

République Algérienne Démocratique et Populaire  
Ministère de l'enseignement

Supérieur et de la Recherche Scientifique

Université A/Mira de Béjaïa  
Faculté des Sciences Exactes



Département d'Informatique  
MEMOIRE DE MASTER PROFESSIONNEL En  
Informatique  
Option Administration et Sécurité des Réseaux

## Thème

---

# Etude comparative du protocole AODV et ses variantes

---

**Présenté par :** *M<sup>elle</sup>* BIROUCHI KAHINA  
*M<sup>elle</sup>* IRID FATIMA

**Devant le jury composé de :**

**Président :** *M<sup>me</sup>* LARBI Wahiba M.C.B, Université A/MIRA BEJAIA.

**Rapporteur :** *M<sup>me</sup>* GHERBI Meriem M.A.A, Université A/MIRA BEJAIA.

**Examineur :** *M<sup>me</sup>* MAMMERI Karima M.A.A, Université A/MIRA BEJAIA.

Année universitaire 2019/2020.

# *Remerciements*

*Tout d'abord, nous remercierons le Bon Dieu de nous avoir donné la force, le courage et la volonté pour mener à bien ce travail.*

*Nos plus sincères remerciements s'adressent à notre promotrice Mme. ZIANE-GHERBI pour nous avoir proposé cet intéressant sujet et pour ses précieux conseils et encouragements, sans lesquels cette étude n'aurait pas vu le jour. Merci pour votre confiance, votre Disponibilité et vos encouragements.*

*Puis, nous tenons également à remercier tous les membres du jury pour avoir accepté d'évaluer notre travail.*

*Enfin, une immense merci à tous mes amies surtout Mlle HAMRAOUI Meriem, AGGAOUA Meriem, AZZOUGUER Dalila, OVASLI Souad pour leur soutien inconditionnel et leur encouragement*

## *Dédicace*

*A mes très chers parents. Aucune dédicace n'est assez éloquente pour vous exprimer ma gratitude pour les sacrifices .la chance que j'ai de vous avoir est inestimable et j'espère que ce travaille vous rendra fières.*

*A mes frères et mes sœurs pour leur soutient morale vous avez toujours été pour m'écouter et me conseiller au mieux et surtout pour me faire rire.*

*A ma chère collègue qui m'accompagné durant ce travail.*

*A toutes mes amies et tous ceux que j'aime et qui m'aiment.*

*B. KAHINA*

## *Dédicace*

*Je rends grâce à dieu de m'avoir donné le courage et la volonté ainsi que la conscience d'avoir pu terminer mes études. J'ai l'immense honneur de dédier ce mémoire :  
À mes très chers parents qui étaient présents pour moi durant toute ma vie.*

*Je dédie ce travail aussi à mon très cher frère :  
KARIM sans oublier ma très chère sœur OUARDIA.*

*À ma très chère cousine, sœur, amie WASSILA que j'aurai aimé elle partagera ce moment avec moi, mais malheureusement le bon dieu préfère de l'accueillir dans son vaste paradis.*

*À ma très chère copine KAHINA qui m'accompagner durant tout ce travail.*

*À tous ceux qui me sont chères.*

*I. Fatima*

# Table des matières

Liste des Figures . . . . .	iv
Liste des Tableaux . . . . .	vi
Liste des abréviations . . . . .	vii
Introduction générale . . . . .	1
<b>Chapitre 1 Etat de l’art sur les réseaux Ad Hoc</b>	<b>4</b>
1.1 Introduction . . . . .	4
1.2 Réseaux informatiques . . . . .	4
1.3 Réseaux sans fil . . . . .	5
1.4 Classification des réseaux mobiles selon l’infrastructure . . . . .	5
1.4.1 Réseaux mobiles sans infrastructure . . . . .	5
1.4.2 Réseaux mobiles avec infrastructure . . . . .	6
1.5 Réseau mobile Ad Hoc . . . . .	6
1.5.1 Définition . . . . .	6
1.5.2 Historique . . . . .	6
1.5.3 Principe de fonctionnement . . . . .	7
1.5.4 Modélisation . . . . .	7
1.5.5 Modes de communication . . . . .	8
1.5.6 Caractéristiques des réseaux Ad Hoc . . . . .	9
1.5.7 Domaines d’applications . . . . .	10
1.5.8 Défis dans les réseaux Ad-Hoc . . . . .	11
1.6 Conclusion . . . . .	12
<b>Chapitre 2 Routage et qualité de service dans les réseaux Ad Hoc</b>	<b>14</b>
2.1 Introduction . . . . .	14
2.2 Routage dans les réseaux . . . . .	14
2.2.1 Définition . . . . .	14
2.2.2 Objectifs généraux du routage . . . . .	15
2.3 Routage dans les réseaux ad hoc . . . . .	15
2.3.1 Difficulté du routage dans les réseaux Ad hoc . . . . .	15

2.3.2	Contraintes de routages dans les réseaux ad hoc . . . . .	15
2.3.3	Protocoles de routage dans les réseaux Ad Hoc . . . . .	16
2.3.4	Classification des protocoles de routage . . . . .	17
2.4	Qualité de service (QoS) . . . . .	21
2.4.1	Définition . . . . .	21
2.4.2	Paramètres de la QoS . . . . .	22
2.4.3	Implémentation de la QoS . . . . .	23
2.4.4	Mécanismes QoS . . . . .	23
2.4.5	Routage avec QoS pour les réseaux Ad Hoc . . . . .	24
2.5	Conclusion . . . . .	25
<b>Chapitre 3 Protocole de routage AODV et ses variantes</b>		<b>27</b>
3.1	Introduction . . . . .	27
3.2	Protocole AODV . . . . .	27
3.2.1	Définition . . . . .	27
3.2.2	Terminologie d'AODV . . . . .	28
3.2.3	Table de routage et paquets de contrôle . . . . .	28
3.2.4	Table d'historique . . . . .	29
3.2.5	Structure des messages échangés . . . . .	30
3.2.6	Principe de fonctionnement . . . . .	33
3.2.7	Discussion . . . . .	35
3.3	Quelques protocoles basés sur AODV . . . . .	35
3.3.1	Protocole AOMDV . . . . .	35
3.3.2	Protocole MAODV . . . . .	36
3.3.3	Protocole QoS-MAODV . . . . .	37
3.3.4	Protocole ER-AODV . . . . .	37
3.3.5	Protocole QoS-AODV . . . . .	38
3.3.6	Protocole AODV-BR . . . . .	39
3.3.7	Protocole AODV-UU . . . . .	41
3.3.8	Protocole MER-AODV . . . . .	42
3.3.9	Protocole AODV-UI . . . . .	43
3.3.10	Protocole Bypass-AODV . . . . .	44
3.4	Comparaison du AODV et ses variantes . . . . .	45
3.5	Conclusion . . . . .	46
<b>Chapitre 4 Amélioration du protocole MAODV</b>		<b>48</b>
4.1	Introduction . . . . .	48
4.2	Protocole MAODV . . . . .	48

4.2.1	Présentation de protocole MAODV . . . . .	48
4.2.2	Format de message de GRouPe Hello (GRPH) . . . . .	49
4.2.3	Chef de groupe . . . . .	49
4.2.4	Table de routage . . . . .	50
4.2.5	Message de requête et message de réponse . . . . .	50
4.2.6	Réponse et activation de branches . . . . .	50
4.2.7	Opérations de maintenance . . . . .	51
4.3	Discussion des failles de MAODV . . . . .	52
4.3.1	Opérations de maintenance . . . . .	52
4.3.2	Maintenance du groupe de l'arbre . . . . .	53
4.4	Amélioration apportée à MAODV . . . . .	54
4.5	Exemple démonstratif de la solution proposée . . . . .	56
4.6	Conclusion . . . . .	58
	Conclusion générale et perspectives . . . . .	59

## Liste des Figures

Figure 1.1 : Réseaux mobiles sans infrastructure	6
Figure 1.2 : Exemple d'un réseau ad hoc simple	7
Figure 1.3 : Modélisation Un réseaux ah doc	7
Figure 1.4 : Changement de la topologie à cause de la mobilité	8
Figure 1.5 : Modes de communication	8
Figure 2.1 : Routage plat	18
Figure 2.2 : Routage hiérarchiques	18
Figure 3.1 : Format de table la de routage	29
Figure 3.2 : Format de la table d'historique	30
Figure 3.3 : Format de RREQ simple	30
Figure 3.4 : Format de la demande de route RREQ détaillée	30
Figure 3.5 : Format RREP simple	31
Figure 3.6 : Format de la demande de route RREP détaillée	31
Figure 3.7 : Format du message HELLO	32
Figure 3.8 : Format de l'erreur de route RRER	32
Figure 3.9 : Format de l'accusé de réponse de route RREP-ACK	33
Figure 3.10 : Inondation de RREQ et le renvoi du RREP	33
Figure 3.11 : Exemple de réparation locale d'une route perdu	34
Figure 3.12 : Arbre de partage	34
Figure 3.13 : Routage AODV-QOS source–destination	36
Figure 3.14 : Routage AODV-QOS destination.-source	38
Figure 3.15 : Protocole AODV-BR	40
Figure 3.16 : Diagramme d'activité pour un nœud source AODV-UU	41
Figure 3.17 : Diagramme d'activités pour un nœud destination AODV-UU	42
Figure 4.1 : Le format du message Group Hello .	49
Figure 4.2 : Ruptures de lien.	52
Figure 4.3 : Trafic normal de paquets.	53
Figure 4.4 : Cas de congestion.	53
Figure 4.5 : Echange de paquets de maintenance "HELLO".	53
Figure 4.6 : Champ « Mem » et le champ « compteur » au paquet RREQ.	54
Figure 4.7 :Routage choisir la route qui la petite moyenne de saturation.	54
Figure 4.8 : Prendre le critère de délai bout en bout.	55
Figure 4.9 : Paquet Rejeté.	55
Figure 4.10 : Algorithme d'amélioration.	56
Figure 4.11 : Exemple de découvertes des routes.	57



## Liste des Tableaux

Table 3.1 : Comparaison du AODV et ses variantes.	45
Table 4.1 : Calcul du compteur et du Mem.	57

## Liste des abréviations

AODV	Ad-hoc On demand Distance Vector
AOMDV	Ad-hoc On-demand Multipath Distance Vector
AODV-BR	AODV with Backup Routes
AODV-UI	AODV-University Indonesia
AODV-UU	AODV Upsala University
CGSR	Cluster-head gateway switch routing
DARPA	Defence Advanced Research Project Agency
DBF	Distribué de BellmanFord
DHCP	Dynamic Host Configuration Protocol
DREAM	Distance routing effect algorithm for mobility
DSDV	Destination Sequenced Distance Vector
ER-AODV	Energy Reverse Ad-hoc On demand Distance vector
FSR	Fisheye Source Routing
GSR	Global state routing
IBSS	Independent Basic Service Set
ICMP	Internet Control Message Protocol
LAR	Location-aided routing
MANET	Mobile Ad Hoc Network
MAODV	Multicast Ad-hoc On-demand Distance Vector
MER-AODV	Minimum Energy routing AODV
M-OLSR	Modified Optimized Link State Routing
OLSR	Optimized Link State Routing
ONR	Office Naval Research
Qos-AODV	Quality of Service-Ad-hoc On demand Distance Vector
QoS-MAODV	Quality of Service-Maodv
QoS	Quality of Service
R-AODV	Reverse AODV
RED	Random Early Discard buffer management
RERR	Route Error
RIPV2	Routing Information Protocol version 2

RREP-ACK	Route REPlY ACKnowledgment
RREQ	Route REQuest
RREP	Route REPlY
RTP	Real-Time Transport Protocol
TCP	Transmission Control Protocol
TTL	Time To Live
VANET	Vehicular Ad-hoc Network
WRP	Wireless Routing Protocol

# Introduction générale

Ces dernières années, l'évolution des technologies du sans-fil a ouvert de nouvelles perspectives dans le domaine des télécommunications. En particulier, les réseaux mobiles sans fil qui connaissent une forte expansion. Les réseaux mobiles offrent une grande flexibilité d'emploi en permettant aux utilisateurs de se déplacer librement, tout en continuant leurs communications. Les réseaux mobiles sans fil se répartissent en deux catégories : ceux avec infrastructure (les modèles cellulaires) et ceux sans infrastructure ou réseaux Ad hoc. Un réseau Ad Hoc est formé d'équipements sans-fil et mobiles qui s'auto organisent sans l'aide d'une quelconque infrastructure, ses équipements peuvent communiquer directement entre eux s'ils sont situés à portée radio.

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

Une fonctionnalité très importante des réseaux ad hoc est le routage. La notion de routage regroupe un ensemble de procédures assurant l'ouverture et l'entretien d'une communication entre deux nœuds. Il existe trois modes de communication pour les réseaux Ad Hoc : la communication unicast, la diffusion et la communication de groupe ou multicast. Les réseaux Ad Hoc peuvent être reliés à d'autres catégories de réseaux (LAN, WAN, . . .) et donc ils sont très utiles pour les communications de groupe. De nos jours, plusieurs travaux ont été menés sur de tels réseaux afin d'intégrer les applications temps réels telles que la voix ou la vidéo exigeant certaines contraintes au niveau des ressources offertes en

terme de délai et de bande passante. Parmi ces applications temps réels, nous pouvons citer la vidéo conférence qui nécessite en plus la communication de groupe.

Dans notre travail, nous avons choisi un protocole de routage réactif qui est utile pour les communications de groupe, c'est le protocole MAODV : Multicast Ad hoc On Demand Vector distance. pour ce protocole, nous avons apporté des modifications afin d'implémenter quelques contraintes de QoS pour les applications mobiles. L'objectif de ce mémoire est de faire une étude comparatives des protocoles basés sur le protocole AODV et de proposer une amélioration du protocole MAODV, en implémentant quelques critères de QoS.

Notre mémoire est subdivisé en quatre principaux chapitres. Le premier chapitre introduit un état de l'art sur les réseaux Ad Hoc, les différents types et caractéristiques des réseaux ad hoc. Dans le second chapitre, nous avons présenté le routage dans les réseaux ad hoc ainsi que la notion de qualité de service. Le troisième chapitre est consacré à l'analyse des spécifications du protocole de routage AODV et une brève description de quelques protocoles basés sur le protocole AODV, par exemple le protocole multicast MAODV. Le quatrième chapitre présente une amélioration du protocole MAODV étudié dans le troisième chapitre, en ajoutant quelques contraintes de QoS. Enfin, nous terminerons notre mémoire par une conclusion générale et perspectives.

# Chapitre 1

## Etat de l'art sur les réseaux Ad Hoc

# Chapitre 1

## Etat de l'art sur les réseaux Ad Hoc

### 1.1 Introduction

L'évolution récente de la technologie dans le domaine de la communication sans fil pousse aujourd'hui les chercheurs à faire des efforts pour mieux assurer la fonction des réseaux, à savoir l'accès rapide à l'information indépendamment du lieu et du temps. Le concept des réseaux ad hoc essaie d'étendre les notions de la mobilité à toutes les composantes de l'environnement. Ici, contrairement aux réseaux basés sur la communication avec infrastructure (cellulaire), aucune administration centralisée n'est disponible, ce sont les hôtes mobiles eux-mêmes qui forment une infrastructure du réseau. Aucune supposition ou limitation n'est faite sur la taille du réseau ad hoc, le réseau ad hoc peut contenir des centaines ou des milliers d'unités mobiles.

Dans ce chapitre, nous allons présenter les réseaux informatiques en général. Ensuite, nous parlerons des réseaux sans fil en particulier ces réseaux sont classés selon deux grandes catégories à savoir : les réseaux mobiles sans infrastructure et les réseaux avec infrastructure mobile. Après cela, nous définissons les réseaux mobiles Ad Hoc, en discuterons la modélisation et ses modes de communication. Ensuite, nous énumérons les différentes caractéristiques des réseaux Ad Hoc, nous citerons quelques applications et les défis liés aux réseaux Ad Hoc, nous terminons par une conclusion.

### 1.2 Réseaux informatiques

Les réseaux informatiques sont des réseaux de communication nés du besoin d'interconnecter un ensemble des équipements terminaux situés à distance les uns des autres. Pratiquement, ils misent à la disposition de ces équipements des ressources afin de transporter

les données d'une source à une ou plusieurs destinataires selon des règles bien définies. Dans un premier temps, ces communications étaient destinées au transport des données informatiques. Aujourd'hui, avec la numérisation, les réseaux informatiques seront aptes à transporter de nombreux types de données (données numériques sous forme d'une série des valeurs binaires), où, l'intégration de la parole téléphonique (voix) et de la vidéo est généralisée dans les réseaux informatiques tout en formant ainsi un environnement vital aux applications multimédias[1].

### 1.3 Réseaux sans fil

Un réseau sans fil (en anglais Wireless Network) est, comme son nom l'indique, un cas particulier des réseaux informatiques dans lequel au moins deux équipements (ordinateur, PDA, imprimante, routeur...) peuvent communiquer sans liaison filaire (indépendamment des prises murales). Néanmoins, il recourt à des ondes hertziennes (radio et infrarouges) comme un support de transmission. Il est plutôt considéré comme une extension de réseau filaire existant, et non pour le remplacer, offrant l'avantage d'une connectivité sans fil. Les équipements terminaux qui se trouvent à l'intérieur de la zone couverte par le réseau peuvent communiquer directement ou par l'intermédiaire d'une borne d'accès (points d'accès ou stations de base) jouant le rôle de routeur. Les communications entre les bornes d'accès peuvent être hertziennes ou par câble[1].

### 1.4 Classification des réseaux mobiles selon l'infrastructure

Les réseaux mobiles peuvent être divisés en deux classes à savoir : les réseaux mobiles basés sur une infrastructure et les réseaux mobiles sans infrastructure[2].

