

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Abderrahmane Mira de Bejaia

Faculté des Sciences Exactes
Département d'Informatique



MÉMOIRE DE FIN D'ÉTUDES

En vue de l'obtention du diplôme d'un Master en Informatique
Option : Administration et Sécurité des Réseaux

Thème

**Protocole réactif versus protocole proactif
dans les réseaux sans fil ad hoc**

Soutenues devant le jury composé de :

Réalisé par :

Président : Mr BAADACHE.Abderrahmane

M^{elle} BELGHAZI Samira

Examineur : Mr SAADI Mustapha

M^{elle} MAHDID Souria

Encadré par : Mr MEHAOUED Kamal

Promotion : 2015/2016

Remerciements

*En premier lieu, nous remercierons le Bon **DIEU** de nous avoir donné la force, le courage et la santé pour accomplir ce travail avec succès.*

Au terme de ce modeste travail nous tenons à remercier chaleureusement et respectivement nos familles, surtout nos parents qui nous ont épaulées, soutenues et suivies tout au long de ce projet.

A nos chères amies qui ont toujours été présents et fidèles.

*Ensuite nos remerciements iront à notre encadreur Monsieur **MEHAOUED. Kamal**, pour son soutien durant tout notre mémoire et nous le remercions pour ses remarques et suggestions. Il a toujours su nous consacrer des moments de son temps, nous guider, nous conseiller.*

Tout notre respect et nos remerciements vont vers les membres du jury qui ont consacré pleinement leur temps et leur attention afin d'évaluer notre travail, qui espérons le sera à la hauteur de leur attente.

Enfin, pour toute personne qui a contribué, de près ou de loin, à l'élaboration de ce mémoire. Veuillez bien trouver ici l'expression de nos sincères remerciements.

Dédicaces

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

Mes frères Samir, Fatah et Slimane et Mes sœurs Hassiba, Kahina, Djamilia et
Lamia et ma cousine salima

Et à mes chères amies Warda, Rosa, Nawal et Lila.

Et un grand remerciement à Samir

BELGHAZI Samira

Dédicaces

A ceux que j'aime surtout aux plus chères personnes du monde, mes parents qui ont toujours souhaité ma réussite.

Mes dédicaces s'adressent aussi à mes chères sœurs ainsi que mes chères frères.

A toute la famille MAHDID.

A tous mes amis .

Merci à vous tous.

MAHDID Souria

Table des matières

Table des Matières	i
Liste des figures	iv
Liste des tableaux	v
Liste des abréviations	vi
Introduction générale	1
1 Généralités sur les réseaux mobiles ad hoc	3
1.1 Introduction	3
1.2 Architectures des réseaux sans fil	3
1.2.1 Architecture avec infrastructure	3
1.2.2 Architecture sans infrastructure (Ad Hoc)	4
1.3 Présentation des réseaux mobiles ad hoc	4
1.3.1 Historique	4
1.3.2 Définition d'un réseau Ad Hoc	5
1.3.3 Modélisation d'un réseau mobile ad hoc	5
1.3.4 Mode de communication dans les MANETS	6
1.4 Types des réseaux Ad hoc	6
1.4.1 Les réseaux de capteurs WSNs (Wireless Sensor Networks)	6
1.4.2 Les réseaux maillés WMNs (Wireless Mesh Networks)	7
1.5 Caractéristiques des réseaux Ad Hoc	7
1.6 Contraintes spécifique aux réseaux ad hoc	8
1.7 Domaines d'applications des réseaux mobiles Ad Hoc	9
1.8 Avantages et inconvénients des réseaux Ad Hoc	9

1.9	Conclusion	11
2	Routage dans les réseaux Ad Hoc	12
2.1	Introduction	12
2.2	Définition du routage	12
2.3	Problématiques de routage dans les réseaux Ad Hoc	12
2.4	Contraintes de routages dans les réseaux ad hoc	13
2.5	Techniques de routage	14
2.5.1	Routage hiérarchique ou plat	14
2.5.2	Routage à la source et le routage saut par saut	15
2.5.3	Routage à état de lien et à Vecteur de distance :	15
2.5.4	L'inondation	15
2.6	Classification de protocoles de routage	16
2.6.1	Définition	16
2.6.2	Protocoles de routage proactifs	17
2.6.3	Protocoles de routage réactifs	18
2.6.4	Protocoles de routage hybrides	18
2.7	Conclusion	19
3	Description de protocole de routage AODV ,DSDV et OLSR	21
3.1	Introduction	21
3.2	Etude détaillée des protocoles AODV ,DSDV et OLSR	21
3.2.1	Protocole AODV	21
3.2.2	Protocole DSDV (Dynamic destination Sequenced Distance Vector)	28
3.2.3	Protocole OLSR (Optimized Link StateRouting)	31
3.3	Conclusion	36
4	AODV versus DSDV avec simulation	36
4.1	Introduction	36
4.2	Présentation de Network Simulator 2	36
4.2.1	Définition	36
4.2.2	Architecture du NS2	37
4.3	Simulation et discussion des résultats	38
4.3.1	Les protocoles simulés	38
4.3.2	Paramètres de simulation choisis	38
4.3.3	Modèle de simulation	38

4.4	Présentation des différents scénarios de simulation	39
4.4.1	Scenario 1 : Etude par rapport au nombre de nœuds	39
4.4.2	Scenario 2 : Etude par rapport à la distance entre l'émetteur et le récepteur	40
4.4.3	Discussion	41
4.5	Conclusion	42
	Conclusion générale	43

Table des figures

1.1	Modèle de réseaux mobile avec infrastructure	4
1.2	Exemple de réseau Ad Hoc	5
1.3	Modélisation d'un réseau ad hoc	5
1.4	différents modes de communication ad hoc	6
1.5	Problème de nœud caché	7
2.1	Routage à plat	14
2.2	Routage hiérarchique	14
2.3	Mécanisme d'innodation	16
2.4	Classification des Protocoles de routage	17
3.1	Inondation de RREQ et le renvoi du RREP	22
3.2	Coupure de route et envoi du RERR	23
3.3	Maintenance des route dans DSDV	30
3.4	Ensemble des MPR d'un nœud	32
4.1	Architecture générale du NS	37
4.2	cas1 : Débit en fonction de nombre de noeuds	40
4.3	cas2 : le débit en fonction de nombre de noeuds	40
4.4	cas1 : le débit en fonction de la distance (grande distance)	40
4.5	cas2 : le débit en fonction de la distance(petite distance)	41
4.6	instalation du NS	46
4.7	Fin d'instalation du NS	47

Liste des tableaux

3.1	Format de la demande de route RREQ	25
3.2	Format de la réponse de route RREP	26
3.3	Format du message HELLO	27
3.4	Format de l'accusé de réponse de route RREP-ACK	27
3.5	Format de l'erreur de route RERR	27
3.6	Format du paquet OLSR	32
3.7	Table de routage OLSR	33
3.8	Format de message MID	34
3.9	Format de message TC	35
3.10	Format de message HELLO	35
3.11	Format de message HNA	36
4.1	Modèle de simulation utilisé.	39

Liste des abréviations

PRN	P acket R adio N etwork
DARPA	D efense A dvanced R esearch P roject A gency
CSMA	C arrier S ense M ultiple A ccess
SURAN	SUR V ivable R adio N etworks
IEEE	I nstitute of E lectrical and E lectronic E ngineer
MANET	M obile A d hoc N ETwork
WSN	W ireless S ensor N etworks
WMN	W ireless M esh N etworks
LAN	L ocal A rea N etwork
PAN	P ersonale A rea N etwork
GSM	G lobal S ystem M obile
UMTS	U niversal M obile T elecommunication S ervice
AODV	A d H oc O n- D emand D istance V ector
DSDV	D estination S equenced D istance V ector
OLSR	O ptimized L ink S tate R outing
DSR	D ynamics S ource R outing
RREQ	R oute R equest
RREP	R oute R eply
RERR	R oute ERR or
HC	H op C ount
SND	S equence N umber D estination
SNS	S equence N umber S ource
TTL	T ime T o L ive
DC	D estination C ount
TC	T opologie C ontrol
MID	M ultiple I nterface D éclaration

HNA	H ost and N etwork A ssociation
MPR	M ulti P oint R elais
NS2	N etwork S imulator 2
TCP	T ransmission C ontrol P rotocol
IP	I nternet P rotocol
NAM	N etwork A ni M ator
CBR	C ontinuous B it R ate

Introduction générale

Ces dernières années, les technologies ont connu un développement énorme dans tous les domaines, en particulier la technologie sans fil qui évolue plus rapide. Pour offrir aux utilisateurs la possibilité de communiquer automatiquement sans avoir des problèmes, par exemple elles pourront pratiquement éliminer le besoin d'acheter un câblage propriétaire pour connecter les différents périphériques individuels. Cette dernière permet l'établissement d'une communication dans des environnements mobiles qui fournissent une grande souplesse d'emploi.

Les réseaux mobiles sans fil, peuvent être classés en deux grandes familles (les réseaux avec infrastructure et les réseaux sans infrastructure), les réseaux avec infrastructure aussi appelé mode cellulaire, s'appuie sur une topologie construite autour de points d'accès fixe. Ces dernières ont pour fonction de gérer les échanges entre les nœuds mobiles situés dans leur zone de couverture. Les réseaux sans infrastructure appelé mode ad hoc, ne requiert aucune infrastructure fixe et qui font l'objet de notre étude.

En d'autres termes un réseau ad hoc est défini comme un ensemble d'entités mobiles interconnectées par une technologie sans fil constituant un réseau sans aucune forme d'administration ou de support fixe. Les applications des réseaux ad hoc sont nombreuses, on cite par exemple leur application dans le domaine militaire et les applications tactiques comme les opérations de secours, les missions d'exploration ...etc. Ce réseau est aussi caractérisé par sa taille qui est illimitée, C'est à dire aucune supposition ou limitation n'est faite sur la taille du réseau.

Dans les réseaux ad hoc, chaque nœud joue le rôle d'un routeur et/ou d'un hôte, alors il doit transmettre les paquets pour les autres nœuds de réseau, d'où la nécessité d'un protocole de routage. Plusieurs protocoles de routage pour les réseaux Ad Hoc

ont été développés, suivant la manière de création et de maintenance de routes lors de l'acheminement des données. Ces dernières peuvent être classifiés en trois catégories : les protocoles réactifs, proactifs et hybrides.

Dans notre travail, nous avons choisi trois protocoles de routage utiles dans les environnements mobile ad hoc :

- **AODV (Ad-hoc On-Demand Distance Vector)** : C'est un protocole de type réactif fondé sur le principe de vecteurs de distance, c'est à dire du nombre des sauts entre l'émetteur et le récepteur. Ce protocole utilise un numéro de séquences dans l'envoi de ces paquets afin d'éviter les problèmes de boucle et de comptage à l'infini.
- **DSDV (Dynamic destination Sequenced Distance Vector)** : C'est un protocole ad hoc de type proactif à vecteur de distance. Dans ce protocole chaque nœud maintient une table de routage qui va être mise à jour périodiquement et la transmettre à travers le réseau afin de maintenir la cohérence des routes.
- **OLSR (Optimized Link State Routing)** : C'est un protocole proactif appartenant à la famille des protocoles à état de liens. Il se base sur la technique de relais multipoint, cette technique permet d'optimiser les diffusions des messages de contrôle dans le réseau et la consommation de la bande passante.

Et afin d'évaluer les performances de ces protocoles et analyser leur fonctionnement, en utilisant l'outil de simulation de réseau NS2 (Network Simulator 2).

Ce mémoire est organisé en quatre chapitres :

Dans le premier chapitre, nous présentons les réseaux mobiles ad hoc, en commençant par introduire les principaux concepts liés à ces environnements, par la suite nous citons quelques applications et caractéristiques de ce type de réseau.

Dans le second chapitre, nous avons abordé le routage dans les réseaux ad hoc, les problématiques et les contraintes liées au routage ainsi que les techniques et les différents protocoles de routage et leurs principale avantages et inconvénients.

Dans le troisième chapitre nous avons présenté les trois protocoles AODV ,DSDV et OLSR. On a expliqué le principe du fonctionnement du chaqu'un des trois , ainsi que les différents types des messages échangés lors d'établissement d'une communication entre les différents nœuds d'un réseau.

