

DEA d'Informatique

Coopération dans les sciences de traitement de l'information

Année universitaire 2005/2006

Analyse du protocole AODV

Préparé par Mariam Dawoud

Responsable Dr. Zoubir Mammeri

Jury Dr. Bilal Chebaro
 Dr. Kablan Barbar
 Dr. Ali Awada

Remerciements

Ce stage s'est déroulé au sein de l'institut de recherche en informatique de Toulouse.

Je suis profondément reconnaissante à monsieur Zoubir Mamméri professeur à l'université Paul Sabatier pour m'avoir soutenue tout au long de la durée de ce stage, ainsi que pour ses conseils et ses critiques.

Je remercie vivement mes professeurs de DEA, ainsi que Docteur Bilal Chebaro et Docteur Jean Paul Bahsoun.

Je remercie aussi les membres du jury d'avoir accepté de jurer ce mémoire.

Je remercie sincèrement mes parents, dont l'aide et l'encouragement m'ont permis de continuer mes études et de préparer ce stage et mes amis surtout Amr Hassan et Abderrahmen Mtibaa pour leurs aides et leurs conseils.

Résumé

Un réseau ad-hoc sans fil est une collection de noeuds mobiles formant un réseau temporaire à topologie variable et fonctionnant sans station de base et sans administration centralisée, les communications multi sauts y sont possibles grâce à des protocoles de routage spécifiques.

La simulation est un outil indispensable pour étudier la performance des protocoles de routage dans ces réseaux.

Dans le cadre de ce stage, l'évaluation de performance du protocole de routage AODV sera abordée par les simulations sous NS2, elle permet de dégager l'évolution de quelques métriques du protocole telles que le délai de sélection de route, l'optimalité de sélection de route et le coût d'établissement de route en fonction de la densité du réseau et la charge circulant dans le réseau.

Ensuite une implémentation d'un schéma de réservation de la bande passante dans le protocole AODV sera développée et comparée au simple protocole AODV en utilisant le simulateur NS2. Cette comparaison montre l'impact de l'ajout d'un contrôle d'admission des nouvelles connexions de qualité de service dans le protocole AODV et ouvre ainsi la porte à des perspectives, tels que l'optimisation ou l'amélioration de la solution proposée.

Mots clés : réseau ad hoc, protocole de routage AODV, simulation NS2, évaluation de performance, qualité de service, réservation de bande passante, contrôle d'admission.

Abstract

An ad hoc network, wireless network, is a collection of mobile nodes forming a temporary network with variable topology and functioning without basic station and centralized administration, the communications multi hops are possible by specific routing protocols. Simulation is an essential tool to study the performance of the routing protocols in these networks.

Within this DEA probation, the performance evaluation of the routing protocol AODV will be approached by simulations under NS2, it makes it possible to release the evolution of some metrics of the protocol such route selection delay, the optimality of the protocol of path selection, the cost of path selection according to the density of the network and the load circulating in the network.

Then an implementation of a reservation scheme of the bandwidth in the protocol AODV will be developed and compared with the simple protocol AODV by using the network simulator NS2. This comparison shows the impact of the addition of an admission control for new connections of quality of service in protocol AODV and thus opens the door with prospects, such as the optimization or the improvement of the solution suggested.

Key words: ad hoc network, AODV routing protocol, NS2 simulation, performance evaluation, quality of service, bandwidth reservation, admission control

Table de matières

Introduction générale	7
------------------------------------	---

Chapitre 1 : Introduction aux réseaux Ad Hoc

1. Les environnements mobiles.....	10
2. Les réseaux mobiles ad-hoc	12
2.1 Les applications des réseaux mobiles ad hoc.....	12
2.2 Les caractéristiques des réseaux ad hoc.....	12
2.3 Communication dans les réseaux ad hoc	13
2.4 Gestion d'énergie en mode Ad-Hoc	14
2.5 Auto configuration des adresses IP dans les réseaux ad hoc	15
3. le standard IEEE 802.11 en mode ad hoc	15
3.1 Le protocole IEEE 802.11.....	15
3.2 Couches physiques.....	15
3.3 Protocole d'accès au medium	16
3.3.1 Description du protocole d'accès au medium.....	16
3.3.2 Principe de base	17
3.3.3 Prévention de collision.....	18
4. Routage dans les réseaux ad hoc.....	19
4.1 Problématiques de routage dans les réseaux ad hoc	19
4.2 La conception des stratégies de routage.....	20

Chapitre 2: Présentation du protocole AODV

1. Les protocoles de routage dans les réseaux ad – hoc.....	22
1.1 Les protocoles de routage proactifs	23
1.2 Les protocoles de routage réactifs (à la demande).....	24
2. Le protocole de routage AODV	24
2.1 Table de routage et paquets de contrôle.....	24
2.2 Fonctionnalité	25
2.3 Maintenance des routes.....	27
2.4 Gestion de la connectivité locale	28

Chapitre 3: Introduction de la qualité de service dans le protocole AODV

1. Qualité de service.....	30
2. Qualité de service pour les réseaux ad hoc	31
3. Le routage AODV avec qualité de service	32
3.1 Problématiques de réservation de bande passante	33
3.2 Estimation de la bande passante	33
3.3 Intégration dans AODV	35
3.3.1 Extensions dans les messages Hello	35
3.3.2 Extensions dans la table de routage	36

3.3.3 Extensions des RREQ et RREP	36
3.4 Découverte des routes du protocole AODV avec Qos.....	36
3.5 Maintenance des routes du protocole AODV avec QoS.....	36
4. Limitations	37
4.1 Identification des brouilleurs potentiels :	37
4.2 Dépassement de la capacité du médium et contrôle de congestion	38
4.3 Contrôle du trafic	39

Chapitre 4: Etude de simulation d'AODV

1. Introduction.....	41
2. Présentation de network simulator:.....	41
2.1 Le modèle de réseau sous ns	42
2.2 Les différents modèles de propagation radio sous NS2.....	42
2.2.1 Le modèle de propagation en espace libre (Free space model):	42
2.2.2 Le modèle de propagation utilisant deux rayons (Two-ray ground reflection model):	43
2.2.3 Le modèle Shadowing:	43
2.3 Les différents modèles de mobilité sous NS2.....	44
2.3.1 Le modèle de mobilité random waypoint (RWP):.....	44
2.3.2 Le modèle Random Walk:	45
2.3.3 Modèle aléatoire de direction (random waypoint direction) :	45
3. Objectifs de la simulation	45
3.1 Délai de sélection d'une route.....	45
3.2. Optimalité de sélection de route du protocole	46
3.3. Coût de sélection de route et l'échange de l'état de lien.....	46
4. Modèle de simulation.....	46
4.1 Modèle de mobilité	47
4.2 Modèle de trafic	47
5. Résultats de simulation et analyse	48
5.1 Délai de sélection de route	48
5.2 Optimalité de sélection de route	50
5.3 Coût de sélection de route.....	51
5.4 Comparaison entre AODV et AODV modifié.....	52
Conclusion et perspectives.....	55
Bibliographie.....	56

Introduction générale

Les réseaux sans fil sont en plein développement du fait de la flexibilité de leur interface, qui permet à un utilisateur de changer facilement de place dans son entreprise. Les communications entre équipements terminaux peuvent s'effectuer directement ou par le biais de stations de base.

Les groupes de travail qui se chargent de la normalisation des produits commercialisés pour les réseaux sans fil sont IEEE aux états unis et l'ETSI. Différentes catégories de réseaux sans fil existent suivant leur étendue. Les principales normes sont IEEE 802.15 Bluetooth et ETSI Hiperpan pour les petits réseaux personnels d'une dizaine de mètres de portée, IEEE 802.11 ou Wi-Fi et ETSI Hyperlan pour les réseaux WLAN (Wireless Local Area Network), IEEE 802.16 et ETSI HyperMAN et HyperACCESS pour les réseaux WMAN (Wireless Metropolitan Area Network) atteignant plus de dix kilomètres, et IEEE 802.20, pour les réseaux WWAN (Wireless Wide Area Network) et 3GPP, EDGE (GSM) c'est-à-dire les très grands réseaux.[1]

La norme 802.11 offre deux modes de fonctionnement, le mode infrastructure et le mode ad-hoc. Le mode infrastructure est défini pour fournir aux différentes stations des services spécifiques, sur une zone de couverture déterminée par la taille du réseau. Les réseaux d'infrastructure sont établis en utilisant des points d'accès qui jouent le rôle de station de base pour l'ensemble de stations. Un réseau en mode ad-hoc est un groupe de terminaux formant un IBSS (Independent Basic Service Set), dont le rôle consiste à permettre aux stations de communiquer sans l'aide d'une quelconque infrastructure, telle qu'un point d'accès.

MANET (Mobile Ad-hoc NETwork) est le groupe de travail de l'IETF qui se préoccupe de la normalisation des protocoles ad-hoc fonctionnant sous IP. Ce groupe s'est appuyé sur les protocoles classiques d'Internet et les a perfectionnés pour qu'ils puissent fonctionner avec des routeurs mobiles.

Deux grandes familles de protocoles ont été définies : les protocoles réactifs et les protocoles proactifs :

- Protocoles réactifs. Les terminaux ne maintiennent pas de table de routage mais s'en préoccupent lorsqu'une émission est à effectuer. Dans ce cas, on se sert essentiellement de techniques d'inondation pour répertorier les mobiles pouvant participer à la transmission.
- Protocoles proactifs. Les mobiles cherchent à maintenir une table de routage cohérente, même en l'absence de communication.

Le protocole dans les réseaux ad hoc qui nous intéresse dans ce sujet de stage est le protocole de routage AODV. C'est un protocole capable de routage unicast et multicast. Il est 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. C'est un protocole réactif qui stocke les routes utilisées dans sa table de routage. La recherche de route s'effectue par diffusion. Chaque nœud enregistre le passage de la requête à l'allée. Une fois la destination atteinte, le dernier nœud envoie un paquet réponse par la route inverse et active la route en même temps.

La qualité de service est toujours un élément essentiel dans un réseau. Il est en effet souhaitable de faire communiquer deux nœuds entre eux de sorte que le flux de données échangées entre ces nœuds possède certaines propriétés.

Les réseaux sans fil posent de nombreux problèmes pour obtenir de la qualité de service. Tout d'abord, le débit réel du réseau n'est pas stable et peut varier dans le temps. Ensuite, le réseau étant partagé, les ressources sont partagées entre tous les utilisateurs.

La grandeur que l'on cherche à garantir dans le protocole AODV est la bande passante: si deux nœuds A et B communiquent, on souhaite garantir que les données pourront être échangées à un certain débit. On note que la bande passante est un paramètre fondamental qu'il est très souvent nécessaire d'assurer avant de se concentrer sur d'autres caractéristiques; en effet on ne peut minimiser le délai si aucune bande passante n'est disponible pour les applications en cours.

Le but général de ce stage est de désigner et implémenter un modèle de simulation afin d'analyser les propriétés du protocole AODV en particulier:

- Évaluer le délai de sélection de route du protocole.
- Évaluer l'optimalité de sélection de route du protocole.
- Évaluer le coût de sélection de route du protocole.

Et enfin discuter comment le protocole AODV peut être étendu pour considérer les exigences de qualité de service.

Ce document est composé de quatre chapitres : Le premier chapitre est consacré à la compréhension des concepts et des caractéristiques inhérents aux réseaux mobiles surtout les réseaux ad hoc.

Dans le second chapitre on a présenté les différents protocoles de routage dans les réseaux ad hoc et on a explicité le principe du fonctionnement du protocole de routage AODV qui est le sujet de notre stage.

Dans le troisième chapitre on a abordé la notion de qualité de service pour développer une solution de routage AODV avec qualité de service tenant compte de la métrique : la bande passante.

Le dernier chapitre montre l'outil de simulation et le modèle de simulation précis suivant lequel les métriques du protocole AODV sont évaluées. Les résultats de la simulation sont représentés sur des graphes et sont interprétés.

Une comparaison du protocole AODV sans qualité de service et AODV modifié est ainsi faite et interprétée concernant le taux d'acceptation des connexions dans les deux protocoles.

Une conclusion générale et des perspectives font la fin de ce mémoire.

Chapitre 1

Introduction aux réseaux Ad Hoc

Dans cette partie de travail il est intéressant de présenter les particularités des réseaux ad hoc avant d'examiner en détail le protocole de routage réactif AODV dans le chapitre 2.

Dans ce chapitre nous présentons les environnements mobiles et les principaux concepts liés à ces environnements. Nous commençons par définir cet environnement et citer les deux classes qui le constituent. Nous introduisons ensuite le concept des réseaux ad hoc et les caractéristiques inhérentes à ces réseaux.

Les applications des réseaux mobiles ad hoc et ses caractéristiques tenant compte de l'accès au médium dans ces réseaux sont présentés. Le standard IEEE 802.11 en mode ad hoc, l'auto configuration des adresses IP dans les réseaux ad hoc, le problème de la station cachée et la gestion d'énergie sont ensuite présentés.

Enfin nous définissons le problème d'acheminement des données dans de tels environnements et nous soulignons sa difficulté et les contraintes principales que les stratégies de routage doivent les respecter.

1. Les environnements mobiles

Un environnement mobile est un système composé de sites mobiles et qui permet à ses utilisateurs d'accéder à l'information indépendamment de leurs positions géographiques. Les réseaux mobiles ou sans fil, peuvent être classés en deux classes : les réseaux avec infrastructure et les réseaux sans infrastructure.

- Le **réseau mobile avec infrastructure** intègre deux ensembles d'entités distinctes :
 1. Les « sites fixes » d'un réseau de communication filaire classique (wired network).
 2. Les sites mobiles (wireless network)

Certains sites fixes, appelés stations support mobile (Mobile Support Station) ou station de base (SB) sont munis d'une interface de communication sans fil pour la communication directe avec les sites ou unités mobiles (UM), localisés dans une zone géographique limitée, appelée cellule (voir figure 1.1).

A chaque station de base correspond une cellule à partir de laquelle des unités mobiles peuvent émettre et recevoir des messages. Alors que les sites fixes sont interconnectés entre eux à travers un réseau de communication filaire, généralement fiable et d'un débit élevé. Les liaisons sans fil ont une bande passante limitée qui réduit sévèrement le volume des informations échangées. Dans ce modèle, une unité mobile ne peut être, à un instant donné, directement connectée qu'à une seule station de base.

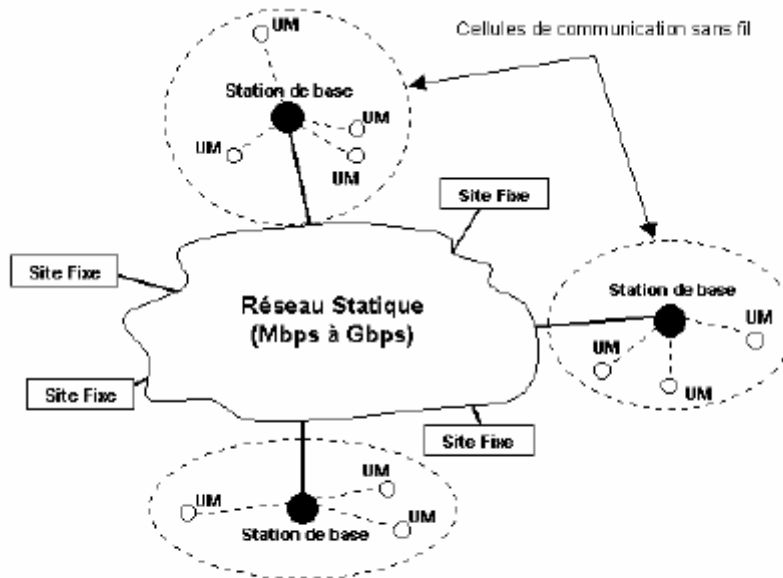


Figure 1.1 : Le modèle des réseaux mobiles avec infrastructure.

