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 :

Un protocole de routage optimisé dans les réseaux Ad Hoc

Présenté par :

Aissaoui Bouthaina **Hemaizia Zineb**

Devant le jury:

Président : M. S. Souahi	M.A.A	Université de Tébessa
Encadreur : M. Mahmoudi	M.A.A	Université de Tébessa
Examinateur : A. Metrouh	M.A.A	Université de Tébessa

Date de soutenance : 30/05/2016

Note : **Mention :**

Promotion : 2015 – 2016

REMERCIEMENTS

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 a nos parents qui nous ont toujours soutenues, encouragé et aidé, ils ont su de nos données toutes les chances pour réussir.

Résumé

Les réseaux mobiles Ad Hoc appelés généralement MANET (Mobile Ad Hoc Network) sont devenus de plus en plus populaires ces dernières années, en raison de l'importance des domaines d'application des réseaux Ad Hoc. Ils sont un nouveau type de réseaux basés sur la technologie sans fil. Les réseaux Ad Hoc sont des systèmes autonome communique avec des ondes radio sans infrastructure. La communication entre les nœuds de réseaux MANET nécessite des protocoles de routage à cause de topologie dynamique et l'absence d'administration centrale, parmi les protocoles existants est le protocole AODV qui offre des meilleures performances que les autres protocoles de routage MANET.
Le besoin de débit ne cesse pas de croitre à cause des applications multimédia, ce qui nécessite de changer la métrique de meilleur chemin au débit au lieu de nombre de sauts. Une version modifiée d'AODV donne une optimisation considérable cotée débit, ceux qui montrent les tests et comparaisons de simulation de ce travail par OPNET.

Mots clés :

MANET, Protocole de routage, simulation, OPNET, AODV, optimisation.

Abstract

Mobile Ad Hoc networks generally called MANET (Mobile Ad Hoc Network) have become increasingly popular in recent years, due to the importance of the application areas of Ad Hoc networks. They are a new type of networks based on wireless technology.
Ad Hoc networks are autonomous systems communicate with radio waves without infrastructure.
Communication between MANET network nodes requires routing protocols because of dynamic topology and lack of central administration, among existing protocols is the AODV protocol that offers better performance than other MANET routing protocols.
The needs for throughput continue to grow because of multimedia applications, which require changing the metrics best way to throughput instead, the number of hops.
A modified version of AODV gives considerable throughput optimization, those who show the simulation tests and comparisons of this work by OPNET.

Keywords:

MANET, routing protocol, simulation, OPNET, AODV, optimization.

الملخص

الشبكات الغير ثابتة Ad Hoc تسمى عموما MANET(MOBILE AD HOC NET WORK) أصبحت هذه السنوات الأخيرة شعبية أكثر فأكثر بسبب أهمية ميادين تطبيقاتها. شبكات Ad Hoc هي نوع جديد من الشبكات ترتكز على التكنولوجيا اللاسلكية ، شبكات Ad Hoc هي أنظمة مستقلة تتصل باستعمال موجات الراديو ودون بنية تحتية.

الاتصال بين عقد الشبكة MANET تحتاج إلى بروتوكولات التوجيه بسبب الطبولوجيا المتحركة وغياب إدارة مركزية،من بين البروتوكولات الموجودة هناك البروتوكول AODV الذي يوفر أفضل فعالية مقارنة بروتوكولات التوجيه الأخرى لل MANET .

الاحتياج للتدفق لم يتوقف عن النمو بسبب تطبيقات الميلتيميديا ، مما تطلب تبديل قياس أفضل طريق إلى التدفق بدلا من عدد الخطوات النسخة المعدلة من AODV أعطت تحسين معتبر من جهة التدفق هذا ما بينته التجارب و المقارنات لمحاكاة هذا العمل باستعمال برنامج OPNET.

الكلمات المفتاحية

بروتوكول التوجيه، MANET ، المحاكاة، OPNET، AODV، التحسين.

Liste des figures

Chapitre 01 : Généralité sur les réseaux Ad Hoc

Chapitre 02 : Les protocoles de routage Ad Hoc

Chapitre 03 : Le protocole de routage AODV

Chapitre 04 : La simulation et les simulateurs réseau

Chapitre 05 : Optimisation de protocole de routage AODV basée sur le débit dans le calcul de meilleur chemin

Chapitre 06 : Tests et résultats

Liste des tableaux

Chapitre 02 : Les protocoles de routage Ad Hoc

Chapitre 03 : Le protocole de routage AODV

Chapitre 06 : Tests et résultats

Glossaire des acronymes et des notations

Acronyme	Description
AODV	Ad-Hoc On Demand Routing Vector.
DES	Data Encryption Standard.
DSR	Dynamic Source Routing.
DSDV	Destination Sequenced Distance Vector.
MANET	Mobile Ad-Hoc Network.
NS-2	Network Simulator version 2.
IETF	Internet Engineering Task Force.
OPNET	Optimized Network Engineering Tools.
OLSR	Optimized Link State Routing.
RERR	Route Error.
RREQ	Route Request.
RREP	Route Reply.
TTL	Time-To-Live.
WiFi	Wireless Fidelity.
WLAN	Wireless Local Area Network.
WMAN	Wireless Metropolitan Area Network.
WWAN	Wireless Wide Area Network.
ZRP	Zone Routing Protocol.

Table des matières

Chapitre 03 : Le protocole de routage AODV

Chapitre 04 : La simulation et les simulateurs réseau

Chapitre 05 : Optimisation de protocole de routage AODV basée sur le débit dans le calcul de meilleur chemin

Chapitre 06 : Tests et résultats

Introduction générale

Depuis l'apparition des réseaux informatiques, ce domaine a connu une évolution sans cesse notamment sur le plan physique et artistique. Avec le développement constant des technologies, l'utilisation des systèmes d'information s'est transformée. Elle s'exprime notamment par un besoin de mobilité des utilisateurs. Les réseaux sans fil sont en plein développement du fait de la flexibilité de leur interface, qui permet à un utilisateur de changer facilement de place. Différentes catégories des réseaux sans fil existent suivant leur étendue (WPAN, WLAN, WMAN, WWAN). Ces dernières années le développement de la technologie sans fil a ouvert de nouvelles perspectives dans le domaine des télécommunications. L'utilisation des terminaux mobiles impose l'emploi d'une infrastructure (points d'accès) parfois coûteuse ou difficile à implanter. De fait, cette solution n'est pas toujours envisageable. Il existe deux types de réseaux mobiles, les réseaux mobiles avec infrastructure et les réseaux mobiles Ad Hoc. Les réseaux mobiles avec infrastructure sont basés sur un ensemble de sites fixes appelés stations de base, ces sites vont relier les différents noeuds mobiles pour former un réseau interconnecté. Par conséquent, des réseaux mobiles dépourvus d'infrastructure ont été déployés. Ces réseaux sont plus connus sous le nom de réseaux Ad Hoc mobiles ou MANETS (Mobile Area NETWORKS).

Un réseau mobile Ad Hoc (MANET) est formé d'équipements sans-fil et mobiles qui s'auto-organisent sans l'aide d'une quelconque infrastructure qui peuvent communiquer directement entre eux s'ils sont situés à portée radio.

La portée des stations de MANET étant relativement limitée, le déploiement d'un réseau à grande échelle nécessite des stations intermédiaires fassent le travail de point de relais permettant des communications grâce à des protocoles de routage spécifiques. Comparativement aux réseaux sans-fil à infrastructure, les nœuds d'un MANET sont davantage sujets aux interférences, à des pertes de données, à des temps d'accès au médium plus long. Parmi les caractéristique de réseau Ad Hoc est que les unités mobiles disposent des ressources matérielles limitées et hétérogènes en terme de batterie et de puissance de calcul et, la mobilité des nœuds génère une topologie dynamique. De plus, la capacité des liens sans fil s'avère relativement limitée offrant par conséquent un débit modeste comparé aux réseaux filaires.

Les réseaux MANETS, grâce à leur auto-organisation peuvent être mis en place facilement et économiquement selon les besoins. Ils offrent en effet un large éventail d'applications, notamment dans les situations géographiques avec des contraintes terrestres telles que les champs de bataille, les applications militaires, les réseaux véhiculaires, d'autres situations d'urgence et de catastrophe, l'embarqué (intégré récemment dans le secteur automobile pour accroître la sécurité des usagers en les informant d'éventuels obstacles sur leur itinéraire) et le cas de la vie courante de l'utilisation des réseaux Ad Hoc. C'est le cas par exemple du réseau créé entre un professeur et ses étudiants pour le besoin d'une séance de cours ou le réseau créé entre les participants à une réunion ou même entre les voyageurs dans un train.

Le problème qui se pose dans ce contexte est l'adaptation de la méthode d'acheminement des données (routage) entre les composants du réseau. Le routage est une fonction important dans les MANETS 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. Les recherches actuelles dans les réseaux Ad Hoc sont dirigées vers les algorithmes de routage.

Plusieurs protocoles de routage ont été développés, chaque protocole essaye de maximiser les performances du réseau Ad Hoc. Le protocole de routage dissémine des informations de routage nécessaires à l'obtention et à la maintenance des routes. Suivant le type de dissémination de l'information, 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'amélioration du protocole de routage réactif AODV (Ad Hoc On-Demand Distance Vector routing).

AODV est un protocole capable de routage unicast et multicast. C'est un protocole de routage à vecteurs de distance. Ce protocole utilise un numéro de séquences dans l'envoi de ces paquets pour éviter les boucles de routage. Il stocke les routes utilisées dans sa table de routage.

Au vu de ses caractéristiques, ce protocole est devenu très connu et beaucoup de travaux ont déjà été réalisés à son propos. Il est tout à fait adapté aux réseaux mobiles Ad Hoc de part sa prise en charge de la mobilité des nœuds dans le réseau, un autre avantage de ce protocole est sa simplicité. Ensuite son ancienneté et sa maturité, AODV existe depuis longtemps.

Dans la littérature, Plusieurs travaux de comparaison sur les protocoles de routage AODV, ces comparaisons montrent que AODV en général est plus performant quelque soit l'environnement de réseau tel que le diamètre de réseau, le nombre de nœuds, la mobilité...etc.

Malgré sa performance des nouveaux besoins sont apparies tel que le besoin de débit ce qui oblige de modifié l'un des caractéristiques principale, qui est la procédure de découverte de route basé sur le nombre de sauts qui nous donne pas toujours des routes à haut débit, le cadre de notre travail est de chercher la modification de ce métrique (nombre de sauts) qui donne des chemins avec meilleur débit.

Problématique

La transmission d'un paquet d'une source vers une destination nécessite un protocole de routage qui achemine les paquets par le "meilleur" chemin, le meilleur chemin pas forcement le plus court chemin suivant la conception d'AODV orignal, le meilleur chemin pour les applications de ces derniers jours qui sont basé sur le multimédia, est le chemin de débit le plus élevé.

Le problématique de ce travail est comment changer la métrique de meilleur chemin et comment tester son performance, on peut le reformuler notre problématique par les sous problématique suivantes:

- Comment changer la métrique de meilleur chemin, et le débit devient le cout à minimiser pour calculer le meilleur chemin.
- Comment choisir l'outil et l'environnement de réalisation de cette optimisation.
- Comment évaluer la performance de réseau par notre modification.
- Quelle sont les paramètres d'évaluation en relation de débit et quel sont les outils de réalisation de cette évaluation.
- Quelle est la référence de comparaison pour évaluer la performance.
- Comment interpréter les résultats obtenus.

Objectifs

Notre objectif est de concevoir et réaliser une version modifiée d'AODV ou la métrique de déterminer le meilleur chemin deviens le débit au lieu de nombre de saut et d'évaluer la performance de ce dernier.

Pour atteindre cet objectif, on peut le reformuler suivant les sous objectifs suivants:

- Conception et réalisation d'un protocole AODV optimisé, où on fait des modifications dans le fonctionnement de protocole AODV, les modifications concernent la création des routes en fonction de débit au lieu de nombre de sauts.
- Création et simulation de notre protocole AODV optimisé par OPNET.
- Evaluation des performances de notre protocole optimisé à travers deux scénarios où dans le premier scénario on change la quantité de trafic dans le réseau et dans le deuxième on change le nombre des nœuds.
- Génération du graphe de statistique concernant les métriques en relation avec le débit telles que le débit de réseau, le nombre des paquets reçu et le délai.
- Comparaison des résultats de simulation de protocole réactif AODV par défaut et le protocole AODV optimisé.
- Analyse des résultats obtenus.

Ce mémoire est structuré en 6 chapitres comme suit:

- **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,** on a parlé en la notion de routage et nous présentons à ce niveau une classification des différentes approches pour le routage dans ce type de réseaux.
- **Le troisième chapitre,** nous allons présenter le protocole de routage AODV, en donnant une description détaillée de ce protocole et son principe de fonctionnement.
- **Le quatrième chapitre,** nous allons présenter les différents types des simulateurs, et l'environnement de notre travail OPNET.
- **Le cinquième chapitre,** nous commençons par une création de notre modèle de simulation. Nous proposons ensuite autre perspectives travail.
- **Le sixième chapitre,** nous allons présenter les résultats de simulation et une comparaison entre les deux versions du protocole: AODV et AODV optimisé. Enfin, nous terminons la mémoire par une conclusion générale et perspective.

CHAPITRE I

Généralité Sur Les Réseaux Ad Hoc

INTRODUCTION

L'évolution rapide de la technologie de la communication sans fil, a permis la manipulation des données à travers des unités de calculs portables. Les environnements mobiles permettent une grande flexibilité d'emploi. En particulier les réseaux sans-fil Ad Hoc ou MANET (Mobile Ad Hoc NETWORK) sont des systèmes autonomes ne nécessitent aucune infrastructure préalable.

Dans cette partie de travail nous visions à donner un aperçu sur les réseaux Ad Hoc, nous commençons par définir les réseaux sans fil et citer les deux classes de ce réseau, ensuite nous allons définir le réseau Ad Hoc ainsi que les principaux caractéristique de ce réseau, les avantages offert et les inconvénients. Enfin nous donnons les domaines d'application de ce réseau.

1. DEFINITION

Un réseau sans fil est un réseau informatique ou numérisé qui connecte différents postes ou systèmes entre eux par ondes radios. Le réseau sans fil peut associer à un réseau de télécommunication pour réaliser des interconnexions entre nœuds. Ces réseaux de communications permettent aux utilisateurs de profiter de tous les services traditionnels des réseaux indépendamment de leurs positions géographiques. Le rayonnement géographique des ondes est relativement limite étant donne la faible puissance d'émission des solutions matérielles actuelles. Pour cette raison, les réseaux sans fil se sont avant tout développés comme réseaux internes, propres à un bâtiment, soit comme réseau d'entreprise, soit comme réseau domestique. **[1]**

2. LES CATEGORIES DES RESEAUX SANS FIL

Les réseaux sans fil peuvent avoir une classification selon deux critères. Le premier est la zone de couverture du réseau. Au vu de ce critère il existe quatre catégories: les réseaux personnels, les réseaux locaux, le réseau métropolitain et les réseaux étendus. Le second critère est l'infrastructure ainsi que le modèle adopté. Par rapport à ce critère on peut diviser les réseaux sans fils en: réseaux avec infrastructures et réseaux sans infrastructure (Ad Hoc). **[3]**

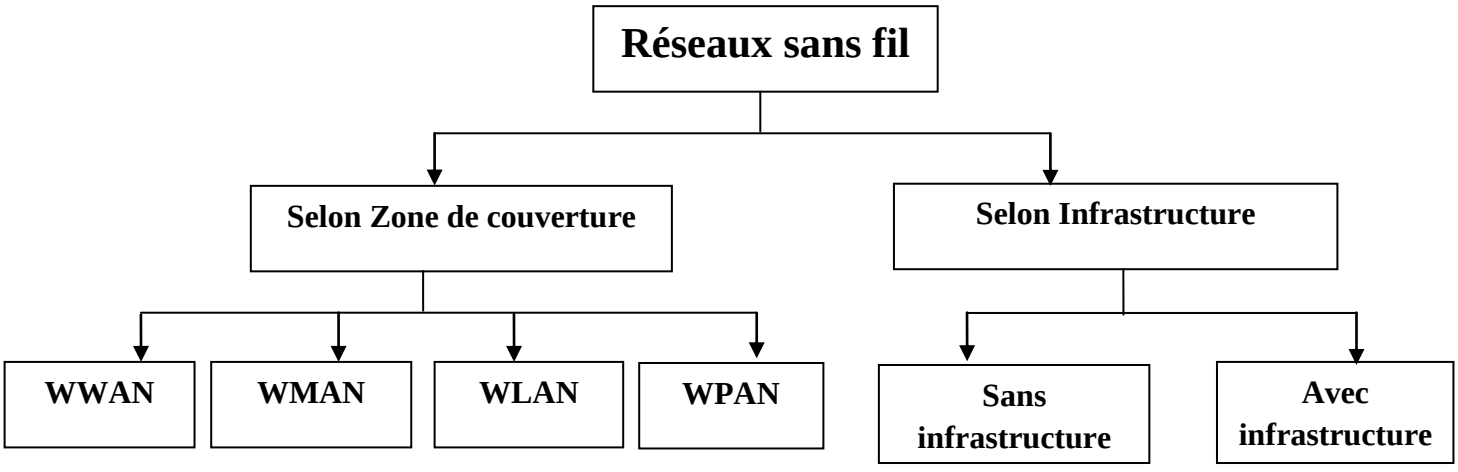


Figure 1.1: Classification des réseaux sans fils.

2.1. Selon la zone de couverture

a. Réseaux personnels sans fil (WPAN)

Les réseaux personnels sans fil ou Wireless Personal Area Network (WPAN), sont des réseaux sans fil à très faible portée, de l'ordre d'une dizaine de mètres. Ils sont le plus souvent

utilisés à faire communiquer entre eux des matériels présents sur une personne (par exemple une oreillette et un téléphone portable). Ils sont également utilisés pour relier des équipements informatiques entre eux sans liaison filaire : par exemple pour relier une imprimante ou un PDA (Personal Digital Assistant) à un ordinateur de bureau ou faire communiquer deux machines très peu distantes. **[3]**

Il existe plusieurs technologies permettant la mise en œuvre de tels réseaux qui sont:

- **Bluetooth**
  La norme Bluetooth (pris en charge par IEEE 802.15.1) est une technologie de moyen débit, elle permet d'atteindre un débit maximal théorique de 1Mbps (environ 720Kbps effectif) à basse consommation énergétique. Bluetooth utilise la bande de fréquence 2.4GHz avec une couverture entre 10 et 30 mètres. Cette technologie permet de créer un réseau de 8 appareils en communication simultanée. La petite taille des composants Bluetooth lui permet d'être inséré dans des équipements tels que les claviers et les souris sans fil, les kits main libre ou écouteur et le transfert de données entre un pc et les PDA (Personal digital assistant) ou téléphones mobiles…etc. **[2]**
- **ZigBee**
  Le standard IEEE 802.15.4 propose une norme pour les couches physique et liaison de données, orientée très faible consommation énergétique, qui rend cette technologie bien adaptée à de petits appareils électroniques (appareils électroménagers, hifi, jouets,.. .), et plus particulièrement aux réseaux de capteurs. La pile proposée par l'IEEE et la ZigBee qui a pour objectif de promouvoir une puce offrant un débit relativement faible (100Kbps environ) mais à un coût très bas, et une consommation électrique extrêmement réduite. **[4] [3]**
- **Liaisons infrarouges**
  Avant l'arrivée des technologies radio comme le Wi-Fi et le Bluetooth, il était malgré tout possible de transférer des données sans fil entre deux appareils, grâce à l'infrarouge. L'IrDA est une technologie qui a été très utilisée dans les années 90 et début des années 2000, surtout sur les téléphones, les PDA et les PC portables. L'IrDA utilise un signal infrarouge, de la même façon que les télécommandes de télévision par exemple, pour effectuer des transferts entre deux périphériques. Le fonctionnement est simple : une lampe émet un rayonnement dans l'infrarouge (invisible pour les humains) avec une fréquence qui permet de travailler en binaire. L'infrarouge a plusieurs défauts: la portée est limitée (entre 5 et 1 mètre), il est nécessaire d'aligner les périphériques (dans un cône de 15° environ) et aucun obstacle ne doit séparer les deux appareils. Actuellement, les usages informatiques ont presque totalement disparu, mais beaucoup de sociétés utilisent encore de l'infrarouge pour leurs télécommandes (l'infrarouge est omniprésent dans le monde audio/vidéo). La raison est simple: la technologie est bien maîtrisée, efficace et consomme peu**. [5]**

b. Réseaux locaux sans fil (WLAN)

Depuis le développement des normes qui offrent un haut débit, les réseaux locaux sans fil ou Wireless Local Area Network (WLAN) sont généralement utilisés à l'intérieur d'une entreprise, d'une université, mais également chez les particuliers.par exemple:

- **IEEE 802.11, WiFi (Wireless Fidelity)**
  IEEE 802.11 ou WIFI est un standard international décrivant les caractéristiques du réseau LAN sans fil (WLAN). Il connecte des ordinateurs portables, des équipements de bureau,

des équipements personnels (PDA)… en créant un réseau sans fil couvrant un rayon de dizaines de mètres et tolérant une mobilité à très petite vitesse**. [6]**

c. Les réseaux métropolitains sans fil (WMAN)

Les réseaux métropolitains sans fil ou Wireless Metropolitan Area Network (WMAN) sont aussi connus sous l'appellation de boucle locale radio (BLR). Les réseaux basés sur la technologie IEEE 802.16 ont une portée de l'ordre de quelques dizaines de kilomètres (50km de portée théorique annoncée) et un taux de transmission radio théorique pouvant atteindre 74 Mbit/s pour IEEE 802.16, plus connu sous le nom commercial de WIMAX. **[3]**

d. Les réseaux sans fil étendus (WWAN)

Les réseaux sans fil (WWAN pour Wireless Wide Area Network). Cette catégorie possède assez peu de technologies à l'heure actuelle. Les seules technologies de WWAN disponibles sont des technologies utilisant les satellites géostationnaires ou en orbite basse pour relayer l'information entre plusieurs points du globe. **[3]**

Parmi les principales technologies, dans ce type de réseaux, sont les suivantes :

- **GSM**

  Le réseau GSM (Global System for Mobile communication) constitue au début du 20e siècle, le standard de téléphonie mobile le plus utilisé. La norme GSM autorise un débit maximal de 9.6kbps, ce qui permet de transmettre la voix ainsi que des données numériques de faible volume, par exemple des messages textes ou des messages multimédias. Les réseaux cellulaires reposent sur l'utilisation d'un émetteur récepteur central au niveau de chaque cellule, appelé station de base (BTS: Base Transceiver Station). Plus le rayon d'une cellule est petit, plus la bande passante disponible est élevée. La carte SIM permet ainsi d'identifier chaque utilisateur, indépendamment du terminal utilisé lors de la communication avec une station de base. La communication entre une station mobile et la station de base se fait par l'intermédiaire d'un lien radio, généralement appelé interface air. **[5]**

- **GPRS**

  Le GPRS (General Packet Radio Services) est une technologie de radiocommunication par commutation de paquets pour les réseaux de GSM. Les connexions des services de GPRS sont toujours ouvertes afin d'offrir aux utilisateurs des terminaux mobiles une disponibilité de réseau identique à celle qu'ils pourraient atteindre par des réseaux d'entreprise. Le GPRS offre une connectivité d'IP de bout en bout, du terminal GPRS jusqu'à n'importe quel réseau IP. Les terminaux peuvent être intégrés efficacement aux réseaux Internet. La vitesse "utile" sera d'environ 40 Kb/s (vitesse maximum : 171 Kb/s), l'un ou l'autre est quatre fois supérieure à celle du GSM. **[3]**

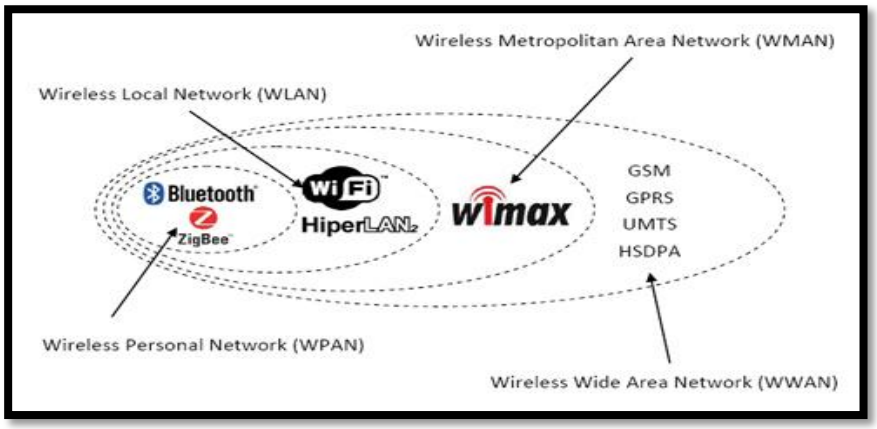


Figure 1.2 : les réseaux sans fils selon la zone de couverture.

2.2. Selon l'infrastructure

Les environnements mobiles sont des systèmes composés de sites mobiles et qui permettent à leurs utilisateurs d'accéder à l'information indépendamment de leurs positions géographiques. Les réseaux mobiles ou sans fil, peuvent être classés en deux classes: les réseaux avec infrastructure et les réseaux sans infrastructure.

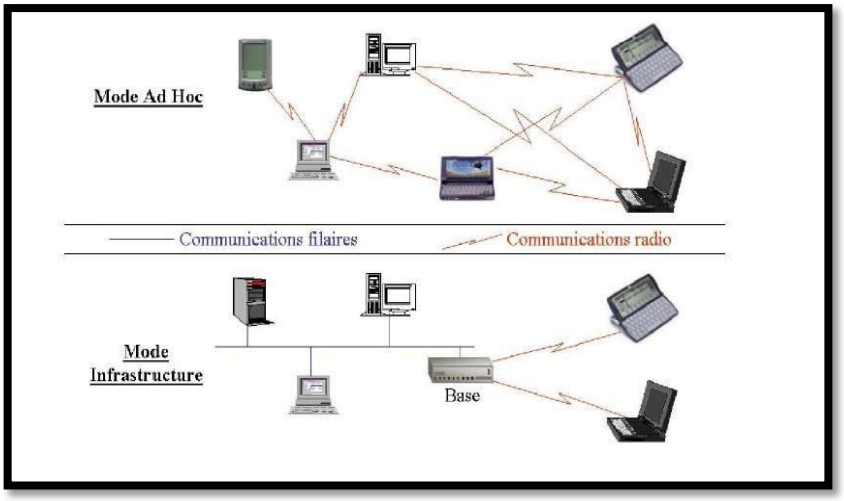


Figure 1.3 : mode infrastructure et mode Ad Hoc.

- **Réseaux sans fil avec infrastructure**

Le modèle de système intégrant des sites mobiles et qui a tendance à se généraliser, est composé de deux ensembles d'entités distinctes: les "sites fixes" d'un réseau de communication filaire classique (wired network), et 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.

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. Elle peut communiquer avec les autres sites à travers la station à laquelle elle est directement rattachée. L'autonomie réduite de sa source d'énergie, lui occasionne de

fréquentes déconnexions du réseau, sa reconnexion peut alors se faire dans un environnement nouveau voire dans une nouvelle localisation. **[7]**

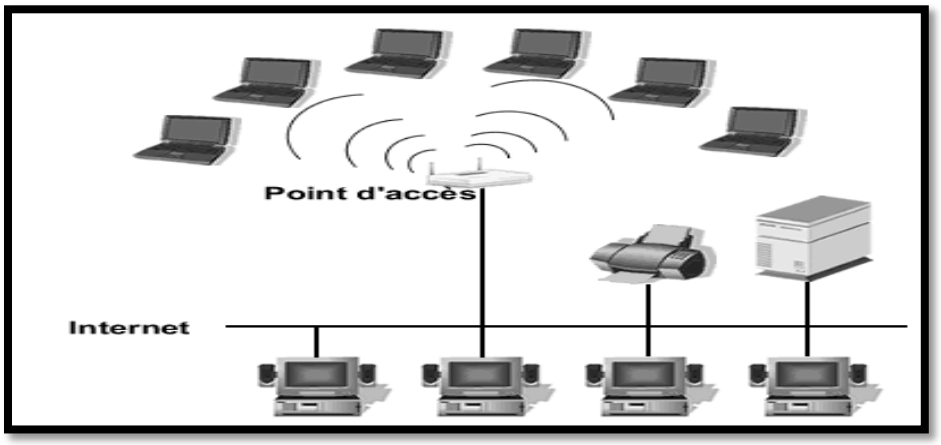


Figure 1.4 : Réseau sans fils avec infrastructure.

3. RESEAUX SANS INFRASTRUCTURE (AD HOC)

3.1. Définition

Une définition formelle des réseaux Ad Hoc MANET **(Mobile Ad Hoc NETWORK)** est donnée par la RFC 2501. Il s'agit de réseaux sans fil composé d'un ensemble relativement des noeuds mobiles qui se déplacent librement dans une certaine zone géographique sans aucune infrastructure fixe préexistante. Un noeud dans le réseau Ad Hoc communique avec un autre noeud directement (en utilisant son interface sans file), si ce dernier est dans son porté de transmission, ou indirectement par l'intermédiaire d'autres noeuds du réseau dans le cas contraire. Chaque noeud dans le réseau Ad Hoc doit se comporter comme un terminal, et aussi comme un routeur, et participer à la découverte et la maintenance des routes entre les noeuds du réseau.

Il y a aucune limitation de taille dans un réseau Ad Hoc, il peut contenir des dizaines ou des milliers de nœuds.

Les réseaux Ad Hoc ont en théorie une très grande robustesse puisque pour que le réseau cesse de fonctionner, il faudrait qu'un nombre important de noeuds qui le compose soit hors service. En effet si un des noeuds du réseau devient indisponible pour cause de défaillance ou de manque d'énergie, cela ne change rien ou presque pour les autres noeuds qui vont se réorganiser et continuer leurs communications. Contrairement aux réseaux mobiles sans infrastructure où tout dépend de l'état des stations de base pour communiquer. **[8]**

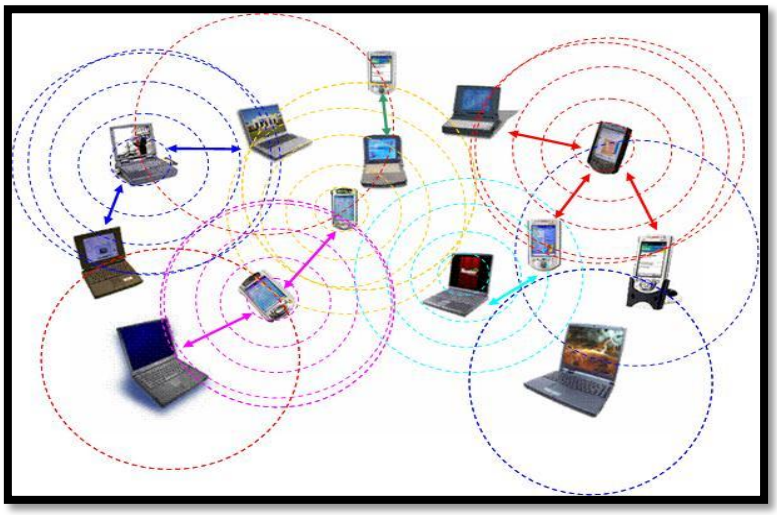


Figure 1.5: Réseau sans fil sans infrastructure (Ad Hoc).

3.2. Historique et évolution des réseaux Ad Hoc

Le projet militaire Américain DARPA (***The Defense Advanced Research Projects Agency***), qui a eu lieu au début des années 1970 a évoqué la naissance des premiers réseaux utilisant le médium hertzien ou radiofréquence. Ces réseaux sont définis par deux composantes:

- La disposition d'une architecture distribuée.
- Le partage d'un canal de diffusion en répétant des paquets pour élargir la zone de couverture globale.

Dans le même axe des applications militaires, dans les années 1983, les Sur vivable Radio Networks (SURAN) furent développer par le DARPA. Leur objectif était de dépasser les limitations. Autrement dit, permettant le passage à des réseaux comportant énormément de nœuds, gérant le domaine de la sécurité et l'énergie.

L'arrivée du protocole 802.11 (WIFI) était le point de départ des réseaux sans fils autour des bases fixes, et qui a permis l'apparition des problématiques liées à ces réseaux par la recherche civile dans les années 90. **[9]**

3.3. Modélisation

Un réseau mobile Ad Hoc, appelé généralement MANET (Mobile Ad Hoc Network), consiste en une grande population, relativement dense, d'unités mobiles qui se déplacent dans un territoire quelconque. Le seul moyen de communication est l'utilisation « des ondes radio » qui se propagent entre les différents nœuds mobiles, sans l'aide d'une infrastructure préexistante ou administration centralisée. Un réseau Ad Hoc peut être modélisé par un graphe **Gt = (Vt, Et)** où **Vt** représente l'ensemble des nœuds (i.e. les unités ou les hôtes mobiles) du réseau et **Et** modélise l'ensemble des connections qui existent entre ces nœuds (figure1.4). Si **e = (u, v)** appartient à **Et**, cela veut dire que les nœuds **u** et **v** sont en mesure de communiquer directement à l'instant **t**. **[9]**

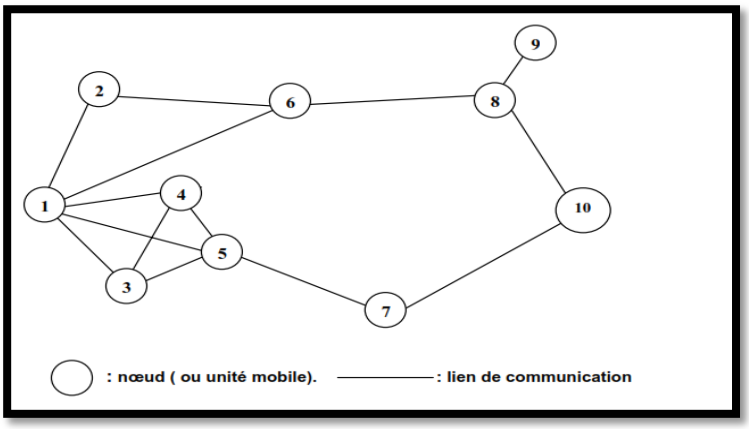


Figure 1.6: La modélisation d'un réseau Ad Hoc.

3.4. Caractéristique des réseaux Ad Hoc

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

- **Sans infrastructure:** Les nœuds d'un réseau Ad Hoc travaillent dans un environnement totalement distribue, ce qui leurs permet de se déplacer librement, Cette caractéristique donne plus de liberté aux nœuds mais ces dernier doivent assurer des fonctionnalités supplémentaires par rapport aux nœuds d'un réseau sans fils avec infrastructure, puisqu'ils doivent agir en tant que routeurs pour relayer la communication des autre nœuds. **[8]**
- **Mobilité et topologie dynamique:** Les unités mobiles du réseau se déplacent d'une façon libre et arbitraire. Par conséquent la topologie du réseau peut changer, à des instants imprévisibles, d'une manière rapide et aléatoire. Les liens de la topologie peuvent être unis ou bidirectionnels. **[8]**

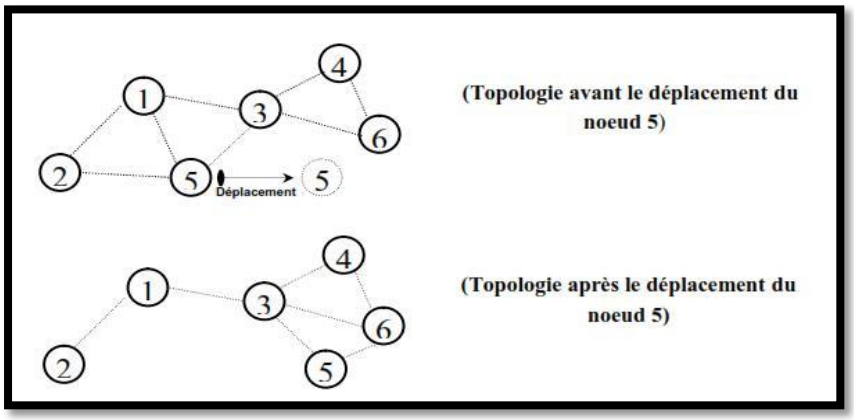


Figure 1.7: Changement de la topologie d'un réseau Ad Hoc.

- **Contraintes de ressources:** Les nœuds disposent de ressources d'alimentation et de capacités de calcul et de stockage limitées. D'où une gestion efficace est nécessaire pour avoir une longue durée de vie, le trafic de routage devrait être maintenu à un minimum. **[8]**

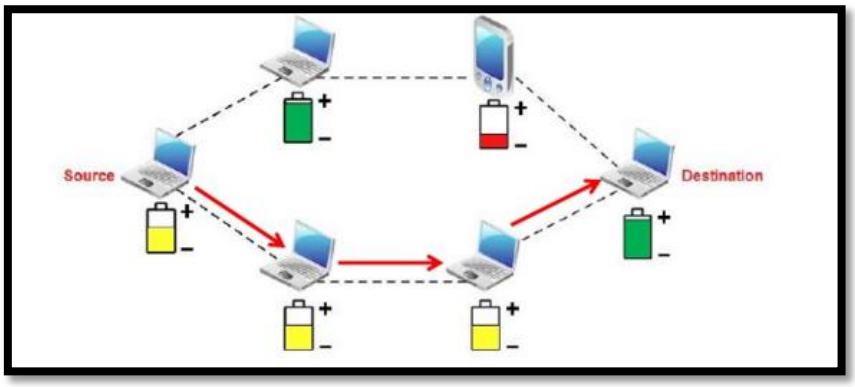


Figure 1.8: durée de vie de batterie des noeuds.

- **Bande passante limitée:** La communication dans les réseaux Ad Hoc se base sur le partage d'un medium sans fil (onde radio). Ce qui induit une bande passante modeste, pour chaque hôte du réseau. **[8]**
- **Interférences:** Dans un réseau Ad Hoc, les liens radio ne sont pas isolés. Ceci peut impliquer que deux transmissions simultanées sur une même fréquence ou sur des fréquences proches peuvent interférer et provoquer des erreurs de transmission. Un grand nombre de paquets peuvent être endommagés et perdus lors du transfert. **[8]**
- **Sécurité physique limitée:** Les terminaux ne sont pas protégés, ils sont menacés de vol ou de destruction. Donc les nœuds d'un réseau Ad Hoc n'ont pas la même protection physique que les nœuds d'un réseau filaire. En effet, ceux d'un réseau Ad Hoc sont censés être mobiles et parfois complètement autonomes, c'est notamment le cas des réseaux de capteurs où les nœuds sont souvent lâchés, dans un environnement particulier et parfois hostile, sans aucune surveillance particulière. **[8]**
- **Sécurité et Vulnérabilité:** Les réseaux sans fil sont par nature plus sensibles aux problèmes de sécurité que les réseaux filaires. Pour les réseaux Ad Hoc, le principal problème ne se situe pas tant au niveau du support physique mais principalement dans le fait que tous les nœuds sont équivalents et potentiellement nécessaires au fonctionnement du réseau. **[8]**

3.5. Points fortes

- **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. **[10]**
- **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. **[10]**
- **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. **[10]**
- **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. **[8]**

3.6. Points faibles

- **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. **[11][12]**
- **Connectivité limité:** Ce qui réduit les possibilités de communication. 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. **[11][12]**
- **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. 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. **[11][12]**
- **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. **[11][12]**
- **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. **[11][12]**
- **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. **[11][12]**

3.7. Domaines d'applications

Les réseaux Ad Hoc sont utilisés dans toutes les applications où le déploiement d'une architecture centralisée est contraignant, voire impossible. En effet, la robustesse, le coût réduit et le déploiement rapide qu'ils présentent leur confèrent un accès à une large palette d'applications dont :

- **Les applications militaires:** Les réseaux Ad Hoc ont été utilisés la première fois par l'armée. En effet ce type de réseaux est la solution idéale pour maintenir une communication sur un champ de bataille entre les différentes troupes unités d'une armée. **[13]**

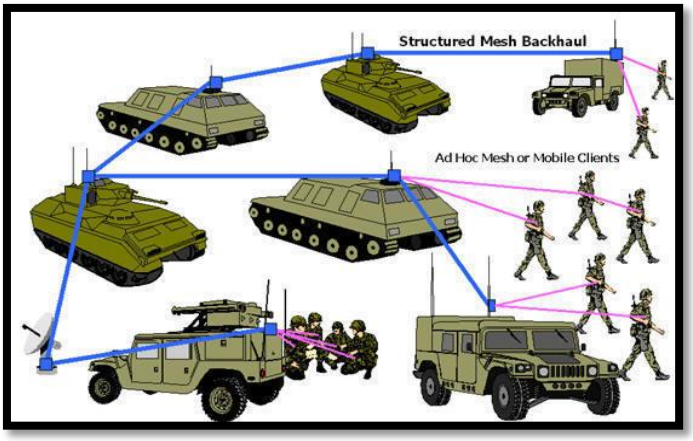


Figure 1.9 : Les applications militaires de réseau Ad Hoc.

- **Les opérations de secours:** Dans les zones touchées par les catastrophes naturelles (cyclone, séisme, etc.), le déploiement d'un réseau Ad Hoc est indispensable pour permettre eux unités de secours de communiquer. **[14]**

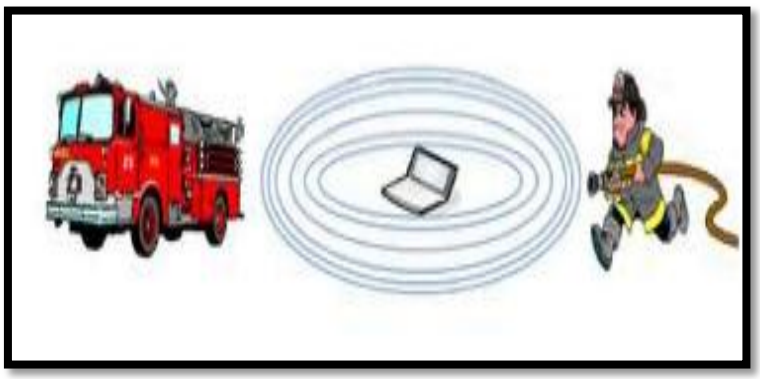


Figure 1.10: applications de secours des réseaux Ad Hoc.

- **L'utilisation à des fins éducatives:** Le déploiement d'un réseau Ad Hoc lors d'une conférence ou d'une séance de cours est très judicieux car cela permet aux chercheurs et étudiants de partager des ressources (fichiers, accès à internet…etc.) et de communiquer sans avoir besoin d'une quelconque infrastructure. **[13]**
- **Applications industrielles:** Des scénarios plus complexes dans le domaine industriel appelés réseaux de capteurs peuvent former un MANET pour s'adapter à différents environnements. Un exemple d'une telle application est la formation d'un MANET pour la surveillance médicale, la détection des Feux de forêt, la surveillance des volcans…etc. **[14]**
- **Mise en œuvre des réseaux véhiculaires:** Sur un réseau routier les véhicules peuvent avoir besoin de communiquer entre eux ou avec leur environnement afin de partager des informations dans le but de gérer et réguler le trafic routier. Les réseaux Ad Hoc sont alors la solution idéale. **[14]**

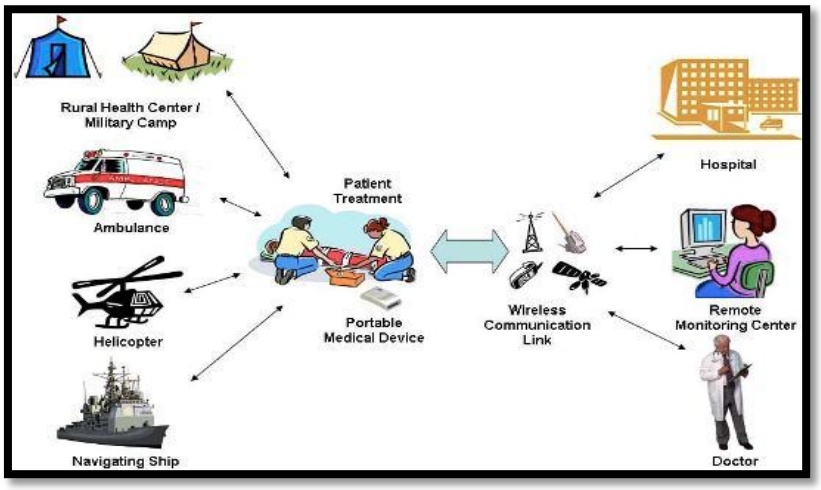


Figure 1.11: domaine d'application des réseaux Ad Hoc.

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.

CHAPITRE II

Les Protocoles De Routage Ad Hoc

INTRODUCTION

Un réseau Ad Hoc est un ensemble des nœuds mobile, l'acheminement de l'information d'une source vers une destination nécessitent des protocoles de routage établissent des routes entre les nœuds de réseau.

Dans ce chapitre nous nous donnerons un aperçu général sur le routage Ad Hoc, Nous commençons par:

- Définir le routage.
- principe de routage dans les réseaux Ad Hoc.
- Citer la classification des protocoles de routage des réseaux Ad Hoc.
- présentant quelques protocoles de routage les plus connus dans ce domaine…etc.

1. DEFINITION DU ROUTAGE

Le routage est une méthode d'acheminement des informations à la bonne destination à travers un réseau de connexion donné. Son intérêt consiste à trouver le chemin optimal au sens d'un certain critère de performance (bande passante, délai, etc.). Il doit aussi être de capable de s'adapter aux événements venant perturber le réseau (panne, congestion, etc.). **[15]**

Son problème réside dans l'effet de trouver l'investissement de moindre coût en capacités nominales et de réserves qui assure le routage du trafic nominal et garantit sa serviabilité en cas de n'importe quelle panne d'arc ou de nœud. **[15]**

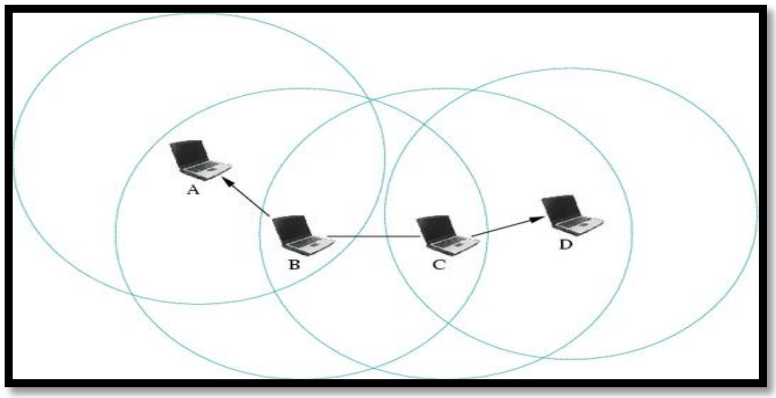


Figure 2.1: Le chemin utilisé dans le routage entre la source et la destination.

2. LE ROUTAGE DANS LES MANETS

Le routage est la tâche d'acheminement de flux des données à partir des nœuds sources vers les nœuds destinations **[17]**. 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. **[16]**

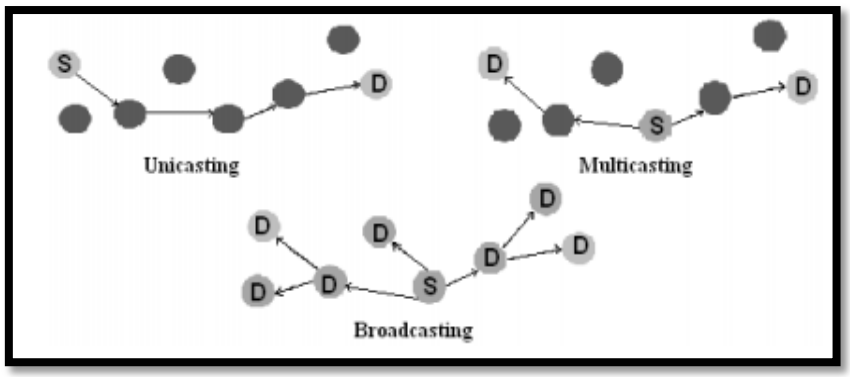


Figure 2.2: Illustration du routage unicast, multicast et broadcast. [16]

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

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

Les propriétés que doivent vérifier les protocoles de routage pour les MANETS peuvent être résumés dans les points suivant: **[19] [20]**

- **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. **[19] [20]**
- **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. **[19] [20]**
- **Optimisation de la consommation d'énergie:** dans un réseau Ad Hoc les nœuds ont besoin que leurs données soient acheminées par plusieurs nœuds intermédiaires pour qu'ils arrivent à leurs destinations. Une réduction en nombre de nœuds dégrade les performances du réseau comme elle peut aussi causer son partitionnement. Pour prolonger la durée de vie de chaque nœud et donc du réseau complet, la consommation d'énergie doit être prise en considération dans la conception des protocoles de routage. **[19] [20]**
- **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. **[19] [20]**
- **Convergence rapide:** après la rupture d'un chemin, un protocole de routage doit rétablir un nouveau chemin le plutôt possible. **[19] [20]**
- **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**. [19] [20]**

- **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**. [19] [20]**
- **Scalabilité:** les protocoles de routage doivent fonctionner efficacement même si la taille du réseau grandisse. Cela n'est pas facile à réaliser, car établir un chemin entre deux nœuds mobiles devient couteux en termes du temps requis, nombre d'opérations, et bande passante dissipée, quand le nombre de nœuds augmente. **[19] [20]**
- **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. **[19] [20]**

2.2. Services de routage dans les réseaux Ad Hoc

Les réseaux Ad Hoc étant de nature multi-sauts, le protocole de routage détermine une route entre un nœud source et un nœud destination. De par la faible bande passante offerte par les réseaux Ad Hoc et du fait de la diffusion des données, les protocoles de routage actuellement utilisés dans les réseaux filaires ne peuvent être utilisés, sans modifications, dans les réseaux MANETS. De fait, des nouveaux protocoles de routage ont dû être développés. **[21]**

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

- **Dissémination de l'information de routage:** elle permet de connaître suffisamment d'éléments sur la topologie pour choisir un chemin atteignant le nœud de destination. Suivant la quantité d'informations échangées, les nœuds obtiennent une vue plus ou moins précise de la topologie du réseau. Le protocole de routage se voit dans l'obligation d'optimiser l'envoi de ces informations, car elles sont fortement consommatrices en bande passante. **[21]**
- **Sélection du chemin:** une fois les informations de routage obtenues, le protocole de routage peut sélectionner une route parmi l'ensemble obtenu en fonction de certains critères. Pour les protocoles Meilleur effort (« Best Effort »), le critère est de minimiser le nombre de sauts du chemin. Ainsi, parmi l'ensemble des routes qui lui sont proposées, le protocole choisit celle traversant le plus faible nombre de nœuds. Les routes choisies doivent être dépourvues de boucles. La présence de boucles rend inefficace le chemin sélectionné puisque le paquet ne pourra pas atteindre la destination consommant inutilement de la bande passante. En effet, un paquet de données transitant sur un chemin, possédant une boucle, va tourner en rond tant que la boucle est présente. Pour éviter qu'un paquet de données tourne indéfiniment, le paquet est détruit lorsqu'il atteint la limite imposée par le champ TTL présent dans le protocole IP. Un protocole de routage peut créer deux sortes de boucles: les boucles temporaires et les boucles permanentes **[22]**.Les premières ont lieu pendant le transfert d'un message de routage. Durant ce temps, des stations peuvent être mises à jour et d'autres non, d'où la possible apparition d'une boucle. Elle dure au maximum la durée de traversée du réseau par un message de routage.

Les boucles permanentes, quant à elles, sont dues au phénomène du bouclage à l'infini **[23]**. Ces boucles peuvent consommer énormément de bande passante.

- **Maintenance des routes:** dans un environnement mobile, la topologie du réseau ne cesse d'évoluer avec le temps. De fait, les routes sont amenées à changer avec le déplacement des nœuds. Une route doit éviter de rester longtemps interrompue, car les paquets ne pourraient atteindre leur destination. Le protocole de routage doit donc tenir compte de ces changements et mettre à jour les routes qui viennent à être coupées. **[21]**

2.3. Les contraintes de routages dans les réseaux Ad Hoc

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

- **Minimisation de la charge du réseau:** l'optimisation des ressources du réseau renferme deux autres sous problèmes qui sont l'évitement des boucles de routage, et l'empêchement de la concentration du trafic autour de certains nœuds ou liens. **[24]**
- **Bon acheminement des données:** le fait que les chemins utilisés pour router les paquets de données puissent évoluer, ne doit pas avoir d'incident sur le bon acheminement des données. L'élimination d'un lien, pour cause de panne ou pour cause de mobilité devrait, idéalement, augmenter le moins possible les temps de latence. **[24]**
- **Assurer un routage optimal:** la stratégie de routage doit créer des chemins optimaux et pouvoir prendre en compte différentes métriques de coûts (bande passante, nombre de liens, ressources du réseau,... etc.). Si la construction des chemins optimaux est un problème dur, la maintenance de tels chemins peut devenir encore plus complexe, la stratégie de routage doit assurer une maintenance efficace de routes avec le moindre coût possible. **[24]**
- **Le temps de latence:** la qualité des temps de latence et de chemins doit augmenter dans le cas où la connectivité du réseau augmente. **[24]**

3. CLASSIFICATION DES PROTOCOLES DE ROUTAGE

Suivant la manière de création et de maintenance de routes lors de l'acheminement des données, les protocoles de routage peuvent être séparés en: **Proactif**, **Réactif** et **Hybride**. Comme il est illustré dans la figure 2.3.

De nombreux protocoles et algorithmes ont été proposés pour rendre la communication dans les réseaux Ad Hoc plus efficace. Et leurs performances ont été analysées dans différentes situations.

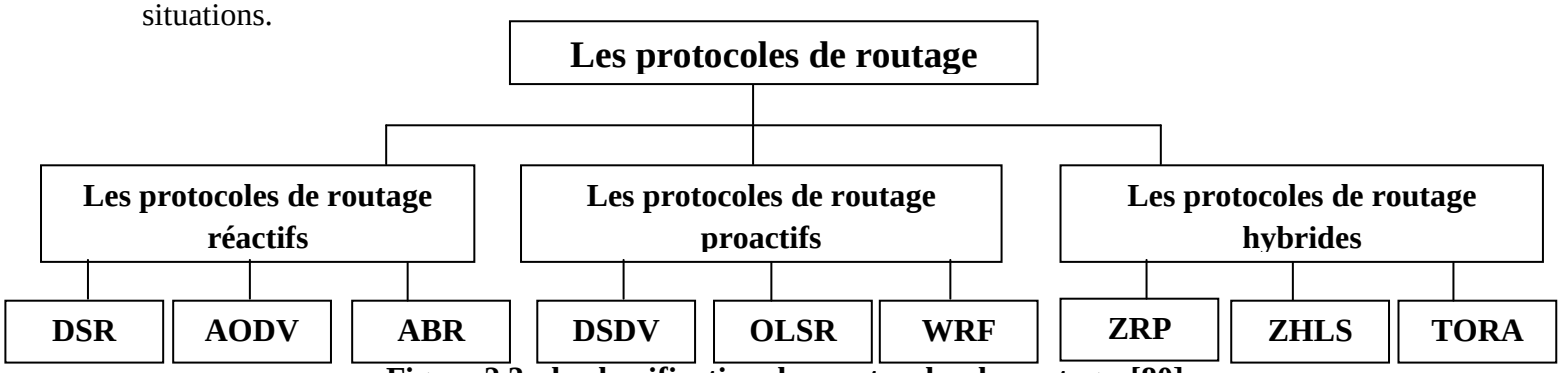


Figure 2.3 : la classification des protocoles de routage. [80]

3.1. Les protocoles à vecteur de distance

Dans les protocoles à vecteur de distances, la table de routage d'un nœud est calculée en fonction des tables reçues par ses voisins, comme son nom l'indique, ce protocole fonctionne selon une notion de distance. Chaque nœud enregistre dans sa table de routage les next-hops et les distances nécessaires pour atteindre toutes les destinations du réseau. Selon le protocole, cette distance peut être le nombre de hop, la bande passante, etc.

À chaque modification de sa table de routage, le nœud broadcaste celle-ci. Cette table peut être modifiée lorsqu'une autre table a été reçue d'un voisin, ou lorsque le nœud a détecté un changement de topologie dans son voisinage. Lorsqu'un nœud reçoit une table de routage d'un de ses voisins, il recalcule les routes les plus courtes pour chaque destination. Ces calculs sont effectués via l'équation de Bellman-Ford. Les vecteurs de distances sont des messages utilisés pour distribuer les informations à propos du réseau. À la création du réseau, chaque nœud crée une table de routage contenant son propre identifiant comme destination et next-hop et un coût associé nul. À intervalles réguliers, chaque nœud envoie sa table de routage à ses voisins via des vecteurs de distances. **[25]**

Le nom de ces messages est issu du fait qu'ils peuvent être vus comme des vecteurs où la direction est le voisin à contacter et la distance est le nombre de hops à effectuer pour atteindre la destination. Lorsqu'un nœud réceptionne un tel message, il utilise l'équation de Bellman-Ford pour déterminer si la table de routage actuelle doit être mise à jour avec celle reçue de son voisin. Si la table est mise à jour, le nœud envoie sa nouvelle table à ses voisins. Ce processus continue tant que des mises à jour sont à réaliser par les nœuds. Une fois que tous les nœuds ont obtenu les informations sur les meilleures routes, le réseau est stabilisé. Si un nœud détecte un changement de topologie, c'est-à-dire que l'un de ses voisins n'est plus accessible, le nœud indique son voisin comme inaccessible dans sa table de routage, partage celle-ci à son voisinage et l'information est transmise sur l'ensemble du réseau. **[25]**

3.2. Les protocoles à état de liens

Dans les protocoles à état de liens, chaque nœud connaît à tout moment la topologie complète du réseau, c'est-à-dire l'état des liens existant entre chaque couple de nœuds du réseau. L'ensemble du réseau peut être comparé à une carte routière. À chaque intersection (c.-à-d. les nœuds du réseau), il faut déterminer quelle est la meilleure direction à prendre (c.-à-d. la liaison vers un nœud voisin) pour atteindre une certaine destination. Pour ce faire, chaque nœud envoie à l'ensemble du réseau tous les nœuds auxquels il est relié. Sur base de ces informations, chaque nœud peut calculer indépendamment le meilleur next-hop pour atteindre chaque destination. Il est possible que certaines routes changent, apparaissent ou disparaissent. Dans ce cas, il faut en informer l'ensemble du réseau. Voici comment se déroulent les communications au sein de ce type de protocole, comme expliqué par J. Doyle. **[25]**

On peut distinguer trois phases :

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

a. Découverte du voisinage

Les messages HELLO sont utilisés pour gérer le voisinage sur le réseau. À intervalles réguliers, chaque nœud broadcaste un message HELLO pour avertir de sa présence. Une fois que

deux nœuds se sont découverts mutuellement, ils se considèrent chacun comme voisins. Ces messages servent aussi à détecter la disparition de nœuds et les défaillances de liens: si un nœud n'a pas reçu de message HELLO d'un de ses voisins endéans un certain temps, le lien avec ce voisin est considéré comme rompu. **[25]**

b. Distribution de la topologie

Pour distribuer les informations sur l'état du réseau, chaque nœud broadcaste un message LSA (Link State Advertisement) à intervalles réguliers. Ce type de message contient l'identifiant du nœud originaire du paquet, une liste de tous les voisins de ce nœud et un numéro de séquence incrémenté à chaque nouvel envoi. Lorsqu'un nœud reçoit un LSA, il sauvegarde les informations sur le nœud d'origine du message ainsi que sur l'ensemble de ses voisins. Ensuite, il rebroadcaste le message LSA à son tour. Il peut arriver qu'un même nœud reçoive plusieurs messages LSA d'une même origine. Dans ce cas, le numéro de séquence présent dans le message est utilisé pour déterminer si celui-ci a déjà été traité ou non. Pour ce faire, chaque nœud enregistre dans une table l'identifiant du nœud ayant envoyé le message et le plus grand numéro de séquence reçu. Si un paquet est reçu avec un numéro de séquence inférieur à celui enregistré, c'est qu'il a déjà été traité. Par la suite, à partir de toutes les informations récupérées, chaque nœud est capable de générer une carte du réseau comprenant l'ensemble des nœuds connus et leurs interconnexions. Cette carte doit être mise à jour à chaque réception d'un nouveau message TC contenant des modifications de topologie. **[25]**

c. Détermination des meilleures routes

Une fois la carte du réseau générée, chaque nœud peut déterminer les meilleurs next-hops pour atteindre chaque destination. Pour ce faire, des algorithmes de calcul de plus court chemin sont utilisés tel que l'algorithme de Dijkstra. Une table de routage contenant les next-hops pour chaque destination du réseau est maintenue et mise à jour à chaque modification de la carte du réseau. Il s'agit là de l'intuition de base pour tout protocole de routage à état de liens. Énormément de protocoles sont basés sur ce modèle, les plus utilisés étant IS-IS **[26]** et OSPF **[27]**. Le principal avantage de ce type de protocole est qu'à tout moment, le meilleur next-hop pour atteindre tout nœud du réseau est connu. On a donc une propagation très rapide des paquets au sein du réseau. Par contre, ce type de protocole a une réaction assez lente aux changements de topologie, étant donné qu'il faut attendre la réception de nouveaux messages LSA pour connaître les mises à jour à effectuer. De plus, la quantité d'informations à maintenir à propos du réseau peut être très importante. Au niveau des réseaux sans fil, ce protocole a d'autres défauts. Dans le cas des réseaux sans fil mobiles, les changements très fréquents de topologie mènent à l'utilisation de routes rapidement périmées. De plus, les broadcasts de messages peuvent vite provoquer de la congestion sur le réseau et encouragent les risques d'interférences de signal. C'est pourquoi d'autres protocoles ont du être inventés afin de remédier à ces problèmes. Les protocoles OLSR et B.A.T.M.A.N. sont basés sur le protocole LSR et proposent certaines optimisations propres aux réseaux mobiles sans fil.

