Couplage Multicast et Mobilité IPv6 dans la plate-forme pair-à-pair JDukeBox

Frédéric Beck, Vincent Delove, Isabelle Chrisment, Olivier Festor

Couplage Multicast et Mobilité IPv6 dans la plate-forme Pair à Pair JDukeBox

Streaming multicast IPv6 avec une application pair à pair sur une architecture Mobile IPv6

Frédéric Beck, Vincent Delove, Isabelle Chrisment, Olivier Festor

Projet MADYNES - INRIA/LORIA
Technopôle de Nancy-Brabois - Campus scientifique
615, rue de Jardin Botanique - B.P. 101
54600 Villers-Lès-Nancy Cedex
France

[frederic.beck,vincent.delove,isabelle.chrisment,olivier.festor]@loria.fr

RÉSUMÉ. *Dans cet article nous présentons les conclusions d'une étude menée dans notre laboratoire sur le couplage de plusieurs protocoles de différents niveaux pour la réalisation d'un juke-box distribué. Si conceptuellement tous ces protocoles ont été conçus pour vivre en harmonie, nous démontrons au travers de cette expérience que la réalité et les implantations en décident parfois autrement.*

ABSTRACT. *In this article we present the conclusions of a study made in our laboratory on the coupling of several protocols from different levels for the realization of a distributed jukebox. If conceptually all these protocols should work in harmony, we demonstrate through this experience that the reality and the implementations often decide differently.*

MOTS-CLÉS : *IPv6, Mobilité, Multicast, Pair à Pair, JXTA*

KEYWORDS: *IPv6, Mobillity, Multicast, Peer to Peer, JXTA*

e soumission à *NOTERE 2006*, le 13 octobre 2006.

1. Introduction

L'explosion du marché des PDA et des ordinateurs portables depuis quelques années facilite grandement le télé-travail, et permet un gain de productivité non négligeable en mettant à profit les temps dits morts, notamment lors des trajets. L'essor des nouvelles technologies de réseaux sans-fil à haut-débit (802.11, UMTS, 3G) introduit une nouvelle problématique : les usagers souhaitent avoir accès aux mêmes fonctionnalités de nomadisme et de mobilité avec leurs PC portables ou PDA que celles disponibles sur les réseaux GSM.

C'est dans cette optique que des recherches ont été menées pour définir la Mobilité IP qui permet à des utilisateurs de rester connectés à l'Internet tout en se déplaçant. Si elle est difficile et contraignante à réaliser en IPv4 [PER 02], l'évolution du protocole IP vers sa nouvelle version, IPv6 [DEE 98], simplifie son architecture et a conduit à la standardisation de la Mobilité IPv6 [JOH 04]. Depuis plusieurs années, de nombreux travaux de validation et d'expérimentations ont été menés pour promouvoir IPv6 et les fonctionnalités offertes par ce nouveau protocole. On peut notamment citer le projet européen 6Net [1]. En 2005, le projet français IPv6 ADIRE [2] avait pour but de promouvoir la mise en production du protocole IPv6 en général, et de la mobilité en particulier. C'est dans ce contexte que cette étude a été réalisée.

Parallèlement les communications de groupe ont suscité beaucoup d'intérêt au cours de la dernière décennie. En effet, les transmissions multicast sont apparues comme un des services de communication les plus efficaces pour l'acheminement de données entre de multiples parties. A l'heure actuelle, le développement des services de diffusion de télévision sur ADSL est une illustration parfaite de son utilisation à grande échelle. Il nous est donc apparu essentiel de tester les possibilités de coupler ces technologies. Ainsi un scénario possible consiste à imaginer un utilisateur mobile souhaitant suivre une diffusion multimédia et en multicast (conférence, émission télé...) au cours d'un de ses déplacements. Le terminal de réception (téléphone, PDA, ordinateur portable) disposant de plusieurs interfaces de connexion (802.11, UMTS, 3G) offrira à Mobile IPv6 un accès à l'ensemble des réseaux permettant de proposer un service de bout-en-bout à l'utilisateur. Cet exemple semble à première vue un scénario standard de l'utilisation de Mobile IPv6. Mais il soulève en fait un certain nombre de problèmes liés au déploiement d'une infrastructure capable de faire cohabiter multicast et mobilité ce qui constitue un sujet assez peu documenté à ce jour.

