



République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et
de la Recherche Scientifique



Université De Akli Mohand Oulhadj – Bouira

Faculté des sciences et des Sciences

Appliquées

Département de Génie Electrique

Mémoire de Master

Spécialité : Technologies des Télécommunications

Thème

**QoS, Routage et prédiction des ruptures de
liens dans les réseaux Ad hoc**

Réalisé par :

**KECHKAR Housseem Eddine
DJEDDI Mohamed Diaa Eddine**

Encadré par :

Dr.SAOUD Bilal

Présenté le 22 septembre 2017 devant le jury composé de :

- **CHALABI Izzedine** (Président)
- **ISSAOUNI Salim** (Examineur)
- **TOUAFEK Med Yaakoob** (Examineur)

2016-2017

Remerciements

Nous remercions Allah notre Dieu qui nous a donné la force et la patience pour accomplir ce travail.

Nous tenons à exprimer nos remerciements à notre promoteur monsieur SAOUD Bilal Qui a mis toute sa compétence à notre disposition et pour son suivi régulier à l'élaboration de ce modeste travail, ses orientations, ses conseils qui nous ont servis de référence.

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

Nous désirons exprimer notre profonde et vive reconnaissance à Monsieur CHALABI Izzedine d'avoir accepté de présider le jury de Soutenance.

Nous adressons un grand merci à monsieur ISSAOUNI Salim ainsi le monsieur TOUAFEK Med Yaakoob pour l'honneur qu'il nous a fait en acceptant à examiner ce mémoire.

Nous tenons à remercier tous ceux qui ont contribué de près ou de loin à concrétiser ce travail.

Bien entendu, nous restons seuls responsables des erreurs et imperfections qui

Pourraient subsister dans ce mémoire.

Dédicace

Ce travail qui marque la fin de mes études pour l'obtention de mon diplôme de master 02, c'est le moment pour moi de partager cette joie avec les êtres qui me sont les plus chers dont beaucoup sont des guides pour la réussite de mes études.

A ma très chère mère qui m'a soutenue durant toute ma vie grâce à son amour, son affection et sa patience.

A mon très cher père qui grâce à ses sacrifices je suis devenu ce que j'ai toujours souhaité.

A mes frères que Dieu veuille sur eux. Bilalou, Salamou et Youyou la source de ma joie

A mes sœurs qui ne cessent de s'inquiéter pour me voir heureux Sarah l'aimable et Asmaa l'adorable

A toute ma famille KECHKAR et HAREM et surtout à mon frère Islam

A ma deuxième famille l'association KAFIL EL YATIM de Bouira particulièrement à Aicha, Dalila, Amel, Louiza, Saadoua, Amar, Sid Ali, Nabil et spécialement à Saadoune.

A tous mes chers amis :

Diaa et sa famille, de tous les moments passés ensemble à la fac en tant que binôme. Krimou, Omar, Nabil, Amir et Lynda qui ont toujours été à mes côtés

A tous mes collègues de ma promotion : Omar, Nacer, Sofiane, Abdellhadi, qui ont fait que toutes ces années d'étude sont passées si vite et si intensément.

*A tous celles et ceux qui connaissent Houssemer
Merci et qu'à l'avenir les liens ne se rompent pas.
J'espère les avoir rendu fiers.*

Houssemer Eddine

Dédicace

Ce travail qui marque la fin de mes études pour l'obtention de mon diplôme de master 02, c'est le moment pour moi de partager cette joie avec les êtres qui me sont les plus chers, dont beaucoup sont des guides pour la réussite de mes études.

A ma très chère mère, qui m'a soutenue durant toute ma vie grâce à son amour, son affection et sa patience.

A mon très cher père qui grâce à ses sacrifices, je suis devenu ce qui j'ai toujours souhaité.

A ma très chère mère qui m'a soutenue durant toute ma vie grâce à son amour, son affection et sa patience.

A mes frères que Dieu veille sur eux. Massi, Abdelmalek et Riad la source de ma joie

A mes sœurs qui ne cessent de s'inquiéter pour me voire heureux Hadjer et Djamila, Ferial, Lamia

A tous mes chers amis :

Housseem et sa famille, de tous les moments passés ensemble à la fac en tant que binôme. Amine, Nabil, Boubouh, Nasro, Amir de toujours me comprendre et à toutes nos longues discussions constructives.

A tous mes collègues de ma promotion

A ma deuxième famille l'association KAFIL EL YATIM de Bouira particulièrement à Aicha, Dalila, Amel, Louiza, Amar, Sid Ali, Nabil et spécialement à Saadoune.

*A tous celles et ceux qui connaissent Diaa
Merci et qu'à l'avenir les liens ne se rompent pas.
J'espère les avoir rendu fiers.*

Diaa Eddine

Résumé

Les réseaux MANET (Mobile Ad Hoc Network) constituent une catégorie de réseaux sans fil. Ces réseaux peuvent être déployés rapidement sans infrastructure donc les nœuds doivent jouer le rôle d'un routeur pour l'acheminement des données de la source vers la destination. Il existe plusieurs protocoles de routage pour assurer l'acheminement de l'information. Dans ce travail nous avons proposé une amélioration de protocole AODV qui est basée sur la puissance de signal dont deux algorithmes pour l'installation et la maintenance des routes entre les sources et les destinations. Une comparaison entre le protocole AODV et notre proposition qui a été faite sur le simulateur OPNET, les résultats obtenus montrent clairement l'efficacité de la nôtre en termes d'installation et maintenance des itinéraires.

Mot clés : MANET, protocole de routage, AODV, métriques de test, simulation

Abstract

MANET (Mobile Ad Hoc Network) is an important category of wireless networks. These networks can be deployed quickly without an infrastructure so the nodes must play the role of a router to route data from the source to the destination. There are several routing protocols for routing information. In this work, we proposed an improvement of AODV protocol. Our proposal is based on power signal between nodes. We proposed two algorithms for the installation and maintenance of roads between sources and destinations. A comparison between the AODV protocol and our proposal was made on the OPNET simulator. The results clearly show the efficiency of ours in terms of installation and maintenance of routes.

Keywords : MANET, routing protocol, AODV, test metrics, simulation

SOMMAIRE

Remerciements	I
Résumé	II
Dédicace	III
Liste des figures	V
Liste des tableaux	VI
Liste des abréviations	VII
Introduction générale	01

Chapitre 1 : Réseaux sans fil

1. Introduction	3
2. Réseau sans fil	4
2.1 Définition	4
2.2 Les catégories des réseaux sans fil	4
2.2.1 Selon la zone de couverture	5
2.2.1.1 Réseaux personnels sans fil (WPAN)	5
2.2.1.2 Réseaux locaux sans fil (WLAN)	6
2.2.1.2 Les réseaux métropolitains sans fil (WMAN)	6
2.2.1.3 Les réseaux sans fil étendu (WWAN)	6
2.2.2 Selon l'infrastructure	7
3. Réseau ad hoc (sans infrastructure)	8
3.1 Définition	8
3.2 Caractéristiques des réseaux ad hoc	10
3.2.1 Mobilité (Une topologie dynamique)	10
3.2.2 Equivalence des nœuds du réseau	10
3.2.3 Liaisons sans fil (Une bande passante limitée)	11
2.2.4 Autonomie des nœuds (Des contraintes d'énergie)	11
3.2.5 Vulnérabilité (Une sécurité physique limitée)	11
3.3 Avantage des réseaux ad hoc	11
3.4 Applications	12
4. Conclusion	12

Chapitre 2 : Protocoles de routages dans les réseaux Ad-hoc

1. Introduction	14
2. Le problème de routage dans les réseaux ad hoc	14
2.1 Les contraintes de routages dans les réseaux ad hoc	15
2.1.1 Minimisation de la charge du réseau	15
2.1.2 Offrir un support pour pouvoir effectuer des communications multipoints fiables	15
2.1.3 Assurer un routage optimal	15

2.1.4 Le temps de latence	16
3. Principe de fonctionnement du routage dans réseau Ad hoc	16
3.1 Gestion et transfert de l'information.....	17
3.1.1 Routage par la source et routage par la cible	17
3.1.2 La notion de "Multihopng"	17
3.1.3 L'inondation	18
3.1.4 Le concept de groupe.....	18
4. Les protocoles de routage ad hoc	19
4.1 Les protocoles proactifs.....	20
4.1.1 Le protocole de routage DSDV	21
4.1.2 Le protocole Global State Routing (GSR).....	23
4.1.3 Le protocole Fisheye State Routing (FSR).....	23
4.1.4 Optimised Link State Routing (OLSR)	23
4.2 Les protocoles de routage réactifs	24
4.2.1 Le protocole Dynamic Source Routing (DSR).....	24
4.2.2 Le protocole de routage AODV.....	25
4.2.3 Le protocole de routage Light-Wight Mobile Routing (LMR)	28
4.2.4 Le protocole de routage TORA (Temporally Ordered Routing Algorithm)	28
4.3 Les protocoles de routage hybride.....	28
4.3.1 Le protocole de routage ZRP	28
5. Conclusion.....	28

Chapitre 3 : Routage avec prédiction de rupture de lien

1. Introduction	30
2. Terminologie de protocole AODV.....	30
2.1 Route active	30
2.2 Diffusion.....	30
2.3 Destination.....	30
2.4 Nœud de transfert	30
2.5 Installation d'itinéraire	31
2.6 Route invalide.....	31
2.7 Nœud d'origine.....	31
2.8 Route inverse	31
2.9 Numéro de séquence.....	31
3. Format des paquets	31
3.1 Format de paquet de demande d'itinéraire (RREQ).....	31
3.2 Format de paquet de réponse RREP	32
3.3 Format de paquet Route Error (RERR).....	33
4. Proposition pour améliorer le protocole AODV.....	34

4.1 Stabilité d'itinéraire	34
4.2 Métrique basé sur la puissance de signal.....	34
4.3 Établissement d'itinéraire dans notre proposition	34
5. Les algorithmes du traitement de paquet.....	37
5.1 Algorithme 1 : Traitement de RREQ.....	37
5.2 Algorithme 2 : Traitement de RREP	38
6. Maintenance d'itinéraire	39
6.1 Zone de rupture.....	39
6.2 Algorithme de prédiction de rupture de route basé sur la puissance de signal.....	39
6.3 Réparation locale	40
6.4 Réparation de bout en bout.....	40
7. Conclusion	41

Chapitre 4 : Simulation et interprétation des résultats

1. Introduction	42
2. Simulation sur OPNET	42
2.1 Présentation du Simulateur OPNET	42
2.2 Les caractéristiques de simulateur OPNET	43
2.3 Principe de fonctionnement	44
2.4 Les avantages de l'utilisation du simulateur OPNET	44
3. Simulation	45
3.1 Random Waypoint(RWP)	46
3.2 L'environnement de simulation	46
3.3 Métrique de performances utilisées.....	47
4. Résultats	48
4.1 Les paquets de RERR	48
4.2 Les paquets de RREP.....	48
4.3 Les paquets rejetés.....	49
5. Conclusion	50
Conclusion et perspective.....	51
Bibliographie.....	52

Liste des figures :

Figure 1.1	Classification des réseaux sans fil.....	5
Figure 1.2	Le modèle des réseaux mobiles avec infrastructure.....	8
Figure 1.3	Modélisation d'un réseau ad hoc.....	9
Figure 1.4	Le changement de la topologie des réseaux ad hoc	10
Figure 1.5	Communication entre les nœuds	10
Figure 2.1	Le mécanisme d'inondation (Broadcast).	18
Figure 2.2	Différentes classes de protocole de routage Ad Hoc.....	20
Figure 2.3	La propagation du paquet RREQ	26
Figure 2.4	Le chemin pris par le paquet RREP (requête de réponse).....	27
Figure 3.1	Format de paquet RREQ	31
Figure 3.2	Format de paquet RREP	32
Figure 3.3	Format de paquet RERR	33
Figure 3.4	Format de paquet RREQ D'AODV modifié.....	35
Figure 3.5	Format de paquet RREP D'AODV modifié.....	36
Figure 3.6	Choix d'itinéraire utilisant la métrique basé sur la puissance de signal.....	36
Figure 3.7	Zone de rupture	39
Figure 4.1	OPNET VERSION 14.0.....	42
Figure 4.2	Fonctionnement d'OPNET.....	44
Figure 4.3	Le déplacement d'un nœud utilisant le Random Waypoint.....	46
Figure 4.4	L'environnement de simulation.....	47
Figure 4.5	Comparaison entre les paquets de RERR envoyés par AODV et AODV modifié	48
Figure 4.6	Les paquets de RREP envoyés par AODV et AODV modifié	48
Figure 4.7	Comparaison entre les paquets rejetés par AODV et AODV modifié.....	49

Liste des tableaux :

Tableau 1	Paramètre de simulation.....	45
-----------	------------------------------	----

Liste des abréviations :

AODV	Ad Hoc On-Demand Distance Vector
BF	Bellman Ford
BS	Base Station
DSDV	Dynamic destination Sequenced Distance Vector
DSR	Dynamic Source Routing
GSM	Global System for Mobile communication
GSR	Global State Routing
GPRS	General Packet Radio Service
HSR	Hierarchical State Routing
IETF	Internet Engineering Task Force
IP	Internet Protocol
LAN	Local Area Network
LMR	Light-Wight Mobile Routing
LP-WPAN	Low Power-Wireless Personal Area Network
MAC	Medium Access Control
MANET	Mobile Ad hoc Network
MIT	Massachsetts Institute of Technology
NFC	Near Field Communication
OLSR	Optimized Link State Routing Protocol
OPNET	Optimized Network Engineering Tools
OSI	Open Systems Interconnection
PDA	Personnel Data Assistant
QOS	Quality Of Service
RFID	Radio Frequency Identification
RREP	Route Reply
RREQ	Route Request
RERR	Route Error
RWP	Random Waypoint
SN	Sequence Number
TORA	Temporary Ordering Routing Algorithm
TTL	Temps d'expiration du paquet
UMTS	Universal Mobile Telecommunication System
Wi-Fi	Wireless Fidelity

WMAN	Wireless Métropolitain Area Network
WPAN	Wireless Personal Area Network
WWAN	Wireless Wide Area Network
ZRP	Zone Routing Protocol

Introduction
générale

Introduction générale

Les nouvelles technologies de l'information et de la communication sont des ensembles de technologies utilisées pour traiter, modifier et échanger des données. Elles sont devenues essentielles dans la vie ce que nécessite une évolution rapide de transmission sur des supports de communication qui servent à véhiculer les données entre un émetteur et un récepteur, en effet il y'a deux classes de support de transmission filaire et sans fil. Les supports de transmission filaires sont nombreux. Parmi ceux-ci, on distingue les supports métalliques, non métalliques. Les supports métalliques comme les paires torsadées et les câbles coaxiaux sont les plus anciens et les plus largement utilisés, ils transportent des courants électriques. Les supports de verre ou de plastique, comme les fibres optiques qui transmettent la lumière. Le deuxième type est les supports sans fil qui ont rendu la possibilité de l'accès au réseau partout et à tout moment sans avoir besoin de brancher les appareils communicants à une infrastructure, ce qui fait que les réseaux sans fils ont été créé pour permettre aux utilisateurs d'effectuer des communications de tel sorte à garder la connectivité des équipements [1].

Les réseaux mobiles sans fil peuvent être classés en deux classes : les réseaux avec infrastructure qui utilisent généralement le modèle de la communication cellulaire et les réseaux sans infrastructure ou les réseaux ad hoc.

Un réseau mobile ad hoc appelé généralement MANET (*Mobile Ad hoc Network*) est une collection de deux périphériques ou plus, interconnecté par une technologie sans fil. Ce réseau peut être formé Dynamiquement par les nœuds sans fil pour échanger des informations sans utiliser aucune infrastructure réseau fixe existante. Chaque Nœud joue un rôle de routeur pour l'acheminement des données (routage) [11].

Le routage est une stratégie d'acheminement des informations vers la bonne destination à travers un réseau de connexion de données. Le routage est effectué par un protocole qui garantit à n'importe quel moment l'établissement de route entre n'importe quelle paire de nœuds appartenant au réseau. Afin d'assure un échange de données d'une manière continue.

Les protocoles existants utilisent une variété de techniques afin de résoudre ce problème d'acheminement des données. Suivant ces techniques plusieurs classifications sont apparues, parmi lesquelles nous allons citer trois grandes catégories de protocoles : Proactifs (tables de routage mises à jour régulièrement) ; réactif (tables de routage établies sur demande) ; hybride (combinaison entre proactif – réactif) [25].

Notre objectif est basé sur l'étude de problème de routage dans les réseaux ad hoc en concentrant sur l'amélioration de protocole AODV. Le protocole de routage AODV est un protocole réactif basé sur le nombre de saut minimum, c'est un choix très important mais ce

n'est pas une meilleure technique pour une bonne stabilité des liens entre les nœuds qui nous amènent de proposer la question primordiale de ce travail : Comment améliorer les performances de ce protocole pour éviter les ruptures de routes dans les réseaux ad hoc ?

Ce travail propose une amélioration de protocole AODV (Ad Hoc On-Demand Distance Vector) qui nous a permis de faire une prédiction de ruptures de lien dans les réseaux ad hoc au lieu de les détecter. Pour faire cela il va falloir impérativement de changer les mécanismes de choix de route de protocole AODV et pour atteindre ce but on a proposé deux algorithmes qui sont basés sur la puissance du signal pour l'établissement d'itinéraire selon notre choix tout en modifiant les paquets de RREQ (Demande de route) et RREP (Réponse de route) et un algorithme de maintenance en exploitant les messages Hello pour assurer une longue durée de vie de liens.

Organisation de mémoire :

Le premier chapitre est un chapitre introductif des réseaux sans fil. Il définit les concepts de base pour plusieurs types de ces réseaux. Ce chapitre introduit aussi les réseaux mobiles Ad Hoc avec leurs caractéristiques, ces avantages et leurs applications.

Le deuxième chapitre présente le processus de routage avec les trois grandes familles de protocoles de routage. Dans les MANET on trouve les protocoles de routage : DSR, DSDV, OLSR, AODV etc. Notre étude se focalise sur ce dernier protocole (AODV).

Le troisième chapitre est consacré à la présentation de notre contribution pour améliorer le protocole AODV. Il propose deux algorithmes pour les traitements de paquet et un algorithme pour la prédiction de rupture de route.

Le dernier chapitre est consacré à la présentation de notre modèle de simulation afin de comparer les deux protocoles (AODV et AODV amélioré) qui comporte aussi une évaluation des Performances des deux algorithmes proposés.