#### 1.4.1 Réseaux mobiles sans infrastructure

En mode sans infrastructure, également appelé le mode IBSS (Independent Basic Service Set) ou le mode ad hoc, tous les sites du réseau sont mobiles et se communiquent d'une manière directe (point à point) en utilisant leurs interfaces de communication sans fil sans besoin d'un point d'accès (voir Figure 1.1). Il n'y a aucune infrastructure fixe. Les



nœuds doivent être dans la portée de communication de chacun d'entre eux pour assurer les échanges.

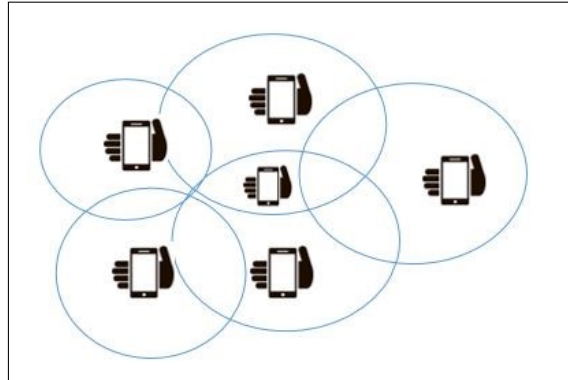


Figure 1.1 : réseaux mobiles sans infrastructure.

### 1.4.2 Réseaux mobiles avec infrastructure

Un réseau mobile avec infrastructure est un ensemble de nœuds mobiles dont son fonctionnement est géré par un système centralisé appelé station de base[3].

## 1.5 Réseau mobile Ad Hoc

### 1.5.1 Définition

Un réseau ad hoc est constitué d'un ensemble d'unités mobiles communiquant via un médium radio et qui ne requiert ni infrastructure fixe ni administration centralisée. De ce fait, les unités mobiles sont obligées de se comporter comme des routeurs qui participent à la découverte et à la maintenance des chemins pour les autres hôtes du réseau. Dans un réseau Ad Hoc, un nœud peut communiquer directement (mode point-à-point) avec n'importe quel nœud s'il est situé dans sa zone de transmission, tandis que la communication avec un nœud situé en dehors de sa zone de transmission s'effectue via plusieurs nœuds intermédiaires (mode multi-sauts)[4]

### 1.5.2 Historique

A l'origine, les réseaux ad-hoc mobiles ont été introduits pour améliorer les communications dans le domaine militaire, vu la nature dynamique de leurs opérations et champs d'action. Les recherches sur ces réseaux ont été financées par le gouvernement américain et supervisées principalement par le DARPA (Defence Advanced Research Project Agency) et l'ONR (the Office Naval Research) en 1994. Aujourd'hui, avec l'émergence des standards tels que Bluetooth, HiperLan et IEEE 802.11, les projets de recherches civiles dans

ce domaine ont afflué de partout dans le monde[5].

### 1.5.3 Principe de fonctionnement

Dans un réseau ad hoc, deux nœuds s'échangent des données sous la forme de paquets à l'aide de nœuds appelés nœuds relais (ou nœuds intermédiaire). Pour cela, le nœud source transmet les paquets à ses voisins. Si le nœud n'est pas la destination du paquet, un nœud relais transmet un paquet à ses voisins, et les voisins transmettent à leurs voisins, jusqu'à ce que le paquet ait atteint la destination (voir Figure 1.2)[6].

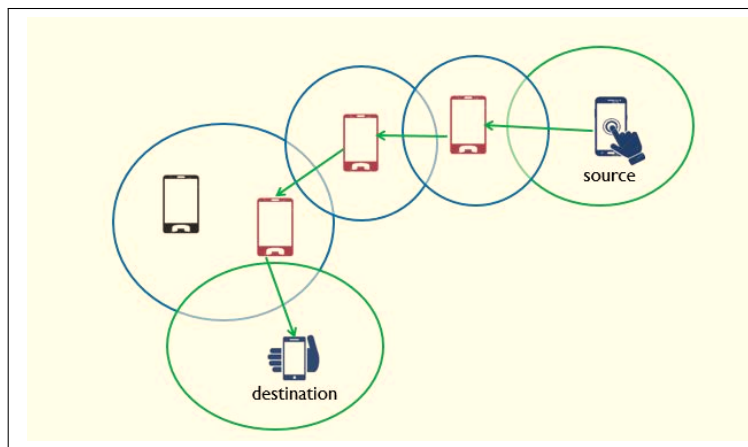


Figure 1.2 : Exemple d'un réseau ad hoc simple.

### 1.5.4 Modélisation

Un réseau Ad Hoc peut être modélisé par un graphe  $G_t=(V_t,E_t)$ .ou :  $V_t$  représente l'ensemble des nœuds (i.e. les unités mobiles ) du réseaux et  $E_t$  est l'ensemble des connexions qui existent entre ces nœuds. Si  $e=(u,v)$  appartient à  $E_t$  cela veut dire que  $u$  et  $v$  sont en mesure de communiquer directement à l'instant  $t$  sinon  $u$  doit passer par des nœuds intermédiaires pour atteindre  $v$  (voir Figure 1.3 ) [7] :

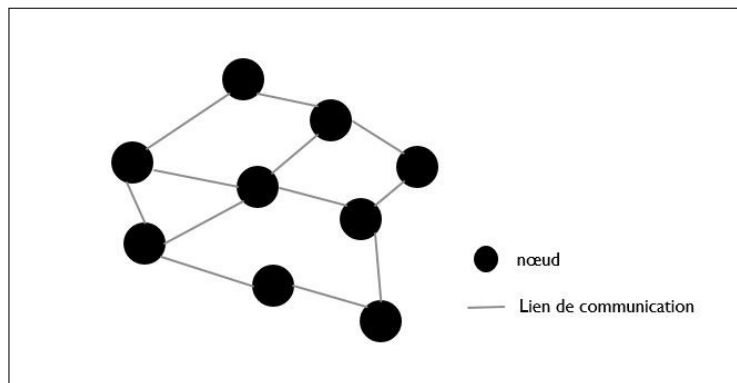


Figure 1.3 : Modélisation d'un réseau Ad Hoc.

La topologie des réseaux peut changer à tout moment, elle est donc dynamique et imprévisible ce qui fait que la déconnexion des unités soit très fréquente. La figure 1.4 montre un exemple de changement de la topologie à cause de la mobilité des nœuds sans fil. Chaque fois qu'un nœud bouge, les tables de routage doivent être recalculées pour prendre en compte les mises à jour. soient A,B,C et d des entités mobiles. A l'instant t1, nous observons dans la figure 1.4 que la route de A vers B est le lien direct  $A \mapsto B$ , si nous considérons le nombre de sauts comme métrique de routage. A l'instant t2, la topologie change : B n'est plus à portée radio avec A, alors le lien n'existe plus. De ce fait, la route de A vers B change et devient :  $A \mapsto F \mapsto B$ . Les nœuds bougent encore à l'instant t3, B s'éloigne de F alors la route qui existe pour l'atteindre devient  $A \mapsto E \mapsto C \mapsto B$ [8].

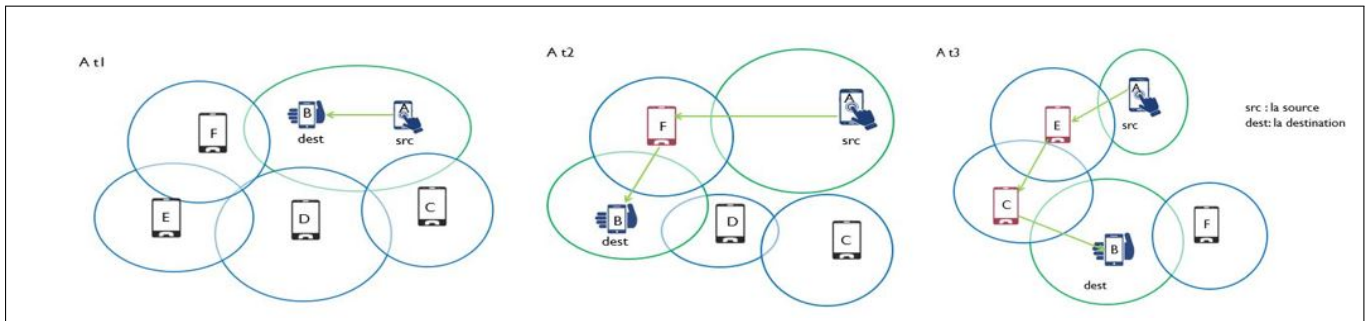


Figure 1.4 : Changement de la topologie à cause de la mobilité.

### 1.5.5 Modes de communication

Les échanges de données dans les réseaux mobiles utilisent trois modes de communications suivants[2] :(voir la figure 1.5)

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

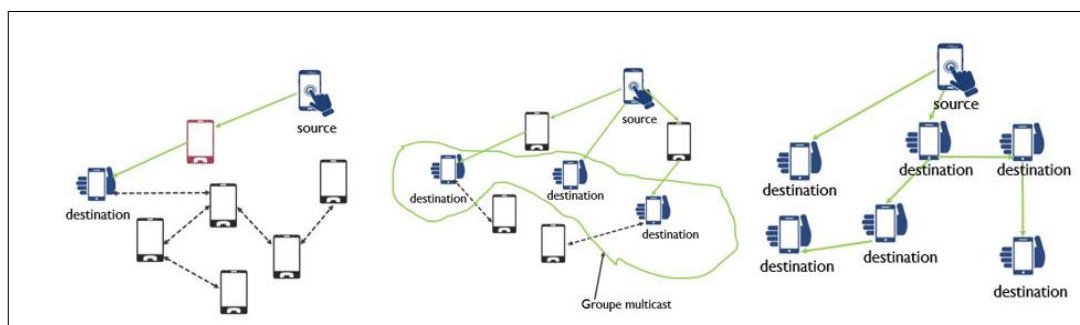


Figure 1.5 : Modes de communication.

## 1.5.6 Caractéristiques des réseaux Ad Hoc

il existe plusieurs caractéristiques des réseaux Ad Hoc :

### 1.5.6.1 Sans infrastructure

Les nœuds d'un réseau Ad Hoc travaillent dans un environnement totalement distribué, ce qui leur permet de se déplacer librement, Cette caractéristique donne plus de liberté aux nœuds. Mais ces derniers doivent assurer des fonctionnalités supplémentaires par rapport aux nœuds d'un réseau sans fil avec infrastructure, puisqu'ils doivent agir en tant que routeurs pour relayer la communication des autres nœuds [4].

### 1.5.6.2 Mobilité et topologie dynamique

Les unités mobiles du réseau, se déplacent d'une façon libre et arbitraire, elles peuvent accéder au réseau ou en sortir. De ce fait, la topologie du réseau peut changer, à des instants imprévisibles de manière rapide et aléatoire, les liens de la topologie peuvent être unidirectionnels ou bidirectionnels. Le changement de la topologie change les routes entre les nœuds et provoque la perte de paquets.

### 1.5.6.3 Contraintes de ressources

Les hôtes mobiles sont alimentés par des sources d'énergie autonomes comme les batteries ou les autres sources consommables. Le paramètre d'énergie doit être pris en considération dans tout contrôle fait par le système.

### 1.5.6.4 Bande passante limitée

Une des caractéristiques primordiales des réseaux basés sur la communication sans fil est l'utilisation d'un médium de communication partagé (ondes radio). Ce partage fait que la bande passante réservée à un hôte soit modeste.

### 1.5.6.5 Sécurité physique limitée

Les réseaux mobiles Ad Hoc sont plus touchés par le paramètre de sécurité que les réseaux filaires classiques. Cela se justifie par les contraintes et limitations physiques qui font que le contrôle des données transférées doit être minimisé.

### 1.5.6.6 Erreur de transmission

Les erreurs de transmission radio sont plus fréquentes dans les réseaux ad hoc que dans les réseaux filaires .

### 1.5.6.7 Interférences

Les liens radios ne sont pas isolés, deux transmissions simultanées sur une même fréquence utilisant des fréquences proches peuvent interférer.

## 1.5.7 Domaines d'applications

Les réseaux Ad Hoc sont utilisés dans toutes les applications où le déploiement d'une architecture centralisée est contraignant, voire impossible. En effet, la robustesse, le coût réduit et le déploiement rapide qu'ils présentent leur confèrent un accès à une large palette d'applications dont :[7].

### 1.5.7.1 Applications militaires

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

### 1.5.7.2 Opérations de secours

Dans les zones touchées par les catastrophes naturelles (cyclone, séisme, etc.), le déploiement d'un réseau Ad Hoc est indispensable pour permettre aux unités de secours de communiquer.

### 1.5.7.3 Utilisation à des fins éducatives

Le déploiement d'un réseau Ad Hoc lors d'une conférence ou d'une séance de cours est très judicieux car cela permet aux chercheurs et étudiants de partager des ressources (fichiers, accès à internet... etc.) et de communiquer sans avoir besoin d'une quelconque infrastructure.

### 1.5.7.4 Applications industrielles

Des scénarios plus complexes dans le domaine industriel appelés réseaux de capteurs peuvent former un MANET pour s'adapter à différents environnements. Un exemple d'une telle application est la formation d'un MANET pour la surveillance médicale, la détection des Feux de forêt, la surveillance des volcans... .

### 1.5.7.5 Mise en œuvre des réseaux véhiculaires

Sur un réseau routier les véhicules peuvent avoir besoin de communiquer entre eux ou avec leur environnement afin de partager des informations dans le but de gérer et réguler le trafic routier. Les réseaux Ad Hoc sont alors la solution idéale.

## 1.5.8 Défis dans les réseaux Ad-Hoc

En raison de la topologie dynamique, des réseaux ad hoc, ces derniers doivent faire face à des défis en matière de routage et de sécurité qui sont détaillés ci-dessous[9].

### 1.5.8.1 Routage

Chaque appareil dans un réseau ad-hoc est libre de se déplacer indépendamment dans n'importe quelle direction, et changera donc fréquemment ses liens avec les autres appareils. Chaque appareil, achemine un trafic qui n'est pas propre à lui, et sera donc un routeur. Le principal défi dans la construction d'un réseau ad-hoc est d'équiper chaque appareil pour maintenir en permanence les informations nécessaires pour acheminer le trafic correctement. Ils peuvent contenir un ou plusieurs émetteurs-récepteurs différents entre les nœuds. Un protocole de routage ad hoc est une convention, ou une norme, qui contrôle la façon dont les nœuds décident de la manière d'acheminer les paquets entre les dispositifs informatiques dans le réseau mobile ad hoc. La garantie de livraison et la capacité à gérer la connectivité dynamique sont les défis les plus importants pour les protocoles de routage dans les réseaux ad hoc. Si la connectivité de deux nœuds change et que les routes sont affectées par ce changement, le protocole de routage devrait être capable de rechercher un autre chemin.

### 1.5.8.2 Sécurité

Garantir les services de sécurité nécessaires est primordiales pour le bon fonctionnement des réseaux ad hoc. Ceci dit en raison des caractéristiques spéciales de ces derniers, fournir ces services fait face à de nombreux défis :

- **Disponibilité** : Selon ce service, chaque nœud autorisé doit avoir accès à toutes les données et services dans le réseau. Le défi de la disponibilité est dû à la topologie dynamique des réseaux ad-hoc et leur frontière ouverte. Le temps d'accès i.e ,le temps nécessaire à un nœud pour accéder aux services réseau ou aux données est important, car

le temps est l'un des paramètres de sécurité. En utilisant beaucoup de niveaux de sécurité et d'authentification, ce service est ignoré.

- **Authentification :** Le but de ce service est de fournir des communications fiables entre deux différents nœuds. Lorsqu'un nœud reçoit des paquets d'une source, il doit être sûr de l'identité du nœud source. Une façon de fournir ce service consiste à utiliser des certifications, or en l'absence d'unité de contrôle, la distribution des clés et leur gestion sont problématiques.

- **Confidentialité :** Selon ce service, chaque nœud ou application doit avoir accès à des services spécifiés auxquels il a l'autorisation d'accéder. On utilise habituellement des méthodes de cryptage, mais dans les réseaux ad-hoc, il n'y a pas de gestion centrale, la distribution de clés est confrontée à de nombreux défis et dans certains cas elle est impossible.

- **Intégrité :** Selon le service de sécurité d'intégrité, seuls les nœuds autorisés peuvent créer, modifier ou supprimer des paquets. À titre d'exemple, l'attaque Man-In-The-Middle est contre ce service. Dans cette attaque, L'attaquant capture tous les paquets puis les supprime où les modifie. Les réseaux ad hoc sont très vulnérables face à une telle menace, ceci est due à leurs caractéristique de frontières ouvertes.

## 1.6 Conclusion

Le réseau Ad hoc manifeste beaucoup de simplicité et assez d'avantages par rapport aux autres réseaux (filaire et cellulaires) par sa facilité de déploiement en cas d'urgence ou de travaux temporaires, dont les autres réseaux engendrent des frais importants. Cependant de nouveaux problèmes apparaissent, en effet l'absence d'une infrastructure centralisée fait du routage dans les réseaux ad hoc un problème très compliqué. Dans la plupart des cas, le nœud destination ne se trouve pas obligatoirement dans la portée du nœud source ce qui implique que l'échange des données entre les deux nœuds, doit être effectué par des stations intermédiaires. Par ailleurs, la topologie de ces réseaux qui peuvent être continuellement mobile, oblige les protocoles de routage à réagir rapidement.

Après avoir présenté les réseaux ad hoc, une étude sur le routage et la qualité de services dans ce dernier sera faite dans le prochain chapitre .