3.3. Les protocoles de routage proactifs

3.3.1. Définition

Dans les protocoles de routage proactifs, chaque nœud maintient les informations de routage concernant tous les autres nœuds du réseau. Ces informations de routage sont généralement

sauvegardées dans quelques tables. Ces dernières sont mises à jour périodiquement et quand il y a des changements de topologie. Les protocoles de routage proactifs ont un problème de scalabilité car la taille des tables de routage ainsi que la taille des paquets contenant les informations de topologie ou de distances échangés augmentent proportionnellement avec le nombre de nœuds dans le réseau. **[28]**

3.3.2. Avantages

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

3.3.3. Inconvénients

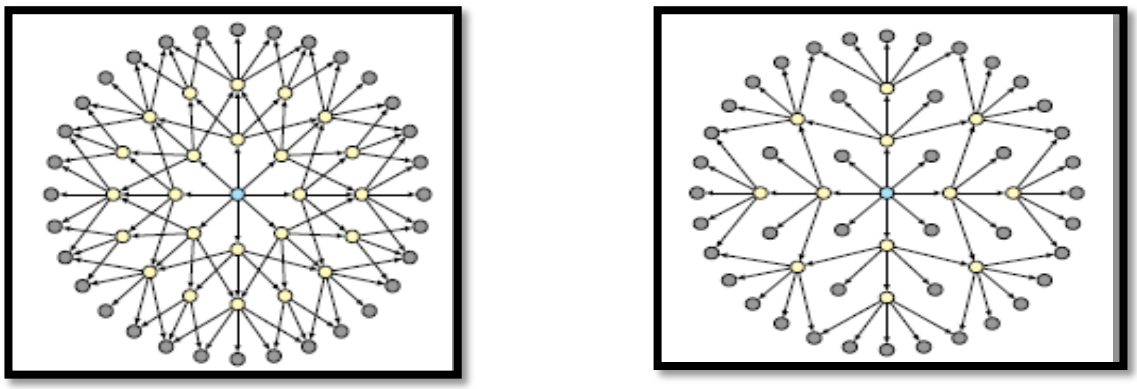
- ✓ Trafic de contrôle important.
- ✓ Capacité d'échange du réseau limitée.

3.3.4. Quelques protocoles de routage proactif

a. OLSR

OLSR **[29]** (Optimized Link State Routing) est un protocole proactif à état de lien (link state). OLSR apporte certaines améliorations sur le principe de base de l'état de lien en vue d'atteindre de meilleures performances dans un contexte Ad Hoc:

Il permet de minimiser l'inondation du réseau en diminuant les retransmissions redondantes dans la même région du réseau et réduit la taille des paquets échangés. Pour cela, OLSR se base essentiellement sur la notion de relais multi-point (MPR, Multi Point Relay), un sous ensemble des voisins à un saut qui permet d'atteindre la totalité des voisins à deux sauts. Ainsi, lors d'une diffusion, tous les voisins reçoivent et traitent le message mais seulement les nœuds choisis comme MPR le retransmettent ce qui diminue considérablement le nombre de messages émis dans le réseau (voir figure 2.4).



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

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

Figure 2.4: Avantage de l'utilisation des MPR. [29]

OLSR étant proactif, chaque nœud construit en permanence une vision de la topologie du réseau sous forme d'un graphe où les arcs constituent les liens entre les nœuds. La cohérence de

cette vision est assurée grâce à des diffusions périodiques des liens sortants. Ainsi, un nœud recevant ces informations met à jour sa vision de la topologie et applique l'algorithme du plus court chemin pour choisir le prochain saut en direction de chaque destination. Nous présentons maintenant les étapes permettant la construction de la topologie:

- **Écoute des voisins (neighbor sensing):** Il s'agit du processus de découverte du voisinage direct et symétrique qui est effectué grâce à la diffusion périodique de messages de type HELLO contenant des informations sur le voisinage ainsi que l'état des liens (link state) le reliant à cet ensemble de nœuds. Ce message de contrôle est destiné exclusivement aux voisins à un saut et n'est donc pas retransmis. De cette manière, un nœud construit la liste des voisins à un saut (Neighbor Set) tout en marquant les liens symétriques et puisqu'il voit aussi la liste des voisins de ceux-ci, il construit la liste des voisins à deux sauts (2-Hops Neighbor Set). **[29]**
- **Sélection des relais multi-point**: Cette sélection est faite de façon indépendante par chaque nœud. Elle passe par le choix du sous ensemble des nœuds à un saut qui permettent d'atteindre l'intégralité de voisins à deux sauts. Dans la figure 2.5, le nœud 1 choisit 2 comme MPR parce que c'est le seul nœud qui lui permet d'atteindre 5. Ensuite, il choisit le nœud 3 lui permettant d'atteindre 6, 7 et 8. De cette manière il couvre la totalité des voisins à deux sauts. Le sous ensemble obtenu est annoncé à tous les voisins dans des messages HELLO ultérieurs. **[29]**

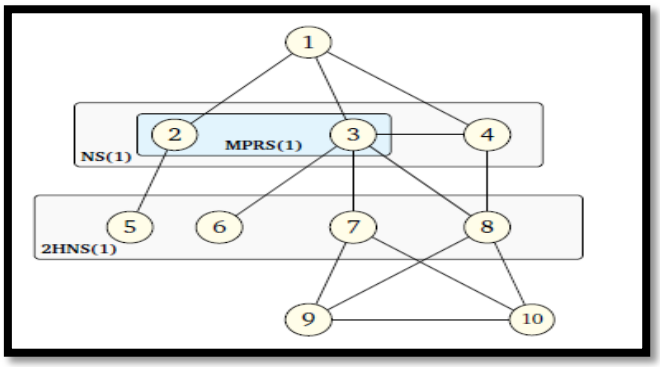


Figure 2.5: Choix des relais multi-point pour le nœud 1. [29]

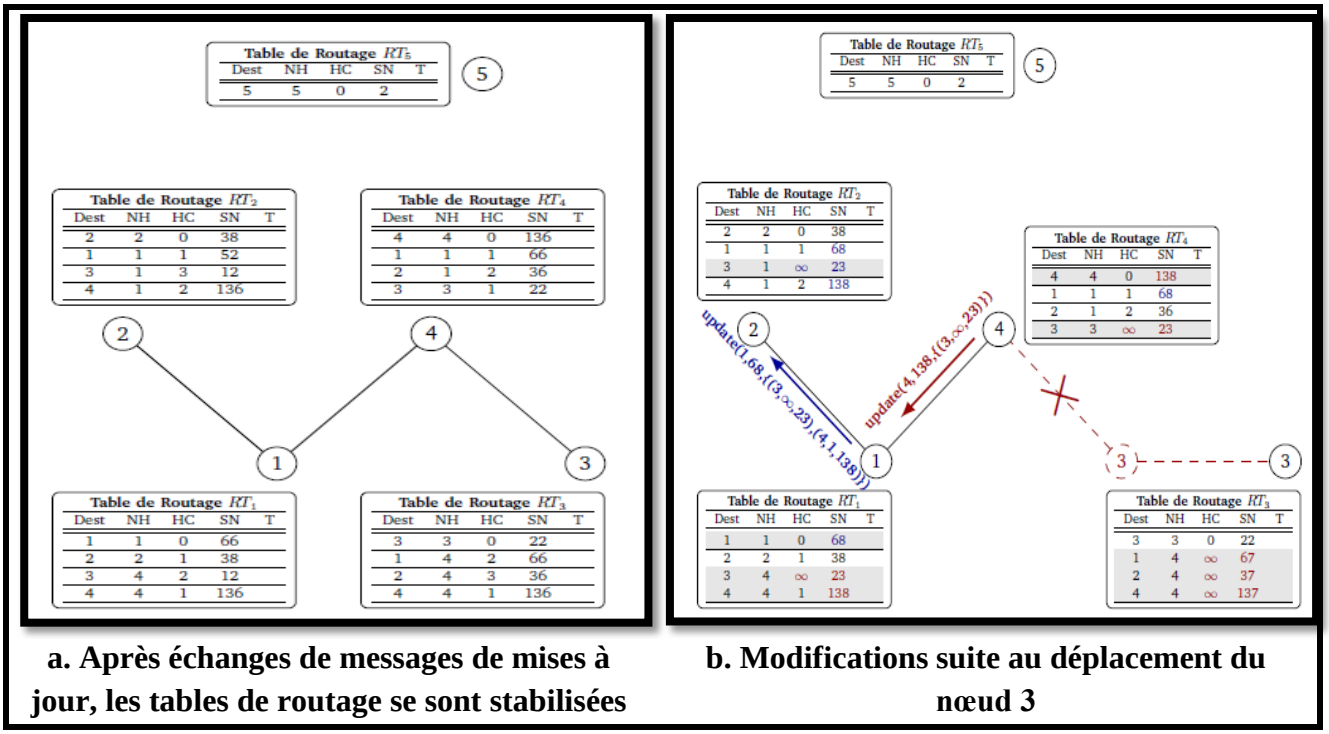
- **Déclaration des relais multi-point**: Les nœuds MPR diffusent des paquets de contrôle spécifiques appelés TC (Topology Control) pour construire une base d'informations sur la topologie du réseau. Les messages TC sont transmis à intervalles réguliers et déclarent l'ensemble MPRSS (Multi Point Relay Selector Set), c'est-à-dire l'ensemble contenant les voisins ayant choisit le nœud origine de ce message comme MPR. Les informations sur la topologie du réseau reçues dans les messages TC sont enregistrées dans la table de topologie (topology table). **[29]**
- **Calcul de la table de routage**: La table des voisins (neighbor table) ainsi que la table de topologie (topology table) sont utilisées pour le calcul de la table de routage qui se base sur l'algorithme du plus court chemin **[30]**. Toute modification de l'une de ces tables entraine la modification de la table de routage.

Cette amélioration à base de relais multi-point fournit des routes optimales en nombre de sauts tout en diminuant le nombre de messages de contrôles qui circulent lors d'une diffusion. Il convient ainsi aux grands réseaux Ad Hoc mais semble être moins efficace pour des petits réseaux. **[31]**

b. DSDV

DSDV **[32]** (Destination-Sequenced Distance-Vector) est l'un des premiers protocoles de routage Ad Hoc proactifs à vecteur de distance. Il se base sur l'algorithme distribué Bellman-Ford DBF (Distributed Bellman-Ford) **[33]** qui a été modifié pour s'adapter aux réseaux Ad Hoc. Comme il s'agit d'un protocole proactif, chaque nœud, à chaque instant une vision complète du réseau. Pour ce faire, chaque nœud récupère les distances le séparant de chaque autre nœud du réseau et ne garde que le plus court chemin. Ceci est fait grâce à des échanges périodiques d'informations sur leurs tables de routage respectives. Ces échanges sont classés en deux types:

- **Les mises à jour incrémentales (incremental updates)**: pour lesquelles seules les données qui ont subit des modifications depuis la dernière mise à jour sont envoyées. Un exemple est présenté dans la figure 2.6 où, suite au déplacement du nœud 3 qui n'est plus à portée radio, le nœud 4 initie une procédure de mise à jour (update) qui ne concerne que l'entrée correspondant au nœud 3 dans sa table de routage (voir figure 2.6b). Chaque nœud recevant ce message le transfère en incluant les entrées qui viennent d'être modifiées. C'est le cas du nœud 1 qui initialise une mise à jour suite à la réception de celle du nœud 4.

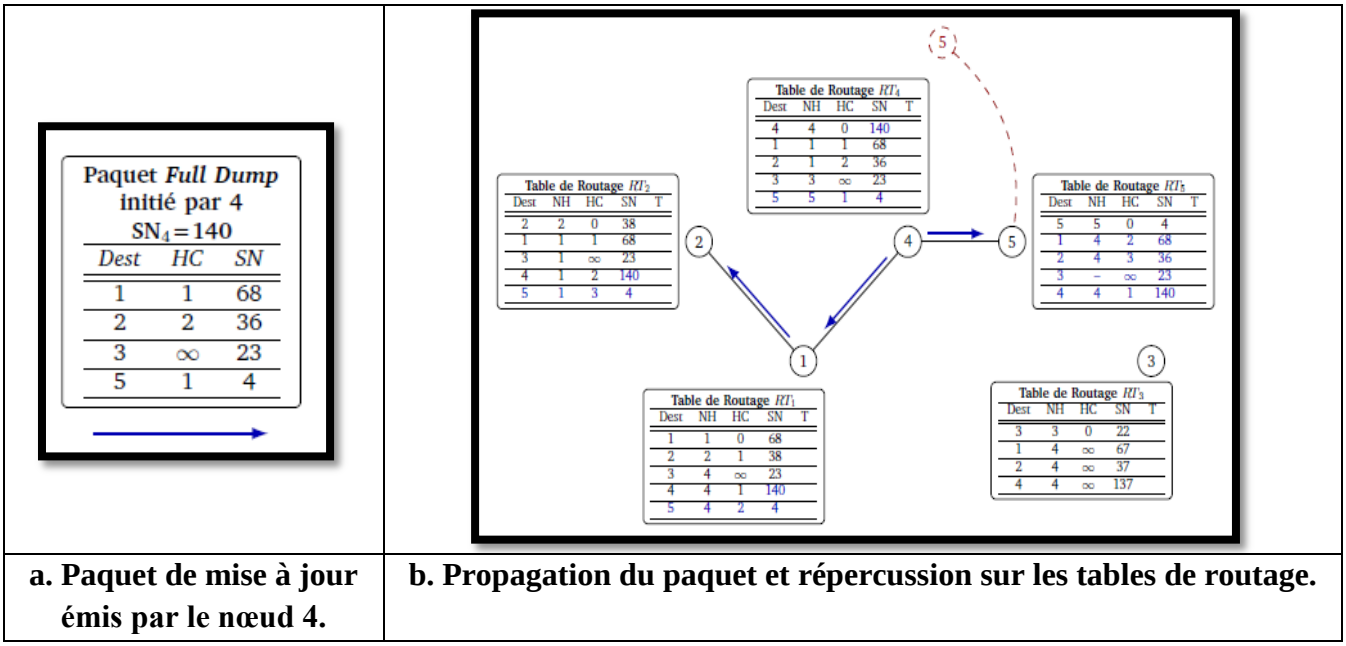


a. Après échanges de messages de mises à jour, les tables de routage se sont stabilisées

b. Modifications suite au déplacement du nœud 3

Figure 2.6 : Mise à jour incrémentale. [32]

- **Les mises à jour complètes (full dump):** pour lesquelles la totalité de la table de routage est envoyée. La figure 2.7 montre un exemple de cette procédure où le nœud 4 envoie la totalité de sa table de routage à tous les nœuds du réseau ce qui induit des changements au niveau de leurs tables de routage. Outre son adresse et son propre numéro de séquence, chaque paquet de mise à jour doit contenir une liste des routes ajoutées/modifiées pour laquelle chaque entrée est un triplet formé par:



a. Paquet de mise à jour émis par le nœud 4. | **b. Propagation du paquet et répercussion sur les tables de routage.**

Figure 2.7 : Mise à jour complète (full dump). [32]

L'adresse de la destination **Dest**, le nombre de sauts **HC** pour l'atteindre (Hop Count) et le dernier numéro de séquence connu associé à cette destination (Sequence Number) qui permet notamment de distinguer les nouvelles routes des anciennes et évite ainsi la formation de boucles de routage. La figure 2.7a montre un exemple de ce paquet de mise à jour.

Pour gérer la mobilité des nœuds, DSDV associe à chaque nœud un minuteur (timer) qui est mis à jour à la valeur maximale à chaque fois qu'un message est reçu du voisin: c'est un indicateur de validité du lien. Ainsi, lorsque ce minuteur expire, le nœud considère que le voisin en question n'est plus à porté radio et que le lien est rompu. Il peut aussi utiliser les messages de la couche 2 pour détecter les ruptures de liens. La détection d'un lien rompu se traduit au niveau de l'entrée correspondante dans la table de routage par l'assignement de la valeur ∞ au nombre de sauts (en pratique, il s'agit de n'importe quelle valeur supérieure au maximum autorisé) et l'incrémentation du numéro de séquence au prochain numéro impair. Toutes les routes utilisant ce nœud qui n'est plus joignable sont aussi mises à jour comme étant des routes invalides. Ces changements sont envoyés en priorité à tous les voisins en utilisant un paquet de mise à jour. Il est à noter que c'est le seul cas où un nœud autre que la destination pourra changer le numéro de séquence de la destination qui n'est plus joignable (voir figure 2.7b cas des nœuds 3 et 4).

À la réception d'un paquet de mise à jour, les routes avec les plus grands numéros de séquences sont privilégiées pour le choix des routes puisque cela signifie une route plus fraîche. Dans le cas de numéros de séquences égaux, le plus court chemin est retenu en se basant sur le nombre de saut. Le nœud intermédiaire procède ensuite à la rediffusion des informations qu'il vient de modifier dans sa table de routage tout en incrémentant son numéro de séquence.

Malgré les améliorations qu'il propose par rapport à DBF en éliminant le problème des boucles de routage (routing loops) et le problème du comptage à l'infini (counting to infinity) grâce notamment à l'utilisation des numéros de séquence, DSDV reste long et coûteux. Il nécessite des mises à jour régulières de ses tables de routage même lorsque le réseau est inactif. À chaque mise à jour, un nouveau numéro de séquence est nécessaire ce qui augmente le temps avant que le réseau converge. Ceci rend DSDV peu adapté aux réseaux très dynamiques.

3.4. Protocole de routage réactif (a la demande)

3.4.1. Définition

Les protocoles de routage réactifs (dits aussi : protocoles de routage à la demande), représentes les protocoles les plus récents proposés dans le but d'assurer le service du routage dans les réseaux sans fil. La majorité des solutions proposées pour résoudre le problème de routage dans les réseaux Ad Hoc, et qui sont évaluées actuellement par le groupe de travail MANET (Mobile Ad Hoc Networking Working Groupe) de l'IETF (Internet Engineering Task Force).

Les protocoles de routage appartenant à cette catégorie, créent et maintiennent les routes selon les besoins. Lorsque le réseau a besoin d'une route, une procédure de découverte globale de routes est lancée, et cela dans le but d'obtenir une information.

Spécifiée, inconnue au préalable. Plusieurs approches peuvent être appliquées dans la découverte des routes. La majorité des algorithmes utilisés, sont basé sur le mécanisme d'apprentissage en arrière (backward learning). **[34]**

Le nœud source, qui est à la recherche d'un chemin vers la destination, diffuse par inondation une requête dans le réseau. Lors de la réception de la requête, les nœuds intermédiaires (ou de transit) essaient de faire apprendre le chemin au nœud source, et de sauvegarder la route dans la table envoyée. Une fois la destination est atteinte, elle peut envoyer une réponse en utilisant le chemin tracé par la requête, un chemin full duplex est alors établit entre le nœud source et le nœud destination. Le travail peut être réduit, dans le cas où un nœud de transit posséderait déjà un chemin vers la destination. Une fois le chemin est calculé, il doit être sauvegardé et mis à jour au niveau de la source, tant qu'il est en cours d'utilisation. Une autre technique pour tracer les chemins demandés, est la technique appelé "routage source".

Le routage à la demande induit une lenteur à cause de la recherche des chemins, ce qui peut dégrader les performances des applications interactives (exemple les applications des bases de données distribuées). En outre, il est impossible de connaître au préalable la qualité du chemin (en termes de bande passante, délais,… etc.). Une telle connaissance est importante dans les applications multimédias. **[34]**

3.4.2. Avantages

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

3.4.3. Inconvénients

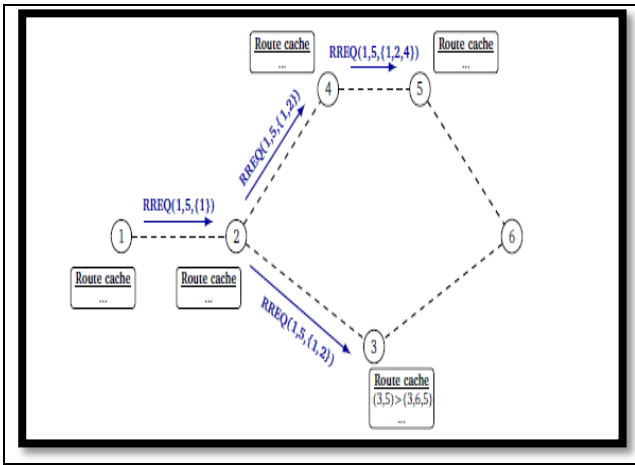
- ✓ Temps de réaction long.
- ✓ Problème en cas de forte mobilité des nœuds.

3.4.4. Quelques protocoles réactifs

a. DSR (Dynamic Source Routing)

Le protocole DSR **[35] [36]** est un protocole de routage Ad Hoc réactif à état de lien. Les routes sont construites à la demande en utilisant le 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 cette liste est renvoyée à la source dans un paquet de réponse de route.

- **Découverte de route:** Lorsqu'un nœud source désire envoyer des données 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). 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. 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). **[35] [36]**
- **Maintenance des routes:** Lors de la transmission d'un paquet, chaque nœud est responsable de l'acheminement des données sur le lien en direction du prochain saut. Il devra s'assurer que les données sont bien parvenues au prochain saut. Un accusé de réception peut garantir la confirmation du destinataire (ou le cas échéant un accusé spécifique à DSR). Si un nœud ne reçoit pas un accusé de réception suite à un envoi de paquet, il considère que le lien est rompu et supprime cette route du cache. Il crée alors un paquet erreur de route RERR (Route ERROR) qu'il envoie à tous les nœuds ayant envoyé un paquet sur ce lien depuis le dernier accusé de réception. Un avantage de DSR est que les nœuds intermédiaires n'ont pas besoin de garder des informations sur les différents chemins pour pouvoir envoyer les paquets de données puisque ces routes sont incluses dans l'entête ce qui garantie l'absence de boucles de routage. À l'inverse, l'utilisation de DSR peut être coûteuse dans un réseau à forte mobilité et densité du trafic car il surcharge le réseau avec un grand nombre de messages de contrôle. **[35] [36]**



a. Propagation de la demande de route. | **b. Propagation de la réponse de route.**

Figure 2.8 : Exemple du processus d'établissement de route entre 1 et 5. [35] [36]

b. AODV (Ad Hoc On demand Distance Vector)

Un des protocoles les plus connus dans cette catégorie est le protocole AODV **[37] [38]** qui n'est en réalité qu'une combinaison entre les deux protocoles DSDV et DSR. En effet, c'est une combinaison de la demande de base de la découverte et le maintien de route de DSR et le routage de saut par saut et des numéros de séquence de DSDV. La route retenue est bidirectionnelle et correspond au plus court chemin (en nombre de sauts) entre la source et la destination. Chaque nœud maintient une table de routage dont les entrées mémorisent, pour une destination:

- ✓ L'identifiant de cette destination.
- ✓ L'identifiant du prochain nœud vers cette destination.
- ✓ Le nombre de nœuds jusqu'à cette destination.

Quand un nœud source **S** veut atteindre la destination **D** pour laquelle il ne possède pas de route, il inonde le message de demande de route RREQ à ses voisins. Le paquet RREQ contient le numéro de séquence pour cette destination, si le numéro de séquence n'est pas connu, la valeur nulle sera prise par défaut, il contient aussi la valeur du numéro de séquence du nœud source. Le RREQ sera propagé jusqu'à ce que le paquet atteigne un nœud qui a une route à la destination. Chaque nœud intermédiaire expédie la demande et crée une route inversée vers **S** (mémorise une route vers la source). Quad un nœud intermédiaire a une route vers **D**, il produit une réponse RREP qui contient le nombre de saut et le numéro de séquence pour **D** (le plus récent). Les nœuds qui portent la réponse vers **S** créent une route vers **D** mais seulement avec le prochain saut et non pas la route toute entière. Cependant, AODV maintient les chemins d'une façon distribuée en gardant une table de routage au niveau de chaque nœud de transit appartenant au chemin recherché.

Pour la mise à jour des routes, le protocole AODV exige des messages HELLO toutes les quelques secondes. Un lien est considéré invalide si trois messages HELLO consécutifs ne sont pas reçus (à travers ce même lien).

Quand un lien devient invalide, tout nœud expédiant à travers celui-ci est informé par un paquet Route Error RERR avec une métrique égale à l'infini. Ce qui conduit au lancement d'une opération de découverte de route.

3.5. Les protocoles de routage hybrides (Les zones)

3.5.1 Définition

Les protocoles de routage hybrides combinent les deux approches de routage réactif et proactif. Dans un protocole de routage hybride, le réseau est décomposé en un ensemble de zones. Le routage à l'intérieur des zones est assuré par un protocole de routage proactif alors que le routage entre les zones est assuré par un protocole de routage réactif. Les protocoles de routage hybrides ont l'avantage de scalabilité, car la taille des tables de routage est réduite à la taille des zones. De plus, ils permettent un temps de réponse plus court que les protocoles de routage purement réactif. **[39]**

3.5.2 Avantages et inconvénients des protocoles hybrides

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

3.5.3 Quelques protocoles hybrides

a. Protocole de routage ZRP

ZRP signifie « Protocole de zone de routage » (« Zone Routing Protocol ») **[40]**. Le protocole de routage ZRP est un modèle hybride entre un schéma proactif et un schéma réactif. Il est basé sur deux procédures: le protocole de routage intra-zone, nommé IARP et le protocole de routage interzone, nommé IERP.

IARP est utilisé uniquement à l'intérieur de la zone de routage. Cette zone est définie pour chaque nœud et comporte une taille de rayon correspondant à une valeur de nombre de saut. Par exemple, pour un nœud, si cette valeur vaut « deux » alors tous les nœuds ayant une distance supérieure à deux sauts ne feront pas parti de la zone de ce nœud. Les nœuds se trouvant à une distance de deux nœuds seront les nœuds périphériques à ce nœud. La valeur doit être fixée par l'administrateur réseau et est équivalente pour chaque nœud du réseau. Elle est importante car elle détermine la performance du protocole ZRP. Plus un réseau est instable plus il est essentiel que la valeur soit faible. **[40]**

IARP est généralement implémenté par des protocoles proactifs variés mais comme cela n'est pas vraiment spécifié, il peut l'être à partir de différents protocoles comme des dérivés de protocoles à vecteur de distance (AODV…). Le protocole doit de toute façon déterminer la distance qui sépare le nœud des autres nœuds du réseau afin qu'il délimite sa zone de routage. Cependant quel que soit le choix, le protocole nécessite d'être modifié afin de le restreindre à la zone de routage du nœud ce qui limite ainsi les mises à jour. Le contenu de la zone est connu par le nœud mais en contre partie il n'a aucune information concernant les autres nœuds appartenant à l'interzone.

Grâce à ce partage entre intra-zone et interzone, les changements de topologies du réseau ont uniquement un impact local et n'est plus répercuté à l'autre bout du réseau ce qui réduit l'utilisation de la bande passante du réseau. IERP est responsable d'établir des liens avec les nœuds situés dans l'interzone. Pour cela, il s'appuie sur les techniques de border casting (via BRP : Protocole de Résolution Bordercast) qui permet d'envoyer un paquet à tous les nœuds périphériques. Lors d'une demande de route, IERP vérifie tout d'abord que le destinataire ne soit pas présent dans l'intra-zone

(pas de requête, la source connaît son contenu). S'il est présent alors aucun processus de connexion n'est nécessaire. En revanche, s'il ne s'y trouve pas alors la source fait une demande d'établissement de route (« Route Request ») à tous les nœuds périphériques. Les nœuds périphériques, à la réception du message, effectuent la même opération. Chaque nœud recevant la requête inscrit son identificateur à l'intérieur avant de la renvoyer, cela s'appelle le processus d'accumulation de route. Le nœud périphérique contenant la destination dans sa zone de routage lui répond, à l'aide des identificateurs présents dans la requête, par un signal « Route Reply » en lui indiquant le chemin à emprunter pour l'atteindre. Comme il préférable qu'une requête de type « Route Request » ne soit pas retransmis à une zone qui a été déjà parcourue, IERP utilise deux mécanismes. Le premier tue les messages qui contiennent un identificateur d'un nœud présent dans son intra-zone (excepté s'il s'agit du nœud précédent évidemment). Le suivant est un mécanisme complémentaire qui enregistre l'identificateur de l'hôte dans sa liste de requête uniquement en période de « Route Request » afin d'ignorer une requête déjà formulée auparavant. **[40]**

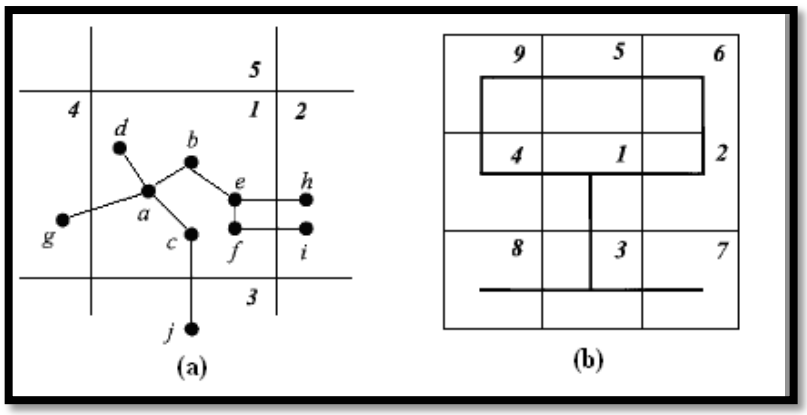
IERP dispose également d'un mécanisme de réponse réactive aux erreurs de route lorsque le saut suivant est déterminé comme inaccessible. Un paquet « Route Failure » est alors envoyé à la source pour l'avertir et la voie de communication ayant expirée est retirée de la table de routage interzone. IERP peut être configuré afin de réparer localement la route interzone endommagée avec une procédure d'établissement de route vers le nœud inaccessible. **[40]**

b. ZHLS (Zone based hierarchical link state)

ZHLS est un protocole de routage hybride où le réseau est décomposé en plusieurs zones non chevauchées. Le partitionnement du réseau à des zones s'effectue en exploitant les informations de géo-localisation obtenues par un système de positionnement comme GPS. Deux niveaux de topologies sont définis dans ZHLS topologie niveau nœuds et topologie niveau zones. La topologie niveau nœuds donne des informations sur comment les nœuds sont reliés par des liens physiques, tandis que la topologie niveau zones donne des informations sur les liens virtuels qui relient les différentes zones. **[41]**

Dans ZHLS, si un nœud **x** veut envoyer un paquet de données vers une destination **d**, il consulte d'abord sa table de routage intra zone pour savoir s'il possède un chemin vers **d**. Si c'est le cas, le paquet de données sera directement envoyé à **d.** Sinon, **d** réside dans une autre zone et **x** envoie des requêtes vers chaque zone. Les nœuds intermédiaires acheminent ces requêtes selon leurs tables de routage interzone. Les nœuds des autres zones qui reçoivent ces requêtes consultent leurs tables de routage intra zone pour savoir si **d** résident dans leurs zones. Un nœud qui est dans la même zone de d envoie une réponse contenant l'identificateur de la zone au nœud source. **[41]**

L'inconvénient de ZHLS est que pour fonctionner, tous les nœuds doivent maintenir une carte de zones prédéfinie. Cela n'est pas faisable dans des applications dont les frontières géographiques du réseau sont dynamiques. **[41]**



(a) Topologie niveau nœuds. (b) Topologie niveau zone.

Figure 2.9 : Les différents niveaux de topologie dans ZHLS. [41]

En résumé :

Approches de routage Caractéristiques	**Approche proactive**	**Approche réactive**	**Approche hybride**
Stratégie de routage	Uniforme et non uniforme.	Généralement uniforme.	Généralement non uniforme.
Disponibilité de chemins	Toujours disponibles.	À la demande.	Dépend de la localisation de la destination.
Sur débit de routage	Elevé.	Inférieure.	plus bas qu'en proactive et en réactive.
MAJ périodiques	Oui.	Non.	Généralement utilisées à l'intérieur des zones.
Gestion de la mobilité	Généralement des MAJ à des intervalles fixes.	Reconstruction de chemins initiée par la source généralement.	En interzone, fréquence de reconstruction de chemins réduite
Espace de stockage Requis	Elevé.	inférieur Dépend du nombre de chemins actifs.	Dépend de la taille des zones.
Délais	Les chemins sont prédéfinis.	Plus élevé qu'en proactive.	Pour les destinations locales il est bas, sinon il est comme en réactive.

Tableau 2.1 : Comparaison des approches de routage proactif, réactif et hybride. [42]

CONCLUSION

L'étude effectuée sur les réseaux mobiles Ad Hoc nous a 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 MANETS.

CHAPITRE III

Le Protocole De Routage AODV

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 un des autres .Cependant on doit faire face à plusieurs défis et difficultés, et trouver des solutions fiables qui aident à trouvé le chemin optimal entre deux nœud source et destination.

Dans ce chapitre, nous commençons par une description de notre travail. Nous détalions le protocole que nous avons choisi (AODV), son fonctionnement et la problématique du routage de ce protocole. Par la suite, nous avons définir l'optimisation.

1. PRESENTATION

AODV (Ad-hoc On-demand Distance Vector), qui a été normalisé dans la RFC 3561 **[43].** AODV a fait l'objet de nombreux travaux. Comme DSR, il s'agit d'un protocole réactif, et donc il existe des similitudes importantes entre les deux protocoles. Néanmoins, AODV n'utilise pas de routage par la source, et utilise des numéros de séquence afin de déterminer si un message est plus récent ou ancien que l'information déjà connue. En outre, une métrique est utilisée afin de pouvoir utiliser une meilleure route si elle devient disponible, il s'agit d'une métrique comptant simplement le nombre de sauts. **[44]**

2. TABLE DE ROUTAGE

AODV maintient les chemins d'une façon distribuée en gardant une table de routage, au niveau de chaque nœud de transit appartenant au chemin cherché. Une entrée de la table de routage contient essentiellement: **[45]**

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

3. LES MESSAGES DE CONTROLE DE PROTOCOLE AODV

Les mécanismes de découverte et de maintenance de routes peuvent s'effectuer par le biais des messages de contrôles suivants: **[45]**

- **RREQ (Route Request):** Message de demande de route.
- **RREP (Route Reply):** Message de réponse à un RREQ.

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

Le format des paquets est donné ci-dessous:

3.1. Message de demande de route RREQ

Il contient essentiellement les champs suivants: **[45]**

Type	J R G D U	Reserved	Hop Count
RREQ ID			
Destination IP Address			
Destination Sequence Number			
Originator IP Address			
Originator Sequence Number			

Tableau 3.1 : Format du message RREQ. [45]

- **Type (8 bits):** ce champ indique le type de paquet, dans ce cas il prend la valeur 1.
- **Flags (drapeaux) (5 bits):** ce champ contient cinq flags (J, R, G, D, U) tel que:
  - ✓ **J (Join flag) et R (Repair flag):** sont réservés pour le multicast.
  - ✓ **G (Gratuitous RREP flag):** indique si un message RREP spécifique doit être envoyé à la destination dans le cas ou un nœud intermédiaire possède un chemin à la destination.
  - ✓ **D (Destination only flag):** ce drapeau indique si seulement la destination qui doit répondre à la requête ou pas.
  - ✓ **U (Unknown sequence number)**: indique le numéro de séquence de la destination est inconnu.
- **Réserved (11 bits):** initialisé à la valeur 0 et ignoré à la réception du message.
- **Hop Count (8 bits):** il contient le nombre de sauts parcourus par RREQ.
- **RREQ ID:** il identifie la requête parmi les requêtes envoyées par la même source.
- **Destination IP Address:** l'adresse IP de destination pour laquelle une route est désirée.
- **Destination Séquence Number:** Le dernier numéro de séquence reçu dans le passé par le créateur pour n'importe quelle route vers la destination.
- **Originator IP Adress:** l'adresse IP de la source de la requête.
- **Originator Sequence Number:** Le nombre de séquence courant de la source contenue dans la table de routage de ce nœud **s**.

3.2. Message de réponse à un RREQ par RREP

Il contient essentiellement les champs suivants: **[45]**

Type	R A	Reserved	Prefix Sz	Hop Count
Destination IP Address				
Destination Sequence Number				
Originator IP Address				
Lifetime				

Tableau 3.2 : Format du message RREP. [45]

- **Type (8 bits):** ce champ indique le type de paquet, dans ce cas il prend la valeur 2.

- **Flags (drapeaux) (2 bits):** ce champ contient deux flags:
  - ✓ **R (Repair flag):** utilisé pour le multicast.
  - ✓ **A (Acknowledgment required):** indique si la source doit envoyer un acquittement pout les messages RREP.
- **Reserved (9 bits):** initialisé à la valeur 0 et ignoré à la réception du message.
- **Préfix Sz (5 bits):** si la valeur de ce champs est différente de zéro, ce dernier indique que le nœud prochain peut être utilisé pour chaque nœud demandant cette destination et qui possède la même valeur de Préfix Sz.
- **Hop Count (8 bits):** il contient le nombre de sauts entre la source jusqu'à la destination.
- **Destination IP Address:** l'adresse IP de la destination du paquet RREQ.
- **Destination Sequence Number:** le numéro de séquence de la destination associé à cette route.
- **Originator IP Adress:** l'adresse IP du nœud qui crée la requête.
- **Lifetime:** le temps pour lequel chaque nœud qui reçoit RREP considère que la route est valide.

3.3. Message de perte de route RERR

Un message d'erreur de route contient essentiellement les champs suivants: **[45]**

Type	N	Reserved	DesCount
Unreachable Destination IP Address (1)			
Unreachable Destination Sequence Number (1)			

Tableau 3.3 : Format du message RERR. [45]

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

4. LE PRINCIPE DE NUMERO DE SEQUENCE

La circulation inutile des paquets de messages, qui peut arriver avec le DBF (Distribution de Bellman Ford), est intolérable dans les réseaux mobiles Ad Hoc, caractérisés par une bande passante limitée et des ressources modestes. **[46]**

L'AODV utilise les principes de numéro de séquence afin d'éviter le problème des boucles infinie et des transmissions inutiles de messages sur le réseau, en plus il permet de maintenir la consistance des informations de routage. A cause de la mobilité des noeuds dans le réseau Ad Hoc, les routes

changent fréquemment ce qui fait que les routes maintenus par certains noeuds, deviennent invalide. Les numéros de séquence permettent d'utiliser les routes les plus nouvelles ou autrement dit les plus fraiches (fresh routes), un noeud les mis à jour chaque fois qu'une nouvelle information provenant d'un message RREQ, RREP ou RERR, il incrémente son propre numéro de séquence dans les circonstances suivantes: **[46]**

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

5. FONCTIONNEMENT DU PROTOCOLE AODV

AODV **[47], [43]** est un protocole de routage réactif à vecteur de distance qui s'inspire de DSDV. Contrairement à celui-ci, il ne construit pas a priori la table de routage mais réagit à la demande et essaie de trouver un chemin avant de router les informations. Tant que la route reste active entre la source et la destination, le protocole de routage n'intervient pas, ce qui diminue le nombre de paquets de routage échangés entre les nœuds constituant le réseau.

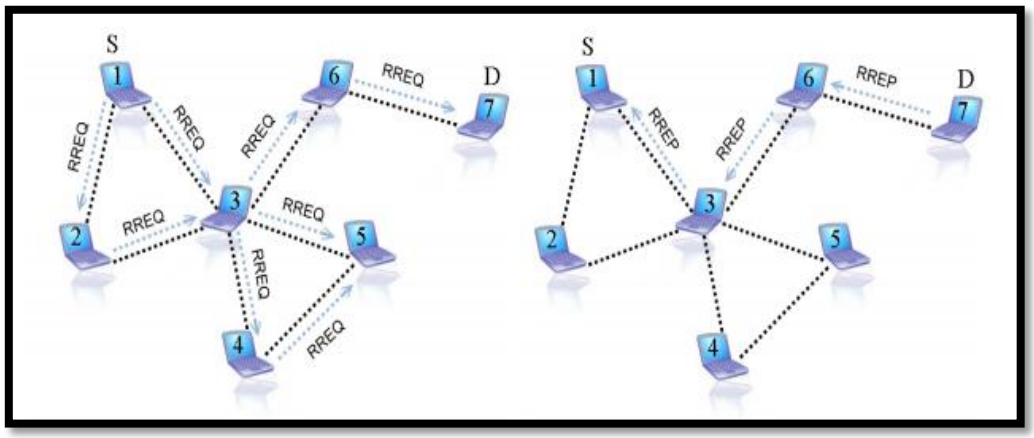


Figure 3.1: les deux requêtes RREQ et RREP utilisées dans le protocole AODV.

Lorsqu'un nœud **S** essaie de communiquer avec un nœud **D**, l'échange de messages se fait en plusieurs étapes décrites ci-dessous à l'aide de l'exemple de la figure 3.2:

5.1. Découverte de route

Lorsqu'un nœud source a besoin d'une route vers une certaine destination (e.g: le nœud 1 dans la figure 3.2 désire envoyer des données au nœud 5) et qu'aucune route n'est disponible (la route peut être non existante, avoir expiré ou être défaillante), la source 1 diffuse en broadcast (voir figure 3.2a) un message de demande de route RREQ (Route REQUEST), ce message contient un identifiant (RREQ_ID) associé à l'adresse de la source (@SRC) qui servira à identifier de façon unique une demande de route. Le nœud 1 enregistre cet identifiant de paquet RREQ ([RREQ_ID, @SRC]) dans son historique (buffer) et l'associe à un timer qui décomptera sa durée de vie au delà de laquelle cette entrée sera effacée. Quand un nœud intermédiaire (cas des nœuds 2 et 4 dans la figure 3.3b) qui n'a pas de chemin valide vers la destination reçoit le message RREQ, il ajoute ou met à jour le voisin duquel le paquet a été reçu. Il vérifie ensuite qu'il ne l'a pas déjà traité en consultant son historique des messages traités. Si le nœud s'aperçoit que la RREQ est déjà traitée, il l'abandonne et ne la rediffuse pas Sinon, il met à jour sa table de routage à l'aide des informations

contenues dans la requête afin de pouvoir reconstruire ultérieurement le chemin inverse vers la source , il incrémente ensuite le nombre de sauts HC (Hop Count) dans la demande de route et la rediffuse. Il est à noter qu'AODV utilise le principe des numéros de séquence pour pouvoir maintenir la cohérence des informations de routage. Ce numéro, noté SN (Sequence Number), est un champ qui a été introduit pour indiquer la fraicheur de l'information de routage et garantir l'absence de boucles de routages. À la réception d'un paquet RREQ (figure 3.2c), la destination 5 ajoute ou met à jour dans sa table de routage un chemin vers le nœud voisin duquel il a reçu le paquet (nœud 4) ainsi qu'un chemin vers la source 1. La destination 5 génère ensuite une réponse de route RREP qu'elle envoie en unicast vers le prochain saut en direction de la source (voir figure 3.2c). Notons qu'un nœud intermédiaire peut aussi générer un RREP si la requête l'autorise à le faire (bit destination only de la RREQ mis à 0) et qu'il dispose déjà dans sa table de routage d'un chemin valide vers la destination 5. Les nœuds intermédiaires qui reçoivent la RREP (cas du nœud 4 dans la figure 3.2d) vont mettre à jour le chemin qui mène à la destination dans leur table de routage et retransmettre en unicast le message (après avoir incrémenté le nombre de sauts) vers le nœud suivant en direction de la source sachant que cette information a été obtenue lors du passage de la RREQ. Lorsque la réponse de route atteint la source (nœud 1 dans l'exemple), un chemin bidirectionnel est établi entre la source et la destination (voir figure 3.2e) et la transmission de paquets de données peut débuter. **[48]**

5.2. Maintenance des routes

Afin de maintenir les routes, une transmission de messages HELLO est effectuée. Ces messages sont en fait des réponses de route (RREP) diffusés aux voisins avec un nombre de sauts égal à un. Si au bout d'un certain temps, aucun message n'est reçu d'un nœud voisin, le lien en question est considéré défaillant. Alors, un message d'erreur RERR (Route ERROR) se propage vers la source et tous les nœuds intermédiaires vont marquer la route comme invalide et au bout d'un certain temps, l'entrée correspondante est effacée de leur table de routage. Le message d'erreur RERR peut être diffusé ou envoyé en unicast en fonction du nombre de nœuds à avertir de la rupture de liaison détectée. Ainsi, s'il y en a un seul, le message est envoyé en unicast sinon, il est diffusé. **[48]**

AODV à l'avantage de réduire le nombre de paquets de routage échangés étant donné que les routes sont créées à la demande et utilise le principe du numéro de séquence pour éviter les boucles de routage et garder la route la plus fraîche. Cependant, l'exécution du processus de création de route occasionne des délais importants avant la transmission de données. **[48]**

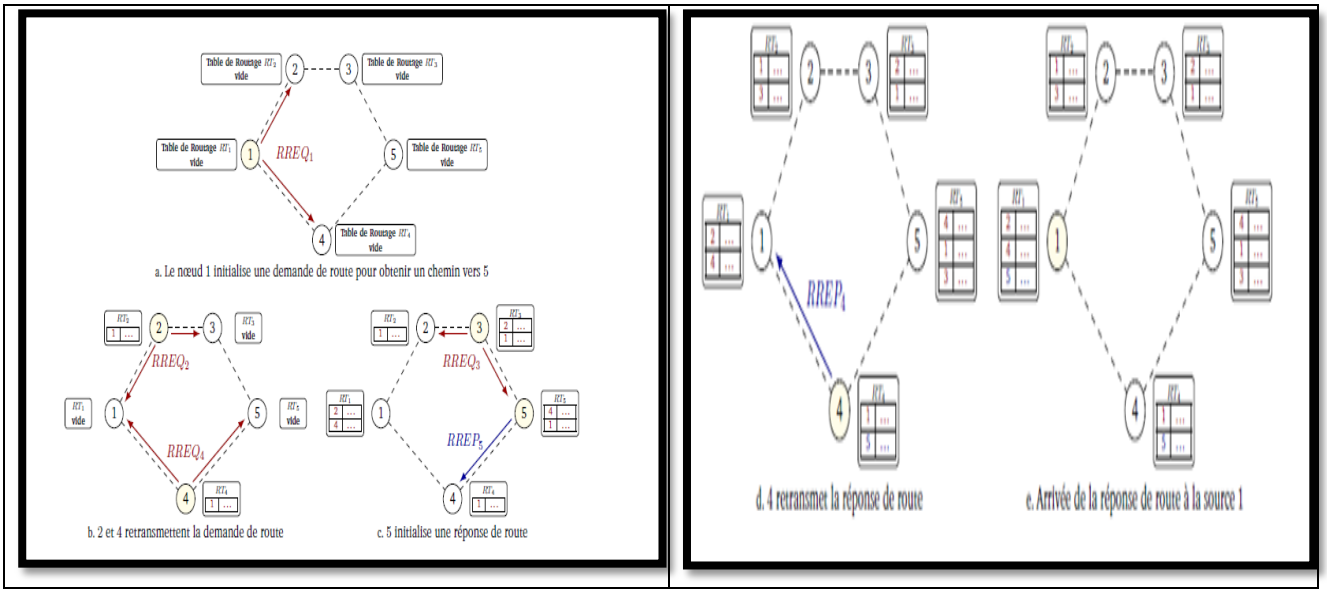


Figure. 3.2: Exemple d'établissement de route entre 1 et 5. [48]

5.3. Gestion des numéros de séquence

Il n'y a pas de numéro de séquence unique pour le réseau car il serait impossible de déterminer en permanence sa valeur de manière distribuée. Chaque nœud possède donc son propre numéro de séquence permettant de dater les informations provenant de lui seul. Un numéro de séquence est incrémenté dans les cas suivants: **[49]**

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

6. ÉVALUATION

Comme tout protocole réactif, AODV souffre d'un délai lors de l'envoi des premiers paquets vers une destination non connue. L'utilisation des numéros de séquence crée aussi une certaine complexité, mais a l'avantage de permettre de fortement limiter les retransmissions inutiles. Ajouté au fait que l'approche réactive du protocole ne pèse que peu sur la charge du réseau, il en résulte qu'AODV n'a que peu d'impact sur celle-ci. Les messages HELLO périodiques restent cependant nécessaires. Une différence majeure d'AODV par rapport à DSR est le fait qu'un nœud intermédiaire sur une route peut modifier la route d'une source à une destination. C'est notamment le cas si un lien est rompu et que le nœud intermédiaire parvient à trouver une route alternative ou si une meilleure route devient disponible entre le nœud intermédiaire et la destination. On peut parler de réparation locale du lien et d'optimisation locale de la route car ces informations n'ont pas à être remontées jusqu'à la source. Cette différence fait qu'AODV est plus adapté que DSR dans le cas d'une importante mobilité des nœuds**,** cela permet notamment à chaque source de choisir une route en fonction de critères qui lui sont propres, comme une métrique particulière ou encore le choix d'éviter certains nœuds ou liens **[50]**. Le routage par la source de DSR reste néanmoins intéressant de par le fait qu'il permet à la source de contrôler exactement quelle route est utilisée.

7. LIMITATION DU PROTOCOLE AODV

Dans le protocole AODV, les routes sont établies en fonction du « nombre minimal des sauts » (le plus court chemin), cependant, si le nombre des communications augmente le principe du plus court chemin n'est plus le critère optimal du choix des routes, il est préférable alors d'utiliser d'autres métriques qui ont un effet significatif sur la connectivité et la durée de vie du réseau. **[51]**

8. QUALITE DE SERVICE DANS LES RESEAUX AD HOC

8.1. Définition

La qualité de service QoS peut être définie comme le degré de satisfaction d'un utilisateur des services fournis par un système de communication. La QoS est définie dans **[52]** comme la capacité d'un élément du réseau (ex: routeur, noeud ou une application) de fournir un niveau de garantie pour un acheminement des données.

Dans les réseaux de télécommunication, l'objectif de la qualité de service est d'atteindre un meilleur comportement de la communication, pour que le contenu de cette dernière soit correctement acheminé, et les ressources du réseau sont utilisées d'une façon optimale.

Le RFC 2386 **[53]** caractérise la QoS comme un ensemble de besoins à assurer par le réseau pour le transport d'un trafic d'une source à une destination.

8.2. Critères

La QoS **[54]** au niveau d'un réseau se décline en quatre paramètres: le délai, la gigue, le débit (la bande passante) et la perte.

- **Le délai de bout en bout:** c'est le temps mis pour transférer un paquet entre deux nœuds.
- **La gigue:** c'est la variation de l'intervalle de temps entre deux paquets durant leur acheminement entre la source et la destination.
- **La bande passante:** c'est le volume total d'informations qui peut absorber un lien entre deux noeuds sans créer de file d'attente.
- **La perte de paquets:** c'est le nombre de paquets perdu par rapport au nombre de paquets émis.

En fonction des applications considérées, le paramètre à prendre en compte varie : par exemple, pour la vidéo, les paramètres importants sont la bande passante, la gigue et le délai, pour un échange de fichiers, il vaut mieux limiter la perte de paquets.

8.3. Qualité de service dans les réseaux Ad Hoc

La recommandation E.800 du CCITT (Consultative Committee for International Telegraph and Telephone) définit la qualité de service (QoS pour Quality of Service ou QoS pour (Qualité de Service) comme: « l'effet général de la performance d'un service qui détermine le degré de satisfaction d'un utilisateur du service ».

Cette définition reflète la perception de la qualité de service de point de vue d'un utilisateur **[55]**. Dans le RFC 2386 **[56]**, la QoS est définit comme un ensemble de besoins à assurer par le réseau pour le transport d'un trafic d'une source à une destination. Ces besoins peuvent être traduits en un ensemble d'attributs pré-spécifiés et mesurables en terme de:

- Délai de bout en bout.
- Variance de délai (gigue).
- Bande passante.

- Pertes de paquets.

8.4. Qualité de service pour le protocole de routage AODV

Cette extension **[57]** utilise également une métrique de bande passante basée sur la gestion du nombre de slots TDMA à partir des besoins de la source. Dans la mesure où le protocole de routage associé est réactif, les routes avec QoS ne sont établies que sur requête. Le routage QoS va donc simultanément déterminer la route et les slots nécessaires pour chaque lien de la route en fonction de la requête initiale. Un algorithme de mesure de la bande passante disponible sur la route tracée par AODV est mis en œuvre en même temps que la recherche de route (RREQ). Chaque noeud est capable de déterminer au fur et à mesure les slots libres pour le nouveau flux. Les slots libres pour chaque noeud sont évalués en fonction des slots occupés pour émettre ou recevoir avec ses voisins. On peut ainsi définir l'ensemble des slots libres pour qu'un noeud ni émettent sans causer d'interférences à ses voisin récepteurs (SRTi) ainsi que l'ensemble des slots libres pour qu'un noeud ni reçoive sans subir d'interférences de ses voisins émetteurs (SSRI).

Les paquets RREQ du protocole AODV sont enrichis avec les informations de bande passante liées à l'algorithme utilisé.

Après évaluation de la bande passante de bout en bout, les paquets de réponse (RREP) remontent et réservent les slots jusqu'à la source.

9. SECURITE DU ROUTAGE DANS LES RESEAUX AD HOC

9.1. Présentation

Les protocoles de routage Ad Hoc **[58]**, tels que conçus, manquent de contrôles de sécurité, ce qui augmente le risque d'attaques qui peuvent être orchestrées par des noeuds externes ou internes.

- **Les attaquants externes:** sont des noeuds qui ne font pas partie du réseau. Dans ce cas, la mise en place de mécanismes cryptographiques peut résoudre le problème seuls les nœuds ayant les autorisations nécessaires pourront accéder au réseau ou déchiffrer le contenu.
- **Les attaquants internes:** sont des noeuds faisant légitimement partie du réseau. Ces nœuds ont les autorisations et les matériels cryptographiques nécessaires pour appartenir au réseau et les autres noeuds leur font a priori confiance.

Les attaquants internes sont plus difficiles à détecter et à éviter que les attaquants externes. Cela requiert de mettre en place des mécanismes de détection des noeuds attaquants et des mécanismes pour contrer leurs agissements.

Quelque soit sa position (interne ou externe), le noeud malhonnête utilise plusieurs techniques pour perturber le bon fonctionnement du protocole. La combinaison de ces techniques peut aboutir à une attaque plus élaborée.

9.2. Les attaques sur le protocole du routage AODV

9.2.1. Attaques élémentaires portant sur les demandes de route

a. Suppression d'une demande de route

Un noeud malhonnête pourrait simplement effacer la demande de route reçue. En appliquant ce genre de comportement à tout message RREQ reçu, l'attaquant ne participe pas au routage : c'est comme s'il ne faisait pas partie du réseau. Une autre variante serait d'effacer sélectivement des messages RREQ. Ce comportement peut être comparé à celui d'un noeud égoïste. **[48]**

b. Modification d'une demande de route

À la réception d'une demande de route, le noeud malhonnête modifie un ou plusieurs champs qu'il n'est pas supposé modifier avant de retransmettre le message. La modification peut aussi porter sur un champ qu'il a le droit de modifier, mais il ne respecte pas la spécification pour le faire. **[48]**

c. Fabrication d'une demande de route

Les attaques par fabrication peuvent être effectuées sans avoir reçu de messages RREQ. Le noeud malhonnête a besoin de collecter certaines informations, en écoutant le trafic par exemple, avant d'injecter le message fabriqué. Il est à noter que l'attaquant peut falsifier autant de champs qu'il veut générant l'effet discuté un peu plus haut dans **Rushing d'une demande de route.[48]**

Dans d'autres cas, le noeud malhonnête peut utiliser la technique du rushing **[59]** qui consiste à diminuer le temps de traitement des messages RREQ et les retransmettre plus rapidement de telle sorte qu'ils atteignent plus rapidement la destination. Ceci garantira pour le nœud malhonnête une place sur le chemin.

9.2.2. Attaques élémentaires portant sur les réponses de route

La mise en place de certaines attaques portant sur les réponses de route dépend de l'emplacement de l'attaquant: il faut qu'il soit choisi sur la route ou qu'il soit voisin d'un noeud faisant partie du chemin pour pouvoir entendre la transmission de la RREP, qui rappelons le, est effectuée en unicast. **[48]**

a. Suppression d'une réponse de route

Ce type d'attaque n'a un sens que si le noeud malhonnête a été choisi sur la route reliant la source à la destination. Dans ce cas, la suppression de la réponse de route empêche la formation du chemin vers la destination et entraine des messages de contrôle supplémentaires suite à l'initialisation d'un nouveau processus de création de route, ce qui dégrade la qualité de service. **[48]**

b. Modification d'une réponse de route

Le noeud malhonnête peut jouer sur le numéro de séquence de la destination et/ou le nombre de sauts dans une RREP en augmentant le premier et en diminuant le second.

Ces paramètres sont pris en compte lors de la mise à jour du chemin vers la destination : une mise à jour est possible si le numéro de séquence reçu dans la demande de route est plus grand que celui stocké dans la table de routage ou les numéros de séquence sont égaux et le nombre de sauts reçu est plus petit que celui stocké dans la table de routage. **[48]**

c. Fabrication d'une réponse de route

Certaines attaques peuvent être effectuées sans pour autant être choisi sur le chemin. C'est le cas des attaques par fabrication:

- **Fausse réponse:** à la réception d'une demande de route, le noeud malhonnête fabrique une réponse de route même s'il n'a pas de chemin valide vers la destination. **[48]**
- **Réponse active:** des réponses de route sont fabriquées et injectées dans le réseau même sans avoir reçu une demande de route au préalable. Dans ce cas le noeud malveillant peut jouer sur tous les champs précédemment présentés pour produire l'effet désiré. Une variante de cette attaque vise à déborder la table de routage d'une cible en proposant des routes (via RREP) vers des noeuds (nouveaux ou inexistants). En écoutant la transmission

d'une réponse de route qui ne lui est pas destinée, un nœud malhonnête peut fabriquer et injecter un paquet RREP proposant un chemin plus court et plus frais provoquant la mise à jour du chemin vers la destination qui passe dorénavant par le noeud malveillant. **[48]**

10. COMPARAISON ENTRE AODV ET DSR

- DSR à moins de frais généraux de routage qu'AODV.
- AODV a en tête MAC moins normalisée que DSR.
- DSR est basée sur un mécanisme de routage source alors qu'AODV utilise une combinaison de DSR et DSDV mécanismes.
- AODV a de meilleures performances que DSR dans des scénarios de meilleure mobilité.
- DSR a des processus itinéraire de découverte moins fréquents qu'AODV.

	DSR	**AODV**
Routes maintenue dans	Cache de route	Table de routage
Découverte de route nécessaire	Oui (agressive)	Oui (complètement)
Mise à jour périodique nécessaire	Non	non
Utilise des messages hello	Non	Oui (aux voisins actifs seulement)
Chemin inséré dans l'en tête du paquet	Oui	non
Utilise des temporisateurs de route	Non	Oui
Multiple routes disponibles	Oui	Non
Mise à jour auprès de	Pas de mise à jour	Pas de mise à jour

Tableau 3.4 : Comparaison entre AODV et DSR.

11. DEFINITION DE L'OPTIMISATION

Est cherché le point ou un ensemble de points de l'espace d'état possible qui satisfait au mieux un ou plusieurs critères. Le résultat est appelé valeur optimale ou optimum. **[61]**

On peut dire qu'un problème d'optimisation se définit comme la recherche du minimum ou du maximum (de l'optimum donc) d'une fonction donnée. On peut aussi trouver des problèmes d'optimisation pour lesquels les variables de la fonction à optimiser sont des contraintes à évoluer dans une certaine partie de l'espace de recherche.

CONCLUSION

AODV est un protocole de routage a 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.

CHAPITRE IV

La Simulation Et Les Simulateurs Réseau

INTRODUCTION

Pour montrer l'efficacité et les performances d'un système, il n'est pas toujours possible d'accéder aux infrastructures nécessaires en raison de leurs coûts élevés. Pour préserver ce problème, on a du faire recours à la simulation qui met à la disposition des utilisateurs un environnement de simulation assez complet. Dans ce chapitre nous commençons par une définition et les différente type de la simulation, ensuite une d'analyse des différents simulateurs (OMNET, NS et OPNET). Pour augmenter notre choix de simulateur sur OPNET (Optimum Network Performance) qui est un outil de simulation de réseaux très puissant, très complet et le moyen le plus adaptable pour tester et évaluer notre solutions.

1. SIMULATION

1.1. Définition

Dans nos jours, la simulation connait un essor considérable, et ce grâce à l'intérêt que présente les modèles informatiques des systèmes simulés. **[62]**

La simulation consiste à la modélisation informatique d'un système quelconque, en offrant une représentation de toutes les entités de ce système, leurs comportements propres, ainsi que leurs interactions. Elle met à la disposition de l'utilisateur un environnement d'expérimentation dont on peut faire varier les paramètres.

Grâce aux progrès réalisés dans le domaine du développement et des techniques de programmation, nous disposons aujourd'hui de langages de programmation très puissants. Ainsi, il devient possible de réaliser un simulateur dans un environnement de programmation existant. **[62]**

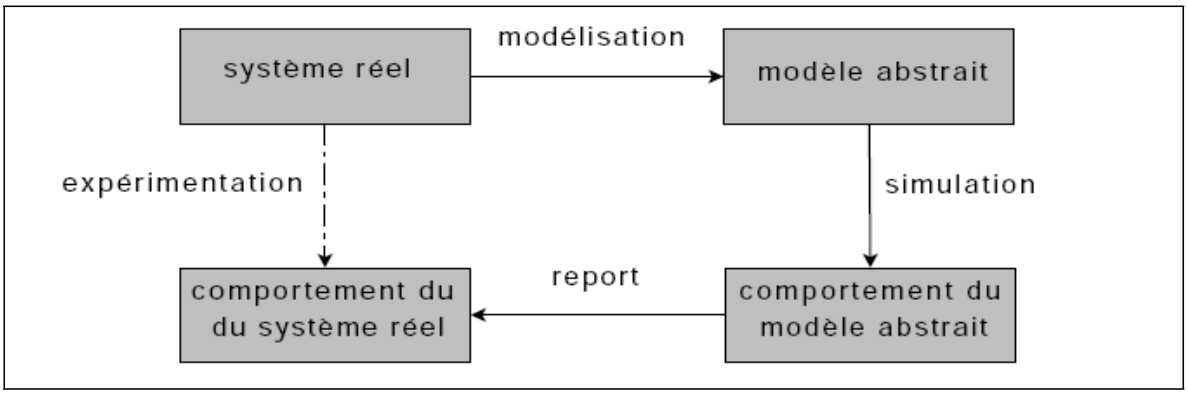


Figure 4.1: Cycle modélisation-simulation. [63]

La simulation d'un système réel devient nécessaire dès lors que les modèles analytiques deviennent, soit trop complexes en termes de calcul et de temps de résolution, soit trop simplifiés vis-à-vis de la réalité rendant, par ce fait, les résultats obtenus non représentatifs du comportement du système dans un environnement réel. Ainsi, la simulation peut s'avérer nécessaire dans les cas suivants**: [63]**

- Les expériences sur système réel sont trop coûteuses en termes de ressources matérielles et Humaines.

- Les expériences sur système réel ne sont pas reproductibles ni représentatives de tous les environnements possibles. Dans ce cas, la simulation permet de caractériser le comportement global du système pour différents environnements.

1.2. Intérêt de la simulation

On fait recours à la simulation dans les différents cas suivant: **[64]**

- Quand le système réel est inobservable ou difficilement observable pour toutes sortes de raisons (dimension, sécurité, coût, inexistence...).
- Quand on ne peut pas facilement observer les états du système.
- Quand on désire analyser l'enchaînement des événements dans le système, ainsi que les relations de causes à effets.
- Quand on désire valider une solution analytique.
- Quand la complexité des interactions dans le système est telle qu'elle ne peut être étudiée qu'au travers de simulations.
- Quand on veut tester différentes optimisations pour améliorer un système déjà existant.