- Le modèle de **réseau mobile sans infrastructure** préexistante ne comporte pas l'entité « site fixe », tous les sites du réseau sont mobiles et se communiquent d'une manière directe en utilisant leurs interfaces de communication sans fil (voir figure 1.2). L'absence de l'infrastructure ou du réseau filaire composé des stations de base, oblige les unités mobiles à se comporter comme des routeurs qui participent à la découverte et la maintenance des chemins pour les autres hôtes du réseau.

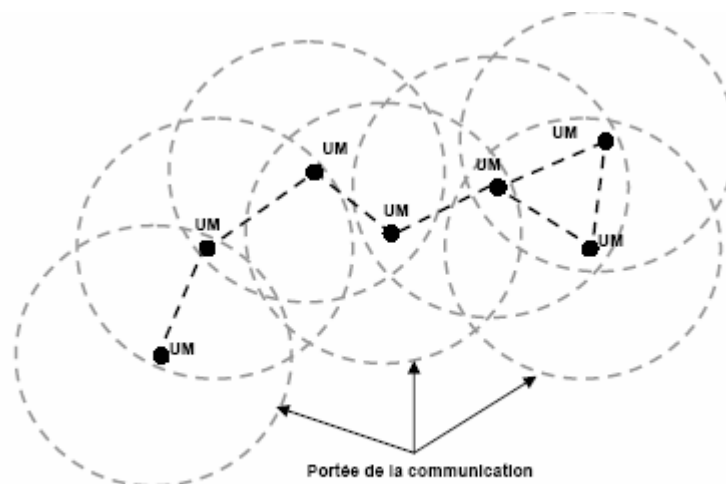


Figure 1.2 : Le modèle des réseaux mobiles sans infrastructure.

2. Les réseaux mobiles ad-hoc

Un réseau mobile ad hoc est un environnement mobile sans infrastructure, appelé généralement MANET (Mobile Ad hoc NETWORK), consiste en une grande population, relativement dense, d'unités mobiles qui se déplacent dans un territoire quelconque et dont le seul moyen de communication est l'utilisation des interfaces sans fil, sans l'aide d'une infrastructure préexistante ou administration centralisée.

Les systèmes de communication cellulaire sont basés essentiellement sur l'utilisation des réseaux filaires (tel que Internet ou ATM) et la présence des stations de base qui couvrent les différentes unités mobiles du système. Les réseaux mobiles «ad hoc» sont à l'inverse, des réseaux qui s'organisent automatiquement de façon à être déployé rapidement, sans infrastructure fixe, et qui doivent pouvoir s'adapter aux conditions de propagation, aux trafics et aux différents mouvements pouvant intervenir au sein des nœuds mobiles.

2.1 Les applications des réseaux mobiles ad hoc

La particularité du réseau Ad hoc est qu'il n'a besoin d'aucune installation fixe, ceci lui permettant d'être rapide et facile à déployer. Les applications tactiques comme les opérations de secours, militaires ou d'explorations trouvent en Ad Hoc, le réseau idéal. La technologie Ad Hoc intéresse également la recherche, des applications civiles sont apparues. On distingue :

- Les services d'urgence : opération de recherche et de secours des personnes, tremblement de terre, feux, inondation, dans le but de remplacer l'infrastructure filaire.
- Le travail collaboratif et les communications dans des entreprises ou bâtiments : dans le cadre d'une réunion ou d'une conférence par exemple.
- Home network : partage d'applications et communications des équipements mobiles.
- Applications commerciales : pour un paiement électronique distant (taxi) ou pour l'accès mobile à l'Internet, où service de guide en fonction de la position de l'utilisateur.
- Réseaux de senseurs : pour des applications environnementales (climat, activité de la terre, suivi des mouvements des animaux, . . . etc.) ou domestiques (contrôle des équipements à distance).
- Réseaux en mouvement : informatique embarquée et véhicules communicants.
- Réseaux Mesh : c'est une technologie émergente qui permet d'étendre la portée d'un réseau ou de le densifier.

2.2 Les caractéristiques des réseaux ad hoc

Les réseaux mobiles ad hoc sont caractérisés par ce qui suit :

Une topologie dynamique : Les unités mobiles du réseau, se déplacent d'une façon libre et arbitraire. Par conséquent la topologie du réseau peut changer, à des instants

imprévisibles, d'une manière rapide et aléatoire. Les liens de la topologie peuvent être unis ou bidirectionnels.

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

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

Une sécurité physique limitée : Les réseaux mobiles ad hoc sont plus touchés par le paramètre de sécurité, que les réseaux filaires classiques. Cela se justifie par les contraintes et limitations physiques qui font que le contrôle des données transférées doit être minimisé.

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 genre d'administration centralisée. Les hôtes mobiles sont responsables d'établir et de maintenir la connectivité du réseau d'une manière continue.

La notion de « multihop » : un réseau ad hoc est qualifié par « multihop » car plusieurs nœuds mobiles peuvent participer au routage et servent comme routeurs intermédiaires.

2.3 Communication dans les réseaux ad hoc

Un réseau est dit sans fil lorsque les machines qui le composent ne sont pas reliées entre elles par des câbles, mais utilisent, pour communiquer, le médium radio ou infrarouge. Comme les signaux propagés sur ces media s'atténuent au fur et à mesure qu'ils s'éloignent de leur émetteur, un nœud ne peut pas communiquer avec un autre s'il est situé trop loin de lui. On définit alors l'ensemble des voisins d'un nœud comme étant l'ensemble des nœuds capables de recevoir et de comprendre les signaux émis par celui-ci.

Avant tout, les conditions suivantes doivent être remplies pour qu'un paquet puisse être reçu :

- La puissance du signal reçu doit dépasser un certain seuil (seuil de communication).
- Le rapport signal sur bruit ambiant doit être suffisamment grand (le signal doit être clairement identifié, et non noyé dans le bruit).

Il existe un seuil de détection de porteuse. Si la puissance du signal est comprise entre ce seuil et le seuil de communication, alors le message n'est pas compris mais l'activité sur le canal est néanmoins détectée. Si le modèle de propagation radio utilisé «two-ray ground» (ou le modèle «free-space»), ces seuils définissent donc deux zones autour d'un nœud. Si le récepteur est placé au centre de la figure 1.3, alors un émetteur placé dans la zone interne (zone de communication) pourra lui envoyer des messages qui seront compris (en l'absence d'autres interférences). Si l'émetteur est placé dans la zone externe

(zone de détection de porteuse), la communication ne sera pas possible mais l'autre mobile sera informé à chaque fois que l'émetteur accédera au canal. Si le modèle de propagation radio utilisé «shadowing», les deux zones sont également définies, mais leurs frontières sont "floues" du fait du caractère probabiliste du modèle.

Le protocole 802.11 impose qu'un mobile qui veut émettre doit d'abord s'assurer qu'aucune autre communication n'est en cours dans son voisinage. Si une telle communication est en cours, et si l'émetteur est suffisamment proche (lui-même dans la zone de communication) du mobile qui voudrait lui aussi émettre, alors ce dernier a reçu l'en-tête du message et sait donc (par l'intermédiaire de son Network Allocation Vector) pour combien de temps le canal doit encore être occupé. Le nœud qui voulait émettre va donc attendre. Par contre, si le mobile qui veut aussi émettre est plus loin (dans la zone de détection de porteuse de l'émetteur) l'en-tête n'a pas pu être compris. Il est impossible dans ce cas de prévoir à l'avance quand on aura à nouveau le droit d'émettre, il faut attendre que l'activité sur le canal disparaisse. Dans ces contextes, les différents nœuds se gênent les uns les autres, et cela se traduit par un partage du canal entre eux.

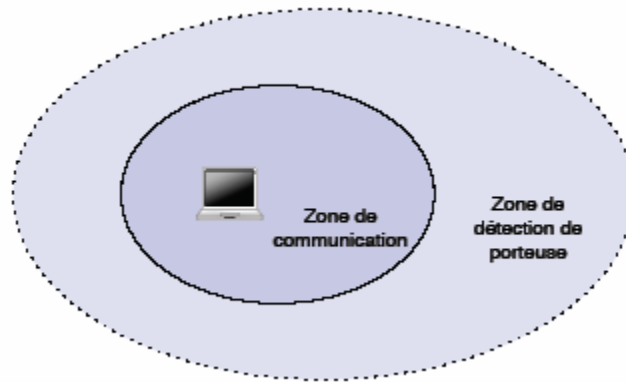


Fig1.3 Zones de communication et de détection de porteuse

2.4 Gestion d'énergie en mode Ad-Hoc

Les réseaux sans fil peuvent posséder des terminaux fixes ou mobiles. Le problème principal des terminaux mobiles concerne leur batterie, qui n'a généralement que peu d'autonomie. Pour augmenter le temps d'activité de ces terminaux mobiles, le standard prévoit un mode d'économie d'énergie.

Il existe deux modes de travail pour le terminal :

- Continuous Aware Mode ;
- Power Save Polling Mode.

Le premier correspond au fonctionnement par défaut : la station est tout le temps allumée et écoute constamment le support. Le second permet une économie d'énergie.

Dans ce second cas, les stations qui sont en mode normal stockeront les paquets pour les stations en mode économie d'énergie et vont jouer le rôle de tampon pour ces stations. Lorsqu'une station reçoit une trame pour une station qui est en mode économie d'énergie

et que celle-ci n'est pas active, il la stocke. La station qui la stocke doit être en mode normal pour remplir cette fonctionnalité. Elle émet ensuite des trames ATIM (*Ad-Hoc Traffic Information Map*) qui informent les stations en mode économie d'énergie, qu'il y a des paquets en attente pour elles. Lorsque, la station en mode économie d'énergie acquitte l'ATIM, la station qui a émis cette trame, lui fait suivre le paquet qu'elle a pour elle.

On peut ajouter que les stations en mode économie d'énergie ne pourront pas, du fait de leur mode de fonctionnement, fournir tout les services réseaux tel que le routage de paquets. Les réseaux Ad-Hoc multi-sauts s'appuient sur les stations en mode normal pour router les paquets vers leurs destinataires.

2.5 Auto configuration des adresses IP dans les réseaux ad hoc

Une spécification d'une auto configuration des adresses IP utilise les messages de protocoles de routage existants. Ce mécanisme ne garantit pas l'unicité dans des réseaux déconnectés.

La détection d'adresse dupliquée (DAD) est le processus par lequel un nœud qui manque une adresse IP détermine si une adresse IP candidate sélectionnée est valide ou non. Un nœud déjà équipé par une adresse IP participe dans le processus DAD dans le but de protéger son adresse IP d'être utilisée par un autre nœud.

D'abord un nœud sélectionne une adresse IP au hasard de 169.254/16. Puis le nœud génère une RREQ vers l'adresse sélectionnée au hasard. Si aucune RREP n'est retournée durant une certaine période, le nœud tente d'envoyer la RREQ un certain nombre de fois atteignant RREQ_RETRIES. Si après toutes les tentatives aucune RREP n'est reçue, le nœud considère que l'adresse n'est assignée à aucun autre nœud, et qu'il peut prendre cette adresse. Sinon, le nœud choisit de nouveau arbitrairement une autre adresse du même rang et le DAD recommence. [4]

3. le standard IEEE 802.11 en mode ad hoc

3.1 Le protocole IEEE 802.11

Le protocole 802.11 de l'Institute of Electrical and Electronics Engineers (IEEE), parfois nommé Wi-Fi, définit plusieurs couches physiques et une couche d'accès au médium pour les réseaux locaux sans fil (Wireless Local Area Networks — WLAN), il est spécifié en [2]. Dans sa première version définie en 1997, les transmissions infrarouges étaient envisagées, les versions les plus récentes du standard telles que IEEE 802.11b pour un débit partagé de 11Mbps, IEEE 802.11g avec un débit de 22Mbps ou encore IEEE 802.11a pour un débit de 56 Mbps sur la base desquelles sont construites l'essentiel des cartes d'interface commercialisées, s'adressent principalement à des transmissions radio fréquences.

3.2 Couches physiques

Les différentes couches physiques définissent différents codages permettant d'assurer une transmission sans fil fiable et un multiplexage de plusieurs canaux de transmission. Elles rendent possible des transmissions à des puissances limitées dans les bandes de

fréquences libres, en particulier la bande de fréquences dédiée aux mondes industriel, scientifique et médical (ISM) située aux alentours de 2.4 GHz, Suivant les pays, différentes fréquences (dans la bande 2.4 GHz, un sous-ensemble des canaux 1-14), différentes modulations sont autorisées avec différentes puissances.

La première déclinaison de cette norme définissait, en sus des transmissions infrarouges, les modalités de transmission dans cette bande de fréquences allant de 2 400MHz à 2 495 MHz. Elle proposait d'utiliser différentes techniques d'étalement de spectre.

Initialement le standard IEEE 802.11 permet l'utilisation de trois différentes technologies pour la couche physique :

- FHSS: Frequency Hopping Spread Spectrum.
- DSSS: Direct Sequence Spread Spectrum.
- IR : Infra Red.

Deux autres couches physiques ont été rajoutées par la suite par 802.11b (1999) pour permettre les hauts débits.

La première est une couche DSSS modifiée afin d'améliorer le débit jusqu' à 5,5 et 11 Mbps, initialement à 1 et 2 Mbps. La deuxième est OFDM (Orthogonal Frequency Division Multiplex) pour les débits jusqu' à 54 Mbps.

Les produits conformes au standard IEEE.802.11b se voient attribuées le logo Wi-Fi (Wire-less Fidelity). Ces produits utilisent la couche physique DSSS dans la bande de fréquence 2.4GHz.

3.3 Protocole d'accès au medium

Au-dessus des différentes couches physiques, la norme définit un unique protocole d'accès au médium, afin de gérer les accès concurrents à un même médium partagé. Ce protocole fait partie de la famille des protocoles de gestion des accès multiples par détection de porteuse avec évitement de collisions (Carrier Sense Multiple Access with Collision Avoidance — CSMA/CA). Il associe un mécanisme de détection de porteuse avant transmission à un mécanisme d'attente aléatoire permettant de limiter le nombre et l'impact des collisions.

En plus, le standard définit un mécanisme supplémentaire RTS/CTS (Request To Send/Clear To Send) pour éviter les collisions et le problème des nœuds cachés.

3.3.1 Description du protocole d'accès au medium

La norme IEEE 802.11 définit deux modes d'accès au médium adaptés aux transmissions radio : le mode centralisé (Point Coordination Function — PCF) peut être utilisé lorsque les communications sont gérées par une station de base fixe et le mode distribué (Distributed Coordination Function — DCF) est utilisé à la fois pour les communications via une station de base et pour les communications directes de mobile à mobile. C'est ce dernier mode qui est utilisé dans le cas des réseaux ad hoc.

Laisser les terminaux transmettre à leur guise ne conduit donc pas à une utilisation de la bande passante efficace.

Les terminaux attendent alors que le canal se libère avant d'émettre un signal. Ce principe simple constitue la base des protocoles dits à détection de porteuse (Carrier Sense Multiple Access — CSMA).

3.3.2 Principe de base

La fonction de coordination distribuée (DCF) du protocole IEEE 802.11 met en œuvre un certain nombre de mécanismes qui visent à éviter les collisions et non pas à les détecter. Elle fait à ce titre parti de la famille CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance).