Les objectifs de notre étude sont multiples. En effet, le multicast et la mobilité IPv6 sont des technologies utiles à de nombreuses applications, mais nous verrons que leur déploiement et leur couplage posent des problèmes. Dans cet article, nous présentons leur intégration dans une application pair à pair. Le plan du papier est le suivant : La section 2 décrit le contexte ainsi que les travaux similaires réalisés à ce jour. La section 3 met en évidence les défis à relever et les solutions apportées en termes de transmission, d'architecture et de sécurité. La section 4 illustre ces solutions en décrivant les

1. http ://www.6net.org
2. https ://ipv6.u-strasbg.fr

mises en œuvre réalisées. Finalement la section 5 résume les contributions apportées et propose plusieurs perspectives.

2. Travaux similaires et contexte

Depuis la standardisation de Mobile IPv6 et des premières implantations, un certain nombre de mises en œuvre ont été réalisées afin de démontrer l'intérêt de ce protocole à travers des cas pratiques d'utilisation. Parmi les travaux les plus aboutis nous pouvons notamment citer ceux réalisés dans le cadre du projet nautilus6 [3]. À titre d'exemple, le E-Bicycle [EBI] est un vélo disposant d'un réseau mobile (NEMO Basic Support [DEV 05]) constitué d'un PDA et de capteurs. L'ensemble permet de collecter diverses informations à distance (localisation, température...) et offre également la possibilité au cycliste de communiquer tout en se déplaçant. Basée sur le même principe, une expérimentation menée au Japon et intitulée "Mobile Emergency Room" [MOB] consiste à intégrer un réseau mobile dans une ambulance dans le but d'échanger des informations précieuses (vidéo, ECG) entre ambulanciers et personnel soignant (docteurs, infirmières). L'utilisation de la mobilité rend alors possible des interactions entre ces deux milieux du début de l'intervention des ambulanciers jusqu'à leur arrivée à l'hôpital.

Afin d'évaluer la continuité de la réception des flux multicast par un mobile lors d'un changement de réseaux nous avons choisi d'utiliser une application multimédia développée au sein de l'équipe MADYNES : le JDukeBox [4]. JDukeBox est un outil collaboratif de diffusion de fichiers multimédia utilisant une architecture pair à pair. Il s'agit plus exactement d'un juke-box coopératif et distribué où les différents utilisateurs ont la possibilité de créer et rejoindre des groupes au sein desquels ils partageront l'ensemble de leurs ressources (audio ou vidéo). Chaque membre d'un groupe pourra alors modifier la liste de lecture associée à ce dernier (playlist) en y ajoutant la ressource de son choix.

L'utilisation de l'architecture pair à pair basée sur les mécanismes JXTA [5] permet de gérer et de contrôler le système distribué sans se soucier de la nature du réseau (IPv4, IPv6...). Les différents pairs constituant la plate-forme s'organisent de la façon suivante. Dans chaque groupe de diffusion, un ou plusieurs pairs jouent le rôle de "rendez-vous". Cette instance particulière a pour fonction principale la découverte des pairs n'étant pas directement connectés. Ces derniers peuvent alors communiquer avec l'ensemble du groupe. En parallèle de la couche de gestion et de contrôle JXTA, le démon MJBox est chargé de la diffusion des ressources multimédia sur IP multicast. La source du flux multicast est toujours le pair qui possède la ressource. Au final, les interactions entre ces deux couches mais aussi entre les différents pairs d'un groupe permettent de réaliser une diffusion multicast séquentielle qui suit l'évolution de la playlist.

3. http ://www.nautilus6.org
4. http ://potiron.loria.fr/projects/madynes/jdukebox
5. http ://www.jxta.org

3. Défis à relever

Notre infrastructure d'étude se compose de plusieurs hôtes, mobiles et fixes, membres d'un même groupe de diffusion JDukeBox. Notre objectif était de permettre aux nœuds mobiles de changer de sous-réseau tout en continuant à recevoir le flux multicast des fichiers actuellement diffusés dans le groupe, après éventuellement une légère interruption due aux mécanismes de mise à jour inhérents à la mobilité. La réalisation de ce scénario fait naître plusieurs difficultés concernant notamment l'association de la mobilité avec le multicast, l'architecture pair à pair et les aspects de sécurité.

