MESURES DES PERFORMANCES DU PROTOCOLE OLSR

Anis Laouiti, Cédric Adjih
Projet Hipercom,
INRIA, Domaine de Voluceau - Rocquencourt
78150 Le Chesnay, France
anis.laouiti@inria.fr, cedric.adjih@inria.fr

Résumé

Dans cet article, nous présentons les mesures de performances d'une implémentation du protocole de routage ad hoc OLSR. OLSR, abréviation de "Optimized Link State Routing", est un protocole de routage pour les réseaux sans fil soumis actuellement au groupe de standardisation MANET de l'IETF. OLSR est un protocole proactif, et par conséquent l'échange des messages de contrôle et les mises à jour de la topologie et se font d'une façon périodique.

L'implémentation du protocole OLSR nous a permis d'améliorer la détection des liens entre les différentes machines et de réduire les instabilités constatées dans notre premier réseau de test. Nous avons effectué par la suite à des tests plus importants avec une vingtaine de machines dont nous donnons des résultats dans cet article.

1 Introduction

Le domaine des réseaux locaux sans fil ad hoc, en même temps que celui des réseaux sans fil tout court, suscite de plus en plus d'intérêt depuis les cinq dernières années. La particularité de ce type réseau est qu'il n'a besoin d'aucune installation fixe à l'inverse d'autres types de réseaux (comme par exemple le GSM). Donc, il est facile et rapide à déployer. De plus, les différents composants de ce réseau sont libres de se mouvoir mais en même temps, ceci résulte en une topologie dynamique susceptible de changer d'une façon imprévisible.

Lorsque des participants n'arrivent pas à s'entendre directement, des nœuds intermédiaires peuvent jouer le rôle de relayeurs par un routage interne. Ce routage interne devient plus complexe lorsque les nœuds bougent. Les protocoles de routage classiques qui s'appliquent aux réseaux filaires deviennent inefficaces. D'où la nécessité de créer de nouveaux protocoles qui répondent aux nouveaux besoins et qui prennent en compte les nouveaux paramètres (mobilité, liens asymétriques, nœuds cachés, ..).

C'est l'objectif des protocoles de routage ad hoc ; ces protocoles de routage doivent être totalement distribués, c'est-à-dire qu'aucune entité centrale ne doit tout régenter ; de plus, les protocoles doivent réagir aux changements imprévisibles et rapides du réseau sans fil. Les nœuds composant le réseau ad hoc sont autonomes et libres de se mouvoir à leur gré.

Parmi de tels protocoles de routage, nous citerons ceux proposés à la standardisation IETF : OLSR[1], AODV[3], DSR[4], FSR[2], ...

De nombreuses études par simulations ont été effectuées pour évaluer les performances des protocoles de routage sans fil ; ces études ont permis de définir et de construire en quelque sorte la plus grande partie des protocoles, en testant l'impact des différentes idées, et ainsi qu'en testant l'influence de différents paramètres de fonctionnement. Mais, les tests sur des démonstrateurs en échelle réelle restent une étape primordiale. En effet, les modèles de couche physique (voire de couche MAC) utilisés dans les simulations sont souvent simplifiés et ne prennent pas en compte convenablement un certains nombre de phénomènes physiques, souvent difficilement modélisables, concernant notamment les aléas des transmissions radios.

Dans cet article, nous nous intéressons en particulier à OLSR (Optimized Link State Routing). C'est un protocole proactif, développé essentiellement par le projet HIPERCOM, dont une implémentation a été réalisée, permettant de faire

des tests en grandeur réelle d'efficacité et de robustesse, très utiles dans le contexte de standardisation des protocoles de communication. L'implémentation est publique et disponible à l'URL `http://hipercom.inria.fr/olsr/`.

Dans la première section nous décrivons brièvement le protocole de routage OLSR et la technique des relais multipoints. Puis dans la section suivante, nous soulignons les problèmes rencontrés lors des premières expériences et nous décrivons les solutions proposées. Enfin, nous rapporterons certains résultats des mesures de performances effectuées sur un réseau de vingt nœuds.

2 Description d'OLSR et des relais multipoints

Comme son nom l'indique, OLSR est un protocole à état de lien optimisé ; il obtient aussi des routes de plus court chemin. Alors que dans un protocole à état de lien, chaque nœud déclare ses liens directs avec ses voisins à tout le réseau, dans le cas d'OLSR, les nœuds ne déclarent qu'une sous-partie de leur voisinage grâce à la technique des relais multipoints.

Relais multipoints

Ils consistent essentiellement, en un nœud donné, à ignorer un ensemble de liens et de voisins directs, qui sont redondants pour le calcul des routes de plus court chemin : plus précisemment, dans l'ensemble des voisins d'un nœud, seul un sous-ensemble des ces voisins est considéré comme pertinent. Il est choisi de façon à pouvoir atteindre tout le voisinage à deux sauts (tous les voisins des voisins), cet ensemble est appelé l'ensemble des relais multipoints. Un algorithme de calcul de relais multipoints est donné dans [5].

Ces relais multipoints sont utilisés de deux façons : pour diminuer le trafic dû à la diffusion des messages de contrôle dans le réseau, et aussi pour diminuer le sous-ensemble des liens diffusés à tout le réseau puisque les routes sont construites à base des relais multipoint.

Diffusion par relais multipoints

La diffusion d'un message, à tout le réseau, par répétition, peut se faire par l'innondation classique utilisant la règle *un nœud retransmet un message si et seulement si il ne l'a pas déjà reçu*. La *diffusion par relais multipoints* (décrite dans [5]), diminue le nombre de retransmissions en utilisant la règle de suivante : *un nœud retransmet un message si et seulement si 1) il ne l'avait pas déjà reçu, et 2) il vient de le recevoir d'un nœud dont il est un relais multipoint.*

La figure 1 donne un exemple de gain en nombre de retransmissions sur un graphe simple. Supposons qu'un nœud émette un message, et que pour diffuser cette information au réseau ses voisins répètent cette information. Dans le premier

FIG. 1 – Les relais multipoints

graphique, à gauche, où tous les voisins d'un nœud retransmettent, six répétitions (les nœuds en noirs) sont nécessaires. Par contre, en utilisant la retransmission par les relais multipoints seuls (à droite), on économise deux retransmissions.

Protocole OLSR

Pour maintenir à jour toutes les informations nécessaires au choix des relais multipoints et le calcul de la table de routage, les nœuds OLSR ont besoin de s'échanger des informations périodiquement.

- Pour s'informer du proche voisinage, les nœuds OLSR envoient périodiquement des messages dits `HELLO` contenant la liste de leurs voisins. Ces messages permettent à chacun de choisir son ensemble de relais multipoints.
- itemize Le deuxième type de message de OLSR sont les message `TC` (*Topology Control*). Par ce message les sous-ensembles de voisinage que constituent les relais multipoints sont déclarés périodiquement dans le réseau.

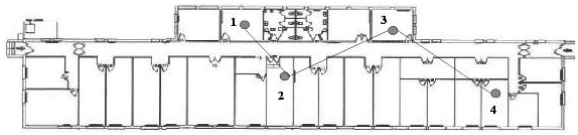

FIG. 2 – Premier réseau de test OLSR

Ils sont diffusés en utilisant une diffusion optimisée par relais multipoints. Ces informations offrent une carte de réseau contenant tous les nœuds et un ensemble partiel des liens, mais suffisant pour la construction la table de routage.

La table de routage est calculée par chacun des nœuds et le routage des données s'effectue saut par saut sans l'intervention d'OLSR dont son rôle s'arrête à la mise à jour de la table de routage de la pile IP.

3 Expérimentation d'OLSR

Le protocole a été développé sous le système Linux avec la famille des noyaux 2.* et le système FreeBSD, et les tests ont été réalisés avec des systèmes Linux.

3.1 Topologie

La topologie du réseau de test est constituée de routeurs disposés, en intérieur, dans quatre bureaux donnant une topologie linéaire représentée sur la figure 2, équipés de cartes sans fil IEEE 802.11b Lucent Silver (avec une modulation jusqu'à 11 Mbps). Cette topologie permet de tester le protocole dans ses conditions extrêmes, c'est-à-dire une connectivité minimale, puisque les routeurs ne disposent que d'un seul chemin disponible pour joindre un nœud donné, et une instabilité dans le réseau peut être paralysante pour l'ensemble et est rapidement mise en évidence. Elle permet de traquer et cerner les problèmes plus facilement.