Compte tenu de l'impossibilité pour les émetteurs de mesurer la qualité du signal au niveau du récepteur, chaque récepteur doit acquitter toute trame qui lui est explicitement destinée. Lorsqu'un terminal reçoit une trame de données, il procède à une détection d'erreurs au moyen d'un CRC standard IEEE sur 32 bits. Si la trame ne contient pas d'erreur, il renvoie à l'émetteur un acquittement. L'intervalle de temps séparant la fin de la réception de la trame de données et le début de l'émission de l'acquiescement est égal à une valeur constante SIFS (Short Inter Frame Spacing). Lorsqu'un terminal désire transmettre une trame, il s'assurera tout d'abord que le médium est libre durant un temps constant DIFS (DCF Inter Frame Spacing) plus long que SIFS afin de donner une priorité absolue aux acquiescements.

Le cas échéant, il effectue la transmission, puis attend l'acquiescement correspondant de la part du récepteur. L'absence de réception de cet acquiescement provoque la retransmission de la trame et ce processus sera répété jusqu'au succès de l'opération ou jusqu'à atteindre le nombre maximal de retransmissions autorisé. Dans ce dernier cas, la trame est détruite. La détection de porteuse permet d'éviter certains cas de figure dans lesquels deux émissions simultanées provoqueraient une collision au niveau d'un récepteur. Cependant, il est impossible de distinguer par ce biais les situations dans lesquelles deux émissions simultanées ne provoqueraient pas de collision, à l'image du scénario représenté en figure 1.4. Dans cette configuration, les émetteurs B et C se trouvent en zone de détection de porteuse, c'est-à-dire que les émissions de l'un bloquent le mécanisme de détection de porteuse de l'autre. Cependant, les deux récepteurs sont suffisamment éloignés des émetteurs perturbateurs pour autoriser la simultanéité des deux communications. Ce problème, connu comme le problème de la station exposée conduit à une sous utilisation de la capacité du canal radio.

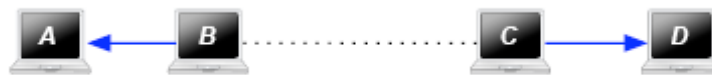


Fig. 1.4- problème de la station exposée

Si l'émetteur constate que le médium est déjà occupé lorsqu'il souhaite émettre, il reporte sa transmission jusqu'à la libération du médium. Lorsque le canal radio se libère, tout émetteur désirant accéder au médium attend un temps aléatoire en plus d'un intervalle DIFS.

Chaque émetteur potentiel tire de façon uniforme un nombre aléatoire (appelé backoff) dans un intervalle appelé fenêtre de contention. Cette valeur est ensuite décrémentée d'une unité à chaque intervalle de temps passé sans que le médium ne soit occupé. La première station à atteindre la valeur 0 émet alors sa trame. Les autres stations

suspendront le processus qui sera repris dès la fin de la transmission. Un nœud voulant émettre plusieurs trames en séquence devra passer par une procédure d'attente aléatoire entre deux trames afin de ne pas monopoliser le canal radio.

Ce mécanisme ne permet évidemment pas de supprimer les collisions entre trames. Si deux émetteurs tirent la même valeur aléatoire, ils émettront au même instant. [1]

3.3.3 Prévention de collision

Il est possible de précéder l'envoi de chaque trame de données par un échange de messages courts. L'émetteur envoie au récepteur une requête d'émission (Request To Send — RTS). Le récepteur, si le canal radio est disponible, autorise l'émetteur à transmettre par une confirmation (Clear To Send — CTS). À la réception de l'autorisation, l'émetteur transmet la trame de données. Tout mobile à portée radio de l'émetteur ou du récepteur captera l'une de ces trames contenant la durée de l'envoi de la trame correspondante. Ces voisins s'abstiendront alors de transmettre jusqu'à la fin de cette trame afin de ne pas provoquer de collision. Ce mécanisme permet de réduire l'impact des collisions puisqu'elles n'arriveront essentiellement que sur des trames courtes.

Ce mécanisme permet en outre de résoudre les situations comme celle qui est représentée en figure 1.5.

Dans ce scénario, appelé problème de la station cachée, deux émetteurs A et C souhaitent émettre une trame en direction du même récepteur B. A et C ne sont pas à portée radio et ne détectent donc pas les émissions de l'autre. Sans échange RTS-CTS préalable à la transmission, les deux trafics engendreraient régulièrement des collisions. Avant de transmettre une trame, A envoie un message RTS à B. B autorise la transmission en répondant par un message CTS à destination de A. Le médium radio étant par nature diffusant, ce message atteindra C qui sera alors informé que le médium sera occupé durant une durée correspondant à l'émission de la trame. C n'émettra alors pas durant cette période et ne provoquera pas de collision au niveau de B. Ce principe de réservation du médium est appelé détection de porteuse (Virtual Carrier Sense) et la période de réservation est appelée vecteur d'allocation du réseau (NAV — Network Allocation Vector).

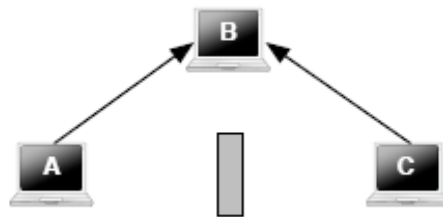


Fig 1.5- problème de la station cachée

Le mécanisme de RTS-CTS ne permet cependant pas de résoudre tous les cas de stations cachées.

Par exemple, considérons le scénario représenté en figure 1.6. Si C émet un RTS à destination de D au moment où B émet un CTS à destination de A, le CTS ne sera pas

compris par C et la transmission entre C et D pourra avoir lieu, provoquant une collision au niveau de B. Ce type de situation survient toutefois rarement puisqu'il est nécessaire que les émissions du RTS de C et du CTS de B débutent simultanément.

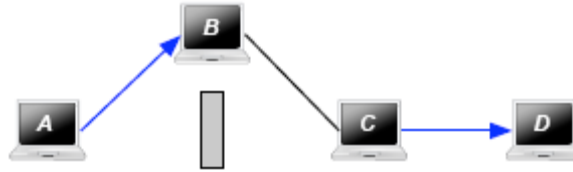


Fig. 1.6- situation mettant en défaut le mécanisme RTS-CTS

Les environnements mobiles sont caractérisés par de fréquentes déconnexions et des restrictions sur les ressources utilisées, surtout si tous les usagers du système sont mobiles ce qui est le cas pour les réseaux ad hoc. Ces limitations transforment certains problèmes, ayant des solutions évidentes dans l'environnement classique, en des problèmes complexes et difficiles à résoudre. Parmi ces problèmes figure le problème de routage que nous allons discuter dans le reste de ce chapitre. [1]

4. Routage dans les réseaux ad hoc

Généralement, le routage est une méthode d'acheminement des informations à la bonne destination à travers un réseau de connexion donné. Le problème de routage consiste pour un réseau dont les arcs, les nœuds et les capacités sur les arcs sont fixés à déterminer un acheminement optimal des paquets (de messages, de produits ...etc.) à travers le réseau au sens d'un certain critère de performance. Le problème consiste à trouver l'investissement de moindre coût en capacités nominales et de réserves qui assure le routage du trafic nominal et garantit sa surveillance en cas de n'importe quelle panne d'arc ou de nœud.

4.1 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.

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

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

Dans le cas où le nœud destination se trouve dans la portée de communication du nœud source le routage devient évident et aucun protocole de routage n'est initié. Malheureusement, ce cas est généralement rare dans les réseaux ad hoc. Une station source peut avoir besoin de transférer des données à une autre station (nœud intermédiaire) qui ne se trouve pas dans sa portée de communication ce qui nécessite un protocole de routage approprié.

Dans la pratique, le problème de routage est plus compliqué à cause de la non uniformité de la transmission sans fil et de la possibilité du déplacement imprévisible de tous les nœuds concernés par le routage.

4.2 La conception des stratégies de routage

L'étude et la mise en œuvre d'algorithmes de routage pour assurer la connexion des réseaux ad hoc au sens classique du terme (tout sommet peut atteindre tout autre), est un problème complexe. L'environnement est dynamique et évolue donc au cours du temps, 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'incident sur le bon acheminement des données. L'élimination d'un lien, pour cause de panne ou pour cause de mobilité devrait, idéalement, augmenter le moins possible les temps de latence.
- 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 de 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.

Ce chapitre a été axé sur le concept des réseaux ad hoc et ses caractéristiques et se finit par le problématique de routage dans les réseaux ad hoc et les stratégies faisant face à ces problématiques pour introduire les protocoles de routage et surtout le protocole AODV dans le chapitre suivant.

Chapitre 2

Présentation du protocole AODV

Dans la suite de chapitre on cite les protocoles de routage existant pour les réseaux ad hoc et leur classification selon deux critères.

Le protocole AODV fait le sujet principal de ce chapitre. On montre les paquets de contrôle utilisés par le protocole ainsi que sa table de routage et son mécanisme de fonctionnement en tant que découverte de route et maintenance des routes.

1. Les protocoles de routage dans les réseaux ad – hoc

Comme nous avons déjà vu, un réseau ad hoc est un ensemble de nœuds mobiles qui sont dynamiquement et arbitrairement éparpillés d'une manière où l'interconnexion entre les nœuds peut changer à tout moment. Dans la plupart des cas, l'unité destination ne se trouve pas obligatoirement dans la portée de l'unité source ce qui implique que l'échange des données entre deux nœuds quelconques, doit être effectué par des stations intermédiaires.

La stratégie de routage est utilisée dans le but de découvrir les chemins qui existent entre les nœuds. Le but principal d'une telle stratégie est l'établissement de routes qui soient correctes et efficaces entre une paire quelconque d'unités, ce qui assure l'échange des messages d'une manière continue. Vu les limitations des réseaux ad hoc, la construction des routes doit être faite avec un minimum de contrôle et de consommation de la bande passante.

Il existe deux grandes familles de protocoles de routage : les protocoles basés sur l'état des liens, et ceux basés sur le vecteur de distance.

Les deux méthodes exigent une mise à jour périodique des données de routage qui doivent être diffusées par les différents nœuds de routage du réseau. Les algorithmes de routage basés sur ces deux méthodes, utilisent la même technique qui est la technique des plus courts chemins, et permettent à un hôte donné, de trouver le prochain hôte pour atteindre la destination en utilisant le trajet le plus court existant dans le réseau.

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

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

Un problème de performance de cet algorithme est dû à l'absence de coordination entre nœuds, dans les modifications des tables de routage qui peuvent être faites en se basant

sur des données erronées (le problème de « *boucles de routage* »). En plus de cela, le DBF ne possède pas de mécanisme précis qui peut déterminer quand est ce que le réseau doit arrêter l'incrémentement de la distance qui correspond à une destination donnée, ce problème est appelé : « *comptage à l'infini* ».

La circulation inutile des paquets de messages, qui peut arriver avec le DBF, est intolérable dans les réseaux mobiles ad hoc, caractérisés par une bande passante limitée et des ressources modestes. En plus de cela, la mobilité fréquente des nœuds met que la convergence du DBF prend beaucoup de temps, ce qui pénalise le routage dans de tels environnements.

Les principaux protocoles de routage dans les réseaux sans fil ad hoc sont les suivants :

- DSR, Dynamic Source Routing.
- DSDV, Destination-Sequenced Distance Vector.
- AODV, Ad-hoc On Demand Distance Vector.
- TORA, Temporally-Ordered Routing Algorithm.
- OLSR Optimized Link State Routing Protocol.
- TBRPF, Topology Broadcast Based on Reverse-Path Forwarding.

Le classement de ces protocoles suivant les deux familles de protocoles est le suivant :

- État des liens : TORA, OLSR et TBRPF.
- Vecteur de distance : DSR, DSDV et AODV.

Suivant la manière de création et de maintenance de routes lors de l'acheminement des données, les protocoles de routage peuvent être séparés en :

- **Proactif** : DSDV, OLSR et TBRPF adoptent ce comportement. Les protocoles proactifs établissent les routes à l'avance en se basant sur l'échange périodique des tables de routage.
- **Réactif** (on demand) : TORA et AODV adoptent ce comportement. Les protocoles réactifs cherchent les routes à la demande. AODV est en fait une version réactive de DSDV.
- **Hybride** : les protocoles hybrides définissent deux zones où ils combinent le comportement proactif à l'intérieur d'une zone et le comportement réactif entre les zones. Par exemple DSR, qui est réactif à la base mais qui peut être optimisé s'il adopte un comportement proactif.

1.1 Les protocoles de routage proactifs

Les protocoles de routage proactifs essaient de maintenir les meilleurs chemins existants vers toutes les destinations possibles (qui peuvent représenter l'ensemble de tous les nœuds du réseau) au niveau de chaque nœud du réseau. Les routes sont sauvegardées mêmes si elles ne sont pas utilisées. La sauvegarde permanente des chemins de routage, est assurée par un échange continu des messages de mise à jour des chemins, ce qui induit un contrôle excessif surtout dans le cas des réseaux de grande taille.

1.2 Les protocoles de routage réactifs (à la demande)

Les protocoles de routage réactifs (dits aussi : protocoles de routage à la demande), représentent les protocoles les plus récents proposés dans le but d'assurer le service du routage dans les réseaux sans fil.

La majorité des solutions proposées pour résoudre le problème de routage dans les réseaux ad hoc, et qui sont évaluées actuellement par le groupe de travail MANET (Mobile Ad Hoc Networking Working Groupe) de l'IETF (Internet Engineering Task Force), appartiennent à cette classe de protocoles de routage.

Les protocoles de routage appartenant à cette catégorie, créent et maintiennent les routes selon les besoins. Lorsque le réseau a besoin d'une route, une procédure de découverte globale de routes est lancée, et cela dans le but d'obtenir une information. Le routage à la demande induit une lenteur à cause de la recherche des chemins, ce qui peut dégrader les performances des applications interactives (exemple les applications des bases de données distribuées). En outre, il est impossible de connaître au préalable la qualité du chemin (en termes de bande passante, délais,... etc.). Une telle connaissance est importante dans les applications multimédias.

2. Le protocole de routage AODV

2.1 Table de routage et paquets de contrôle

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

Le mécanisme de fonctionnement du protocole est détaillé dans [3].

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

L'AODV utilise une *requête de route* dans le but de créer un chemin vers une certaine destination.

Cependant, l'AODV maintient les chemins d'une façon distribuée en gardant une table de routage, au niveau de chaque nœud de transit appartenant au chemin cherché. Une entrée de la table de routage contient essentiellement :

- L'adresse de la destination.
- Le nœud suivant.
- La distance en nombre de nœud (i.e. le nombre de nœud nécessaire pour atteindre la destination).

- Le numéro de séquence destination qui garantit qu'aucune boucle ne peut se former.
- Liste des voisins actifs (origine ou relais d'au moins un paquet pour la destination pendant un temps donné).
- Le temps d'expiration de l'entrée de la table (temps au bout duquel l'entrée est invalidée).
- Un tampon de requête afin qu'une seule réponse soit envoyée par requête.

A chaque utilisation d'une entrée, son temps d'expiration est remis à jour (temps courant + active route time).

Si une nouvelle route est nécessaire, ou qu'une route disparaît, la mise à jour de ces tables s'effectue par l'échange de trois types de messages entre les nœuds :

- RREQ Route Request, un message de demande de route.
- RREP Route Reply, un message de réponse à un RREQ.
- RERR Route Error, un message qui signale la perte d'une route.

Format général d'une RREQ :

@source	Num. seq. Source	Broadcast id	@destination	Num. seq. Destination	Nombre de sauts
---------	---------------------	--------------	--------------	--------------------------	-----------------

Format général d'une RREP :

@source	@destination	Num. seq. destination	Nombre de sauts	life time
---------	--------------	--------------------------	-----------------	-----------

2.2 Fonctionnalité

Un nœud diffuse une *requête de route* (RREQ : Route REQuest), dans le cas où il aurait besoin de connaître une route vers une certaine destination et qu'une telle route n'est pas disponible (figure 3.9 (a)). Cela peut arriver si la destination n'est pas connue au préalable, ou si le chemin existant vers la destination a expiré sa durée de vie ou il est devenu défaillant (i.e. la métrique qui lui est associée est infinie). Le champ *numéro de séquence destination* du paquet RREQ, contient la dernière valeur connue du numéro de séquence, associé au nœud destination. Cette valeur est recopiée de la table de routage. Si le numéro de séquence n'est pas connu, la valeur nulle sera prise par défaut. Le *numéro de séquence source* du paquet RREQ contient la valeur du numéro de séquence du nœud source. Comme nous avons déjà dit, après la diffusion du RREQ, la source attend le paquet réponse de route (RREP : Route REPLY). Si ce dernier n'est pas reçu durant une certaine période (appelée RREP_WAIT_TIME), la source peut rediffuser une nouvelle requête RREQ.

Quand un nœud de transit (intermédiaire) envoie le paquet de la requête à un voisin, il sauvegarde aussi l'identificateur du nœud à partir duquel la première copie de la requête est reçue. Cette information est utilisée pour construire le chemin inverse (figure 3.9 (b)), qui sera traversé par le paquet *réponse de route* de manière unicast (cela veut dire qu'AODV supporte seulement les liens symétriques). Puisque le paquet *réponse de route*

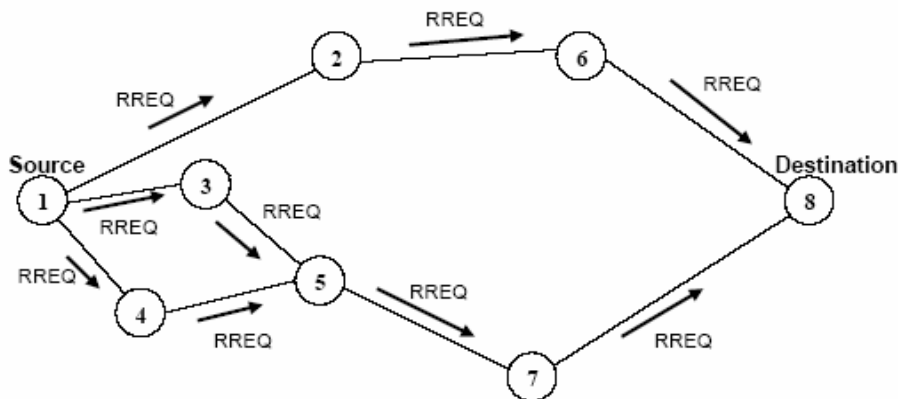
va être envoyé à la source, les nœuds appartenant au chemin de retour vont modifier leurs tables de routage suivant le chemin contenu dans le paquet de réponse (temps d'expiration, numéro de séquence et prochain saut).

Afin de limiter le coût dans le réseau, AODV propose d'étendre la recherche progressivement. Initialement, la requête est diffusée à un nombre de sauts limité. Si la source ne reçoit aucune réponse après un délai d'attente déterminé, elle retransmet un autre message de recherche en augmentant le nombre maximum de sauts. En cas de non réponse, cette procédure est répétée un nombre maximum de fois avant de déclarer que cette destination est injoignable.

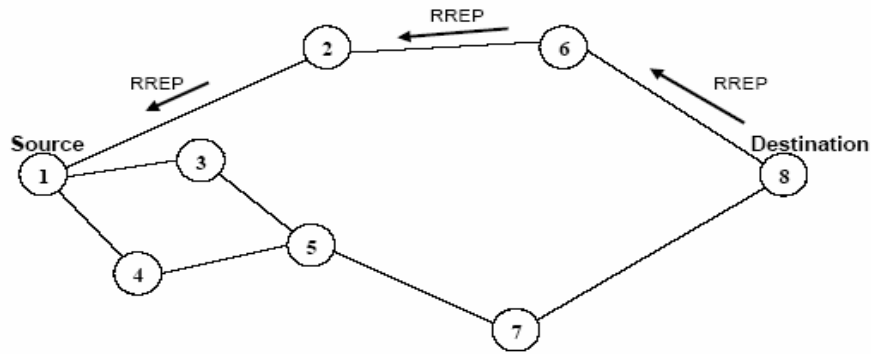
A chaque nouvelle diffusion, le champ *Broadcast ID* du paquet RREQ est incrémenté pour identifier une requête de route particulière associée à une adresse source. Si la requête RREQ est rediffusée un certain nombre de fois (*RREQ_RETRIES*) sans la réception de réponse, un message d'erreur est délivré à l'application.

La destination renvoie un message RREP, ce message peut donc être acheminé vers la source. Chaque nœud traversé incrémentera le nombre de sauts. Et ajoutera une entrée à sa table pour la destination.

Une réponse adéquate peut aussi être donnée par un nœud situé entre la source et la destination. Dans ce cas l'obtention de routes bidirectionnelles est néanmoins possible grâce au drapeau "Gratuitous RREP". Le nœud intermédiaire enverra alors en plus un RREP vers la destination. Les nœuds entre le nœud intermédiaire et la destination ajouteront donc à leur table une entrée vers la source du RREQ. Cette disposition permettra à la destination d'envoyer directement des paquets à la source sans devoir procéder à la recherche d'une route. C'est utile lors de l'établissement de communications TCP pour l'envoi du premier ACK.



(a) La propagation du paquet RREQ (requête de route).



(b) Le chemin pris par le paquet RREP (requête de réponse).

Figure 3.9 : Les deux requêtes RREQ et RREP utilisées dans le protocole AODV.

2.3 Maintenance des routes

Afin de maintenir des routes consistantes, une transmission périodique du message « HELLO » (qui est un RREP avec un TTL de 1) est effectuée. Si trois messages « HELLO » ne sont pas reçus consécutivement à partir d'un nœud voisin, le lien en question est considéré défaillant. Les défaillances des liens sont, généralement, dues à la mobilité du réseau ad hoc. Les mouvements des nœuds qui ne participent pas dans le chemin actif, n'affectent pas la consistance des données de routage. Quand un lien, reliant un nœud p avec le nœud qui le suit dans le chemin de routage, devient défaillant, le nœud p diffuse un paquet *UNSOLICITED RREP*, avec une valeur de numéro de séquence égale à l'ancienne valeur du paquet RREP incrémentée d'une, et une valeur *infinie* de la distance. Le paquet *UNSOLICITED RREP* est diffusé aux voisins actifs, jusqu'à ce qu'il arrive à la source. Une fois le paquet est reçu, la source peut initier le processus de la découverte de routes.

L'AODV maintient les adresses des voisins à travers lesquels les paquets destinés à un certain nœud arrivent. Un voisin est considéré actif, pour une destination donnée, s'il délivre au moins un paquet de données sans dépasser une certaine période (appelée *active timeout period*). Une entrée de la table du routage est active, si elle est utilisée par un voisin actif. Le chemin reliant la source et la destination en passant par les entrées actives des tables de routage, est dit un *chemin actif*. Dans le cas de défaillances de liens, toutes les entrées des tables de routage participantes dans le chemin actif et qui sont concernées par la défaillance sont supprimées. Cela est accompli par la diffusion d'un message d'erreur entre les nœuds actifs.

Le protocole de routage AODV, n'assure pas l'utilisation du meilleur chemin existant entre la source et la destination. Cependant, des évaluations de performances récentes ont montré qu'il n'y a pas de grandes différences (en terme d'optimisation) entre les chemins utilisés par le protocole AODV et celles utilisées par les protocoles basés sur les algorithmes de recherche des plus courts chemins. En plus de cela, le protocole AODV ne présente pas de boucle de routage, et évite le problème « comptage à l'infini » de

Bellman-Ford, ce qui offre une convergence rapide quand la topologie du réseau ad hoc change. En effet :

Dans AODV, chaque nœud maintient une table qui contient une entrée pour chaque destination accessible. Pour éviter le problème du comptage à l'infini de Bellman-Ford. On a recours à l'utilisation de numéros de séquences dans les tables de routage en plus de la distance.

Chaque nœud possède un numéro de séquence. Il est le seul habilité à l'incrémenter.

Ce numéro personnel ne peut être incrémenté que dans deux situations :

- Avant d'entreprendre un processus de recherche de route par l'envoi d'un paquet RREQ, le nœud incrémente son numéro.
- Avant de répondre à un message RREQ par un message RREP, le numéro de séquence doit être remplacé par la valeur maximale entre son numéro de séquence actuel et celui contenu dans le message RREQ.

Ce numéro accompagne son adresse dans les messages de contrôle et permet aux autres de distinguer les messages importants des messages redondants.

Une mise à jour de la table de routage ne s'effectue que si les conditions suivantes sont observées :

- Le numéro de séquence du paquet de contrôle est strictement supérieur au numéro de séquence présent dans la table.
- Les numéros de séquence (de la table et du paquet) sont égaux mais, la distance en nombre de sauts du paquet plus 1 est inférieure à la distance actuelle dans la table de routage.
- Le numéro de séquence pour cette destination est inconnu.

Cette façon de procéder garantit la création de route sans boucles.

Donc, Si la source se déplace, la procédure de détermination de route peut être ré initié.

- Si un nœud intermédiaire ou la destination se déplacent, un RREP spécial est émis au nœud source (reconstruisant la route au passage).
- Messages *hello* périodiques pour détecter les coupures de lien.

2.4 Gestion de la connectivité locale

Lorsqu'un nœud reçoit un paquet en Broadcast, il met à jour ses informations de connectivité locale pour s'assurer qu'elles incluent ce voisin.

Si aucun paquet n'est émis aux voisins actifs pendant le dernier `hello_interval`, un nœud va envoyer un hello (RREP non sollicité) contenant :

- son identité.
- son numéro de séquence (non modifié pour les hello).
- time to live de 1 pour ne pas être retransmis.
- liste des nœuds pour lesquels il a reçu un hello.

Après avoir explicité le fonctionnement du protocole AODV et le format de ses paquets, l'extension de ce protocole pour garantir des exigences de la qualité de service est traité dans le chapitre suivant

Chapitre 3

Introduction de la qualité de service dans le protocole AODV

Ce chapitre traite une solution qui permet d'étendre le protocole AODV pour garantir de la qualité de service en termes de bande passante. On a commencé par présenter la notion de qualité de service et ses solutions dans les réseaux ad hoc et on s'est intéressé au routage AODV avec qualité de service et ses problématiques. On a explicité la solution à implémenter pour dégager le comportement du protocole AODV suite à l'introduction d'un contrôle d'admission des nouvelles connexions en se basant sur la bande passante disponible au niveau de chaque nœud. En effet l'estimation de la bande passante disponible et les extensions nécessaires au protocole AODV pour garantir de la qualité de service sont bien précisés et sont suivis par une description du nouveau fonctionnement du protocole.

Ce chapitre finit par l'exposition des limitations de la solution proposée et par la mise en clair des considérations à bien tenir en compte dans un contexte de réservation de la bande passante dans les réseaux ad hoc surtout au niveau du routage par flux, le contrôle de congestion, le dépassement de la capacité du médium et de la connaissance du voisinage étendu au niveau de chaque nœud.

1. Qualité de service

La différenciation des services est la dernière méthode proposée permettant à internet de fournir d'autre services de transfert que le traditionnel « service au mieux » (BE : best effort).

Dans le domaine des réseaux, la notion de qualités de services ou QoS (Quality of Service) est évoqué pour désigner la capacité du réseau à fournir un service : transfert de données par exemple.

La performance d'un réseau est un élément fondamental et nécessaire pour l'utilisation d'applications, notamment les applications temps réels. Les protocoles de l'internet subissent des fortes pressions pour offrir des garanties de qualité de service. Ces demandes proviennent des applications multimédias réparties. Ces applications exigent un transfert de données complexe telles que la téléphonie, la vidéo à la demande ou la conférence multimédia.

La QoS au niveau d'un réseau se décline en quatre paramètres : débit, latence, la gigue et la perte.

Le débit communément appelé « bande passante » représente la ressource de transmission qu'occupe ou reçoit un flot. La gestion de la bande passante est un élément important pour la garantie de la qualité de service. La latence est définie par le délai de transfert de bout en bout d'un paquet d'un flot. Les applications interactives ont une latence maximale tolérable. Si un paquet subit un retard important, au-delà de la valeur tolérable, les données qu'il contient deviennent inutiles pour l'application. La gigue correspond aux variations de latence des paquets. La cause principale de l'apparition de la gigue dans les flots provient des changements d'intensité de trafic sur les liens de sorties des commutateurs. La perte signifie la perte de paquets. Elle se produit lorsqu'il y a des erreurs d'intégrité sur les données. Dans les réseaux actuels où la qualité des transmissions est très bonne, cette cause est marginale. La perte de paquet se produit principalement lorsque l'intensité du trafic sur les liens de sorties devient supérieure à leur capacité d'écoulement. Elle est une indication de congestion.

Ces quatre paramètres, à priori indépendants, sont en vérité tous concernés par la congestion. En l'absence de congestion, chaque flot peut utiliser le niveau de bande passante qu'il souhaite, aucun paquet n'est perdu, la latence est minimale et la gigue est quasiment nulle. Ces paramètres se dégradent quand la contention sur les ressources augmente. La congestion est si répandue dans l'Internet d'aujourd'hui, qu'aucun des 4 paramètres ne peut être garanti. C'est la raison pour laquelle on qualifie le service rendu de BE : il traite tous les paquets de la même manière quel que soit le service qu'il souhaiterait recevoir.

La solution tient donc à la capacité du réseau à isoler les flots pour leur fournir la QoS requise. L'isolation des flots consiste à fournir aux flots demandant une QoS particulière une protection contre les flots perturbateurs et autres trafics BE.

Le routage au mieux consiste souvent à rechercher le plus court chemin en termes de distance entre une source et une destination afin de transférer des données. Dans le cas du routage avec qualité de service, le but n'est pas simplement de trouver le meilleur chemin selon un certain critère mais de trouver le meilleur chemin admissible. Pour cela, un certain nombre de contraintes sur les routes sont imposées afin de déterminer leur éligibilité. Par exemple, on peut vouloir rechercher une route disposant d'une certaine quantité de bande passante pour un trafic vidéo ou une route assurant que les paquets seront reçus par la destination moins d'un certain temps après leur émission par la source. Toute route satisfaisant un certain critère quantitatif peut être qualifiée de route assurant une certaine qualité de service.

Les métriques de QoS peuvent être additives, concaves ou multiplicatives. La bande passante est une métrique concave, alors que le délai et la gigue sont des métriques additives. La disponibilité d'un lien, basée sur des critères comme la probabilité de perte du lien quant à elle est une métrique multiplicative.

Une métrique additive A_m est définie comme $\sum_{i=1}^h L_i(m)$ où $L_i(m)$ est la valeur de la métrique m sur le lien L_i et $L_i \in P$. h représente la longueur du chemin P .

Une métrique concave définit la valeur minimale sur un chemin P et représenté comme suit : $C_m = \min(L_i(m)), L_i(m) \in P$.

Une métrique multiplicative représente le produit des valeurs des métriques de QoS, elle est définie comme le produit des $L_i(m)$ avec i allant de 1 à h , $L_i(m) \in P$.

Pour trouver une route qui satisfait une métrique concave, les ressources disponibles dans chaque lien doivent être au moins égales à la valeur désirée de la métrique.

