

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université A.MIRA Bejaïa
Faculté des Sciences exactes
Département d'informatique



Mémoire de fin d'étude

En vue de l'obtention du diplôme de Master 2 en Informatique
Option : Administration et sécurité des réseaux

Thème :

Étude et simulation du protocole de Routage AOMDV dans les réseaux mobiles ad hoc

Présentée par :

Melle ZIADA Khawla.

Melle BENMAMACE Yasmina.

Encadrer par :

Mr MEHAOEUD Kamal.

Devant le Jury composé de :

Mme ELBOUHISSI Houda.

Mr AMROUN Kamal.

Année Universitaire : 2020/2021.

Remerciement

Avant de commencer la présentation de ce rapport nous tenons à remercier "Allah" le tout puissant qui nous a donné le courage, la volonté et la force pour accomplir ce modeste travail. Merci de nous avoir éclairé le chemin de la réussite.

Nous tenons à exprimer notre profonde reconnaissance à Mr MEHLOUED Kamel professeur encadrant pour son soutien et pour son aide.

Nous adressons nos vifs remerciements aux membres des jurys pour avoir bien voulu examiner et juger ce travail.

Nous tenons à remercier également tous ceux qui nous ont aidé de près et de loin pour l'élaboration de ce mémoire.

Dédicaces

Je dédie ce travail

À mes très chers parents, source de vie,

D'amour et d'affection

À mes chers frères et leurs enfants, source de

Joie et de bonheur

À toute ma famille, source d'espoir et

De motivation

À tous mes amis qui sans leur encouragement ce travail

N'aura jamais vu le jour

À Khawla, chère amie, avant d'être binôme

Yasmina

Je dédie ce modeste travail

À mes chers parents pour leur soutien, leur patience, leur encouragement durant mon parcours scolaire.

À mes sœurs "Bouthaina et Ahelem" et mes frères « Younes, Walid et Mohamed » source de Joie et de bonheur.

À mon fiancé Mohand Akli qui m'est toujours poussé et motive dans mes études.

À ma grande famille et mes amies.

À Yasmina, chère amie, avant d'être binôme.

Khawla

Résumé

La technologie ad hoc est parmi les technologies les plus actives dans le domaine de télécommunication. Son déploiement a commencé depuis les années 1970 et continue jusqu'à aujourd'hui en raison de la flexibilité et la robustesse offertes. Cette technologie est le sujet principal de plusieurs travaux de recherche qui essayent de proposer des approches visant à améliorer le déploiement du réseau ad hoc. L'absence d'une administration centralisée et son remplacement par l'approche distributive diminuent énormément le coût de déploiement dans le plan réel. Chaque nœud est responsable et autonome dans ses décisions. Le niveau de routage fait partie des niveaux critiques durant l'exploitation de cette technologie. 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. La possession des mécanismes de contrôle et de maintenance capables d'assurer une configuration valide et adéquate aux circonstances du réseau est primordiale pour un protocole de routage dans le réseau ad hoc. La rapidité dans la recherche du trajet optimal et la disponibilité des informations caractérisent l'efficacité du protocole de routage. Plusieurs approches de routage ont été proposées afin de garantir un routage fiable dans un environnement dynamique. Dans ce contexte, on a choisi protocole de routage AOMDV qu'influence les performances résultantes dans le réseau entier. Durant ce projet, nous avons approfondi le concept de routage dans le réseau ad hoc en détaillant les mécanismes les plus répandus. Une comparaison qualitative a été élaborée entre AOMDV, DSDV et AODV et des résultats qualitatifs sont présents afin de garantir le choix convenable du protocole de routage. Une description précise des mécanismes et des algorithmes utilisés par le protocole choisi vise à éclaircir les futurs usagers sur les différentes étapes de la réalisation. Enfin, une évaluation du protocole choisi a été effectuée par l'analyse des performances données dans le réseau entier.

Abstract

Ad hoc technology is among the most active technologies in the field of telecommunications. Its deployment began in the 1970s and continues to this day due to the flexibility and robustness offered. This technology is the main subject of several research works which try to propose approaches aimed at improving the deployment of the ad hoc network. The lack of centralized administration and its replacement with the distributive approach dramatically decreases the cost of deployment in the real plan. Each node is responsible and autonomous in its decisions. The routing level is one of the critical levels during the operation of this technology. Considering the dynamism characterizing ad hoc technology and caused by the random movements of the nodes, an adequate routing protocol must have certain characteristics. Possession of control and maintenance mechanisms capable of ensuring a valid configuration and adequate to the circumstances of the network is essential for a routing protocol in the ad hoc network. The speed in finding the optimal route and the availability of information characterize the efficiency of the routing protocol. Several routing approaches have been proposed in order to guarantee reliable routing in a dynamic environment. In this context, we chose the AOMDV routing protocol that influences the resulting performance in the entire network. During this project, we deepened the concept of routing in the ad hoc network by detailing the most common mechanisms. A qualitative comparison was made between AOMDV, DSDV and AODV and qualitative results are present in order to guarantee the appropriate choice of the routing protocol. A precise description of the mechanisms and algorithms used by the chosen protocol aims to clarify the future users on the various stages of the realization. Finally, an evaluation of the chosen protocol was carried out by analyzing the performance data in the entire network.

Table des matières :

Table des matières.....	i
Liste des figure.....	iv
Liste des tableaux.....	v
Liste des abréviations.....	v
Introduction générale	1
CHAPITRE I	
I Introduction aux réseaux ad hoc	3
I.1 Introduction :	3
I.2 Bref historique :	3
I.3 Présentation des réseaux mobiles ad-hoc (MANETs) :	4
I.4 Modalisation des réseaux ad-hoc :	4
I.5 Topologies d'un réseau Ad-Hoc :	5
I.6 Modes de communications dans les réseaux Ad-hoc :	5
I.7 Types des réseaux ad-hoc :	6
I.7.1 Les réseaux personnels :	6
I.7.2 Les réseaux poste à poste ou Peer to Peer :.....	6
I.7.3 Les réseaux de capteurs (WSNs) :	6
I.7.4 Les réseaux véhiculaires :	6
I.8 Les Caractéristiques des réseaux ad hoc :	7
I.9 Les problèmes liés à réseau ad-hoc :	7
I.9.1 Le problème des stations exposées :	7
I.9.2 Problème de station caché :.....	8
I.10 Les applications des réseaux Ad hoc :	9
I.11 Les normes IEEE 802 :	9
I.12 Tableau des normes IEEE [10] :	10
I.13 Les avantages :	12
I.14 Les inconvénients :	12
I.15 Conclusion :	13
CHAPITRE II	
II Le routage dans les réseaux ad hoc	14
II.1 Introduction :	14
II.2 Le routage dans les réseaux ad-hoc :	15
II.3 Les phases de routage dans les réseaux ad hoc :	15
II.4 Les difficultés de routage dans le réseau ad hoc :	16
II.5 La conception des stratégies de routage dans les réseaux ad hoc :	16

II.6	L'objectif de protocole de routage dans les réseaux ad hoc :	17
II.7	Techniques de routage dans les réseaux ad hoc :	17
II.7.1	Routage hiérarchique ou plat :	17
II.7.2	Le routage à la source et le routage saut par saut :	18
II.7.3	État de lien et Vecteur de distance :	19
II.8	L'inondation :	19
II.9	Le concept de groupe :	20
II.10	Protocoles uniformes et non-uniformes :	20
II.11	La classification des protocoles dans les MANETs :	20
II.11.1	<i>Les protocoles de routage Proactif :</i>	22
II.11.2	<i>Les protocoles de routage réactif :</i>	23
II.11.3	<i>Les protocoles de routage hybrides :</i>	25
II.12	Avantages et inconvénient des protocoles hybrides :	27
II.13	Conclusion :	27
CHAPITRE III		
III	Le protocole de routage AOMDV :	28
III.1	Introduction :	28
III.2	Le protocole AOMDV (Adhoc On Demand Multipath Distance Vector) :	29
III.2.1	Définition du AOMDV :	29
III.2.2	Découverte de route [36] :	29
III.2.3	Maintien de la route :	30
III.2.4	La problématique de AOMDV :	31
III.2.5	Caractéristique supplémentaire du AOMDV :	31
III.2.6	Les avantage et les inconvénients :	31
III.3	Le protocole AODV « Ad hoc On Demand Distance Vector » :	32
III.3.1	Définition du AODV :	32
III.3.2	Découverte de route [37] :	32
III.3.3	Maintenance de la route :	33
III.3.4	Les avantages et les inconvénients :	33
III.4	Le protocole DSDV « Destination-Sequenced Distance Vector » :	33
III.4.1	Definition du DSDV :	33
III.4.2	Mécanismes de création des routes :	34
III.4.3	Mécanismes de maintenance des routes :	34
III.4.4	Les avantage et les inconvénients :	35
III.5	Comparaison entre les protocoles AOMDV, AODV et DSDV [39] :	35

III.6 Conclusion:	35
CHAPITRE IV	
IV Simulations et évaluation des performances.	36
IV.1 Introduction :	36
IV.2 Les différents outils des simulations :	37
IV.2.1 Le simulateur ns2 :	37
IV.2.2 Le simulateur ns-3 :	37
IV.2.3 Le simulateur OMNET++ :	37
IV.2.4 Le simulateur J-SIM :	37
IV.2.5 Le simulateur Glomosim :	37
IV.3 Domaine d'utilisation de Ns2 et Ns3 :	37
IV.4 Le choix de NS2 :	38
IV.5 Présentation du NS 2 :	38
IV.5.1 Définition :	38
IV.5.2 Script TCL-OTCL :	38
IV.5.3 NAM :	39
IV.5.4 Avantages :	39
IV.5.5 Inconvénients :	39
IV.6 Présentation de logiciel Gnu plot :	39
IV.6.1 La commande plot :	39
IV.6.2 La commande set :	40
IV.7 Étude de performance du protocole AOMDV :	40
IV.7.1 Les fichiers du protocole AOMDV :	40
IV.7.2 Paramètres de configuration :	41
IV.7.3 Scénarios de simulation :	41
Conclusion générale	45

Liste des Figures :

Figure I-1 : Exemple d'un réseau Ad Hoc simple[4].	4
Figure I-2 : Réseau en mode ad-hoc.....	5
Figure I-3 : Le changement de topologie dans les réseaux Ad-hoc.....	5
Figure I-4 : Mode communication dans les réseaux Ad-Hoc.....	6
Figure I-5 : Exemple du problème des stations exposées.....	8
Figure I-6 : Exemple de station cachés.....	8
Figure II-1 : routage à plat.....	17
Figure II-2 : routage à hiérarchique.....	18
Figure II-3 : Mécanisme d'inondation.....	20

Figure II-4: Classification des protocoles de routage MANET.....	21
Figure II-5: Processus de création de route.	24
Figure II-6: la relation entre les protocole de routage AD HOC.	25
Figure II-7: Décomposition en zones dans ZRP.....	26
Figure II-8 : La décomposition du réseau en zones.....	26
Figure III-1 : Exemple de formation d'une boucle.	29
Figure III-2: structure des table de routage dans AOMDV et AODV.....	30
Figure III-3: Schéma montrant le fonctionnement du protocole Aodv.	32
Figure III-4 : Exemple de réseau mobile Ad hoc.	33
Figure IV-1: Structure du Network Simulator 2.....	38
Figure IV-2 : le débit du protocole AOMDV.....	41
Figure IV-3 : le débit du protocole AODV.	42
Figure IV-4 : le débit du protocole DSDV.	42
Figure IV-5 : la comparaison entre les trois protocoles.....	43
Figure IV-6: le débit du protocole AOMDV avec grande/petite distance entre l'émetteur et récepteur.	43
Figure IV-7 : le débit du protocole AOMDV en fonction de nombre de nœuds.....	44

Liste des Tableaux :

Tableau I-1 : tableau des normes IEEE[10].	12
Tableau II-1: Description des critères adaptés dans la classification des protocoles de routage MANET.....	21
Tableau III-1 : La table de routage du nœud R1.....	34
Tableau IV-1 : paramètre de configuration dans le fichier.TCl.	41

Liste des abréviations:

ABR: Associativity Based Routing protocol.
AODV: Ad hoc On Demand Distance Vector.
BRP: BordQA1Zercast Resolution Protocol.
CBRP: Cluster Based Routing Protocol.
CCK: Complementary Code Keying.
CCK: Complementary Code Keying.
CGSR: Cluster head Gateway Switch Routing protocol.
CLR: CLear.
CTS: Clear-To-Send.
DAG: Directed Acyclic Graph.
DARPA: Défense Advanced Research Projects Agency.
DFS: Dynamic Frequency Selection.
DREAM: Distance Routing Effect Algorithm for Mobility.
DSDV: Destination-Sequenced Distance Vector.
DSR: Dynamic Source Routing.
DSSS: Direct-Sequence Spread Spectrum.
EWC: Enhanced Wireless Consortium.
FSR: Fisheye State Routing.
GSR: Global State Routing.
HSR: Hierarchical State Routing.

IARP: Intra-Zone Routing Protocol.
IEEE: Institute of Electrical and Electronics Engineers.
IERP: Inter-Zone Routing Protocol.
IETF: Internet Engineering Task Force.
IMEP : Internet MANET Encapsulation Protocol.
IR: InfraRouge.
MAC: Medium Access Control.
MANET: Mobile Ad-hoc Networks.
MIMO : Multiple Input Multiple Output.
MPR: Relais Multipoints.
OFDM: Orthogonal Frequency Division Multiplexing.
OLSR: Optimized Link State Routing.
OPT: Optimized.
PAN: Personal Area Network.
PDA: Personal Digital Assistant.
PSK : Phase-Shift Keying.
PSK: Phase-Shift Keying.
QRY: Query.
RERR: Route Error.
RREP: Route Reply.
RREQ: Route Request.
RTS: Request To Send.
Su RaN: *Survivable Radio Network*.
TORA: Temporary Ordering Routing Algorithm.
TPS: Transmit Power Control.
UPD: Update.
WLAN: Wireless Local Area Network.
WRP: Wireless Routing Protocol.
WSN: Wireless Sensor Network.
ZHLS: Zone-Based Hierarchical Link State Protocol.
ZRP : Zone Routing Protocol.

Introduction générale :

L'explosion des communications téléphoniques ou informatiques dans les dernières années a donné naissance à une utilisation plus croissante des réseaux de communication. L'apparition d'internet et son succès, et l'évolution des terminaux (ordinateurs, PDA, téléphones,) sont autant d'éléments qui changent notre mode de vie, et la manière dont nous utilisons ces technologies. Ce changement s'est aussi opéré dans notre relation avec les moyens de communication. Dans un tel contexte, il n'est pas surprenant de voir apparaître des solutions de communication sans fil de plus en plus performantes et évoluées. Les réseaux ad hoc répondent à ce besoin en supprimant le besoin d'infrastructure fixe pour communiquer.

Un réseau Ad hoc mobile (MANET) est un système autonome constitué de nœuds mobiles reliés par des liens sans fils. Les nœuds du MANET jouent le rôle de routeurs, se déplaçant d'une façon aléatoire, et s'organisant arbitrairement. En conséquence, la topologie du réseau MANET peut changer rapidement et de manière imprévisible. Ce type de réseau est sans infrastructure et représente une option attractive pour connecter spontanément des terminaux mobiles. MANET est appliqué dans le domaine militaire ou dans des situations de secours parce qu'il permet l'établissement d'un réseau de transmission à très court terme et à un coût très bas. Cependant, le réseau MANET est limité par différentes contraintes telles que la largeur de bande, le délai, la mobilité, etc...

Trois principales stratégies de routage sont utilisées dans les réseaux mobiles Ad hoc. Ainsi, il existe ceux qui sont basés sur l'état des liens et ceux, basés sur le vecteur de distance. Ils exigent une mise à jour périodique des données de routage qui doivent être diffusées par les différents nœuds de routage du réseau. De nombreux protocoles de routage ont été conçus pour la découverte et la maintenance des routes. La stratégie de routage est utilisée dans le but de découvrir les chemins qui existent entre les nœuds. Le but principal d'une telle stratégie est l'établissement de routes qui soient correctes et efficaces entre une paire quelconque d'unités de communication, ce qui assure l'échange des messages d'une manière continue.

Notre objectif est de modifier ou d'effectuer une extension d'un protocole existant afin de prendre en compte la stabilité des liens, l'augmentation du trafic délivré et la réduction des pertes de paquets de données. Nous allons implémenter l'extension du protocole dans le simulateur ns2 qui permet de modifier rapidement les protocoles standards existants, Les simulations effectuées vont nous permettre de vérifier si les résultats obtenus du protocole sont satisfaisants.

Le simulateur permet de faire varier les différents facteurs de l'environnement tel que le nombre d'unités mobiles, l'ensemble des unités en mouvements, les territoires du réseau et la distribution des unités dans ce territoire. Initialement, chaque unité est placée aléatoirement dans l'espace de simulation. Notre mémoire qui est subdivisée en quatre principaux chapitres :

Le premier chapitre on a introduit les réseaux ad hoc, les différents types et caractéristiques des réseaux ad hoc ainsi que ces modes de la communication.

Dans le second chapitre, nous avons présenté le routage et ses différentes phases dans les réseaux Ad hoc ainsi que la classification de ces protocoles

Le troisième chapitre est consacré à la description des trois protocoles AODV, AOMDV et DSDV. Et dans le dernier chapitre, nous avons vu le résultat de simulation des trois protocoles

Enfin, on conclut ce mémoire par un récapitulatif sur le travail réalisé dans le cadre de notre projet de fin d'études.

I Introduction aux réseaux ad hoc

I.1 Introduction :

L'évolution récente de la technologie dans le domaine de la communication sans fil et l'apparition des unités de calcul portables poussent aujourd'hui les chercheurs à faire des efforts pour mieux assurer la fonction des réseaux, à savoir l'accès rapide à l'information indépendamment du lieu et de temps. [1]

Dans un tel contexte, il n'est pas surprenant de voir apparaître des solutions de communication sans fil de plus en plus performantes et évoluées. Un réseau ad hoc ne se base sur aucune infrastructure définie au préalable, ceci revient aux exigences de la nature des applications qui supportent le modèle Ad-Hoc (fort dynamisme, surpassez le problème structure, cout et délai d'installation, etc.).

I.2 Bref historique :

Le début des années 1970 voit, au sein du projet militaire Américain DARPA (The Defense Advanced Research Projects Agency), la naissance des premiers réseaux utilisant le médium radio. Ces réseaux disposaient déjà d'une architecture distribuée, partageaient le canal de diffusion en répétant des paquets pour élargir la zone de couverture globale.

Par la suite, en 1983, les Survivable Radio Networks (Su RaN) furent développés par le DARPA. L'objectif était de dépasser les limitations (en particulier permettre le passage à des réseaux comportant énormément des nœuds, gérant la sécurité, l'énergie). Mais les recherches sur ces réseaux restaient exclusivement militaires. Ce n'est qu'avec l'arrivée du protocole 802.11 de l'IEEE (Institute of Electrical and Electronics Engineers) qui permet de bâtir des réseaux sans fil autour de bases fixes, que la recherche civile s'empare à la fin des années 90 des problématiques liées à ces réseaux. [2]

I.3 Présentation des réseaux mobiles ad-hoc (MANETs) :

Un réseau ad-hoc est constitué d'un ensemble d'unités mobiles communiquant via un médium radio et qui ne requiert ni infrastructure fixe ni administration centralisée [3], formant ainsi un réseau temporaire. Chaque station peut être par ailleurs, mise à contribution par d'autres stations pour effectuer le routage de données.