Chapitre 1

Les Réseaux sans fil

1. Introduction

L'essor des technologies sans fil offre actuellement des perspectives importantes en télécommunications. Les réseaux sans fil présentent un moyen de communication qui permet la transmission de l'information à travers des unités de calculs portables qui ont des caractéristiques particulières (une faible capacité de stockage, une source d'énergie autonome). Comparant avec l'ancien environnement (l'environnement statique), le nouvel environnement résultant appelé l'environnement mobile, permet aux unités de calculs, une libre mobilité et il ne pose aucune limitation sur la localisation des utilisateurs, ces nouveaux environnements offrent une grande flexibilité d'emploi [1]. En particulier, ils permettent la mise en réseau des sites dont le câblage serait trop onéreux à réaliser dans leur totalité.

La mobilité est le nouveau mode de communication utilisé, mais elle génère des problèmes, tel que : les fréquentes déconnexions, un débit de communication modeste avec des sources d'énergie limitées [1].

Les réseaux sans fil nous envahissent sans que nous ayons la moindre sensation de leurs présences. Ces ondes radioélectriques parcourent les airs jusqu'à la limite de leur puissance.

Pour clarifier les problèmes d'interférences, de conflit, et d'écoute (car d'autres services comme les militaires les utilisent), des normes et des protocoles ont été mis en place. [8]

L'évolution des dispositifs de calcul et les progrès dans l'infrastructure de communication ont abouti à la croissance rapide des réseaux sans fil. Ceux-ci sont géographiquement étendus (GSM, Wi max), locaux (802.11, Zig bée) ou personnels (Bluetooth). On trouve également les NFC (Near Field Communication) utilisés pour de nouveaux services (paiement des transports, affichage d'informations contextuelles...) et des RFID qui permettent d'optimiser le fonctionnement des processus internes de l'entreprise, comme la logistique, la traçabilité ou la production par exemple.

On assiste à la croissance exponentielle des réseaux cellulaires qui sont basés sur la combinaison de technologies câblées et sans fil. Dans les réseaux cellulaires, comme les GSM, chaque antenne couvre un territoire défini et lors des déplacements de l'utilisateur le téléphone mobile change de cellule. On dit que ce type de réseau a une infrastructure fixe bien définie [1]. Le réseau ad hoc se caractérise par l'absence d'infrastructure pour les nœuds qui le composent.

Ce premier chapitre a pour but de définir le réseau sans fil avec une description de ces différentes catégories. Après avoir abordé une présentation générale sur les réseaux sans fils, ce chapitre est consacré aussi à la description des principales caractéristiques du réseau ad hoc.

2. Réseau sans fil

2.1 Définitions

Réseau est un concept qui mentionne la structure ayant une forme caractéristique. Le concept est utilisé pour nommer l'ensemble des équipements (ordinateurs) interconnectés qui partagent des services, des informations et des ressources.

Les systèmes dits sans fil, puisque sont des systèmes de communication qui n'utilisent pas de fils conducteurs électriques. Cela signifie que cette communication est établie sans faire appel à des câbles qui interconnectent physiquement les appareils. Donc il connecte différents postes ou systèmes entre eux par ondes radios [9].

Le réseau sans fil peut associer à un réseau de télécommunication pour réaliser des interconnexions entre nœuds .la norme la plus utilisée actuellement pour les réseaux sans fil est la norme IEEE802.11.

Le rayonnement géographique des ondes est relativement limité étant donné la faible puissance d'émission des solutions matérielles actuelles. Pour cette raison, les réseaux sans fils se sont avant tout développés comme réseaux internes, propres à un bâtiment, soit comme réseau d'entreprise, soit comme réseau domestique [1].

2.2 Les catégories des réseaux sans fils

Un réseau sans fil (Wireless network) est un réseau où au moins deux nœuds peuvent avoir une communication sans liaison filaire. Ces réseaux de communications permettent aux utilisateurs de profiter de tous les services traditionnels des réseaux indépendamment de leurs positions géographiques. Les réseaux sans fil peuvent avoir une classification selon deux critères. Le premier est la zone de couverture du réseau. Au vu de ce critère il existe quatre catégories : les réseaux personnels, les réseaux locaux, le réseau métropolitain et les réseaux étendus. Le second critère est l'infrastructure ainsi que le modèle adopté. Par rapport à ce critère on peut diviser les réseaux sans fils en : réseaux avec infrastructures et réseaux sans infrastructure, comme on le voit dans l'illustration de la figure suivante [2].

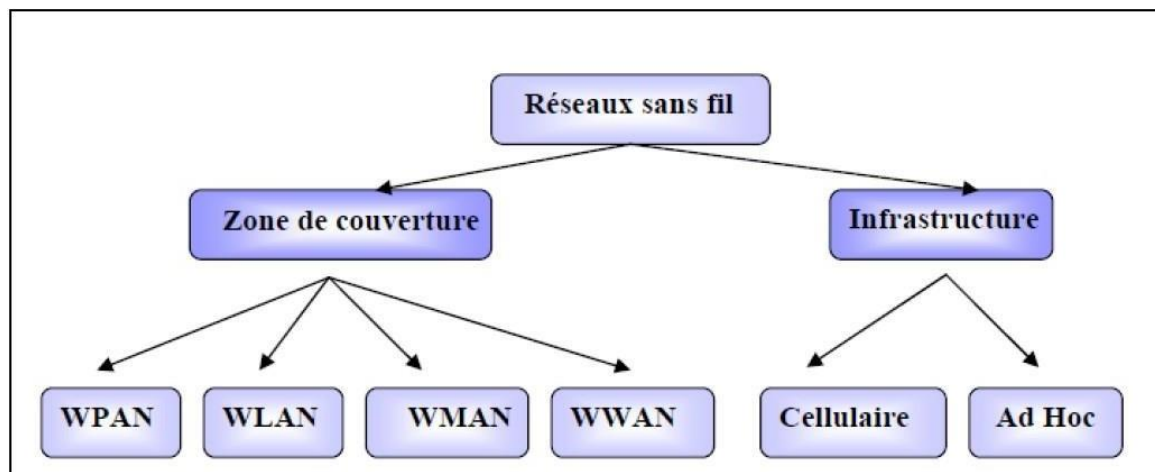


Figure 1.1 Classification des réseaux sans fil [2].

2.2.1 Selon la zone de couverture

2.2.1.1 Réseaux personnels sans fil (WPAN)

Le réseau personnel sans fil (appelé également réseau individuel sans fil ou réseau domestique sans fil et noté WPAN pour Wireless Personale Area Network) concerne les réseaux sans fil d'une faible portée : de l'ordre de quelques dizaines mètres. Ce type de réseau sert généralement à relier des périphériques (imprimante, souris et les appareils CVAC, thermostat ou bien à permettre la liaison sans fil entre deux machines très peu distantes [2].

Il existe plusieurs technologies utilisées pour les WPAN (Bluetooth, Wifi, NFC...) Dans cet article nous parlerons plus particulièrement du Bluetooth et Zig Bee.

Le Bluetooth est une technologie de réseau personnel sans fils, les appareils équipés du Bluetooth ne nécessitent pas d'être dirigés l'un vers l'autre pour communiquer, ce qui rend plus souple son utilisation et permet notamment une communication d'une pièce à une autre, sur de petits espaces. Chaque appareil doit disposer d'une puce électronique contenant le protocole Bluetooth.

L'objectif de Bluetooth est de permettre de transmettre des données ou de la voix entre des équipements possédant un circuit radio de faible coût, sur un rayon de l'ordre d'une dizaine de mètres à un peu moins d'une centaine de mètres et avec une faible consommation électrique[4].

Zig Bee est un LP-WPAN (Low Power-Wireless Personale Area Network) : c'est un réseau sans-fil à courte portée et à faible consommation énergétique. Autrement dit, c'est un protocole de communication sans-fil conçu par la Zig Bee Alliance basé sur la norme IEEE

802.15.4 qui définit les couches PHY (Physique) et MAC (Medium Access Control). ZigBee est donc un standard de communication sans-fils tout comme le Wifi ou le Bluetooth.

Il est utilisé aussi bien pour des applications grand public telles que celles liées à la domotique que pour des domaines plus liés aux communications sans fil en milieu industriel[6].

2.2.1.2 Réseaux locaux sans fil (WLAN)

Le réseau local sans fil correspond au périmètre d'un réseau local installé dans une entreprise, dans un foyer ou encore dans l'espace public. Il permet de relier entre eux les terminaux présents dans la zone de couverture du WLAN. On peut passer facilement d'un WLAN à l'autre comme l'on bascule d'une cellule à l'autre avec son téléphone mobile. En revanche, plusieurs WLAN peuvent être synchronisés et configurés de telle manière que l'effet de traverser plusieurs zones de couverture est pratiquement indécélable pour un utilisateur [3].

Le terme « Wi-Fi » (contraction de l'anglais « Wireless Fidelity ») désigne un protocole de communication sans fil dont le standard technique a été normalisé par le groupe IEEE 802.11. La norme Wi-Fi est une technologie de réseau informatique qui décrit les couches physiques et MAC d'interfaces réseau radio et infrarouge. Elle offre des débits allant jusqu'à 54 Mbps (tout dépend du milieu) sur une distance de plusieurs centaines de mètres suivant les techniques et les éventuelles extensions de la norme employée. Dans la pratique, le Wi-Fi permet de relier des ordinateurs portables, des ordinateurs fixes, des assistants personnels PDA (Personnel Data Assistant) ou tout type de périphérique à une liaison haut débit (11 Mbps ou supérieur).

Le Wi-Fi cible deux contextes d'utilisation distincts pour un réseau Wi-Fi ayant chacun des caractéristiques propres. Il s'agit du mode infrastructure et du mode ad hoc (sans infrastructure) [5].

2.2.1.3 Les réseaux métropolitains sans fil (WMAN)

Les réseaux métropolitains sans fil ou Wireless Métropolitain Area Network (WMAN) sont aussi connus sous l'appellation de boucle locale radio (BLR). Les réseaux basés sur la technologie IEEE 802.16 ont une portée de l'ordre de quelques dizaines de kilomètres (50km de portée théorique annoncée) et un taux de transmission radio théorique pouvant atteindre 74Mbit/s pour IEEE 802.16, plus connu sous le nom commercial de Wi MAX [2].

2.2.1.4 Les réseaux sans fil étendus (WWAN)

Le réseau étendu sans fils (WWAN pour Wireless Wide Area Network) est également connu sous le nom de réseau cellulaire mobile. Il s'agit des réseaux sans fils les plus répandus puisque tous les téléphones mobiles sont connectés à un réseau étendu sans fils. Les principales technologies sont les suivantes :

GSM (Global System for Mobile Communication ou Groupe Spécial Mobile) est une norme élaborée au cours des années 80 et 90 qui a défini les paramètres pour un réseau de communication cellulaire numérique. La norme GSM est utilisée pour les réseaux de communication sans fil à travers le monde.

GPRS (General Packet Radio Service) est un service de communication sans fil par paquets qui propose aux utilisateurs de téléphone mobile et d'ordinateurs des débits de 56 à 114 Kbp/s. Il est parfois appelé "2.5 G".

UMTS (Universal Mobile Telecommunication System) est un standard qui permet d'atteindre un débit de 10 Mbit/s en réception et de 5 Mbit/s en émission. Afin de faire transiter toutes ces données, une nouvelle bande de fréquences a été allouée à l'UMTS dans le spectre radio aux alentours de 2100 MHz.

Wimax (standard de réseau sans fils poussé par Intel avec Nokia, Fujitsu et Prowim). Basé sur une bande de fréquence de 2 à 11 GHz offrant un débit maximum de 70 Mbits/s sur 50 km de portée certains le placent en concurrent de l'UMTS même si ce dernier est destiné d'avantage aux utilisateurs itinérants [7].

2.2.2 Selon l'infrastructure

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

2.2.2.1 Réseaux cellulaires (avec infrastructure)

Ce type de réseaux se compose des éléments suivants [11] :

- Les "sites fixes" du réseau filaire.
- Les "sites mobiles", 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 comme le montre la figure suivante

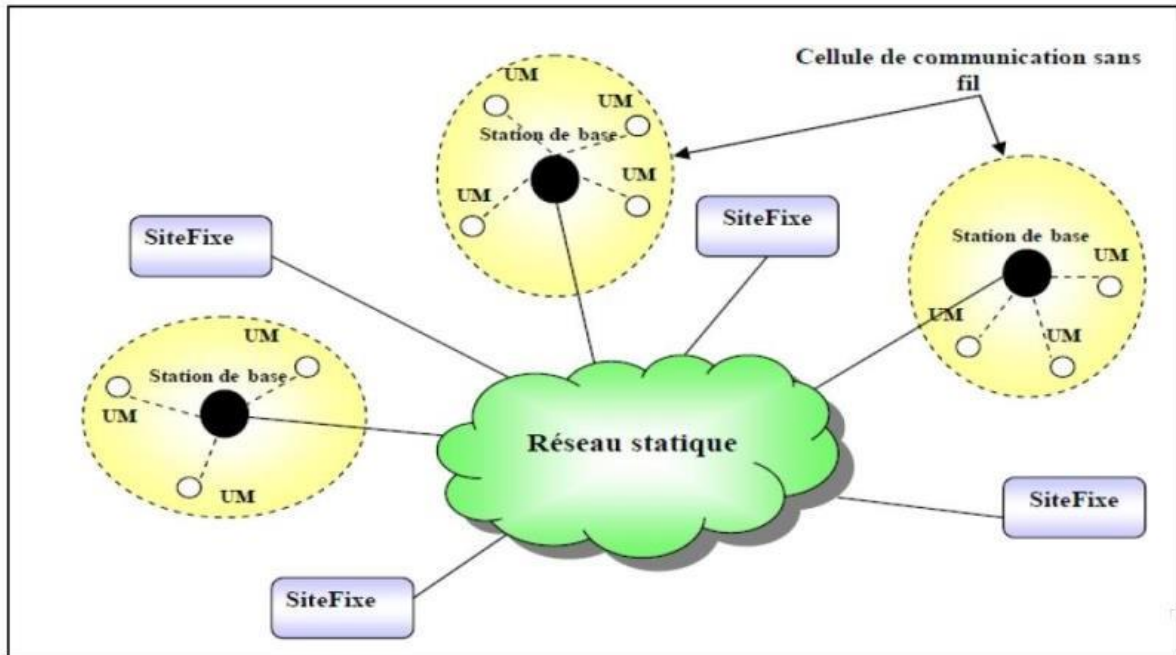


Figure 1.2 Le modèle des réseaux mobiles avec infrastructure [11].

Comme montre la figure 1.2 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 [11].

L'évolution récente de la technologie dans le domaine de la communication sans fil et l'apparition des unités de calculs portables (les lap tops par exemple) poussent aujourd'hui les chercheurs à faire des efforts afin de réaliser le but des réseaux.

3. Réseau ad hoc (sans infrastructure)

Le réseau mobile sans infrastructure également appelé réseau Ad hoc ou IBSS (Independent Basic Service Set) ne comporte pas l'entité « site fixe », tous les sites du réseau sont mobiles et se communiquent d'une manière directe en utilisant leurs interfaces de communication sans fil. L'absence de l'infrastructure ou du réseau filaire composé des stations de base oblige les unités mobiles à se comporter comme des routeurs qui participent à la découverte et la maintenance des chemins pour les autres hôtes du réseau [8].

3.1 Définition

La RFC 2501[15] de IETF (Internet Engineering Task Force) définit les réseaux mobiles ad hoc (appelés généralement MANET pour Mobiles Ad hoc Network) de la manière suivante: " Un réseau ad hoc est un système autonome de plates-formes mobiles (par exemple un routeur interconnectant différents hôtes et équipements sans fil) appelées nœuds qui sont libres de se déplacer aléatoirement et sans contraintes. Ceci provoque des changements rapides et prédictibles de la topologie du réseau, ce système peut fonctionner d'une manière isolée ou s'interfacer à des réseaux fixes à travers des passerelles. Dans ce dernier cas un réseau ad hoc est un réseau d'extrémité".

Modélisation : Un réseau mobile ad hoc peut être modélisé par un graphe $G_t = (V_t, E_t)$

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

E_t : modélise l'ensemble des connexions qui existent entre ces nœuds. (Figure 3).

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

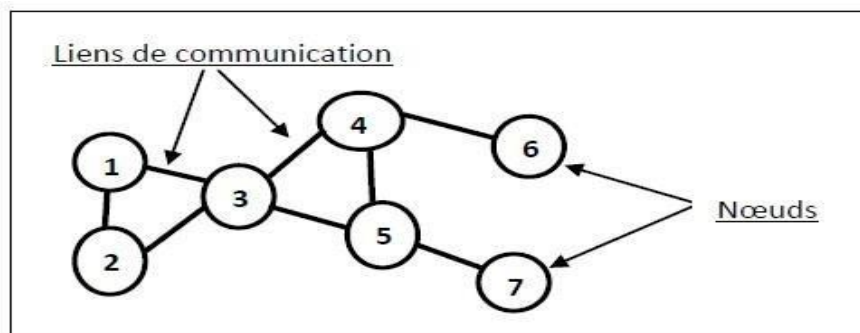


Figure 1.3 Modélisation d'un réseau ad hoc [11].

Un réseau ad hoc doit être facilement déployé les nœuds peuvent rejoindre et quitter le réseau de façon totalement dynamique sans devoir informer le réseau et si possible sans perturber les communications entre les autres nœuds du réseau [12].

La figure 1.4 montre que la topologie des réseaux ad hoc est dynamique et décentralisée, elle peut changer aléatoirement et les unités mobiles sont libres de se déplacer arbitrairement de ce fait la déconnexion de ces unités est très fréquente [12].

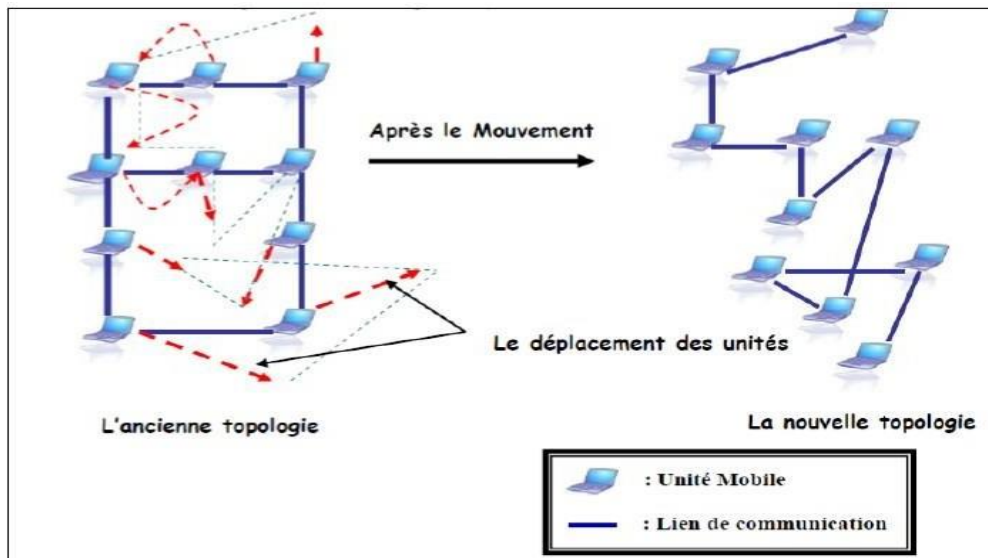


Figure 1.4 Le changement de la topologie des réseaux ad hoc [12].

