Projet Réseau :
Etude de l'effet de Mobile IP sur le routage.
Application à NS-2.

Julien Casteras & Etienne Coumont

12 janvier 2005

Table des matières

Chapitre 1

Etude du simulateur NS-2

1.1 Présentation

1.1.1 Introduction

Depuis de nombreuses années, les réseaux de télécommunications, et plus particulièrement les réseaux informatiques sont en pleine expansion, tant au niveau étendue qu'au niveau technologique. Mais cette évolution ne se fait pas sans rencontrer de problèmes. Une bonne méthode pour les anticiper, les analyser et les corriger est d'avoir recours à la **simulation** grâce à des outils tels que **NS**.

1.1.2 Historique

NS a été créé en 1989 à partir du Real Network Simulator.Il a été considérablement utilisé et amélioré au cours des dernières années par de nombreux chercheurs. Il en est actuellement à sa version 2.

1.1.3 NS-2 et NAM

NS est un simulateur. Il permet de définir un réseau en créant des noeuds, des connexions, en ajoutant des flux de données, des protocoles à utiliser, etc ... pour ensuite simuler les communications ayant lieu.

Le langage utilisé par NS-2 est OTcl (Object Tools Command Language), un dérivé de TCL orienté Objet.

Cette définition du réseau se fait sous la forme d'un fichier texte, que NS va ensuite interpréter afin de produire un fichier de résultats, qui pourra être visualisé par l'utilitaire NAM (voir schéma page suivante).

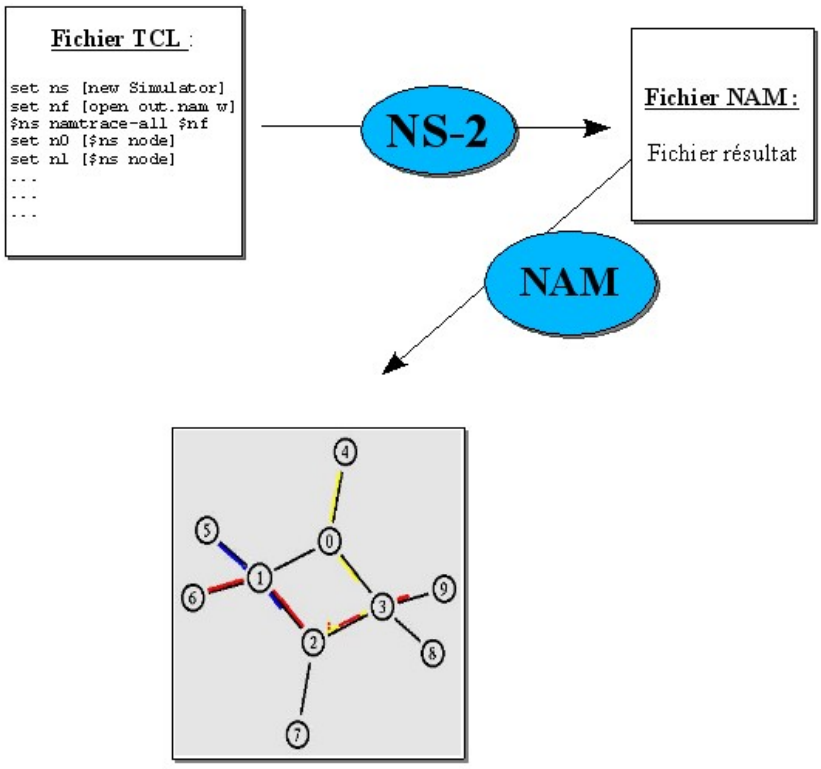

FIG. 1.1 – Fonctionnement de NS-2 et NAM

1.2 Principe de fonctionnement de NS

1.2.1 Les objets de base

Voici les objets de base utilisables avec NS et permettant de créer la topologie du réseau :

- **Le simulateur** : C'est l'objet global qui contiendra le réseau. Il se crée via la commande :

```
set ns [new Simulator]
```

- **Les nœuds** : ils représentent les différentes machines du réseau, qui peuvent être des postes fixes, des routeurs, des noeuds mobiles, etc ... et se créent en tapant :

```
set n0 [$ns node] % Crée un noeud « n0 »
```