Le terme latin « ad-hoc », qui peut être littérairement traduit en « pour ceci », veut dire « pour cet objectif seulement ». Souvent, on emploie le terme « mobile » pour dire « réseaux ad-hocs mobiles » ou MANET (Mobile Ad-hoc Networks) pour désigner toutes sortes de réseaux multi sauts sans fil, sans infrastructure et parfaitement auto organisée. La configuration d'un réseau ad-hoc se fait d'une manière spontanée et temporaire une fois que plusieurs nœuds mobiles se trouvent à la portée radio les uns des autres. Lorsque le réseau est étendu, certains nœuds peuvent se comporter comme des routeurs afin de permettre la communication entre des unités mobiles hors de portée immédiate (voir Figure 1.1).

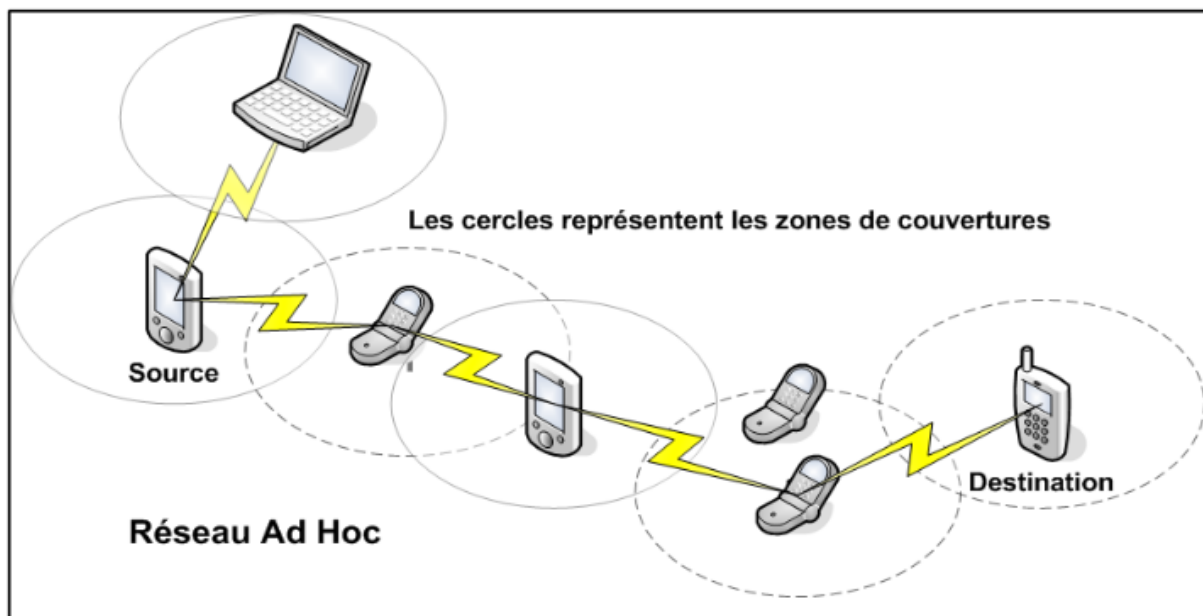


Figure I-1 : Exemple d'un réseau Ad Hoc simple[4].

I.4 Modalisation des réseaux ad-hoc :

Un réseau ad-hoc peut être modélisé par un graphe $G_t = (V_t, E_t)$. Où : V_t représente l'ensemble des nœuds (i.e. les unités ou les hôtes mobiles) du réseau et E_t modélise l'ensemble des connexions qui existent entre ces nœuds (i.e. les arcs). Soit i et j deux nœuds de V_t , l'arc (i, j) existe, si et seulement si, i peut envoyer directement un message à j on dit alors que j est voisin de i . Les couples appartenant à E_t dépendent de la position des nœuds et de leur portée de communication. Si on retient l'hypothèse que tous les nœuds ont une portée R identique, et si $d(i, j)$ désigne la distance entre les nœuds i et j , alors l'ensemble E_t peut être défini comme suit[5] :

$$E_t = \{ (i, j) \in V_t^2 \mid d(i, j) \leq R \}$$

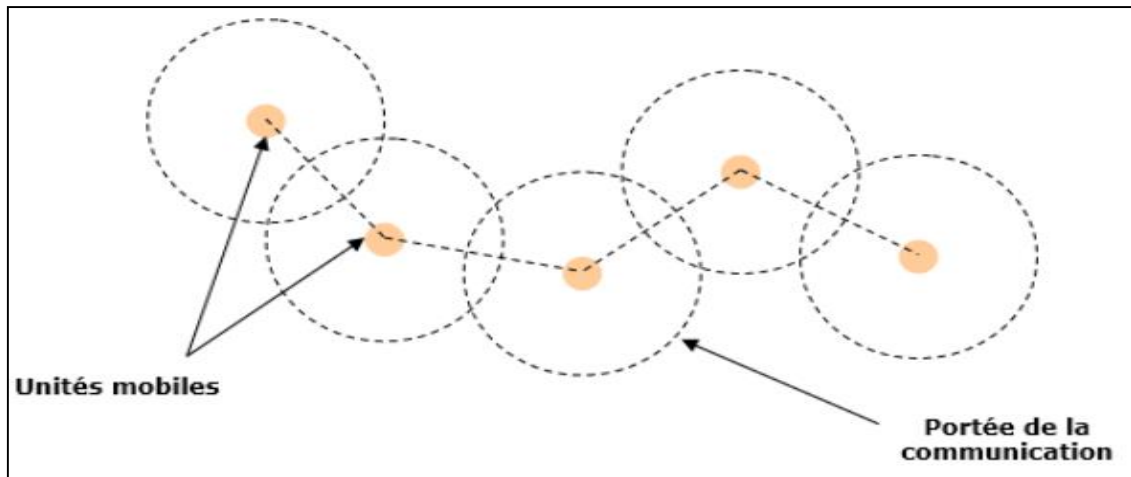


Figure I-2 : Réseau en mode ad-hoc.

I.5 Topologies d'un réseau Ad-Hoc :

La topologie du réseau peut changer à tout moment, elle est donc dynamique et imprévisible ce qui fait que la déconnexion des unités soit très fréquente.

Exemple :

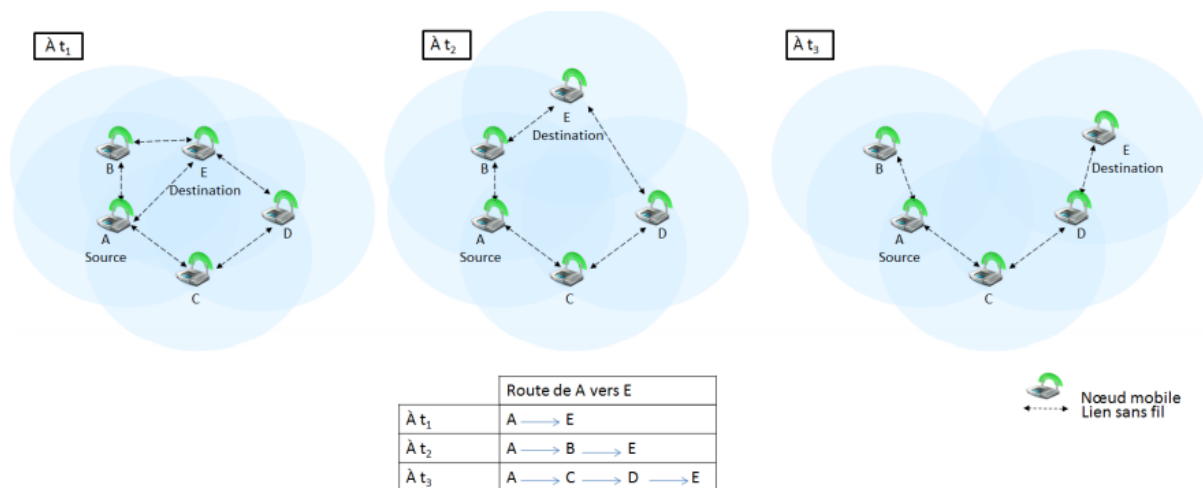


Figure I-3 : Le changement de topologie dans les réseaux Ad-hoc.

I.6 Modes de communications dans les réseaux Ad-hoc :

Avant de parler des protocoles de routage proprement dit, nous allons rappeler quels sont les principaux modes de communication dans les réseaux, et particulièrement dans les réseaux ad-hoc :

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

Ces trois modes de communication sont schématisés par la figure suivante :

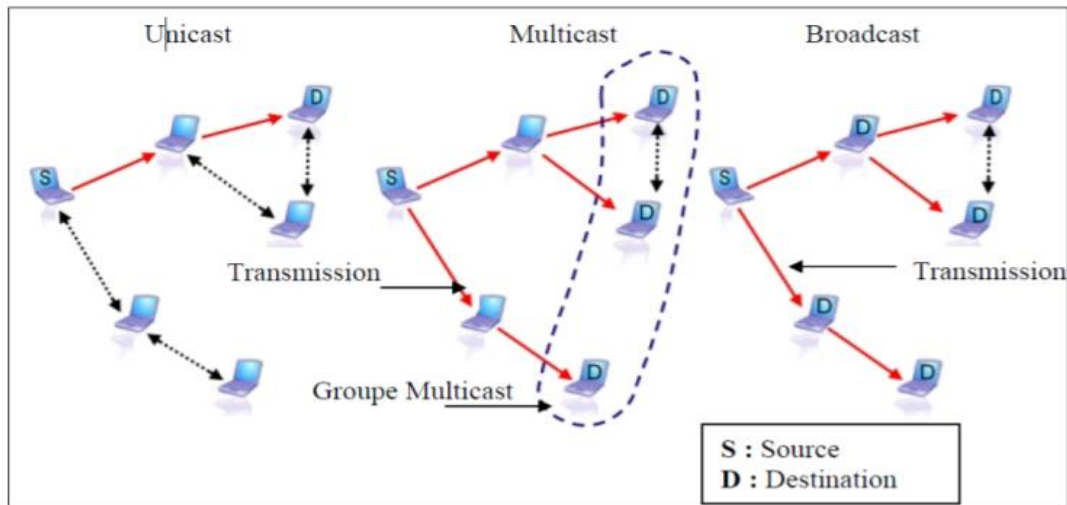


Figure I-4 : Mode communication dans les réseaux Ad-Hoc.

I.7 Types des réseaux ad-hoc :

Les types des réseaux ad hoc sont divers, nous pouvons en citer quelques-uns :

I.7.1 Les réseaux personnels :

PAN (Personal Area Network) : désigne un réseau restreint d'équipement informatique habituellement utilisées dans le cadre d'une utilisation personnelle. Parmi les technologies sans fil utilisées par les réseaux PAN, nous pouvons citer le Bluetooth, l'infrarouge (IR), ou le zigbee (la technologie 802.15.4).

I.7.2 Les réseaux poste à poste ou Peer to Peer :

Les réseaux poste à poste : sont des réseaux, dont le fonctionnement est décentralisé entre les différents utilisateurs du réseau, dont les machines sont simultanément, client et serveurs (routeur) des autres machines.

I.7.3 Les réseaux de capteurs (WSNs) :

Les réseaux de capteurs (Wireless Sensor Networks) : sont des réseaux composés de nœuds, intégrant une unité de mesure chargée de capter des grandeurs physiques (chaleur, humidité, vibration) et de le transformer en grandeurs numériques, une unité de traitement informatique de stockage de données et un module de transmission sans fil.

I.7.4 Les réseaux véhiculaires :

Les voitures de nos jours embarquent de plus en plus de technologie, et ont de plus en plus, besoin de communiquer avec l'extérieur. Les voitures équipées par des capteurs sur les toits et/ou, les pare-chocs sont capables de créer des plateformes des réseaux mobiles ad hoc et de relier en réseau les automobiles passant à proximité les uns des autres. Des prototypes ont déjà été développés pour les véhicules d'urgence (les ambulances, les voitures des pompiers, etc.).

I.8 Les Caractéristiques des réseaux ad hoc :

Les réseaux ad hocs se distinguent des réseaux cellulaires par plusieurs caractéristiques. Celles-ci doivent être prises en considération dans tout processus de conception de protocoles. Elles sont résumées dans les paragraphes suivant :

L'absence d'infrastructure : les réseaux Ad-hoc se distinguent des autres réseaux mobiles par la propriété d'absence d'infrastructure préexistante et de tout administration centralisée. Les hôtes mobiles sont responsables de l'établissement et du maintien de la connectivité du réseau de manière continue [6].

Contrainte d'énergie : les nœuds dans un réseau ad hoc sont alimentés typiquement par des batteries dont la capacité en puissance est souvent limitée. Par conséquent, elle ne peut satisfaire les demandes d'énergie d'un Nœud pour un fonctionnement normal durant une période de temps raisonnable.

Une topologie dynamique : les unités mobiles du réseau, se déplacent d'une façon libre et arbitraire. Elles peuvent accéder au réseau ou en sortir. De ce fait, la topologie du réseau peut changer, à des instants imprévisibles, de manière rapide et aléatoire. Les liens de la topologie peuvent être unis ou bidirectionnels [7].

Une bande passante limitée, une capacité des liens limitée et variable : celle-ci est limitée, par rapport à la capacité des réseaux filaires, et peut varier au cours du temps pour au moins deux raisons principales : le changement des conditions de propagation et la variation des distances entre les nœuds.

Sécurité limitée : les réseaux ad hocs mobiles sont plus vulnérables par rapport aux autres réseaux filaires et cellulaires. Cette vulnérabilité est due essentiellement à la nature du médium de propagation sans fil qui rend possibles certaines attaques malicieuses allant de l'écoute clandestine passive aux interférences actives. D'autres attaques redoutables, dues à la topologie du réseau, peuvent aussi être envisagées comme par exemple l'attaque Worm Hole [11].

Erreur de transmission : les erreurs de transmission radio sont plus fréquentes que dans les réseaux filaires.

Interférences : les liens radio ne sont pas isolés, deux transmissions simultanées sur une même fréquence ou, utilisant des fréquences proches peuvent interférer.

I.9 Les problèmes liés à réseau ad-hoc :

I.9.1 Le problème des stations exposées :

La transmission des données des nœuds voisins peut empêcher un nœud de transmettre aux autres nœuds. Il s'agit d'un problème des nœuds exposés. Un nœud exposé est un nœud dans la portée de transmission de l'émetteur mais hors de la portée du récepteur. Soit l'exemple de la Figure 1.6, quand C transmet à D. Puisque B peut « entendre » C et B n'a aucun moyen de savoir que la transmission qu'elle veut engager avec A n'entraînerait pas de collision, alors B ne peut pas risquer de transmettre à A par crainte de causer une collision à C, alors B « est exposé » au C.

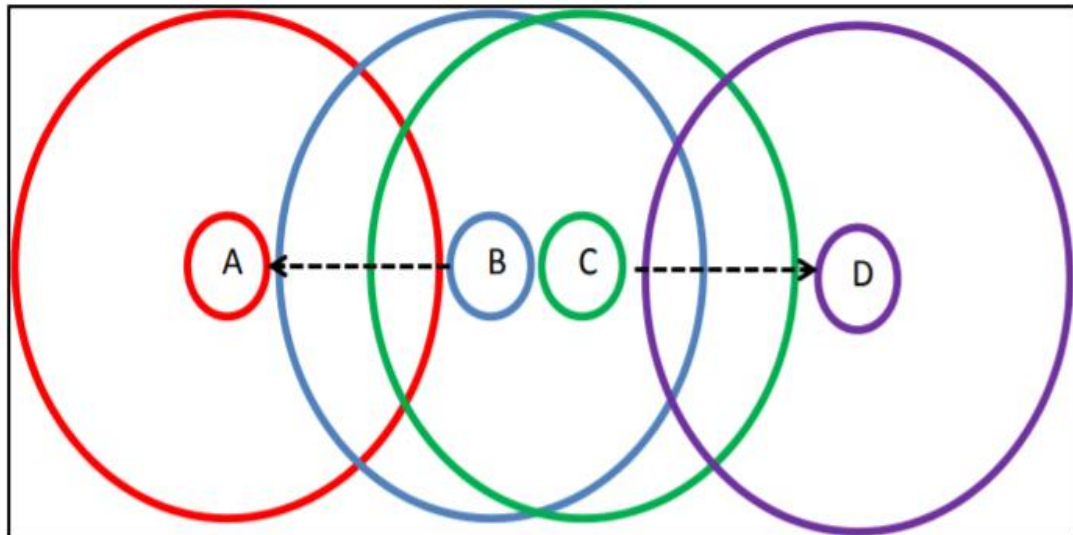


Figure I-5 : Exemple du problème des stations exposées.

La solution du problème de nœud exposé est l'utilisation des canaux de contrôle et de données de façon séparée ou l'utilisation des antennes directionnels [8].

I.9.2 Problème de station caché :

Ce phénomène est très particulier à l'environnement sans fil. Ce scénario consiste à créer une barrière dans le réseau, entre la source et la destination. La « barrière » ne doit pas être physique ; la distance assez grande séparant deux nœuds est la « barrière » qui peut se produire fréquemment dans les réseaux Ad hoc. Cette méthode est nommée le problème du terminal caché. Pour mieux comprendre ce phénomène, considérons trois nœuds A, B et C dans un réseau MANET, tels que A communique avec les deux autres nœuds, alors que B et C sont cachés l'un par rapport à l'autre (B hors de la portée de la transmission de C et contrairement). Cette situation peut générer une collision, dans le cas où B et C veulent transmettre des paquets à A en même temps.

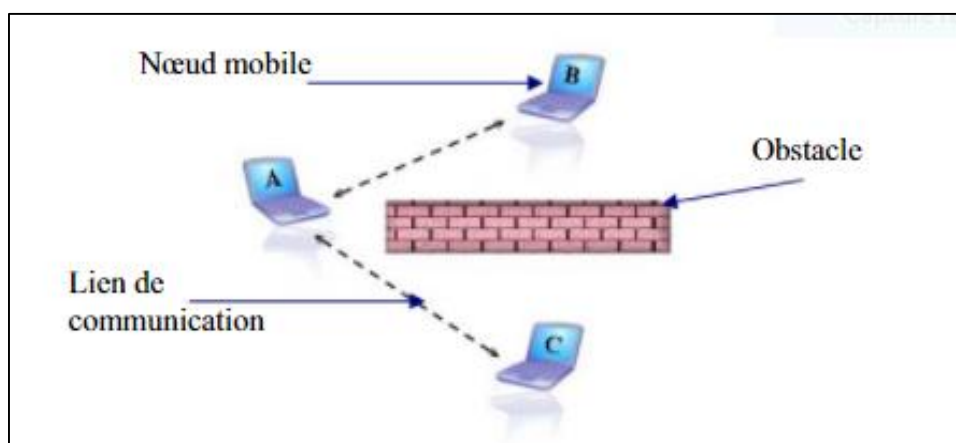


Figure I-6 : Exemple de station cachés.