Et enfin dans le dernier chapitre nous avons présenté l'outil de simulation de

réseau NS2. Nous avons analysé et discuté les résultats des simulations des protocoles AODV et DSDV.

Nous terminons notre mémoire par une conclusion générale et quelques perspectives.

Généralités sur les réseaux mobiles ad hoc

1.1 Introduction

Les réseaux mobiles ad hoc sont un cas des réseaux mobiles. Ils sont le résultat de l'interconnexion d'un grand nombre de nœud mobiles. Un réseau mobile peut se déployer facilement et rapidement et n'a besoin d'aucune infrastructure fixe ou contrôle centralisé. Dans ce premier chapitre, nous précisons les notions de base des réseaux ad hoc, l'historique, les avantages et les inconvénients, la sécurité et les principales caractéristiques des réseaux ad hoc ainsi que les domaines d'application liés à ce type de réseau...etc.

1.2 Architectures des réseaux sans fil

Les réseaux mobiles sans fil permettent à leurs utilisateurs d'accéder à l'information indépendamment de leurs positions géographiques. Ils peuvent être classés en deux catégories, Les réseaux avec infrastructure (mode cellulaire), et les réseaux mobiles sans infrastructure (mode ad hoc).

1.2.1 Architecture avec infrastructure

Un réseau mobile avec infrastructure est un ensemble de nœuds mobile, le fonctionnement des réseaux est géré par un système centralisé appelé «station de base» Comme le montre la figure(1.1) :

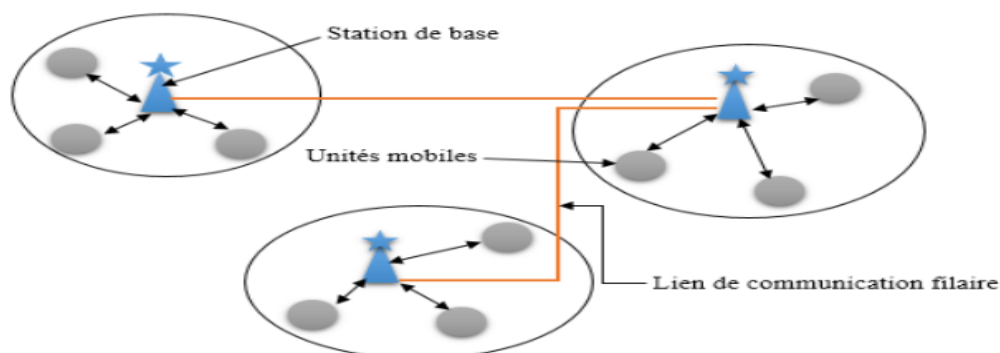


FIG. 1.1 – Modèle de réseaux mobile avec infrastructure

1.2.2 Architecture sans infrastructure (Ad Hoc)

Contrairement à la catégorie précédente, dans cette classe du réseau les entités mobiles communiquent entre elles directement sans utilisation d'un point d'accès, tous les sites du réseau sont mobiles et communiquent d'une manière directe en utilisant leurs interfaces de communication sans fil.

1.3 Présentation des réseaux mobiles ad hoc

1.3.1 Historique

Historiquement, les réseaux mobiles ad hoc sont employés dans le domaine militaire, pour améliorer et garantir la communication sans fil dans ce domaine. Tout a commencé au début des années 70, quand sont apparu les premières applications des réseaux ad hoc par le département de la défense américaine DARPA (Defense Advanced Research Project Agency). Un réseau ad hoc dispose d'une architecture distribuée qui partage le canal de diffusion par la combinaison des protocoles CSMA et ALOHA. Ensuite en milieu des années 80, le SURAN (Survivable Radio Networks) a été développé par DARPA afin de dresser les lacunes au sein du projet PRN et de permettre au réseau d'avoir une dizaine de milliers de nœuds mobiles qui peuvent être évolués par des protocoles avec des mécanismes radio simple. A partir des années 90 le groupe de travail MANET a lancé des recherches dans ce domaine. Il a pris son essor avec l'arrivée des technologies radio, spécialement la norme IEEE 802.11 et ses différentes dérivées. Cette norme a été standardisée en 1999 par l'IEEE (Institute of Electrical and Electronics Engineers), dans le but d'assurer la communication entre ordinateurs utilisant le médium radio.

1.3.2 Définition d'un réseau Ad Hoc

Un réseau mobile ad hoc appelé MANET (Mobile Ad hoc Network), est formé d'un ensemble de nœuds mobiles qui sont dynamiquement et arbitrairement éparpillés d'une manière où l'interconnexion entre ces nœuds peut changer à tout moment.

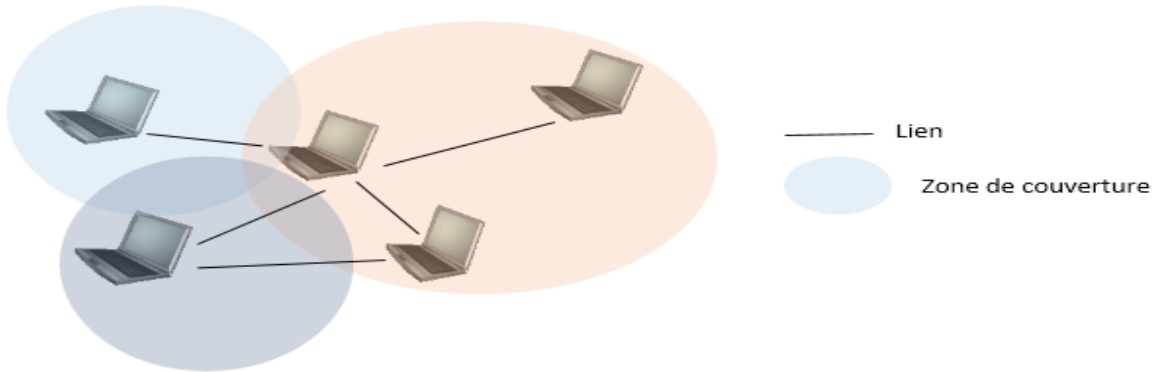


FIG. 1.2 – Exemple de réseau Ad Hoc

1.3.3 Modélisation d'un réseau mobile ad hoc

Les réseaux ad hoc peuvent être modélisés par un graphe $G_t = (V_t, E_t)$. Où :

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

E_t : représente l'ensemble des connexions qui existent entre ces nœuds (liens de communication).

Cette présentation de topologie du réseau est dynamique, car elle peut changer sa forme au fur et à mesure. Dans la figure(1.3) on vous représente un réseau ad hoc de 6 unités mobiles sous forme d'un graphe.

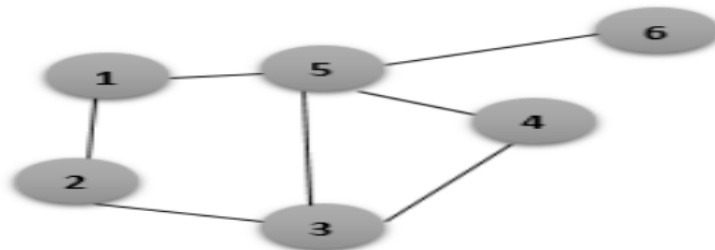


FIG. 1.3 – Modélisation d'un réseau ad hoc

1.3.4 Mode de communication dans les MANETS

Les réseaux mobiles Ad Hoc utilisent, trois principaux modes de communication :

1. **Communication «point à point» ou Unicast** : on spécifie le nœud suivant sur la route d'un paquet de données ;
2. **Communication «multipoint» ou Multicast** : chaque nœud source va transmettre ces paquets à un groupes de nœuds ;
3. **Communication par la «diffusion» ou Broadcast** : dans ce mode un nœud source va transmettre les paquets à tous les nœuds voisins, chaque nœud mobile réémet à son tour les Paquets qu'il reçoit à ses voisins jusqu'à ce qu'ils arrivent à la destination.

Ces trois modes de communication sont schématisés dans la figure(1.4) :

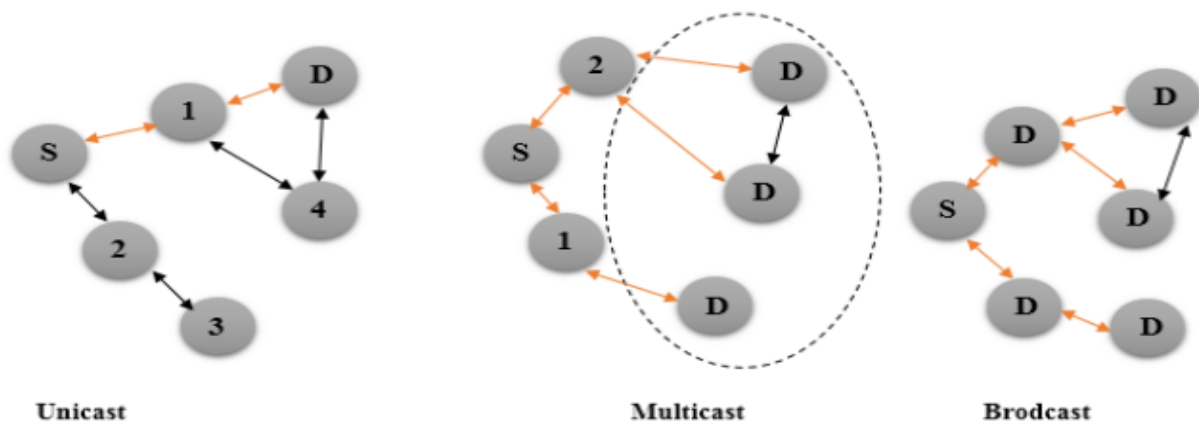


FIG. 1.4 – différents modes de communication ad hoc

1.4 Types des réseaux Ad hoc

1.4.1 Les réseaux de capteurs WSNs (Wireless Sensor Networks)

Dans un WSN les nœuds capteurs sont statiques, la communication est initiée toujours vers ou à partir des nœuds puits qui sont plus sensibles à la panne qu'à celle des capteurs, mais les communications capteur-à-capteur sont rares.

1.4.2 Les réseaux maillés WMNs (Wireless Mesh Networks)

C'est un réseau dans lequel deux stations de travail peuvent être mises en relation par différents chemins. Cette mise en relation s'effectue à l'aide de commutateurs, chaque commutateur constituant un nœud du réseau.

1.5 Caractéristiques des réseaux Ad Hoc

Les réseaux Ad Hoc sont caractérisés principalement par :

- **Une topologie dynamique** : La mobilité des nœuds dans le réseau ad hoc provoque un changement rapide et aléatoire dans sa topologie.
- **Bande passante limitée** : Lors de communication sans fil on utilise un médium de communication partagé (ondes radio), dont la bande passante réservée à un hôte soit modeste.
- **Contraintes d'énergie** : Dans les réseaux ad hoc les hôtes sont alimentés par des sources d'énergie autonomes qui ont des capacités limitées.
- **Erreur de transmission** : Les erreurs de transmission radio sont plus fréquentes que dans les réseaux filaires. [2]
- **Absence d'infrastructure** : Les réseaux Ad Hoc se diffèrent des autres réseaux mobiles par l'absence d'infrastructures et tout genre d'administration centralisée.
- **Problème de nœuds cachés** : Ce phénomène est très particulier à l'environnement sans fil. Une illustration très simple de ce problème est possible avec seulement trois stations **A**, **B** et **C** positionnées comme dans la figure 1.5. **B** ne peut pas entendre **C** lorsqu'elle émet vers **A**, et donc **B** considère pouvoir utiliser le canal. En cas d'émission de **C**, des collisions au niveau de **A** seront donc causées.

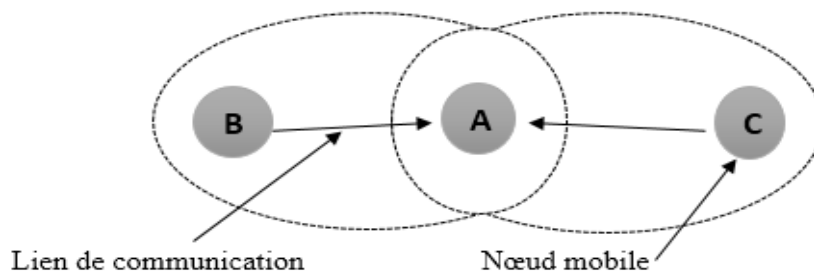


FIG. 1.5 – Problème de nœud caché

- **Qualité de service** : Dans les réseaux ad hoc il est très difficile d'assurer certaines garanties comme le débit, le délai ..etc., est tout ça à cause de la nature du canal radio (interférences et taux d'erreur élevés) et que les liens entre les mobiles peuvent partager les ressources alors qu'en filaire, deux liens sont indépendants.

1.6 Contraintes spécifique aux réseaux ad hoc

L'évolution des technologies sans fil a poussé au développement de protocoles pour accéder facilement et efficacement à l'information. Parmi ces contraintes nous citons :

- ✓ Une topologie dynamique, qui évolue rapidement, d'où la nécessité d'un mécanisme de routage qui s'adapte à cette évolution.
- ✓ Le seul moyen de communication entre les nœuds mobiles au sein d'un réseau ad hoc est l'utilisation d'un canal radio. En effet, les liaisons sont à débits variables et la bande passante est limitée.
- ✓ Une autonomie réduite en termes d'énergie vu que les nœuds fonctionnent avec des batteries. Chaque nœud joue le rôle d'un routeur et utilise par conséquent sa propre énergie pour acheminer des paquets destinés à d'autres nœuds du réseau. Sachant qu'une partie de cette énergie est déjà consommée par le mécanisme de routage, ceci limite les services et les applications supportés par chaque nœud mobile.
- ✓ Les liens radios ne sont pas isolés et le nombre de canaux disponibles est limité. Par conséquent, les interférences augmentent le nombre d'erreurs sur la transmission. De plus, à cause du partage de l'interface radio, chaque donnée est réceptionnée par tous les nœuds avec des puissances variables. Il faut ajouter également, que des interférences conduisent à une grande versatilité des liens qui peuvent apparaître ou être coupés de manière durable et à tout moment.
- ✓ La puissance du signal qui, non seulement, est atténuée rapidement avec la distance, mais est soumise à des réglementations très strictes, ceci empêche un émetteur de dépasser une certaine puissance lors de l'émission.

1.7 Domaines d'applications des réseaux mobiles Ad Hoc

Les réseaux ad hoc sont utilisés dans les domaines militaires comme ils sont aussi utilisés dans des domaines civils. On peut citer :

- 1. Applications militaires :** les réseaux ad hoc sont une solution pour le maintien d'une communication sur un champ de bataille entre les différentes unités d'une armée.
- 2. Les services d'urgence :** les secours des personnes en cas de catastrophe naturelle, (tremblement de terre, les inondations, feux...etc.).
- 3. Systèmes de conférence :** Les réseaux ad hoc facilitent l'échange et le partage d'informations entre les participants d'une conférence par exemple.
- 4. Applications commerciales :** Pour un paiement électronique distant, pour l'accès mobile à l'Internet, service de guide en fonction de la position de l'utilisateur...etc.
- 5. Réseaux de senseurs :** pour des applications environnementales (climat, activité de la terre, suivi des mouvements des animaux, etc.) ou domestiques (contrôle des équipements à distance).
- 6. Au niveau des véhicules (Intervehicle Networks) :** Ces réseaux sont utilisés aussi avec les véhicules routiers, Pour assurer entre ces derniers le transfert des messages de demande de secours ou des messages sur les conditions de la route.
- 7. Campus universitaires :** l'utilisation des réseaux mobiles peut être très utile pour les étudiants qui pourront se connecter sur leurs comptes et travailler à partir de la bibliothèque ou de leurs chambres.

1.8 Avantages et inconvénients des réseaux Ad Hoc

a) Avantages

Les avantages de réseau ad hoc sont nombreux du fait :

- ✓ Les réseaux ad hoc peuvent être déployés dans un environnement quelconque ;
- ✓ Le cout d'exploitation du réseau est faible : aucune infrastructure n'est à mettre en place initialement et surtout aucun entretien n'est à prévoir ;
- ✓ Le déploiement d'un réseau ad hoc est simple : ne nécessite aucun prérequis puisqu'il suffit de disposer d'un certain nombre de terminaux dans un espace pour créer un réseau ad hoc, et rapide puisqu'il est immédiatement fonctionnel dès que les terminaux sont présents ;
- ✓ La souplesse d'utilisation : est un paramètre très important puisque les seuls éléments pouvant tomber en panne sont les terminaux eux-mêmes. Autrement dit, il n'y a pas de panne " pénalisante " de manière globale (une station qui sert au routage peut être remplacée par une autre si elle tombe en panne). [3]

b) Inconvénients

Même si les perspectives pour les réseaux ad hoc sont prometteuses, plusieurs inconvénients restent encore à traiter à savoir :

- ✓ La connectivité limite les possibilités de communication. Ainsi, deux stations ne sont joignables que s'il existe un ensemble de stations pouvant assumer la fonction de routeur afin de faire suivre les paquets de données échangées entre les deux stations ;
- ✓ 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'autres paramètres telle que la bande passante et la consommation de batterie ;
- ✓ La sécurité dans les réseaux ad hoc est difficile à contrôler, notamment parce que dans l'interface air l'écoute clandestine est très simple à réaliser ;
- ✓ Enfin, la faible autonomie des batteries constitue un frein à une utilisation longue du terminal et à la mise en place de nouveaux services, c'est une contrainte qui existe dans les réseaux avec infrastructure, mais qui est plus forte dans les réseaux ad hoc, puisque les ressources énergétiques sont utilisées pour les besoins du routage.[3]

1.9 Conclusion

Dans ce chapitre, on a décrit le réseau ad hoc, les principales applications et ces différentes caractéristiques, ainsi que ces avantages et ces inconvénients. Dans le deuxième chapitre, nous allons présenter les différents points sur le routage dans les réseaux ad hoc.

Routage dans les réseaux Ad Hoc

2.1 Introduction

La communication entre un nœud source et nœud destination nécessite la présence d'un protocole de routage qui établira une route correcte, et acheminera les informations vers la bonne destination. Dans les réseaux ad hoc plusieurs protocoles ont été proposées (AODV,DSDV, OLSR, DSR , ...etc.). Dans ce qui suit nous allons décrire le routage dans les réseaux ad hoc ainsi que les principales contraintes et techniques dans ce dernier, ensuite on décrira les protocoles réactifs et proactifs.

2.2 Définition du routage

Le routage est le mécanisme par lequel des chemins sont sélectionnés dans un réseau pour acheminer les données d'un expéditeur jusqu'à un ou plusieurs destinataires à travers un réseau de connexion donné, il consiste à assurer une stratégie qui garantit, à n'importe quel moment, un établissement de routes qui soient correctes et efficaces entre n'importe quelle paire de nœuds appartenant au réseau, ce qui assure l'échange des messages d'une manière continue [4].

2.3 Problématiques de routage dans les réseaux Ad Hoc

Dans le but d'assurer la connectivité du réseau, malgré l'absence d'infrastructure fixe 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, tout nœud joue ainsi le rôle de station et de routeur. 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 [5].

2.4 Contraintes de routages dans les réseaux ad hoc

Pour assurer la connexion dans les réseaux ad hoc, plusieurs algorithmes de routage sont mis en œuvre, mais le changement fréquent de topologie de réseau reste un problème à résoudre, donc il est important que toute conception de protocole de routage étudie les problèmes suivants :

- **La minimisation de la charge du réseau** : se fait par l'amélioration des ressources du réseau, pour réduire le nombre des boucles de routage ainsi que 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'incident sur le bon acheminement des données. L'élimination d'un lien, pour cause de panne ou de mobilité devrait, idéalement, augmenter le moins possible les temps de latence. [6]
- **Assurer un routage optimal** : la stratégie de routage doit créer des chemins optimaux et pouvoir prendre en compte différentes métriques de coûts (bande passante, nombre de liens, ressources du réseau, . . .etc.). Si la construction des chemins optimaux est un problème dur, la maintenance de tels chemins peut devenir encore plus complexe, donc la stratégie de routage doit assurer une maintenance efficace de routes avec le moindre coût possible. [6]
- **Le temps de latence** : l'augmentation de la connectivité du réseau influence l'augmentation de la qualité des temps de latence.

2.5 Techniques de routage

Il existe différentes stratégies qui utilisent une variété de techniques afin de résoudre le problème de routage dans les réseaux Ad Hoc. Parmi lesquelles nous allons citer :

2.5.1 Routage hiérarchique ou plat

- **Routage à plat** : dans ce type de routage, les nœuds sont identiques, la décision d'un nœud de router des paquets vers un autre dépendra de sa position, AODV est l'un des protocoles qui utilise cette technique. La figure(2.1) illustre un exemple du routage à plat.

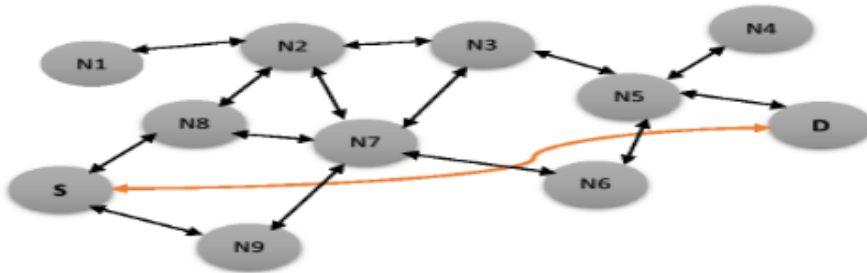


FIG. 2.1 – Routage à plat

- **Routage hiérarchique** : dans cette technique, chaque nœud racine donne des rôles particuliers à des nœuds feuille pour la recherche de bon chemin, Ce processus se répète jusqu'à atteindre tous les nœuds. La figure(2.2) illustre cette technique de routage .

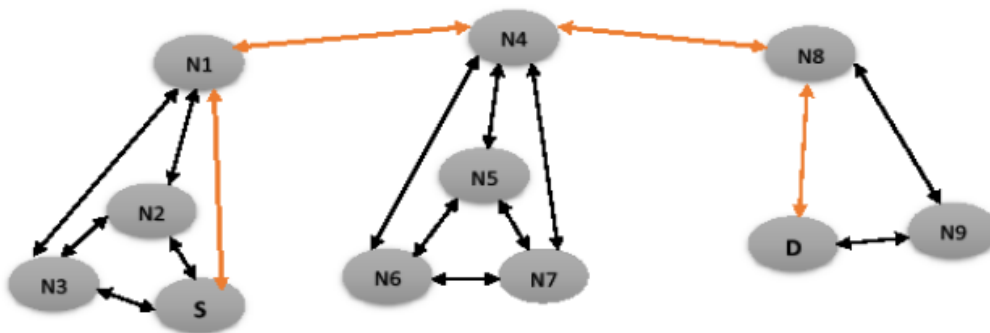


FIG. 2.2 – Routage hiérarchique

2.5.2 Routage à la source et le routage saut par saut

- **Le routage à la source (source routing)** : dans cette technique le paquet à envoyer doit contenir la liste des différents nœuds relayeurs vers la destination. Ainsi que le chemin que devra suivre. Le protocole le plus connu se basant sur cette stratégie est DSR.
- **Le routage saut par saut (hop by hop)** : 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. Parmi Les protocoles qui utilisent cette technique est AODV.

2.5.3 Routage à état de lien et à Vecteur de distance :

Cette stratégie basée sur deux méthodes essentielles, la création des routes et la maintenance de ces dernières lors de l'acheminement des données. Selon les informations de routage échangées et les méthodes de calcul des routes utilisées, on distingue deux grandes familles de routage, les routages à vecteurs de distance et les routages à état de liens et un autre hybride entre les deux.

- **Routage à vecteurs de distance** : dans cette famille de routage, chaque nœud a une table qui contient les adresses des nœuds destination du réseau et la distance (par rapport au nombre de sauts); cette table va être diffusée à tous les voisins et mise à jour périodiquement lorsqu'un nœud trouve une route plus courte que celle qu'il a dans sa table, ou bien si le nœud par lequel il passe pour atteindre une destination donnée change la distance vers cette destination, ou encore s'il trouve un nœud qui n'existe pas dans sa table.
- **Routage à état de liens** : Dans un routage à état de liens, chaque nœud vérifie l'état des liaisons avec ces voisins, et diffuse un paquet contenant ces informations à tout le réseau. Ces diffusions permettent à chaque nœud d'avoir une connaissance complète de la topologie du réseau. [1]
- **Routage hybride** : ce type de routage combine les aspects de routage à état de liens et le routage à vecteur de distance.

