République Algérienne Démocratique et Populaire.

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique.

Université A. MIRA – Bejaïa.

Faculté des Sciences Exactes.

Département d'Informatique.

Mémoire de fin d'étude

Pour l'obtention du diplôme de MASTER
En : Informatique.

***Option** : Administration et sécurité des réseaux*

Thème

Etude de performances de protocole de routage dans les réseaux Ad hoc

Réalisé par :

- *FARHI LOUIZA.*
- *NAIT IGHIL Atika.*

Encadré et suivi par :

- *M^me^ SABRI Salima* (MCB)

***Examiné par** :*

- *M^me^ GASMI Badrina (MAA)*

Président :

- *M^me^ GHANEM Souhila (MAA)*

Année universitaire : 2019-2020

Remerciements

Nous remercions Dieu le tout puissant et Miséricordieux de nous avoir donné le courage, la patience et la volonté pour réaliser ce modeste travail.

Nos remerciements vont à notre encadreur M. SABRI Salima d'avoir accepté d'être notre encadreur durant cette année de master, pour la préciosité de ses conseils, son infinie disponibilité et ses orientations qui ont constitués un mémoire considérable grâce auquel ce travail a pu être mené à bon port.

Nous remercions tous nos enseignants de la faculté sciences exactes surtout ceux de département informatique

Nous tenons à remercier chacun des membres de jury pour avoir accepté d'examiner notre travail et de l'enrichir par leurs propositions.

Nous remercions tous les étudiants de notre promotion

Ainsi qu'à tous ce et celles qui ont contribué de près ou de loin à la préparation et l'accomplissement de ce mémoire

Pour conclure merci vivement a toute nos familles qui nous 'a toujours supporté moralement et financièrement pendant toutes notre longues années d'étude.

Dédicace

A ceux que j'aime surtout aux plus chères personnes du monde, mama et papa à qui je dois mon éducation et ma réussite

Mes sœurs : Yasmine, Cylia, et Dadou, mon frère Fares

A toute ma grande famille : mes grands-mères, grands-pères, oncles, tantes, cousins et cousines

A mon binôme et ma meilleure amie : Louiza

A toutes mes chères amies : Kenza, Sabrina, Amel, Kahina, Liza, Nacera, Thinhinane, Roza, … etc.

Et a tous mes amis : Nadir, Moussa, Oussama, Omar, Chikh Toufik, Chikh Baker.

Nait ighil Atika

Dédicace

Je dédie ce modeste travail

A mes très chers parent

Mon très cher père pour sa patience et tous ses efforts

A ma mère pour m'avoir épaulé, encouragé à reprendre les études et motivé dans les moments les plus difficiles

A mes grandes soeurs : Thinhinane et Thileli pour tous leurs encouragements

A mes petites soeurs : Thiziri et Ines

A mes grands-parents : Malek et Zahra

A mes oncles : Hakim, Cherif, Abed EL Ghani, Brahim

A mes tentes: Sakina, Liala.

A mes cousines : Mélina, Maya.

A mes cousins : Hocine, Massi, Amine, Ahmed.

Mon beau-frère : Lamine

A mes amis : Louans , Kamel ,Mohamed, Chikh Baker ,Oussama, Chikh Toufik

A mon binôme et ma meilleure amie : Atika

A mes copines: Kenza, Sabrina, Amel, Samira, Chafika, Dihiya , Wissam,Silia, kahina.

Farhi Louiza

Table de matières

Liste des Figues

Liste des tableaux

Liste des abréviations

Anonyme	Description
AODV	Ah-doc on demand ditance vector
AOMDV	Ah-doc on demand multipath ditance vector
AOMDV-SB	Ah-doc on demand multipath ditance vector-stable balancing
BLR	Boucle locale radio
CBRP	Cluster based routing protocol
CEDAR	Core extraction destrubited ah-doc routing
DSR	Dynamic Source Routing
DSDV	Destination Sequenced Distance Vector.
DARPA	Defense Advanced Research Projects Agency.
GSM	Global System for Mobile
GPRS	General Packet Radio Service.
GPS	Global Positionning System
HomeRF	Home Radio Frequency
HSR	Hierarchical State Routing
MANET	Mobile Ad-Hoc Network.
MAN	Metropolitan Area Network.
NS-2	Network Simulator version2
LAN	Local area network.
LBAR	Load Balenced Ad Hoc routing.
OPNET	Optimized Network Engineering Tools.
OLSR	Optimized Link State Routing
OTCL	Object Oriented Tool
QOS	Quality of service.
RERR	Route Error
RCSF	Réseau de Capteurs Sans Fil
RREQ	Route Request
RREP	Route Reply
PAN	personnel area network
PDR	Packet Delivery Ratio
SB	Stations de base

TTL	Time-To-Live
UMTS	Universal Mobile Telecommunication System.
VHR	Virtual Home Region.
WAN	Wide Area Network.
WiFi	Wireless Fidelity
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network.
WRP	Wireless Routing Protocol
WPAN	Wireless Personal Area Network.
WWAN	Wireless Wide Area Network
ZRP	Zone Routing Protocol

Introduction générale

Depuis l'apparition des réseaux informatiques, ce domaine a connu une évolution sans cesse notamment sur le plan physique et artistique. Dans nos jours, le besoin à plus de mobilité et à pouvoir partager ou échanger de l'information à tout moment, en utilisant des dispositifs mobiles (téléphones portables, PC portables) a rendu très répandu la notion de réseau sans infrastructure, ou réseaux Ad Hoc. Ces technologies sont en plein développement du fait de la flexibilité de leur interface, permettent aux utilisateurs de connecter facilement et simplement dans un large éventail de dispositifs informatiques et de télécommunications, sans avoir besoin d'acheter, de transporter ou de connecter des câbles ou de place dans son entreprise.

Différentes catégories des réseaux sans fil existent suivant leur étendue (WPAN, WLAN, WMAN, WWAN). Les réseaux locaux filaires ou câblés (LAN) ont très bien réussi dans les dernières années ; et maintenant à l'aide des technologies de connectivité sans fil, les réseaux locaux sans fil (WLAN) ont commencé à émerger comme étant plus puissants et présentant une alternative flexible des réseaux câblés.

Jusqu'à un passé très récent, la vitesse du réseau local sans fil a été limitée à deux mégabits par seconde (2 Mbps), mais avec l'introduction de nouvelles normes, nous constatons que les réseaux locaux sans fil peuvent supporter jusqu'à une centaine de Mbps en milieux industriel, scientifique et médical.

De nos jours, l'utilisation de la technologie sans fil a envahi le marché des réseaux de télécommunication. Plusieurs standards ont vu le jour, on peut citer à titre d'exemple: WiFi (IEEE 802.11), Bluetooth (IEEE 802.15.1), Zigbee (IEEE 802.15.4). Ces standards équipent une large gamme d'équipements mobiles et aussi sont concurrentes dans certains aspects et sont complémentaires dans d'autres cas. Ce progrès technologique fait que les réseaux de télécommunication sans fil sont actuellement un des domaines de recherche de l'informatique les plus actifs.

On distingue deux grandes familles de réseaux sans fil: les réseaux avec infrastructure et les réseaux sans infrastructure ou Ad Hoc. Les réseaux mobiles avec infrastructure sont basés sur un ensemble de sites fixes appelés stations de base, ces sites vont relier les différents nœuds mobiles pour former un réseau interconnecté. L'inconvénient de ce type de réseau c'est qu'il requière le déploiement d'une importante infrastructure fixe. Cette approche est utilisée dans les réseaux sans fil traditionnels comme les réseaux GSM, et les réseaux locaux sans fil. Par conséquent, les communications dans les réseaux mobiles s'effectuent en absence de toute infrastructure de

communication fixe préexistante. Ces réseaux sont plus connus sous le nom de réseaux Ad Hoc mobiles ou MANETS (Mobile Area NETWORKS).

Un réseau Ad Hoc (MANET) est une collection d'entités mobiles interconnectées par une technologie sans fil formant un réseau temporaire sans l'aide de toute administration centralisée ou de support fixe. Comme la portée des nœuds est relativement limitée, le déploiement d'un réseau à grande échelle nécessite que le réseau soit multi-sauts, c'est à dire que des nœuds intermédiaires jouent le rôle de relais. Avec l'état imprévisible des liens et les changements continus de la topologie, les réseaux sans fil soulèvent de nombreuses questions notamment concernant le routage.

Plusieurs protocoles de routage pour les réseaux Ad Hoc ont été développés. Chaque protocole essaie de maximiser les performances du réseau en minimisant le délai de livraison des paquets, l'utilisation de la bande passante et la consommation d'énergie. Le but principal d'une telle stratégie est l'établissement de routes qui soient correctes et efficaces entre une paire quelconque d'unités de communication, ce qui assure l'échange des messages d'une manière continue. Les algorithmes de routage pour les réseaux Ad Hoc peuvent se classer ce qui ont basés sur l'état des liens et ceux, basés sur le vecteur de distance, ces méthodes exigent une mise à jour périodique des données de routage qui doivent être diffusées par les différents nœuds de routage du réseau. 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 AOMDV (Ad Hoc On-Demand Multipath Distance Vector routing).

AOMDV 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 par 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, AOMDV existe depuis longtemps.

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'AOMDV orignal, ces derniers jours le meilleur chemin pour les applications est basé sur l'équilibrage de charge et garantir les qualités de service.

On peut reformuler notre problématique par les sous problématique suivantes:

- Comment intégrer la métrique d'équilibrage de charge dans ce protocole et garantir quelque qualité de service ?
- Comment choisir l'outil et l'environnement de réalisation de cette optimisation ?
- Comment évaluer la performance du réseau par notre modification ?
- Comment comparer pour évaluer la performance ?
- Comment interpréter les résultats obtenus ?

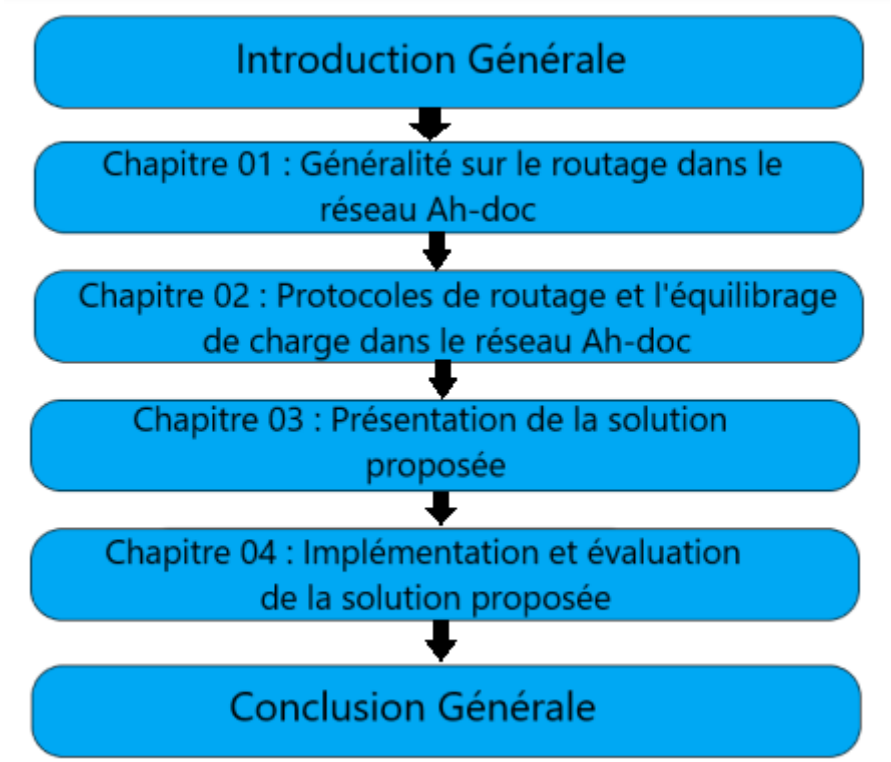
Objectifs

Notre objectif est de modifier ou d'effectuer une extension d'un protocole existant afin de prendre en compte la stabilité des liens et d'améliorer la fonction de routage en terme de la technique ≪ load balancing ≫ équilibrage de charge.

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

- Conception et réalisation d'un protocole AOMDV-SB proposé, où on fait des modifications dans le fonctionnement de protocole AOMDV, cela pour garantir l'équilibrage de charge dans le réseau et la stabilité des liens.
- Création et simulation de notre protocole AOMDV-SB proposé par NS2.
- Evaluation des performances de notre protocole proposé à travers deux scénarios où on change le nombre des nœuds dans chaque scénario.
- Génération du graphe de statistique concernant les métriques en relation avec pourcentage de livraison de paquets, surcharge de routage, charge de routage normalisée.
- Comparaison des résultats de simulation de protocole réactif AOMDV par défaut et le protocole AOMDV-SB proposé.
- Analyse des résultats obtenus.

Ce mémoire est structuré en 4 chapitres comme suit:



Le premier chapitre, présente les différents concepts liés aux réseaux sans fil et réseaux mobiles Ad Hoc, en mettant la lumière sur ses caractéristiques et ses spécificités et les domaines d'application.

Le deuxième chapitre, explique la notion de routage et présente à ce niveau une classification des différentes approches pour le routage dans ce type de réseaux et les métriques de qualité de service plus l'équilibrage de charge.

Le troisième chapitre, présente les protocoles de routage AOMDV et LBAR, en donnant une description détaillée de ces protocoles et leurs principes de fonctionnements et les catégories de solutions existantes de routage avec qualité de service (*QoS*). Et l'explication de notre proposition pour l'amélioration de la stabilité des itinéraires dans les réseaux Ad-Hoc et l'ajout de la fonction du cout de protocole LBAR. Nous décrirons les extensions faites au protocole *AOMDV Standard* ainsi que la méthode d'estimation de la stabilité des itinéraires.

Le quatrième chapitre, présente les différents types des simulateurs, et l'environnement de notre travail NS2, nous allons présenter les résultats de simulation et une comparaison entre les deux versions du protocole: AOMDV et AOMDV-SB proposé. Enfin, nous terminons le mémoire par une conclusion générale et perspective.

Chapitre 01 : Généralité sur le routage dans les réseaux Ad hoc

1.1 Introduction

Les réseaux informatiques en général ont été créés pour permettre aux utilisateur de garder la connectivité réseau des périphériques et a l'échange des informations, puis avec le temps ces réseaux ont été développés pour obtenir des réseaux sans fil, des réseaux numériques qui connectent différents postes ou systèmes entre eux par ondes radio.

Tout au long de ce chapitre, notre intérêt se portera sur les réseaux sans fils et leurs catégories en s'intéressant aux réseaux ah doc.

1.2 Réseaux sans fils

1.2.1 Définition

Un réseau sans fil est un réseau qui permet de connecter différents nœuds sans l'aide d'une connexion physique mais qui établit la communication par des ondes infrarouges ou des ondes radios. La transmission et la réception des données ont besoin de dispositifs agissant comme des ports. Les réseaux sans fil permettent de relier des ordinateurs et d'autres appareils informatiques sans avoir à installer de câblage, ce qui représente plus de confort et fait économiser de l'argent au niveau des infrastructures. **[1]**

1.2.2 Catégories des réseaux sans fils

On distingue plusieurs catégories de réseaux sans fil, selon des caractéristiques spécifiées comme le périmètre géographique, la topologie, etc.…

1.2.2.1 Selon la zone de couverture

Selon ce paramètre géographique qui veut dire la zone de couverture, on peut classer les réseaux sans fils en 4 catégories :

La figure suivante montre les technologies des réseaux sans fil avec des exemples :

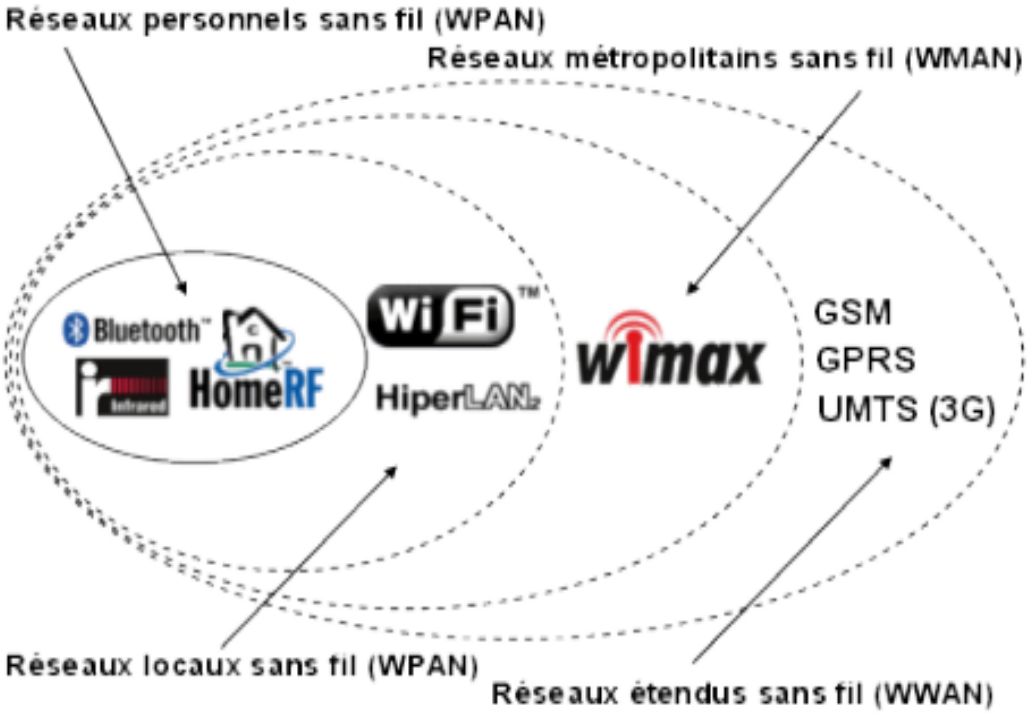


Figure 1.1 : Les technologies des réseaux sans fils. **[17]**

- **WPAN (Wireless Personal Area Network)**

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 utilisés pour relier des équipements informatiques entre eux sans liaison filaire : par exemple : relier une imprimante ou un ordinateur de bureau ou faire communiquer deux machines très peu distantes **[2]**. Il existe plusieurs technologies permettant la mise en œuvre de tels réseaux qui sont :

a. HomeRF

HomeRF (pour Home Radio Frequency), lancée en 1998 par le HomeRFWorking Group (formé notamment par les constructeurs Compaq, HP, Intel, Siemens, Motorola et Microsoft) propose un débit théorique de 10 Mbps avec une portée d'environ 50 à 100 mètres sans amplificateur. **[3]**

b. ZigBee

ZigBee permet d'obtenir des liaisons sans fil à très bas prix et avec une très faible consommation d'énergie, ce qui la rend particulièrement adaptée pour être directement intégrée dans de petits appareils électroniques, elle est opérant sur la bande de fréquences des 2,4GHz et sur 16 canaux, permet d'obtenir des débits pouvant atteindre 250 Kb/s avec une portée maximale de 100 mètres environ. **[4][3]**

c. Liaisons Infrarouge

Les liaisons infrarouges permettent de créer des liaisons sans fil de quelques mètres avec des débits pouvant monter à quelques mégabits par seconde. Cette technologie est largement utilisée pour la domotique (télécommandes) mais souffre toutefois des perturbations dues aux interférences lumineuses. **[4]**

- **WLAN (Wireless Local Area Network)**

Le réseau local sans fil WLAN, est un réseau permettant de couvrir l'équivalent d'un réseau local d'entreprise, à la portée d'une centaine de mètres. Il permet de relier entre tous les terminaux qui existent dans la zone de couverture. Il existe plusieurs technologies concurrentes. **[5]**

a. IEEE 802.11, WiFi (Wireless Fidelity)

IEEE 802.11est un standard de réseau sans fil local proposé par l'organisme de standardisation Américain IEEE.