Dans le cas le plus compliqué où un nœud voudrait communiquer avec un autre se trouvant hors de portée, chaque nœud du réseau peut alors servir de routeur. Dans la figure 1.5 ci-dessous le nœud A veut communiquer avec le nœud C se trouvant hors de son champ de réception. Pour aboutir la connexion réseau va donc utiliser le nœud B se trouvant à la fois à la portée de réception des nœuds A et C [12].

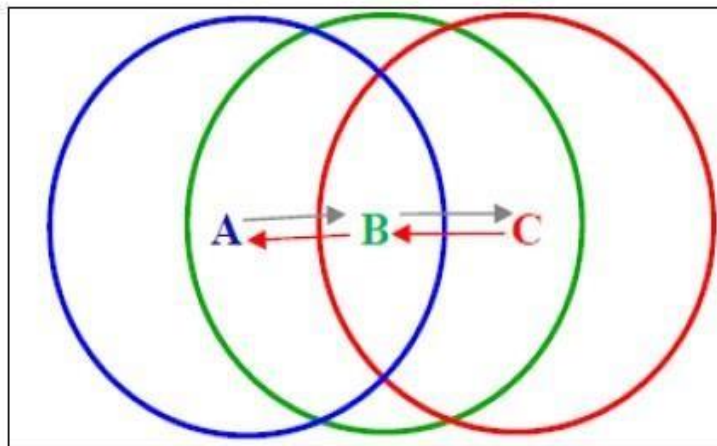


Figure 1.5 Communication entre les nœuds [12].

A partir de cette définition générale il est intéressant de mettre en avant les caractéristiques principales qui différencient un réseau ad hoc d'un réseau classique.

3.2 Caractéristiques des réseaux ad hoc

3.2.1 Mobilité (Une topologie dynamique)

La mobilité des nœuds constitue à l'évidence une caractéristique très spécifique des réseaux ad hoc. Cette mobilité est intrinsèque au fonctionnement du réseau. Dans un réseau ad hoc la topologie du réseau peut changer rapidement de façon aléatoire et non prédictible et les techniques de routage des réseaux classiques basées sur des routes préétablies ne peuvent plus fonctionner correctement [1].

3.2.2 Equivalence des nœuds du réseau

Dans un réseau classique il existe une distinction nette entre les nœuds terminaux (stations, hôtes) qui supportent les applications et les nœuds internes (routeurs par exemple) du réseau en charge de l'acheminement des données.

Cette différence n'existe pas dans les réseaux ad hoc car tous les nœuds peuvent être amenés à assurer des fonctions de routage [1].

3.2.3 Liaisons sans fil (Une bande passante limitée)

Les technologies de communications sans fil sont indispensables à la mise en place d'un réseau ad hoc. Malgré des progrès très importants leurs performances restent et resteront en dessous de celles des technologies des réseaux filaires. La bande passante est moins importante alors que le routage et la gestion de la mobilité génèrent davantage de flux de contrôle et de signalisation que dans une architecture de réseau filaire. Ces flux doivent être traités de façon prioritaire pour prendre en compte rapidement les modifications de topologie [1].

3.2.4 Autonomie des nœuds (Des contraintes d'énergie)

La consommation d'énergie constitue un problème important pour des équipements fonctionnant grâce à une alimentation électrique autonome. Ces équipements intègrent des modes de gestion d'énergie et il est important que les protocoles mis en place dans les réseaux ad hoc prennent en compte ce problème [1].

3.2.5 Vulnérabilité (Une sécurité physique limitée)

Les réseaux sans fil sont par nature plus sensibles aux problèmes de sécurité. Pour les réseaux ad hoc le principal problème ne se situe pas au niveau du support physique mais principalement dans le fait que tous les nœuds sont équivalents et potentiellement nécessaires au fonctionnement du réseau [1].

3.3 Avantage des réseaux ad hoc

Comme nous venons de le voir, contrairement à un réseau à infrastructure les réseaux ad hoc ou « réseaux à la volée » sont caractérisés par l'absence de contrôle centralisé. Ceci représente un acte avantageux car les nœuds dans un réseau mobile ad hoc sont libres de circuler et de s'organiser de manière non contraignante. Chaque utilisateur est libre de se déplacer tout en communiquant avec les autres. Le chemin entre chaque paire d'utilisateurs peut avoir des liens multiples et les liens entre eux peuvent être hétérogènes. Cela permet à une association de divers liens de faire partie du même réseau. Les réseaux ad hoc peuvent fonctionner de façon autonome et éventuellement être reliés à un réseau plus large comme l'Internet [10].

Les réseaux ad hoc sont adaptés pour une utilisation dans des situations où une infrastructure n'est pas disponible ou lorsqu'un déploiement n'est pas rentable. Des nombreuses utilisations possibles des réseaux mobiles ad hoc dans certains milieux d'affaires où la nécessité pour un traitement collaboratif pourrait être plus important en dehors de bureau qu'à l'intérieur comme dans une réunion d'affaires en dehors de bureau pour des clients succincts sur une mission donnée [10].

3.4 Applications

Les domaines d'applications de réseaux ad hoc : Les premières applications des réseaux ad hoc concernaient les communications et les opérations dans le domaine militaire. Cependant avec l'avancement des recherches dans le domaine des réseaux et l'émergence des technologies sans fil (ex : Bluetooth, IEEE 802.11 et Hyperplan) d'autres applications civiles sont apparues. Ainsi on distingue [10] :

- Les services d'urgence : opérations de recherche et de secours des personnes, tremblements de terre, incendies, inondations, dans le but de remplacer l'infrastructure filaire.
- Le travail collaboratif et les communications dans des entreprises ou bâtiments dans le cadre d'une réunion ou d'une conférence par exemple.
- Home network : partage d'applications et de communications des équipements mobiles.
- Applications commerciales : pour un paiement électronique distant (taxi) ou pour l'accès mobile à l'Internet, ou service de guide en fonction de la position de l'utilisateur.
- Réseaux de senseurs : pour des applications environnementales (climat, activité de la terre, suivi des mouvements des animaux, etc.) ou domestiques (contrôle des équipements à distance).

- Réseaux en mouvement : informatique embarqué et véhicules communicants. D'une façon générale, les réseaux ad hoc sont utilisés dans toute application où le déploiement d'une infrastructure filaire est trop contraignant soit parce qu'il est difficile à mettre en place ou parce que la durée d'installation du réseau ne justifie pas le recours au câblage à demeure[10].

4. Conclusion

Après avoir abordé le concept des environnements mobiles et l'utilisation de la technologie de communication sans fil. Nous avons vu dans ce chapitre l'évolution rapide qu'a connu la technologie sans fil récemment et qui a permis d'apparaître de nouveaux systèmes de communication, elle offre plus d'avantages que les systèmes classiques. Ces nouveaux systèmes ne maintiennent plus l'utilisateur à une localisation fixe mais lui permettent une libre mobilité.

Les environnements mobiles sont caractérisés par des changements de topologies avec l'instabilité de lien surtout si tous les utilisateurs du système sont mobiles ce qui est le cas pour les réseaux ad hoc. Ces limites transforment certains problèmes ayant des solutions évidentes dans l'environnement classique qui sont complexes et difficiles à résoudre.

Parmi ceux-ci figure le problème de routage pour cela on va traiter dans le prochain chapitre les protocoles de routage avec détails sur les caractéristiques et l'intérêt qu'apporte chaque protocole.

Chapitre 2

Protocoles de routages dans les réseaux Ad-hoc

1. Introduction

Comme nous avons déjà vu, un réseau MANET est un ensemble de nœuds mobiles qui sont dynamiquement et arbitrairement éparpillés d'une manière où l'interconnexion entre les nœuds peut changer à tout moment. Donc il est nécessaire de faire appel à un protocole de routage qui est défini par l'acheminement des informations vers la bonne destination à travers un réseau de connexion de donnée son but est d'assurer une stratégie qui garantit à n'importe quel moment d'un établissement de routes qui soit correcte et efficace entre n'importe quelle paire de nœuds Appartenant au réseau, en assurant l'échange des messages d'une manière continue.

Vu les limitations des MANET la construction des routes doit être faite avec un minimum de contrôle et de consommation de la bande passante. Dans la plupart des cas l'unité de destination ne se trouve pas obligatoirement dans la portée de l'unité source ce qui implique la nécessité de la mise en œuvre des protocoles.

Dans ce chapitre nous entamons le processus de routage et les trois classes de ces protocoles (Proactif, Réactif, Hybride) dans les MANET en présentant dans chaque catégorie quelques protocoles proposés par L'IETF(Internet Engineering Task Force), nous présenterons leurs principales caractéristiques et fonctionnalités qui permettent de garantir l'acheminement des données entre les différents nœuds.

2. Le problème de routage dans les réseaux ad hoc

Le problème du routage dans les réseaux ad hoc est le défi le plus difficile à effectuer car il s'agit d'une topologie du réseau qui peut changer fréquemment donc il faut découvrir une route optimale multi sauts qui relie deux nœuds quelconques du réseau.

Les contraintes les plus connues sont les changements de topologies et l'instabilité des liens, la capacité limitée de la bande passante. La longueur du chemin entre un nœud source et un nœud de destination ne peut pas être la seule métrique à améliorer. L'optimisation peut consister à une combinaison complexe de facteurs tels que le délai de bout en bout, la fiabilité et stabilité des liens ; la durée de vie du chemin ; la bande passante disponible sur les liens ; le niveau d'énergie dans les batteries [14].

Dans la pratique il est impossible qu'une hôte puisse garder les informations de routage concernant tous les autres nœuds dans le cas où le réseau serait volumineux. Certains protocoles, comme le DSR et l'AODV utilisent la sauvegarde des données de routage concernant une destination de donnée (dans le cas où la source ne possède pas déjà de telles informations). Cependant ces protocoles ne spécifient pas les destinations que les nœuds

doivent garder leurs données de routage. Le problème ne se pose pas dans le cas de réseaux de petites tailles car l'inondation (la diffusion pure) faite dans ces réseaux n'est pas coûteuse, par contre dans un réseau volumineux le manque des données de routage concernant les destinations peut impliquer une diffusion énorme dans le réseau et cela si on considère seulement la phase de découverte de routes. Le trafic causé par la diffusion dans ce cas est rajouté au trafic déjà existant dans le réseau ce qui peut dégrader considérablement les performances de transmission du système caractérisé principalement par une faible bande passante [13].

2.1 Les contraintes de routages dans les réseaux ad hoc

Le problème qui se pose dans le contexte des réseaux MANET est l'adaptation de la méthode d'acheminement utilisée avec le grand nombre d'unités existant dans un environnement caractérisé par de modestes capacités de calculs et de sauvegarde. Il semble donc important que toute conception de protocole de routage doit étudier les contraintes suivantes :

2.1.1 Minimisation de la charge du réseau

L'optimisation des ressources du réseau renferme deux autres sous problèmes qui sont l'évitement des boucles de routage et l'empêchement de la concentration du trafic autour de certains nœuds ou liens [15].

2.1.2 Offrir un support pour pouvoir effectuer des communications multipoints fiables

Le fait que les chemins utilisés pour router les paquets de données puissent évoluer ne doit pas avoir d'incidents sur le bon acheminement des données. L'élimination d'un lien, pour cause de panne ou pour cause de mobilité devrait idéalement augmenter le moins possible les temps de latence [15].

2.1.3 Assurer un routage optimal

La stratégie de routage doit créer des chemins optimaux et pouvoir prendre en compte différentes métriques de coûts (bande passante, nombre de liens, ressources du réseau,... etc.). Si la construction des chemins optimaux est un problème dur, la maintenance de tels chemins peut devenir encore plus complexe, la stratégie de routage doit assurer une maintenance efficace de routes avec le moindre coût possible [15].

2.1.4 Le temps de latence

Le temps nécessaire pour passer de la source vers la destination [16].

3. Principe de fonctionnement du routage dans réseau 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 de destination et par la faible bande passante offerte par les réseaux ad hoc et du fait de la diffusion des données, les protocoles de routages actuellement utilisés dans les réseaux filaires ne peuvent être utilisés sans modification dans les réseaux MANET. De fait de nouveaux protocoles de routage ont dû être développés. Le but principal pour ces protocoles de routage est le même temps minimisé de nombre de paquets de contrôle avec le taux de perte et la consommation d'énergie [17].

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

1. Découverte de l'information de routage

Cette étape permet de connaître les éléments nécessaires sur la topologie utilisée pour choisir un chemin qui peut atteindre le nœud de destination. En fonction de la quantité d'informations échangées les nœuds obtiennent une vue plus précisément de la topologie du réseau. Le protocole de routage est dans l'obligation d'optimiser l'envoi de ces informations car elles sont fortement consommatrices en bande passante et d'énergies [18].

2. Choix du chemin

Après la collecte des informations de routage obtenues, le protocole de routage peut choisir une route en fonction de certains critères. Pour les protocoles de types Meilleurs efforts (« Best effort ») le critère est le nombre minimum de sauts dans la route, le protocole choisit la route ayant le plus petit nombre de nœuds à traverser. Parmi les critères on trouve aussi le critère d'économie d'énergie. Il faut aussi qu'on ne trouve pas de boucle dans les routes choisies. La présence de boucles va rendre le chemin choisi inutilisable par ce que le paquet ne pourra pas atteindre la destination en consommant inutilement de la bande passante et l'énergie. Un protocole de routage peut créer deux sortes de boucles : les boucles provisoires et les boucles permanentes [19]. Les premières ont lieu pendant le temps transfert d'un message de routage durant ce temps, des destinations peuvent être mises à jour et d'autres non d'où la possibilité d'apparition d'une boucle. Elle permet au maximum la durée de traversée du réseau par un message

de routage. Le deuxième type est les boucles permanentes qu'elles sont reliées à des phénomènes du bouclage à l'infini [20]. Ces boucles peuvent consommer énormément de bandes passantes et par conséquent de l'énergie en plus.

3. Maintenance des routes

La topologie du réseau Ad hoc n'arrête pas d'évoluer avec le temps. De fait à cause de la nature mobile des nœuds, les routes sont dans l'obligation de changer avec la mobilité des nœuds. Une route doit éviter de rester longtemps invalide Car les paquets ne pourraient pas atteindre leur destination. Le protocole de routage doit prendre en considération ces changements et met à jour les routes qui viennent d'être coupées [17].

3.1 Gestion et transfert de l'information

Nous allons dans un premier temps faire un rapide rappel sur quelques notions essentielles de routage dans les réseaux avant de nous déverser sur les protocoles de routage dans la section suivante :

3.1.1 Routage par la source et routage par la cible

Dans les routages par la source ce sont les nœuds qui émettent les messages et déterminent la liste des nœuds dont les paquets doivent traverser. Par contre dans le cas du routage par la cible le nœud source signale qu'il souhaite transmettre un message et la destination l'informerait de la route à utiliser [21].

3.1.2 La notion de "Multihopping"

Les stratégies de routage utilisées dans les réseaux Ad hoc sont caractérisées par le fait de pouvoir acheminer les paquets de données sans l'aide des stations de base utilisées dans la communication cellulaire (*Base Station, Mobile Station*).

Dans le modèle cellulaire, la communication entre deux nœuds est faite en utilisant les stations de base (*Base Station*) par conséquent aucune unité mobile n'est utilisée comme routeur intermédiaire, le modèle cellulaire est dit alors "*Single Hop*" (i.e. le nombre de routeurs mobiles intermédiaires est nul). La contrepartie de ce modèle est le modèle de communication sans infrastructure. Dans ce modèle plusieurs nœuds peuvent participer au routage c'est pour cela que l'environnement des réseaux Ad hoc est dit "*Multihop*" (i.e. le nombre de stations mobiles qui peut être utilisé comme routeurs intermédiaires peut dépasser un) [22].

3.1.3 L'inondation

L'inondation ou la diffusion pure (Broadcast) consiste à faire propager un paquet (de données ou de contrôle) dans le réseau entier. Un nœud qui initie l'inondation envoie le paquet à tous ses voisins directs. De même si un nœud quelconque du réseau reçoit le paquet il le rediffuse

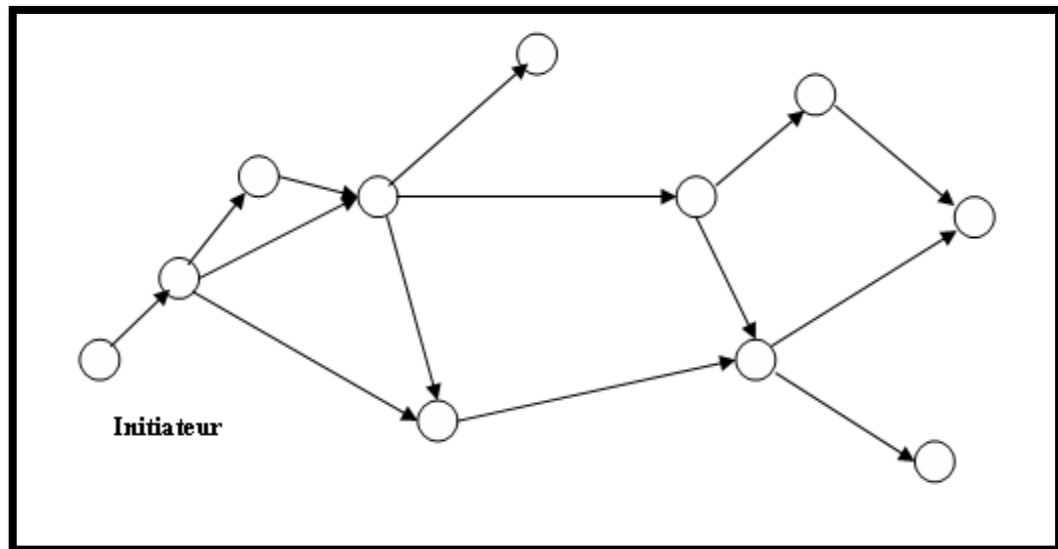


Figure 2.1 Le mécanisme d'inondation (Broadcast) [23].