2.5.4 L'inondation

L'inondation ou la diffusion pure, consiste à répéter un message dans tous 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. Ce comportement se répète jusqu'à ce que le paquet atteigne tous les nœuds du réseau (voir figure 2.3). [7]



FIG. 2.3 – Mécanisme d'innodation

2.6 Classification de protocoles de routage

2.6.1 Définition

Un protocole de routage ad hoc est un ensemble de règles appliquées au format et à la signification des trames, paquets ou messages échangés entre les nœuds. Il doit être capable de suivre la nature dynamique des réseaux ad hoc qui emmène à un changement dans la topologie. [8]

La plupart des protocoles de routages ad hoc prennent en compte 3 phases :

1. **La découverte de l'information de routage** : cette phase permet à des nœuds communicants de connaître les éléments essentiels sur la topologie qu'ils vont utiliser pour choisir le chemin par lequel ils peuvent atteindre le nœud de destination. Ils peuvent aussi obtenir une vue plus précise sur la topologie de réseau.
2. **Le choix du chemin** : dans cette phase, le choix de la route par un protocole de routage doit respecter certains critères comme :
 - Le nombre minimum de sauts dans la route (il faut choisir la route ayant le plus petit nombre de nœud à traverser) ;
 - Le critère d'économie d'énergie ;
 - L'absence des boucles dans les routes.

3. **Maintenance des routes** : dans la troisième phase la topologie du réseau ad hoc évolue au fil de temps, à cause de la mobilité des nœuds, qui oblige les routes à changer. Donc une route doit éviter de rester longtemps invalide, car les paquets ne pourraient pas atteindre leur destination. De ce fait, le protocole de routage doit prendre en considération ces changements et met à jour les routes

Généralement dans les réseaux ad hoc on trouve trois protocoles de routage, les protocoles de routage proactifs qui prévoit la demande de routage de paquet, et les protocoles de routage réactifs qui réagissent à la demande. Entre ces deux familles, on trouve une autre approche qui fait un mélange entre les deux approches précédentes, il s'agit des protocoles hybrides qui utilisent à la fois les protocoles proactifs et les protocoles réactifs.

Dans La figure(2.4) on présente les protocoles les plus utilisés et nous donnons ci-après une vue globale de ces protocoles et leurs caractéristiques essentielles.

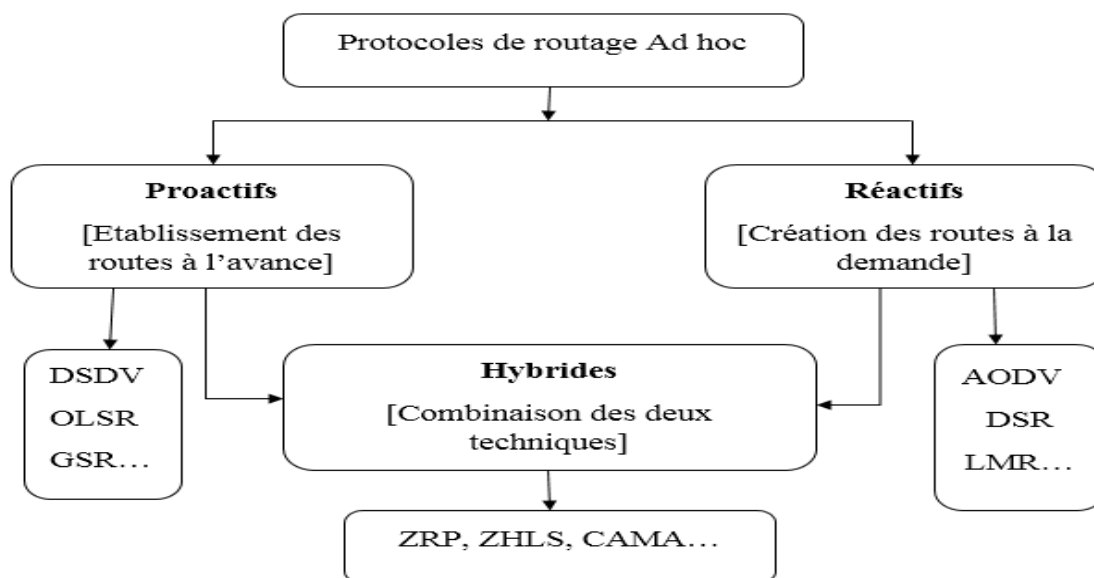


FIG. 2.4 – Classification des Protocoles de routage

2.6.2 Protocoles de routage proactifs

Dans ce type de protocoles de routage, l'établissement de routes se fait à l'avance. Chaque nœud met à jour régulièrement les données de routage de manière à obtenir le plus court chemin (nombre de nœuds intermédiaires, ou bien nombre de sauts)

vers tous les nœuds du réseau. De ce fait, si un nœud veut transmettre un paquet vers une destination, il consulte sa table de routage qui lui indique le chemin à suivre.

Ce protocole utilise deux principales méthodes :

- Méthode Etat de Lien (Link State) ;
- Méthode du Vecteur de Distance (Distance Vector).

2.6.2.1 Avantages et inconvénients des protocoles proactifs

L'avantage de ces protocoles réside dans la disponibilité des informations de routage pour router un paquet vers n'importe quelle destination. L'inconvénient majeur est le coût de maintenance des connaissances sur la topologie et de routage dû à l'envoi périodique des messages. Ceci génère une consommation continue de la bande passante. [2]

2.6.3 Protocoles de routage réactifs

Dans ce type des protocoles de routage la découverte de route se fait à la demande, donc lorsqu'un nœud veut transmettre des données vers un ou plusieurs nœuds destinations, il est obligé d'initier un processus appelé «processus de découverte de la route». Le plus connu de ces protocoles est AODV.

2.6.3.1 Avantages et inconvénients des protocoles réactifs

L'avantage de ce type de protocole est la réduction de la surcharge des réseaux par la mise à jour régulière des tables de routage. Cependant, la recherche des chemins peut dégrader les performances des applications interactives par exemple en termes de délai d'établissement de la route.[4]

2.6.4 Protocoles de routage hybrides

Cette catégorie de protocoles est une combinaison d'un protocole réactif et d'un protocole proactif. Ce type de protocoles adopte une approche proactive pour avoir des informations sur les voisins les plus proches, qui se trouvent au maximum à deux sauts du nœud mobile et utilise une approche réactive au-delà de cette limite, afin de chercher des routes. L'un des protocoles utilisés dans ce type est, ZRP (Zone Routing Protocol) et CBRP (Cluster Based Routing Protocol).

2.7 Conclusion

Dans ce chapitre, nous avons abordé les notions et les problèmes de routage dans les réseaux Ad hoc, et nous avons présenté les classifications de protocole de routage, ainsi que les techniques qui nous permettent de connaître la distribution des nœuds et la transmission des données dans les réseaux ad hoc. Dans le chapitre suivant, nous allons détailler les trois protocoles AODV, DSDV et OLSR.

Description de protocole de routage AODV ,DSDV et OLSR

3.1 Introduction

Les réseaux avec infrastructures sont basés sur la présence des stations de base qui couvrent les différents nœuds mobiles de réseau. Contrairement aux réseaux ad hoc, qui sont des réseaux sans infrastructures fixe, et qui s'organisent automatiquement de façon à être déployé rapidement.

Plusieurs protocoles de routage ont été conçus mais non encore standardisés. Ils font l'objet d'un grand effort de tests d'évaluations et d'améliorations. Nous avons essayé à travers ce travail d'étudier trois protocoles de routage dans les réseaux ad hoc parmi les plus connus : le protocole AODV ,DSDV et OLSR. Nous avons présenté dans ce chapitre ces protocoles ainsi que leur principe de fonctionnement, leurs avantages et inconvénient et à la fin une petite comparaison entre eux.

3.2 Etude détaillée des protocoles AODV ,DSDV et OLSR

3.2.1 Protocole AODV

AODV (ad hoc On demande Distance Victor) AODV (ad hoc On demande Distance Victor) est un protocole de routage réactif de type Vecteur de distance. C'est un protocole représentatif de diverses techniques et est le plus avancé sur la voie d'une normalisation. Il utilise un mécanisme de diffusion (broadcast) dans le réseau pour

découvrir les routes valides. Il est aussi basé sur l'utilisation de deux mécanismes «Découverte de route» et «maintenance de route».

AODV fonctionne par l'utilisation de trois types de messages :

- Les messages de demande de route **RREQ** : Route Request Message.
- Les messages de réponse de route **RREP** : Route Reply Message.
- Les messages d'erreur de route **RERR** : Route Error Message.

3.2.1.1 Principe de fonctionnement

1. Découverte de route

Lorsque les nœuds veulent établir une communication et il n'existe pas de route valide entre un nœud source et destinataire, AODV diffuse dans le réseau une requête de demande de route RREQ (Route REQuest). Si un nœud quelconque dans le réseau possède une route à la destination il renvoie une réponse par la requête RREP (Route REPLY) à l'émetteur, et si ce dernier ne reçoit pas de réponse RREP pendant une Période appelé (RREP-WAIT-TIME) il inonde encore une fois la requête RREQ, si cette dernière est rediffusée un certain nombre de fois (RREQ-RETRIES) sans recevoir de réponse une erreur est signalé.

La figure(3.1) illustre une recherche de route à l'initiative du nœud **S** et en direction de nœud **D**. La diffusion du message RREQ à partir de **S** se fait en broadcast vers tous ses voisins. Lorsque **D** reçoit le message il retourne un message RREP à **S** en passant par **4** et **1**.

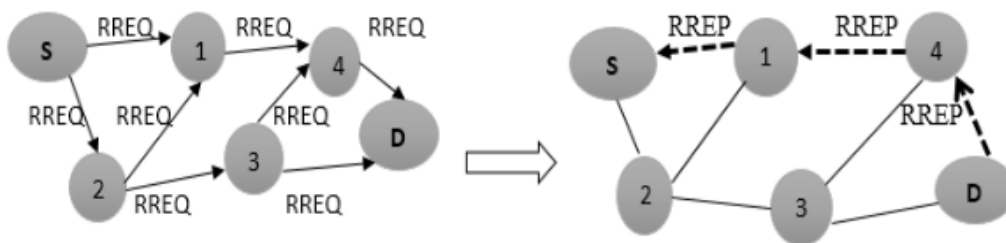


FIG. 3.1 – Inondation de RREQ et le renvoi du RREP

2. Maintenance de route

Chaque nœud dans AODV met à jour périodiquement la liste de ses voisins, un

nœud transmet un message HELLO, Si un nœud ne reçoit pas d'un voisin trois messages HELLO consécutifs le lien avec le voisin est considéré invalide. Et si ce dernier est invalide (à cause de la mobilité ou la défaillance d'un nœud), les nœuds utilisant ce lien sont prévenus par un message d'erreur (RERR), ils vont alors diffuser une autre requête. La figure(3.2) illustre la coupure d'un lien entre deux nœuds et l'envoi du RERR dans AODV.

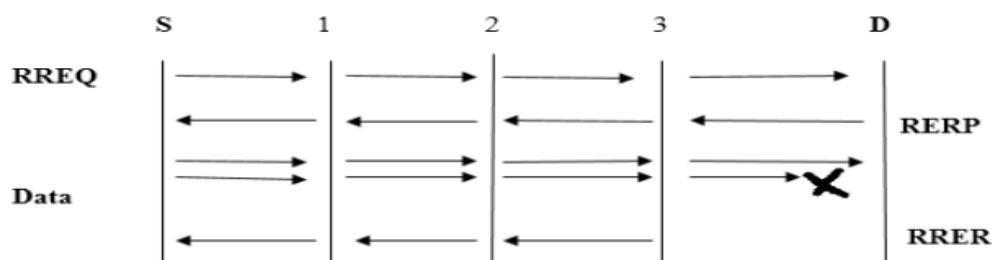


FIG. 3.2 – Coupure de route et envoi du RERR

3.2.1.2 Principe de numéro de séquence

A cause de la mobilité des nœuds dans le réseau ad hoc, les routes changent fréquemment ce qui fait que les routes maintenues par certains nœuds, deviennent invalides . Le numéro de séquence est utilisé afin d'éviter le problème des boucles infinies et des transmissions inutiles des messages sur le réseau, en plus il permet de maintenir la consistance des informations de routage.