1.3. Différents type de simulation

Les types de simulation sont: **[65]**

- **Simulations statiques:** Méthode applicable seulement si le temps n'a pas d'influence, utilise des tirages aléatoires et souvent uniformes.
- **Simulations dynamiques:** Système qui change dans le temps.
- **Simulations Déterministes:** Qui ne contient pas de variable aléatoire, une variable d'entrée donnée, produit toujours le même résultat.
- **Simulations Stochastiques:** Entrées et sorties sont aléatoires.
- **Simulations à événements discrets:** La simulation à événements discrets permet de modéliser un système réel dont le comportement peut changer en fonction de l'apparition d'événements au cours du temps. Par exemple, en considérant un réseau avec des entités communicantes, les événements peuvent être: la transmission d'un nouveau paquet, la réception d'un paquet, la mobilité d'une des entités, etc. Ces différents événements apparaissent à des instants biens spécifiques du temps.

1.4. Avantages et inconvénients de la simulation

Nous trouvons aussi dans la simulation et les avantages et les inconvénients: **[65]**

- **Avantage**:
  - ✓ Observations des états du système.
  - ✓ Etudes des points de fonctionnement d'un système.
  - ✓ Etudes de l'impact des variables sur les performances du système.
  - ✓ Etude d'un système sans les contraintes matérielle.
- **Inconvénients:**
  - ✓ La conception de modèles peut nécessiter des compétences spéciales.
  - ✓ Résultats pas forcément généralisable.

2. SIMULATEUR

Nous appelons simulateur un programme qui met en œuvre un modèle de simulation par événements discrets. La tache première d'un simulateur est d'assurer que la chronologie des événements soit respectée. A chaque occurrence d'un événement, les actions qui sont associées à celui-ci sont exécutées. **[66]**

3. SIMULATION DANS LE RESEAU

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. **[67]**

4. OUTILS DE SIMULATION

a. NS (Network Simulator)

- **Présentation**

C'est un simulateur **[68]** qui permet la description et la simulation de réseaux IP filaires et sans fil. Il est certainement le plus populaire des simulateurs de réseau. Son projet a débuté en 1989 avec le simulateur réseau REAL, il a connu plusieurs extensions via les contributions de la communauté scientifique. Il est aussi accompagné d'outils de visualisation graphique, le **nam** (Network Animation), permettant d'observer graphiquement le comportement des objets durant la simulation.

NS-2 se base sûr deux langages de programmations distinctes:

- ✓ C++ qui constitue la partie centrale du simulateur (le noyau) et qui définit tout le mécanisme interne des objets de simulation.
- ✓ OTCL (Object Oriented Tool Command Langage) qui met en place la simulation par l'assemblage et la configuration des objets.

- **Fonctionnement**

L'application NS est composée de deux éléments fonctionnels: **[68]**

- ✓ Un interpréteur.
- ✓ Un moteur de simulation.

Au moyen de **l'interpréteur** l'utilisateur est capable de créer le modèle de simulation, ce qui revient à assembler les différents composants nécessaires à l'étude. Les composants du modèle de simulation sont appelés objets ou encore instances de classe. **Le moteur de simulation** quant à lui effectue les calculs applicables au modèle préalablement construit par l'utilisateur via l'interpréteur. **[68]**

- **Avantages**
  - ✓ La flexibilité.
  - ✓ La richesse.
  - ✓ La réutilisabilité.
  - ✓ L'extensibilité.
  - ✓ La disponibilité de son code.

- **Inconvénients**

La modélisation dans NS-2 reste une tâche complexe:

- ✓ Il n'y a pas d'interface graphique.
- ✓ Une forte technicité est requise pour utiliser ce simulateur.

b. Le simulateur OMNET

- **Présentation**

Le simulateur OMNET++ est un simulateur à évènements discrets dans lequel les différents éléments du réseau communiquent par envoi de messages. OMNET++ est un projet open source dont le développement a commencé en 1992 par Andras Vargas à l'université de Budapest. C'est une bibliothèque de simulation écrite en C++ pour construire des simulateurs des réseaux au sens large, c.-à-d réseaux filaires et sans fils, mais également des réseaux internes aux machines (BUS de processeur par exemple). **[65]**

OMNET **[65]** se distingue par son orientation objet et l'utilisation de modules hiérarchisés qui permet une grande flexibilité dans la création de nœuds complexes au sein du réseau. Il peut donc être utilisé pour:

- ✓ La modélisation de trafic de réseaux de communication.
- ✓ La modélisation de protocoles.
- ✓ La modélisation de réseaux de files d'attente.
- ✓ et d'autres systèmes distribués.

- **Structure d'OMNET**

L'architecture d'OMNET++ est hiérarchique composé de modules. Un module peut être soit module simple ou bien un module composé. Les feuilles de cette architecture sont les modules simples qui représentent les classes C++. Pour chaque module simple correspond un fichier **.cc** et un fichier **.h**. Un module composé est composé de simples modules ou d'autres modules composés connectés entre eux. Les sous modules et les ports de chaque module sont spécifiés dans un fichier **.ned**. **[65]**

La communication entre les différents modules se fait à travers les échanges de messages. Les messages peuvent représenter des paquets, des trames d'un réseau informatique, des clients dans une file d'attente ou bien d'autres types d'entités en attente d'un service. **[65]**

- **Avantage**

L'avantage de OMNET ++ est sa facilité d'apprentissage, d'intégration de nouveaux modules et la modification de ceux déjà implémentés. Ainsi il n'est pas payant.

5. ENVIRENNEMENT DE SIMULATION: OPNET MODELER

L'environnement OPNET permet la modélisation et la simulation de réseaux de communication grâce à ses bibliothèques de modèles (routeurs, commutateurs, stations de travail, serveurs …) et de protocoles (TCP/IP, FTP, FDDI, Ethernet, ATM …). Le module Radio OPNET permet la simulation des réseaux de radiocommunication: hertzien, téléphonie cellulaire et satellitaire. **[69]** Ce simulateur peut être très flexible quand il est utilisé dans l'étude: [**70]**

- ✓ de la communication dans les réseaux.
- ✓ des protocoles de communications.

- ✓ des équipements.
- ✓ des applications.

Il 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. Une technique de programmation orienté objet est utilisée pour créer le ''mapping'' de la synthèse graphique réalisée vers l'implémentation de systèmes réels. **[70]**

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

Figure 4.2: Versions du simulateur OPNET.

Un exemple de l'interface graphique utilisateur de l'OPNET est présenté sur la figure suivante:

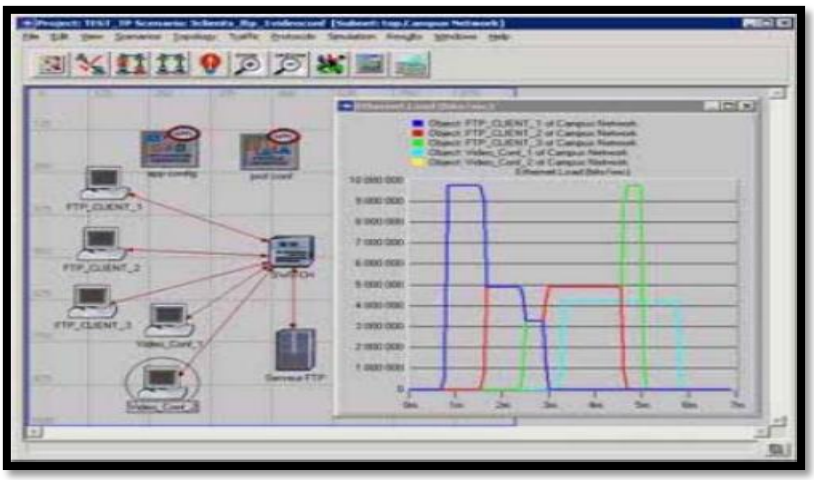


Figure 4.3: exemple d'interface d'OPNET.

L'OPNET **[70]** présente trois fonctions principales:

- **Modélisation**: il dispose d'un environnement graphique pour créer tout type de modèles de protocoles.
- **Simulation:** il utilise trois différentes technologies avancées de simulation.
- **Analyse:** les données et résultats de simulation peuvent être analysés et affichés d'une manière assez simple en utilisant entre autres des graphes, des cartes, des statistiques.

5.1. La structure d'OPNET

OPNET dispose de trois niveaux hiérarchiques imbriqués:

- **Le module réseaux**

Dans ce domaine, la portée et l'étendu globaux du réseau à simuler sont spécifiés. C'est une description haut-niveau des objets contenu dans le système. Ce domaine permet le développement des modèles réseaux spécifiant les objets du système tout comme leurs localisations physiques, interconnections et configurations. **[71]**

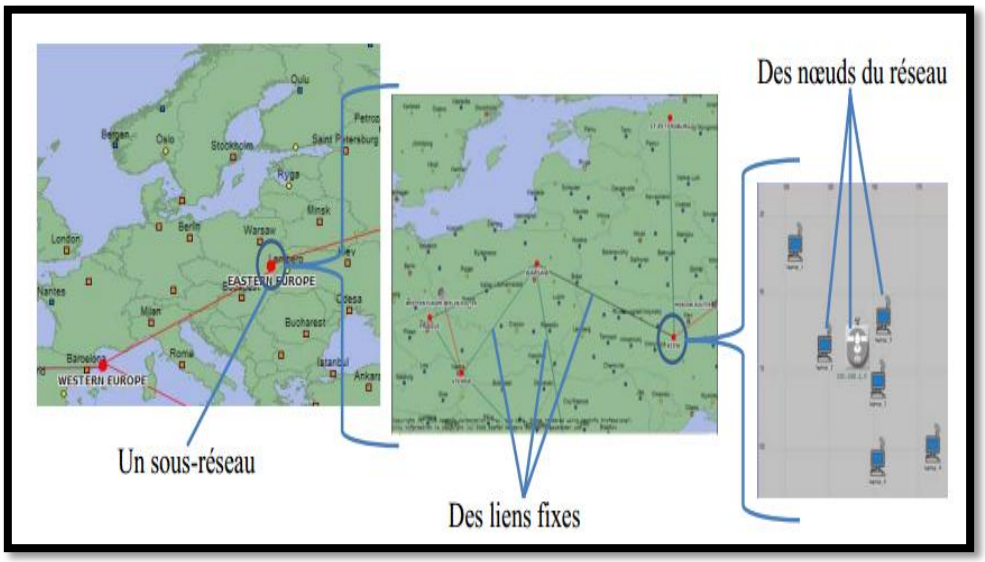


Figure 4.4: Exemple de modélisation d'un réseau WLAN sous OPNET.

Ce domaine **[70]** permet aussi de spécifier les réseaux mobiles et sans-fils. Dans ce sens, OPNET offre des fonctions pour modéliser des éléments mobiles tels que les satellites. La mobilité peut être réalisée de trois façons:

- ✓ **Mobilité par trajectoire**: un nœud suit une trajectoire prédéfinie durant la simulation. Cette trajectoire peut être dessinée ou définie pas à pas.
- ✓ **Mobilité par vecteur**: un nœud se déplace par rapport à un vecteur de mobilité défini avec les attributs du nœud qui peuvent être modifiés durant la simulation.
- ✓ **Mobilité des coordonnées des nœuds**: un module processeur est créé, et ce dernier modifie les coordonnées des nœuds durant la simulation selon le modèle spécifié.

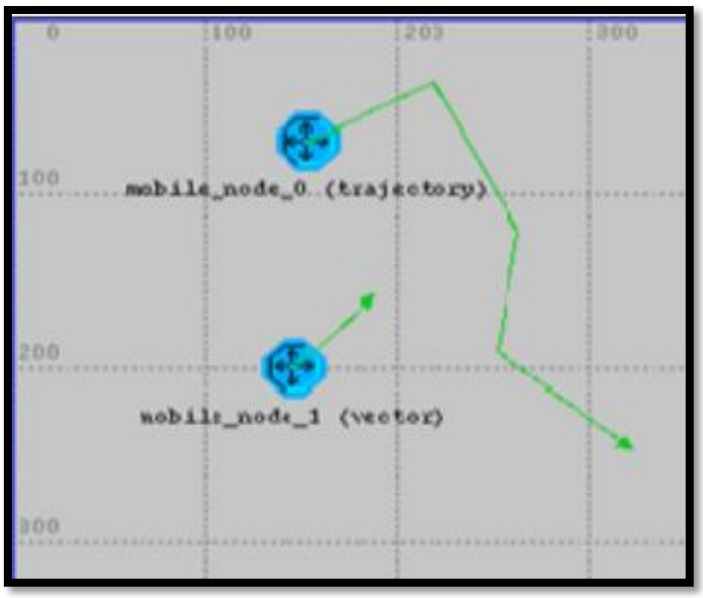


Figure 4.5: Exemple de modélisation de trajectoire sous OPNET.

- **Le module node**

Il sert à définir le fonctionnement d'un nœud d'un réseau construit grâce au « Project editor » mais dans le cadre de notre simulation, il sert à simuler l'ensemble du réseau. Les nœuds spécifient la structure interne d'un nœud réseau. Des nœuds typiques incluent les stations de travail, les switches des paquets, les terminaux satellites, les capteurs à distances, etc. Trois types de nœuds sont considérés : fixe, mobile et satellite. Un nœud peut aussi être un type spécial de nœud représentant par exemple un réseau Ethernet et son trafic agrégé comme une seule entité. **[71]**

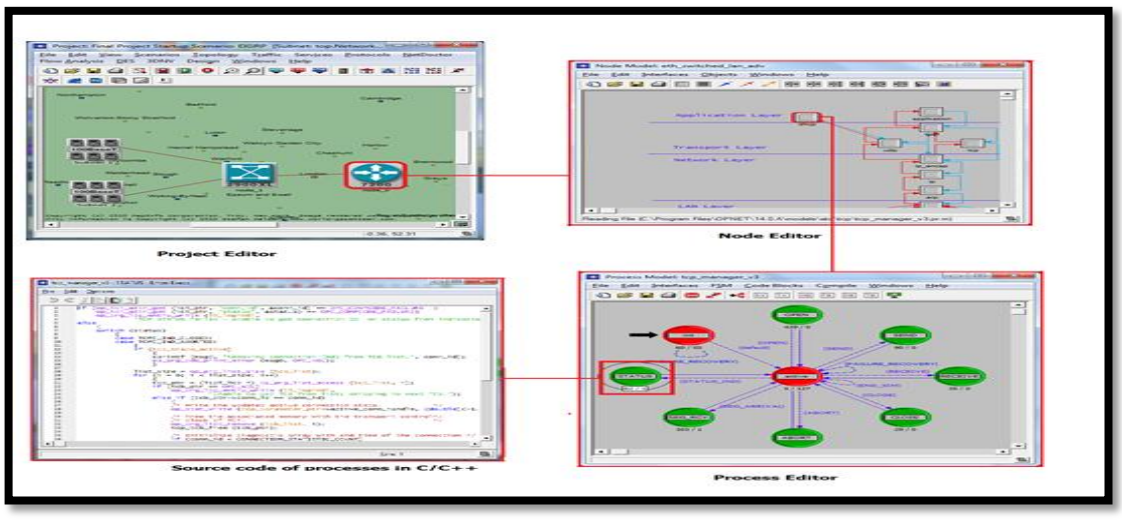


Figure 4.6: Architecture d'OPNET.

- **Le module process**

Il définit normalement la machine à états d'un élément du nœud mais, dans notre cas le protocole « AODV ». L'ensemble de ce protocole est codé en **C** en utilisant des packages fournis par OPNET. Les modèles de processus sont employés afin de spécifier le comportement des processeurs ou des modules de files qui existent dans les modèles de nœuds. Un module est représenté par une machine à états finis qui est constituée d'un ensemble d'états et de transitions et

de conditions entre ces états. L'éditeur de modèles de processus n'est qu'un outil pour faciliter le développement des codes sources **C** et **C++** du modèle souhaité. **[70]**

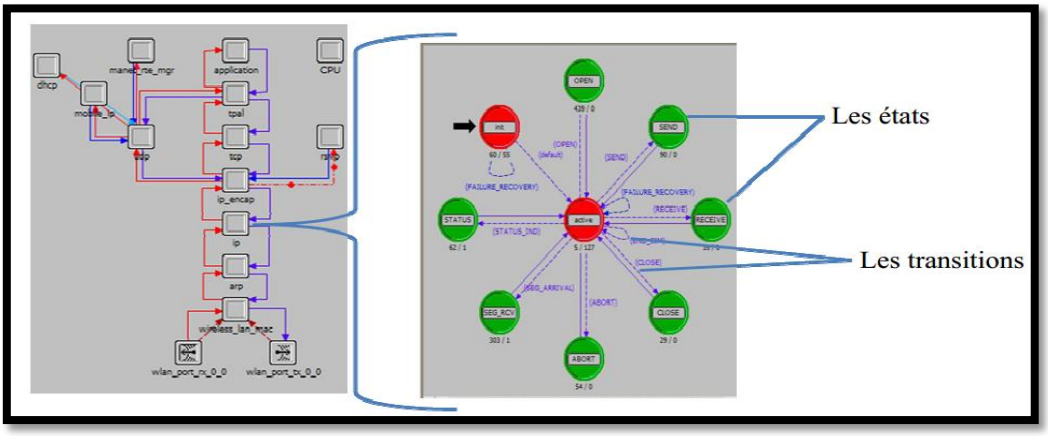


Figure 4.7: Exemple de modélisation de processus sous OPNET.

- **Avantages**

Il permet de concevoir et d'étudier des réseaux de communications, des nouvelles technologies, des protocoles et des applications avec facilité et évolutivité. **[65]**

- **Inconvénients**

Parmi les problèmes d'OPNET: **[65]**

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

5.2 Exemple de création d'un réseau Ad Hoc sur OPNET

Après avoir lancé OPNET Modeler et validé les conditions d'utilisation, vous allez créer une topologie du réseau.

Pour créer un nouveau projet, utiliser le menu File>New, puis compléter chaque étape de la manière suivante :

- **Nom de projet :** reseau ad_hoc
- **Scénario name :** scenario1
- **Initial topology :** create empty scenario
- **Network Scale :** Office
- **Size :** 100m*100m (unites metres)
- **Select technologies :**Manet, wireless_lan ,wireless_ lan_adv

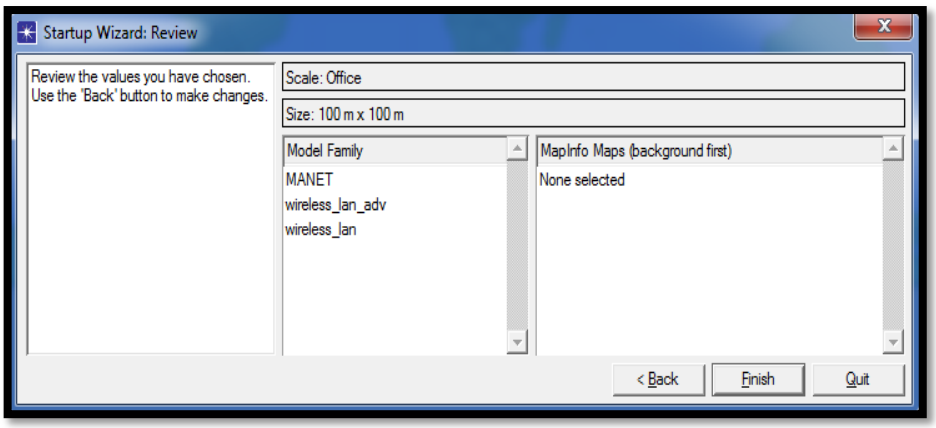


Figure 4.8: Choix de la surface de simulation du réseau Ad Hoc.

Vous allez maintenant créer votre réseau en utilisant topology > deploy wireless network. (NOTE : on peut utiliser des objets venant de palettes par defaut)

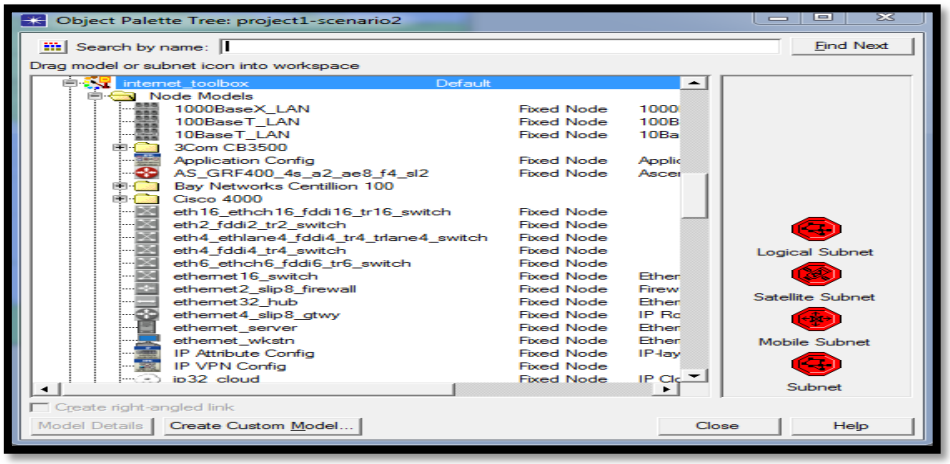


Figure 4.9: Palette offrant les composantes nécessaires à la création du réseau Ad Hoc.

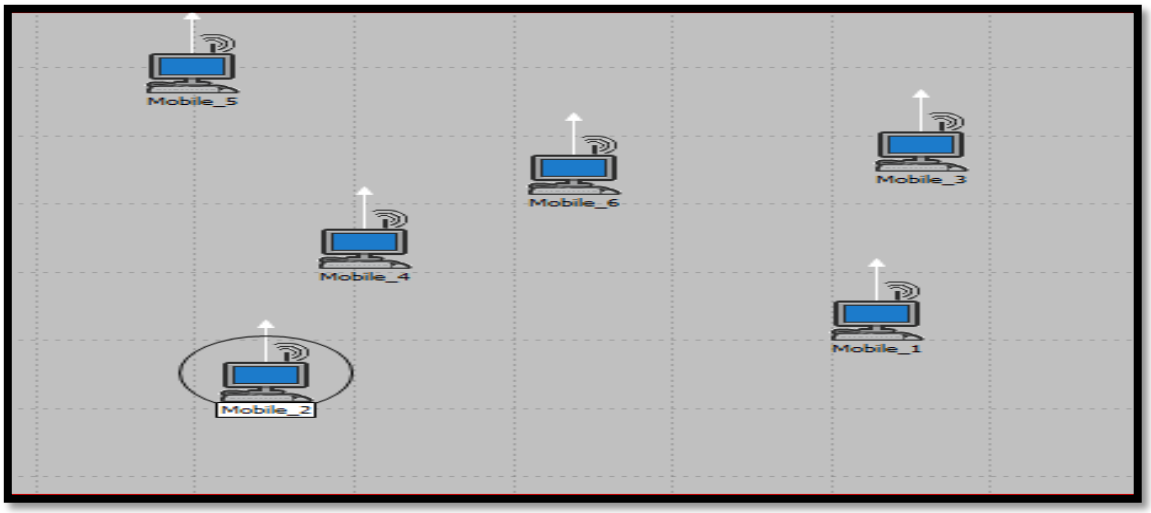


Figure 4.10: réseau Ad Hoc.

CONCLUSION

Il existe une grande variété de simulateurs de réseau. On citer par exemple Network Simulator 2 et son extension « sans fil », OPNET...etc. Ceux-ci permettent de simuler une topologie dans laquelle il est possible de faire transiter des données et pour tester un protocole de routage on a recours souvent à la simulation. Dans le chapitre suivant, nous proposons une version améliorée et simplifiée de protocole AODV.

CHAPITRE V

Optimisation De Protocole De Routage AODV Basée Sur Le Débit Dans Le Calcul De Meilleur Chemin

INTRODUCTION

Parmi Les inconvénients majeurs de protocole AODV est qu'il choisi le meilleur chemin a base de nombre de saut. L'objectif principal de ce chapitre est de présenter notre contribution qui consiste de modifier le protocole de routage AODV de sorte que les routes sont choisis a base de débit le plus élevé au lieu de nombre de sauts le plus bas. Au début nous avons cité les travaux d'optimisation de protocole AODV. Ensuite nous avons faire une description du protocole proposé et enfin on a discuté l'environnement utilisé pour l'implémentation de solution de notre contribution.

1. TRAVAUX ANTERIEURS SUR L'OPTIMISATION DU PROTOCOLE DE ROUTAGE AODV

1. P. Parvathi **[76]** avait fait l'analyse comparative des CBRP, AODV et DSDV. Il a observé que DSDV consomme plus de bande passante, en raison de la diffusion des mises à jour fréquentes et que AODV est meilleur que DSDV puisqu'il ne maintient pas de tables de routage au niveau des nœuds.
2. Hemant G. et.al. **[78]** ont proposé une étude sur la façon de perte des paquets dans le protocole AODV et qui peut être minimisé dans un réseau donné. Ils ont développé une technique qui identifie le lien rompu entre deux noeuds quelconques puis réparé la même voie.
3. Li Y.et.al **[77]** avait fait une optimisation dynamique non linéaire lors de la phase de découverte de route de AODV et ceci en simulant puis analysant le taux de livraison des paquets. Les résultats ont montré que le protocole proposé améliore la capacité de transmission de données du nœud tout en réduisant le taux de perte de paquets.
4. Au regard de l'importance de la conservation d'énergie dans les réseaux mobiles Ad Hoc, les auteurs **[51]** proposaient ER-AODV (Energy Reverse Ad-hoc On-demand Distance Vector routing), un protocole de routage réactif qui repose sur une politique combinant deux mécanismes appliqués au protocole AODV. Ils visent à incorporer l'énergie comme métrique de routage dans le processus de sélection de la route. En effet les énergies résiduelles des noeuds mobiles ont été considérées lors de la prise des décisions de routage. Les résultats de simulation montrent que le protocole ER-AODV répond à une meilleure conservation d'énergie.
5. Sujata et.al. **[75]** avaient fait la comparaison des AODV et RAODV. En RAODV, ils avaient changé la configuration des paquets de rediffusion de route d'AODV et l'a nommé RRREQ. Ils ont montré que les résultats de simulation de RAODV obtenus sont meilleurs par rapport aux autres versions d protocole AODV. Ensuite, ils ont travaillé sur le concept d'énergie dans RAODV, de sorte qu'ils peuvent affecter la priorité des différents chemins dédiés entre la source et la destination en se basant sur l'énergie ainsi que la stabilité des nœuds ou des chemins.
6. Les auteurs **[79]** proposent un algorithme de routage qui est adopté par optimiser Ad- hoc protocole de vecteur de distance (OAODV) pour améliorer l'énergie des appareils mobiles. Lorsque l'énergie d'un noeud atteint ou au-dessous de ce niveau, le noeud ne doit pas être considère comme un noeud intermédiaire, jusqu'à ce que et à moins qu'aucun autre chemin d'accès est disponible.

- **Résultat et simulation**
  - ✓ **débit**

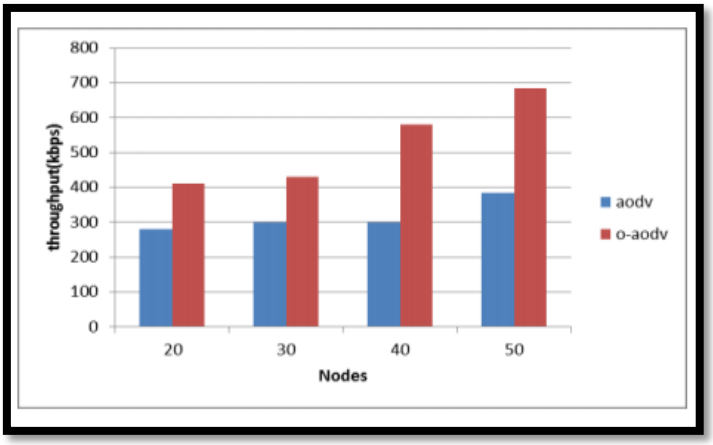


Figure 5.1: Débit d'AODV et O-AODV.

Le résultat de la simulation indique que le schéma proposé fournit des performances améliorées. OAODV génère un bon débit par rapport à AODV.

- ✓ **taux de livraison de paquets:**

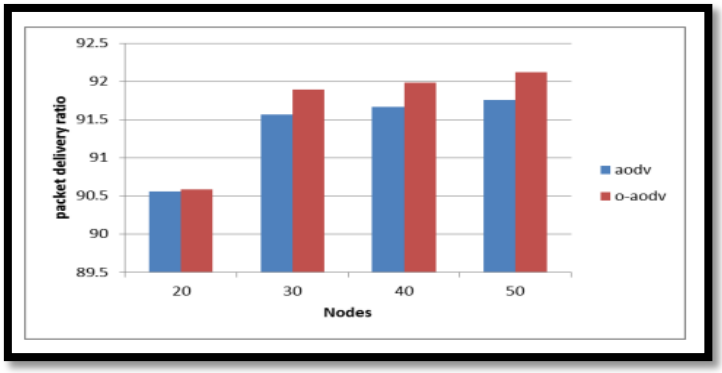


Figure 5.2: Paquet reçu d'AODV et O-AODV.

La simulation montre que le rapport de distribution de paquets est beaucoup mieux dans OAODV par rapport à l'AODV.

- ✓ **Consommation de l'énergie**

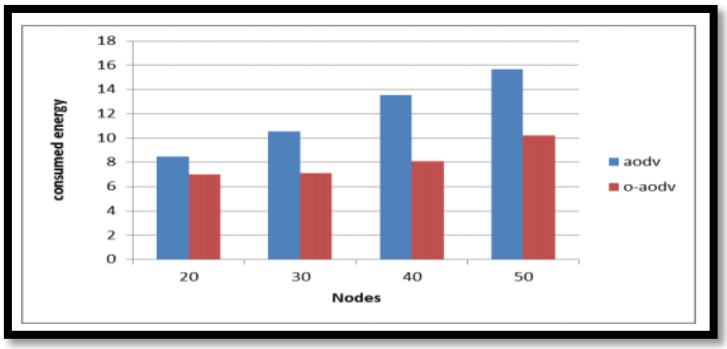


Figure 5.3: Energy consomé d'AODV et O-AODV.

Le résultat montre que l'énergie consommée par AODV est plus qu'OAODV, cela indique que le protocole proposé est plus performant qu'AODV.

7. Dans **[72]**, les auteurs proposent un mécanisme amélioré pour estimer la largeur de bande passante disponible dans les réseaux Ad Hoc IEEE 802,11. Ils ont intégré cette technique d'évaluation de largeur de bande (ABE) dans le protocole AODV utilisant NS-2 comme environnement de simulation. Le protocole proposé est fut t'appeler l'ABE-AODV.
8. Dans **[73]**, un protocole mutant AODV appelé ICBCC-AODV (Integration of current bandwidth capacity calculation) a été proposé. L'idée principale consiste à calculer la largeur de bande actuelle et la comparer avec la largeur de bande requise ensuite l'envoie des données au nœud destination sera effectué. ICBCC_AODV c'est une version améliorée du protocole de routage AODV. Ils ont mis en œuvre des Mécanisme de commande à l'aide de simulateur de réseau (NS2). Lorsque le nœud source vérifie le retard de bout en bout, tous les nœuds intermédiaires effectuent le contrôle de la bande passante. L'algorithme est basé sur la modification du RREQ et paquets RREP, l'utilisateur calcule également la Capacité actuelle de la bande passante (CBC) pour un noeud donné qui sera mis en œuvre et incorporée dans l'AODV dans NS2.

