



REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEURE ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE IBN KHALDOUN - TIARET

MEMOIRE

Présenté à :

FACULTÉ DES MATHÉMATIQUES ET DE L'INFORMATIQUE
DÉPARTEMENT D'INFORMATIQUE

Pour l'obtention du diplôme de :

MASTER

Spécialité : Réseau et télécommunication

Par :

-Zoubir Khaldia

-Yazid Sichem

Sur le thème

Protocoles de routage ad-hoc : étude et simulation

Soutenu publiquement le 28 / 06 / 2022 à Tiaret devant le jury composé de :

Mr HATTAB Nouredine

MAA Université Iben khaldoun

Président

Mr Nassane Samir

MAA Université Iben khaldoun

Encadrant

Mr BOUALEM Adda

MCB Université Iben khaldoun

Examineur

2021-2022

Remerciement

Nous tenons d'abord à remercier Dieu tout puissant, qui nous avoir donné le courage et la volonté de réaliser ce travail.

Nous remercions chaleureusement notre encadreur Monsieur « Nassane Samir » pour son aide, son encouragement, sa patience, sa disponibilité et ses précieux conseils durant notre préparation de ce projet.

Nous remercions également les membres de jury pour l'honneur d'avoir accepté de juger ce mémoire de fin d'étude.

Nous tenons également à remercier tout enseignant qui a contribué à nous former au cours de Ces année passées.

En fin, nous remercions notre familles, nos amis, no collègues et tous ceux qui nous ont aidé à faire ce travail.

Dédicace

Je Dédie ce travail

A mes chers parents pour tous leurs sacrifices, leur amour, leur soutien et leurs prières tout au long de mes études,

A mes chères sœurs (Ritage, IMANE) pour leur encouragement permanent, et leur soutien moral,

A mes chers frères (ALI, TAYEB, Walid) pour leur appui et leur encouragement,

A ma chère amie Sihem

A mes amies, mes collègues et tous ceux qui m'aiment

Merci d'être toujours là pour moi

Zoubir khaldia

Dédicace

Je Dédie ce travail

A mes chers parents et mes grands-parents, pour tous leurs sacrifices, leur amour, leur soutien et leurs prières tout au long de mes études,

A mes chères sœurs (SARAH, IMANE) pour leur encouragement permanents, et leur soutien moral,

A mes chers frères (ALI, TAYEB, MOHAMED), pour leur appui et leur encouragement,

A ma chère amie KHALDIA

A mes amies, mes collègues et tous ceux qui m'aiment

Merci d'être toujours là pour moi

Yazid sihem

TABLE DES MATIERES

INTRODUCTION GENERALE	1
I.1 Introduction	4
I.2 Définition.....	4
I.3 Principes de fonctionnement	5
I. 4 Historique des réseaux Ad Hoc	5
I.5 Les caractéristiques des réseaux mobiles ad hoc.....	5
I.6 Types des réseaux ad hoc	7
I.6.1 Réseau mobile ad-hoc :	7
I.6.2 Réseau véhiculaire (VANET) :	8
I.6.3 Réseau maillé :	8
I.6.4 Les réseaux de capteurs (WSN) :	9
I.7 Domaines d'utilisation des réseaux ad hoc :	9
I .8 Avantage des réseaux Ad hoc.....	11
I.9 Inconvénients de réseau Ad hoc	11
I. 10 Conclusion	12
II.1 Introduction	14
II.2 Définition de routage.....	14
II.3 Problème de routage dans les réseaux ad hoc	14
II.4 Contraintes de routage dans les réseaux ad hoc	15
II.5 Protocoles de routage dans les réseaux ad hoc.....	15
5.1. Protocole de routage.....	16
II.6 Stratégies de routage ad hoc [19, 20]	16
6.1 Routage hiérarchique ou plat.....	16
6.1.1 Les protocoles de routage à plat :	16
6.1.2 Les protocoles de routage hiérarchique :	16
6.2 Le routage à la source et le routage saut par saut.....	17
6.2.1 Le routage à la source :	17
6.2.2 Le routage saut par saut :	17
6.3 Routage à état de lien / à Vecteur de distance	17
6.3.1 Les protocoles basés sur l'état de lien	17
6.3. 2 Les protocoles basés sur le vecteur de distance	18
6.4 L'inondation.....	18
II.7 Les différentes familles de protocoles de routage MANET.....	19
7.1. Les protocoles de routages proactifs	19

7.1.1 Le protocole DSDV (Destination Sequenced Distance Vector).....	19
1. Principe de fonctionnement	20
2. Les avantages et les inconvénients [3].....	21
7.1.2 Le protocole OLSR (Optimized Link State Routing)	22
1. Description du protocole OLSR	22
2. Détection de voisinage.....	23
3. Types de messages.....	23
4. Sélection de relais multipoints.....	25
5. Déclaration des relais multipoints	26
6. Découverte de la topologie :.....	27
7.1.3 Le protocole de routage TBRPF (Topology Braocast Protocol for Dynamic Networks)	27
7.1.4 Le protocole LSR	29
7.2 Routage réactif	29
7.2.1 Le protocole Ad hoc AODV	30
7.2.2 Le protocole DSR (Dynamic Source Routing).....	31
7.2.3 Le protocole ABR.....	32
7.2.4 Le protocole AOMDV	33
7.3 Routage Hybrides :.....	35
7.3.1 Le protocole ZRP (Zone Routing Protocole).....	35
7.3.2 Le protocole CBRP :.....	36
7.3.3 Le protocole ZHLS (Zone Based Routing Protocol):.....	37
7.4 Protocoles de routage géographique.....	38
7.4.1 Le protocole LAR (Location Aided Routing) [24] :.....	39
7.4.2 Le protocole GPSR (Greedy Perimeter Stateless Routing):.....	40
II.8 les avantages et les Inconvénients des classes de routage ad-hoc :.....	41
II .9 Comparaison entre les approches de routage ad-hoc	41
II .10 Comparaison entre les protocoles de routage ad-hoc.....	42
II.12 Conclusion.....	43
III.1.Introduction.....	46
III.2. Outils de simulation	46
2.1 Simulateur SINALGO.....	46
2.2 Caractéristiques clés de Sinalgo	46
2.3 Installation	47
1. Pre-requis :.....	47
2. Installation :	47

3. En ligne de commande :	47
4 Avec Eclipse	48
3.3. Organisation	48
III.3. Simulation :.....	48
7.2) Exécution du protocole DSR.....	53
III.4 Résultats de la simulation	56
III. 5 Conclusion	56
CONCLUSION GENERALE :	57

LISTE DE FIGURE

Figure I.1 Exemple d'un réseau ad hoc	4
Figure I.2 Principes de fonctionnement	5
Figure I.3 Changement de la topologie d'un réseau ad hoc.....	6
Figure I.4 durée de vie de batterie des nœuds.....	7
Figure I.5 Architecture VANET	8
Figure I.6 Architecture générale d'un réseau maillé.....	8
Figure I.7 Architecture d'un réseau de capteur sans fil	9
Figure I.8 Domaine d'application des réseaux ad hoc	10
Figure I.9 Les applications militaires de réseau ad hoc	10
Figure II.1 Routage dans les réseaux ad hoc	14
Figure II.2 Protocole de routage à plat	16
Figure II.3 Routage hiérarchique	17
Figure II.4 Le mécanisme d'inondation.....	18
Figure II.5 Classification des protocoles de routage ad hoc	19
Figure II.6 Exemple de routage protocole DSDV	20
Figure II.7 Protocole OLSR.....	23
Figure II.8 Echange des messages HELLO	25
Figure II.9 Format message HELLO	25
Figure II.10 Exemple de la sélection des relais multipoints	26
Figure II.11 Format du message TC	26
Figure II.12 Exemple de routage dans OLSR.....	27
Figure II.13 Principe de l'arborescence dans le protocole TBRPF	28
Figure II.14 Découvert de routes entre deux nœuds A et J	31
Figure II.15 Découverte de route.....	32
Figure II.16 Un exemple de protocole ABR.....	33
Figure II.17 Exemple de formation d'une boucle de routage	34
Figure II.18 Exemple de Zone dans le protocole ZRP	36
Figure II.19 Formation des clusters dans CBRP	37
Figure II.20 Topologie niveau intra-zone	37

Figure II.21 Topologie niveau interzone	38
Figure II.22 La zone de diffusion dans LAR	39
Figure II.23 Méthode transmission gloutonne	40
Figure II.24 W est le voisin de S le plus proche de la destination D	40
Figure III.1 Exemple d'interface Sinalgo	47
Figure III.2 Lancement de l'environnement Eclipse	48
Figure III.3 l'interface principale de simulation de protocole AODV	49
Figure III.4 Sélection d'un nœud source pour envoyer un message	50
Figure III.5 Sélection du nœud destinataire	50
Figure III.6 Message RREQ distribué en broadcast	51
Figure III.7 L'envoi du message RREP à la source	51
Figure III.8 la source envoie les données à la destination	52
Figure III.9 Table de routage du nœud source	52
Figure III.10 Message RREQ distribué en broadcast	53
Figure III.11 : L'envoi du message RREP par un nœud intermédiaire	53
Figure III.12 la sélection d'une nouvelle source pour envoyer un message	54
Figure III.13 la sélection d'une même destination	54
Figure III.14 Message RREQ redistribué jusqu'à la destination	55
Figure III.15 : Le chemin de la source qui mène à la destination	55

LISTE DES TABLEAUX

Table II.1 : Structure des entrées des tables de routage d'AODV et AOMDV	35
Table II 2 : Les classes des protocoles de routage ad- hoc	41
Table II 3: Comparaison entre les approches de routage ad-hoc	42
Table II 4: Comparaison entre les protocoles de routage ad-hoc	43

LISTE DES ACRONYMES ET ABREVIATIONS

ABR: Associativity-Based Routing.

AODV: Ad hoc On-demand Distance Vector.

AOMDV: On-Demand Multipath Vector Routing in Ad Hoc Networks.

BQ: broadcast Query.

CBRP: Cluster Based Routing Protocol.

DARPA: Defence Advanced Research Project Agency.

DSDV: Destination Sequenced Distance Vector.

DSR: Dynamic Source Routing.

GPS: Global Positioning System.

GPSR: Greedy Perimeter Stateless Routing.

HNA: Host and Network Association.

IEEE :Institute of Electrical and Electronics Engineers.

IPTV Internet Protocol Television

LAR: Location Aided Routing.

LSR: Link State Routing.

MANET: Mobile ad hoc network.

MID: Multiple Interface Declaration.

MPR: Multi-Point Relays.

OLSR: Optimized Link State Routing.

ONR: Office Naval Research.

RD: Route Delete.

RREP: Route Reply.

RREQ: Route Request.

SINALGO Simulator for Network Algorithmes

TBRPF: Topology Broadcast Protocol for Dynamic Networks.

TC: Topology Control.

VANET: Vehicular Ad-Hoc Network.

WSN : Les Réseaux de capteurs sans fil.

ZHLS: Zone-Based Hierarchical Link State Protocol.

ZRP: Zone Routing Protocol.

INTRODUCTION GENERALE :

Les années 1990 ont été marquées par une croissance rapide des intérêts de recherche dans le domaine des réseaux mobiles ad hoc. En effet, L'évolution des dispositifs sans fil a permis la manipulation de l'information à travers des unités de calculs mobiles qui ont des caractéristiques particulières (une faible capacité de stockage, une source d'énergie autonome.). Contrairement à l'environnement filaire, l'environnement sans fil permet aux unités de calcul une mobilité plus libre sans aucune restriction sur le positionnement des usagers. La mobilité et le mode de communication sans fil, engendrent de nouvelles caractéristiques plus précisément de nouveaux inconvénients propres à l'environnement mobile, à savoir : une fréquente déconnexion, un débit de communication et des ressources modestes, et des sources d'énergie limitées.

Le réseau mobile ad hoc (MANET) est un réseau sans fil, dynamique, sans infrastructure, auto-organisé, à saut multiple et décentralisé. Dans ce type de réseau, les nœuds sont à un instant donné ; des nœuds d'extrémité (émetteur et/ou récepteur) ou des nœuds de transfert (routeurs) qui participent à la découverte et à la maintenance des routes pour l'acheminement des paquets de données entre les nœuds d'extrémités. L'autonomie et la mobilité sont d'une grande influence sur la procédure de routage.

Cette dernière vise à assurer l'acheminement des informations d'une source vers une destination à travers un réseau donné. La particularité du routage est de prendre en considération les changements de la topologie ainsi que les autres caractéristiques du réseau (bande passante, nombre de liens, ressources du réseau...etc.). Par conséquent, la méthode adoptée dans le routage, doit offrir le meilleur acheminement des données en respect des différentes métriques utilisées.

À cet effet, plusieurs protocoles de routage ont été proposés. Chaque protocole essaie de maximiser les performances du réseau en minimisant : le délai de livraison des paquets, l'utilisation de la bande passante et la consommation d'énergie. Les algorithmes de routage ad hoc peuvent se classer en trois catégories : les protocoles proactifs, les protocoles réactifs et les protocoles hybrides.

Les protocoles proactifs maintiennent à jour des tables de routage qui indiquent les routes vers chaque destination du réseau. L'avantage de ces protocoles c'est que la connexion entre les nœuds est immédiate puisque les routes sont calculées à l'avance, ce qui lui permet d'avoir une vue globale

du réseau. Cependant, leur inconvénient c'est qu'ils utilisent beaucoup de paquets de contrôle qui occupent davantage la bande passante.

Par contre, les protocoles réactifs ne cherchent une route qu'à la demande. L'avantage de ces protocoles c'est qu'ils réduisent considérablement le nombre de paquets de contrôle. Cependant, ils consomment un délai initial important pour calculer une route.

Enfin, Les protocoles hybrides essaient de combiner les deux approches précédentes tout en bénéficiant de leurs avantages, mais ils cumulent aussi leurs inconvénients. Le problème est donc de trouver un compromis et essayer d'avoir un délai initial court tout en utilisant un minimum de paquets de contrôle.

Ainsi, Le but général de notre travail est de présenter, en détails, les différentes techniques de routage ad hoc proposés dans le domaine sans fil, et d'en simuler le fonctionnement afin de montrer visuellement la procédure de routage, d'une part, et de toucher réellement les avantages et les lacunes décrits précédemment, d'une autre part.

Chapitre I :
Généralités sur les réseaux
Ad Hoc

I.1 Introduction

Grâce à divers avantages, les réseaux ad hoc ont connu un succès sans cesse croissant dans le marché des réseaux de télécommunication, ils permettent de réduire considérablement le rôle de l'infrastructure fixe car ils contribuent à relier les terminaux qui doivent entrer en communication sans passer par aucun câblage. Ainsi, on peut considérer ces réseaux comme une ultime généralisation des réseaux sans fil.

Dans ce chapitre nous visons à donner un aperçu général sur ce type de réseau, tout en citant les concepts qui y sont liés ; tels que les principales caractéristiques, les contraintes qui en découlent, et les domaines d'application.

I.2 Définition

un réseau ad hoc peut être défini comme une collection d'entités mobiles interconnectées par une technologie sans fil (ondes radio) formant par conséquent un réseau temporaire, sans l'aide d'aucune infrastructure préexistante ou administration centralisée, que ce soit pour sa configuration ou pour sa gestion[1]. 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 couverture, tandis que la communication avec un nœud situé en dehors de sa portée s'effectue via plusieurs nœuds intermédiaires (mode multi-sauts) [2].

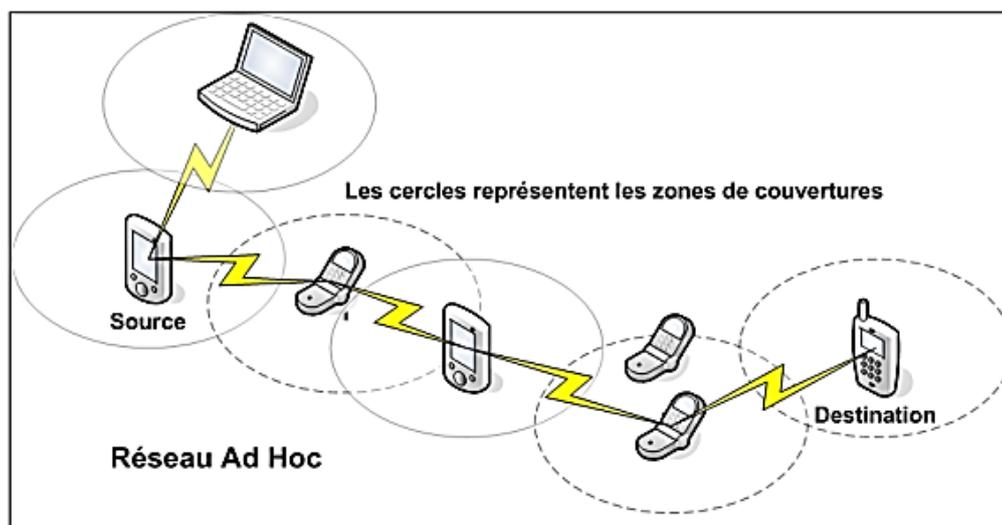


Figure I. 1 : Exemple d'un réseau Ad hoc [18].

I.3 Principes de fonctionnement

Dans le réseau Ad hoc décrit ci-dessous, le nœud mobile A communique avec le nœud voisin B directement, c'est une communication à simple saut. Par contre, dans la communication multi-sauts, un nœud intermédiaire, au moins, doit nécessairement agir comme un routeur entre la source et la destination. Par exemple, entre A et C ou A et E, il n'y a aucun lien radio direct, alors les nœuds B et D doivent servir comme des routeurs intermédiaires entre A - C, et A - E, respectivement. En effet, Dans ce type de réseau, les nœuds peuvent être considérés comme des routeurs à la demande [4].

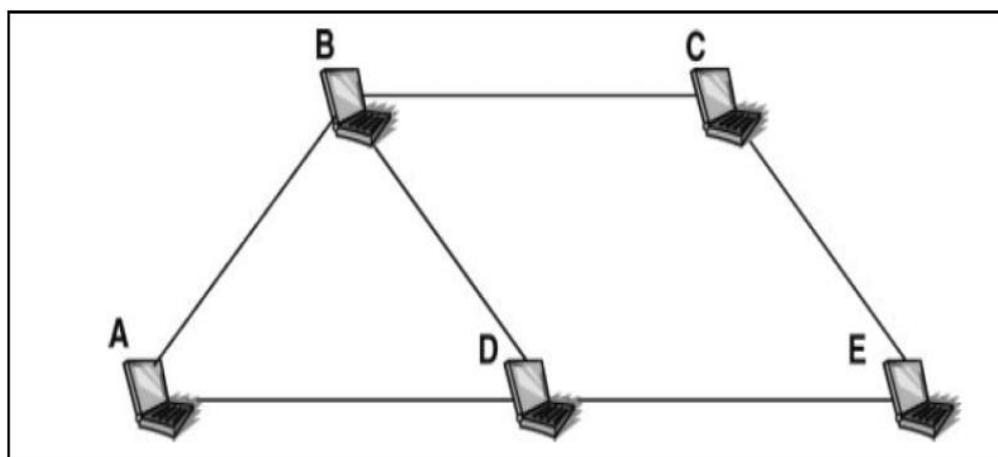


Figure I. 2 : Principes de fonctionnement [4].

I. 4 Historique des réseaux Ad Hoc

Les réseaux ad-hoc mobiles ont été conçus 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 et l'ONR en 1994. Aujourd'hui, avec l'émergence des standards tels que Bluetooth, Hyperplan et IEEE 802.11, les projets de recherches civiles dans ce domaine ont afflué de partout dans le monde [3].

I.5 Les caractéristiques des réseaux mobiles ad hoc

A partir de la définition d'ad hoc nous avons trouvé beaucoup de caractéristiques qui sont résumés dans les points suivants :

- **Absence d'infrastructure** : les réseaux Ad hoc se distinguent des autres réseaux mobiles par l'absence de l'infrastructure fixe et par leurs contrôles décentralisés [4].
- **Mobilité** : La mobilité des nœuds constitue à l'évidence une caractéristique très spécifique des réseaux ad hoc. Cette mobilité est intrinsèque au fonctionnement du réseau. Elle se distingue de la nomadicité (mobilité des seuls nœuds terminaux) ou de l'itinérance (équipements statiques mais pouvant être déplacés) [5].
- **Topologie dynamique** : Dans un réseau ad hoc, les nœuds sont libres de se déplacer aléatoirement, par conséquent la topologie du réseau peut changer d'une façon brusque et rapide [4].

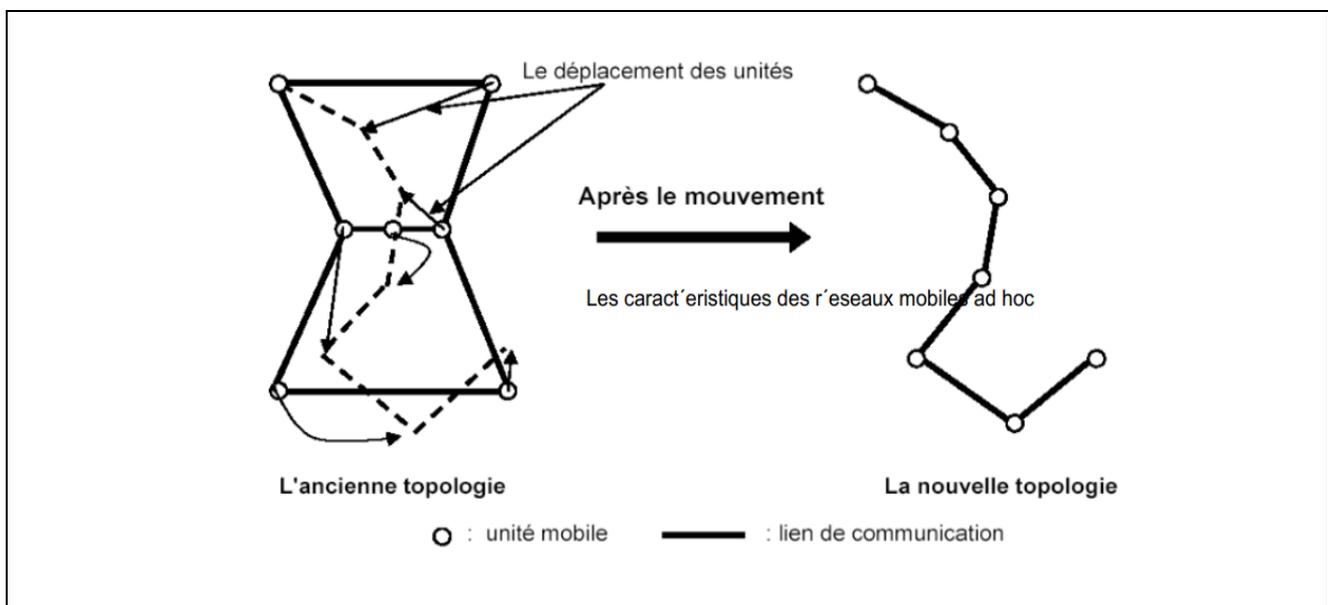


Figure I. 3 : Changement de la topologie d'un réseau ad hoc [3].

- **Equivalence des nœuds du réseau** : Dans un réseau classique, il existe une distinction nette entre les nœuds terminaux (stations, hôtes) qui supportent les applications et les nœuds internes (routeurs par exemple) du réseau, chargés de l'acheminement des données. Cette différence n'existe pas dans ces réseaux car tous les nœuds sont censés jouer les deux rôles en même temps [5].
- **Liaisons sans fil** : Les technologies de communication sans fil sont indispensables à la mise en place d'un réseau ad hoc. Malgré des progrès très importants, leurs performances restent en deçà de celles des technologies des réseaux filaires. La bande passante est moins importante, alors que la gestion de la mobilité génère davantage de flux de contrôle que dans une architecture filaire [5].

- **Vulnérabilité aux différentes attaques** : généralement tous Les réseaux sans fil sont par nature plus sensibles aux problèmes de sécurité. Quant aux réseaux ad hoc, le principal problème réside dans le fait que tous les nœuds sont équivalents et potentiellement nécessaires au fonctionnement du réseau. En conséquence, La possibilité de s'infiltrer facilement dans le réseau devient plus grandes. De plus, l'absence de centralisation rend la détection d'intrusions plus délicate [5].
- **Autonomie des nœuds** : La consommation d'énergie constitue un problème important pour des équipements fonctionnant grâce à une alimentation électrique autonome. Ces équipements intègrent des modes de gestion d'énergie et il est important que les protocoles mis en place prennent en compte ce problème [5].

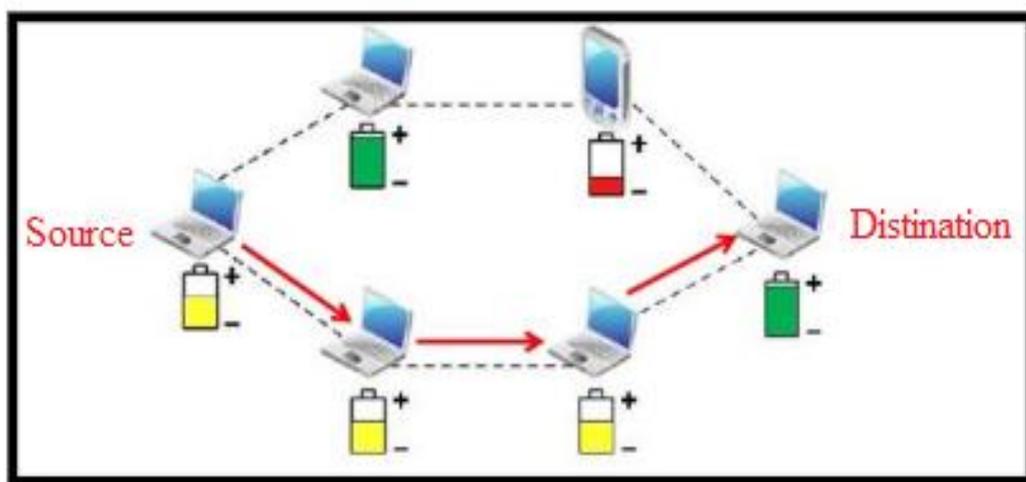


Figure I. 4 : Durée de vie de batterie des nœuds [38].

- **Le Multi-saut** : c'est le point fondamental des réseaux ad-hoc. Tous les nœuds doivent participer au routage et servir comme routeurs intermédiaires [15].

I.6 Types des réseaux ad hoc

I.6.1 Réseau mobile ad-hoc : appelé généralement MANET. Ce type de réseau est formé par plusieurs appareils mobiles se connectant ensemble. Dans ce réseau les nœuds sont libres de se déplacer dans n'importe quelle direction. Ainsi, la topologie change plus fréquemment, et chaque nœud agit comme un périphérique de routage pour propager le trafic vers d'autres périphériques. Ce type ne nécessite pas beaucoup d'intervention humaine [7] [8].

I.6.2 Réseau véhiculaire (VANET) : c'est une extension de MANET, ou le réseau est formé d'un ensemble de véhicules. Ainsi, la topologie du réseau peut changer plus fréquemment par rapport au MANET. Un VANET est représenté en deux structures, la première est l'infrastructure du bord de la route et la seconde est le véhicule lui-même [7] [8].

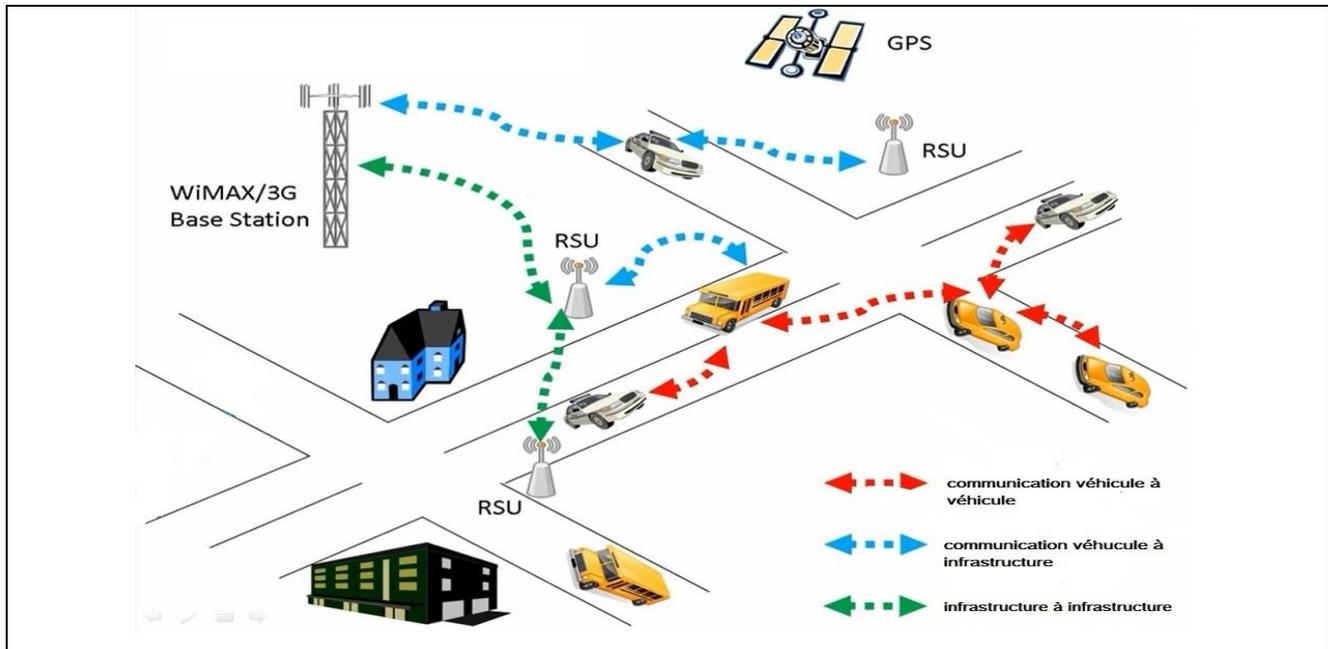


Figure I. 5 : Architecture VANET [34].

I.6.3 Réseau maillé : Ce type de réseau est construit sur le contexte de nœuds radio organisés dans une topologie maillée où les nœuds d'infrastructure sont capables de se connecter directement et sans hiérarchie [8].

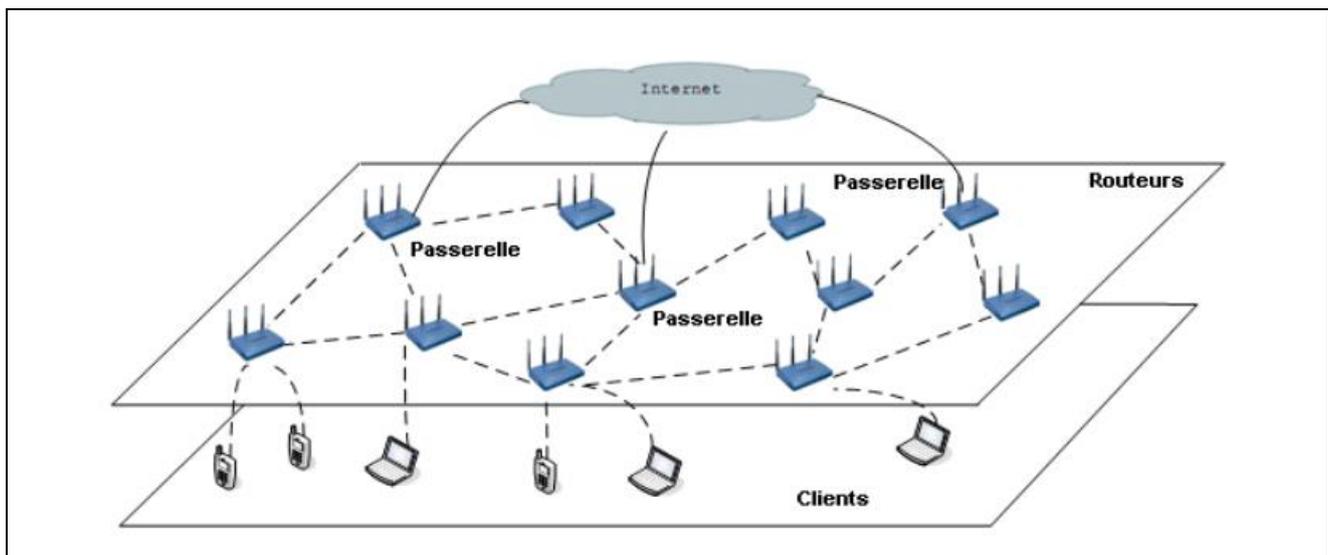


Figure I. 6 : Architecture générale d'un réseau maillé [10].

I.6.4 Les réseaux de capteurs (WSN) :

Ce sont des réseaux ad-hoc composé de nombreux capteurs dotés de capacités de traitement et de stockage réduites. En effet, ces capteurs sans fil sont chargés d'accomplir trois tâches principales, à savoir : le relevé d'une grandeur physique ou environnementale (par exemple : température, pression, pollution...etc), le traitement éventuel de cette donnée et enfin la transmission d'informations vers l'utilisateur final. Ce réseau peut comporter un grand nombre de capteurs (des milliers) généralement statiques et déployés aléatoirement dans des environnements pouvant être dangereux. De plus, ce type de réseau comprend des stations de base (nœuds puits) caractérisées par des capacités de traitement et de stockage plus importantes. Ils agissent comme des passerelles entre les capteurs et l'administrateur final. [11].

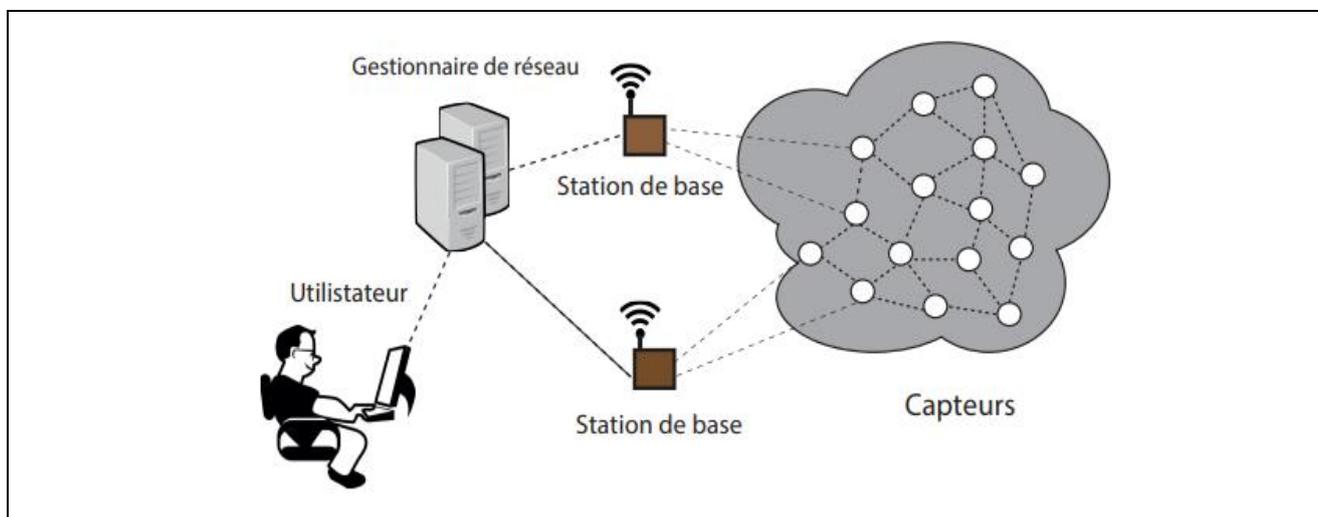


Figure I. 7 : Architecture d'un réseau de capteurs sans fil [37].

I.7 Domaines d'utilisation des réseaux ad hoc :

D'une façon générale, les réseaux ad hoc sont utilisés dans toutes les applications où le déploiement d'une architecture centralisée est contraignant, Soit parce qu'il est difficile à mettre en place, soit parce que la durée d'installation du réseau ne le justifie pas dans ces points, nous abordons certains domaines d'application de réseau ad hoc :

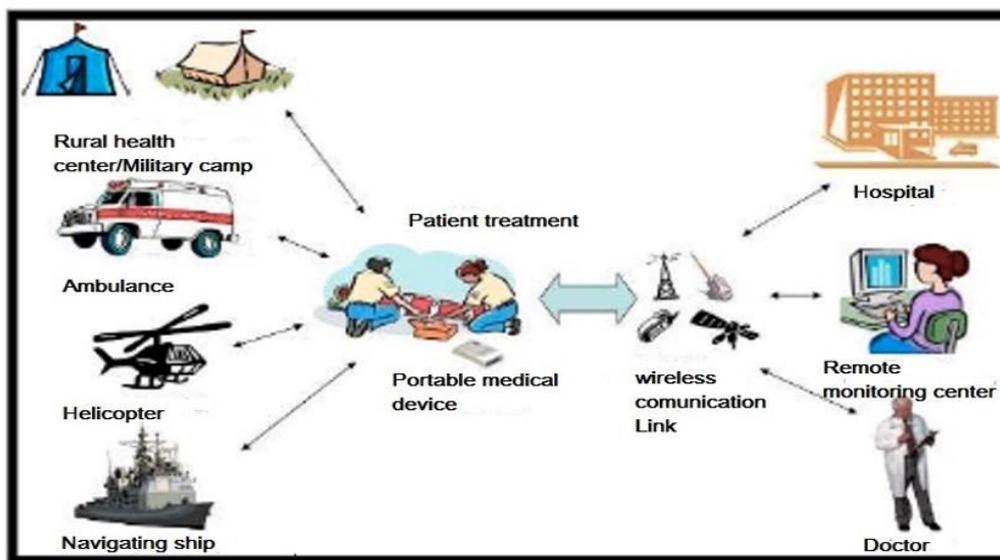


Figure I.8 : Domaines d’application des réseaux Ad Hoc [38].

- **Les applications militaires :** Les réseaux ad hoc ont été utilisés la première fois par les forces armées. En effet ce type de réseaux est la solution idéale pour maintenir une communication sur un champ de bataille entre les différentes troupes militaires [6].

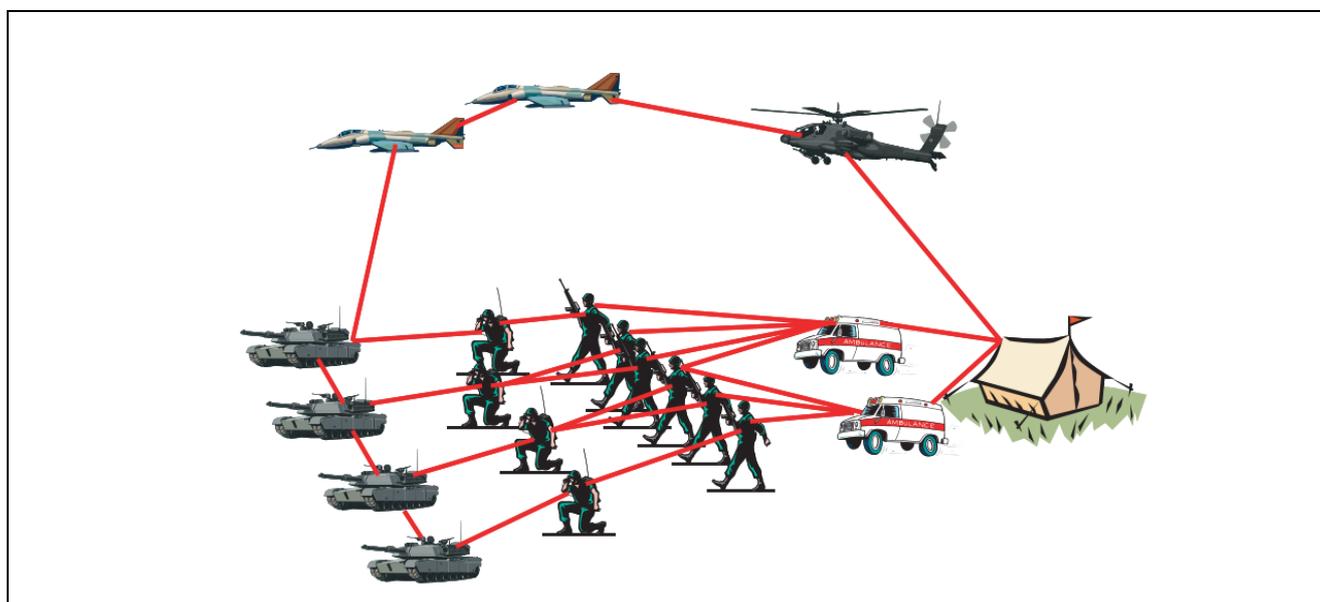


Figure I.9 : Les applications militaires de réseau Ad Hoc [12].

- **Les opérations de recherche et 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, et pour remplacer rapidement l’infrastructure détruite [6].

- **Applications industrielles** : Des scénarios plus complexes dans le domaine industriel appelés réseaux de capteurs peuvent former un MANET pour s'adapter aux différents environnements. Un exemple d'une telle application est la formation d'un MANET pour la surveillance médicale, la détection des Feux de forêt, la surveillance des volcans...etc [6].
- **Les entreprises** : dans le cadre d'une réunion ou d'une conférence [9].
- **Les gares et aéroports** : pour la communication et la collaboration entre les membres du personnel [9].
- **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 [6].

I.8 Avantage des réseaux Ad hoc

- **Absence de câblage** : éliminant toutes les connexions filaires qui sont remplacées par des connexions radio [6].
- **Déploiement facile, rapide et économique** : l'absence du câblage permet de déployer un réseau ad hoc facilement et rapidement. L'absence d'une infrastructure préexistante permet, ainsi, d'économiser tout le temps de déploiement et d'installation du matériel nécessaire [6].
- **Tolérance aux pannes** : un réseau ad-hoc continue à fonctionner même si quelques nœuds tombent en panne, ceci est dû au fait qu'il ne comporte pas de nœuds centraux [10].

I.9 Inconvénients de réseau Ad hoc

Malgré ses avantages, le déploiement de la technologie ad hoc présente certains problèmes liés essentiellement au caractère imprévisible des nœuds, au médium et au routage. Parmi ces problèmes, on peut citer les plus importants :

- **Sécurité** : dans les réseaux ad hoc est difficile à contrôler, notamment parce que dans l'interface air l'écoute clandestine est très simple à réaliser [11].
- **La bande passante** : La bande passante est partagée par tous les nœuds. Ainsi sa disponibilité est affectée par le nombre des nœuds et les trafics à envoyer [12].
- **L'interférence** : Si des transmissions se font sur une même fréquence, des interférences peuvent prendre place, ce qui mène à une perturbation des connexions et à une réduction dans la qualité de liens [12].

- **Débit** : Il est influencé par plusieurs facteurs dans le réseau comme l'occurrence des collisions et la disponibilité du canal. Ce défi s'aggrave avec le déploiement de certains services comme la communication vidéo et l'IPTV [12].
- **Énergie** : Les nœuds dans le réseau ad hoc sont caractérisés par des ressources d'énergie limitées. La consommation d'énergie accroît avec la mobilité des nœuds et l'acheminement multi sauts des paquets. Une gestion de la consommation énergétique est importante afin de garantir une continuité des services [12].
- **La connectivité** limite les possibilités de communication ; ainsi deux stations ne sont joignables que s'il existe un ensemble de terminaux pouvant assumer la fonction de routeur afin de faire acheminer les paquets de données entre ces deux stations [11]

I. 10 Conclusion

Dans ce chapitre, nous avons donné un aperçu général sur les réseaux ad hoc mobiles. En effet, on a cité de nombreuses caractéristiques qui y sont liées, telles que l'absence d'infrastructure et la topologie dynamique. Ce type de réseau présente d'énormes avantages, mais malheureusement, il souffre de plusieurs lacunes dont le plus important est le problème de routage qui reste un défi majeur.

Dans le chapitre suivant, nous allons exposer en détail les principaux protocoles de routage proposés dans ce domaine par la communauté scientifique.

Chapitre II :
**Protocoles de routage dans
les réseaux Ad Hoc Mobiles**

II.1 Introduction

Le service de routage est une opération essentielle dans le réseau ad-hoc, il vise à assurer l'échange des données entre les nœuds mobiles en se basant sur des protocoles adéquats.

Dans ce chapitre, nous présentons en premier lieu les concepts fondamentaux du routage. En deuxième lieu, nous décrivons certains protocoles de routage qui sont développés particulièrement pour les réseaux ad-hoc. En dernier lieu, nous donnons une comparaison entre ces différents protocoles basés sur des paramètres bien définis.

II.2 Définition de routage

Le routage est une méthode d'acheminement des informations vers la bonne destination à travers un réseau de connexion donnée, il consiste à garantir, 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 [13].

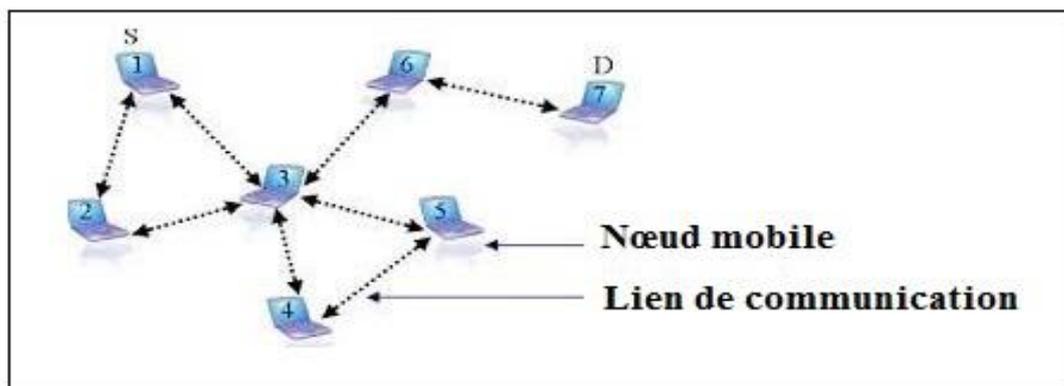


Figure II.1 : routage dans les réseaux ad-hoc [15].

II.3 Problème de routage dans les réseaux ad hoc

Comme nous l'avons vu précédemment, un réseau mobile ad hoc est caractérisé par une absence d'infrastructure fixe et ses nœuds sont libres de s'organiser iniquement. Ainsi, le routage ad hoc consiste à déterminer un acheminement optimal des informations au sens d'un certain critère de performance. En effet, il y a une difficulté dans le choix du critère permettant de dire qu'un chemin est meilleur que l'autre.

Un autre problème qui se pose dans le contexte ad hoc est l'adaptation de la méthode d'acheminement dans un environnement caractérisé par de modestes capacités de calcul et de sauvegarde.

De plus, dans un réseau volumineux, le manque d'informations concernant les destinations peut déclencher une inondation énorme dans le réseau, et cela si on considère seulement la phase de découverte de routes. Le trafic généré par la diffusion, dans ce cas, est rajouté au trafic déjà existant, ce qui dégrade amplement les performances de transmission du système caractérisé principalement par une faible bande passante.

En effet, le problème de routage est plus compliqué à cause du déplacement imprévisible de tous les nœuds concernés par le routage [14, 15].

II.4 Contraintes de routage dans les réseaux ad hoc

La Tache de routage est le plus gros problème des réseaux ad hoc, vu le dynamisme caractérisant la topologie ad hoc et le mouvement des nœuds. Ainsi, tout protocole de routage doit prendre en considération les exigences suivantes :

- Totalemment distribué (tolérance aux pannes).
- Délai minimal pour la recherche de route.
- Convergence vers la solution optimale.
- Mise à jour de route doit impliquer un minimum de nœuds.
- Adaptation rapide aux différents changements de topologies.
- Rafraichissement instantané des tables de routage.
- Surcoût minimal (peu de calcul, peu de paquets de contrôle).
- Exploitation optimale des ressources du réseau.
- Capacité à sécuriser les données [15].

II.5 Protocoles de routage dans les réseaux ad hoc

Les protocoles de routage visent à assurer le transfert des données d'un mobile à un autre. Les liens radio changent d'une manière dynamique et fréquente à cause du déplacement libre des mobiles. Ainsi, Les protocoles de routage doivent s'adapter à ces changements de routes. De plus, ils doivent tenir compte des contraintes des ressources limitées qui caractérisent les réseaux MANET [17].

5.1. Protocole de routage

Le protocole de routage est un algorithme qui sert à déterminer la route optimale pour le transfert des données entre deux nœuds. Le routage dans les réseaux mobiles ad hoc dépend de plusieurs facteurs dont la mobilité, la topologie, la manière de la sélection de la route. Il est à noter que les protocoles de routage ad hoc peuvent être séparés en trois classes essentielles, selon la manière de création et de maintenance de routes lors de l'acheminement des données [3].

II.6 Stratégies de routage ad hoc [19, 20]

Plusieurs stratégies de routage sont apparues, parmi lesquelles nous citons :

6.1 Routage hiérarchique ou plat : premier critère utilisé pour classifier les protocoles de routage dans les réseaux ad hoc concerne le type de vision qu'ils ont du réseau et les rôles qu'ils accordent aux différents mobiles [19].

6.1.1 Les protocoles de routage à plat : considèrent que tous les nœuds sont égaux. La décision d'un nœud de router des paquets pour un autre dépendra de sa position et pourra être remise en cause au cours du temps. Parmi les protocoles utilisant cette technique, on cite l'AODV [19].

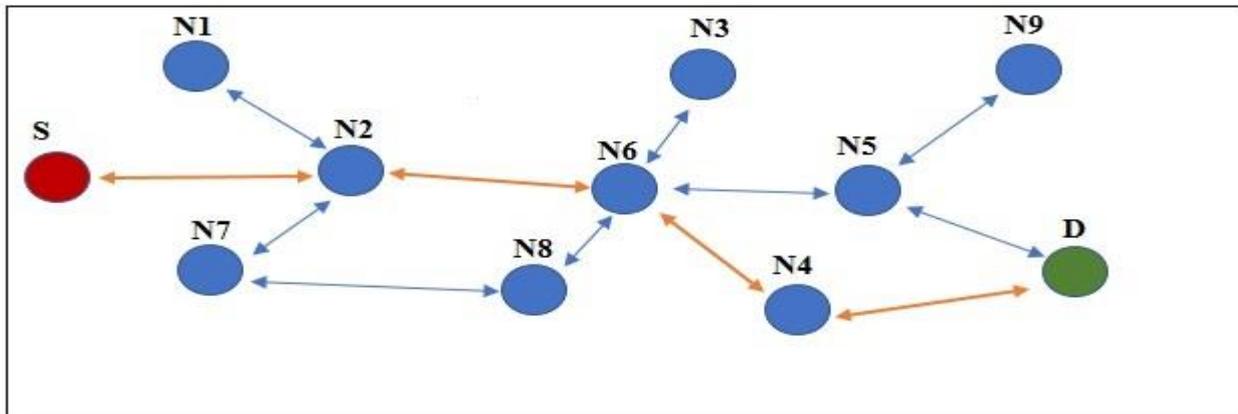
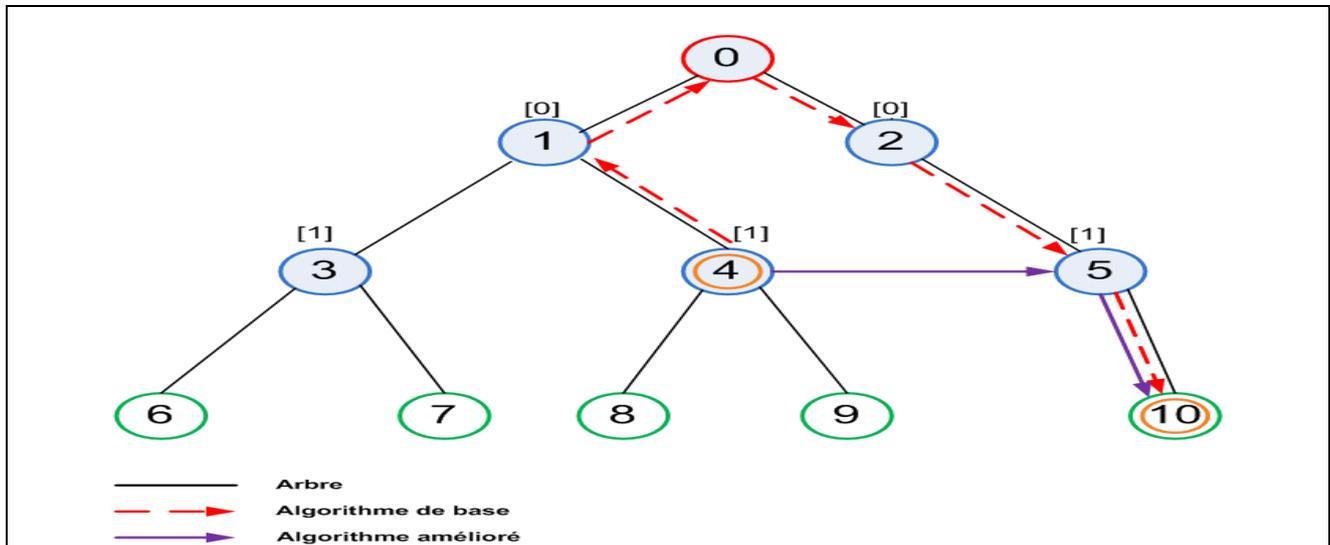


Figure II.2 : protocole de routage à plat [3].

6.1.2 Les protocoles de routage hiérarchique : fonctionnent en confiant aux mobiles des rôles qui varient de l'un à l'autre. Certains nœuds sont élus et assument des fonctions particulières qui conduisent à une vision en plusieurs niveaux de la topologie du réseau. Par exemple, un mobile pourra servir de passerelle pour un certain nombre de nœuds qui seront attachés à lui. Le routage

sera simplifié, puisqu'il se fera de passerelle à passerelle, jusqu'à celle directement attachée au destinataire. Un exemple de protocole utilisant cette stratégie est l'OLSR [20].



FigureII.3 : Routage hiérarchique [39].

6.2 Le routage à la source et le routage saut par saut

6.2.1 Le routage à la source : le routage à la source ou « source routing » consiste à indiquer dans le paquet routé l'intégralité du chemin que devra suivre le paquet pour atteindre sa destination. L'entête de paquet va donc contenir la liste des différents nœuds relayeur vers la destination. Le protocole basé sur cette stratégie est : DSR [19].

6.2.2 Le routage saut par saut : le routage saut par saut ou « hop by hop » consiste à donner uniquement à un paquet l'adresse du prochain nœud vers la destination. L'AODV fait partie des protocoles adoptant cette technique [19].

6.3 Routage à état de lien / à Vecteur de distance

Autres stratégies, héritées du monde filaire, sont faisables pour le routage ad hoc : les protocoles basés sur l'état des liens et ceux basés sur les vecteurs de distance. Les deux méthodes exigent une mise à jour périodique des données de contrôle qui doivent être diffusées par les différents nœuds du réseau. Les algorithmes de routage basés sur ces deux méthodes permettent à un nœud donné de trouver la destination en utilisant le plus court chemin existant dans le réseau [19].

6.3.1 Les protocoles basés sur l'état de lien

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 distribuées 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. En générale, ces algorithmes se basent sur le principe de l'algorithme de Dijkstra pour calculer les chemins les plus courts entre un nœud source et les autres nœuds du réseau. Les principaux protocoles appartenant cette classe sont : OLSR et TBRPF [19].

6.3. 2 Les protocoles basés sur le 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 jusqu'à ce que le réseau atteigne un état stable. Parmi les protocoles basés sur les vecteurs de distance, on cite : DSR, DSDV et AODV [19].

6.4 L'inondation

L'inondation ou la diffusion générale, consiste à envoyer un message dans tout le réseau. Un nœud qui initie l'inondation envoie le paquet à tous ses voisins directs, de même si un nœud quelconque de réseau reçoit le paquet pour la première fois, il le rediffuse à tous les voisins, ainsi de proche en proche, le paquet inonde le réseau.

Notons que le mécanisme d'inondation est utilisé généralement dans la première phase du routage, plus exactement dans la procédure de découverte des routes, et cela dans le cas où le nœud source ne connaît pas la localisation exacte de la destination [19].

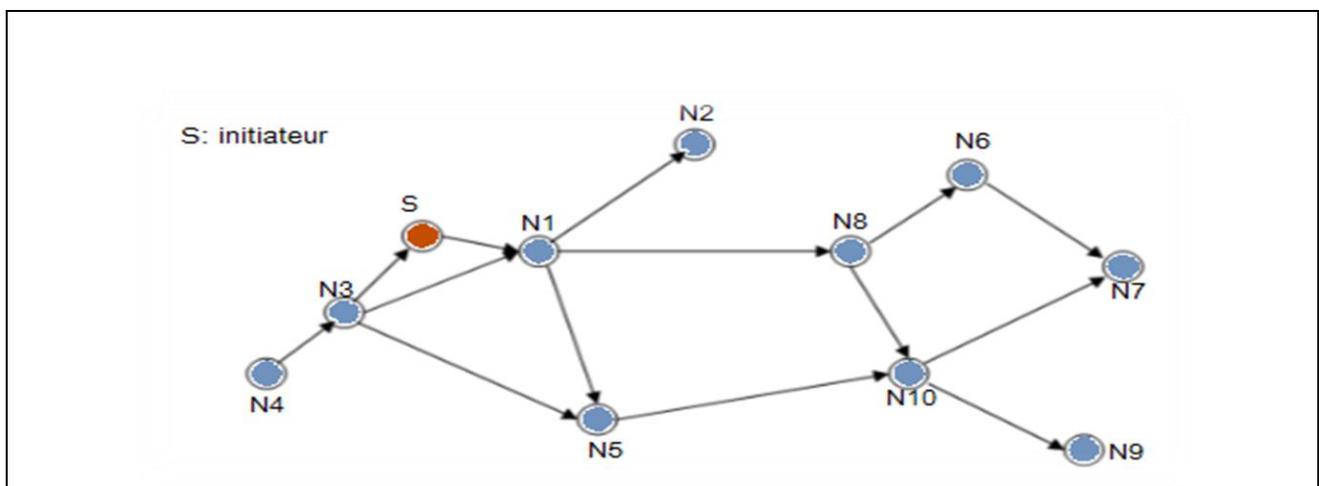


Figure II.4: Le mécanisme d'inondation [19].

II.7 Les différentes familles de protocoles de routage MANET

L'objectif principal de chaque protocole est d'assurer un routage efficace dans un environnement dynamique, A cet effet, plusieurs protocoles de routage ont été proposés, On peut les regrouper en plusieurs catégories : les protocoles de routage proactifs, les protocoles de routage réactifs et les protocoles de routage hybrides, géographiques, hiérarchiques, à qualité de service et multicast...etc.

Nous expliquerons chaque catégorie avec ces propres protocoles en détails dans ce qui suit :

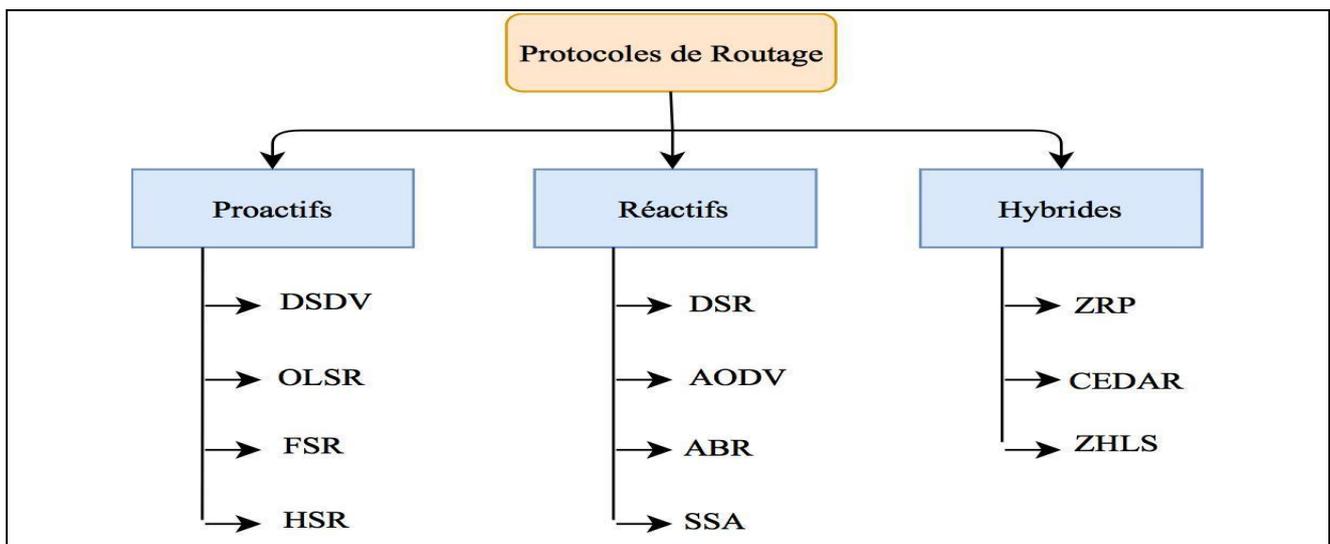


Figure II.5 : Classification des protocoles de routage ad-hoc [15].

7.1. Les protocoles de routages proactifs

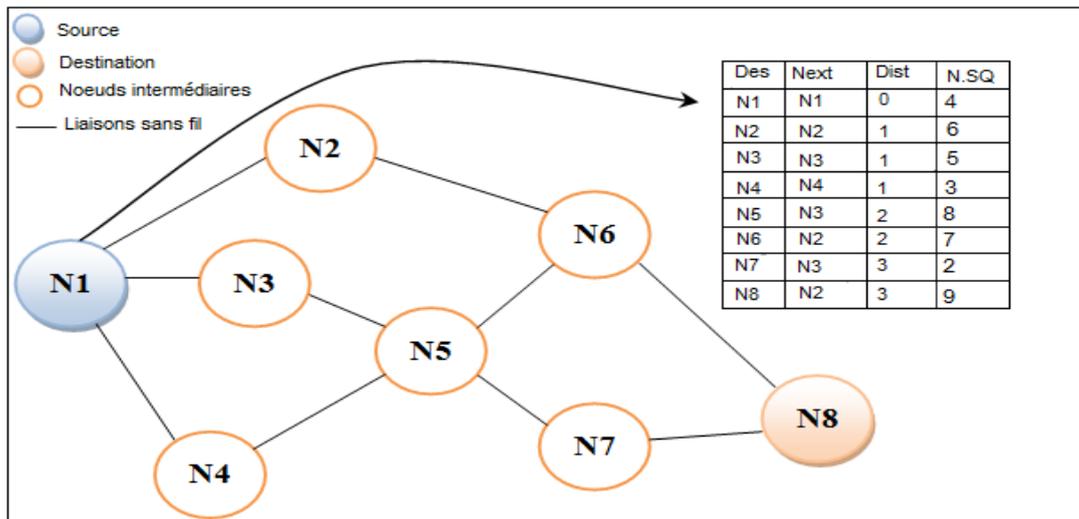
Les protocoles de routage proactifs essaient de maintenir, au niveau de chaque nœud du réseau, les meilleurs chemins existants vers toutes les destinations possibles. Les routes sont sauvegardées mêmes si elles ne sont pas utilisées [21]. La sauvegarde permanente des chemins de routage, est assurée par un échange continu des messages de mise à jour des chemins [3].

Deux méthodes fondamentales sont utilisées dans cette catégorie de protocoles proactifs : La méthode à état de lien et la méthode à vecteur de distance [16].

7.1.1 Le protocole DSDV (Destination Sequenced Distance Vector)

L'algorithme de routage appelé "Vecteur de Distance à Destination Dynamique Séquencieé" ou DSDV a été conçu spécialement pour les réseaux mobiles. Il est basé sur l'idée classique de l'algorithme distribué de Bellman-Ford (DBF) en rajoutant quelques améliorations. Chaque station mobile maintient une table de routage qui contient :

- Toutes les destinations possibles.
- Le nombre de nœud (ou de sauts) nécessaire pour atteindre la destination.
- Le numéro de séquences "SN "qui correspond au nœud destination.



FigureII.6 : Exemple de routage protocole DSDV.

1. Principe de fonctionnement

Périodiquement chaque nœud dans le réseau diffuse par inondation un paquet de mise à jour des tables de routage qui inclut les destinations accessibles et le nombre de sauts exigé pour atteindre chaque destination avec le numéro de séquence lié à chaque route. Des paquets de mise à jour sont aussi diffusés immédiatement s'il y a un changement dans la topologie du réseau afin de propager les informations de routage aussi rapidement que possible. A la réception d'un paquet de mise à jour, chaque nœud le compare avec les informations existantes dans sa table de routage. Les routes les plus récentes (qui ont le plus grand numéro de séquence) avec la distance la plus courte sont gardées, les autres sont simplement ignorées [3].

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

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

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

qui réduit le nombre de paquets transmis. La façon de faire la mise à jour est liée à la stabilité du réseau. Dans le cas où le réseau serait relativement stable, la mise à jour incrémentale est utilisée pour réduire le trafic de la communication, la mise à jour complète n'est pas fréquente dans ce genre de situation. Dans le cas opposé, où le réseau subit des changements rapides, le nombre de paquets incrémentaux envoyés augmente, ce qui fait que la mise à jour complète est fréquente.

Un paquet de mise à jour contient

- 1- Le nouveau numéro de séquence incrémenté.
- 2- L'adresse de la destination.
- 3- Le nombre de nœuds (ou de sauts) séparant le nœud de la destination.
- 4- Le numéro de séquence tel qu'il a été estampillé par la destination.

Les données de routage reçues par une unité mobile, sont comparées avec les données déjà disponibles. La route étiquetée par la plus grande valeur du numéro de séquence (i.e. la route la plus récente), est la route utilisée. Si deux routes ont le même numéro de séquence, alors la route qui possède la meilleure métrique, est celle qui sera utilisée.

Le DSDV élimine les deux problèmes de routage "boucle de routage" et celui du "compter jusqu'à l'infini". Cependant, dans ce protocole, une unité mobile doit attendre jusqu'à ce qu'elle reçoive la prochaine mise à jour initiée par la destination, afin de mettre à jour l'entrée associée à cette destination. Ce qui fait que le DSDV est lent [14].

2. Les avantages et les inconvénients [3]**Avantage :**

- Il est adapté au réseau ad-hoc de petite taille.
- Il élimine les problèmes de boucle.
- Le trafic supplémentaire peut être évité avec les mises à jour par accroissement.
- DSDV maintient un seul chemin vers une destination.

Inconvénients :

- La bande passante est souvent occupée en raison de l'envoi périodique des vecteurs de distance.
- DSDV ne supporte pas le routage multi-chemins.

- Il est difficile de déterminer le délai nécessaire pour la découverte des routes.
- Il est difficile de maintenir une table de routage pour un réseau de grande taille.
- DSDV exige une mise à jour régulière qui épuise la puissance de batterie.

7.1.2 Le protocole OLSR (Optimized Link State Routing)

1. Description du protocole OLSR

Le protocole "OLSR" appartient à la famille des protocoles de routage à état de lien (Link State Routing) où chaque nœud découvre ses voisins, et les déclare à tous le réseau par diffusion [22].

Le concept fondamental utilisé dans ce protocole est l'utilisation des relais multipoints "MPR" (Multi-Point Relays) Chaque nœud choisit dans son voisinage un ensemble des nœuds "MPR". L'ensemble des nœuds MPR sont choisis de sorte qu'il couvre tous les nœuds qui sont à deux sauts. Les MPR expédient des messages de diffusion pendant le processus d'inondation et ils sont les seuls à déclarer leurs liens. Cette technique réduit considérablement la surcharge du réseau par rapport au mécanisme classique d'inondation où chaque nœud retransmet chaque message [17].

Le protocole "OLSR" déclenche des échanges périodiques de messages HELLO pour permettre à chaque nœud de connaître ces voisins à 1-saut et à 2-sauts. Par la suite, "OLSR" utilise une diffusion optimisée des messages de contrôle grâce à l'utilisation des relais multipoints MPR. Ceci permet à chaque nœud d'avoir une vue de la topologie et ainsi utiliser un algorithme de plus court chemin pour calculer sa table de routage vers toutes les destinations [23].

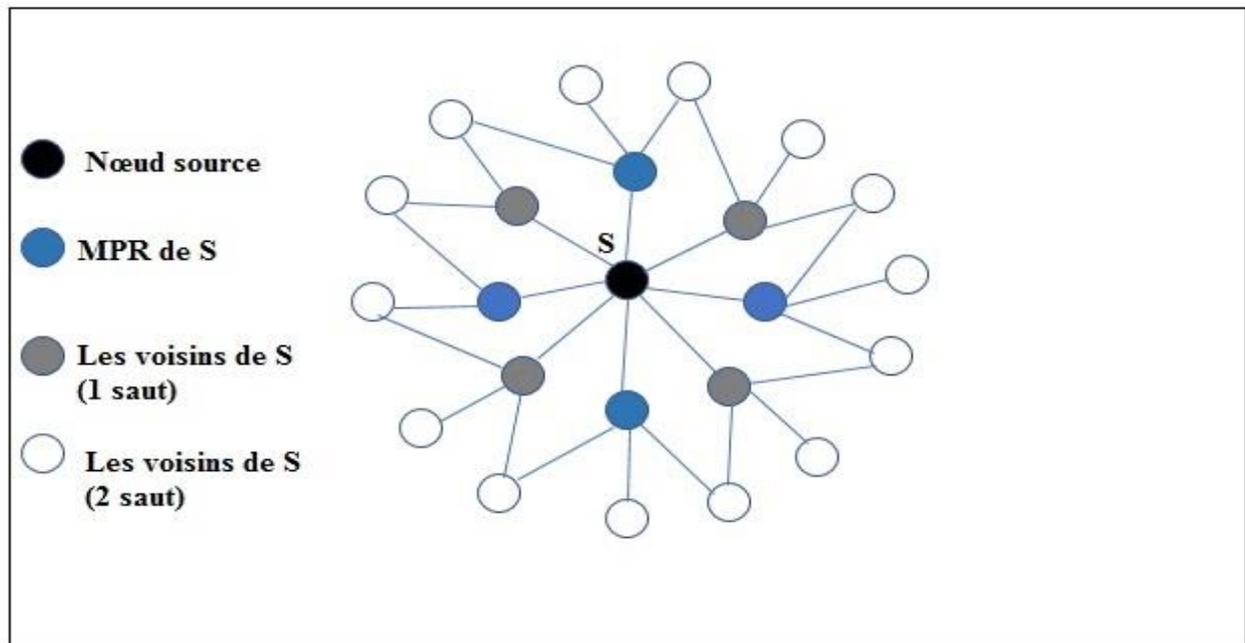


Figure II.7 : protocole OLSR.

2. Détection de voisinage

Les réseaux ad-hoc sont caractérisés par une topologie dynamique. Afin de détecter tout changement dans le réseau et générer les informations sur la topologie, le protocole "OLSR" se base essentiellement sur la détection et la mise à jour de la liste des voisins de chaque nœud. Dans tout ce qui suit, on considère que tous les nœuds ont une seule interface sans fil [23].

On peut classer les liens entre deux nœuds en trois catégories :

- **Asymétrique** : Un lien est dit asymétrique si un nœud reçoit des messages de l'autre nœud mais ce dernier n'a pas reçu la confirmation que le premier nœud l'entend.
- **Symétrique** : Un lien est dit symétrique si chaque nœud entend l'autre.
- **Perdu** : Un lien est dit perdu s'il a été déclaré précédemment symétrique ou asymétrique mais à ce moment il est disparu [23].

3. Types de messages

Le protocole "OLSR" utilise quatre types de messages :

- **HELLO** : utilisé pour la détection de voisinage.
- **TC** : permet la diffusion des informations de topologie.
- **MID** : permet de publier la liste des interfaces de chaque nœud.

- **HNA** : utilisé pour déclarer les sous-réseaux et hôtes joignables par un nœud jouant le rôle de passerelle.

Ainsi OLSR effectue deux actions principales :

- **La détection de voisinage**, grâce à l'envoi de messages HELLO et à la détermination des MPRs.
- **Le contrôle de la topologie**, effectuée par l'intervention des messages TC, MID et HNA et aboutissant à une table de routage globale dans chaque entité mobile [22].

Chaque nœud du réseau diffuse périodiquement des messages 'HELLO' pour détecter ses voisins directs. Ces messages contiennent la liste des voisins connus du nœud et leur état de liens. L'état de la liaison peut-être soit symétrique, asymétrique, perdu ou relais multipoint. Ce dernier état signifie que le lien est symétrique et que l'expéditeur du message HELLO a choisi ce nœud comme un MPR. Les messages HELLO sont diffusés à chaque intervalle de temps, fixé à deux secondes par défaut. Ces HELLO sont reçus par tous les voisins à un saut, mais ils ne sont pas transmis. Ainsi, les messages HELLO permettent la découverte de voisinage à un saut, et à deux sauts pour chaque nœud. Un intervalle de maintien de validité est associé aux informations de voisinage à un saut et à deux sauts. La figure II.8 montre un exemple de détection de voisinage par échange de messages HELLO :

1. A envoie un HELLO vide à B qui enregistre A comme voisin asymétrique puisque l'adresse de B ne figure pas dans le message HELLO ;
2. B envoie un HELLO à A en déclarant ce dernier comme son voisin asymétrique en mettant son adresse dans le message;
3. A trouve sa propre adresse dans le HELLO envoyé par B, alors il envoie un HELLO à B en enregistrant l'adresse de B comme voisin symétrique ;
4. De même B trouve son adresse dans le HELLO envoyé par A, alors il envoie un HELLO à A en enregistrant l'adresse de A comme voisin symétrique ;

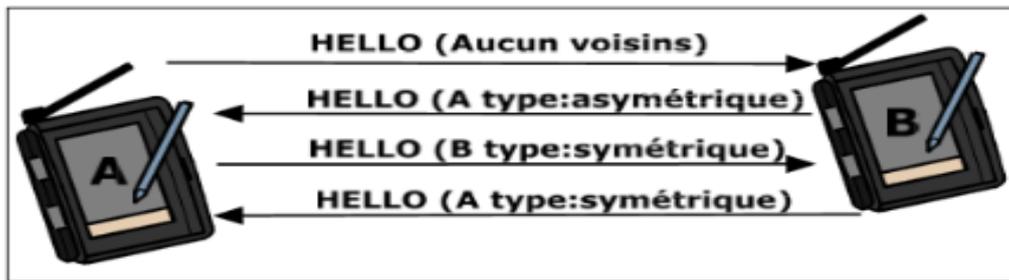


Figure II.8: Échange des messages HELLO [23].

La Figure II.9 présente le format des messages HELLO. Chaque message se compose en plusieurs sections qui correspondent à différents états de liens. La liste des adresses des interfaces voisines qui possèdent un lien symétrique sont listés dans les champs Neighbors Interface Adresse [23].

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
Réservé										Htime										Volonté											
Code de lien					Réservé										Taille du message de lien																
Adresse de l'interface voisine																															
Adresse de l'interface voisine																															
...																															

Figure II.9: Format message HELLO [23].

4. Sélection de relais multipoints

Chaque nœud du réseau sélectionne d'une façon indépendante son ensemble de relais multipoints. Dans le but de construire la liste des voisins à deux sauts d'un nœud donné, il suffit de garder une trace de la liste des nœuds ayant des liens symétriques et trouvés dans les messages HELLO transmis par les voisins et reçus par ce nœud. Les relais multipoints d'un nœud sont décalés dans les messages HELLO, ainsi qu'à la réception des messages HELLO, chaque nœud met à jour sa table d'électeur MPR, dans laquelle il met les adresses des voisins qui l'ont choisi comme MPR avec un numéro de séquence. L'élection des relais multipoints permet donc de réduire le nombre de retransmissions inutiles [16].

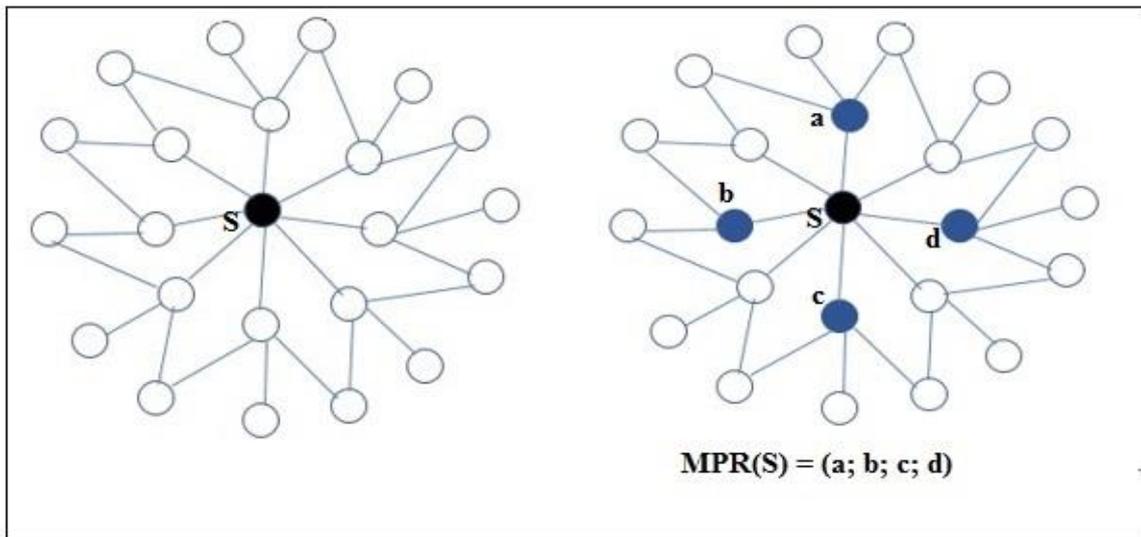


Figure II .10 : Exemple de sélection des relais multipoints [23].

5. Déclaration des relais multipoints

Un algorithme approprié est utilisé par chaque nœud pour construire l'ensemble des relais multipoints. Afin de fournir les informations sur la topologie nécessaire pour construire les routes et ainsi garantir le routage des paquets, chaque nœud qui a été sélectionné comme étant MPR, diffuse périodiquement des messages de contrôle de la topologie "TC". Ces messages sont reçus par tous les nœuds mais transmis juste par les MPRs.

Chaque nœud x qui a été sélectionné comme MPR maintient une liste des voisins MPR-Sel(x) Qui l'ont sélectionné comme relais multipoint.

Chaque message "TC", envoyé par un nœud "x", contient la liste MPR-Sel(x) ainsi qu'un numéro de séquence (ANSN) associé au message. Ces messages permettent à chaque nœud de maintenir à jour sa table d'information sur la topologie et ainsi faciliter le calcul de sa table de routage [23].

0										1										2										3	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
ANSN										Réservé																					
Adresse principale du voisin annoncée																															
Adresse principale du voisin annoncée																															

Figure II.11: Format du message TC [23].

6. Découverte de la topologie :

Les informations spécifiques à la découverte des voisins et à la découverte de la topologie sont mis à jour périodiquement. Ces informations permettent à chaque nœud de calculer des chemins vers toutes les destinations connues. Les chemins étant calculés selon l’algorithme Dijkstra, par conséquent, Ils sont optimaux en termes de nombre de sauts. Chaque fois qu’il y a un changement dans les informations de voisinage ou de la topologie, la table de routage est recalculée.

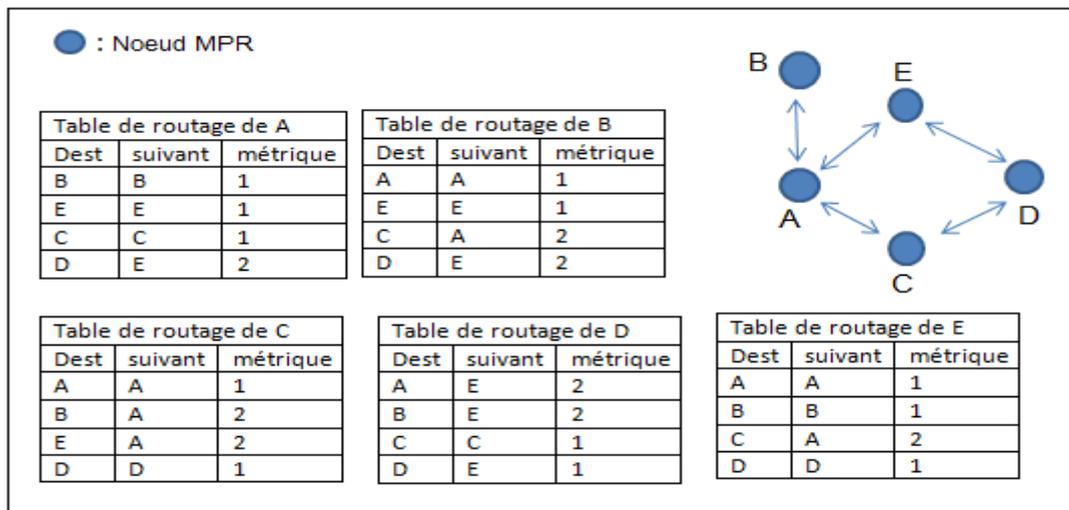


FIGURE II.12: Exemple de routage dans OLSR [17].

Le routage dans OLSR se fait saut par saut. La figure II.12 illustre un exemple de routage "OLSR" dans un petit réseau ad hoc. Chaque nœud du réseau calcule sa table de routage pour atteindre les autres nœuds, en se basant sur les informations de voisinage et de topologie mises à jour périodiquement. Dans la figure, nous observons que chaque nœud maintient sa propre table de routage. Cette table contient l’adresse de chaque nœud du réseau comme destination, le nœud suivant à utiliser pour atteindre la destination, et la métrique exprimée en nombre de sauts.

A Partir de ces informations, une table de topologie globale est construite qui donne une idée sur la topologie du réseau. Cette table contient les adresses de tous les nœuds comme destination et le nœud last qui précède la destination [17].

7.1.3 Le protocole de routage TBRPF (Topology Braocast Protocol for Dynamic Networks)

TBRPF est un protocole de routage proactif à état de liens. Chaque nœud calcule un arbre ayant comme racine la destination (un arbre est calculé pour toute destination accessible du réseau), le

calcul de l'arbre se fait par l'algorithme de Dijkstra en se basant sur la table de topologie et la table des voisins.

Chaque nœud maintient à son niveau les informations suivantes :

- La table de topologie qui contient tous les arcs du réseau, chaque arc a un coût et un numéro séquentiel de mise à jour.
- La table des voisins.
- Pour chaque destination du réseau, le nœud maintient l'information nœud père et les nœuds fils appartenant à l'arbre qui a comme racine cette destination.

Le nœud père est calculé par l'algorithme de Dijkstra en se basant sur la table de topologie et la table des voisins. Un message est envoyé au père pour l'informer de ce choix, ce message sert aussi à construire la liste des fils.

L'arbre est construit à partir des feuilles vers la racine, par contre, la mise à jour se fait à partir de la racine par envoi des tables de topologie. TBRPF utilise une mise à jour périodique et différentielle, où chaque nœud diffuse sa table pour ses fils seulement, ce qui réduirait le trafic par rapport à la diffusion classique.

TBRPF utilise aussi des messages d'information entre voisins pour mettre à jour l'état des liens entre eux [24]

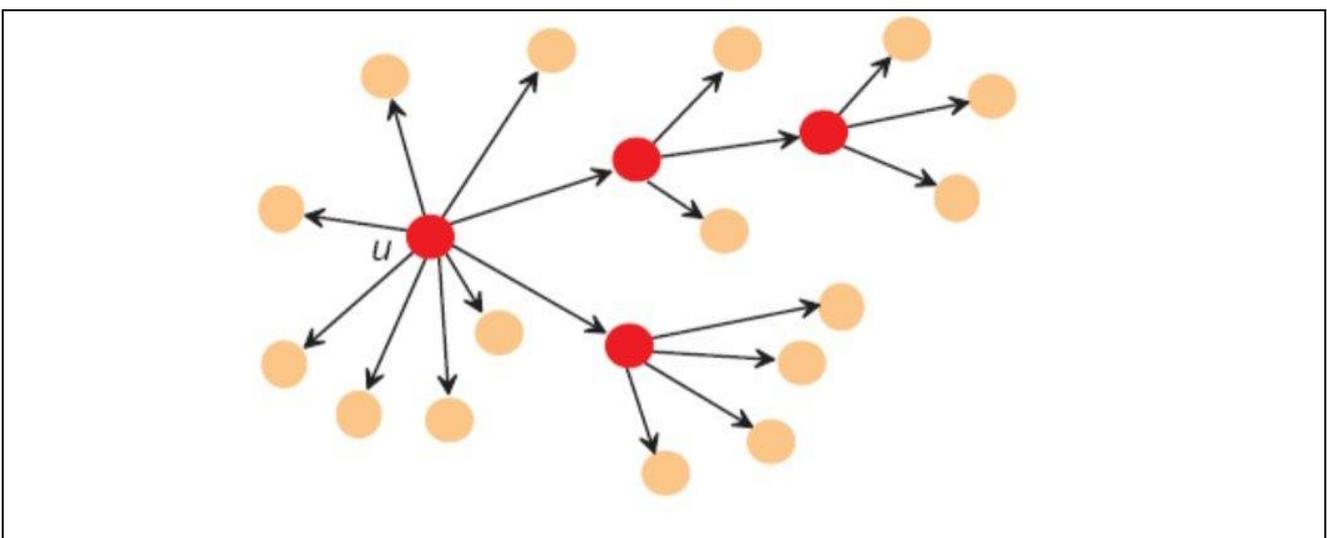


Figure II.13: Principe de l'arborescence dans le protocole TBRPF.

7.1.4 Le protocole LSR

Dans le protocole LSR (Link State Routing) chaque station envoie constamment à ses voisins l'état de ses liens. Ces derniers acheminent à leur tour, et de proche en proche les informations qu'ils reçoivent, jusqu'au moment qu'elles soient connues de toutes les stations. De cette façon, chaque station va pouvoir former ainsi sa propre table de routage, qui va être utilisée lorsque la station souhaitera joindre un destinataire : une simple recherche dans la table va suffire pour trouver le récepteur. Ce protocole illustre parfaitement le concept de routage proactif, et cumule les défauts inhérents à cette technologie (une diffusion parfois excessive des données de routage, gaspillage de la bande passante). En faible mobilité, ce protocole fournit de bons résultats, mais il s'affaiblit progressivement quand la mobilité des stations augmente [10].

7.2 Routage réactif

Un protocole de routage réactif est un protocole caractérisé par le fait que la mise à jour des informations de routage se fait à la demande. Ainsi, lorsqu'un nœud source a besoin de transmettre les données vers une destination, il doit rechercher une route en diffusant des messages de contrôle sur le réseau. Contrairement aux algorithmes proactifs qui maintiennent les routes vers l'ensemble des stations du réseau, les protocoles réactifs ne conservent que les routes qui ont une utilité. En générale, ce type de protocole fonctionne comme suit [25, 10] :

- Le nœud émetteur diffuse une requête « Route Request RREQ » au niveau de son rayon de propagation.
- Le mécanisme d'inondation permet à cette requête de se propager sur tout le réseau.
- À chaque fois que le paquet passe par un nœud mobile, jouant dans ce cas le rôle d'un routeur, une information portant l'identifiant du nœud est ajoutée à la route jusqu'à ce que le paquet arrive à sa destination.
- À la réception du paquet, le nœud destinataire renvoie le tracé du chemin à la source en suivant le chemin inverse.
- Parmi toutes les routes renvoyées par le nœud destinataire, le nœud source sélectionne la plus petite et la sauvegarde dans son cache afin de l'utiliser en cas de besoin [26].

Le problème avec ces protocoles c'est qu'ils ont un délai initial avant de commencer la transmission des paquets provoqué par la procédure de découverte de route, aussi la redécouverte de route en cas de panne génère une charge supplémentaire [9].

7.2.1 Le protocole Ad hoc AODV

Est un protocole de routage réactif à vecteur de distance qui s'inspire de DSDV. Ce protocole crée les routes au besoin pour réduire le nombre de diffusions de messages de contrôle. AODV utilise les numéros de séquence pour déclarer les chemins les plus récents, forcer les mises à jour si nécessaires et éviter les boucles. De plus, il utilise le nombre de sauts comme métrique pour choisir entre plusieurs routes disponibles. Trois types de paquets sont utilisés par AODV : les paquets de requête de route RREQ (Route Request Message), les paquets de réponse de route RREP (Route Reply Message) et les paquets d'erreur de route RERR (Route Error Message). En outre, AODV déclenche périodiquement des paquets de contrôle « HELLO » pour s'assurer de la validité des liens [27].

La fonction des nœuds intermédiaires n'est pas seulement de retransmettre des RREQ mais aussi de se mettre à jour avec les informations de la source. AODV repose sur deux mécanismes [27] :

- Découverte de voisinage :

L'envoi de messages entre un nœud source **S** et une destination **D** se déroule selon le principe suivant [27, 31] :

- Lorsque **S** ne possède pas de route valide à **D** dans sa table de routage. Il diffuse une requête de route RREQ. Cette requête RREQ contient un identifiant (RREQ ID) unique pour tous les voisins. Cet identifiant est une incrémentation de la dernière valeur connue du numéro de séquence, associé au nœud destination. Cette valeur est recopiée de la table de routage, s'il n'est pas connu, la valeur nulle sera prise par défaut. Après la diffusion du message RREQ, la source attend le paquet réponse de route (RREP : Route Reply). Si ce dernier n'est pas reçu durant une certaine période (appelée RREP_WAIT_TIME), la source peut rediffuser une nouvelle requête. A chaque nouvelle diffusion, le champ RREQ ID du paquet est incrémenté. Si la requête RREQ est rediffusée un certain nombre de fois (RREQ_RETRIES) sans la réception de réponse, un message d'erreur est délivré à l'application.
- Quand un nœud intermédiaire reçoit le message RREQ, il met à jour le numéro de séquence dans sa table de routage pour pouvoir reconstruire ultérieurement le chemin inverse, qui sera traversé par le paquet de réponse de la route.

- Quand la requête atteint la destination ou un nœud qui possède une route récente, un paquet de réponse RREP est envoyé à la source. Cette réponse est émise à destination de l'initiateur de la requête sur la route inverse de celle parcourue par la requête.

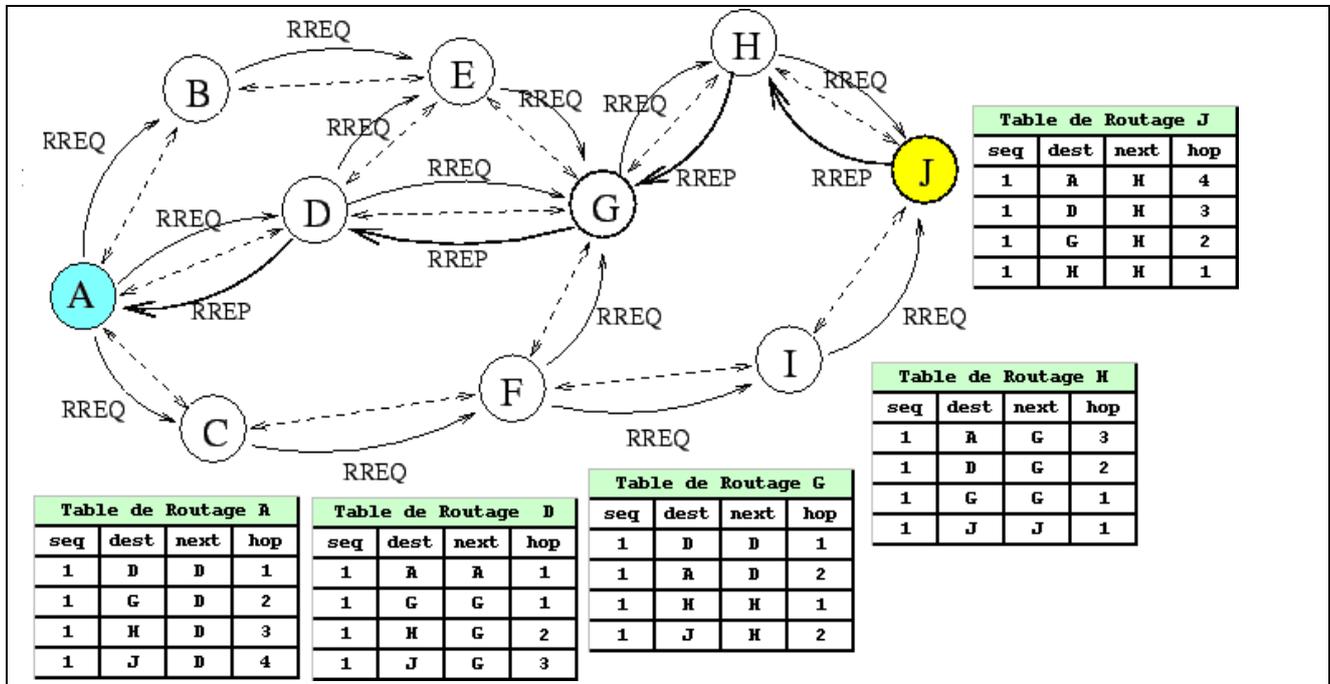


Figure II.14: découverte de routes entre deux nœuds "A" et "J".

-Maintenance de route

La maintenance des routes est réalisée en deux étapes. La première étape consiste en la détection de la perte d'une route. Quand un nœud sur une route établie se déplace, les routes qui passent par ce nœud peuvent être rompues. Les nœuds en amont, détectant la perte de connectivité grâce aux paquets HELLO, préviennent les sources affectées en émettant une requête d'erreur RERR. A la réception de ce paquet, le nœud source engage la deuxième étape de la maintenance des routes. Il lance une nouvelle phase de découverte des routes pour trouver un autre chemin [27].

7.2.2 Le protocole DSR (Dynamic Source Routing)

Le protocole Routage à la Source Dynamique est un protocole de routage réactif, efficace et dédié aux réseaux ad hoc mobile multi-sauts.

Ce protocole est basé sur la technique de routage à la source. Avec cette technique, la station source détermine la séquence complète des nœuds que doivent traverser les paquets de données afin d'atteindre la destination. [26]

Le principe du protocole DSR, se décompose en deux phases principales :

La découverte de route : la source émet une requête RREQ (Route Request), contenant un champ de route, en diffusion à ses voisins qui diffusent à leur tour cette requête, en ajoutant dans le champ de route leur propre identifiant, jusqu'à atteindre la destination cible. Le nœud destinataire répond alors par un paquet RREP, en diffusion inverse vers la source, contenant la route complète [28].

Maintenance des routes : durant laquelle, si une station route un message en utilisant une liaison devenue invalide, la station émet un message d'erreur de route RERR, vers les nœuds qui sont à l'origine du message. De cette façon, tous les récepteurs retirent le lien erroné de tous les chemins utilisés et effectuent de nouvelles découvertes de route pour chacun de ces chemins. [28]

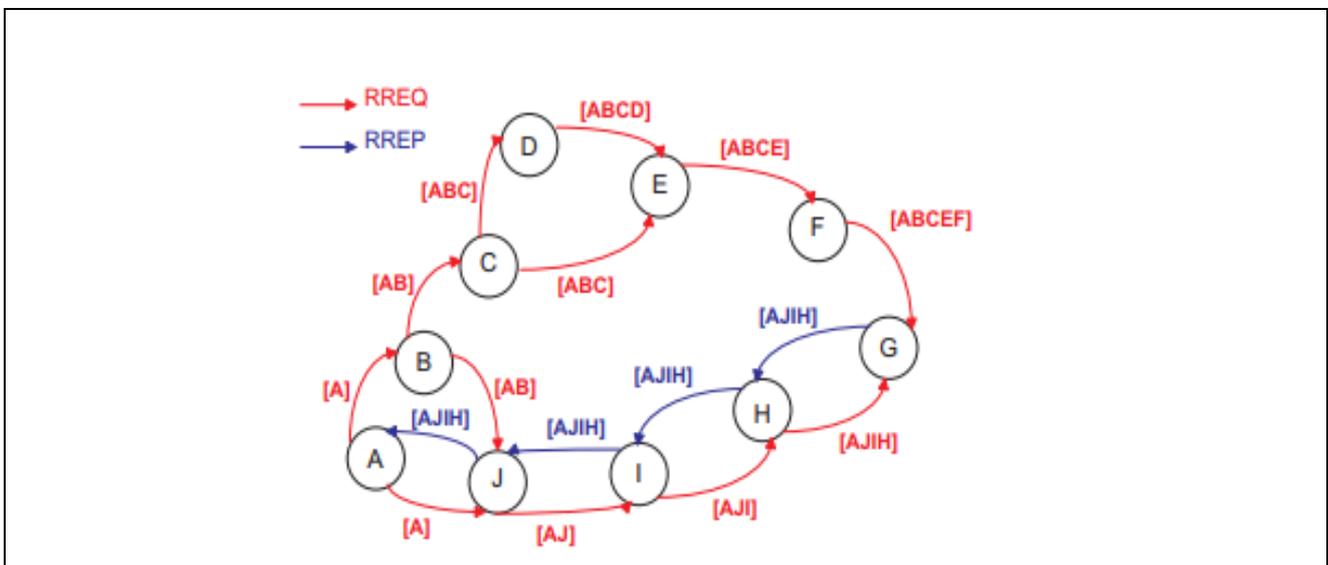


Figure II.15: découverte de route [29].

7.2.3 Le protocole ABR

Est un protocole réactif basé sur l'associativité entre les nœuds, cette dernière est une nouvelle métrique qui permet de choisir la meilleure route possible. L'associativité entre les nœuds est mesurée par la diffusion de paquets de type HELLO vers les voisins. À chaque fois qu'un nœud reçoit ce type de paquet d'un de ses voisins, le compteur d'associativité s'incrémenter dans la table de routage. Plus la valeur du compteur est élevée, plus le lien entre ces deux nœuds devrait être stable [30].

Le protocole ABR consiste en trois phases principales : la découverte des routes, la reconstruction des routes et la suppression des routes.

- **Phase de découverte des routes** : cette phase représente un cycle de diffusion de requête et d'attente de réponse. Le nœud source diffuse un paquet BQ (broadcast Query) afin de trouver

les nœuds qui mènent vers la destination. Un nœud fait commuter le BQ reçu, au plus une fois, Un nœud de transit (ou intermédiaire), rajoute son adresse et son intervalle d'associativité au paquet BQ avant de le transmettre aux voisins. Le nœud suivant dans le chemin, ne maintient que l'intervalle d'associativité qui lui est associé et celui du nœud précédent dans le chemin.

- **Phase de reconstruction des routes** : La phase de reconstruction des routes (RRC), consiste en une découverte partielle de routes, une suppression de routes invalides, une mise à jour de route valide et enfin une nouvelle sélection de routes. Différents scénarios de reconstruction existent selon le type d'interruption de la route : déplacement du nœud source et déplacement de nœud de destination et du nœud intermédiaire.
- **Phase de suppression de route** : Quand un chemin établi ne devient plus utilisé par la source, une diffusion de message de suppression de route RD (Route Delete) sera lancée en conséquence. Tous les nœuds qui appartient au chemin non utilisé, détruisent les entrées correspondantes de leurs tables de routage. La diffusion de message de suppression de route, doit être faite d'une manière globale pour supprimer toutes les routes qui pouvaient être instaurées suite à une phase de reconstruction de route [6].

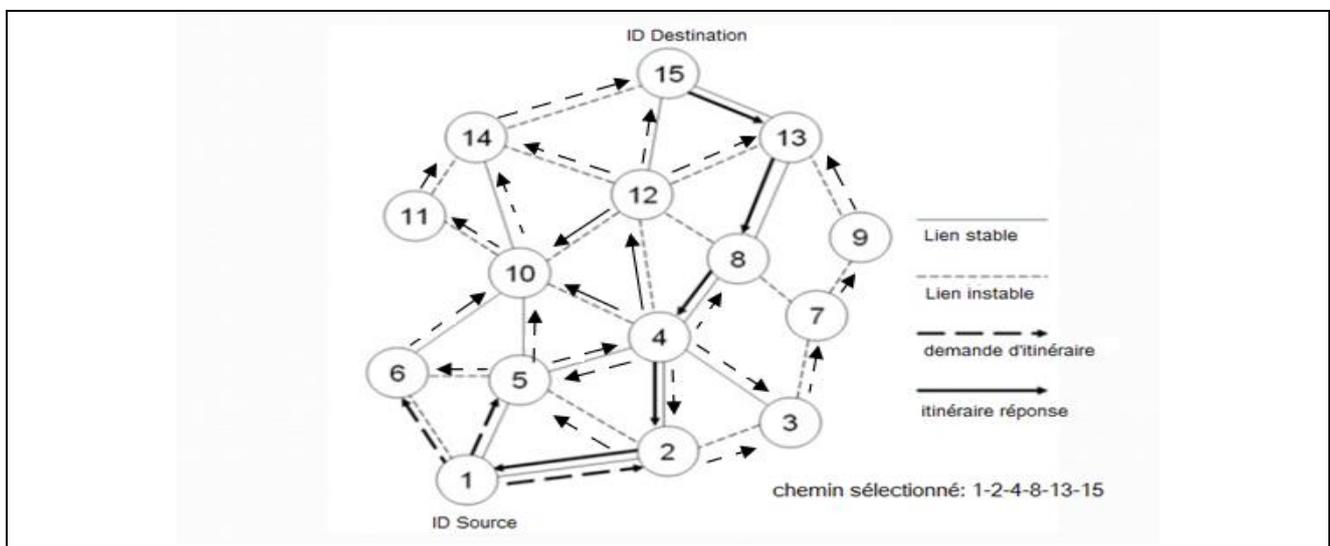


Figure II .16 : un exemple de protocole ABR.

7.2.4 Le protocole AOMDV

Est une extension multi-chemin du protocole AODV qui permet de déterminer plusieurs chemins à liens disjoints entre une paire de nœuds. Deux chemins sont à liens disjoints s'ils n'ont pas de liens en commun. Ce protocole cherche plusieurs chemins pendant une même phase de découverte

de routes. Mais uniquement la meilleure route en termes de nombre de saut est utilisée pour la transmission de données. Les autres routes calculées ne seront utilisées que lorsque la route principale est rompue. L'utilisation de chemins disjoints garantit que la rupture d'un lien sera répercutée sur un seul chemin. Néanmoins, le calcul et le maintien de plusieurs routes entre une source et une destination génère une occupation plus importante de la bande passante et exige plus de mémoire pour les informations de routage [27].

Principe de routage

AOMDV utilise le plus grand nombre d'informations disponibles dans "AODV". Ainsi, pour calculer des routes multiples, il ajoute un nombre supplémentaire de paquets de contrôles. AOMDV est basé sur deux mécanismes :

1. Mise à jour d'une route pour maintenir plusieurs routes sans boucle de routage.
2. Mécanisme distribué entre les différents nœuds du réseau afin de calculer des routes disjointes [32].

Pour voir comment les boucles peuvent se produire, considérons l'exemple suivant. La source S diffuse un paquet "RREQ" qui sera intercepté par le nœud intermédiaire A. Ce dernier le rediffuse à son voisins B. Le nœud B envoie ce paquet au nœud C qui le retransmet à son tour au nœud A. Si A accepte cette copie de "RREQ", alors il formera une boucle [33].

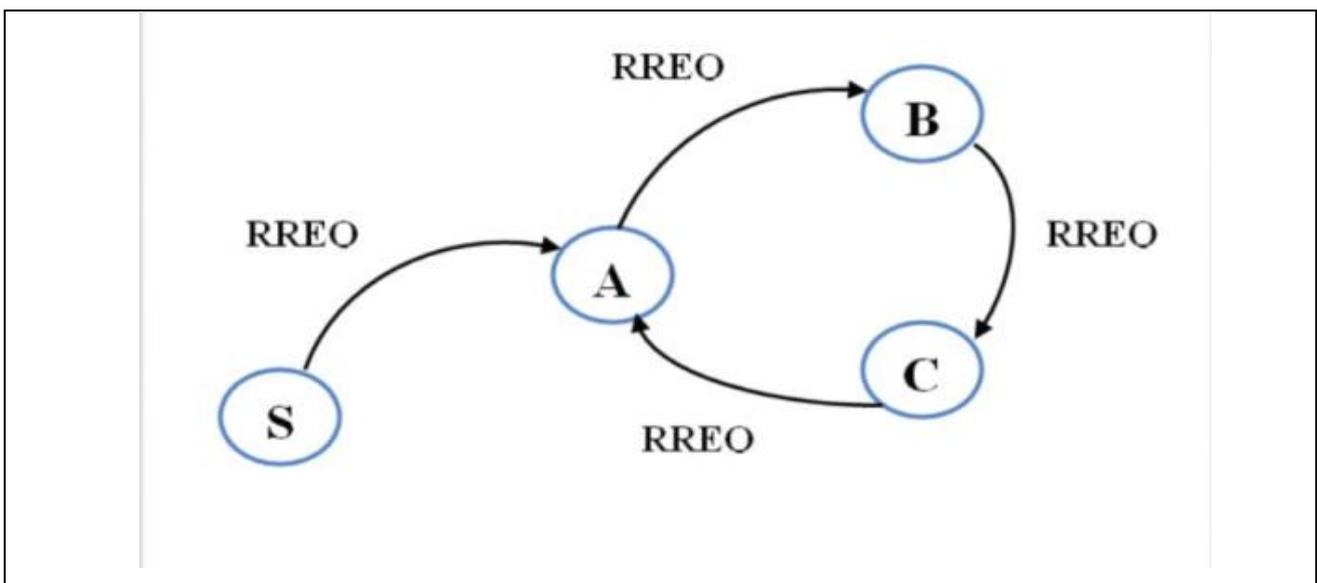


Figure II .17 : Exemple de formation d'une boucle de routage [18].

"AOMDV" permet d'accepter seulement les routes alternatives ayant un nombre de saut inférieur ou égal à l'Advertised_hopcount. Cette condition est nécessaire pour garantir des routes sans boucles de routage [33].

AODV	AOMDV
Destination	Destination
Sequence_number	Sequence_number
Hopcount	Advertised_hopcount
Nexthop	Route list {(nexthop1, hopcount2) ;(nexthop2hopcount2)}
Expiration timeout	Expiration_timeout

Table II.1 : Structure des entrées des tables de routage d'AODV et AOMDV [18].

7.3 Routage Hybrides :

Entre ces deux familles précédentes, une nouvelle approche commence à émerger : il s'agit des protocoles dit « hybrides » pour bénéficier de leurs avantages. Ils utilisent un protocole proactif, pour apprendre le proche voisinage (voisinage à deux sauts ou trois sauts), dans le but de réduire le délai et un protocole réactif au-delà de cette zone prédéfinie dans le but de réduire la charge des paquets de contrôle. Il est de grande importance de noter que cette technique est bien adaptée aux réseaux à grande échelle, puisqu'elle cumule les qualités des deux approches. Cependant, elle englobe les points faibles des deux types de protocoles à savoir la surcharge des messages de contrôle envoyés périodiquement par l'approche proactive ainsi que le coût d'établissement d'une route par l'approche réactive [25], [9].

7.3.1 Le protocole ZRP (Zone Routing Protocole)

Est un protocole de routage hybride qui combine les avantages d'un protocole réactif avec les avantages d'un protocole proactif. Une taille de zone en nombre de sauts est définie, par exemple, comme illustré sur la figure II.19. Les nœuds présents dans la zone A à deux sauts, dont le chef est le nœud S, sont gérés suivant un protocole proactif, Les paquets de contrôle possèdent une durée de vie en nombre de sauts. Lorsqu'un nœud reçoit un paquet de contrôle, il actualise sa table de routage et il le retransmet en décrémentant sa durée de vie. Lorsque la durée de vie du paquet de contrôle est nulle, la bordure de zone est atteinte et le paquet n'est plus retransmis. Les nœuds hors de la zone A sont atteints grâce à un protocole réactif [29].

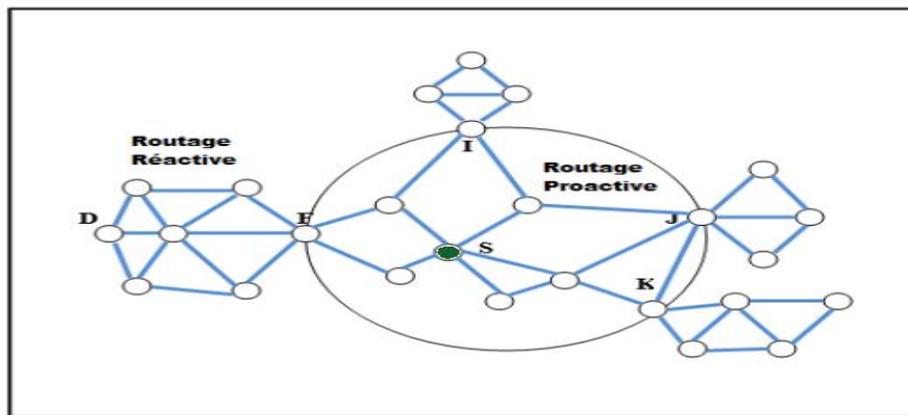


Figure II.18 : Exemple de zone dans le protocole ZRP [29].

7.3.2 Le protocole CBRP :

Le protocole de routage CBRP (Cluster Based Routing Protocol) est un protocole Hybride. Il utilise deux niveaux hiérarchiques pour effectuer le routage. Les nœuds dans CBRP sont rassemblés en groupes appelés « Clusters », avec un chef au centre de chaque groupe appelé « Cluster Head ». Les clusters sont reliés entre eux par des nœuds passerelles qui se trouvent à l'extrémité des clusters. CBRP utilise un protocole proactif pour maintenir les membres du cluster, et un protocole réactif pour découvrir les nœuds en dehors du cluster.

Le diamètre d'un cluster dans CBRP est de deux sauts, un exemple d'assemblage en cluster est illustré dans la figure II.19.

Le principe de formation des clusters dans CBRP est le suivant :

1. Les nœuds s'échangent des messages « Hello » pour connaître leurs voisinages.
2. Le nœud ayant le plus petit identifiant est élu chef de cluster.
3. Un nœud qui n'a pas de chef de cluster comme voisin devient chef de cluster.
4. Le chef de cluster prend tous ses voisins comme membres de son cluster [9].

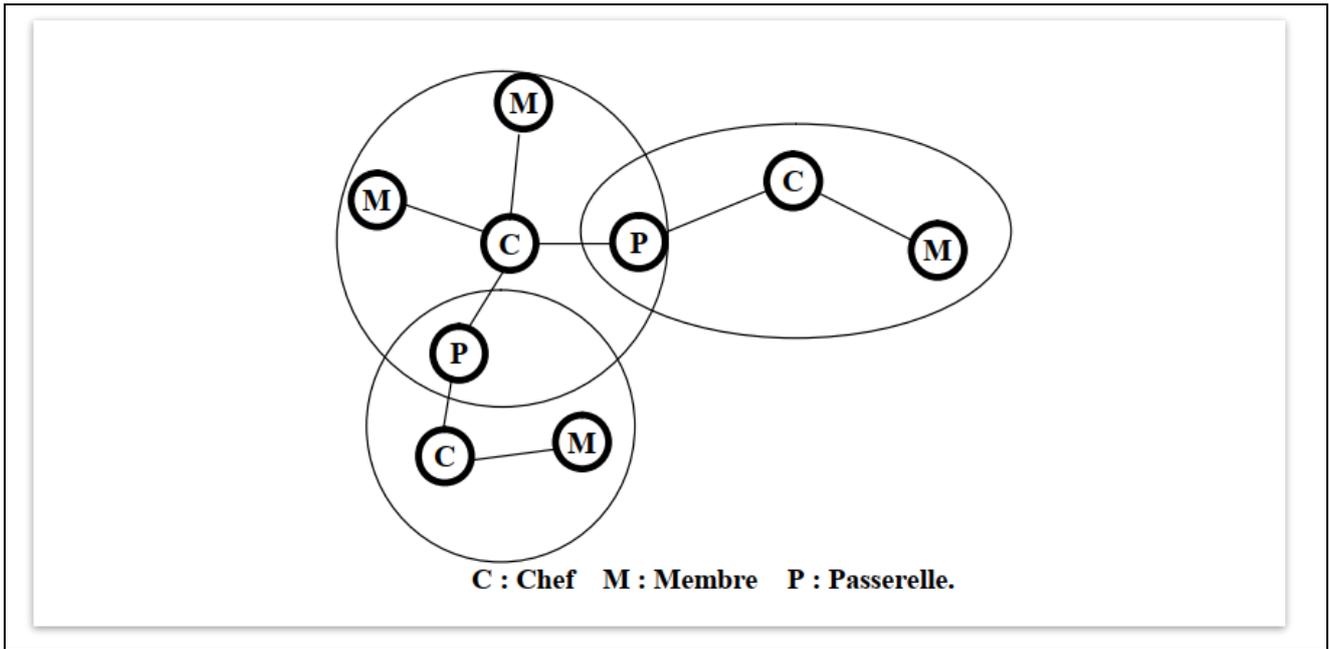


Figure II.19: Formation des clusters dans CBRP [9].

7.3.3 Le protocole ZHLS (Zone Based Routing Protocol):

Est un protocole de routage ad hoc hybride qui se base sur la décomposition du réseau en zones géographiques fixes et chaque nœud peut se localiser dans une zone grâce à ses coordonnées GPS (Global Positioning System). Ainsi, la topologie du réseau est divisée en deux niveaux :

Niveau intra-zone présentant les liens qui existent entre les nœuds appartenant à la même zone et les liens éventuels vers des nœuds d'autres zones .Ceci est matérialisé par une table de routage intra-zone au niveau de chaque nœud.

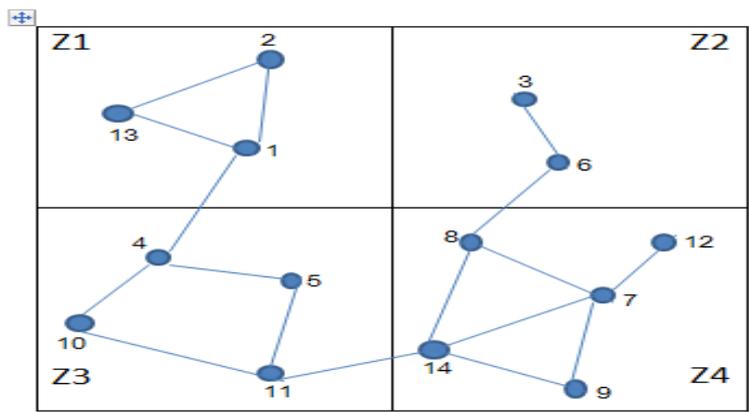


Figure II. 20 : Topologie niveau intra_zone [36].

– Niveau inter-zone présentant le schéma de connexion entre les zones et qui est matérialisé par une table de routage inter-zone au niveau de chaque nœud, établissant ainsi la carte des zones.

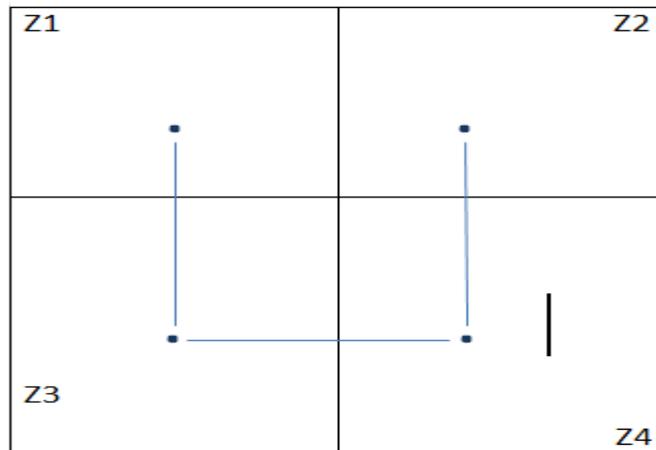


Figure II. 21 : Topologie niveau inter_zone [36].

Le protocole ZHLS maintient à jour les tables de routage intra-zone et inter-zone et utilise une technique réactive pour retrouver la zone à laquelle appartient un nœud destinataire.

En effet, pour atteindre une destination, un nœud commence par consulter sa table de routage intra-zone. S’il ne trouve pas la destination, il initialise une demande de localisation qui permet de retrouver la zone à laquelle appartient le nœud recherché. Ainsi, le chemin menant à la destination est connu puisqu’on a la zone à laquelle il appartient et le transfert des données peut débuter [36].

7.4 Protocoles de routage géographique

Les protocoles de routage géographique se basent sur la localisation des nœuds pour assurer le routage des paquets [22]. En effet, Ils utilisent les positions des nœuds pour éviter de faire la diffusion pure, réduire davantage le nombre de nœuds participants à la découverte de route et par la même occasion diminuer le taux de congestion du réseau.

Dans un protocole de routage géographique, un nœud qui veut obtenir une route vers un autre nœud, doit connaître sa position, celle de ses voisins immédiats et celle du nœud destinataire. Ces informations vont permettre de sélectionner qui, parmi les nœuds voisins, seront choisis pour acheminer la requête de route vers la destination [24].

Ce type de protocole n’ont pas besoin de tables de routage, ce qui élimine les paquets de contrôle utilisés pour maintenir ces tables d’une part, et permet d’optimiser la bande passante et l’énergie des nœuds d’une autre part [22].

7.4.1 Le protocole LAR (Location Aided Routing) [24] :

LAR se propose comme une amélioration des protocoles de routage qui utilisent la diffusion pour la découverte de route. Cette amélioration est obtenue en utilisant les positions des nœuds. Le nœud source calcule la zone dans laquelle la destination est prévue se trouver en se basant sur sa dernière position, soit un cercle centré en D, telle que D est la dernière position de la destination connue par la source. La zone de diffusion est déterminée par le rectangle qui comprend le nœud source et le cercle centré en D.

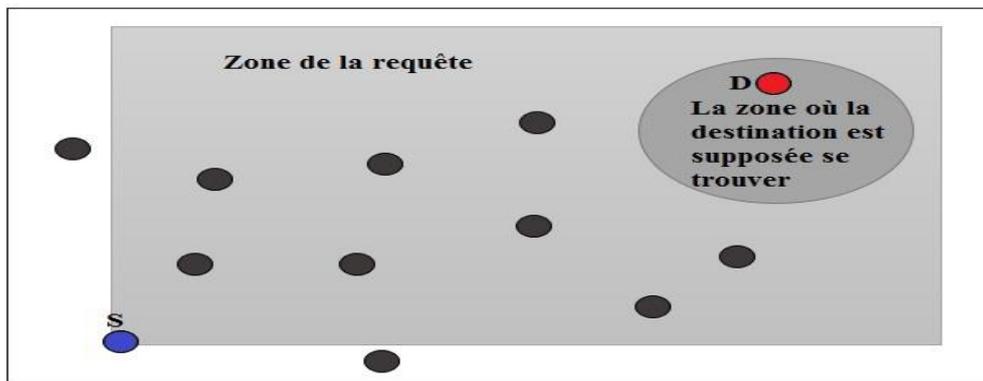


Figure II .22 : la zone de diffusion dans LAR [24].

La source envoie la requête de route uniquement vers les nœuds voisins situés dans sa zone de diffusion et qui sont plus proches de la destination que lui. Chaque nœud intermédiaire fait la même chose jusqu'à ce que la requête arrive à destination.

L'absence d'infrastructure fixe ou de station fixe pour récupérer les positions des nœuds dans les réseaux ad hoc, pose le problème de mise à jour des positions. En effet, en utilisant le système GPS (ou une autre méthode) le nœud ne peut connaître que sa propre position. Le problème de trouver la position du nœud destination se révèle être aussi complexe que le problème de routage lui-même. Plusieurs méthodes ont été proposées, ces méthodes vont de la diffusion simple de position à l'élection de serveurs de position selon leur degré de voisinage (nombre de voisins) et leur position.

Les méthodes de découverte de route utilisées par les protocoles de routage géographiques peuvent, dans certain cas, échouer à trouver un chemin vers la destination. Une procédure de recouvrement qui assure la livraison du paquet de découverte de route est adoptée pour remédier à ce problème. Dans le cas de LAR, la diffusion classique est utilisée comme procédure de

recouvrement. Si un nœud ne reçoit pas de réponse de route après un temps déterminé, il diffuse une requête de route qui se propagera dans tout le réseau.

7.4.2 Le protocole GPSR (Greedy Perimeter Stateless Routing):

GPSR permet de marquer les paquets avec la position géographique de leurs destinations et par la suite chaque nœud émetteur peut faire un choix optimal de son prochain saut en se basant sur la méthode transmission gloutonne (Greedy Forwarding) [34]. Cette dernière construit un chemin parcourant les nœuds de la source à la destination où chaque nœud qui reçoit un paquet l'achemine vers le nœud intermédiaire le plus proche de la destination dans sa zone de couverture [35].

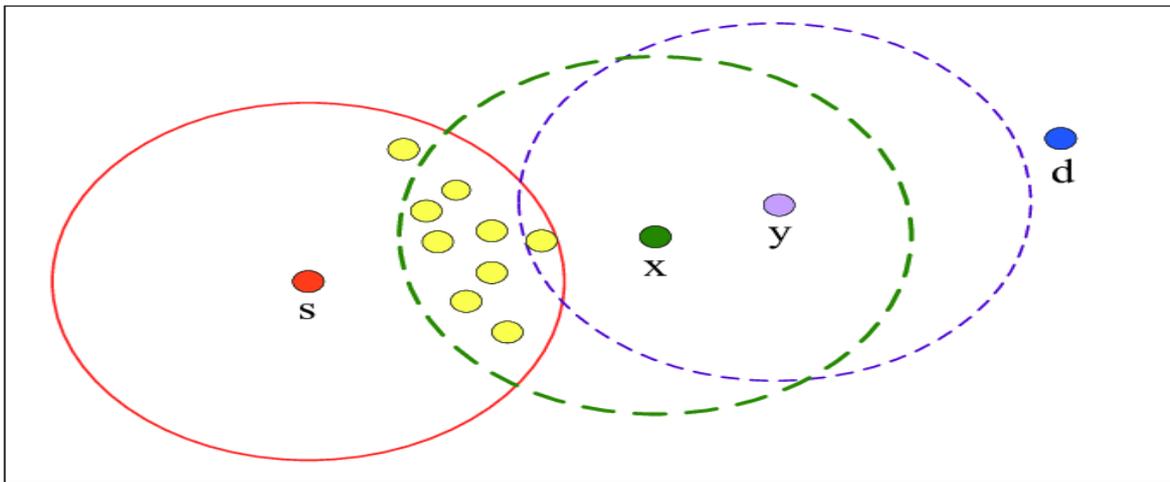


Figure II .23 : Méthode transmission gloutonne [40].

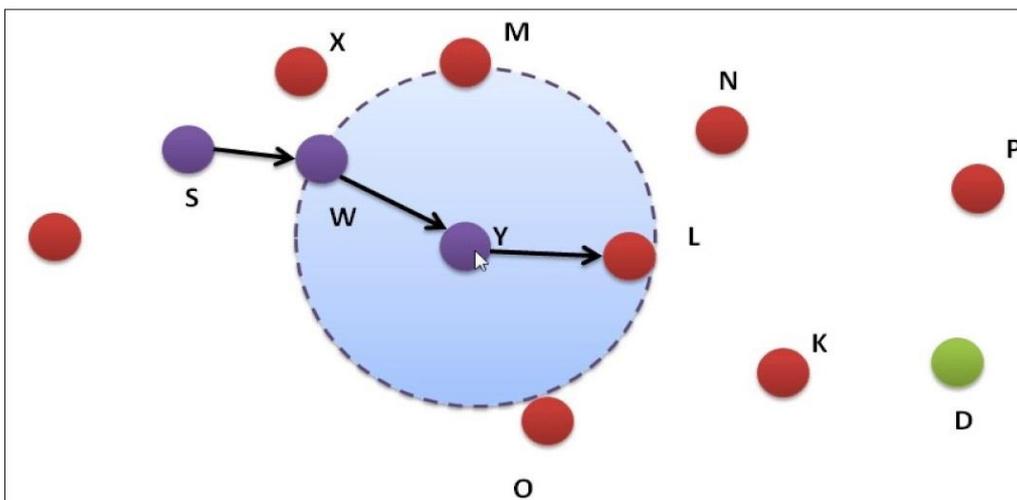


Figure II .24 : Noeud "W" est le voisin de " S" le plus proche de la destination D.

II.8 les avantages et les Inconvénients des classes de routage ad-hoc :

Les tableaux ci-dessous récapitulent les caractéristiques, les types, les avantages et les inconvénients des protocoles de routage ad-hoc exposés dans ce chapitre :

Classes	Caractéristiques	Avantages	Inconvénients
Proactifs	-Calculer les routes à l'avance.	- les routes sont disponibles immédiatement. - le gain de temps lors d'une demande de route.	-Utiliser beaucoup de paquets de contrôles.
Réactifs	-Calculer les routes a la demande.	-Pas de trafic de contrôle continu pour les routes non utilisées	-Délais importants avant l'établissement de chaque route
Hybride	-Combinaison des deux approches précédentes.	-Bénéficier des avantages des deux approches précédentes	-Cumuler les inconvénients des deux approches précédentes.

Table II 2 : Les classes des protocoles de routage ad- hoc [9].

II .9 Comparaison entre les approches de routage ad-hoc

Approches de routage	Approche proactive	Approche réactive	Approche hybride
Caractéristiques			
chemins.	Toujours disponibles ¹	À la demande.	Dépend de la localisation de la destination.
Surcharge de routage.	Elevé, mais il existe des tentatives de réduction par exemple : OLSR.	Inférieure qu'en proactive, et mieux en utilisant GPS (par exemple LAR).	Généralement plus bas qu'en proactive et en réactive.
Mise à jour périodique.	Oui.	Non.	Généralement utilisées à l'intérieur des zones.
Gestion de la mobilité des nœuds.	Généralement des MAJ à des intervalles fixes.	Reconstruction de chemins initiée par la source généralement.	En inter zone, fréquence de reconstruction de chemins est réduite. la topologie intra-zones est relativement

			stable dans ZHLS.
Espace de stockage requis pour les tables de routage.	Elevé	Dépend du nombre de chemins actifs.	Dépend de la taille des zones.
Délais	Les chemins sont prédéfinis.	Plus élevé qu'en proactive.	Pour les destinations locales ² il est bas, sinon il est comme en réactive.
Niveau de scalabilité ³ .	Jusqu'à 100 nœuds, mais OLSR permet plus.	En cas de routage source, jusqu'à quelques centaines de nœuds. Pour le routage saut-par saut, un plus haut niveau de scalabilité peut être atteint	Conçue pour des réseaux disposant de plus de 1000 nœuds.

¹Si les nœuds sont joignables.

²Les destinations locales sont ceux qui résident dans la même zone que le nœud source.

³La capacité de réaliser un routage efficace jusqu'à un certain nombre de nœuds.

Table II 3: Comparaison entre les approches de routage ad-hoc [11].

II .10 Comparaison entre les protocoles de routage ad-hoc

Protocole	Type	Avantages	Inconvénients
DSDV	proactif	Simple, absence de problème de boucle de routage.	Mise à jour élevée; Convergence lente; Tendance à créer des boucles de routage dans les réseaux à grande taille.
OLSR	proactif	Diffusion optimisée des messages de contrôle par rapport aux autres protocoles basés sur l'état des liens.	Mise à jour importante.
TBRPF	proactif	Peu de message requis pour une mise à jour.	La charge du routage augmente avec la mobilité des nœuds et la taille du réseau
AODV	réactif	Adapté aux topologies très dynamiques, Possibilité de routage Multicast.	Ne supporte pas des routes multiples, délai important pour la découverte de route.
DSR	réactif	Routes multiples, Les nœuds intermédiaires ne stockent pas les informations sur les routes.	Grand délai pour établir une route.
ZRP	hybride	La charge de communication réduite, Découverte rapide des routes par rapport aux protocoles réactifs.	Problème de chevauchement des zones.

Table II 4: Comparaison entre les protocoles de routage ad-hoc [15,22].

II.12 Conclusion

Dans ce chapitre, nous avons donné un aperçu général sur le routage ad-hoc. En effet, nous avons décrit son concept, ses problèmes, ses contraintes et ses approches. Par la suite, nous avons détaillé les algorithmes de routage correspondants, tout en présentant leurs caractéristiques, leurs fonctionnements, leurs avantages et inconvénients. A la fin, nous avons résumé les points précédents dans des tableaux comparatifs.

Chapitre III : Partie Simulation

III.1. Introduction

Face à la complexité des réseaux de communication, la simulation reste l'outil le plus pratique pour évaluer les performances de réseaux et étudier le comportement des protocoles.

La simulation est une technique informatique permettant de reconstituer le déroulement d'un phénomène en le modélisant par ordinateur et en introduisant certains paramètres dont les valeurs sont saisies par l'utilisateur.

Dans le cadre de notre projet, nous avons simulés deux protocoles de routage à savoir : AODV et DSR, en utilisant le simulateur SINALGO (Simulator for Network Algorithms), dans le but de bien comprendre leur aspect théorique et de faire une éventuelle comparaison entre eux.

III.2. Outils de simulation

2.1 Simulateur SINALGO

Sinalgo est un simulateur permettant de tester et valider des algorithmes de réseau. Contrairement à la plupart des autres simulateurs de réseau, qui passent plus de temps à simuler les différentes couches de la pile réseau, Sinalgo en fait l'abstraction et se concentre uniquement sur la vérification des algorithmes de réseau.

Grâce au prototypage rapide de l'algorithme en JAVA, Sinalgo se propose comme premier environnement de test, avant de déployer l'algorithme sur le matériel. Le prototypage en JAVA au lieu du langage spécifique au matériel est non seulement beaucoup plus rapide et plus simple, mais simplifie également le débogage. En outre, Sinalgo peut être utilisé comme une application autonome pour obtenir des résultats de simulation d'algorithmes réseautiques.

2.2 Caractéristiques clés de Sinalgo

Quelques-unes des principales caractéristiques de sinalgo :

- Prototypage rapide de vos algorithmes réseaux en JAVA.
- Extensibilité directe pour couvrir presque tous les scénarios de simulation.
- De nombreux plug-ins intégrés, mais toujours réglables
- Haute performance - exécutez des simulations avec des milliers de nœuds dans un délai acceptable.
- Simulation asynchrone et synchrone.
- Visualisation personnalisable du graphique du réseau.

- Indépendant de la plateforme - le projet est écrit en Java.
- Sinalgo est gratuit, publié sous licence BSD.

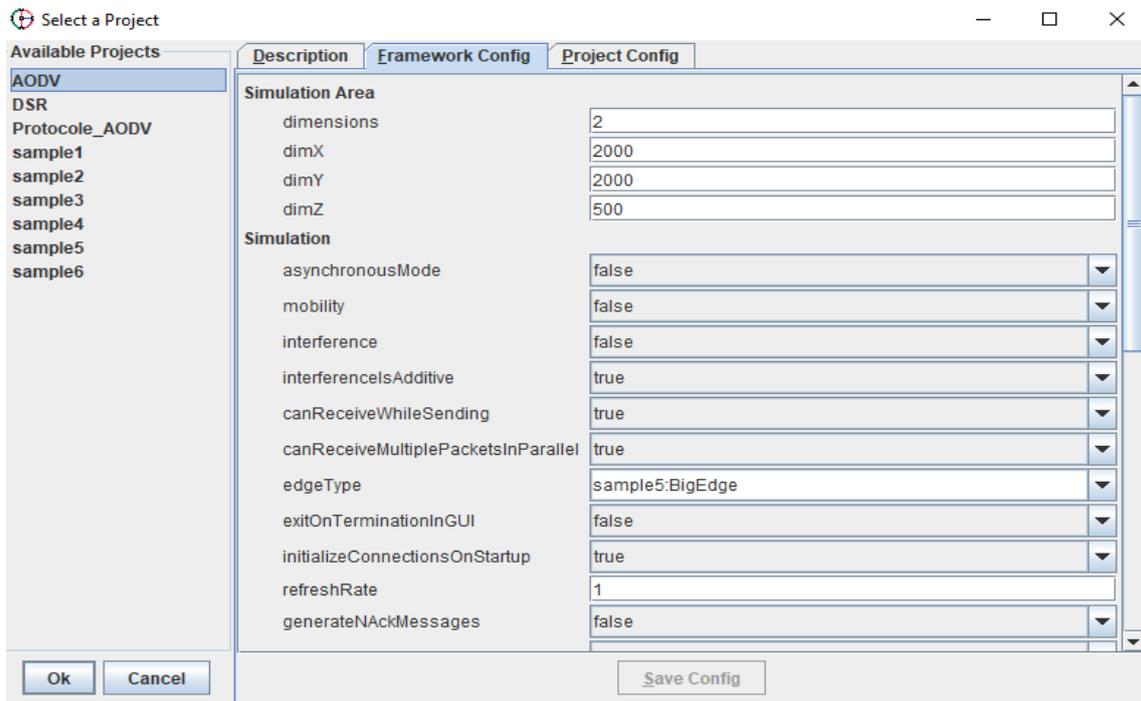


Figure III.1 : Exemple d'interface Sinalgo.

2.3 Installation :

1. Pre-requis

Sinalgo nécessite que **Java 5.0** ou une version supérieure soit installée sur votre machine. Sinalgo fonctionne aussi avec des environnements de développement de type Eclipse.

2. Installation

Télécharger le fichier `sinalgo-0.75.3-regularRelease.zip` [41] et décompressez-le dans un sous-répertoire `sinalgo` de notre répertoire de travail. Ce répertoire contient notamment les sources dans `src`. On a deux options à choisir : soit travailler en ligne de commande, soit utiliser un environnement de développement comme Eclipse.

Depuis le site suivant : <https://sourceforge.net/projects/sinalgo/>

3. En ligne de commande

Commencez par recompiler tout le logiciel en tapant `ant`. La compilation devrait se terminer par le message `BUILD SUCCESSFUL`. Puis lancer le script `sinalgo` ou `sinalgo.bat` selon le système d'exploitation.

4. Avec Eclipse

1. Lancez Eclipse.



Figure III.2 : Lancement de l'environnement Eclipse.

2. Créez un nouveau projet java (File →New→Java Project). Nommez-le sinalgo. Cochez la case « créer un projet à partir d'une source existant » et sélectionnez le répertoire sinalgo créé précédemment. Cliquez sur « finish ».

3.3. Organisation

Le cœur du logiciel se trouve dans src/sinalgo. Sinalgo propose ensuite de développer des protocoles dans le répertoire src/Project.

Le répertoire noedes contient le code du protocole. Ce code est subdivisé en plusieurs fichiers répartis dans plusieurs répertoires :

- A. Edges : Contient le code relatif aux liens de communication.
- B. Messages : Contient la description de chaque type de message utilisé dans la simulation.
- C. NodeImplementations : Implémente le comportement des nœuds.
- D. timers : Contient le code des timers utilisés dans la simulation.

III.3. Simulation :

Après la création du projet AODV et DSR et la programmation des code correspondant en java, on peut lancer l'exécution, il suffit de faire un clic droit sur src dans le navigateur de package et de sélectionner « Run → as → Java Application → Run → sinalgo → OK » pour démarrer l'application.

3.1) Exécution du protocole AODV

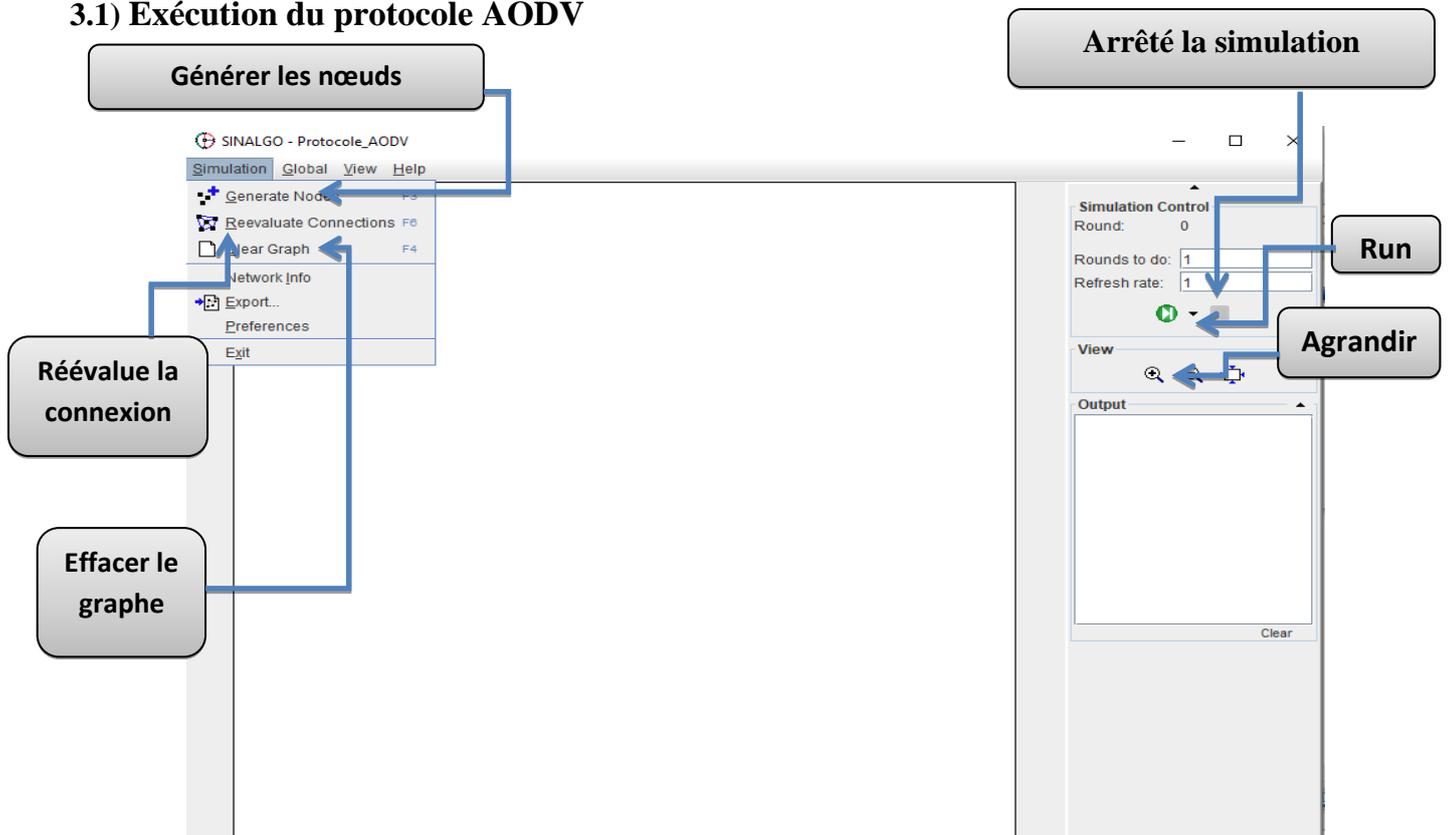


Figure III.3 :l'interface principale de simulation de protocole AODV.

- Créer les nœuds à l'aide du bouton générer les nœuds (Add Nodes), et cliquer sur OK.

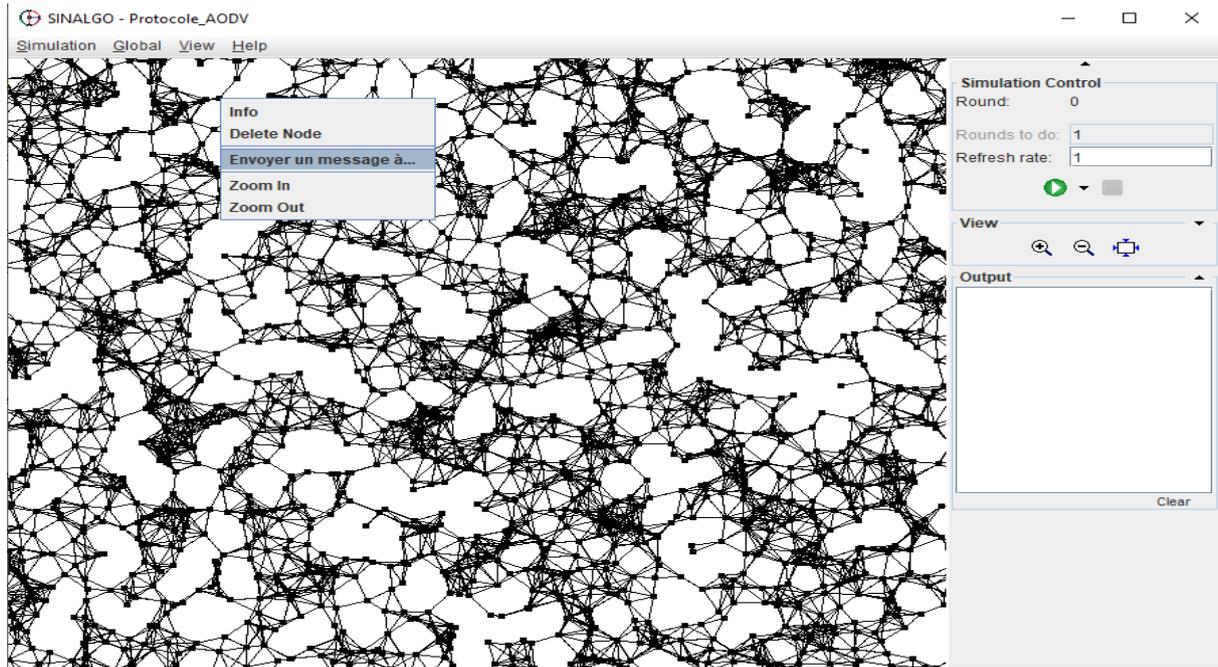


Figure III.4 : Sélection d'un nœud source pour envoyer un message.

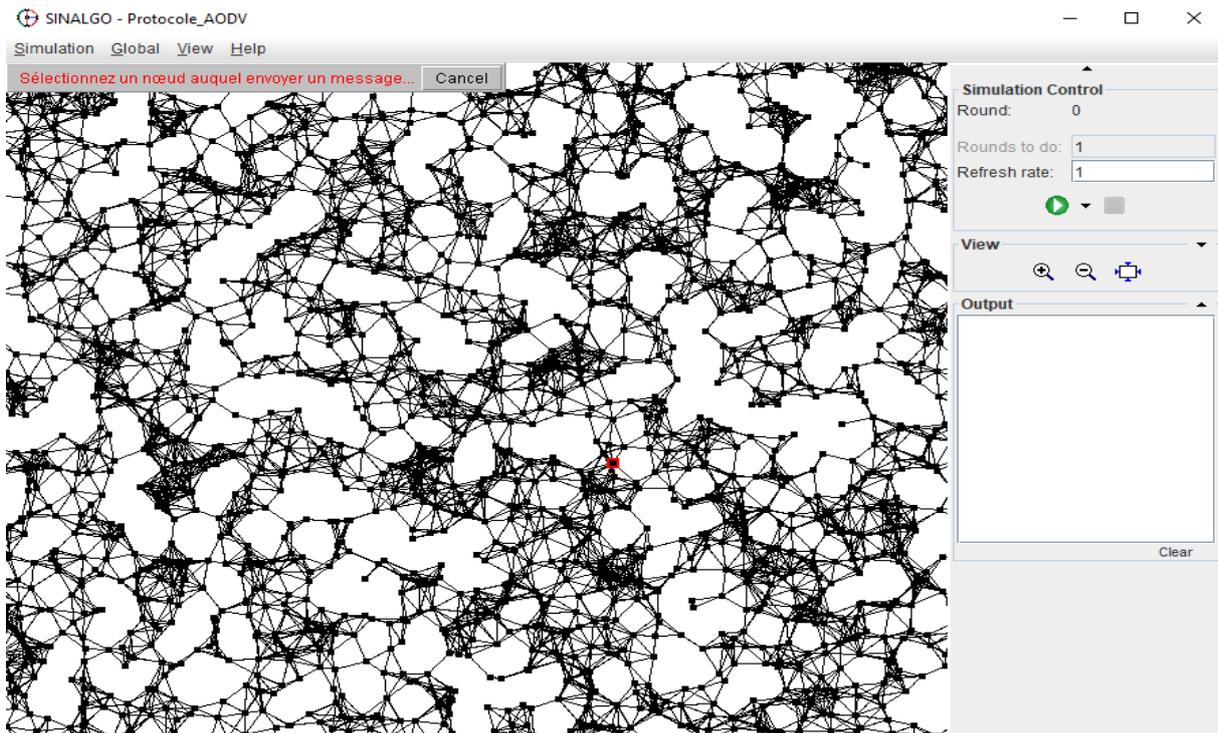


Figure III.5 : Sélection du nœud destinataire.

- la source diffuse le message RREQ vers tous les nœuds en mode Broadcast, pour chercher le chemin qui mène vers la destination.

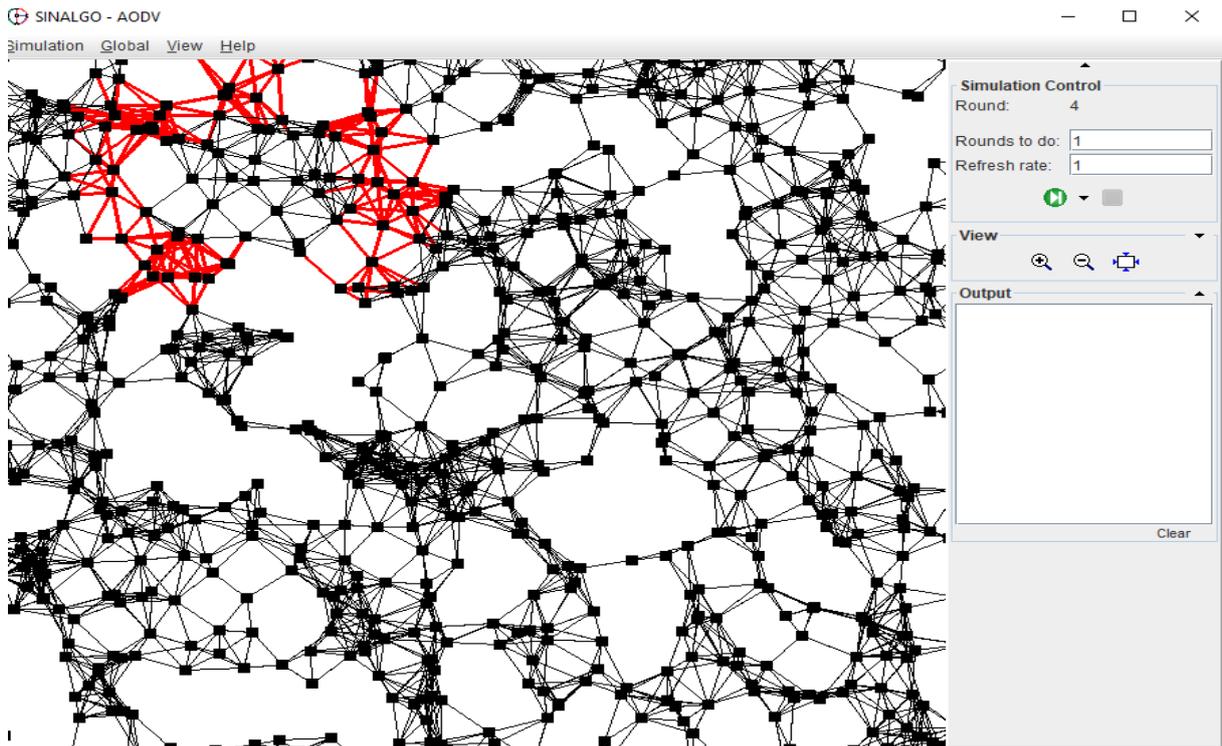


Figure III.6 : Message RREQ distribué en broadcast.

- Lorsque la destination, colorée en bleu, reçoit la requête RREQ, elle répond par un message RREP envoyé en mode unicast vers la source.

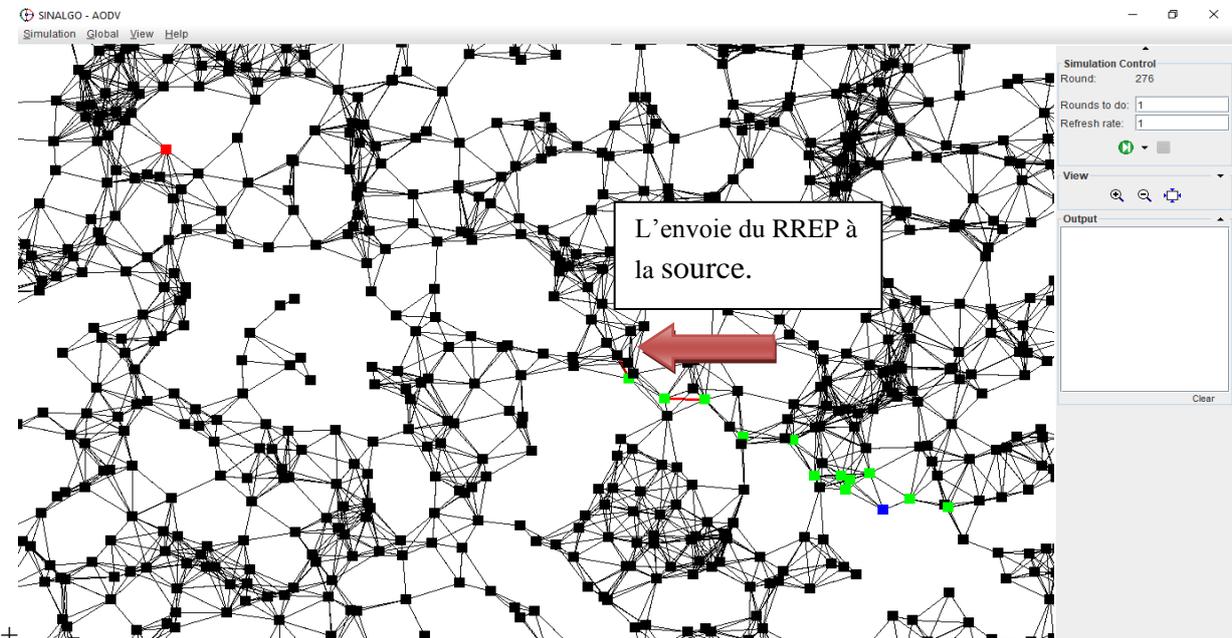


Figure III.7 : L'envoi du message RREP à la source.

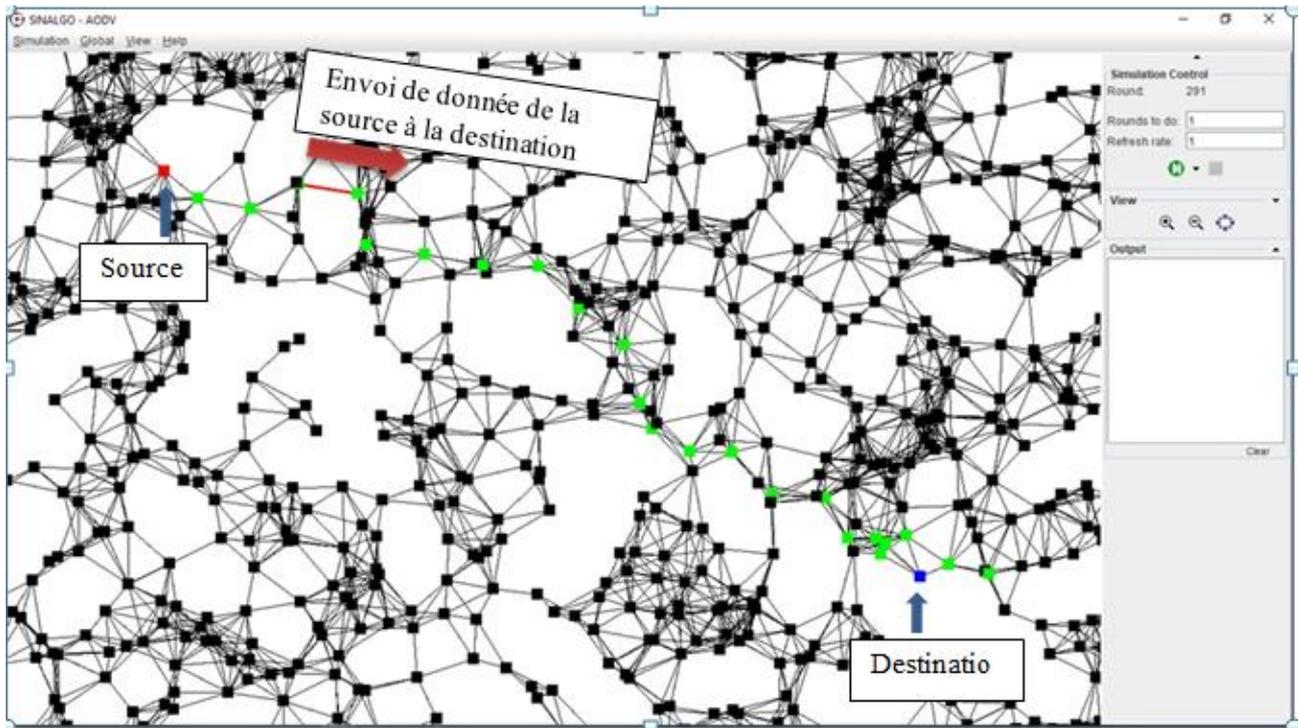


Figure III.8 : la source envoie les données à la destination.

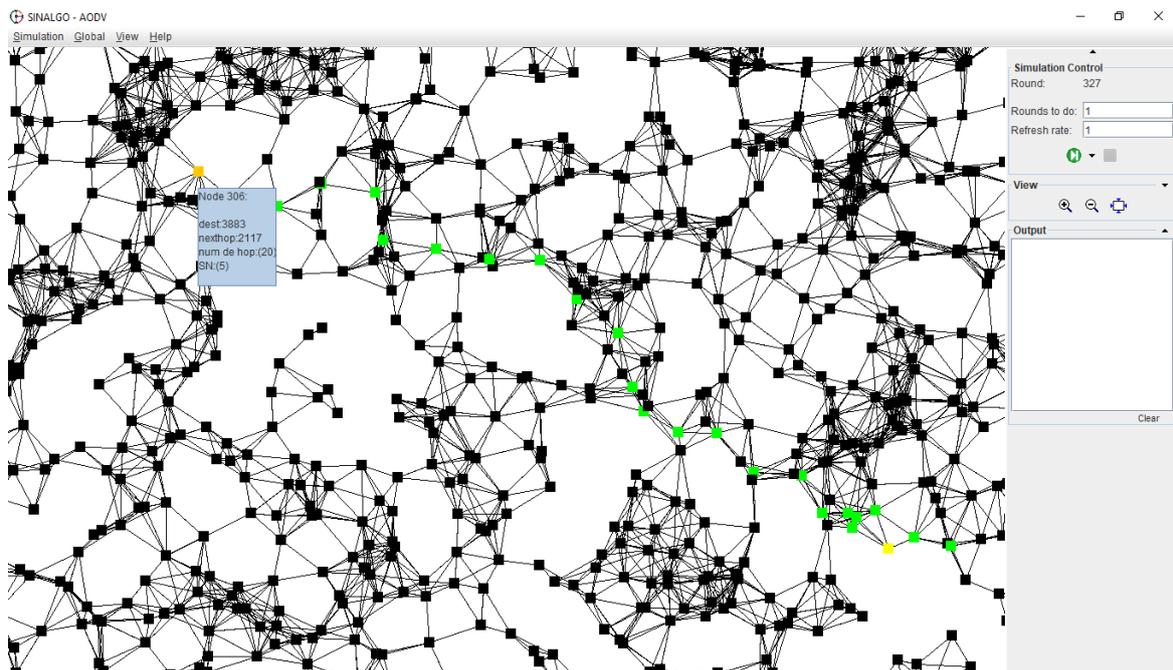


Figure III.9 : Table de routage du nœud source.

- Lorsqu'une nouvelle source veut échanger des données avec la même destination, elle lance la recherche de chemin. Chaque nœud intermédiaire vérifie sa table de routage si elle contient une entrée vers la destination demandée. Une fois trouvée, ce nœud intermédiaire répond directement à la nouvelle source, par un message RREP transmis en unicast. Cela permet d'accélérer considérablement le processus de calcul de chemin.

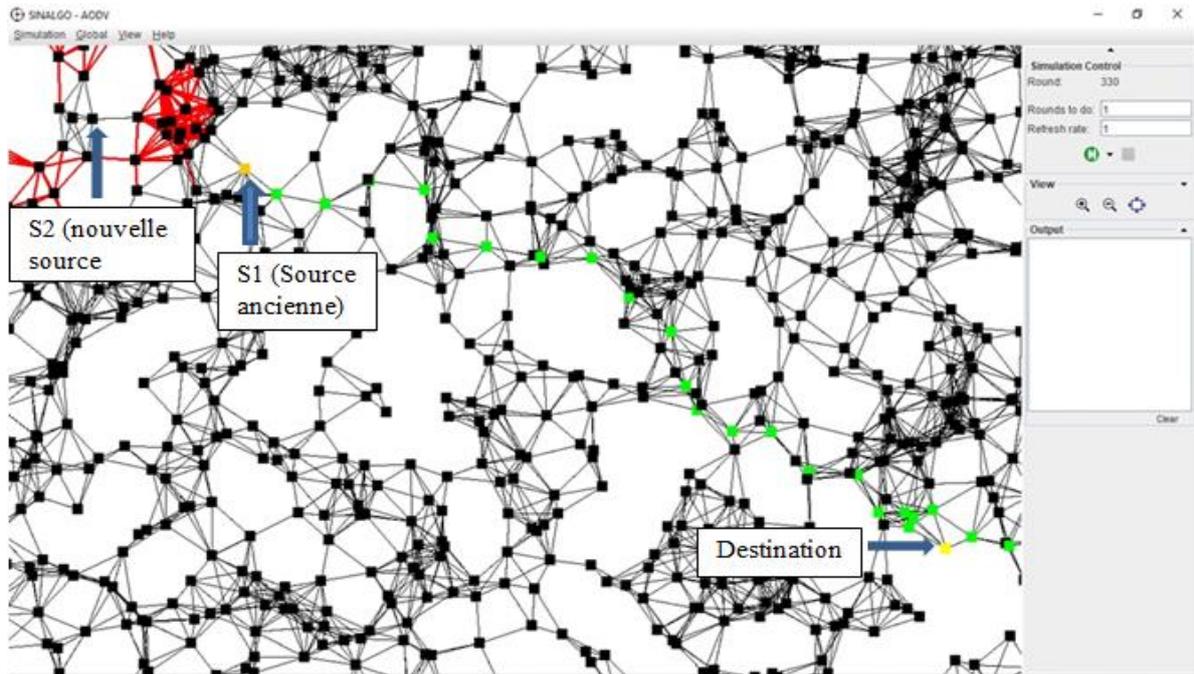


Figure III.10 : Message RREQ distribué en broadcast.

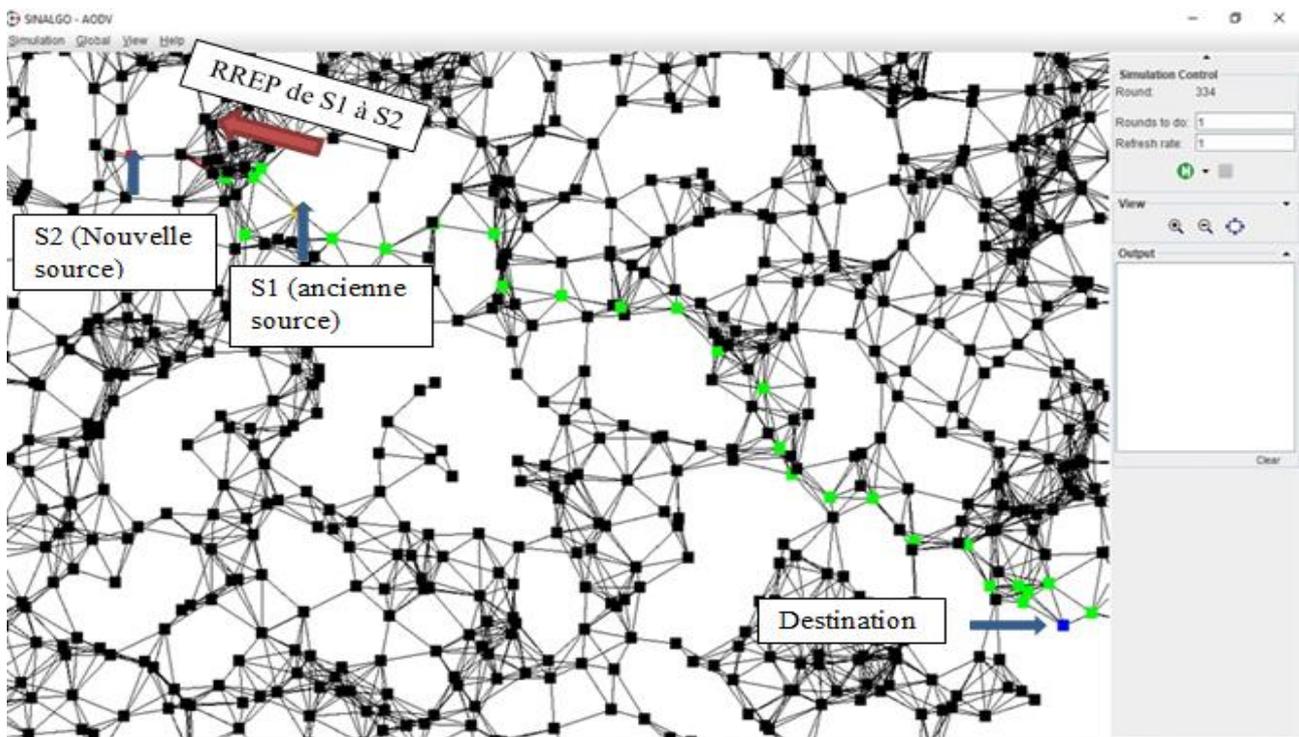


Figure III.11 : L'envoi du message RREP par un nœud intermédiaire.

7.2) Exécution du protocole DSR

Les premières étapes exécutées par le protocole AODV (de la figure III.3 jusqu'à la figure III.8) sont aussi déclenchés par le protocole DSR, la seule différence réside dans les prochaines étapes :

Lorsqu’une nouvelle source souhaite envoyer des données à la même destination, elle relance le même processus, et attend de recevoir le message RREP envoyé uniquement par la destination car les nœuds intermédiaire ne possèdent pas l’ancienne trace qui mène vers elle.

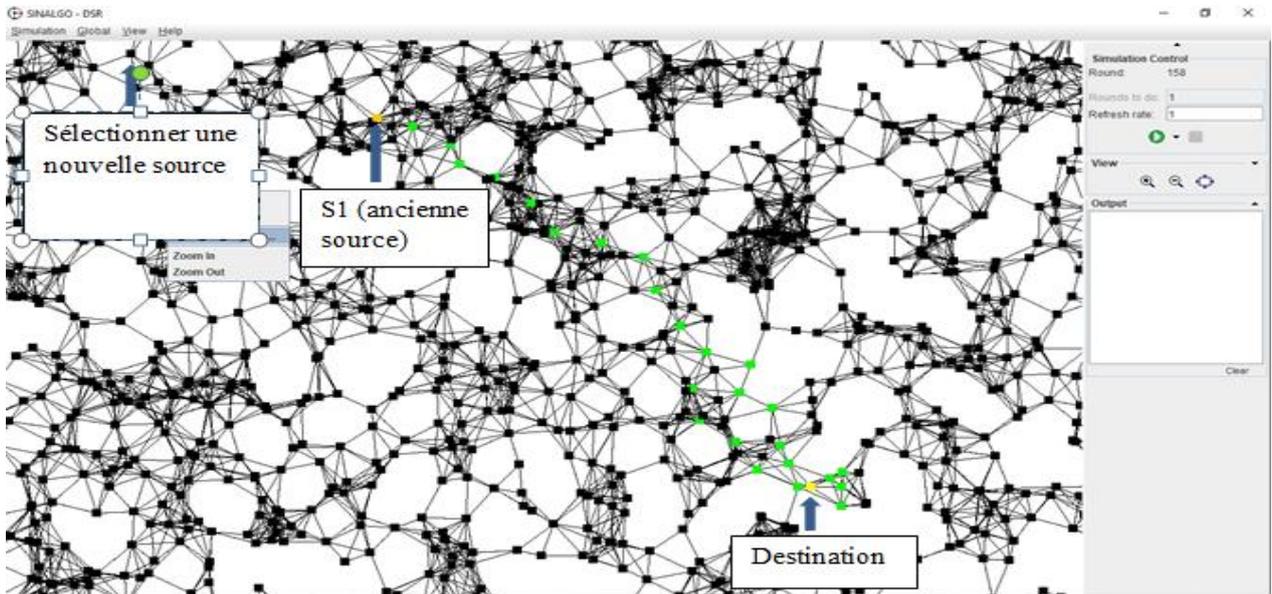


Figure III.12 : la sélection d’une nouvelle source pour envoyer un message.

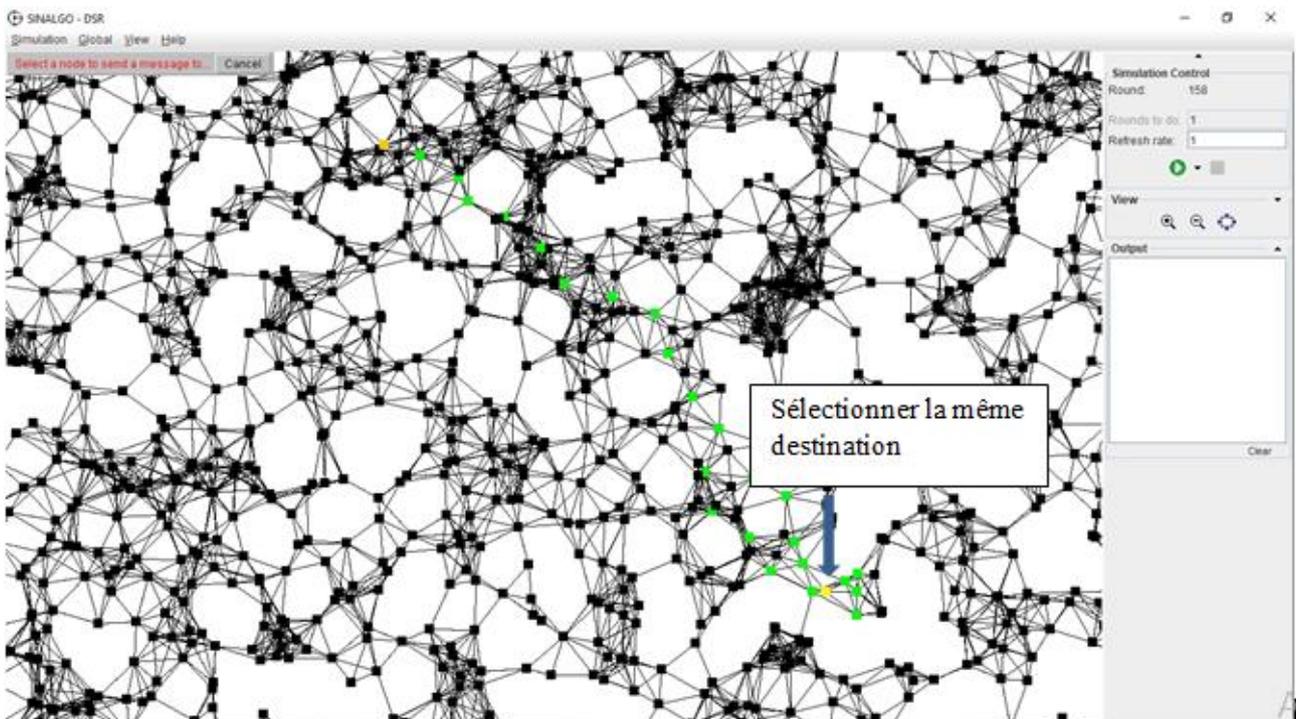


Figure III.13 : la sélection d’une même destination.

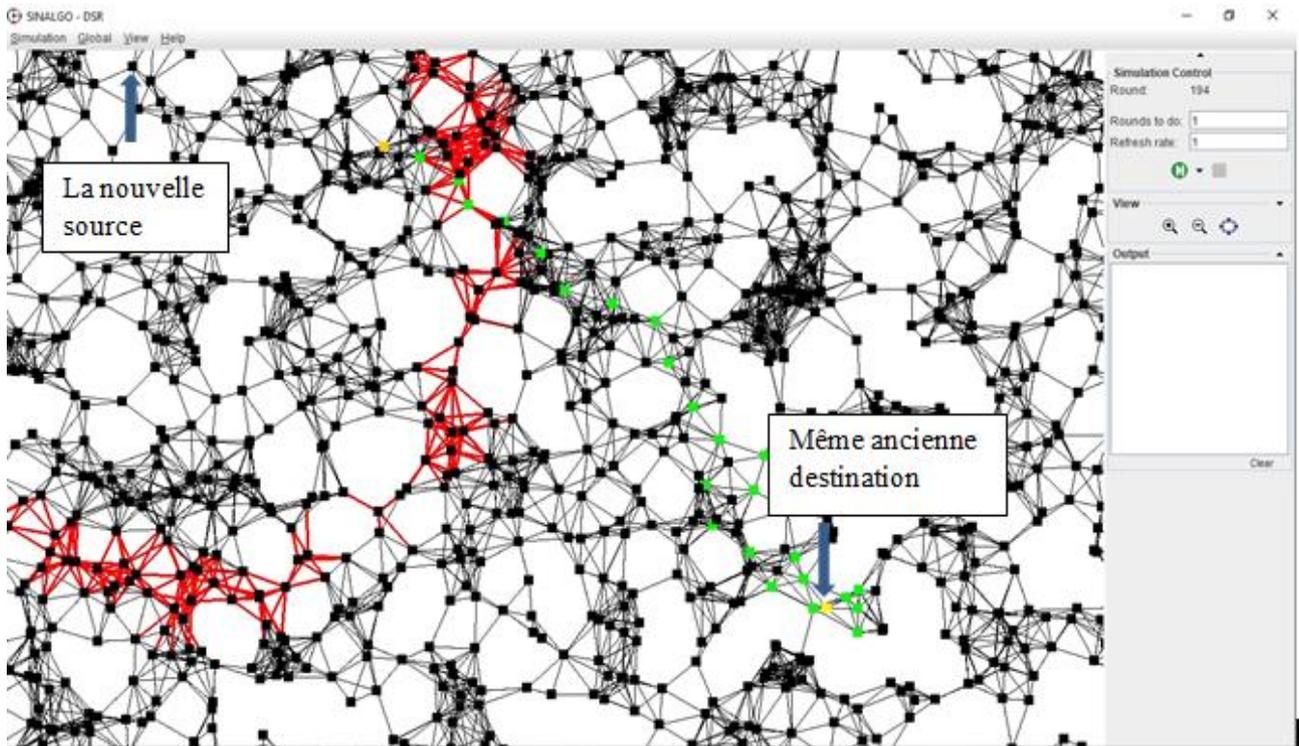


Figure III.14 : Message RREQ redistribué jusqu'à la destination.

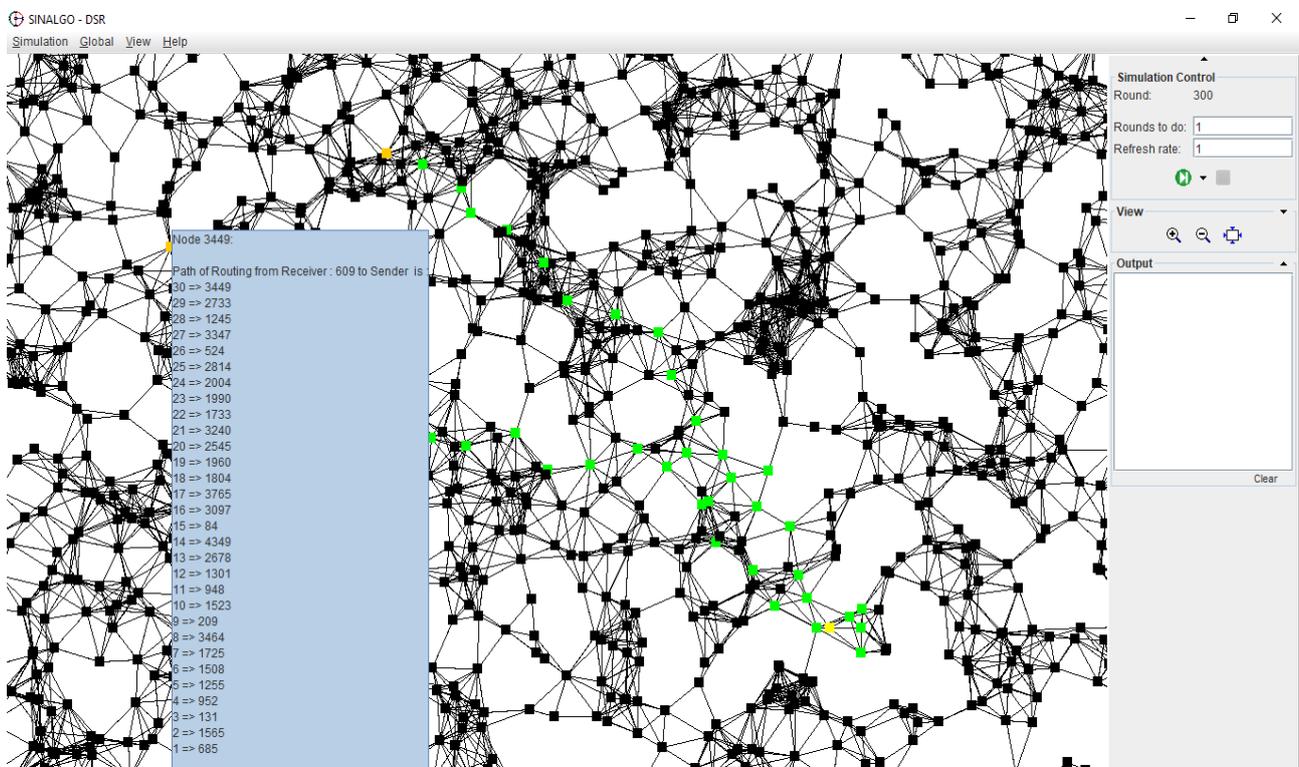


Figure III.15 : Le chemin de la source qui mène à la destination.

III.4 Résultats de la simulation

AODV et DSR utilisent une approche réactive pour la découverte de routes, mais avec un mécanisme différent :

DSR utilise le routage à la source et ne mémorise aucune trace vers la destination. Par contre, l'AODV utilise des tables de routage qui lui permettent d'accélérer le processus de calcul de route vers les destinations déjà atteintes. Ainsi, par rapport au DSR, l'AODV permet de réduire considérablement les délais d'établissement des routes, d'une part, et de diminuer énormément le nombre de message RREQ et libérer en conséquence la bande passante pour l'envoi effectif de données, de l'autre part.

III. 5 Conclusion

Dans ce chapitre, nous avons simulé deux protocoles de routage réactif ; à savoir DSR et L'AODV en utilisant le simulateur SINALGO (Simulator for Network Algorithmes), dans le but de bien appréhender leur fonctionnement et de voir les différences qui existent entre eux. En effet, nous pouvons signaler que l'AODV permet d'améliorer davantage les performances du protocole DSR en termes de délai de recherche des routes.

CONCLUSION GENERALE :

Les réseaux informatiques basés sur la communication sans fil peuvent être classés en deux catégories : les réseaux avec infrastructure, et les réseaux sans infrastructure. Dans ce mémoire, nous sommes intéressés à la deuxième catégorie où toutes les unités du réseau se déplacent librement et aucune administration centralisée n'est disponible. Les réseaux de cette catégorie sont appelés : les réseaux mobiles ad hoc.

Dans le but de faire une étude de performances, nous avons présenté plusieurs protocoles de routage qui ont été proposés pour assurer le service de routage dans ce type de réseau.

Les protocoles proposés sont classés en deux catégories principales : les protocoles proactifs qui maintiennent périodiquement des tables de routage qui indiquent à l'avance les routes vers chaque destination du réseau, et les protocoles réactifs qui établissent des routes sur demande. Les protocoles des deux catégories essaient de s'adapter aux contraintes imposées par les réseaux ad hoc afin d'assurer l'acheminement de données.

Dans ce mémoire, nous avons simulé deux protocoles réactifs à savoir le DSR et l'AODV, en utilisant le simulateur Sinalgo, dans le but d'apercevoir visuellement leur fonctionnement, d'une part, et de montrer réellement leurs avantages et leurs inconvénients, de l'autre part.

Références bibliographiques

- [1] S. MAAMAR, A.LAMIA, G.Leila, et A.Bilami, « **Etude des Performances des Protocoles de Routage dans les Réseaux Mobiles Ad-Hoc** », Article de revue, Université El Hadj Lakhdar - Batna, janv.2007.
- [2] A.BERRABAH, H.SAIDI, « **Balancement de charges dans les réseaux Ad Hoc** », Mémoire de fin d'études, Université Abou Bakr Belkaid– Tlemcen,2013.
- [3] A.BESSAIH, S.BOUCHAKEL, « **Routage et simulation dans les réseaux mobiles ad hoc**», Mémoire de fin d'études, Université A/Mira de Bejaïa, 2016.
- [4] YOUNES NADINE «**la qualité de service des services multimédia sur les réseaux ad hoc sans fil à multi-sauts**», Mémoire de fin d'études, école de technologie supérieure université du Québec, 2009.
- [5] JEAN-MARC PERCHER¹, BERNARD JOUGA², « **détection d'intrusions dans les réseaux ad hoc** », Article de revue, Ecole Supérieure d'Electronique de l'Ouest (ESEO), France.
- [6] OMAR LAHLOU « **Routage multi-chemin basé sur la fiabilité des routes dans les réseaux mobiles ad hoc** », Mémoire de maitrise en sciences appliquées, Université de Sherbrooke – canada, juillet 2005.
- [7] SUN DONGLAI «**exploring QOS and security in wireless ad-hoc network**», these de doctorate, February 2013.
- [8] <https://www.educba.com/ad-hoc-network-types/2022>.
- [9] BOUKHECHEM NADHIR, « **routage dans les réseaux mobiles ad hoc par une approche à base d'agents**», Mémoire de pour l'obtention du diplôme de Magister en informatique, Faculté des sciences et science de l'ingénieur, Constantine ,2008.
- [10] TAHAR ABBES MOUNIR, « **proposition d'un protocole a économie d'énergie dans un réseau hybride GSM et AD HOC** », thèse de doctorat, Faculté des sciences, Oran ,2011.
- [11] SALOUA CHETTIBI, « **Protocole de routage avec prise en compte de la consommation d'énergie pour les réseaux mobiles ad-hoc**», Mémoire de Magister, Université Mentouri Constantine, 2008.
- [12] SANA JGUIRIM, « **analyse et simulation du routage dans un réseau ad hoc**», », mémoire de fin d'études, école de technologie supérieure université du QUEBEC, 2018.

- [14] M. BOULKAMH CHOUAIB « **prise en compte de la QOS par les protocoles de routage dans les réseaux Mobiles Ad Hoc** », Mémoire de fin d'études, Université El Hadj Lakhdar de Batna 2007/2008.
- [15] AKRAM KOUT, « **Contributions à la Résolution du Problème de Routage dans les Réseaux Mobiles Ad-hoc par les Méthodes Bio-inspirées** », thèse de doctorat, Université Abdelhamid Mehri – Constantine, 2017.
- [16] YAHYI Siham, MALLEK Farida «**Sécurité et Routage dans les réseaux Ad hoc** », Mémoire de fin d'études, Université Mouloud MAMMERRI de TIZI-OUZOU 2012/2013.
- [17] SABRINE NAIMI «**Gestion de la mobilité dans les réseaux Ad Hoc par anticipation des métriques de routage** », thèse de doctorat, ÉCOLE DOCTORALE STITS - 22 juillet 2015.
- [18] A. OUNI, H. RIVANO, ET F. VALOIS, « Capacité de réseaux maillés sans fil : éléments déterminants et caractères insensibles », mars 2010.
- [19] FATIMA AMEZA « **Les technologies sans fil: Le routage dans les réseaux ad hoc (OLSR et AODV)**», Mémoire de fin d'études, Université de Bejaia - Licence en informatique 2007.
- [20] DOMINIQUE DHOUTAUT « **étude du standard IEEE 802.11 dans le cadre des réseaux ad hoc : de la simulation à l'expérimentation** », Thèse, l'institut national des sciences appliquées de Lyon, Le 11 Décembre 2003
- [21] HADDAD SOUHILA « **Etat de l'art sur les systèmes de détection d'intrusion dans les protocoles de routages dans les réseaux ad hoc** », Mémoire de fin d'études, université mouloud Mammeri de Tizi Ouzou 2012/2013.
- [22] DERRICHE OUIZA «**Etude et simulation des attaque dans les réseaux ad hoc** », Mémoire de fin d'études, Université Mouloud Mammeri De Tizi-Ouzou 2010/2011.
- [23] ABDELLAOUI, R « **su-olsr une nouvelle solution pour la sécurité du protocole olsr** », Mémoire de fin d'études, école de technologie supérieure université du Québec - 05 MAI 2009.
- [24] REDOUANE HAMZA «**Protocoles de routage pour les réseaux ad hoc** », Mémoire de fin d'études, Université de Montréal - Novembre 2004.

Références bibliographiques

- [25] BELKHIRA SID AHMED HICHAME «**Optimisation de la QoS dans les Réseaux Ad hoc Mobiles**», Thèse de Doctorat, Université Djilali Liabès de Sidi Bel Abbés.
- [26] BENALI A, DABO M « **Routage réactif et proactif (Unicast) dans les réseaux mobiles Ad Hoc** », MEMOIRE DE FIN D'ETUDES, UNIVERSITE ABDELHAMID IBN BADIS MOSTAGANEM, 2011.
- [27] BADR EDDINE GUIZANI « **algorithmes de cautérisation et routage dans les réseaux Ad Hoc** », Thèse de Doctorat, École Nationale des Sciences de l'Informatique (Tunisie) ,2012.
- [28] MR GUY PUJOLLE « **routage dans les réseaux ad hoc minimisant la consommation des batteries** » rapport de stage, université pierre et marie curie-CNRS UMR 7606,2002.
- [29] JEAN-PIERRE CHANET « **Algorithme de routage coopératif à qualité de service pour des réseaux ad hoc agro-environnementaux** » Thèse de Doctorat, Université Blaise Pascal - Clermont II, 2007.
- [30] EERIC THIBODEAU, « **stratégies de prévention de perte de route dans les réseaux ad hoc mobiles** », thèse de doctorat, université de Sherbrooke faculté de génie, canada,2014
- [31] HASSIBA-ASMAA ADNANE, « **La confiance dans le routage Ad hoc étude du protocole OLSR** », Thèse de Doctorat, 'Université de Rennes 1,2008
- [32] KETTOUCHE FERIEL, LATROCHE HASNIA « **Protocole de routage multi-chemins EAOMDV avec consommation d'énergie dans les réseaux sans fil Ad Hoc** », Mémoire De fin D'études, Universite abdelhamid ibn badis mostaganem Faculté des Sciences Exactes & de l'Informatique Département 2012\2013.
- [33] DJABALLAH SAMI, DJOUFELKIT HAMZA «**Etude des performances du protocole AOMDV avec prise en charge du problème d'énergie et de l'attaque du trou noir** », Mémoire De fin D'études, Université Mohamed Sadik BENYAHYIA-JIJEL Faculté des Science Exactes et Informatique 2015\2016
- [34] DIAWARA MAHAMADOU «**Contribution et étude d'un scénario réel de la télésurveillance en utilisant les drones et en appliquant l'intelligence**», Projet de fin d'études, Centre Universitaire Belhadj Bouchaib d'Ain-Temouchent Institut de Technologie 2019\2020

Références bibliographiques

- [35] SIDI IKHLEF ABDELLATIF, DJABAR ANES « **Proposition d'un algorithme de polarisation d'un graphe de connections d'un réseau Ad-hoc basé sur un modèle radio réaliste** », Projet de fin d'études, Centre Universitaire Belhadj Bouchaib d'Ain-Temouchent Institut de Technologie 2016\2017
- [36] 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 de Rennes 1 / Université 7 Novembre à Carthage sous le sceau de l'Université Européenne de Bretagne, le 24/02/2011
- [37] BELFKIH A, DRUVALLET C « **Les bases de données dans les réseaux de capteurs sans fil** », Article, Techniques et Sciences Informatiques, Décembre 2014.
- [38] AISSAOUI B, HEMAIZIA Z « **Un protocole de routage optimisé dans les réseaux Ad Hoc** » MEMOIRE DE MASTER, Université de Tébessa, 2015.
- [39] https://www.researchgate.net/figure/Routage-hierarchique-et-routage-hierarchique-ameliore_fig13_278637195
- [40] https://www.researchgate.net/figure/An-example-of-greedy-forwarding_fig2_328241617
- [41] <https://sourceforge.net/projects/sinalgo/>

Résumé

Un réseau ad hoc est une collection d'entités mobiles interconnectées par une technologie sans fil formant un réseau temporaire sans l'aide d'aucune infrastructure préexistante ou administration centralisée. Dans ces réseaux, Les nœuds sont libres de se déplacer, indépendants les uns des autres, la topologie de ces réseaux change dynamiquement, ce qui rend le routage très difficile. Par conséquent, le routage est l'un des domaines les plus préoccupants dans ces réseaux. Vu le dynamisme caractérisant la technologie ad hoc et causé par les mouvements aléatoires des nœuds, un protocole de routage adéquat doit posséder certaines caractéristiques et doit être plus dynamique afin de répondre rapidement aux changements topologiques. Parmi les protocoles existants, on trouve les protocoles DSDV, OLSR, AODV, DSR...Etc. Dans ce travail, nous avons présenté, en détails, les différents algorithmes de routage ad hoc proposés. De plus, nous avons simulé deux protocoles réactifs à savoir ; DSR et AODV, dans le but de découvrir visuellement leur fonctionnement et de toucher réellement leurs avantages et leurs inconvénients.

Mot clé : réseau, ad hoc, routage, réactif, AODV, DSR.

Abstract

An ad hoc network is a collection of mobile entities interconnected by wireless technology forming a temporary network without the aid of any pre-existing infrastructure or centralized administration. In these networks, nodes are free to move around, independent of each other, and the topology of these networks changes dynamically, making routing very difficult. As a result, routing is one of the areas of greatest concern in these networks. Given the dynamism that characterizes ad hoc technology and is caused by the random movement of nodes, a suitable routing protocol must have certain characteristics and must be more dynamic in order to respond quickly to topological changes. Among the existing protocols, we find DSDV, OLSR, AODV, DSR...Etc. In this work, we have presented, in detail, the different proposed ad hoc routing algorithms. Moreover, we have simulated two reactive protocols namely; DSR and AODV, in order to discover visually their functioning and to really touch their advantages and disadvantages.

Keyword : network, ad hoc, routing, reactive, AODV, DSR

ملخص :

الشبكة المخصصة هي مجموعة من الكيانات المتنقلة المترابطة بواسطة تقنية لاسلكية تشكل شبكة مؤقتة دون مساعدة من أي بنية تحتية موجودة مسبقاً أو إدارة مركزية. في هذه الشبكات ، تكون العقد حرة في التحرك ، مستقلة عن بعضها البعض ، تتغير طوبولوجية هذه الشبكات ديناميكياً ، مما يجعل التوجيه صعباً للغاية. لذلك ، يعد التوجيه أحد المجالات الأكثر إثارة للقلق في هذه الشبكات بالنظر إلى الديناميكية التي تميز التكنولوجيا المخصصة والتي تسببها الحركات العشوائية للعقد ، يجب أن يمتلك بروتوكول التوجيه المناسب خصائص معينة ويجب أن يكون أكثر ديناميكياً من أجل الاستجابة السريعة للتغيرات الطوبولوجية ، من بين البروتوكولات الحالية بروتوكولات DSDV و OLSR و AODV و DSR وما إلى ذلك، في هذا العمل ، قدمنا بالتفصيل خوارزميات التوجيه المختلفة المقترحة. بالإضافة الى ذلك، قمنا بمحاكاة بروتوكولين تفاعليين هما : DSR و AODV، بهدف اكتشاف كيفية عملهما بصرياً ولمس مزاياها وعيوبها حقاً.

كلمات السر : الشبكات، الشبكات المخصصة، التوجيه التفاعلي، AODV,DSR