Chaque nœud maintient également un numéro de séquence dans sa table de routage , ce numéro de séquence est mis à jour dans deux situations :

- Lors de l'expiration d'une route ou d'une cassure sur le chemin. Un nœud peut alors incrémenter le numéro de séquence du destinataire et invalider la route auprès des autres nœuds ;
- A la réception d'un message contenant un numéro de séquence plus élevé pour le même destinataire, le paquet contient alors des informations plus fraîches sur la route. [11] ;

Ainsi chaque nœud du réseau est aussi chargé de maintenir à jour son numéro de séquence en l'incrémentant dans deux cas :

- Avant d'initier un processus de découverte de route, ce qui permet d'éviter les conflits avec les routes précédemment construites par ce même nœud ;

- Avant l'émission d'un RREP par le destinataire, et ça permet de mettre à jour les informations de routage des nœuds traversés par le paquet ;

3.2.1.3 Processus d'envoi des messages dans AODV

Comme tout les protocoles de routage, AODV suit un processus pour router des informations envoyées par l'émetteur afin d'arriver à la bonne destination. On vous montre dans ce qui suit ce processus avec l'illustration par un diagramme

Si un nœud quelconque veut émettre un paquet de données vers n'importe quelle destination il est indispensable de :

1. Envoyer en Broadcast un message de type **RREQ** qui contient un identifiant (**RREQ-ID**) associé à l'adresse de la source (**@SRC**) qui servira à identifier de façon unique une demande de route.
2. Quand la requête RREQ arrive à un nœud intermédiaire il vérifie qu'il n'a pas encore traité cette requête, si c'est le cas il met à jour sa table de routage, à l'aide des informations contenues dans la requête afin de pouvoir reconstruire ultérieurement le chemin inverse vers la source.il incrémente ensuite le nombre de sauts **HC (Hop Count)** dans la demande de route et la rediffuse ; Sinon il l'abandonne et ne la rediffuse pas.
3. À la réception d'un paquet **RREQ** à la destination désirée, il ajoute ou met à jour dans sa table de routage un chemin vers le nœud voisin duquel il a reçu le paquet. Ainsi qu'un Chemin vers la source. La destination génère ensuite une réponse de route **RREP** qu'elle envoie en unicast vers le prochain saut en direction de la source.
4. Les nœuds intermédiaires qui reçoivent la **RREP** vont mettre à jour le chemin qui mène à la destination dans leur table de routage et retransmettent en unicast le message (après avoir incrémenté le nombre de sauts) vers le nœud suivant en direction de la source.
5. Une fois que la source a reçu les paquets **RREP**, elle peut commencer à émettre des paquets de données vers la destination.
6. Afin de maintenir les routes, une transmission de messages **HELLO** est effectuée. Ces messages sont en fait des réponses de route (**RREP**) diffusées aux voisins. Si au bout d'un certain temps, aucun message n'est reçu d'un nœud voisin, le lien en question est considéré défaillant. Alors, un message d'erreur **RERR** (Route ERRor) se propage vers la source et tous les nœuds intermédiaires vont marquer la route comme invalide.

3.2.1.4 Type des messages échangés

1. **Demande de route RREQ (Route REQuest)** : lorsqu'un nœud a besoin d'une route vers une destination et il ne dispose pas d'une route disponible dans sa table, il envoie un message de type RREQ présenté dans le tableau au-dessous

Type = 1	J	R	G	D	U	Reserved	#HC
#ID RREQ Identifier							
@D-Destination IP Address							
#SND- Destination Sequence Number							
@Src-Source IP Address							
#SNS-Source Sequence Number							

TAB. 3.1 – Format de la demande de route RREQ

- **Type (8 bits)** : ce champ indique le type de paquet, dans ce cas il prend la valeur 1.
 - **Flags (drapeaux) (5 bits)** : ce champ contient cinq flags (**J**, **R**, **G**, **D**, **U**) tel que : **J** : Join flag, réservé au multicast, **R** : Repair flag, réservé au multicast, **G** : Gratuitous RREP, **D** : Destination only flag (indique que seulement la destination doit répondre à cette demande de route), et en fin **U** : Unknown Séquence Number (indique que le numéro de séquence de la destination est inconnu).
 - **Reserved** : mis à zéro lors de l'envoi et ignorés à la réception.
 - **#HC (Hop Count)** : Le nombre de saut de la source de la RREQ au nœud en cours de traitement de la demande
 - **#ID** : Un numéro de séquence identifiant de manière unique une demande de route lorsqu'il est associé à l'adresse de la source (@Src.
 - **@D** : Adresse IP de la destination à laquelle une route est demandée.
 - **#SND** : Le dernier numéro de séquence connu pour la destination.
 - **@Src** : Adresse IP de la source (nœud qui a initialisé la demande de route).
 - **#SNS** : Numéro de séquence actuel de la source qui sera associé à l'entrée de la table de routage dans les nœuds traitant le message RREQ.
2. **Réponse de route RREP (Route REPLY)** : ce type de message est renvoyé en unicast à la source par la destination ou par un nœud ayant un chemin

valide vers la destination, ce message est considéré comme une réponse à la demande de route qui est envoyée par l'émetteur. Le format de paquet de réponse est représenté dans le tableau suivant.

Type = 2	R	A	Reserved	Prefix Sz	#HC
@D- Address IP Destinataire					
#SND-Numéro de séquence de destinataire					
@ Src-Originator IP Address					
Lifetime					

TAB. 3.2 – Format de la réponse de route RREP

- **Type (8 bits)** : ce champ indique le type de paquet, dans ce cas il prend la valeur 2.
 - **Flags drapeaux (2 bits)** : ce champ contient deux flags, **R** : Repair flag, utilisé en multicast, et **A** : Accusé de réception requis.
 - **Reserved (9 bits)** : mis à zéro lors de l'envoi et ignorés à la réception.
 - **Préfix Sz (5 bits)** : Si c'est différent de zéro, cela signifie que le prochain saut peut être utilisé pour n'importe quel nœud avec le même préfixe.
 - **#HC (Hop Count) (8 bits)** : Nombre de sauts de la destination de la RREQ au nœud en cours de traitement.
 - **@D** : Adresse IP de la destination à laquelle une route est demandée.
 - **#SND** : Numéro de séquence de la destination.
 - **@Src** : Adresse IP de la source, nœud qui a initialisé la demande de route RREQ.
 - **Life Time** : Temps en millisecondes pour lequel les nœuds recevant la RREP considèrent la route valide.
4. **HELLO** : Les messages HELLO offrent des informations sur la connectivité. Ils sont utilisés seulement par les nœuds faisant partie d'une route active pour valider les connexions avec les voisins. Ainsi, à chaque intervalle (Hello-Interval), le nœud vérifie qu'il a diffusé au moins un message et s'il ne l'a pas fait, il envoie une réponse de route avec un TTL (Time To Live) égal à 1. Il s'agit du message HELLO. [1]

Type = 2	R	A	Reserved	Prefix Sz	#HC=0
@D=Address IP de l'émetteur					
SND-Numéro de séquence de l'émetteur					
@ Src-Originator IP Address de l'émetteur					
Lifetime					

TAB. 3.3 – Format du message HELLO

5. Accusé de réception de réponse de route RREP-ACK(ACKnowledgment) :

L'accusé de réception doit être envoyé en réponse à une RREP

Type = 4	Reserved
----------	----------

TAB. 3.4 – Format de l'accusé de réponse de route RREP-ACK

6. Erreur de route RERR (Route ERROR) : ce type de message est envoyé lorsqu'un nœud source ne peut pas retransmettre un paquet vers sa destination (à cause d'une coupure d'un Lien). Son format est représenté dans le tableau suivant.

Type = 3	N	Reserved	#DC
Unreachable Destination IP Address(1)			
Unreachable Destination Sequence Number(1)			
Additional Unreachable Destination IP Address(if needed)			
Additional Unreachable Destination Sequence Number(if needed)			

TAB. 3.5 – Format de l'erreur de route RERR

- **Type (8 bits)** : la valeur de ce champ prend 3 dans le message RERR.
- **Flag (1 bits)** : il contient un drapeau, **N (No delete flag)** : mis à 1 lorsque le nœud effectue une réparation locale de la route et les nœuds en amont ne doivent pas effacer la route.
- **Reserved (5 bits)** : mis à zéro lors de l'envoi et ignorés à la réception.
- **#DC (Destination Count sur 8 bits)** : Le nombre des destinations non joignables incluses dans le message. Cette valeur doit être au minimum 1.
- **Unreachable Destination IP Adresse** : L'adresse IP de la destination qui n'est plus accessible.
- **Unreachable Destination Séquence Number** : Le numéro de séquence de la destination (pris de la table de routage) dont l'adresse IP est juste au-dessus.

3.2.1.5 Avantages et inconvénients d'AODV

Le protocole de routage AODV a des avantages comme il a des inconvénients parmi lesquels on cite quelques-uns :

a) Avantages

- ✓ L'utilisation d'un numéro de séquence qui permet d'éviter les boucles infinies et qui est nécessaire au processus de mise à jour de la table de routage.
- ✓ Le rappel de l'adresse IP du nœud origine dans chaque message qui permet de garder la trace du nœud à l'origine lors de l'envoi du message.

b) Inconvénients

- ✓ Il n'existe pas de format générique des messages, chacun a son format RREQ, RREP, RERR...etc.

3.2.2 Protocole DSDV (Dynamic destination Sequenced Distance Vector)

DSDV est un protocole de routage ad hoc de type proactif à vecteur de distance. Comme il s'agit d'un protocole proactif, chaque nœud maintient une table de routage qui contient toutes les destinations possibles, le nombre de sauts pour atteindre la destination et le numéro de séquences (SN) lié au nœud

destinataire. Ce protocole met à jour des tables de routage périodiquement et les transmet à travers le réseau afin de maintenir la cohérence des routes. La mise à jour de cette table peut se faire de deux façons [12] :

- **Les mise à jour complète (full dump)** : c'est une mise à jour périodique, où chaque nœud de réseau transmet la totalité de sa table de routage vers tous ses voisins, ce qui nécessite l'envoi de plusieurs paquets de données
- **Les mise à jour incrémentale (incrémental updates)** : pour lesquelles seules les entrées qui ont subi des modifications par rapport à la dernière mise à jour, sont envoyées par exemple l'apparition d'un nouveau voisin, disparition d'un nœud ...etc. et ça va réduire le nombre de paquets transmis.

DSDV a quelques caractéristiques on cite :

- ✓ Chaque nœud maintient une table de routage qui stocke toutes les informations sur tous les destinataires .
- ✓ Chaque nœud transmet périodiquement sa table de routage à ses voisins.
- ✓ Un numéro de séquence qui est créé par la destination lui-même
- ✓ Chaque nœud doit ajouter son numéro de séquence lors de l'envoi de sa table de routage.
- ✓ Quand un nœud trouve qu'une route est cassée, il incrémente le numéro de séquence de la route

3.2.2.1 Principe de fonctionnement de protocole DSDV

1. **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 nœud 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. Par exemple en cas de déplacement d'un nœud, nouvelle route vers une destination, nouveau numéro de séquence.
2. **Maintenance des routes** : Un numéro de séquence d'une destination servira à sélectionner la meilleure route vers celle-ci et déterminer si la route est encore valide ou pas. En effet, le numéro de séquence le plus récent

détermine généralement la meilleure route. Pour cela on distingue 3 cas pour la sélection de route .

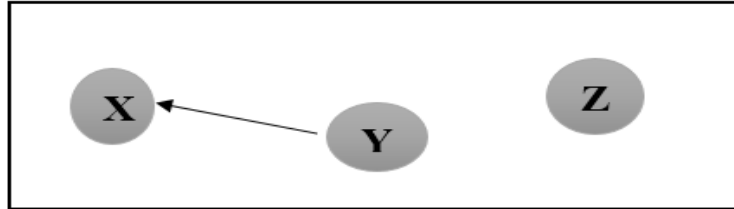


FIG. 3.3 – Maintenance des route dans DSDV

Soit le numéro de séquence de destination Z à X est $S(X)$, $S(Y)$ est envoyé à partir de Y (figure 3.4).

- ✓ Si $S(x)$ **Supérieur** à $S(y)$, alors X ne tient pas compte des informations de routage reçu de Y .
- ✓ Si $S(X) = S(Y)$, et le coût de passer par Y est plus petit que l'itinéraire connu X , alors X définit Y comme le prochain saut à Z .
- ✓ Si $S(X)$ **Inférieur** à $S(Y)$, alors X définit Y comme le prochain saut à Z , et $S(X)$ est mis à jour.

3.2.2.2 Avantages et Inconvénients de DSDV

a) Avantages

- ✓ Il est adapté à des réseaux ad-hoc avec petit nombre de nœuds.
- ✓ Il garantit les chemins libres de boucle.
- ✓ Le trafic supplémentaire peut être évité avec les mises à jour par accroissement.
- ✓ Dans la table de cheminement, DSDV ne maintient pas les chemins multiples à la destination.

b) Inconvénients

- ✓ En raison de la publicité inutile d'information de cheminement la largeur de bande est gaspillée.
- ✓ DSDV ne soutient pas le multi-cheminement de route.
- ✓ Il est difficile de déterminer le délai pour la déclaration des chemins.
- ✓ Il est difficile de maintenir une table de routage pour un plus grand réseau.
- ✓ DSDV exige une mise à jour régulière de ses tables de routage qui épuise la puissance de batterie.

3.2.3 Protocole OLSR (Optimized Link State Routing)

OLSR (Optimized link state routing Protocol) est un protocole de routage proactif à état de lien optimisé. Il propose des routes optimales en termes de nombre de sauts dans le réseau où les nœuds ne déclarent qu'une sous partie de leur voisinage en utilisant une règle qui s'appelle «relais multipoints ou MPRs» et les MPRs sont utilisés dans le but de minimiser le trafic dû à la diffusion des messages de contrôle dans le réseau.

OLSR utilise 4 types de messages :

- **HELLO** : utilisé pour la détection de voisinage
- **TC (Topologie Control)** : diffuse des informations de topologie
- **MID (Multiple interface déclaration)** : permet de publier la liste des interfaces de chaque nœud.
- **HNA** : Host and Network Association.

Ainsi, le protocole OLSR effectue deux actions principales :

- ✓ La détection de voisinage, grâce à l'envoi de messages HELLO et à la détermination des MPRs.
- ✓ La gestion de topologie, réalisée par l'intervention des messages TC, MID et HNA et aboutissant à une table de routage globale dans chaque entité.

3.2.3.1 Principe de relais multipoint(MPR)

Le concept des relais multipoint vise à réduire le nombre de messages de contrôle inutiles lors de l'inondation dans le réseau. Le principe se base sur une règle (appelé règle de multipoint) : dont chaque nœud choisit une sous partie minimale de ses voisins symétriques à un saut, de tel sorte à pouvoir atteindre tout le voisinage à deux saut (les voisins des voisins). Cet ensemble de nœuds choisis, s'appelle «le relais multipoint» (MPR). [9]

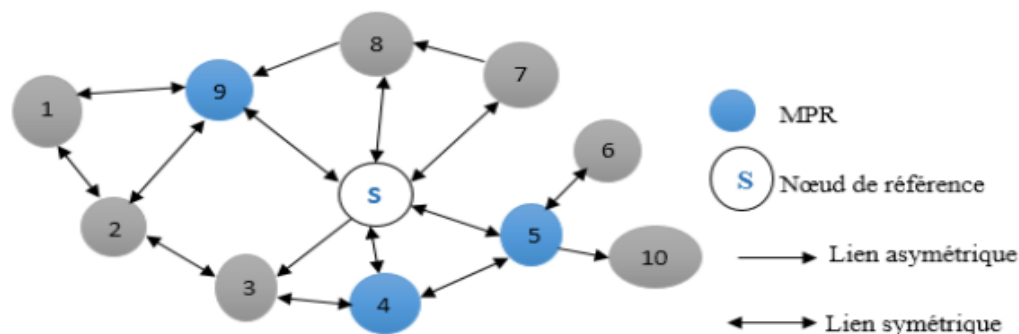


FIG. 3.4 – Ensemble des MPR d'un nœud

3.2.3.2 Format du paquet OLSR

Le protocole OLSR, définit un format unique pour tous les messages qui circule sur le réseau.(voir le tableau 3.6)

IL propose plusieurs types de messages comme HELLO et TC (Topologie Control) qui sont des messages d'échange de trafic de contrôle et deux autres messages MID (Multiple Interface Déclaration) et HNA (Host and Network Association).

Longueur de paquet		Num de séquence du paquet
Type de message	Temps de validité	Taille de message
@ d'expéditeur		
TTL=nbr max de sauts	Nbr de sauts atteints	Num de séquence de message
Message		

TAB. 3.6 – Format du paquet OLSR

3.2.3.3 Fonctionnement du protocole OLSR

1. **Détection de voisinage** : dans cette étape chaque nœud doit déterminer ses voisins symétriques directs, mais vue la mobilité des réseaux Ad hoc, certains liens peuvent devenir asymétriques, par conséquent, il faut tester tous les liens dans les deux sens avant de les considérer valides. Pour cela OLSR propose le mécanisme de détection de voisinage, ce mécanisme est assuré par l'échange périodique des messages «HELLO» qui contient des informations sur les voisins connus et l'état des liens avec ceux-ci.

2. **Gestion de topologie** : la topologie dans les réseaux Ad hoc est dynamique et les nœuds se déplacent de manière automatique pour cela les nœuds considérés comme MPRs ont la responsabilité de contrôler à chaque instant la topologie du réseau, leurs travail consiste à diffuser périodiquement des messages de contrôle de la topologie TC (Topology Control).
3. **Calcul de la table de routage** : Chaque nœud maintient une table de routage qui permet de router des données vers toutes les destinations présentées dans le réseau. Le calcul de la table de routage est basé sur les informations contenues dans la base d'informations de voisinage ainsi que celui de la base de topologie tout en les combinant avec les associations des interfaces. De ce fait, à chaque fois que l'une de ces bases d'information change, la table de routage doit être recalculée. La table de routage possède le format suivant :

Destination	Suivant	Distance	Interface
-------------	---------	----------	-----------

TAB. 3.7 – Table de routage OLSR

3.2.3.4 Processus d'envoi des messages dans OLSR

OLSR étant proactif, chaque nœud construit en permanence une vision de la topologie du réseau. Nous présentons au-dessous les étapes permettant la construction de cette dernière :

1. De manière périodique, chaque nœud envoie un message HELLO (afin de découvrir des voisinages direct et symétrique) à tous ses voisins. Ce message contient trois listes de nœuds :
 - La liste des adresses des voisins pour lesquels le nœud a reçu un paquet HELLO ;
 - La liste des adresses des voisins qui sont accessibles par un lien bidirectionnel ;
 - La liste des adresses des voisins que le nœud a choisis comme relais multipoints.
2. Selection des relai multipoint MPRs, ce processus fait que les liens entre un nœud et ses relais multipoints sont tous bidirectionnels.

3. Tous les nœuds choisis comme MPRs doivent diffuser périodiquement un message TC (Topology Control) à destination de l'ensemble du réseau afin de déclarer l'ensemble de ses sélectionneurs multi-relais. La réception de ces messages permet à chaque nœud de construire une topologie du réseau basée sur les relais multipoints.
4. utilisation de la table des voisins (neighbor table) et la table de topologie (topology table pour calculer la table de routage. Pour cela l'algorithme de Dijkstra est mis en œuvre, et le calcul de cette table est faite comme suit :
 - Détruire tous les entrées ultérieures de la table ;
 - On insère dans la table tous les voisins directs qui sont les voisins symétriques à un saut ;
 - Ensuite, on insert les destinations à plus d'un saut ;
 - On termine par l'insertion des routes vers l'ensemble des associations des réseaux et les hôtes rattachés.

3.2.3.5 Messages échangés

1. **MID (Multiple interface déclaration) :** Le message MID (tableau 3.8) contient la liste d'adresses des interfaces associées à son adresse principale. Il est envoyé par le nœud dans le réseau pour les déclarer à tous les autres nœuds. Pour obtenir une meilleure fiabilité et un meilleur débit, les messages MID peuvent servir à sélectionner plusieurs interfaces comme principales et ainsi établir des chemins multiples entre deux nœuds voisins.

Longueur de paquet		Num de séquence du paquet
MID-MESSAGE	MID-HOLD-TIME	Taille de message
@ d'expéditeur		
TTL=255	Nbr de sauts atteints	Num de séquence de message
@ interface		

TAB. 3.8 – Format de message MID

2. **TC (Topologie Control) :** Chaque nœud dans le réseau maintient une base d'informations de la topologie du réseau. Ces informations sont collectées par l'analyse des messages TC reçus par ce nœud. Seul les MPR envoient des messages TC. Ainsi le MPR peut transmettre la liste de ses

voisins qui l'on choisit comme MPR. Cela sert essentiellement à établir les tables de routage. Le tableau 3.9 illustre le format du message TC

Longueur de paquet		Num de séquence du paquet
TC-MESSAGE	TOP-MID-HOLD-TIME	Taille de message
@de l'expéditeur		
TTL=255	Nbr de sauts atteints	Num de séquence de message
@ principale voisin 1		
@ principale voisin 2		
@ principale voisin 3		
...		

TAB. 3.9 – Format de message TC

3. **HELLO** : dans le but de découvrir des voisinages, chaque nœud diffuse autour de lui un message HELLO, ce message contient des informations relatives aux interfaces que ce nœud entend, ainsi que leur état de lien. Le tableau 3.10 présente le format de message HELLO.

Longueur de paquet		Num de séquence du paquet
HELLO-MESSAGE	NEIGHB-HOLD -TIME	Taille de message
@de l'expéditeur		
TTL=1	Nbr de sauts atteints	Num de séquence de message
Réservée	Intervalle d'émission	Volonté
Code lien	Réservée	Taille de message lien
@ interface du nœud voisin		
...		

TAB. 3.10 – Format de message HELLO

4. **HNA (Host and Network Association)** : utilisés pour déclarer les sous-réseaux et hôtes (hors MANET) joignables par un nœud jouant le rôle de passerelle. Le tableau 3.11 illustre le format d'un message HNA .

Longueur de paquet		Num de séquence du paquet
HNA-MESSAGE	HNA-HOLD -TIME	Taille de message
@de l'expéditeur		
TTL=255	Nbr de sauts atteints	Num de séquence de message
@ réseau		
Masque réseau		
...		

TAB. 3.11 – Format de message HNA

3.2.3.6 Avantages et inconvénients d'OLSR

D'après la présentation ci-dessus de protocole de routage OLSR, nous remarquons qu'il a les avantages et les inconvénients suivants :

a) Avantages

- ✓ Il offre des fonctionnalités intéressantes tout en recherchant des routes optimales en termes de nombre de sauts.
- ✓ Il diminue au maximum le nombre de messages de contrôle transmis sur le réseau, en utilisant la technique de sélection des MPR.
- ✓ OLSR offre la possibilité de communication entre un réseau MANET et un réseau filaire (par des messages HNA).
- ✓ OLSR gère correctement la topologie du réseau, en expédiant régulièrement des messages TC.
- ✓ Il peut contrôler l'utilisation multiple des interfaces (messages MID).

b) Inconvénients

- ✓ Il pose un problème de sécurité, il reste toujours vulnérable malgré les recherches faites pour améliorer sa protection contre les attaques.

3.3 Conclusion

Dans ce chapitre, nous nous sommes focalisées sur les protocoles de routage AODV,DSDV et OLSR qui sont concernés par notre étude. Ce chapitre a été

axé sur le fonctionnement et le comportement de chacun de ces protocoles dans les réseaux Ad hoc . Dans le chapitre qui suit on va montrer la simulation des deux protocoles AODV et DSDV.

AODV versus DSDV avec simulation

4.1 Introduction

Comme on a vu dans les chapitres précédents, les réseaux ad hoc sont des réseaux qui englobent plusieurs unités mobiles et qui se déplacent dans un territoire quelconque. Pour ça, il est difficile de tester certains critères sur ces réseaux ; et pour évaluer ces critères dans ce réseau on a fait recours à la simulation des protocoles que on a déjà étudié précédemment (AODV, DSDV).

Dans ce chapitre on va présenter l'outil de simulation NS2 ainsi que quelque exemple pour mieux comprendre le fonctionnement de ce dernier, après on va montrer les résultats de la simulation des deux protocoles qui nous permettent de déduire les différences entre ces deux protocoles.