Ce comportement se répète jusqu'à ce que le paquet atteigne tous les nœuds du réseau notons que les nœuds peuvent être amenés à appliquer durant l'inondation à certains traitements de contrôle dans le but d'éviter certains problèmes tels que le bouclage et la duplication des messages.

Le mécanisme d'inondation est utilisé généralement dans la première phase du routage plus exactement dans la procédure de découverte des routes et cela dans le cas où le nœud source ne connaît pas la localisation exacte de la destination. Un paquet de requête de route est inondé par la source afin qu'il atteigne la station de destination. Il faut noter que l'inondation est très coûteuse surtout dans le cas où le réseau est volumineux (latence, surcharge des messages...etc.), c'est pour cela que les protocoles de routage essaient de minimiser au maximum la propagation des paquets inondés en rajoutant d'autres paramètres de diffusion [23].

3.1.4 Le concept de groupe

Dans la communication de groupes les messages sont transmis à des entités abstraites ou groupes, les émetteurs n'ont pas besoin de connaître les membres du groupe destinataire. La communication de groupe a fait déjà l'objet de nombreux travaux principalement dans le cadre des projets ISIS, TRANSIS et HORUS. La gestion des membres d'un groupe dynamique permet

à un élément de se joindre à un groupe, de quitter ce groupe, se déplacer ailleurs puis rejoindre le même groupe. C'est en ce sens que la communication de groupe assure une indépendance de la localisation ce qui la rend parfaitement adaptée à des topologies de réseaux reconfigurables telles que les architectures avec sites mobiles. [24]

Le concept de groupe facilite les tâches de la gestion du routage (telles que les transmissions des paquets, l'allocation de la bande passante, la réutilisation spatiale,...etc.) et cela en décomposant le réseau en un ensemble de groupes connectés mais indépendants du point de vu contrôle. [24]

4. Les protocoles de routage ad hoc

Comme nous avons déjà vu les réseaux ad hoc se caractérisent par une absence d'infrastructure et de gestion centralisée. Dans ce type de réseaux chaque élément peut bien évidemment émettre et recevoir des messages mais assure également un rôle de relais de l'information afin que les messages circulent dans le réseau de proche en proche. Chaque nœud du réseau doit donc posséder des capacités de routage, c'est le routage dit ad hoc.

Grâce à ce routage, la portée radio d'un nœud peut être virtuellement étendue en utilisant ses voisins comme relais de l'information. La problématique du routage de l'information dans ce type de réseau est complexe. En effet les réseaux ad hoc sont souvent peu stables :

- * Les nœuds peuvent être mobiles ;
- * Les nœuds peuvent entrer et sortir du réseau à tout moment soit parce qu'ils s'éteignent soit parce qu'ils sortent de la portée radio de nœuds du réseau ;
- * Les ressources des nœuds sont souvent limitées (capacité de calcul, énergie...) car ce sont des équipements embarqués légers et mobiles ;
- * Les liens radio peuvent être asymétriques, l'information passe dans un sens mais pas dans l'autre (à cause des irrégularités des ondes électromagnétiques).

Il existe différentes méthodes pour résoudre cette problématique qui correspond à autant de protocoles de routage différents. Classiquement trois grandes familles de protocoles peuvent être distinguées : les proactifs, les réactifs et les hybrides. Les protocoles proactifs se comportent comme les protocoles de routage des réseaux filaires : les routes pour atteindre les nœuds du réseau sont maintenues en permanence et stockées dans des tables de routage au niveau des nœuds. Les protocoles réactifs ou "On Demand" ne calculent pas les métriques de routage avant qu'il n'y ait une demande par un nœud pour une transmission. Les routes sont donc uniquement cherchées à la demande. Les protocoles hybrides mélangent les techniques des deux précédents [25].

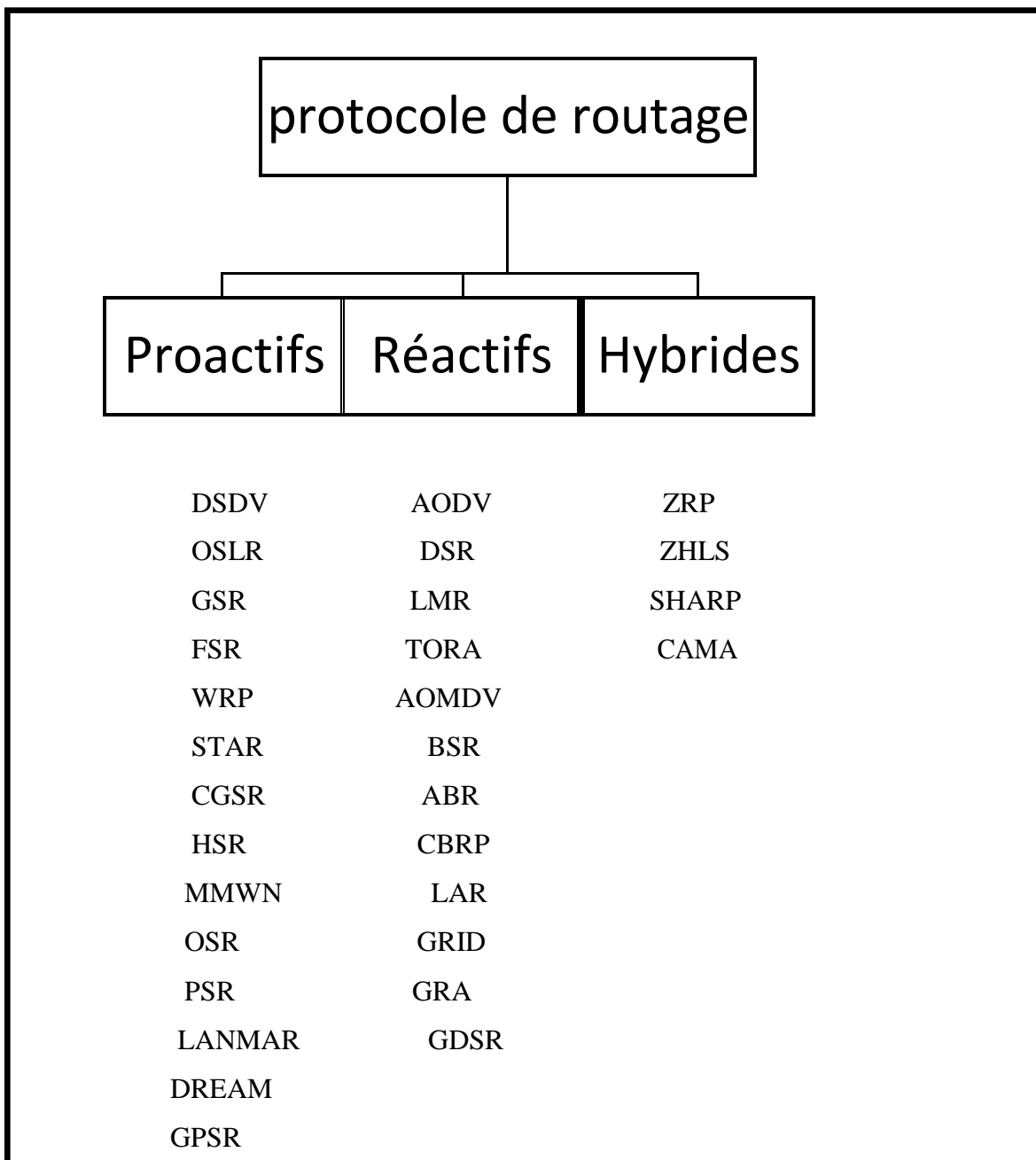


Figure 2.2 Différentes classes de protocole de routage Ad Hoc

Dans les paragraphes suivants on va représenter quelques protocoles de ces différentes familles avec leurs principales caractéristiques

4.1 Les protocoles proactifs

Les protocoles de routage proactifs tentent de maintenir à jour dans chaque nœud les informations de routage concernant tous les autres nœuds du réseau. Il nécessite ainsi que chaque nœud maintient une ou plusieurs tables pour stocker les informations de routage qui grandissent avec la taille du réseau. Ils répondent aux changements de topologies du réseau en

propageant à chaque voisin les mises à jours des routes afin que chacun puisse maintenir une vue consistante du réseau.

Cette politique de routage est proche de celle des réseaux filaires actuels basés sur des méthodes de vecteur de distance ou d'état de lien où chaque nœud maintient une vision globale de la topologie. Cette famille convient donc bien aux applications interactives mettant en scène chaque nœud du réseau.

Les différences entre les protocoles membres de cette famille se situent au niveau du nombre de table nécessaire pour stocker l'information et la manière dont ils propagent les changements de topologie.

Malheureusement ces protocoles atteignent rapidement leurs limites avec l'accroissement du nombre de nœuds et de leur mobilité. Les changements de topologies sont fréquents, le réseau sera ainsi constamment inondé par les paquets de contrôle qui ne se propagent pas assez vite pour que chaque nœud soit informé à temps des changements. Il en résulte des incohérences dans les tables un problème de convergence du réseau et une bande passante réduite par la surcharge des paquets de mise à jour.

Cette famille de protocole est ainsi limitée à des réseaux de petites tailles avec une faible mobilité et où chaque nœud a besoin d'être en permanence connecté avec les autres membres du réseau [26].

Dans le prochain paragraphe nous présentons quelques exemples de protocoles proactifs :

4.1.1 Le protocole de routage DSDV

L'algorithme de routage appelé "Vecteur de Distance à Destination Dynamique Séquencée" ou DSDV (Dynamic Destination-Sequenced Distance-Vector) a été conçu spécialement pour les réseaux mobiles. Il est basé sur l'idée classique de l'algorithme distribué de Bellman-Ford, DBF, en y apportant des solutions à ses éventuels problèmes. Ce protocole fonctionne de façon suivante :

Chaque nœud maintient une table de routage qui contient :

- Toutes les destinations possibles.
- Le nombre de saut nécessaire pour atteindre la destination.
- Le numéro de séquences (SN : Sequence Number) qui correspond à un nœud de destination. Afin de maintenir la solidité des tables de routage dans une topologie qui varie rapidement, chaque nœud du réseau transmet périodiquement sa table de routage à ses voisins directs. Le nœud peut aussi transmettre sa table de routage si le contenu

de cette dernière subit des changements significatifs par rapport au dernier contenu envoyé.

La mise à jour doit permettre à un nœud de pouvoir localiser dans la plupart des cas une autre unité de réseau.

La mise à jour de la table de routage peut se faire de deux façons :

- Une mise à jour complète.
- Une mise à jour incrémentale.

Dans la mise à jour complète le nœud transmet la totalité de la table de routage aux voisins ce qui nécessite l'envoi de plusieurs paquets de données alors que dans une mise à jour incrémentale juste les entrées qui ont subi un changement par rapport à la dernière mise à jour sont envoyées ce qui réduit le nombre de paquets transmis.

Un paquet de mise à jour contient :

- a. Le nouveau numéro de séquence incrémenté du nœud émetteur et pour chaque nouvelle route .
- b. L'adresse de la destination.
- c. Le nombre de nœuds (ou de sauts) séparant le nœud de la destination.
- d. Le numéro de séquence (des données reçues de la destination) tel qu'il a été affranchi par la destination.

Les données de routage reçues par un nœud sont comparées avec les données déjà disponibles. La route étiquetée par la plus grande valeur du numéro de séquence (i.e. la route la plus récente) est la route utilisée. Si deux routes ont le même numéro de séquence alors la route qui possède la meilleure métrique (nombre de sauts) est celle qui sera utilisée. Les modifications faites sur les données de routage locales sont immédiatement diffusées à l'ensemble courant des voisins. Les routes reçues par une diffusion seront aussi envoyées quand le récepteur procédera à l'envoi de ses paquets de routage. Le récepteur doit incrémenter les métriques des routes reçues avant l'envoi car il représente un nœud en plus il participe dans l'acheminement des messages vers la destination. Un lien rompu est matérialisé par une valeur infinie de sa métrique, i.e. une valeur plus grande que la valeur maximale permise par la métrique.

Parmi les améliorations apportées au DBF classique le concept de numéro de séquence qui permet à tout moment de se renseigner sur la validité des routes qui ont permis au DSDV de résoudre le Problème de boucle de routage et du comptage à l'infini. Comme tout protocole de routage proactif le DSDV connaît la route ponctuellement au même moment où un nœud doit procéder à une transmission ce qui permet d'être efficace en délais de transmission.

Cependant ce protocole ne résout pas la lenteur de la convergence des tables qui héritent du DBF à l'échange périodique des tables de routage, pour maintenir les routes même si elles ne

seront pas utilisées génèrent un nombre de paquet de contrôle énorme. Pour finir les auteurs de ce protocole l'ont renoncé aux profits de l'AODV [27].

4.1.2 Le protocole Global State Routing (GSR)

Ce Protocole est similaire à DSDV. Il est basé aussi sur la méthode d'état des liens et utilise une vue globale du réseau. Mais GSR améliore ces deux algorithmes (l'algorithme DSDV et l'algorithme à état de liens) en évitant l'inondation des messages car il utilise une méthode de dissémination de BF qui implique l'absence d'inondation [28]. La façon dont les informations de routage circulent dans le réseau est la différence clé entre l'algorithme GSR et l'algorithme à état de liens. La maintenance dans GSR de la table la plus récente est effectuée à partir de l'échange périodique d'état des liens à travers les voisins locaux uniquement [29].

4.1.3 Le protocole Fisheye State Routing (FSR)

Ce protocole est une amélioration du protocole GSR, il est basé sur la technique "œil de poisson" (fisheye). Dans GSR une grande quantité de la bande passante est gaspillée à cause de la grande taille des messages de mise à jour [30].

Par contre dans FSR les messages de mise à jour contiennent des informations sur les nœuds les plus proches en réduisant la taille de ces messages. Ainsi la précision de l'information diminue quand la distance du nœud augmente [29].

4.1.4 Optimised Link State Routing (OLSR)

Le protocole OLSR est un protocole à état de liens qui forme des routes de plus court chemin. Contrairement aux algorithmes traditionnels de routage à état de liens dans lesquels chaque nœud diffuse sur tout le réseau les liens directs qu'ils ont avec leurs voisins dans le protocole OLSR, les nœuds ne déclarent qu'une sous-partie de leur voisinage grâce à la technique des relais multipoints. Ces derniers sont des nœuds qui n'ont pas la connaissance de nœud pertinents. Les nœuds considèrent comme redondants pour le calcul des plus courts chemins ne font pas partis de la liste des nœuds connus par ces relais multipoints.

Les nœuds pertinents sont sélectionnés de façon à pouvoir atteindre tout le voisinage à deux sauts. Cet ensemble est appelé l'ensemble des relais multipoints dont le rôle est :

- diminuer la trace engendrée par la diffusion des messages de contrôle dans le réseau.
- diminuer le nombre de liens diffusés à tout le réseau puisque les routes sont construites à base de relais multipoints.

Pour maintenir à jour toutes les informations nécessaires au choix des relais multipoints et effectuer le calcul des tables de routage, les nœuds OLSR ont besoin d'échanger des informations périodiquement.

Pour s'informer du proche voisinage les nœuds OLSR envoient périodiquement des messages de type hello contenant la liste de leurs voisins. Ces messages permettent à chacun de choisir son ensemble de relais multipoints. Un deuxième type de message est également utilisé, ce sont des messages appelés topologie de control. Par ces messages les sous-ensembles de voisinage qui constituent les relais multipoints sont déclarés périodiquement dans le réseau. Ils sont propagés sur le réseau en utilisant une diffusion optimisée par relais multipoints. Ces informations offrent une carte de réseau contenant tous les nœuds et un ensemble partiel de liens suffisant pour la construction de la table de routage. Cette table est alors calculée par chaque nœud et le routage des données s'effectue saut par saut sans l'intervention d'OLSR dont le rôle s'arrête à la mise à jour des tables de routage de la pile IP [21].

4.2 Les protocoles de routage réactifs

Comme nous l'avons mentionné au cours du paragraphe précédent les protocoles de routage proactifs essaient de maintenir les meilleurs chemins vers toutes les destinations du réseau par l'échange périodique des messages de contrôle de la mise à jour. Les routes sont sauvegardées même si elles ne sont pas utilisées ce qui induit un contrôle excessif surtout dans le cas des réseaux denses.

Les protocoles de routage réactifs créent et maintiennent les routes selon les besoins des émetteurs et de leurs applications. Dans ce cas une procédure de découverte globale de routes est lancée qui permet d'avoir une information bien spécifique mais inconnue au préalable. Les protocoles basés sur ce principe dits aussi à la demande. Dans ce paragraphe nous présentons quelques exemples de protocoles de routage réactifs :

4.2.1 Le protocole Dynamic Source Routing (DSR)

Ce type de protocole considère le routage à la source du fait que la source désigne le chemin complet vers la destination dans l'en-tête du paquet. Le long de ce chemin chaque nœud expédie tout simplement le paquet destiné au prochain saut indiqué dans le chemin grâce à un cache de route. Ainsi une source cherche tout d'abord dans son cache de route pour déterminer la route à la destination, si elle existe la source utilise cette route. Sinon la source lance une procédure de découverte de route pour construire une autre. Dans cette procédure de découverte le nœud source diffuse une requête par inondation dans le réseau. La réponse est retournée par la destination ou un autre nœud si celui-ci a une route dans son cache pour cette destination.

Dans DSR, peu de messages de contrôle circulent dans le réseau même si peu de sources veulent communiquer ce qui représente l'avantage principal de ce protocole. Mais dans le cas des réseaux de grande taille DSR peut présenter des problèmes de passage à l'échelle (scalability). Dans ce cas les paquets augmentent de taille car ils doivent véhiculer les adresses des nœuds existants dans le chemin et l'inondation pour la recherche de routes devient plus importante[34].

4.2.2 Le protocole de routage AODV

Le protocole "Routage avec Vecteur de Distance à la Demande" (AODV : Ad hoc On Demand Distance Vector) représente essentiellement une amélioration de l'algorithme DSDV discuté dans la section 3.1.1. Le protocole AODV réduit le nombre de diffusions de messages et cela en créant les routes lors du besoin contrairement au DSDV qui maintient la totalité des routes. L'AODV est basé sur l'utilisation des deux mécanismes "Découverte de route" et "Maintenance de route" (utilisés par le DSR) en plus du routage nœud-par-nœud, le principe des numéros de séquence et l'échange périodique du DSDV.