- **Résultat de simulation**
  - ✓ **Paquet reçu**

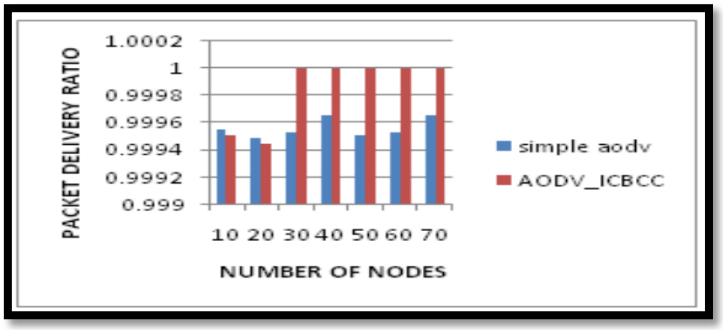


Figure 5.4: Paquet reçu d'AODV et AODV_ICBCC.

  - ✓ **Délais**

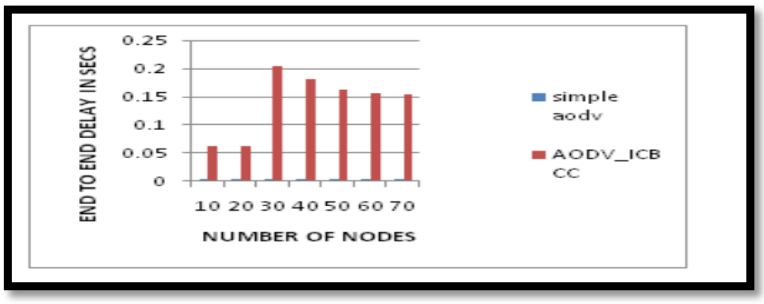


Figure 5.5: Délais d'AODV et AODV_ICBCC.

D'après les résultats de la simulation de son proposition, le protocole ICBCC_AODV donne un très bon rapport de livraison de paquets ainsi améliore les performances de traitement de bande passante de noeud.

2. CONTRIBUTION

Dans MANET, la topologie du réseau est dynamique c'est -à-dire il y a des changements fréquents dans la topologie en raison de défaillances des nœuds et des liens. Le routage dans les réseaux Ad Hoc est confronté à plusieurs problèmes et défis. Le protocole AODV ne tient pas compte le débit des routes sélectionnées. Donc, pour parler d'un protocole de routage fiable il faut résoudre les principaux problèmes pour augmenter les performances d'acheminement des informations entre les nœuds. Le débit de transmission joue un rôle important dans les réseaux Ad Hoc. Le protocole de routage optimal doit ainsi privilégier les routes possédant un débit de transmission élevé. Choisir de telles routes permet une augmentation de débit utile du réseau lors de l'émission d'un paquet. Notre approche consiste à proposer une optimisation pour le protocole de routage AODV.

2.1. Motivation de choix de ce paramètre

La technologie de communication sans fil a rapidement augmenté au cours des dernières décennies. La connectivité sans fil a donné aux utilisateurs la liberté de se déplacer où ils désirent.

De nos jours, le besoin de débit dans les applications ne cesse de croître. En effet, proposant toujours plus de fonctionnalités aux utilisateurs, ce besoin s'avère croissant.

Le domaine d'application des réseaux Ad Hoc s'étend aussi bien à des applications peu consommatrices en débit, Ce débit reste très faible comparé aux débits que peuvent atteindre les réseaux filaires (plusieurs centaines de Gbits/s avec la fibre optique). Pour supporter le plus grand nombre d'applications sur un réseau Ad Hoc, il est nécessaire d'optimiser au maximum le débit.

Dans notre approche nous essayons de proposer comme métrique de recherche d'une nouvelle route, le débit est le Nombre de données qui peuvent être transmises d'un point à un autre en un laps de temps déterminé. Le débit détermine la vitesse de transmission des informations sur un réseau informatique.

Le débit est généralement mesuré en bits par seconde (bit/s ou bps), et parfois dans les données paquets par seconde ou des paquets de données par intervalle de temps.

Il existe des nœuds qui ont un faible débit, ces nœuds se trouvent au milieu de chemin entre la source et la destination quand on utilise la métrique de nombre de sauts le minimum, mais lorsqu'on utilise le débit comme métrique de choix de meilleur route, les nœuds de débit plus important sont plus utilisé dans les routes de transmission.

2.2 L'optimisation d'AODV proposé

Notre principal objectif de ce travail est de proposer un AODV optimisé pour l'amélioration de la performance de ce protocole. L'idée consiste à augmenter le débit dans le réseau en choisissant le chemin avec un débit élevé, si les nœuds ont des grandes débits de données, il peut être avantageux d'éviter les nœuds à faible débit Pour cela, nous avons attribué la notion de «coût» pour le débit de données sans fil. Afin d'effectuer «un routage avec coût minimum" au lieu d' "un routage avec nombre de sauts minimum".

Le protocole de routage AODV, repose sur le mécanisme de découverte de chemins à la demande comme on a le détaillé dans **le chapitre 3.**

Dans notre travail des modifications ont été apportés, pour améliorer le débit du meilleur chemin. On propose l'optimisation suivante:

- Le calcul du coût de chaque interface dans les nœuds de réseau en fonction de débit.
- Périodiquement les nœuds mis a jour leur table de routage par le débit de ses interfaces au lieu de nombre de sauts.

- Modifier la métrique de l'algorithme de découverte de route, par le changement de nombre de sauts avec le cout, ce dernier représente l'inverse de débit, car on veut maximiser le débit.

De ce fait le fonctionnement de processus de découverte de route du protocole AODV devient de la manière suivante:

- la source diffuse le paquet RREQ quand il n'a pas une route pour transmettre des données à une destination.
- L'utilisation d'un champ réservé dans la structure de RREQ, on ajoute la valeur de cout d'un nœud, chaque nœud calcule le cout de l'interface par la formule suivante:

Coût de nœud = 1 / débit de données.

- À Chaque réception du paquet RREQ par un nœud intermédiaire, il calcule le coût et l'ajoute au coût cumulatif pendant le transfert de la demande de route jusqu'à ce qu'il atteigne la destination. La destination choisi la voie qui a le coût le plus minimum.

On a expliqué notre proposition avec les organigrammes suivant :

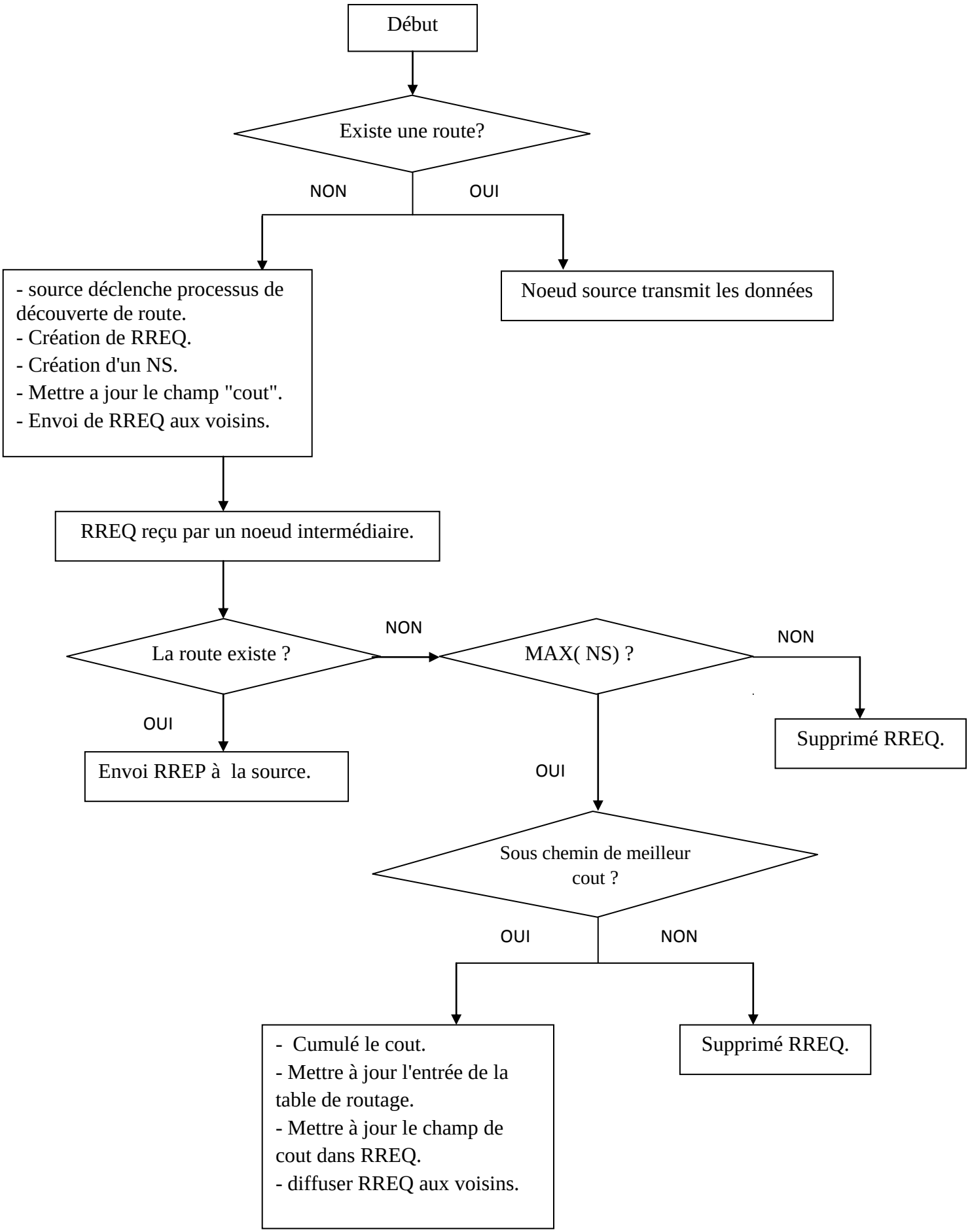


Figure 5.6 : Organigramme de noeud source et de noeud intermédiaire.

Cet organigramme présente le processus de découverte de route quand un noeud source souhaite envoi un message a un autre nœud, et le processus fait lorsque un noeud intermédiaire reçu un RREQ.

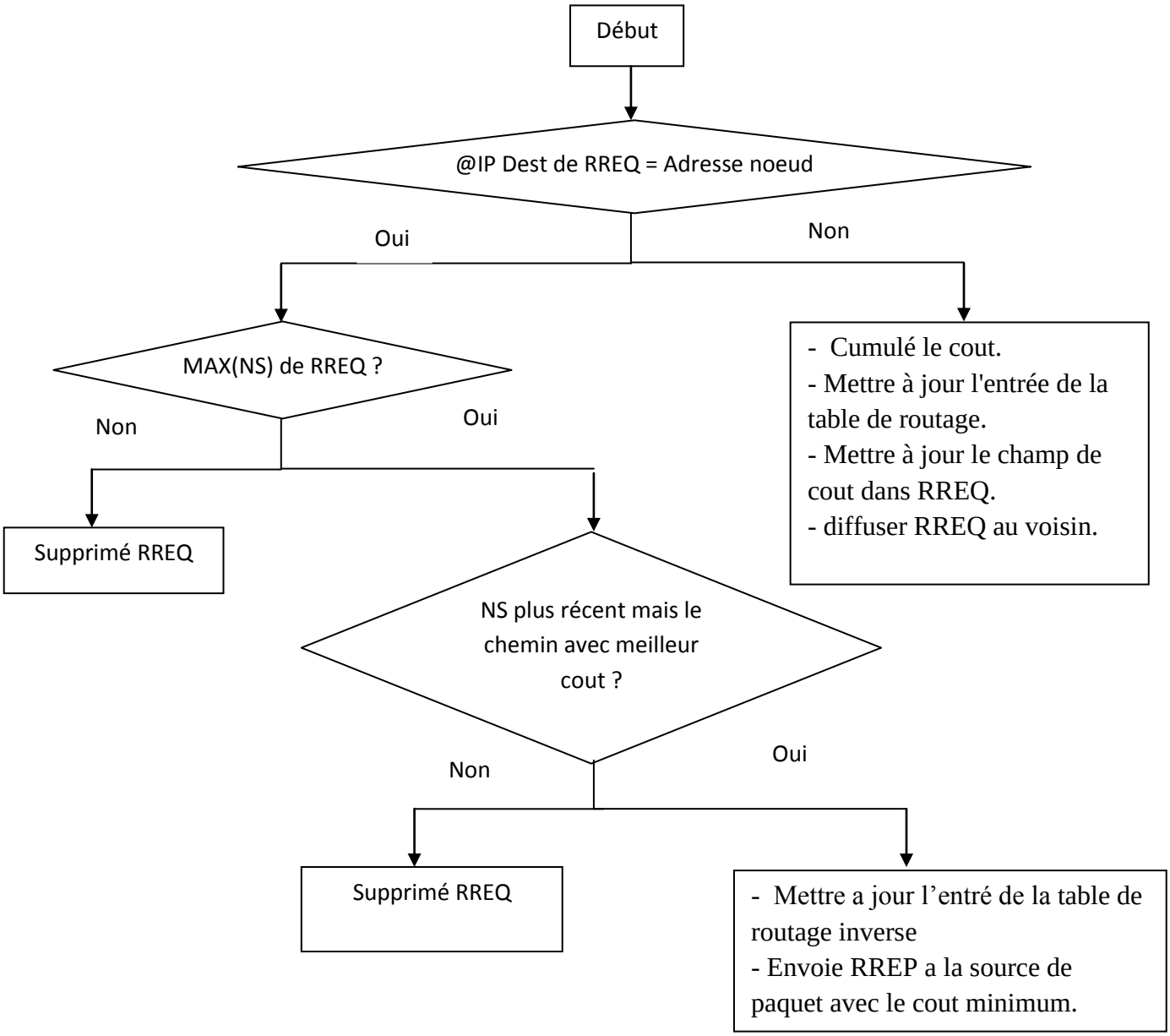


Figure 5.7 : Organigramme de nœud destination.

Cet organigramme présente le processus de découverte de route quand la requête RREQ est reçu par le nœud destination est la renvoyé au nœud source comme RREP.

Apres on fait l'implémentation et la simulation en utilisant le simulateur OPNET MODULER, et on a comparé les performances du protocole AODV VS à celui basant sur le nombre de sauts et discuter les résultats obtenus.

3. REALISATION DE L'OPTIMISATION

3.1 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.

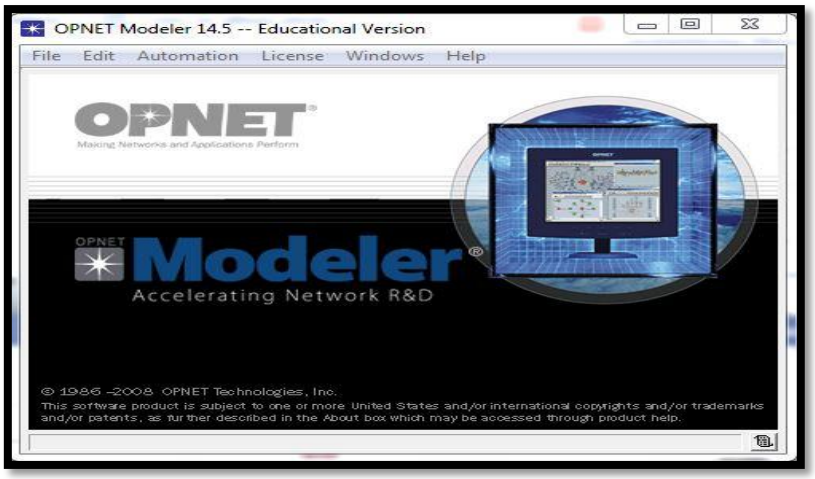


Figure 5.8: Environnement de simulation OPNET.

3.2 Simulation de réseau

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

- **Première étape :** elle consiste à simuler le réseau Ad Hoc comme suit:

ouvrir OPNET => file => new project => initialisation de topologie => insertion des composant (les nœuds mobile, la mobilité…etc).

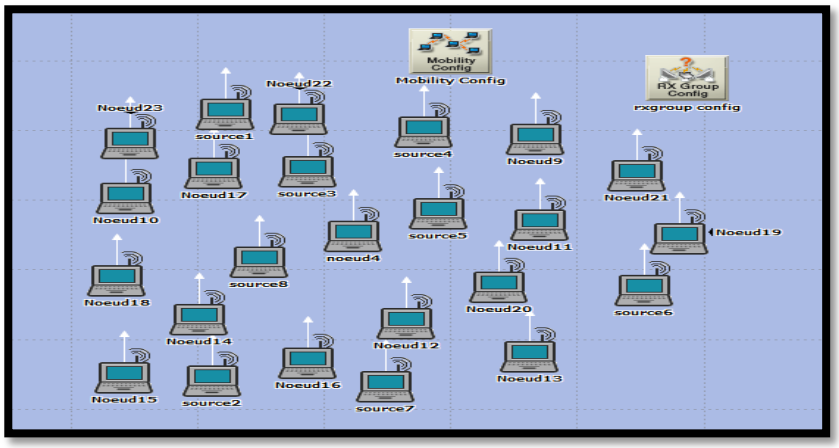


Figure 5.9 : L'envirenement de notre travail.

Cette fenétre montre un réseau avec 24 nœuds mobile et le type de mobilité est aléatoire.

- **Deuxième étape:** après l'insertion des composant en passe à l'étape de configuration de réseau (l'adressage des nœuds,définition des nœuds source…).

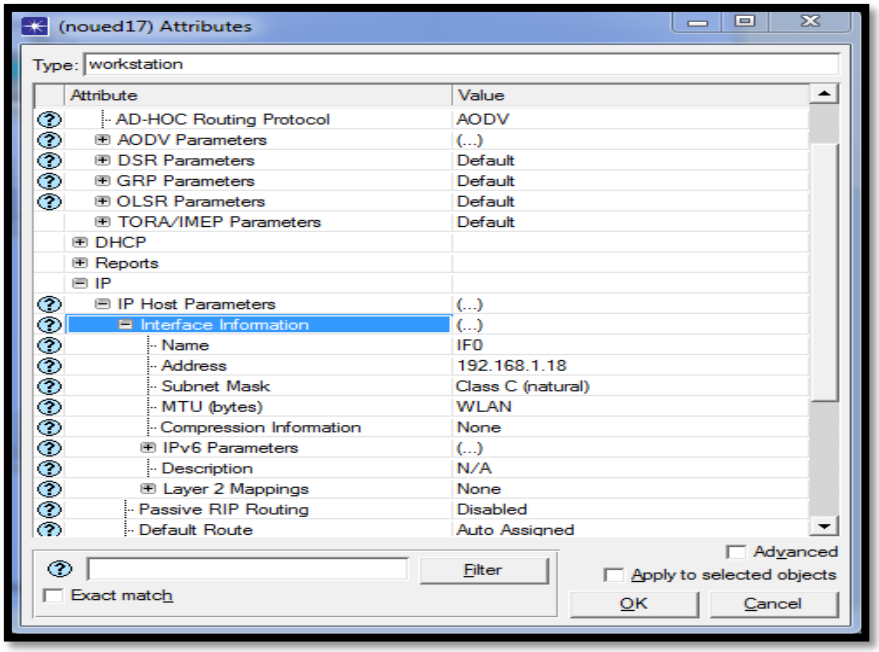


Figure 5.10: définir l'adressage des differentes nœuds.

Cette fenêtre montre la configuration des nœuds par l'adressage à partir de :

« **IP**» => « **IP Host Parameters**» => « **Interface information** » => « **Address** ».

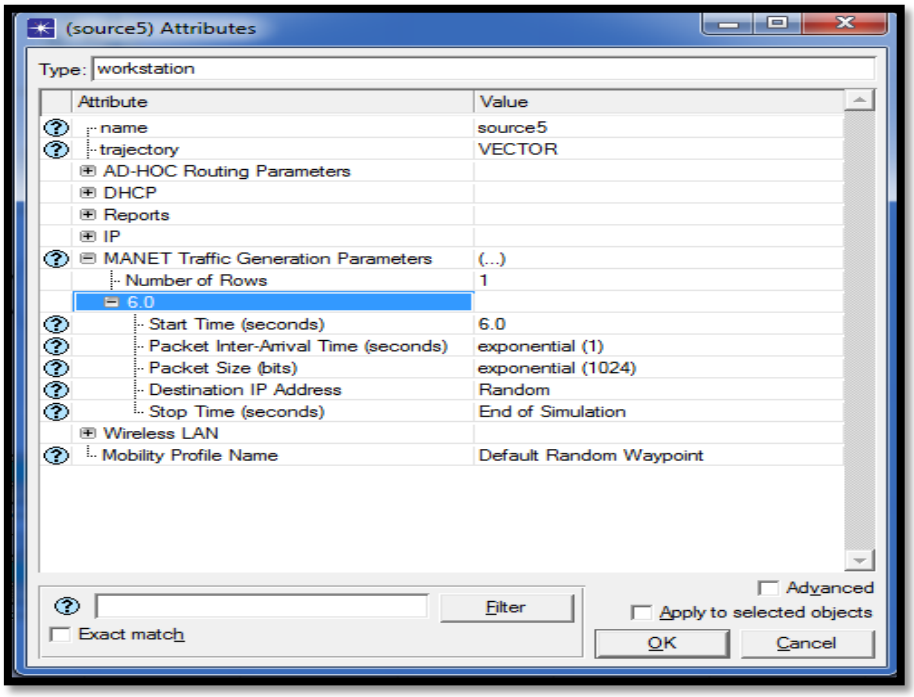


Figure 5.11: paramétrage de la source.

Cette fenêtre montre comment créé une source par la création d'un seul trafic à partir de « **MANET Traffic Generation Parameters** » après 6 seconds.

- **Troisiéme étape :** après la configuration des noeuds de réseau nous avons implimenter notre proposition dans le model process d'AODV fournis par OPNET.

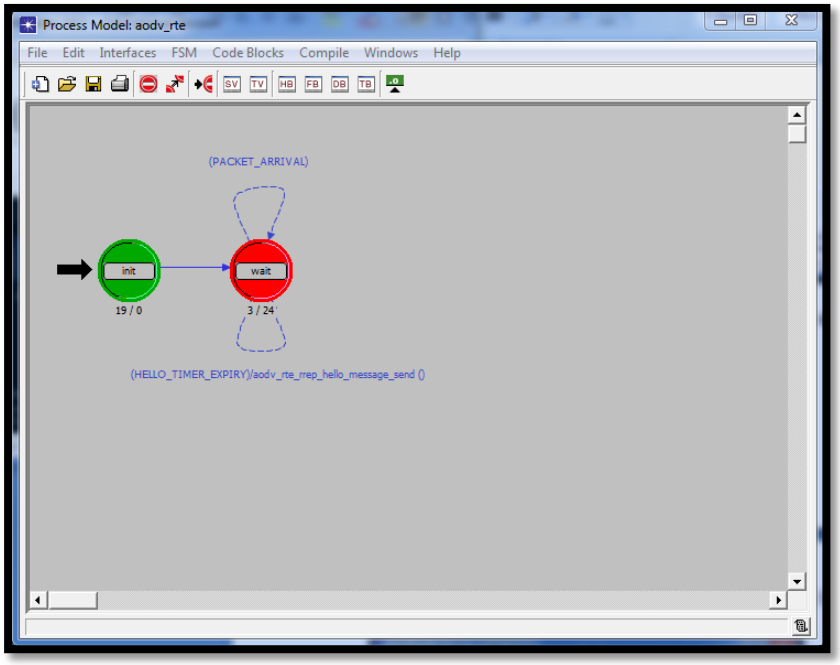


Figure 5.12: modèle process de protocole AODV.

Le code source de protocole AODV est implimenté dans OPNET sous fome d'un modèle process montré dans la figure 5.12.

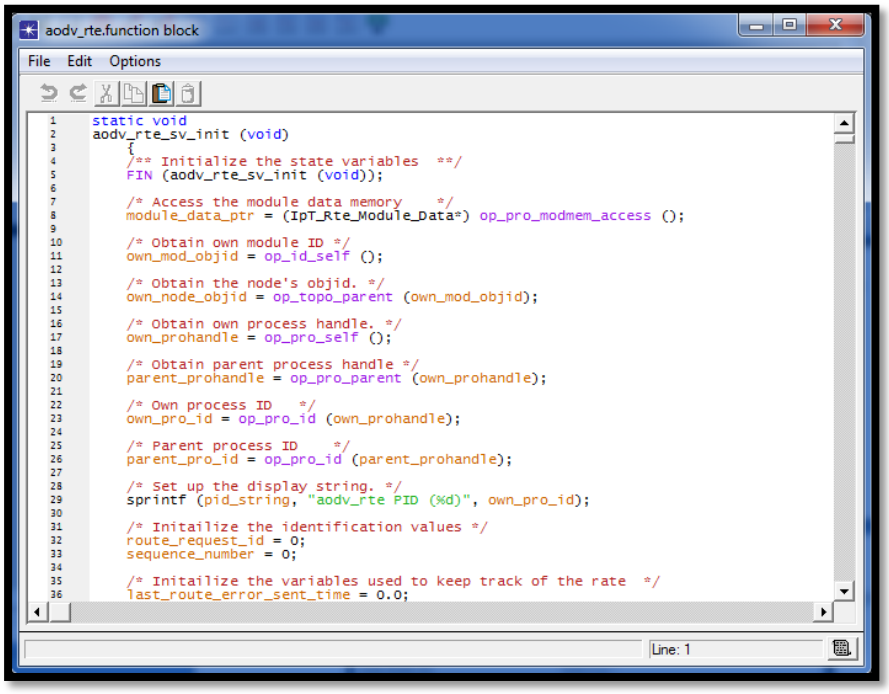


Figure 5.13: le bloque de fonctionnement de protocole AODV.

Cette figure represente le bloque de fonctionement de protocole AODV implimenté par le language C++ .

- **Qutriéme étape**: l'éxecution de la simulation réalisée.

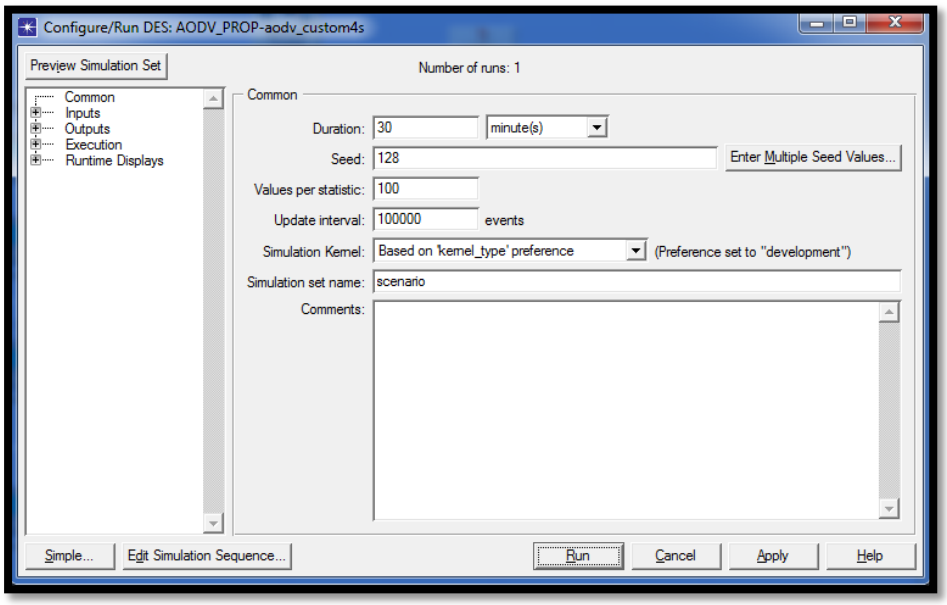


Figure 5.14: paramétre de simulation.

Cette fenétre montre l'execution d'un sénario, en spécifiant la durée a 30 minutes, avec 10000 évenements.

- **cinquiéme étape:** à la fin de la phase d'implémentaion et l'éxécution 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.

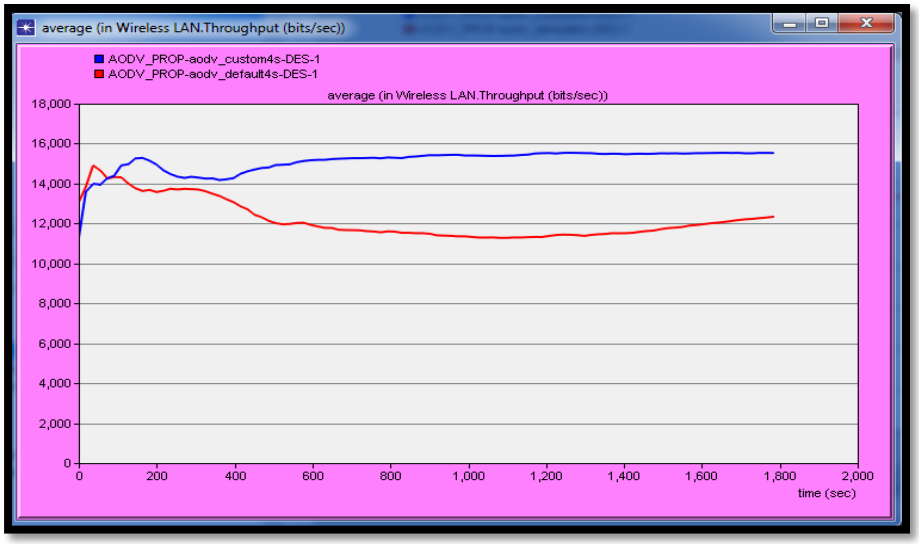


Figure 5.15: résultat de simulation sous forme de graphe.

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.

CONCLUSION

L'objectif principal de ce chapitre de décrire notre contribution qui consiste a proposé un protocole AODV optimisé et détaillé son fonctionnement. Ensuite l'environnement de simulation choisi ainsi les étapes principal de 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

INTRODUCTION

Pour tester les performances d'une solution apportée à un problème de communication dans un réseau, il serait très coûteux de mettre en place un réseau pour tester certains critères. Pour remédier à ce problème, on utilise des simulateurs.

Dans ce projet nous réalisons deux scénarios de simulations :

Dans le premier scénario on teste notre protocole AODV optimisé par l'augmentation successive du trafic dans le réseau avec la fixation de l'autre caractéristique de réseau.

Dans le deuxième scénario on fixe tout les paramètres et les caractérisques de réseau et on change seulement le nombre de nœuds plusieurs fois.

On a évalué notre travail par la définition des paramètres qui ont une relation directe avec le débit comme le nombre de paquet reçu, délai et le débit. On termine par l'analyse des résultats et une conclusion.

1. LES PARAMÈTRES A EVALUÉ

Avant de commencer l'étude et l'analyse de protocole AODV il faut définir les métriques et les critères sur les quelles on va décider que tel ou tel protocole est optimal par rapport à l'autre, soient:

- **Le nombre de paquets reçu:** c'est le nombre total des paquets reçu par tous les nœuds de réseau par unité de temps mesuré en paquets par seconde.
- **Débit:** c'est la quantité de données transmises par unité de temps (débit).
- **Délai:** c'est le temps nécessaire pour transmettre un paquet d'une source vers la destination (le temps de bout en bout) mesuré en seconde.

2. LES SCENARIOS DE SIMULATION

2.1 Premier scénario

Dans le premiére scénario nous avons comparer la perfermance d'AODV par défaut avec l'AODV optimisé, ou chaque fois on change le nombre de source (auguementation de trafic dans le réseau) et on fixe les autres paramétres de simulation comme la surface, temps de simulation et la norme…etc

Paramètres	Valeurs
Nombre de stations	7 nœuds
Simulateur	OPNET
Surface	200x400 m2
Mobilité des stations	Random Mobility
Protocole choisi	AODV
Temps de simulation	30 min
Norme WLAN choisie	802.11g
Longueur du paquet	1024 bits
Débit binaire	54 Mbps
Nombre de source	1, 2,4

Tableau 6.1: Les paramètres choisis pour les simulations.