Pour éviter la collision, tous les nœuds voisins au récepteur doivent être informés que le canal est occupé. Ce qui peut être atteint par un protocole simple d'échange de message. Quand C souhaite transmettre à A, il envoie d'abord un message RTS (Request to Send) à A. Dans la réponse, A annonce un message CTS (Clear-To-Send) qui est reçu par B et C. Puisque B a reçu

le message de CTS non sollicité, B sait que A accordé la permission d'envoyer à une borne cachée et par conséquent s'abstient à la transmission. Lors de la réception du message CTS d'A en réponse à son message RTS, C transmet son propre message.

Notons que la méthode RTS-CTS n'est pas une solution parfaite pour le problème de nœud caché. Parce qu'il y aura des cas où des collisions se produisent quand les messages de contrôle RTS et CTS sont envoyés par des nœuds différents [8][9].

I.10 Les applications des réseaux Ad hoc :

Quelques applications de la technologie MANET peuvent inclure des applications industrielles et commerciales, entraînant des échanges de données dans le cas de réunions comme des conférences. En plus, des applications lors de catastrophes naturelles (tremblement de terre, désastre naturel, etc.) ou ce qu'on appelle application civile pour la mise en communication d'unités de secours sur des zones larges. Il y a aussi des applications militaires pour assurer la liaison entre les différentes unités d'une armée. Les réseaux MANET peuvent être utilisés au niveau local pour faire un réseau multimédia autonome instantané à l'aide des ordinateurs portables ou des PDA (Personal Digital Assistant) dans une salle de classe (par exemple). Ceci permet le Transfer d'information entre différents équipement sans aucun branchement filaire. Les réseaux Ad hoc sont utilisables aussi comme des réseaux de capteurs (sensor-networks) où les nœuds détiennent des capteurs, par exemple de température, et une autre application des MANET est dans les réseaux domestiques (home networks) [12].

I.11 Les normes IEEE 802 :

IEEE 802 est un ensemble de normes de l'institut « Institute of Electrical and Electronics Engineers (IEEE) » qui couvre les couches physique et liaison de données du modèle OSI. une partie de IEEE définit des normes et des protocoles pour les réseaux sans fil; Il définit les caractéristiques, les procédures d'exploitation, les protocoles et les services pour les réseaux transportant des paquets de tailles variables et spécifie le développement et la gestion des périphériques et des équipements compatibles. Les spécifications les plus connues pour les réseaux ah doc (dans le tableau ci-dessous) incluent 802.11 Wi-Fi, 802.15 Bluetooth/ZigBee. La modulation utilisée dans la norme 802.11 était la modulation par décalage de phase (PSK : phase-shift keying). Pourtant, d'autres schémas, tels que le codage complémentaire (CCK : Complementary Code Keying), sont utilisés dans certaines des spécifications les plus récentes. Les nouvelles méthodes de modulation permettent une vitesse de transmission plus élevée et une vulnérabilité réduite aux interférences [10].

I.12 Tableau des normes IEEE [10] :

802	Spécification	Principes de base
802.11	Wifi	-Contrôle d'accès au média LAN sans fil et spécification de la couche physique. 802.11a, b, g, etc. sont des amendements à la norme d'origine 802.11. Les produits qui implémentent les normes 802.11 doivent réussir les tests et sont qualifiés comme certifiés.
802.11a	–	-Utilise le multiplexage par répartition orthogonale de la fréquence. -Débit de données amélioré jusqu'à 54 Mbps. -Ratifiée après 802.11b.
802.11b	–	-Amélioration de la norme 802.11 qui ajoute des modes de débit de données plus élevés au DSSS (spectre de répartition directe) déjà défini dans la norme 802.11. -Débit de données accéléré à 11 Mbps. -La bande passante de 22 MHz donne 3 canaux sans chevauchement dans la gamme de fréquences de 2.400 GHz à 2.4835 GHz.
802.11d	–	-Amélioration des normes 802.11a et 802.11b permettant une itinérance mondiale. -Les détails peuvent être définis dans la couche de contrôle d'accès au support (MAC).
802.11e	–	-Amélioration de la norme 802.11 qui inclut des fonctionnalités de qualité de service. -Facilite la hiérarchisation des transmissions de données, vocales et vidéo.
802.11g	–	-Étend le débit de données maximal des périphériques WLAN fonctionnant dans la bande 2,4 GHz, de manière à permettre une interopérabilité avec les périphériques 802.11b. -Utilise la modulation OFDM (FDG orthogonale). -Fonctionne jusqu'à 54 mégabits par seconde (Mbps), qui incluent les vitesses « b ».

802.11h	–	<p>-Amélioration de la norme 802.11a qui résout les problèmes d'interférence.</p> <p>-Sélection dynamique de fréquence (Dynamic frequency selection – DFS).</p> <p>-Contrôle de la puissance d'émission (Transmit power control - TPC).</p>
802.11i	–	<p>-Amélioration de la norme 802.11 offrant une sécurité supplémentaire pour les applications WLAN.</p> <p>-Définit un cryptage, une authentification et un échange de clés plus robustes, ainsi que des options pour la mise en cache et la pré-authentification des clés.</p>
802.11j	–	<p>-Extensions réglementaires japonaises à la spécification 802.11a.</p> <p>-Gamme de fréquence 4,9 GHz à 5,0 GHz.</p>
802.11k	–	Mesure des ressources radio pour les réseaux utilisant les spécifications de la famille 802.11.
802.11m	–	<p>-Maintenance des spécifications de la famille 802.11.</p> <p>-Corrections et modifications de la documentation existante.</p>
802.11n	–	<p>-Normes plus rapides.</p> <p>-Plusieurs technologies concurrentes et non compatibles.</p> <p>-Les vitesses maximales annoncées de 108, 240 et 350+ MHz.</p> <p>-Les propositions concurrentes proviennent des groupes EWC, TGn Sync sont toutes des variantes basées sur MIMO (entrées multiples, sorties multiples).</p>
802.11x	–	-Terme générique mal utilisé pour les spécifications de la famille 802.11.
802.13	Non utilisé	-Non utilisé.
802.15	Réseaux personnels sans fil	-Spécification de communication approuvée au début de 2002 par l'IEEE pour les réseaux personnels sans fil.

802.15.1	Bluetooth	-Technologie sans fil à courte portée (10 m) pour les souris sans fil, clavier et kit libres à 2,4 GHz.
802.15.4	ZigBee	Réseaux de capteurs sans fil à courte portée.
802.15.5	Réseau maillé	-Extension de la couverture réseau sans augmenter la puissance d'émission ou la sensibilité du récepteur. -Fiabilité améliorée par redondance de route. -Configuration réseau simplifiée – Meilleure durée de vie de la batterie du périphérique.

Tableau I-1 : tableau des normes IEEE[10].

I.13 Les avantages :

Pas de câblage : l'une des caractéristiques des réseaux Ad hoc est l'absence d'un câblage, et ce en éliminant toutes les connexions filaires qui sont remplacées par des connexions radio.

Déploiement facile : l'absence du câblage donne plus de souplesse, et permet de déployer un réseau Ad hoc facilement et rapidement. Cette facilité peut être justifiée par l'absence d'une infrastructure [13].

Mobilité : les réseaux Ad hoc permettent une certaine mobilité à leurs nœuds, de ce fait, ces derniers peuvent se déplacer librement à condition de ne pas s'éloigner trop les uns des autres. Pour garder leur connectivité [14].

Le coût d'exploitation du réseau : est faible aucune infrastructure n'est à mettre en place initialement et surtout aucun entretien n'est à prévoir.

La souplesse d'utilisation : est un paramètre très important puisque les seuls éléments pouvant tomber en panne sont les terminaux eux-mêmes [4].

Extensible : l'une des propriétés est plus importantes d'un réseau Ad hoc est la possibilité de l'entendre et d'augmenter sa taille très facilement et sans nécessiter trop de moyen.

I.14 Les inconvénients :

Capacité limitée : dans un tel réseau la configuration de la porte de la communication des nœuds est importante, il faut qu'elle soit suffisante pour assurer la connectivité du réseau.

Taux d'erreur important : les risques de collision augmentent avec le nombre de nœuds qui partagent le même médium.

Sécurité : un réseau Ad hoc ne permet pas d'assurer la confidentialité de l'information échangé entre les nœuds.

Topologie non prédictible : l'activité permanentes et les déplacements fréquents des nœuds d'un réseau Ad hoc rendent son étude très difficile, le changement rapide de sa topologie dû aux déplacement des nœuds.

Les liens entre les stations ne sont pas isolés les uns des autres et polluent le voisinage, par diffusion, lors de chaque émission ou réception de données. Par conséquent tout paquet de diffusion émis vers une station en cours de communication va altérer la communication de cette station .la diffusion est un facteur qui alourdit aussi d'autre paramètres telle que la bande passante et la consommation de batterie [4].

I.15 Conclusion :

Dans ce chapitre, nous avons présenté les réseaux mobiles ad hoc qui est un système autonome de nœuds reliés par des liens sans fil. Dans le but d'assurer la connectivité du réseau malgré l'absence d'infrastructure et la mobilité des stations, chaque nœud est susceptible d'être mis à contribution pour participer au routage et pour retransmettre les paquets d'un nœud qui n'est pas en mesure d'atteindre sa destination. Chaque nœud joue ainsi le rôle de station et de routeur et participe donc à une stratégie de routage qui lui permet de découvrir les chemins existants, afin d'atteindre les autres nœuds du réseau. Dans le chapitre suivant nous allons étudier les différents points sur le routage dans les réseaux ad-hoc.

II Le routage dans les réseaux ad hoc

II.1 Introduction :

Le routage est une méthode d'acheminement des informations à la bonne destination à travers un réseau donné. Le rôle de routage est de déterminer un acheminement optimal des paquets à travers le réseau selon un certain critère de performance [9]. Les changements rapides de la topologie dans les réseaux Ad hoc demandent des protocoles de routage spéciaux qui s'adaptent facilement. Ces dernières années plusieurs protocoles de routage pour les réseaux ad hoc ont été développés dans le cadre du groupe de recherche MANET de IETF (Internet Engineering Task Force), ces protocoles essayent de maximiser les performances en minimisant le délai de livraison des paquets, l'utilisation de la bande passante et la consommation d'énergie. Dans ce chapitre nous allons définir le routage et mentionner leur phase. Par la suite nous allons parler sur la conception des stratégies, ainsi que l'objectif de protocole de routage, enfin nous allons présenter les classifications des protocoles de routage existants et le fonctionnement de quelques protocoles tout en indiquant leurs avantages et leurs inconvénients.

II.2 Le routage dans les réseaux ad-hoc :

Dans les réseaux ad hoc il existe aucune infrastructure fixe ou élément centrale qui peut gérer le routage. Chaque nœud doit donc participer à un protocole de routage qui lui permet de communiquer avec les autres nœuds du réseau.

La stratégie (ou le protocole) de routage est utilisée dans le but de découvrir les chemins qui existent entre les nœuds d'un réseau. Le but principal d'une telle stratégie est de trouver la route optimale.

À cause de la mobilité des nœuds dans les réseaux ad hoc il est très difficile de localiser une destination à un instant donné, les protocoles de routage conçus pour des réseaux statiques sont inadaptés pour ce type de réseaux. Un protocole de routage pour les réseaux ad- hoc doit organiser le réseau, il doit construire et maintenir les routes entre les différents nœuds et s'adapter à la topologie changeante et imprévisible.

Avant d'entamer les protocoles de routage utilisés dans les réseaux ad-hoc nous allons d'abord faire un petit rappel sur quelque notion essentielle.

➤ **Définition du routage :**

Le routage est un processus qui permet de sélectionner des chemins dans un réseau pour transmettre des données depuis un expéditeur jusqu'à un ou plusieurs destinataires, il consiste à assurer une stratégie qui garantit, à n'importe quel moment, un établissement de routes (protocole de routage) 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.

➤ **Définition de protocole :**

Le protocole est une série d'étapes à suivre pour permettre une communication harmonieuse entre plusieurs ordinateurs, c'est-à-dire l'ensemble de règles qui régissent les échanges de données ou le comportement collectif de processus en réseaux .il existe plusieurs protocoles selon ce que l'on attend de la communication.

II.3 Les phases de routage dans les réseaux ad hoc :

Pour être réellement opérationnel dans un environnement mobile, le protocole de routage prend en compte trois phases [4] :

1. *Découvert de l'information de routage* : cette étape permet de connaître les éléments nécessaires sur la topologie utilisée pour choisir un chemin de qui peut atteindre le nœud de destination. En fonction de la quantité d'informations échangées, les nœuds obtiennent une vue plus précise de la topologie du réseau. Les protocoles de routage optimisent l'envoi de ces informations.
2. *Choix de chemin* : : Après la collecte des informations, le protocole de routage choisit une route en fonction de nombre minimum de sauts dans la route, le protocole choisit la route ayant le plus petit nombre de nœuds à traverser. Il faut aussi qu'on ne trouve pas de boucle dans Les routes choisies. La présence de boucles va rendre le chemin choisi inexploitable parce que le paquet ne pourra pas atteindre la destination en consommant inutilement de la bande passante et l'énergie [15].

3. *Maintenance des routes* : La topologie du réseau Ad Hoc n'arrête pas d'évoluer avec le temps. De fait à cause de la nature mobile des nœuds, les routes sont dans l'obligation de changer avec la mobilité des nœuds. Une route doit éviter de rester longtemps invalide, car les paquets ne pourraient atteindre leur destination. Le protocole de routage doit prendre en considération ces changements et met à jour les routes qui viennent d'être coupées [16].

II.4 Les difficultés de routage dans le réseau ad hoc :

Afin de pallier aux problèmes dues aux différents mouvements des nœuds mobiles qui pourront modifier le trafic, un réseau ad-hoc doit donc pouvoir s'ordonner automatiquement de telle sorte à être déployable rapidement, et de pouvoir s'adapter aux conditions de propagation, dans le cas où le nœud destinataire se trouve dans la portée du nœud émetteur nous n'aurons pas besoin de routage, chaque nœud sera donc susceptible de jouer un rôle dans l'acheminement des paquets vers sa destination finale, chaque nœud participera au processus de routage des paquets. Le fait que la taille d'un réseau Ad Hoc peut être énorme, souligne que la gestion de routage de l'environnement doit être complètement différente des approches utilisées dans le routage classique. Le problème qui se pose dans le contexte des réseaux Ad Hoc est l'adaptation de la méthode d'acheminement utilisée avec le grand nombre d'unités existant dans un environnement caractérisé par de modestes capacités de calcul et de sauvegarde [7]. Ce qui nous pousse à dire que la gestion du routage dans un environnement ad-hoc diffère de loin à celle utilisée dans les réseaux filaires.

II.5 La conception des stratégies de routage dans les réseaux ad hoc :

L'étude et la mise en œuvre d'algorithmes de routage pour assurer la connexion des réseaux ad hoc au sens classique du terme (tout sommet peut atteindre tout autre sommet) sont un problème complexe. L'environnement est dynamique et évolue donc la topologie du réseau peut changer fréquemment. Il semble donc important que toute conception de protocole de routage doive tenir compte de tous les facteurs et limitations physiques imposées par l'environnement afin que les protocoles de routage résultant ne dégradent pas les performances du système :

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

• *Le temps de latence* : la qualité des temps de latence et de chemins doit augmenter dans le cas où la connectivité du réseau augmente [17].

II.6 L'objectif de protocole de routage dans les réseaux ad hoc :

On peut se résumer en cinq points :

- Découvrir dynamiquement les routes vers les sous réseaux d'un réseau et les inscrire dans une table de routage.
- S'il existe plusieurs routes vers un sous réseau, inscrire le plus court chemin.
- Détecter les routes qui ne sont plus valides et les supprimer de la table de routage.
- Ajouter le plus rapidement possible de nouvelles routes, ou mettre à jour le plus vite possible les meilleures routes.
- Empêcher les boucles de routage.

II.7 Techniques de routage dans les réseaux ad hoc :

Le principal but de toute stratégie de routage est de mettre en œuvre une bonne gestion d'acheminement qui soit robuste et efficace. D'une manière générale, toute stratégie de routage repose sur des méthodes et des mécanismes que l'on peut regrouper en plusieurs classes : le routage hiérarchique ou plat, le routage à la source et le routage saut par saut, le routage à État de lien et Vecteur de distance [17].

II.7.1 Routage hiérarchique ou plat :

- **Les protocoles de routage à plat** : les protocoles de routage « 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 [1].

La figure illustre un exemple du routage à plat.

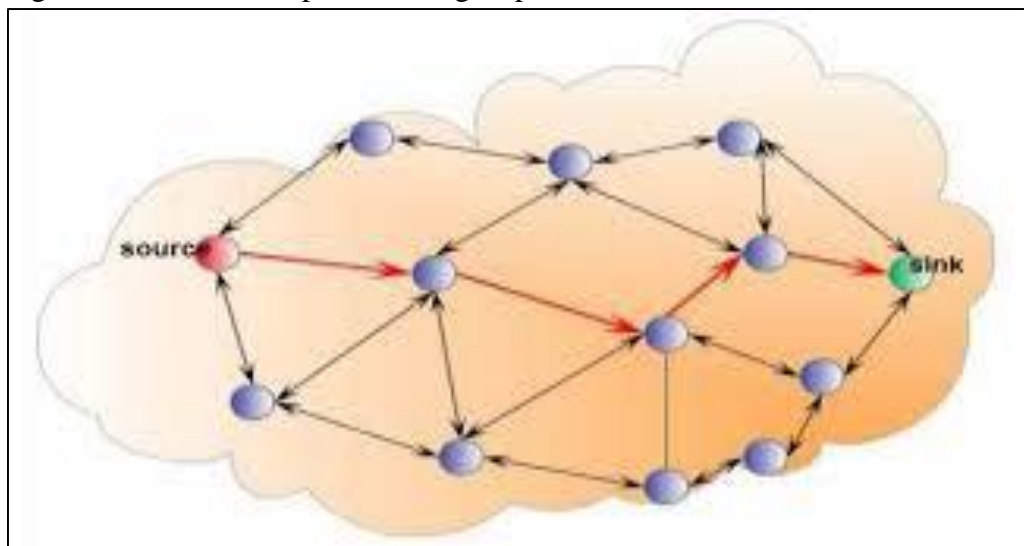


Figure II-1 : routage à plat.

- **Les protocoles de routage à hiérarchique** : la hiérarchisation des nœuds peut être vue comme un arbre hiérarchique dans une compagnie. Les nœuds les plus hauts dans la hiérarchie dirigent les nœuds se trouvant dans une position plus basse. Les nœuds dans la base de hiérarchie dépendent directement de leur supérieur. Ainsi, les nœuds se voient

attribués différentes suivant leurs positions dans la hiérarchie. Nous détaillons dans un premier temps les réseaux de clusters, puis un sous-ensemble de ce type de réseau, les réseaux backbone.