## Chapitre 2

### Routage et qualité de service dans les réseaux Ad Hoc



# Chapitre 2

## Routage et qualité de service dans les réseaux Ad Hoc

### 2.1 Introduction

Pour acheminer un paquet du nœud source au nœud destinataire, nous avons besoin d'un protocole de routage. Le but du protocole de routage est de trouver la meilleure route selon les critères précis de la qualité de service souhaitée (délai, taux de perte, quantité de bande passante, ...), et reposant sur des liens fiables.

Dans ce chapitre, Nous allons décrire les différents défis liés au routage dans les réseaux Ad Hoc et nous citerons la classification des protocoles de routage, Nous parlerons également sur la qualité de service et enfin nous terminerons ce chapitre par une conclusion.

### 2.2 Routage dans les réseaux

#### 2.2.1 Définition

Le routage est une méthode d'acheminement des informations à la bonne destination à travers un réseau de connexion donné (transiter une information depuis un émetteur vers une destination). Il consiste à assurer une stratégie qui garantit, à n'importe quel moment, un établissement de routes qui soient correctes et efficaces entre n'importe quelle paire de nœuds appartenant au réseau, ce qui assure l'échange des messages d'une manière continue[10].

### 2.2.2 Objectifs généraux du routage

- Calcul et maintenance des meilleures routes dans un contexte de topologie dynamique
- Limiter les temps de latence.
- Minimiser les coûts en temps de calcul et en mémoire.
- Minimiser le trafic propre au routage (taille et nombre de messages)[11].

## 2.3 Routage dans les réseaux ad hoc

Dans le cas des réseaux ad hoc, l'architecture est caractérisée par une absence d'infrastructure fixe, les nœuds doivent donc s'organiser automatiquement et réagir rapidement aux différents mouvements. Ainsi, dans le cas des réseaux ad hoc, les nœuds sont considérés comme des routeurs, chaque nœud participe dans le fonctionnement de routage, c'est à dire chaque nœud est responsable de relayer le trafic (contrôle de données) des autres nœuds [10].

### 2.3.1 Difficulté du routage dans les réseaux Ad hoc

De fait qu'un réseau ad hoc est un ensemble de nœuds mobiles qui sont dynamiquement et arbitrairement éparpillés d'une manière ou l'interconnexion entre les nœuds peut changer à tout moment. Il se peut qu'un hôte destination soit hors de la portée de communication d'un hôte source, ce qui nécessite l'emploi d'un routage interne par les nœuds intermédiaires afin de faire acheminer les paquets de message à la bonne destination.

En effet, la topologie évoluant constamment en fonction des mouvements des nœuds mobiles, Le problème qui se pose dans le contexte des réseaux Ad Hoc 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 calcul et de sauvegarde.

Dans la pratique, il est impossible qu'un hôte puisse garder les informations de routage concernant tous les autres nœuds, dans le cas où le réseau serait volumineux[12].

### 2.3.2 Contraintes de routages dans les réseaux ad hoc

L'étude et la mise en œuvre d'algorithmes de routage pour assurer la connexion des réseaux ad hoc au sens classique du terme (tout sommet peut atteindre tout autre), est un problème complexe. L'environnement est dynamique et évolue au cours du temps,

la topologie du réseau peut changer fréquemment. Il semble donc important que toute conception de protocole de routage doit étudier les problèmes suivants[7] :

### **2.3.2.1 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.

### **2.3.2.2 Offrir des communications multipoints fiables**

Le fait que les chemins utilisés pour router les paquets de données puissent évoluer, ne doit pas avoir d'incident sur le bon acheminement des données. L'élimination d'un lien, pour cause de panne ou pour cause de mobilité devrait, idéalement, augmenter le moins possible les temps de latence[12].

### **2.3.2.3 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[13].

### **2.3.2.4 Temps de latence**

La qualité des temps de latence et de chemins doit augmenter dans le cas où la connectivité du réseau augmente.

## **2.3.3 Protocoles de routage dans les réseaux Ad Hoc**

### **2.3.3.1 Définition**

Comme nous avons déjà vu, un réseau ad hoc 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. Dans la plupart des cas, l'unité destination ne se trouve pas obligatoirement dans la portée de l'unité source ce qui implique que l'échange des données entre deux nœuds quelconques, doit être effectué par des stations intermédiaires. La stratégie de routage est utilisée dans le but de découvrir les chemins qui existent entre les nœuds. Le but principal d'une telle stratégie est l'établissement de routes qui soient correctes et efficaces entre une paire quelconque d'unités, ce qui assure

l'échange des messages d'une manière continue. Vu les limitations des réseaux ad hoc, la construction des routes doit être faite avec un minimum de contrôle et de consommation de la bande passante. Il existe deux grandes familles de protocoles de routage : les protocoles basés sur l'état des liens, et ceux basés sur le vecteur de distance[33].

### **2.3.3.2 Protocoles basés sur l'état des liens**

La famille des protocoles à état de liens se base sur les informations rassemblées sur l'état des liens dans le réseau. Ces informations sont disséminées dans le réseau périodiquement ce qui permet ainsi aux nœuds de construire une carte complète du réseau. Un nœud qui reçoit les informations concernant l'état des liens, met à jour sa vision de la topologie du réseau et applique un algorithme de calcul des chemins optimaux afin de choisir le nœud suivant pour une destination donnée. Un exemple des algorithmes les plus connus appliqué dans le calcul des plus courts chemins, est celui de Dijkstra.

### **2.3.3.3 Protocoles à vecteur de distance**

Les protocoles à vecteur de distance se basent sur un échange, entre voisins, des informations de distances des destinations connues. Chaque nœud envoie à ses voisins la liste des destinations qui lui sont accessibles et le coût correspondant. Le nœud récepteur met à jour sa liste locale des destinations avec les coûts minimums. Le processus de calcul se répète, s'il y a un changement de la distance minimale séparant deux nœuds, et cela jusqu'à ce que le réseau atteigne un état stable. Cette technique est basée sur l'algorithme distribué de BellmanFord (DBF).

## **2.3.4 Classification des protocoles de routage**

Les protocoles de routage destinés aux réseaux mobiles ad hoc peuvent être classés de différentes manières, selon plusieurs critères. Ils peuvent être classés selon leurs architectures (uniformes ou non uniformes), leurs approches de routage (protocole proactif, réactif, hybride ou géographique), et leurs modes de communication (unicast, multicast, broadcaste).

### **2.3.4.1 Classification selon architecture**

La première classification des protocoles de routage ad hoc concerne le type de vision qu'ils ont du réseau et les rôles qu'ils accordent aux différentes unités mobiles. Ce critère divise les protocoles de routage en deux classes [14].

- **Protocoles de routage uniformes**

Les protocoles de routage uniformes "à plat" considèrent que tous les nœuds sont égaux (figure 2.1), dans le même niveau hiérarchique et possèdent ainsi, les mêmes rôles et fonctions. Par conséquent, aucune hiérarchie n'est définie entre les nœuds du réseau, chaque nœud envoie et reçoit des messages de contrôle de routage. La décision d'un nœud de router des paquets pour un autre dépendra de sa position. Parmi les protocoles utilisant cette technique, on cite l'AODV (Ad hoc on Demand Distance vector).

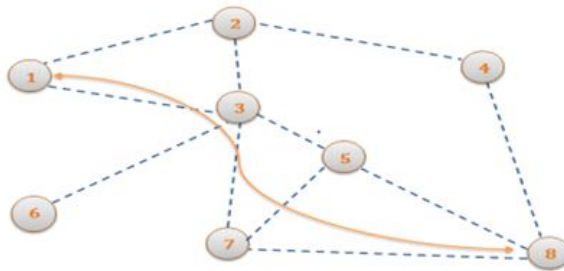


Figure 2.1 : Routage plat.

- **Protocoles de routage non uniformes**

Les protocoles de routage non uniformes "hiérarchiques" tentent de limiter la complexité du routage en réduisant le nombre de nœuds qui contribuent à la détermination des routes. Ils fonctionnent en confiant aux mobiles des rôles qui varient de l'un à l'autre. Une structure hiérarchique entre les nœuds est définie selon leurs fonctions. Certains nœuds sont élus et assument des fonctions particulières qui conduisent à une vision en plusieurs niveaux de la topologie du réseau. Par exemple, un mobile pourra servir de passerelle pour un certain nombre de nœuds qui sont reliés à lui. Le routage en sera simplifié, puisqu'il se fera de passerelle à passerelle, jusqu'à la destination. Un exemple est donné par la figure 2.2, où le nœud 1 passe par les passerelles P1, P2 et P3 pour atteindre le nœud 7.

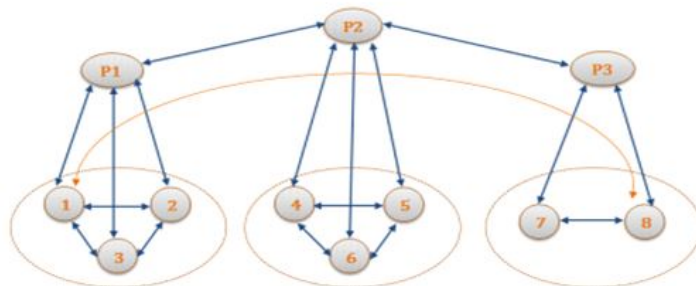


Figure 2.2 : Routage hiérarchique.

### 2.3.4.2 Classification selon l'approche de routage

Dans cette classification basée sur le mécanisme d'établissement de la route, nous distinguons deux grandes catégories : le routage proactif et le routage réactif. A ces deux familles, on ajoutera d'autres propositions plus ou moins hybrides impliquant par exemple la création de structure interne au réseau, ou s'appuyant sur la supposition que chaque nœud du réseau connaît sa position dans un plan[2].

#### • Protocoles proactifs

Un protocole de routage est dit proactif si les procédures de création et de maintenance des routes, durant la transmission des paquets de données, sont contrôlées périodiquement. Dans le routage proactif, chaque nœud maintient une ou plusieurs tables contenant l'information de routage vers chacun des autres nœuds du réseau. Tous les nœuds mettent leurs tables à jour de façon à maintenir une vue consistante et réelle du réseau. Lorsque la topologie du réseau change, les nœuds propagent des messages de mise à jour à travers le réseau afin de garder cette consistance et de garder à jour l'information de routage pour l'ensemble du réseau. Ces protocoles diffèrent sur la manière par laquelle des changements de topologies sont distribués à travers le réseau et sur le nombre de tables nécessaires au routage. Il existe plusieurs protocoles connus de cette catégorie, à titre d'exemples, nous pouvons citer DSDV, OLSR, GSR, WRP, FSR, CGSR[2].

#### • Avantages et inconvénients des protocoles proactifs

Avec un protocole proactif, les routes sont disponibles immédiatement, ainsi l'avantage d'un tel protocole est le gain de temps lors d'une demande de route. Le problème est que, les changements de routes peuvent être plus fréquents que la demande de la route et le trafic induit par les messages de contrôle et de mise à jour des tables de routage peut être important et partiellement inutile, ce qui gaspille la capacité du réseau sans fil. De plus, la taille des tables de routage croît linéairement en fonction du nombre de nœud. De ce fait, un nouvel type de protocole est apparu, il s'agit des protocoles de routage réactifs [15].

#### • Protocoles réactifs

Dans ces protocoles, la mise à jour ou le contrôle des routes se fait à la demande, c'est-à-dire, lorsqu'une source veut transmettre des paquets de données vers une destination. Les protocoles réactifs représentent les protocoles les plus récents proposés dans le but d'assurer le service de routage dans les réseaux sans fil. Ces protocoles suivent une politique radicalement opposée à celle des protocoles proactifs. Ici aucune maintenance régulière n'est effectuée. Les protocoles de routage appartenant à cette catégorie, créent

et maintiennent les routes selon leurs besoins. Lorsque le réseau a besoin d'une route, une procédure de découverte globale de routes est lancée, et ce, dans le but d'obtenir une information spécifique. Cette information reste valide tant que la destination est joignable ou jusqu'à ce que la route devienne inutile[2].

### • **Avantages et inconvénients des protocoles réactifs**

A l'opposé des protocoles proactifs, dans le cas d'un protocole réactif, aucun message de contrôle ne charge le réseau pour des routes inutilisées ce qui permet de ne pas gaspiller les ressources du réseau. Mais la mise en place d'une route par inondation peut être coûteuse et provoquer des délais importants avant l'ouverture de la route et les retards dépassent bien souvent les délais moyens admis par les logiciels, aboutissant à une impossibilité de se connecter alors que le destinataire est bien là . De ce fait, un nouvel type de protocole est apparu, il s'agit des protocoles de routage hybrides[15].

### • **Protocoles hybrides**

Les protocoles hybrides combinent les deux approches : celle des protocoles proactifs et celle des protocoles réactifs. Généralement, le réseau est divisé en deux zones et le principe est d'utiliser une approche proactive pour avoir des informations sur les voisins les plus proches, qui se trouvent au maximum à deux sauts du nœud mobile. Une approche réactive est utilisée au-delà de cette zone prédéfinie afin de chercher des routes.[2]

### • **Avantages et inconvénient des protocoles hybrides**

Le protocole hybride est un protocole qui se veut comme une solution mettant en commun les avantages des deux approches précédentes, en utilisant une notion de découpage du réseau. Cependant, il rassemble toujours quelques inconvénients des deux approches proactives et réactives [15].

### • **Protocoles géographiques**

Les protocoles de routage géographiques se différencient de ceux précédemment présentés par l'utilisation d'une donnée supplémentaire dans la recherche des routes : la position géographique des nœuds du réseau afin d'améliorer le processus de routage. Un système de localisation est donc mis en place afin de connaître à un instant donné la position des mobiles. Le GPS (Global Positioning System) est le système de localisation le plus utilisé même si d'autres algorithmes proposent de calculer la position des mobiles à l'aide d'autres paramètres comme par exemple la puissance du signal. Une fois que la position du mobile destinataire est évaluée, la diffusion des messages de recherche de route peut être orientée vers une direction précise, réduisant considérablement le trafic de décou-

verte de route . Nous donnons des exemples représentatifs des protocoles géographiques, le protocole LAR, DREAM et GPSR [2].

### 2.3.4.3 Classification selon le mode de communication

Cette classification concerne le type de destination lors des transmissions de paquets. [16]

- **Routage unicast**

C'est le type de routage le plus simple. Il consiste en une communication point-à-point entre les nœuds, on entend par là le fait de communiquer entre deux nœuds identifiés chacun par une adresse réseau unique. Exemple des protocoles de ce type de routage : AODV et OLSR.

- **Routage multicast**

Le routage multicast permet de diffuser un flux réseau depuis une source vers plusieurs destinations. Source et destinations sont alors réunies dans un groupe multicast. Ce type de routage est utilisé pour des applications du type télé séminaires (pas d'interaction des destinataires), téléconférences (chaque membre du groupe peut être source du flux), diffusion de tables de routage pour le protocole RIPv2, amorçage réseau à distance. Les protocoles MAODV et M-OLSR sont des protocoles multicast .

- **Routage Broadcast**

La communication dans le routage broadcast consiste à diffuser les données vers tous les nœuds du réseau. Quelques exemples des protocoles qui utilisent le broadcast sont DHCP et ICMP.

## 2.4 Qualité de service (QoS)

### 2.4.1 Définition

Dans les réseaux de télécommunication, l'objectif de la qualité de service est d'atteindre un meilleur comportement de la communication, pour que le contenu de cette dernière soit correctement acheminé, et que les ressources du réseau soient utilisées d'une façon optimale. La qualité de service peut être définie comme le degré de satisfaction d'un utilisateur des services fournis par un système de communication. La QoS est définie comme la capacité d'un élément du réseau (ex : routeur, nœud ou une application) de fournir un niveau de garantie pour un acheminement des données [13].



### 2.4.2 Paramètres de la QoS

La QoS peut se mesurer de manière quantitative, à l'aide notamment des paramètres suivants :

- **Gigue**

Elle peut apparaître en cas d'encombrement du réseau, de dérive temporelle ou de changement d'acheminement. Si elle est trop importante, la qualité de la communication vocale ou vidéo se dégrade.

- **Bande passante**

C'est la capacité maximale de transmission, d'un point à un autre, d'un volume de données sur une ligne de communication en un temps donné. La QoS optimise le réseau en gérant la bande passante et en hiérarchisant les applications selon les ressources dont elles ont besoin.

- **Disponibilité du service**

Elle désigne la fiabilité de la connexion des utilisateurs à l'appareil Internet.

- **Délai**

C'est le temps nécessaire à un paquet pour traverser le réseau d'un bout à l'autre.

- **Délai Jitte**

Délai Jitte est la variation du délai rencontrée par des paquets similaires suivant le même itinéraire à travers le réseau.

- **Débit**

Le débit est la quantité de données qui transite sur un réseau pendant une durée déterminée.

- **Taux de perte de paquets**

C'est le taux auquel les paquets sont perdus ou endommagés (certains bits sont modifiés dans le paquet) en passant par le réseau.

### 2.4.3 Implémentation de la QoS

Il existe trois modèles d'implémentation de la QoS : l'obligation de moyens, les services intégrés et les services différenciés[34].

- L'obligation de moyen (Best Effort) est un modèle de qualité de service sans hiérarchie entre les paquets et sans garantie de livraison des paquets. Ce modèle s'applique lorsqu'aucune politique de QoS n'est configurée sur un réseau ou quand l'infrastructure est incompatible avec la QoS.
- Les services intégrés (IntServ) sont un modèle qui réserve de la bande passante sur un chemin spécifique du réseau. Les applications demandent au réseau de réserver une ressource et les équipements réseau surveillent le flux des paquets pour s'assurer que les ressources réseau sont en mesure de les accepter.
- Les services différenciés (DiffServ) sont un modèle de qualité de service dans lequel les éléments du réseau (routeurs, commutateurs) sont configurés pour traiter différentes classes de trafic selon des priorités différentes. Le trafic réseau doit être répertorié en classes selon les critères de l'entreprise.