Elle décrit les couches physique et MAC d'interfaces réseau radio et infra-rouge. Les débits possibles varient entre 1 et 54 Mbit/s suivant les techniques et les éventuelles extensions de la norme employée. Les portées prévues varient entre quelques dizaines et quelques centaines de mètres en fonction de la vitesse choisie et de l'environnement. **[5]**

b. HiperLAN 1

High Performance Local Area Network type 1 (HiperLan 1) est un standard de l'European Technical Standard Institute (ETSI). Il décrit le fonctionnement d'´équipements travaillant dans la bande des 5.15-5.30 GHz et permettant d'atteindre des débits de 23.5 Mbit/s sur une distance d'environ 50 mètres. L'architecture est totalement décentralisée. Il n'y a pas de notion de point d'accès mais les nœuds HiperLAN 1 peuvent cependant avoir des rôles de passerelles. **[5]**

c. HiperLAN 2

L'organisation générale d'HiperLAN type 2 est présentée sur la figure 1.2 On remarque en premier lieu que la norme prévoit la compatibilité avec diverses technologies (TCP/IP bien sûr, mais aussi ATM, UMTS et l'IEEE 1394 connue aussi sous le nom de Firewire). HiperLAN type 2 est très différent dans son architecture d'HiperLAN type 1. Contrairement au type 1, le type 2 est basé sur une centralisation poussée. Les points d'accès sont d'ailleurs indifféremment appelés Access Points (AP) ou Central Contrôler (CC). Les points d'accès sont reliés entre eux par une infrastructure réseau filaire ou non-filaire (qui doit simplement disposer d'une interface adéquate dans

HyperLAN 2, comme celles de la liste donnée précédemment). Les mobiles s'attachent ensuite à ces points d'accès pour accéder aux ressources du réseau. **[5]**

La figure ci-dessus présent l'organisation générale d'Hyperplan type 2

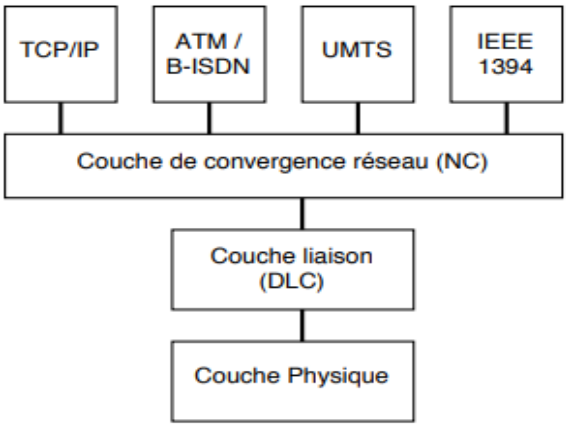


Figure 1.2 : L'organisation générale d'Hyperplan type 2. **[5]**

- **WMAN (Wireless Metroplitan Area Network)**

Le réseau métropolitain sans fil WMAN, est connu sous le nom de Boucle Locale Radio (BLR). Les WMAN sont basés sur la norme IEEE 802.16. La boucle locale radio offre un débit utile de 1 à 10 Mbit/s pour une portée de 4 à 10 kilomètres. **[5]**

- **WWAN (Wireless Wide Area Network)**

Le réseau étendu sans fil WWAN, connu sous le nom de réseau cellulaire mobile. Il s'agit des réseaux sans fil les plus répandus puisque tous les téléphones mobiles sont connectés à un réseau étendu sans fil. Les principales technologies sont les suivantes :

• GSM (Global System for Mobile Communication ou en français Groupe Spécial Mobile),

• GPRS (General Packet Radio Service),

• UMTS (Universal Mobile Telecommunication System).**[5]**

1.2.2.2 Selon infrastructure

- **Réseau cellulaire**

Ce type de réseaux se compose de deux type de sites, les "sites fixes" du réseau filaire et les "sites mobiles" pour les réseaux sans fils.

Certains sites fixes, appelés stations de base (SB) sont munis d'une interface de communication sans fil pour la communication directe avec les sites mobiles 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. 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. **[2]**

- **Réseau de capteur**

Un Réseau de Capteurs Sans Fil (RCSF) est un ensemble de dispositifs très petits, nommés nœuds capteurs, variant de quelques dizaines d'éléments à plusieurs milliers. Dans ces réseaux, chaque nœud est capable de surveiller son environnement et de réagir en cas de besoin en envoyant l'information collectée à un ou à plusieurs points de collecte, à l'aide d'une connexion sans fil. **[7]**

- **Réseau ad hoc**

Réseau ad hoc, réseau sans infrastructure ne comporte pas l'entité « site fixe », tous les sites du réseau sont mobiles et se communiquent d'une manière directe en utilisant leurs interfaces de communications sans fil. L'absence de l'infrastructure ou du réseau filaire composé des stations de base, oblige les unités mobiles à se comporter comme des routeurs qui participent à la découverte et à la maintenance des chemins pour les autres hôtes du réseau. **[8]**

1.3 Réseaux infrastructure Ad hoc

1.3.1 Définition

Une définition formelle des réseaux Ad Hoc MANET (Mobile Ad Hoc NETWORK) est donnée par la RFC 2501. C'est un réseau sans fil composé d'un ensemble des nœuds mobiles qui se déplacent librement dans une certaine zone géographique sans aucune infrastructure fixe préexistante. Un nœud dans le réseau Ad Hoc communique avec un autre nœud directement (en utilisant son interface sans fil), si ce dernier est dans sa portée de transmission, ou indirectement par l'intermédiaire d'autres nœuds du réseau dans le cas contraire.

Chaque nœud 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 nœuds du réseau. **[13]**

La figure 1.3 présente un réseau sans infrastructure Ad Hoc.

Figure 1.3 : Réseau sans fil sans infrastructure (Ad Hoc). **[13]**

1.3.2 Historique et évaluation 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. **[9]**

On compte parmi les chercheurs Robert Elliot Kahn, Jerry Burchfiel, **[10]** 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. **[9]**

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]**

Un autre protocole de routage connu sous le nom de AODV(Ad-Hoc On Demand Routing Vector) est subséquemment présenté puis, plus tard, prouvé et implémenté en 2005 , en 2007, David Johnson et Dave Maltz proposent le DSR : Dynamic Source Routing.**[10]**

1.3.3 Modélisation

Un réseau mobile ad hoc peut être modélisé par un graphe Gt = (Vt , Et) où :

Vt : représente l'ensemble des nœuds (les unités ou les hôtes mobiles) du réseau.

Et : modélise l'ensemble des connexions qui existent entre ces nœuds. (Figure 1.4).

Si e = (u, v) Є Et, cela veut dire que les nœuds u et v sont en mesure de communiquer directement à l'instant t. **[11]**

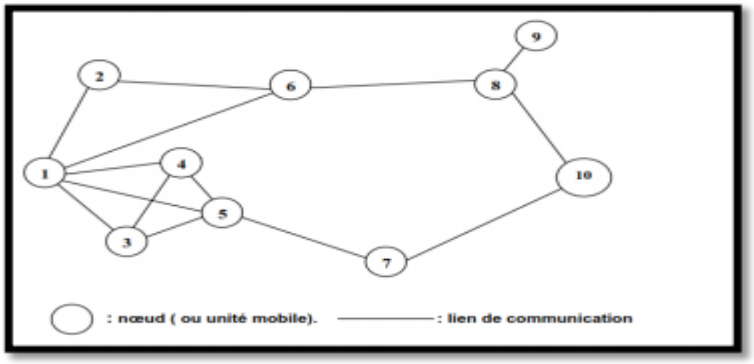


Figure 1.4 : La modélisation d'un réseau Ad Hoc**. [11]**

1.3.4 Caractéristiques des réseaux Ad hoc

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

- **Sans infrastructure** : i.e. doivent assurer des fonctionnalités supplémentaires par rapport aux nœuds, car ils doivent agir en tant que routeurs pour relayer la communication des autres nœuds. **[12]**
- **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. **[12]**

La figure 1.5 suivante montre le changement de topologiedes nœuds :

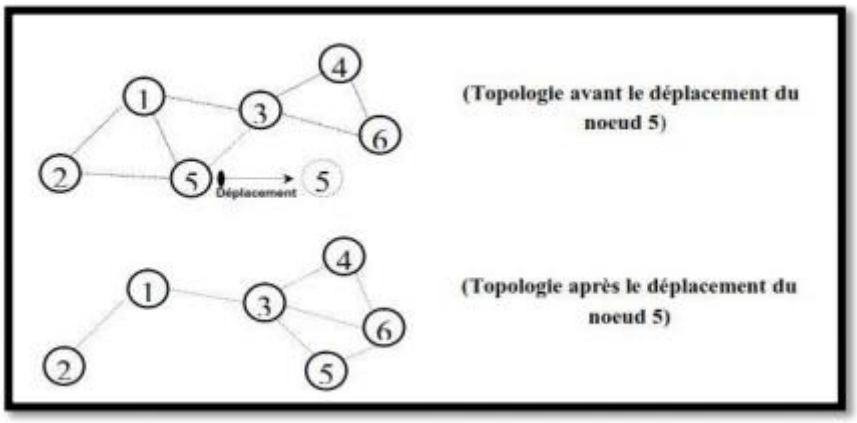


Figure 1.5 : Changement de la topologie d'un réseau Ad Hoc**. [12]**

- **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. **[12]**

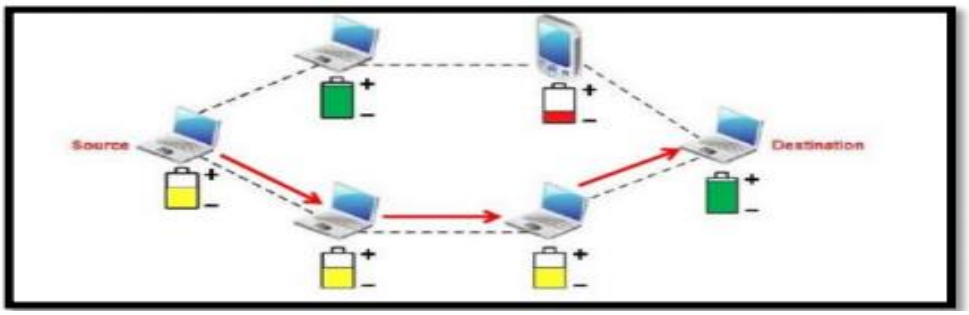


Figure 1.6 : durée de vie de batterie des nœuds. [12]

- **Bande passante limitée :** La communication est basée sur le partage d'un medium sans fil (onde radio). Donc il faut une bande passante modeste, pour chaque hôte du réseau. **[12]**
- **Interférences** : Dans un réseau Ad Hoc, les liens radio qui 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. **[12]**
- **Sécurité et Vulnérabilité :** 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. **[12]**

1.3.5 Avantages des réseaux Ad hoc

- **Pas de câblages :** C'est en éliminant toute les connexions filaires qui sont remplacées par des connexions radio. **[13]**

- **Déploiement facile :** l'absence d'une infrastructure préexistante permettant ainsi d'économiser tout le temps de déploiement et d'installation du matériel nécessaire**. [13]**
- **Mobilité permise :** les réseaux mobiles Ad Hoc peuvent se déplacer librement à condition de ne pas s'éloigner trop les uns des autres pour garder leur connectivité. **[13]**
- **Cout :** Le déploiement d'un réseau Ad Hoc ne nécessite pas d'installer des stations de base. **[13]**
- Distribution rapide d'information autour de l'émetteur. **[14]**

1.3.6 Inconvenants de réseau Ad hoc

- **Débit faible :** l'air étant un support moins fiable et soumis aux bruits parasites par rapport aux réseaux filaires. **[13]**
- **Connectivité limité :** une communication n'est possible que si la collaboration entre stations est suffisante pour lier l'émetteur jusqu' au récepteur**. [13]**
- **Sécurité difficile :** Les terminaux ne sont pas protégés, ils sont menacés de vol ou de destruction. **[13]**
- **Difficulté d'adopter des politiques de gestion globale du réseau** : difficulté de mettre en place un système de facturation à cause de l'absence de centralisation. **[13]**
- **Pollution du voisinage :** tout paquet de diffusion émis vers une station réceptrice en cours de communication va altérer la communication, et rendre celle-ci inexploitable pour la station réceptrice. **[13]**

1.3.7 Domaines d'application

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, où les soldats communiquent en terrain étranger, leur donnant la supériorité sur le champ de bataille.

Des MANETs tactiques peuvent être formés automatiquement pendant la mission, et le réseau "disparaît" quand la mission s'arrête. Ils sont parfois appelés réseaux sans fil tactiques "à la volée"**. [13]**

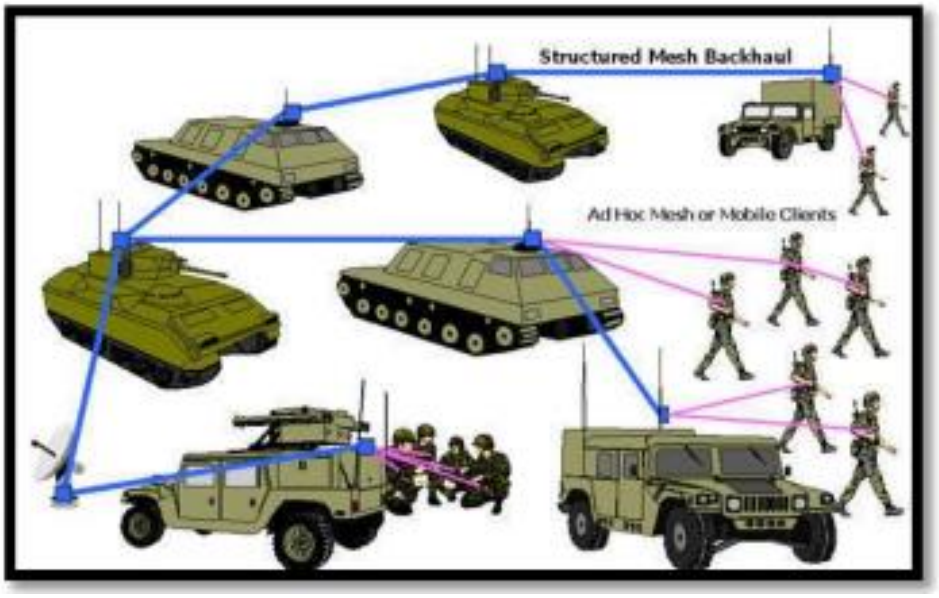


Figure 1.7 : Les applications militaires de réseau Ad Hoc. **[13]**

- **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, En particulier lors de tremblements de terre lorsque les tours radio se sont effondrées ou ont été détruites, des réseaux sans fil ad hoc peuvent être formés indépendamment. Les pompiers et les secouristes peuvent utiliser des réseaux ad hoc pour communiquer et secourir les blessés. Des radios commerciales avec de telles capacités sont disponibles sur le marché**. [13]**

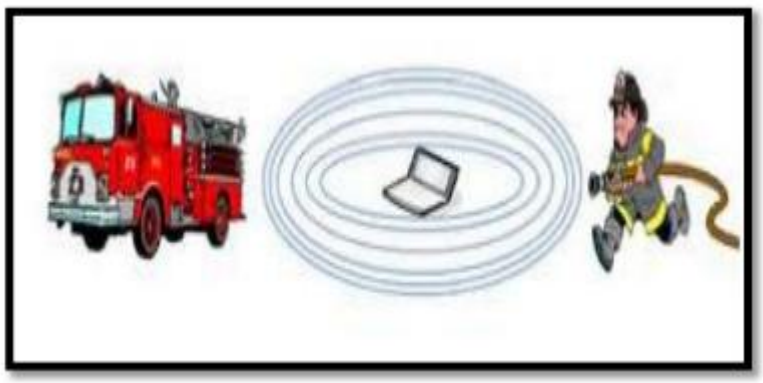


Figure 1.8 : Applications de secours des réseaux Ad Hoc**. [13]**

- **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. **[15]**

- **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. **[15]**
- **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. Par exemple les VANETs sont utilisés pour la communication entre véhicules et équipements routiers. Les réseaux véhiculaires ad hoc intelligents (InVANETs) sont un type d'intelligence artificielle qui aide les véhicules à se comporter de manière intelligente lors de collisions vehicle-to-vehicle ou accidents. Les véhicules utilisent des ondes radios pour communiquer entre eux, créant instantanément des réseaux de communication à la volée alors qu'ils se déplacent sur les routes. **[16]**
- **Réseaux de capteurs :** généralement exploités pour des applications environnementales (météo, activité terrestre, suivi animale, etc.). Leur usage permet l'analyse et la gestion de phénomènes complexes sur une longue période de temps et sur une large zone géographique tel que : la température, l'humidité, la pression, le bruit, etc. Les capteurs sont de plus en plus connectés sans fil afin de permettre la collecte de données de capteurs à grande échelle. **[11]**

La figure 1.9 résume les domaines d'application des réseaux ah doc :

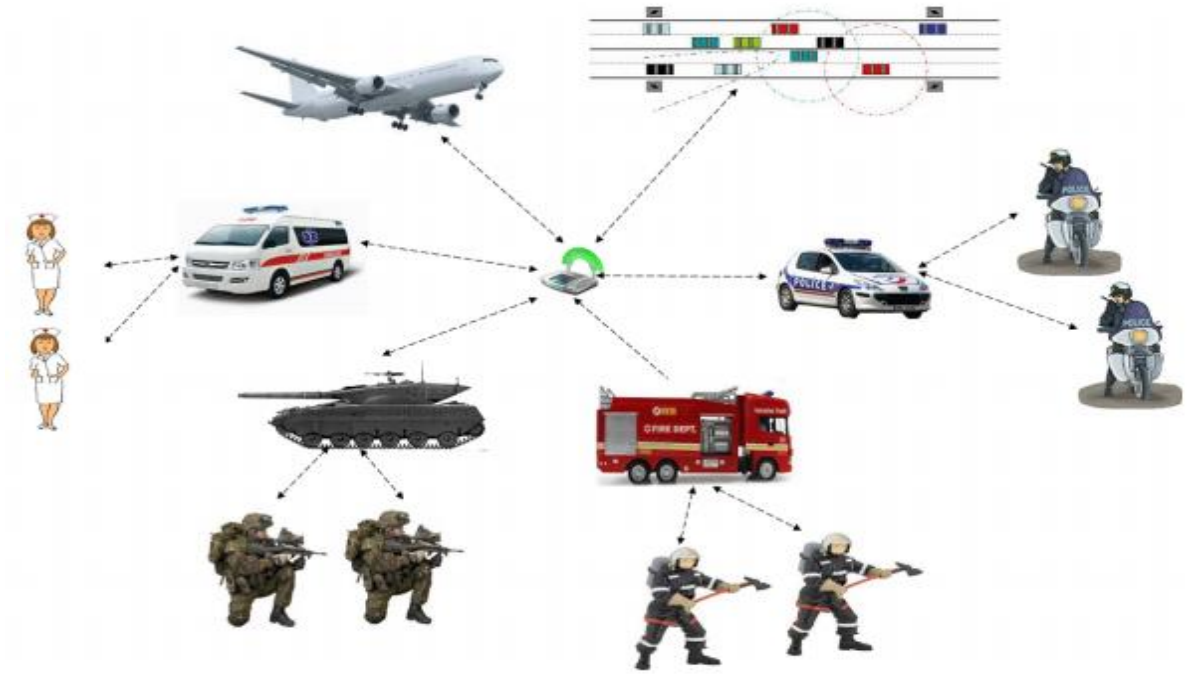


Figure 1.9 : Domaine d'application des réseaux Ad Hoc**. [9]**

1.4 Routage dans le réseau Ad hoc

1.4.1 Définition 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 capable de s'adapter aux événements venant perturber le réseau (panne, congestion, etc.). **[13]**

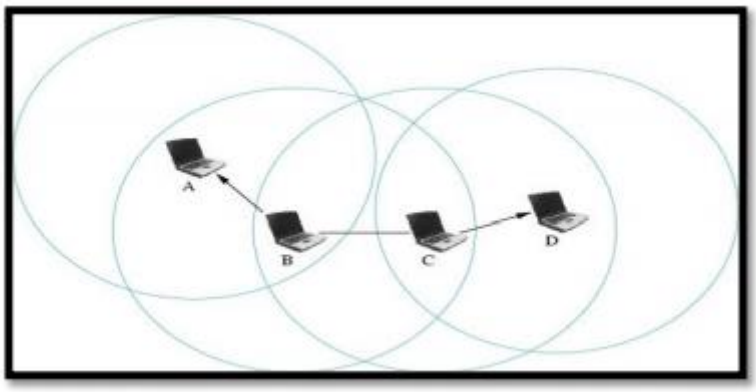


Figure 1.10 : Le chemin utilisé dans le routage entre la source et la destination**. [13]**

1.4.2 Méthodes de routage

Certains algorithmes de routage ont été définis très tôt mais restent des méthodes solides et éprouvées qui sont encore utilisées aujourd'hui, les différentes méthodes qui existent sont :

1.4.2.1 Routage par inondation

Le routage par inondation est la méthode de routage la plus triviale : chaque routeur recevant un paquet le réémet sur toutes les interfaces s'il n'est pas la destination du paquet. Pour que la fin de l'inondation soit garantie, plusieurs techniques peuvent être employées**. [18]**

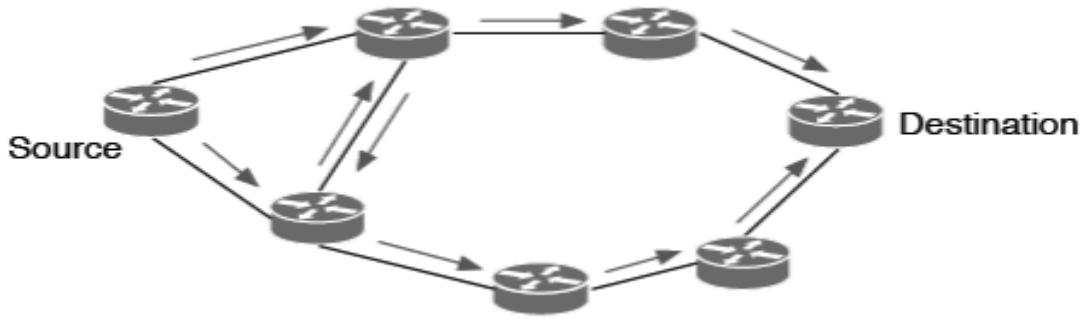


Figure 1.11 : Émission d'un paquet dans le cas du routage par inondation**. [18]**

Le routage par inondation a en outre pour particularité une grande robustesse en raison de la redondance liée à l'inondation. Si le paquet vers une destination est perdu sur un chemin, il suffit qu'un autre chemin disjoint du premier existe pour que le paquet parvienne tout de même à destination**. [18]**