4.2 Présentation de Network Simulator 2

4.2.1 Définition

NS2 (Network Simulator 2) est un simulateur à évènements discrets développé dans un but de recherche. Il fournit un environnement assez détaillé permettant entre autres de réaliser des simulations d'IP, TCP, du routage et des protocoles multicast aussi bien sur des liens filaires que sans fil.[14]

4.2.2 Architecture du NS2

L'architecture générale du NS2 (voir figure 4.1) consiste en deux types de Langage de programmation : le C++ et l'OTcl (Object-oriented Tool Command Language). Le C++ est utilisé pour programmer les entités internes des systèmes simulés, alors que l'OTcl est utilisé pour définir les scénarios des simulations et les paramètres de configuration. Ces deux types de langages sont, ensuite, liés via le TclCL qui permet le passage des codes C++ vers les codes en OTcl et vice versa.

Une fois la simulation terminée, NS génère des fichiers particuliers dits fichiers de traces contenant un ensemble d'informations sur le déroulement de la simulation. Ces fichiers permettent d'évaluer les performances de réseau étudié selon des critères précis. Ils peuvent être interprétés en utilisant les outils : NAM (Network AniMator) et Xgraph. [14]

On distingue deux types de fichiers de trace :

- **Les fichiers trace «. NAM »** : ces fichiers contiennent des informations utiles pour la visualisation des nœuds et leurs déplacements ainsi que le parcours des paquets entre les nœuds.
- **Les fichiers trace «.tr»** ces fichiers contiennent un ensemble de lignes tel que chaque ligne correspond à un événement daté concernant soit un nœud ou un paquet, ils servent à calculer les différents critères et taux utiles pour évaluer les performances du réseau étudié.

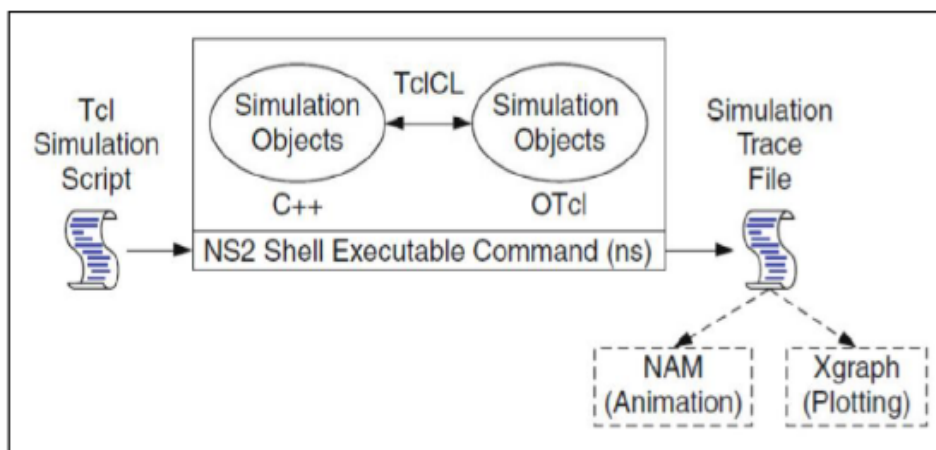


FIG. 4.1 – Architecture générale du NS

4.3 Simulation et discussion des résultats

4.3.1 Les protocoles simulés

Nous avons simulé deux protocoles qui rentrent dans le cadre des deux types réactif et proactif.

✓ **Réactif** : protocole AODV

✓ **Proactif** : protocole DSDV .

4.3.2 Paramètres de simulation choisis

- **Bande passante** : la bande passante est le débit en bit par seconde. Il est mesuré par la différence entre la fréquence de transmission la plus haute et la fréquence de transmission la plus basse. Ces fréquences sont mesurées en Hertz, l'unité fondamentale de ce paramètre est bit par seconde (bit/s) [13].

4.3.3 Modèle de simulation

Avant de lancer la simulation des scénarios, nous devons fixer certains paramètres qui vont constituer le contexte de notre simulation. Ces paramètres sont illustrés dans le tableau 4.1 :

Parametre	Valeur
Temps de simulation	100s
Temps de pause des nœuds	1s
Protocoles	AODV et DSDV
Taille de paquet de données	1024 octets
Model de mouvement	Random Waypoint
Nombre des nœuds	25
Nombre de scénarios pour un même contexte	2
Model de propagation	Two Ray Ground
Type d'interface de reseau	WirelessPhy
Couche MAC	802.11
Topologie de réseau	1000x600
Trafic d'application	CBR (Continous Bit Rate)
Le paramètre simulé	Débit

TAB. 4.1 – Modèle de simulation utilisé.

4.4 Présentation des différents scenarios de simulation

Dans notre étude, on va traiter deux scenarios : l'impact de nombre de nœuds du réseau et l'impact de la distance entre émetteur et récepteur.

4.4.1 Scenario 1 : Etude par rapport au nombre de nœuds

Nous varions le nombre de nœuds et nous gardons les autre paramètres fixe .

- cas 1 : nombre de nœuds=25
- cas 2 : nombre de nœuds=10

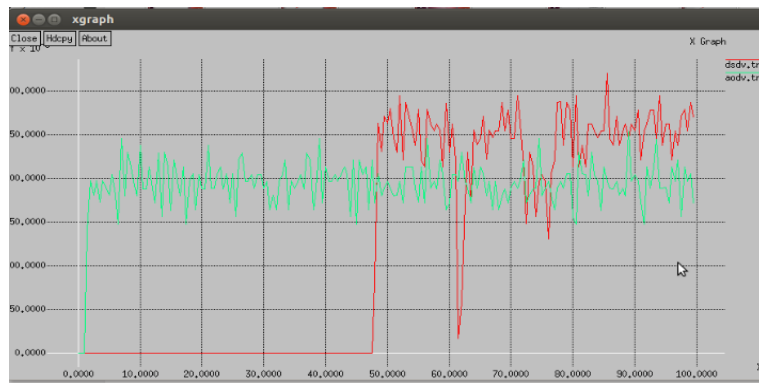


FIG. 4.2 – cas1 : Débit en fonction de nombre de noeuds

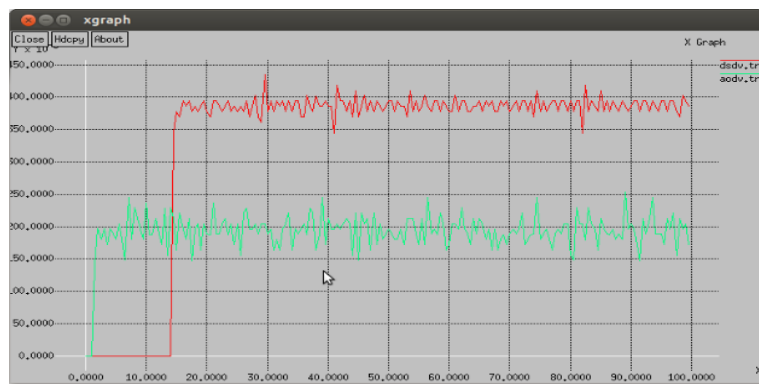


FIG. 4.3 – cas2 : le débit en fonction de nombre de noeuds

4.4.2 Scenario 2 : Etude par rapport à la distance entre l'émetteur et le récepteur

Nous varions la distance entre l'émetteur et le récepteur et nous gardons les autres paramètres fixes.



FIG. 4.4 – cas1 : le débit en fonction de la distance (grande distance)

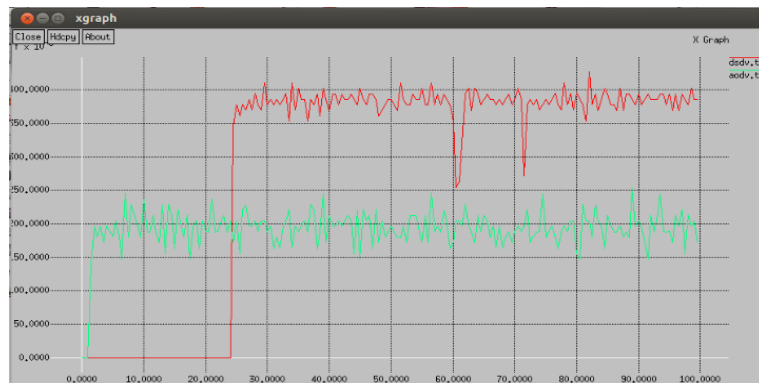


FIG. 4.5 – cas2 : le débit en fonction de la distance(petite distance)

4.4.3 Discussion

D'après les résultats présentés dans les graphes obtenus précédemment, nous avons vu pour chaque scénario et pour chaque protocole une mesure retenue qui est le débit par rapport à la distance entre l'émetteur et le récepteur et le nombre de nœuds dans le réseau.

Les graphes présentés dans la **Fig.4.3** et **Fig.4.4** montrent que le débit par rapport au nombre de nœuds change dans les deux cas pour les deux protocoles AODV et DSDV, on remarque qu'à chaque fois on minimise le nombre de nœuds le débit augmente dans le cas de DSDV, car dans DSDV la recherche d'une route est faite à l'avance mais dans le cas d'AODV le débit est presque le même dans les deux cas.

Les graphes présentés dans la **Fig.4.5** et **Fig.4.6** montrent le débit par rapport à la distance entre la source et la destination. On remarque que quand la distance entre la source et la destination est grande (**Fig.4.5**), le débit dans le cas de AODV et DSDV est le même. Même si le temps de délivrance des paquets n'est pas le même à cause des mises à jour des tables de routages pour DSDV. Dans le cas où la distance entre la source et la destination est plus petit (**Fig.4.6**) on remarque que le débit pour le protocole DSDV augmente, mais pour AODV le débit reste le même dans les deux cas.

4.5 Conclusion

Dans ce chapitre on a évalué le débit des protocoles AODV et DSDV, ainsi que la simulation de chacun. Et on a illustré les résultats avec des graphes.

Conclusion générale

Le travail qu'on a effectué sur les réseaux mobiles ad hoc nous a permis de connaître leurs différentes caractéristiques (absence d'infrastructure, topologie dynamique, bandes passantes limitées, sécurité physique limitée, contraintes d'énergie, . . .etc.), et on a constaté que leur apparition certes a facilité la mise en œuvre d'applications mobiles. Mais malgré toutes ces caractéristiques, il reste un nombre de problèmes à résoudre dont celui du routage. Pour ça, plusieurs protocoles de routage ont été développés ces dernières années. Dans ce travail on a cité quelques algorithmes de routage existant dans les réseaux ad hoc, dans le but de faire une étude des performances de ces derniers.

Ainsi que l'objectif était d'étudier le comportement des protocoles de routage opérant dans le domaine des réseaux Ad hoc. Pour cela nous avons présenté aux premiers lieux le concept de ces réseaux, par la suite on a étudié le routage dans tel environnement, dont on a donné une présentation des protocoles de routage AODV, DSDV et OLSR qui appartiennent à deux classes : proactive et réactive.

Notre étude est suivie par des simulations, ou on a simulé le protocole AODV et DSDV sous l'outil de simulation NS-2. Les résultats de simulation ont été représentés sur des graphes et interprétés. Ces simulations nous ont permis de voir la variation de débit de chaque protocole par rapport à l'impact de densité du réseau (nombre de nœuds) et la distance entre l'émetteur et le récepteur.

A partir des résultats trouvés, nous constatons qu'il n'y a pas un protocole qui est favori par rapport à l'autres dans les deux scénarios qu'on a effectué et

les critères d'évaluation, quel que soit la mobilité des nœuds ou la densité du réseau Ad hoc. Cela ouvre des ports à des contraintes et perspectives à poser comme :

- On propose dans le futur, d'intégrer le protocole OLSR dans NS-2 et le simuler afin d'évaluer leur performance.
- Perfectionner nos simulation en considérant d'autre métrique comme le taux de délivrance des paquets (PDR), le délai de bout en bout et le niveau d'énergie de chaque nœud.
- L'extension de nos simulations aux autres protocoles de routage du groupe MANET à savoir les protocoles hybrides, afin de pouvoir comparer les trois classes : réactives, proactifs et hybrides.