2. Qualité de service pour les réseaux ad hoc

Les solutions de qualité de service pour les réseaux ad hoc peuvent être classifiées en quatre catégories :

- Les modèles de qualité de service regroupent les définitions d'architectures destinées à assurer une certaine qualité de service (par exemple intserv et diffserv)

- Les mécanismes de réservation définissent un ensemble de messages de contrôle, destinés par exemple à provoquer la réservation de ressources dans les routeurs (par exemple RSVP). [7]
- Les protocoles de routage avec qualité de service sont chargés de la recherche de routes répondant à certains critères.
- Différenciation des services fournissent un ensemble d'outils permettant de mettre en œuvre certaines règles de qualité de service.

La première architecture de qualité de service a été définie par IETF et nommée Integrated Services ou Intserv. [5] Ce modèle est défini pour assurer aux différents flux de données des garanties sur le délai de bout en bout, le débit, etc.

L'architecture Differentiated Services (DiffServ) [6] définit plusieurs classes de trafic, les différents flux s'intégrant à une de ces classes afin de bénéficier des garanties correspondantes.

Le modèle de qualité de service proposé par Xiao et al, a Flexible Quality of Service Model for Mobile Ad Hoc Networks (FQMM) définit une architecture hybride adaptée à des réseaux ad hoc de taille moyenne. Ce modèle définit plusieurs classes de trafic, l'une de ces classes étant dédiée aux réservations explicites de bande passante. Le routage est assuré par un protocole de routage au mieux et une vérification à posteriori du respect des contraintes est effectuée.

Le modèle Two-Layered Quality of Service Model for Reactive Routing Protocols for Mobile Ad Hoc Networks (2LqoS) proposé par Nikaein et al considère deux types de métriques de qualité de service afin de définir des classes de trafic. Les métriques en rapport avec le bon fonctionnement du réseau, telles que le nombre de sauts des routes, le niveau de batteries des mobiles routeurs, ou encore la stabilité des routes sont utilisées lors de la découverte de chemin.

Le modèle in-band signaling protocol (INSIGNIA) désigné explicitement pour les réseaux ad hoc et doit être intégré dans un protocole de routage pour les réseaux ad hoc. D'autres modèles de qualité de service ont été proposés dans la littérature et s'adressant à plusieurs aspects de qualité de service.

Les protocoles de différenciation de services cherchent à mettre en œuvre des priorités entre différents flux ou différents terminaux. Au sein d'un même mobile il est possible de définir des priorités entre plusieurs flux émis ou routés au moyen des files d'attente dont le fonctionnement est plus souple que la simple file FIFO. Une multitude de politiques de gestion de files d'attente sont envisageables telle que la file à priorité (priority queing), tourniquet (round robin) et les files de type weighted fair queing.

On s'intéresse dans notre stage aux protocoles de routage avec qualité de service en particulier le protocole AODV. Le contrôle d'admission, l'équilibrage de la charge du réseau ainsi que la recherche de routes répondant aux critères des applications sont en général les tâches incombant à un protocole de routage avec qualité de service.

3. Le routage AODV avec qualité de service

L'introduction de la qualité de service dans AODV repose sur l'ajout d'un champ dans les paquets de contrôle RREQ, RREP. Ce champ peut être associé au paramètre délai ou

au paramètre bande passante. À la réception d'un message RREQ, chaque mobile vérifie qu'il est en mesure d'honorer le service demandé, avant de retransmettre le message.

Le protocole de routage AODV avec QOS a pour objectif de :

- Améliorer la QOS dans les réseaux ad hoc.
- Introduire une métrique plus appropriée que la distance (nombre de sauts).
- faire face aux changements fréquents de la topologie due à la mobilité des nœuds.

Dans ce qui suit on présente une proposition qui intègre de la qualité de service dans le protocole AODV en termes de bande passante.

3.1 Problématiques de réservation de bande passante

Tout mécanisme de réservation repose sur un mécanisme de contrôle d'admission qui doit d'être le plus fiable possible. En effet, il est indispensable, lorsqu'on souhaite offrir des garanties en termes de bande passante il faut évaluer de façon précise la disponibilité des ressources. Dans les réseaux filaires, mesurer la disponibilité des ressources revient à évaluer la capacité résiduelle des liens du réseau.

Le médium radio, en revanche, est un médium partagé. Il n'est pas possible d'isoler des liens. Lorsqu'une trame est émise, elle est reçue par l'ensemble des mobiles dans une certaine zone géographique, la couche MAC déterminant alors si la trame doit être transmise à la couche IP ou tout simplement ignorée.

Le contrôle d'admission devra simplement s'assurer, que nulle part dans le réseau, la capacité du médium n'est dépassée. En d'autres termes, pour chaque mobile du réseau, il convient de s'assurer que la somme des émissions de chaque nœud et des nœuds voisins ne dépasse pas la capacité du médium.

En réalité l'estimation de la bande passante est un problème difficile, d'une part à cause du problème de la station cachée et des interférences pouvant survenir dans un contexte multi sauts, et d'autre part à cause des variations de topologie liées à la mobilité des nœuds et des variations de charge du réseau liées à l'apparition et à la disparition des flux.

On propose un mécanisme de réservation consistant à apporter à chaque mobile la connaissance du volume de trafic émis dans son voisinage à un seul saut.

3.2 Estimation de la bande passante

Deux méthodes sont envisageables pour estimer la bande passante. La première consiste à écouter le support de transmission et estimer la bande passante comme étant le rapport entre le temps durant lequel le médium est libre et celui durant lequel le médium est occupé en utilisant 802.11 MAC. La deuxième consiste à la dissémination des informations concernant la bande passante en utilisant les messages « Hello » et un nœud doit calculer sa bande passante disponible en se basant sur la consommation de la bande passante indiquée dans les messages « Hello ».

La première méthode compte la bande passante utilisée mais ne distingue pas le coût de la bande passante correspondante à chaque connexion et par suite ne peut pas la libérer ce qui affecte énormément la précision de l'estimation de la bande passante suite à une cassure d'une route.

On adopte la deuxième méthode pour l'estimation de la bande passante puisqu'elle prévient la génération des messages de contrôle supplémentaires en utilisant les messages « Hello » pour disséminer l'information de bande passante et permet la libération des ressources suite à des cassures de routes ou à la dégradation des exigences de qualité de service.

On considère dans le modèle de réservation de la bande passante le suivant :

- La capacité du support de transmission sans fil (wireless media) utilisé par les connexions avec Qos en chaque nœud mobile (MN) est $\leq Q$ bps
- Un appel à un contrôle d'admission (CA) est utilisé pour bloquer des nouvelles connexions si les contraintes de qualité de service ne sont pas disponibles. Ce contrôle d'admission est simple puisqu'on considère des sources de trafic CBR et qui sont entièrement définies par leur débit. La session ne sera pas acceptée que si le débit demandé par la source ajouté au chargement courant d'un lien est inférieur à la capacité du lien et ce, pour tous les liens de la route.

On qualifie le trafic de Qos généré ou en transit en un nœud MN_i par la réservation de bande passante (x_i) au nœud MN_i .

Si r_{ij} la quantité de trafic avec Qos envoyé de MN_i à MN_j alors :

$$x_i = \sum r_{ij} \text{ tel que } j \in N_i \quad (1)$$

Où N_i est l'ensemble des nœuds voisins de MN_i , par exemple $\{MN_j / j \in N_i\}$ est l'ensemble des nœuds voisins de MN_i .

On définit la bande passante maximale disponible MAB_i pour allouer des nouvelles réservations au nœud MN_i comme suit :

$$MAB_i = Q - x_i \quad (2)$$

On définit la bande passante disponible AB_i , pour allouer des nouvelles réservations au nœud MN_i par :

$$AB_i = \min \{MAB_i, MAB_j\}, j \in N_i \quad (3)$$

Effectuer une simple comparaison du débit demandé par l'application et de la bande passante disponible ne prend pas en compte le fait que ce flux sera routé par des mobiles voisins du nœud effectuant le contrôle d'admission. Pour cela le contrôle d'admission que nous proposons tient en compte ce fait et on prévient le problème de sous-estimation de l'impact des flux interférents de la manière suivante : Lors du contrôle d'admission,

on estime le nombre de ré émissions de la requête de route dans la zone de couverture du nœud recevant cette requête avant de parvenir à destination. Ce phénomène est pris en considération en multipliant, lors du contrôle d'admission de la requête de route, la bande passante demandée par le nombre de ces ré émissions.

Si le mobile concerné est la source de la requête de route et si la destination n'est pas dans sa liste de voisins, il sait que le flux devra être retransmis sur le lien vers cette destination sinon le flux devra être retransmis au moins sur deux liens vers la destination. Alors que si le mobile concerné est un nœud intermédiaire et la destination se configure dans la liste de ses voisins alors on considère le lien duquel le flux provient et le lien sur lequel il va être routé vers la destination. Alors que si la destination ne se configure pas dans sa liste des voisins, on considère le lien duquel le flux provient et on considère qu'il sera routé au moins deux fois avant de parvenir à destination.

On note $MN_i \rightarrow MN_j$ deux nœuds consécutifs appartenant à un même chemin à réserver pour une connexion de Qos. On suppose qu'une nouvelle connexion de Qos demande r bps à établir. Une nouvelle réservation au nœud MN_i est satisfaite si le contrôle d'admission CA suivant est rempli :

Si la connexion de Qos est générée par le nœud MN_i :

- accepter si la destination est un nœud voisin et $AB_i \geq r$
- accepter si la destination n'est pas un nœud voisin et $AB_i \geq 2r$

Si la connexion de Qos est générée par autre nœud MN (trafic en transit) :

- accepter si la destination est un nœud voisin et $AB_i \geq 2r$
- accepter si la destination n'est pas un nœud voisin et $AB_i \geq 3r$

Sinon la requête de réservation n'est pas admise. On note que ces conditions doivent être remplies par chaque nœud le long de la route.

Dans ce schéma de réservation de la bande passante, On traite le problème de réservation en tenant en compte la bande passante disponible dans la zone de couverture du nœud et le trafic généré et diffusé par les voisins et les unités mobiles interférents dans la zone de couverture du nœud.

3.3 Intégration dans AODV

Plusieurs extensions doivent être introduites dans la structure de la table de routage, dans la requête de route (RREQ) et dans la réponse de route (RREP) pour que le modèle de réservation décrit précédemment soit intégré dans le protocole AODV. Pour les extensions on s'inspire des travaux faits par MANet. [8]

3.3.1 Extensions dans les messages Hello

Les messages Hello d'AODV doivent être modifiés de façon que chaque nœud MN_i connaît une valeur concernant ses voisins : la bande passante maximale disponible ($MAB_j, j \in N_i$). Cela peut être implémenté de façon que chaque nœud MN_i diffuse des paquets HELLO contenant MAB_i .

L'émission régulière de ces informations permet de rendre compte de l'évolution du réseau, due à l'apparition ou à la disparition de routes, ou à la mobilité des nœuds.

3.3.2 Extensions dans la table de routage

On ajoute à chaque entrée dans la table de routage correspondant à chaque destination demandant de Qos la bande passante minimale disponible.

3.3.3 Extensions des RREQ et RREP

La requête de route est étendue pour inclure un champ qui spécifie la bande passante demandé par l'application. Alors que la réponse de route est étendue pour inclure un champ qui spécifie la bande passante accordé à l'application ou garantie.

3.4 Découverte des routes du protocole AODV avec Qos

Chaque nœud MN_i collecte les messages Hello de ses voisins pour calculer sa bande passante disponible.

A la réception de RREQ, un nœud intermédiaire applique le contrôle d'admission décrit précédemment. La bande passante demandée n'est plus modifiée par les nœuds. Si la réservation est admise, la RREQ est diffusée sinon elle est détruite. En tout cas la réservation n'est faite que si la RREP est reçue par la source de la destination. En opposition avec AODV, si un nœud intermédiaire a une route disponible vers la destination, ce nœud ne peut pas envoyer un RREP destinée à la source car ce nœud ne connaît pas a priori l'état de l'ensemble des mobiles intermédiaires en aval sur la route. Dans le but de prévenir cette situation, le drapeau D de RREQ est activé indiquant que seule la destination peut envoyer un RREP.

La destination envoie un paquet RREP si la demande est satisfaite. A la réception du RREP chaque nœud intermédiaire compare sa BP disponible à la bande passante indiquée dans l'extension, si sa BP disponible est inférieur à la bande passante indiquée dans l'extension il met à jour le champ de la BP du RREP avant de le retransmettre sinon il le retransmet directement.

C'est à ce moment que les ressources nécessaires sont réservées définitivement sur chaque nœud. La communication entre source et destination peut alors avoir lieu au débit requis par la source, jusqu'à ce que l'une des extrémités ferme la connexion, ou jusqu'à ce que la route utilisée se brise ou se dégrade.

3.5 Maintenance des routes du protocole AODV avec QoS

AODV détecte une cassure de route grâce aux messages « Hello ». Si un nœud ne reçoit pas un message « Hello » d'un certain voisin durant un intervalle de temps prédéfini, il marque les routes utilisant ce voisin comme invalide et envoie un message d'erreur aux voisins en amont de la route. Seule la source initie de nouveau une procédure de découverte de route après avoir reçu le message d'erreur.

Lorsqu'une route disparaît du fait de la mobilité d'un routeur, les nœuds se situant après le point de cassure n'ont plus de paquets à transmettre, qu'il s'agisse de paquets de

données effectifs ou de paquets de rafraîchissement de route. En revanche, les routeurs en situés avant le point de cassure continueront à retransmettre les paquets du flux, ceux-ci étant perdus au niveau du dernier routeur avant le point de cassure. C'est ce dernier routeur qui pourra avertir la source de la cassure par l'envoi d'un message explicite (un message d'erreur) qui traversant les routeurs, provoquera la libération des ressources. A la réception d'un tel message, la source devra effectuer de nouveau une recherche de route.

Une autre situation pouvant conduire à l'émission d'un paquet RERR est la dégradation de la bande passante, à cause d'une augmentation des interférences. Ce mécanisme nécessite une surveillance de la valeur de la bande passante disponible ce qui n'est pas pris en considération dans notre implémentation.

Généralement les erreurs de routes et les coupures de route impliquent les étapes suivantes :

- invalider des routes existantes.
- Lister les destinations affectées.
- Déterminer les voisins affectés.
- Délivrer un message d'erreur de route approprié à chacun des voisins.
- Libérer les ressources allouées.

4. Limitations

La solution déjà présenté dans le but de l'intégrer dans le protocole AODV a été proposé dans le but de conclure l'impact de l'introduction d'un contrôle d'admission des connexions basé sur la disponibilité de la bande passante dans le protocole AODV, pour des applications demandant un même débit de 80kbps.

Or toutes les applications n'ont pas les mêmes contraintes de qualité de service ainsi suite à des erreurs de routes déjà établies ou à la dégradation de la qualité de service sur une route active, une libération des ressources allouées pour chaque application doit être bien accomplie. Dans ce but un identifiant de flux doit être associé à une application réservant de la qualité de service. En utilisant Ipv6 [9] ce qui permet la spécification des labels aux flux. Les connexions seront identifiées par un triplet <adresse source, adresse destination, label de flux > qui sera l'identifiant de l'entrée de la table de routage. On note que des paquets des flux différents suivent différents chemins vers la même destination, on parle donc d'un routage par flux.

La réservation effective de la bande passante dans un réseau ad hoc réside un problème difficile à assurer et donc plusieurs considérations qu'on va citer dans la suite doivent être prises en compte.

4.1 Identification des brouilleurs potentiels :

Les réseaux ad hoc sont sensibles au phénomène d'interférences ; deux communications non voisines directement mais s'effectuant dans une même zone d'interférences vont se partager la bande passante.

L'identification des brouilleurs potentiels est une tâche nécessaire lorsqu'on souhaite effectuer un contrôle d'admission, elle ne peut s'effectuer que si l'on peut communiquer avec eux ou s'il existe un nœud intermédiaire pour relayer les informations.