1.4.2.2 Routage par vecteur de distance

Routage par vecteur de distance est basé sur l'algorithme de Bellman-Ford distribué. Chaque routeur possède une table de routage qui consiste en un couple de données pour chaque destination : le routeur par lequel passer pour atteindre cette destination et le coût associé selon une métrique définie. Ces informations sont transmises périodiquement à tous les voisins, et donc chaque routeur reçoit ces informations de ses voisins. Il en résulte que, pour un routeur, toute destination existante dans la table de routage d'un voisin devient connue et donc accessible par ce routeur**. [18]**

Figure 1.12 : Réseau utilisant le routage par vecteur de distance. **[18]**

Cet algorithme forme le cœur du protocole RIP, qui fut utilisé au début d'Internet. En raison du problème majeur qu'est la convergence des informations de routage en cas de rupture de lien et parce qu'il était plus adapté à des réseaux de taille limitée, le routage par vecteur de distance a été assez rapidement abandonné au profit du routage par état de lien**. [18]**

1.4.2.3 Routage par état de lien

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. 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**. [13]**

On peut distinguer trois phases :

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

1.4.2.4 Routage à la source

Le routage à la source ou " source routing" consiste à indiquer dans le paquet routé l'intégralité du chemin que devra suivre le paquet pour atteindre sa destination. L'entête de paquet va donc contenir la liste des différents nœuds relayeur vers la destination**. [19]**

1.4.2.5 Routage saut par saut

Le routage saut par saut ou "hop by hop" consiste à donner uniquement à un paquet l'adresse du prochain nœud vers la destination**. [19]**

1.4.3 Stratégies de routage

Le réseau doit être robuste aux changements de topologie (pannes d'´équipements, extensions temporaires du réseau) et à l'´évolution de la demande (mobilité des utilisateurs ou variabilité des applications). **[9]** Les stratégies optimales de routage doivent pouvoir faire face à ces types de

dynamiques afin que les protocoles de routage résultants ne dégradent pas les performances du système:

- **La minimisation de la charge du réseau :** les stratégies de routage déterminent les goulots d´étranglement dans le réseau et donc les limites de la capacité offerte aux utilisateurs. **[9]**
- **Offrir un support pour pouvoir effectuer des communications multipoints fiables** L'élimination d'un lien, pour cause de panne ou pour cause de mobilité devrait, idéalement, augmenter le moins possible le temps de latence**. [9]**
- **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 etc.) **[13].** Si la construction des chemins optimaux est un problème dur, la maintenance de tels chemins peut devenir encore plus complexe, on doit assurer une maintenance de routes sans coût supplémentaire. **[9].**
- **Le temps de latence :** la qualité des temps de latence et de chemins doit augmenter dans le cas où la connectivité du réseau augmente**. [13]**

1.4.4 Routage sans fil 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. Les protocoles de routage actuellement utilisés dans les réseaux filaires ne peuvent être utilisés dans les réseaux MANETs. De fait de nouveaux protocoles de routage ont dû être développés. Ils ont le même but qui consiste à maximiser le débit, et en même temps minimiser le nombre de paquets de contrôle, le taux de perte. **[17]**

1.4.5 Classification des protocoles de routage

Pour résoudre la difficulté du routage dans les réseaux ah doc, plusieurs classifications sont apparues, et parmi lesquelles on a :

1.4.5.1 Routage hiérarchique ou plat

Le premier critère utilisé pour classifier les protocoles de routage dans les réseaux Ad Hoc concerne le type de vision qu'ils ont du réseau et les rôles qu'ils accordent aux différents mobiles**. [19]**

1.4.5.2 Routage à plat

Considèrent que tous les nœuds sont égaux. La décision d'un nœud de router des paquets pour un autre dépendra de sa position. Comme présenté sur la figure 1.13, tous les nœuds du réseau ont la même tâche : relayer l'information reçue vers le nœud suivant. **[19]**

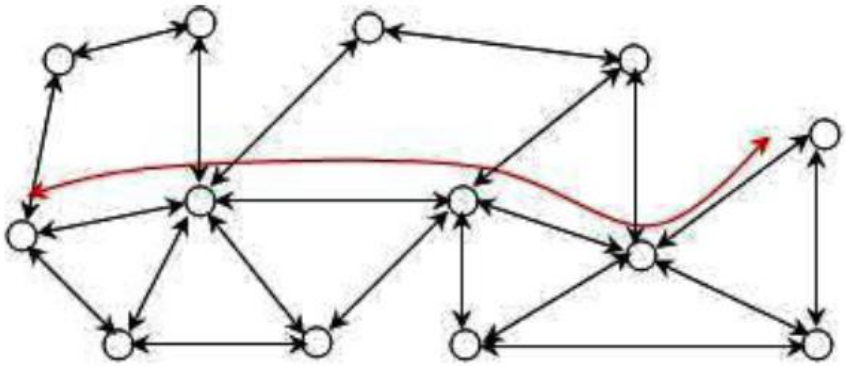


Figure 1.13 : Routage à plat. **[20]**

1.4.5.3 Routage hiérarchique :

Fonctionnent en confiant aux mobiles des rôles qui varient de l'un à l'autre. Certains nœuds sont élus et assument des fonctions particulières qui conduisent à une vision en plusieurs niveaux de la topologie du réseau. Les nœuds seront utilisés comme passerelles et le reste des nœuds seront attachés à la passerelle la plus proche, la figure suivante montre que si le nœud N1 veut envoyer un paquet a un nœud N7, il doit passer d'abord par la passerelle p1, p2 ensuite p3. **[19]**

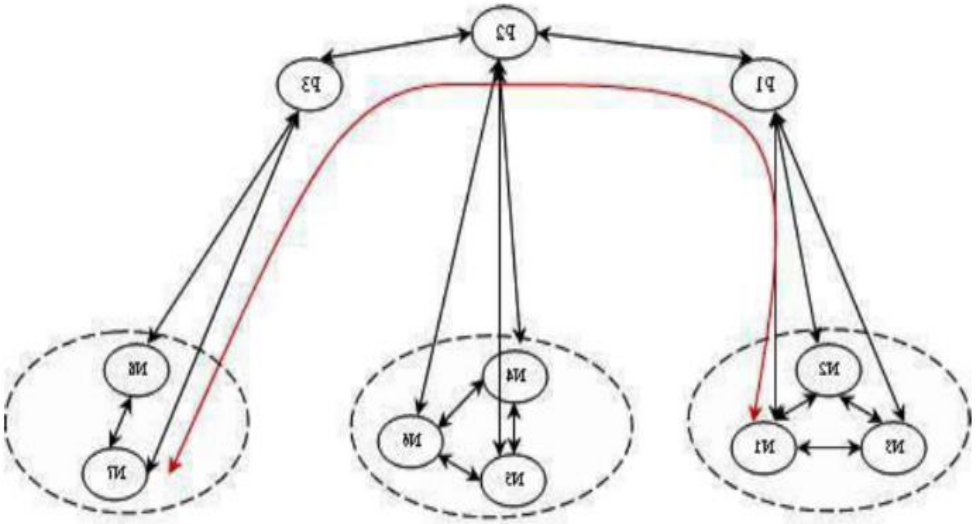


Figure 1.14 : Routage hiérarchique. **[20]**

1.4.6 Modes de communication dans les réseaux Ad Hoc

Il existe trois principaux mode de communication dans ces réseaux et particulièrement dans les réseaux Ad-Hoc : **[9]**

- La communication point à point ou unicast, pour laquelle il y a une source et une seule destination**.**
- La communication multipoint ou multicast, qui permet d'envoyer un message à plusieurs destinataires.
- La diffusion ou broadcast, qui envoie un message à tous les nœuds du réseau.

La figure 1.15 montre les différents modes de communication dans les réseaux mobiles :

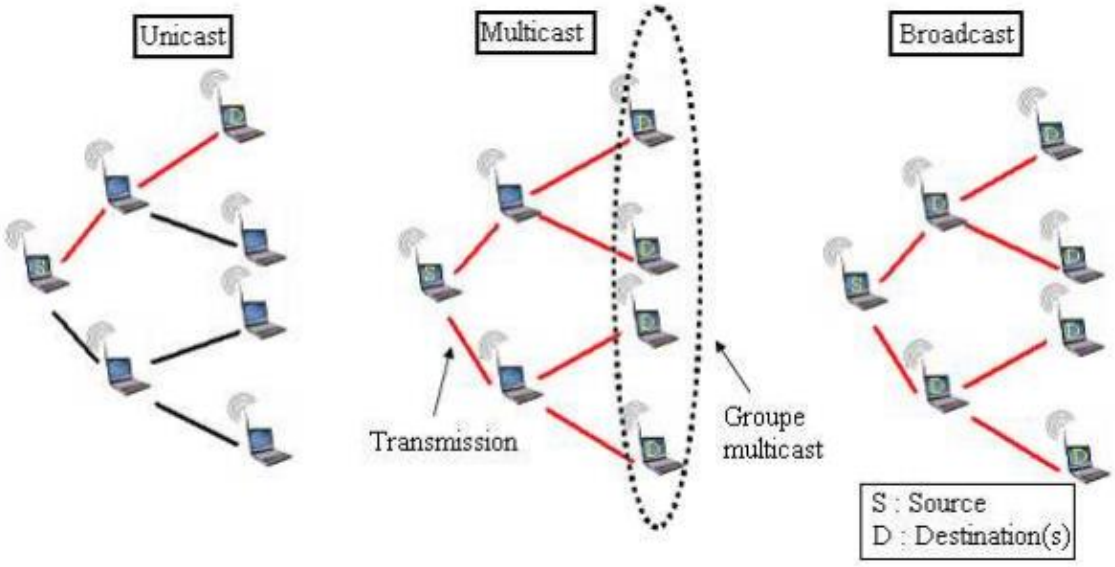


Figure 1.15 : Modes de communication dans les réseaux mobiles. **[9]**

1.5 Conclusion

Ce chapitre s'est focalisé sur les concepts des environnements mobiles et en particulier sur les réseaux Ad Hoc. Dans ce chapitre, nous avons présenté les réseaux sans fil, et ses catégories selon leurs zones de couverture (WAN – MAN- PAN –LAN) et selon l'infrastructure.

Puis nous avons vu la définition et l'historique et l'évolution des réseaux ad hoc, ainsi que sa modalisation. Ensuite, nous avons exposé les caractéristiques ainsi que les avantages et les inconvenants des réseaux ah doc puis on a vu ses domaines d'applications.

Puis nous avons étudié la définition, les méthodes de routage, ainsi que les stratégies de routage. Et on passe au routage sans fil ad hoc, les différents modes de communication dans les réseaux MANETs. Ensuite, l'étude effectuée sur les réseaux mobiles Ad Hoc nous a permis de connaître leurs modes de transmissions, les différentes caractéristiques et ces classifications.

Chapitre 2 : Protocoles de routage et l'équilibrage de charge dans le réseau Ah doc

2.1 Introduction

Pour assurer le routage dans les réseau ah doc et garantir l'équilibrage de charge entre les nœuds il existe un nombre assez important de protocoles de routage, qui consistent à assurer une stratégie qui garantit à n'importe quel moment la connexion entre les nœuds appartenant au réseau. Cette stratégie doit prendre en considération les changements de la topologie du réseau, ainsi que d'autres caractéristiques comme la bande passante, le nombre de liens, limitation d'énergie, etc.
Dans ce chapitre nous allons présenter quelques protocoles de routage qui ont été développés dans les réseaux mobiles Ad-hoc.

2.2 Métriques de la qualité de service

Les principaux aspects connus de la qualité de service sont : la bande passante, le délai de bout en bout, la gigue (variation du délai), et les pertes de paquets ou taux d'erreurs.

2.2.1 Bande passante

La bande passante est un facteur sensible dans les réseaux MANETs. Elle représente la source de transmission qu'occupe ou reçoit un flot. La bande passante est basés sur la communication sans fil est l'utilisation d'un médium de communication partagé (ondes radio). Elle est donc nécessaire de l'optimiser au maximum pour permettre au plus grand nombre de flux d'accéder au réseau, pour éviter les collisions. Et l'élément qui sert à les contrôler c'est le protocole de routage. **[9]**

2.2.2 Estimation du Délai

Les applications multimédia nécessitent très souvent le respect d'un délai borné de bout en bout. L'estimation du délai, entre nœuds voisins ou de bout en bout d'un chemin, est dans ce cas indispensable. Il existe des modèles qui estiment le délai de bout en bout, afin d'estimer le temps de service d'un paquet dans la file d'attente de l'émetteur. Ces modèles sont liés au fonctionnement de CSMA/CA, et tiennent compte des flux qui traversent un nœud ou ses voisins. **[21]**

2.2.2.1 Modèle d'estimation de délai à sonde

Ce modèle estime le délai d'un lien en calculant la différence de temps s'écoulant entre la création d'un paquet Hello et la réception de ce dernier par le destinataire. Les nœuds doivent être synchronisés entre eux car ils doivent avoir des horloges synchronisées pour ne pas fausser l'estimation du délai. Ainsi que les collisions ne sont pas prises en compte, quel que soit la charge à la réception. **[21]**

2.2.2.2 Modèle d'estimation de délai de bout en bout

Ce modèle d'estimation du délai de bout en bout englobe en réalité trois aspects temporels différents :

- **Le délai de propagation** : en effet, c'est la distance physique qui sépare la source de la destination (plus la distance est grande, plus le délai est important). **[21]**
- **Le délai d'attente et de traitement des paquets** : on peut déterminer la charge du réseau, ainsi que les politiques de traitement de l'information dans les nœuds pour obtenir une fluidité maximale de l'écoulement de l'information, c'est-à-dire à l'intérieur des files d'attente. **[21]**
- **Le délai de transmission :** C'est un paramètre qui est lié à l'utilisation du réseau et au partage de la bande passante disponible et qui dépendant de la taille des flots. **[21]**

2.2.3 La Gigue

La gigue est due principalement aux délais de traitement, elle correspond à la variation de délai de transmission de bout en bout entre les différents paquets d'un flot à travers un réseau. **[9]**

2.2.4 Perte de paquets

La perte de paquets se produit principalement lorsqu'il y a des erreurs d'intégrité sur les données et l'intensité du trafic sur les liens de sorties. Lorsqu'il y a un affaiblissement important ou à grande mobilité, la probabilité que le signal émis n'arrive pas est en fonction de la distance qu'il parcourt. Les données transportées sont donc sujette à de nombreuses perturbations et le taux d'erreur des paquets seras augmentée. **[9]**

2.3 Sécurité du routage Ad hoc

Les réseaux mobiles sont plus touchés par le paramètre de sécurité que les autres réseaux classiques. Plusieurs protocoles de routage ont été base pour assurer une communication fiable entre les nœuds, mais moins d'attentionné sur la sécurité lors de la conception de ces protocoles, les pirates peuvent lancer de nombreuses attaques de sécurité Par exemple, des attaques peuvent permettre la modification des bases de données des clés publiques et perturber ainsi les services de sécurité tels que l'authentification, la confidentialité et l'intégrité. **[18]**

Plusieurs propositions ont vu le jour, mais jusqu'à nos jours il n'y a pas une solution qui fais le compromis attendu par les utilisateurs entre sécurité et c'est pourquoi ce domaine est encore en exploration par les chercheurs mais y a pas mal de solution, exemple **TinySec** qui présente comme une couche de sécurité au niveau liaison de données**. [18]**

2.3.1 Attaques sur le routage Ad hoc

Plusieurs caractéristiques peuvent être utilisées pour classer les attaques dans les réseaux ad hoc. Elles peuvent être classées suivant le comportement des attaquants (passive et active), suivant la source des attaques (externe ou interne), suivant la capacité de traitement des agresseurs (mobile ou câblé), ou suivant le nombre des attaquants (unique ou plusieurs). **[18]**

2.3.2 Attaques contre les messages de routage

Dans une attaque de modification de message, les nœuds malveillants apportent quelques modifications aux messages de routage, et donc endommagent l'intégrité des paquets dans le réseau. Et comme les nœuds sont libres alors à un certain moment, ils peuvent inclure des nœuds malveillants. **[18]**

L'importance des messages de routage a fait d'eux une cible privilégiée par les attaquants pour lancer des attaques contre les réseaux ad hoc, les informations ou les messages peuvent être déviés à partir du fonctionnement normal à l'aide d'attaques de modification, d'interception, d'interruption ou des attaques de fabrication de paquets. Dans un cas plus grave, les attaquants peuvent également utiliser n'importe quelle combinaison de ces attaques pour perturber la circulation normale de l'information. **[18]**

2.3.3 Modification de trafic

Lors d'une attaque de paquets mal acheminés, les nœuds malveillants font dériver le trafic de son chemin original pour le faire atteindre de fausses destinations et ils peuvent exploiter cette faille pour se faire passer pour un autre nœud en modifiant le contenu des paquets. Les attaquants peuvent acheminer un paquet pour le faire rester dans le réseau plus longtemps que ce que permet sa durée de vie, ainsi il sera supprimé du réseau. Par conséquent, il aura la consommation de plus de bande passante, et augmentera aussi la surcharge du réseau. **[18]**

2.3.4 Besoin de sécurité du routage ad hoc

Les exigences de sécurité, dans les réseaux ad hoc, dépendent de la nature de l'application. Les applications militaires sont très exigeantes en sécurité. Mais dans des applications de surveillance de l'environnement, par exemple, la sécurité n'est pas très exigeante. N'importe quel algorithme de routage doit intégrer dans son système un mécanisme de sécurité qui dépendra de plusieurs facteurs (authentification, intégrité, confidentialité et disponibilité) et qui concerne deux aspects : la sécurité du routage et la sécurité des données. **[18]**

Quelque besoin de la sécurité du routage ad hoc :

- **Faible capacité :** La capacité souvent limitée des nœuds et l'utilisation de batteries pour l'alimentation des équipements sont aussi des faiblesses des réseaux ad hoc. **[18]**
- **Manque de coopération :** Comme les nœuds dans un réseau ad hoc ont tendance à être égoïstes à cause du manque de ressource, nous devons assurer la coopération entre eux. Mais il est difficile de détecter des nœuds égoïstes. **[18]**
- **Mobilité** : Les attaquants peuvent diffuser de fausses informations et peut aussi les rendre plus difficiles à détecter ou à localiser, car les nœuds rendent la topologie des MANETs instable. **[18]**
- **Interface sans-fil** (radio) : À cause de la nature de transmission radio qui est la diffusion, chaque paquet émi dans le réseau, pourrait être reçu par tous les voisins de l'émetteur. De plus, le problème des nœuds cachés où deux émetteurs qui ne peuvent pas s'entendre l'un et l'autre, envoient à un même récepteur en même temps, peut, causer des collisions. En outre, le problème de nœud exposé, où les nœuds dans la portée d'un émetteur d'une session en cours sont interdits d'émettre, peut gaspiller la bande passante du réseau et les pertes de paquets. **[18]**

2.4 Contraintes de routage dans le réseau ad hoc

2.4.1 Distribution de charge

La distribution de charge consiste à distribuer la charge de manière égale entre tous les nœuds. La distribution de charge devrait suggérer que le trafic ne soit partagé que sur différents liens sans pour autant être nécessairement équilibré.

Les protocoles ont souvent du mal à assurer des transmissions fiables de données en cas de fréquentes ruptures de liens et ne fournissent pas forcement une distribution équilibrée de la charge dans le réseau MANET. Alors que certains nœuds sont peu impliqués dans le routage, d'autres sont fortement congestionnes et acheminent la plupart du trafic du réseau. Cette distribution de charge inhomogène conduit à une consommation rapide des ressources par les nœuds satures ce qui engendre des coupures de liens et déconnexion du réseau, de même elle peut provoquer une forte congestion dans certaines parties du réseau. **[26]**

2.4.2 Equilibrage de charge

L'équilibrage de charge est la répartition équitable des activités de traitement et de communication sur les différentes entités d'un réseau informatique afin de n'en surcharger aucun élément, il est particulièrement important pour les réseaux ou il est difficile de prédire le nombre de demande émi, il s'appuye sur des principes, permettant la distribution du trafic entre les différents nœuds du réseau MANET.

En d'autres termes c'est le fait de repartir le trafic a un ensemble de nœuds constituant le réseau, afin de lisser la charge du réseau. Ce mécanisme permet de repartir la charge globale vers les différents éléments du réseau, de s'assurer de la disponibilité du réseau.

L'équilibrage de charge a pour objectif d'augmenter la capacité du réseau, de prolonger la durée de vie et augmenter les performances du réseau, tout en minimisant la surcharge des liens et des nœuds ainsi que la réduction de la congestion.

Son principe repose sur l'idée d'utiliser simultanément toutes les ressources disponibles. En utilisant deux chemins disjoints ou plus entre une source et une destination.