### 2.4.4 Mécanismes QoS

Les mécanismes QoS appartiennent à différentes catégories selon leur rôle dans la gestion du réseau [24].

- Les outils de classification et de marquage différencient les applications entre elles et trient les paquets selon les types de trafic. Le marquage estampille chaque paquet comme appartenant à une classe réseau que les équipements du réseau seront en mesure de reconnaître. La classification et le marquage sont implémentés sur les équipements réseau comme les routeurs, les commutateurs et les points d'accès.
- Les outils de gestion des encombrements vont placer les paquets dans les files d'attente en fonction de leur classification et de leur marquage. Ils incluent la mise en file d'attente selon la priorité, la méthode du premier entré, premier sorti et la mise en file d'attente de faible latence.
- Les outils de prévention des encombrements guettent les goulets d'étranglement sur

le trafic réseau et, s'ils en trouvent, ignorent les paquets de faible priorité. Ils utilisent notamment la détection précoce aléatoire pondérée (WRED) et la détection précoce aléatoire (RED).

- Les outils d'efficacité des liaisons optimisent l'utilisation de la bande passante et évitent aux paquets d'arriver en retard sur le réseau. Si leur usage ne se limite pas à la QoS, ces outils sont utilisés conjointement à d'autres mécanismes QoS. Ils comprennent la compression des en-têtes du protocole de transport en temps réel (RTP, Real-Time Transport Protocol).

### 2.4.5 Routage avec QoS pour les réseaux Ad Hoc

Généralement, dans un réseau, le routage permet d'établir une route de plus court chemin en terme de distance ou de délai entre deux noeuds source et destination. Dans le cadre d'une qualité de service, le but du protocole de routage est de trouver la meilleure route selon les critères précis de la qualité de service souhaitée (délai, taux de perte, quantité de bande passante, ...), et reposant sur des liens fiables.

Ce dernier point est à la fois important et difficile à assurer dans le cas des réseaux ad hoc en raison de leur topologie dynamique. Les noeuds constituant le réseau ad hoc doivent stocker et mettre à jour les états des liens dans un environnement qui est mobile. Ce processus est donc très complexe et couteux car des ruptures de liens peuvent intervenir à tout moment beaucoup plus fréquemment que dans des réseaux classiques[20].

## 2.5 Conclusion

Dans ce chapitre, nous avons discuté du concept et des problèmes de routage dans les réseaux ad hoc. Le routage est nécessaire pour faire fonctionner les réseaux ad hoc mais il est très difficile car il ne prend pas en compte les changements fréquents de sa structure, la consommation de bande passante limitée et d'autres facteurs. Nous avons aussi abordé la notion de QoS ainsi que ses différents paramètres et l'intérêt d'intégrer la QoS au routage dans les réseaux Ad Hoc.

## Chapitre 3

### Protocole de routage AODV et ses variantes

# Chapitre 3

## Protocole de routage AODV et ses variantes

### 3.1 Introduction

Dans ce chapitre, nous allons présenter AODV et ses variantes, en commençant par une étude détaillée sur le protocole de routage AODV et sa manière d'agir, nous décrirons par la suite, les différents protocoles basés sur AODV.

### 3.2 Protocole AODV

#### 3.2.1 Définition

Le protocole AODV (Ad hoc On-Demand Distance Vector Routing Protocol) est un protocole de routage réactif de type vecteur de distance, conçu par Charles E. Perkins et Elizabeth M. Royer, qui a été normalisé avec la RFC de l'IETF.

Ce protocole est devenu très connu et a fait l'objet d'un grand nombre de recherches. Il est tout à fait adapté aux réseaux mobiles ad hoc de par sa prise en charge de la mobilité des nœuds dans le réseau. Ce protocole permet à des nœuds mobiles d'obtenir des routes rapidement pour les nouvelles destinations sans maintenir des routes pour lesquelles il n'existe pas de communication active, ainsi l'établissement d'une rte se fait uniquement en cas de besoin, Si un nœud source veut envoyer des paquets de données vers un nœud destination, il doit établir et maintenir une route vers ce nœud destination durant le temps qu'il en fait usage [13].

### 3.2.2 Terminologie d'AODV

Dans ce qui suit nous allons définir quelques terme que nous allons utilisé lors de de la présentation de mécanisme de protocole AODV.

#### 3.2.2.1 Itinéraire actif

Une entrée de table de routage avec une métrique finie dans la zone de comptage de saut. Une table de routage peut contenir les entrées qui ne sont pas en activité (les itinéraires ou les entrées inaccessibles). Ils ont une métrique infinie dans la zone de comptage de saut. Seulement des entrées actives peuvent être employées pour expédier des paquets de données, les entrées inaccessibles sont par la suite supprimées. [18]

#### 3.2.2.2 Nœud intermédiaire

Un nœud qui accepte d'expédier des paquets destinés pour des autres nœuds, en les retransmettant à un prochain saut qui est plus près de la destination le long d'un chemin qui a été installé en utilisant des messages de contrôle de routage.

#### 3.2.2.3 Chemin (route )

Une installation d'itinéraire pour envoyer des paquets de données d'un nœud lançant une opération de découverte d'itinéraire vers sa destination désirée.

#### 3.2.2.4 Nœud source

Un nœud qui lance un message AODV à traiter et être probablement retransmis par d'autres nœuds dans le réseau Ad Hoc. Par exemple, le nœud lançant un procédé de découverte d'itinéraire et envoie le message RREQ (Route Request) s'appelle le nœud origine du message de RREQ.

### 3.2.3 Table de routage et paquets de contrôle

Le protocole AODV (Ad-hoc On demand Distance Vector) représente essentiellement une amélioration de l'algorithme proactif DSDV(Destination Sequenced Distance Vector). 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 », en plus du routage nœud par nœud. 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 les routes maintenues par certains nœuds, deviennent invalides. Les numéros de séquence permettent d'utiliser les routes les plus récentes ou autrement dit les plus fraîches (fresh routes). 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. Les informations sur les routes doivent être conservées même pour les liaisons de courtes durées. La structure de cette table est présentée dans la figure suivante [18].

<b>@D</b>	<b>#SN</b>	<b>Valid_SN</b>	<b>State</b>	<b>Iinterface</b>	<b>#HC</b>	<b>@NH</b>	<b>PL</b>	<b>LT</b>

Figure 3.1 : Format de la table de routage.

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

### 3.2.4 Table d'historique

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

- \* ID : Identifiant de la demande de route RREQ.



- \* @S : Adresse de source.
- \* LT : Temps au-delà duquel l'entrée sera effacée.

#ID	@S	LT

Figure 3.2 : Format de la table d'historique.

### 3.2.5 Structure des messages échangés

#### 3.2.5.1 Demande de route RREQ (Route REQuest)

Ce message est diffusé lorsqu'un nœud détermine qu'il a besoin d'une route vers une destination et ne dispose pas d'une route disponible. C'est le cas lorsque la destination est inconnue ou lorsqu'une route précédemment valide dans sa table de routage expire ou est marquée invalide. Le nœud crée le paquet présenté dans la figure 3.3 et le format détaillé est présenté dans la figure 3.4 [19].

@source	Num,seq source	Broadcast id	@Destination	Num,seq Destination	Nombre de saut
---------	----------------	--------------	--------------	---------------------	----------------

Figure 3.3 : Format de RREQ simple .

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Type = 1								J	R	G	D	U	Reserved								#HC										
#ID - RREQ Identifier																															
@D - Destination IP Address																															
#SND - Destination Sequence Number																															
@Src - Source IP Address																															
#SNS - Source Sequence Number																															

Figure 3.4 : Format de la demande de route RREQ détaillée.

- \* Type (8 bits) : ce champ indique le type de paquet, dans ce cas il prend la valeur 1.
- \* Flags (drapeaux) (5 bits) : ce champ contient cinq flags (J, R, G, D, U) tel que :
  - J : Join flag, réservé au multicast.
  - R : Repair flag, réservé au multicast.
  - G : Gratuitous RREP flag : indique la nécessité de générer une réponse de route vers la destination en plus de celle générée vers la source pour l'informer qu'une telle source

cherche à la joindre et ainsi un chemin bidirectionnel est établie. Une RREP de ce genre (gratuitous) est généré seulement lorsqu'il s'agit d'un nœud intermédiaire qui répond.

- D : Destination only flag : indique que seulement la destination doit répondre à cette demande de route.
- U : Unknown Sequence Number : indique que le numéro de séquence de la destination est inconnue.
- \* Reserved : mis à zéro lors de l'envoi et ignorés à la réception.
- \* #HC (Hop Count) : Le nombre de saut de la source de la RREQ au nœud en cours de traitement de la demande.
- \* #ID : Un numéro de séquence identifiant de manière unique une demande de route lorsqu'il est associé à l'adresse de la source (@Src).
- \* # @D : Adresse IP de la destination à laquelle une route est demandée.
- \* #SND : Le dernier numéro de séquence connu pour la destination.
- \* @Src : Adresse IP de la source (nœud qui a initialisé la demande de route).
- \* #SNS : Numéro de séquence actuel de la source qui sera associé à l'entrée de la table de routage dans les nœuds traitant le message RREQ.

### 3.2.5.2 Réponse de route RREP (Route REPLY)

Lorsqu'une demande de route atteint la destination ou un nœud ayant un chemin valide vers la destination, celui-ci génère une réponse de route qui sera envoyé en unicast d'un nœud à un autre jusqu'à atteindre la source. Le paquet de réponse de route est représenté par la figure 3.5 le format détaillé est présenté dans la figure 3.6[19].

@source	@Destination	Num,seq Destination	Nombre de saut	Life Time
---------	--------------	------------------------	----------------	-----------

Figure 3.5 : Format RREP simple.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Type = 2		R	A	Reserved								Prefix Sz				#HC															
@D - Destination IP Address																															
#SND - Destination Sequence Number																															
@Src - Originator IP Address																															
Lifetime																															

Figure 3.6.Format de la demande de route RREP détaillée.

### 3.2.5.3 HELLO

Les messages HELLO (voir la figure 3.7) offrent des informations sur la connectivité. Ils sont utilisés par seulement les nœuds faisant partie d'une route active pour valider les connexions avec les voisins. Ainsi, à chaque intervalle (Hello\_Interval), le nœud vérifie qu'il a diffusé au moins un message et s'il ne l'a pas fait, il envoie une réponse de route avec un TTL (Time To Live) égal à 1 : Il s'agit du message HELLO [19].

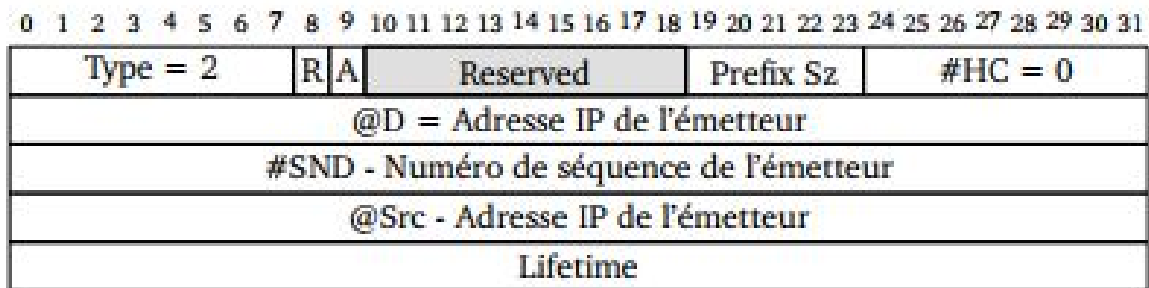


FIGURE 3.7 : Format du message HELLO.

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

### 3.2.5.4 Erreur de route RERR (Route ERRor)

Une erreur de route est envoyée à chaque fois que la rupture d'un lien rend inaccessible l'accès à une ou plusieurs destinations [19].

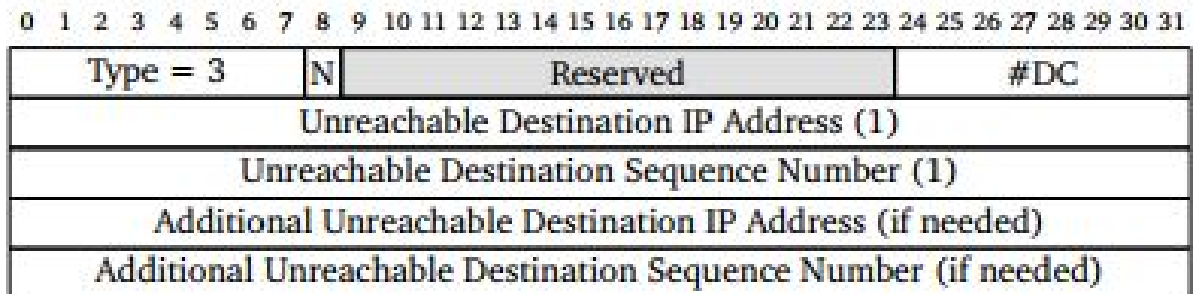


FIGURE 3.8 : Format de l'erreur de route RERR

\* Type : 3.

\* N : No delete flag : mis à un lorsque le nœud effectue une réparation locale de la route et les nœuds en amont ne doivent pas effacer la route.

- \* Reserved : mis à zéro lors de l’envoi et ignorés à la réception.
- \* #DC : Destination Count : Le nombre des destinations non joignables incluses dans le message. Cette valeur doit être au minimum 1.
- \* Unreachable Destination IP Address : L’adresse IP de la destination qui n’est plus accessible.
- \* Unreachable Destination Sequence Number : Le numéro de séquence de la destination (pris de la table de routage) dont l’adresse IP est juste au dessus.

### 3.2.5.5 Accusé de réception de réponse de route RREP-ACK

L’accusé de réception (ACKnowledgment) (voir la figure 3.9 )doit être envoyé en réponse à une RREP dont le bit “A” est à 1. Ceci est utilisé lorsque le nœud craint l’existence d’un lien unidirectionnel empêchant l’achèvement du processus de découverte de route [19].



FIGURE 3.9 : Format de l’accusé de réponse de route RREP-ACK

- \* Type : 4.
- \* Reserved : mis à zéro lors de l’envoi et ignorés à la réception.

## 3.2.6 Principe de fonctionnement

AODV définit deux types de procédures : la découverte de route et la maintenance de route.

### 3.2.6.1 Découverte de Route

Dans cette procédure, Si un nœud cherche à émettre un paquet vers une destination pour laquelle il n’a pas de route valide, le nœud initie une découverte de route vers la destination à travers une requête de demande de route RREQ diffusé en broadcast dans le réseau, lorsque le destinataire reçoit cette dernière ; il renvoi un paquet RREP au nœud intermédiaire ayant effectué la transmission ; chacun des nœuds intermédiaires remonte le paquet RREP jusqu’à la source en transitant via le nœud qui leur avait annoncé la requête comme la montre la figure 3.10 Si l’émetteur ne reçoit pas un RREP pendant un quantum de temps (RREP-WaitTime) il rediffuse la requête RREQ encore une fois, s’il

atteint un certain nombre de diffusion de la requête sans avoir une réponse une erreur va être signalée [20].

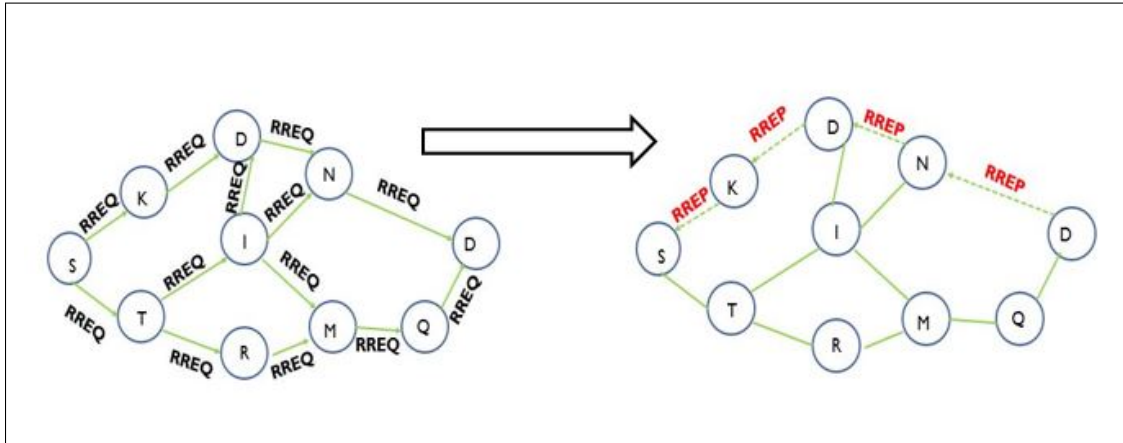


Figure 3.10 : Inondation de RREQ et le renvoi du RREP

### 3.2.6.2 Maintenance de route

Dès qu'un chemin est établi entre la source et la destination, le mécanisme de maintenance est déclenché automatiquement, ce mécanisme gère essentiellement les ruptures de liens entre les nœuds, il est basé sur la transmission périodique des messages HELLO, si trois messages Hello ne sont pas reçus consécutivement à partir d'un nœud voisin, le lien en question est considéré défaillant, lorsque un nœud détecte une rupture de lien dans chemin actif, ce dernier envoie un paquet d'erreur RERR au nœud qui le précède, quand un nœud reçoit ce type de message il cherche dans sa table de routage un chemin alternatif vers le nœud destination, sinon il consulte son prédécesseur, ce mécanisme est répété jusqu'au nœud source, dans le cas échéant il lance une nouvelle découverte (voir la figure 3.11) [20].