3.1. *Mobilité IPv6 et multicast*

Le couplage de la mobilité IPv6 et du multicast nécessite d'apporter le multicast aux nœuds mobiles. Dans la pratique, deux choix existent.

La première solution consiste à rejoindre le groupe multicast lors de chaque changement de réseau avec son adresse correspondant au réseau dit visité, ou Care-of Address (CoA). Cette solution est difficile à mettre en œuvre. En effet, elle dépend fortement des réseaux visités et émet l'hypothèse que TOUS les réseaux que l'on va visiter offrent le support du multicast, ce qui n'est pas réaliste aujourd'hui. D'autre part, à chaque changement de réseau, en plus de la procédure de mise à jour des adresses pour la Mobilité IPv6 en elle-même, il faudrait que l'application (ou un middleware) détecte les modifications de la CoA et rejoigne à nouveau le groupe multicast avec cette nouvelle adresse, ce qui complique la phase de "roaming" et allonge l'interruption.

Une autre approche consiste à utiliser l'adresse mère, ou Home Address (HoA), du nœud mobile (MN) pour rejoindre les groupes multicast. Ceci implique que les données multicast soient encapsulées par les démons de mobilité et passent par les tunnels lorsque le MN est dans un réseau visité. Cette solution est plus séduisante que la précédente, car elle tire pleinement partie des mécanismes de mobilité, et l'utilisation de l'adresse mère permet d'éviter de nombreux problèmes liés à la reconstruction des arbres multicast lorsque le mobile est récepteur, ou de son identification lorsqu'il est source, notamment avec le modèle SSM [HOL 01]. Cependant, avec la mobilité IPv6, il est possible que le nœud mobile dialogue directement avec ses correspondants (sans tunnel via le Home Agent) par l'usage de la Return Routability Procedure [JOH 04]. Néanmoins ce mode de fonctionnement implique que le correspondant dispose lui aussi d'une implantation de la mobilité mais surtout, que le mobile utilise sa CoA pour les communications. Dans ce contexte on se retrouve donc dans la même situation que précédemment où le mobile doit rejoindre le groupe multicast dans chaque réseau visité, ce qui explique pourquoi nous n'avons pas utilisé cette optimisation.

3.2. *Mobilité IPv6 et sécurité*

Il est également obligatoire de s'attarder un moment sur les possibilités de sécurité qu'apporte Mobile IPv6. En effet, la mobilité introduit un certain nombre de risques supplémentaires et peut constituer une faille quant à la protection du réseau mère. Pour pallier cela, le protocole inclut des spécifications de sécurité reposant sur l'utilisation d'IPsec [ARK 04] pour la protection des messages de signalisation. La mise en œuvre de ces spécifications permet alors notamment l'authentification des acteurs (Mobiles, Correspondants, Agent mère) et le chiffrement de certaines données de signalisation, pour contrer partiellement les attaques visant le Home Agent, les correspondants ou directement le mobile. L'absence d'authentification des acteurs offrirait par exemple la possibilité à une machine mal intentionnée de détourner le trafic afin de récupérer les données en provenance d'un mobile (usurpation de l'identité du Home Agent) ou à destination d'un mobile (usurpation de l'identité du mobile). Les attaques visant les correspondants dans un cadre d'utilisation de la Return Routability Procedure sont sans aucun doute les risques les plus probables puisqu'il n'est pas raisonnable d'envisager que le lien de confiance entre ces deux acteurs est aussi fort que celui établi entre le mobile et son agent mère. Par conséquent, une sécurisation entre ces deux entités reste aujourd'hui difficile à mettre en œuvre. Cependant comme nous l'avons brièvement expliqué ce mode de fonctionnement de Mobile IPv6 ne convient pas ici pour faire cohabiter multicast et mobilité. D'une manière plus générale il est important de souligner que l'utilisation de cette optimisation de route entre un mobile et son correspondant reste à l'heure actuelle très peu utilisée.