Les graphes et les résultats obtenus pour le scénario 01

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

Evaluation de trafic reçu (packet/second)

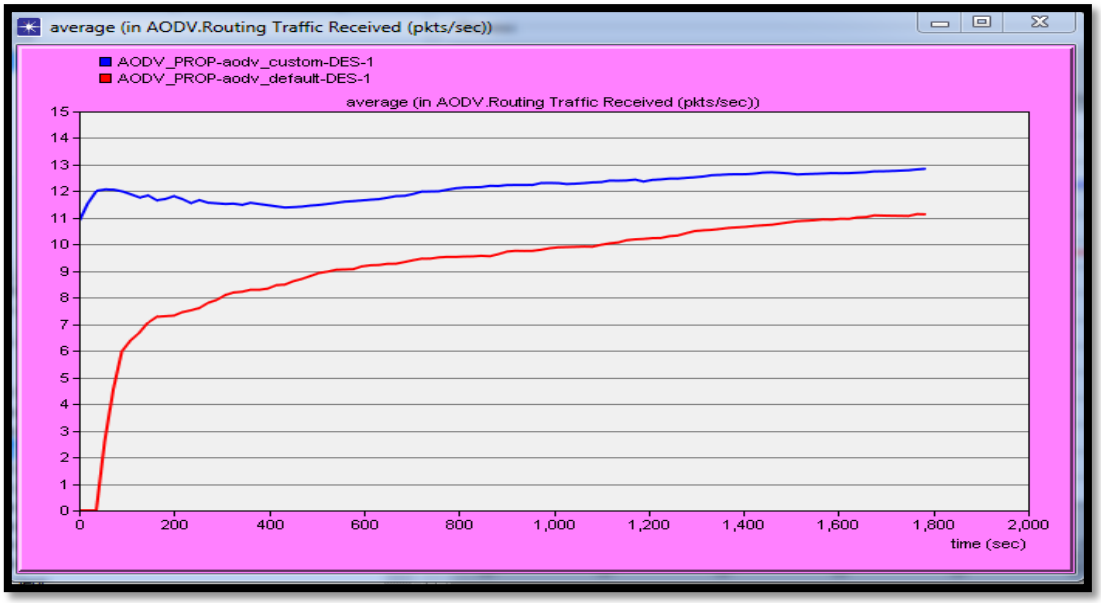


Figure 6.1 : trafic reçu d'AODV vs AODV optimisé avec une seule source.

D'après la figure 6.1 Comme prévu, le graphe de la métrique route **trafic reçu** d'AODV optimisé est plus performant qu'AODV par défaut avec une seule source. La performance d'AODV optimisé égale a 20% par rapport a AODV par défaut.

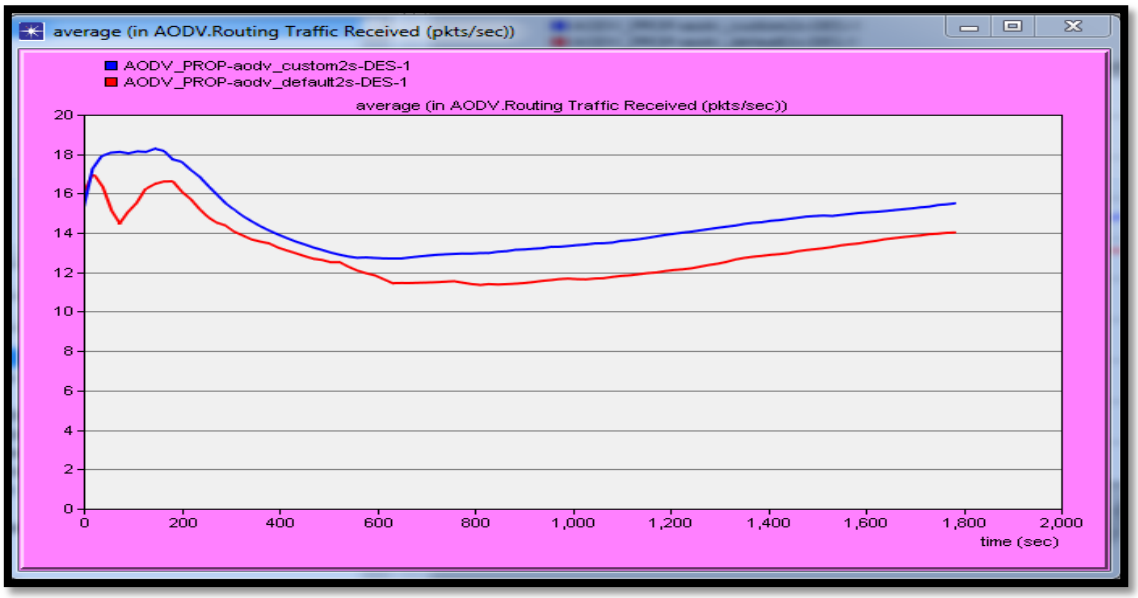


Figure 6.2: trafic reçu d'AODV vs AODV optimisé avec 2 sources.

Cette figure montre que le nombre de paquet reçu d'AODV optimisé est beaucoup mieux par rapport à l'AODV par défaut malgré l'ajout d'une deuxième source.

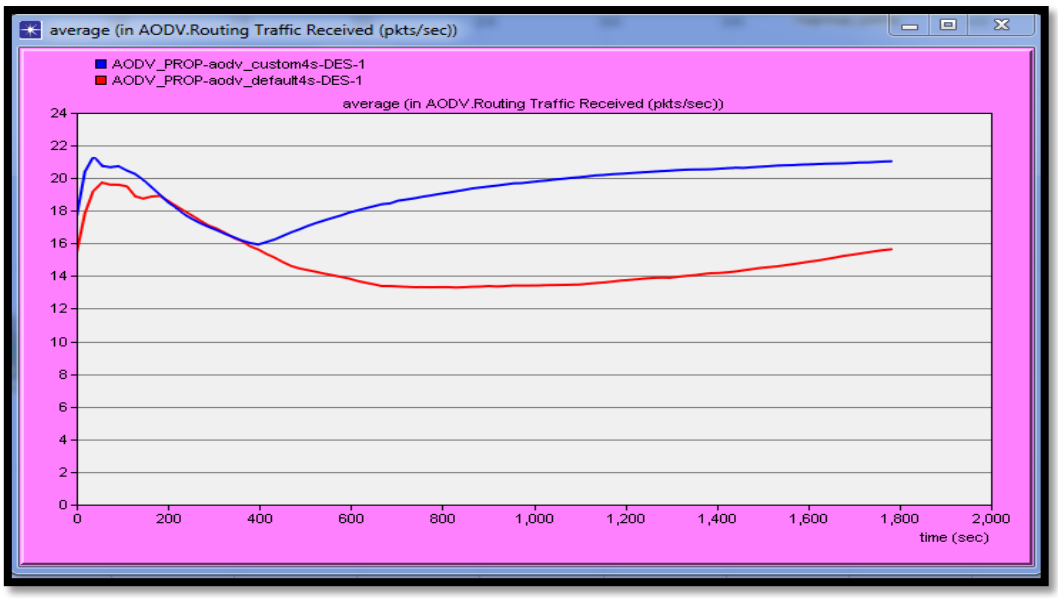


Figure 6.3 : trafic reçu AODV vs AODV optimisé avec 4 sources.

D'après le graphe, pourtant l'augmentation des nombres de source (4 sources) notre protocole reste toujours plus performant que AODV par défaut dans le nombre de paquet reçu pendant toute la période de simulation.

- **Résumé :**

Le trafic reçu dans l'AODV optimisé reste toujours plus performant que le protocole AODV par défaut puisque il choisi le chemin de grand débit par conséquence le nombre de paquet reçu augmente.

Evaluation de Délais (Delay)

Figure 6.4: Délais d'AODV vs AODV optimisé avec une seule source.

D'après ce graphe avec une seule source, ce dernier montre que le délai de bout en bout dans AODV par défaut est plus grand qu'AODV optimisé.

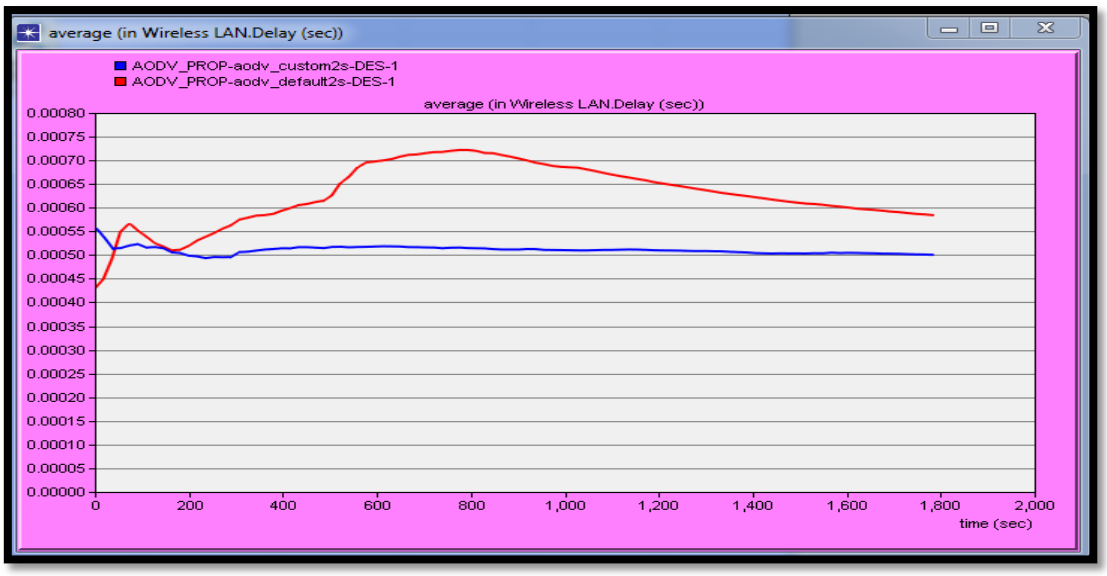


Figure 6.5: Délais d'AODV vs AODV optimisé avec 2 sources.

Avec deux source le délai de AODV par défaut est égale a 0.00060 second et de L'AODV optimisé 0.00050 second .les courbes montre que le délai dans AODV optimisé est mieux que AODV par défaut.

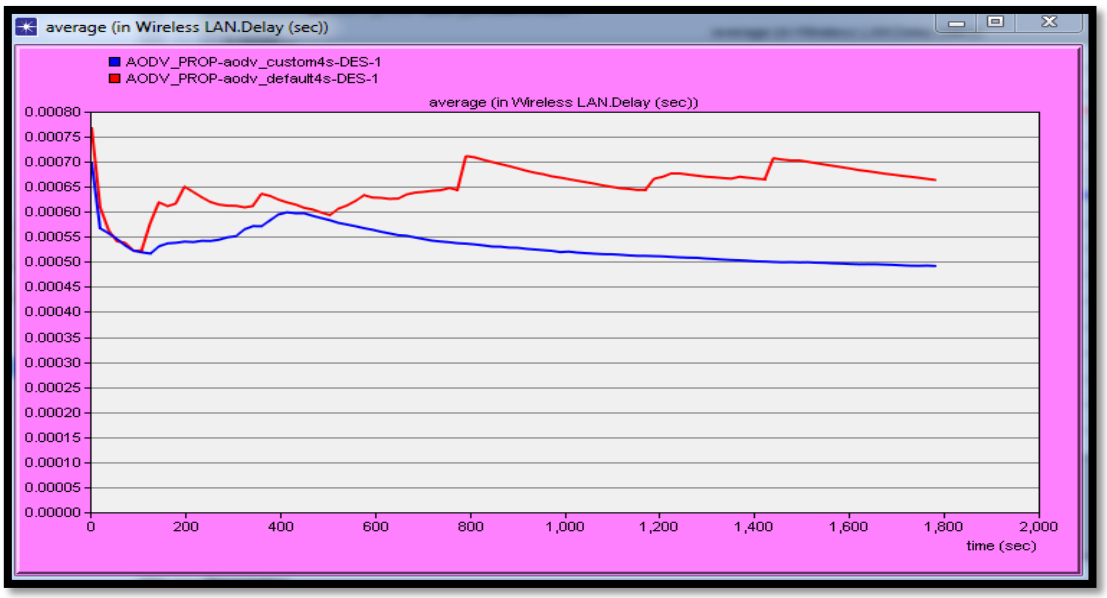


Figure 6.6: Délais d'AODV vs AODV optimisé avec 4 sources.

Dans la figure 6.6 on remarque que le délai de bout en bout dans AODV par défaut est plus qu'AODV optimisé avec 4 sources

- **Résumé :**

Le Délai de transmission des paquets de protocole AODV optimisé a diminué et le délai de protocole AODV par défaut augmenté car ce dernier peut avoir une saturation des nœuds intermédiaire qui sont utilisé dans le processus de découverte de route (dans le fils d'attente).

- **Evaluation de Débit (Throughput)**

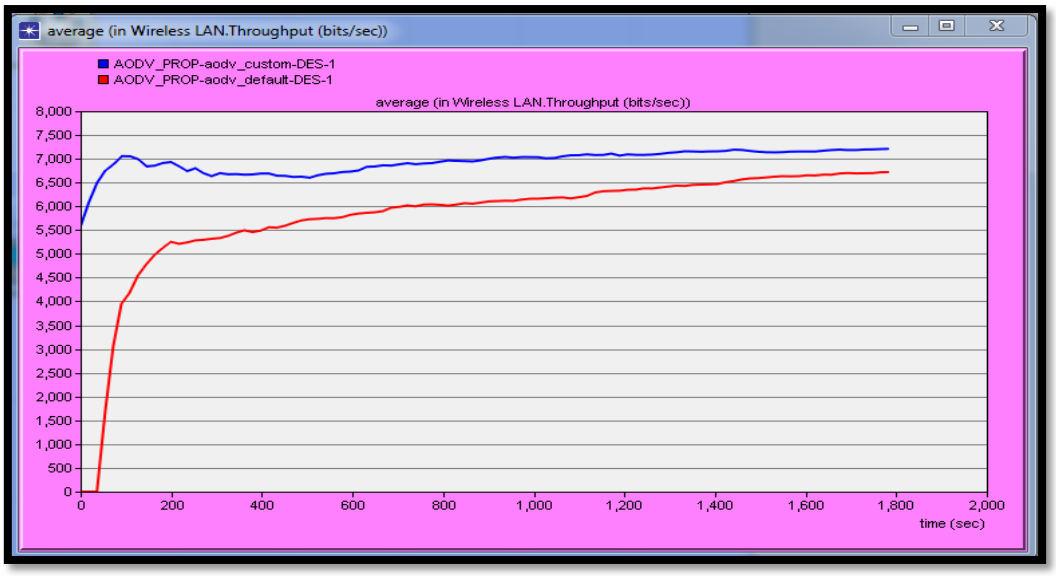


Figure 6.7: Débit AODV vs AODV optimisé avec 1 source.

Dans la figure 6.7 la quantité totale des données qui arrive à la destination de la source (Throughput) est égale à 7500 bits/second pour AODV optimisé, par contre pour l'AODV par défaut le débit est égal à 6500 bits/second. Les courbes montrent que le protocole AODV optimisé donne un débit supérieur à celui de l'AODV par défaut.

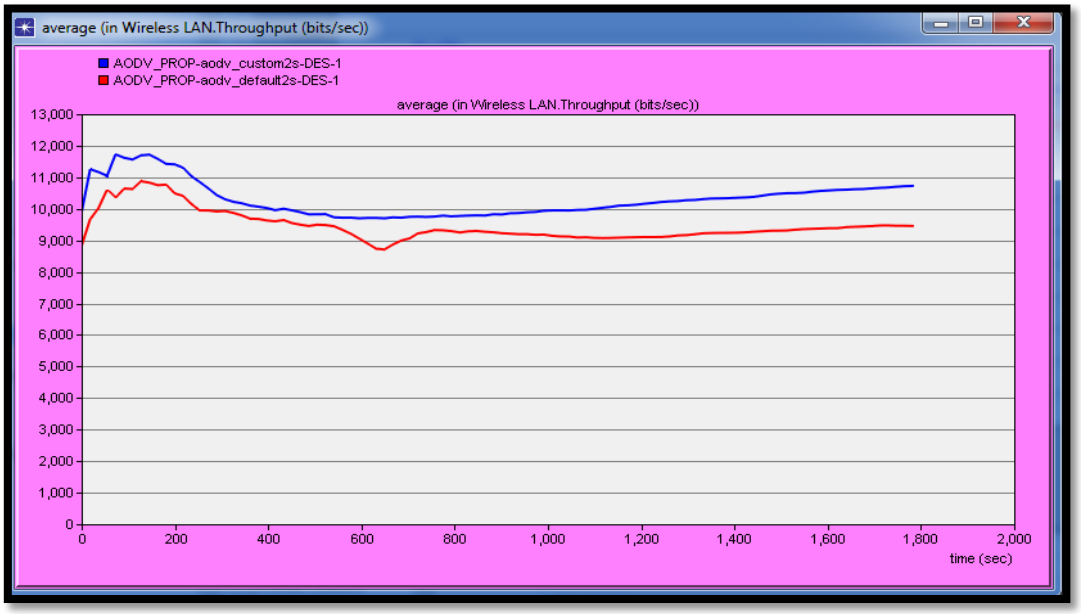


Figure 6.8: Débit AODV vs AODV optimisé avec 2 sources.

Dans la figure 6.8 la quantité des données qui arrive à la destination des 2 sources est égale à 11000 bits/second pour AODV optimisé, mais pour l'AODV par défaut le débit est égal à 9500 bits/second. Les courbes montrent que le protocole AODV optimisé donne un débit supérieur à celui de l'AODV par défaut.

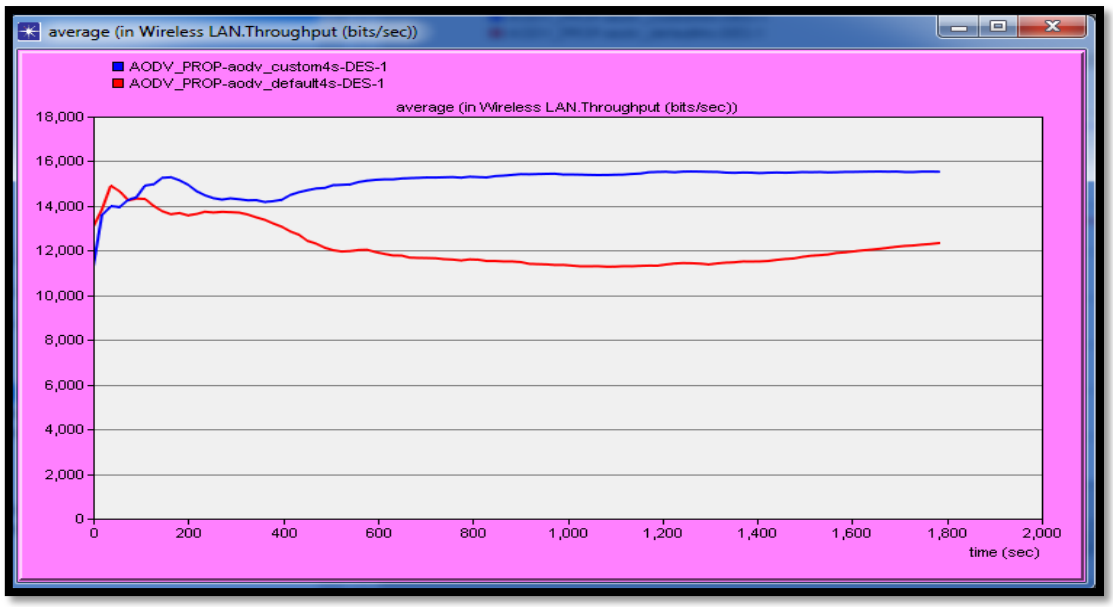


Figure 6.9: Débit AODV vs AODV optimisé avec 4 sources.

Dans cette figure la quantité des données qui arrive à la destination des 4 sources (Throughput) est égale à 16000 bits/second pour AODV optimisé, mais pour l'AODV par défaut le débit est égal à 12000 bits/second.

- **Résumé**

Le débit de réseau est supérieur par rapport a celui de AODV par défaut puisque notre protocole proposé et basé sur le débit.

- **Résumé de scénario 1**

D'après les résultats obtenus dans le premier scenario, en conclut que Le protocole AODV optimisé est plus performant qu'AODV par défaut, puisque malgré l'augmentation dans le nombre de source qui génère un grand trafic sur le réseau. le trafic reçu dans l'AODV optimisé reste toujours plus performant car il choisi le chemin de grand débit par conséquence le nombre de paquet reçu augmente et le délai de transmission des paquets a diminué car se dernier choisis le chemin le plus optimal et l'AODV par défaut peut avoir une saturation des nœuds intermédiaire qui sont utilisé dans le processus de découverte de route (dans le fils d'attente), et le débit de réseau reste toujours supérieur par rapport a celui de AODV par défaut. Puisque notre protocole proposé et basé sur le métrique débit, donc il garanti que la quantité des donné transmis grande que l'AODV par défaut.

2.2 Deuxième scénario

Dans le deuxiéme scénario nous avons évalué AODV par défaut avec AODV optimisé, ou chaque fois on change augmente le nombre des nœuds on gardons le méme poursentage de source et on fixe les autres paramétres de simulation comme la surface, temps de simulation et la norme…etc.

Paramètres	Valeurs
Nombre de stations	8, 16,24
Simulateur	OPNET
Surface	200x400 m2
Mobilité des stations	Random Mobility
Protocole choisi	AODV
Temps de simulation	30 min
Norme WLAN choisie	802.11g
Longueur du paquet	1024 bits
Débit binaire	54 Mbps
Nombre de source	2, 4,8

Tableau 6.2 : Les paramètres choisis pour la simulation.

Les graphes et les résultats obtenus pour le scénario 02

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

Evaluation du Paquet reçu(packet/second)

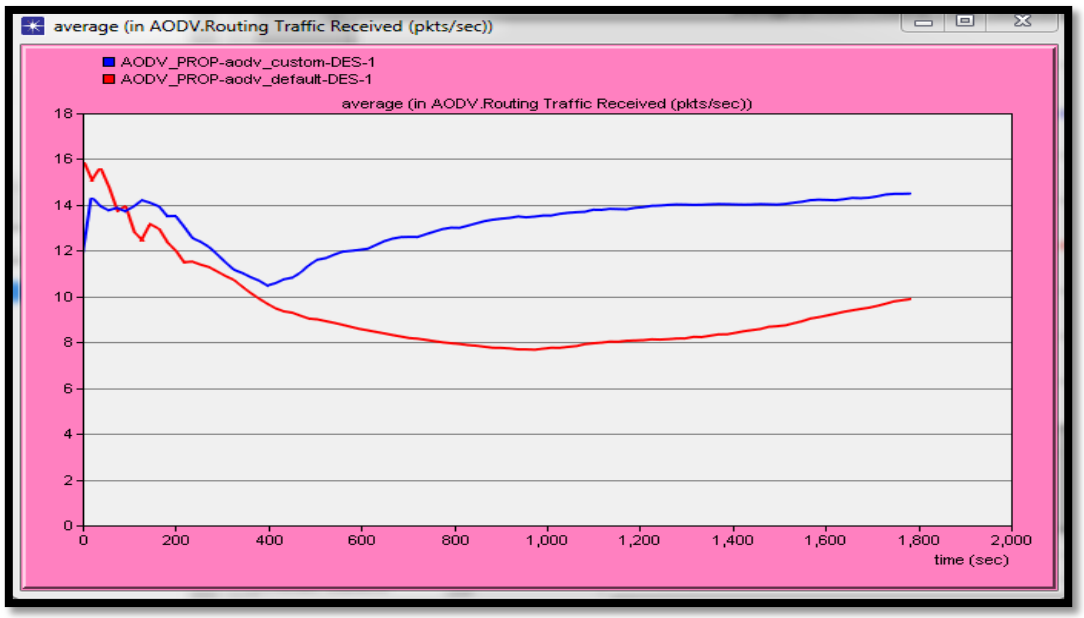


Figure 6.10: trafic reçu AODV vs AODV optimisé avec 8 nœuds.

Le nombre de paquet reçu dans le protocole AODV par défaut est 10 paquets / second et dans le protocole AODV optimisé est 14 paquets / second. D'après le graphe, on observe que les totaux paquets reçu dans AODV optimisé est plus performant qu'AODV par défaut dans le cas de 8 nœuds.

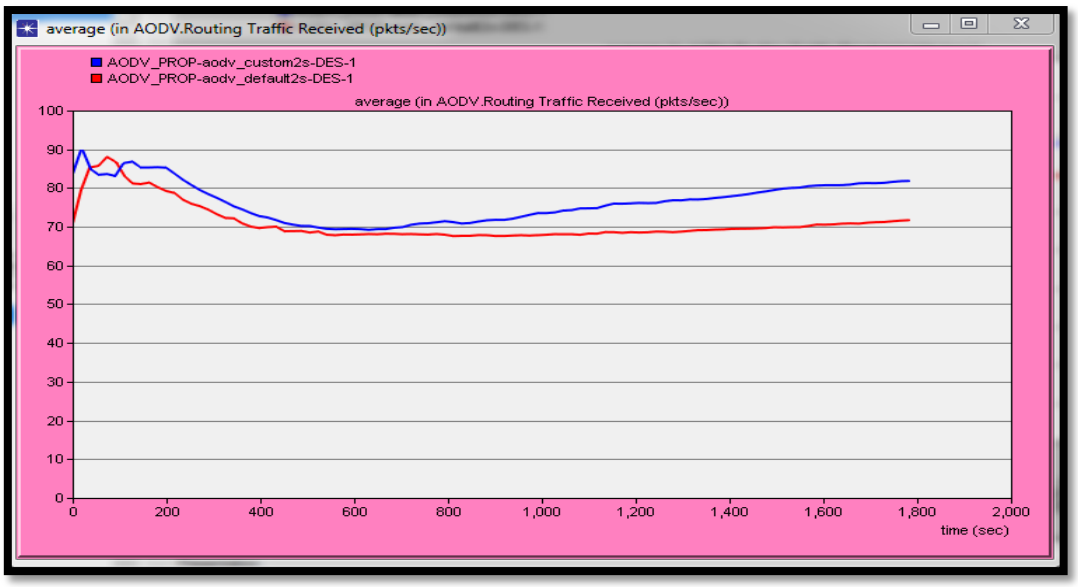


Figure 6.11: trafic reçu AODV vs AODV optimisé avec 16 nœuds.

Le nombre de paquet reçu dans le protocole AODV par défaut est 70 paquets / second et dans le protocole AODV optimisé est 80 paquets / second, on observe que les totaux paquets reçu dans AODV optimisé est plus performant qu'AODV par défaut dans le cas de 16 nœuds.

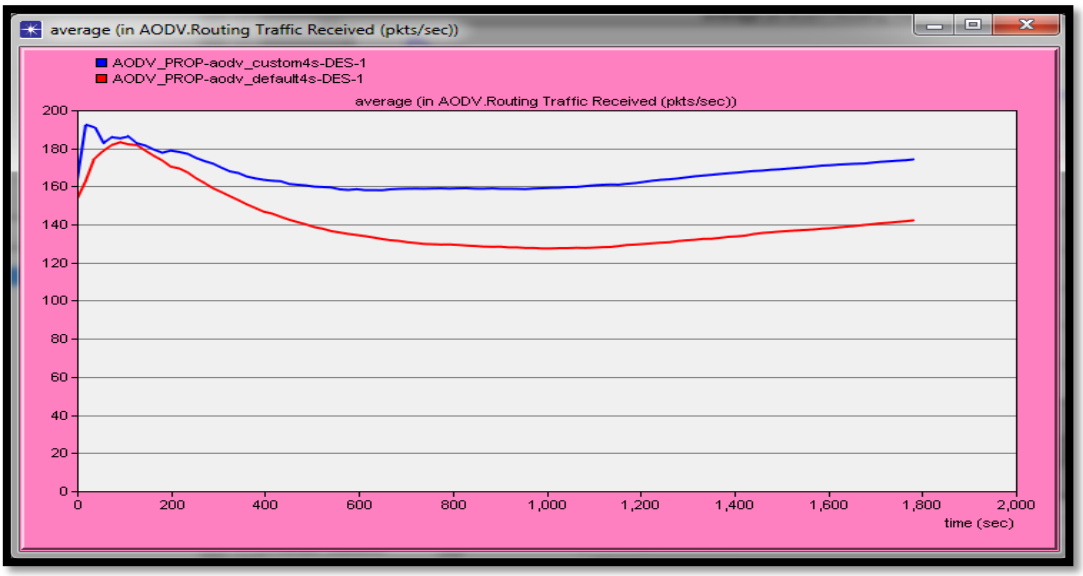


Figure 6.12: trafic reçu AODV vs AODV optimisé avec 24 nœuds.

D'après le graphe on observe que Le nombre de paquet reçu dans le protocole AODV par défaut est 140 paquets / second et dans le protocole AODV optimisé est 175 paquets / second, donc l'AODV optimisé est plus performant qu'AODV par défaut dans le cas de 24 nœuds.

- **Résumé :**

Les graphes montre que le trafic reçu dans l'AODV est plus performant qu'AODV par défaut, parce que il choisi le chemin de grand débit par conséquence le nombre de paquet reçu augmente.

Evaluation de Délai (second)

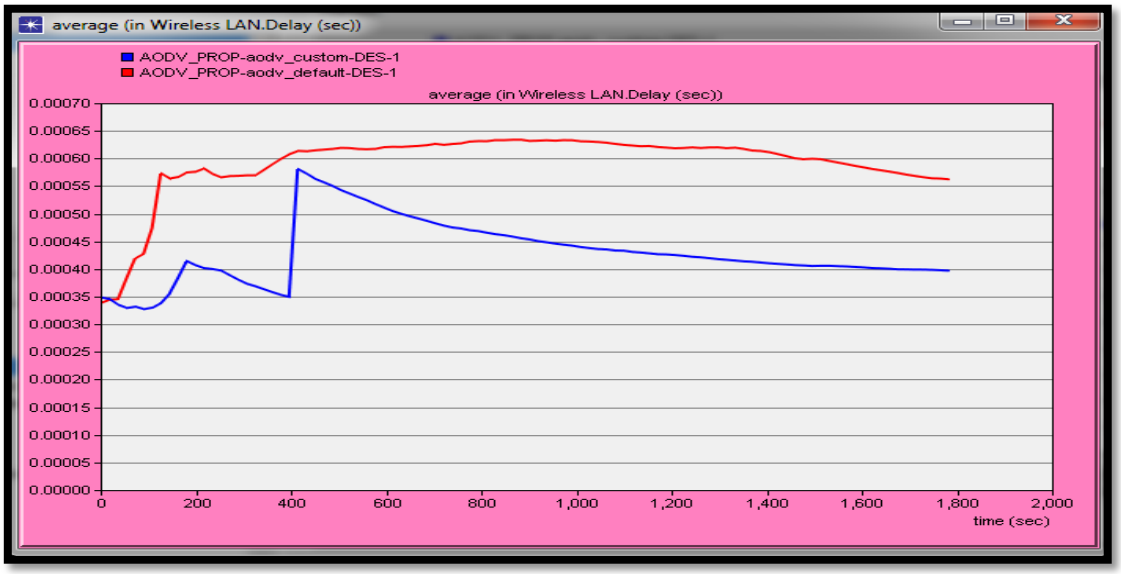


Figure 6.13: délai AODV vs AODV optimisé avec 8 nœuds.

D'après le graphe on observe que le délai dans le protocole AODV par défaut est 0.00055 second et Dans le protocole AODV optimiser est 0.0004 second, donc l'AODV optimisé est plus performant qu'AODV par défaut dans le cas de 8 nœuds.