De ce fait, il faut disposer d'une vue centralisée des charges clients sur tous les nœuds, l'utilisation de cette visibilité peut influencer le choix des nœuds intermédiaires pour acheminer le trafic vers la bonne destination. Cette technique permet d'améliorer les performances du réseau. La capacité est ainsi harmonieusement repartie sur l'ensemble du réseau. **[32] [33]**

2.4.2.1 Niveau d'équilibrage de charge dans le réseau ad hoc

D'après des travaux de recherche sur l'équilibrage de charge on peut distinguer deux niveaux sur lesquels il serait possible de définir une stratégie d'équilibrage de charge :

- **Equilibrage de charges au niveau communication :**

L'équilibrage de charges au niveau communication est devenu un mécanisme efficace pour répondre aux exigences de qualité de service des applications. Il consiste à choisir le meilleur chemin en évitant les chemins encombrés. Son but est de repartir la charge excessive d'un nœud sur ses voisins afin d'améliorer les performances, d'exploiter efficacement les ressources réseaux (buffer, canal radio) et de réduire le taux de perte des paquets et les délais d'acheminement. **[34]**

- **Equilibrage de charges au niveau calcul :**

Dans des différents contextes d'application, (par exemple un utilisateur a besoin d'accéder aux ressources présentes dans le réseau ad hoc. Ces ressources peuvent correspondre à des documents mis à disposition) un mobile doit pouvoir accéder de façon transparente aux ressources de calcul présentes dans le réseau ad hoc. Les stratégies développées dans ce sens tentent de distribuer les taches de calcul d'une manière à équilibrer la charge afin de réduire les temps d'exécution et améliorer l'utilisation des nœuds mobiles. **[34]**

2.4.2.2 Réduction de l'espace de recherche

L'espace de recherche est une zone du réseau dans laquelle sont propagées les informations de routage. Le nœud source envoie un paquet RREQ, pendant la phase de découverte des routes. Alors une réduction de l'espace de recherche réduit les informations de routage nécessaires à la détermination d'une route. **[21]**

Généralement, un protocole de routage, réduisant l'espace de recherche, est conjointement utilisé avec un protocole de détermination de la position de la destination. **[21]**

2.4.2.3 Détermination de la position de la destination

Chaque nœud a besoin de connaître sa position géographique par rapport aux autres nœuds. D'où il doit déterminer ses coordonnées (X, Y) dans une zone donnée. Pour cela, un récepteur GPS (Global Positionning System) et les protocoles de gestion de la localisation peut être utilisé pour récupérer ses coordonnées et connaître la position de ses voisins dans le réseau. Donc une station définit d'autres nœuds dans une certaine zone comme ses serveurs de localisation et envoie périodiquement ses informations de localisation à ses serveurs de localisation. Et pour connaître la

position d'une station en interrogeant les serveurs de localisation de cette station. Chaque nœud définit une zone virtuelle, noté VHR (Virtual Home Region), pour enregistrer les informations de localisation. Lorsqu'un nœud veut en contacter un autre, il contacte d'abord son VHR pour obtenir sa position. Donc les nœuds nécessitent de connaître approximativement la zone de couverture du réseau. **[21] [22]**

2.5 Famille des protocoles de routage

De nombreux protocoles de routage ont été développés pour les MANETs faisant face aux contraintes spécifiques de ce type de réseaux. La fonction principale de ces protocoles de routage est de fournir le chemin le plus court, en terme nombre de sauts, entre une source et une destination. Ces protocoles de routage se décomposent en quatre familles qui sont : proactifs, réactifs, hybrides ou géographiques. **[9]**

2.5.1 Routage proactif

Les protocoles de routage proactifs dans les réseaux ad hoc sont basés sur le même principe des protocoles de routage utilisés dans les réseaux filaires. Les deux principes méthodes utilisées sont : la méthode "état de lien " (ou link state) et la méthode "vecteur de distance " (ou distance victor). Ces deux méthodes imposent une mise à jour régulière des données de routage qui doit être diffusée par les différentes nœuds de routage de réseaux. **[17]**

2.5.2 Routage réactif

Les protocoles de routage réactifs (ou sur demande) ne maintiennent une route que si elle est utilisée. Lorsqu'un nœud source a besoin de transmettre les données vers une source de destination, il doit au préalable déterminer une route. Pour cela, des informations de contrôle sont transmises sur le réseau. Comparés aux protocoles proactifs qui conservent les routes vers l'ensemble des stations du réseau dans leur table de routage, les protocoles réactifs ne conservent que les routes qui ont une utilité. Par conséquent, la taille des tables de routage contenues en mémoire est moins importante que pour les protocoles proactifs. **[17]**

La figure suivante montre la recherche d'une route par protocole réactif :

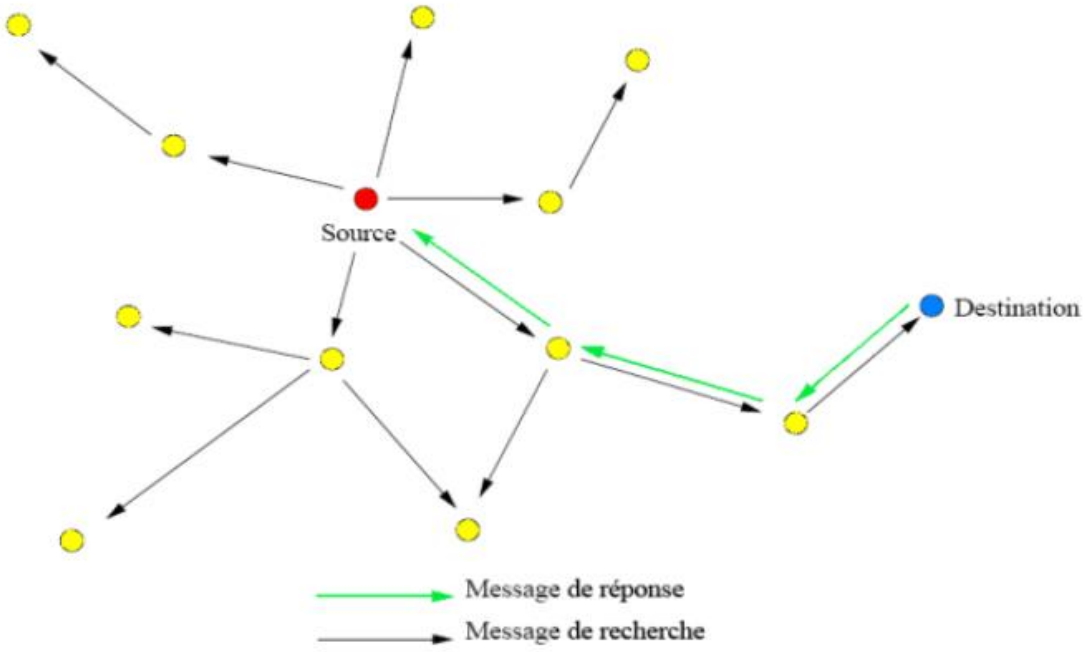


Figure 2.1 Recherche de route par un protocole réactif. [9]

2.5.3 Routage hybride

Les protocoles de routage hybrides combinent les avantages des protocoles proactifs et réactifs. Un nœud va utiliser dans son proche entourage, un algorithme de routage proactif. Ainsi, chaque nœud a une connaissance globale de son voisinage. Puis à l'extérieur de son entourage immédiat, il va utiliser un algorithme de routage réactif. Ce type d'algorithme s'inspire du comportement humain, c'est-à-dire que nous avons une bonne connaissance du quartier où l'on habite, mais plus on s'en éloigne, plus on ne connait que les axes pour atteindre notre lieu de destination, et pas ce qui l'entoure. **[17]**

2.5.4 Routage géographique

Les protocoles de routage géographiques se basent sur des coordonnées géographiques afin de d'envoyer les messages vers la destination, en routant les messages de façon efficace dans la direction de la destination. Par exemple le GPS (Global Positioning System) est actuellement le système de localisation le plus utilisé. Les coordonnées géographiques des nœuds sont incluses dans les tables de routage, c'est-à-dire un nœud inclut l'adresse IP et la position de la destination (fournie par le protocole de routage) dans le message de données à expédier, et envoie ce message dans la direction de la destination. Les nœuds intermédiaires répètent le même mécanisme jusqu'à ce que le message atteigne la destination. **[9]**

2.6 Description de quelque protocole de routage

2.6.1 Protocoles de routage proactif

2.6.1.1 Protocole de routage DLOA

Le protocol Delay-based Load-Aware On-demand Ad-hoc Routing (DLOA**)** est une extension de l'AODV, basé à la demande sur le délai et sur la charge, il utilise le meilleur chemin qui se base sur le retard de chemin total Dp et le nombre de sauts. Le retard de chaque nœud est calculé sur la base du temps de transmission des paquets et du temps d'arrivée des paquets, il fonctionne comme suit :

- D-LOA permet aux nœuds intermédiaires de relayer les paquets RREQ en double si le nouveau chemin (P ') vers La source de RREQ est plus courte que le chemin précédent (P) en nombre de sauts, et DP 'est inférieure à DP (c'est-à-dire, DP' <DP).
- Chaque nœud met à jour l'entrée de route uniquement lorsque le chemin nouvellement acquis (P ') est inférieur à celui du chemin précédent (P) en nombre de sauts, et DP' est inférieur à DP (c'est-à-dire DP '<DP).

Avantage:

Augmente la fraction de livraison des paquets et diminue le délai de bout en bout.

Limitation:

Il collecte les informations sur les autres nœuds du réseau. Les frais généraux de routage sont donc relativement élevés**. [35]**

2.6.1.2 Protocole de routage WLAR

Le protocole **Weighted Load Aware Routing (WLAR)** est une extension d'AODV, il répartit les trafics entre les nœuds via un mécanisme d'équilibrage de charge. Il considère la charge de trafic totale comme une métrique de sélection d'itinéraire. La taille de la file d'attente et les nœuds de partage sont utilisés pour trouver le trafic total. Le trafic total est le produit de la taille moyenne de la file d'attente et du nombre de nœuds de partage, il fonctionne comme suit :

- Dans la phase de découverte d'itinéraire, lorsque les messages RREQ arrivent au nœud central, il le rediffuse en fonction de sa propre charge de trafic totale afin que les RREQ i qui traversent les itinéraires fortement chargés se trouvent au nœud de destination ou déposé en cours de route.
- Le nœud de destination sélectionnera le meilleur itinéraire et répond RREP.

Avantage:

Il se concentre principalement sur le routage basé sur le retard. Donc, évite l'influence du trafic en rafale.

Limitation:

Il recueille toutes les informations sur le routage. Ainsi, la surcharge des paquets de demande d'itinéraire est augmentée. **[35]**

2.6.2 Protocoles de routage réactif

2.6.2.1 Protocole de routage LBAODV

Équilibrage de charge + Ad hoc On-demand Distance Vector Routing Protocol (LBAODV) Similaire à AODV, LBAODV est un protocole de routage à la demande qui réduit le nombre de transmissions inutiles de messages de routage et empêche la congestion du réseau en séparant les nœuds sources dans différents groupes et permettant aux nœuds source de relayer les paquets générés uniquement par les membres de leur propre groupe, les nœuds mobiles sont partitionnés en plusieurs groupes logiques, tous les nœuds communs sont autorisés à relayer les paquets de n'importe quel groupe vers la passerelle. Qui se compose de trois phases principales: **[23] [24] [25]**

- Processus de découverte de chemin.
- Envoi de données.
- Entretien de l'itinéraire.

2.6.2.2 Protocole de routage AODV

L'AODV (Ad-hoc On-demand Distance Vector) est considéré comme la combinaison de DSR et de DSDV, Il combine le mécanisme de demande de base de la découverte et de l'entretien de route de DSR et de l'utilisation du routage de saut-par-saut, en y associant le numéro de séquence (pour le maintien de la consistance des informations de routage) et les mises à jour périodiques de DSDV. AODV conserve sur chaque nœud des informations sur la route découverte, les tables de routages AODV contiennent :

- L'adresse de destination
- Le nœud suivant
- La distance en nombre de nœuds à traverser
- Le numéro de séquence de destination
- Le temps d'expiration de l'entrée de la table

Quand un nœud envoi le paquet de la requête à un voisin, il sauvegarde l'identificateur du nœud dans la table de routage à partir duquel la première copie de la requête est reçue. Cette information est utilisée pour construire le chemin inverse. **[26] [27]**

La figure suivante montre la recherche d'une route par inondation :

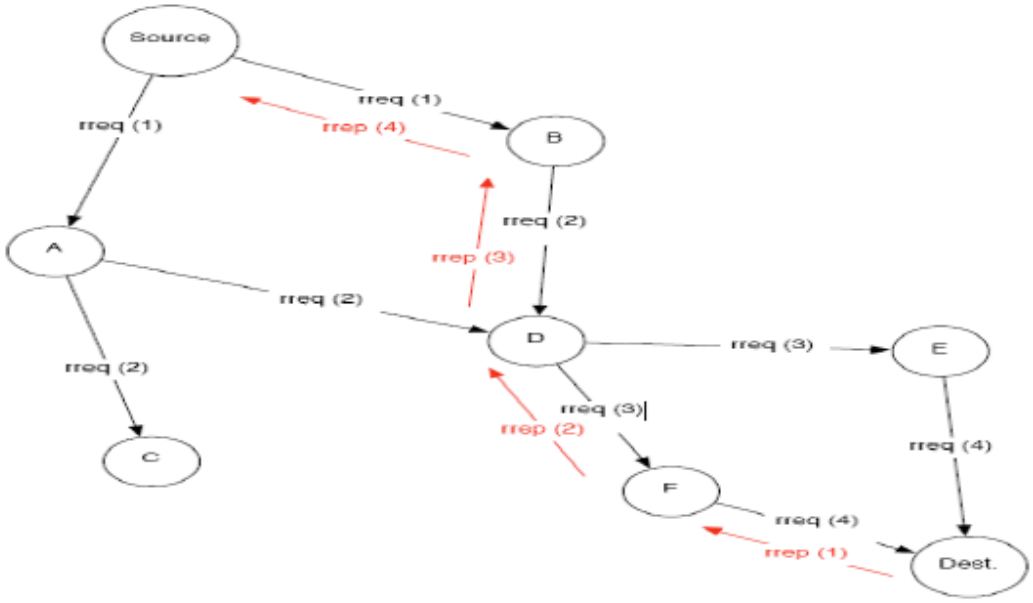


Figure 2.2 : Recherche de route par inondation dans AODV. **[20]**

2.6.2.3 Protocole de routage DSR

DSR (Dynamic Source Routing) est basé sur l'utilisation de la technique "routage à la source" c'est-à-dire c'est à la source de déterminer la séquence complète des nœuds selon lesquelles, les paquets de données seront envoyés. Les nœuds n'ont pas besoin de tables de routage. Les deux opérations de base de DSR sont : **[28] [17] [26]**

- La découverte de routes (route discovery).
- La maintenance de routes (route maintenance).

2.6.2.4 Protocole de routage LBAR

LBAR "Load Balenced Ad Hoc routing" est un protocole de routage à la demande destiné pour le délai des applications sensibles quand les utilisateurs sont plus concernés par le délai de transmissions de paquet.

Par conséquent, LBAR se concentre à comment trouver le chemin qui reflète la moins charge de trafic afin que les paquets de données peuvent être acheminés avec moins de retard. L'algorithme a 4 composants: **[20] [28]**

- Découverte de routes.
- Maintenance de chemins.
- Gestion de la connectivité locale.
- Fonction de calcul de coût.

2.6.2.5 Protocole de routage DLAR

Le protocole DLAR permet de sélectionner le chemin le moins chargé, Ce protocole prend la charge des nœuds centraux comme une métrique pour choisir l'itinéraire, puis il définit le statut des itinéraires qui sont actifs pour construire les chemins lorsque les nœuds de l'itinéraire ont surchargé. L'avantage de DLAR surveille périodiquement l'état de congestion des sessions de données actives et reconfigure automatiquement la route encombrée, mais il se concentre uniquement sur le trafic dans la sélection de l'itinéraire, la longueur de la file d'attente d'interface ne donne pas une vraie image de la charge réelle. **[30]**

2.6.3 Protocoles de routage hybride

2.6.3.1 Protocole de routage LARA

LARA « Load Aware Routing » est un protocole de routage qui assure une transmission efficace des données dans les réseaux mobiles ad hoc, Les réseaux LARA définissent une nouvelle métrique appelée « densité du trafic » utilisée pour l'équilibrage de charge et pour représenter le degré de conflit au niveau MAC. La densité du trafic d'un nœud est la somme de la file d'attente de trafic du nœud plus les files d'attente de trafic de tous ses voisins. Son avantage c'est qu'il répartit uniformément la charge entre tous les nœuds de réseau conduisant à de meilleures performances globales. Ce protocole fait une tentative de sélection d'itinéraire améliorée basée sur la densité du trafic et le coût du trafic. **[31] [30]**

2.7 Conclusion

Au terme de ce chapitre nous avons présenté plusieurs protocoles qui ont été proposés pour assurer le routage dans les réseaux mobiles Ad Hoc.

Certains problèmes liés aux protocoles de routage des réseaux mobiles Ad Hoc sont l'équilibrage de charge, ces protocoles de routage ont différentes métriques de charge comme critères de sélection de route pour mieux utiliser les ressources et améliorer les performances MANET. Avec la notion d'équilibrage de charge, la durée de vie des nœuds mobiles, le taux de livraison des paquets, le débit peuvent être maximiser au contraire de l'encombrement du trafic qui va être minimiser.

Dans le chapitre suivant nous exposera notre contribution d'un protocole de routage afin de minimiser le délai et atteindre notre objectif de l'équilibrage de charge dans les réseaux Ad Hoc.

Chapitre 03 : Présentation de la solution proposée

3.1 Introduction

Il existe deux approches révolutionnaire qui sont possibles pour la conception d'un protocole de routage avec qualité de service (*QoS*) :

- Approche révolutionnaire qui consiste à concevoir un nouveau protocole avec des nouvelles fonctionnalités.
- Approche révolutionnaire qui consiste à apporter des améliorations au protocole de routage avec *QoS* en ajoutant, par exemple, d'autres métriques.

Dans ce chapitre nous avons choisi cette dernière pour l'appliquer au protocole de routage réactif (AOMDV) dans le réseau MANET car il est plus efficace et facile et encore moins couteux d'améliorer un travail existant que de refaire un nouveau travail.

Lors de la transmission d'un paquet de données d'une source vers une destination, il est nécessaire de faire appel à un protocole de routage qui acheminera correctement le paquet par le meilleur chemin. En fait un inconvénient majeur de tous les protocoles de routage existant dans Ad Hoc, c'est qu'ils n'ont pas de dispositions pour le transport de la charge et / ou la qualité d'un chemin lors de la configuration de la route. Par conséquent, ils ne peuvent pas équilibrer la charge ou garantir la qualité de service sur les différentes voies. D'où L'équilibrage de charge et la qualité de service a une grande importance dans les réseaux mobiles Ad Hoc.

Donc nous nous intéressons aux solutions de l'équilibrage de charge et garantir la qualité de service en termes de stabilité des itinéraires dans *MANET.* Nous avons commencé par présenter les deux protocoles de routage qui sont LBAR et AOMDV, et nous présentons les principales métriques de qualité de service où nous avons calculé la stabilité d'un itinéraire dans les réseaux Ad Hoc.

3.2 Protocole AOMDV

Le protocole AOMDV (Adhoc On Demand Multipath Distance Vector) est un protocole multi-chemin, c'est une extension du protocole AODV (Adhoc On Demand Distance Vector), il s'agit aussi d'un protocole à la demande, c-à-dire, il découvre la route lorsqu'une source a besoin de communiquer avec une destination.

Le fonctionnement du protocole AOMDV se base sur le principe suivant : Lorsque la source reçoit un ou plusieurs paquets RREP de nombreux chemins disjoints, elle décide :

- Si Il n'y a pas de route à la destination alors initier découverte de route selon l'AOMDV.
- Si un RREP est reçu, alors il y'aura un seul chemin de la source à la destination qui sera utilisée pour transférer les paquets de données à la route précise.
- Si beaucoup de RREP sont reçus, la source choisit la meilleure route en fonction du nombre de minimum sauts. **[33]**

3.3 Protocole de routage LBAR

Load Balenced Ad Hoc routing : C'est un protocole de routage à la demande où les utilisateurs (destinations) sont les plus concernés par le délai de transmission de paquets. LBAR se concentre donc sur la façon de trouver un chemin, qui reflèterait le moins de trafic, afin que les paquets de données puissent être acheminés avec le moins de retard possible i.e. moins de délai. L'algorithme est présenté en quatre composantes : **[36] [37] [38]**

- Découverte de routes.
- Maintenance de chemin.
- Gestion de connectivite locale.
- Calcul de la fonction de cout.