4. Mise en œuvre

Notre application utilise les mécanismes JXTA pour gérer le système distribué pair à pair. Or, L'introduction de la mobilité sur une architecture pair à pair ne nuit pas conceptuellement à son fonctionnement. Une étude détaillée des protocoles et des configurations est cependant indispensable pour s'assurer de la validité de cette affirmation. Dans cette section, nous détaillons les choix effectués pour faire face aux défis présentés dans la précédente section, ainsi que les conclusions relatives au couplage de la mobilité et du pair à pair.

4.1. *Un "Home Agent Multicast"*

L'idée revient à mettre en œuvre un "Home Agent Multicast", c'est-à-dire un Home Agent intégrant un routeur multicast IPv6. De cette façon, tous les nœuds du réseau mère ainsi que les nœuds mobiles présents dans un réseau visité auront accès au multicast.

La mise en œuvre du Home Agent Multicast a été réalisée en plusieurs étapes. La première étape consiste à choisir l'implantation de la mobilité la plus adaptée à notre objectif. Les implantations de Home Agent actuellement disponibles sont Mobile IPv6

for Linux (MIPL) [6] et SHISA sous BSD grâce à KAME [7]. Cisco propose également une implantation d'un agent mère dans les dernières versions de l'IOS, mais celle-ci ne pouvait nous satisfaire du fait de son status trop expérimental. Les implantations MIPL et SHISA sont toutes deux fonctionnelles, stables et nous avons pu vérifier leur interopérabilité. Nous nous sommes donc intéressés à leur cohabitation avec le multicast. L'implantation SHISA agit comme une "boîte noire" (les tunnels ne sont pas visibles et ne peuvent donc pas être pris en compte par les démons de routage). SHISA ne permet donc pas une utilisation conjointe du multicast et de la mobilité. Nous avons donc retenu MIPL.

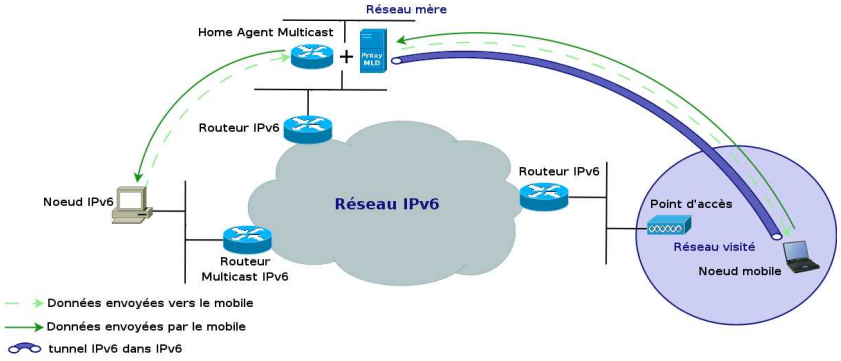

Figure 1. *Scénario d'utilisation d'un Home Agent multicast*

Nous avons déployé le démon de routage mrd6 [8] qui intègre le support de PIM-SM [EST 97] et MLD [VID 04]. Ce démon offre l'avantage de réaliser une découverte dynamique des interfaces ce qui permet dans notre cas de détecter sans redémarrage l'apparition ou la disparition des tunnels lorsqu'un nœud mobile s'attache ou se détache du Home Agent. D'autre part, le support de MLD et du *forwarding* des paquets est inclus dans le démon lui-même, ne nécessitant pas de recompiler le noyau.

À ce stade, nous disposons d'un Home Agent agissant comme un routeur multicast. Au niveau des nœuds mobiles, s'ils sont dans un réseau visité, un tunnel est donc créé entre eux et le Home Agent. Ce tunnel devient l'interface par défaut pour les paquets unicast, mais pas pour le multicast. Pour tous les paquets multicast (correspondant au préfixe ff00 : :/8), l'interface physique reste l'interface par défaut. Les messages MLD envoyés pour joindre et quitter les groupes, ainsi que les données émises par les mobiles, sont donc envoyés sur le réseau visité et non pas vers le Home Agent via les tunnels Mobile IPv6. Pour corriger ce comportement, il est nécessaire d'intervenir sur la table de routage du mobile pour que l'interface tunnel soit utilisée par défaut pour l'ensemble du trafic multicast.

6. http ://www.mobile-ipv6.org
7. http ://www.kame.net
8. http ://artemis.av.it.pt/mrd6/

Ainsi, les messages MLD et les données émises à destination de groupes multicast sont bien envoyés dans le tunnel et réceptionnés par le Home Agent. Mais si les messages MLD sont bien pris en compte par le démon de routage multicast, permettant ainsi au nœud mobile d'être récepteur pour un groupe multicast, les données émises par ce même mobile sont ignorées par mrd6. Il semblerait que ce comportement soit lié à une relation d'ordre de désencapsulation. Nous supposons en effet que les paquets vus par le démon mrd6 sont les paquets unicast de la mobilité et pas les paquets multicast en eux-mêmes, ce qui expliquerait qu'ils soient ignorés et non routés. L'utilisation conjointe d'un proxy MLD avec le démon de routage permet de résoudre ce problème.

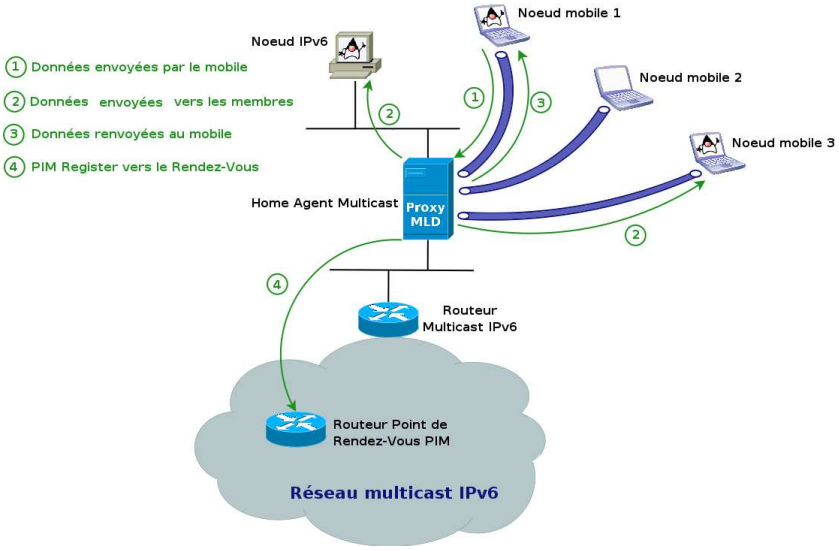

Figure 2. *Fonctionnement du proxy MLD*

Le Proxy MLD[9] a été conçu pour permettre à un nœud mobile d'avoir accès aux fonctionnalités multicast IPv6 en utilisant les tunnels Mobile IPv6, pour éviter les problèmes liés à la présence non garantie de multicast dans les réseaux visités, et ce lorsque le Home Agent n'est pas un routeur multicast. La seule hypothèse à émettre quant au fonctionnement du proxy, est que le Home Agent dispose d'une interface sur un réseau qui offre les services multicast. Nous avons donc adapté ce proxy à notre problématique pour obtenir le comportement décrit dans la figure 2. Lorsqu'un mobile envoie des données multicast dans le tunnel vers le Home Agent (étape 1 dans la figure 2), ces données sont captées par le proxy. Elles sont envoyées vers les membres directement connectés à le Home Agent (2 dans la figure 2), c'est-à-dire les nœuds mobiles associés et les nœuds du réseau mère qui appartiennent au groupe en question. Ensuite,

9. http ://www-r2.u-strasbg.fr/~jelger/MLD/MLD_Proxy_Main.htm

les données sont renvoyées au mobile (3 dans la figure 2) pour lui permettre de recevoir ce qu'il émet. En effet, même par l'utilisation de l'option IPV6_MULTICAST_LOOP sur la socket, l'émetteur ne pourrait pas écouter la chanson qu'il émet. Finalement, les données sont encapsulées dans un message PIM Register [EST 97] et envoyées au routeur dit Point de Rendez-Vous pour le groupe multicast (4 dans la figure 2) afin que tous les membres du groupe puissent avoir accès au flux via l'arbre de diffusion multicast.