Les paramètres du noeud sont réglables préalablement via la commande

```
$ns node-config -nomduparametre valeurduparametre
```

Une même commande peut modifier plusieurs paramètres. Par exemple, la création d'un noeud mobile se fait en ayant modifié les paramètres suivants :

```
$ns_ node-config
    -addressType hierarchical
    -adhocRouting AODV
    -llType LL
    -macType Mac/802_11
    -ifqType Queue/DropTail/PriQueue
    -ifqLen 50
    -antType Antenna/OmniAntenna
    -propType Propagation/TwoRayGround
    -phyType Phy/WirelessPhy
    -topologyInstance $topo
    -mobileIP ON
    -channel Channel/WirelessChannel
    -agentTrace ON
    -routerTrace ON
```

```
-macTrace OFF
-movementTrace OFF
```

- **Les liens** : représentent les connexions présentes entre les noeuds. Ils modélisent le système de transmission. On peut régler le type de lien, le débit, le temps de latence ainsi que le comportement de la file d'attente. Ils se créent par une commande du style :

  ```
  $ns duplex-link $n0 $n1 1Mb 10ms DropTail
  ```

- **Les agents** : rattachés à des noeuds, ils définissent les producteurs et les consommateurs de paquets IP.

  ```
  set tcp1 [new Agent/TCP]
  ```

- **Les applications** : rattachées à un agent producteur, elles permettent de générer du trafic.

  ```
  set ftp0 [new Application/TCP]
  ```

1.2.2 L'ordonnanceur

Il permet de définir une chronologie pour le scénario à modéliser. Il gère les événements, exécute les traitements, fait progresser le temps simulé, etc ...

Les principales commandes associées sont « at » qui permet de définir un événement devant se passer à un instant donné. Ex :

```
$ns at 0.5 "$ftp0 start"
```

et « run » qui permet de lancer la simulation :

```
$ns run
```

1.2.3 Interprétation

Il existe deux méthodes pour récupérer les données de la simulation :

- **La Trace** : Elle enregistre dans un fichier les changements d'états d'un paquet à partir d'une file d'attente d'un lien. Une ligne de trace se présente sous le format suivant : opération (+ : mise en file d'attente ; - :

sortie de la file d'attente ; d : suppression de la file d'attente ; r réception au noeud ; l perte suite à une erreur binaire), temps, noeud source, noeud destination, type de paquet, taille du paquet, drapeaux, flot id, adresse source du paquet, adresse destination du paquet, numéro du paquet, id du paquet. Il est aussi possible de tracer les changements de la valeur d'une variable.

- **Le moniteur** : c'est un objet pouvant faire des calculs sur différentes grandeurs tel que le nombre de paquets ou d'octets arrivée, etc... Nous ne l'utiliserons pas ici.

Chapitre 2

Etude de l'effet de Mobile IP sur le routage

2.1 Introduction

Depuis maintenant quelques années, on remarque l'emergence de nouveau moyens de se connecter à internet (PDAs, téléphones portables, ...). Ces moyens ont fait apparaitre un nouveau besoin dans la gestion de l'internet : la mobilité.

2.2 La necessité de Mobile IP

Le fonctionnement d'internet à l'heure actuel est régit par le protocole IPv4 qui obéit à certaine règle qui étaient logiques à l'époque de sa création. Ces règles sont :

- Chaque noeud est identifié par une adresse IP unique.
- Avec cette adresse IP, on peut derterminer le sous réseau auquel le noeud appartient.
- Une connection TCP est déterminé par les deux adresses des noeuds qui correspondent.

Evidemment, ces règles conviennent parfaitement pour des réseaux à noeuds statiques. Mais elles ne sont plus adaptées quand on parle de mobilité où un noeud doit pouvoir changer de sous réseau tout en gardant ces connections établies. En effet, la deuxième règle impose que le noeud change d'adresse IP en changeant de sous réseau, il pert donc ces connections d'après la troisième règle.

D'où la necessité d'un protocole compatible avec le protocole IP actuel qui permette à un noeud mobile de garder la même IP (au moins pour les correspondants) où qu'il se trouve pour ne pas couper ses connections.

La réponse à ce problème est MobileIP.