Ci-dessous, nous donnons une description des problèmes réseau rencontrés au cours des tests, suivie d'une explication sur leurs origines et des solutions trouvées.

3.2 Problèmes constatés :

1. Instabilité des liens : en suivant l'évolution du contenu de les tables de voisinage et de routage, nous avons constaté l'apparition et la disparition d'un lien entre le nœud 2 et 4. Ce phénomène rendait la table de routage instable. De plus, ce lien ne permet pas une transmission de données satisfaisante.
2. Communication impossible entre deux voisins, alors que, d'après les tables de voisinage et du routage celle-ci devait être possible.

3.3 Origines des problèmes :

1. La puissance de réception est sujette à des variations continuelles et imprévisibles dues à plusieurs facteurs. L'environnement local et ou même les conditions climatiques peuvent jouer un rôle dans la propagation des ondes magnétiques. Une porte qui se ferme, ordinateur déplacé, un obstable proche de la carte sans fil, peuvent influer sur

les réflexions et les interférences des signaux et peuvent impliquer un changement de chemins. Un lien initialement asymétrique, peut devenir temporairement symétrique suite à un échange avec succès de trois messages de HELLO successif. Par la suite, le lien peut redevenir asymétrique rapidement. Cette situation est gênante, elle provoque parfois un changement dans les relais multipoints et en conséquence dans la table de routage ; donnant une configuration des routes incorrecte et bloquant les communications en point à point. Le but est alors d'éliminer ces liens transitoires à courte durée de vie, inutilisables ; ceci peut se faire par le biais de hystérésis des liens.

2. Ce type de problème peut provenir de l'incompatibilité de certaines techniques de codage utilisées dans les cartes sans fil. Nous avons utilisé des cartes compatibles. En examinant de plus près le fonctionnement de la carte, nous avons constaté que les messages en broadcast (broadcast IP) sont transmis avec une modulation à 1 Mbps, tandis l'unicast peut être transmis à 2, 5.5 ou 11 Mbps. Or les émissions à 1 Mbps sont plus naturellement plus fiables (rapport signal/bruit nécessaire plus faible) avec donc une portée plus grande.

   Comme l'échange des paquets de contrôle dans OLSR se fait en broadcast, l'image du réseau fournie par ces paquets peut se révéler incorrecte pour des paquets unicast (avec des liens inutilisables). L'introduction de la mesure de puissance réduit considérablement l'influence de ce phénomène.

4 Hystérésis des liens (Link Hysteresis)

Dans cette section, nous détaillons les solutions introduites, visant à améliorer la détection des bons liens et la mise à l'écart des mauvais liens.

- La méthode des N hellos consécutifs : Cette méthode, la plus simple, consiste à considérer un lien comme valide si l'on reçoit un nombre N de messages de Hellos consécutifs d'un voisin. Cette méthode contrôle la qualité d'un lien seulement à sa détection et ne prend pas en compte les fluctuations qui suivent.
- La méthode du Link Hysteresis proposée par Joe Maker[1]. La variable du Link hysteresis est mise à jour à chaque réception de message de Hello. En utilisant le numéro de séquence dans les messages de Hellos, nous pouvons détecter le nombre de messages perdus et en déduire une métrique de la qualité du lien $N\_Quality$:

$$N\_Quality = (1-\alpha) * N\_Quality * (Miss\_Hellos) + \alpha \quad (1)$$

- La Link Hysteresis améliorée, où la détection de la perte d'un hellos se fonde sur la détection d'un numéro de séquence de hello manquant. Nous avons ajouté une nouvelle variable, *Link hysteresis estimée*, qui est mise à jour chaque période de Hello. Cette méthode permet d'avoir une meilleure estimation que la précédente parce qu'elle n'attend pas une réception d'un nouveau hello pour la mise à jour, et donc prend en compte rapidement les pertes.
- La méthode se basant sur la puissance du signal. Comme nous l'avons dit, les paquets de broadcast sont envoyés avec une modulation à 1 Mbps, plus facile à recevoir au niveau du récepteur, alors que les données sont envoyées plus rapidement à 11 Mbps. Cette différence, faisait que les messages de contrôles sont reçus plus facilement et la conclusion qu'un lien est symétrique était erronée dans certains cas.
  Dans l'implémentation d'OLSR et dans les tests qui suivent, la puissance du signal reçu est prise en compte.