L'AODV utilise les principes des numéros de séquence afin de maintenir la consistance des informations de routage. A cause de la mobilité des nœuds dans les réseaux ad hoc les routes changent fréquemment ce qui fait que certaines routes maintenues par certains nœuds deviennent invalides. Les numéros de séquence permettent d'utiliser les routes les plus nouvelles ou autrement dit les plus fraîches (fresh routes).

De la même manière que dans le DSR, l'AODV utilise une requête de route dans le but de créer un chemin vers une certaine destination. Cependant l'AODV maintient les chemins d'une façon distribuée en gardant une table de routage au niveau de chaque nœud de transit appartenant au chemin cherché. Une entrée de la table de routage contient essentiellement :

- L'adresse de la destination.
- Le nœud suivant.
- La distance en nombre de nœud (i.e. le nombre de nœud nécessaire pour atteindre la destination).
- Le numéro de séquence destination.
- Le temps d'expiration de l'entrée de la table.

Quand un nœud de transit (intermédiaire) envoie le paquet de la requête à un voisin il sauvegarde aussi l'identificateur du nœud à partir duquel la première copie de la requête est reçue. Cette information est utilisée pour construire le chemin inverse qui sera traversé par le paquet réponse de route (cela veut dire que l'AODV supporte seulement les liens symétriques). Puisque le paquet réponse de route va être envoyé à la source les nœuds appartenant au chemin

de retour vont modifier leurs tables de routage suivant le chemin contenu dans le paquet de réponse.

Un nœud diffuse une requête de route (RREQ : Route Request), dans le cas où il aura 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 (La métrique qui lui est associée est infinie). Le champ numéro de séquence destination du paquet RREQ contient la dernière valeur connue du numéro de séquence associé au nœud destination. Cette valeur est recopiée de la table de routage. Si le numéro de séquence n'est pas connu, la valeur nulle sera prise par défaut. Le numéro de séquence source du paquet RREQ contient la valeur du numéro de séquence du nœud source.

Comme nous avons déjà dit après la diffusion du RREQ la source attend le paquet réponse de route (RREP : Route Reply). Si ce dernier n'est pas reçu durant une certaine période (appelée RREP_WAIT_TIME) la source peut rediffuser une nouvelle requête RREQ, à chaque nouvelle diffusion le champ Broadcast ID du paquet RREQ est incrémenté. Si la requête RREQ est rediffusée un certain nombre de fois (RREQ_RETRIES) sans la réception de réponse, un message d'erreur est délivré à l'application.

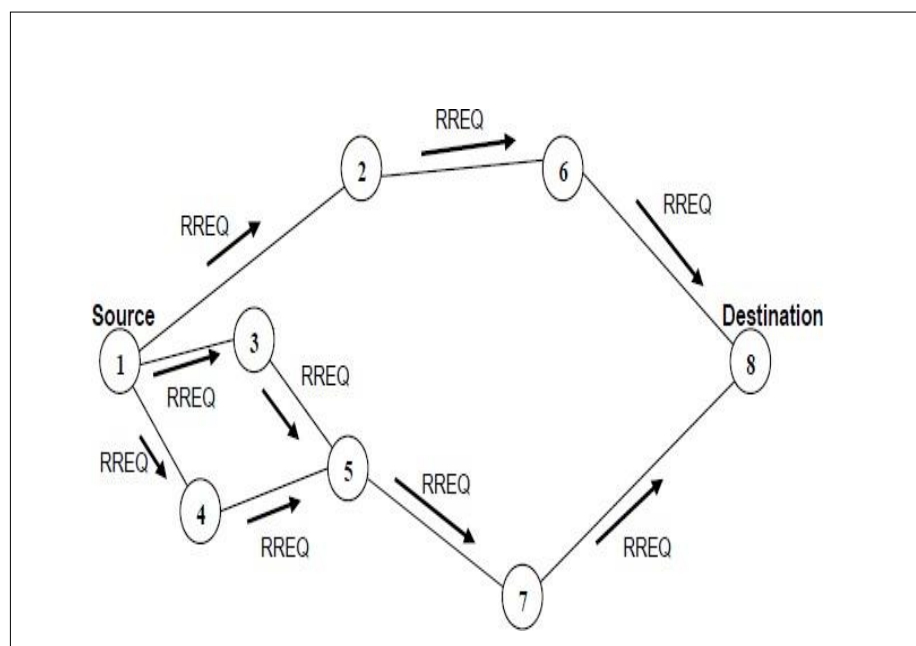


Figure 2.3 La propagation du paquet RREQ (requête de route) [24].

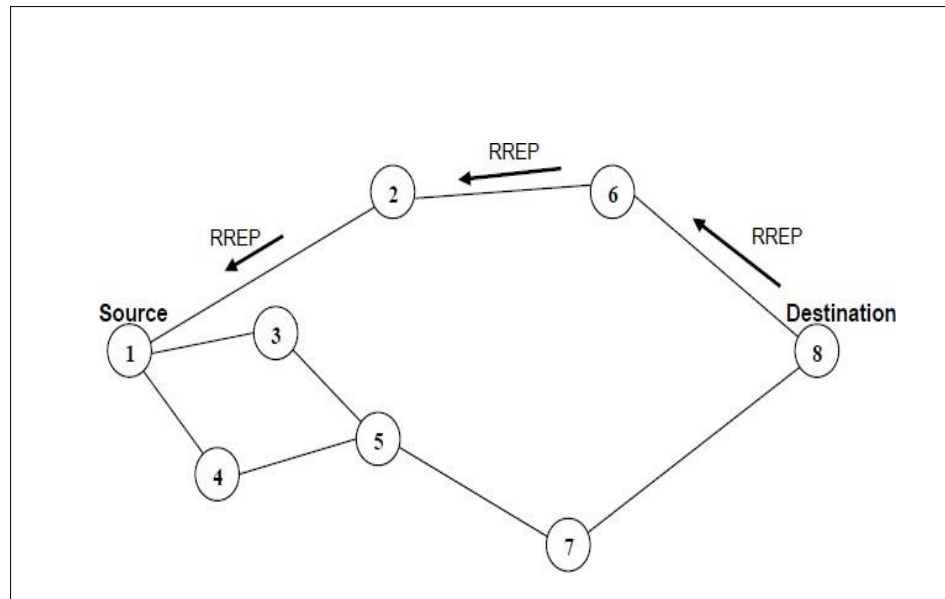


Figure 2.4 Le chemin pris par le paquet RREP (requête de réponse) [24].

Afin de maintenir des routes consistantes une transmission périodique du message "HELLO" est effectuée. Si trois messages "HELLO" ne sont pas reçus successivement à partir d'un nœud voisin le lien en question est considéré défaillant. Les défaillances des liens sont généralement dues à la mobilité du réseau ad hoc. Les mouvements des nœuds qui ne participent pas au chemin actif n'affectent pas la consistance des données de routage. Quand un lien reliant un nœud p avec le nœud qui le suit dans le chemin de routage devient défaillant et le nœud diffuse un paquet UNSOLICITED RREP avec une valeur de numéro de séquence égale à l'ancienne valeur du paquet RREP incrémentée à une valeur infinie de la distance. Le paquet UNSOLICITED RREP est diffusé aux voisins actifs jusqu'à ce qu'il arrive à la source. Une fois le paquet est reçu elle peut initier le processus de la découverte de routes.

L'AODV maintient les adresses des voisins à travers lesquels les paquets destinés à un certain nœud arrivent à leurs destinations. Un voisin est considéré actif pour une destination donnée, s'il délivre au moins un paquet de donnée sans dépasser une certaine période (appelée active timeout période). Une entrée de la table du routage est active si elle est utilisée par un voisin actif. Le chemin reliant la source et la destination en passant par les entrées actives des tables de routage est dit un chemin actif. Dans le cas de défaillances de liens toutes les entrées des tables de routage participantes dans le chemin actif et qui sont concernées par la défaillance sont supprimées. Cela est accompli par la diffusion d'un message d'erreur entre les nœuds actifs et le protocole de routage AODV (et même le protocole DSR) n'assure pas l'utilisation du meilleur chemin existant entre la source et la destination. Cependant des évaluations de performances récentes ont montré qu'il n'y a pas de grandes différences en termes

d'optimisation entre les chemins utilisés par le protocole AODV et celles utilisées par les protocoles basés sur les algorithmes de recherche des plus courts chemins. En plus de cela le protocole AODV ne présente pas de boucle de routage et évite le problème "counting to infinity" de Bellman-Ford, ce qui offre une convergence rapide quand la topologie du réseau ad hoc change [24].

4.2.3 Le protocole de routage Light-Wight Mobile Routing (LMR)

C'est un protocole de routage réactif qui utilise la diffusion pour déterminer les routes. Les nœuds dans LMR maintiennent de multiples routes pour chaque destination garder plusieurs routes qui rendent le protocole de routage moins sensible aux changements de topologie. En effet il n'est pas systématiquement nécessaire de déterminer une route qui engendre un certain délai .Dans LMR si une autre route est disponible elle est utilisée par contre ce protocole peut produire temporairement des routes invalides avec la présence de boucles [35].

4.2.4 Le protocole de routage TORA (Temporally Ordered Routing Algorithm)

Protocole basé sur le protocole LMR de fait il détermine plusieurs routes pour joindre une destination. L'avantage de TORA comparé à LMR est qu'il obtient plus rapidement une nouvelle route lors de la rupture d'un lien. En effet lorsqu'un nœud détecte un lien coupé et qui n'en a plus aucune route pour joindre la destination il doit en déterminer une nouvelle. Le protocole TORA réalise cette opération dans un laps de temps plus court que LMR. Contrairement à LMR, TORA ne nécessite pas de confirmation lors de l'obtention d'une nouvelle route [36].

4.3 Les protocoles de routage hybride

4.3.1 Le protocole de routage ZRP

Ce protocole découpe le réseau en zones. Chaque zone du réseau inclut un ensemble de nœuds dont le nombre de sauts ne dépasse pas un certain nombre prédéfini appelé aussi rayon de la zone. Des messages de mise à jour sont échangés localement dans chaque zone afin de permettre aux nœuds de connaître localement la topologie du réseau.

5. Conclusion

Ce chapitre était consacré pour les problèmes de routages des réseaux ad hoc avec son principe de fonctionnement, le problème de routage est loin d'être évident dans les réseaux ad hoc, où l'environnement impose de nouvelles limitations par rapport aux environnements classiques.

Les stratégies de routage doivent garder compte de modifications habituelles de la topologie, et de la consommation de la bande passante qui est limitée. Lorsque le protocole de routage est conçu une détermination de performance doit être faite pour éprouver la fiabilité et le taux de perte et la consommation d'énergie.

Nous avons aussi présenté dans ce chapitre les protocoles de routages qui ont été conçu pour garantir le bienfait de routage dans les réseaux MANET. Nous avons étudié les principales caractéristiques pour bien comprendre les protocoles utilisés dans l'acheminement des données entre les différents nœuds.

Comme nous avons vu les protocoles proposés sont classés en trois catégories : les protocoles proactifs et les protocoles réactifs ainsi les protocoles hybrides. Les protocoles réactifs et proactifs essaient de s'adapter aux contraintes imposées par le réseau MANET, en proposant une méthode qui soit de faible coût en capacités et ressources et qui assure la serviabilité du routage en cas de n'importe quelle panne de lien ou de nœuds. Les protocoles de routage étudiés offrent des avantages qui sont en réalité complémentaires et préférables pour différents types d'applications.

Le prochain chapitre sera basé sur la catégorie de protocole réactif en se concentrant sur l'amélioration de protocole AODV avec une prédiction des ruptures des liens.

Chapitre 3

Routage avec prédiction de rupture de lien

1. Introduction

Nous avons présenté dans le deuxième chapitre quelques protocoles de routages réactifs dans les réseaux Ad Hoc tel que le protocole de routage Ad hoc On-Demand Distance Vector (AODV) qui est utilisé par des nœuds mobiles dans un réseau Ad hoc en offrant une adaptation rapide aux conditions de liaison dynamiques avec un faible traitement et de frais généraux de mémoire. Ce dernier utilise les numéros de séquences de destination pour éviter le problème de boucles infinies. Malheureusement AODV ne garantit pas l'installation des liens stables.

Dans ce chapitre nous allons présenter notre proposition pour améliorer le protocole de routage AODV afin d'installer des liens stables entre les nœuds intermédiaires et les routes avec une longue durée de vie entre la source et la destination. Notre proposition est basée sur la puissance du signal reçu.

2. Terminologie de protocole AODV

Dans cette section nous allons présenter les termes les plus importants pour éclaircir notre proposition.

2.1 Route active

Une route vers une destination comportant une entrée dans la table de routage qui est marquée comme valide. Seules les routes actives peuvent être utilisées pour transférer des paquets de données [34].

2.2 Diffusion

La diffusion signifie que l'adresse IP soit 255.255.255.255. Elle est utile pour permettre la propagation des messages AODV dans tout le réseau ad hoc [35].

2.3 Destination

Une adresse IP à laquelle les paquets de données doivent être transmis.

2.4 Nœud de transfert

Un nœud qui accepte de transférer des paquets destinés à un autre nœud en les retransmettant à un prochain saut qui est plus proche de la destination.

2.5 Installation d'itinéraire

Une route configurée pour envoyer des paquets de données à partir d'un nœud qui lance une opération de découverte de route vers sa destination désirée.

2.6 Route invalide

Une route non valide ne peut pas être utilisée pour transférer des paquets de données mais elle peut fournir des informations utiles sur la réparation d'itinéraires et également pour les futurs messages RREQ (Rout Request).

2.7 Nœud d'origine

Un nœud qui diffuse un message de découverte d'itinéraire (source).

2.8 Route inverse

Une route configurée pour transmettre un paquet de réponse à la source.

2.9 Numéro de séquence

Un nombre totalement monotone maintenu par chaque nœud d'origine (source) pour comparer les chemins les plus récents. Ces numéros de séquences nous permettent d'utiliser les routes les plus nouvelles ou autrement dit les plus fraîches (fresh routes). Un nœud mis à jour chaque fois qu'une nouvelle information provenant d'un message de RREQ, RREP, RERR et il incrémente son propre numéro de séquence pour éviter les boucles [36].

3. Format des paquets

3.1 Format de paquet de demande d'itinéraire (RREQ)

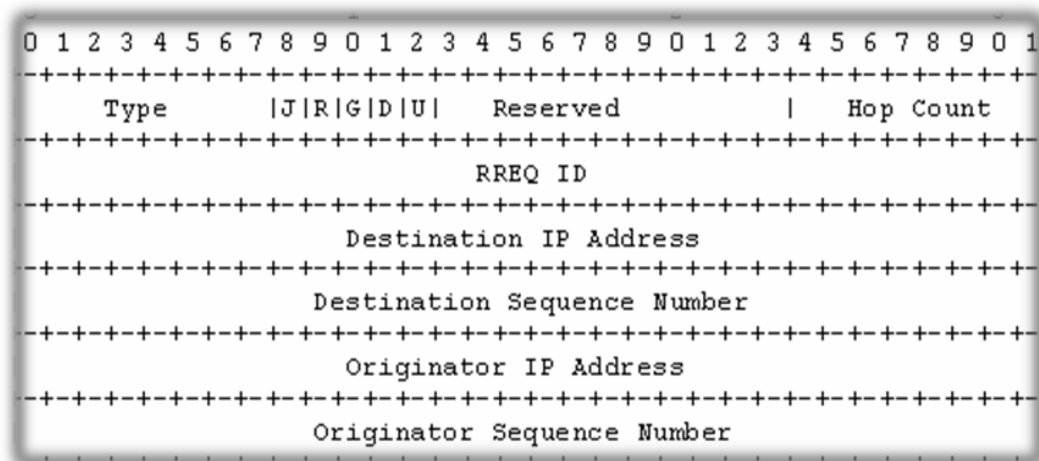


Figure 3.1 Format de Paquet RREQ [36].

Le paquet de demande d'itinéraires (RREQ) [37] illustré ci-dessus et contient les champs suivants :

Type :

J : réservé pour le multicast (multi diffusion)

R : réservé pour la diffusion.

G : indique que RREP devrait être unicast au nœud spécifique dans le domaine d'IP adresse de destination.

D : Drapeau de destination indique seulement la destination peut répondre à ce RREQ.

U : Numéro de séquence est inconnu.

Reserved : envoyé en tant que 0 ignoré à la réception.

Hop count : le nombre de saut de source vers la destination.

RREQ ID : Un numéro de séquence identifiant de manière unique RREQ particulier pris en relation avec l'adresse IP du nœud source.

Destination IP Address : L'adresse IP de la destination pour laquelle un itinéraire est désiré.

Destination Sequence Number : Le dernier numéro de séquence reçu.

Originator IP Address : L'adresse IP du nœud qui a généré la demande d'itinéraire (source).

Originator Sequence Number : Le numéro de séquence actuel à utiliser dans l'itinéraire.

3.2 Format de paquet de réponse RREP

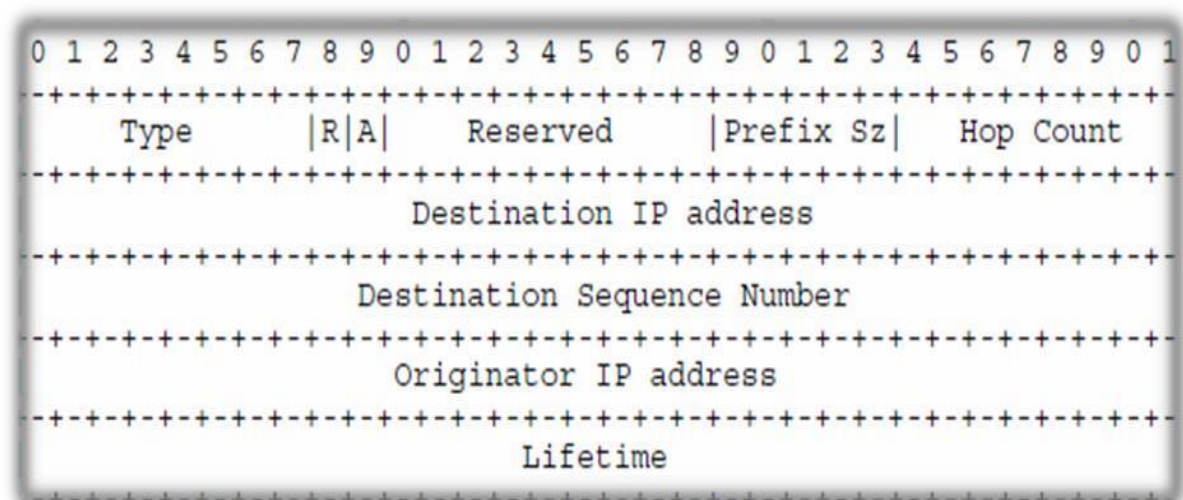


Figure 3.2 Format de paquet RREP [37]

Le paquet RREP contient les champs suivants [37]

Type :

R : réservé pour le multicast.

A : Confirmation requise.

Reserved : envoyé en tant que 0 ignoré à la réception.

Prefix Size : S'il est non nul la taille de préfixe de 5 bits indique que le prochain saut peut être utilisé pour tous les nœuds.

Hop count : le nombre de saut de source vers la destination.

Lifetime : le temps en millisecondes pour lequel les nœuds reçoivent le RREP et on considère que la route est valide.

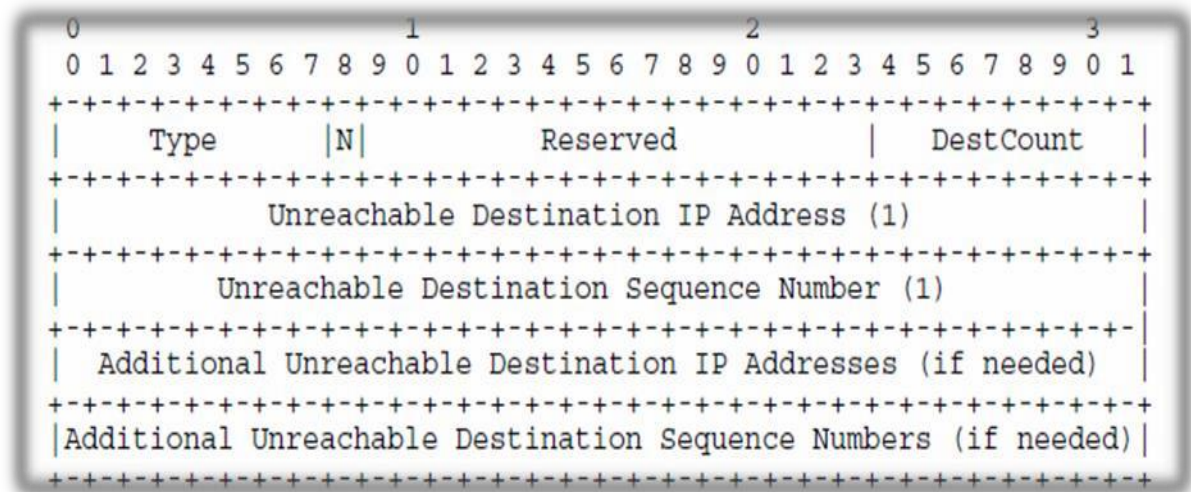
3.3 Format de paquet Route Error (RERR)

Figure 3.3 Format de Paquet RERR [37].

Le paquet Route Error RERR contient les champs suivants [34] :

Type :

N : il est défini lorsqu'un nœud a effectué une réparation locale d'un lien.

DestCount : Le nombre de destinations inaccessibles inclus dans le message doit être au moins 1

Unreachable Destination IP Address : L'adresse IP de la destination qui est devenue inaccessible en raison d'une rupture de lien.

Unreachable Destination Sequence Number : Le numéro de séquence dans l'entrée de la table d'itinéraire est devenu inaccessible.

Le message RERR est envoyé chaque fois que plusieurs destinations deviennent inaccessibles à cause d'une rupture de lien entre les nœuds des voisins.

Après l'étude de protocole AODV on a découvert que ce n'est pas une meilleure technique pour une bonne stabilité des liens entre les nœuds car ce protocole AODV ne garantit pas l'utilisation du meilleur chemin existant entre la source et la destination. Dans la prochaine section on va entamer une proposition pour améliorer ce protocole.

4. Proposition pour améliorer le protocole AODV

Dans cette section nous présentons la notion d'un lien stable pour les protocoles de routage dans les réseaux ad-hoc. La stabilité des liens est basée sur la qualité du signal, la procédure d'établissement des routes de protocole AODV est améliorée par l'utilisation de la notion de stabilité des liens.

La puissance du signal est utilisée pour déterminer la qualité d'un lien cela nous aide non seulement à rendre les routes entre la source et destination plus robuste mais également à anticiper les ruptures de liens.

4.1 Stabilité d'itinéraire

Un chemin stable est un chemin composé d'un ensemble des liens stables. Un lien stable est une liaison entre deux nœuds où le signal est reçu avec une bonne qualité.

4.2 Métrique basé sur la puissance de signal

Pour permettre à l'AODV le choix d'un itinéraire stable de longue durée de vie il va falloir impérativement de changer les mécanismes de choix des routes de ce protocole (AODV). Nous proposons une idée pour choisir les itinéraires qui restent en état cohérente pendant une durée très longue.

Chaque nœud diffuse un signal avec une certaine puissance et reçoit un signal avec celle qui varie selon l'emplacement des nœuds. En effet on choisit les liens entre les nœuds avec une meilleure qualité de réception de signal entre ces nœuds, c'est à dire la distance entre les nœuds est faible donc les nœuds de routage entre la source et la destination sont très proches l'un de l'autre et par conséquent un itinéraire avec une forte stabilité.

4.3 Établissement d'itinéraire dans notre proposition

La source est faite un broadcaste de paquet RREQ pour atteindre la destination si l'adresse de destination ne figure pas dans la table de routage.

Le paquet RREQ dans notre proposition contient les champs suivants :

- Adresse de la machine source (@ source)
- Numéro de séquence source

- Identification d'émission (Broadcast ID)
- Adresse de la machine destination (@ destination)
- Numéro de séquence destination
- Liste-puissance-signaux (liste contenant les puissances de signaux de l'itinéraire)
- Liste-nœuds-intermédiaire (liste contenant les adresses des nœuds intermédiaire de routage)

La paire « ID, @source » identifie RREQ. L'ID est incrémentée, à chaque fois que la source diffuse un nouveau paquet de RREQ.

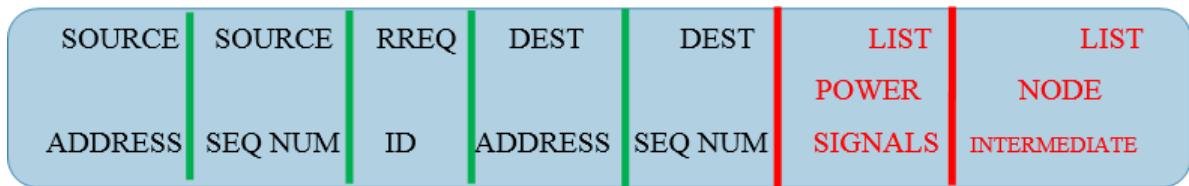


Figure 3.4 Format de paquet RREQ D'AODV modifié

Chaque nœud recevant un paquet de requête (RREQ) vérifie s'il a déjà reçu un RREQ avec le même ID et adresse d'émetteur de paquet ou si son adresse appartient à la liste-nœuds-intermédiaire, le nœud doit ignorer le paquet RREQ. Dans le cas contraire la paire (@ source, ID de requête) sera inscrit dans la table historique pour rejeter le futur doublon et le nœud continue le traitement de paquet RREQ alors on a les cas suivants :

- Si le nœud intermédiaire trouve un chemin vers la destination et si son numéro de séquence de destination est supérieur ou égale au numéro de séquence dans le paquet RREQ, il envoie un paquet réponse de route (RREP) à la source qui indique comment atteindre la destination.
- Dans le cas où le nœud intermédiaire ne trouve pas un itinéraire vers la destination alors le signal du paquet RREQ reçu et son adresse (@nœud) sont enregistrés respectivement dans la Liste-puissance-signaux et Liste-nœud-intermédiaire. Le paquet RREQ mis à jour est rediffusé à nouveau à tous ses voisins.
- Si le paquet RREQ arrive au nœud destination elle extrait la Liste-puissance-signaux et calcule la valeur minimale du chemin qui est à son tour insérée dans le paquet RREP. On note que le paquet de réponse de route (RREP) est unicast.

Le paquet RREP modifié, contient alors les champs suivants :

- Adresse de la machine source (@ source)
- Adresse de la machine destination (@ destination)
- Numéro de séquence destination
- Lifetime (durée de vie de paquet TTL)

- Val-signal (valeur minimale du signal de l'itinéraire)

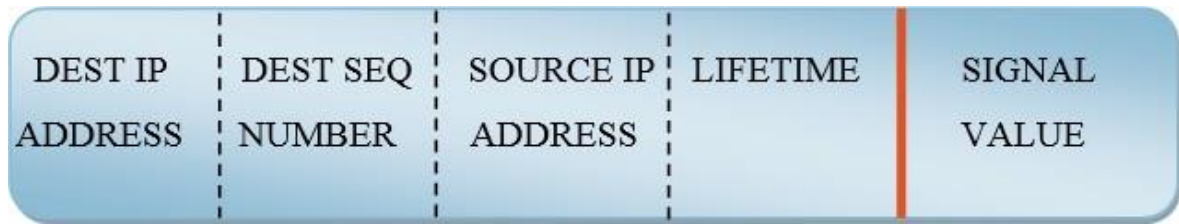


Figure 3.5 Format de paquet RREP D'AODV modifié

Chaque nœud intermédiaire reçoit la réponse RREP et rajoute une entrée vers la destination dans sa table de routage si :

- ✓ Aucune route vers la destination n'est connue
- OU
- ✓ Le numéro de séquence pour la destination dans le paquet de réponse est supérieur à la valeur dans la table de routage
- OU
- ✓ Le numéro de séquence de la destination dans le paquet RREP est le même dans la table de routage. Mais la valeur Val-signal de RREP est supérieure à l'ancien valeur de Val-signal qui est dans la table de routage (la nouvelle route est plus stable).

Pour une même requête RREQ, le nœud source, reçoit plusieurs réponses RREP : la route qui à la valeur maximum de Val-signal, sera choisi.

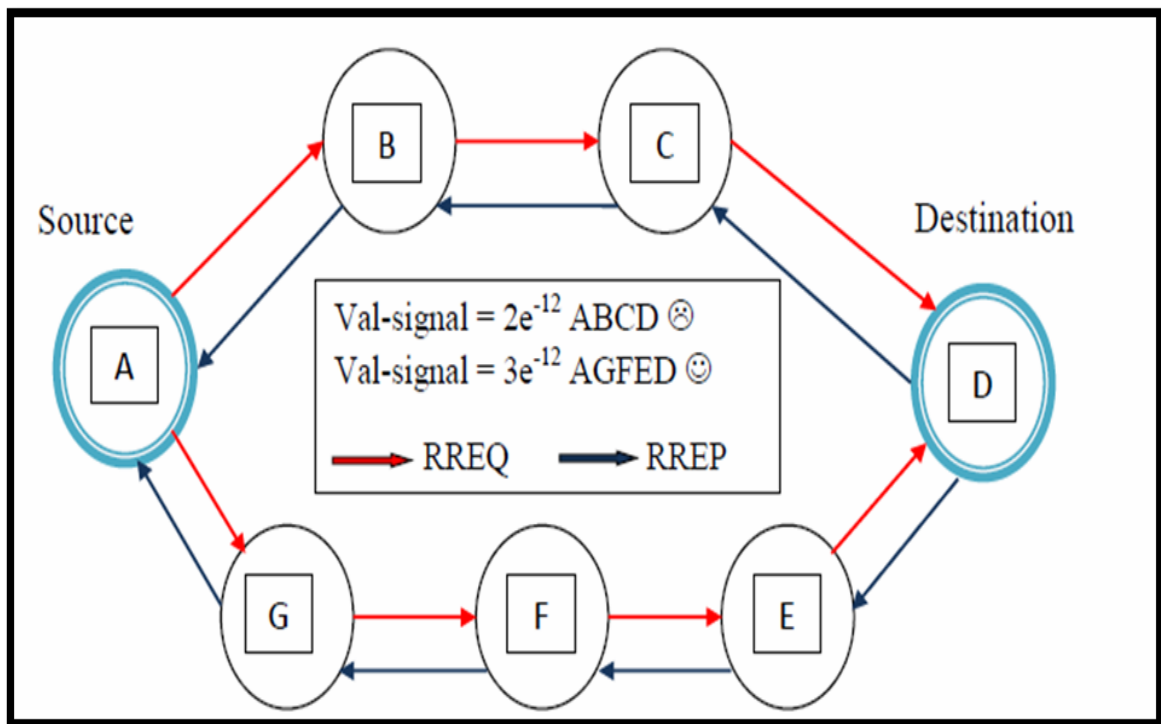


Figure 3.6 Choix d'itinéraire utilisant la métrique basée sur la puissance de signal

Le nœud source A reçoit deux paquet RREP, l'un selon le chemin inverse «DCBA» avec la valeur de Val-signal= 2e-12, et l'autre avec la valeur Val-signal= 3e-12 selon le chemin inverse «DEFGA», le nœud source choisi alors, l'itinéraire «AGFED».

Dans la prochaine section, on va entamer les Algorithmes qui résument le traitement de paquet RREQ et RREP aux niveaux des nœuds intermédiaires, destinations et sources.

5. Les algorithmes du traitement de paquet

5.1 Algorithme 1 : Traitement de RREQ

SI (RREQ id @nœud intermédiaire qui diffuse RREQ appartient à la table de RREQ)

```

|   Détruire (RREQ) ;
|   SINON
|       SI (Mon adresse appartient au RREQ.Liste-nœuds-intermédiaire)
|           Détruire (RREQ) ;
|           SINON
|               Lire (puissance, pkt) ; /*pkt : paquet de RREQ* /
|               Inséré (RREQ.Liste-puissance-signaux, puissance) ;
|               SI ce nœud est la destination
|                   Val-signal = minimum (RREQ.Liste-puissance-signaux) ;
|                   Créer (RREP) ;
|                   Envoi unicast (RREP) ; /*suivante le chemin inverse*/
|                   SINON
|                       SI le nœud intermédiaire trouve un chemin vers la destination
|                           Envoyer (RREP) ;
|                           SINON
|                               Insérer (RREQ.Liste-nœud-intermédiaire, Mon adresse) ;
|                               Diffuse (RREQ) ; /*à ses propre voisin*/
|                               FINSI
|                           FINSI
|                       FINSI
|                   FINSI
|               FINSI
|           FINSI
|       FINSI
|   FINSI

```

5.2 Algorithme 2 : Traitement de RREP

```

SI TTL < TTL_prédefini
|
| SI ce nœud est la source
| |
| | SI c'est une nouvelle entrée dans la table de routage
| | | Ajouter l'entrer dans la table de routage ;
| | |
| | | SINON
| | | | SI (RREP.Seq_numdest > Table.Seq_numdest)
| | | | | Mise à jour la table de routage ;
| | | | |
| | | | | SINON
| | | | | | SI (RREP.Seq_numdest = Table.Seq_numdest)
| | | | | | | (RREP.Val-signal > Table.Val-signal)
| | | | | | | Mise à jour la table de routage ;
| | | | | |
| | | | | FINSI
| | | |
| | | FINSI
| |
| | FINSI
|
| FINSI
|
| SINON /* c'est un noeud intermédiaire */
| |
| | SI c'est une nouvelle entrée dans la table de routage
| | | Ajouter l'entrer dans la table de routage ;
| | | Envoyer (RREP) ;
| | |
| | | SINON
| | | | SI RREP.Seq_numdest > Table.Seq_numdest
| | | | | Mise à jour la table de routage ;
| | | | | Envoyer (RREP) ;
| | | | |
| | | | | SINON
| | | | | | SI (RREP.Seq_numdest = Table.Seq_numdest)
| | | | | | | (RREP.Val-signal > Table.Val-signal)
| | | | | | | Mise à jour la table de routage ;
| | | | | | | Envoyer (RREP) ;
| | | | | |
| | | | | FINSI
| | | |
| | | FINSI
| |
| | FINSI
|
| FINSI
|
| FINSI

```

6. Maintenance d'itinéraire

Selon le protocole AODV si le nœud "E" (figure 3.6) dans le réseau ne reçoit pas de message Hello de son voisin "F", cela signifie que ce dernier (nœud F) a déplacé hors de la portée du nœud "E". Dans ce cas le nœud "E" consulte sa table de routage pour trouver une entrée qui a comme prochain nœud le nœud "F". Si une telle entrée est trouvée le nœud "E" lance une procédure de maintenance ou de rétablissement de chemin. L'opération de maintenance peut prendre un délai important avant qu'un autre chemin ne soit établi. C'est pour ces raisons que nous avons préféré de prédire la rupture au lieu de la détecter.

Nous avons proposé un algorithme de prédiction de rupture de route à base de la puissance de signal. Notre algorithme est basé sur la puissance de signal et utilise la notion de zone de rupture. Nous définissons la zone de rupture ensuite l'algorithme de prédiction de rupture de route basé sur la puissance de signal.

6.1 Zone de rupture

Un nœud B dans la zone de rupture de nœud A, si le signal diffusé par B est reçu au niveau de nœud A avec une faible puissance. Alors B a une forte probabilité de sortir de la portée de A dans un délai très court. Donc on dit que B dans la zone de rupture de A.

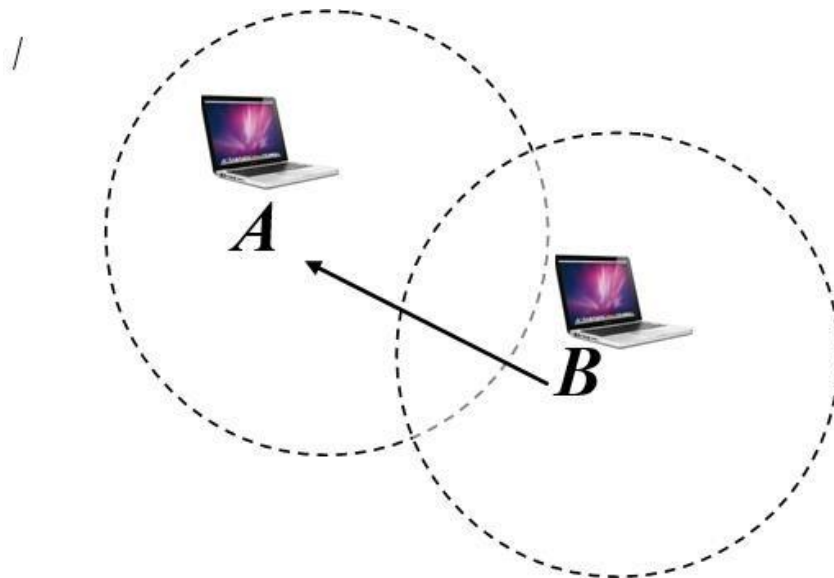


Figure 3.7 Zone de rupture

6.2 Algorithme de prédiction de rupture de route basé sur la puissance de signal

On associe à chaque lien un seuil pour la définition de la stabilité d'un lien. Lorsque la valeur de la puissance de signal reçu est inférieure à ce seuil alors le lien est considéré instable lorsqu'elle passe au-dessus de ce seuil il est stable.