Grâce à ces modifications, nous obtenons le comportement souhaité, à savoir un mobile capable d'être source et récepteur pour des groupes multicast, et ce tout en changeant de réseau IPv6.

4.2. *JXTA et mobilité IPv6*

L'utilisation des protocoles JXTA a facilité la configuration de l'application JDukeBox sur un poste mobile. En effet les outils de configuration mis à disposition de l'utilisateur se sont avérés très pertinents. Ils offrent la possibilité de choisir l'ensemble des interfaces utilisées pour communiquer avec les autres pairs de la plateforme. Dans un contexte de mobilité il convient de choisir l'interface adressée avec le préfixe du réseau mère (interface tunnel) afin de rendre les changements de réseaux transparents aux yeux de l'application.

Comme l'illustre la figure 3, l'architecture d'un réseau virtuel JXTA introduit des pairs spécifiques, dits points de rendez-vous. Cette instance particulière d'un pair a pour fonction principale la découverte des pairs n'étant pas directement connectés. Ces derniers peuvent alors communiquer avec l'ensemble du groupe. L'utilisation de l'adresse mère d'un mobile s'avère ici très utile car elle permet à un mobile de jouer le rôle de rendez-vous, son adresse restant unique aux yeux des autres pairs lors de ses déplacements.

4.3. *Sécurisation*

La sécurité est un point épineux de la mobilité. En effet, en réponse aux risques d'attaques évoqués, IPSec [KEN 98b] a été utilisé pour sécuriser les messages de signalisation entre les différents acteurs. La mise en œuvre de cette sécurisation consiste donc à définir les associations de sécurité IPsec correspondant aux messages Binding Updates et Binding Acknowledgements émis respectivement par un mobile et son agent mère. A l'heure actuelle, seules les implantations MIPL (Linux) et Shisa (BSD) offrent cette possibilité et peuvent, à ce titre, être envisagées dans des systèmes de production. L'implantation BSD fournit de plus des outils facilitant l'élaboration des fichiers de configuration IPsec. Ces fichiers de configuration définissent l'utilisation d'ESP [KEN 98a] en mode transport pour la mise à jour d'association entre le nœud mobile et son agent mère.

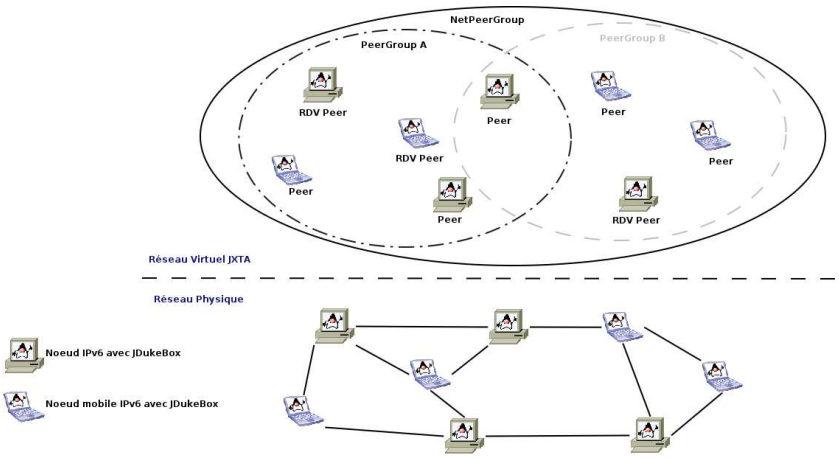

Figure 3. *Architecture du réseau JXTA*

On notera tout de même que seuls les messages de signalisation sont ici authentifiés et/ou chiffrés. Dans ces conditions et comme la mobilité est logiquement associée à l'utilisation de réseaux à diffusion (802.11, 3G...), l'utilisateur devra veiller à ne pas émettre d'informations sensibles. En effet un nœud mobile sera par définition amené à visiter un nombre important de réseaux disposant très certainement de niveaux de sécurisation inégaux (WEP, WPA...). Il sera alors primordial que ce dernier utilise des applicatifs suffisamment sécurisés (HTTPS, POPS, IMAPS) pour éviter le vol d'informations ou de comptes. Un mécanisme de sécurité pour les communications multicast est d'ailleurs en cours de développement dans l'équipe et devrait prochainement intégrer l'application JDukeBox.