Les méthodes de contrôle de qualité de lien utilisent l'hystérésis ; ils fixent deux seuils, un seuil haut et un seuil bas. Un lien est initialement accepté lorsque son indice de qualité franchit le seuil haut et rejeté lorsque ce dernier devient inférieur au seuil bas. Entre les deux seuils, le lien est gardé et considéré comme valide et utilisable. La figure 3 donne un exemple de l'évolution de la qualité d'un lien. Les parties grises sont des zones où le lien est considéré comme mauvais. La qualité d'un lien peut être par exemple, la puissance du signal reçu ou la valeur du Link Hysteresis.

L'idéal serait de combiner la puissance du signal reçu et les paramètres du Link Hysteresis ; la première fournit la puissance du signal et la deuxième nous renseigne sur la qualité du lien.

[1] Chairman du groupe de travail MANET à l'IETF et chercheur travaillant à la Navy Research Laboratory aux Etats-Unis

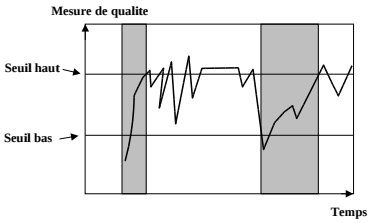

FIG. 3 – Contrôle de la qualité des liens dans OLSR

5 Mesures des performances du réseau OLSR

Nous avons intégré le contrôle de la puissance dans le démon OLSR et nous l'avons installé sur une vingtaine de machines pour mesurer les performances de ce réseau. Les seuils de puissance choisis étaient -81 dB et -87 dB, à partir de valeurs de sensibilité de la vitesse indiquées dans le manuel des cartes sans fil pour les débits de 5.5 et 11 Mbps. Les tests étaient effectués une nouvelle fois en intérieur avec deux types de mesures :

- Des mesures de performances du réseau sans trafic de données : les paquets de contrôles échangés dans le réseau sont enregistrés.
- Le deuxième type de mesures est effectué avec deux types de trafic de données UDP et TCP : un ensemble du trafic de données est injecté suivant un scénario déterminé.

iperf[6] est l'outil utilisé pour la génération de trafic de données.

5.1 Le réseau expérimental

Le réseau expérimental est composé de vingt nœuds, douze routeurs industriels, 6 PC, et 2 ordinateurs portables. Ils sont équipés de cartes à 11 Mbps Wi-Fi de Lucent et Compaq. Le réseau formé est statique (sans mobilité).

Les nœuds sont disposés sur tout le bâtiment de 50 mètres de long. comme indiqué sur la figure 4. Les numéros figurant sur le schéma sont les derniers octets des adresses

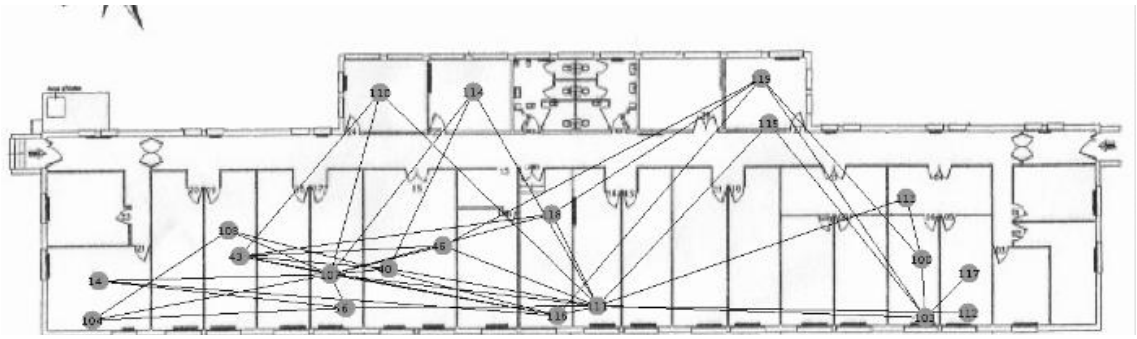

FIG. 4 – Réseaux expérimental à 20 nœuds

5.2 Performances sans trafic de données

Dans ces premières mesures, nous avons enregistré une trace du trafic de tous les messages de contrôle. Essentiellement les messages Hellos et TC reçus, émis, rejetés, et relayés. Les mesures présentées ont été effectuées sur huit heures.