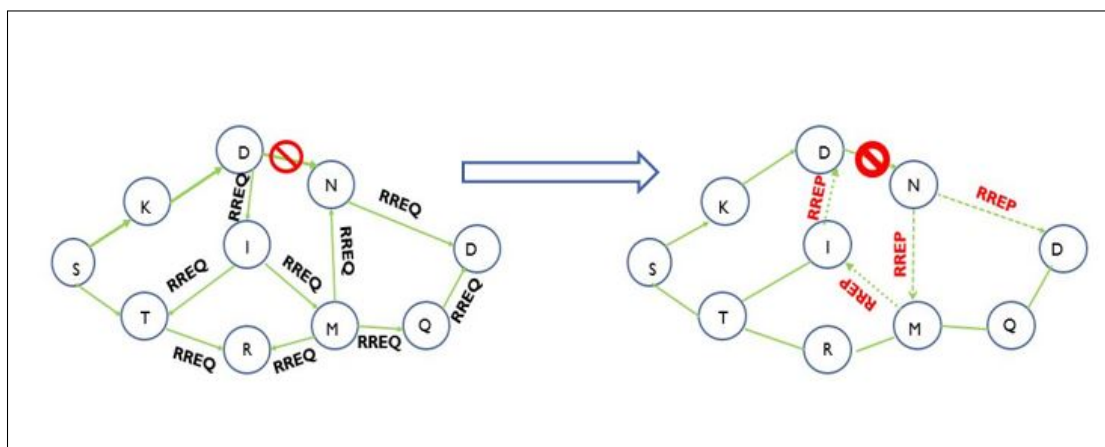


Figure 3.11 : Exemple de réparation locale d'une route perdu.

### 3.2.7 Discussion

L'utilisation de numéro de séquence dans les messages qui permet d'éviter les problèmes de boucles infinies qui est essentiels au processus de mise à jour de la table de routage et Rappel sur l'adresse IP du nœud origine dans chaque message qui permet de garder la trace du nœud d'origine de l'envoi du message. par contre Il n'existe pas de format générique des messages. Chaque message a son propre format : RREQ, RREP, RERR (surcharge de paquet de contrôle[4]. Et protocole de routage AODV est le fait qu'il n'assure pas l'utilisation du meilleur chemin existant entre la source et la destination [3].

## 3.3 Quelques protocoles basés sur AODV

Nous avons détaillé le protocole AODV précédemment, dans ce qui suit par la suite,nous allons présenter brièvement quelques variantes de ce dernier :

### 3.3.1 Protocole AOMDV

#### 3.3.1.1 Définition

AOMDV(Ad-hoc On-demand Multipath Distance Vector Routing protocol) qui veut dire protocole de routage vectoriel à distance multi-chemins à la demande dans les réseaux Ad Hoc. Le protocole AOMDV est donc une extension multi-chemins du protocole AODV. Dans AOMDV, plusieurs itinéraires sont établis entre la source et la destination. Il utilise des routes alternatives quand il y a échec de route. Donc dans le protocole AOMDV, une nouvelle découverte d'itinéraire est nécessaire seulement quand toutes les routes échouent. Dans le protocole AOMDV, le routage par trajets multiples est l'amélioration du routage mono-chemin dans lequel l'avantage est de gérer la charge dans le réseau et éviter la possibilité de congestion [21].

#### 3.3.1.2 Discussions

Si une rupture de lien arrive à la source, elle change de chemin sans avoir à déclencher une nouvelle phase de découverte. Aussi il établit une route sur demande. Il crée des nœuds libres de boucles et Il maintient la connectivité.

Par contre il occupe un espace plus important dans la table de routage ce qui implique la consommation de la mémoire de chaque nœud.[12]

### 3.3.2 Protocole MAODV

#### 3.3.2.1 Définition

MAODV (Multicast Ad hoc On-Demand Distance-Vector Routing Protocol) est basé sur AODV et fonctionne de manière réactive également, à la demande. Il utilise le même principe qu'AODV, et les mêmes formats de requêtes de recherche de routes.

Dans AODV, les tables de routage de chaque nœud sont mises à jour lorsque ceux-ci désirent connaître le chemin vers une destination non répertoriée (ou pour laquelle l'information correspondante est périmée) ou lorsqu'ils participent à une recherche de route lancée par un autre nœud. Le protocole MAODV construit un arbre partagé (voir la figure 3.12) centré sur un noyau (le leader du groupe) pour chaque groupe multicast du réseau. Le nœud leader est le premier participant au groupe, il est chargé de le gérer et de le maintenir en place. L'arbre peut contenir des nœuds qui ne font pas partie du groupe. Un numéro de séquence est associé à chaque groupe[22].

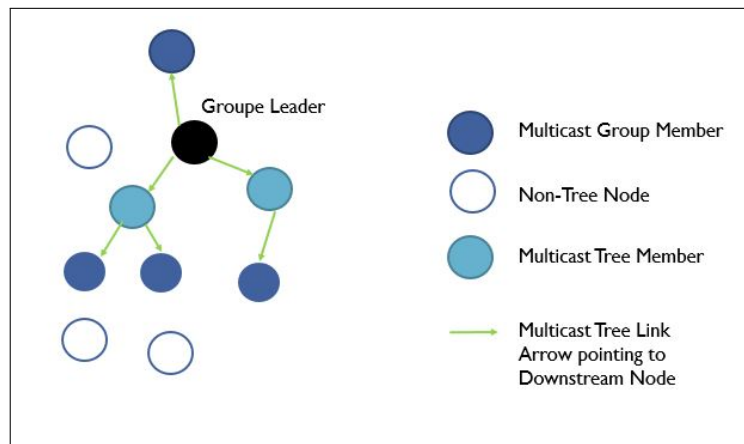


Figure 3.12 : Arbre de partage.

#### 3.3.2.2 Discussions

MAODV se révèle être le plus performant des protocoles multicast employant une structure d'arbre. Les routes sont construites à la demande en un temps restreint et les ruptures de liens sont réparées efficacement. De plus, il ne souffre pas de la création de boucles temporaires. Cependant, il reste sensible au déplacement des nœuds, caractéristique essentielle des réseaux ad hoc. En effet, ces protocoles, bien qu'étant économiques en terme de bande passante, ne sont pas robustes à la mobilité. Au contraire, la présence de chemins alternatifs dans les protocoles employant une structure de maillage leur assure de ne pas souffrir de la perte d'un lien ou de l'éloignement d'un nœud [23].

Le protocole MAODV permet de connaître le chemin du transfert de données. Mais le

simple MAODV a le problème de la consommation d'énergie. Cette technique consomme beaucoup de batterie et prend également beaucoup de temps. Plus aucun nœud n'est consommé dans ce processus.

### 3.3.3 Protocole QoS-MAODV

#### 3.3.3.1 Définition

QoS-MAODV est un protocole basé sur les arbres partagés (Source SharedTrees ), c'est-à-dire que pour chaque communication multicast est créé un arbre multicast composé uniquement des sources et destinations, ainsi que d'éventuels intermédiaires. Tous les nœuds d'un arbre multicast doivent être en mesure de prendre en charge les contraintes des QoS requises [16].

#### 3.3.3.2 Discussion

Lorsque les nœuds se déplacent, il se produit un changement fréquent de topologie et certaines routes se retrouvent indisponibles ; la procédure de découverte des routes doit donc être relancée à chaque fois .

Plusieurs simulations du protocole QoS-MAODV ont été effectuées dans différentes conditions (nombre de nœuds, mobilité, taille du réseau, etc..), et la grande majorité d'entre elles ont montré des problèmes récurrents de congestion au sein des arbres multicast [16].

### 3.3.4 Protocole ER-AODV

#### 3.3.4.1 Définition

Le protocole ER-AODV (Energy Reverse Ad-hoc On demand Distance vector) est un protocole de routage réactif qui vise à maximiser la durée de vie du réseau et d'améliorer les performances obtenues par le protocole de routage de base AODV. Ainsi, le but est de diminuer le coût des paquets de contrôle employés pour maintenir le réseau en intégrant le mécanisme nommé "Reverse AODV", et dérouter autour des nœuds possédant une plus grande énergie résiduelle en intégrant le mécanisme "Energy AODV" à le protocole[25].



### 3.3.4.2 Discussion

ER-AODV consomme moins d'énergie que AODV et il a un temps d'arrivé inférieur à celui de AODV.

### 3.3.5 Protocole QoS-AODV

#### 3.3.5.1 Définition

AODV se base sur un algorithme « à la demande » cela veut dire qu'il ne construit des routes entre nœuds que lorsqu'ils sont demandés par des nœuds sources. L'ajout dans les paquets de contrôle d'un champ 'route réponse' RREP associé au paramètre délai ou au paramètre bande passante, À la réception d'un message 'route requête' RREQ ajouté également. Du fait que les informations suivantes sont ajoutées dans la table de routage : bande passante minimale, délai maximum, et la liste des sources qui ont demandé des garanties de délai ou de bande passante. Chaque mobile vérifie s'il est en mesure d'honorer le service demandé, avant de retransmettre le message. Si un nœud détecte que la QoS demandée n'est pas satisfaite alors il envoie un message à la source ayant initiée cette demande de QoS, pour l'informer[26].

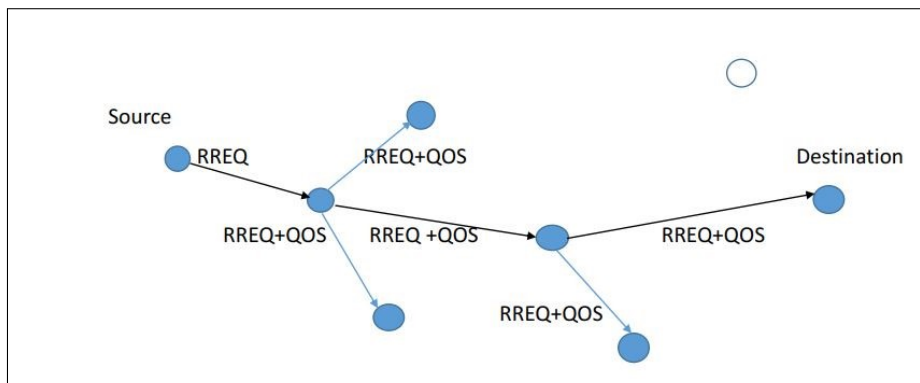


Figure 3.13 : Routage de QoS-AODV source-destination.

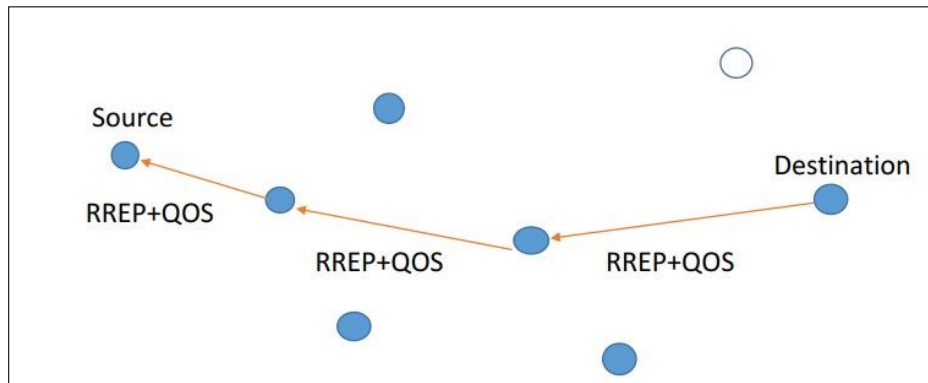


Figure 3.14 : Routage de QoS-AODV destination-source.

### 3.3.5.2 Discussion

Améliorer la QoS dans les réseaux ad hoc tel que introduire une métrique plus appropriée que la distance (nombre de sauts) et faire face aux changements fréquents de la topologie due à la mobilité des nœuds. [18]

## 3.3.6 Protocole AODV-BR

### 3.3.6.1 Définition

Le protocole AODV-BR (AODV with Backup Routes) utilise les avantages de la diffusion sans fil pour mettre en place des nœuds primaires et des nœuds de secours entre la source et la destination par découverte. Son processus de découverte de routes reste identique à celui proposé par le protocole AODV (cycle de requête de routes RREQ/ réponse de routes RREP, suppression des copies d'un RREQ déjà reçu par les nœuds intermédiaires, sauvegarde d'une seule route dans la table de routage par destination).

Cependant, contrairement au protocole AODV où les nœuds ne traitent que les paquets qui leur sont destinés (adresse de diffusion ou son adresse IP), un nœud dans le protocole AODV-BR traite tous les paquets de réponse de routes RREP reçus (même ceux qui ne lui pas sont destinés).

Les nœuds primaires reçoivent la réponse de route RREP après avoir diffusé la requête de route RREQ. Les nœuds de secours sont les voisins des nœuds primaires ; ils n'appartiennent pas à la route de retour empruntée par la réponse mais l'entendent à cause du caractère de diffusion des communications sans fil. Lorsqu'un nœud de secours entend une réponse de route destinée à un de ses voisins, il enregistre l'émetteur du paquet RREP comme le prochain nœud pour atteindre la destination dans sa table alternative.

Dans AODV-BR, une découverte de routes permet aux nœuds primaires de construire (ou de mettre à jour) leur table primaire et aux nœuds de secours de mettre en place leur table alternative.

Lorsqu'un nœud primaire détecte une rupture de communication avec un voisin dans sa table primaire, il diffuse sa donnée pour demander un routage de secours (indiqué dans l'entête du paquet de données). Cette donnée sera relayée en routage de secours lorsqu'elle est reçue par un nœud de secours possédant dans sa table alternative une route pour atteindre la destination. Dans le cas où la communication entre le nœud de secours et son prochain saut (qui est un nœud primaire) n'est pas rompue, la transmission de la donnée (ré)basculera sur la route primaire jusqu'à atteindre une autre défaillance de communication entre deux nœuds primaires adjacents. Après la détection de cette panne, le nœud primaire en amont de la panne procédera comme précédemment en demandant un routage de secours[27].

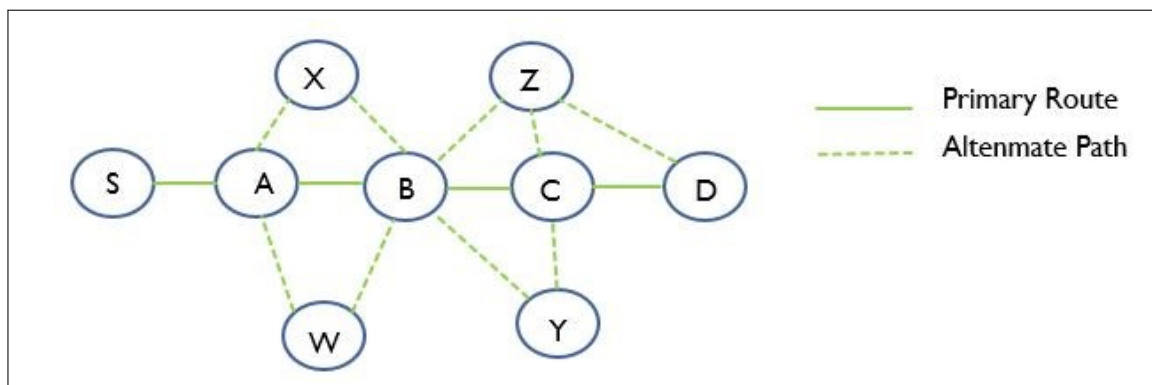


Figure 3.15 : Protocole AODV-BR.

### 3.3.6.2 Discussion

Cette approche ne considère que des nœuds de secours à un saut des nœuds primaires, ce qui augmente les probabilités de collisions lorsque les paquets circulent simultanément sur les routes primaires et secondaires. Un même paquet de données peut être relayé en routage de secours par plusieurs nœuds de secours (par exemple les nœuds X et W) se trouvant dans le voisinage du nœud primaire A ayant détecté une panne de communication avec le nœud B (figure 3.15). Ce qui entraîne une mauvaise utilisation des ressources et peut être facteur d'autres collisions. Par ailleurs, le protocole AODV-BR oblige la couche routage à traiter tous les paquets reçus au niveau MAC au lieu de permettre à celle-ci de supprimer immédiatement les paquets inutiles (ceux dont l'adresse MAC ne correspondent pas au sien). Ce processus entraîne une augmentation de la taille de files d'attente au niveau routage, une utilisation supplémentaire du temps CPU et une perte

de temps.[27]

### 3.3.7 Protocole AODV-UU

#### 3.3.7.1 Définition

Le protocole AODV-UU (AODV Upsala University) est une amélioration du protocole AODV, Nous présentons les diagrammes d'activités du processus de routage et le comportement de chaque nœud selon sa position dans le réseau : source, intermédiaire ou destination. Ces diagrammes mettent l'accent sur les activités des différents nœuds et leurs relations[28].

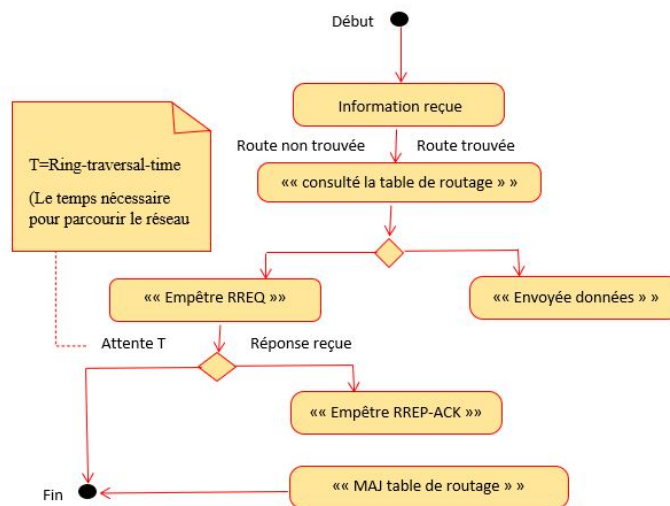


Figure 3.16 : Diagramme d'activité pour un nœud source AODV-UU.

