

Architecture Multi Domiciliée dans les Réseaux Mobiles : Diminution de l'Impact de la Mobilité sur les Protocoles de Transport

Lionel Bertaux^{*,**} Pascal Berthou^{*,**}
Thierry Gayraud^{*,**}

*CNRS ; LAAS ; 7 avenue du Colonel Roche, F-31077 Toulouse, France
lbertaux, pberthou, tgrayraud@laas.fr,

**Université de Toulouse ; UPS, INSA, INP, ISAE ; LAAS ; F-31077 Toulouse, France

Résumé. Les routeurs mobiles fournissent une connexion fiable avec une mobilité transparente à tous les nœuds connectés à leur réseau. Les protocoles de Transport sont affectés par cette transparence car l'état du réseau d'accès change sans avertissement, rendant l'évaluation du réseau difficile. Notre architecture propose d'informer les protocoles de Transport lorsqu'un changement de réseau est effectué afin de diminuer l'impact sur les communications. Cette solution est basée sur la définition de plusieurs interfaces réseaux au niveau des nœuds du réseau mobile et l'utilisation du protocole de Transport multi domicilié SCTP.

1 Introduction et Problématique

Les appareils mobiles se démocratisent depuis plusieurs années et font aujourd'hui partie de notre quotidien : téléphones intelligents, tablettes, ordinateurs portables... Les utilisations et fonctionnalités de ces appareils augmentent sans cesse mais restent limitées par leur autonomie et leur faible encombrement. Notamment les tablettes et téléphones qui sont conçus pour consulter du contenu en ligne et non stocker les informations. Il est donc nécessaire d'être connecté à Internet ou un autre réseau de grande envergure pour utiliser pleinement un appareil mobile. Dans un contexte nomade, des réseaux Wi-Fi sont disponibles dans la plupart des maisons et dans quasiment tous les bureaux. Dans un contexte mobile, une connexion au réseau 3G/UMTS est indispensable et peut engendrer une consommation excessive de la batterie et/ou des frais supplémentaires. Les transports en commun sont amenés à évoluer pour offrir de nouveaux services sur les appareils mobiles des usagers : de la consultation des horaires et des trajets à un accès complet à Internet (mails, blogs, streaming).

La grande autonomie des transports en commun ainsi que l'espace disponible à bord rend possible le déploiement de plusieurs interfaces réseaux de technologies différentes : Wi-Fi, 3G/UMTS, satellite... Ces véhicules peuvent alors agir comme des routeurs mobiles (MR) et fournir un accès aux nœuds mobiles qui sont connectés. Pour cela, ils doivent implémenter un gestionnaire de mobilité capable de garantir une connexion stable entre les différents points d'accès (AP) extérieurs et les nœuds finaux (appareils des utilisateurs). Les nœuds finaux ne sont pas informés de la mobilité et n'ont rien à gérer.

Architecture Multi Domiciliée dans les Réseaux Mobiles

Chaque réseau possède des caractéristiques qui lui sont propres : congestion, délai, bande-passante... En changeant de réseau d'accès, le chemin utilisé par les communications est modifié et les réseaux traversés sont différents. Les caractéristiques du chemin sont alors modifiées immédiatement et d'une grande ampleur suivant les technologies (voir le tableau 1 qui contient des exemples de délais et débits). Pour les nœuds finaux, effectuer un changement de réseau de manière transparente revient donc à modifier les caractéristiques du réseau sans prévention. Pour garantir la fiabilité de la communication ou limiter la congestion dans le réseau, certains protocoles de Transport évaluent l'état du réseau et le mémorise à l'aide de différents paramètres. Les plus connus sont :

- Fenêtre de congestion : quantité de données en vol, permet d'évaluer la bande-passante et la congestion en se basant sur le « Round Trip Time » (RTT) ;
- « Smoothed Round Trip Time » (SRTT) : délai aller-retour lissé, permet d'évaluer le délai subit par la communications et son évolution ;
- « Retransmission Time Out » (RTO) : valeur du temporisateur au-delà duquel un paquet est considéré comme perdu si non-acquitté, permet de détecter les pertes ;

En modifiant brutalement les caractéristiques du réseau, l'évaluation faite avec ces paramètres devient erronée et les conditions de communication sont mal estimées par les protocoles de Transport. Leurs réactions à certains évènements vont donc être induites en erreur par une mauvaise estimation de la situation. Pour cette raison, la plupart des protocoles de Transport supportent mal le changement de réseau.

Pour éviter une telle situation, nous proposons de notifier le protocole de Transport dans les nœuds finaux quand un changement de réseau est effectué afin que celui-ci puisse évaluer les caractéristiques du nouveau réseau plus précisément et ainsi améliorer son rendement. Les protocoles de Transport multi domiciliés sont conçus pour gérer plusieurs interfaces réseaux et chemins simultanément. Le protocole de Transport SCTP (Stream Control Transport Protocol) utilise la multi domiciliation pour basculer sans pertes entre différents réseaux et s'adapter rapidement aux conditions du nouveau réseau. En définissant plusieurs interfaces réseaux au niveau des nœuds utilisateurs, nous étendons la connaissance des chemins du routeur vers les nœuds mobiles. Le protocole SCTP est alors capable de communiquer sur l'interface voulu suivant la situation.

La section suivante est un état de l'art sur la mobilité des réseaux IP et l'impact sur les protocoles de Transport. Deux protocoles de Transport multi domiciliés y sont aussi présentés. La section 3 décrit la conception de l'architecture avec les composants nécessaires à sa mise en place puis les échanges entre le routeur mobile et les nœuds du réseau. L'impact du changement de réseau et la contribution de l'architecture sont analysés dans la section 4. Le papier finit par une conclusion et les futurs travaux.

Technologie de communication	Bande-Passante	Délai
Wi-Fi	plus de 10 Mbps	inférieur à 50 ms
3G/UMTS	entre 1 Mbps et 5 Mbps	entre 50 ms et 100 ms
Satellite	moins de 2 Mbps	de 110 ms à 250 ms

TAB. 1 – Exemples de bande-passante et délai pour différentes technologies de communication.

2 Etat de l'Art

L'architecture proposée repose sur plusieurs règles et mécanismes définis dans des RFC (Request For Comments) de l'IETF (Internet Engineering Task Force). La suite de cet article se base sur ces définitions pour la description des mécanismes existants et la définition des nouvelles actions. La gestion de la mobilité, la configuration du réseau et l'impact de la mobilité sur les protocoles de Transport sont introduits dans les sous sections suivantes.

2.1 Gestion de la mobilité dans les réseaux mobiles

Mobile IPv6 (mIPv6) Perkins et al. (2011) introduit les mécanismes de mobilité pour un hôte simple utilisant IPv6. Des règles et des échanges y sont définis pour le nœud mobile (« Mobile Node » MN), le nœud correspondant (« Corresponding Node » CN) et l'agent mère (« Home Agent » HA). Plusieurs améliorations ont été proposées pour réduire l'impact du changement de réseau et notamment diminuer la latence introduite par le changement de réseau : Hierarchical mIPv6, Fast Handover mIPv6, PmIPv6...

Avec la miniaturisation des composants électroniques et l'amélioration de leur rendement électrique, il devient possible d'inclure plusieurs interfaces réseaux dans les appareils mobiles. Le standard « Multiple Care-of-Addresses Registration » définit dans Wakikawa et al. (2009) permet l'utilisation de toute interface disponible avec mIPv6 et ses extensions. En apportant les règles et les mécanismes permettant de gérer la mobilité avec plusieurs interfaces réseaux, cette extension apporte la multi domiciliation à mIPv6. Les apports de la multi domiciliation ne concernent pas uniquement la mobilité : « Make Before Break » facilité lors du changement de réseau, amélioration de la connectivité, augmentation du débit en partageant la charge... Tsirtsis et al. (2011) définit l'extension « Flow Binding » qui va plus loin en proposant d'associer un flux à une interface réseau précise. Cette fonctionnalité peut s'avérer utile pour limiter la concurrence entre flux ou par exemple assigner un flux critique à une connexion stable.

Les standards présentés ci-dessus permettent à un nœud mobile simple de gérer sa mobilité sans pertes de données ou en minimisant les pertes. Dans le cas où les nœuds mobiles sont connectés à un routeur lui-même mobile, il est possible de simplifier la gestion de la mobilité dans les nœuds finaux en ajoutant au routeur des fonctionnalités rendant le réseau mobile. Le standard Network Mobility (NEMO) définit dans Devarapalli et al. (2005) ajoute les différents mécanismes permettant au routeur de gérer la mobilité du réseau entier. La figure 1 montre un réseau où les nœuds mobiles sont connectés à un routeur mobile (MR) et n'ont aucune connaissance des points d'accès. Toute donnée échangée entre les nœuds mobiles et les nœuds correspondants passe par le routeur. En s'enregistrant auprès d'un agent mère, le routeur peut gérer sa mobilité et reste joignable à tout instant. Le support de la multi domiciliation dans NEMO est discuté dans Ng et al. (2007) avec une étude de cas adaptée à notre situation : un routeur mobile, un agent home et plusieurs préfixes pour le réseau mobile.

L'utilisation d'un routeur mobile permet de proposer aux nœuds mobiles une connexion de meilleure qualité, soit en utilisant des technologies différentes de celles présentes dans les appareils mobiles, soit en embarquant des antennes mieux adaptées. Les nœuds connectés au réseau mobile n'ayant aucune connaissance des changements de réseau ou des chemins utilisés, la mobilité leur est totalement transparente. Cette transparence peut avoir un impact au niveau des performances comme nous le verrons en 2.2.

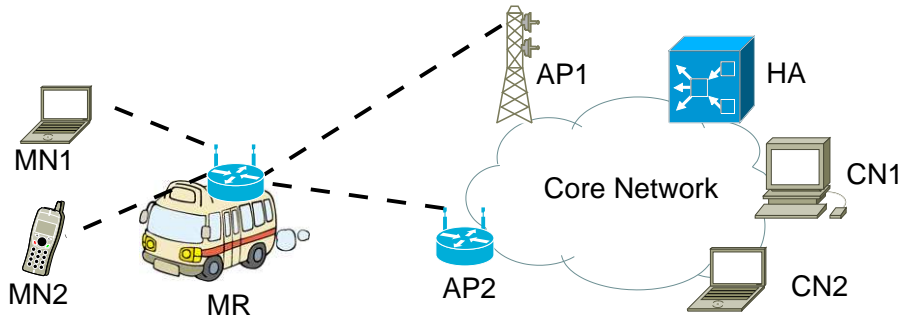


FIG. 1 – Composants présents dans un réseau mobile multi domicilié géré par NEMO.

2.2 Les Protocoles de Transport et la Mobilité

Lors d'un changement de réseau, plusieurs paramètres de la communication sont modifiés : l'identifiant réseau (adresse IP) change, une latence correspondant à la configuration de l'interface réseau peut être introduite et les caractéristiques du réseau sont modifiées. Si les solutions décrites précédemment permettent de gérer la mobilité de manière transparente c.-à-d. ne pas changer l'adresse IP du nœud et réduire la latence, certains événements liés au changement de réseau ne peuvent être « cachés » aux nœuds finaux :

- Réception non-ordonnée de paquets de données ;
- Modification du délai et/ou de la bande passante.

Ces événements ont un impact particulier sur les protocoles de Transport et sont difficilement évitables.

Afin d'améliorer les communications (adapter le débit d'émission, détecter la congestion et/ou les pertes, ...), les protocoles de Transport évaluent l'état du réseau et gardent un historique dans plusieurs paramètres : SRTT, RTO, fenêtre de congestion... Quand un événement se produit, les protocoles se basent sur leurs évaluations pour prendre les décisions adaptées. Comme le changement de réseau modifie l'état du chemin, les paramètres ne sont plus valides et peuvent induire en erreur le protocole de Transport : les livraisons non-ordonnées de paquets sont interprétées comme des pertes, l'augmentation du délai est perçue comme de la congestion... Les actions effectuées par le protocole de Transport après le changement de réseau peuvent donc être inappropriées :

- Retransmissions inutiles (perte de temps et surdébit) ;
- Mauvaise adaptation du débit d'émission :
 - Sous-utilisation de la bande-passante : perte de performance ;
 - Sur-utilisation de la bande-passante : introduction de congestion.

Le protocole de Transport le plus utilisé de nos jours est Transmission Control Protocol (TCP), il a été développé pour les réseaux filaires et supporte difficilement les changements de réseau ainsi que les spécificités des réseaux sans fils. Une synthèse de l'impact du changement de réseau sur TCP est donnée dans Hansmann et Frank (2003). L'étude se focalise sur la réorganisation des paquets et l'augmentation ou la réduction du produit délai bande-passante (BDP). Il est démontré que ces phénomènes introduisent respectivement des rafales de paquets,

un remplissage des mémoires au niveau du goulet d'étranglement ou une sous utilisation de la bande passante disponible. Plusieurs solutions sont discutées, la plupart consistant à modifier le protocole TCP. Néanmoins, l'utilisation de versions TCP spécifiques supportant le changement de réseau affecte les communications sur un lien stable et n'est donc pas la solution optimale. De plus, une version est difficile à déployer puisque les deux hôtes de la communication doivent l'implémenter pour que les fonctionnalités soient utilisées correctement.

Le nombre de réseaux d'accès augmentant et les cartes réseaux se miniaturisant, il est fréquent qu'un appareil possède plusieurs interfaces réseaux. Pour les protocoles de Transport fonctionnant en mode connecté, il est difficile de tirer partie de cette multi domiciliation. En effet, l'utilisation d'un identifiant basé sur l'adresse IP ne permet pas de basculer d'une interface à une autre facilement. À cette fin, des protocoles de Transport multi domiciliés ont été développés : Multipath Transmission Control Protocol (MPTCP) Ford et al. (2011) et Stream Control Transmission Protocol (SCTP) Stewart (2007).

Au sein de l'Internet Engineering Task Force, le groupe de travail MPTCP vise à ajouter la capacité de multi domiciliation à TCP. Le principe utilisé pour la conception de MPTCP est similaire à celui présenté dans Ford et Iyengar (2008) pour les protocoles de Transport de nouvelle génération : une « division » de la couche Transport avec une couche supérieure servant d'interface à l'application et chargée de gérer les multiples connexions établies dans la couche inférieure. Les connexions de la couche inférieure sont alors de simples connexions TCP mono domiciliées. Afin d'obtenir des performances optimales, un contrôle de congestion permettant la gestion des différents sous-flux a aussi été proposé dans Raiciu et al. (2011). MPTCP dans sa version basique ne propose pas de gestion de la mobilité même si le groupe de travail précise que le protocole doit être conçu pour la supporter. Des travaux proposent l'ajout de la mobilité : dans Sun et al. (2011), les auteurs se basent sur l'utilisation d'une adresse permanente utilisée par l'application et d'adresses IP temporaires utilisées au niveau IP pour le routage. MPTCP est donc un protocole de Transport prometteur porté par l'omniprésence de TCP dans Internet. Néanmoins, il s'agit d'un protocole encore récent et dont la standardisation est toujours en cours.

SCTP est un protocole de Transport offrant des services similaires à TCP : fiabilité, livraison ordonnée, contrôle de flux et évitement de la congestion. En plus de cela, SCTP supporte la multi domiciliation : plusieurs interfaces réseaux peuvent être utilisées dans une même association et sont référencées comme des chemins. Un des chemins est considéré comme primaire et utilisé pour transférer les données dans des « chunks » (morceaux contenues dans un paquet SCTP). Dans la version originale de SCTP, les adresses IP disponibles étaient définies lors de l'initiation de l'association et le changement de chemin primaire se faisait uniquement en cas de rupture du lien primaire. En ajoutant la modification dynamique des adresses IP de l'association, l'extension décrite dans Stewart et al. (2007) permet le support de la mobilité : ajouter une adresse IP puis utiliser celle-ci comme chemin primaire permet de basculer vers un nouveau réseau. L'échange des informations au cours de la communication introduisant une faille de sécurité, l'extension de Tuexen et al. (2007) ajoute un mécanisme d'authentification des messages de contrôles. Ces deux extensions ajoutées à SCTP sont communément appelées mobile SCTP (mSCTP).

SCTP permettant de réaliser un changement de réseau au cours de la communication, il pourrait être impacté similairement à TCP comme décrit dans Hansmann et Frank (2003). Afin d'éviter les problèmes relatifs au changement de réseau, SCTP utilise un jeu de paramètres

pour chaque chemin : le SRTT « Smoothed Round Trip Time », le RTO « Retransmission Time Out » et la fenêtre de congestion sont calculées pour un seul chemin. Les performances du protocole sur un nouveau réseau ne sont donc pas influencées par les caractéristiques de l'ancien réseau. Lors du transfert de données sur un chemin pour la première fois, les valeurs initiales sont utilisées, assurant ainsi un comportement au moins aussi performant que si une nouvelle association était initiée. En cas de retour sur un chemin précédemment utilisé, les dernières valeurs calculées sur ce chemin sont utilisées.

2.3 Configuration des réseaux IP

Neighbor discovery for IPv6, Narten et al. (2007) décrit les échanges permettant la configuration d'un réseau et le partage d'informations (préfixe IP, route) dans un réseau. Les messages échangés entre le routeur et les nœuds y sont définis. Les messages « Router Advertisement » (RA) permettent au routeur de diffuser ses différents préfixes IP et sont diffusés périodiquement. Les messages « Router Solicitation » (RS) sont des requêtes envoyées par les nœuds au routeur afin de solliciter l'émission d'un RA. Notre architecture va se baser sur ces messages pour diffuser les préfixes correspondants aux sous-réseaux et sur les mécanismes introduits par le standard pour la définition des différentes adresses

Afin de limiter le flux d'information, un routeur recevant un RS attend un certain délai avant de répondre avec un RA et ainsi répondre à plusieurs RS le cas échéant. Pour augmenter la réactivité du système, Daley et al. (2003) propose de répondre directement (FastRA) lors de la réception d'un RS et montre que l'impact sur les communications est insignifiant. En revanche, les temps de configuration des nœuds s'en trouvent améliorés.

3 Définition de l'Architecture

Les changements transparents de réseau impactent les performances des protocoles de Transport dans les nœuds finaux. Nous proposons une architecture qui réduit cet impact en informant les nœuds mobiles d'un changement de réseau d'accès au niveau du routeur. Une fois informés, les protocoles de Transport des nœuds utilisateurs peuvent s'adapter plus facilement aux conditions du nouveau réseau et répondre plus précisément aux événements provoqués par un changement de réseau. Les sous-sections suivantes décrivent plus précisément l'architecture : son fonctionnement, les composants du réseau qui sont nécessaires à sa mise en place et une proposition d'implémentation suivie de la définition des messages utilisés.

3.1 Fonctionnement

Notre architecture se base sur deux principes : (i) la définition d'un sous-réseau par interface possédée par le routeur et donnant vers l'extérieur, (ii) l'obligation pour les nœuds mobiles de configurer une adresse par sous-réseau. Si le nœud ne possède pas assez d'interfaces, des interfaces réseau virtuelles doivent être créées. En utilisant la fonctionnalité de multi domiciliation de SCTP, les nœuds sont capables de choisir l'interface envoyant les données et peuvent ainsi suivre les indications du routeur sur le sous-réseau à utiliser. Lors d'un changement de réseau, le routeur demande aux nœuds de changer de sous-réseau et les associations SCTP sélectionnent le chemin primaire correspondant.

La figure 2 illustre un réseau mobile utilisant notre architecture : deux nœuds mobiles sont connectés à un routeur et le routeur est connecté à deux points d'accès (AP). À chaque point d'accès correspond un sous-réseau à l'intérieur du réseau mobile. Les nœuds sont connectés aux deux sous-réseaux et un protocole de Transport multi domicilié est alors conscient de la présence de deux chemins.

3.2 Composants du réseau

L'implémentation d'une telle architecture nécessite la présence de plusieurs composants et services.

Le routeur mobile doit implémenter ou supporter :

- NEMO ou un service équivalent permettant la mobilité du réseau ;
- La gestion de la mobilité avec plusieurs interfaces ;
- La définition de plusieurs préfixes IP permettant de définir les sous-réseaux ;
- « Flow Binding » pour améliorer les performances.

Le dernier service est optionnel mais peut améliorer l'efficacité en sélectionnant uniquement les flux devant changer de réseau d'accès.

Le nœud mobile doit implémenter :

- Mobile SCTP avec ses extensions permettant la mobilité ;
- La capacité de définir plusieurs adresses IP pour une seule interface.

Optionnellement, la présence de FastRA de réduire le temps de réaction lors d'échanges de messages entre un nœud et le routeur. Ces fonctionnalités étant déjà définies dans la littérature, la suite du papier suppose leur implémentation dans les nœuds du réseau.

3.3 Echanges entre Routeur Mobile et Nœuds

De nombreux évènements liés à la mobilité induisent des prises de décisions de la part du routeur mobile et les communications peuvent être impactées. Le tableau 2 liste plusieurs de ces évènements ainsi que les actions effectuées par le routeur en conséquence. La troisième colonne contient de nouvelles actions nécessaires à la mise en place de notre solution. