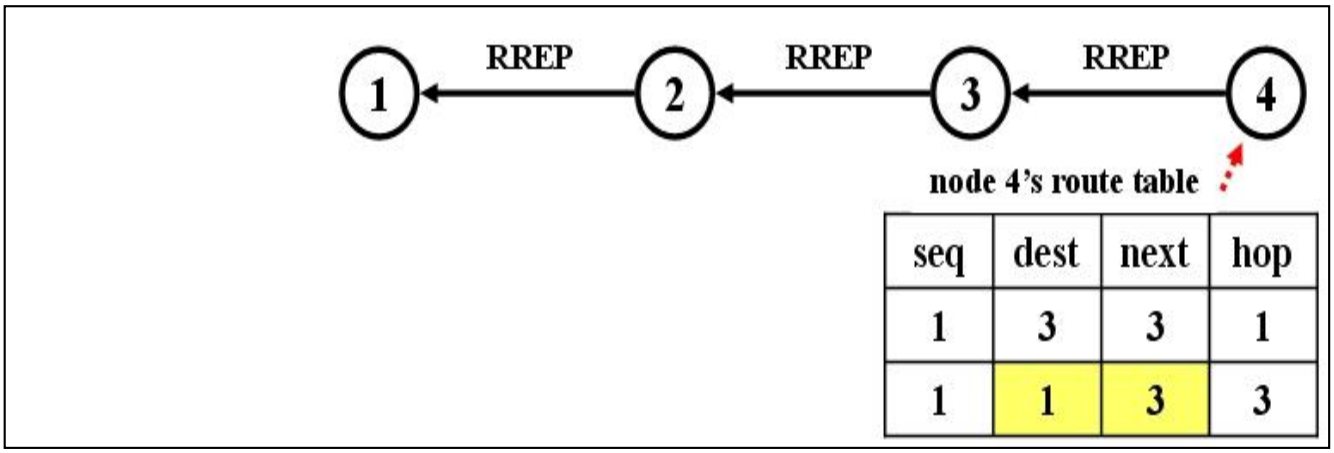


Figure 3.3 : La raiponce de route RREP

Lorsque le nœud 4 reçoit le RREQ, la route inverse est établi (4 jusqu'à 1) et le nœud 4 essaie d'envoyer la réponse de route (RREP) au nœud 1 (la source du RREQ).

Voir la figure ci-dessus. RREP est transmis au nœud 4, à cause des informations de nœud de saut suivantes dans la table de routage.

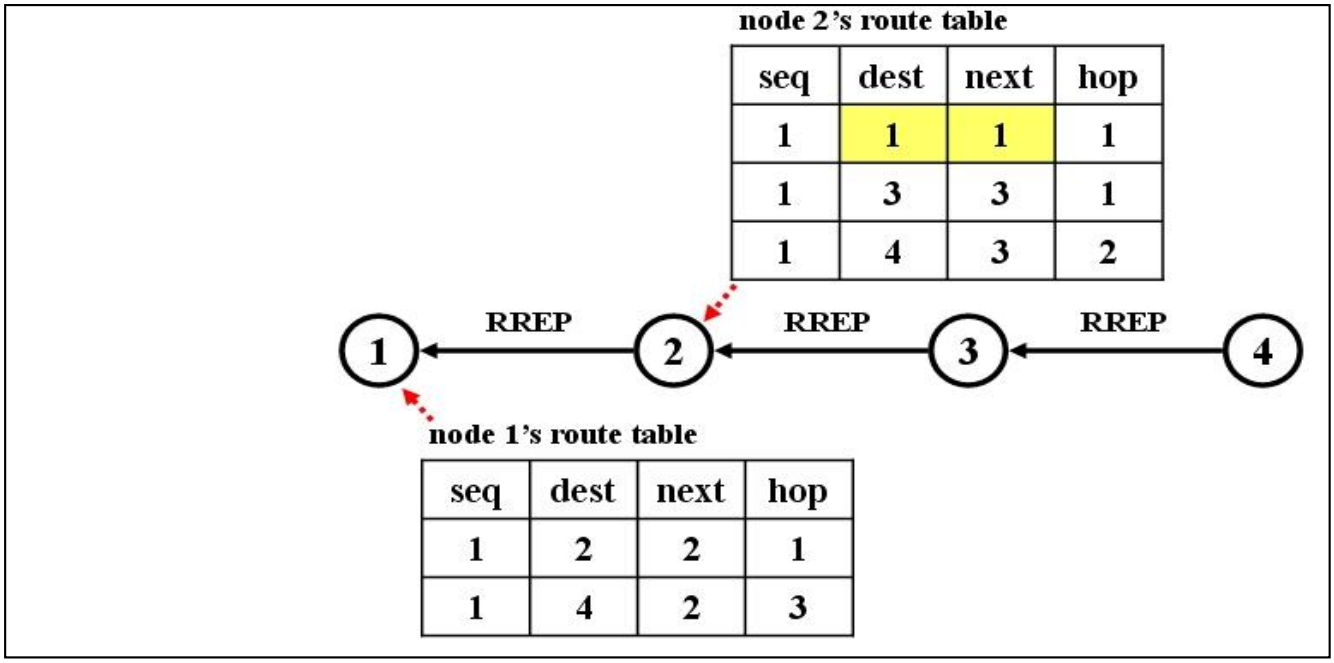


Figure 3.4 : Le RREP est envoyé en unicast

Pendant que le RREP transmet au nœud 1, la route aller (1 jusqu'à 4) est établie.

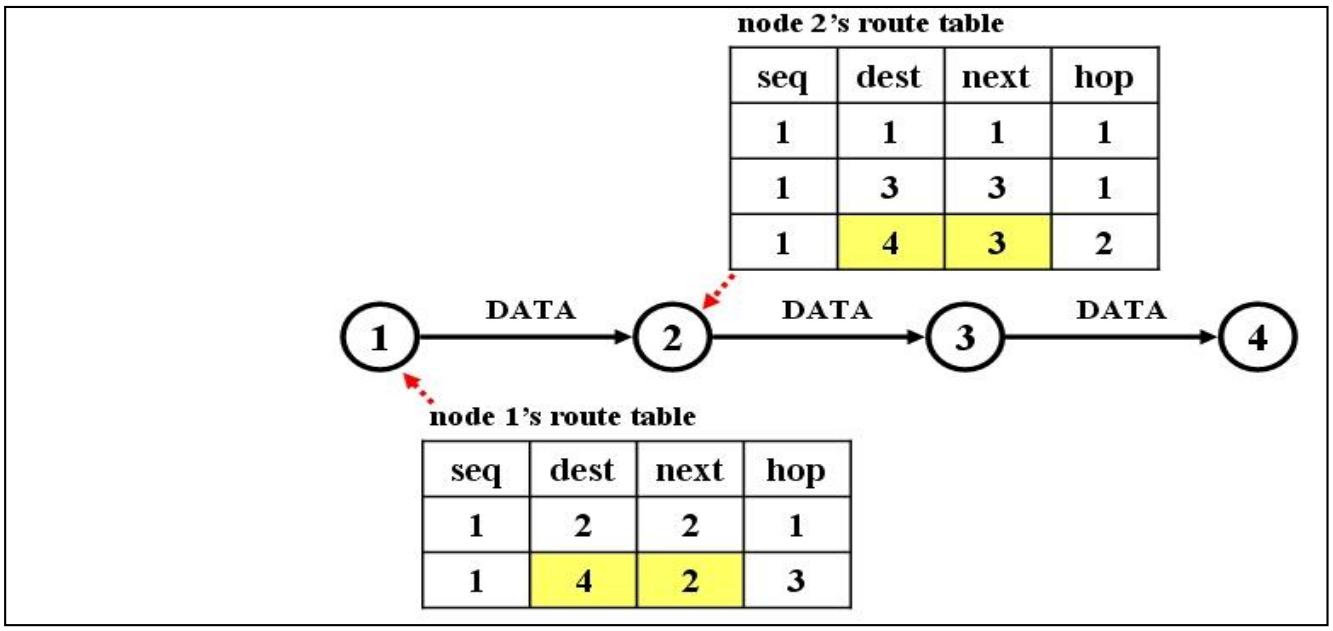


Figure 3.5 : La transmission de DATA

Ensuite, les messages de données peuvent être transmis du nœud 1 au nœud 4 par la route établi.

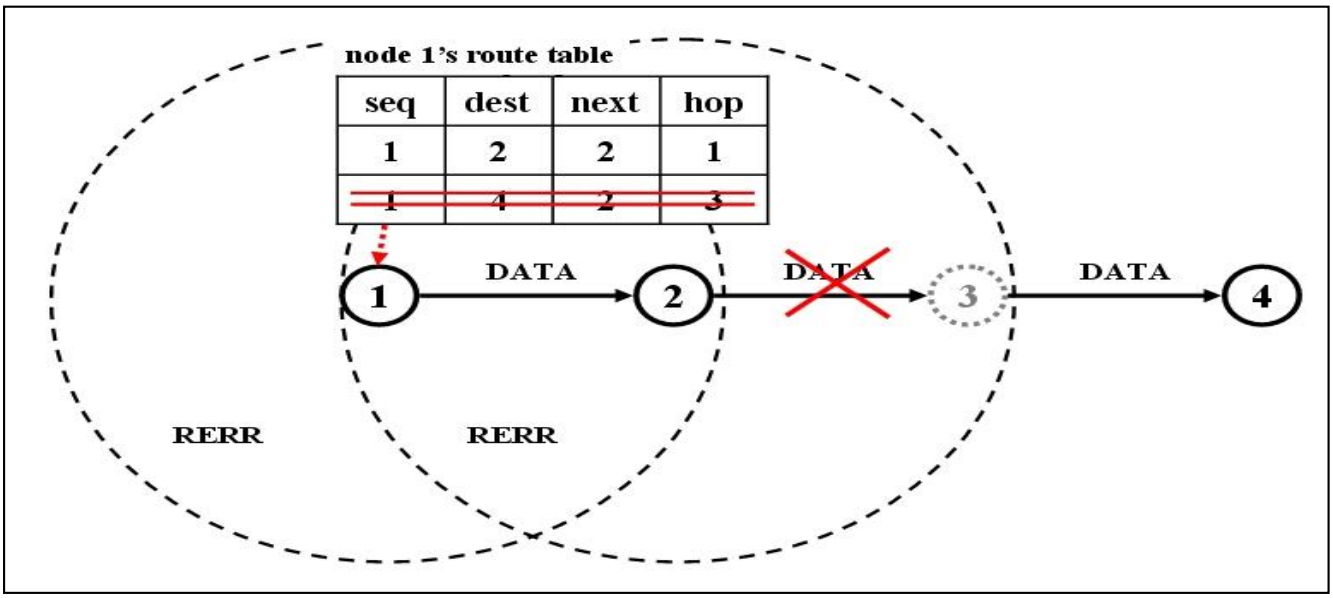


Figure 3.6 : La maintenance de route

Lorsque la transmission de données échoue plusieurs fois, le paquet d'erreur (RERR) est envoyé au nœud source.

Lors de la réception du RERR, un nœud supprime les informations de route, pour la paire source et destination, dans la table de route. Lorsque le nœud source reçoit le RERR, il redémarre la découverte route en diffusant un nouveau paquet RREQ.

8. Conclusion

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.

Dans le chapitre qui suit nous allons mettre le point sur la simulation et les simulateurs réseaux.

CHAPITRE IV

SIMULATION ET SIMULATEURS RÉSEAU

1. Introduction

L'exécution de vraies expériences sur un banc d'essai est coûteuse et difficile, de sorte que la simulation est souvent nécessaire dans la phase de conception du réseau avant la mise en œuvre effective. Il existe de nombreux outils de simulation différents pour WSN, tels que NS-2, TOSSIM, OMNeT ++, OPNET, GloMoSim, UWSim, Avrora, SENS, COOJA, Castalia, Shawn, EmStar, J-Sim, SENSE, etc.

Les méthodes de simulation, conçues pour être utilisées en statistique et en recherche opérationnelle, ont connu et connaissent encore un développement rapide dû à l'extraordinaire évolution des ordinateurs. Des applications se rencontrent tant dans l'industrie qu'en économie, ou encore en sciences sociales, en informatique et dans de nombreux autres domaines. Dans ce chapitre nous présenterons, en particulier le choix du simulateur et présentation de simulateur OPNET.

2. Simulation

2.1. Définition

Méthode de mesure et d'étude consistant à remplacer un phénomène, un système par un modèle plus simple mais ayant un comportement analogue. [60]

La simulation, selon Shannon (1975), est «le processus de conception d'un modèle de système réel et de réalisation d'expériences avec ce modèle afin de bien comprendre le comportement du système ou d'évaluer diverses stratégies (Dans les limites imposées par un critère ou ensemble de critères) pour l'exploitation du système ». [61]

2.2. Techniques de modélisation de simulation [62]

Pour bien comprendre ce qui constitue la simulation et comment ils peuvent être utilisés dans l'éducation, il faut avoir une compréhension des processus et des techniques utilisés pour produire et utiliser un modèle informatique d'un système (simulation). Un diagramme du processus impliqué dans la simulation et la modélisation est présenté ci-dessous à la figure 4.1.

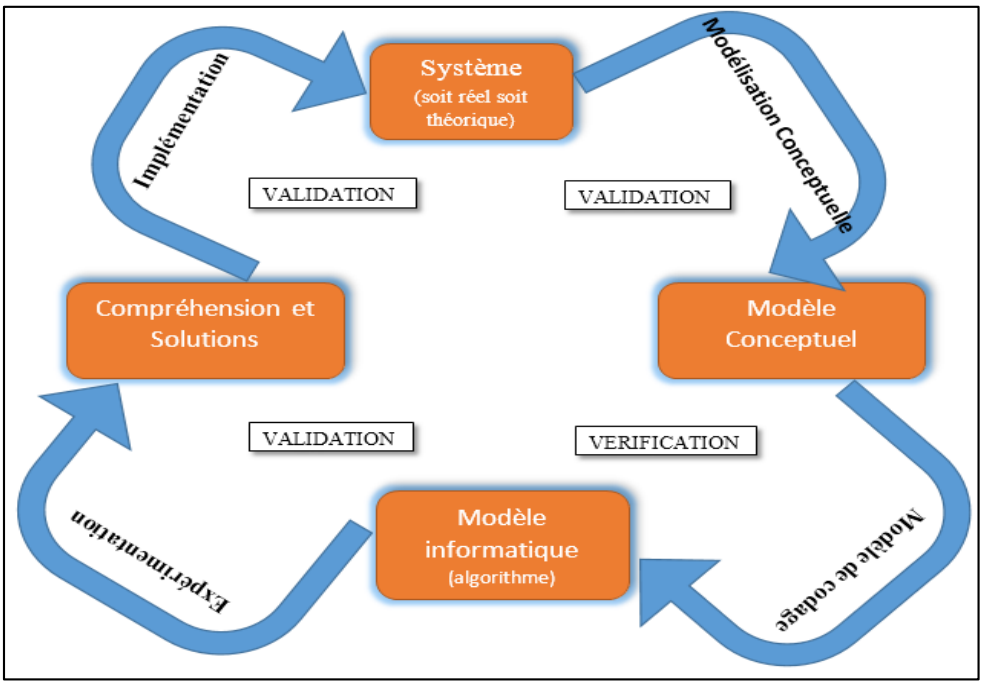


Figure 4.1 : Le processus de modélisation et de simulation

Le processus illustré dans le diagramme peut être appliqué à n'importe quel système soit réel soit théorique. L'objectif du processus de modélisation est de pouvoir prévoir et comprendre le comportement du système dans une gamme de conditions. Le système modélisé peut être dynamique et présenter un comportement qui évolue avec le temps ou être stable qui peut être perturbé en modifiant les paramètres du système.

2.2.1. Modélisation conceptuelle

La modélisation conceptuelle est le processus par lequel le modificateur définit une représentation simplifiée d'un système. Des approbations ou des simplifications (par exemple, ignorer la traînée et la rotation dans une simulation du mouvement du projectile) sont introduites pour réduire la complexité, les besoins informatiques ou le temps des solutions.

2.2.2. Modèle de codage

Au cours du codage, le modèle est converti en un algorithme pouvant être exécuté sur un ordinateur. L'algorithme informatique doit être vérifié pour s'assurer qu'il correspond au modèle et validé pour s'assurer que la sortie reflète le comportement du système. Il s'agit d'un processus itératif répété jusqu'à l'obtention d'un modèle suffisamment précis.

2.2.3. Expérimentation

Une fois que le modèle informatique est construit, le modélisateur expérimente le modèle pour résoudre les problèmes au sein du système et pour mieux comprendre le système.

2.2.4. Mise en œuvre

Après avoir obtenu une compréhension du système, des décisions peuvent être prises et des mesures prises qui affectent le système du monde réel. Le cycle de modélisation peut alors recommencer, car le système original est modifié par ces interventions.

2.3. Usages de la simulation

À l'heure actuelle, la plupart des utilisations de simulation appartiennent aux catégories suivantes:

2.3.1. Recherche

La recherche sur les simulations est importante pour explorer la précision et l'utilité des nouvelles techniques analytiques qui peuvent s'avérer utiles dans la conception et l'analyse; Cela implique la dérivation et la vérification des modèles de systèmes. Les simulations sont utilisées comme outils de recherche pour établir des tendances, démontrer les relations entre les paramètres du système ou faire des prédictions sur l'avenir.

2.3.2. Design

Les concepteurs utilisent des simulations pour caractériser ou visualiser un système qui n'existe pas encore pour obtenir une solution optimale. Par exemple, en utilisant la simulation pour modéliser une installation de fabrication pour expérimenter la mise en page de différentes machines à capacité et des bacs de stockage, des temps de préparation et de transfert de matériaux afin d'améliorer l'efficacité.

2.3.3. Analyse

L'analyse se réfère au processus par lequel la simulation est utilisée pour déterminer le comportement ou la capacité d'un système en cours d'opération ou pour vérifier son exactitude. Il peut également être utilisé pour tester les systèmes de la vie réelle dans des conditions extrêmes voire impossibles. Le comportement du modèle est établi par la collecte des données du système. Par exemple. Optimisant la gestion d'un hôpital, en simulant la programmation des médecins, du personnel, du matériel et des patients.

2.3.4. Formation

Les simulations de formation sont utilisées pour recréer des situations auxquelles les gens font face et permettre aux stagiaires de pratiquer une séquence d'actions ou d'apprendre la réponse correcte à un événement. La formation permet aux apprenants de commettre des erreurs potentiellement fatales sans blessure. Une très large gamme de formation peut être réalisée à l'aide de simulations, du très complexe qui utilise des matériels sur mesure (p. Ex. Simulateurs de vol ou maquettes de centrales nucléaires) à une formation plus simple disponible sur un PC de bureau (p. Ex. Formation en informatique).

2.3.5. Éducation

Dans l'éducation, les apprenants ne doivent pas seulement savoir "comment" faire quelque chose; Ils doivent savoir "pourquoi". Les simulations représentent un monde exploratoire où les élèves peuvent utiliser des modèles pour expérimenter, créer et tester des hypothèses et construire leur propre compréhension d'un système. Les simulations peuvent fournir des outils aux enseignants pour démontrer et expliquer le comportement de systèmes complexes et dynamiques. Potentiellement, toute simulation peut être utilisée dans l'éducation à un niveau ou à un autre.

2.3.6. Simulation de réseau

La simulation des réseaux est une technique par laquelle un logiciel (simulateur) modélise le comportement d'un réseau, soit par le calcul de l'interaction entre les entités du réseau en utilisant des formules mathématiques, ou en capturant et reproduisant des observations à partir d'un réseau réel.

2.4. Avantages et inconvénients de la simulation

2.4.1. Avantages: [63]

- Peut analyser des problèmes grands et complexes du monde réel pour lesquels il n'existe aucune solution analytique en forme fermée.
- Peut inclure des complications du monde réel que la plupart des autres techniques ne peuvent pas.
- Permet la "compression du temps".
- N'interfère pas avec le système réel
- Observations des états du système.
- Etudes des points de fonctionnement d'un système.
- Etude d'un système sans les contraintes matérielle.

2.4.2. Inconvénients: [63]

- Peut-être coûteux et prend du temps
- Ne produit pas une solution optimale
- Nécessite un bon apport de gestion
- Les résultats ne sont pas généralisables à d'autres situations

3. SIMULATEUR [64]

Nous appelons simulateur un programme qui met en œuvre un modèle de simulation. La première tâche d'un simulateur est d'assurer que la chronologie des évènements soit respectée.
A chaque occurrence d'un évènement, les actions qui sont associées à celui-ci sont exécutées.

3.1 Choix de simulateur [65]

Au cours de cette recherche sur le choix du simulateur réseau, nous avons été amenés à définir une grille d'analyse fonctionnelle d'un simulateur pour argumenter notre choix et permettant de proposer une implémentation d'un simulateur. Pour ce faire, nous avions dressé une liste des simulateurs de réseau les plus populaires utilisées et en termine par la sélection d'un outil parmi eux.

Les Outils / *Les Critères*	**NS2**	**GloMo-Sim**	**J-Sim**	**OMNet++**	**OPNet**	**QualNet**
Applicabilité	Net/Sys	Net/Sys	Net	Net/Sys	Net/Sys	Net/Sys
Les Modules disponibles	T/W/Ad/ WSNA	T/W/Ad	T/W/Ad/ WSNA	T/W/Ad	T/W/Ad/ WSNA	T/W/Ad/ WSNA
Mobilité	Supporté	Supporté	Supporté	Non	Supporté	Supporté
Interface graphique	Nom	Limité	Bien	Très bien	Excellent	Très bien
Parallélisme	Non	SMP/Beowulf	RMI-based	MPI/PVM	Oui	SMP/Beowulf
Licence	Open Source	Open Source	Open Source	Gratuit pour l'utilisation Académique	Commercial + Licence académique Gratuit pour l'utilisation limitée	Commercial
Évolutivité	Petit	Large	Petit	Large	Moyenne	Très large
Documentation	Excellent	Pauvre	Pauvre	Bien	Excellent	Bien
Extension	Excellent	Excellent	Excellent	Excellent	Excellent	Excellent

Tableau 4.1 : Comparaison entre différents simulateurs réseaux

On déclarant les abréviations utilise suivant :

Net : Network, Sys : System.

T : Les modèles traditionnelles (eg. TCP/IP, Ethernet).

W : Wireless Support (eg. Propagation model, IEEE 802.11).

Ad : Ad-Hoc Support (eg. AODV, DSR).

WSN : Wireless Sensor Networks Support (eg. S-MAC, Direct Diffusion).

WSNA : Advance Wireless Sensor Networks Support (eg. Zigbee, Energy Model).

Pour choisir l'outil adéquat nous avons utilisé la méthode « Making a Decision By Weighing Up Different Factors » [66]. On résume les étapes de cette méthode dans les paragraphes sous dessous suivant :

- On prépare une liste des options que on va choisir une parmi celle, et on les place en colonnes d'une table, et une liste des facteurs que nous devons considérer dans les lignes. Ensuite on va évaluer chaque option/facteur association par une note comprise entre 0 (faible) et 5 (très bon).
- La prochaine étape est de travailler sur l'importance relative aux facteurs dans notre décision. On va allouer à chaque facteur un coefficient de 0à 5, où 0signifie que le facteur est absolument négligeable dans la décision finale, et 5signifie qu'il est très important. (Il est parfaitement acceptable d'avoir des facteurs ayant la même importance)
- Ensuite, on va multiplier chaque option/facteur par le coefficient du facteur associe, Cela donne un score pondéré pour chaque option/facteur combinaison.
- En fin, on va additionner ces scores pondérés pour chacun des options. L'option qui a obtenu le plus grand nombre gagne, et elle doit être sélectionnée.

Dans notre cas la liste des options est : [NS2, GloMo-Sim, J-Sim, OMNet++, OPNet, QualNet] ce sont les simulateurs réseaux qu'on va choisir un parmi eux, el la liste des facteurs est : [applicabilité, Les modules disponibles, la mobilité, L'interface graphique, Contrat, Evolutivité, parallélisme, la documentation, extensibilité]. On applique la méthode précédant sur ces donnes et on a le résultat suivant :

	Coefficient	NS-2	GloMo-Sim	J-Sim	OMNet++	OPNet	QualNet
Applicabilité	5	5	5	2,5	5	5	5
Les modules disponibles	4	5	3	5	3	4	5
Mobilité	4	5	5	5	0	5	5
Interface graphique	5	1	2	3	4	5	4
Parallélisme	3	0	3	2	3	5	3
Contrat	4	5	5	5	4	3	1
Evolutivité	3	2	4	2	4	3	5
Documentation	5	5	1	1	3	5	3
Extensibilité	4	5	5	5	5	5	5
Total	37	141	133	124,5	129	167	148

Tableau 4.2 : Grille d'analyse d'un simulateur

3.2 Le simulateur retenu

Après avoir analysé et comparé plusieurs simulateurs disponibles, et après le résultat obtenu dans le tableau 4.2, notre choix de simulateur d'implémentation c'est porté sur le simulateur OPNET (Optimized Network Engineering Tools), Ce choix est motivé par ces propriété qu'on à vue dans le tableau 4.1 tel que l'interface graphique et la mobilité …

4. Présentation du Simulateur OPNET

OPNET (OPtimized Network Engineering Tools) [65] Modeler est un simulateur de réseau à événements discrets, a été proposé premièrement par Massachusetts Institute of Technology (MIT) en 1986 et commercialisé en 1987 comme le premier simulateur de réseaux et écrit en langage C++. Il est bien établi et une suite commerciale professionnelle pour la simulation de réseau. Actuellement, il est l'environnement de simulation commercial le plus largement utilisé. Toutefois, il peut être utilisé gratuitement par les chercheurs s'appliquant aux programmes d'université. Contrairement NS-2 et GloMoSim, OPNET soutient l'utilisation de la modélisation de réseau différent et matériel spécifique, comme lien physique émetteurs-récepteurs et d'antennes.

OPNET modeler dispose d'un environnement de développement interactif permettant la conception et l'étude des réseaux, des dispositifs, des protocoles et des applications. Pour ce faire, une longue liste de protocoles est supportée. En particulier, les protocoles MAC comprennent (wifi) IEEE 802.11a/b/g et ceux de Bluetooth. OPNET peut également être utilisé pour définir les formats de paquets personnalisés. Le simulateur aide les utilisateurs au développement des différents modèles par le biais d'une interface graphique. L'interface peut également être utilisée pour modèle, graphe, et d'animer le résultat obtenu. Une des caractéristiques les plus intéressantes d'OPNET est sa capacité à exécuter et suivre plusieurs scénarios d'une manière simultanée. Cependant, OPNET souffre également des mêmes problèmes d'évolutivité orienté objet comme NS2. OPNET Modeler fonctionne sur Windows XP/2K, Windows 7, Windows 8, Linux et Solaris.

OPNET présente une très bonne interface graphique relativement complète avec une librairie suffisamment fournie pour une très large gamme d'utilisation et d'application. Evidemment, l'éditeur graphique de ce simulateur ou GUI (Graphic User Interface) nous permet, entre autre, de construire différentes topologies et architectures de réseaux pour différentes applications et avec différents protocoles. [65]

4.1. Fonctionnement

OPNET est fonctionné en quatre étapes, proposer du modèle, spécification des statistiques, exécution de la simulation, obtenu les résultats. Si les résultats ne sont pas corrects il faut retourner à la première étape et fait les corrections du modèle puis continue les autres étapes. La figure 4.2 représente le fonctionnement général d'OPNET.

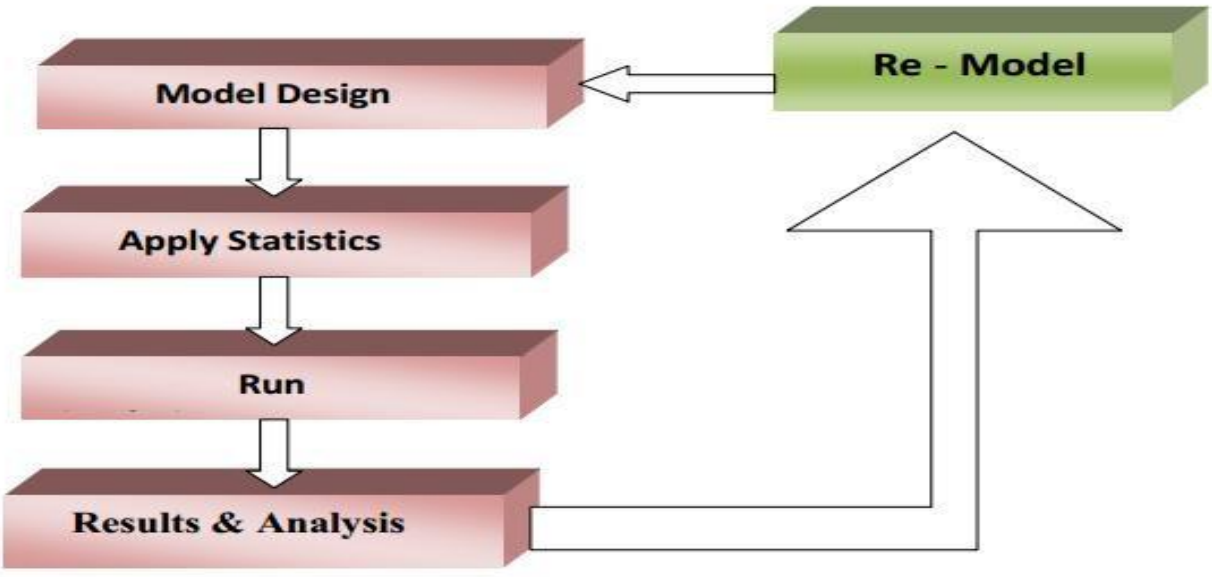


Figure 4.2 : Fonctionnement d'OPNET

4.2. Caractéristiques:[65]

- Lot de bibliothèque de composants avec code.
- Fournit un support pour des simulations sans fil évolutives.
- Il fournit un modèle hiérarchique.
- Fournir un noyau de simulation 32 et 64 bits.
- Diverses simulations comme événement discret, analytique et hybride sont fournies.

4.3 Préparation de l'Environnement d'Implémentation

La préparation de l'environnement d'implémentation consiste à installer le simulateur de réseau OPNET sous le système d'exploitation Windows 7. Nous avons utilisé la version académique d'OPNET 14.5. Avons l'installation d'OPNET on a besoin d'installer Microsoft Visual Studio10.

L'installation d'OPNET s'effectue sur les étapes suivantes :

Ajouter les variables suivant dans le variable d'environnement du système.

Nom de variable	Valeur de variable
DevEnvDir	C:\Program Files\Microsoft Visual Studio10\Common7\IDE ;
Framework35Version	v3.5
FrameworkDir :	C:\Windows\Microsoft.NET\Framework ;
FrameworkSDKDir :	v2.0.50727 ;
Include	C:\Program Files\Microsoft Visual Studio10\VC\atlmfc\include ; C:\Program Files\Microsoft Visual Studio10\VC\include ; C:\Program Files\Microsoft SDKs\Windows\v7.0A\include\
LIB	C:\Program Files\Microsoft Visual Studio10\VC\atlmfc\lib\ ; C:\Program Files\Microsoft Visual Studio10 \VC\lib\;C:\Program Files\Microsoft SDKs\Windows\v7.0A\lib\
LIBPATH	C:\Windows\Microsoft.NET\Framework\v3.5\;C:\Windows\Microsoft.NET\Framework\v2.0.50727\;C:\Program Files\Microsoft Visual Studio10\VC\atlmfc\lib\ ; C:\Program Files\Microsoft Visual Studio 10\VC\lib\

Path	C:\Program Files\Microsoft Visual Studio10\VC\bin;C:\Windows\Microsoft.NET\Framework\v3.5\;C:\Windows\Microsoft.NET\Framework\v2.0.50727\;C:\Program Files\Microsoft Visual Studio10\VC\vcpackages\ ; C:\Program Files\Microsoft Visual Studio10\Common7\IDE\ ; C:\Program Files\Microsoft Visual Studio 10\Common7\Tools\ ; C:\Program Files\Microsoft SDKs\Windows\v7.0A\Bin\ ;
VCINSTALLDIR	C:\Program Files\Microsoft Visual Studio 10\VC\
VS100COMNTOOLS	C:\Program Files\Microsoft Visual Studio 10\Common7\Tools
VSINSTALLDIR	C:\Program Files\Microsoft Visual Studio10\
WindowsSdkDir	C:\Program Files\Microsoft SDKs\Windows\v7.0A\

Tableau 4.3 : Variables d'environnement d'OPNET

Le logiciel OPNET contient trois fichiers exécutables OPNET Modeler.exe, OPNET Modeler_docs.exe et OPNET Modeler_library.exe. On commence par installer l'un après l'autre respectivement.

Avant d'exécute OPNET il faut d'abord lancer License maker.exe, puis on clique sur OK pour générer (file License) dans la partition C, cela pour la version académique seulement, donc il faut lancer OPNET Modeler en tant que administrateur.

(a) version académique. **(b) version commerciale.**

Figure 4.3 : Les versions du simulateur OPNET.

4.4 La structure d'OPNET : [68]

OPNET Modeler fournit de nombreux modèles et outils pour la modélisation, la simulation et l'analyse des performances des réseaux. OPNET Modeler comprend un environnement de modélisation graphique et un menu permettant d'accéder aux fonctionnalités du simulateur ainsi qu'à des modules optionnels (figure 4.4).Une documentation complète décrivant tous les modules, les concepts clés relatifs à chaque modèle ainsi que les fonctions, les variables et les valeurs utilisables pour les différents paramètres est accessible en local (Help).

La modélisation du réseau se construit de façon hiérarchique. Il existe 3 niveaux hiérarchiques dans OPNET.

- Le domaine réseau « Network domain»
- Le domaine de nœud « Node domain »
- Le domaine de processus « Process domain »

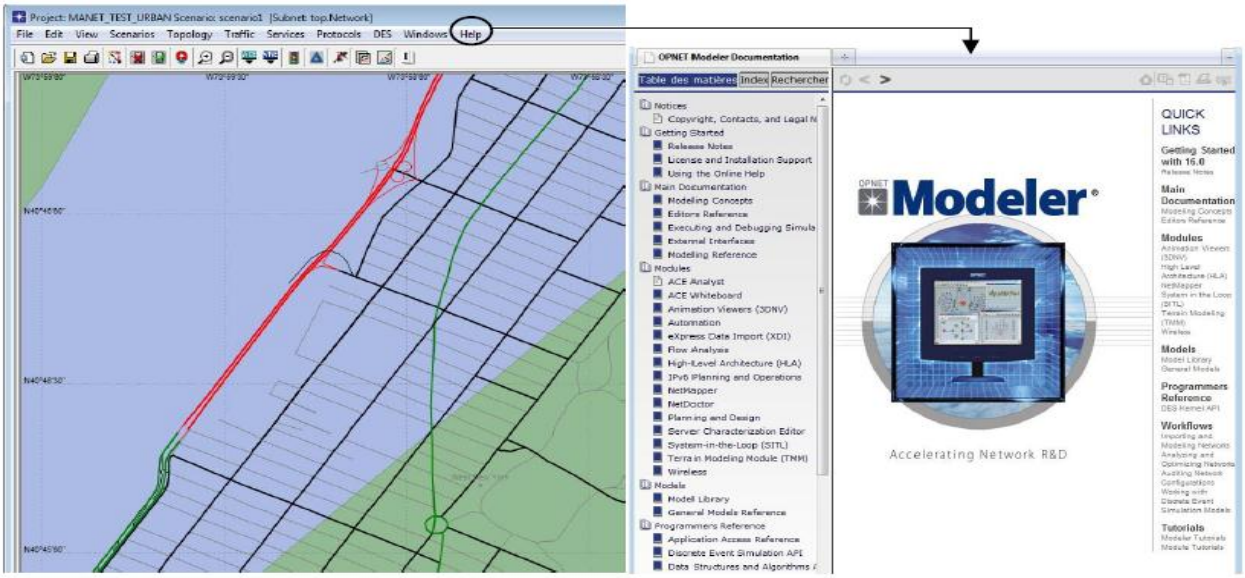


Figure 4.4 : Interface du OPNET Modeler 14.5 et module d'aide à l'utilisateur

4.4.1. Le domaine réseau « Network domain»

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

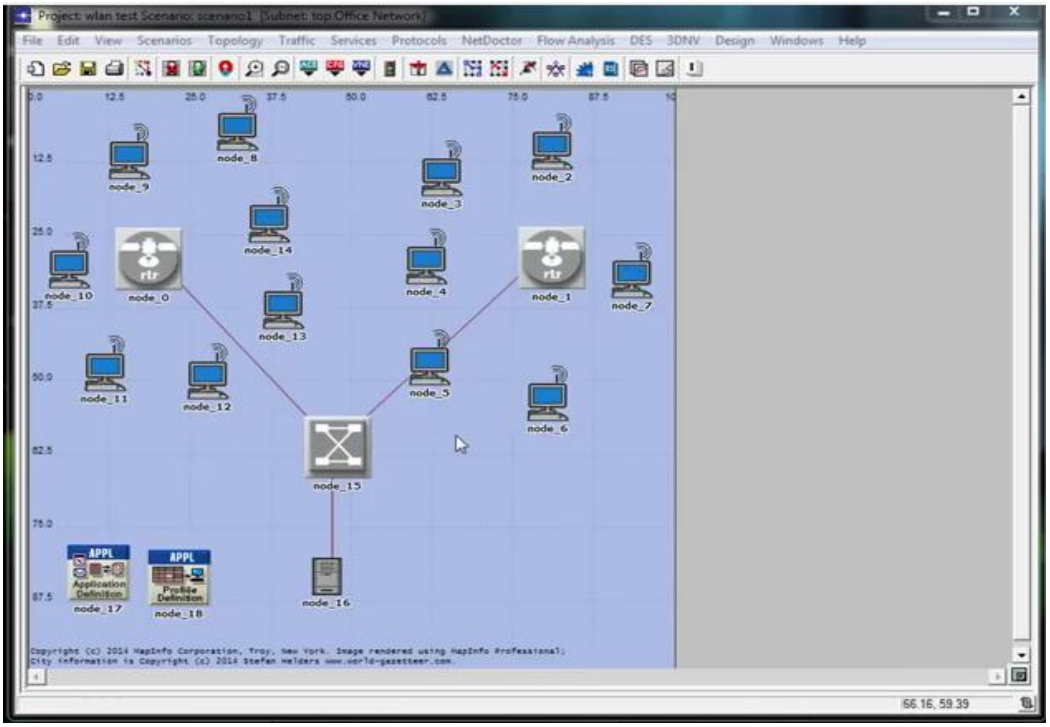


Figure 4.5 : Un réseau sans fil modélisé sous OPNET Modeler

4.4.2. Le domaine de nœud « Node domain »

Le domaine de nœud (Node domain) permet de définir la constitution des nœuds (routeurs, stations de travail, hub, …). Le Node domain montre l'organisation des différentes machines à état et la façon dont ils communiquent via des bus. Le Node domain permet de mettre en œuvre divers objets de type « générateur de paquets », « Queue », « émetteur point à point », « bus », etc… On peut concevoir ses propres objets au niveau **Process domain**.

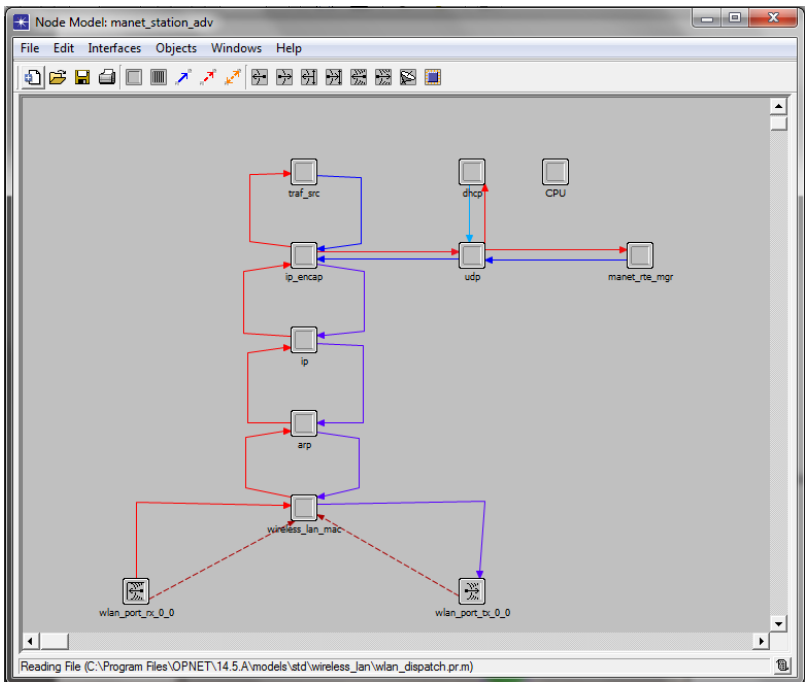


Figure 4.6 : Node domain

4.4.3. Le domaine de processus « Process domain »

La définition de chaque module programmable se fait à ce niveau. Un processus, ou process, est représenté comme une machine à états. Chaque état peut être dans l'état ouvert (couleur verte) ou fermé (couleur rouge). L'entrée dans un état ouvert est immédiatement et automatiquement suivie de la sortie de cet état. Par contre on ne sort d'un état fermé que lorsqu'il advient un événement. Un événement provoque le passage d'un état à un autre.

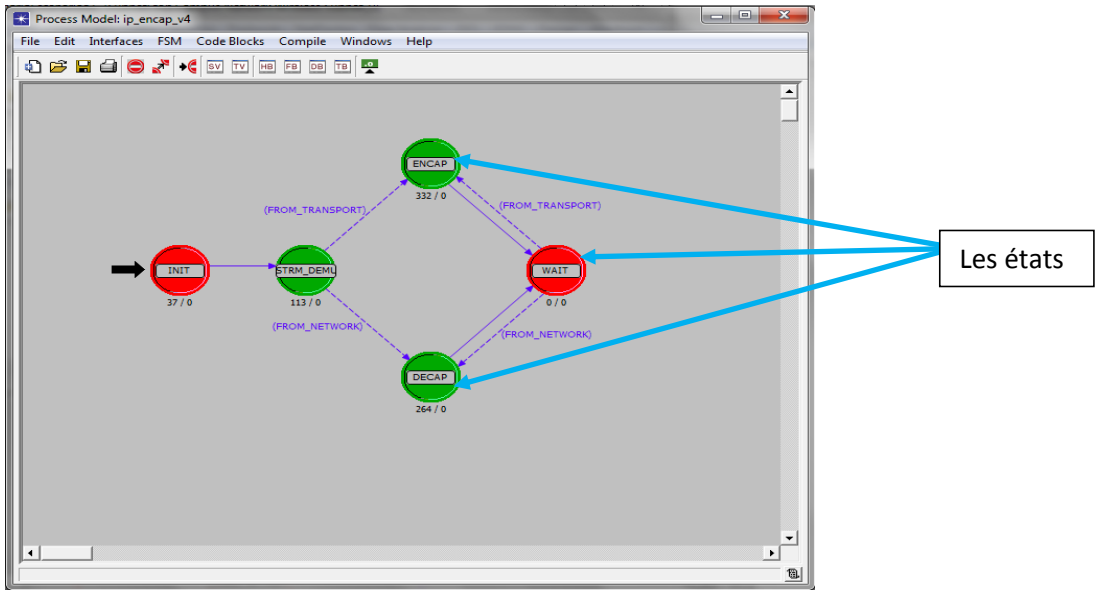


Figure 4.7 : Process domain

4.5 Exemple de déploiement d'un réseau sans-fil ad hoc

Pour utiliser l'assistant de démarrage pour configurer un nouveau scénario, procédez comme suit:

1- Sélectionner **File** puis **New**....
2- Sélectionner Project dans le menu déroulant et en clique sur **OK**
3- Nommer le projet et le scénario, comme suit:

Le nom du projet « ***Projet_MANET*** »

Le nom du scenario « ***Scenario1*** » puis en clique sur **OK**

L'assistant de démarrage s'ouvre.

4- Entrez les valeurs indiquées dans le tableau suivant dans les boîtes de dialogue de l'assistant de
5- démarrage:

Nom de boîte de dialogue	Valeur
1. Initial Topology	Sélectionnez la valeur par défaut: **CreateEmpty Scenario.**
2. Choose Network Scale	Sélectionnez **Office**. Cochez la case **Use MetricUnits**.
3. Specify Size	Sélectionnez la taille par défaut: **100 m x 100 m**
4. Select Technologies	Incluez la famille de modèles **MANET**.
5. Review	Vérifiez les valeurs, puis cliquez sur **Finish**

Tableau 4.4 : valeur de déploiement d'un réseau sans-fil ad hoc

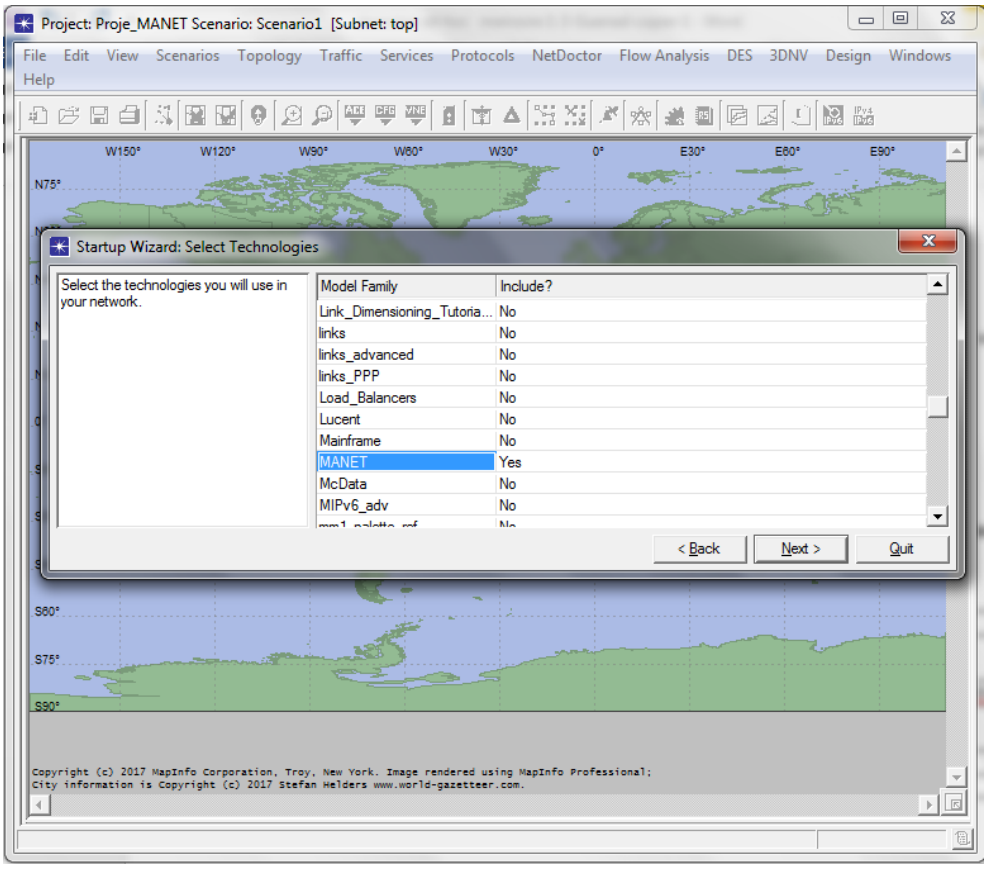


Figure 4.8 : La sélection de la technologie MANET

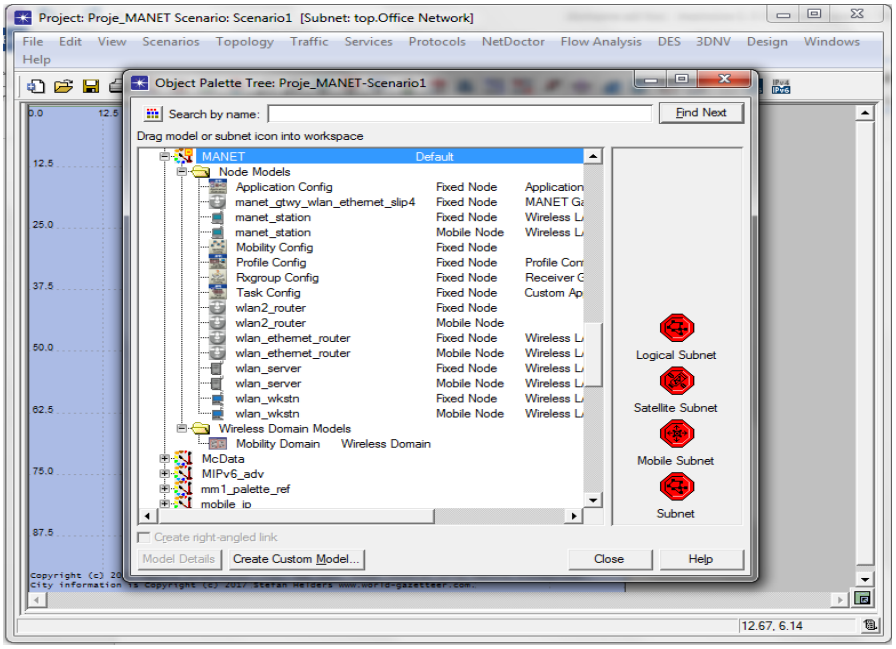


Figure 4.9 : La Palette des objets

Le menu Topology permet d'accéder à un Assistant de déploiement de réseau sans fil aussi bien en mode Infrastructure qu'en mode Ad hoc. L'utilisateur définit l'espace de déploiement qui peut être un lieu géographique réel, ou un espace logique non rattaché à un lieu géographique particulier. Après avoir défini les dimensions et la surface couverte par les nœuds, il détermine la technologie utilisée ainsi que le protocole de routage. Une fois le nombre de nœuds, leur disposition et leur profil de mobilité définis, l'Assistant affiche un résumé du déploiement.