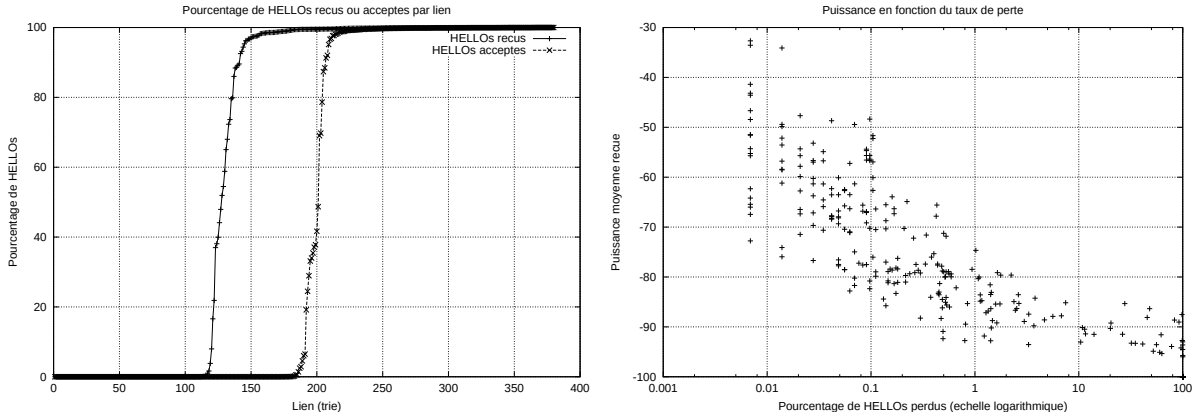

FIG. 5 – Pourcentage de Hellos reçus ou acceptés par un lien et Puissance en fonction du taux de perte (Echelle logarithmique)

La droite de la figure 5 représente le pourcentage des messages Hello reçus et celui de ces messages acceptés. Un phénomène intéressant pour notre protocole est la distribution des pourcentages de réception. Il y a essentiellement une concentration sur deux états : ou bien la quasi-totatalité des paquets sont reçus, ou bien la quasi-totalité des paquets ne sont pas reçus. Les cas intermédiaires existent toujours ou les messages sont reçus partiellement même en appliquant les seuils de réception. Les valeurs intermédiaires, peuvent encore être corrigées en appliquant la méthode du Link Hysteresis qui permet de suivre les fluctuations de la qualité d'un lien sur le temps. La figure de gauche 5 illustre la puissance moyenne des messages Hellos reçus en fonction de pourcentage des messages Hellos non reçus sur le même lien. On remarque une forte concentration des points entre 0 et 1%. Une autre conclusion qui confirme le fait attendu que plus la puissance est forte, plus la probabilité des paquets d'être acceptés est élevée.

5.3 Performances avec trafic de données UDP et TCP

Les modèles de trafic choisis sont les modèles 1 à N, et N à 1. Plus explicitement, le modèle 1 à N, consiste à prendre une seule machine source et ouvrir autant de flux que de machines N. Ce type de communication apparaît lorsqu'il y a un seul point de sortie d'un réseau et que tous les nœuds reçoivent les données par l'intermédiaire de celui-ci. Le modèle N à 1 est le modèle inverse. Ces types de réseaux servent à tester les nœuds passerelles et la robustesse du réseau dans des conditions d'utilisation. Nous avons testé ces deux modèles avec des flux de données TCP et UDP. Les tests consistent à ouvrir des connexions entre la source et la destination et émettre des données pendant une dizaine de minutes, avec des longueurs de trames des données est de 1400 octets. Chaque configuration est testée dix fois de suite, à partir de l'état de repos.

5.3.1 Avec trafic TCP

Ci-après, les tableaux résument les résultats de débit des données transférées sur dix minutes pour les dix expériences en TCP selon les modèles 1 à N et N à 1. Les débits affichés dans les tableaux sont les débits exprimés en kilo (K) ou méga (M) bit par seconde reçus par les destinations.