Des messages hello sont envoyés périodiquement entre les nœuds pour tester la connectivité.

L'idée de notre algorithme est :

- Il s'agit de changer la qualité du lien lorsque la puissance du signal agrandit et inversement dans le cas contraire.
- Lorsqu'un nœud se rapproche à la métrique du lien prendra la valeur stable et sera instable quand un nœud s'éloigne (dans la zone de rupture) de manière à revalider le lien juste avant que le nœud sorte de la portée radio.
- On utilise alors un seuil (S_s seuil) associés à la puissance du signal. Lorsque la puissance du signal du Hello reçue est en dessous du seuil (S_s seuil), la métrique de qualité est non stable. Lorsque la puissance du signal est au-dessus du seuil, la qualité du lien est stable.

Nous donnons ci-dessous l'algorithme de prédiction de rupture de route basé sur la puissance de signal.

Si l'adresse de nœud qui a diffusé le paquet Hello est une entrée dans la table de

```

Routage
    /* ss est la valeur de la puissance du signal du Hello reçu */
    SI ss > ss_seuil
    |   Qualité_lien := stable
    SINON (le nœud dans la zone de la rupture)
    |   Qualité_lien := non stable ;
    |   Lancé la procédure de la réparation de route ;
    FINSI
FINSI
  
```

Notre algorithme de prédiction de rupture de route basé sur la puissance de signal assure la prédiction de rupture d'un lien(s) afin de le maintenir soit localement soit de bout à bout.

6.3 Réparation locale

Comme dans AODV, le nœud qui déclenche la procédure de maintenance diffuse à ses voisins un paquet RREQ pour atteindre la destination si n'est pas le cas alors il diffuse un paquet RERR unicast à la source.

6.4 Réparation de bout en bout

Dans le cas où la procédure de réparation locale échoue. Le nœud qui a détecté ou prédit la rupture de route envoie un message RERR à la source pour informer l'échec de l'itinéraire. Après la réception du paquet RERR la source déclenche une nouvelle procédure

de l'installation de route pour atteindre la destination de bout à bout (de la source à la destination).

7. Conclusion

Dans ce chapitre nous avons présenté une proposition pour améliorer le protocole AODV. Le but de cette dernière est l'installation des itinéraires plus stables et prédire les ruptures de routes. Notre proposition est basée sur la qualité de signal reçu entre les nœuds de réseau.

Dans le chapitre suivant nous allons montrer l'efficacité de notre proposition par des simulations sur le simulateur OPNET.

Chapitre 4

*Simulation et interprétation
des résultats*

1. Introduction

Dans le chapitre précédent nous avons présenté une amélioration de protocole AODV, notre proposition est basée sur la qualité de signal reçu entre les nœuds de réseaux pour établir des routes et prédire des ruptures de routes.

Après l'implémentation de notre proposition, une simulation a été effectuée sur le simulateur OPNET [38]. Ce simulateur est très utile et très efficace en matière de modélisation et simulation d'un système de communication.

Ce chapitre présente une comparaison entre notre protocole développé (amélioration d'AODV) avec le protocole AODV suivant les métriques de test [24].

2. Définition sur OPNET

OPNET (Optimized Network Engineering Tools) est un simulateur créé pour permettre de concevoir, étudier des réseaux numériques et des protocoles de communication avec une grande flexibilité. Il travaille sur toutes les couches du modèle OSI et permet de récupérer une grande quantité d'informations [39].

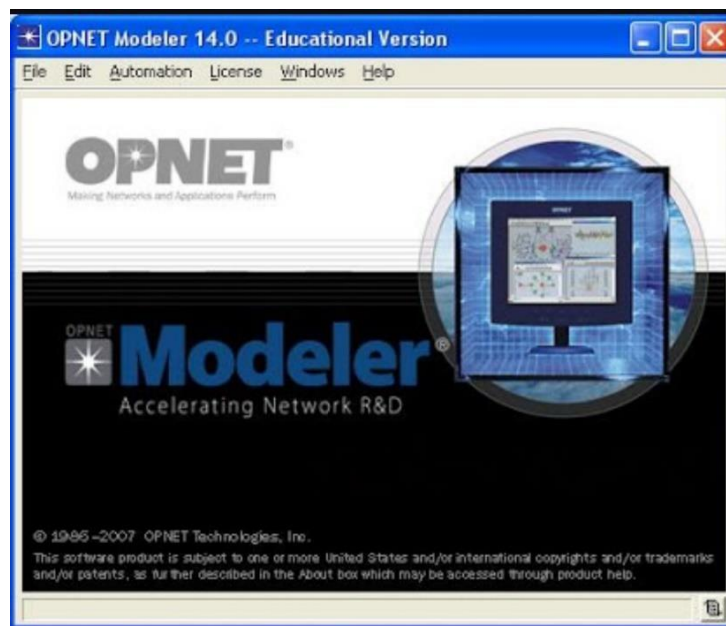


Figure 4.1 OPNET VERSION 14.0 [39].

2.1 Présentation du Simulateur OPNET

OPNET Modeler est un simulateur de réseau à événements discrets, il a été proposé premièrement par Massachusetts Institute of Technology (MIT) en 1986 et écrit en langage C++. Il est bien établi et une suite commerciale professionnelle pour la simulation de réseau. Actuellement, il est l'environnement de simulation commercial le plus utilisé [39].

2.2 Les caractéristiques de simulateur OPNET

Modeler : est le moteur le plus modulable et plus évolutif des moteurs de simulation. Modeler permet de dessiner et d'étudier des réseaux de communications, des équipements, des protocoles et des applications avec facilité et évolutivité. Modeler est utilisé par les entreprises technologiques les plus performantes pour accélérer leurs procédés de recherches et développements, il permet aussi d'utiliser des runtimes de simulation qui utilisent des techniques d'accélération.

Les modèles hiérarchisés de réseaux : gèrent des topologies complexes avec un nombre de sous réseaux imbriqués illimité.

La programmation des modèles est orientée objet : les équipements et les protocoles sont programmés sous forme de modules de classes incluant héritage et organisation des classes.

La modélisation est claire et simplifiée : c'est le cas pour la modification du comportement des différents objets au niveau processus et l'intégration entre eux au niveau équipements.

Il en est de même au niveau réseau pour la création des liens entre les équipements.

Il est possible de lancer scénarios au sein des projets afin de pouvoir comparer les différentes architectures.

Support complet : pour la réalisation de protocoles. Plus de 1000 fonctions sont incluses et les bibliothèques assurent l'aide à la réalisation des protocoles.

Totalement ouvert : le code source est disponible pour tous les modèles.

Debugger Intégré : il permet de valider rapidement une simulation ou de trouver les problèmes.

Outil d'analyse intégré : interface simple pour visualiser les résultats d'une simulation. Interface permettant de visualiser des séries, des courbes, des fonctions de probabilité.

Animations : il est possible de visualiser le comportement d'un modèle sous forme d'une animation. Il est possible de visualiser graphiquement les données statistiques pendant l'exécution de la simulation.

Analyse financière du coût des équipements : exportation des coûts sous forme de bilans avec présentation du total des coûts.

Les équipements réseaux : la bibliothèque de modèles standard inclut de nombreux équipements des constructeurs sous une forme générique dont des routeurs, des switches, des stations de travail, des générateurs de paquets. Cet ensemble permet de réaliser des modèles de simulation rapidement. Il est possible d'agréer du trafic venant d'un LAN ou d'un réseau matérialisé par un nuage [38].

2.3 Principe de fonctionnement

OPNET fonctionne en quatre étapes, ces étapes sont proposition d'un modèle, spécification des statistiques, exécution de la simulation et collection des résultats. Si les résultats ne sont pas corrects il faut retourner à la première étape et fait les corrections du modèle puis continue les autres étapes. La figure suivante représente le fonctionnement général d'OPNET [40].

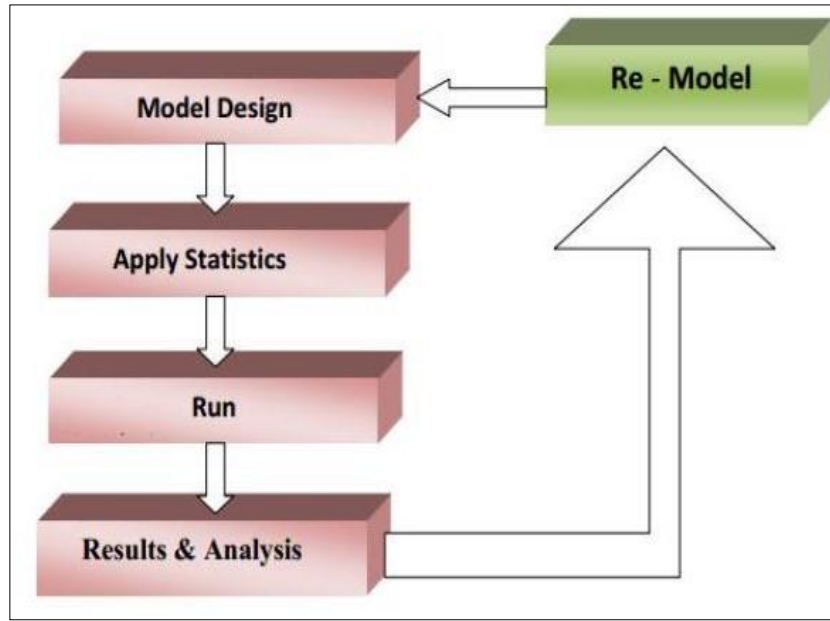


Figure 4.2 Fonctionnement d'OPNET [40].

2.4 Les avantages de l'utilisation du simulateur OPNET

Parmi les avantages de l'utilisation de ce simulateur sont :

- La possibilité de comparer facilement les conceptions alternatives afin de choisir le système Optimal.
- Au cours de développement de la simulation, elle peut nous fournir des indications précieuses sur le fonctionnement interne du réseau qui peut à son tour être utilisé à un stade ultérieur.
- Ce simulateur peut réduire les inconnues et les obstacles. En permettant de voir tout ce qui peut arriver et tous les scénarios possibles.
- La phase de simulation donne aux développeurs une bonne idée de l'ampleur de l'implémentation réelle de l'application.
- OPNET permet de mieux comprendre les protocoles ou des applications.
- OPNET fournit une bibliothèque de plus de 400 fonctions propriétaires spécifiques à l'usage des réseaux (création, envoi et réception de paquets, extraction de valeurs) [41].

3. Simulation

Dans cette section nous allons présenter notre simulation dans le cadre de l'évaluation de notre proposition. Nous avons choisi d'utiliser le simulateur OPNET. Nous allons commencer par la présentation du modèle de simulation. Ensuite nous donnerons les résultats de notre proposition et les résultats de protocole AODV. Une interprétation de ces résultats sera montée à la fin de cette section. Le tableau suivant résume les paramètres de notre modèle de simulation.

Tableau 1: paramètre de simulation

Paramètre de Simulation	
Simulateur	OPNET 14.0
Protocole de routage	AODV, Notre proposition
Temps de simulation	1800s
Nombre des nœuds	35
Surface	2000/2000 m
Vitesse	0.25m/s
Pause Time	4s
Start Time	10s
Modèle de mobilité	Random Waypoint
Trajectory	VECTOR
TTL Start	6
Increment	2
TTL Theshold	15

3.1 Random Waypoint (RWP)

Ce modèle a été utilisé par Johnson et Maltz [27] dans l'évaluation du protocole de routage DSR [34]. Le Random Waypoint modélise tous les scénarios dans lesquelles les nœuds se déplacent avec des pauses. Dans ce modèle chaque nœud choisit aléatoirement un point comme destination de coordonnées (x, y) dans la surface de simulation, avec une vitesse entre 0 et V_{max} . Le nœud déplace vers la destination (le point) choisie avec la vitesse choisie. A l'arrivée, le nœud prend un temps de repos (pause) avant de choisir à nouveau une nouvelle destination et une nouvelle vitesse pour répéter le même processus. Des études ont été faites sur ce modèle puisqu'il est le modèle le plus utilisé dans les simulations dû à la facilité de son implémentation.

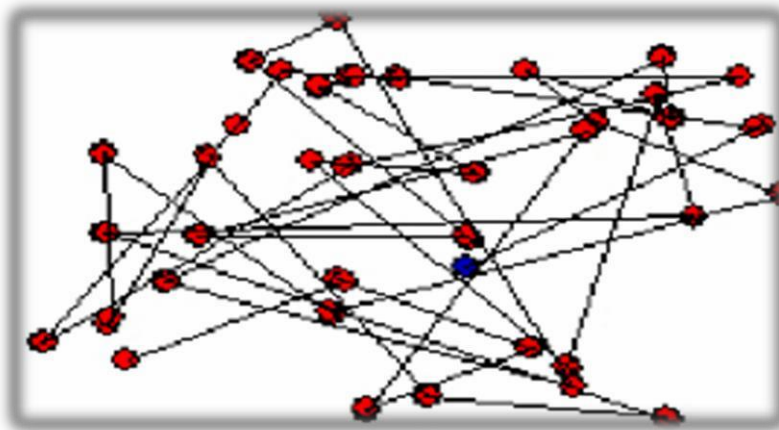


Figure 4.3 Le déplacement d'un nœud utilisant le Random Waypoint [27].

3.2 L'environnement de simulation

La figure suivante représente l'environnement de la simulation qui contient 35 nœuds mobiles se déplacent dans un espace de 2000×2000 m avec une vitesse de 0.25 m/s, Packet Inter-Arrival Time (sec) est exponentiel (1) s, Radom waypoint mobility est sélectionnée. Tous les nœuds supportent notre proposition et le protocole AODV comme un protocole de routage, le nœud Source va envoyer des paquets au nœud Destination.

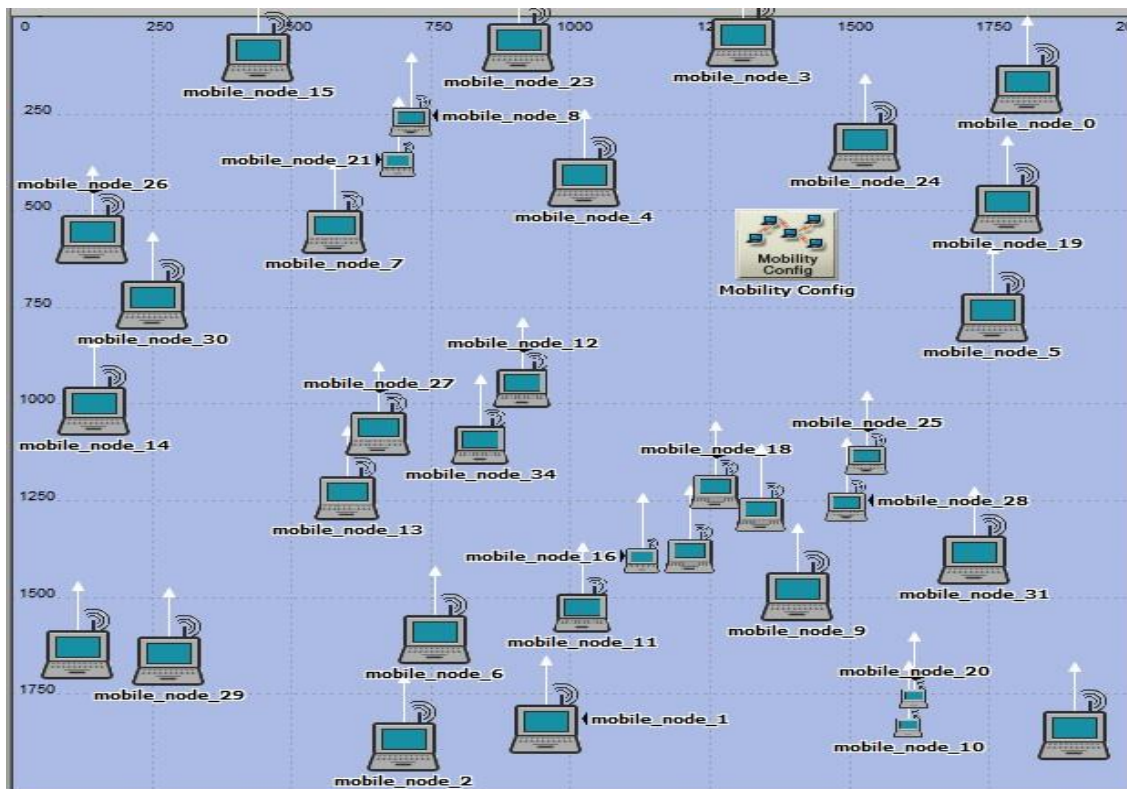


Figure 4.4 L'environnement de simulation

3.3 Métrique de performances utilisées

Dans OPNET, chaque simulation génère un ensemble de graphes. C'est à base de ces graphes que nous avons analysé les résultats de la simulation. Nous avons décidé de baser sur trois métriques pour évaluer notre proposition :

- Total Replies Sent From Destination (Totale de réponses envoyées par la destination) :
- Ce paramètre mesure le taux de livraison de paquet RREP par la destination pour répondre sur la RREQ. Ce paramètre est très important pour valider l'implémentation de notre proposition en termes de l'établissement d'itinéraires.
- Total Route Errors Sent (Totale de route erreurs envoyées) : Avec ce paramètre, nous pouvons mesurer le taux de paquet RERR envoyé dans le réseau, pour l'informer les nœuds sur les ruptures de liens. Ce paramètre est très important pour voir l'efficacité de la prédiction au lieu la détection de route.
- Total Packet Dropped (Totale de paquets perdus) : En terme de rendement ce paramètre mesure le taux de paquet perdu dans notre réseau. Ce paramètre est très important pour valider notre proposition [38].