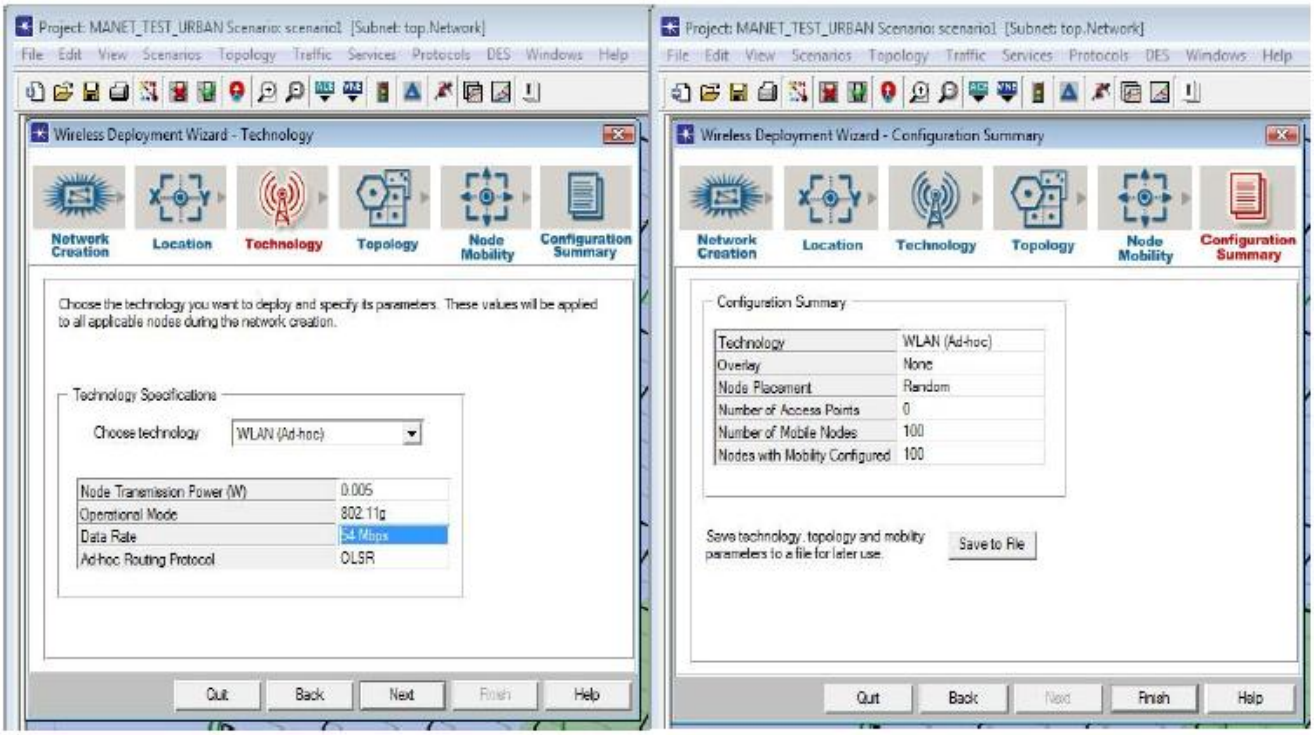


Figure 4.10 : Assistant de déploiement de réseau sans-fil AD-HOC

5. Conclusion

Les simulateurs ne permettent pas de rendre certains aspects de la réalité, Plusieurs simulateurs pour les réseaux sans fil existent et présentent différents modèles et caractéristiques. Le choix d'un simulateur peut être difficile.

Comme les simulateurs permettent de traiter les réseaux en totalité, il est bien pratique de les utiliser surtout qu'ils rendent leur surveillance plus facile. En outre, comme les expérimentations sont décrites comme des scénarios de fichiers, ces derniers sont évidemment reproductibles.

Les simulateurs permettent d'avoir un environnement totalement contrôlé, et un accès à toutes les variables pertinentes durant l'expérience.

Les simulateurs doivent présenter plusieurs propriétés pour l'amélioration de leur précision, leur rapidité, leur facilité d'utilisation, etc.

Notre choix de simulateur OPNET est fait apprêt une méthode fonctionnelle.

CHAPITRE V

OPTIMISATION DE PROTOCOLE DE ROUTAGE AODV BASÉE SUR LA MODIFICATION DES PARAMÈTRES

1. Introduction

Dans ce chapitre, nous avons présenté notre contribution qui consiste d'optimisé le protocole de routage (AODV) avec une amélioration de performance par la modification de 05 valeurs de paramètres de la version originale, on utilisant une approche expérimentale (comparative) basé sur les tests de toute les combinaisons possible, avec une vue globale sur les recherches existent dans ce contexte (état de l'art), et on termine par une conclusion.

2. Travaux antérieurs :

Au court de la recherche bibliographique de ce mémoire, nous avons trouvé plusieurs études dans le contexte de notre sujet, et des solutions proposées sur les paramètres de protocole (AODV), pour une meilleure optimisation et une amélioration des performances, nous les résumons, dans les paragraphes suivants :

En 2004 [Nabil tabbane, Sami tabbane, Ahmed mehaoua], sont réaliser une étude de mesure de performance de protocole AODV basé sur l'analyse et l'évaluation de certain scenarios simulées avec des modifications sur les valeurs des paramètres dans diffèrent situations, tel que (la surface et le nombre de nœud.

A la suite de la simulation qu'ils sont effectuée, ils constatent que le protocole AODV offre une bonne adaptabilité vis à vis de la mobilité des nœuds dans un réseau en terme de délai, de temps d'acquisition de route, de trafic de contrôle et de longueur de route.

D'autre part, ils sont conclus qu'AODV présente un taux de livraison des paquets avec succès qui se dégrade avec l'augmentation de la mobilité des nœuds du réseau.

En 2007 [Teresa Albero, vector M] sont réaliser une étude d'évaluation et proposition de performance par la modification de quelque paramètres de ce protocole, pour le trafic multimédia de type vidéo, ils sont suivie une méthode expérimentale.

Ils sont conclus que la difficulté de fournir des services multimédias à flux constant qui remplissent les paramètres QoS tels que le taux d'erreur ou débit constant dans les réseaux ad hoc. Plus précisément, Le protocole AODV ne fonctionne pas correctement lorsque la valeur par défaut de ses paramètres est utilisée. La technologie sans fil a du bruit (qui Provoque le phénomène d'intermittence de route, générant Retards continus et pertes de connectivité) et élevé.

Avec les valeurs qu'ils sont proposées pour certains paramètres de protocole AODV qui a été obtenu à partir d'expériences Tests dans un environnement bruyant, la force du protocole Face au phénomène de l'intermittent de la route est Augmenté, réduisant les retards et augmentant le temps de réaction Lorsqu'il

s'agit de changements de topologie, sans affecter les Débit de la communication. Cela améliore le Comportement des applications multimédia, permettant un nettoyage, Communication plus fluide.

En 2008 [wadhah al-mandhari, koichi gyoda, nobuo nakajima] sont fait une étude d'amélioration de la performance de protocole de routage AODV avec la modification de valeur de paramètre (active route time- out) et ils sont concluent :

Que la valeur par défaut des paramètres ART (active route timeout), les valeurs PDR (Packet delivery ratio) étaient très faibles, en particulier à des vitesses de déplacement élevées. C'est à cause de la lente adaptation aux positions de la nouvelle station en raison du mouvement rapide. L'effet de l'évolution des paramètres de l'ART pour l'AODV était très apparent à partir des résultats simulés. L'augmentation de vitesse a affecté le PDR pour tous les scénarios de simulation. La réduction des valeurs d'ART a permis une meilleure performance du réseau, par particularité pour des vitesses plus élevées. Le nombre accru de stations n'a pas atteint les résultats escomptés. C'est parce qu'il est difficile de réaliser et de mesurer le nombre de connexions pour une section sélectionnée dans le réseau.

Le second modèle simulé illustre l'incrément de retard avec l'augmentation du nombre de nœud. Les valeurs ART ont affecté le délai de bout en bout. D'autre part, ce retard n'a pas semblé affecter les valeurs PDR significativement comme observé à partir du deuxième scénario. Et ils sont concluent, pour le second modèle simulé, pour les applications sensibles au temps, il est recommandé d'utiliser de faibles valeurs ART dans un réseau sans fil à plusieurs bonds pour réduire le délai de fin à bout. Pour des applications exigeant un débit élevé, on préfère des valeurs ART élevées pour obtenir un meilleur rendement dans le cas de nœuds non mobiles.

En 2014 [Amol R. kothar et nilesh S vani] sont proposé une méthode méta- heuristique dans VANET basé sur l'algorithme PSO (optimisation de l'essorage des particules) pour trouver une combinaison optimale des valeurs des paramètres AOMDV.

Ils sont concluent que La performance de la plupart des protocoles de routage dépend de leur valeur de paramètres et il y a de grandes Nombre de combinaisons de paramètres ayant une valeur combinatoire. Il est peu pratique de trouver une solution optimale.

Un algorithme basé sur PSO (un méta heuristique) est implémenté et testé sur un scénario de carte réelle pour obtenir l'optimum Valeur des paramètres dans AOMDV. La valeur obtenue des paramètres montre une amélioration de la QoS par rapport à La valeur par défaut des paramètres. Il y a 80,65%, 37,05% et 1,96% de baisse d'AE2ED, de NRL et de PDR respectivement.

Seul le problème avec l'approche est dans la grande carte, il y a une baisse de la PDR, mais la performance globale est significative. Pour Une meilleure QoS dans un scénario donné, la configuration du protocole de routage est très importante et cette configuration peut être Obtenue en utilisant des Méta-heuristiques en raison d'un grand nombre de combinaisons.

En 2015 [Amol R. kothar et nilesh S vani] sont fait un travail de recherche, comprend également l'évaluation de performance dans AODV en fonction des différents paramètres d'entrée.

Dans cet article, ils sont évalué les performances des Protocole de routage Ad-hoc On Demand Distance Vector (AODV) dans MANET. Ils prennent le général Paramètres métriques d'évaluation de performance telle que (Packet Ratio de livraison et délai de fin à bout). Le travail de simulation a été fait en Java. Ils sont fourni une vaste information Concernant le protocole AODV et ses diverses modifications. Le Travail effectué dans ce sondage, la recherche vise à développer un bon Compréhension du protocole AODV et des améliorations apportées à pour améliorer ses performances.

En 2016 [samiksha nikam, B.T jadhav] sont réaliser un recherche d'analyse du protocole AODV sur la base des valeurs des paramètres avec un temps de pause variable. , avec le simulateur NS2.

Le but de cette expérience est d'examiner et de calculer la performance d'un réseau ad hoc lorsque le protocole de routage AODV est utilisé. Chaque exécution du simulateur accepte le fichier de scénario comme entrée. Le fichier de scénario décrit le mouvement exact de chaque nœud et la séquence de paquets provenant de chaque nœud ainsi que l'heure exacte à laquelle le changement de paquet ou de mouvement se produit. Pour évaluer la performance du réseau ad hoc, ils considèrent 10 simulations aléatoires pour générer 10 schémas de scénarios aléatoires. Le résultat est calculé en prenant la moyenne de ces 10 sorties. Les expériences sont réalisées de deux manières. Les simulations s'exécutent pendant 100 secs et le résultat est stocké dans un tableau.

A partir de ces travaux on conclut que, La performance de ce protocole dépend de la valeur de paramètres.

3. Contribution :

Le routage dans les réseaux Ad Hoc est confronté à plusieurs problèmes et défis. Le protocole AODV est devenu très connu et beaucoup de travaux ont déjà été réalisés à son propos, à partir de ces travaux on conclut que, La performance de ce protocole dépend de la valeur de paramètres, Donc pour parler d'un protocole de routage fiable il faut résoudre les principaux problèmes pour augmenter les performances, nous avons pris l'idée de modifier 05 valeurs de paramètres principaux, de la version originale, pour une meilleur optimisation de ce protocole.

On utilisant une approche expérimentale (comparative), basé sur les tests de toutes les combinaisons possibles de ses valeurs, pour trouver une meilleure combinaison des valeurs optimales.

Notre contribution consiste à optimiser le protocole AODV, avec la recherche des valeurs optimale de paramètres sans modifier l'algorithme (code source) de ce protocole, et sont principe de fonctionnement.

3.1 Présentation de notre solution :

Notre principale objectif, de ce travail est la proposition d'une version optimisé de protocole de routage AODV, basé sur la modification de 05 valeurs de paramètres, avec la suivie d'une stratégie comparative pour trouver les valeurs optimaux, ces paramètres sont :

- **Allowed_hello_loss :** Cet attribut définit le nombre de perte de paquets hello qu'un nœud peut supporter avant de déclarer la rupture de liaison.
  Si un paquet hello n'est pas reçu du voisin dans ALLOWED_HELLO_LOSS * HELLO_INTERVAL, la connexion au voisin est perdue.
- **Route request retries :** Cet attribut spécifie le nombre maximal de fois qu'un nœud tentera à nouveau de découvrir une route en diffusant une autre demande route.
- **Active route timeout (second) :** c'est La durée de vie d'une route dans la table de routage.
- **Net diameter :** Cet attribut a induit le diamètre du réseau, c'est-à-dire le nombre maximal possible de sauts entre deux nœuds du réseau. Cet attribut doit être défini par l'utilisateur en fonction de la taille du réseau utilisé dans la simulation.
- **Node traversal time (second) :** représente Le Temps de Traversée des Nœuds est une estimation prudente du temps moyen de traversée d'un saut pour les paquets et devrait inclure les retards des files d'attente, les temps de traitement des interruptions et les temps de transfert. La valeur par défaut (0.04 secondes : prise de RFC) est estimée pour un réseau de diamètre 35. Cette valeur peut être inférieure pour un réseau plus petit et grand pour une plus grande netowrk en fonction de la taille du réseau.

Par conséquent, nous avons présenté l'intervalle des valeurs des paramètres de notre étude, comme indiqué dans le tableau 5.1 suivant :

Paramètre	Valeurs par default	Range
ACTIVE_ROUTE_TIMEOUT	3.0S	1 to 10
ALLOWED_HELLO_LOSS	2 HELLO Packets	1 to 10
NET_DIAMETER	35 Nodes	1 to 50
NODE_TRAVERSAL_TIME	0.04 s	1.01 to 1.00
RREQ_RETRIES	2 tries	1 to 10

Tableau 5.1 : Intervalle de valeurs de paramètres AODV

On le voit à partir du tableau 5.1, que chaque valeur de paramètre appartient à un intervalle de [1 à 10],

Dans ce travail, nous avons utilisé une approche comparative, basé sur les tests de toutes les combinaisons possibles, avec l'outil de simulation OPNET14.5.

Nous avons choisi une surface de travail compatible avec le nombre de nœud, on a suivi la mesure d'un facteur essentiel, c'est le nombre de saut par route, que soit élevé (number of hops per route), qui justifier l'existence d'une complexité au niveau de découverte des routes, pour découvrir le meilleur chemin basé sur le moindre nombre de saut.

D'après les tests expérimentaux, par l'outil OPNET, nous avons fixé la surface et le nombre de nœud comme suite : surface =5000m*5000m et nombre de nœud =15, dans un environnement trajectoire (mobilité aléatoire), la figure ci-dessous représente notre environnement de cet étude :

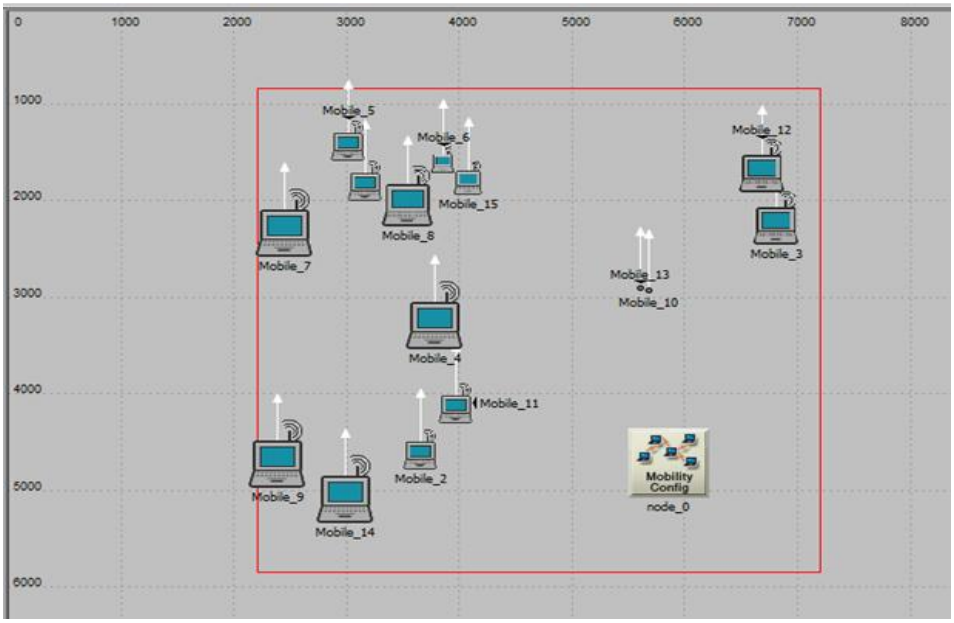


Figure 5.1 :L'environnement de notre étude

- Le graphe ci-dessous représente le nombre de saut par route (number of hops per route), de cette configuration :

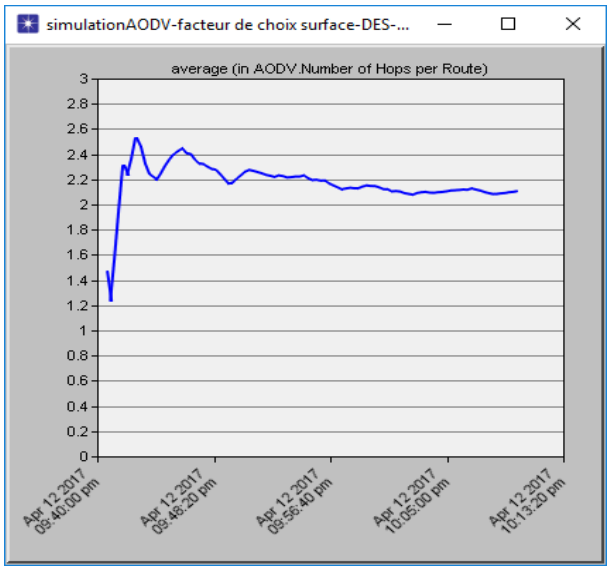


Figure 5.2 : Moyen nombre de saut par route

Pour trouver les valeurs optimales des paramètres, nous avons simulé dix (10) scenarios, pour chaque valeur de paramètre, avec un test de toute les combinaisons possible dans l'intervalle [1 a 10] , par une comparaison avec le scénario originale, suivant l'évaluation de certains aspects de performance tel que le débit (Throughput), nombre des paquets perdus (total packets dropped), le temps de découverte de route (route discovery time), délai (Delay), on sélectionner la valeur optimale, de meilleur scénario.

Les valeurs optimales des paramètres sélectionnées sont configurées dans un scénario final, ce scénario comporte la nouvelle version optimale AODV modifié, on termine par une comparaison finale avec le scénario qui représente la version originale AODV, avec une évaluation des métriques de performances précédents.

Le schéma ci-dessous résume notre méthode utilisé :

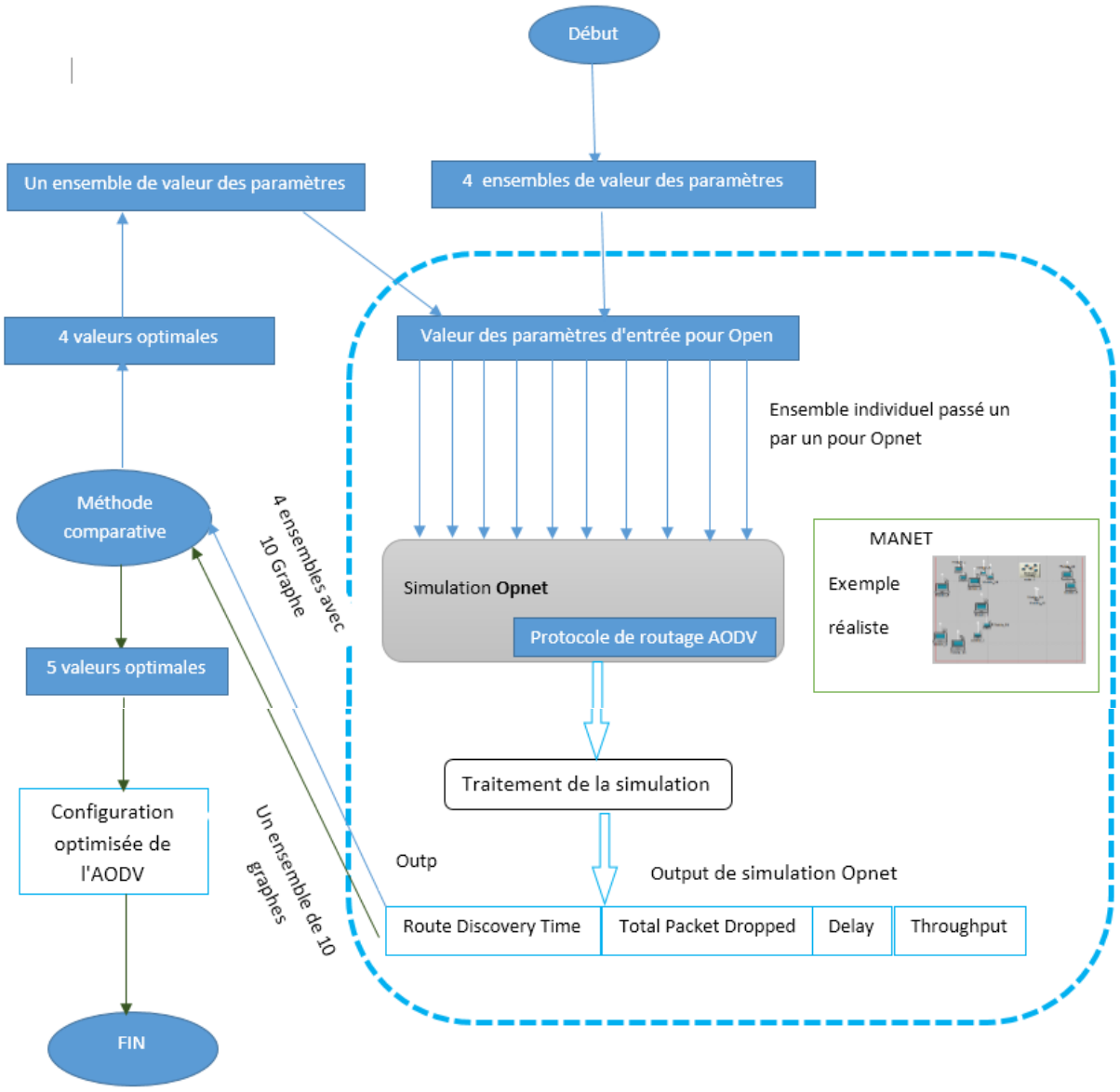


Figure 5.3 : Représentation de l'approche utilise

Cette évaluation est faite suivant la simulation suivante :

protocole	AODV
AREA	5000m*5000m
TIME SIMULATION	30 min
NOMBRE DE NOEUDS	15
Packet Size	512 BYTE
MAC Layer	802.11b
MOBILITY MODEL	RANDOM WAIPOINT
Pause time	0 sec
speed	10 m/s

Tableau 5.2 : Paramètres de simulation

4. Réalisation de l'optimisation

4.1 Environnement du travail choisi

L'environnement OPNET permet la modélisation et la simulation des réseaux de communication, grâce à ses bibliothèques de modèles (routeurs, commutateurs, stations de travail, serveurs …) et les protocoles (TCP/IP, FTP, Ethernet …). Le module Radio OPNET permet la simulation des réseaux de radiocommunication : téléphonie cellulaire et satellitaire.

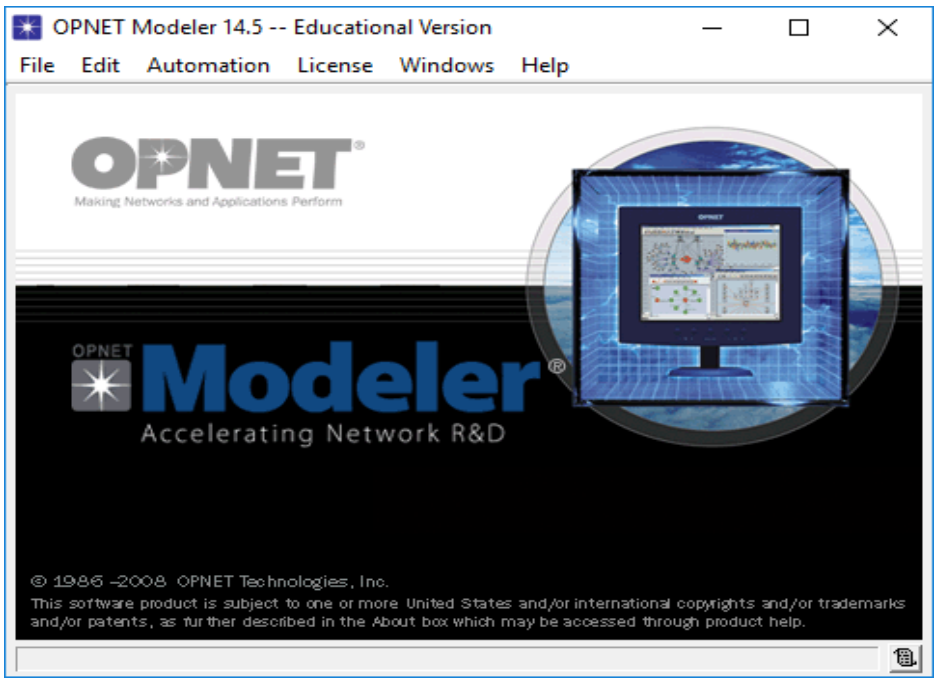


Figure 5.4 : Environnement de simulation OPNET

4.2. Simulation de réseau

Pour simuler notre AODV optimisé on utilise OPNET comme outils de simulation. Lasimulation avec OPNET passe par plusieurs étapes :

4.2.1. Première étape : elle consiste de créer le projet de réseau Ad Hoc comme suit :

Ouvrir OPNET => file => new Project

- Il apparaisse la fenêtre ci-dessous, qui contient le nom de projet et nom du scénario, sachant que le projet peut contient plusieurs scenarios :

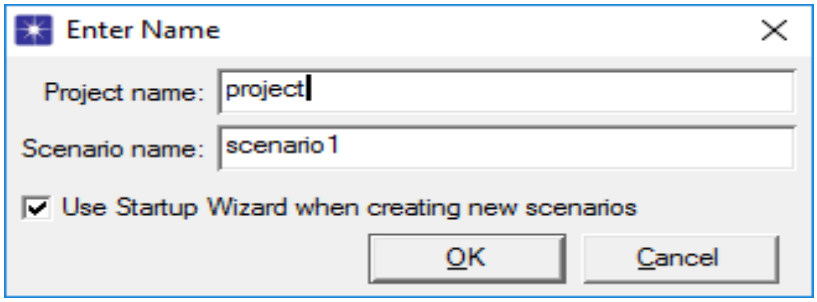


Figure 5.5 : Fenêtre de nom du projet

Ouvrir OPNET => file => new Project \create empty scenario

- On créer notre scénario, avec (create empty scenario) et on tape « NEXT » comme indique la fenêtre suivante :

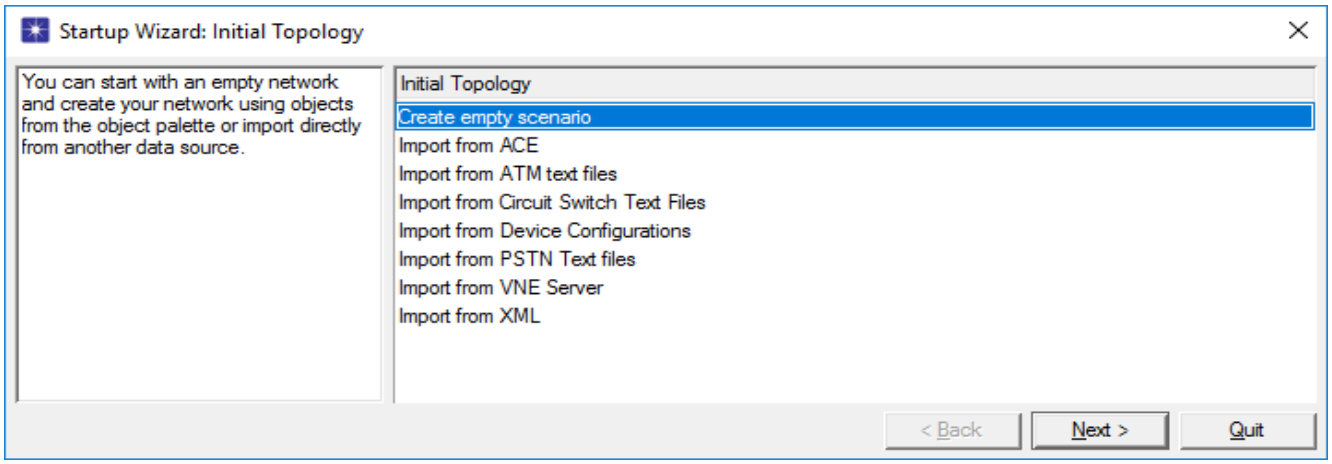


Figure 5.6 : fenêtre de création de scenario

- On définit notre surface de travaille, dans ce projet c'est 5000m*5000m, on utilisant la case « COMPUS », suivant la fenêtre ci-dessous :

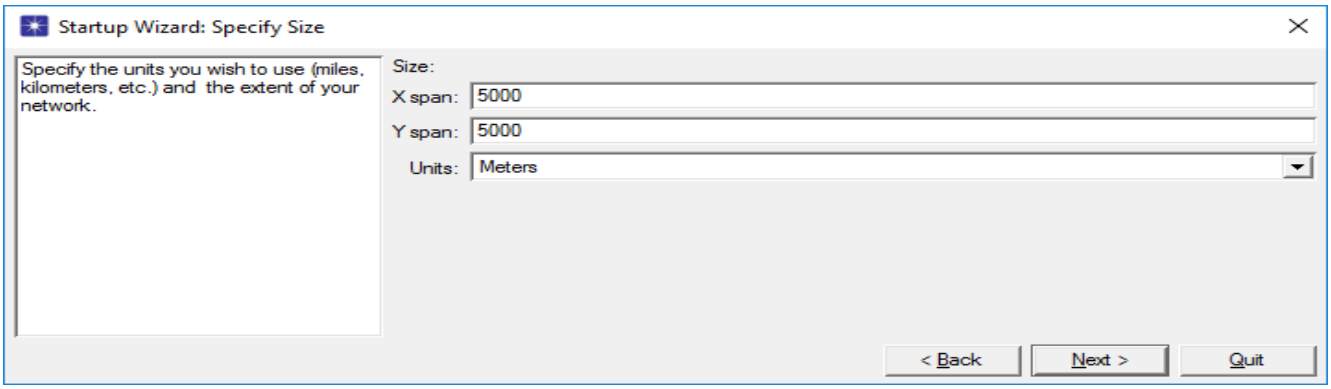


Figure 5.7 : Fenêtre de définition de la surface

- On tape « NEXT », la fenêtre ci-dessous apparaisse :

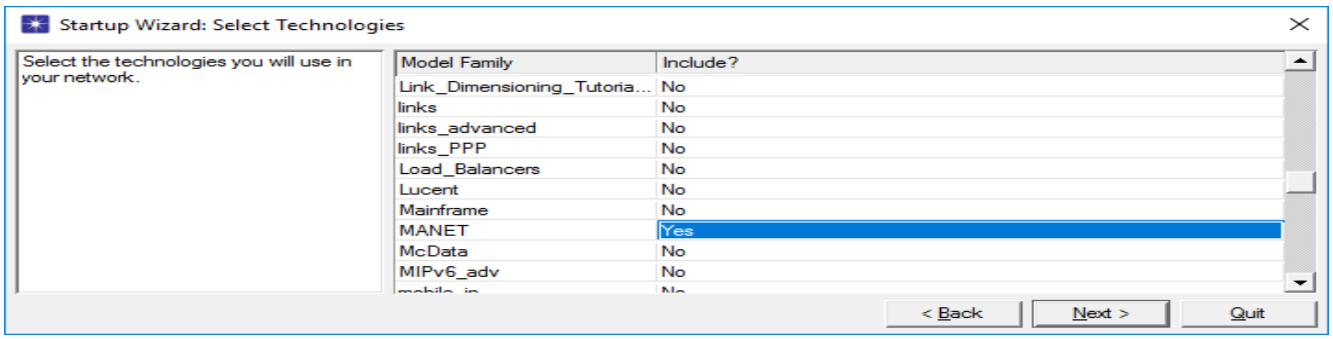


Figure 5.8 : Fenêtre de choix de MANET

- On choisit « MANET » /NEXT/FINISH.

4.2.2. Deuxièmes étape : On configure notre topologie comme suite :

- On tape, MENU/TOPOLOGY/DEPLOY WIRLESS NETWORK
- La fenêtre suivant apparaisse, on tape « CONTINU »

Figure 5.9 : Fenêtre de choix de MANET

➢ On définit les caractéristiques de notre réseau AD HOC comme indique la fenêtre suivante :

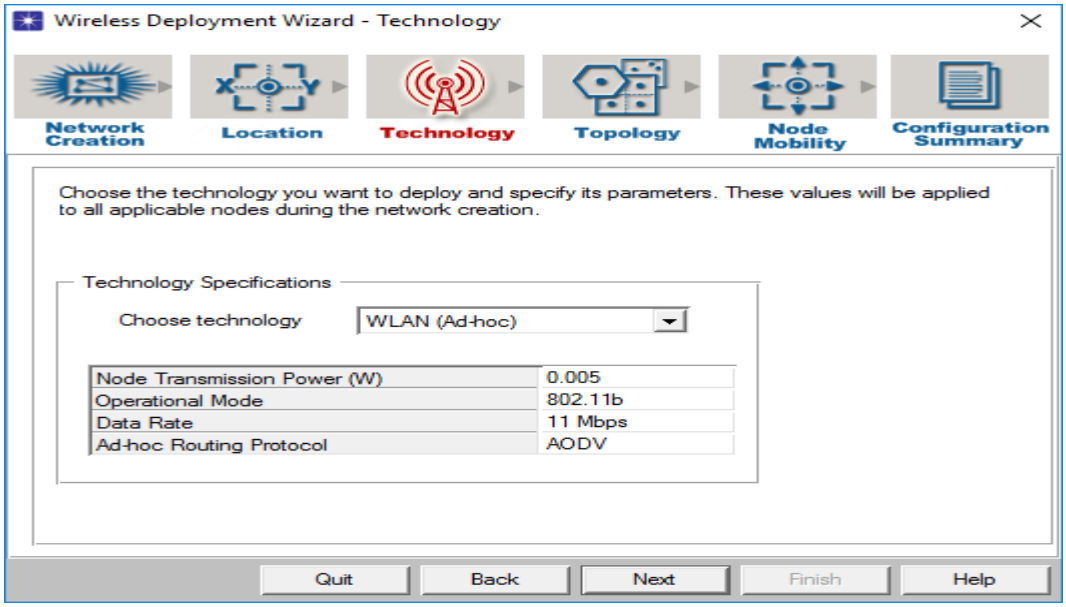


Figure 5.10 : Fenêtre de choix de caractéristiques

➢ On choisit le nombre de nœud : dans cette étude c'est : 15 comme indique-la figure suivante :

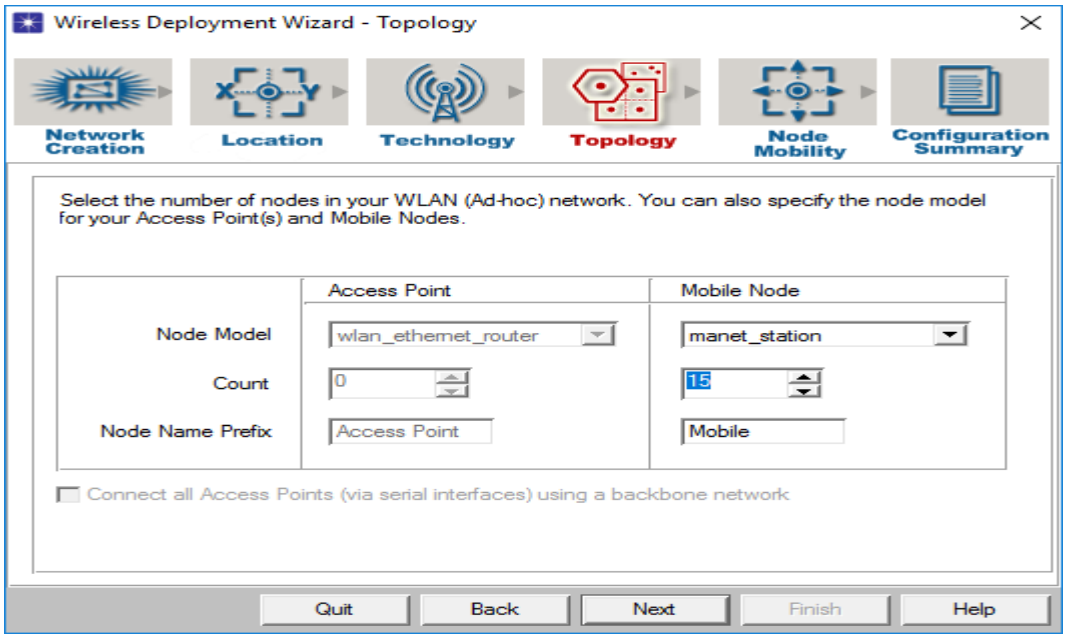


Figure 5.11 : Fenêtre de choix de nombre de nœud

➢ On obtient notre topologie comme indique la figure ci-dessous :

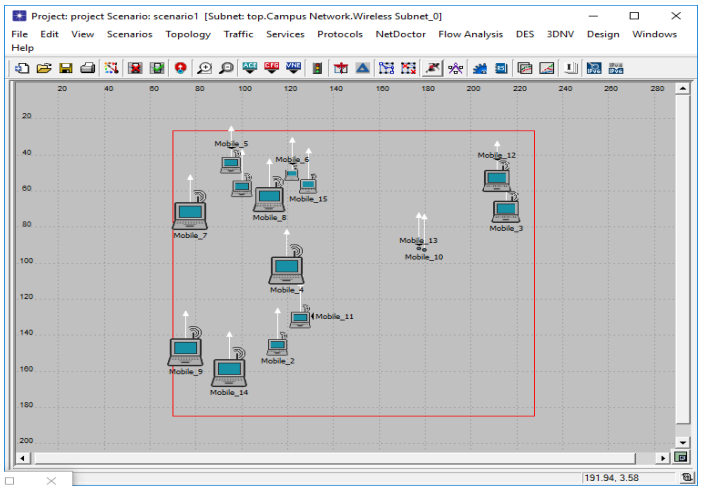


Figure 5.12 : La topologie de cette étude

4.2.3. Troisième étape : configuration du trafic et du paramètre du protocole AODV, comme indique les deux fenêtres suivantes :

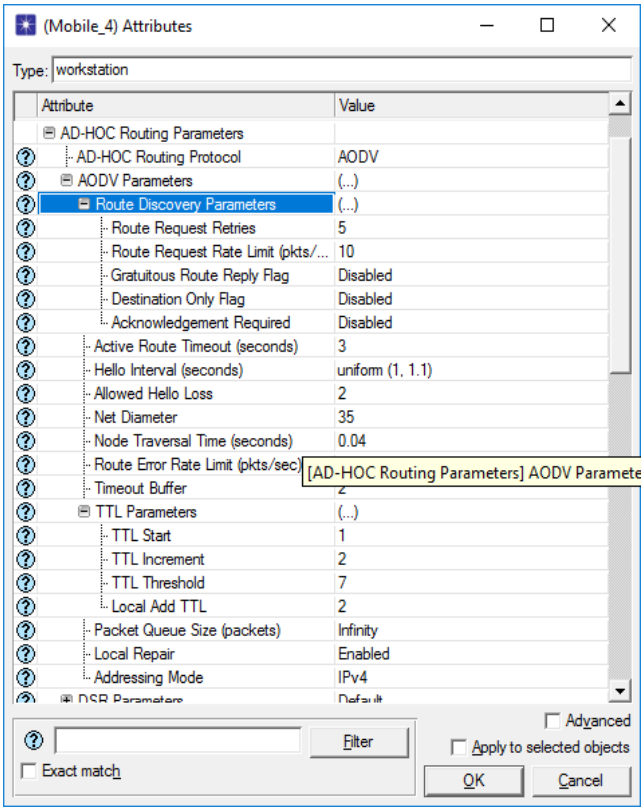


Figure 5.13 : Valeurs de paramètre par default de protocole AODV

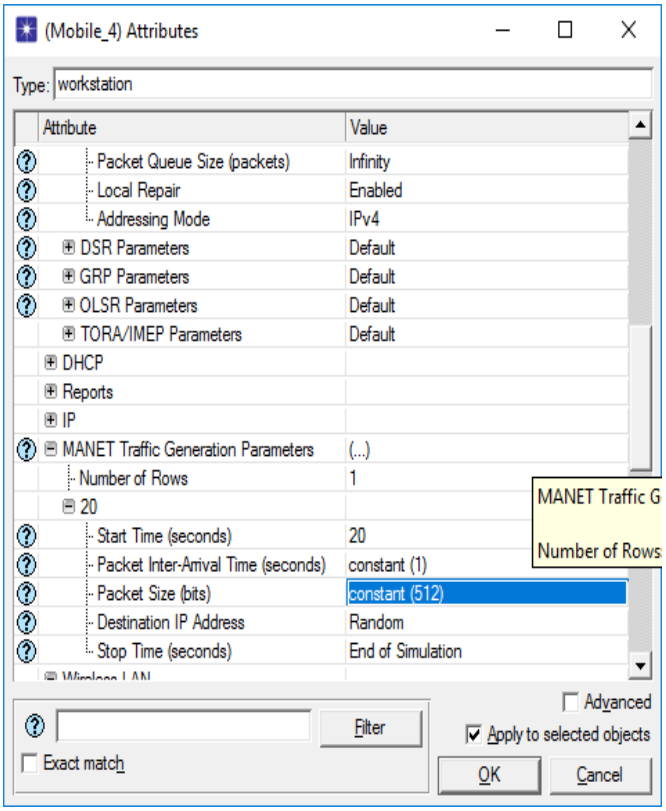


Figure 5.14 : Configuration des paramètres du trafic

4.2.4. Quatrième étape : le choix des aspects des performances, on choisit le débit (Throughput), nombre des paquets perdus (total packets dropped), le temps de découverte de route (route discovery time), délai (Delay), comme indique la figure suivant :

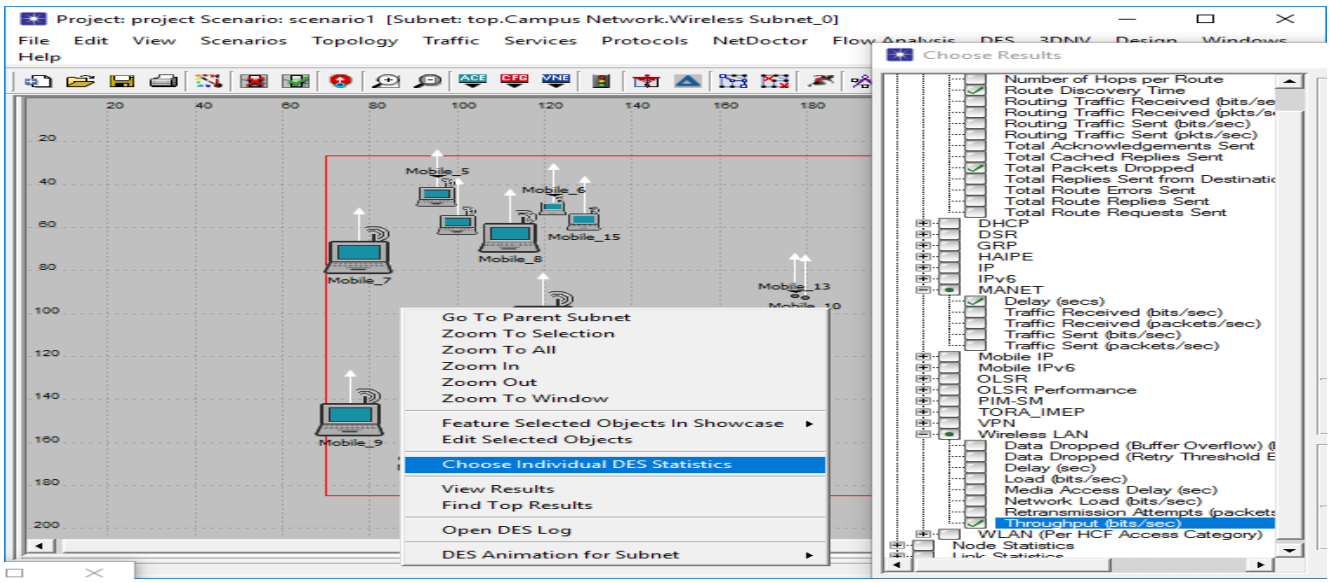


Figure 5.15 : Choix des performances

4.2.5. Cinquième étape : exécution de la simulation, on tape MENU/DES /ren discrete event simulation, il apparaisse la fenêtre suivant :

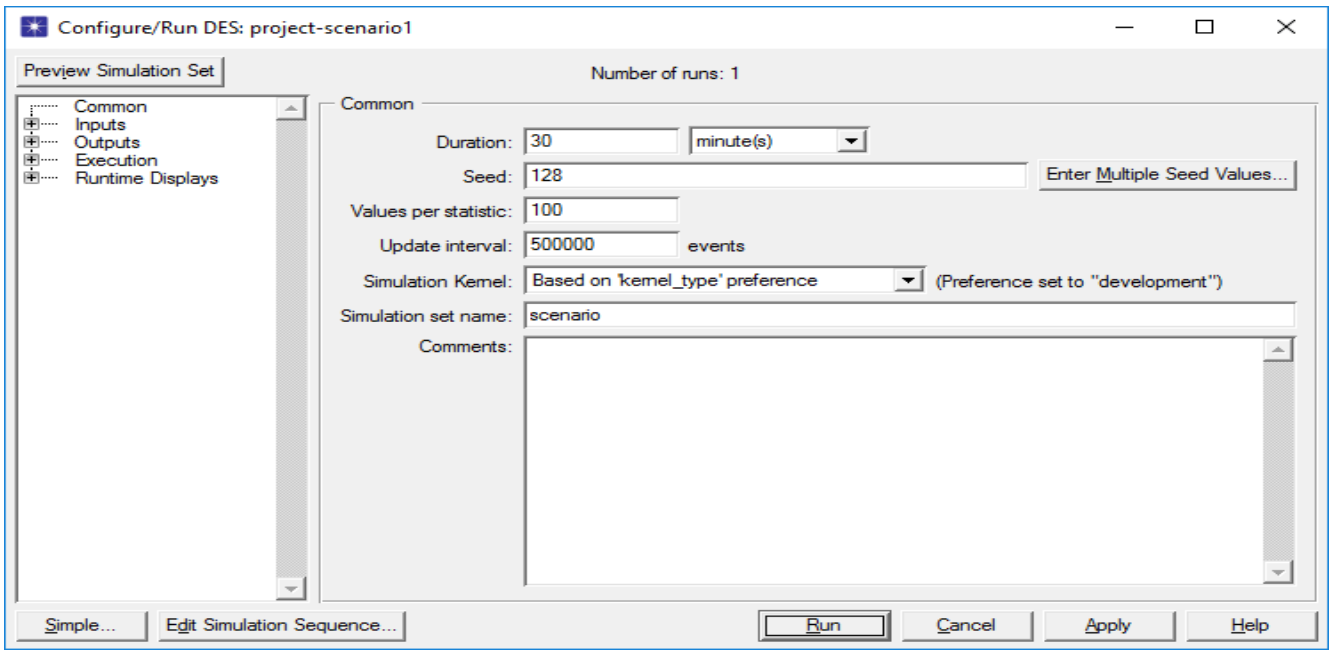


Figure 5.16 : Exécution de la simulation (temps d'exécution 30 min)

4.2.6. Sixième (dernière) étape : à la fin de la phase d'implémentation et l'exécution de la simulation,

On passe à l'étape d'évaluation des résultats sous forme des graphes obtenus par la simulation et l'étude de ses graphes seront présentée dans le chapitre suivant.