3.3.1 Principe de fonctionnement

3.3.1.1 Découverte de routes

Le processus de découverte de routes est démarré par un nœud source où un message de configuration est diffusé à ses voisins lorsqu'il ne connaît pas la route. La découverte de routes est divisée en deux phases :

- **FORWARD (étape ascendante) :** un nœud source envoie un message RREQ a ses voisins afin de découvrir la route. **[36] [37] [38]**
- **BACKWARD (étape descendante) :** c'est une réponse de message RREQ, un message RREP est reçu, alors il y'aura un chemin de la source a la destination qui sera utilisée pour envoyer des paquets de données. **[36] [37] [38]**

3.3.1.2 Maintenance de chemin

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. 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. **[36] [37] [38]**

3.1.1.3 Gestion de connectivite locale

Le nœud met à jour ses informations de la table de routage à chaque fois qu'il reçoit un paquet de données d'un voisin afin de garantir la connectivité de ses voisins. Dans le cas où un nœud n'a pas envoyé les paquets de données à aucun de ses voisins actifs dans un temps prédéfinit " hello-interval ", il diffuse "un hello message" contenant son identité et son activité. **[36] [37] [38]**

3.3.1.4 Fonction de calcul de coût

La fonction de cout a pour but de trouver un chemin moins encombré afin que les paquets de données puissent se transmettre à la destination, en respectant l'objectif de l'équilibrage de la charge dans tout le réseau. Ces définitions sont utilisées : **[36] [37] [38]**

- **Le chemin actif** : un chemin de la source jusqu'au la destination qui est suivie par les paquets le long de ce chemin sélectionné. **[36] [37] [38]**
- **Nœud actif**: un nœud est considéré actif s'il est la source, la destination ou un nœud intermédiaire qui transmit les paquets de données. **[36] [37] [38]**
- **Nœud inactif** : un nœud est considéré inactif s'il n'est pas dans le chemin actif. **[36] [37] [38]**

La fonction du coût est représentée comme suit : **[36] [37] [38]**

$$\mathbf{C_k} = \sum_{i \in k}(A_i + TI_i) = \sum_{i \in k}\left(A_i + \sum_{\forall j} A_j^i\right) \quad \textbf{(1)}$$

- **Activité *Ai*** : le nombre de chemin actif par rapport au nœud est défini comme une métrique qui mesure l'activité du nœud. **[36] [37] [38]**
- **Coût** : le minimum d'interférence de trafic est proposé comme une métrique pour le meilleur cout. **[36] [37] [38]**
- **Trafic interférence TI i** : c'est la somme de l'activité de nœuds voisins du nœud i. **[36] [37] [38]** j est un nœud voisin du nœud i. **[36] [37] [38]**

i est un nœud sur le chemin k. (Chaque chemin avec une paire source-destination identifiée comprend la même source et la même destination, donc pour plus de simplicité, les activités de la source et de la destination sont exclues.). **[36] [37] [38]**

$$\boldsymbol{TI_i = \sum_{\forall j} A_j^i} \qquad \textbf{(1.1)}$$

L'inconvénient du protocole LBAR réside dans la fonction de cout, qui calcule seulement, le nombre de sauts entre la source et la destination. Alors on peut envisager des scenarios ou ce protocole pourrait améliorer la qualité de service pour prémunir contre les ruptures de liens.

C'est pourquoi il semble important d'estimer la qualité de service en terme de la stabilité des itinéraires, car les protocoles multi-sauts construisent leurs routes de manière à minimiser le nombre de sauts intermédiaires entre la source et la destination. D'où les données transportées sont donc sujette à de nombreuses perturbations et le taux d'erreurs des paquets y est important. Donc cette nouvelle métrique, basée sur la probabilité de rupture du lien *PR(ij*) au niveau d'un nœud *i* avec un nœud *j*, pour la construction de ses routes. Et cette probabilité est fonction de la distance qui sépare les nœuds communiquant et qu'il convient donc de la minimiser. C'est pour cela que nous avons d'abord calculé la probabilité de rupture des liens *PR(ij*) constituant la route, puis on en déduit la stabilité d'un itinéraire de bout en bout.

3.4 Calcul de la stabilité d'un itinéraire

La stabilité d'un itinéraire *MPS,D* est la stabilité totale de bout en bout entre une source « *S* » et une destination « *D* » est égale au produit des probabilités de rupture *PR(ij*) de tous les liens *(i,j)* constituants cette trajectoire. Elle est écrite sous la forme : **[13] [9]**

$$\boldsymbol{MP_{S,D}(K) = \Pi_{i,j\in[S,D]} PR(i,j)} \qquad \textbf{(2)}$$

PR(ij) : La probabilité de rupture d'un lien.

PR(i,j) : c'est la puissance du signal reçu de *i (émetteur)* qui est récupérée à partir de la couche *MAC*, et de la puissance maximum de réception du nœud *j* (*récepteur*) .

C'est-à-dire la puissance de transmission utilisée. Elle est déterminée par la formule suivante : **[13] [9]**

$$\boldsymbol{PR(i,j) = \frac{Puissance\ Max\ P_{Max}(i) - Puissance\ Reçue\ P_r(j)}{Puissance\ Max\ P_{Max}(i)}} \qquad (2.1)$$

On sait que la *Puissance Max PMAX(i)* reçue par un nœud *i* ne peut pas dépassée sa puissance de transmission (*Pt*) qui est toujours fixe c'est-à-dire *Pt = PMax(i)*. La formule (A) peut alors être écrite sous la forme (B) suivante : **[13] [9]**

$$\boldsymbol{PR(i,j) = \frac{Puissance\ transmission P_t - Puissance\ Reçue\ P_r(j)}{Puissance\ transmission\ \ P_t}} \qquad (2.2)$$

Ainsi (lien très stable) la probabilité de rupture d'un lien *PRi(ij)* tend vers zéro si la puissance reçue du signal *Pr(j)* atteint sa valeur maximum c.à.d. la valeur de la puissance de transmission (*Pr(j) = Pt = PMax(i))*, par contre (lien cassé) elle tend vers un si la puissance reçue du signal *Pr(j)* est en dessous de son minimum (*Pr(j)* < Seuil de sensibilité fixé). [4][5]
C'est pour cela que nous avons d'abord calculé la probabilité de rupture des liens *PR(ij*) constituant la route, puis on en déduit la stabilité d'un itinéraire de bout en bout. **[13] [9]**

Donc, notre objectif est de sélectionner un chemin dont le *MPS,D(k)* de la *kème* route est le minimum *MPS,D** (itinéraire le plus stable) parmi tous les itinéraires trouvés durant le processus de découverte de routes. **[13] [9]**

$$\boldsymbol{MPS,D^* = min\ \{\ MPS,D\ (k)\ \}}$$

Tel que *k = 1..n* c'est le nombre d'itinéraires trouvés lors de l'opération de découverte de route initiée par le nœud source « *S* ». **[13] [9]**
On explique ça avec un exemple de la figure 3.4, le deuxième itinéraire (*AGFED*) est ça valeur calculée de son MPA,*D(2) = 1*PR(AG)*PR(GF)*PR(FE)*PR(ED) = 0,9999998660* est inférieure à celle premier *MPA,D(1) = 1*PR(AB)*PR(BC)*PR(CD) = 0,9999999703*. Donc, on estime que le chemin (*AGFED*) est plus stable que le second (*ABCD*) malgré que celui-ci soit plus long en nombre de sauts. **[13] [9]**

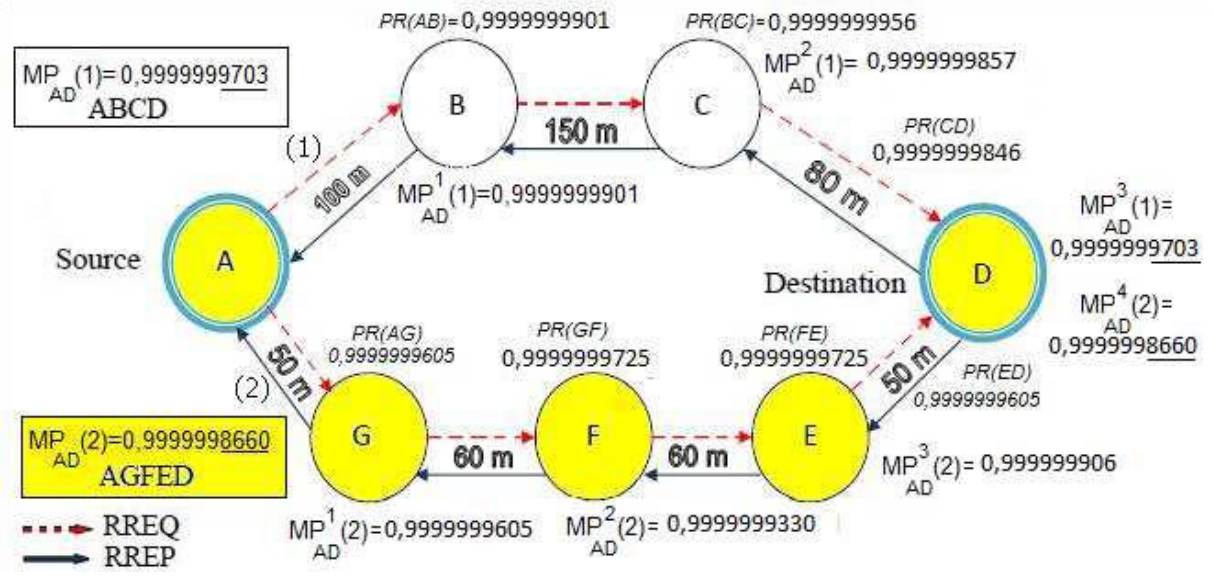


Figure 3.1 : Sélection du chemin le plus stable (*MPAD(k)* le plus faible)**. [9]**

3.5 Intégration dans AOMDV

Pour introduire la fonction de calcul de cout dans LBAR et la qualité de service (la stabilité d'un itinéraire) pour la sélection des chemins au protocole AOMDV, l'idée repose sur l'ajout d'un champ dans les paquets de contrôle, c'est à dire redéfinir la structure du message RREP et la table de routage, de manière à intégrer un nouveau champ qui renfermera la charge de la route.

Cette modification est présente sous la formule suivant c'est-à-dire à base de la formule **(1)** et **(2)** on aura ce résultat :

$$\boldsymbol{C\text{-}MP = MPS,D(k) + Ck} \qquad \textbf{(A)}$$

C : le cout minimum d'interférence de trafic de la fonction LBAR.

MP : le degré de stabilité d'un itinéraire (M : minimiser, P : probabilité de rupture).

La fonction de calcul de cout dans LBAR est **(1)** :

$$\mathbf{C_k} = \sum_{i \in k}(A_i + TI_i) = \sum_{i \in k}\left(A_i + \sum_{\forall j} A_j^i\right)$$

Le calcul de la stabilité d'un itinéraire **(2)** :

$$MP_{s,D}(K) = \Pi_{i,j \in [S,D]} PR(i,j)$$

Pour distinguer le protocole *AOMDV Standard* de l'extension faite dans ce travail, nous avons appelé notre protocole: *AOMDV-SB* (pour Ad Hoc On Demand Multipath Distance Vector *Stable* Balancing), ou *AOMDV* avec équilibrage de charge et Stabilité d'Itinéraire.

3.5.1 Extension des messages *RREP*

Les messages *RREP* sont étendus pour inclure un nouveau champ (*C-MP*), il spécifie le cout minimum d'interférence de trafic et le degré de stabilité d'un itinéraire entre la source et la destination. La valeur de (C-*MP*) est calculée à partir de formule (**A),** qui est décrite précédemment. Ce champ sera mis à jour, au fur et à mesure, et l'envoi en mode unicast vers la source suivant le chemin inverse trouvé.

Type	*Flags*	*Reserved*	*Prefix Sz*	*Hop Count*
Destination IP address				
Destination Sequence Number				
Originator IP Address				
Lifetime				
C-MP (champ incluant la qualité de service et la fonction du cout(LBAR))				

Tableau 3.1 : Format de message *RREP* de *AOMDV-SB.*

Ce tableau possède les différents types de format de message RREP qui sont : **[13]**

- *Type* (8 bits): ce champ indique le type de paquet.
- *Flags* ou *drapeaux* (*2 bits*): ce champ contient deux *flags.*
    1. R *(Repair flag)* : utilisé pour le multicast.
    2. A (*Acknowledgment required*): indique si la source doit envoyer un acquittement pour le message *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 champ 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 *Prefix Sz*.
- *Hop Count* (*8 bits*): il contient le nombre de sauts entre la source jusqu'à la destination.
- *Destination IP Address (32 bits)*: l'adresse *IP* de la destination du paquet *RREQ*.
- *Destination Sequence Number (32 bits)*: le numéro de séquence de la destination associé à cette route.

- *Originator IP Adress (32 bits)*: l'adresse *IP* du nœud qui crée la requête.
- *Lifetime (32 bits)*: le temps pour lequel chaque nœud qui reçoit *RREP* considère que la route est valide.
- C-*MP (32 bits):* Il contient le cout minimum d'interférence de trafic et le degré de stabilité d'un itinéraire possible entre la source et la destination. C'est à partir de cette valeur que la source va sélectionner un chemin.

3.5.2 Table de routage

Une table de routage est étendue pour inclure un nouveau champ (*C-MP*), il spécifie le cout minimum d'interférence de trafic et le degré de stabilité d'un itinéraire entre la source et la destination. La valeur de (C-*MP*) est calculée à partir de la formule (A) décrite précédemment. Ce champ sera mis à jour, au fur et à mesure.

Destination
Sequence_number
Advertised_hopcount
Route_list {(nexthop1,hopcount1,C-MP1), (nexthop n,hopcountn,C-MPn), …}
Expiration_timeout

Figure 3.2 *:* Structure des entrées de la table de routage pour AOMDV-SB.

3.5.3 Mécanisme de découverte des routes dans AOMDV-SB

Puisque le protocole *AOMDV-SB* est une extension du protocole *AOMDV*, il garde la plupart de ces mécanismes de fonctionnement avec quelques modifications pendant la diffusion de la requête de découverte des routes. En premier lieu, un nœud répand à une requête de découverte de route (*RREQ*), dans le cas où il aurait besoin de connaître une route vers une certaine destination et qu'une telle route n'est pas disponible. Cela peut arriver si la destination n'est pas connue au préalable, ou si le chemin existant vers la destination a expiré sa durée de vie ou il est devenu défaillant. Par la suite, un contrôle d'admission est effectué, si la vérification est admise, la *RREQ* est rediffusée

sinon elle est détruite. Enfin, la réservation n'est faite que si la *RREP* de la destination est reçue par la source.

Donc, Le champ de contrôle *C-MP* contient le cout minimum d'interférence de trafic plus le degré de stabilité d'une trajectoire parcourue par les requêtes de découverte de route *RREP*. Quand un nœud *i* de transit (intermédiaire) reçoit un *RREQ*, il récupère d'abord la puissance du signal reçu du nœud émetteur *j* (à partir de sa couche *MAC*) et calcule la probabilité de rupture du lien *PR(i,j) plus* le cout minimum d'interférence de trafic. Si cette valeur est en dessous du seuil fixé, la requête de découverte de route *RREQ* est rejeté sinon la nouvelle valeur du C-*MP* est calculée suivant la formule **(A),** c'est-à-dire, l'ancienne valeur du C-*MP* seras remplacée par la nouvelle valeur. Cette valeur sera réaffectée au champ C-*MP dans la table de routage et dans* la requête de réponse de route *RREP* puis cette dernière sera envoyée en mode *unicast* vers la source par le chemin inverse pour la réservation et la validation de la route concernée. Ces calculs seront effectués à chaque saut, et ainsi de suite, jusqu'à ce que le nœud destination soit localisé.

L'algorithme de l'AOMDV-SB est décrit ci-dessous :

```
Si (pas de route a la destination)
{
Initier découverte de route selon l'AOMDV-SB;
}
Si (unique route connue)
{
Transférer les paquets de données sur la route précisée;
}
Sinon
*/ s'ils existent plusieurs route N vers la source */
{
Distribuer les Paquets de données sur les meilleures routes
Découvertes selon leur cout de charge (C-MP);
  Si (C-MPnv> C-MPanc) {
   La requête de découverte de route RREQ est rejeté
     C-MP : = C-MPanc
  }si non {
      C-MP : = C-MPnv
}
}
```

Figure 3.3 : Algorithme de AOMDV-SB.

3.6 Conclusion

Les protocoles de routage dans les réseaux ad hoc sont des protocoles qui assure la recherche de chemin optimal sans garantis de service, mais, avec l'expansion des données multimédia dans les réseaux ad hoc, la qualité de service est devenu une obligation. Une des méthodes de qualité de service est la stabilité d'itinéraires.

Ad Hoc on demand Multipath distance vector routing (AOMDV) est le plus populaire des protocoles réactifs, son fonctionnement est basé sur la découverte de plusieurs routes et la maintenance de ces routes en utilisant des paquets de contrôle: route request, route reply, route error. Dans le cadre de notre travail, nous avons proposé une amélioration pour ce protocole : LBAR le protocole duquel on a introduit l'une de ses algorithmes de fonctionnement au protocole AOMDV afin d'équilibrer la charge, ainsi, nous avons explicité la qualité de service par rapport au processus de maintenance des itinéraires pour trouver des itinéraires ayant un degré important de stabilité.

Cette amélioration consiste à limiter le nombre de chemin actifs en fonction de la charge dans chaque nœud et pour augmenter la stabilité des routes, en utilisant la formule que nous avons proposé qui se base sur la fonction du cout de LBAR et la stabilité d'itinéraires.

Dans le chapitre suivant, on va traiter l'implémentation et l'évaluation de l'application, nous allons réalisé une série de simulations à l'aide de l'outil NS-3 pour mettre en relief les performances des résultats de notre proposition (le protocole *AOMDV-SB)* en les comparant avec ceux du protocole *AOMDV* standard.

Chapitre 04 : Implémentation et évaluation de la solution proposée

4.1 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 dû faire recours à la simulation qui met à la disposition des utilisateurs un environnement de simulation assez complet. Ce présent chapitre couvre, l'étude et l'évaluation des performances du protocole de routage *AOMDV-SB*. Pour cela, une série de simulations a été faite. L'objectif de cette évaluation est de comparer les performances de l'*AOMDV-SB* avec celles du protocole AOMDV Standard. Il est composé de trois parties :

- La première est organisée comme suit : premièrement nous parlons de la simulation et son intérêt, après les différents types de simulation et ses outils.
- La deuxième partie est organisée comme suit: Tout d'abord montrons l'environnement de simulation choisi NS-2 ensuite passons à l'objectif de simulation.
- La troisième partie est aussi organisée comme suit : englobe tous les résultats du protocole AOMDV et les modifications apportées à ce protocole.

4.2 Simulation

4.2.1 Définition

La simulation est un outil utilisé par le chercheur, l'ingénieur, etc. pour étudier les résultats d'une action ou la modélisation informatique d'un système quelconque sur un élément sans réaliser l'expérience sur l'élément réel. **[13] [38]**

Aujourd'hui, il devient possible de réaliser un simulateur dans un environnement de programmation existant, Grâce aux langages de programmation qui sont très puissants. **[13] [38]**

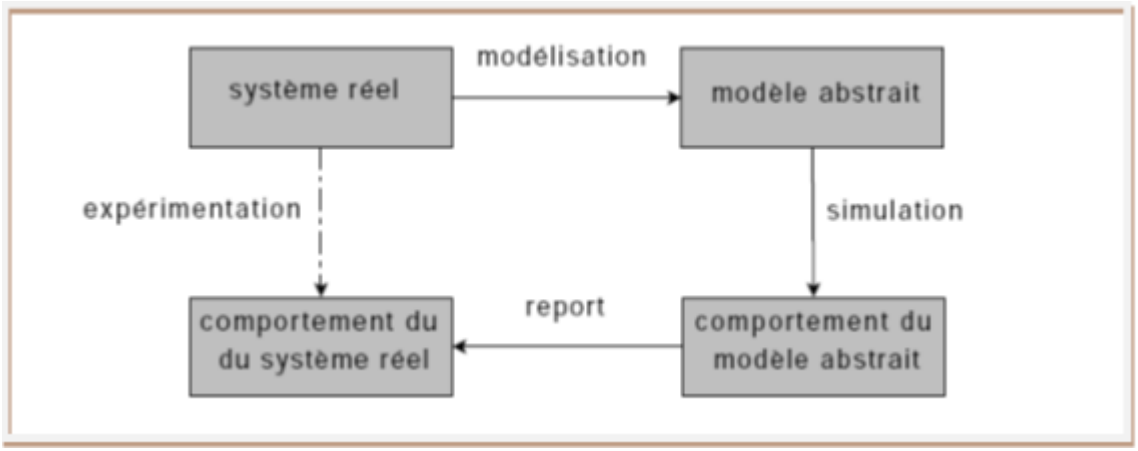


Figure 4.1: Cycle modélisation-simulation. **[40]**

Les modèles analytiques souffrent, soit trop complexes en termes de calcul et de temps de résolution, soit il est trop simplifié, d'où nous obtiendrons des résultats non représentatifs du comportement du système dans un environnement réel, pour cela la simulation d'un système réel devient nécessaire dans les cas suivants : **[13] [40]**

- 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.

4.2.2 Outil de simulation

a. NS (Network Simulator) : [13] [9]

Est créé en 1989 avec le simulateur réseau REAL, utilisé sur la plate-forme *Unix* (*Linux, Solaris, Mac OS*), *Microsoft Windows,* qui permet la description et la simulation de réseaux IP filaires et les réseaux Ad-Hoc. 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 sur 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.

b. Simulateur OMNET : [13] [9]

Le simulateur OMNET++ est un projet open source dont le développement a créé en 1992 par Andras Vargas à l'université de Budapest, Utilisé sur la plate-forme *Microsoft* W*i*ndows, *Unix*, c'est un élément du réseau communiquent par envoi de messages. 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).

c. GlomoSim : [13] [9]

Le simulateur ***GlomoSim*** est utilisé sur la plate-forme *Unix.* Peu de modèles semblent disponibles. Le moteur de *GlomoSim* est basé sur la bibliothèque *Parsec* (le langage de programmation de *GlomoSim*). Le simulateur peut donc être parallélisé, et l'apprentissage de cette API peut se révéler difficile.

d. Jist/SWANS : [13] [9]

Le simulateur **Jist/SWANS** est développé sous le langage *Java*. *Jist* est le moteur de simulation permet d'utiliser, comme générateur de trafic, n'importe quelle application Java, *SWANS* est le simulateur (l'interface). Il souffre cependant du manque de modèles lié à sa jeunesse. Les protocoles sont conçus comme des composants indépendants interconnectés par des interfaces.

e. OPNET : [13] [9]

Le simulateur **OPNET** utilise la plate-forme *Microsoft Windows (NT, 2000, XP)* et *Solaris*. Le développement s'effectue en *C++*, au travers de l'interface du logiciel. L'approche orientée objet associée à des éditeurs graphiques intégrés simplifie la composition des réseaux et des équipements. Il est réputé dans l'industrie pour la modélisation et la simulation de réseaux.