2.3 Fonctionnement de Mobile IP

2.3.1 Actionnaires

Le fonctionnement de Mobile IP fait intervenir plusieurs actionnaires[1] :

- **Le Noeud mobile** : C'est le noeud qui peut éventuellement voyager de réseaux en réseaux. Il a un réseau initial (réseau mère) qui lui fournit son adresse IP permanente. C'est celle qui sera donnée aux correspondants.
- **Le Réseau Mère (Home network)** : C'est le réseau initial du noeud mobile qui lui donne son IP permanente.
- **Le Home Agent (HA)** : C'est un routeur du réseau mère qui s'occupe d'intercepter et de rediriger les paquets à destination du noeud mobile quand il n'est pas dans son réseau mère.
- **Le Réseau visité (Foreign network)** : C'est un réseau auquel le noeud mobile peut se connecter.
- **Le Foreign Agent (FA)** : C'est un routeur du réseau visité qui sert de lien entre le HA et le noeud mobile.

2.3.2 Fonctionnement global de Mobile IP

Le principe de Mobile IP est de donner *deux* adresses IP au noeud mobile : une adresse permanente, utilisée par ses correspondants pour le joindre, et une adresse temporaire, la *Care-of-adress* (COA), qui est son adresse réelle, dépendant du réseau où il se trouve et nécessaire pour le routage.

Ainsi, lorsqu'un correspondant envoie des paquets au noeud mobile ; il utilise son adresse permanente. Si le noeud est dans son réseau mère, tout est normal. Sinon, le home agent présent dans son réseau mère se charge de transmettre ces paquets au réseau visité. Le correspondant n'a donc pas besoin de savoir où se trouve le noeud.

Lorsque le noeud mobile change de réseau, il doit enregistrer sa nouvelle adresse (la COA) à son home agent. Puis, lors de la redirection des paquets, le home agent devra changer la destination des paquets grace au mécanisme de l'encapsulation. Ensuite, la décapsulation se fera au niveau du foreign agent sui delivrera ensuite le paquet au noeud mobile.

2.3.3 Découverte du foreign agent et recupération de la COA

Deux cas de figure peuvent se produre ici (d'après la RFC2002[2]) :

- Le noeud mobile détecte la présence d'un foreign agent et négocie une care-of-adress avec lui (il utilise celle du FA), on parle alors de « foreign agent care-of-adress »
- Le noeud mobile noeud mobile obtient une adresse IP pour son interface réseau (par le protocole DHCP par exemple), il s'en sert alors

comme care-of-adresse et joue aussi le rôle de foreign agent, on parle alors de « collocated care-of-adresse »

Comme souligné dans [1] ainsi que dans [2], le premier cas est préférable car il minimise le nombre d'adresses IP en cours d'utilisation, le nombre total d'adresses IP étant limité par IPv4.

La découverte du foreign agent dans ce cas se fait par la lecture des messages ICMP (Internet Control Message Protocol) envoyé péridiquement par les foreign agent. Ces messages sont de type « agent advertisement » et sont envoyé en broadcast ou multicast. Le noeud mobile peut éventuellement faire une demande explicite de COA à l'aide d'un message ICMP de type « agent sollicitation message ».

Ces messages donnent donc l'adresse du foreign agent qui sera utilisé comme COA ainsi qu'une durée de validité de cette adresse.

2.3.4 Enregistrement de la COA auprès du HA

Après avoir reçu sa COA, le noeud doit l'enregistrer auprès de son HA. Cela se fait par une procédure de dialogue envoyé par UDP sur le port 434 [2].

Le noeud contacte d'abort le FA, qui contacte le HA par des « Registration Request ». Ce dernier renvoie une notification d'acceptation ou de refus (Registration Reply) au FA qui transmet au noeud.

Il est à noter que l'ensemble de cette procédure doit impérativement être sécurisé pour empêcher d'éventuels problèmes (en fait, elle est sécurisée par MD5 [1]).

2.3.5 Le tunneling

C'est l'action de l'HA qui, recevant les paquets pour le noeud mobile, doit échanger l'adresse de destination avec la COA, sans toutefois masquer l'adresse permanente du noeud (elle est utile au noeud pour maintenir ses connexions TCP). Pour ce faire, deux méthodes sont utilisées : l'encapsulation IP dans IP et l'encapsulation minimale.