Ce diagramme montre le rôle d'un nœud source dans la découverte de route vers une destination. L'émission d'une RREQ ne se fait que lorsque la route désirée pour atteindre la cible n'existe pas dans la table de routage de la source ou lorsque cette route n'est pas assez fraîche pour être utilisée lors de l'envoi des données. Dans le cas contraire, la communication entre les nœuds est considérée valide et l'appel du protocole de routage n'aura pas lieu[28].

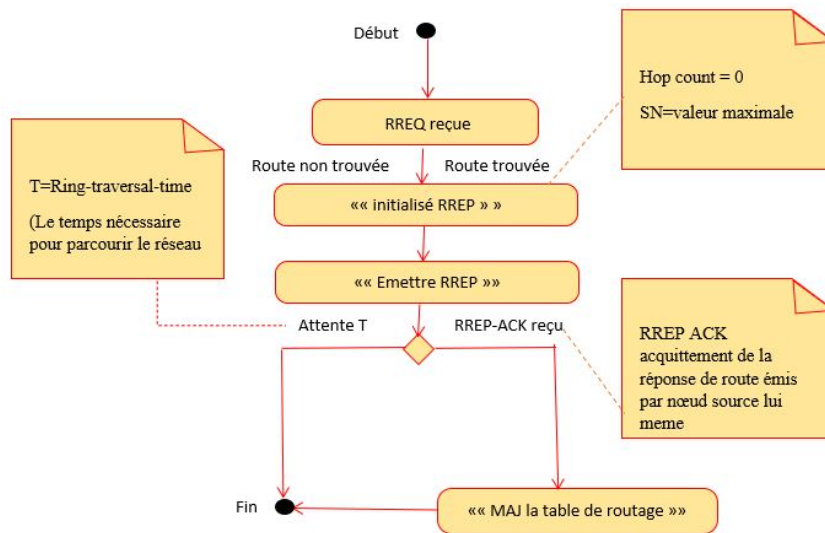


Figure 3.17 : Diagramme d'activités pour un nœud destination AODV-UU.

Le diagramme d'activités de la Figure 3.17 montre les étapes de réponse à la RREQ par un nœud destination. A la réception de la RREQ, celui-ci prépare une RREP en initialisant les champs « hop count » à zéro et «Destination Sequence Number» à sa nouvelle valeur maximale.

### 3.3.7.2 Discussion

Amélioration des opérations de mise à jour des tables de routage ; et génération de moins de trafic de contrôle, tout en gardant le même niveau de maintenance de route et minimise le délai de transfert des paquets.

## 3.3.8 Protocole MER-AODV

### 3.3.8.1 Définition

Le MER-AODV est un protocole de routage réactif permettant d'équilibrer la consommation d'énergie entre tous les nœuds du réseau. À la recherche d'une route, chaque nœud utilise des informations locales concernant le niveau de sa propre batterie pour décider de participer ou non au processus de sélection de rout, La prise de décision dans MER-AODV est distribuée sur tous les nœuds, et ne requiert pas des informations globales sur le réseau Le but est de choisir une route qui fait un équilibrage entre le niveau minimum d'énergie de chaque nœud dans la route et l'énergie consommée dans toute la route. [29]

### 3.3.8.2 Discussion

MER-AODV, équilibre la consommation de l'énergie dans un réseau en se basant seulement sur des informations locales. Effectivement, la prise de décision dans MER-AODV est distribuée sur tous les nœuds, et ne nécessite pas d'informations globales sur le réseau (elle n'a besoin que du niveau d'énergie du nœud). Un avantage de MER-AODV réside dans son interopérabilité avec AODV (un réseau peut contenir un ensemble de nœuds exécutant MER-AODV, et un autre ensemble de nœuds exécutant AODV). Un autre avantage réside dans sa simplicité et dans sa facilité à être intégré dans tous les algorithmes de routage ad hoc existants (réactifs ou proactifs). mais Le protocole MER-AODV enregistre un délai un peu élevé comparé à AODV. Le délai est augmenté dans les topologies denses à cause du mécanisme du rejet de message RREQ afin de préserver un niveau d'énergie acceptable dans les nœuds participant à la construction d'une route. même le débit de transfère est impacté par une légère diminution de ca valeur, cela est due aux changements des modes radio vers le mode veille et la façon de calculer la période dans laquelle le nœud doit changer son mode.

### 3.3.9 Protocole AODV-UI

#### 3.3.9.1 Définition

AODV-UI une nouvelle variante du protocole de routage AODV avec combinaison de AODV + et RAODV. le principale caractéristique d'AODV-UI est qu'il peut être utilisé en hybride réseaux ad hoc et il a quelques suggestions d'amélioration dans les frais généraux de routage et la consommation d'énergie AODV-UI une nouvelle variante du protocole de routage AODV avec combinaison cle mode passerelle, adopté à partir d'AODV et la route inverse, adoptée à partir de R-AODV ,objectif est de concevoir un algorithme capable de déterminer quels nœuds en tant que nœud intermédiaire., AODV-UI, a des objectifs principaux pour sélectionner un nœud avec l'énergie comme paramètre. Chaque nœud mobile a une quantité d'énergie initiée. Afin d'augmenter la durée de vie du nœud, il est souhaitable de prendre en compte l'énergie restante. Par conséquent, il est important de sélectionner un nœud avec une énergie résiduelle élevée [30].

#### 3.3.9.2 Discussion

Amélioration dans les frais généraux de routage et la consommation d'énergie et plus stable en point de cheminement aléatoire avec un nombre différent de sources et de vitesse. En terme de routage et AODV-UI donne le résultat le plus bas de 53468 octets

lorsqu'il est utilisé dans un point de cheminement aléatoire avec 2 sources de nœuds avec une vitesse maximale de 10 m / s. La surcharge de routage la plus élevée est de 1165 072 octets lorsqu'il est sous RPGM modèle de mobilité avec 6 sources et 40 m / s de vitesse.

### 3.3.10 Protocole Bypass-AODV

#### 3.3.10.1 Définition

Le protocole de routage Bypass-AODV réduit la consommation de bande passante et augmente le débit du réseau en augmentant la fiabilité de l'itinéraire pour les réseaux sans fil ad hoc hautement mobiles. Le Bypass-AODV suit initialement le mécanisme de découverte d'itinéraire de l'AODV. Ensuite, en cas de défaillance de la route principale, le protocole proposé utilise une notification MAC inter-couche pour identifier la perte de paquets liée à la mobilité, puis il installe un contournement entre le nœud sur lequel la défaillance de la route s'est produite et son successeur précédent via une alternative nœud tandis que continue sur le reste de l'itinéraire. Le mécanisme proposé peut réduire considérablement la surcharge de routage et conduire à une augmentation correspondante du débit en évitant l'invocation inutile du mécanisme de récupération d'erreur. La construction du contournement est indépendante de l'emplacement de l'échec de la route et augmente la fiabilité de la route en diminuant le nombre de largages de paquets, les paquets peuvent être récupérés en les redirigeant sur le contournement[31].

#### 3.3.10.2 Discussion

amélioration de la fiabilité des routes en réduisant la fréquence de maintenance des routes et la quantité de perte de paquets. En comparant les performances de Bypass-AODV avec AODV, les résultats montrent que pour une connexion TCP longue (en termes de nombre de sauts), Bypass-AODV améliore le débit TCP de plus de 100 % pour une connexion TCP unique et de plus de 24 % pour plusieurs connexions TCP. En outre, le pourcentage de perte de paquets est réduit considérablement. En outre, Contournement-AODV les performances surpassent l'AODV pour différentes densités de nœuds. De plus, le good put Bypass-AODV est insensible à l'évolution des vitesses mobiles. Cette caractéristique rend le protocole de routage proposé très attractif pour les applications VANET.

### 3.4 Comparaison du AODV et ses variantes

Protocole	Approche de routage	Architecture du réseau	Mode de communication	Paramètres de Qos	Simulateur
AODV	Réactif	Uniforme	Unicast Multicast	/	NS2
MAODV	Réactif	Uniforme	Multicast	Délai	NS2
AOMDV	Réactif	Uniforme	Unicast	Délai	NS2
QoS-MAODV	Réactif	Non uniforme	Multicast	Bande passante	Qualnet
ER-AODV	Réactif	uniforme	Unicast	Délai	NS2
QoS AODV	Réactif	uniforme	Unicast	Délai	
AODV-UU	Réactif	Uniforme	Unicast	délai	NS2
Mer-AODV	Réactif	Non uniforme	Unicast	Délai Débit	GloMoSim
AODV-UI	hybride	Uniforme	Unicast	Délai Perte de paquets	NS-2.34
Bypass -AODV	Réactif	Uniforme	Unicast	Délai Bande passante	NS-2
AODV-BR	Réactif	Uniforme	Multicast	Débit Perte de paquets	GloMoSim

Table 3.1 : Comparaison du AODV et ses variantes.



Afin de résumer les différentes spécificités des protocoles que nous avons étudiés, nous avons jugé utile d'établir un tableau comparatif de ces derniers en citant leurs spécificités. En ce qui concerne notre classification selon l'Architecture du réseau nous avons remarqué que la plupart des protocoles sont uniforme puisque la décision d'un nœud de router des paquets vers un autre dépendra de sa position. La quasi-totalité des protocoles étudiés et exposés dans ce tableau sont de nature réactive. Cela s'explique par la nature du réseau ad hoc ; étant donné la mobilité permanente des nœuds, il n'est pas intéressant d'établir préalablement les routes, puisque la plupart de celles-ci ont de grandes chances de devenir indisponibles. Les protocoles proactifs ne sont donc généralement pas efficaces dans les réseaux mobiles. On remarque également que la métrique de QoS commune à tous les protocoles est la quantité minimale de bande passante. La disponibilité d'un large débit de transmission est indispensable à toute communication, l'objectif est donc de faire transmettre les données le plus rapidement possible.

### **3.5 Conclusion**

Dans ce chapitre, nous avons étudié en détail le fonctionnement et le comportement du protocole de routage réactif AODV et ses variantes dans les réseaux ad hoc, et nous avons comparé ses protocoles avec quelques paramètres de comparaison. Dans le chapitre qui suit, nous allons présenter une amélioration du protocole AODV en ajoutant quelques solutions.

## Chapitre 4

### Amélioration du protocole MAODV

# Chapitre 4

## Amélioration du protocole MAODV

### 4.1 Introduction

Ce chapitre concerne la majeure partie de notre travail. Nous allons particulièrement nous intéresser à une variante de protocole AODV que nous avons expliqué brièvement dans le chapitre précédent MAODV, nous allons l'analyser un peu plus en profondeur afin de mettre en lumière ses défauts, les discuter et proposer une solution qui corrige au mieux.

### 4.2 Protocole MAODV

Lors du chapitre précédent, nous avons présenté une brève définition du protocole MOADV. Ici nous présenterons plus en détails afin de comprendre précisément les mécanismes qui composent ce protocole.

#### 4.2.1 Présentation de protocole MAODV

L'algorithme de routage "MAODV" (Multicast Ad hoc On Demand Vector) est un protocole de routage destiné aux réseaux mobiles. MAODV est un algorithme "On Demand" c'est-à-dire qu'il ne construit des routes entre nœuds que lorsqu'elles sont demandées par des nœuds sources. Il maintient ces routes aussi longtemps que le nœud source en a besoin. De plus, MAODV constitue des arborescences connectant les membres des groupes Multicast. Les arbres sont composés des membres des groupes et des nœuds nécessaires pour connecter les membres. MAODV utilise un numéro de séquence pour assurer la "fraîcheur" des routes (voir Figure 3.12)[32].

### 4.2.2 Format de message de GRouPe Hello (GRPH)

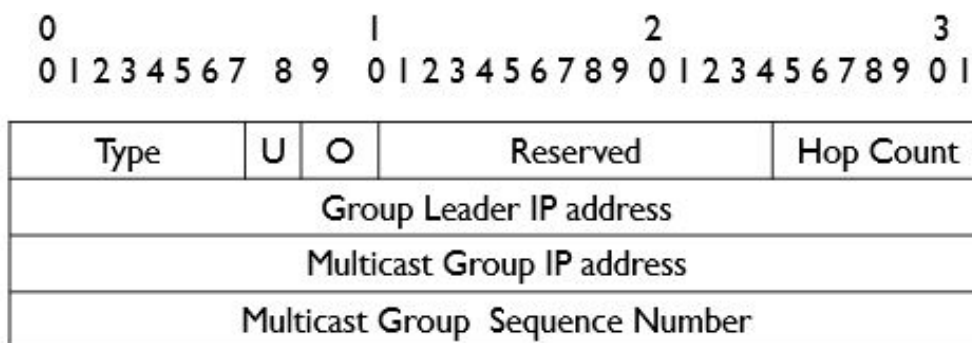


Figure 4.1 : Format du message Group Hello .

Le format du message Group Hello est illustré ci-dessus, et contient les champs suivants[35] :

- \* *Type* : 5
- \* *U* : Mettre à jour le drapeau ; réglé lorsqu'il y a eu un changement de groupe informations sur le leader.
- \* *O* : Off\_Mtree flag ; fixé par un nœud recevant le groupe hello ce n'est pas sur l'arborescence de multidiffusion.
- \* *Reserved* : Sent as 0 ; ignoré à la réception..
- \* *Hop Count* : Le nombre de sauts parcourus par le paquet. Utilisé par nœuds d'arborescence de multidiffusion pour mettre à jour leur distance par rapport au chef de groupe lorsque l'indicateur M n'est pas défini.
- \* *Group Leader IP Address* : L'adresse IP du chef de groupe.
- \* *Multicast Group IP Address* : L'adresse IP du groupe de multidiffusion pour lequel le numéro de séquence est fourni.
- \* *Multicast Group Sequence Number* : Numéro de séquence actuel du groupe de multidiffusion.

### 4.2.3 Chef de groupe

C'est le membre de groupe premier qui construit l'arbre ,il est responsable de la maintenance du groupe de l'arbre par une diffusion périodique de messages "Group-Hello" dans tout le réseau. Le chef de groupe maintient également le numéro de séquence du groupe, qui est propagé dans le réseau à travers le message [34].

#### 4.2.4 Table de routage

Un nœud MAODV maintient une table de routage comme dans AODV pour le routage unicast (l'algorithme AODV maintient une table sur chaque nœud, indexée par destination et notamment le voisin auquel envoyer le paquet pour atteindre cette destination. Si la destination recherchée n'est pas dans la table, on doit donc découvrir une route jusqu'au destinataire. L'algorithme agit à la demande : recherche d'une route uniquement lorsque c'est nécessaire), mais aussi une table de routage pour la structure en arbre du groupe. Cette table contient l'adresse du groupe multicast (identifiant du groupe), le numéro de séquence, l'adresse du leader du groupe, le nombre de sauts jusqu'au leader, et les informations sur le saut suivant, qui correspondent aux voisins qui sont dans l'arbre. Les voisins peuvent être fils ou père, chaque nœud possède au plus un père, et le leader ne peut posséder des fils que s'il y a d'autres membres dans le groupe [17].

#### 4.2.5 Message de requête et message de réponse

Les messages de demande de routes et de réponse sont ceux de AODV, adaptés pour le multicast. Une requête est envoyée lorsqu'un nœud source désire envoyer un message multicast. Le même type de message de requête REQ (voir la Figure 3.3) est utilisé lorsqu'un nœud désire rejoindre un groupe multicast. Dans les deux cas, il s'agit donc de trouver une route vers l'arbre multicast. Si le nœud source connaît le leader du groupe, il peut envoyer son message directement au leader en mode unicast. Sinon, le message REQ est relayé saut par saut jusqu'à trouver un nœud qui appartient déjà à l'arbre multicast. Le nœud récepteur de la requête répond alors en mode unicast au nœud demandeur, par un message de réponse REP (voir la Figure 3.5). Les requêtes sont envoyées avec des TTLs de plus en plus grands, et si le nœud n'obtient pas de réponse après plusieurs tentatives de connexion à un arbre multicast, il se considère comme étant le premier membre de ce groupe, et il initialise le numéro de séquence du groupe [17].

#### 4.2.6 Réponse et activation de branches

Dans AODV, le message de réponse à une demande de route active directement la route, alors que dans MAODV, la réponse indique seulement une route possible jusqu'à l'arbre, sans l'activer. Le nœud qui a émis la requête attend une certaine période, puis choisit la meilleure route à utiliser pour atteindre l'arbre parmi les réponses qu'il a reçues. Il envoie alors un message MACT (Multicast Activation) pour activer la route jusqu'à l'arbre, ou activer une nouvelle branche de l'arbre multicast. La meilleure route est la plus récente

(en regardant le numéro de séquence), et la plus courte parmi ces dernières (en termes de nombre de sauts jusqu'à l'arbre) [17].

### 4.2.7 Opérations de maintenance

Les opérations de maintenance lors de départ de nœuds sont plus complexes en multicast que pour le protocole AODV unicast.

Le leader du groupe envoie périodiquement un message Hello de groupe. Ce message est broadcasté dans tout le réseau, pour indiquer l'adresse du leader du groupe et le numéro de séquence courant du groupe. Le numéro de séquence de groupe est incrémenté avant chaque envoi de ce message Hello.

Pour un départ d'un membre du groupe, si le nœud n'est pas une feuille de l'arbre, il doit rester dans l'arbre et faire office de routeur pour le groupe multicast. Sinon, il faut enlever la branche de l'arbre désormais inutilisée, cela se fait par l'envoi d'un message MACT avec un flag spécial.