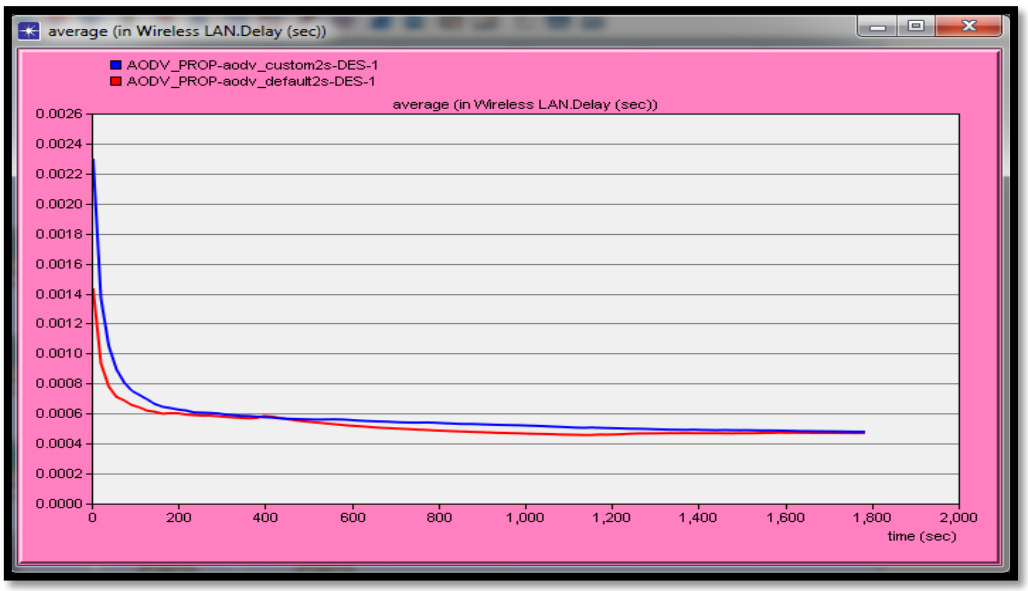


Figure 6.14: délai AODV vs AODV optimisé avec 16 nœuds.

D'après le graphe on remarque que le délai dans notre AODV optimisé n'est pas dégradé.

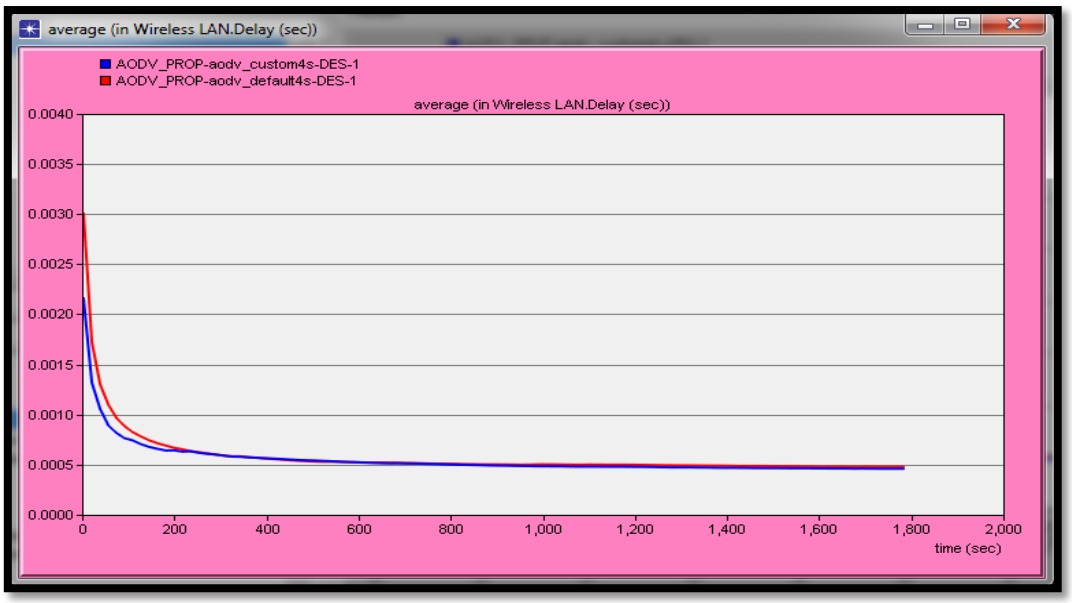


Figure 6.15: délai AODV vs AODV optimisé avec 24 nœuds.

D'après le graphe on remarque que le délai dans notre AODV optimisé n'est pas dégradé et garde les mêmes valeurs.

- **Résumé :**

Dans le cas ou le nombre de nœuds est moins important (8 nœuds) notre AODV optimisé donne un délai plus performant que AODV par défaut. Au fur et à mesure dans l'augmentation de nombre de nœud, les graphes convergent vers les mêmes résultats, mais moins pas de dégradation de performance de cette métrique.

Evaluation du débit (bits/s)

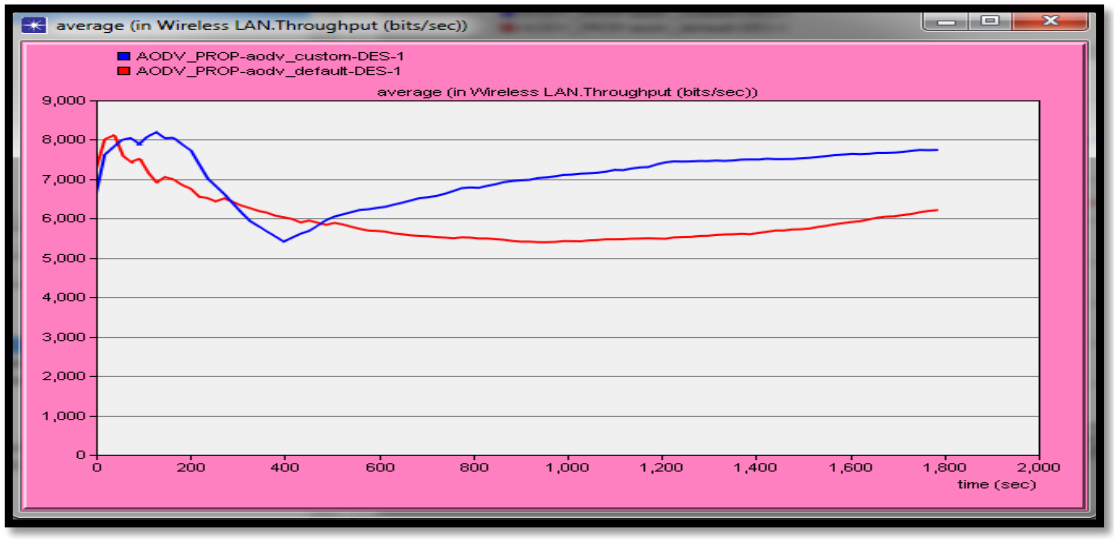


Figure 6.16: débit AODV vs AODV optimisé avec 8 nœuds.

Le résultat de simulation dans la figure montrent que le protocole AODV optimisé et plus performant que l'AODV par défaut dans le cas de 8 nœuds.

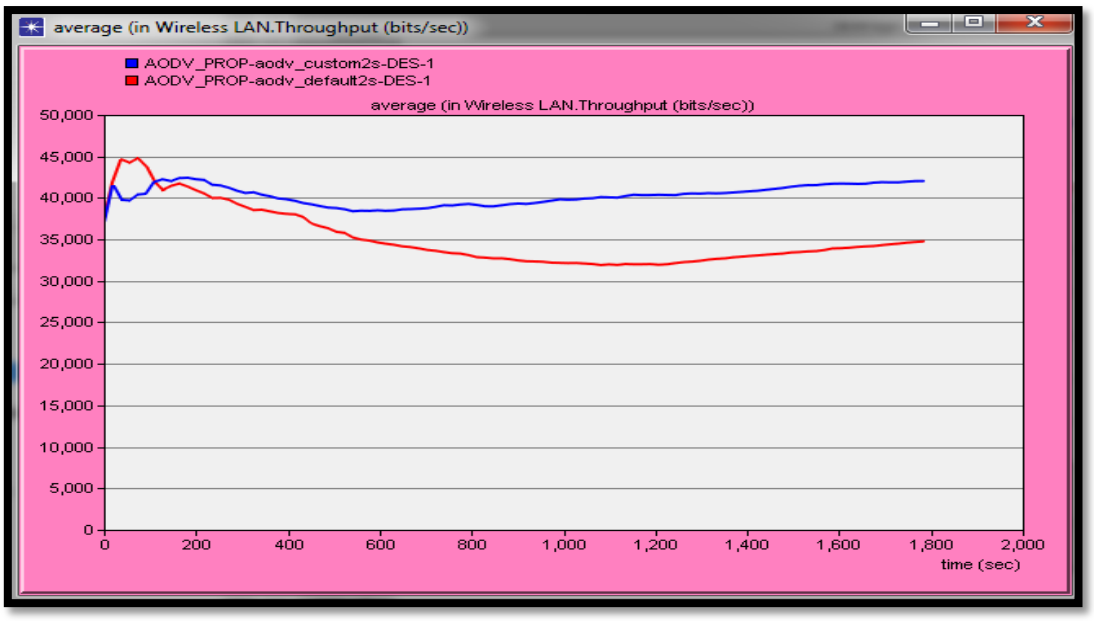


Figure 6.17: débit AODV vs AODV optimisé avec 16 nœuds.

Le résultat de simulation dans la figure montrent que le protocole AODV optimisé et plus performant que l'AODV par défaut malgré le changement de la taille de réseau avec 16 nœuds.

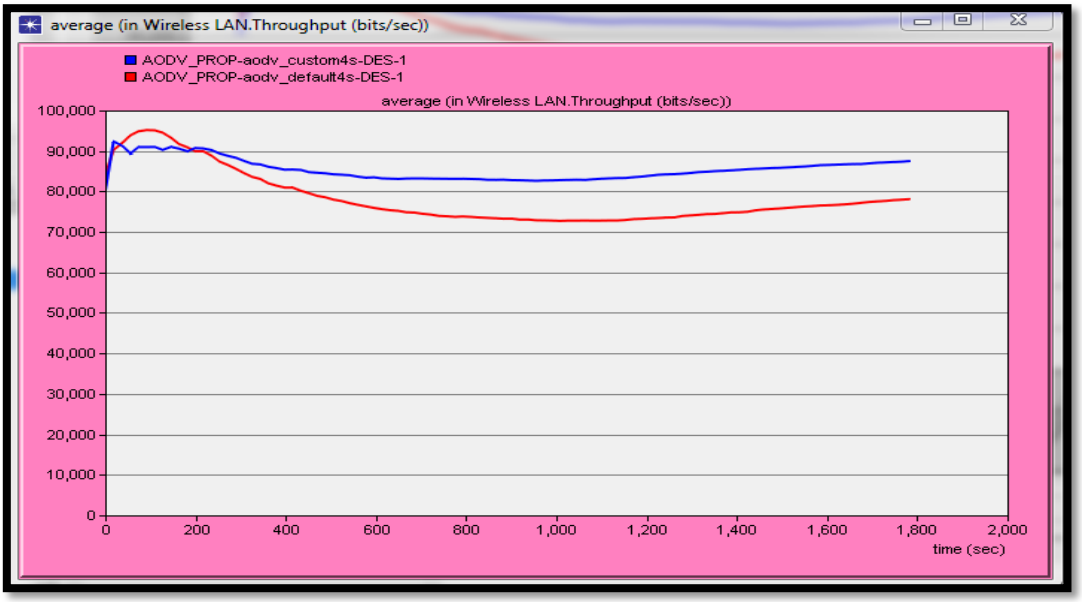


Figure 6.18: débit AODV vs AODV optimisé avec 24 nœuds.

Dans le cas de 24 nœuds les résultats de simulation montrent que le protocole AODV optimisé et plus performant que l'AODV par défaut malgré l'augmentation de la taille de réseau.

- **Résumé:**

  Les résultats montre que le débit dans AODV optimisé est plus performant puisque il est basé sur le métrique « débit » et il choisi le chemin qui a un grande débit.

- **Résumé de scénario 02**

L'augmentation de nombre des nœuds n'influe pas sur les métriques de notre simulateur sauf le délai ou ces valeurs dans le cas ou le nombre de nœud est plus important ce converge vers les mêmes valeurs que AODV par défaut mais ne le dégrade pas.

CONCLUSION

D'après les résultats obtenus dans les deux scenarios de simulation qui ont été faites avec variations des deux situations :

- ✓ Nombre de source.
- ✓ Nombre des nœuds.

En conclut que la performance de la version améliorée du protocole est plus efficace et améliorer qu' AODV par défaut ,puisque malgré l'augmentation dans le nombre de source qui génère un grand trafic sur le réseau et l'augmentation de nombre de nœud (la taille de réseau) , le trafic reçu dans l'AODV optimisé reste toujours plus performant et le délai de transmission des paquets a diminué , et le débit de réseau reste toujours supérieur par rapport a celui de AODV par défaut . Donc le protocole AODV optimisé est plus efficace et plus performant en terme d'assurer un plus important débit de transmission et de l'acheminement des informations par rapport au protocole AODV par défaut. Car le protocole AODV optimisé garantit l'optimalité des routes en terme de débit et de paquet reçu et en terme de minimiser de temps de bout en bout.

CONCLUSION GENERALE ET PERSPECTIVES

Depuis la fin du 20e siècle, le monde a de plus en plus besoin de la mobilité, de l'accès et du partage de l'information. Les réseaux sans fil et les réseaux mobiles sont devenus très populaires ces dernières années. Les réseaux informatiques basés sur la communication sans fil sont classés en des réseaux avec infrastructure et des réseaux sans infrastructure

Les réseaux Ad Hoc permettent aux utilisateurs de communiquer tout en se déplaçant librement. Ces réseaux attirent de plus en plus d'attention grâce leurs avantages.

Le routage présent la fonction essentielle dans le réseau Ad Hoc. Le problème du routage est le défi le plus difficile à réaliser, car il s'agit de trouver une route optimale entre les nœuds.

Ce travail a été principalement axé sur l'optimisation de protocole de routage AODV qui offre des meilleures performances que les autres protocoles de routage MANET.

Nous avons fait des modifications sur le fonctionnement général du protocole AODV qui favorise le débit comme métrique de choix de meilleur chemin. Des modifications ont été apporté sur le processus de création de route par le changement de nombre de sauts avec le cout, ce dernier représente l'inverse de débit, car on veut maximiser le débit et nous avons l'implémenté sous le simulateur de réseau OPNET.

Afin de réaliser notre objectif de ce travail nous avons réalisé les taches suivantes:

- Simulation d'un réseau Ad Hoc sous le simulateur 14.5.
- Modification dans la source d'AODV afin de changer la création des niveaux routes a base de débit au lieu de nombre de sauts.
- Création de premier scénario ou chaque fois en modifiant le nombre de trafic sur le réseau.
- Activation d'AODV par défaut et d'AODV optimisé dans ce scénario.
- Sélection des paramètres d'évaluation pour évaluer la performance.
- Exécution des scénarios de simulation et afficher les résultats a travers des graphes de visualisation des paramètres de performance.
- Analyse et interprétation des résultats.
- Refaire les mêmes étapes dans le deuxième scénario qui concerne le changement de nombre de nœuds.

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…etc.
- Tester l'influence de notre AODV optimisé sur les autres paramètres de performance de réseau.
- Enrichir le calcule de cout avec d'autre métrique au lieu le débit seulement.
- Eventuelle proposition d'intégration de QoS dans notre protocole AODV optimisé.
- Intégration de débit comme métrique de calcule de route dans autre protocole de routage réactif et proactif tel que: OLSR, DSR, DSDV,…etc.

Bibliographie

[1] Samir Athmani ; «Protocole de sécurité pour les réseaux de capteurs sans fil ». Thèse de Magistère ; Université de Hadj Lakhdar-Batna ; Juillet 2010.

[2] Belkheir Khaled et Haned Ahmed ; « Réseaux WiFi Ad Hoc ». Mémoire d'ingéniorat ; Institut de télécommunication d'Oran ; Juin 2008.

[3] Boudjaadar Amina « Plateforme basée Agents pour l'aide à la conception et la simulation des réseaux de capteurs sans fil ». Thèse de Magistère ; Université de Skikda ; 2009/2010.

[4] J.Lanford-Home RF: Bringing Wireless Connectivity home-Intel Home RF technology Tutorial; Avril 1999.

[5] ABOURA Wissam et BENHABIB Imane , Etude et caractérisation de la couche physique du standard IEEE802.16/WIMAX , Octobre 2013
Gsm ref dans chap1

[6] A.Prasina, M.Thangaraja, "Interoperability of Wireless Mesh and Wi –Fi network using FPGA for 4G Solutions", IEEE-International Conference on Recent Trends in Information Technology, Anna University, Chennai, PP_491–496, June 3-5, 2011.

[7] J.Van der Meerschen. Hybridation entre les modes ad-hoc et infrastructure dans les réseaux de type Wi-Fi. Université Libre de Bruxelles. 2006.

[8] Mémoire ROUTAGE DANS LES RESEAUX MOBILES Ad Hoc PAR UNE APPROCHE A BASE D'AGENTS Présenté par : Mr BOUKHECHEM Nadhir Promotion 2007-2008

[9] Van der Meerschen Jerome, « Hybridation entre les modes ad-hoc et infrastructure dans les réseaux de type Wi-Fi », Mémoire de fin d'études, Année 2006, Université Libre de Bruxelles

[10] Melle. Saloua CHETTIBI ; "Protocole de routage avec prise en compte de la consommation d'énergie pour les réseaux mobile Ad Hoc". université Ourgla 2012

[11] Rapport de stage : routage dans les réseaux Ad Hoc minimisant la consommation des batteries laurent Ouakil september 2002

[12] R. Bedouhene et M. Benmedour. ft Protocole de Connexion des Réseaux Ad Hoc à Internet w. Mémoire de fin d'études, université des sciences et de la technologie Houari Boumediene, 2004.

[13] Mme LABRAOUI Nabila, Pour l'obtention du diplôme de DOCTORAT « La sécurité dans les réseaux sans Fil Ad Hoc » Soutenue en 2012 a l'université de Tlemcen faculté des sciences

[14] KHADIDJA AYAD Mémoire MAGISTER Thème "Sécurité du routage dans les réseaux Ad Hoc mobile" Option : Informatique Répartie et Mobile Présenté par : 14 Novembre 2012

[15] T. Lemlouma. Le routage dans les réseaux mobiles Ad Hoc. Mini projet, Université d'Alger USTHB, 2000. (Cité pages 8, 14 et 15.)

[16] B. Tavli, W. Heinzelman; "Mobile Ad Hoc Networks: Energy-Efficient Real-Time Data Communications"; Netherlands, Springer, ISBN-13 978-1-4020-4633-9, 2006.

[17] F. Ducatelle; "Adaptive Routing in Ad Hoc Wireless Multi-hop Networks"; PHD thesis, Università della Svizzera italiana, 2007.

[18] R. Meraihi ; "Gestion de la qualité de service et contrôle de topologie dans les

réseaux Ad Hoc" ; Thèse de doctorat, École nationale supérieure des télécommunications, Paris, 2004.

[19] S. Corson; "Routing protocol performance issues and evaluation Considerations"; ftp://ftp.isi.edu/in-notes/rfc2501.txt, 1999

[20] C.-K. Toh; "Maximum battery life routing to support ubiquitous mobile computing in wireless Ad Hoc networks"; IEEE communications Magazine, June 2001.

[21] David Espès, Protocoles de routage réactifs pour l'optimisation de bande passante et la garantie de délai dans les réseaux Ad Hoc mobiles THÈSE En vue de l'obtention du DOCTORAT DE L'UNIVERSITÉ DE TOULOUSE , Le 27 novembre 2008

[22] C. Cheng, R. Riley, S. Kumar et J.J. Garcia-Luna-Aceves. A Loop-Free Bellman-Ford Routing Protocol without Bouncing Effect. ACM SIGCOMM'89. Sept 1989

[23] G. Malkin. RIP Version 2-Carrying Additional Information. RFC 1388. Internet Engineering Task Force. January 1993

[24] J.CARSIQUE, N.DAUJEARD, A.LALLEMAND, and R.LADJADJ. Le routage dans les réseaux mobiles Ad Hoc. 2003

[25] J. DOYLE. Routing TCP/IP. Certification and Training Series vol. 1. Macmillan, 1998. ISBN : 9781578700417..

[26] D. ORAN. OSI IS-IS Intra-domain Routing Protocol. RFC 1142 (Informational). Internet Engineering Task Force, fév. 1990. URL : http : //www.ietf.org/rfc/rfc1142.txt.

[27] J. MOY. OSPF Version 2. RFC 2328 (Standard). Updated by RFCs 5709, 6549. Internet Engineering Task Force, avr. 1998. URL : http://www. ietf.org/rfc/rfc2328.txt.

[28] M. Abolhasan , T. Wysocki , E. Dutkiewicz; "A review of routing protocols for mobile Ad Hoc networks"; Ad Hoc Networks 2, pp. 1-22, 2004

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

[30] E.W. Dijkstra. A note on two problems in connexion with graphs. Numerische mathematik, 1 (1) : 269–271, 1959.

[31] J-M. Percher and B. Jouga. DÃctection d'intrusions dans les rÃcseaux Ad Hoc. In Proc. of 1er Symposium sur la SÃccuritÃc des Technologies de l'Information et de la Communication (SSTIC'03), juin 2003.

[32] C.E. Perkins and P. Bhagwat. Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers. In Proc. of the conference on Communications architectures, protocols and applications (SIGCOMM'94), pages 244–254. ACM, August 1994.

[33] D.P. Bertsekas, R. Gallager, and T. Nemetz. Data networks. Prentice-hall Englewood Cliffs, NJ, 1987.

[34] Mario Gerla, Guangyu Pei, and Sung-Ju Lee. "Wireless, mobile ad-hoc network routing". Computer Science Departement, University of California, Los Angeles. 1999

[35] D.B. Johnson and D.A. Maltz. Dynamic source routing in Ad Hoc wireless networks. In Thomasz Imielinski and Hank Korth, editors, Mobile Computing, volume 353, chapter 5, pages 153–181. Kluwer Academic Publishers, 1996.

[36] JHM07 D. Johnson, Y. Hu, and D. Maltz. The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4. http ://tools.ietf.org/html/rfc4728, February 2007. RFC4728.
Perkins E et royer M.99]

[37] C.E. Perkins and E.M. Royer. Ad-hoc on-demand distance vector routing. In Proc. 2nd IEEE Workshop on Mobile Computing Systems and Applications, 1999. Proceedings(WMCSA'99), volume 2, pages 90–100. IEEE Computer Society, February 1999

[38] C. Perkins, E. Belding-Royer, and S. Das. Ad Hoc On-Demand Distance Vector (AODV)
Routing. http ://tools.ietf.org/html/rfc3561, July 2003. RFC3561.

[39] M. Abolhasan , T. Wysocki , E. Dutkiewicz; "A review of routing protocols for mobile Ad Hoc networks"; Ad Hoc Networks 2, pp. 1-22, 2004

[40] Z.J. Haas : A new routing protocol for the reconfigurable wireless networks. In IEEE 6th International Conference on Universal Personal Communications Record Conference Record, volume 2, page 562—566, octobre 1997.

[41] Abolhasan M. , Wysocki T. , Dutkiewicz E. 2004] M. Abolhasan , T. Wysocki , E. Dutkiewicz; "A review of routing protocols for mobile Ad Hoc networks"; Ad Hoc Networks 2, pp. 1-22, 2004 .

[42] Laurent Ouakil ,LIP6, routage dans les réseaux Ad Hoc minimisant la consommation des batteries, septembre 2006

[43] C. Perkins, E. Belding-Royer, S.Das: «Ad Hoc On-Demand Distance Vector (AODV)Routing, Network Working Group, July 2003:ftp://ftp.nordu.net/rfc/rfc3561.txt

[44] Meriem BELGAID Saida OUHAB« Routage et qualité de service dans AODV etOLSR » Mémoire 2006-2007 Université A/Mira de Bejaïa.

[45] Meriam Dawoud, « Analyse du protocole AODV » rapport de stage, Université PaulSabatier-I.R.I.T, 2005/2006.http://phdgroup.org/LebaneseUniversityArchive/CSTI/2005-2006/5.pdf.

[46] Daniel MABELE MONDONGA ,Etude sur les protocoles de routage d'un réseau sans fils en mode Ad Hoc et leurs impacts « Cas de protocoles OLSR et AODV » 2009-2010

[47] C.E. Perkins and E.M. Royer. Ad-hoc on-demand distance vector routing. In Proc. 2nd IEEE Workshop on Mobile Computing Systems and Applications, 1999. Proceedings (WMCSA'99), volume 2, pages 90–100. IEEE Computer Society, February 1999

[48] Mohamed Ali Ayachi Contributions à la détection des comportements malhonnêtes dans les réseaux Ad Hoc AODV par analyse de la confiance implicite. Université de Carthage 2011

[49] Vincent Untz. Les r´eseaux sans fil spontan´es pour l'Internet Ambiant. R´eseaux et t´el´ecommunications [cs.NI]. Institut National Polytechnique de Grenoble - INPG, 2007. Fran¸cais.

[50] S. Ranjan Das, C. E. Perkins, and E. M. Royer. Performance Comparison of Two On-demand Routing Protocols for Ad Hoc Networks. In INFOCOM (1), pages 3–12, 2000.

[51] Said K, Zoulikha M, Un protocole de routage ER-AODV à basse consommation d'énergie pour les réseaux mobiles Ad Hoc, Oran,Algérie

[52] QoS Forum. QoS protocols and architectures. White paper of QoS Forum, July 1999.
http ://www.qosforum.com

[53] E. Crawley, R. Nair, B. Rajagopalan, H. Sandick, "A Framework for QoS-based Routingin the Internet", IETF RFC2386

[54] Jean-Pierre CHANET, « Algorithme de routage coopératif à qualité de service pour des réseaux Ad Hoc agri- environnementaux «, Thèse pour obtenir le grade de DOCTEUR D'université Blaise Pascal - Clermont II, 20 avril 2007.

[55] Leila TOUMI : « Algorithmes et mécanismes pour la qualité de service dans les réseauxhétérogènes » Thèse de doctorat Institut National Polytechnique de Grenoble, décembre 2002

[56] [E. Crawley,R. Nair,B.Rajagopalan, andH. Sandick .,« A Framework for QoS-basedRouting in the Internet», IETF RFC 2386, Aug. 1998.ftp://ftp.nordu.net/rfc/rfc2386.txt.]

[57] C. Zhu and M. Scott Corson. QoS routing for mobile Ad Hoc networks. In IEEE Infocom 2002, New York, NY, USA, June 2002.

[58] R. Shirey. Internet security glossary, version 2. http ://tools.ietf.org/html/rfc4949, August 2007.

[59] Y.C. Hu, A. Perrig, and D.B. Johnson. Rushing attacks and defense in wireless Ad Hoc network routing protocols. In Proc. of the 2nd ACM workshop on Wireless security,page 40. ACM, 2003.

[60] THÈSE En vue de l'obtention du DOCTORAT DE L'UNIVERSITÉ DE TOULOUSE Délivré par L'INSTITUT NATIONAL POLYTECHNIQUE DE TOULOUSE Discipline ou spécialité : Réseaux et Télécommunications Présentée et soutenue par Sakuna CHAROENPANYASAK Le 23/06/2008

[61] Alain Berro ; Optimisation Multiobjectif et Stratégie d'évolution en environnement Dynamique (thèse de Doctorat) ; 18 Décembre 2001 ; Université des sciences sociales ToulouseI ; page 14, 27, 29.

[62] Leila Imane NIAR Soutenue en ..JUILLET 2012,Mémoire Magister : Informatique,option : Analyse, Commande et Surveillance des SystemesThème:Analyse Graphique pour la surveillance dans unréseau de capteurs sans fils (RCSF)Simulateur : OMNET++

[63] H. Luo, F. Ye, J. Cheng, S. Lu, and L. Zhang. TTDD : Two-tier data dissemination in largescalewireless sensor networks. ACM Journal of Mobile Networks and Applications (MONET),Special Issue on ACM MOBICOM (2003), 2003

[64] G. Fleury, P. Lacomme, and A. Tanguy. Simulation à événements discrets, chapter 1, page pp. 6. 2006

[65] k.BABOURI , L.KHELASSI , k. DJEBROUNI et M.BESSES ,Les simulateurs réseaux Technologie réseau ,L3-GTR 2013/2014

[66] Pierre-jean Erard pontien déguénon ouvrage simulation par evenement discrtes 1996

[67] C. LOUATI, S. ELHOUSSAINI, I.WANN et A. HAZAOUD , simulateur interactif de la qualité de service dans un routeur 2013/214

[68] BABOURI Karima, KHELLASI Linda, DJEBROUNI Karima, BESSES Malika. (2013). Les simulateurs réseaux (Technologie réseau). Université des

Sciences et de la Technologie Houari Boumediene USTHB. 2013. 19 pages.

[69] Fabrice Valois, « Introduction à la simulation de réseaux Où il sera question de modélisation, de simulation et de l'usage d'OPNET Modeler », dernière m-a-j : le 27/09/2006.

[70] Reinforce Networking Theory with OPNET Simulation Jinhua Guo, Weidong Xiang, and Shengquan Wang University of Michigan-Dearborn, MI, USA 2007

[71] SAADANE HOUDA ,La qualité de service d'un streaming vidéo Dans un réseau Ad Hoc (égale à égal),2012

[72] Cheikh Sarr, Claude Chaudet, Guillaume Chelius, and Isabelle Guérin Lassous: Bandwidth Estimation for IEEE 802.11-Based Ad Hoc Networks. IEEE transaction on mobile computing, vol. 7, No. 10, october 2008, pp 1228-1241.

[73] POONAM N GHOLAP & RINKU SHAH : MODIFIED AODV WITH CURRENT BANDWIDTH CALCULATION FOR MOBILE Ad Hoc NETWORKS ,Department of Computer, VIT, Mumbai University, Mumbai, Maharashtra, India, Apr 2014

[74] Tooska Dargahi, Amir Masoud Rahmani, Ahmad Khademzadeh, ―SP-AODV: A Semi-Proactive AODV Routing Protocol for Wireless Networks power‖, International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume-1, Issue-2, pp.109-112, July2012.

[75] Sujata Wasudeorao Wankhade, P. R. Deshmukh, ―Comparison of AODV and RAODV Routing Protocols in Mobile Ad Hoc Networks, International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 1, pp.374-377, January 2013.

[76] [P.Parvathi, ―Comparative Analysis of CBRP, AODV, DSDV Routing Protocols in mobile Ad-hoc Networks‖, International Conference on Computing, Communication and applications (ICCCA), pp. 1 – 4, 2012]

[77] Li Yuanzhou, Hu Weihua, ―Optimization Strategy for Mobile Ad Hoc Network Based on AODV Routing Protocol‖, 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM), 2010 , pp-1-4, Sept. 2010

[78] Hemant Kumar Garg, P.C.Gupta, ―Minimization of Average Delay, Routing Load and Packet Loss Rate in AODV Routing Protocol‖,International Journal of Computer Applications, Volume 44, pp.14-17, April 2012.

[79] Performance Analysis of Optimize AODV and AODV Routing Protocol Amrapali Arya , B.P. Chaurasia , S.K. Gupta September 2015

[80] http://file.scirp.org/Html/5-7800164_34631.htm Journal of Information Security Vol. 4 No. 3 (2013) , Article ID: 34631 , 15 pages, date 22/05/2016.