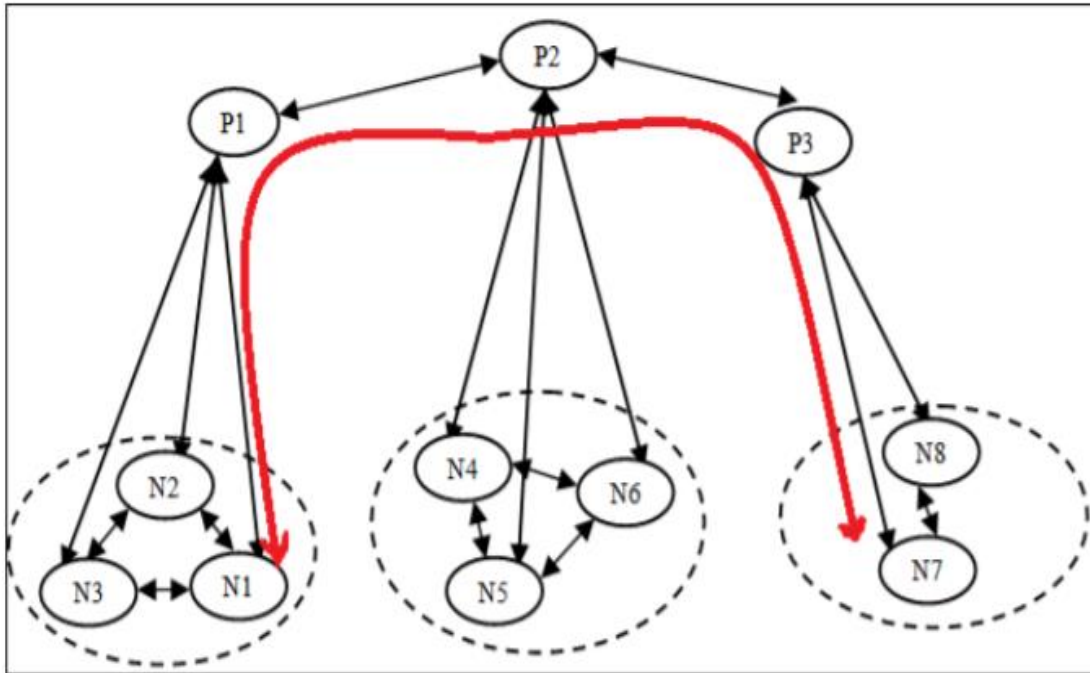


Figure II-2 : routage à hiérarchique.

II.7.2 Le routage à la source et le routage saut par saut :

- **Le routage à la source :** Dans cette technique, le nœud source détermine toute la liste des nœuds par lesquels doit transiter le message. (Pour envoyer un paquet de données d'un nœud à l'autre, l'émetteur construit une route source et l'inclut en tête du paquet. La construction se fait en spécifiant l'adresse de chaque nœud à travers lequel le paquet va passer pour atteindre la destination) livre. Par la suite, le nœud source transmet le paquet au premier nœud spécifié dans la route. Notons que chaque nœud par lequel le paquet transite, supprime son adresse de l'entête du paquet avant de le retransmettre. Une fois que le paquet arrive à sa destination, il sera délivré à la couche réseau du dernier hôte. (Le protocole le plus connu se basant sur cette stratégie est DSR) routage et simulation.
- **Le routage saut par saut (hop by hop) :** les protocoles de routage saut par saut ont de meilleures performances que les protocoles de routage à la source, dans ce type de routage, les chemins sont établis donc le paquet à envoyer doit contenir juste l'adresse du prochain nœud vers la destination.

II.7.3 État de lien et Vecteur de distance :

Cette classification est basée sur la propagation des informations d'un nœud à Travers tout le réseau. Nous allons présenter dans ce qui suit les deux approches qui se basent sur ce principe :

- **État de lien** : dans cette approche chaque nœud maintient sa propre vision de toute la topologie du réseau. La mise à jour de cette vision se fait par diffusion périodique des requêtes par chaque nœud déclarant l'état des liens de ses voisins à tous les nœuds du réseau. L'opération de mise à jour peut se faire aussi dans le cas de changement d'un état des liens. Une fois que la mise à jour est effectuée, chaque nœud change sa vision de la topologie en se basant sur l'image complète du réseau formé des liens les plus récents. Ensuite, il applique un algorithme de calcul dans cette approche, chaque nœud diffuse à ses voisins sa vision des distances qui le séparent de tous les hôtes du réseau. Chaque nœud calcule le chemin le plus court vers n'importe quelle destination en se basant sur les informations reçues par tous ses voisins. Cette approche est basée sur l'algorithme distribué de Bellman Ford (BF) [19]. Le processus de calcul de plus court chemin se répète jusqu'à ce que le réseau atteigne un état stable [18].
- **Vecteur de distance** : par contre dans cette technique, chaque nœud diffuse à ses voisins sa vision des distances qui le séparent de tous les hôtes du réseau. Chaque nœud calcule le chemin le plus court vers n'importe quelle destination en se basant sur les informations reçues par tous ses voisins. Cette approche est basée sur l'algorithme distribué de Bellman Ford (BF) [20]. Le processus de calcul de plus court chemin se répète jusqu'à ce que le réseau atteigne un état stable [18].

II.8 L'inondation :

L'inondation ou la diffusion pure, consiste à répéter 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 les nœuds peuvent appliquer (durant l'inondation) certains traitements de contrôle dans le but d'éviter certains problèmes, tel que le blocage et la duplication des messages, Le mécanisme d'inondation est utilisé généralement dans la première phase du routage plus exactement dans la procédure de découverte des routes, et cela dans le cas où le nœud source ne connaît pas la localisation exacte de la destination.

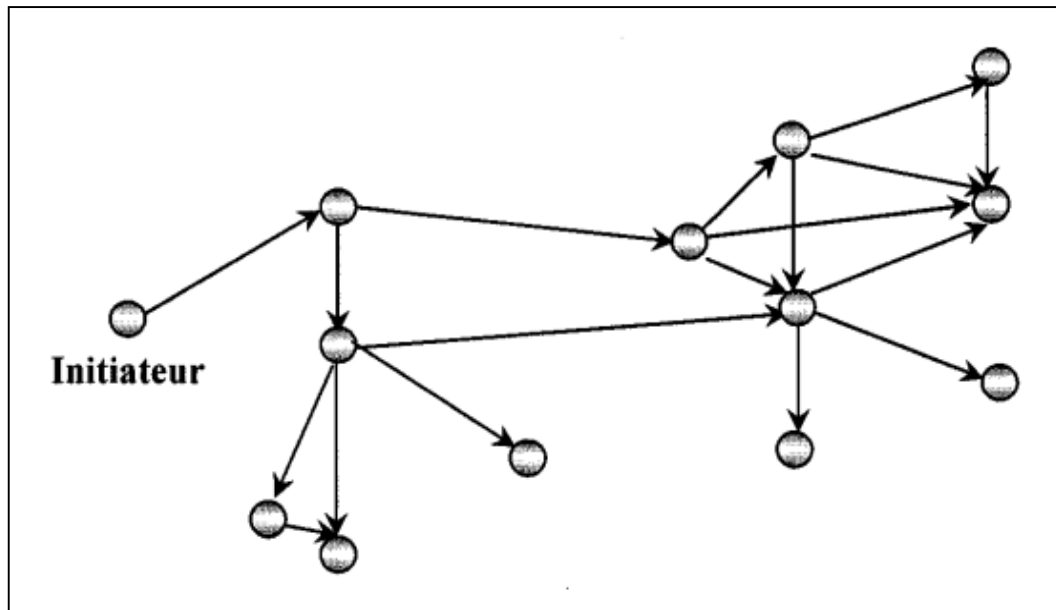


Figure II-3 : Mécanisme d'inondation.

II.9 Le concept de groupe :

Dans la communication de groupe, les messages sont transmis à des entités abstraites ou groupes, les émetteurs n'ont pas besoin de connaître les membres du groupe destinataire. La gestion des membres d'un groupe permet à un élément de se joindre à un groupe, de quitter ce groupe, se déplacer ailleurs puis rejoindre le même groupe. C'est en ce sens que la communication de groupe assure une indépendance de la localisation, ce qui la rend parfaitement basée sur les groupes. Le concept de groupe facilite les tâches de la gestion du routage (telles que les transmissions des paquets, l'allocation de la bande passante etc.) et cela en décomposant le réseau en un ensemble de groupes connectés.

II.10 Protocoles uniformes et non-uniformes :

Certains protocoles de routage n'utilisent pas tous les nœuds d'un réseau pour faire transiter les messages, au contraire ils en sélectionnent certains, en fonction du voisinage ou pour former des cellules, ces protocoles sont dits non-uniformes. Ceux qui utilisent tous les nœuds du réseau capables de router sont appelés protocoles uniformes.

II.11 La classification des protocoles dans les MANETs :

Les protocoles de routage pour les réseaux ad hoc peuvent être classés de différentes manières. Le tableau suivant décrit quelques critères adaptés dans cette classification. Elle peut dépendre de [18] :

- ≈ **Le principe de conception** : proactif, réactif, ou hybride.
- ≈ **La structure du réseau** : qui peut être uniforme ou non uniforme.
- ≈ **L'état des informations** : obtenues par chaque nœud dans le réseau comme pour les protocoles de routage orientés topologie ou les protocoles de routage orientés destination.

Tableau II-1: Description des critères adaptés dans la classification des protocoles de routage MANET.

Type	Description
Uniforme	tous les nœuds du nœud agissent de la même manière pour la fonction de routage : aucune hiérarchie dans le réseau.
Non Uniforme	quelques nœuds participent dans la fonction du routage : structure hiérarchique du réseau.
Protocoles orientés topologie	chaque nœud collecte des informations sur l'état de ses connexions avec ses voisins et les transmet aux autres nœuds pour leur garantir une connaissance précise de la topologie du réseau.
Protocoles orientés destination	chaque nœud échange ses estimations de distance avec chacun de ses voisins directs pour tous les nœuds de réseau.
Les protocoles à partitionnement	le réseau est découpé en zones dans lesquelles le routage est assuré par un unique nœud maître.
Les protocoles à sélection de voisins	chaque nœud traitent la fonction de routage à un sous ensemble de ses voisins directs.

Sur la base des critères décrits dans tableau 1.1, la figure 1.7 présente une classification des protocoles de routage MANET [18].

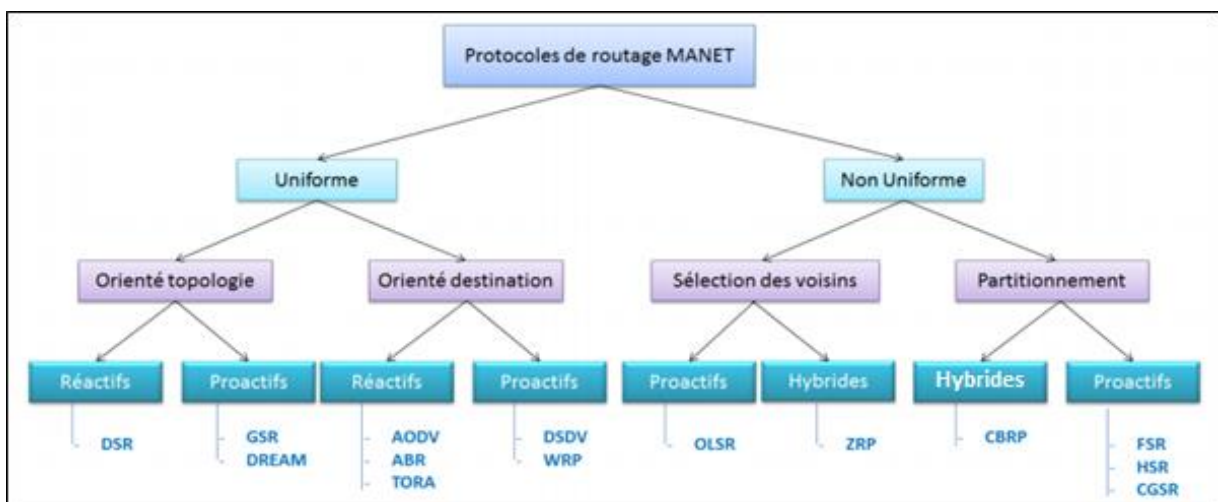


Figure II-4: Classification des protocoles de routage MANET.

II.11.1 Les protocoles de routage Proactif :

II.11.1.1 Définition :

Les protocoles de routage proactif diffusent des messages de contrôle périodiques pour la création, la maintenance et la mise à jour des routes, et ce en parallèle de la transmission des données. Même s'il n'y a pas de trafic, cette maintenance reste toujours active [18]. Cette classe de protocole est basée sur la même philosophie des protocoles de routage utilisés dans les réseaux câblés traditionnels tels que les protocoles d'état de lien (Link State) et ceux du vecteur de distance (Distance Victor) [12]. Les protocoles de routage proactifs réunissent les idées des deux types de protocoles. Ils essaient de réduire leurs limitations, et de prendre en compte les caractéristiques des environnements mobiles afin de les adapter à ce nouvel environnement et de maintenir les meilleurs chemins vers toutes les destinations du réseau par l'échange périodique de messages de contrôle de mise à jour. Les protocoles basés sur ce principe sont : DSDV, GSR, OLSR, etc...

II.11.1.2 Exemples de protocole de routage proactif :

OLSR « Optimized Link State Routing / Routage à Etat de Lien Optimisé » : Comme son nom l'indique, OLSR [21] est un protocole à état de lien. Il n'y a pas d'inondation du réseau avec les messages de contrôle car les requêtes sont diffusées à un certain ensemble de nœuds appelés relais multipoints (MPR) qui servent à joindre les voisins à deux sauts. La table de routage est déterminée dynamiquement et contient des routes optimales en termes de nombre de sauts. Pour maintenir à jour les informations nécessaires au calcul de la table de routage, les nœuds OLSR ont besoin de s'échanger des informations périodiquement. Pour ceci ils envoient des messages HELLOs contenant la liste de leurs voisins. Ce type de message fournit une connaissance locale de la topologie qui ne dépasse pas deux sauts. Les informations collectées offrent une carte complète du réseau contenant tous les nœuds et cela est suffisant pour la construction de la table de routage [17].

DREAM « Distance Routing Effect Algorithm for Mobility » : Le protocole appelé "Algorithme d'Effet de Routage basé sur la Distance, pour la Mobilité" [22] procède par inondation partielle afin de découvrir une route inexistante. Si la source dispose d'informations récentes elle choisit de diffuser sa requête sur un ensemble précis de nœuds voisins. Sinon elle inonde tout le réseau. Nous économisons ainsi le nombre de paquets en circulation. Quand le nœud destination reçoit les données, il envoie des acquittements à la source d'une manière similaire. Dans le cas où la source envoie les données, un *timer* associé à la réception des acquittements est activé. Si aucun acquittement n'est reçu avant l'expiration du timeout, les données seront retransmises en utilisant une diffusion ordinaire [17].

II.11.1.3 Avantage et Inconvénient des protocoles proactifs :

L'avantage est qu'une route est toujours disponible entre une source et une destination sans pour autant déclencher des mécanismes de recherche de route, et le gain de temps lors d'une demande de route.

L'inconvénient de tels protocoles est la signalisation qui peut affecter la bande passante. Les changements de routes peuvent être plus fréquents que la demande de la route et le trafic induit par les messages de contrôle et de mise à jour des tables de routages peut être important et partiellement inutile, ce qui gaspille la capacité du réseau sans fil.

II.11.2 Les protocoles de routage réactif :

II.11.2.1 Définition :

Au lieu de maintenir des tables de routage en tout temps, le routage réactif crée les routes à la demande du nœud émetteur. Quand un nœud a besoin de connaître une route vers une destination donnée, une procédure de découverte de route est lancée. Une fois que la route est déterminée, elle sera maintenue par une procédure de maintenance de route. L'instabilité des liens dans les réseaux ad-hoc due aux déplacements des nœuds rend le routage réactif plus adapté à ces réseaux par rapport au routage proactif [23].

II.11.2.2 Exemples de protocole de routage réactif :

DSR « Dynamic Source Routing » : Il est basé sur l'utilisation de la technique « routage source » [24] [25]. Dans cette technique, la source détermine la séquence complète des nœuds intermédiaires à travers lesquels les paquets de données seront envoyés. Les deux opérations de base dans DSR sont :

- Découverte de route.
- Maintenance de route.

Dans la première opération, un hôte diffuse un paquet de type 'requête de route'. Cette requête est propagée dans le réseau jusqu'à ce qu'elle atteigne la destination qui répond par un paquet 'réponse de route' avec la séquence des nœuds visités. Une fois la route construite, elle est incluse en tête du paquet de donnée. Un nœud qui reçoit le paquet de données supprime son adresse de l'entête du message reçu puis le transmet au nœud suivant. La deuxième opération assure la validité des chemins utilisés en exécutant une procédure de maintenance de route. Quand un nœud détecte un problème fatal de transmission il envoie un message 'erreur de route' à l'émetteur d'origine. Ce dernier doit initier une nouvelle opération de demande de route [17].

TORA « **Temporary Ordering Routing Algorithm** » : utilise une technique de routage appelée "Inversement de Liens" (Link Reversal), et possède quatre fonctions de base :

- ◆ Création de routes.
- ◆ Maintenance de routes.
- ◆ Elimination de routes.
- ◆ Optimisation de routes.

Il est basé sur le principe des graphes acycliques orientés (DAG : Directed Acyclic Graph) pour la création d'une route vers la destination. Le nœud source diffuse un paquet QRY (QueRY) spécifiant l'identificateur de la destination, qui identifie le nœud pour lequel l'algorithme est exécuté. Le récepteur répond par l'envoi d'un paquet UPD (UPDate) qui contient sa propre taille.

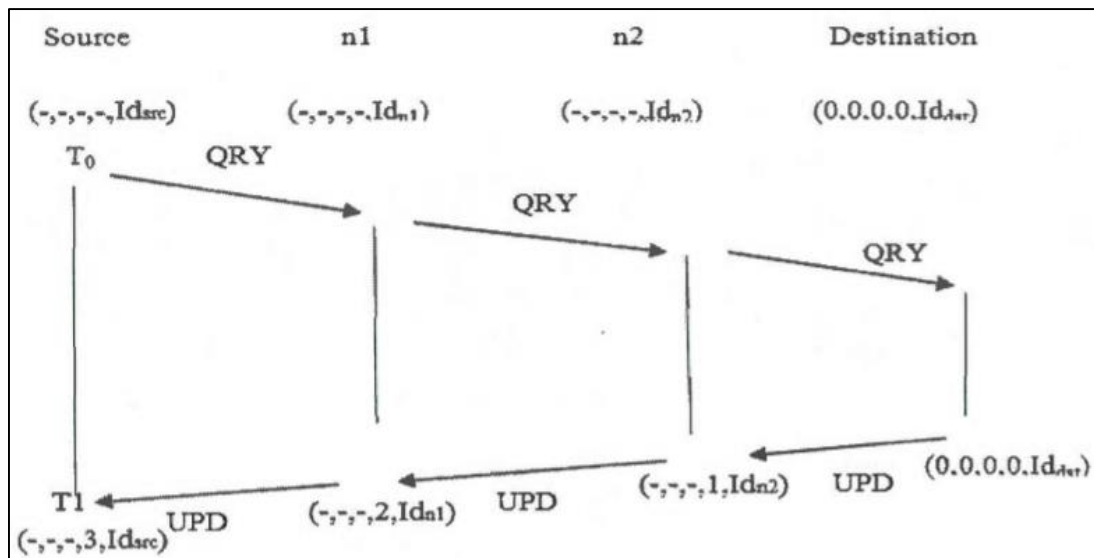


Figure II-5: Processus de création de route.

Le processus de maintenance de route est moins coûteux en paquets de contrôle que l'établissement d'un nouveau chemin car l'algorithme analyse l'état des nœuds les plus proches de l'endroit de la rupture. Cela se fait selon les deux cas suivants. Dans le premier cas, le nœud traité n'a aucun lien sortant après un échec de lien. Donc, il doit définir un nouveau niveau de référence et mettre à jour la valeur correspondante au niveau du quintuple de chaque nœud. Dans le deuxième cas, le nœud traité n'a aucun lien sortant car une inversion de lien a été faite après la réception d'un paquet UPD [26].

La fonction de l'effacement des routes utilise le paquet de contrôle CLR (CLear). Au niveau du nœud à traiter, il faut mettre la valeur de la hauteur à "Nul/" ainsi que celles de tous ses voisins directs.

L'optimisation des routes utilise des paquets de contrôle OPT (OPTimized). Elle est employée lorsque tous les chemins vers une destination sont découverts. Il est à signaler que tous les paquets transmis par TORA d'un nœud source vers un nœud destination doivent être encapsulés par le protocole IMEP (Internet MANET Encapsulation Protocol), avant d'être transmis. IMEP fait la liaison de ces paquets à la couche liaison. Le protocole TORA est informé par le protocole IMEP de tout changement d'état des liens vers les voisins via des paquets de contrôles (beacons) [26].

II.11.2.3 Les avantages et les inconvénients des protocoles réactifs :

Les avantages de ce type de protocole est la réduction de la surcharge des réseaux par la mise à jour régulière des tables de routage, la conservation d'énergie et la bande passante. Cependant, la recherche des chemins peut dégrader les performances des applications interactives par exemple en termes de délai d'établissement de la route.

II.11.3 Les protocoles de routage hybrides :

II.11.3.1 Définition :

Les protocoles hybrides combinent les deux protocoles proactif et réactif pour bénéficier de leurs avantages, ils utilisent un protocole proactif, pour connaître les voisins les plus proches, 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 [27].

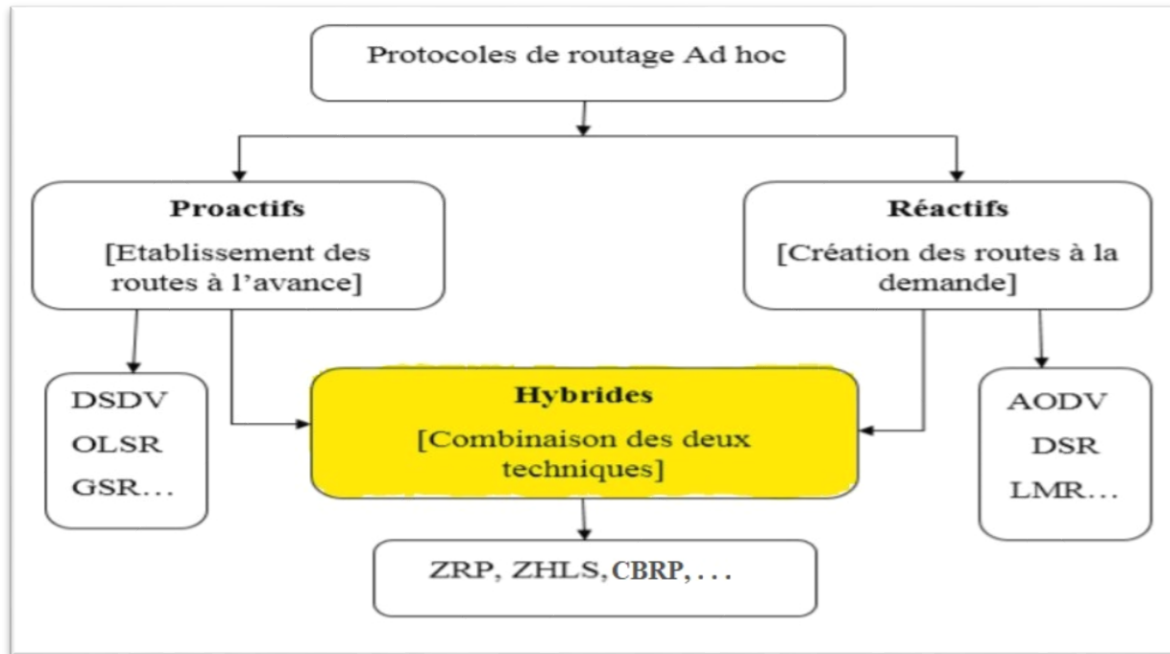


Figure II-6: la relation entre les protocoles de routage AD HOC.

Les protocoles hybrides s'adaptent bien aux grands réseaux, cependant, ils comportent aussi les inconvénients des protocoles réactifs tels que : les messages de contrôle périodiques, plus le coût de recherche d'une nouvelle route [28].

Plusieurs protocoles hybrides existent dont le), ZRP (Zone Routing Protocol ZHLS et CBRP (Cluster Based Routing Protocol).

II.11.3.2 Exemple de protocole de routage hybride :

Le protocole ZRP (Zone Routing Protocol) : est un protocole de routage hybride combinant des mécanismes réactifs et proactifs. Chaque nœud possède une zone de routage, délimitée par un nombre de sauts à partir du nœud considéré (rayon de la zone). La zone de routage regroupe tous les nœuds dont la distance en nombre de sauts est inférieure ou égale au rayon de la zone. Le fonctionnement de ZRP s'appuie sur trois protocoles [29] [30] :

- le protocole IARP (Intra-Zone Routing Protocol) : c'est un protocole proactif qui permet à chaque nœud de connaître la topologie de sa zone de routage (comme OLSR par exemple).
- le protocole IERP (Inter-Zone Routing Protocol) : c'est un protocole réactif pour découvrir les routes vers les nœuds externes à la zone de routage (comme DSR ou AODV).
- le protocole BRP (Bordercast Resolution Protocol) : il est utilisé en association avec le protocole IERP. Au lieu d'utiliser la diffusion classique, ce protocole permet de ne relayer la requête de route d'un nœud qu'aux nœuds périphériques de sa zone (connus grâce à l'IARP).

Les nœuds périphériques de la zone sont les nœuds situés à une distance en nombre de sauts égale au rayon de la zone [31].

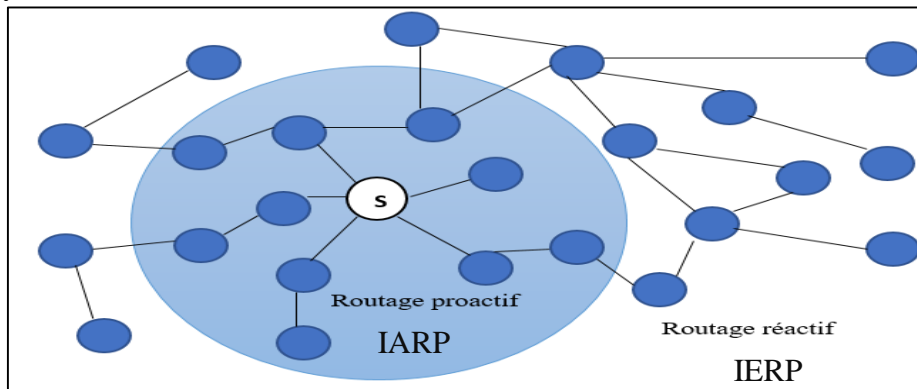


Figure II-7: Décomposition en zones dans ZRP.

Le protocole ZHLS (Zone-Based Hierarchical Link State Protocol) [16] : comme ZRP allie une recherche proactive dans l'Intra zone et une recherche réactive dans l'Interzone. Il suppose que le réseau est divisé en zones qui ne se chevauchent pas, (Figure 4). ZHLS utilise le principe des protocoles à état de liens pour déterminer l'ensemble des nœuds qui la composent. Il définit deux niveaux de topologie : niveau de nœud et niveau de zone. Une topologie de niveau de nœud indique que les nœuds d'une zone sont reliés entre eux physiquement. Un lien virtuel entre deux zones existe si au moins un nœud d'une zone est physiquement relié à un certain nœud de l'autre zone. La topologie de niveau de zone indique comment les zones sont reliées ensemble. Connaissant la topologie, chaque nœud détermine les routes pour joindre l'ensemble des nœuds de sa zone. Le routage dans l'interzone consiste, dans un premier temps, à déterminer les nœuds frontières faisant liaison avec les zones voisines. Lorsqu'une zone a déterminé celles qui l'entourent, la totalité des nœuds du réseau propage cette information. De fait, chaque nœud détermine un chemin vers les autres zones du réseau. Lors de la recherche d'une route dont la destination est située dans l'Interzone, la source interroge l'ensemble des zones du réseau pour déterminer à quelle zone appartient la destination. Une fois la zone identifiée, la source peut envoyer vers cette zone des paquets de données qui arriveront à destination. Ce protocole réduit le nombre d'informations de contrôle échangé pour déterminer un chemin. Par contre, il suppose que le réseau est déjà divisé en zones qui ne se chevauchent pas.

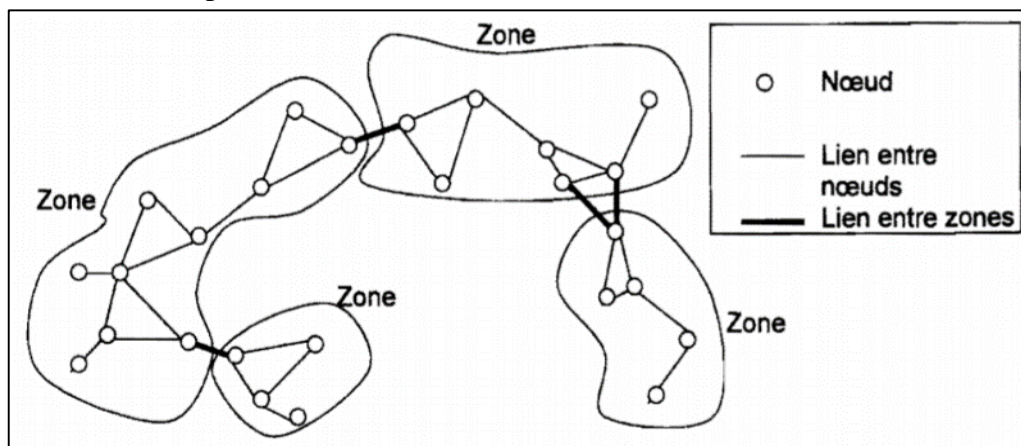


Figure II-8 : La décomposition du réseau en zones.

II.12 Avantages et inconvénient des protocoles hybrides :

Le protocole hybride est un protocole qui se veut comme une solution mettant en commun les avantages des deux approches précédentes en utilisant une notion de découpe du réseau.

Cependant, il rassemble toujours quelques inconvénients des deux approches proactives et réactives.

II.13 Conclusion :

Nous avons présenté dans ce chapitre une classification des protocoles de routage pour les réseaux ad hoc. Ces protocoles peuvent se classer en trois grandes catégories. Les protocoles proactifs qui réduisent le délai de livraison de paquets mais utilisent beaucoup de paquets de contrôle, les protocoles réactifs qui réduisent l'utilisation des paquets de contrôle mais qui ont un délai de livraison des paquets élevé, En plus des deux catégories de protocoles de routage, proactifs et réactifs, il existe une autre catégorie appelée hybride qui combine les précédentes. Cette catégorie fera l'objet du chapitre suivant.

III Le protocole de routage AOMDV

III.1 Introduction :

Lors de la transmission d'un paquet de données d'une source vers une destination, il est nécessaire de faire appel à un protocole de routage qui acheminera correctement le paquet par le meilleur chemin. Dans la plupart des cas, l'unité destination ne se trouve pas obligatoirement dans la portée de l'unité source ce qui implique que l'échange des données entre deux nœuds quelconques, doit être effectué par des stations intermédiaires. Chaque unité devient donc un nœud susceptible d'être mis à contribution pour participer au routage. De nombreux protocoles ont été proposés, ils peuvent être classés en deux catégories, les protocoles proactifs comme DSDV qui établissent les routes à l'avance en se basant sur l'échange périodique de tables de routage et les protocoles réactifs comme AODV et AOMDV qui recherchent les routes à la demande du réseau.

III.2 Le protocole AOMDV (Adhoc On Demand Multipath Distance Vector) :

III.2.1 Définition du AOMDV :

AOMDV (Adhoc On Demand Multipath Distance Vector) est un protocole de routage réactif multi chemin. Il s'agit d'une extension d'AODV et fournit également deux services principaux, à savoir la découverte et la maintenance des routes. AOMDV est un protocole de routage à la demande qui découvre une route lorsqu'une source doit communiquer avec une destination. Le protocole de routage multi-chemin construit plusieurs chemins disjoints sans boucle de routage [33] allant de la source vers la destination mais il n'utilise que le meilleur chemin en terme de nombre de saut comme chemin primaire pour transfère les données. Ces chemins multiples peuvent être utilisés pour la répartition de la charge ou comme routes de secours lorsque la route principale échoue [34].

III.2.2 Découverte de route [36] :

L'idée principale dans AOMDV consiste à calculer différentes routes, allant de la source de trafic jusqu'à la destination, tout en évitant la formation de boucles de routage.

Au début de la procédure, la source envoie le message de demande de route RREQ (Route_ReqUest) à ses nœuds voisins. Les nœuds voisins reçoivent le RREQ et envoient à leur tour un RREQ à leurs nœuds voisins. Cette opération est répétée jusqu'à ce que le nœud destination reçoive la demande de route. Ce dernier génère une réponse de route RREP (Route_RepLy) pour chaque RREQ reçu. Le nœud source reçoit plusieurs RREPs correspondants aux chemins découverts, Si un seul RREP est reçu donc une seule route est reconnue entre la source et la destination, alors elle envoie les paquets de données sur cette route, Sinon, si plusieurs RREP ont été reçu, la source choisit la meilleure route c'est-à-dire celle ayant le plus petit nombre de saut « hopcount ». Les autres routes restent en attente de l'arrivée d'un paquet RERR indiquant la rupture de la route principale, dans ce cas la meilleure route parmi les routes alternatives est sélectionnée pour retransmettre les données. Si aucun RREP n'est reçu, une nouvelle phase de découverte de route est déclenchée.

III.2.2.1 Construction de chemins multiples sans boucle de routage :

Pour voir comment les boucles peuvent se produire, considérez le simple exemple ci-dessous : la source S diffuse des paquets de requête RREQ, qui seront interceptés par le nœud intermédiaire A. le nœud A le diffuse à nouveau aux nœuds voisins (nœud B incluse). Le nœud B envoie cette requête au nœud C. Ce dernier qui est un voisin du nœud A, va rediffuser cette requête, qui sera entendue par le nœud A aussi. Si le nœud A accepte cette copie de RREQ, une boucle va se former (comme illustre dans la figure III.1).

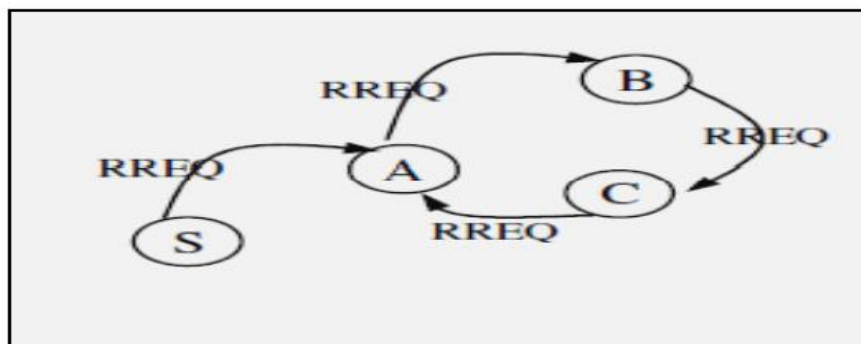


Figure III-1 : Exemple de formation d'une boucle.

Afin de garder la trace de plusieurs chemins, AOMDV introduit deux champs qui sont Route List et Advertised_hopcount. Le champ Route List remplace celui de next_hop du protocole AODV. Cette liste définit pour chaque prochain saut (nexthopk), le nombre de saut (hopcount) nécessaire pour atteindre la destination en passant par ce nœud. Le champ Advertised_hopcount remplace le Hopcount de AODV. L'Advertised_hopcount d'un nœud I, pour une destination D, représente le maximum des hopcount associés aux routes multiples disponibles pour I vers la destination D. La figure suivante montre la structure des tables de routage dans AODV et AOMDV.

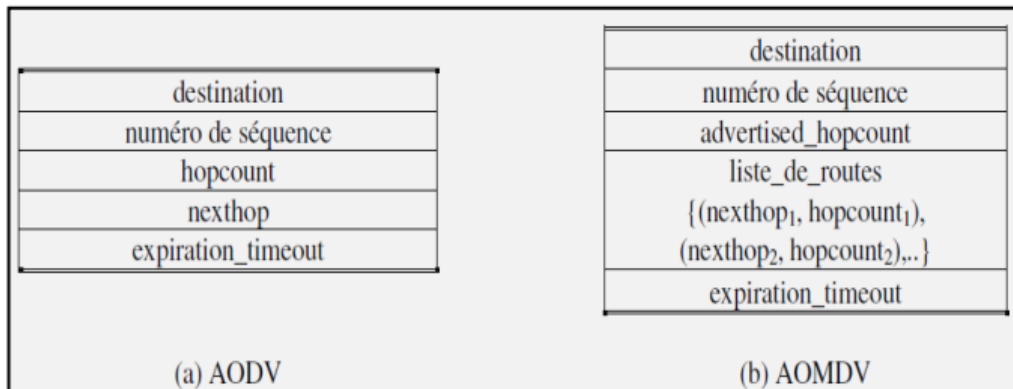


Figure III-2: structure des table de routage dans AOMDV et AODV.

III.2.2.2 Recherche des chemins disjoints :

AOMDV ajoute un nouveau champ appelée Firsthop pour chaque paquet RREQ. Ce champ indique le premier saut qui signifie le voisin de la source qui l'acheminée. En plus, chaque nœud maintient une liste, Firsthop_list, pour chaque RREQ afin de garder une trace de la liste des voisins de la source à partir desquels une copie de RREQ a été reçue. Une seule copie de chaque RREQ est rediffusée par chaque nœud intermédiaire. Cependant, chaque nœud intermédiaire X conserve en mémoire plusieurs voisins ayant transmis une copie de RREQ dans la mesure que les FirstHop de ces copies sont distincts. Ceci garantit que X connaît plusieurs chemins à nœuds disjoints pour retourner à la source. En effet, deux chemins distincts dès le début ne peuvent converger dans la mesure où chaque nœud intermédiaire ne retransmet qu'une seule copie de RREQ. Le nœud destination répond à K copies d'une RREQ en provenance d'un même voisin en envoyant une réponse de route RREP. Chaque réponse de route RREP est ensuite retransmise par chaque nœud intermédiaire à l'un des voisins enregistrés dans sa table de routage. Si plusieurs requêtes arrivent à un même nœud, ce dernier prend soin de les diriger vers des voisins distincts. De ce fait, les chemins suivis par les RREPs sont disjoints.

III.2.3 Maintien de la route :

Une nouvelle découverte de route est nécessaire uniquement lorsqu'aucune des routes précédemment établies n'est valide. Lorsqu'aucune route vers la destination n'est valide, le nœud envoie un paquet d'erreur RERR a tous ses voisins qui utilisent ce nœud comme prochain saut dans la route vers cette destination. Ces routes sont effacées des tables de routage des nœuds récepteurs de ce paquet d'erreur. En revanche, contrairement au protocole AODV, ces paquets d'erreur ne sont pas relayés jusqu'à la source. Si la source de trafic reçoit un paquet RERR, elle lance une nouvelle découverte de route dans le cas où elle souhaite toujours émettre [32].

III.2.4 La problématique de AOMDV :

Dans ce protocole lors d'une rupture de liens au niveau de la route principale, à travers laquelle on transmet les données, la source change cette route par une des routes alternatives au lieu de déclencher une nouvelle phase de découverte des routes. Ainsi une nouvelle phase de découverte des routes n'est déclenchée que lorsque toutes les routes multiples alternatives sont rompues. Le problème de ce protocole [35] est que pendant une même phase de découverte des routes, plusieurs routes qui mènent entre une source et une destination sont établies mais uniquement le meilleur chemin en termes de nombre de sauts est sélectionné pour la transmission des données entre une source et une destination. Les autres routes ne seront utilisées que lorsque la première route sélectionnée est rompue. En effet, le calcul et le maintien de plusieurs routes entre une source et une destination exige une occupation plus importante de la table de routage, consomme de la mémoire du nœud et accroît la taille des entêtes des paquets alors qu'on ne bénéficie que d'une seule route pour la transmission ce qui constitue un handicap majeur dans notre contexte.

III.2.5 Caractéristique supplémentaire du AOMDV :

III.2.5.1 EAOMDV ou Energy efficient AOMDV :

Une caractéristique des réseaux ad hoc est qu'un hôte/nœud a généralement une puissance de batterie limitée. Cela signifie que l'indisponibilité d'un nœud à cause de manque d'énergie est très probable. Ceci nous conduit à proposer un AOMDV économe en énergie dans lequel les nœuds qui sont entre la source et la destination sont sélectionnés sur la base de leur énergie résiduelle. Les nœuds doivent donc diffuser leurs niveaux d'énergie à leurs voisins afin que chaque nœud a conscience du niveau d'énergie de ses voisins. Ainsi, si un nœud veut envoyer un paquet il choisira le voisin qui a le plus d'énergie résiduelle [37].

III.2.6 Les avantages et les inconvénients :

✚ Les avantages :

- AOMDV est sans boucle car les boucles sont surmontées en utilisant le numéro de séquence.
- Réduisez le temps de découverte de route et limitez les messages de contrôle dans la découverte de route.

✚ Les inconvénients :

- AOMDV a plus de frais généraux de message lors de la découverte de route en raison d'une inondation accrue et comme il s'agit d'un protocole de routage multi-chemins, la destination répond aux multiples RREQ, ces résultats sont plus longs.
- Un encombrement peut survenir en raison d'un plus grand nombre de messages RREQ et RREP.

III.3 Le protocole AODV « Ad hoc On Demand Distance Vector » :

III.3.1 Définition du AODV :

AODV « Ad hoc On Demand Distance Vector » : est un protocole de routage réactif destiné aux réseaux mobiles, se base sur le principe des vecteurs à distance. Il est libre de boucle auto-démarrant et s'accommode d'un grand nombre de nœuds mobiles, résister à une variété de comportements de réseau tels que la mobilité des nœuds, les pannes de liaison et les pertes de paquets. Le protocole AODV utilise un mécanisme de découverte de route à la demande et les routes sont maintenues grâce à des échanges périodiques entre les nœuds.

III.3.2 Découverte de route [37] :

Un nœud diffuse un RREQ lorsqu'il a besoin d'une route vers une destination et n'en a pas une de disponible. Ceci peut se produire si la route vers la destination est inconnue ou si une route précédemment valide expire. Après avoir diffusé une RREQ, le nœud attend un RREP. Si la réponse n'est pas reçue dans un certain délai, le nœud peut rediffuser le RREQ ou supposer qu'il n'y a pas de route vers la destination [38].

L'acheminement des RREQ est effectué lorsque le nœud recevant un RREQ n'a pas de route vers la destination. Il rediffuse ensuite le RREQ. Le nœud crée également une route inverse temporaire vers l'adresse IP source dans sa table de routage avec le saut suivant égal au champ d'adresse IP du nœud voisin qui a envoyé le diffuser RREQ. Ceci est fait pour garder une trace d'un itinéraire vers le nœud original faisant la demande, et peut être utilisé pour un éventuel RREP pour retrouver son chemin vers le nœud demandeur. Cette route est temporaire dans le sens qu'elle est valable pour une durée beaucoup plus courte, qu'une entrée de route réelle.

Lorsque le RREQ atteint un nœud qui est le nœud de destination ou un nœud avec une route valide vers la destination, un RREP est généré et retourné au nœud demandeur. Pendant que ce RREP est transmis, une route est créée vers la destination et lorsque le RREP atteint le nœud source, ce dernier aura une route vers la destination.

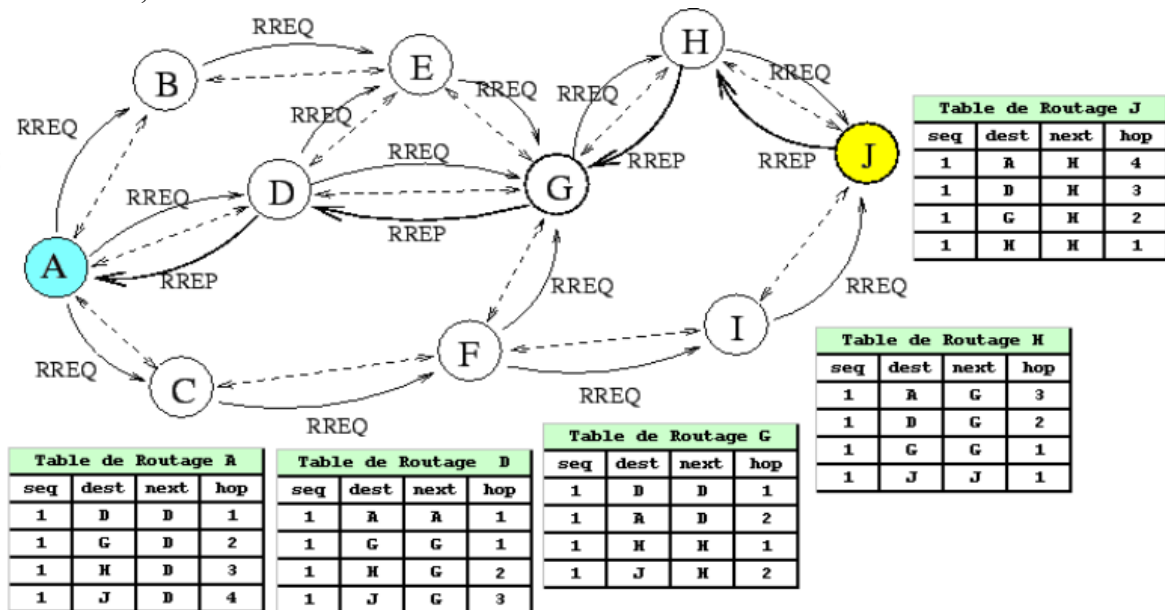


Figure III-3: Schéma montrant le fonctionnement du protocole Aodv.

III.3.3 Maintenance de la route :

Lorsqu'un nœud détecte qu'une route vers un voisin n'est plus valide, il supprime l'entrée dans la table de routage et envoie un message de type "Link error message", informant les voisins que cette route n'est plus valide. À cette fin, AODV utilise une liste de voisins actifs pour connaître les voisins qui utilisent une route particulière. Les nœuds qui reçoivent ce message répèteront cette procédure. Le message sera éventuellement reçu par les sources affectées qui peuvent choisir d'arrêter d'envoyer des données ou demander une nouvelle route en envoyant un nouveau RREQ [38].

III.3.4 Les avantages et les inconvénients :

✚ Les avantages :

- Il utilise un numéro de séquence dans les messages.
- Rappel de l'adresse IP du nœud origine dans chaque message.

✚ Les inconvénients :

- Il n'existe pas de format générique des messages. Chaque message a son propre format : RREQ, RREP, RERR.

III.4 Le protocole DSDV « Destination-Sequenced Distance Vector » :

III.4.1 Définition du DSDV :

DSDV « Destination-Sequenced Distance Vector » : ce protocole a été conçu spécialement pour les réseaux mobiles il est basé sur l'algorithme distribué de Bellman-Ford en rajoutant quelques améliorations. Les nœuds maintiennent une certaine connaissance de la topologie du réseau à travers une table de routage indiquant les routes possibles vers chaque destination, le nombre de sauts nécessaire pour atteindre la destination et le numéro de séquences qui correspond à un nœud destination. La mise à jour de la table de routage dépend des deux paramètres qui sont la période de transmission et les événements. La mise à jour du paquet contient le nouveau numéro de séquence incrémenté du nœud émetteur ainsi que l'adresse de la destination, le nombre de sauts et le numéro de séquence tels qu'ils ont été écrits par la destination pour chaque nouvelle route. Le DSDV élimine les deux problèmes de boucle de routage "routing loop", et celui du "counting to infinity". Ainsi, La Figure 1.7 illustre un exemple d'un réseau Ad hoc constitué de 5 nœuds (de R1 à R5) et le Tableau 1.1 montre la table de routage du nœud R1 [12].

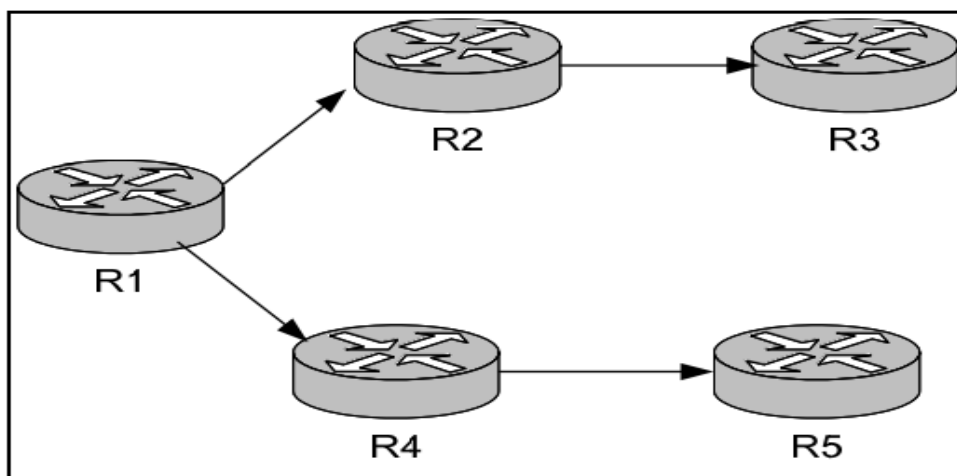


Figure III-4 : Exemple de réseau mobile Ad hoc.

Tableau III-1 : La table de routage du nœud R1.

Destination	Nombre de sauts	Prochain nœud	Numéro de séquence
R1	0	R1	1
R2	1	R2	4
R3	2	R2	5
R4	1	R4	6
R5	1	R5	3

III.4.2 Mécanismes de création des routes :

La table de routage de chaque nœud dans le protocole DSDV doit contenir la liste de toutes les destinations possibles ainsi que le nombre de hop pour les atteindre. Chaque route vers une destination est décrite par un numéro de séquence. Comme le réseau est mobile, les changements de topologie doivent être pris en considération dans les tables de routage. Pour cela, chaque nœud doit transmettre de façon périodique à tous ses voisins l'information sur sa table de routage et, surtout, chaque nouvelle mise-à-jour de celle-ci. Le processus de transmission des mises-à-jour est géré par le protocole DSDV de façon à apporter au nœud une connaissance quasiment continue de la topologie qui l'entoure. À chaque fois qu'un nœud détecte une nouvelle information sur la topologie (du fait d'un déplacement d'un nœud, nouvelle route vers une destination, nouveau numéro de séquence, ...), cette information est propagée après un certain délai. Ce délai est choisi comme décrit de telle façon à ne pas se précipiter pour propager cette information au cas où une meilleure mise-à-jour arrive juste après. De cette manière, le débit des mises-à-jour est limité. Les paquets de mises-à-jour contiennent des informations sur l'adresse de la destination, le nombre de hop nécessaires pour l'atteindre, et le numéro de séquence de cette destination. Chaque nœud partage sa table de routage avec le réseau, où il inclut son numéro de séquence. Comme les tables de routage pourraient dépasser la taille limite des paquets du Protocole, le protocole DSDV prévoit d'envoyer les tables de routage en plusieurs séquences. Les modifications à ces tables de routage sont envoyées sous forme de mises-à-jour.

III.4.3 Mécanismes de maintenance des routes :

Un numéro de séquence d'une destination servira à sélectionner la meilleure route vers celle-ci. En effet, le numéro de séquence le plus récent détermine généralement la meilleure route. En effet, il faut que le nœud qui reçoit ce numéro de séquence tienne compte d'un certain délai d'attente avant d'adopter cette route pour cette destination. Le nombre de hop est utilisé pour sélectionner la meilleure route entre les routes ayant le même numéro de séquence pour la même destination. Le numéro de séquence d'une destination peut servir à déterminer si la route est encore praticable ou pas. En effet, tous les numéros de séquences sont des chiffres pairs. Un nœud qui ne peut plus atteindre une destination, propage un nouveau numéro de séquence de celle-ci et qui est un chiffre impair. Ainsi, chaque nœud qui reçoit ce nouveau numéro de séquence pour cette destination conclut que cette route n'est plus valide et propage encore cette nouvelle mise-à-jour à ses voisins.

III.4.4 Les avantages et les inconvénients :

+ Les avantages :

- Il élimine les deux problèmes de boucle de routage "Routing Loop", et celui du "Counting to infinity".
- Utilise une mise à jour périodique et basée sur les événements.

+ Les inconvénients :

- 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, dans la table de distance. Ce qui fait que le DSDV est lent.
- Il cause un contrôle excessif dans la communication.

III.5 Comparaison entre les protocoles AOMDV, AODV et DSDV [39] :

* Débit :

AOMDV affiche un meilleur débit que AODV à chaque temps de pause, ainsi qu'il est faible dans DSDV.

*Paquets abandonnés :

Avec l'augmentation du temps de pause, Le nombre de paquets abandonnés dans AOMDV et DSDV est très faible par rapport à AODV.

*Taux de livraison des paquets :

Un très petit changement dans le rapport de livraison de paquets d'AOMDV est observé. Ainsi, AOMDV a un meilleur taux de livraison de paquets que AODV en raison de la disponibilité de plusieurs chemins, par contre dans le protocole DSDV il est fiable.

*Frais généraux de routage :

Le temps de pause varie à nouveau et les résultats montrent que la surcharge de routage diminue à un temps de pause plus faible mais augmente à un temps de pause plus élevé pour les deux protocoles, mais AOMDV a une surcharge de routage faible à chaque temps de pause par rapport aux protocoles AODV et DSDV.

*Délai de bout en bout :

Avec l'augmentation du temps de pause (de la mobilité élevée à la mobilité faible), le délai de bout en bout augmente pour les deux protocoles, mais AOMDV a toujours un délai de bout en bout inférieur à celui de l'AODV.

* Longueur de chemin optimale :

AOMDV a une meilleure longueur de chemin optimale que AODV avec un temps de pause croissant.

* Retard :

Le retard dans AOMDV est légèrement et semblable à AODV et DSDV.

III.6 Conclusion:

Dans ce chapitre nous avons étudié les trois protocoles de routage AOMDV, AODV et DSDV dans les réseaux ad-hoc. Nous avons cité les stratégies utilisées dans l'acheminement des données entre les différentes unités mobiles. Dans ce qui suit nous allons présenter la simulation de ses derniers protocoles avec le résultat obtenu.

IV Simulations et évaluation des performances.

IV.1 Introduction :

La simulation est une démarche clé dans le processus de développement des protocoles qui permet l'évaluation des performances d'une nouvelle approche avant son implémentation réelle.

Dans ce chapitre, on vise à évaluer le protocole AOMDV en analysant les performances résultantes après son intégration dans le simulateur. et on va présenter les simulateurs réseaux les plus répandus à l'instar de NS2, NS3 et OMNET++ et enfin le comparer avec les deux protocoles AODV et DSDV et souligner les diverses notifications apportées par routage multi-chemin avec équilibrage de charge de point de vue performance et répartition de charge du réseau.

IV.2 Les différents outils des simulations :

Il existe plusieurs simulateurs de modèles de nœuds ou de réseaux virtuels. Nous allons présenter et étudier quelques outils les plus connus et les plus utilisés [40].

IV.2.1 Le simulateur ns2 :

NS2 (Network Simulator 2) est un logiciel de simulation multicouche. Le simulateur NS-2 fonctionne en combinaison avec différents outils de développement et langages, principalement, les langages orientés objets et de script, C++ et OTcl sont utilisés. Le C++ est utilisé pour développer et implémenter des algorithmes et des opérations de bas niveau alors que l'OTcl est utilisé pour les codes scripts des scénarios externes de simulations.

IV.2.2 Le simulateur ns-3 :

NS3 (Network Simulator 3) est un logiciel libre et open source, Successeur de ns-2, plus performant que ns-2. Il est composé d'un code C++ pour l'implémentation de modèles de simulation. Ns-3 n'utilise pas le script oTcl pour le contrôle des changements dans le réseau, plus rapide en terme d'exécution.

IV.2.3 Le simulateur OMNET++ :

OMNET++ (Objective Modular Network Testbed in C++) est un simulateur à événements discrets orienté objet, basé sur C++ Il a été conçu pour simuler les systèmes réseaux de communication, les systèmes multi processeurs, et d'autres systèmes distribués, ... OMNET++ est utilisé pour l'analyse de performance et l'évaluation de protocoles de communication. Sa licence est gratuite pour les universitaires et pour toute utilisation non lucrative.

IV.2.4 Le simulateur J-SIM :

J-SIM (Java simulator) est un simulateur de temps réel axé sur les processus, il permet de simuler des réseaux de l'ordre de 1000 nœuds. J-Sim a été conçu pour soutenir les langages de script (Tcl, Perl ou Python), J-Sim comprend la plateforme INET qui est dédié à la simulation des réseaux, J-Sim est un logiciel gratuit de mise en œuvre de charge pour la simulation d'une architecture à base de composants.

IV.2.5 Le simulateur Glomosim :

GlomoSim (Global mobile simulateur) permet la simulation d'environnement à grande échelle pour des réseaux sans fil et filaires. Il est capable de simuler un réseau purement sans fil avec tous les protocoles de routage que cela inclus (AODV, DSR, ODMRP, WRP, FSR).

IV.3 Domaine d'utilisation de Ns2 et Ns3 :

Les deux simulateurs de réseaux ciblent un même domaine d'utilisation qui est : « la recherche et l'éducation ». Ce domaine-là apparaît par exemple dans la mise en place d'une topologie qui n'a pas encore été testée et de pouvoir modifier ses paramètres tout comme ces simulateurs sont utilisés pour tester de nouveaux protocoles avant de les utiliser réellement [40].