4. Résultats

4.1 Les paquets de RERR

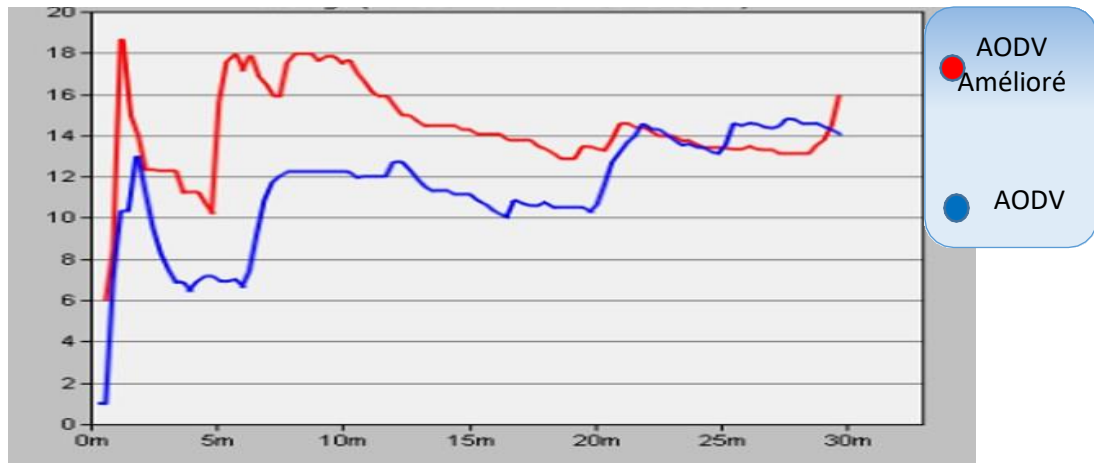


Figure 4.5 Comparaison entre les paquets de RERR envoyés par AODV et AODV modifié

Cette figure représente une comparaison en termes de messages d'erreurs envoyés (RERR) par les deux protocoles AODV (en Blue) et L'AODV modifié (en rouge).

Nous remarquons que les paquets d'erreurs sont envoyés de plus par notre proposition par rapport à l'AODV, on peut exprimer cette grande variation par notre mécanisme de prédiction de route établie par ce que à chaque fois un nœud va sortir de l'apportée, notre proposition va génère des paquets d'erreurs (RERR) indiquant à la source que ces liens ne sont pas stables donc on peut dire que la maintenance des routes dans notre cas est plus fréquente que le protocole AODV.

4.2 Les paquets de RREP

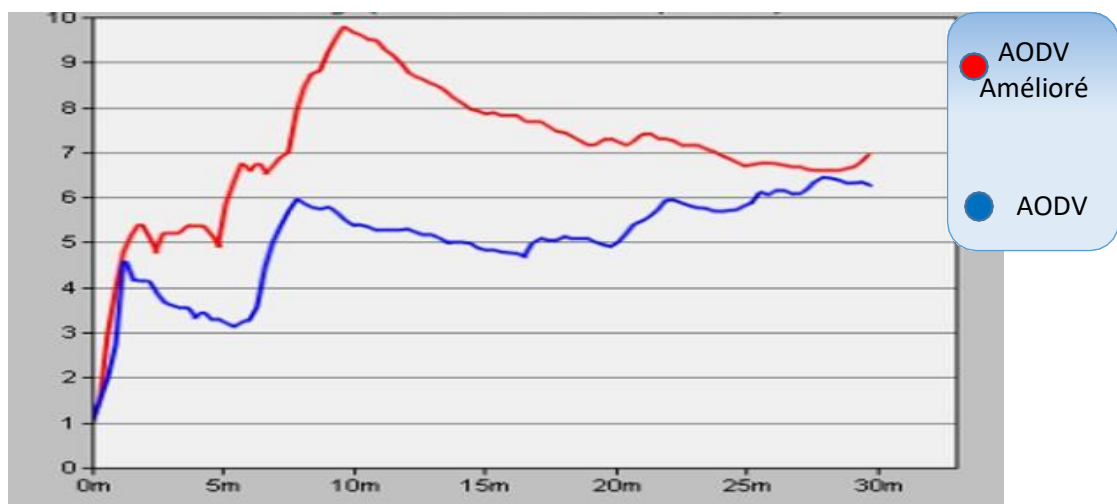


Figure 4.6 les paquets de RREP envoyés par AODV et AODV modifié

Cette figure représente une comparaison entre protocoles AODV (en Blue) et L'AODV modifié (en rouge) en termes de paquet de RREP.

Nous remarquons que le nombre de paquets RREP envoyés par notre proposition est plus important que le protocole AODV. Dans notre proposition nous cherchons à trouver l'itinéraire le plus stable parmi plusieurs itinéraires possibles entre la source et la destination. Cependant AODV réponds seulement à la première RREQ.

4.3 Les paquets rejetés

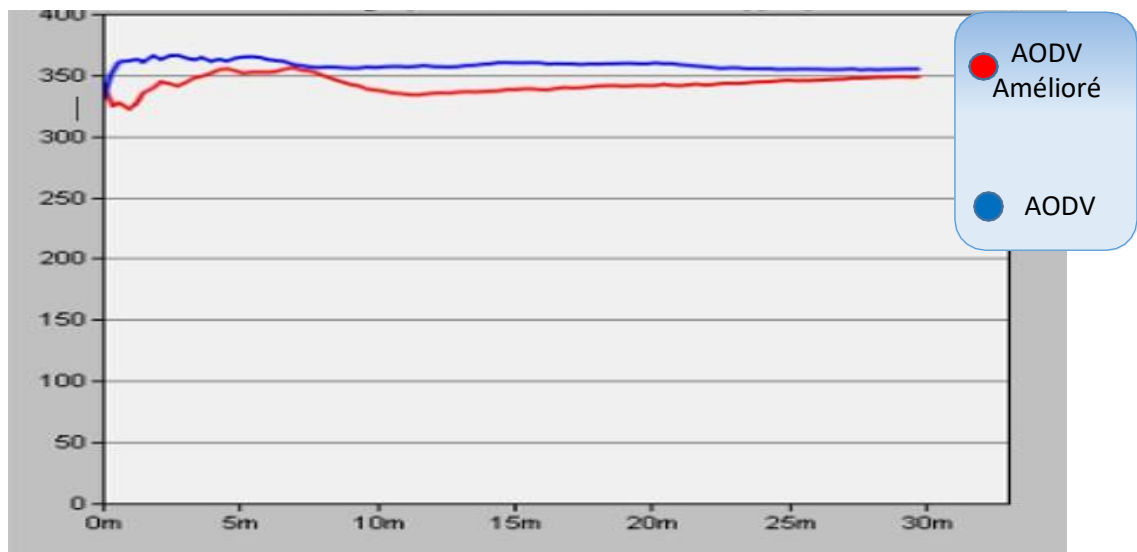


Figure 4.7 Comparaison entre les paquets rejetés par AODV et AODV modifié.

Cette figure représente une comparaison en termes de nombre total de paquet perdu au cours d'acheminement des données de source vers destinataire entre AODV, qui utilise hop count (le graph en bleu) et notre AODV modifié basé sur la puissance du signal (le graph en rouge), on peut subdiviser l'analyse de ce résultat en trois sections :

➤ **Première section :**

0m -8m : on observe qu'au début de transmission le paquet perdus par L'AODV sont un peu supérieurs par rapport à notre AODV modifié et cela due à conséquence que liens ne sont pas en cours stables pour permettre de maintenir la stabilité des routes.

➤ **Deuxième section :**

8m-20m : dans cette section on remarque que les paquets perdus par notre AODV modifié sont très faibles par rapport à l'AODV et cela due grâce à notre mécanisme de prédiction des ruptures de routes donc les liens vont devenir très stables, et par conséquence le nombre de paquet perdu va diminuer, ce qui reflète les performances de notre proposition.

➤ **Troisième section :**

20m-30 : on remarque dans cette section que les paquets perdus par notre AODV modifié sont augmenté à cause de la mobilité des nœuds mais ça reste encore faible par rapport au protocole AODV.

5. Conclusion

Ce chapitre était sacrifié pour la partie de simulation sur le simulateur OPNET, donc nous avons fait une présentation rapide de ce logiciel qu'est très utile et très efficace en matière de modélisation et simulation. Nous avons implémenté notre proposition sur ce simulateur.

Notre simulation effectuée était en terme de trois paquets RERR, RREP, cette simulation nous a permis de faire une comparaison entre les deux protocoles AODV et AODV modifié, alors les résultats obtenus nous ont confirmé que l'ajout de paramètre de puissance de signal rend le protocole AODV amélioré plus puissant pour atteindre le but souhaité de faire prédire les routes au lieu de les détecter, cela veut dire aussi que notre mécanisme de prédiction de rupture a assuré et amélioré la qualité du service (QOS) dans le réseau Ad hoc.

Conclusion et perspective

Conclusion et perspective

Un réseau mobile ad hoc ou MANET est un système constitué d'un ensemble de nœuds mobiles interconnectés par une technologie sans fil. L'acheminement des données dans un réseau Ad Hoc est un problème très compliqué vu les changements des topologies et l'instabilité des liens en effet il existe plusieurs protocoles de routage. Mais ces protocoles ont un certain nombre d'avantages et d'inconvénients. Nous avons choisi d'améliorer le protocole AODV qui est standardisé par IETF.

Notre proposition est basée sur un changement de mécanismes d'installation des itinéraires en basant sur la puissance de signal de paquet RREQ et RREP. Nous avons proposé aussi un mécanisme pour prédire les ruptures de routes.

Les résultats obtenus sur simulateur OPNET montrent clairement l'efficacité de notre proposition qui assure des itinéraires plus stables avec une longue durée de vie. Par conséquent on peut dire qu'on a augmenté la qualité du service (QOS) dans les réseaux MANET.

Les travaux entrepris au cours de cette thèse nous inspirent plusieurs voies de recherche. Nous proposons de simuler d'autres scénarios plus complexes avec différents protocoles de routage et modèles de mobilité. Nous pouvons également compléter nos travaux en s'intéressant à d'autres problématiques dans le vaste champ du routage de réseaux Ad Hoc, ainsi par exemple de tester notre proposition dans un environnement très dense, l'exploitation de la proposition dans un contexte de maison de repos avec l'utilisation des capteurs sans fil pour surveiller les patients sans l'intervention des infirmiers.

- [1] Amar BOURI, Abdelhamid BENTABET. « Mise en œuvre d'un réseau de senseurs sans fil pour la détection et la localisation d'un incendie ». Thèse de MASTER 2, Université de Abou Bekr Belkaid Tlemcen, 2009.
- [2] Amina, 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.
- [3] Fabrice, MFUAMBA KABONZO. « Etude portant sur l'implantation d'un réseau sans fil WIFI » <http://www.memoireonline.com/11/12/6515/Etude-portant-sur-limplantation-dun-reseau-sans-fil-WIFI.html> (Accédé au 5 mai 2017).
- [4] Steven, ASSAD. « Les réseaux sans fil : Le Bluetooth » www.supinfo.com/articles/single/3021-reseaux-sans-fil-bluetooth (Accédé au 5 mai 2017).
- [5] David, Elorrieta. « Protocole de routage pour l'interconnexion des réseaux Ad hoc », mémoire de doctorat, Université Libre de Bruxelles.
- [6] LAUREN. « GÉNÉRALITÉS SUR LE ZIGBEE » <http://blog.domadoo.fr/guides/generalites-sur-le-zigbee> ,(Accédé au 5 mai 2017).
- [7] Kadima, KALALA. « Mise en place sur le point d'accès d'un réseau wifi ». Institut supérieur d'informatique programmation et d'analyse (ISIPA) RDC – Graduat 2010.
- [8] MABELE MONDONGA, Daniel. « Etude sur les protocoles de routage d'un réseau sans fil en mode Ad Hoc et leurs impacts ». Institut supérieur d'informatique, programmation et analyse de Kinshasa - Ingénieur informaticien 2010.
- [9] Eric, BOSASI DOYI. « Gestion des ressources radios dans les réseaux sans fils : cas d'un réseau wimax ». Thèse de doctorat, Université de Kinshasa - Gradué en Sciences Appliquées 2010.
- [10] HAJAMI, Abdelmadjid. « Sécurité du routage dans les réseaux sans fil spontanés : cas du protocole OLSR ». Thèse de doctorat, Université Mohammed V Souissi, 2011.
- [11] BOUDJAADAR Amina, « Plateforme Basée Agents Pour l'Aide à la Conception et la Simulation des Réseaux de Capteurs Sans Fil » Thèse de magistère, Université 20 AOUT 55 DE SKIKDA, 2010.
- [12] Belkheir Khaled et Haned Ahmed. « Réseaux WiFi ad hoc ». Mémoire d'ingénieur, Institut de télécommunication d'Oran, Juin 2008.

- [13] LEMLOUMA, Tayeb. « Le Routage dans les Réseaux Mobiles Ad Hoc ». Thèse de Master, Université des Sciences et de la Technologie Houari Boumediene, Septembre 2010.
- [14] AMEZA, Fatima. «Les technologies sans fil : Le routage dans les réseaux ad hoc (OLSR et AODV) ». Mémoire de master , Université de Bejaia, Septembre 2007
- [15] MABELE MONDONGA, Daniel.« Etude sur les protocoles de routage d'un réseau sans fil en mode Ad Hoc et leurs impacts. "cas de protocoles OLSR et AODV ».mèmoire de doctorat, Université de Congo, 2010.
- [16]J. CARSIQUE, N. DAUJEARD, A. LALLEMAND, et R. LADJADJ. « *Le routage dans les réseaux mobiles Ad hoc* ».mémoire de doctorat, Université de Lyon, 2010.
- [17] Azzedine Boukerche, Begumhan Turgut, Nevin Aydin, Mohammad Z, Ladislau Blind, Dalman Turgut, «Routing protocols in ad hoc networks: A survey, Computer Networks 55 » (2011), pp 3032-3080, 2011.
- [18] TAHAR ABBES, Mounir.« Proposition d'un protocole a économie d'énergie dans un réseau hybride GSM et AD HOC ». Thèse de doctorat, Université d'Oran, 2012.
- [19] C. Cheng, R. Riley, S. Kumar et J.J. Garcia-Luna-Aceves.A Loop-Free Bellman- Ford «Routing Protocol without Bouncing Effect».ACM SIGCOMM489.Sept 1989
- [20] G. Malkin RIP Version 2-Carrying Additional Information.RFC 1388. « Internet Engineering Task Force », January 1993.
- [21] HAGGAR, Bachar, Salim.« Auto-organisation et routage dans les réseaux mobiles ad hoc» Thèse de doctorat, Université de Reims Champagne-Ardenne, 2009.
- [22] M. Boulkamh Chouaib.« Prise en Compte de la QoS par les Protocoles de Routage dans les Réseaux Mobiles Ad Hoc », Thèse de Magistère, Université El Hadj Lakhdar de Batna, 2008.
- [23] ZABDI, Abdelhamid. « DZ-MAODV : NOUVEAU PROTOCOLE DE ROUTAGE MULTICAST POUR LES RÉSEAUX ADHOC MOBILES BASÉ SUR LES ZONES DENSES », mémoire présenté à l'université du Québec à Trois-Rivières, Avril 2006.
- [24] N,.Badache. « Le routage dans les réseaux mobiles ad hoc»,Thèse de doctorat, Septembre 2000. Université Houari Boumediene, Algérie.

- [25] Jean-Pierre , CHANET.« Algorithmes de routage coopératif à qualité de service pour des réseaux ad hoc agri- environnementaux ». Thèse pour obtenir le grade de DOCTEUR D'université Blaise Pascal - Clermont II, 20 avril 2007.
- [26] David, Elorrieta. « Protocoles de routage pour l'interconnexion des réseaux Ad- Hoc et UMTS». mémoire de doctorat, Année 2006-2007, Université Libre de Bruxelles.
- [27] Bécaye DIOUM, « Effets de la mobilité sur les protocoles de routage dans les réseaux ad hoc », Année 2006-2007, Université MOULOUD MAMMERI de TIZI OUZOU (Algérie).
- [28] Tsu-Wei C. and M. Gerla. «Global state routing: a new routing scheme for ad-hoc wireless networks. In IEEE International Conference on Communications (ICC 98) », volume 1, pages 171–175 vol.1, Jun 1998.
- [29] N. Badache, D. Djenourf, A. Derhab, and T. Lemlouma. « Les protocoles de routage dans les réseaux mobiles ad hoc. RIST : Revue d'Informatique Scientifique et Technique », 12(02) :77–112, 2002.
- [30] G. Pei, M. Gerla, and T.W. Chen. «Fisheye state routing in mobile ad hoc networks. In ICDCS Workshop on Wireless Networks and Mobile Computing», pages 71–78, Jun 2000.
- [31] C. Ching-Chuan and M. Gerla. Routing and multicast in Multihop, «mobile wireless networks. In IEEE 6th International Conference on Universal Personal Communications Record», volume 2, pages 546–551 vol.2, Oct 1997.
- [32] A. Iwata, C.C. Chiang, G. Pei, M. Gerla, and T.W. Chen. «Scalable routing strategies for ad hoc wireless networks». volume 17, pages 1369–1379, Aug 1999.
- [33] S. Basagni, I. Chlamtac, V.R. Syrotiuk, and B.A. Woodward. A distance routing effect algorithm for mobility (dream). In Proceedings of the 4th Annual ACM/IEEE International Conference on Mobile Computing and Networking, MobiCom '98, pages 76–84, New York, NY, USA, 1998. ACM.
- [34] Fei Dai. «Proactive Route Maintenance in Wireless Ad Hoc Networks»,Florida Atlantic University,June 2005.
- [35] Jérémie, ANZEVUI. « Les réseaux sans fil »,Projet d'ingéniorat , Université de Genève, 2006-2007.
- [36] C. Perkins, E. Belding-Royer, and S. Das. Ad hoc on-demand distance vector (AODV) routing, RFC3561, 2003. URL <http://www.ietf.org/rfc/rfc3561.txt>.
- [37] T. Clausen and P. Jacquet. Optimized link state routing protocol (OLSR), RFC3626, oct 2003. URL <http://www.ietf.org/rfc/rfc3626.txt>.

- [38] Jean Pierre. OPNET Technologies. 2004.URL <http://www.didierfavre.net/Opnet-Modeler.htm> (Consulté le 12/07/2017)
- [39] Abass Mohamed, Ahmed Kapashi . Performance Evaluation of IPv4 Vs Ipv6 and Tunnelling Techniques Using Optimized Network Engineering Tools (OPNET).URL <http://iosrjournals.org/iosr-jce/papers/Vol17-issue1/Version-4/M017147275.pdf>(Consulté le 12/07/2017)
- [40] Bruno, OUELLET. «Etude de faisabilité d'intégration entre les technologies sans fil de relais sous-réseau (SNR) et de L'IEEE 802.11b».Mémoire de magister , Université du QUEBEV,2004.
- [41] Paul-Antoine,Bisgambiglia. «Modulisation de réseau». Thèse de Master, Université de Corse, Pasquale PAOLI,2009.