Modèle 1 à N

machine	exp. 1	exp. 2	exp. 3	exp. 4	exp. 5	exp. 6	exp. 7	exp. 8	exp. 9	exp. 10
108	**1.33 M**	**1.45 M**	**1.55 M**	**1.53 M**	**1.34 M**	**1.33 M**	**1.29 M**	**1.45 M**	**1.47 M**	**1.42 M**
110	**1.36 M**	**1.48 M**	**1.59 M**	**1.54 M**	**1.42 M**	**1.36 M**	**1.34 M**	**1.49 M**	**1.50 M**	**1.47 M**
112	**0.20 M**	**0.16 M**	**0.12 M**	14.61 K	**0.14 M**	**0.14 M**	**0.41 M**	87.47 K	83.84 K	**0.20 M**
115	**0.99 M**	**0.94 M**	**0.85 M**	**1.02 M**	**0.96 M**	**0.89 M**	**0.72 M**	**0.99 M**	**0.93 M**	**0.87 M**

TAB. 1 – Débit reçu en TCP utilisant le modèle 1 à N avec 4 destinations et une source (machine 116) située au milieu du bâtiment

machine	exp. 1	exp. 2	exp. 3	exp. 4	exp. 5	exp. 6	exp. 7	exp. 8	exp. 9	exp. 10
108	**2.44 M**	**2.39 M**	**2.39 M**	**2.39 M**	**2.41 M**	**2.38 M**	**2.39 M**	**2.38 M**	**2.39 M**	**2.41 M**
110	**2.62 M**	**2.71 M**	**2.73 M**	**2.72 M**	**2.72 M**	**2.70 M**	**2.73 M**	**2.72 M**	**2.73 M**	**2.72 M**
112	-	0.00	-	0.00	-	0.96 K	0.00	0.00	-	-
115	0.00	-	-	0.11 K	-	-	-	0.25 K	-	-

TAB. 2 – Débit reçu en TCP utilisant le modèle N à 1 avec 4 sources et une destination (machine 116) située au milieu du bâtiment

La source est placée au milieu du bâtiment mais le nombre de connexions TCP est limité à quatre. Les résultats sont donnés dans le tableau 1. Avec ce scénario, on obtient des résultats relativement stables sur les dix expériences consécutives. le débit le plus important atteint $1,59$ Mbps.

Modèle N à 1 Le tableau 2 donne les résultats du scénario de 4 machines sources et une machine destination située au milieu du bâtiment. La même remarque que précédemment s'impose encore plus clairement. Cette fois, deux sources se partagent toute la bande passante (les machines 108 et 110)

5.3.2 Avec trafic UDP

Pour cette série d'expériences le débit d'émission des paquets est fixé à 1 Mbps pour chaque flux, et la taille des paquets étant la même que précédemment (1400 octets). Le débit est fixé à 1 Mbps pour chaque flux contrairement au "meilleur effort" de TCP.

Modèle 1 à N

Le tableau 3 illustre les résultats de tests du modèle 1 à N avec 4 machines destinations et une machine source (machine 116 située au milieu du bâtiment). Avec ce troisième tableau 3, les débits reçus se rapprochent des débits émis. Le réseau est nettement moins chargé et permet un trafic plus fluide. La machine par exemple 112 reçoit plus de trafic UDP qu'avec TCP.

Modèle N à 1 Le tableau 4 illustre les débits enregistrés avec un trafic UDP pour 4 machines sources et une machine destination 116. Contrairement au cas du TCP, là encore, aucune machine n'est limitée aux profit des autres car le débit maximal est fixé à 1 Mbps par source. Ce qui laisse une chance aux autres stations de transmettre leurs données.

machine	exp. 1	exp. 2	exp. 3	exp. 4	exp. 5	exp. 6	exp. 7	exp. 8	exp. 9	exp. 10
108	**0.91 M**	**0.90 M**	**0.90 M**	**0.92 M**	**0.91 M**	**0.90 M**	**0.89 M**	**0.89 M**	**0.88 M**	**0.89 M**
110	**0.92 M**	**0.90 M**	**0.91 M**	**0.91 M**	**0.91 M**	**0.91 M**	**0.90 M**	**0.88 M**	**0.89 M**	**0.88 M**
112	**0.73 M**	**0.67 M**	**0.75 M**	**0.76 M**	**0.69 M**	**0.69 M**	**0.66 M**	**0.63 M**	**0.71 M**	**0.68 M**
115	**0.84 M**	**0.80 M**	**0.84 M**	**0.85 M**	**0.84 M**	**0.85 M**	**0.79 M**	**0.77 M**	**0.82 M**	**0.82 M**