4.3 Environnement de simulation choisi ns2

NS est un outil logiciel de simulation de réseaux informatiques. Il est essentiellement élaboré avec les idées de la conception par objets, de la réutilisation du code et de modularité. Il est aujourd'hui un standard de référence en ce domaine, plusieurs laboratoires de recherche recommandent son utilisation pour tester les nouveaux protocoles.

Le simulateur NS actuel est particulièrement bien adapté aux réseaux à commutation de paquets et à la réalisation de simulations de grande taille. Il contient les fonctionnalités nécessaires à l'étude des algorithmes de routage unicast ou multicast, des protocoles de transport, de session, de

réservation, des services intégrés, des protocoles d'application comme FTP. **[43]** Ce que nous a motivé à choisir cet environnement est :

- NS 2 est le système de référence.
- Un outil libre.
- Un logiciel de simulation multicouche.
- Interface Otcl.
- Couches réseaux code en C++.
- Etc…

4.3.1 Structure de ns2

L'architecture réseau de NS-2 est fortement basée sur le modèle des couches OSI.
Le simulateur NS-2 est écrit en deux langages *C++* et OTcl. Les composantes en *C++* sont utilisées pour faire fonctionner le corps du simulateur. OTcl est une extension orientée objet de Tcl (Tool command language) qui permet une facile intégration avec d'autres langages, il est utilisé comme interface et interprète pour les scripts de simulation, la configuration des noeuds et pour faire la liaison avec les classes objets de *C++* de NS-2.**[44]**

Chaque simulation dans ns-2 est exécutée à partir d'un script écrit en Tcl avec la commande : ns « fichier.tcl ». Dans ce script, on spécifie les paramètres de simulation (temps de simulation, modèle de propagation radio, type de canal sans fil, modèle de mobilité, nombre de nœud, type de protocole, bande passante, type de trafic, etc.). Les résultats des simulations sont fournis dans NS-2 sous forme de fichiers traces. Chaque événement survenu durant la simulation est inscrit dans une ligne du fichier texte.

La figure suivante montre l'architecture générale de NS-ALLINONE :

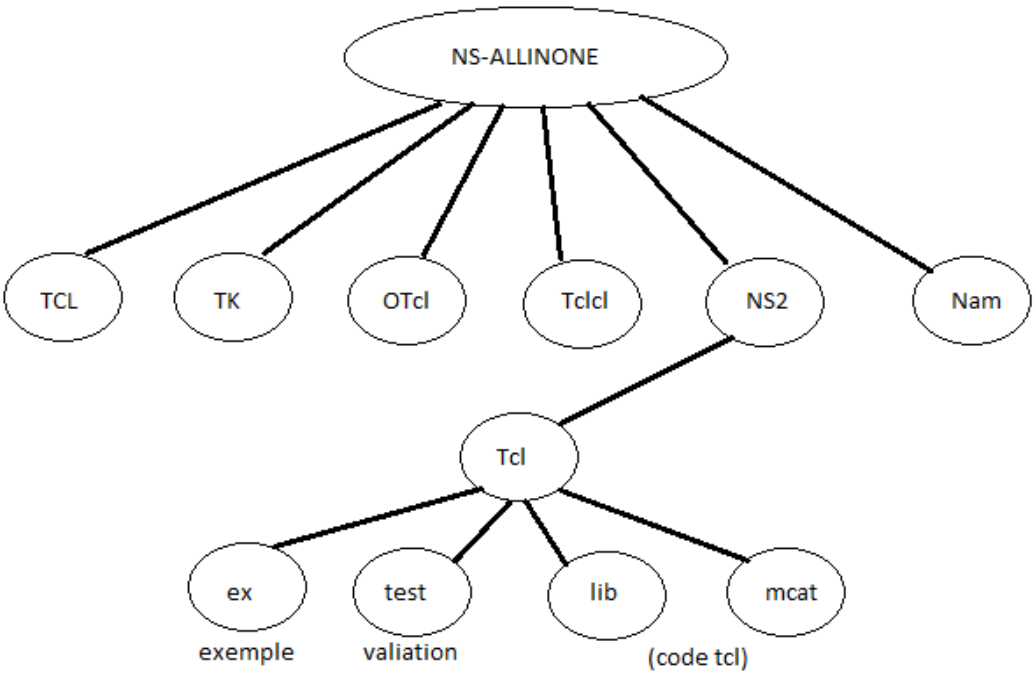


Figure 4.2 : La structure de NS 2.

4.3.2 Xgraph

Xgraph est utilisé dans ns2 pour tracer les caractéristiques des paramètres du réseau comme le débit, le retard, la gigue, la latence, etc. **[44]**, comme le montre la figure 4.3 capturée dans notre machine.

Xgraph est une application qui comprend:

- Tracé et graphique interactifs.
- Animation et directives.
- Portabilité et corrections de bugs.

Cette figure illustre l'interface graphique de Xgraph d'un exemple d'une simulation d'un protocole.

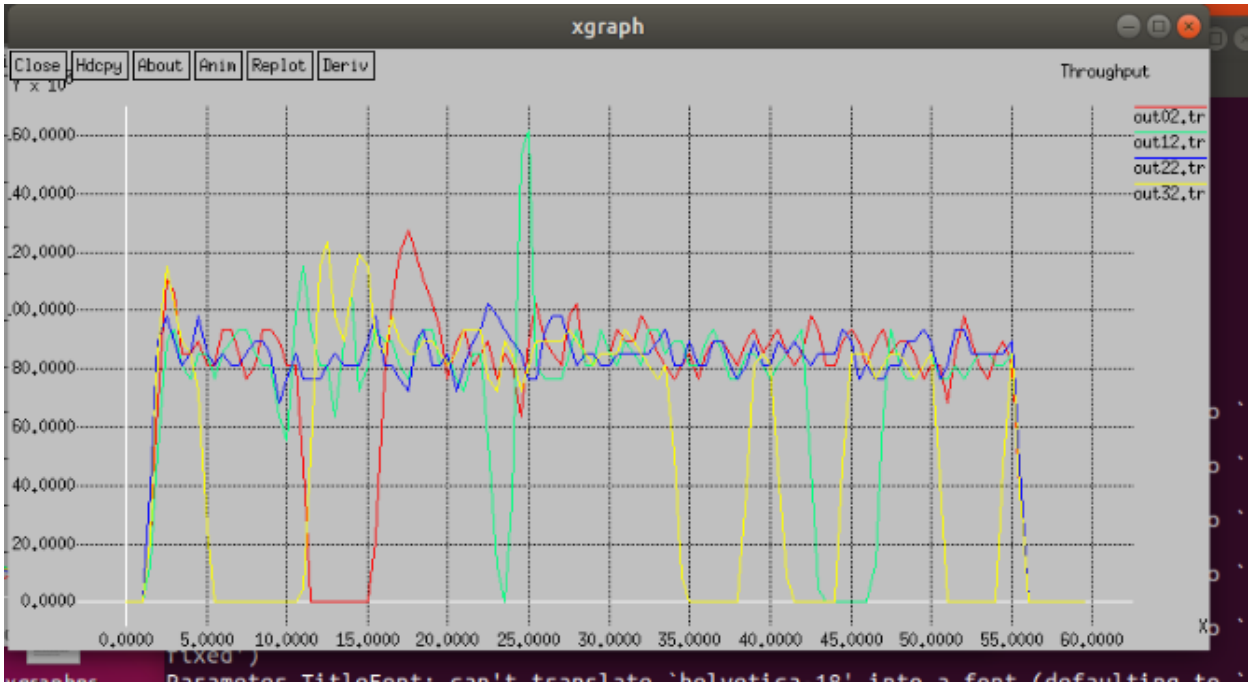


Figure 4.3 : Interface graphique de l'application Xgraph.

4.3.3 NAM

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

NAM est un outil de visualisation qui présente deux intérêts principaux : représenter la topologie d'un réseau décrit avec NS-2, et afficher temporellement les résultats d'une trace d'exécution NS-2. Par exemple, il est capable de représenter la rupture d'un lien entre nœuds, ou encore de représenter les paquets rejetés d'une file d'attente pleine. Ce logiciel est souvent appelé directement depuis les scripts TCL pour NS-2, pour visualiser directement le résultat de la simulation. **[44]**

La figure 4.4 suivante montre l'interface de NAM capturée dans notre machine.

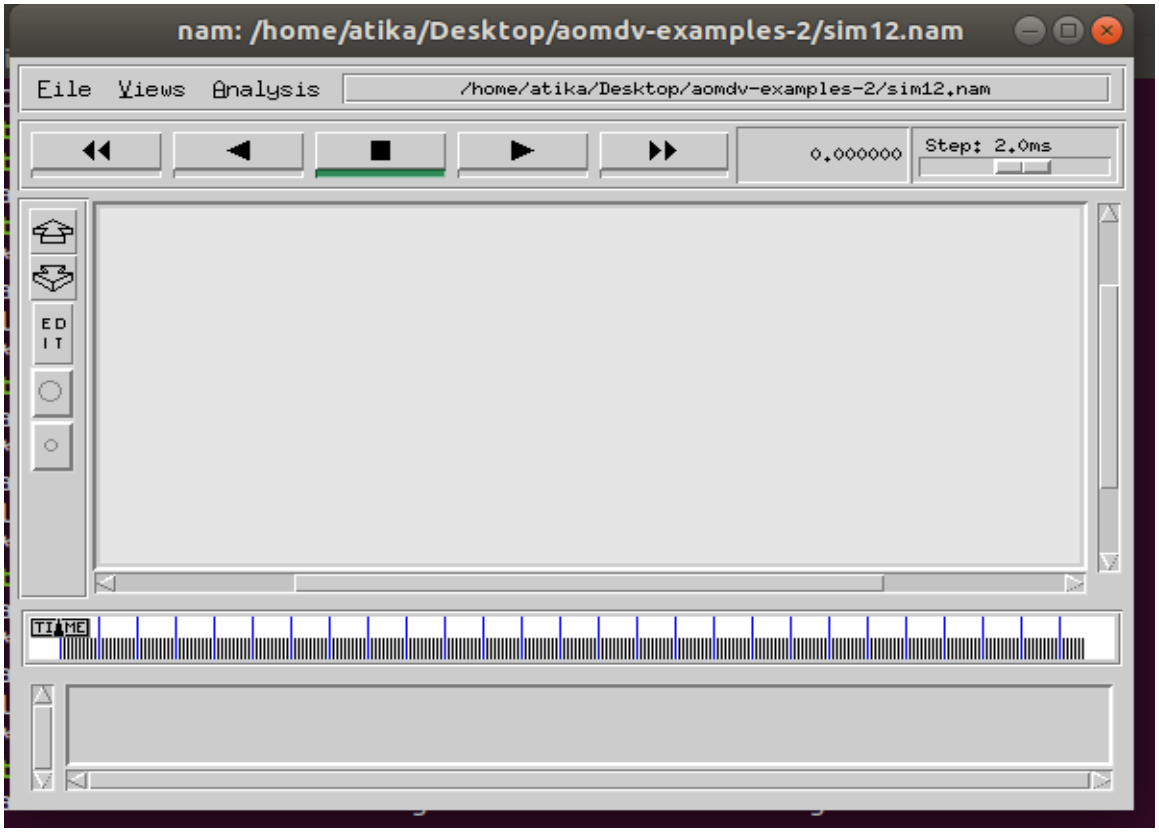


Figure 4.4 : Interface graphique de l'application Nam.

4.3.4 Les différentes phases de simulation

- Créer les nœuds du réseau (nœud d'extrémité et de transit).
- Définir des liens entre ces nœuds (débit, délai, type file ...).
- Définir le routage.
- Créer des agents de transport et les lier aux nœuds (tcp, udp ...).
- Créer des générateurs de trafic (applications) et les lier aux agents de transport.
- Lancer la simulation et créer des fichiers de trace pour effectuer des mesures Visualiser le réseau et tracer des graphes. Le résultat de simulation donne deux types de fichiers : fichier.tr et fichier Nam.

4.4 Mesure de simulation

La simulation est réalisée à l'aide de logiciel NS2 sur Ubuntu 18.04 pour simuler et étudier les comportements de notre nouveau protocole AOMDV-SB.

Nous avons utilisé le protocole AOMDV-Standard pour obtenir de meilleures performances par rapport aux protocoles réactifs d'origine AOMDV avec l'ajout d'une fonction de calcul du cout qu'on a retiré dans le protocole LBAR et une qualité de servie qui est la stabilité d'itinéraire ceci pour garantir la notion d'équilibrage de charge, car si cette dernière est inefficace ça va produire une augmentation de la surcharge de routage, un faible taux de livraison des paquets, un faible débit et d'autres paramètres de qualité de service (QoS).

4.4.1 Configuration de la simulation :

Le réseau simulé se compose des nœuds répartis aléatoirement dans une zone carrée de 800 × 800 m. Chaque simulation a duré 100 s (pour que dans le temps d'attente AOMDV peut trouver un itinéraire alternatif si le lien actuel est rompu, la performance se dégrade a 50s de temps de pause alors que AOMDV attend jusqu'à 100 s).

L'IEEE 802.11 est utilisé comme modèle de communication de couche. Le temps de pause est mis à 10 et la vitesse des nœuds est de 10 m/s. Débit binaire constant Le trafic (CBR) avec des paquets de données de 512 octets est utilisé. Le nombre de connexions CBR varie entre 30 et 100. Les débits d'envoi de paquets utilisés dans la simulation sont de 4, 8, 12, 15 et 20 paquets / s.

4.4.2 Métriques utilisées pour évaluer les performances des protocoles de routage simulés

De nombreuses mesures de performance ont été développées et adoptées pour mesurer et évaluer les performances des protocoles. Tous les processus de mesure des performances nécessitent l'utilisation d'une modélisation statistique pour estimer ces valeurs de paramètres, dans notre cas, ces métriques d'évaluation ont été estimées et utilisées :

- **Charge de routage normalisée**: le nombre moyen de paquets de routage transmis par paquet de données livré. Les paquets de routage sont calculés en termes de différents paquets de contrôle qui sont utilisés par l'algorithme de protocole de routage. Il donne une mesure de la surcharge du protocole. **[45]**
- **Débit moyen**: Le débit est défini comme la taille moyenne d'un bloc de donnée indiquée, divisée par le délai d'accès moyen correspondant. Cet index est lié à l'indice d'utilisation,

qui peut être défini comme la fraction de la capacité du canal utilisée pour la transmission réussie des données. **[45]**

- **Stabilité d'itinéraire** : Un chemin est dit stable s'il est formé uniquement par des liens stables.
- **Pourcentage de livraison de paquets :** le nombre moyen de paquets de données transmis par la source par paquet de données livré à la destination. Les paquets perdus ne sont pas pris en compte.
- **Délai moyen de bout en bout**: délai moyen entre le moment où le paquet est généré à la source et le moment où il atteint la destination. Ce délai comprend le temps de retard du processus de découverte d'itinéraire, le délai de mise en mémoire tampon au niveau de la file d'attente d'interface des nœuds intermédiaires, le processus de transmission au niveau de la couche MAC, le traitement des paquets et les temps de transfert et de propagation. **[46]**

4.5 Teste et résultat

Pour étudier la performance du AOMDV-SB et la comparer à l'AOMDV, nous propose 2 scénarios de simulation :

4.5.1 Scenario 1 : Varier le taux de débit des paquets pour voir comment les protocoles se comportent lorsque la charge est élevée avec 20 nœuds :

Les figure suivante montre les fichier trace des résultats de simulation :

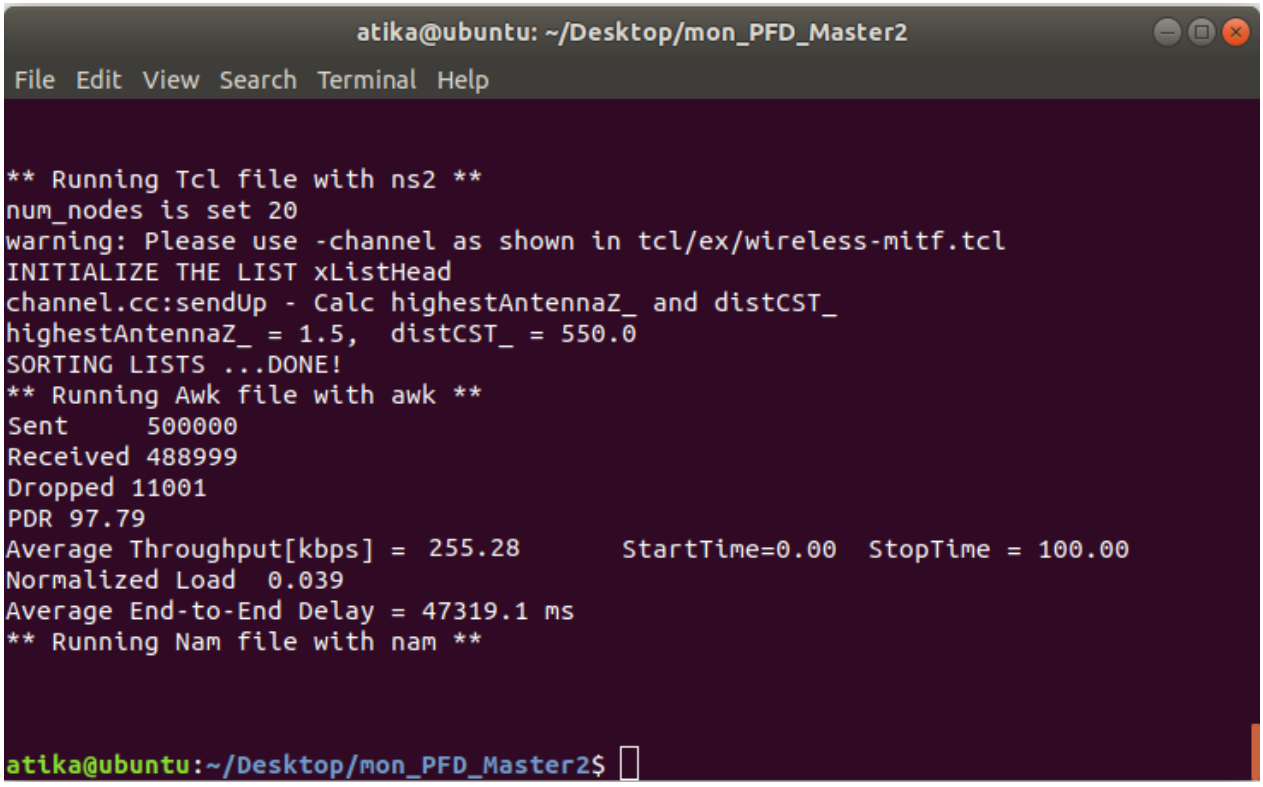


Figure 4.5 :Le fichier trace de AOMDV standard avec 20 nœuds.

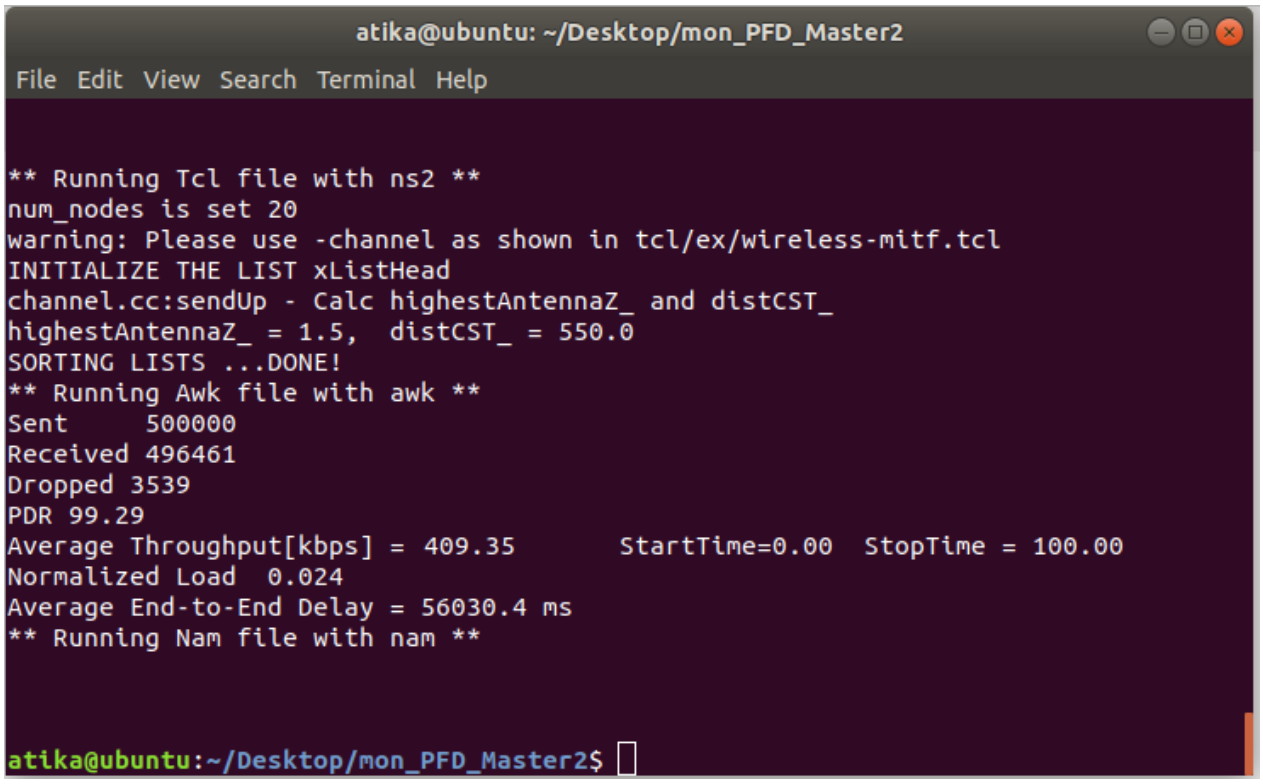


Figure 4.6 : Le fichier trace de AOMDV-SB proposé avec 20 nœuds.