Les nœuds servant de routeur pour le nœud qui quitte le groupe sont également supprimés de l'arbre, et ce jusqu'à ce qu'un membre du groupe soit rencontré.

Les problèmes propres à l'ad hoc sont bien sur les ruptures de lien dues à la mobilité, et cela peut entraîner des envois à une partie seulement du groupe multicast. Les ruptures de lien peuvent être détectées de la même façon que dans AODV, mais AODV se contente d'effacer la route des tables de routage et de rechercher une nouvelle route, alors que dans MAODV la procédure a lieu localement, seul le nœud fils du lien cassé peut initier la procédure de réparation. Le nœud fils envoie en mode broadcast un message de requête REQ en demandant à rejoindre l'arbre, indiquant également son nombre de sauts jusqu'au leader (pour éviter qu'un de ses descendants renvoie une réponse).

Lorsqu'une réponse est obtenue, le nœud envoie un MACT pour raccorder sa branche à l'arbre, et il envoie également un MACT avec un flag de mise à jour à ses descendants pour qu'ils puissent changer leur compteur de sauts jusqu'au leader du groupe[17].

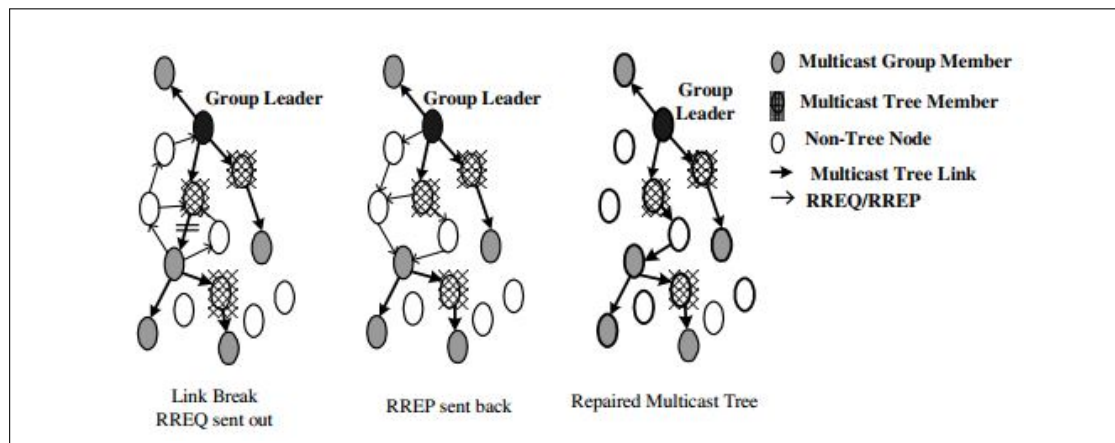


Figure 4.2 : Ruptures de lien.

Si aucune réponse n'est reçue après une tentative de re-connexion de la branche (après plusieurs essais), la source suppose alors que l'arbre est partitionné, et il faut sélectionner un nouveau leader pour l'arbre partitionné. Si le nœud source est un membre du groupe, il devient le leader. Sinon, il oblige un de ses descendants à devenir le leader.

### 4.3 Discussion des failles de MAODV

Maintenant que nous avons minutieusement étudié les détails du mécanisme MAODV, nous allons discuter certains points qui, à notre sens, entravent le bon déroulement des communications dans le réseau. Notre critique repose essentiellement sur deux points ; le délai de bout en bout lors de transmission des paquets, ainsi que le taux élevé de congestion lors de l'utilisation de MAODV.

#### 4.3.1 Opérations de maintenance

les problèmes récurrents de la congestion au sein des arbres multicast sont dus à deux raisons principales.

- **L'appartenance des nœuds à plusieurs arbres**

Au fur et à mesure que le réseau grandit (en termes de nombre de nœuds souhaitant communiquer), le nombre d'arbres multicast augmente lui aussi et plusieurs nœuds se retrouvent à faire partie de plusieurs arbres à la fois, et sont de plus en plus sollicités. La fonction normale d'un nœud intermédiaire est de recevoir et retransmettre les paquets qu'il reçoit.

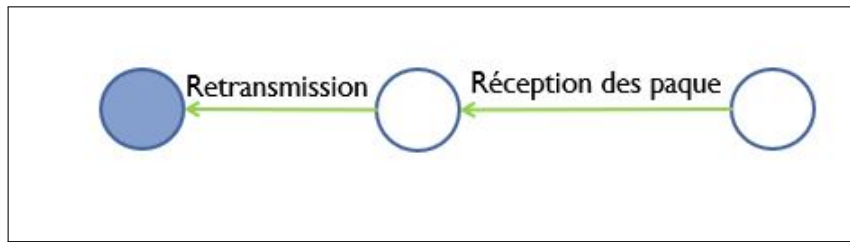


Figure 4.3 : Trafic normal de paquets.

Lorsqu'un nœud appartient à divers arbres, il peut être sollicité par plusieurs nœuds à la fois, et si le nombre de paquets devient trop grand, la mémoire du nœud (appelée buffer) sature et il se produit un retard dans la retransmission, voire une perte totale de certains paquets.

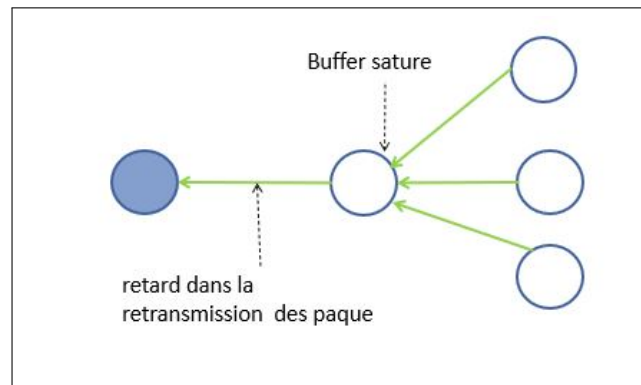


Figure 4.4 : Cas de congestion.

### 4.3.2 Maintenance du groupe de l'arbre

Il est important de rappeler que le protocole MAODV entretient une maintenance du groupe de l'arbre par une diffusion périodique de messages "Group-Hello" (GRPH) dans tout le réseau. Le chef de groupe maintient également le numéro de séquence du groupe, qui est propagé dans le réseau à travers le message GRPH, ce qui augmente le trafic de manière significative, surtout lorsqu'un nœud appartient à plusieurs arbres et doit émettre et recevoir un paquet pour chaque arbre.

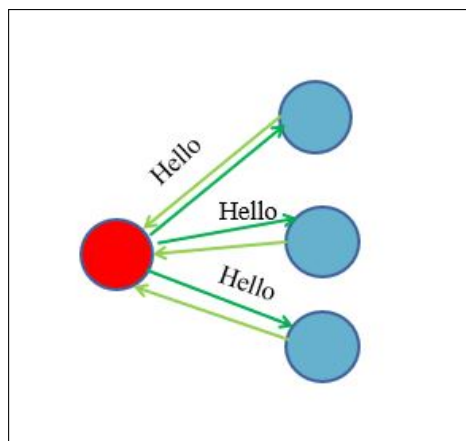




Figure 4.5 : Echange de paquets de maintenance "HELLO".

Cette étude a donc mis en lumière le second grand défaut de MAODV qu'est la congestion réseau, notamment lorsque le nombre de nœuds est relativement élevé.

## 4.4 Amélioration apportée à MAODV

Dans le but de régler le problème de congestion qu'on a cité précédemment, nous avons pensé à une solution qui sera utilisé durant la découverte des routes. Cette solution se résume en deux idées qui consistent à l'ajout de champ « Mem » et le champ « compteur » au paquet RREQ voici sa structure :

@source	Num,seq source	Broadcast id	@Destination	Num,seq Destination	Nombre de saut	Mem	Compteur
---------	----------------	--------------	--------------	---------------------	----------------	-----	----------

Figure 4.6 : champ « Mem » et le champ « compteur » au paquet RREQ.

- Le champ mem évitera le choix d'une route saturée grâce au calcul des moyennes de saturation des routes. cette moyenne DS sera calculé pour chaque noeud Ni et on l'ajoute au Mem comme le montre la formule suivante :

$$\text{Mem} = \text{Mem} + \text{DS}(\text{Ni})$$

Les paquets RREP que recevra la source contiendra la moyenne de saturation de mémoires tampons des nœuds du chemin traversé par le paquet entre la source et la destination ce qui offre à la source le choix d'une rote adéquate à savoir celle qui comporte une moyenne de saturation moins importante pour emmètre ses données comme le montre la figure suivante :

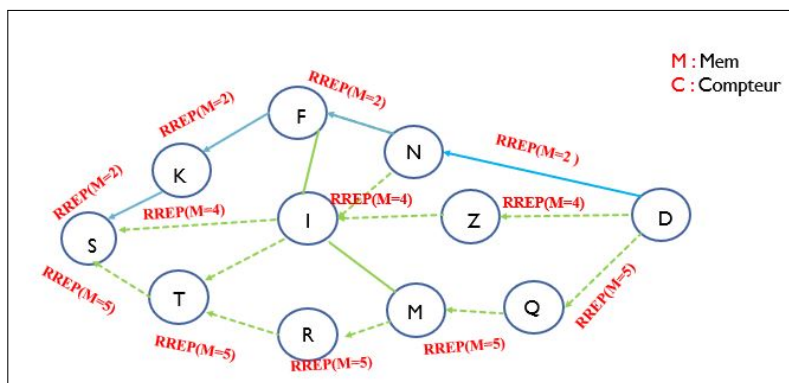


Figure 4.7 : Route choisie contient la petite moyenne de saturation.

- Mais dans le cas où les moyennes de saturations sont égales ou bien convergentes alors nous avons pensé à ajouter un autre champ que nous appellerons « compteur » dans le paquet RREQ. Chaque nœud qui recevra le paquet RREQ mémorisera et additionnera grâce au champ compteur intégré le délai de transmission entre lui (TNi) et le nœud précédant (TNi-1) afin d'aboutir le délai bout en bout grâce à la formule suivante :

$$\text{Compteur} = \text{Compteur} + (\text{TNi} - \text{TNi-1})$$

Les paquets RREP que recevra la source contiendra la moyenne de saturation de mémoires tampons des nœuds du chemin traversé et le délai de bout en bout. Dans ce cas elle va prendre le critère de délai bout en bout pour choisir la route dont elle va emmener ses données comme la montre la figure(4.8) suivante :

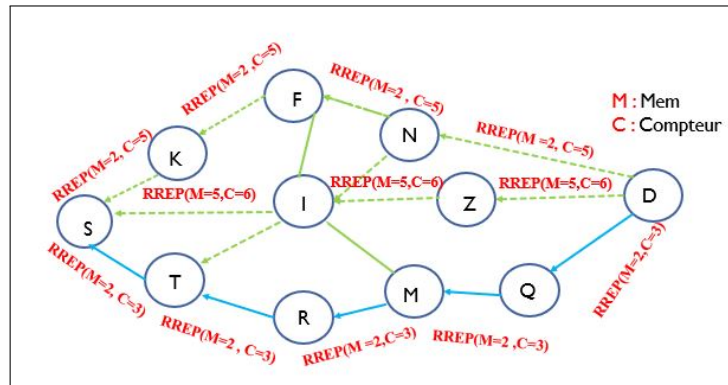


Figure 4.8 : Prendre en charge le critère du délai bout en bout.

Cependant ce critère ne sera pris en considération seulement si les moyenne de saturation sont égaux ou bien convergentes.

- Mais si le nœud est saturé le paquet sera rejeté sans aucun traitement comme l'illustre le schéma suivant :

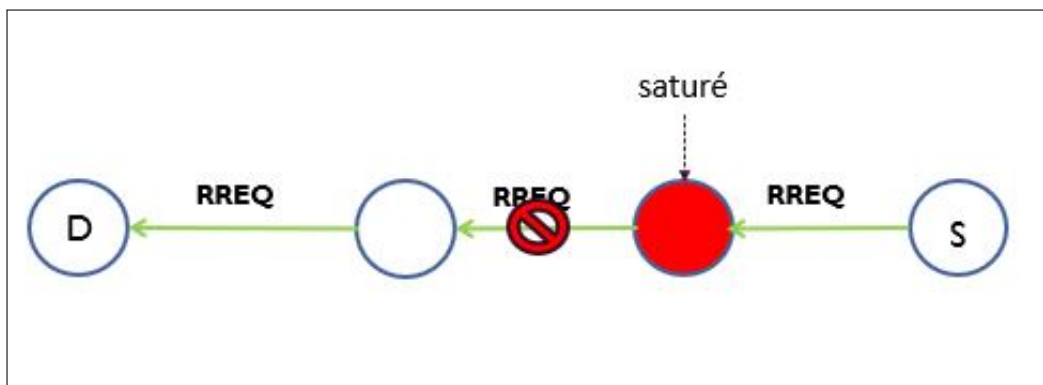


Figure 4.9 : Paquet Rejeté.

L'algorithme suivant montre la solution proposée pour l'amélioration du MAODV :

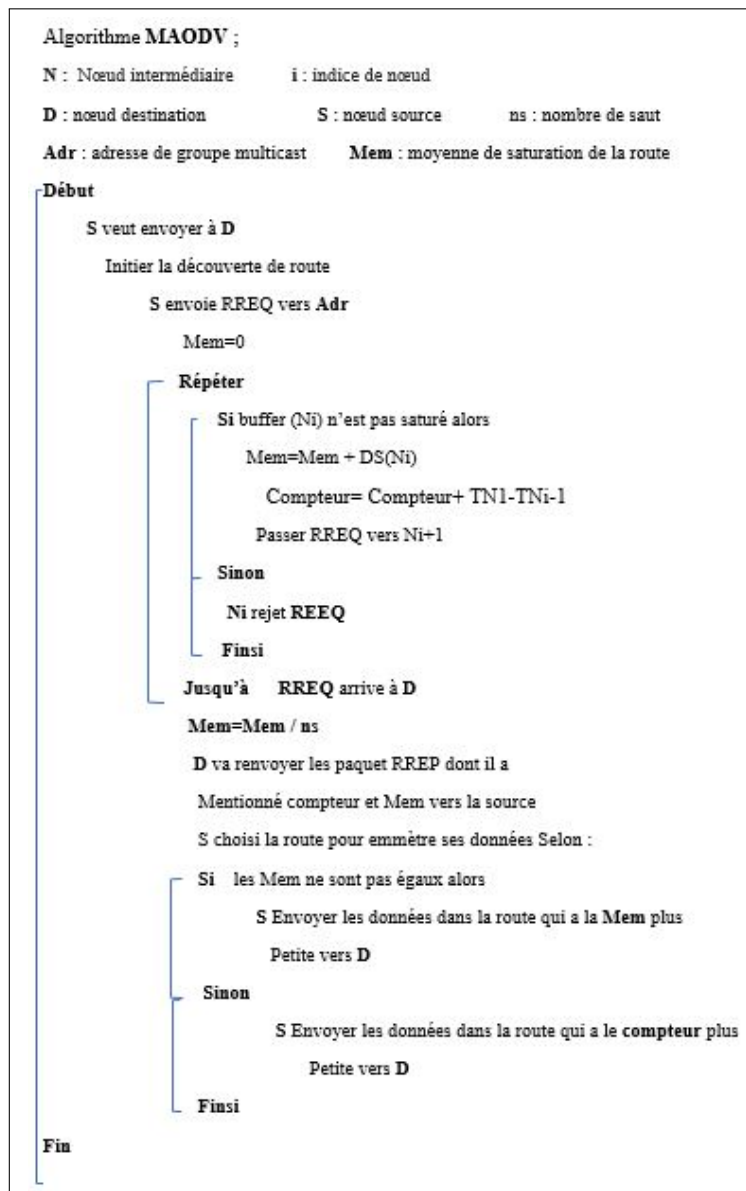


Figure 4.10 : Algorithme d'amélioration.

## 4.5 Exemple démonstratif de la solution proposée

- Notre solution repose essentiellement dans la phase de découvertes des routes, voici un schéma qui illustre comment se déroulera la phase de découverte des routes

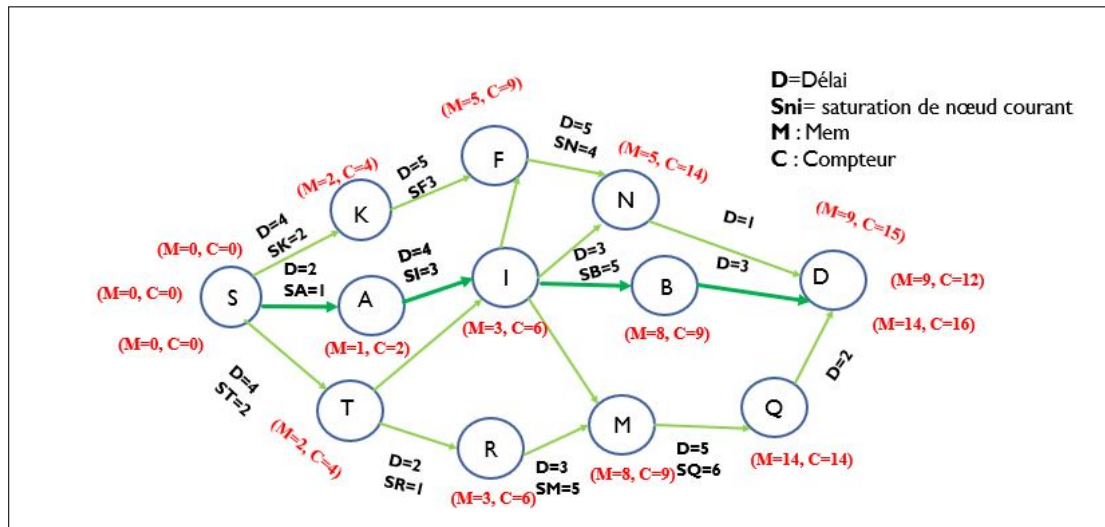


Figure 4.11 : Exemple de découverte des routes.

le nœud source (S) diffuse le paquet RREQ, au début le champ compteur =0 et mem =0 en suite à chaque fois il transit un nœud les valeurs de ces deniers vont changer comme le montre le tableau ci dessous (Table 4.1). Après y avoir la destination recevra tous les paquet RREQ va générer les paquet RREP dont elle va mentionnera les valeurs des champs compteur et Mem Et enfin la source choisi la route qui a la valeur moyenne minimale de Mem dans notre exemple c'est le chemin 3

- La tableau suivant montre comment chaque nœud calcule le compteur et le Mem :

	Noeud	Délai	Saturation	Compteur	Mem
Chemin 1	SK	4	2	0+4=4	2+0=2
	KF	5	3	4+5=9	2+3=5
	FN	5	4	9+5=14	5+4=9
	ND	1	/	14+1=15	9/3=3
Chemin 2	ST	4	2	4+0=4	0+2=2
	TR	2	1	4+2=6	2+1=3
	RM	3	5	6+3=9	3+5=8
	MQ	5	6	9+5=14	8+6=14
	QD	2	/	9+2=16	14/4=3.5
Chemin 3	SA	2	1	2+0=2	0+1=1
	AI	4	3	2+4=6	1+3=4
	IB	3	5	6+3=9	4+5=9
	BD	3	/	9+3=12	9/3=3

Table 4.1 : Calcul du compteur et du Mem.

## 4.6 Conclusion

Au cours de ce chapitre nous avons étudié en détail le mécanisme de MAODV, nous avons discuté certaines fonctionnalités qui nous semblaient défailantes, en l'occurrence le taux élevé de congestion réseau et le délai lors de transmission des paquets. Nous avons par la suite proposé quelques idées permettant de limiter ces failles, en ajoutant quelques fonctionnalités au protocole.

# Conclusion générale et perspectives

La recherche dans le domaine des réseaux mobiles Ad Hoc est en plein essor. En effet, plusieurs protocoles de routage ont été développés ces dernières années. Dans ce mémoire nous avons passé en revue le protocole de routage AODV et ses quelques variantes, nous avons fait une comparaison entre ces protocoles, nous avons également choisi le protocole MAODV dans le but d'étudier en détail afin d'extraire ses défauts et proposer une amélioration.

D'abord nous avons commencé par la présentation des réseaux ad hoc et nous avons donné une classification selon l'architecture (uniforme et non uniforme), selon le Routage (proactif, réactif, hybride et géographique) et selon le mode de communication (unicast, multicast et broadcast) en suite nous sommes passé à la définition et aux paramètres de qualité de service de ses réseaux (QoS) puis nous sommes passés à ses modèles d'implémentation ainsi qu'à son mécanisme, pour enfin entamer le routage avec QoS dans les réseaux ad hoc.

Ensuite, nous nous sommes concentrés sur le protocole AODV, pour cela nous avons décrit en détail les mécanismes et le principe de fonctionnement pour qu'ils assurent l'acheminement des données entre un nœud source et un nœud destination. Puis, nous sommes passés à la présentation de dix protocoles basés sur le mécanisme d'AODV et les discuter dans le but d'aboutir à une table comparative entre ces protocoles selon les critères suivants ; approche de routage, architecteur de réseaux, mode de communication et paramètre de QoS.

En dernier lieu, et d'après ce que nous avons étudié précédemment nous avons remarqué que la plupart des protocoles que nous avons cité ne répondent pas aux paramètres de QoS. C'est pour cela que nous avons pris le protocole

MAODV a fin de l'étudier en profondeur dans le but d'émettre quelques critiques à son égard, notamment en soulignant ses lacunes en termes de congestion, ainsi nous sommes arrivés à proposer quelques améliorations permettant de combler ses failles, parmi ces améliorations l'ajout de deux paramètres de QoS : la perte de paquet et délai bout en

bout.

En perspective, nous souhaitons mettre en place une implémentation de notre amélioration dans un simulateur réseau, afin de comparer ses performances par rapport à MAODV dans le but de vérifier si les failles de ce dernier sont effectivement soignées par les améliorations que nous avons proposées.

# Bibliographie

- [1] KHEBBACHE MOHIBEDDINE,"PROTOCOLE DE TRANSPORT MULTICAST FIABLE POUR LES RÉSEAUX SANS FIL",MÉMOIRE DE FIN D'ÉTUDES ,UNIVERSITÉ HADJ LA-KHDAR –BATNA- ,2014.
- [2] SEBAHI YAZID, YESSAD NAWEL," ROUTAGE AVEC QUALITÉ DE SERVICE DANS LES RÉSEAUX MOBILES AD HOC",MÉMOIRE DE FIN D'ÉTUDES ,UNIVERSITÉ ABDERRAHMANE MIRA DE BÉJAIA,2013.
- [3] A. BENSKY R.OLEXA D.A. LIDE F. DOWLA P. CHANDRA, D.M. DOBKIN. "WIRELESS NETWORKING". ELSEVIER INC, UK, 2008.
- [4] BERRABAH ABDELKRIM SAIDI HASSIBA , "BALANCEMENT DE CHARGES DANS LES RÉSEAUX AD HOC", MÉMOIRE DE FIN D'ÉTUDES,UNIVERSITÉ ABOU BAKR BELKAID–TLEMCEM, 2012-2013.
- [5] ALLALI MAHAMED ABDELMADJID," INGÉNIEURIE ET CONTRÔLE DU TRAFIC DANS LES RÉSEAUX SANS FIL",THÈSE DE DOCTORAT, UNIVERSITÉ DES SCIENCES ET DE LA TECHNOLOGIE D'ORAN MOHAMED-BOUDIAF USTOMB,2017 – 2018.
- [6] B. TAVLI AND W.HEINZELMAN. "MOBILE AD HOC NETWORKS". SPRINGER, NETHERLANDS, 2006.
- [7] AISSAOUI BOUTHAINA, HEMAIZIA ZINEB," UN PROTOCOLE DE ROUTAGE OPTIMISÉ DANS LES RÉSEAUX AD HOC" ,MÉMOIRE DE FIN D'ÉTUDES,UNIVERSITÉ DE TÉBESSA, 2015 – 2016.
- [8] SABRINE NAIMI,"GESTION DE LA MOBILITÉ DANS LES RÉSEAUX AD HOC PAR ANTICIPATION DES MÉTRIQUES DE ROUTAGE",THÈSE DE DOCTORAT, UNIVERSITÉ PARIS SUD - PARIS , 2015.
- [9] AIJAZ AHMAD ANCHARI , ASIFA AMIN, SUHAIL ASHRAF,"ROUTING PROBLEMS IN MOBILE AD HOC NETWORKS (MANET)",INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND MOBILE COMPUTING, VOL.6 ISSUE.7, JULY- 2017, PG. 9-15
- [10] BESSAIH ALDJA BOUCHAKEL SIHAM , "ROUTAGE ET SIMULATION DANS LES RÉSEAUX MOBILES AD HOC" ,MÉMOIRE DE FIN D'ÉTUDES,UNIVERSITE ABDERRAHMANE MIRA BÉJAIA,2016-2017
- [11] [HTTPS ://WWW.IRISA.FR/PRIVE/BERNARD.COUSIN/JOURNEE %20A.NET-9FEV2007/PRESENTATION\\_IRISA\\_09\\_02.PDF](https://www.irisa.fr/PRIVE/BERNARD.COUSIN/JOURNEE%20A.NET-9FEV2007/PRESENTATION_IRISA_09_02.PDF)



## BIBLIOGRAPHIE

---

- [12] ALLOUACHE SOUAD ,TAYEB CHERIF RAHMA, "ETUDE COMPARATIVE ENTRE AODV ET AOMDV DANS LE CADRE DES RÉSEAUX AD HOC " ,MÉMOIRE DE FIN D'ÉTUDES, UNIVERSITE ABDERRAHMANE MIRA BÉJAIA, 2016-2017.
- [13] BOULKAMH CHOUAIB " PRISE EN COMPTE DE LA QoS PAR LES PROTOCOLES DE ROUTAGE DANS LES RÉSEAUX MOBILES AD HOC" ,MÉMOIRE DU MAGISTÈRE,UNIVERSITÉ EL HADJ LAKHDAR DE BATNA,ANNÉE 2007-2008.
- [14] DANIEL MABELE MONDONGA, "ETUDE SUR LES PROTOCOLES DE ROUTAGE D'UN RÉSEAU SANS FIL EN MODE AD HOC ET LEURS IMPACTS. CAS DE PROTOCOLES OLSR ET AODV",MÉMOIRE FIN D'ÉTUDE, INSTITUT SUPÉRIEUR D'INFORMATIQUE, PROGRAMMATION ET ANALYSE DE KINSHASA, CONGO, 2009-2010.
- [15] FATIMA AMEZA, "LES TECHNOLOGIES SANS FIL : LE ROUTAGE DANS LES RÉSEAUX AD HOC (OLSR ET AODV)", MÉMOIRE DE FIN D'ÉTUDES, UNIVERSITE ABDERRAHMANE MIRA BÉJAIA, 2006-2007.
- [16] LAIDI MASSYLE ,LARABI MALEK ,"ETUDE COMPARATIVE DES PROTOCOLES DE ROUTAGE MULTICAST AVEC QoS DANS LES RÉSEAUX AD-HOC", MÉMOIRE DE FIN D'ÉTUDES , UNIVERSITE ABDERRAHMANE MIRA BÉJAIA,JUILLET 2019.
- [17] ANNE BENOIT, « ALGORITHMIQUE DES RÉSEAUX ET DES TÉLÉCOMS », 2006. [HTTP ://GRAAL.ENS-LYON.FR/ ABENOIT/RESO05/COURS/3-ADHOC.PDF](http://GRAAL.ENS-LYON.FR/ABENOIT/RESO05/COURS/3-ADHOC.PDF)
- [18] KETTOUCHE FERIEL ET LATROCHE HASNIA « PROTOCOLE DE ROUTAGE MULTI-CHEMINS EAOMDV AVEC CONSOMMATION D'ÉNERGIE DANS LES RÉSEAUX SANS FIL AD HOC » , MÉMOIRE FIN D'ÉTUDE , UNIVERSITE ABDELHAMID IBEN BADIS MOSTAGANEM, 2012/ 2013.
- [19] MOHAMED ALI AYACHI, “ CONTRIBUTIONS À LA DÉTECTION DES COMPORTEMENTS MALHONNÊTES DANS LES RÉSEAUX AD HOC AODV PAR ANALYSE DE LA CONFIANCE IMPLICITE“,THÈSE DE DOCTORAT,UNIVERSITÉ 7 NOVEMBRE À CARTHAGE,24/02/2011.
- [20] ALLOUACHE SOUAD, TAYEB CHERIF RAHMA , “ ETUDE COMPARATIVE ENTRE AODV ET AOMDV DANS LE CADRE DES RÉSEAUX AD HOC“ , MÉMOIRE FIN D'ÉTUDE, UNIVERSITÉ DE BEJAIA, 2016-2017.
- [21] PREETI AGGARWAL, II ER. PRANAB GARG, "AOMDV PROTOCOLS IN MANETS : A REVIEW" , INTERNATIONAL JOURNAL OF ADVANCED RESEARCH INCOMPUTER SCIENCE AND TECHNOLOGY,(32-34),2016.
- [22] FELLAH SOUMAYA ,“OPTIMISATION DU ROUTAGE MULTICAST DANS LES RESEAUX SANS FIL MAILLES“, MÉMOIRE FIN D'ÉTUDE, UNIVERSITÉ D'ORAN, 2010
- [23] CÉDRIC FERRARIS," MULTICAST EXPLICITE DANS LES RÉSEAUX AD HOC MOBILES : IMPLÉMENTATION, ANALYSE ET SIMULATIONS D'UN NOUVEAU PROTOCOLE MULTICAST POUR MANETS",MÉMOIRE FIN D'ÉTUDE, UNIVERSITÉ DE MONTRÉAL, MARS 2007.

## BIBLIOGRAPHIE

---

- [24] R. MERAIHI. "GESTION DE LA QUALITÉ DE SERVICE ET CONTROLE DE TOPOLOGIE DANS LES RÉSEAUX AD HOC". THÈSE DE DOCTORAT, ÉCOLE NATIONAL SUPÉRIEUR DES TÉLÉCOMUNICATION, PARIS, 2004.
- [25] S KHELIFA, Z MEKKAKIA MAAZA, "AN ENERGY REVERSE AODV ROUTING PROTOCOL IN AD HOC MOBILE NETWORKS", WORLD ACADEMY OF SCIENCE, ENGINEERING AND TECHNOLOGY 68 (2010), 1508-1512.
- [26] BENREDJEM GHANIA, «LE ROUTAGE AVEC QOS DANS LES RESEAUX AD HOC», MÉMOIRE FIN D'ÉTUDE, UNIVERSITÉ DE ANNABA , 2016.
- [27] BAGAYOKO AMADOU BABA, « POLITIQUES DE ROBUSTESSE EN RÉSEAUX AD HOC », THÈSE DOCTORAT, UNIVERSITÉ DE TOULOUSE, 2012
- [28] TOUMI-SAIDANE LEYLA, SEFI AHMED, « AODV-US : UN PROTOCOLE DE ROUTAGE SÉCURISÉ POUR LES RÉSEAUX SANS-FIL AD HOC », 4TH INTERNATIONAL CONFERENCE : SCIENCES OF ELECTRONIC, TECHNOLOGIES OF INFORMATION AND TELECOMMUNICATIONS, MARCH 25-29, 2007 – TUNISIA.
- [29] TAHAR ABBES MOUNIR, « PROPOSITION D'UN PROTOCOLE Á ÉCONOMIE D'ÉNERGIE DANS UN RÉSEAU HYBRIDE GSM ET AD HOC » MÉMOIRE FIN D'ÉTUDE, UNIVERSITÉ D'ORAN, 2011/2012.
- [30] ABDUSY SYARIF, RIRI FITRI SARI. «PERFORMANCE ANALYSIS OF AODV-UI ROUTING PROTOCOL WITH ENERGY CONSUMPTION IMPROVEMENT UNDER MOBILITY MODELS IN HYBRID AD HOC NETWORK», VOL. (3), 2911-2916. 2011
- [31] FERRARIS CÉDRIC ,« MULTICAST EXPLICITE DANS LES RÉSEAUX AD HOC MOBILES : IMPLÉMENTATION, ANALYSE ET SIMULATIONS D'UN NOUVEAU PROTOCOLE MULTICAST POUR MANETs» , MÉMOIRE FIN D'ÉTUDE ,UNIVERSITÉ DE MONTRÉAL , MARS 2007
- [32] ABDELHAMID ZEBDI, « DZ-MAODV : NOUVEAU PROTOCOLE DE ROUTAGE MULTICAST POUR LES RÉSEAUX Ad HOC MOBILES BASÉ LES ZONES DENSES », MÉMOIRE FIN D'ÉTUDE, UNIVERSITÉ DU QUÉBEC, AVRIL 2006.
- [33] MERATATE SOUMIA,« LES PROTOCOLES DE ROUTAGE DANS LE RESEAU AD-HOC » ,MEMOIRE DE FIN D'ÉTUDE,UNIVERSITÉ DE MOHAMED BOUDIAF- M'SILA,2015.
- [34] SABEUR KAMMOUN,« IMPLÉMENTATION DE LA QOS SUR UN PROTOCOLE DE ROUTAGE (MULTICAST)AD HOC » ,MEMOIRE DE FIN D'ÉTUDE,ECOLE SUPÉRIEURE DES COMMUNICATION DE TUNIS ,2005-2006.
- [35] [HTTPS ://TOOLS.IETF.ORG/HTML/DRAFT-IETF-MANET-MAODV-00.](https://tools.ietf.org/html/draft-ietf-manet-maodv-00)

## Résumé

Les réseaux ad hoc désignent un système de communication informatique établi temporairement par un ensemble d'utilisateurs souhaitant communiquer entre eux, ceci sans entité centrale pour administrer le réseau, rendant ainsi le routage une tâche propre aux nœuds. Des protocoles de routage adaptés à cette situation sont donc nécessaires.

En plus de l'absence d'administration centrale, les réseaux ad hoc sont caractérisés par une topologie dynamique, de faibles capacités de traitement et de stockage au niveau des nœuds, enfin un médium de communication partagé. Toutes ces caractéristiques imposent aux réseaux ad hoc des défis en matière de routage et de sécurité durant ce modeste travail nous avons étudié le protocole AODV et ses quelques variantes et établi une table de comparaison entre ces protocoles, après nous nous sommes intéressés au protocole MAODV afin d'apporter des améliorations en matière de qualité de service qui sont la perte de paquet et le délai de transmission.

**Mots clés:** Réseaux Ad Hoc, Routage multicast, QoS, Protocole AODV.

## Abstract

Ad hoc networks refer to a computer communication system established temporarily by a set of users wishing to communicate with each other, without central authority to administer the network, thus making routing a task specific to the nodes. Routing protocols adapted to this situation are therefore necessary.

In addition to the absence of central administration, ad hoc networks are characterized by a dynamic topology, low processing and storage capacities at the nodes, and finally a shared communication medium. All of these characteristics impose routing and security challenges on ad hoc networks. During this work, we will study the AODV protocol and establish a comparison table between these protocols, after we are interested in the MAODV protocol in order to bring improvements in terms of quality of service which are the loss of packets and the transmission delay.

**Keywords:** Ad Hoc networks, Multicast routing, QoS, AODV protocol.