Transmettre dans les paquets Hello des informations sur le voisinage direct pour calculer la bande passante disponible ne permet donc pas de prendre en compte toutes les émissions interférences lors du contrôle d'admission. Il est alors légitime d'accroître la vision des nœuds en ne transmettant plus uniquement le voisinage direct mais le voisinage à deux ou trois sauts dans chaque paquet Hello.

Dans ce cas la stratégie de maintenance des routes d'AODV pour le routage Qos ne peut pas être directement utilisée. En effet L'intervalle de temps séparant la cassure de la route et l'initiation d'une nouvelle découverte d'une route est de quelques millisecondes. Et les tables des voisins concernant leur bande passante consommée par chacun ne sont pas encore mises à jour quand la nouvelle RREQ arrive. Il faut incorporer une mise à jour obligatoire dans la stratégie de maintenance des routes. Des messages particuliers « immediate Hello » peuvent être utilisés pour ce but. Le contenu de ce message particulier est le même que celui des messages « Hello » à l'exception que le type du paquet est marqué « immediate Hello » dans le but de différencier les messages réguliers « Hello ».

Si une cassure de route se produit un message « immediate Hello » est envoyé vers les nœuds situés avant la cassure de la route et est suivi par le message d'erreur. Quand un nœud reçoit le message « immediate Hello » il émet ses messages «Hello» réguliers immédiatement à ses voisins.

4.2 Dépassement de la capacité du médium et contrôle de congestion

Puisque la topologie du réseau ad hoc n'est pas connue à priori et évolue au cours du temps, alors nombreuses situations peuvent s'occourir mettant en défaut le mécanisme de contrôle d'admission.

Un mauvais contrôle d'admission se traduira par l'acceptation de trafics qu'il n'est pas possible de router. Par ailleurs, la mobilité de certains nœuds modifiera l'état des ressources disponibles d'autres nœuds alors que ces derniers sont en train de retransmettre des flux acceptés au préalable. Chacune de ces deux situations se traduira par un dépassement local de la capacité du médium, provoquant des pertes de paquets, un accroissement des délais de transmission et un remplissage des files d'attente important.

Toutes les applications n'ont pas les mêmes contraintes. Certaines applications, comme le transfert de données pourront être ralenties de façon quelconque sans que cela ait un impact sur le bon déroulement des opérations. Les applications présentant de fortes contraintes de délais, comme la voix, ne devraient pas subir de dégradation du fait de congestion. Le fait de les router de nouveau dans certains cas présente un coût raisonnable. Enfin, certaines applications dites adaptatives, pourront modifier leur débit d'émission en fonction des conditions du réseau pour peu qu'elles soient averties des changements.

Pour faire face à ces situations on propose que chaque requête de route ne contienne pas uniquement une demande de bande passante mais aussi un profil de dégradation. Ce profil sera constitué de deux valeurs : un incrément et un seuil. Lorsqu'un routeur constate une dégradation des performances, il examine les différents profils de dégradation des connexions et retranchera de la bande passante allouée à chaque connexion l'incrément. Si l'application émettrice l'a spécifié dans la requête de route, elle sera avertie de ce changement, lui permettant d'adapter son débit d'émission aux nouvelles conditions du réseau. Lorsque décrémenter le débit d'un flux conduirait à dépasser le seuil prescrit par l'application émettrice, la route est considérée comme cassée et un message est envoyé à la source afin qu'elle effectue une nouvelle demande de route. Un message de libération des ressources est envoyé en parallèle à la destination.

4.3 Contrôle du trafic

Le contrôle du trafic ne peut être mis en œuvre que si on est capable d'identifier pour chaque paquet le flux auquel il appartient.

Une fois les flux de données sont bien identifiés, le contrôle de trafic est mis en œuvre grâce à des seaux percés à jetons (token buckets). Cette structure permet d'éviter que trop de données ne soient émises simultanément par suite le débit du flux est uniformisé. On obtient donc un lissage de trafic ce qui permet de garantir que le débit demandé ne sera pas dépassé. Sinon les nœuds devront maintenir des statistiques pour vérifier que la bande passante effective de chaque flux est bien égale à celle demandé et générer des erreurs de routage si la bande passante effective vient de se dégrader.

La coexistence du trafic au mieux avec les trafics privilégiés sur le même canal impose la limitation du trafic au mieux au plus juste sans sur-limiter ce type de trafic. En effet il peut être contrôlé en chaque nœud du réseau à l'aide d'un seau percé de sorte à ne pas saturer la bande passante et empêcher les nœuds d'honorer les requêtes de qualité de service qu'ils ont acceptées.

On note que La gestion des ressources par flot nécessite le stockage et la maintenance de nombreux états dans chaque routeur. Ce type de mécanisme est donc impossible à appliquer dans des réseaux à grande échelle tels que l'Internet, car le surcoût en traitement engendré dans les routeurs des réseaux d'interconnexion serait trop élevé et dégraderait les performances globales du réseau de façon significative.

Dans ce chapitre, on a introduit la notion de qualité de service en se concentrant sur le routage AODV avec qualité de service. Une proposition d'un schéma de réservation de bande passante est présentée pour être implémentée et elle est étendue pour concerner un routage par flux garantissant de la qualité de service aux applications en clarifiant les situations à prendre en compte pour de telles garanties.

Chapitre 4

Simulation d'AODV

Dans ce chapitre on évalue la performance du protocole AODV au moyen du simulateur NS2. On présente tout d'abord l'outil de simulation NS2 et le modèle de réseau sous NS. Plusieurs modèles de propagation radio et des modèles de mobilité supportés par NS sont ensuite listés pour permettre le choix d'un modèle de simulation suivant lequel les métriques de performance du protocole AODV sont évaluées. Une fois que le modèle de simulation est précisé, ces métriques sont ainsi évaluées et interprétés.

Des simulations aussi sont faites montrent une comparaison en tant que taux d'acceptation de connexions entre le protocole AODV et sa modification résultante de l'intégration de la solution proposée dans le chapitre précédent.

1. Introduction

Pour tester un protocole de routage on a recours souvent à la simulation. En effet il serait très coûteux voire impossible de mettre en place un réseau à des fins de tests pour certains critères.

Dans la seconde moitié des années 90, avec l'élaboration de plusieurs normes pour les réseaux sans fil à portée limitée (visant des usages à l'échelle du bureau ou du bâtiment), un certain nombre de simulateurs ont été développés conjointement. On cite par exemple Network Simulator 2 et son extension « sans fil », OPNET ou encore GloMoSim / Qualnet.

NS2 est certainement le simulateur de réseaux le plus utilisé par la communauté ad hoc. Il est gratuit et son code source est disponible.

Dans notre simulation on met à contribution le NS2 pour analyser quelques propriétés du protocole du routage AODV.

2. Présentation de network simulator:

Le simulateur du réseau NS2 est un outil logiciel de simulation de réseaux informatiques. Il est principalement bâti avec les idées de la conception par objets, de réutilisation du code et de modularité.

NS2 est écrit en C++ et utilise le langage OTCL (Object Tools Command Language) dérivé de TCL. A travers OTCL, l'utilisateur décrit les conditions de la simulation : la topologie du réseau, les caractéristiques des liens physiques, les protocoles utilisés, les communications qui ont lieu. La simulation doit d'abord être saisie sous forme de fichier que NS va utiliser pour produire un fichier contenant les résultats. Mais l'utilisation de l'Otcl permet aussi à l'utilisateur de créer ses propres procédures (par exemple s'il souhaite enregistrer dans un fichier l'évolution d'une variable caractéristique du réseau au cours du temps).

Il contient les fonctionnalités nécessaires à l'étude des algorithmes de routage unicast ou multicast, des protocoles de transport, de réservation, des services intégrés, des protocoles d'application. De plus le simulateur possède déjà une palette de systèmes de transmission, d'ordonnanceurs et de politiques de gestion de files d'attente pour effectuer des études de contrôle de congestion. La liste des principaux composants actuellement disponible dans NS par catégorie est :

- Application Web, ftp, telnet, générateur de trafic (CBR, ...)
- Transport TCP, UDP, RTP, SRM
- Routage statique ou dynamique (vecteur de distance)
- Routage Multicast (DVMRP, PIM)
- Gestion de file d'attente : RED, DropTail, Token bucket, etc

- Discipline de service : CBQ, SFQ, DRR, Fair Queueing
- Système de transmission : CSMA/CD, CSMA/CA, lien point à point

Prises ensembles, ces capacités ouvrent le champ à l'étude de nouveaux mécanismes au niveau des différentes couches de l'architecture du réseau.

NS2 implémente la version de 1997 de la norme 802.11. A ce titre, le débit maximum possible est de 2 Mbit/s.

NS permet de positionner sur un plan virtuel des mobiles équipés d'émetteurs radio, et il gère la mobilité de ces nœuds dans le temps. Pour qu'un paquet émis sur une interface sans fil sous NS2 soit reçu, il faut qu'il arrive au destinataire avec un niveau de signal supérieur à un certain seuil. Ce seuil est par défaut de 3.652×10^{-10} W, et on l'a laissé à cette valeur dans notre simulation.

Pour une documentation générale de NS, on a référé à [10] et au tutorial disponible sur les sites web cités après.

2.1 Le modèle de réseau sous ns

Un modèle de réseau sous NS est constitué :

- de nœuds de réseau : endroits où est généré le trafic, ou nœuds de routage ;
- de liens de communication entre les réseaux.
- d'agents de communication, représentant les protocoles de niveau transport (TCP, UDP) ; ces agents sont attachés aux nœuds et connectés l'un à l'autre, ce qui représente un échange de données (connexion TCP, flux UDP).
- d'applications qui génèrent le trafic de données selon certaines lois (CBR, VBR), et se servent des agents de transport.

2.2 Les différents modèles de propagation radio sous NS2

NS2 permet également de choisir parmi les modèles de propagation suivants, qui influenceront en particulier sur la manière dont seront atténués les signaux en fonction de la distance :

2.2.1 Le modèle de propagation en espace libre (Free space model):

Ce modèle considère le cas idéal où il y a un seul chemin de propagation entre l'émetteur et le récepteur et qu'il est en vue directe.

L'équation suivante permet de calculer la puissance du signal reçu en environnement libre à une distance d de l'émetteur.

$$Pr(d) = \frac{P_t G_t G_r \lambda^2}{(4\pi)^2 d^2 L} \quad (2.1)$$

Où P_t est la puissance d'émission, G_t et G_r les gains respectifs des antennes de l'émetteur et du récepteur. L (avec $L \geq 1$) est la perte du système, et λ est la longueur d'onde. Ce modèle de propagation représente les zones de communication comme un cercle autour de l'émetteur.

Si un récepteur est dans ce cercle il reçoit tous les paquets, s'il est en dehors il n'en reçoit aucun.

2.2.2 Le modèle de propagation utilisant deux rayons (Two-ray ground reflection model):

En environnement réel, il est en fait peu probable que le seul chemin de propagation soit le chemin direct. Le modèle two-ray ground considère donc à la fois le chemin direct et une réflexion sur le sol. Ce modèle donne des résultats plus justes que le modèle de propagation en espace libre quand la distance est assez grande. La puissance reçue à une distance d est calculée de la manière suivante :

$$Pr(d) = \frac{P_t G_t G_r h_t^2 h_r^2}{d^4 L} \quad (2.2)$$

Où h_t et h_r sont les hauteurs des antennes de transmission et de réception. Afin que NS soit cohérent avec le modèle de propagation en espace libre, L a été ajouté à l'équation. L'équation précédente présente une décroissance de la puissance reçue en fonction de la distance plus rapide que l'équation (2.1). Cependant, pour des distances courtes, le modèle à deux rayons ne donne pas de bons résultats. Le modèle de propagation en espace libre est donc utilisé à la place de celui-ci quand d est suffisamment petit.

2.2.3 Le modèle Shadowing:

Les modèles de propagation en espace libre ou utilisant deux rayons calculent de manière déterministe la puissance reçue en fonction de la distance. Ils représentent tous deux la zone de communication comme un cercle idéal. Dans la réalité, la puissance reçue à une certaine distance varie de manière aléatoire, à cause des effets de propagation par des chemins multiples. En fait, les deux modèles précédents calculent la puissance moyenne reçue à une distance d .

Le modèle "shadowing" est composé de deux parties. La première est le modèle d'atténuation en fonction de la distance, qui calcule la puissance moyenne reçue à une distance d , notée $Pr(d)$. Il utilise une distance courte comme référence, notée d_0 . $Pr(d)$ est calculé relativement à $Pr(d_0)$ de la manière suivante :

$$\frac{Pr(d_0)}{Pr(d)} = \left(\frac{d}{d_0} \right)^\beta \quad (2.3)$$

β est appelé l'exposant d'atténuation en fonction de la distance, et est généralement déterminé de façon empirique par des mesures en environnement réel. Les grandes valeurs de β correspondent à une obstruction plus forte et donc à une décroissance plus rapide de la puissance reçue en fonction de la distance.

$Pr(d_0)$ peut être calculé à partir de l'équation (4.1), en prenant par exemple $d_0 = 1$ mètre.

L'atténuation en fonction de la distance est souvent mesurée en dB. A partir de l'équation (2.3) nous avons :

$$\left[\frac{P_r(d)}{P_r(d_0)} \right]_{dB} = -10\beta \log\left(\frac{d}{d_0}\right) \quad (2.4)$$

La seconde partie du modèle shadowing reflète les variations de la puissance reçue à une distance donnée. C'est une variable suivant une loi log-normale, c'est-à-dire dont la distribution mesurée en dB est gaussienne. L'ensemble du modèle shadowing est représenté par :

$$\left[\frac{P_r(d)}{P_r(d_0)} \right]_{dB} = -10\beta \log\left(\frac{d}{d_0}\right) + X_{dB} \quad (2.5)$$

Où X_{dB} est la variable aléatoire gaussienne dont la moyenne est zéro et l'écart type sigma dB. Sigma dB est appelée shadowing déviation, et est également obtenue par des mesures en environnement réel. L'équation (2.5) est aussi connue sous le nom de log-normal shadowing model.

Le shadowing model étend le cercle idéal de communication à un modèle statistique plus riche ; les nœuds ne peuvent communiquer qu'avec une certaine probabilité lorsqu'ils sont vers la limite de portée.

2.3 Les différents modèles de mobilité sous NS2

Puisque les réseaux ad hoc (MANET) sont souvent analysés par des simulations, leurs résultats d'exécution dépendent légèrement des paramètres de réseau de simulation. Ainsi, l'évaluation d'un protocole de routage ad hoc dépend de choisir soigneusement un modèle de mobilité pour illustrer les mouvements réalistes des utilisateurs.

Les modèles de mobilité d'entité représentent les nœuds mobiles dont les mouvements sont indépendants l'un de l'autre. D'autre part, les modèles de mobilité de groupe représentent les nœuds mobiles dont les mouvements dépendent l'un de l'autre et ils tendent à être plus réalistes dans les applications impliquant la communication de groupe.

2.3.1 Le modèle de mobilité random waypoint (RWP):

Dans ce modèle la mobilité des nœuds est typiquement aléatoire et tous les nœuds sont distribués uniformément dans l'espace de simulation. En effet il consiste en :

- Le placement d'un certain nombre de mobiles dans une zone carrée de laquelle ils ne peuvent sortir.
- L'affectation d'une position, d'une vitesse et d'une destination initiale à chaque mobile.
- Le déroulement proprement dit de la simulation, où à chaque fois que les mobiles atteignent leur destination dans le carré, ils repartent vers une autre destination choisie aléatoirement après un éventuel temps de pause.

Du fait de la simplicité de ce modèle, il n'est pas toujours adapté pour décrire des comportements de mobilité complexes.