4.5.1.1 Animation avec NAM

Dans les figures suivantes 4.7 et 4.8 on peut voir l'emplacement des nœuds et la variation des paquets dans network animateur :

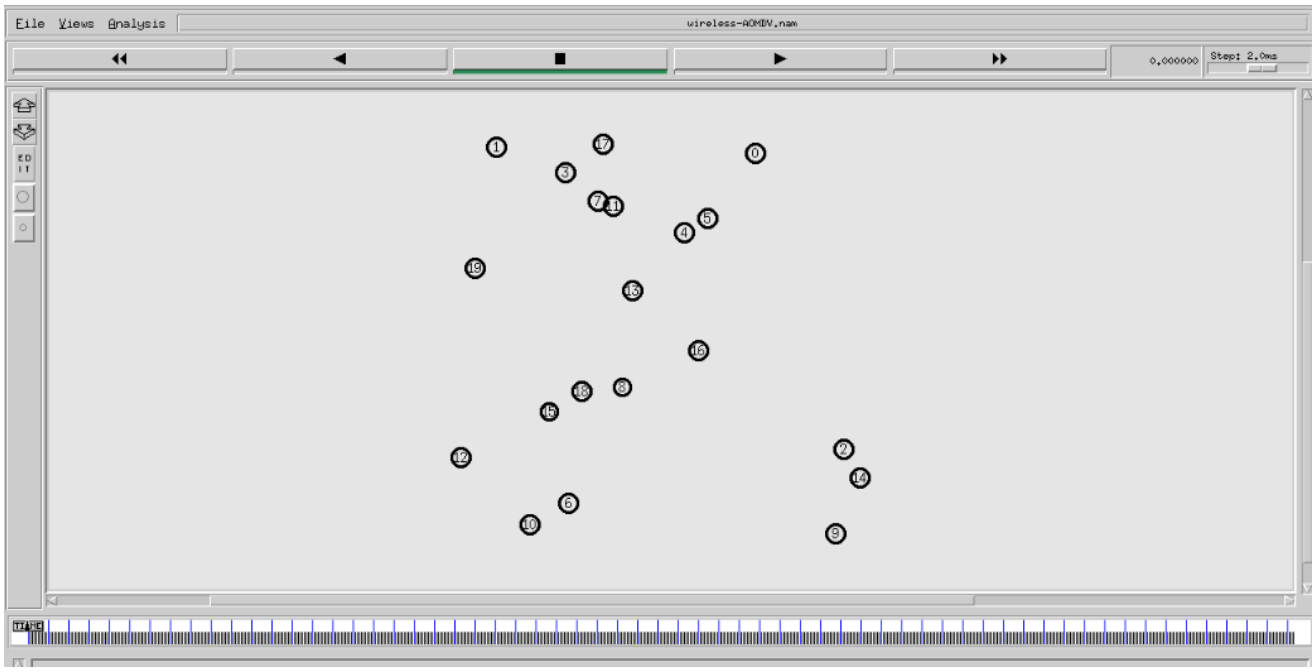


Figure 4.7 : L'emplacement des 20 nœuds.

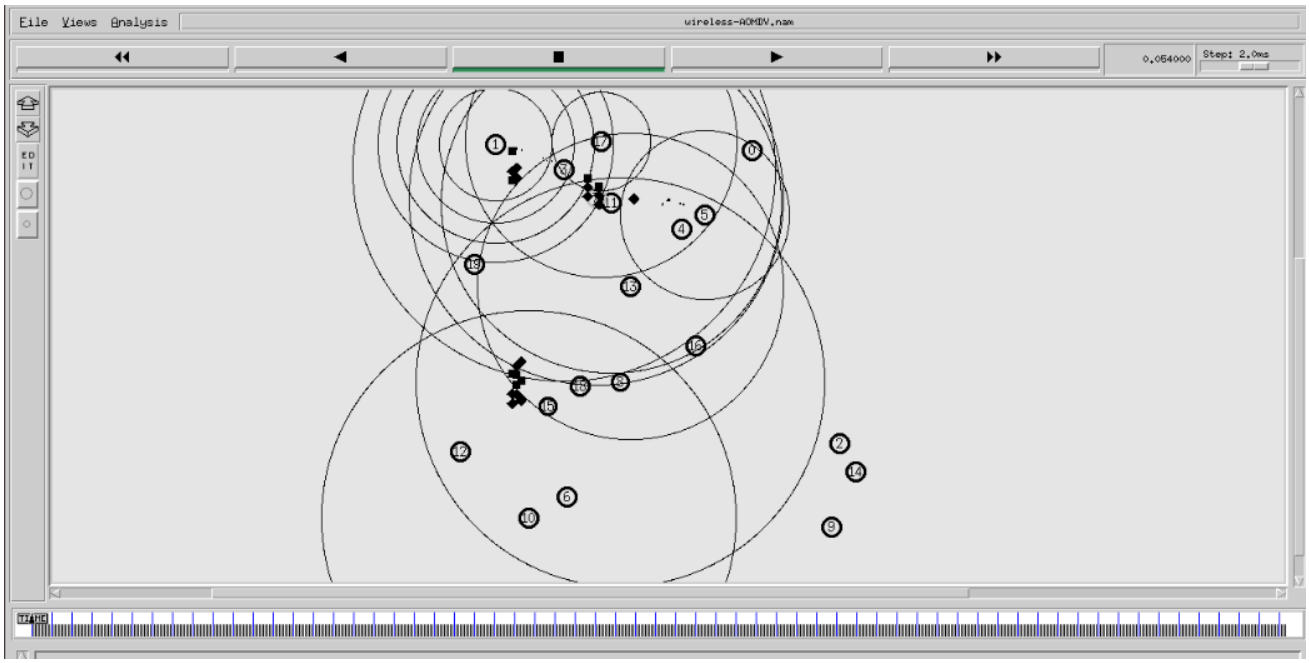


Figure 4.8 : Variation des paquets en fonction du temps.

4.5.1.2 Interprétation des résultats sous forme de tableau :

Les tableaux ci-dessous résume les paramètres de simulation mentionnés dans le ficher trace, par rapport aux paquets reçus, paquets envoyés, délai moyen de bout en bout, pourcentage de livraison de paquets…etc. Ces tableaux montrent que le protocole d'AOMDV-SB est beaucoup mieux par rapport à l'AODV par défaut malgré le délai moyen de bout en bout qui n'est pas optimisé par rapport au AOMDV.

Paramètres	Valeurs
Nombre de stations	**20**
Simulateur	**NS-2**
Protocole choisi	**AOMDV-SB**
MAC	**IEEE 802.11b**
Début de transmission des paquets (*Start Time, en seconde*)	**0.00**
Fin de transmission des paquets (*Stop Time, en seconde*)	**100.00**
Débit	**409.35 Kbps**
charge de routage normalisée	**0.024**
Délai moyen de bout en bout	**56030.4 ms**
Pourcentage de livraison de paquets	**99.29**
Nombre de paquet envoie	**500000**
Nombre de paquet reçu	**496461**
Nombre de paquet perdue	**3539**

Tableau 4.1 : Paramètres de simulation du protocole AOMDV-SB.

Ce tableau résume les paramètres de simulation du protocole AOMDV

Paramètres	Valeurs
Nombre de stations	**20**
Simulateur	**NS-2**
Protocole choisi	**AOMDV**
Début de transmission des paquets (*Start Time, en seconde*)	**0.00**
Fin de transmission des paquets (*Stop Time, en seconde*)	**100.00**
Débit	**255.28 Kbps**
charge de routage normalisée	**0.039**
Délai moyen de bout en bout	**47319.1 ms**
Pourcentage de livraison de paquets	**97.79**
Nombre de paquet envoie	**500000**
Nombre de paquet reçu	**488999**
Nombre de paquet perdue	**11001**

Tableau 4.2 : Paramètres de simulation du protocole AOMDV.

4.5.2. Scenario 2 : Varier le taux de débit des paquets pour voir comment les protocoles se comportent lorsque la charge est élevée avec 60 nœuds, les figures suivantes montre les fichier traces de cette simulation

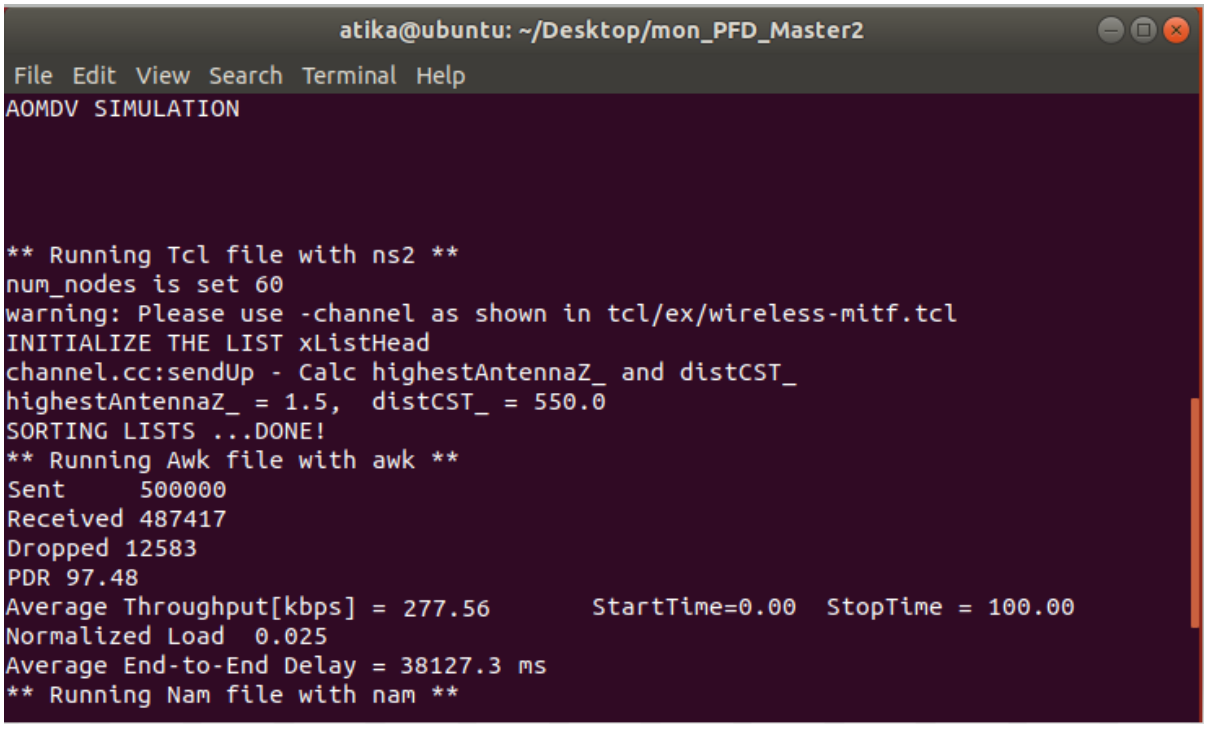


Figure 4.9 : Le fichier trace de protocole AOMDV avec 60 nœuds.

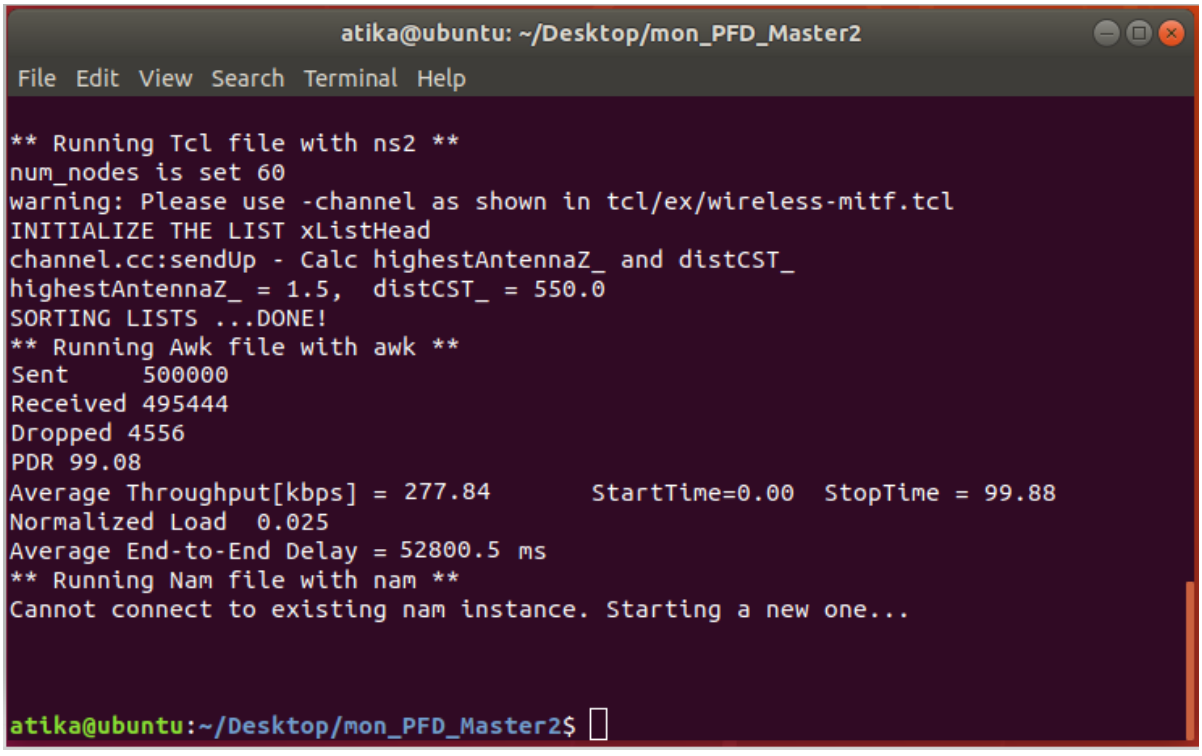


Figure 4.10 : Le fichier trace de AOMDV-SB avec 60 nœuds.

4.5.2.1 Animation avec NAM

Dans la figure suivante on peut voir l'emplacement des 60 nœuds et la variation des paquets dans network animateur

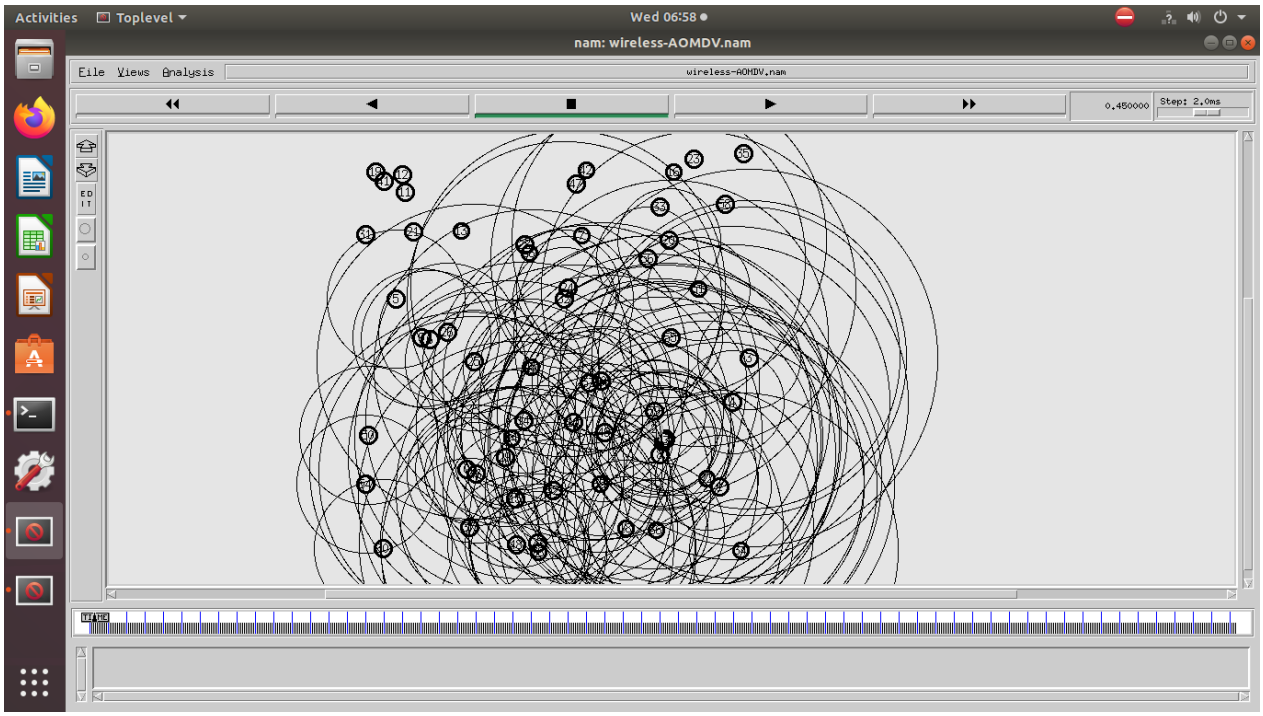


Figure 4.11 : Variation des nœuds en fonction de temps.

4.5.2.2 Interprétation des résultats sous forme de tableau :

Les tableaux ci-dessous résument les paramètres de simulation mentionnés dans le fichier trace, par rapport aux paquets reçus, paquets envoyés, délai moyen de bout en bout, pourcentage de livraison de paquets, etc… Ces tableaux nous montrent que le protocole d'AOMDV-SB est beaucoup mieux par rapport à l'AODV par défaut malgré le délai moyen de bout en bout qui encore n'est pas optimisé par rapport au AOMDV.

Dans ce tableau on peut voir les paramètres de simulation de AOMDV-SB avec 60 nœuds :

Paramètres	Valeurs
Nombre de stations	**60**
Simulateur	**NS-2**
Protocole choisi	**AOMDV-SB**
Début de transmission des paquets (*Start Time, en seconde*)	**0.00**
Fin de transmission des paquets (*Stop Time, en seconde*)	**100.00**
Débit	**277.84 Kbps**
charge de routage normalisée	**0.025**
Délai moyen de bout en bout	**52800.5 ms**
Pourcentage de livraison de paquets	**99.08**
Nombre de paquet envoie	**500000**
Nombre de paquet reçu	**495444**
Nombre de paquet perdue	**4556**

Tableau 4.3 : Paramètres de simulation du protocole AOMDV-SB.

Ce tableau décrit les paramètres de simulation de AOMDV avec 60 nœuds :

Paramètres	Valeurs
Nombre de stations	**60**
Simulateur	**NS-2**
Protocole choisi	**AOMDV**
Début de transmission des paquets (*Start Time, en seconde*)	**0.00**
Fin de transmission des paquets (*Stop Time, en seconde*)	**100.00**
Débit	**277.56 Kbps**
charge de routage normalisée	**0.025**
Délai moyen de bout en bout	**38127.3 ms**
Pourcentage de livraison de paquets	**97.48**
Nombre de paquet envoie	**500000**
Nombre de paquet reçu	**487417**
Nombre de paquet perdue	**12583**

Tableau 4.4 : Paramètres de simulation du protocole AOMDV.

4.6 Analyse des résultats sous formes des graphes avec l'application Xgraph

Dans ce qui suit, nous présentons les résultats de l'évaluation des performances de notre proposition sous forme de graphes illustratifs avec 20 noeuds (scenario 1). Pour faire une décision sur la qualité de ces performances, nous les comparons avec les performances de protocole AOMDV (AOMDV est déjà implémenter dans NS2)

4.6.1 Normaliser la charge de routage

La figure 4.12 présente la charge de routage normalisée (Normalized Load) en fonction de temps (seconde), elle nous montre que la charge de routage dans AOMDV-SB proposé est moins réduite par rapport à AOMDV tel que à la fin de la simulation on a obtenue dans

AOMDV= 0.039, par contre dans AOMDV-SB=0.024, d'où notre proposition prouve la performance de la charge de routage normalisée.

X : temps (seconde).
Y : Normalized load.

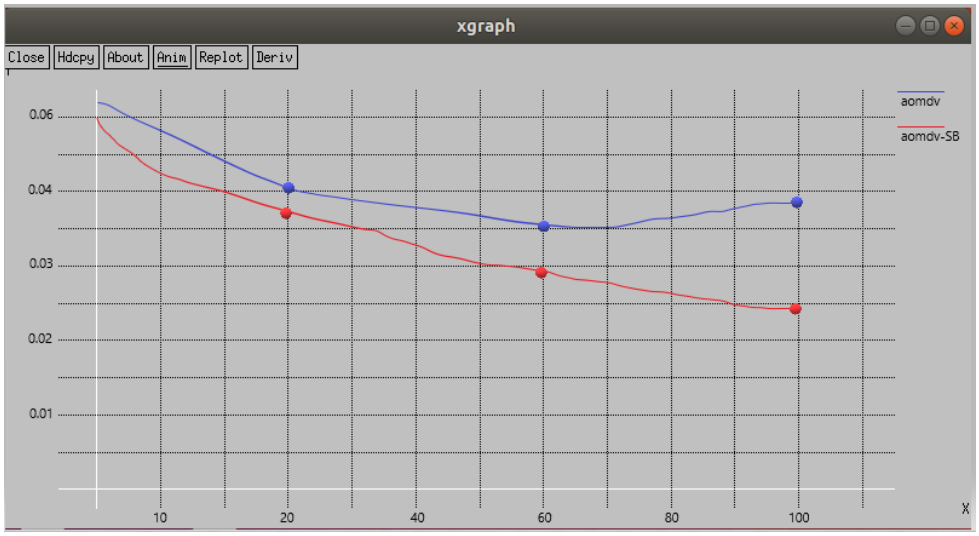


Figure 4.12 : Graphe comparatif de la charge normalisé.