IV.4 Le choix de NS2 :

NS-2 est utilisé sous un environnement Linux. Certains membres de l'équipe utilisent Cygwin pour utiliser NS-2 sous Windows. Le logiciel doit donc être compatible avec Unix et Windows. Le choix s'est donc porté sur Java. Ce langage en plus d'être multiplateforme dispose de nombreuses API répondant à nos besoins. La partie principale de l'application est la création graphique de la topologie. L'ergonomie étant très importante, l'utilisation d'un module graphique complet est nécessaire. L'API JGraph présente ces caractéristiques. Ce composant permet de créer des diagrammes, des graphes à état, ou toute sorte de graphe basé sur des principes de nœuds et de liens. De plus les entités peuvent prendre n'importe quelle forme afin de correspondre aux besoins du développeur. Cette API dispose de fonctions de sauvegarde qui ne seront pas utilisés puisque le logiciel a besoin de stocker d'autres informations propres à chaque entité. Pour la gestion des sauvegardes de graphes ainsi que des sauvegardes de configuration le choix s'est porté sur l'utilisation de Extensible Markup Language (XML). L'API retenue pour cette tâche est JDom, car cette API propose une interface d'exploitation simple [40].

IV.5 Présentation du NS 2

IV.5.1 Définition :

Le Network Simulator 2 est un ensemble d'outils qui simule le comportement du réseau, il permet de créer des topologies réseaux, consigner les événements qui se produisent dans toute charge et aussi d'analyser ces événements afin de comprendre le comportement du réseau. Le simulateur utilise le langage orienté objet OTCL dérivé de TCL pour la description des conditions de simulation sous forme du script en fournissant les caractéristiques des liens physiques, les protocoles utilisés, le type de trafic généré par les sources, les événements, etc. L'observation de ce comportement est se fait via le NAM.

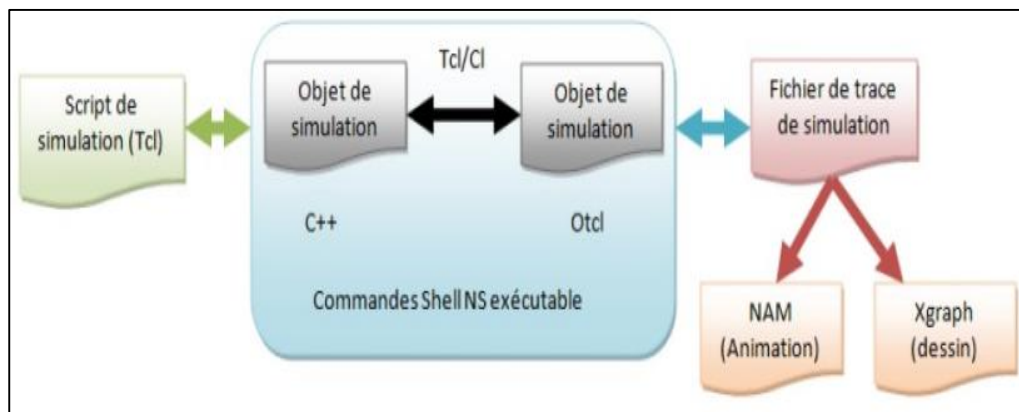


Figure IV-1: Structure du Network Simulator 2.

IV.5.2 Script TCL-OTCL :

TCL est un langage conçu pour une utilisation par un développeur de l'application qui peut être participé à travers une demande ou pourrait être utilisé par une application de diverses manières, Ce langage à typage dynamique est multiplateforme, extensible, facile à apprendre. Tcl s'interface très aisément avec le langage C, ce qui lui permet de servir par exemple d'interprète embarqué dans des applications. L'OTCL est un TCL avec les extensions orientée objet.

NS2 utilise OTCL pour le programmeur de simulation pour créer les objets de réseau dans la mémoire et d'insérer des événements initiaux dans la file d'attente de l'événement [40].

IV.5.3 NAM :

NAM est un outil de visualisation qui présente deux intérêts principaux : représenter la topologie d'un réseau décrit avec NS-2, et afficher temporellement les résultats d'une trace d'exécution. NS-2 Il prend en charge la topologie mise en page, l'animation au niveau du paquet, et divers outils de contrôle de données. Cette visualisation fournit une représentation du graphe du réseau sur laquelle on peut voir les paquets circuler, les paquets rejetés d'une file d'attente et observer le débit courant des liaisons.

IV.5.4 Avantages :

- Observations des états des systèmes.
- Études des points de fonctionnement d'un système.
- Études de systèmes à échelle de temps variable.
- Études de l'impact des variables sur les performances du système.
- Étude d'un système sans les contraintes matérielles.

IV.5.5 Inconvénients :

- La conception de modèles peut nécessiter des compétences spéciales.
- Une autre forme d'analyse plus proche de la réalité est peut-être nécessaire.
- Résultats difficilement interprétables.
- Résultats pas forcément généralisable.
- Résultats sont en fonction des entrées du système.

IV.6 Présentation de logiciel Gnu plot :

Gnuplot est un programme de tracé de fonctions et de données en lignes de commande. Ce logiciel "libre" permet de tracer très rapidement des courbes à partir d'une équation, ou de tableaux de données. Pour démarrer gnuplot, il suffit de taper gnuplot en ligne de commande. On obtient alors la bannière, suivie de l'invite : gnuplot>. Le logiciel attend alors les commandes.

IV.6.1 La commande plot :

Plot est la commande qui permet de faire des tracés de courbes. Vous pouvez accéder à sa documentation avec *help plot*.

L'autre grande utilisation de Gnuplot est le tracé de courbes de données qui sont traité dans un fichier data. Par exemple, le fichier se nommera "aomdv.dat". On peut tracer un courbe avec la commande suivante :

```
> plot "aomdv_09.dat" with lines
```

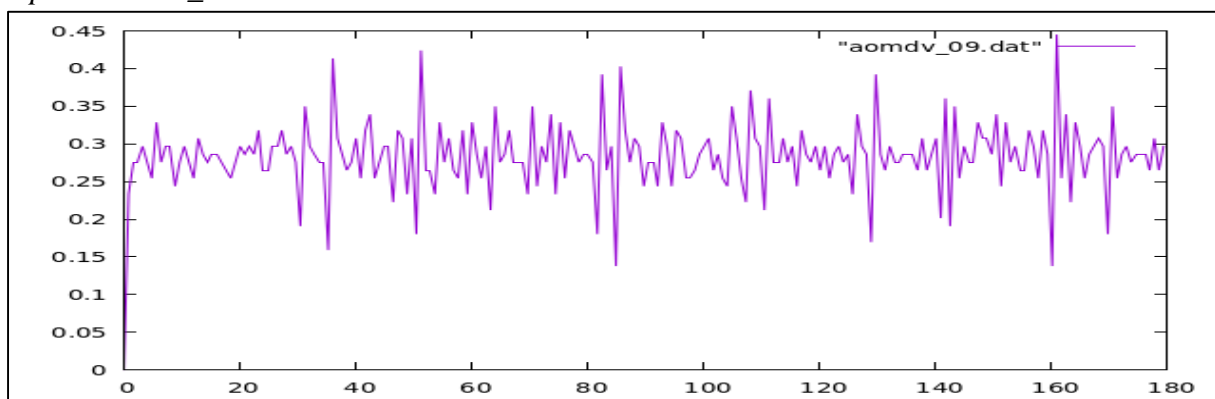


Figure IV-2: exemple de courbe de AOMDV.

Remarquons que l'on peut tracer simultanément deux courbes en utilisant la commande `plot` et en séparant les deux courbes par une virgule. Par exemple:

```
>plot "aomdv.dat " using 1/2 title "aomdv" with lines, "aodv.dat" using 1/2 title "aodv" with lines
```

IV.6.2 La commande `set` :

La commande `set` permet de régler l'allure du dessin, et aussi de choisir la cible dans laquelle on va le placer. Elle permet de régler un très grand nombre d'options et de paramètres par défaut de Gnuplot. Les commandes suivantes permettront de donner des titres :

```
>set xlabel "titre de l'axe des x"
```

```
>set ylabel "titre de l'axes des y"
```

```
>set title "analyse de aomdv" (voire la figure IV-3).
```

IV.7 Étude de performance du protocole AOMDV :

IV.7.1 Les fichiers du protocole AOMDV :

Dans cette partie, nous présentons les fichier d'implémentation du protocole de routage AOMDV dans le simulateur NS-2.

L'implémentation du protocole AOMDV se trouve sous le répertoire :
`hp@hp-HP-15-Notebook-PC:~/ns-allinone-2.35/ns-2.35/aomdv.`

Le dossier `aomdv` contient les fichiers suivants :

- `aomdv.h` : le fichier d'entête principal dans lequel sont définis les procédures de routage et les fonctionnalités du protocole.
- `aomdv.cc` : c'est le fichier principal qui contient l'implémentation des procédures du fonctionnement du protocole, ainsi que les fonctionnalités de routage.
- `aomdv_packet.h` : ici sont déclarés tous les types des paquets qu'utilise AOMDV dans les échanges entre les nœuds du réseau.
- `aomdv_rqueue.h` : ce fichier définit la file d'attente utilisée par le protocole et la déclaration de différentes fonctions utilisées pour la manipulation de cette file.
- `aomdv_rqueue.cc` : il contient l'implémentation de la file d'attente.
- `aomdv_rtable.h` : le fichier d'entête où la table de routage est déclarée.
- `aomdv_rtable.cc` : implémentation de la table de routage.

IV.7.2 Paramètres de configuration :

Tableau IV-1 : paramètre de configuration dans le fichier.TCl.

Paramètres	Valeur
Type Channel	Channel/wirelesschannel
Modèle de propagation radio	Propagation/ TwoRayGround
Type d'interface réseau	Phy/WirelessPhy
Couche MAC	Mac/802_11
Type de file d'attente	Queue/DropTail/PriQueue
Type de couche de liaison	LL
Modèle d'antenne	Antenna/OmniAntenna
Paquet max dans ifq	50
Nombre de nœud	10-20
Protocole de routage	AOMDV / AODV / DSDV
Surface de réseau	1000*1000
Temps de la simulation	180
Paramètre simulé	débit

IV.7.3 Scénarios de simulation :

IV.7.3.1 Simulation 1 : Étude par rapport trois protocole AOMDV, AODV et DSDV.

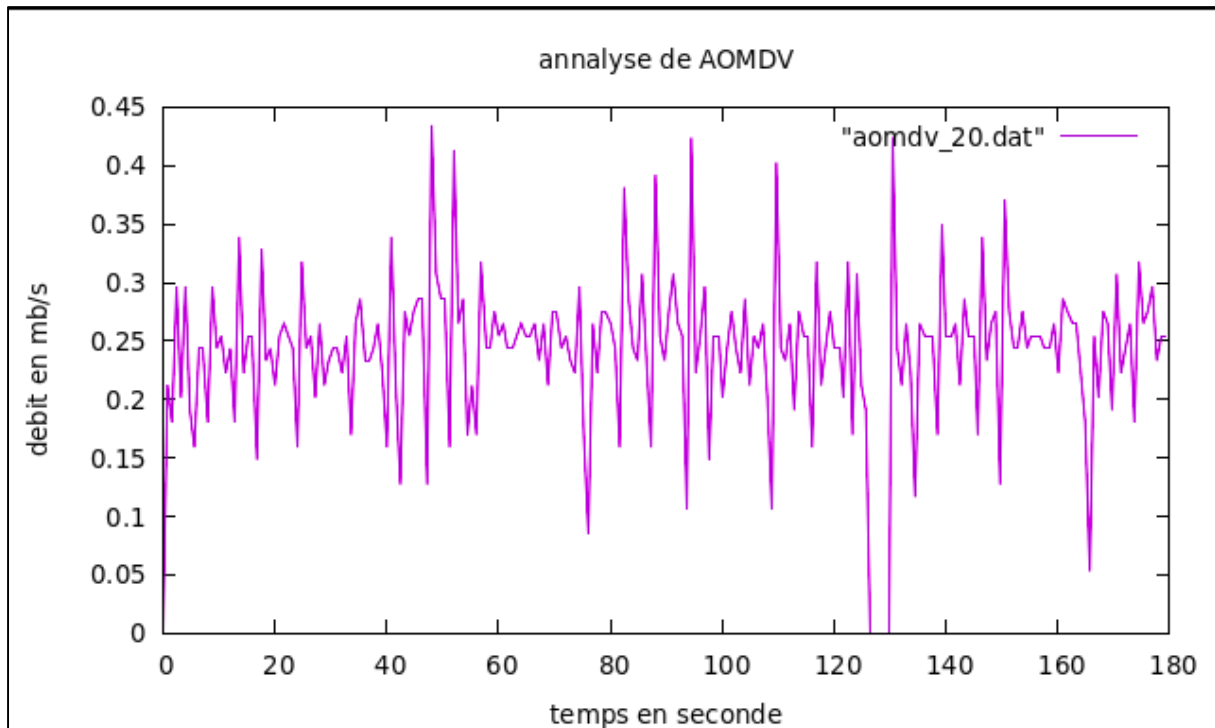


Figure IV-3 : le débit du protocole AOMDV.

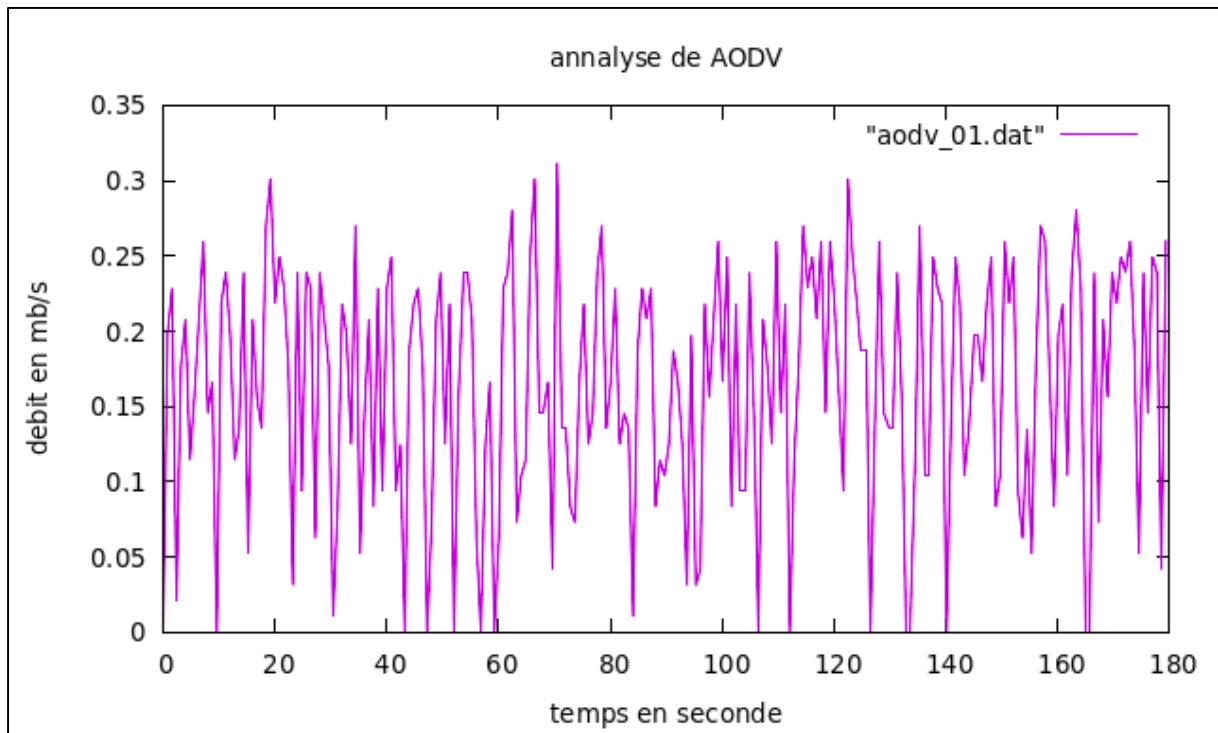


Figure IV-4 : le débit du protocole AODV.

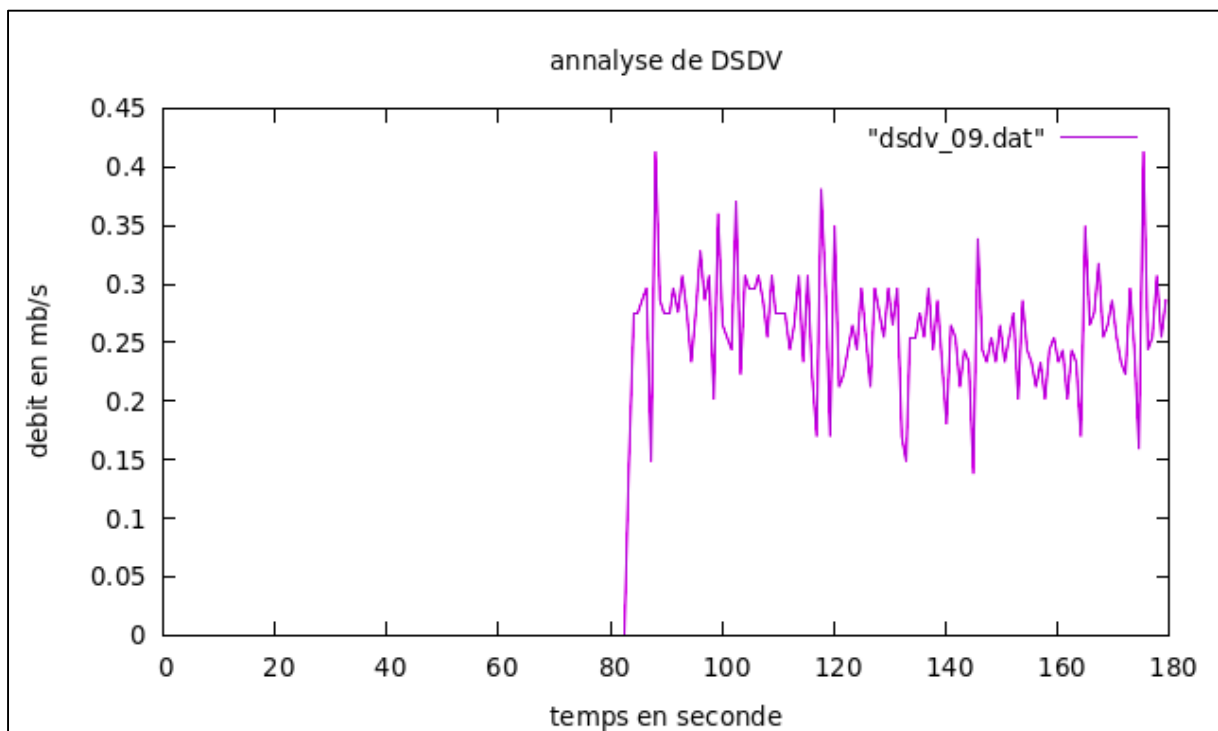


Figure IV-5 : le débit du protocole DSDV.