ANNEXE

Les étapes d'installation de NS2 sou linux

1. Télécharger le dossier ns-allinone-2.35.tar.gz à partir de site : **http://sourceforge.net/projects/nsnam/files/** ;
2. Copier le dossier **ns-allinone-2.35.tar.gz** au desktop ;
3. Ouvrir un terminal puis lancer cette commande : **sudo apt-get update** (pour obtenir la liste de la mise à jour packages/libraries dans l'Open Source) ;
4. Installer les bibliothèques requises pour ns2 à l'aide d'un terminal
sudo apt-get install build-essential autoconf automake libxmu-dev sudo apt-get install xorg-dev g++ xgraph
5. Extraire le dossier de ns-allinone-2.35.tar.gz par la frappe des commandes suivant dans le terminal. Après la fin d'exécution de ces commandes un nouveau folder nommé ns-allinone-2.35 va se générer.
cd Desktop <Entrer>
tar zxvf ns-allinone-2.35.tar.gz <Entrer>
6. Pour éviter des erreurs d'installation modifier les dossiers indiqués dans la chemise ns-allinone-2.35 comme indiqué ci-dessous :
 - dans ns-allinone-2.35/otcl-1.13/configure changer en **SHLIB-LD="gcc-shared"** ; au lieu de **SHLIB-LD="ld-shared"** ;
 - dans ns-allinone-2.35/ns-2.35/tools/ranvar.cc **line :219** changer :
return GammaRandomVariable : GammaRandomVariable (1.0 + alpha-, beta-).value ()pow (u, 1.0 / alpha-) ; à **return GammaRandomVariable (1.0 + alpha-, beta-).value () * pow (u, 1.0 / alpha-)** ;

- Changer dans les lignes 183 et 185 dans ns-allinone-2.35/ns-2.35/mobile/nakagami.cc à

```
resultPower = ErlangRandomVariable (Pr/m, int-m).value ();
```

et

```
resultPower = GammaRandomVariable (m, Pr/m).value ();
```

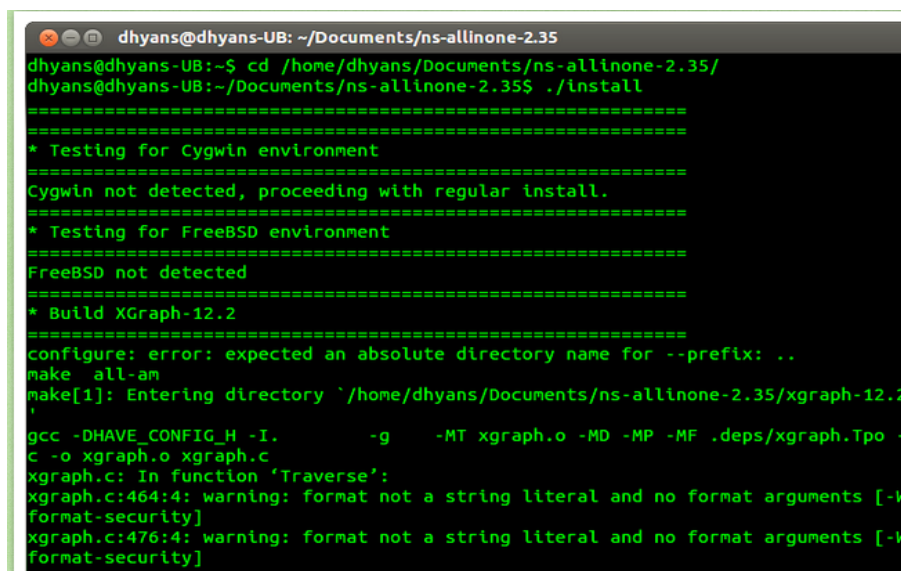
respectivement.

- Ajouter après la ligne 64 dans ns-allinone-2.35/ns-2.35/mac/mac-802-11Ext.h cette commande :

```
#include <stddef.h>;
```

7. Dans le terminal aller au Desktop/ns-allinone-2.35 et taper cette commande pour l'installation :

```
./install
```



```

dhyans@dhyans-UB: ~/Documents/ns-allinone-2.35
dhyans@dhyans-UB:~$ cd /home/dhyans/Documents/ns-allinone-2.35/
dhyans@dhyans-UB:~/Documents/ns-allinone-2.35$ ./install
=====
* Testing for Cygwin environment
=====
Cygwin not detected, proceeding with regular install.
=====
* Testing for FreeBSD environment
=====
FreeBSD not detected
=====
* Build XGraph-12.2
=====
configure: error: expected an absolute directory name for --prefix: ..
make all-am
make[1]: Entering directory `/home/dhyans/Documents/ns-allinone-2.35/xgraph-12.2'
gcc -DHAVE_CONFIG_H -I.      -g      -MT xgraph.o -MD -MP -MF .deps/xgraph.Tpo -
c -o xgraph.o xgraph.c
xgraph.c: In function 'Traverse':
xgraph.c:464:4: warning: format not a string literal and no format arguments [-W
format-security]
xgraph.c:476:4: warning: format not a string literal and no format arguments [-W
format-security]

```

FIG. 4.6 – installation du NS

Ceci prend environ 5min et note en bas des instructions que tu obtiens pour placer le chemin.

8. Réglage du Chemin :

- sur un terminal tapée `sudo gedit ~/.bash-aliases` ;
- copier le chemin suivant dans des bash-aliases et modifier le selon vos instructions :

```
# LD-LIBRARY-PATH
```

```
OTCL-LIB=/home/anurag/Desktop/ns-allinone-2.35/otcl-1.13
```

```
NS2-LIB=/home/anurag/Desktop/ns-allinone-2.35/lib
```

```

X11-LIB=/usr/X11R6/lib
USR-LOCAL-LIB=/usr/local/lib
export LD-LIBRARY-PATH=$LD-LIBRARY-PATH:$OTCL-
LIB:$NS2-LIB:$X11-LIB:$USR-LOCAL-LIB
# TCL-LIBRARY
TCL-LIB=/home/anurag/Desktop/ns-allinone-2.35/tcl8.4.18/library
USR-LIB=/usr/lib
export TCL-LIBRARY=$TCL-LIB:$USR-LIB
# PATH
XGRAPH=/home/anurag/Desktop/ns-allinone-2.35/bin:/home/anurag/Desk
allinone-2.35/tcl8.4.18/unix:/home/anurag/Desktop/ns-allinone-
2.35/tk8.4.18/unix
NS=/home/anurag/Desktop/ns-allinone-2.35/ns-2.35/
NAM=/home/anurag/Desktop/ns-allinone-2.35/nam-1.14/
PATH=$PATH:$XGRAPH:$NS:$NAM

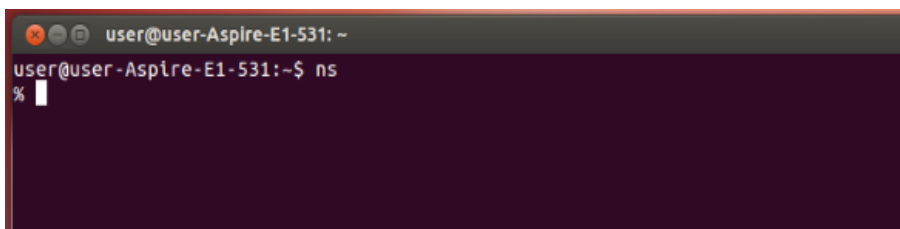
```

- À l'aide de terminal. On ajout cette commande :
source ~/.bashrc

9. Se déplacer maintenant à Desktop/ns-allinone-2.35/ns-2.35 et taper :
./validate

Des essais de validations sont réalisés pendant environ 10-15 minutes.

10. Nous pouvons maintenant exécuter le ns à partir de terminal on tape la commande ns et à la fin d'exécution, si un signe % est apparu alors NS est bien installé. Comme le montre la figure suivant :



```

user@user-Aspire-E1-531:~$ ns
%

```

FIG. 4.7 – Fin d'instalation du NS

Bibliographie

- [1] : BERRABAH Abdelkrim, SAIDI Hassiba, Balancement de charges dans les réseaux Ad Hoc, Mémoire de fin d'études, Faculté des Sciences, Université Abou Bakr Belkaid- Tlemcen, 2012-2013.
- [2] : N. BOUKHECHEM, routage dans les réseaux mobiles Ad Hoc par une approche à base d'agents, Mémoire Magister, Faculté des sciences et science de l'ingénieur, Université de Constantine, 2008.
- [3] : TAHAR ABBAS Mounir, Proposition d'un protocole à économie d'énergie dans un réseau hybride GSM et AD HOC, Mémoire de doctorat, université d'Oran, 2011-2012.
- [4] : M .BOUZAHER Abdelaziz, Approche agent mobile pour l'adaptation des réseaux mobiles ad hoc, Mémoire de Magister en Informatique, Faculté des Sciences et des Sciences de l'ingénieur Département d'Informatique Ecole doctorale, Université Mohamed Khider Biskra.
- [5] : M. Dawoud, Analyse du protocole AODV, DEA d'Informatique, Faculté des sciences Université libanaise, 2005-2006.
- [6] : Abdelmajid HAJAMI, Sécurité du routage dans les réseaux sans fil spontanés : cas du protocole OLSR, thèse doctorat, Ecole Nationale Supérieure d'Informatique et d'Analyse des Systèmes (ENSIAS)- Rabat, Université Mohammed V .

- [7] : Daniel MABELE MONDONGA, Etude sur les protocoles de routage d'un réseau sans fil en mode Ad Hoc et leurs impacts " Cas de protocoles OLSR et AODV", Institut supérieur d'informatique, programmation et analyse de Kinshasa, Ingénieur informaticien 2010.
- [8] : M. Mohammed, routage dans les réseaux maillés sans fil, mémoire de magister Université M'Hamed Bougrra-Boumerdés.
- [9] : AMZA.F, les technologies sans fil : le routage dans les réseaux ad hoc (OLSR et AODV), Université de Bejaïa.
- [10] : BEN SALEM Mohamed djihad, BOUGOFFA Oussama, Etude comparative de deux simulateurs pour les réseaux ad-hoc sans fil, Master en Informatique, Faculté des Nouvelles Technologies de l'Information et de la Communication, Université Kasdi Merbah Ouargla , Soutenu publiquement 14/06/2014.
- [11] : David Elorrieta, Protocoles de routage pour l'interconnexion des réseaux Ad-Hoc et UMTS, Licencié en Informatique, Faculté des Sciences, Département d'Informatique, Université libre de Bruxelles, Année académique 2006–2007
- [12] : Jaya Bhatt, Naveen Hemrajani. Effective Routing Protocol (DSDV) for Mobile Ad Hoc Network, «International Journal of Soft Computing and Engineering (IJSCE) ISSN : 2231-2307, Volume-3, Issue-5, November 2013»
- [13] : BELGAIAD.M et OUHAB.S ,routage et qualité de service dans AODV et OLSR Université A/MIRA de bejaia.
- [14] : Pascal Anelli ,Introduction à l'utilisation de NS (Network Simulator)

WEBOGRAPHIE

<http://sourceforge.net/projects/nsnam/files/>

<http://www.isi.edu/nsnam/nstutorial/index.html>

Résumé

Les réseaux mobiles ad-hoc sans fils sont des réseaux sans infrastructure, fonctionnant sans station de base et sans administration centralisée. Tel que tous Les nœuds dans ces réseaux peuvent être reliés de façon arbitraire et formant un réseau temporaire à topologie variable.

Notre mémoire a pour objectif de faire une étude comparative entre deux protocoles de routage connus dans les réseaux ad hoc, cette comparaison portera sur un protocole de type réactif (AODV) et un autre de type proactif (DSDV). Et afin d'évaluer les performances des deux protocoles on a fait recours à la simulation à l'aide d'un outil de simulation réseau NS2 (Network Simulator2).

Mots clés : Réseaux Ad hoc ; mobilité ; routage ; protocole de routage ; AODV ; OLSR ; DSDV ; débit ; simulateur NS-2.

Abstract

The Wireless ad hoc mobile networks are networks without infrastructure, functioning without basic station and centralized administration. Such as all the nodes in these networks can be connected arbitrarily and forming a temporary network with variable topology.

Our memory aims to make a comparative study between two protocols of routing known in the ad hoc networks, this comparison will relate to a reactive protocol (AODV) and another of proactive type (DSDV). And in order to evaluate the performances of the two protocols one made recourse to simulation using one of simulation network NS2 (Network Simulator2).

Key words: Ad hoc networks; Mobility; routing; protocol of routing; AODV; OLSR; DSDV; simulator NS-2.