4.6.2 Délai moyen de bout en bout

Dans ce graphe illustré dans la figure suivante nous pouvons observer clairement que le délai moyen de bout en bout dans notre proposition n'est pas satisfaisant, il est plus grand que dans le AOMDV.

Y = Average end to end delay (ms).
X = temps de pause (s).

La figure suivante montre le graphe dont la comparaison entre les deux protocoles :

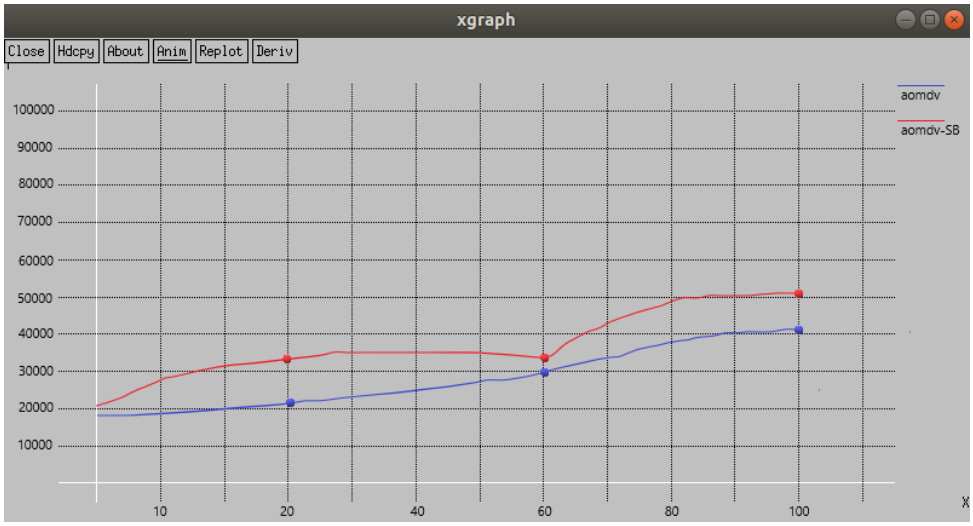


Figure 4.13 : Graphe comparatif du délai de bout en bout.

4.6.3 Pourcentage de livraison de paquets (PDR)

Le but général de notre proposition est de réduire la charge de routage au niveau maximum possible tout en maintenant le PDR(Packet Delivery Ratio) aussi proche que possible du protocole AOMDV. Les résultats obtenus montrent que PDR du AOMDV-SB est plus grand que celui de protocole AOMDV tel que à la fin de simulation AOMDV a livré 97.79 % des paquets envoyé et AOMDV-SB 99.29 % comme on le voit sur la figure 4.14.

X = temps de pause (s).

Y = pourcentage de livraison de paquet.

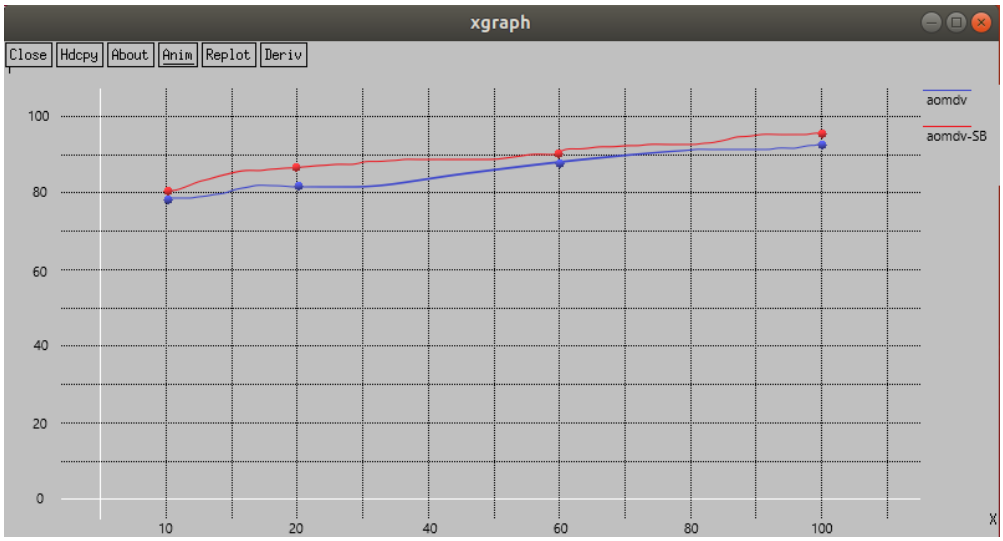


Figure 4.14 : Graphe comparatif de PDR.

4.6.4 Débit

La figure 4.16 montre que le débit (Average Throughput) augmente avec le temps dans les deux protocoles, on remarque que le débit de AOMDV-SB est plus fort que le débit de AOMDV standard, donc on conclut que le AOMDV-SB est meilleur car il s'adapte aux pannes dans le réseau plus rapide.

X = temps de pause (s).

Y = le débit (Kbts).

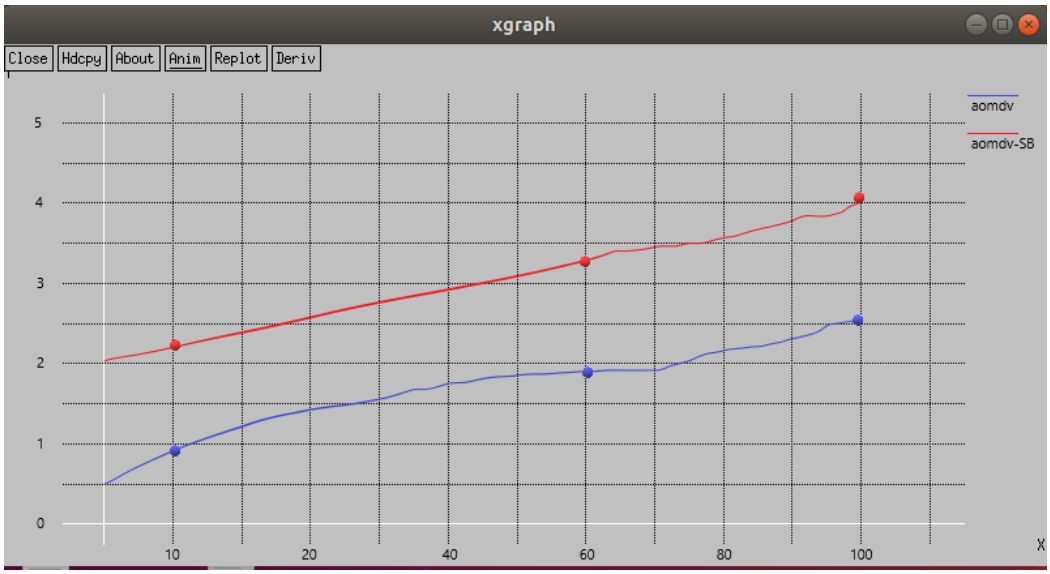


Figure 4.15 : Graphe comparatif de Débit.

4.7. Conclusion

Dans ce chapitre, nous avons proposé une fonction multicritère pour le calcul du cout minimum d'interférence de trafic et le degré de stabilité d'un itinéraire dans les réseaux MANET. Cette fonction a été implémentée dans le protocole multipath réactive AOMDV que nous avons appelé AOMDV-SB.

L'objectif est d'assurer, lors de la découverte du chemin, la sélection de chemins stables et fiables ainsi que garantir l'équilibrage de charge. La sélection repose sur quatre métriques : charge de routage normalisé, débit moyen, stabilité d'itinéraire et pourcentage de livraison de paquet.

Le but de ce travail est d'éviter les ruptures dans les liens fréquents qui provoquent la perte de paquets de données pour la maintenance des chemins et aussi, le tout pour un meilleur équilibrage de charge.

C'est clair d'après les résultats de simulation, on conclut que le protocole AOMDV-SB montre son efficacité et offre de meilleures performances (en termes de taux de paquets reçus et paquet perdue, pourcentage de livraison de paquets, surcharge de routage) face à AOMDV standard, que nous réalisons la simulation en évaluant ses performances via le simulateur de réseau NS2.

Conclusion générale

Au cours de ce mémoire, qui avait pour ambition d'étudier et d'évaluer les performances des protocoles de routage dans le réseau ah doc, réactif, proactif et hybride on a décrit les types de ces derniers et la différence entre eux, ainsi que leur caractéristique en insistant sur le but d´un protocole de routage qui est l´établissement de routes qui soient correctes et efficaces entre une paire quelconque d´unités. Par la suite on a présenté la notion d'équilibrage de charge qui est l'une des clés importantes pour améliorer la performance des réseaux Ad hoc. L'un de ses principaux objectifs est de garantir la stabilité du réseau et assurer la connexion de tous les nœuds d´un réseau ad hoc pour satisfaire les besoins des utilisateurs en termes de temps d'exécution de leurs applications, si cette notion n'est pas réalisable un problème très complexe se produira vu le dynamisme et l´évolution rapide de la topologie, en effet les unités mobiles sont dynamiquement et arbitrairement éparpillés d´une manière où l´interconnexion peut changer à tout moment.

Dans ce contexte, nous avons proposé une solution d'équilibrage de charges qui est générique et peut s'appliquer à tout type de réseau sans fil ad hoc et garantir la qualité de service en termes de stabilité des itinéraires dans MANET en introduisant une fonction de calcul de cout et la qualité de service (la stabilité d'un itinéraire) pour la sélection des chemins au protocole AOMDV, par l'ajout d'un nouveau champ dans les paquets de contrôle de AOMDV standard, qui renfermera la charge de la route. Cette modification nous a donné un nouveau protocole qu'on a appelé AOMDV-SB (pour Ad Hoc On Demand Multipath Distance Vector Stable Balancing), ou AOMDV avec équilibrage de charge et Stabilité d'Itinéraire.

Afin de valider l'approche proposée et atteindre notre objectif on a utilisé le simulateur NS2, qui nous a permis de présenter les résultats de la simulation dans le but de montrer l'apport de la solution proposée par rapport au protocole AOMDV-standard.
D'après les tests réalisés et les résultats qui ont étés récupérés, traités puis représentés dans des graphes, tableaux et fichier trace on a pu conclure que notre protocole AOMDV-SB est plus performant et plus adéquat pour la majorité des métrique étudié (stabilité d'itinéraire, débit, charge de routage normalisé et pourcentage de livraison de paquet). Par conséquent on a pas pu réalisé la métrique de délai moyen de bout en bout à cause de nouveau champ qu'on avait ajouté dans la table de routage qui calcule le coût d'interférence de trafic plus la stabilité d'un itinéraire qui prend plus de temps par rapport au AOMDV-standard qui ne le possède pas.

Dans le futur, Pour les perspectives de ce projet, on peut citer des idées qui guident les chercheurs de ce domaine :

- Ajouter d'autres paramètres comme l'état de la file d'attente et de vitesse de déplacement.
- Intégration de débit comme métrique de calcul de route dans autre protocole de routage réactif et proactif tel que: OLSR, DSR, DSDV, etc.
- Enrichir le calcul de cout avec d'autre métrique comme optimisation de la bande passante.
- Inclure un certain nombre de critères de sécurité et de gestion des ressources en énergie lors de la sélection des routes pour la transmission des données.

Bibliographie

[1] S. Guidoum, M. Hadiouche, « Etude et implantation d'un réseau wifi sécurise au sein de l'inped », mémoire fin d'étude, université mouloud Mammeri, Tizi-Ouzou, 2010-2011.

[2] T.Lemlouma , « Le routage dans les réseaux mobiles ad hoc », Mini projet, September 2000.

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

[4] A.Boudjaadar, « 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.

[5] D.Dhoutaut, « Etude du standard IEEE 802.11 dans le cadre des réseaux ad hoc : de la simulation à l'expérimentation », Thèse de doctorat, L'Institut national des sciences appliquées de Lyon, 11 Décembre 2003.

[6] B.Guizani, «Algorithme de clusterisation et protocoles de routage dans les réseaux ad hoc», Thèse de doctorat , Université de Technologie de Belfort-Montbeliard, avril 2012.

[7] K.B.Kredo, B. Mohapatra, «Medium access control in wireless sensor networks», Computer network 51(4), pp 961-994, 2007, rmatique, IFSIC-Rennes 1, 2009/2010.

[8] B.Khaled ET H.Ahmed,« Réseaux Wi-Fi ad hoc »,Mémoire d'ingéniorat, Institut de télécommunication d'Oran , Juin 2008.

[9] B.Abdelghani, « Routage avec QoS dans les réseaux mobiles Ad-Hoc », magistère en informatique, RESYD, Bejaia, 2008-2009.

[10] L. Gadoum, S. Haouari, « Modélisation Analytique de la norme IEEE 802.11e mode EDCA Bloc ACK avec les chaines de Markov », mémoire fin d'études, RESYD, université Bejaia, 2015-2016.

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

[12] N. Boukhechem, « Routage dans les réseaux mobiles ad hoc par une approche a base d'agents », Mémoire de fin d'études, Promotion 2007-2008.

[13] A.Bouthaina, Z.Hemaizia, « Un protocole de routage optimisé dans les réseaux Ad Hoc » MASTER, RESYD, Tbessa, 2015-2016.

[14] "IETF, Mobile Ad hoc Network (manet)". www.ietf.org/html.charters/manetcharter.html, date d'accés : 04/2020.

[15] N.Labraoui, « La sécurité dans les réseaux sans Fil Ad Hoc », thèse doctorat, université Tlemcen, année 2012.

[16] K.Ayad, « Sécurité du routage dans les réseaux Ad Hoc mobile », Mémoire magister, Novembre 2012.

[17] T.mounir , «Proposition d'un protocole à économie d'énergie dans un réseau hybride GMS & Ad hoc» ,Thèse doctorat, Université Oran ,année 2012.

[18] A.Hajami, « Sécurité du routage dans les réseaux sans fil spontanés : cas du protocole OLSR », Thèse doctorat, Université de Mohammed V Souissi, année 2011.

[19] A. Berraba, H.Hsaidi, « balancement de charge dans les réseaux ad hoc » mémoire fin d'études, université Abbou Bekr Blkaid,2012,2013.

[20] Y. Sadqi, M. Zaoui, « Les protocoles de routage mis en place dans le cadre de réseaux ad hoc mobiles (caractéristiques, comparaison) », Année universitaire, 2010 /2011.

[21] E. David, « Protocoles de routage réactifs pour l'optimisation de bande passante et la garantie de délai dans les réseaux ad hoc mobiles », Thèse de doctorat, Université de Toulouse, septembre 2008.

[22] K. Mehaoued, « les réseaux mobile », cour master 2, Université de Bejaia, janvier 2020.

[23] A. Darehshoorzadeh, Nastooh, T. Javan, M. Dehghan, M. khalili « LBAODV: A new load balancing multipath routing algorithm for mobile ah doc networks », juillet 2008.

[24] B. Guizanil, « Protocoles de routage dans les réseaux ad hoc » Thèse de doctorat, juillet 2012.

[25] A.Rani, « Load balanced routing in mobile ad hoc networks », Thèse de doctorat, Département d'ingénierie informatique institut national de technologie kurukshetra, Octobre 2009.

[26] M. Sedrati, L. Aouragh, L. Guettala, A. Bilami « Etude des Performances des Protocoles de Routage dans les Réseaux Mobiles Ad-Hoc », Article universitaire, Université El Hadj Lakhdar - Batna, 03-04 Novembre 2007.

[27] N. Badache, D. Djenourf, A. Derhab, T. Lemlouma « Les protocoles de routage dans les réseaux mobiles Ad Hoc », Article universitaire, Laboratoire des logiciels de base cerist, 2002.

[28] : D. Elorrieta, « Protocoles de routage pour l'interconnexion des réseaux Ad-Hoc et UMTS », Thèse de Magistère, Université Européen Bruxelles Wallonie, Juillet 2007.

[29] H. hassanein, Z. audry, « Routing with load balancing in wirless ah doc networks», article universitaire, Université Queen's.

[30] V. Kalaiyarasi, M. Tamilarasi, « Survey of load balancing routing protocols in MANET », Article universitaire, Revue internationale des technologies de la communication et de l'informatique, 02/11/2015.

[31] Bharadwaj, V. Kumar, A. Verma « A Review of Load Balanced Routing Protocols in Mobile Ad hoc Networks », article universitaire, Journal international des tendances et technologies de l'ingénierie, juillet-aout 2011.

[32] Définition de terme load balancing, www.webopedia.com/TERM/1/load_balancing.html, date d'accès :13/05/2020.

[33] M. Allali, « Ingénierie et contrôle du trafic dans les réseaux sans fil », Thèse de doctorat, université Oran science et technologie Mohamad Boudiaf, 2017 – 2018.

[34] R. AOUDJIT, « Répartition et Equilibrage de Charges dans les hôtes mobiles », Thèse de doctorat, université Mouloud Mammeri, Tizi-Ouzou.

[35] N. Sabrine, « Gestion de la mobilité dans les réseaux Ad Hoc par Anticipation des métriques de routage », Thèse de doctorat, Université de Paris Sud, juillet 2015.

[36] B.Abdelkrim, H.Saidi, « Balancement de charges dans les réseaux Ad Hoc », Master, Réseaux et Systèmes Distribués, Tlemcen, Juillet 2013.

[37] Dr.M.Tamilaras, «Survey of load balancing routing protocols in MANET », Article universitaire, Department of Computer Science Engineering, Published online: 02-11-2015

[38] A.berrabah, « Balancement des charges dans les réseaux ad hoc » , Article universitaire , laboratoire Systèmes et technologies de l'information et de la communication, Sidi-Bel-Abbès.

[39] L.Niar, « Analyse Graphique pour la surveillance dans un réseau de
Capteurs sans fils (RCSF)Simulateur : OMNET++ », Mémoire Magister, Informatique, option : Analyse, Commande et Surveillance des Systèmes, Juillet 2012.

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

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

[42] S. Vaton, T.Chonavel (TB),MTS445 : Modélisation et Simulation , chapitre 1, page pp .4. Mai 2014.

[43] site officiel de network simulator, http:/www.nsnam.org, date d'accès 09/2020.

[44] introduction à NS, université la Réunion, http:/www2.univreunion.fr, date d'accès 09/2020.

[45] A.Moussaoui, « Routage QOS et prédiction de rupture dans les réseaux ad hoc », Mémoire Magister en informatique , RESYD, Université Bejaia , 2005-2006.

[46] Y.khamayseh , G.Obeidat , M.Bani « Protocole de routage compatible avec la mobilité et la charge pour les Réseaux ad hoc », article universitaire king Saud , juillet 2011.

Résumé : Les réseaux mobiles ad-hoc (MANET) sont une technologie sans fil très prometteuse qui assure la communication et la mobilité entre les nœuds sans fil sans avoir besoin d'une infrastructure physique ou de dispositifs centralisés tels qu'un point d'accès ou une station de base. Les échange des données dans les réseaux ah-doc est réalisé à travers des protocoles de routage. Il existe différentes catégories de protocoles de routage qui ont des différents buts et objectifs (proactifs, réactifs, géographiques et protocoles de routage hybrides, etc.…)

Dans ce travail, nous proposons une nouvelle approche qu'on a appelé AOMDV-SB pour Ad Hoc On Demand Multipath Distance Vector Stable Balancing, qui est à la base le protocole AOMDV-standard avec l'ajout d'une fonction de calcul du cout qu'on a retiré dans le protocole LBAR et une qualité de servie qui est la stabilité d'itinéraire ceci a l'objectif de rendre le protocole AOMDV-standard plus performant et garantir la notion d'équilibrage de charge, car si cette dernière est inefficace ça va produira une augmentation de la surcharge de routage, un faible taux de livraison des paquets, un faible débit et d'autres paramètres de qualité de service (QoS).

Abstract : Mobile ad-hoc networks (MANETs) are a very promising wireless technology that provides communication and mobility between wireless nodes without the need for a physical infrastructure or centralized devices such as an access point or a base station. The exchange of data in the ah-doc networks is carried out through routing protocols. There are different categories of routing protocols which have different goals and objectives (proactive, reactive, geographic and hybrid routing protocols, etc…)

In this work, we propose a new approach that we called AOMDV-SB for Ad Hoc On Demand Multipath Distance Vector Stable Balancing, which is at the base of the AOMDV-standard protocol with the addition of a cost calculation function. which has been removed from the LBAR protocol and a quality of service which is the stability of the route, this has the objective of making the AOMDV-standard protocol more efficient and guaranteeing the notion of load balancing, because if the latter is is inefficient it will produce increased routing overhead, low packet delivery rate, low throughput, and other Quality of Service (QoS) parameters.