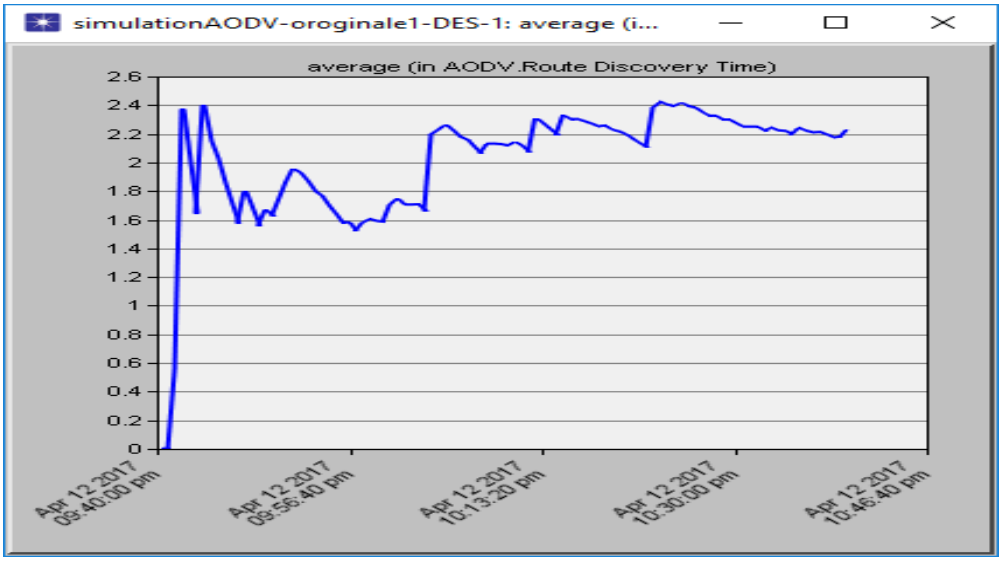


Figure 5.17 : Résultat de simulation sous forme de graphe.

Après l'exécution des différents scénarios avec AODV par défaut et AODV optimisé on Obtient des graphes de statistique de paramètre de performance de réseau pour l'analyse et la Comparaison des résultats obtenus.

5. Conclusion

L'objectif principal de ce chapitre est de décrire notre contribution qui consiste a proposé une version optimisé de protocole de routage AODV, basé sur la recherche des nouveaux valeurs optimaux de cinq paramètres principaux de ce protocole tel que (Route request retries, Active route timeout (second), Allowed hello loss (second), Net diameter, Node traversal time (second)).

Ensuite l'environnement de simulation choisi, ainsi les étapes principales de la simulation de ce travail. Dans le chapitre suivant on va simuler et Tester notre proposition, et analysé les résultats obtenus.

CHAPITRE VI

TESTS ET RÉSULTATS

1. Introduction :

Dans ce chapitre, nous avons testé et évalué, les différents résultats obtenus, avec une comparaison de notre version optimisé de protocole AODV, par rapport la version par default, par une évaluation des aspects des performances, à travers des graphes d'évaluation résultant de l'exécution de plusieurs scenarios, on cherche les valeurs optimaux qui augmente la performance de réseau.

2. Les métriques de performance :

- **Le Débit (throughput) :** c'est la quantité de données transmises par unité de temps (débit), une Valeur élevée est préférée.
- **Délai (delay) :** c'est le temps nécessaire pour transmettre un paquet d'une source vers la Destination, c'est-à-dire, le délai de bout en bout qui fait référence au temps pris pour qu'un paquet soit transmis sur un réseau de source vers destination, une baisse valeur est préférée.
- **Le temps de découverte de la route (route discovry time)** :c'est temps nécessaire pour découvrir une route, c'est-à-dire le temps pris à partir du moment où un RREQ est émis jusqu'à ce que le RREP soit reçu, une baisse valeur est préférée.
- **Nombre des paquets perdus (total packets dropped)** : cet aspect de performance représente, le nombre total des paquets perdus dans le réseau, une petite valeur est préférée.

3. Les scenarios de la simulation

Le tableau 6.1 ci-dessous représente, les valeurs des paramètres de la version originale :

Route request retries	5
Route request rat limit (pkt /s)	10
Active route timeout (second)	3
Hello interval (second)	Uniform (1.1.1)
Allowed hello loss (second)	2
Net diameter	35
Node traversal time (second)	0.04
Route error rate limit (pck/sec)	10
Timeout buffeur	2
TTL start	1
TTL increment	2
TTL threshold	7
Local ad TTL	2

Tableau 6.1 : Paramètres de protocole (AODV) original

Dans la section suivante nous allons présenter le processus de la simulation :

Le tableau 6.2 ci-dessous résume les valeurs des paramètres testées, dans les différents scénarios :

Active route timeout (second	**Senario1**	Senario2	Senario3	Senario4	Senario5	Senario6	Senario7	Senario8	Senario9	Senario10
	Valeur originale	Valeur testé	Valeur optimale	Valeur teste	Valeur testé	Valeur testé	Valeur testé	Valeur testé	Valeur testé	Valeur testé
	03	01	02	04	05	06	07	08	09	10
Allowed hello loss	**Senario11**	Senario12	Senario13	Senario14	Senario15	Senario16	Senario17	Senario18	Senario19	Scenario 20
	Valeur originale	Valeur testé	Valeur testé	Valeur testé	Valeur testé	Valeur testé	Valeur testé	Valeur testé	Valeur testé	Valeur testé
	02	01	03	04	05	06	07	08	09	10
Net diameter	**Senario21**	Senario22	Senario23	Senario24	Senario25	Senario26	Senario27	Senario28	Senario29	Senario30
	Valeur original	Valeur testé	Valeur teste	Valeur teste	Valeur testé	Valeur testé	Valeur testé	Valeur testé	Valeur testé	Valeur testé
	35	05	10	15	20	25	30	40	45	50
Route request retries	**Senario31**	Senario32	Senario33	Senario34	Senario35	Senario36	Senario37	Senario38	Senario39	Senario40
	Valeur original	Valeur testé	valeur teste	Valeur teste	Valeur testé	Valeur testé	Valeur testé	Valeur testé	Valeur testé	Valeur testé
	05	01	02	03	04	06	07	08	09	10

Le tableau 6.2 : Scenarios de la simulation

3.1. Les graphes et les résultats obtenus pour les scénarios du paramètre (Active route timeout (second)) ;

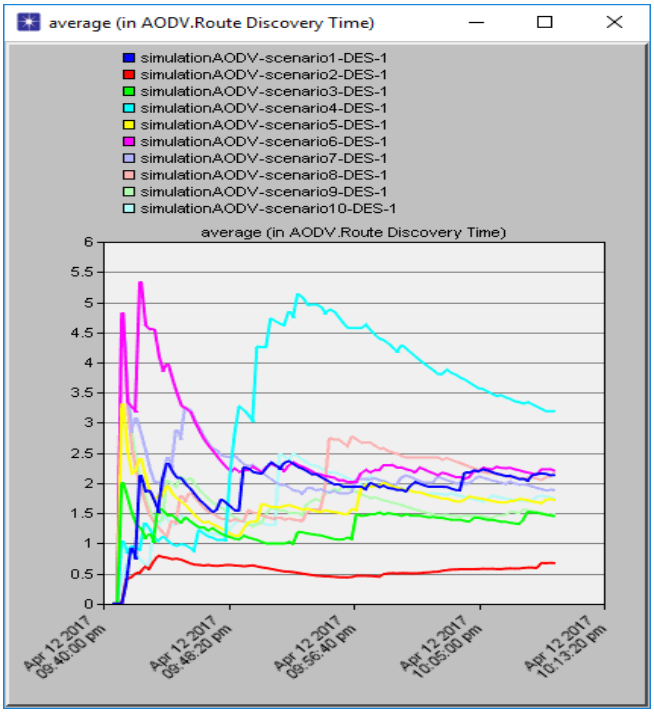


Figure 6.1: Route discovry time

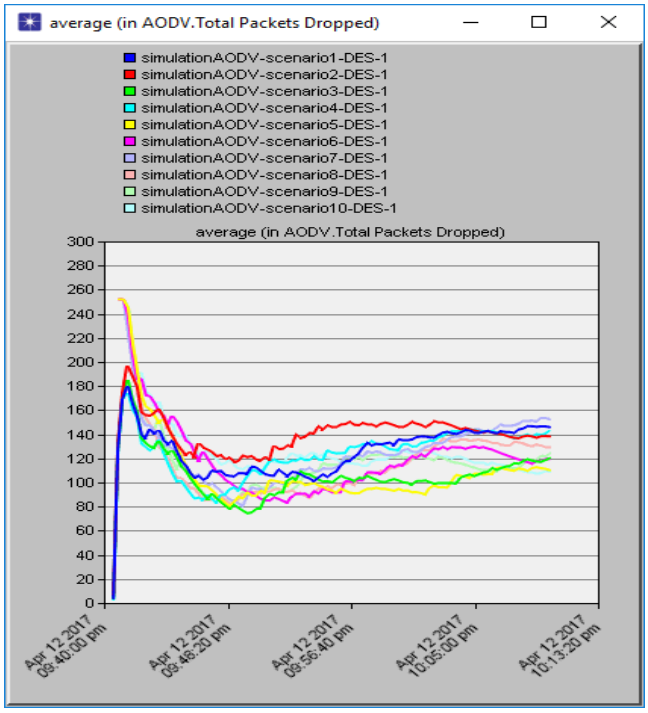


Figure 6.2: Total packets dropped

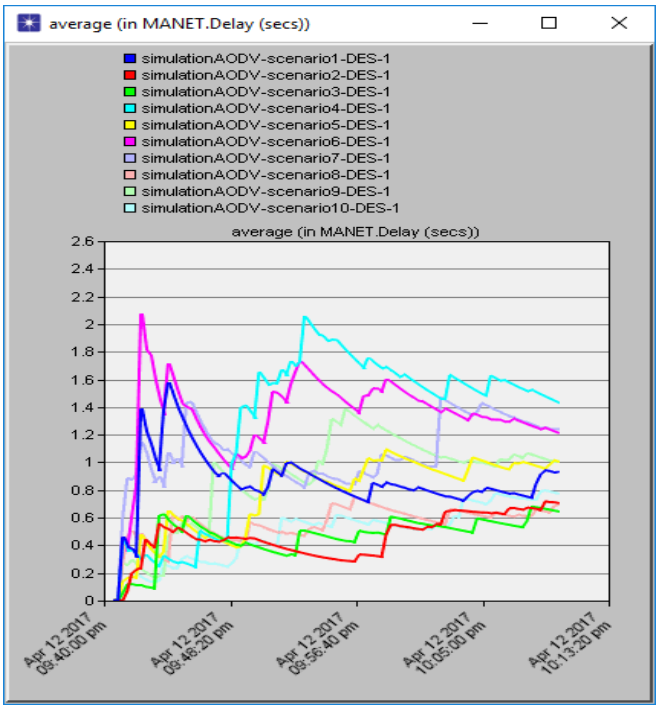


Figure 6.3: Délai (Delay (secs)

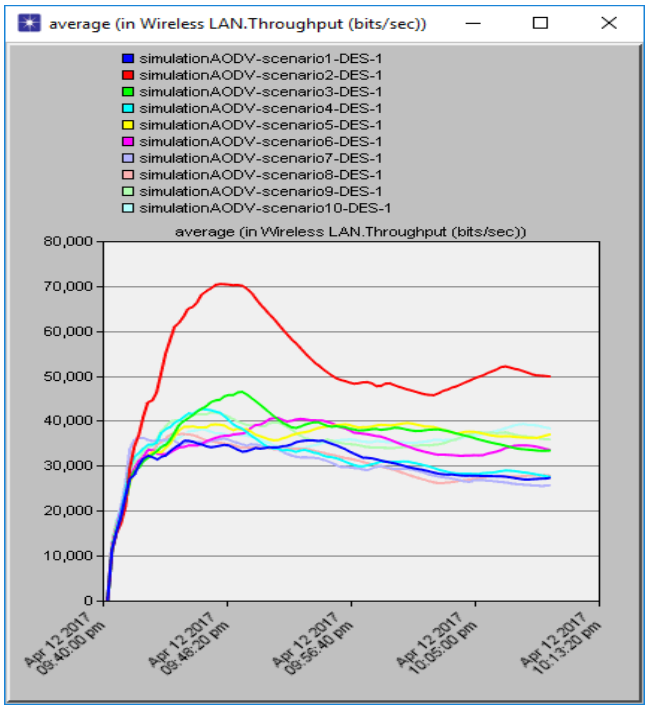


Figure6.4: Débit (throughtput)

D'après les quatre graphes précédents La valeur optimale du paramètre (Active route timeout (second)) c'est [02] du senario3 (couleur vert)

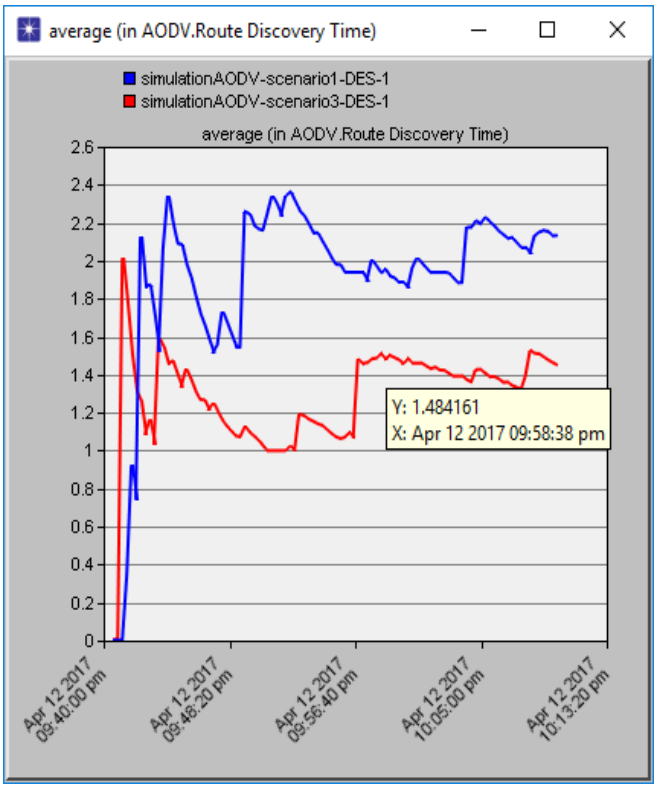


Figure 6.5: Route discovry time

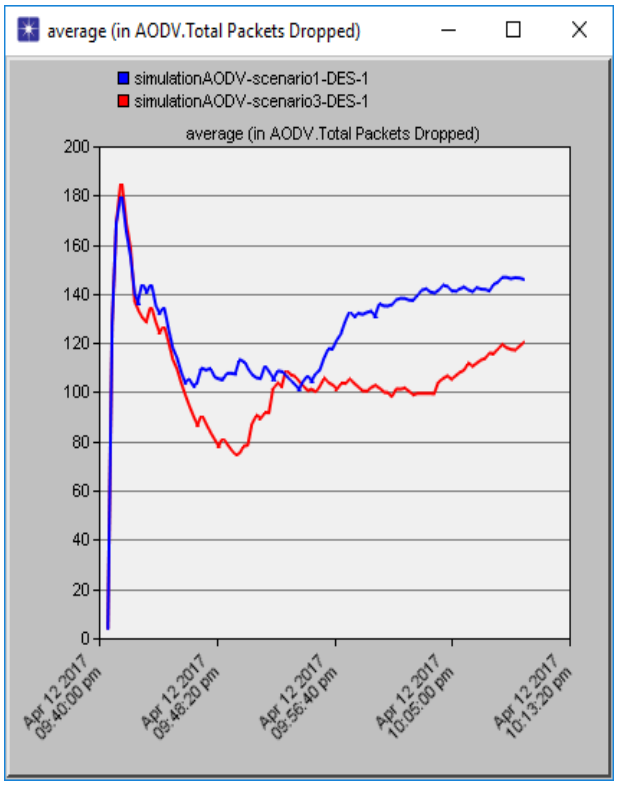


Figure 6.6: Total packets dropped

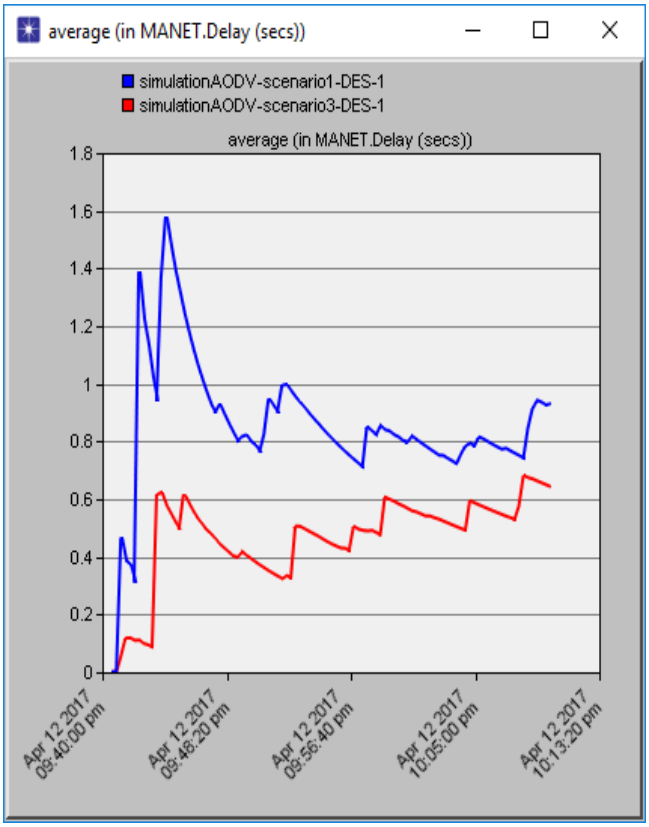


Figure 6.7: Délai (Delay secs)

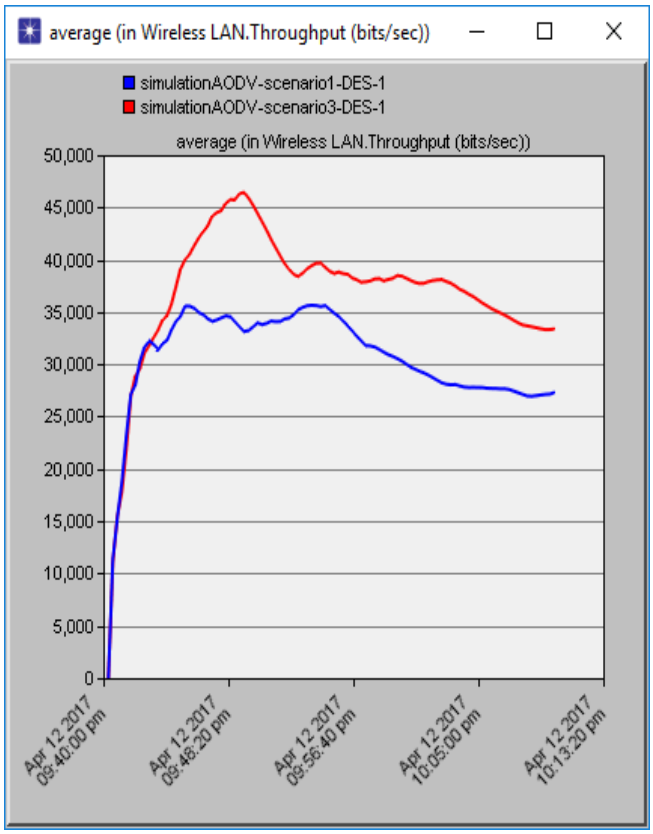


Figure 6.8: Débit (throughtput)

Ces quatre graphes représente l'optimisation de la valeur optimale obtenue (2) par rapport la valeur originale d'Active route timeout (3)