L'encapsulation IP dans IP consiste tout simplement à rajouter un en-tête IP identique au paquet où l'adresse de destination à été remplacée par la COA, l'adresse source par l'adresse du HA et le type de protocole par « Protocole IP »(4). Cette méthode a le mérite d'être simple à réaliser mais induit une augmentation conséquente de la taille des paquets.

Le solution alternative de l'encapsulation minimale consiste à ne reprendre dans l'en-tête IP que les champs qui ont changé, l'adresse du correspondant passant dans le champ de données du paquet. Cette méthode permet de réduire la taille du paquet mais est plus compliquée à mettre en oeuvre (fusionnement des en-têtes) et génère des problèmes de fragmentation du fait que l'adresse source passe en donnée.

2.4 Problèmes soulevés par Mobile IP

2.4.1 Problèmes du routage triangulaire

Le problème majeur de Mobile IP vient du fait que le routage entre le correspondant et le noeud mobile n'est pas optimal parce qu'il passe par le home agent. Ce problème peut même atteindre des proportions absurdes quand le noeud et le correspondant se trouvent sur le même sous-réseau, et le home agent sur un autre.

Une solution proposée [3] est le « Routage Optimisé » qui consiste à avertir le correspondant de la COA du noeud mobile. Cependant, cette solution n'est pas très satifaisante en ce sens qu'elle ne respecte pas la transparence par rapport au correspondant.

2.4.2 Autres problèmes

Un autre problème soulevé par Mobile IP est le problème de congestion au niveau d'un home agent. En effet, si un home agent appartient au réseau mère de nombreux noeuds mobiles et que ceux-ci sont tous partis, cet home agent devra à la fois gérer l'encapsulation de tous ces noeuds, les connexions et dialogues avec tous les foreigns agents ce qui peut générer un important trafic au niveau de l'agent.

Un autre problème est la perte de bande passante due à l'envoi de tous les messages d'enregistrement de COA dans le cadre de changement féquent de réseau.

Finalement, on peut aussi noter l'apparition de délai, voire de perte de paquet, lors d'un changement de réseau, dû au mécanisme un peu lourd d'enregistrement de COA (les paquets envoyés pendant le transfert de COA seront perdu car envoyés à l'ancien FA).

2.4.3 Conclusion

Mobile IP est un protocole efficace pour la mobilité IP compte tenu des grandes exigences inhérentes à IPv4. En pratique, il marche plutôt bien pour des noeuds peu mobiles, se déplaçant surtout entre réseau (macro-mobilité) et peu fréquemment. Il arrive cependant rapidement à ses limites dès lors que les noeuds bougent beaucoup et au sein d'un même réseau (micro-mobilité). Pour répondre à ce problème de micro-mobilité, d'autres protocoles ont été implémenté sur le même modèle comme CellularIP par exemple.

Cependant, la plus grande amélioration à Mobile IP viendra de son implémentation sur IPv6, offrant une grande quantité d'adresses IP, ce qui permettra notamment que tous les noeuds aient des « collocated care-of-adress ».

Chapitre 3

Simulation

3.0.4 Etude du hand-off de base

Etudions le comportement d'un noeud mobile lorsqu'il se déconnecte de son Home Agent pour se reconnecter plus tard via un Foreign Agent. Voir figure.

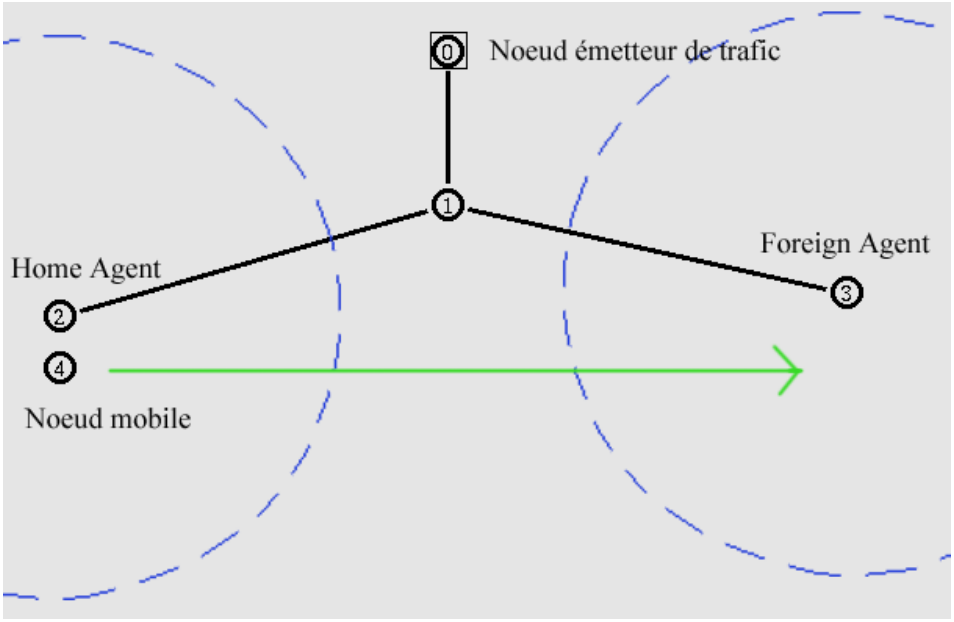

FIG. 3.1 – Hand-off basique

Pour cette simulation, les champs d'action des deux agents sont dissociés. Leur rayon d'action est de 250m alors qu'ils sont séparés de 600m.

On crée une source UDP au noeud 0 qui émettra en continu (Constant BitRate) en direction du noeud mobile (à partir de t=10s). Celui-ci, initialement placé au niveau du Home Agent (et connecté à lui), se déplacera

lentement en direction du Foreign Agent, à partir de t=20s et à une vitesse de 10m/s.

On étudie alors les délais obtenus ainsi que la présence ou l'absence de paquet droppés. XGraph nous donne le résultat sous forme graphique (voir figure).

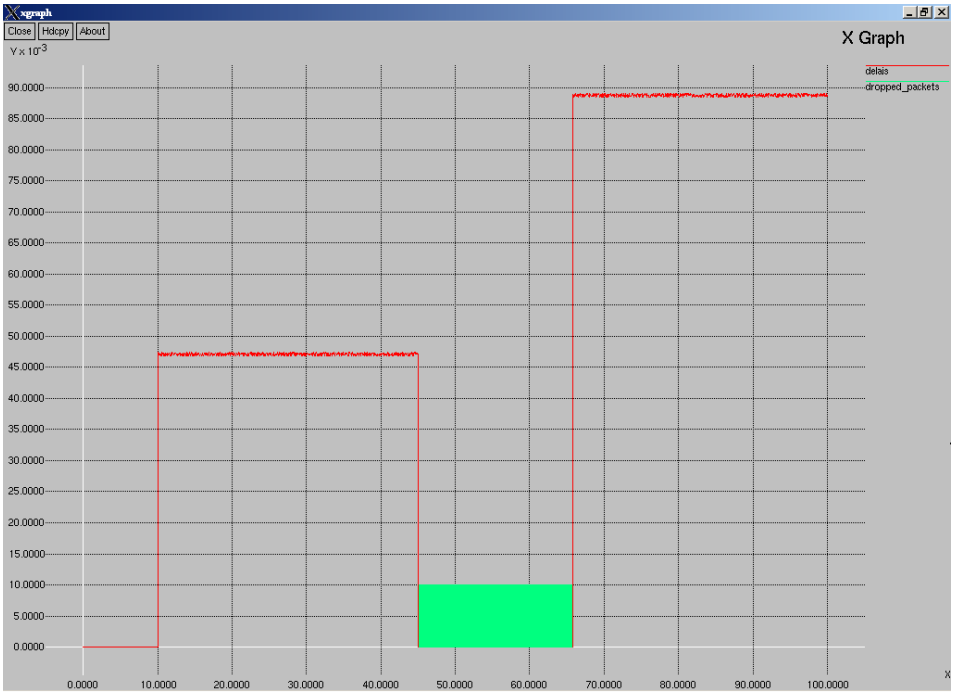

FIG. 3.2 – Graphique obtenu

On peut voir que tant que le noeud mobile reste dans le champ d'action du Home Agent, la connexion est stable, il n'y a aucun paquet perdu et les délais sont quasiment constants.

Au bout de 45s de simulation, le noeud mobile sort de ce champ d'action et la connexion est alors interrompue. Tous les paquets sont perdus.

Au bout de 55s, le noeud mobile pénètre dans le champ d'action du Foreign Agent. S'ensuit alors un processus d'authentification et d'enregistrement auprès du Home Agent qui peut se vérifier dans la trace par des échanges de paquets udp entre le noeud et les deux agents.

Quelques secondes plus tard, l'authentification est effectuée, la connexion peut reprendre. Les paquets ne sont plus droppés, mais comme ils doivent transiter par le Home Agent, les délais de transmission ont considérablement augmenté (routage triangulaire).

3.0.5 Comparaison UDP / TCP

Reprenons l'exemple précédent en remplaçant notre application à débit constant par une application de type FTP utilisant TCP.

On obtient le résultat présenté sur la figure.

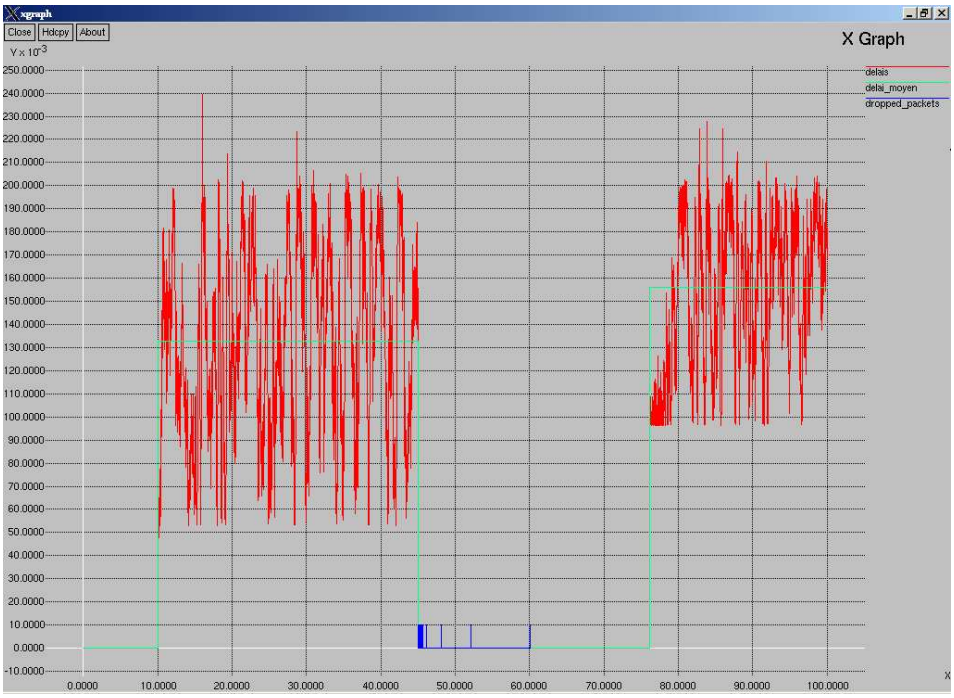

FIG. 3.3 – Graphique obtenu

On remarque tout d'abord que les délais sont beaucoup plus variables qu'avec l'UDP. Cela peut s'expliquer par les caractéristiques spécifiques du protocole TCP utilisées à des fins de fiabilité (TCP handshake, contrôle, ...).

Grâce à ce contrôle, l'application émettrice s'aperçoit que les paquets n'arrivent plus à destination et va alors réémettre le paquet qui n'est pas arrivé (cela se vérifie dans la trace grâce au numéro de séquence des paquets) à des intervalles de plus en plus longs. L'avantage de cette méthode est que l'on n'encombre plus le réseau. L'inconvénient est que l'on "rate" le début de la reconnexion s'il survient au milieu d'un intervalle. Au final, la durée de déconnexion du noeud mobile est plus longue qu'avec UDP.

Une fois le paquet arrivé, la connexion peut reprendre en transitant par les agents. Ce qui cause une augmentation très nette du délai moyen de transmission des paquets (en vert sur la figure).

3.0.6 Application à un réseau encombré

On reprend la connexion UDP décrite plus haut mais on ajoute un trafic externe pour simuler un réseau presque saturé.

Ce trafic va se faire entre le Foreign Agent et le Home Agent.

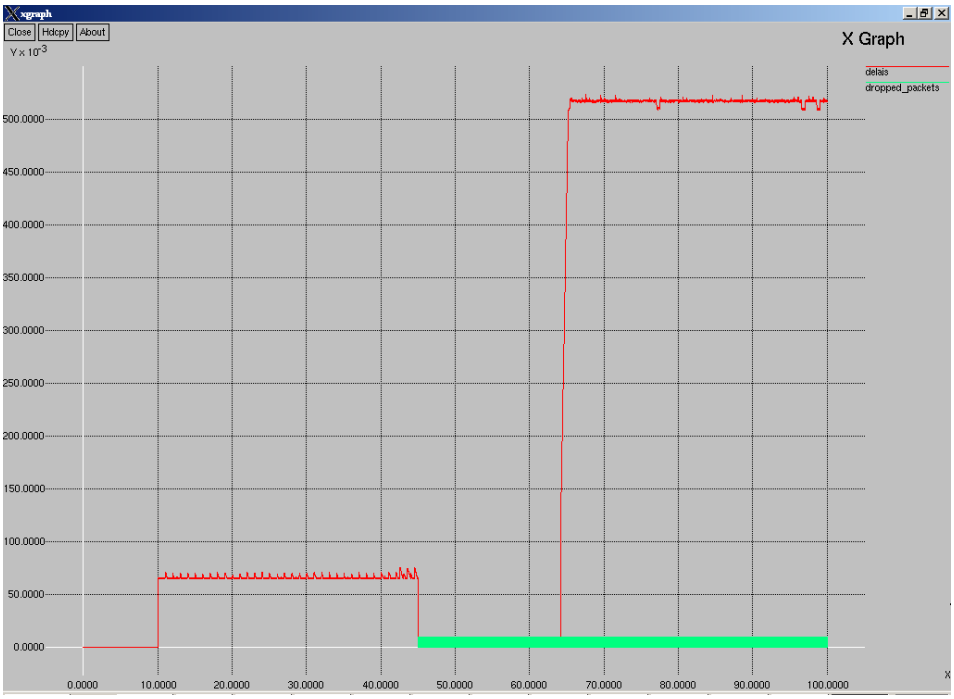

FIG. 3.4 – Graphique obtenu

On voit donc qu'alors qu'aucun paquet n'est perdu lorsqu'on est dans le Home Network, le fait de passer dans le Foreign Network sature complètement le réseau filaire, ce qui se traduit par des pertes de paquets pour les deux connexions ainsi que par une importante augmentation des délais.

3.0.7 Chevauchement des zones de couverture des agents

On voudrait voir ce qu'il se passe si les champs d'action des deux agents ne sont plus clairement séparés comme précédemment mais se chevauchent en partie.

Au cours de nos essais, nous avons remarqué que si au départ le noeud mobile est situé dans les deux zones de couverture des agents, NS le relie d'emblée au Foreign Agent et effectue un routage triangulaire non nécessaire.

On prend donc une distance de 300 mètres entre les deux agents afin d'éviter ce phénomène (à partir du test TCP de base). On obtient le résultat de la figure.