5. Conclusion et perspectives

L'objectif de cette étude était de coupler plusieurs technologies telles que le multicast, la mobilité IPv6 et les architectures Pair à Pair. Nous avons néanmoins identifié plusieurs problèmes, liés au passage du multicast dans les tunnels Mobile IPv6, et plus particulièrement lorsqu'un mobile est source, à l'introduction de la mobilité dans une architecture pair à pair, où la couche applicative (JXTA) impose une contrainte à une couche inférieure (IP), et enfin, nous avons mis en évidence l'importance de sécuriser une telle architecture.

Par l'utilisation de JDukeBox, nous avons démontré que ce couplage était possible, au prix de nombreuses adaptations. Cette étude a été validée par une démonstration réalisée dans le cadre des JRES'2005 [10].

10. http ://www.jres.org

Les travaux présentés ouvrent plusieurs perspectives. Contrairement à mrd6, le proxy MLD n'effectue pas de découverte dynamique des interfaces et donc des tunnels. Une extension est ici nécessaire. La solution évoquée pour permettre au mobile de recevoir les données qu'il envoie dans le tunnel fonctionne, mais comme l'adresse source est modifiée, cela peut être problématique quant à l'identification de la source. De plus, le trafic est doublé ; si cela fonctionne pour le mode multicast ASM [DEE 91], cela ne fonctionnera pas pour le modèle SSM [HOL 01]. Enfin, des améliorations et des optimisations sont possibles pour diminuer l'interruption pendant la période de *roaming* ; l'utilisation d'optimisations telles que FMIP [KOO 05] est ici envisageable.

6. Bibliographie

[ARK 04] ARKKO J., DEVARAPALLI V., DUPONT F., « Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents », RFC 3776 (Proposed Standard), juin 2004.

[DEE 91] DEERING S., « Multicast routing in a datagram internetwork », PhD thesis, Standford University, décembre 1991.

[DEE 98] DEERING S., HINDEN R., « Internet Protocol, Version 6 (IPv6) Specification », RFC 2460 (Draft Standard), décembre 1998.

[DEV 05] DEVARAPALLI V., WAKIKAWA R., PETRESCU A., THUBERT P., « Network Mobility (NEMO) Basic Support Protocol », RFC 3963 (Proposed Standard), janvier 2005.

[EBI] « E-Bicycle - A Live Light-Weight IPv6 Demonstration Platform for ITS Usages - http ://demo.nautilus6.org ».

[EST 97] ESTRIN D., FARINACCI D., HELMY A., THALER D., DEERING S., HANDLEY M., JACOBSON V., LIU C., SHARMA P., WEI L., « Protocol Independent Multicast-Sparse Mode (PIM-SM) : Protocol Specification », RFC 2117 (Experimental), juin 1997, Obsoleted by RFC 2362.

[HOL 01] HOLBROOK H., « A channel model for multicast », PhD thesis, Standford University, août 2001.

[JOH 04] JOHNSON D., PERKINS C., ARKKO J., « Mobility Support in IPv6 », RFC 3775 (Proposed Standard), juin 2004.

[KEN 98a] KENT S., ATKINSON R., « IP Encapsulating Security Payload (ESP) », RFC 2406 (Proposed Standard), novembre 1998.

[KEN 98b] KENT S., ATKINSON R., « Security Architecture for the Internet Protocol », RFC 2401 (Proposed Standard), novembre 1998, Updated by RFC 3168.

[KOO 05] KOODLI R., « Fast Handovers for Mobile IPv6 », RFC 4068 (Experimental), juillet 2005.

[MOB] « Mobile Emergency Room - An IPv6-based Video System for Emergency Care Support - http ://www.ipv6style.jp/en/special/20051031_2/index.shtml ».

[PER 02] PERKINS C., « IP Mobility Support for IPv4 », RFC 3220 (Proposed Standard), janvier 2002, Obsoleted by RFC 3344.

[VID 04] VIDA R., COSTA L., « Multicast Listener Discovery Version 2 (MLDv2) for IPv6 », RFC 3810 (Proposed Standard), juin 2004.