3.2. Les graphes et les résultats obtenus pour les scénarios du paramètre (Allowed hello loss) :

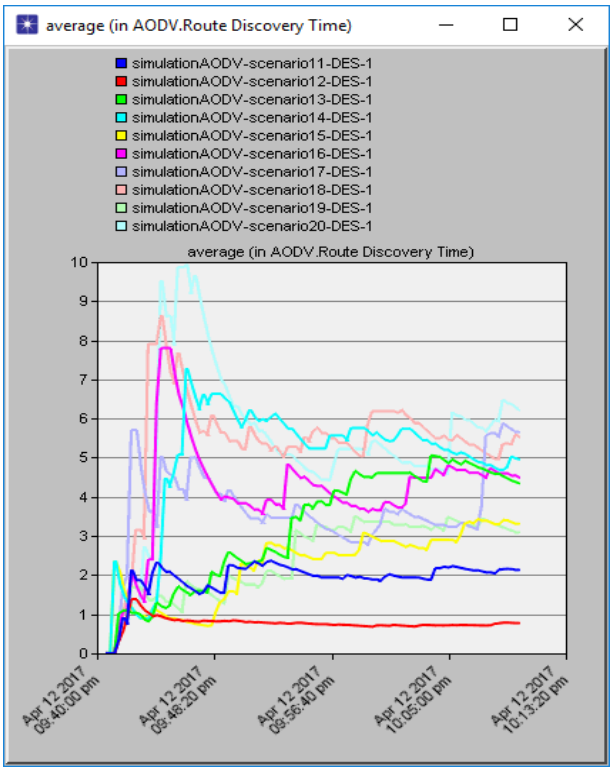


Figure 6.9: Route discovry time

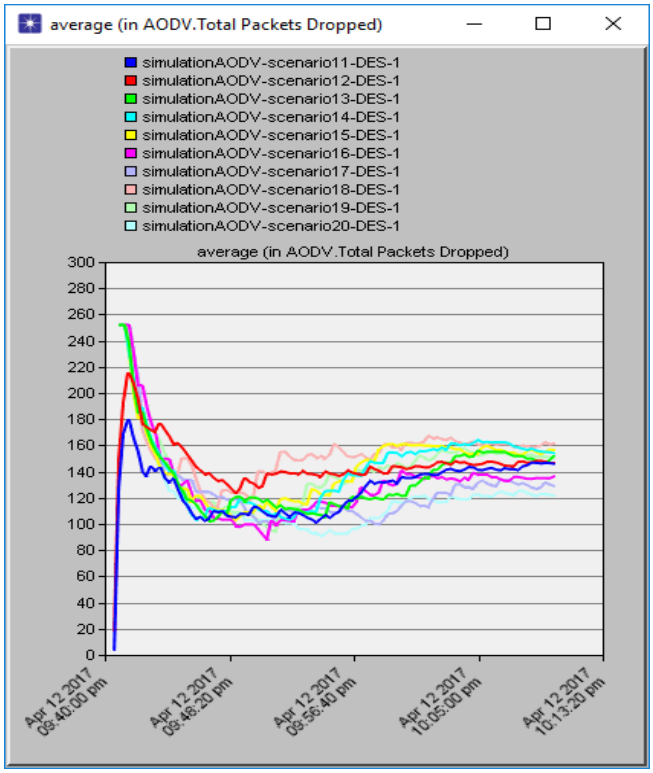


Figure 6.10: Total packets dropped

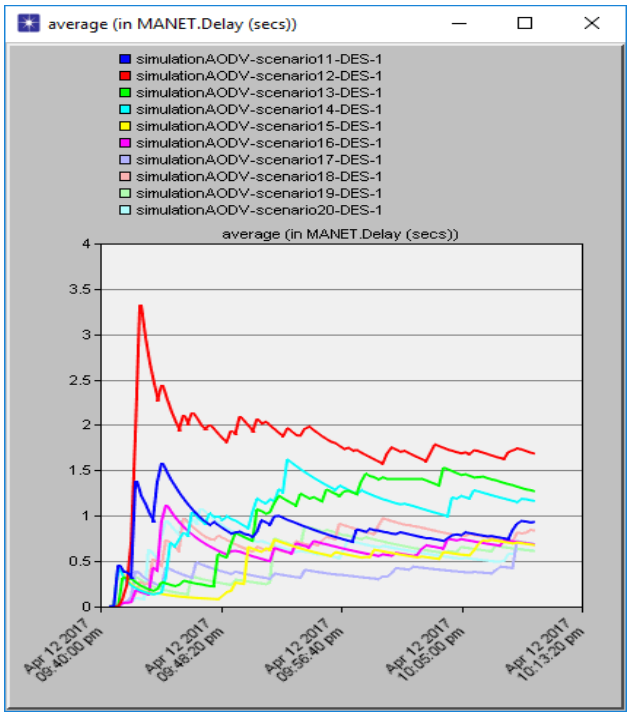


Figure 6.11: Délai (Delay secs)

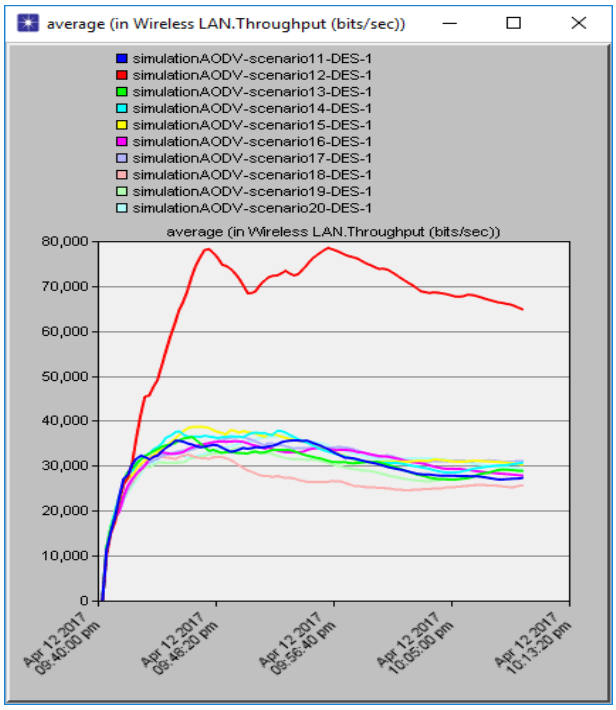


Figure 6.12: Débit (throughtput)

D'après les quatre graphes précédents La valeur optimale du paramètre Allowed hello loss c'est [**02**] du senario12 (originale, couleur rouge).

3.3. Les graphes et les résultats obtenus pour les scénarios du paramètre (Net diameter) :

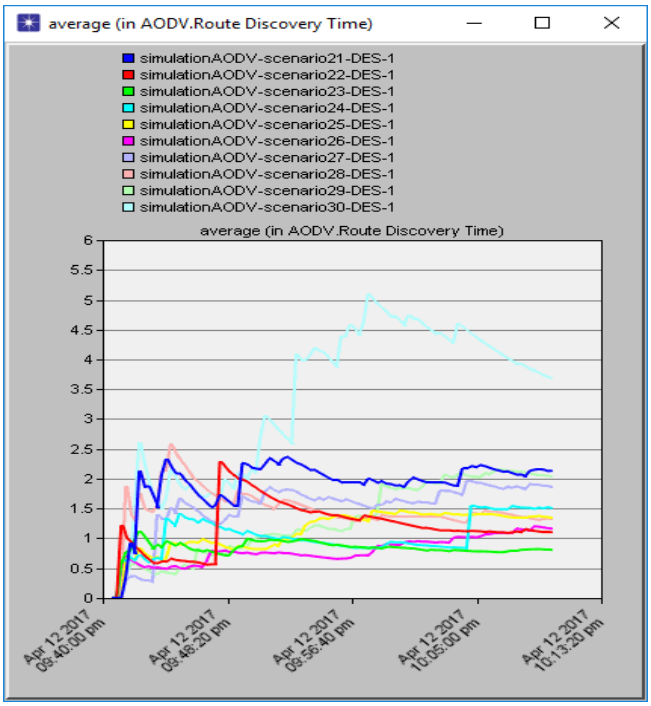


Figure 6.13: Route discovry time

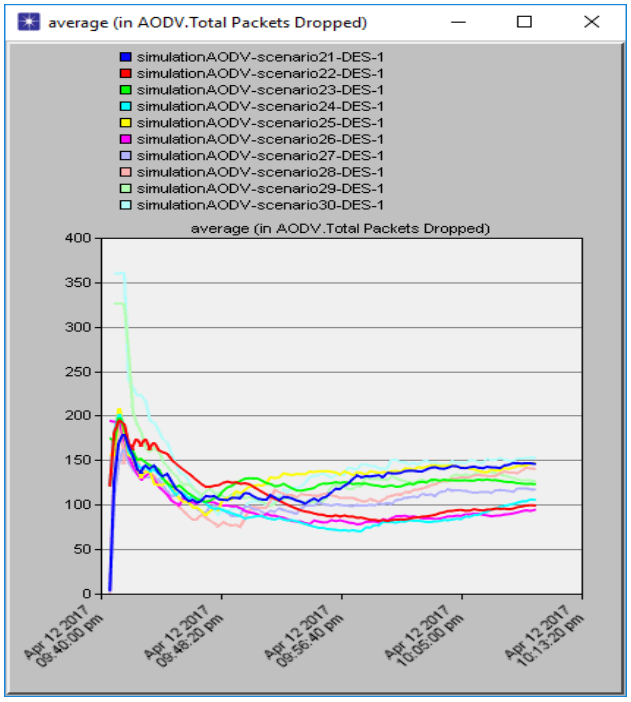


Figure 6.14: Total packets dropped

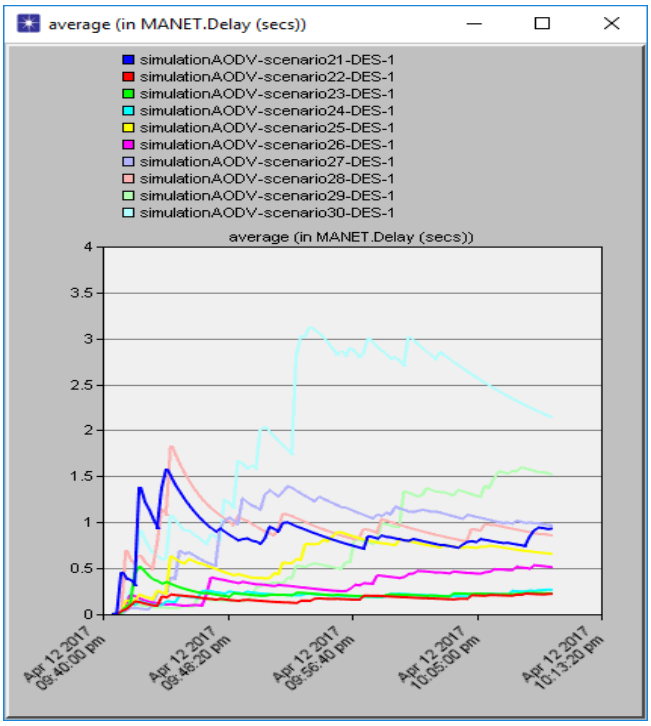


Figure 6.15: Délai (Delay (secs)

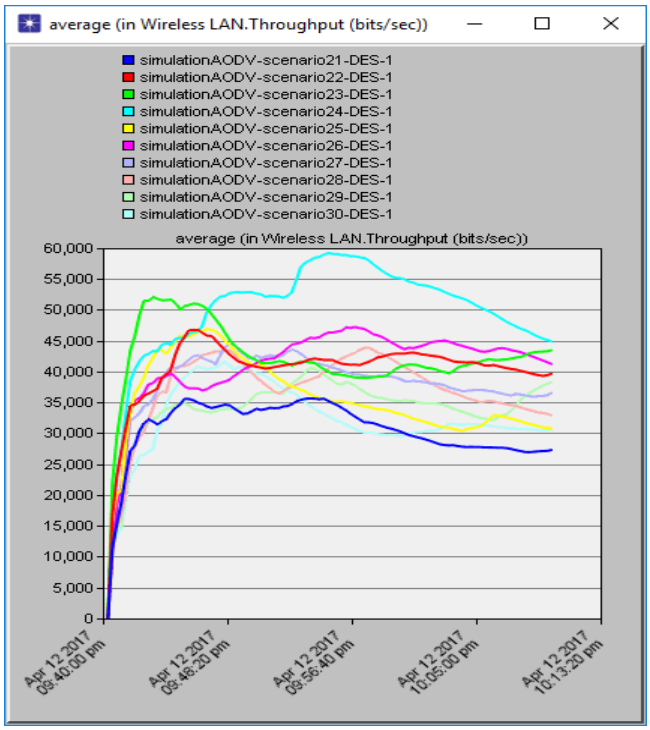


Figure 6.16: Débit (throughtput)

D'après les quatre graphes précédents La valeur optimale du paramètre (Net diameter) c'est [15] du senario24 (couleur bleu).

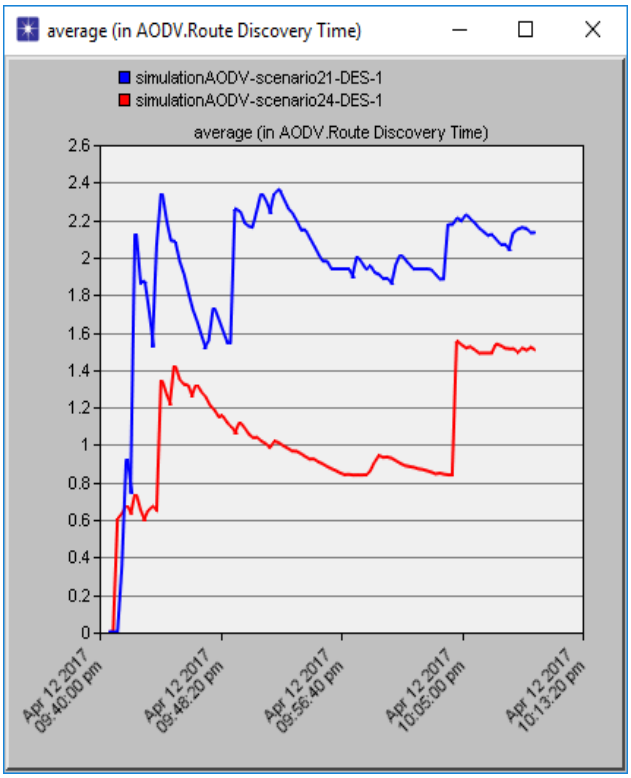


Figure 6.17: Route discovry time

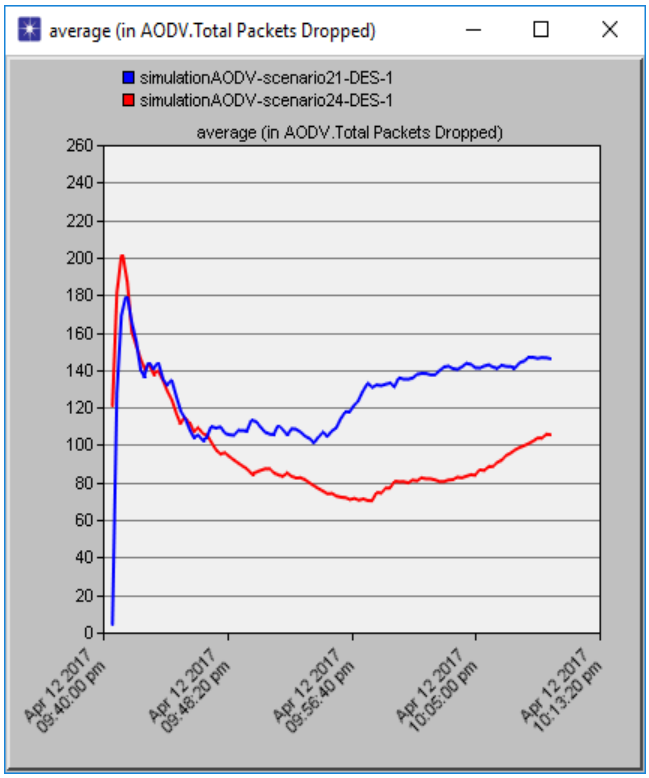


Figure 6.18: Total packets dropped

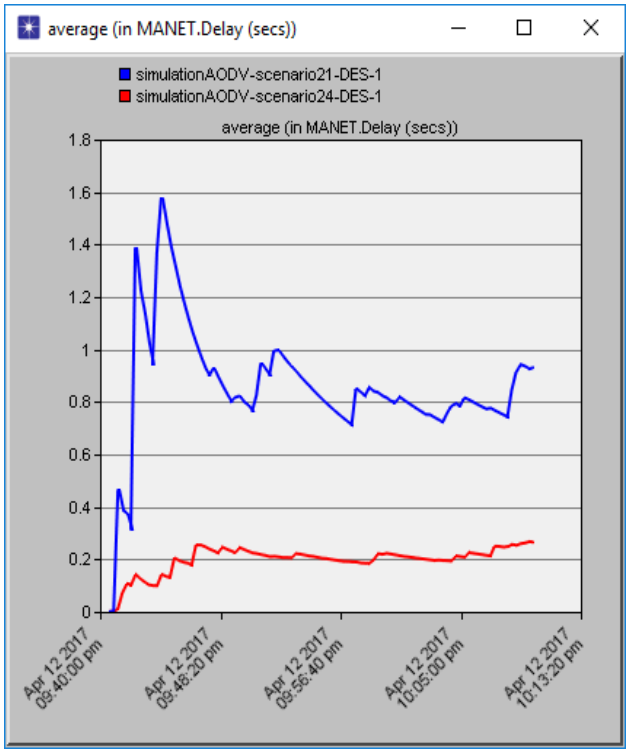


Figure 6.19: Délai (Delay secs)

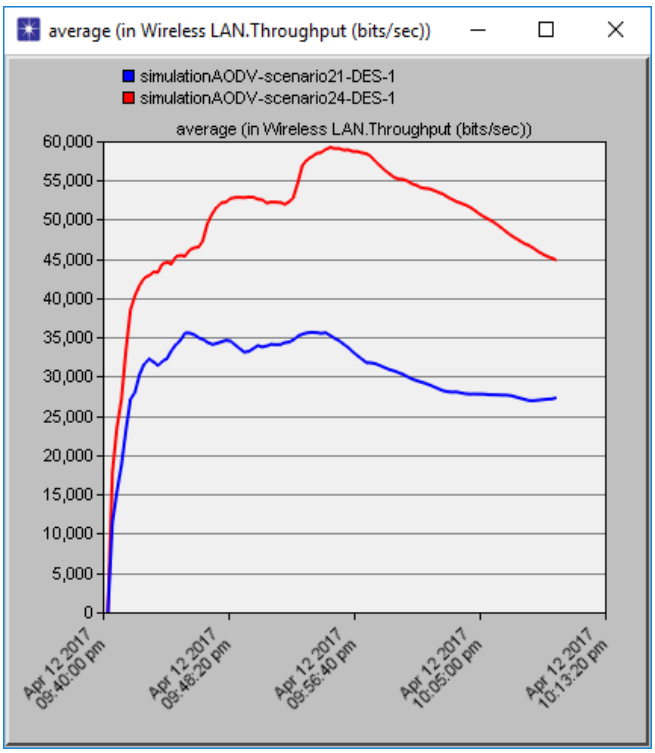


Figure 6.20: Débit (throughtput)

Ces quatre graphes représentent l'optimisation de la valeur optimale obtenue (**15**) par rapport la valeur originale de Net diameter (**35**)

3.4. Les graphes et les résultats obtenus pour les scénarios du paramètre (Route request retries) :

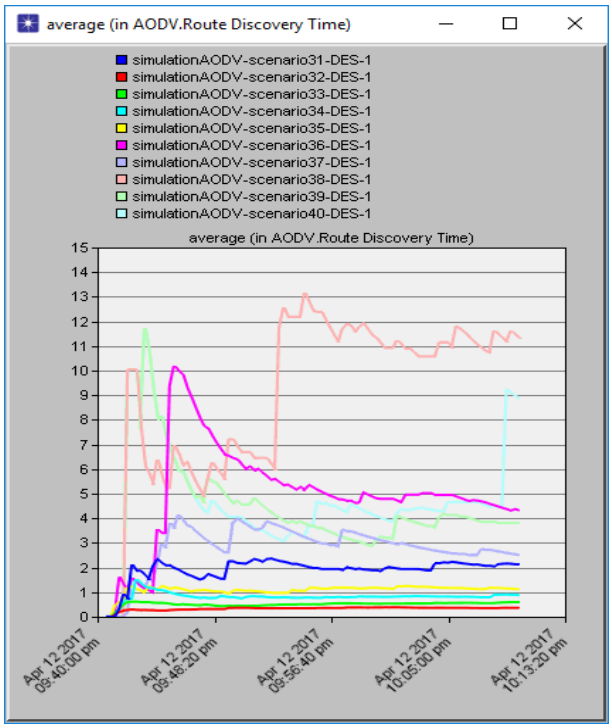


Figure 6.21: Route discovry time

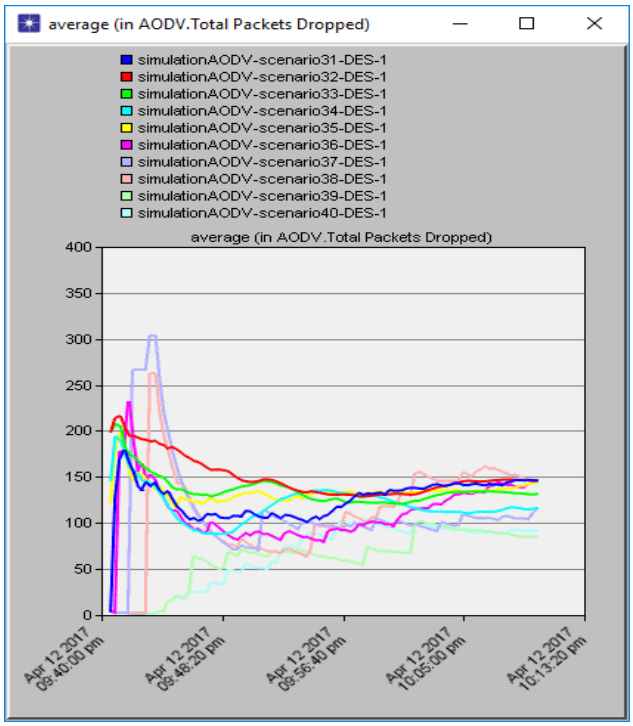


Figure 6.22: Total packets dropped

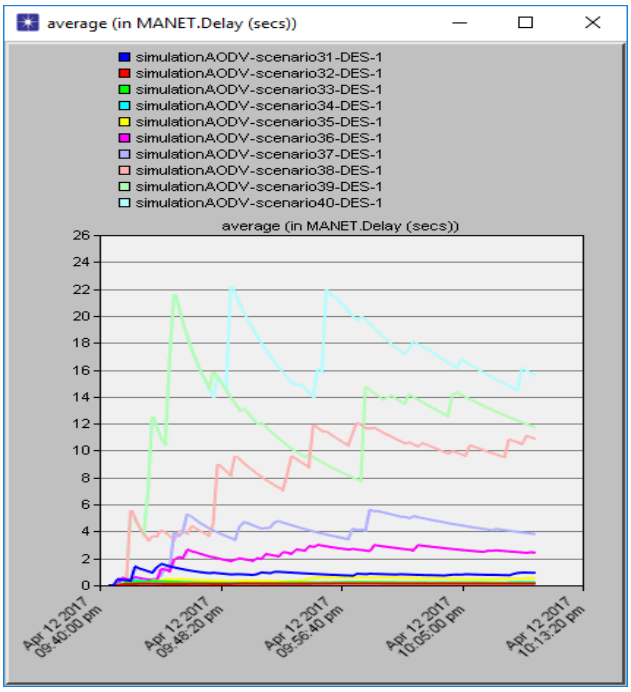


Figure 6.23: Délai (Delay secs)

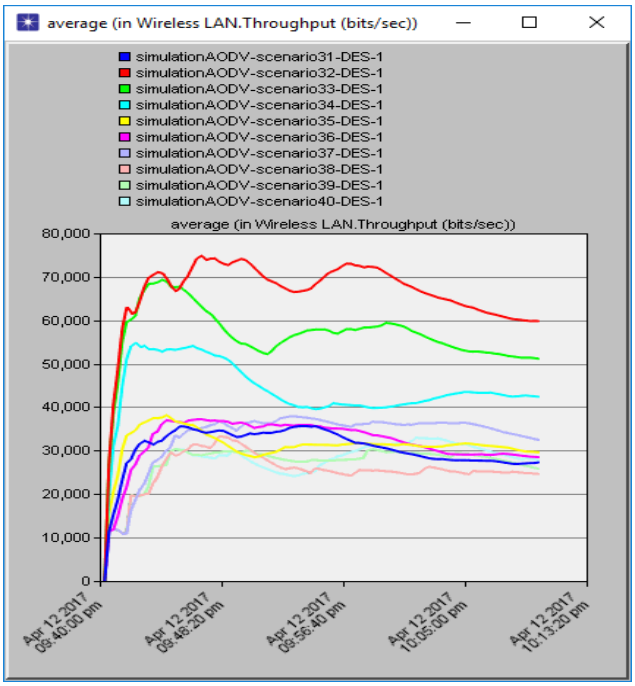


Figure 6.24: Débit (throughtput)

D'après les quatre graphes précédents, La valeur optimale du paramètre Route request retries c'est [**03**] du senario34 (couleur bleu).