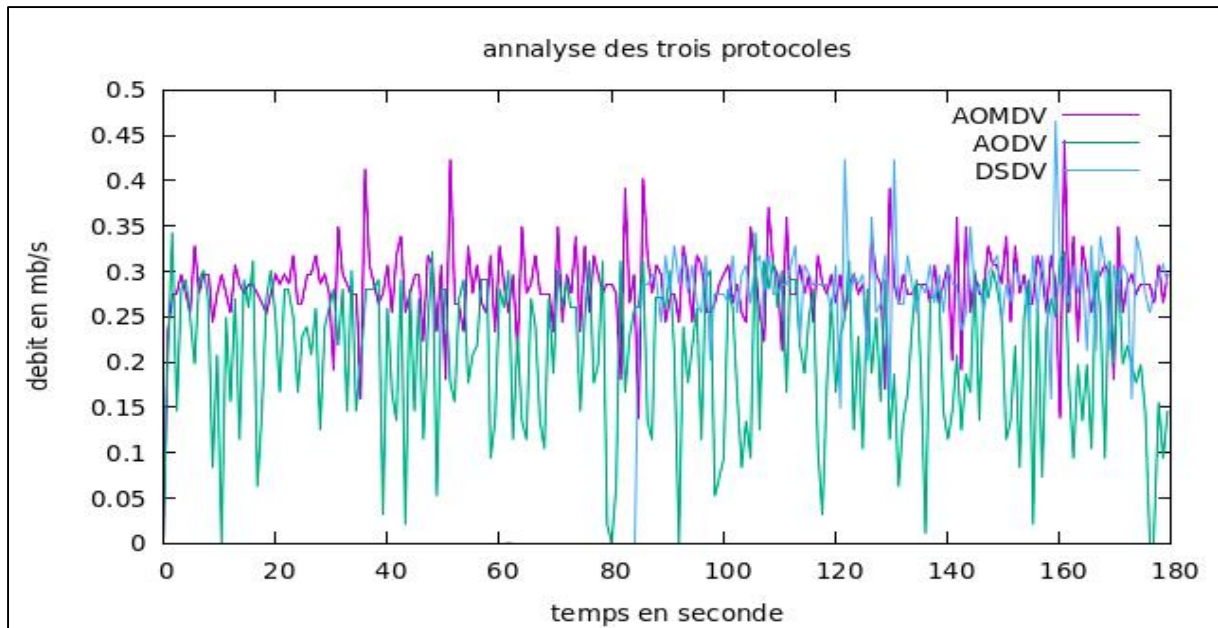


Figure IV-6 : la comparaison entre les trois protocoles.

La figure IV-5 montre une comparaison entre les trois protocoles (AOMDV, AODV et DSDV). Au début de la simulation les débits des deux protocoles AOMDV et AODV sont très élevés par rapport au DSDV car le protocole DSDV attend la création de sa table de routage mais une fois créée, d'après le graphe, les débits des protocoles DSDV et AOMDV sont presque les mêmes et ils sont plus performants par rapport à AODV.

IV.7.3.2 Simulation 2 : Étude par rapport à la distance entre l'émetteur et le récepteur.

Nous allons faire une simulation du protocole AOMDV par rapport à la distance entre l'émetteur et le récepteur :

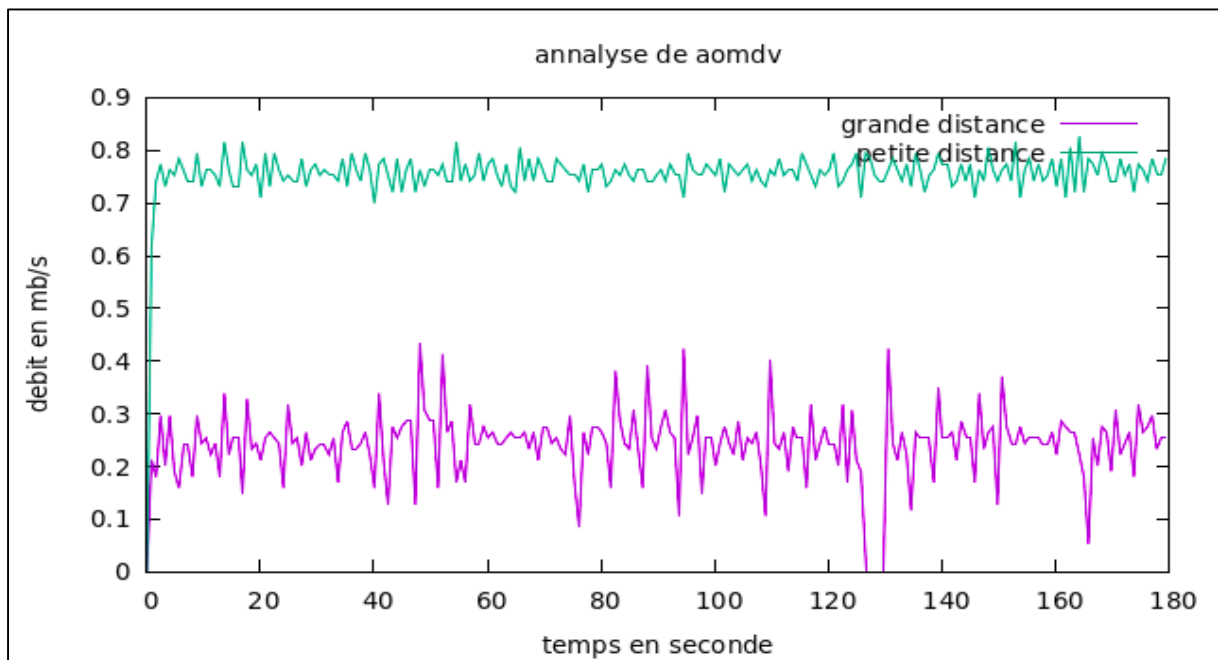


Figure IV-7: le débit du protocole AOMDV avec grande/petite distance entre l'émetteur et récepteur.

La figure IV-6 montre la comparaison en fonction de la grande distance et petit distance entre l'émetteur et le récepteur en remarque que le débit du protocole AOMDV est plus performant si la distance entre l'émetteur et le récepteur est petite.

IV.7.3.3 Simulation 3 : Étude par rapport au nombre de nœuds.

Dans cette simulation, le nombre de nœuds varie (cas 1 : avec 10 nœud et cas2 : avec 20 nœud) :

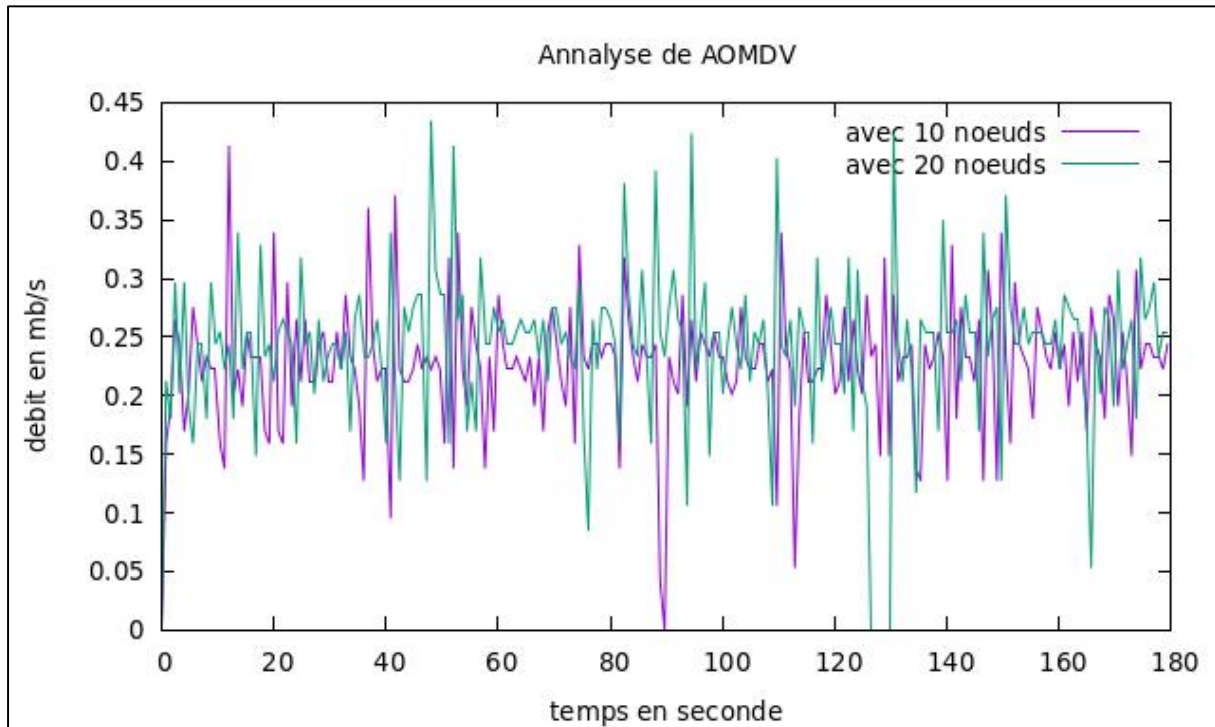


Figure IV-8 : le débit du protocole AOMDV en fonction de nombre de nœuds.

La figure IV-6 montre que le débit de protocole aomdv est plus performant si le nombre de nœuds est grand.

Conclusion :

Dans ce chapitre nous avons cite en premier lieu les différents outils de la simulation dans les réseaux MANETs, ensuite nous avons décrit les avantages et les inconvénients du choix du ns2 comme étant un bon simulateur. Aussi nous avons étudié les performances de protocole de routage AOMDV et enfin les résultats de simulation a montré l'efficacité du protocole proposé

Conclusion générale :

La technologie ad hoc présente une évolution dans la communication numérique. L'auto-organisation associée à la robustesse et la fiabilité des liens établis donnent la possibilité d'exploiter cette technologie dans divers domaines (le domaine militaire, le domaine industriel, etc...).

Le niveau de routage est un des niveaux à considérer lors du déploiement de cette technologie. L'autonomie et la mobilité caractérisant les nœuds dans le réseau ad hoc imposent aux protocoles de routage d'épouser l'aspect distributif et le dynamisme de la topologie. Plusieurs approches ont été proposées afin de garantir une convergence de données et le choix optimal des trajets. L'approche proactive avec ses mécanismes de mise à jour périodique vise à fixer toutes les routes optimales vers tous les autres nœuds dans le réseau et à rendre le tableau de routage disponible à tout moment. L'approche réactive avec son mécanisme de recherche de route sous demande a pour but de réduire la charge de trafic de contrôle dans le réseau. L'approche hybride essaye de combiner les mécanismes des approches réactives et proactives afin de créer plus de flexibilité face aux changements imprévisibles dans le réseau ad hoc.

L'objectif de ce mémoire était l'étude des du protocole de routage réactif AOMDV et l'intégrer dans le simulateur. Une étude performances comparative qualitative a été effectuée dans le but de garantir le bon choix. La sélection a été basée sur les critères les plus importants caractérisant la qualité de déploiement de la technologie ad hoc. Ces critères sont le taux de paquets livrés, le délai de bout en bout, le volume de trafic de contrôle, la longueur de route, le débit et le taux de perte de paquets. Après une analyse des différents scénarios et des conclusions tirées sur les trois protocoles AODV, AOMDV, DSDV nous constatons que le protocole AOMDV améliore considérablement les performances du réseau en termes du délai d'acheminement de données par rapport à AODV tout en assurant un taux de livraison des paquets de données acceptables.

Nous aurions aimé approfondir notre recherche dans ce sujet, mais le temps attribué à la réalisation de notre travail est insuffisant, en plus de notre expérience de débutante dans l'utilisation de l'outil NS2. Notre ambition reste grande à vouloir continuer ce travail

Bibliographie :

- [1] Mounir Frikha. Réseau Adhoc. Paris.2010,263p
- [2] Daniel mabele Mondonga, https://www.memoireonline.com/05/12/5873/m_etude-sur-les-protocoles-de-routage-d-un-reseau-sans-fil-en-mode-adhoc-et-leurs-impacts-cas-de10.html
- [3] Haas(z.), Gerla (M.), Johnson(D), perkins (C.), pursley (M.), Steenstrup (M.) et toh (C.).
_Spécial issue on Wireless Adhoc networks. IEEE journal on selected Areas in communication, Vol.17, N :8,1999
- [4] TAHAR ABBES Mounir, Proposition d'un protocole a économie d'énergie dans un réseau hybride GSM et ad hoc, présenté pour obtenir le diplôme doctorat Spécialité informatique, université d'Oran 2011-2012.
- [5] M. Mehdi, A. Anou. S. Zair, M. Djebari, « la sécurité dans les réseaux adhoc, université Blida .2007
- [6] Abdelhamid Zebdi, Nouveau protocole de routage Multicast pour les réseaux adhoc mobiles basé sur les zones denses, université de Québec,2006
- [7] H. Liu, X, Jia-WAN, « On Energy efficiency in Wireless Adhoc networks », Book chapter on: Adhoc and Sensor Networks, ISBN :1-59454-396-8, Nova sciences Publishers, Inc., pp-31-54,2006
- [8] Toh, C K. 2002. Ad Hoc Mobile Wireless Networks Protocols and systems: Age of Pervasive Mobile Networks and Computing Upper Sadde River: Prentice Hall
- [9][e] YOUNES, Nadine, LA QUALITÉ DE SERVICE DES SERVICES MULTIMÉDIA SUR LES RÉSEAUX AD HOC SANS FIL À MULTI-SAUTS, COMME EXIGENCE PARTIELLE À L'OBTENTION DE LA MAÎTRISE EN GÉNIE CONCENTRATION : RÉSEAUX DE TÉLÉCOMMUNICATIONS, UNIVERSITÉ DU QUÉBEC, MONTRÉAL, LE 7 AOÛT 2009.
- [10] <https://waytolearnx.com/2019/06/les-normes-ieee-802.html>
- [11] R. Poovendran, L. Lazos, « Agraph theoretic Framework for preventing the wormhole attack in Wireless networks.
- [12] Younes, Nadine, « la qualité de service des services multimédias sur les réseaux adhoc sans fil a multi-sauts, université de Québec, 2009.
- [13] Saloua Chettibi, Protocole de routage avec prise en compte de la consommation d'énergie pour les réseaux mobile adhoc, université Ouargla ,2012.
- [14] Nadir Boukhchem, Routage dans les réseaux adhoc par une approche a base d'agents mobiles.
- [15] c. Cheng, R. Riley, S. Kumar et J.J. Garcia-Luna-Aceves. ALoop-Free Bellman-Ford Routing Protocole without Bouncing Effect. ACM SIGCOMM'89. Sept 1989.
- [16] Azzedine Boukerche, Begumhan Turgut, Nevin Aydin, Mohammad Z.Ahmad, Ladislau Blni, Damla Turgut, Routing protocols in ad hoc networks : A survey, Computer Networks 55(2011),pp 30 32-3080,2011.
- [17] Henoune Mohammed Mokhtar, La securite des reseaux sans fil, memoire pour obtenir le diplome de magistere Spécialité Informatique Option : Ingénierie des logiciels et des réseaux, université d'Oran, 2010/2011.
- [18] Sabrine NAIMI, Gestion de la mobilité dans les réseaux Ad Hoc par anticipation des métriques de routage, THÈSE DE DOCTORAT, UNIVERSITÉ PARIS-SUD, le 22 juillet 2015
- [19] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein. Dijkstra's algorithm. MIT Press.
- [20] D. Bertsekas and R. Gallager. Data Networks (2nd Ed.). Prentice-Hall, Inc., Upper Saddle River, NJ, USA, 1992.

- [21] T. Clausen, P. Jacquet. «Optimized Link State Routing Protocol». IETF RFC 3626. 2003.
- [22] Karthik Ramakrishnan. « An Improved Model for the Dynamic Routing Effect Algorithm for Mobility Protocol ». Electronic Theses and Dissertations (UW). Appears in Collections: Faculty of Engineering Theses and Dissertations Electronic Theses and Dissertations (UW). 2005.
- [23] Redouane Hamza, Protocoles de routage pour les réseaux ad hoc, Mémoire présenté à la Faculté des études supérieures en vue de l'obtention du grade de Maître ès sciences (M.Sc.) en informatique, Université de Montréal, Novembre 2004, pp 105.
- [24] D.B. Johnson, D.A. Maltz, Y.-C. Hu and J.G. Jetcheva, The dynamic source routing protocol for mobile ad hoc networks, Internet-draft, draft-ietf-manet-dsr-07.txt (February 2002), work in progress.
- [25] Yih-chun Hu and A. Perrig « Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks ». Article de recherche publié dans Computer Engineering & Systems, 2007. ICCES apos; 07. International Conference 27-29 Nov. 2007.
- [26] Vincent D. Park et M. Scott Corson (1997). Temporally-Ordered Routing Algorithm (TORA) Version 1 Functional Specification. Novembre 2011.
- [27] [Boukhechem, 2008] Boukhechem, S. (2008). Contribution à la mise en place d'une plateforme open-source MPSoC sous SystemC pour la Co-simulation d'architectures hétérogènes. PhD thesis, Dijon
- [28] Akram KOUT, Contributions à la Resolution du Problème de Routage dans les Réseaux Mobiles Ad-hoc par les Méthodes Bio-inspirées, THESE Pour l'obtention du diplôme de Docteur en 3 ème cycle LMD Option : Systèmes Complexes, Universite Abdelhamid Mehri - Constantine 2, 02 Juillet 2017.
- [29] Haas (Z.). – A new routing protocol for the reconfigurable wireless networks. Dans: ICUPC, pp. 562–566. – octobre 1997.
- [30] Haas (Z.J.) et Pearlman (M.R.). – The performance of a new routing protocol for the reconfigurable wireless networks. Dans : ICC, pp. 156–160. – juin 1998
- [31] Farid JADDI, CSR : une extension hiérarchique adaptative du protocole de routage ad hoc DSR, le titre de docteur de l'institut national polytechnique de Toulouse, 25/10/2006.
- [32] M. Rahoual, P. Siarry, Réseaux informatique : conception et optimisation, THECNIP, page 117, 2006.
- [33] I. Doghri, "Stratégies de routage multi-chemin dans les réseaux sans FILS multisauts", Thèse de doctorat de l'École Normale Supérieure de Lyon, Mai 2012.
- [34] M. K. Marina et S. R. Das, "Ad hoc on-demand multipath distance vector routing", Wireless Communications And Mobile Computing, pages 969–988, 2006.
- [35] S. MUELLER, P. TSANG, GHOSAL « multipath routing in mobile Ad Hoc networks: Issues and challenges» 2003, info communication.
- [36] KETTOUCHE FERIEL, LATROCHE HASNIA, Protocole de routage multi-chemins EAOMDV avec consommation d'énergie dans les réseaux sans fil Ad Hoc, UNIVERSITE ABDELHAMID IBN BADISMoustaganem,2012/2013,52p
- [37] EAOMDV ou Energy efficient AOMDV,
https://www.academia.edu/36979883/Contribution_à_la_QoS_dans_le_protocole_AOMDV
- [38] Prashant Kumar Maurya, Gaurav Sharma, Vaishali Sahu, Ashish Roberts4, Mahendra Srivastava, "An Overview of AODV Routing Protocol", International Journal of Modern Engineering Research (IJMER) Vol.2, Issue.3, May-June 2012 pp-728-732.
- [39] METRICS FOR PERFORMANCE COMPARISION,

<https://www.ijert.org/simulation-and-comparision-of-aodv-and-aomdv-routing-protocols-in-manet>

[40]Le choix de ns <https://pdfslide.net/reader/f/simulation-dun-reseau-ad-hoc-sous-ns2>