TAB. 3 – Débit reçu en UDP utilisant le modèle 1 à N avec 4 destinations et une source (machine 116) située au milieu du bâtiment

machine	exp. 1	exp. 2	exp. 3	exp. 4	exp. 5	exp. 6	exp. 7	exp. 8	exp. 9	exp. 10
108	**1.01 M**	**1.01 M**	**1.01 M**	**1.01 M**	**1.01 M**	**0.99 M**	**1.00 M**	**1.00 M**	**0.99 M**	**1.00 M**
110	**1.02 M**	**1.02 M**	**1.02 M**	**1.02 M**	**1.02 M**	**1.02 M**	**1.02 M**	**1.02 M**	**1.02 M**	**1.02 M**
112	80.41 K	**0.53 M**	**0.52 M**	**0.14 M**	**0.55 M**	**0.65 M**	**0.55 M**	**0.36 M**	**0.43 M**	**0.53 M**
115	**0.69 M**	**0.54 M**	**0.51 M**	**0.73 M**	**0.62 M**	**0.52 M**	**0.51 M**	**0.65 M**	**0.64 M**	**0.63 M**

TAB. 4 – Débit reçu en UDP utilisant le modèle N à 1 avec 4 sources et une destination (machine 116) située au milieu du bâtiment

5.3.3 Conclusion sur les performances

Nous avons utilisé deux types de modèles : 1 à N, et N à 1. Avec un trafic de type TCP, le modèle 1 à N favorise les stations se trouvant à un saut, mais permet aussi d'acheminer des données vers des machines à plus de 1 saut, surtout dans le cas où le nombre de destinations est de quatre seulement. Dans le cas du modèle N à 1 avec 4 destinations, les machines se trouvant à un saut de la destination monopolisent la bande passante aux dépends des autres stations, et certaines d'entres elles n'arrivant même pas à établir une connexion ; c'est un problème d'équité dans le routage multisaut. Avec UDP, et en fixant le débit maximal à l'émission à 1 Mbps par source, nous remarquons, que les les machines sources ont des débits plus équitables : en effet, la bande passante n'est pas saturée par un seul ensemble de machines, et laisse une opportunité aux autres. Ceci indique qu'un système pour rétablir l'équité pourrait être mis en place, et serait utile pour les flux TCP.

6 Conclusion

Nous avons présenté les résultats expérimentaux du protocole de routage OLSR, qui a été implémenté sous deux systèmes d'exploitation (Linux et FreeBSD). Les expérimentations sur un petit réseau de quatre nœuds, ont permis d'étudier le problème d'instabilité des liens radio. Nous avons proposé des méthodes pour surmonter le problème causé au routage par ce phénomène, notamment, les méthodes de Link Hysteresis et le contrôle de puissance de réception. Dans la deuxième étape, nous avons utilisé une vingtaine de machines et avons procédé à plusieurs de types de tests et de mesures de performances. Ils ont fait apparaître une bonne résistance et un bon partage du réseau dans les cas où les débits en émissions sont limités, mais des problèmes d'équité pour TCP.

Références

[1] P. Jacquet, P. Mühlethaler, A. Qayyum, A. Laouiti, T. Clausen, L. Viennot, "Optimized Link State Routing Protocol" , IEEE INMIC Pakistan, Dec 2001.

[2] G. Pei, M. Gerla, T. W. Chen, "Fisheye State Routing : A Routing Scheme for Ad hoc Wireless Networks", Proceedings of the IEEE International Conference on Communications (ICC), pages 70-74, New Orleans, LA, June 2000.

[3] C. Perkins, E. Royer, "Ad Hoc On-Demand Distance Vector Routing", Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, pages 90-100, New Orleans, LA, February 1999.

[4] David B. Johnson,David A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks", Mobile Computing , volume 5, pages 153-181, Kluwer Academic Publishers, 1996.

[5] A. Qayyum, A. Laouiti, L. Viennot,"Multipoint relaying technique for flooding broadcast messages in mobile wireless networks", HICSS, Hawaii, Jan 2002.

[6] IPERF, http ://dast.nlanr.net/Projects/Iperf/.

[7] NETPERF, http ://www.netperf.org/.