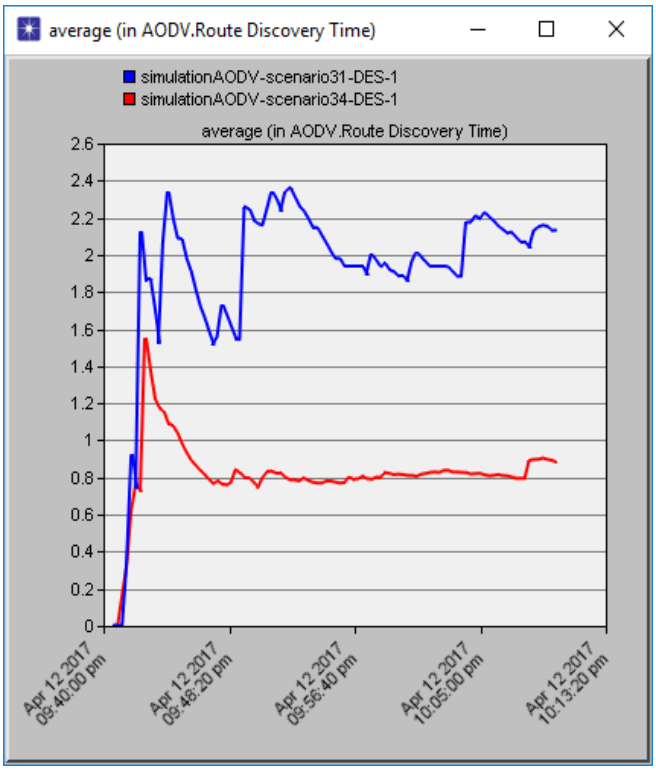


Figure 6.25: Route discovry time

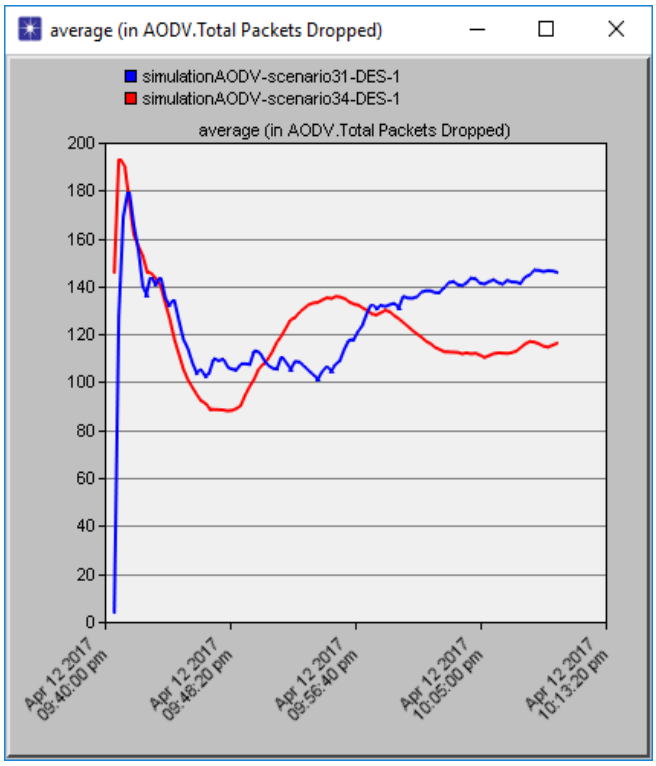


Figure 6.26: Total packets dropped

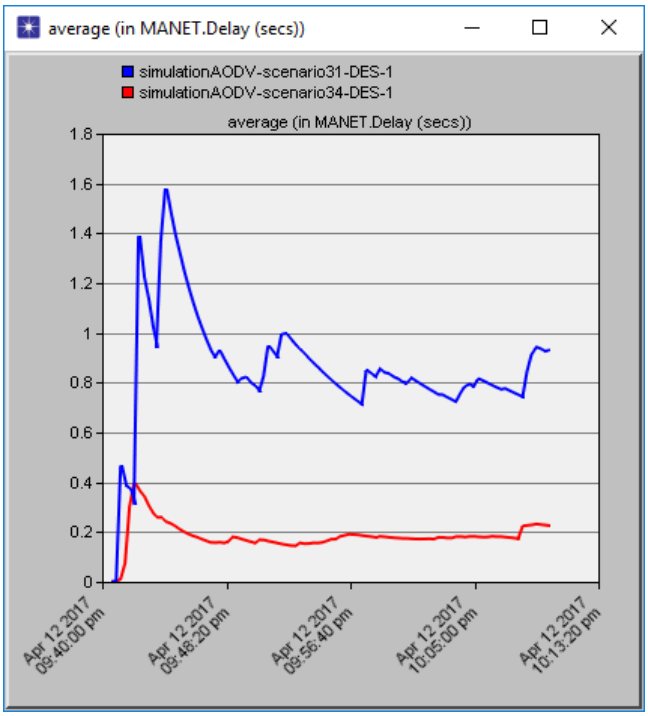


Figure 6.27: Délai (Delay secs)

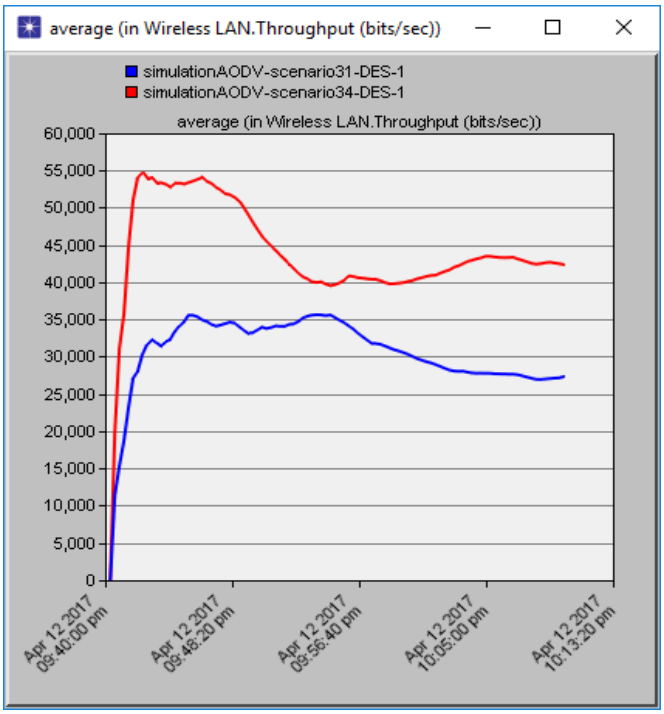


Figure 6.28: Débit (throughtput)

Ces quatre graphes représente l'optimisation de la valeur optimale obtenue (3) par rapport la valeur originale de Route request retries (5)

4. Déduction de scenario optimale finale :

Nous avons créé dix (10) scénarios avec les quatre valeurs optimales obtenues, et on fait une modification de la valeur de paramètre (Node traversal time (second)) dans l'intervalle de [0.01 à 0.1].

On compare ces scenarios avec le scénario originale, avec l'évaluation des métriques de performance précédents, pour déduire le scénario optimale qui représente la version AODV optimisé finale, qui contient les Cinque (05) valeurs optimales obtenues (les quatre valeurs optimales précédents + la valeur optimale trouvé de paramètre « Node traversal time ») comme indique les graphes ci-dessus :

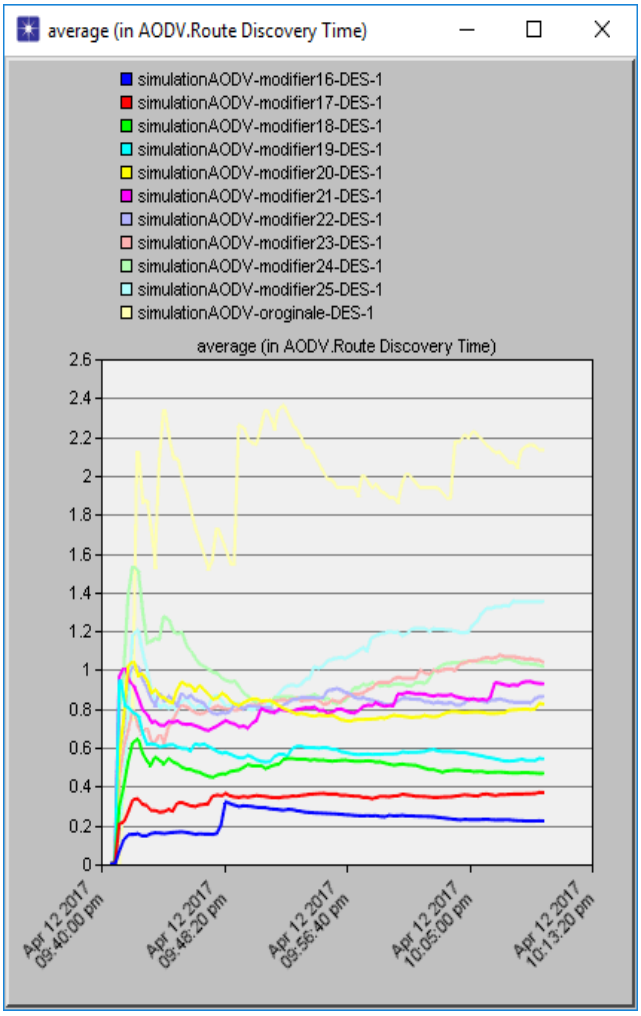


Figure 6.29: Route discovry time

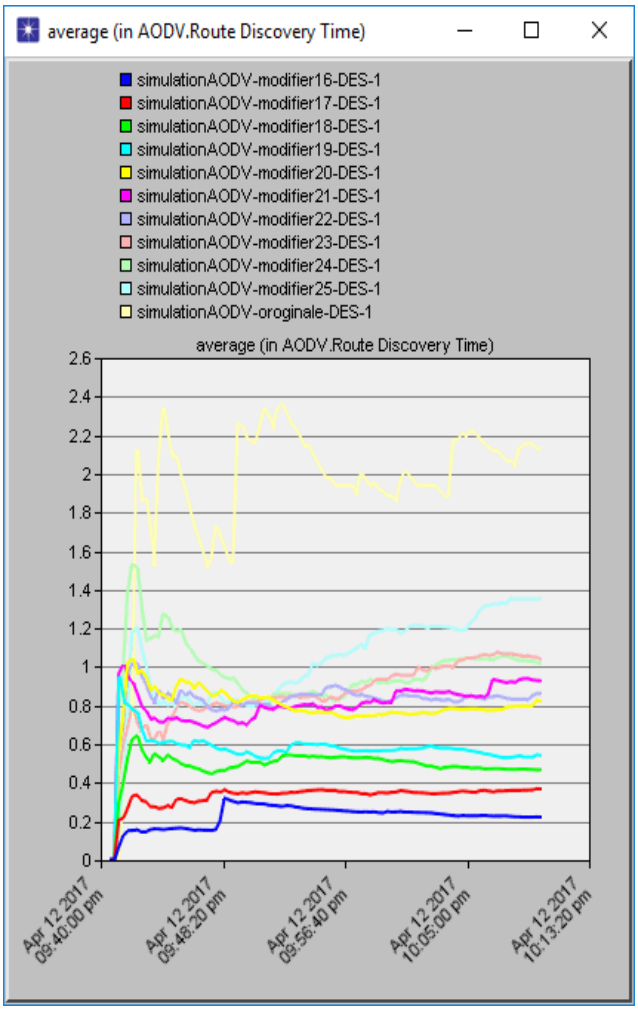


Figure 6.30: Total packets dropped

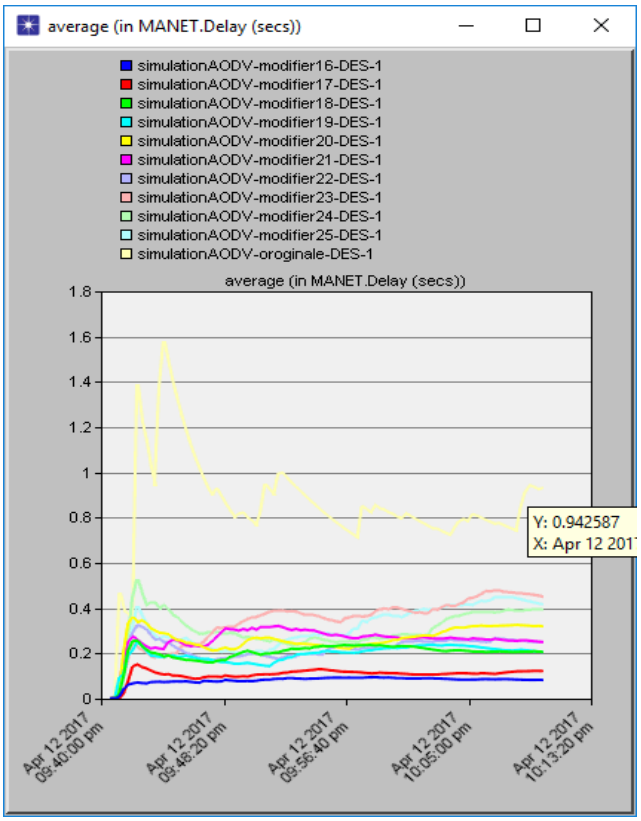


Figure 6.31: Délai (Delay secs)

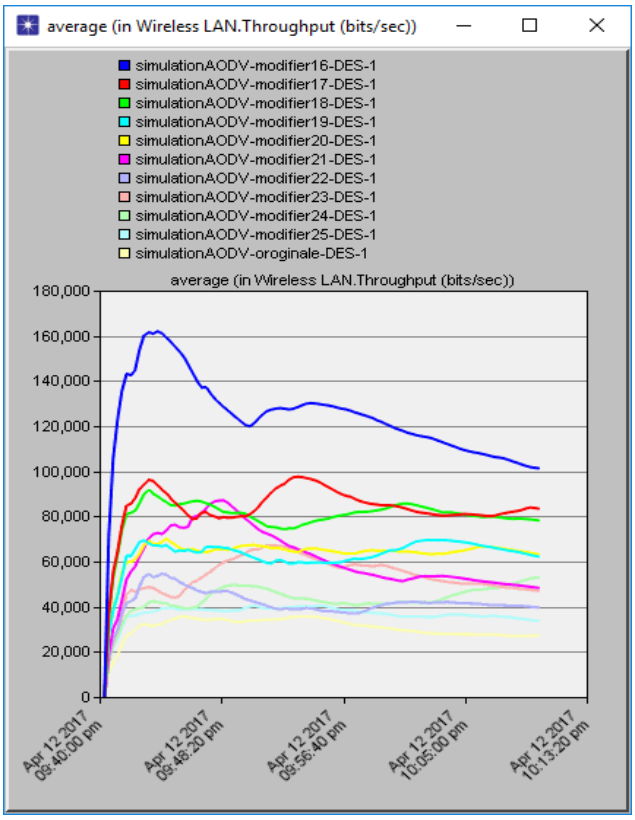
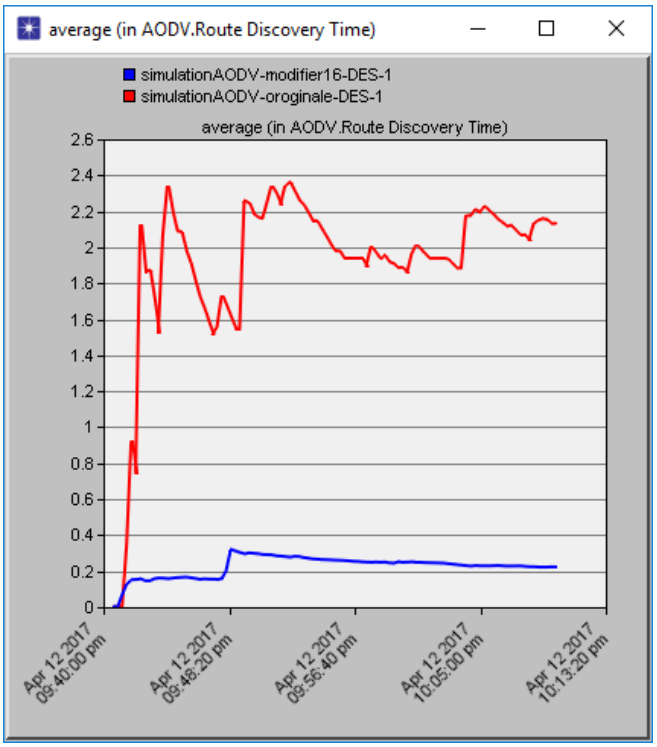


Figure 6.32: Débit (throughtput)

D'après les quatre graphes précédents, La valeur optimale du paramètre Node traversal time c'est [0,01] du senario16.

4.1 Résultat finale :

D'après les quatre graphes précédents, on a sélectionné le scénario optimal qui contient la valeur optimale du paramètre (Node traversal time (second)), c'est [0.01] du scénario (modifier16), donc ce dernier représente notre version optimisé de protocole AODV, les figure ci-dessous montre la comparaison entre cette version modifié et la version originale :

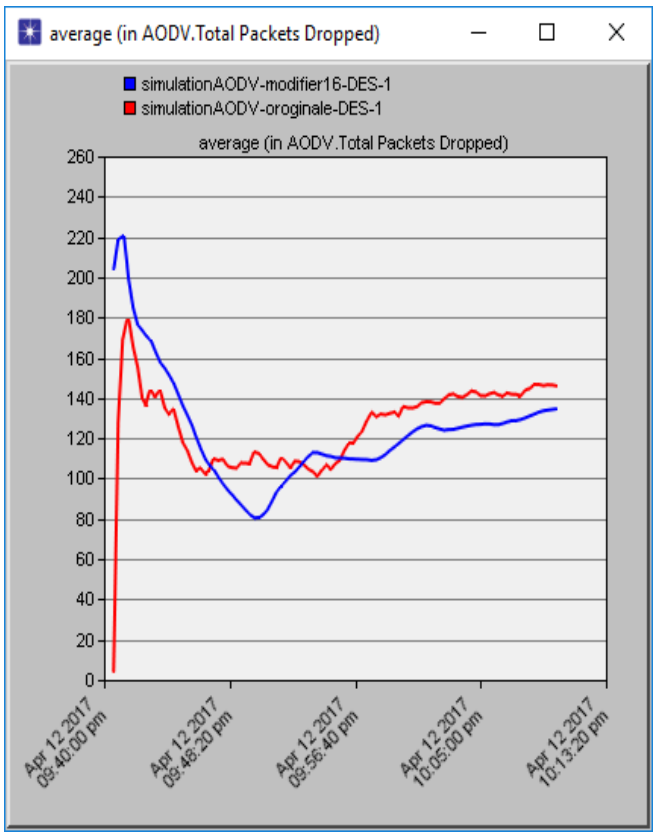


Suivant le graphe :

On constate que,le temps du découverte des routes (**route discovry time),** du scenario (originale) qui représente la version originale est égale à 2.18 second, par contre pour le scenario (modifier16) qui représente notre version optimisé est égale à 0.22 second, donc il y a une grande amélioration sur ce temps, avec une différence de 1.96 second.

Le pourcentage d'amélioration de la performance de (**route discovry time**):c'est 890% (8.9 fois).

Figure 6.33: Le temps de découvert de route (route discovry time)



Dans le graphe :

On constate que, Le nombre total des paquets perdus (total packets dropped), du scenario (originale) qui représente la version originale est égale a 147 paquets, par contre pour le scenario (modifier16) qui représente notre version optimisé est égale à 136 paquets, donc il y a une amélioration sur le nombre des paquets perdus avec une différence de 11 paquets.

Le pourcentage d'amélioration de la performance de (total packets dropped) : c'est 8,08%(0.08 fois).

Figure 6.34: Les paquets perdus (total packets dropped)

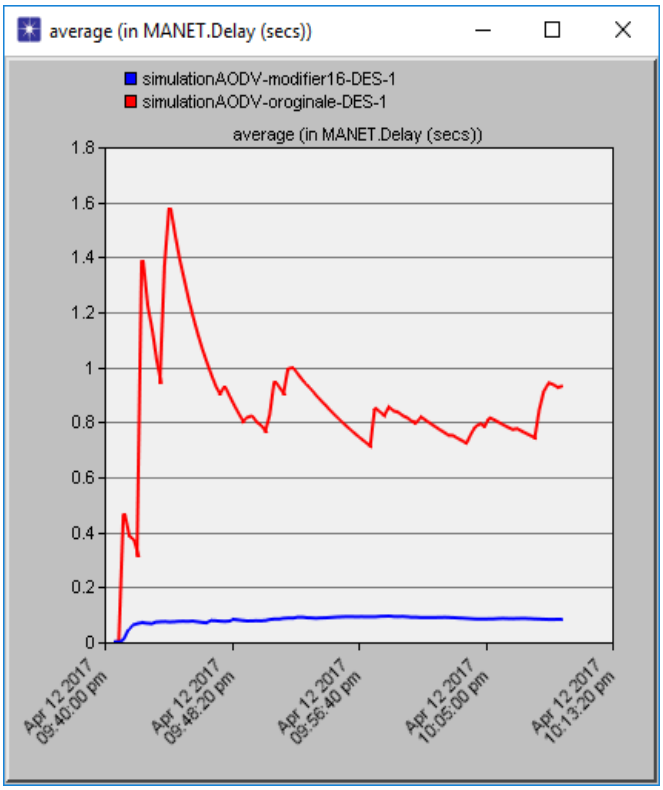


Figure 6.35: Délai (Delay secs)

Dans le graphe :

On constate que, le délai (delay), dans le scenario (originale) qui représente la version originale est égale à 0.96 second, par contre pour le scenario (modifier16) qui représente notre version optimisé est égale à 0.08 second, donc il y a une grande amélioration sur ce temps, avec une différence de 0.88 second.

Le pourcentage d'amélioration de la performance de délai (Delay) :c'est 270% (2.7 fois).

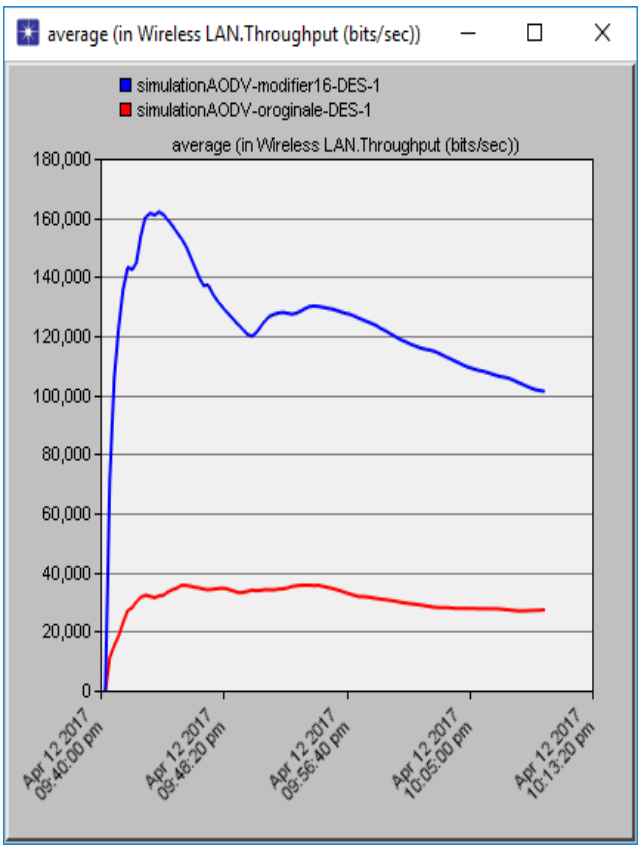


Figure 6.36: Débit (throughtput)

Dans le graphe :

Dans le scenario (originale) de la version originale on observe que, La quantité totaledes données qui arriveàladestination dela source (Throughput) est égale à27000bits/second, par contrepour le scenario (modifier16) de la version optimisé, est égale à 100.000 bits /second, il y a une grande amélioration, la différence est 73000 bits/second.

Le pourcentage d'augmentation de performance de débit (Throughput) : c'est 270% (2.7 fois).

Le résultat de la simulation dans les quatre graphes ci-dessus, montrent que le protocole AODV optimisé et plus performant que l'AODV par défaut, avec une modification des valeurs paramètres comme indique le tableau 6.3 suivant :

Route request retries	3
Route request rat limit (pkt /s)	10
Active route timeout (second)	2
Hello interval (second)	Uniform (1.1.1)
Allowed hello loss (second)	2
Net diameter	15
Node traversal time (second)	0.01
Route error rate limit (pck/sec)	10
Timeout buffeur	2
TTL start	1
TTL increment	2
TTL threshold	7
Local ad TTL	2

Tableau 6.3 : Paramètres de protocole (AODV) modifie

5. Conclusion

D'après l'analyse et les comparaisons des résultats obtenus, en conclut que la performance de notre version optimisée, est plus améliorée par rapport de la version originale, par la modification des valeurs des paramètres (Route request retries=3, Active route timeout (second) = 2, Allowed hello loss (second)= 2, Net diameter = 15, Node traversal time (second) = 0,01.

Cette modification améliore la performance de débit (throughput), jusqu'à 270% (2.7 fois), ainsi le délai (Delay) jusqu'à 1100% (11 fois), le total des paquets perdus (total packets dropped) jusqu'à 8,08% (0.08 fois), et le temps du découverte des routes (route discovry time) jusqu'à 890% (8.9 fois).

Conclusion générale et perspective

Dans le paradigme de réseau ad hoc mobile, il n'y a pas d'infrastructure fixe et les paquets sont livrés à leurs destinations par la connectivité sans fil. Les MANET sont en général caractérisés par des nœuds mobiles avec une énergie limitée, une capacité informatique limitée et l'absence de base Stations. Les nœuds mobiles s'engagent dans le rôle des routeurs qui s'engagent dans un protocole de routage requis pour décider et maintenir les routes. MANET permet la mobilité illimitée des terminaux mobiles tant qu'au moins un terminal dans la portée de transmission. . Les protocoles de routage réactifs sont favorisés chez les MANET car ils contribuent à réduire les charges réseau, en envoyant continuellement les données pour mieux communication. AODV montre par rapport aux autres protocoles de routage réactifs, une meilleure performance d'après beaucoup d'études de comparaison tel que « [Rajiv Misra and C.R Mandal référence performance comparison of AODV/DSR on-demand routing protocols for ad hoc networks in constrained situation], [Mohammed BOUHORMA and H. BENTAOUIT, A.BOUDHIR Performance Comparison of Ad-hocRouting Protocols AODV and DSR],[Asma Tuteja and M.TRajneesh Gujral and Sunil Thalia Comparative Performance Analysis of DSDV, AODV and DSR Routing Protocols in MANET using NS2]».

Dans notre travail, on a suivi une approche expérimentale (comparative), basé sur les tests de toutes les combinaisons possibles des valeurs de ces paramètres, avec l'outil de simulation OPNET 14.5.

Nous avons simulé un réseau ad hoc, avec 15 nœuds sur une surface de 5 km * 5 km, ainsi nous avons activé le protocole AODV dans ce réseau.

A travers les ensembles des scenarios simulés, nous avons évalué les valeurs de cinq paramètres par la comparaison avec les valeurs par defaults, un scénario final représente notre version optimisé, configuré par l'ensemble des valeurs des paramètres optimaux trouvées.

Les cinq paramètres optimisés sont : le nombre de perte de paquets hello **(Allowed_hello_loss),** le nombre de fois de demande de route **(Route request retries),** la durée de vie d'une route dans la table de routage **(Active route timeout (second)),**le diamètre de réseau, c'est le nombre maximal possible de sauts entre deux nœuds du réseau**(Net diameter)**, le Temps de Traverse de Nœud **(Node traversal time (second)).**

La comparaison se concentre sur l'ensemble des métriques de performance suivante :

Le temps de découverte de la route (route discovry Time), le totale des paquets perdus (total packets dropped), le débit du réseau (throughput), le Délai (Delay).

L'évaluation de performance de notre version AODV optimisé, par rapport la version originale, montre une meilleure amélioration du protocole, par exemple notre valeurs optimaux augmentent le débit (throughput), jusqu'à 270% (2.7 fois), ainsi diminue le délai (Delay) jusqu'à 1100% (11 fois).

D'après notre étude, on conclut qu'une meilleure optimisation de ce protocole de routage est possible, avec une modification de certains ses paramètres, sans modifié l'algorithme de protocole (code source).

Comme des travaux futurs, et perspectifs de ce projet, on peut citer des idées qui guident les chercheurs de ce domaine :

- Tester notre protocole AODV optimisé avec d'autre situation tel que : la mobilité des Nœuds dans le réseau, le diamètre de réseau, variation de nombre de nouds…etc.
- Construction d'une version AODV optimisé basé sur, la recherche de toutes les valeurs optimales des paramètres de ce protocole au lieu de cinq paramètres.
- Utilisation d'une approche heuristique basée sur des algorithmes de recherche, pour trouver les valeurs optimale des paramètres.
- chercher les valeurs optimales d'autre protocole de routage, réactif et proactif tel que DSR, OLSR, TORA….etc.

Bibliographie

[1] BOUDJAADAR Amina, Mémoire Pour l'Obtention du Diplôme de Magistère « Plateforme Basée Agents Pour l'Aide à la Conception et la Simulation des Réseaux de Capteurs Sans Fil » UNIVERSITE 20 AOUT 55 DE SKIKDA 2009/2010.

[2] Eric BOSASI DOYI 2010, Gestion des ressources radios dans les réseaux sans fils : cas d'un réseau WiMax, http://www.memoireonline.com le 20/04/2017.

[3] Saida HEDNA Université El Hadj Lakhdhar-BATNA, Mémoire Magister « Gestion De L'économie D'énergie Dans Les Réseaux Sans Fil 802.11 Ad Hoc ».

[4] Ahizoune Ahmed Pour l'Obtention du grade de **Maîtrise** « Un protocole de diffusion des messages dans les réseaux véhiculaires » Université de Montréal Canada 2011.

[5] https://fr.scribd.com/doc/ Houari MAOUCHI de TIZI-OUZOU, « Routage avec Qualité deService dans AOD » Université Mouloud MAMMERI 2009.

[6] Mohammad Ilyas The Handbook of Ad Hoc Wireless Networks Edited by Electrical Engineering Handbook., Florida Atlantic University Boca Raton, Florida 2002 « Body, Personal, and Local Ad Hoc Wireless Networks » Marco Conti Consiglio Nazionale delle Ricerche.

[7] Abdesselem BEGHRICHE MÉMOIRE DE MAGISTÈRE EN INFORMATIQUE « De la Sécurité à l'E-Confiance basée sur la Cryptographie à Seuil dans les Réseaux sans fil Ad hoc » 2009.

[8] J. Westcott and G. Lauer, « Hierarchical routing for very large networks » Proceeding of the IEEE MILCOM 1984, pp. 214-218, 21-24 Octobre 1984.

[9] Frédéric BESSE Thèse « Réseaux ad hoc aéronautiques » université de Toulouse France2013.

[10] BOUKHECHEM Nadhir Mémoire Présenté en vue de l'obtention du diplôme de Magister en informatique « ROUTAGE DANS LES RESEAUXMOBILES AD HOC PAR UNE APPROCHE A BASE D'AGENTS » Université de Constantine 2008.

[11] Abdelmajid HAJAMI THÈSE de Doctorat « Sécurité du routage dans les réseaux sans fil spontanés : cas du protocole OLSR » Université Mohammed V Souissi Rabat Maroc.

[12] Abderrezak Rachedi THÈSE pour obtenir le diplôme de DOCTORAT « Contributions à la sécurité dans les réseaux mobiles ad Hoc » Université d'Avignon et des Pays de Vaucluse

[13] YAHIATENE Youcef MEMOIRE DE MAGISTER « Traffic Encryption Keys distribution models in Mobile Ad hoc Networks (Distribution de clés dans un réseau dynamique) » université M'Hamed Bougara de Boumerdes

[14] BERRABAH Abdelkrim diplôme de Master « Balancement de charges dans les

réseaux Ad Hoc » Université Abou Bakr Belkaid– Tlemcen 2013

[15] Mandicou BA Thèse pour obtenir le diplôme de DOCTORAT « Vers une structuration auto-stabilisante des réseaux ad hoc: cas des réseaux de capteurs sans fil » Universite de Reims Champagne-Ardenne, France 2014.

[16] Mehdi Bouallegue. Pour l'obtention du grade de Docteur « Protocoles de communication et optimisation de l'énergie dans les réseaux de capteurs sans fil » Réseaux et télécommunications Université du Maine, France 2016.

[17] Yassine SNOUSSI pour l'obtention de la Maîtrise « mécanisme de sécurité pour la famille de protocoles ad-hoc olsr organisés en grappes (clusters) » université du Québec Canada 2011.

[18] Abderrezak RACHEDI THÈSE pour l'obtenir le diplôme de DOCTORAT « Contributions à la sécurité dans les réseaux mobiles ad Hoc » Université d'Avignon France 2012.

[19] Tahar Abbas Mounir thèse pour l'obtenir le diplôme de DOCTORAT « Proposition d''un protocole à économie d'énergie dans un réseau hybride GSM et AD HOC » Université d'Oran 2012.

[20] Nabil Ammar TABBANE Pour obtenir le grade de DOCTEUR « Modèles Stochastiques pour la Prévision de la Qualité de Service dans les Réseaux Ad Hoc Multimédia » Université de Versailles Saint Quentin en yvelines 2006.

[21] S. Corson University of Maryland, J. Macker Naval Research Laboratory « Mobile Ad hoc Networking (MANET):Routing Protocol Performance Issues and Evaluation Considerations » Network Working Group Corson & Macker Informational 1999 RFC 2501.

[22] Chai-Keong Toh « A novel distributed routing protocol to support ad-hoc mobile computing »; University of Cambridge Computer Laboratory IEEE 15th Annual Int. Phoenix Conf., pp. 480–486, University of Cambridge Computer Laboratory United Kingdom 1996.

[23] BERRABAH Abdelkrim pour l'obtention du diplôme de Master « Balancement de charges dans les réseaux Ad Hoc » Université Abou Bakr Belkaid– Tlemcen 2013.

[24] Dominique Dhoutaut thèse pour obtenir Le grade de docteur « Etude du standard IEEE 802.11 dans le cadre des réseaux ad hoc : de la simulation à l'expérimentation. » Institut national des Sciences Appliquées de Lyon France 2003.

[25] Saloua CHETTIBI Mémoire de Magister « Protocole de routage avec prise en compte de la consommation d'énergie pour les réseaux mobiles ad-hoc » Université Mentouri Constantine 2008.

[26] BOUZAHER Abdelaziz Mémoire l'obtention du diplôme de Magister

« Approche agent mobile pour l'adaptation des réseaux mobiles ad hoc »
Université Mohamed Khider Biskra.

[27] Sedrati Maamar, Aouragh Lamia, Guettala Leila, Bilami Azeddine « Etude des Performances des Protocoles de Routage dans les Réseaux Mobiles Ad-Hoc » Université El Hadj Lakhdar - Batna. 4th International Conférence on Computer Intgrated Manufacturing CIP'03-04 November 2007.

[28] Jean-Michel « Hybridation entre les modes ad-hoc et infrastructure dans les r´eseaux de type Wi-Fi » Universit´e Libre de Bruxelles Belgique 2006.

[29] Dr. Gerard McLean « Routing in Ad Hoc Networks of Mobile Hosts » University of Victoria, Victoria, BC, Canada 1998. http://ghost.lesiuk.org/AdHoc/adhoc/

[30] Marine Minier INSA de Lyon « Sécurité dans les réseaux ad hoc » http://perso.citi.insa-lyon.fr/mminier/images/MASTER_part2.pdf le 10/05/2017

[31] Charles E. Perkins IBM, T.J. Watson Research Center, Pravin Bhagwat Computer Science Department University of Maryland « Highly Dynamic Destination-Sequenced Distance-VectorRouting (DSDV) for Mobile Computers » SIGCOMM 94 London England UK

[32] Bryan Cameron LesiukMasters Of Applied Science « DynamicRouting for Measurement Networks » University of Victoria, Canada 1994.

[33] Kamal OUDIDI Thèse pour obtenir le grade de Docteur en Sciences Appliquées « Systèmes d'Information Multimédia et Mobile à l'Ecole Nationale Supérieure d'Informatique et d'Analyse des Systèmes » Université Mohammed V – Souissi RABAT Maroc.

[34] Mohamed Ali Ayachi THÈSE pour obtenir le grade de Docteur « Sécurité du routage dans les réseaux sans fil spontanés : cas du protocole OLSR » Université Mohammed V Souissi Rabat Maroc. 2011

[35] Anuj K. Gupta, Member, IACSIT, Dr. Harsh Sadawarti, Dr. Anil K. Verma « Performance analysis of AODV, DSR & TORA Routing Protocols » IACSIT International Journal of Engineering and Technology, Vol.2, No.2, April 2010 ISSN: 1793-8236.

[36] Sakuna CHAROENPANYASAK Thèse pour obtenir le grade de DOCTEUR « Optimisation inter-couches du protocole SCTP en réseaux ad hoc » Université De Toulouse France 23/06/2008.

[37] Guizani Badreddine.(2012). Algorithme De Clustérisassions Et Protocoles De Routage Dans Les Réseaux Ad Hoc. Thèse de doctorat de l'université de Technologie de Belfort-Montbéliard Tunisie.

[38] David Oliver Jörg « Performance Comparison Of MANET Routing Protocols In Different Network Sizes » Institute of Computer Science and Applied Mathematics Computer Networks and Distributed Systems (RVS) University of Berne, Switzerland 2003.

[39] Dinesh Singh1, Ashish K. Maurya2, Anil K. Sarje « Comparative Performance Analysis of LANMAR, LAR1, DYMO and ZRP Routing Protocols in MANET using Random

Waypoint Mobility Mode » Department of Electronics & Computer Engineering Indian Institute of Technology Roorkee Roorkee, India, IEEE 2011.

[40] Shaily Mittal, Prabhjot Ka Institute of Technology and Management, Gurgaon « PERFORMANCE COMPARISION OF AODV, DSR and ZRP ROUTING PROTOCOLS IN MANET'S » International Conference on Advances in Computing, Control, and Telecommunication Technologies 2009.

[41] Tony Larsson, Nicklas Hedman MASTER'S THESIS « Routing Protocols in Wireless Ad-hoc Networks A Simulation Study » Luleå University of Technology Stockholm, Suède 1998.

[42] Mukesh Kumar, Rahul Rishi, D.K. Madan « Comparative Analysis of CBRP, DSR, AODV Routing Protocol in MANET » The Technological Institute of Textile and Science, Bhiwani-127021, Haryana – Indi Mukesh Kumar et. al. / (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 09, 2010, 2853-2858.

[43] Ms. Deepika M. Tech Student, « Cluster Based Routing Protocol in MANETs » Department of Computer Science & Engineering MDU Maharshi Dayanand University Rohtak (Haryana) India, international Journal of in Multidisciplinary and Academic Research (SSIJMAR) Vol. 5, No.2, April 2016 (ISSN 2278–5973).

[43] Seyed-Amin Hosseini-Seno, Tat-Chee Wan, Rahmat Budiarto « Energy Efficient Cluster Based Routing Protocol for MANETs » Universiti Sains Malaysia, Penang, Malaysia 2009 International Conference on Computer Engineering and Applications PCSIT vol.2(2011) © (2011) IACSIT Press, Singapore.

[44] Seyed-Amin Hosseini-Seno, Tat-Chee Wan, Rahmat Budiarto « Energy Efficient Cluster Based Routing Protocol for MANETs » Universiti Sains Malaysia, Penang, Malaysia 2009 International Conference on Computer Engineering and Applications PCSIT vol.2(2011) © (2011) IACSIT Press, Singapore.

[45] Imran Khan and Amir Qayyum « Performance Evaluation of AODV and OLSR in Highly Fading Vehicular Ad hoc Network Environments » Center of Research in Networks and Telecom (CoReNeT) M. A. Jinnah University, Jinnah, 978-1-4244-4873-9/09/$25.00 ©2009 IEEE.

[46] Elizabeth M. Royer Dep. Of Electrical and Computer Engineering University of California Santa Barbara, And Charles E. Perkins Networking and Security Center Sun Laboratory « An Implementation Study of the AODV Routing Protocol ».

[47] Mahesh K. Marina Samir R. Das « On-demand Multipath Distance Vector Routing in Ad Hoc Networks » Department of Electrical & Computer Engineering and Computer Science University of Cincinnati U.S.A

[48] HONG-PENG WANG, LIN CUI « An Enhanced Aodv For Mobile Ad Hoc Network » Mobile Computing Center, Department of Computer Science and Technology, HIT SGS, Shenzhen 518055, China, Proceedings of the Seventh International Conference on Machine Learning and Cybernetics, Kunming, 12-15 July 2008.

[49] Catherine Loison Thomas Ruocco Camille Rives « Routage multicast dans les réseaux véhiculaires (VANET) » Université Avignon France 2013.

[50] Yihai Zhang « Quality of Service for Ad hoc On-demand Distance Vector Routing » A Thesis for the Degree of Master Department of Electrical and Computer Engineering University of Victori 2005.

[51] Krishna Gorantala « Routing Protocols in Mobile Ad-hoc Networks » Master's Thesis in Computing Science, Umea University Department of Computing Science SWEDEN 2006.

[52] Malika BELKADI THESE DE DOCTORAT « Contrôle intelligent de flux capable de s'adapter à l'état d'un MANET » UNIVERSITE MOULOUD MAMMERI DE TIZI OUZOU

[53] Mariam Dawoud DEA d'Informatique « Analyse du protocole AODV » Université libanaise Paul Sabatier – I.R.I.T Faculté des sciences 2006.

[54] Boulkamh Chouaib « Prise en Compte de la QoS par les Protocoles de Routage dans les Réseaux Mobiles Ad Hoc » Université El Hadj Lakhdar de Batna 2008.

[55] C. Perkins Nokia Research Center E. Belding-Royer University of California, Santa Barbara S. Das University of Cincinnati « Ad hoc On-Demand Distance Vector (AODV) Routing » July 2003.

[56] BELGHACHI Mohamed Faculté des sciences et technologies, Université de Béchar; FEHAM Mohammed Laboratoire STIC, Faculté des sciences de l'Ingénieur, Université de Tlemcen « Conception d'une nouvelle approche pour le routage dans un réseau de capteurs sans fil » MajecSTIC 2009 Avignon, France, du 16 au 18 novembre 2009.

[57] Youcef Ziani Comme Exigence Partielle De La Maîtrise En Génie Electrique « Etude Comparative De Méthodes De Routage Dans Les Réseaux Decapteurs Sans Fil Pour Le Domaine Résidentiel » 'Université Du Québec A Trois-Rivières CANADA 2013.

[58] Rakesh kumar, Siddharth Kumar, Sumit Pratap Pradhan, Varun Yadav, Rakesh kumar et al. / International Journal on Computer Science and Engineering (IJCSE) « Modified route-maintenance in AODV Routing protocol using static nodes in realistic mobility model » Department of Computer Science and Engineering, Madan Mohan Malaviya Engineering College, Gorakhpur, India, Vol. 3 No. 4 Apr 2011.

[59] KAIS MNIF Thèse à l'obtention du Doctorat en génie ph.d. « Construction et Maintenance d'une Dorsale Virtuelle dans les Reseaux Ad Hoc Mobiles » Ecole De Technologie Supérieure Université Du Québec CANADA 2006.

[59a] Junseok Kim AODV « implementation on TinyOS-2.x » PhD Candidate Department of Electric and Computer Engineering (ECE), University of Arizona États-Unis 2011. http://www2.engr.arizona.edu/~junseok/AODV.html

[60] Larousse français.

[61] Ricki G. Ingalls « INTRODUCTION TO SIMULATION » School of Industrial Engineering and Management 322 Engineering North Oklahoma State University Stillwater, OK 74078, U.S.A. Proceedings of the 2008 Winter Simulation Conference

[62] Ruth Thomas What Are Simulations? –TheJeLSIMPerspective2003. http://www.jelsim.org/

[63] Dr. Mourad Ykhlef King « IS 466 – Simulation » Saud University, College of Computer & Information Sciences Arabie saoudite http://faculty.ksu.edu.sa

[64] Pierre-jean Erard ouvrage simulation par évènement discrets 1996 1er Edition

[65] S. Mehta, Mst. NajninSulatan, H.Kabir, N.Ullah and K. S. KwakInha « Network and System Simulation Tools for Next Generation Networks » A Case Study Inha University Korea 2010.

[65a] https://fr.scribd.com/doc/53640582/OPNET-14-5-Installation-for-Windows19.05.2017

[66] www.mindtools.com

[67] https://academiccollegeprojects.com/opnet-projects/

[68] Juan LU thèse de doctorat « Modeling, simulation and implementation of an 802.15.4 based adaptive communication protocol in wirelesssensor network: application to monitoring the elderly at home » Université de Toulouse France février 2013.

[69] Nabil Tabbane, Sami Tabbane SUPCOM Tunisia , Ahmed Mehaoua University of Versailles France « SIMULATION ET MESURE DES PERFORMANCES DU PROTOCOLE DE ROUTAGE AODV » JTEA'2004, 21 au 22 Mai 2004, Hammamet, Tunisie.

[70] WADHAH AL-MANDHARI, NOBUO NAKAJIMA, KOICHI GYODA Department of Human Communications The University of Electro-Communications Tokyo JAPAN, « Ad-hoc On Demand Distance Vector (AODV) Performance Enhancement with Active Route Time-Out parameter » Shibaura Institute of Technology**, journal** *WSEAS Transactions on Communications*, *7*(9), 912-921. 2008.

[71] Teresa Albero-Albero, Salvador Santonja-Climent, Víctor-M. Sempere-Payá, Instituto Tecnológico de Informática Universidad Politécnica de Valencia Spain, Jordi Mataix-Oltra, Universidad Politécnica de Cataluña (UPC) Spain, « AODV Performance Evaluation and Proposal of Parameters Modification for Multimedia Traffic on Wireless Ad hoc Networks » Publisher: IEEE DOI: 10.1109/WD.2009.5449691, 2009.

[72] D K Lobiyal, C P Katti, Jawaharlal Nehru University, New Delhi, India, A K Giri, Krishna Institute of Engineering &Technology, Ghaziabad, India « Parameter Value Optimization of Ad-hoc On Demand Multipath Distance Vector Routing using Particle Swarm Optimization » International Conference on Information and Communication Technologies (ICICT 2014) www.sciencedirect.com.

[73] Amol R. Kotkar, Nilesh S. Vani, Assistant Professor, Department of Computer Engineering, GF's Godavari College of Engineering, Jalgaon India « Performance Analysis of AODV Routing Protocol in MANET: An Overview » International Journal of Scientific Engineering and Research (IJSER), ISSN (Online): 2347-3878, Impact Factor (2014): 3.05, www.ijser.in, Paper ID: IJSER15134 May 2015.

[74] Samiksha Nikam, College of Conputer Application for Women's University, Mumbai, Santacruz(w) India, B.T. Jadhav Y.C. Institute of sciences, Satara, University, Kolhapur India « Analysis of AODV Protocol against Pause Time Using NS2.34 » I.J. Wireless and Microwave Technologies, 2016, 6, 63-71 Published Online November 2016 in MECS(http://www.mecs-press.net) DOI: 10.5815/ijwmt.2016.06.07.

[75] Rajiv Misra and C.R Mandal « Performance comparison of AODV/DSR on-demand routing protocols for ad hoc networks in constrained situation » Personal Wireless Communications, 2005. ICPWC 2005. 2005 IEEE International Conference on, 23-25 Jan. 2005.

[76] Mohammed BOUHORMA, H. BENTAOUIT, A.BOUDHIR, Département Génie Informatique, ERIT Faculté des Sciences et techniques de Tanger Tanger Maroc « Performance Comparison of Ad-hoc Routing Protocols AODV and DSR » Conference: Multimedia Computing and Systems, 2009. ICMCS '09. IEEE, International Conference on May 2009.

[77] Asma Tuteja, Rajneesh Gujral , Sunil Thalia , « Comparative Performance Analysis of DSDV, AODV and DSR Routing Protocols in MANET Using NS2 » 2010 International Conference on Advances in Computer Engineering 20-21 June 2010 India.

[78] Yahia KORICHI Otmane BOUHAMIDA, Master en Informatique « Modélisation et simulation du problème du trou noir dans les réseaux mobiles P2P » Université Kasdi Merbah – Ouargla 2013.