2.3.2 Le modèle Random Walk:

Ce modèle est développé pour imiter un mouvement imprévisible. Un nœud mobile dans ce modèle se déplace de son endroit courant à un nouvel endroit en choisissant aléatoirement une direction et une vitesse suivant lesquelles il se déplace. La nouvelles vitesse et direction toutes les deux sont choisies dans des gammes prédéfinies, [speedmin, speedmax] et $[0, 2\pi]$ respectivement. Un nœud mobile atteignant la frontière de simulation, rebonds avec l'angle déterminé par la direction entrante et puis continue le long du nouveau chemin.

2.3.3 Modèle aléatoire de direction (random direction model) :

Il vient comme une modification sur le modèle de RWP. Dans RWP, la probabilité d'un nœud mobile de choisir une nouvelle destination située au centre du la zone de simulation ou une destination qui nécessite un déplacement par le centre est haute. Ce modèle essaye d'alléger ce comportement, fournissant un nombre constant de voisins dans toute la simulation. Les nœuds mobiles choisissent une direction aléatoire suivant laquelle ils se déplacent en tant que modèle de mobilité de random walk, où ils se déplacent vers la frontière de la simulation dans cette direction. Une fois que la frontière est atteinte, le nœud mobile fait une pause pendant le temps indiqué, choisit une autre direction angulaire entre (0 et 180) continue alors le processus.

3. Objectifs de la simulation

Le but général de notre expérimentation est d'analyser quelques propriétés du protocole AODV en particulier :

- évaluer le délai de sélection de route.
- évaluer l'optimalité de la sélection de route du protocole.
- évaluer le coût de la sélection de route et le coût d'échange des états de liens.

Le délai de découverte de routes ainsi que l'optimalité de sélection de route et le coût de sélection de route sont fonction de plusieurs paramètres tels que la taille du réseau (le nombre de nœuds dans le réseau), la mobilité des nœuds du réseau, le débit des flux en d'autre terme le taux d'émission des paquets et le nombre de connexions en présence dans le réseau.

Dans nos simulations on évalue les propriétés déjà mentionnées du protocole AODV en tenant compte du nombre des nœuds du réseau et le nombre de flux circulant dans le réseau.

3.1 Délai de sélection d'une route

Si un nœud veut communiquer avec un autre nœud et n'a pas une entrée dans sa table de routage pour cette destination spécifique, une procédure de découverte de route est initiée. Le temps pris pour découvrir cette route est important pour qualifier le protocole de routage.

Ce qui nous intéresse est le temps entre le début de l'assemblage d'une RREQ jusqu'à la réception d'une RREP, ce qui se qualifie par le temps de découverte de route.

Quand un nœud a à transmettre une requête de route, il consulte d'abord sa table de routage si une entrée existe pour cette destination. S'il n'y a pas d'entrée il mémorise le

message et diffuse le message RREQ. Après avoir reçu le message RREP, le nœud source transmet les messages mémorisés. AODV note dans son fichier de sortie les actions currentes.

En consultant ce fichier, il est possible de déterminer la différence en temps entre l'assemblage de la requête de route RREQ et la réception du RREP.

3.2. Optimalité de sélection de route du protocole

La qualité des routes sélectionnées par le protocole est fortement dépendante des conditions du réseau. Un routage réactif ne produira pas systématiquement des routes optimales en termes de nombre de sauts.

Le rapport entre la longueur des routes générées par le protocole AODV et la longueur des routes optimales représente une mesure de l'optimalité de sélection de routes.

3.3. Coût de sélection de route et l'échange de l'état de lien

Transmettre les paquets de contrôle nécessaires à l'établissement et à la maintenance de routes engendre un surcoût en trafic de contrôle, les paquets concernant RREQ, RREP, ERROR, HELLO représentent le volume de signalisation généré par les nœuds du réseau.

On propose de représenter le volume de paquets de contrôle émis par la charge de ces paquets mesuré en kbps.

4. Modèle de simulation

Les simulations sont faites sur ns version 2.29 sous fedora. La table 4.1 liste les constantes utilisées pour le protocole AODV dans notre simulation. On note que le mécanisme de détection de coupures de liens est garantie dans le protocole AODV soit par l'émission périodique les messages Hello standards du protocole AODV ce qui est le cas dans notre simulation soit par la couche liaisons de données (activation de AODV_LINK_LAYER_DETECTION).

Temps d'attente d'une réponse de route	1s
Nombre de fois pour lequel une nouvelle RREQ est émise	3
Temps avant qu'une RREQ est émise à nouveau	10s
Temps pour lequel l'identifiant d'une diffusion (broadcast id) est maintenue	6s
Temps pour lequel les informations de la route inverse sont maintenues	6s
Intervalle de temps entre les messages Hello	1s
Temps pour lequel un lien coupé est maintenu dans la table de routage	3s

On a choisi de simuler des réseaux de taille 20, 30, 40 et 50 nœuds et dans chacun les propriétés du protocole AODV sont évaluées.

La topologie dans laquelle les nœuds bougent aléatoirement est de 1000m x1000m et le temps de simulations est mis à 900 secondes.

Dans toutes ces simulations on utilise les paramètres standards pour le médium et du modèle de propagation radio : la capacité du médium est de 2MB/s et le modèle de propagation radio two ray ground et la portée de communication est de 250 m. Le protocole IEEE 802.11 est utilisé comme protocole d'accès au médium. Le type de la l'interface de la queue en chaque nœud est «drop tail». Dans ce type de file, les paquets venant de différents flots sont traités de la même manière: ils sont tous placés dans la file suivant leur ordre d'arrivé et en ressorte dans le même ordre: c'est le principe d'une FIFO. Une fois que la file se vide, le routeur peut accepter de nouveau des paquets. Si le tampon est plein le dernier paquet qui arrive est supprimé. Et le nombre de paquets maximum dans le tampon d'émission en chaque routeur est de 50 paquets.

Chaque simulation exécutée accepte en entrée deux fichiers décrivant le scénario de la simulation : en effet ils définissent le mouvement exact de chaque nœud et l'ordre exact des paquets lancés par chaque nœud, ainsi que le temps exact auquel un changement de mouvement ou changement des origines de paquets devant être produit.

Pour chaque réseau de taille bien déterminé c'est le même modèle de mobilité qui est utilisé et seul le fichier de trafic entre les nœuds change.

4.1 Modèle de mobilité

Les nœuds mobiles utilisent random waypoint comme modèle de mobilité. Ce modèle est utilisé souvent dans l'analyse de performance des protocoles de routage. Puisque dans nos simulations on se restreint aux paramètres qui sont la taille du réseau et le nombre de flux, on a choisi de simuler une mobilité moyenne suivant laquelle les mobiles se déplacent et dont la vitesse est uniformément distribuée entre 0 et 10m/s. On note que la vitesse des mobiles décroît avec la progression de la simulation. Le temps de pause est de 30 secondes.

La création des mouvements des nœuds pour ce scénario est faite par l'utilisation d'un générateur de mouvements des nœuds qui génère un fichier décrivant la mobilité des nœuds utilisant l'algorithme «random waypoint» pour chaque taille de réseau. Puisqu'on a quatre réseaux de taille différents, On a crée quatre modèles de mobilité correspondant à chacun.

4.2 Modèle de trafic

Puisque le but de nos simulations est d'analyser les propriétés du protocole AODV, on a choisi que les sources de trafics soient à débit constant CBR (constant bit rate), en variant le nombre de sources CBR est équivalent à la variation du taux d'émission des paquets. Pour nos simulations on a choisi de fixer le taux d'émission des paquets à 4 paquets par seconde et utiliser différents modèles de trafics correspondant à 2, 10,15 et 50 flux pour chaque taille du réseau.

Le trafic entre les nœuds est produit en utilisant un générateur de trafic qui crée aléatoirement des connexions de trafics de type CBR qui commencent à des instants distribués uniformément entre 0 et 180 secondes. La taille des paquets de données est 512 octets. Par la suite quatre modèles de trafics sont générés pour chaque taille du réseau ce qui correspond à 16 modèles de trafics générés en total.

On n'a pas employé des sources de trafic tcp parce que le tcp offre une charge conforme à l'état du réseau, c'est à dire le trafic tcp change les temps auquel il envoie des paquets en se basant sur sa perception de la capacité du réseau de délivrer ces paquets.

5. Résultats de simulation et analyse

NS2 écrit les résultats de ses simulations dans un fichier texte où chaque ligne correspond à un événement qui s'est produit à un niveau ou à un autre de la pile protocolaire. Il est possible de configurer NS2 de telle sorte qu'il ne garde une trace que de certains types d'événements (par exemple tout ce qui concerne le routage, mais pas ce qui concerne la couche MAC). Ceci est en particulier utilisé pour accélérer la simulation et réduire la taille du fichier.

Ce fichier texte peut porter en lui même énormément d'informations. Mais pour extraire et représenter de manière synthétique ces informations, il faut souvent appliquer de nombreux traitements à ce fichier.

L'analyse des fichiers de trace dans nos simulations est réalisée en utilisant le langage puissant perl pour extraire les champs nécessaires au calcul des différents paramètres du protocole. Enfin les graphes sont obtenus en utilisant Excel.

5.1 Délai de sélection de route

Comme on a déjà dit ce temps est mesuré comme la différence entre l'instant où l'initiateur d'une connexion reçoit la confirmation de route et l'instant où il avait émis la requête de route correspondante.

Les figures 4.1 et 4.2 représente le temps moyen d'établissement des routes par AODV sur le nombre de nœuds sources qui ont généré des requêtes de route et qui ont reçus les réponses de route correspondantes.

On remarque que ce temps augmente essentiellement avec le nombre de nœuds du réseau. En effet, la procédure de découverte de route se fait en mode diffusion, plus la densité du réseau augmente, plus la probabilité de collision entre deux messages de recherche de route sera élevée. Les nœuds cherchant des routes vont initier des nouvelles procédures de découverte de routes ce qui va augmenter le délai de sélection de route.

D'autre part on remarque que ce délai augmente avec le nombre de flux en présence dans le réseau. En effet plus le nombre de connexions à établir entre source et destinations augmente, plus on a des nœuds qui vont générer des procédures de découverte de route ce qui aboutit à des situations de congestion et de collisions entre les paquets. La perte des paquets de découverte de route conduit à une diffusion des nouvelles requêtes de route cherchant la destination désirée ce qui engendre un délai supplémentaire dans le processus d'établissement de connexion.

On note que pour un nombre de flux faible, le délai de découverte de route ne dépasse pas 200ms même pour un réseau dense de 50 nœuds. Alors que pour un nombre de flux important dans le réseau, une cinquantaine de flux, le délai de découverte de route est énormément grand et dépasse 1 seconde pour un réseau de 50 nœuds.

On note que pour un nombre de flux faible, le délai est à peu près stable suite à l'absence de congestion dans le réseau.

Suite à la grande différence entre les valeurs de délai pour les réseaux surchargés de 50 flux et les réseaux peu surchargés, la différence entre les courbes correspondantes à des réseaux peu surchargés ne va pas être différenciée dans une même échelle que pour des réseaux surchargés de 50 flux. Pour cela on a représenté deux figures : la figure 4.1 montre le délai en fonction du nombre de nœuds pour des réseaux chargés de 2, 10 et 15 flux et la figure 4.2 montre le délai en fonction du nombre de nœuds avec 2, 10, 15 et 50 flux.

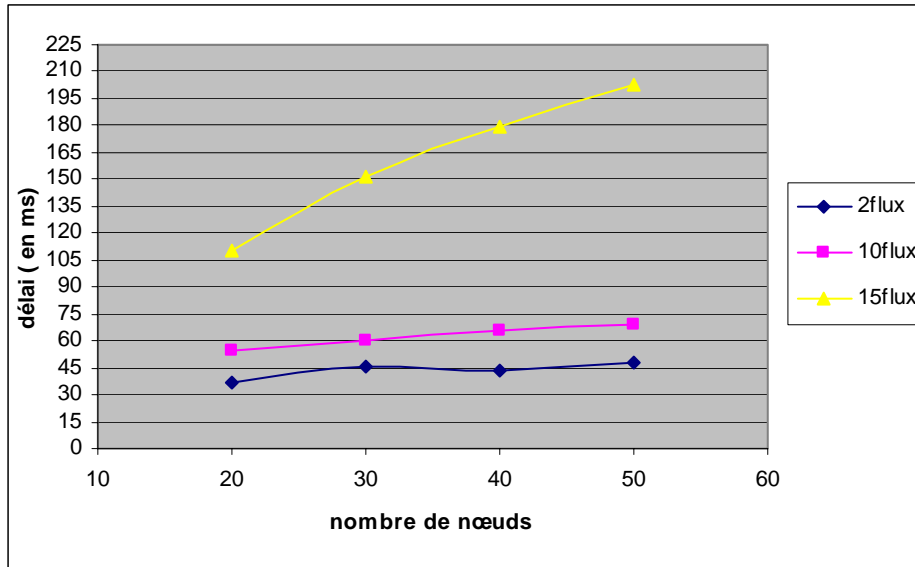


Figure 4.1 : délai moyen d'établissement des routes mesuré en millisecondes.

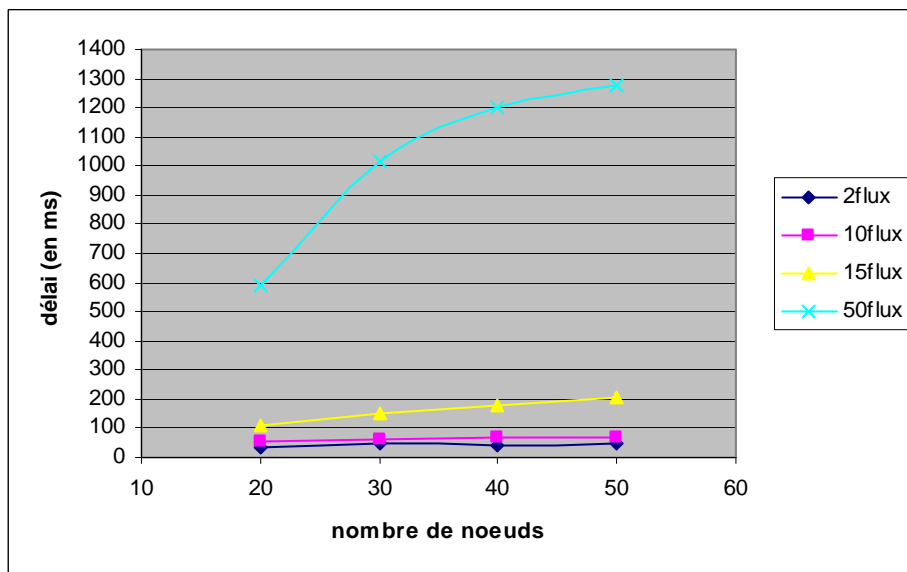


Figure 4.2 : délai moyen d'établissement des routes mesuré en millisecondes.

5.2 Optimalité de sélection de route

Un routage réactif ne produira pas systématiquement des routes optimales en termes de nombre de sauts.

La figure 4.3 représente la moyenne des rapports entre la longueur des routes déterminées par AODV et la longueur du plus court chemin entre les nœuds source et destination correspondants sur le nombre de sources qui ont généré des requêtes de route et qui ont reçus les réponses de route correspondantes.

La longueur du plus court chemin entre source et destination est obtenue grâce aux directives de God qui se trouvent dans le fichier de mouvement des nœuds. Les opérations générales de l'objet (God) sont employées pour stocker des informations globales sur l'état de l'environnement, du réseau, ou des nœuds. L'objet God est employé pour stocker seulement un tableau du plus court nombre de sauts exigés à atteindre d'un nœud à un autre.

On peut remarquer qu'AODV s'éloigne des routes optimales avec l'augmentation de la densité du réseau. Comme on a déjà dit, plus la densité du réseau augmente plus la probabilité de collision entre deux messages de recherche de route sera élevée. Ces messages étant transmis en diffusion et non acquittés, leur perte n'est pas détectée et ils ne sont pas retransmis. En conséquence, de nombreux chemins ne seront pas explorés. Et des routes non optimales seront sélectionnées par le protocole.

D'autre part, un trafic élevé dans le réseau dû à nombre de flux élevé implique des situations de congestion et des pertes des paquets de recherche de route au niveau des routes optimales, par la suite une requête de route arrive à la destination par un chemin plus long et c'est elle qui arrive la première à la destination et qui précise la route sélectionnée. D'où les routes sélectionnées sont plus loins des routes optimales dans un réseau surchargé que dans un réseau peu surchargé.

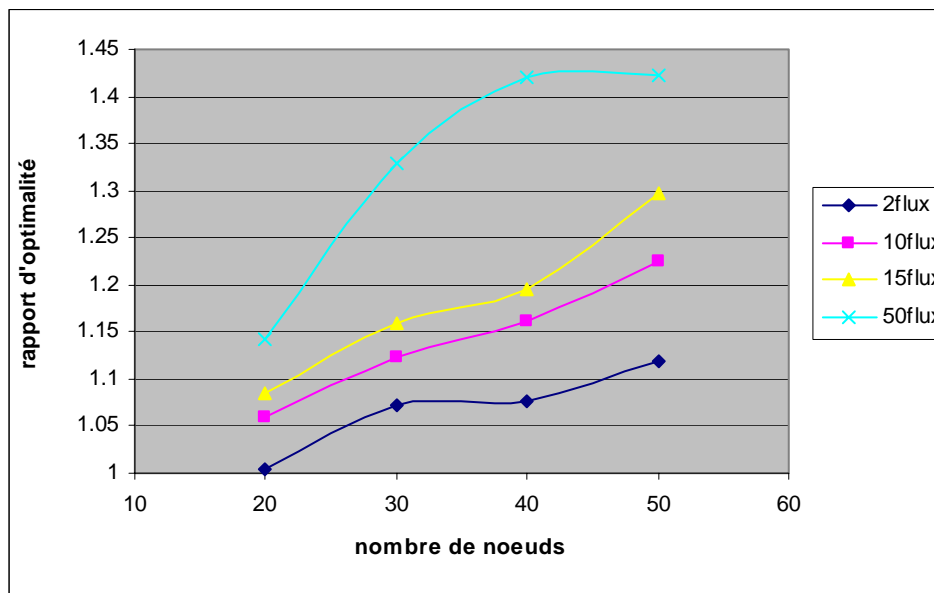


Figure 4.3 : rapport entre la longueur des routes déterminées et les plus courts chemins correspondants.

On remarque aussi dans la figure 4.3 que dans un réseau de 40 nœuds et de 50 nœuds, le rapport d'optimalité est presque le même. On note que plus la densité du réseau augmente, plus la probabilité que les nœuds soient distribués sur toute la zone de simulation est grande, les nœuds se trouvent dans la zone de transmission l'un de l'autre et peuvent plus se communiquer. On peut dire que la connectivité du réseau de 40 nœuds et le réseau de 50 nœuds est presque la même et le plus grand nombre de sauts entre un couple source destination ne diffère pas beaucoup dans les deux réseaux et par suite le trafic de 50 flux engendre des congestions dans les deux réseaux aboutissant à des rapports d'optimalité voisins.

5.3 Coût de sélection de route

On choisit de mesurer le coût de sélection de route par les paquets de contrôle nécessaires à l'établissement d'une route. Ce trafic de contrôle est défini comme étant la charge des paquets de contrôle émis dans le réseau durant toute la simulation mesuré en kbps.

Dans la figure 4.4 On remarque que le coût de sélection de route augmente avec l'augmentation du nombre des nœuds dans le réseau. En effet lorsque le réseau est dense le nombre des paquets Hello font partie du calcul et contribuent à l'augmentation de ce coût, d'autre part dans AODV la découverte de route se fait par inondation des voisins et générera en conséquence un volume important de signalisation même si le protocole n'émet des requêtes que lorsqu'une route est requise.

On remarque que ce coût augmente aussi avec le nombre de flux en présence dans le réseau, en effet lorsqu'un nombre important de connexions va être établi entre sources et destinations correspondants, le protocole AODV souffrira de nombreuses cassures de routes dues à la présence de congestion. Ce qui implique une circulation plus importante des paquets de contrôle servant à la réparation des routes et à leur maintenance.

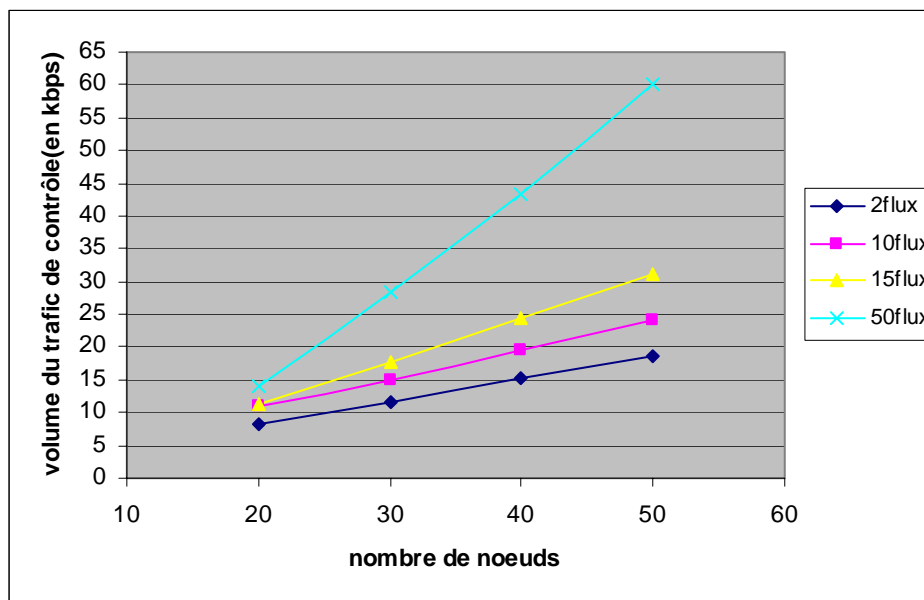


Figure 4.4 : volume du trafic de contrôle nécessaire à l'établissement des routes mesuré en kbps.

5.4 Comparaison entre AODV et AODV modifié

Dans ces simulations, les valeurs des paramètres utilisées par le simulateur correspondent à un débit binaire de 2 Mbps. Les mêmes fichiers de mouvement sont utilisés et les fichiers de trafics correspondent à 50 connexions de type CBR entre les noeuds sources destinations et dont le débit correspond à 80 kbps.

La figure 4.5 représente une comparaison du taux d'acceptation des requêtes émises pour le protocole AODV et AODV modifié.

Le rapport entre le nombre de flux pour lesquels une route sans contrainte de qualité de service peut être trouvée par le protocole AODV et le nombre total de flux est représenté dans une courbe. La figure montre aussi une courbe représentant ce même rapport mais pour les routes exigeant de la contrainte de bande passante découvertes par AODV modifié.

La figure représente l'évolution de ce taux d'acceptation au fur et à mesure que le nombre de noeuds croit.

On remarque que le taux d'acceptation croit avec la densité du réseau. En effet plus un réseau est dense, plus la probabilité qu'il existe une route d'une source à une destination donnée est importante. En conséquence, la probabilité qu'une route admissible existe augmente aussi avec le nombre de noeuds en présence.

La différence entre les résultats obtenus par le protocole AODV et AODV modifié permet d'évaluer l'impact de l'ajout des contraintes de qualité de service sur le routage. Le contrôle d'admission d'AODV modifié accepte moins de flux qu'AODV. En effet le protocole AODV modifié refusera les réservations qu'il considère comme pouvant surcharger le réseau.

On note que ce taux trouvé ne dépasse pas 40% dans nos simulations, en effet le nombre de flux en présence est considéré important. Comme on pouvait s'y attendre, le taux d'acceptation décroît alors que le nombre de flux augmente, la capacité du réseau demeurant constante.

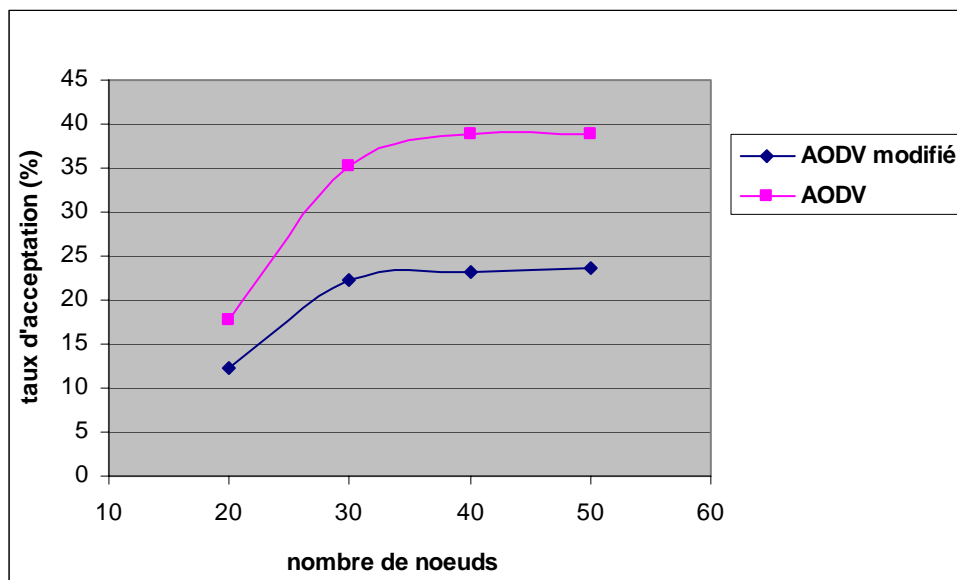


Figure 4.5 : taux d'acceptation moyen de 50 flux de 80 kbps, capacité du lien: 2 Mbps.

Les simulations présentées dans ce chapitre ont permis de valider le fonctionnement du protocole AODV. Elles indiquent en particulier comment le protocole réagit face à la densité du réseau et à la charge du trafic circulant dans le réseau. Et ceci en termes de délai de sélection de route, de l'optimalité de cette sélection ainsi que le coût d'établissement des routes.

La comparaison entre le protocole AODV et sa modification nous a permis de dégager le comportement du protocole face aux connexions demandant un certain débit suite à l'intégration d'un contrôle d'admission.

Toutefois, les performances réelles de ce protocole ne peuvent être déduites de simples simulations. Il est en effet difficile, en simulation, de concevoir les scénarios pertinents conduisant à l'évaluation du comportement du protocole.

Conclusion et perspectives

Dans le cadre de ce stage, l'objectif était d'analyser les propriétés du protocole de routage AODV opérant dans les réseaux ad hoc, en particulier le délai de découverte de route, l'optimalité de sélection des routes et le coût de sélection des routes.

Puisque le protocole AODV est un protocole de routage destiné à router des paquets dans un réseau ad hoc sans fil, nous avons tout d'abord présenté le concept des environnements mobiles et les caractéristiques des réseaux ad hoc dans le premier chapitre.

Le second chapitre a été consacré à la présentation du protocole de routage AODV et son mécanisme de fonctionnement : ses procédures de découverte de routes et leur maintenance.

Le troisième chapitre consiste en une solution du routage AODV supportant la notion de qualité de service en termes de bande passante. La solution consiste en l'extension des paquets de contrôle du protocole pour contenir des champs supplémentaires répondant aux exigences de qualité de service. En plus la solution propose un contrôle d'admission des nouvelles connexions devant être exécutées dans chaque nœud de la route demandée. Ce contrôle d'admission prend en compte les interférences dans la zone de couverture du nœud mobile.

Toutefois une réservation effective de la bande passante reste un problème difficile à réaliser suite à la mobilité permanente des nœuds du réseau et au problème des stations cachées. Même si les messages « Hello » assurent une connaissance de la bande passante utilisée par le voisinage à deux sauts, le problème de la station cachée réside un problème pertinent dans un réseau mobile. En effet un nœud B peut exister dans la zone d'interférence d'un nœud A et ne se trouve dans aucune zone de réception d'un nœud voisin de A.

Le dernier chapitre est destiné à des simulations du protocole en utilisant le simulateur de réseau NS2. Les résultats de simulation ont été représentés sur des graphes et interprétés. Ces simulations nous ont conduit à bien savoir comment le protocole AODV opère face à la densité du réseau et à la charge du trafic y circulant ainsi que de valider la variation du taux d'acceptation de connexions en présence d'un contrôle d'admission basé sur la disponibilité de la bande passante dans les nœuds de routage.

On propose dans le futur d'intégrer dans le protocole AODV une réservation effective de la bande passante basé sur la dissémination des messages hello à deux sauts et de changer le mécanisme de maintenance des routes comme déjà expliqué ainsi que surveiller la garantie de la qualité de service sur les routes actives et envoyer des messages d'erreur suite à la dégradation de la qualité de service sur ces routes. On propose aussi de simuler des réseaux dans lesquels circulent des trafics privilégiés et des trafics best effort afin de réguler la consommation de la bande passante entre les deux types de trafics et de permettre aux applications d'être adaptatives et changer leur débit en fonction de l'état du réseau.

Bibliographie

- [1] Guy Pujolle – *Les Réseaux* édition 2005, Groupe Eyrolles 2004
- [2] IEEE Standard for Information technology– Telecommunications and information exchange between systems– Local and metropolitan area networks– Specific requirements, Part 11 : Wireless LAN Medium, Access Control (MAC) and Physical, Layer (PHY) Specifications ISO/IEC 8802-11 :1999(E).
- [3] C. Perkins, E. Belding-Royer, S. Das: *Ad hoc On-Demand Distance Vector (AODV) Routing*, Network Working Group, July 2003 available on: <ftp://ftp.nordu.net/rfc/rfc3561.txt>
- [4] Charles E. Perkins, Elizabeth M. Royer, Samir R. Das: *IP Address Autoconfiguration for Ad Hoc Networks*, Mobile Ad Hoc Networking Working Group, July 2000
- [5] Robert Braden, David Clark, ET Scott Shenker: *Integrated Services in the Internet Architecture: An Overview*. Internet Request for Comments RFC 1633, Internet Engineering Task Force, Juin 1994.
- [6] Steven Blake, David Black, Mark Carlson, Elwyn Davies, Zheng Wang, ET Walter Weiss: *An Architecture for Differentiated Services*. Internet Request for Comments RFC 2475, Internet Engineering Task Force, Décembre 1998.
- [7] Robert Braden, Lixia Zhang, Steven Berson, Shai Herzog, ET Sigih Jamin: *Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification*. Internet Request For Comments RFC 2205, Internet Engineering Task Force, Septembre 1997.
- [8] C. Perkins and E. Belding-Royer: *Quality of Service for Ad hoc On-Demand Distance Vector Routing* (work in progress), Oct 2003, draft-perkins-manet-aodvqos-02.txt.
- [9] J. Rajahalme, A. Conta, B. Carpenter and S. Deering RFC 3697: *IPv6 Flow Label Specification*, March 2004.
- [10] P. Anelli & E. Horlait : *NS-2: Principes de conception et d'utilisation*, Version 1.3

Tutorial de NS disponible sur :

<http://titan.cs.uni-bonn.de/~greis/ns/>

<http://titan.cs.uni-bonn.de/~greis/ns/nstutorial.tar.gz>