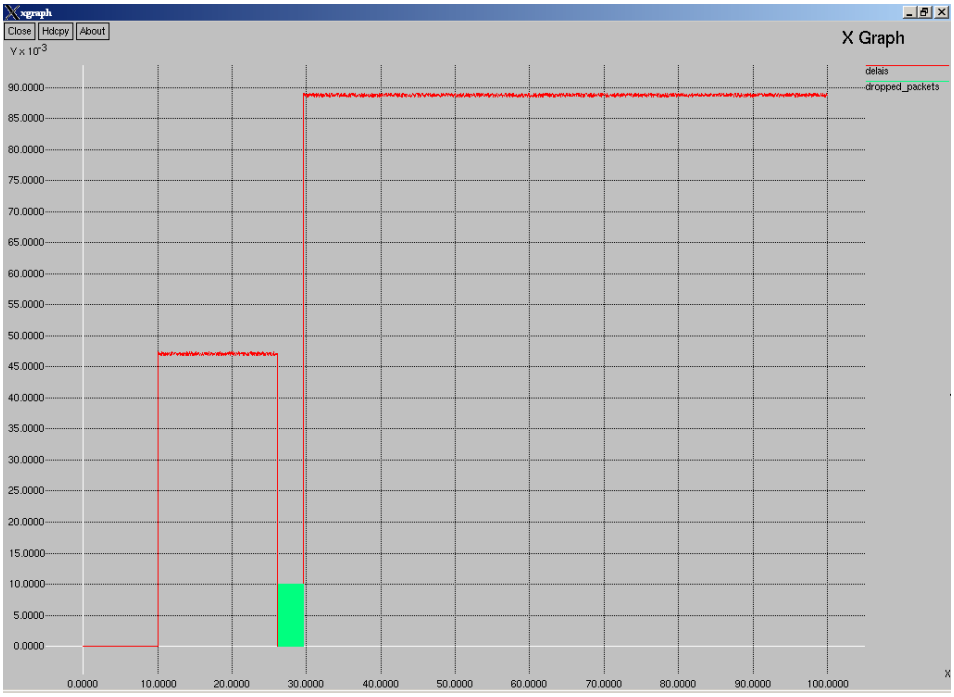

FIG. 3.5 – Graphique obtenu

On remarque que le noeud mobile se connecte au Foreign Agent dès qu'il arrive à sa portée (à t=25s). Cette fois-ci, le temps de déconnexion et de perte des paquets est un peu moins long qu'auparavant. Il fait à peine 5 secondes. Ce qui est tout à fait honorable en pratique.

On peut donc imaginer un réseau d'agents permettant de couvrir une zone importante à l'intérieur de laquelle on pourrait circuler librement sans connaître de déconnexions importantes. C'est là tout l'avantage de Mobile IP.

On peut cependant s'interroger sur l'intérêt de préférer une connexion passant par le Foreign Agent plutôt que par le Home Agent. Il y a là une perte de performances regrettable. On pourrait imaginer à la place un algorithme permettant à un noeud mobile de s'identifier auprès du Foreign Agent tout en continuant à communiquer avec le réseau via le Home Agent tant qu'on le peut. Celui-ci attend pour faire transiter les paquets via le Foreign Agent que le noeud mobile soit hors de portée. Cela réduirait de plus considérablement la durée de déconnexion (puisque le noeud mobile est déjà identifié auprès du Foreign Agent) et par conséquent le nombre de paquets perdus.

Chapitre 4

Compte-rendu du projet

Nous avons été confrontés à plusieurs problèmes au cours de ce projet. Tout d'abord nous nous sommes vite rendus compte que le programme NAM n'était pas vraiment compatible avec les technologies sans-fil. D'une part il est incapable de représenter les échanges ayant lieu entre des noeuds mobiles. D'autre part, il ne peut pas placer correctement les noeuds appartenant à la fois au réseau filaire et au réseau sans fil. Les différents agents n'étant plus à leur place, la simulation ne nous est plus vraiment utile, sauf pour voir les paquets échangés via le réseau filaire.

Par ailleurs, l'apprentissage de NS a été difficile. Mis à part les quelques tutoriaux expliquant les bases, la documentation disponible est très obscure et nécessite de nombreuses recherches avant de pouvoir trouver ce que l'on veut.

La plus grosse partie du temps a donc été passée à ce travail de recherche et de documentation.

Bibliographie

[1] *Présentation de Mobile IPv4 et QoS dans Mobile IPv4* par Chloé Rolland (2004)

[2] *RFC 2002 — Mobile IP standard*

[3] *Route optimisation in Mobile IP internet Draft* par le Mobile IP Working Group (1997)

[4] *Tutorial : Mobile Networking Through Mobile IP* par Charles E. Perkins

[5] *The Network Simulator 2* — Site officiel,
`http://www.isi.edu/nsnam/ns/`

[6] *Tutorial for the Network Simulator « ns »* par Mark Greis,
`http://www.isi.edu/nsnam/ns/tutorial/index.html`

[7] *NS2 : principes de conception et d'utilisation* par des chercheurs du lip6, `ftp://www-rp.lip6.fr/pub/pan/papers/Manuel_NS1.3.pdf`

[8] *Mobile IP Testing* par Syed Shahzad Ali,
`http://www.geocities.com/shezy22/cisco_mip/config_mip_01.html`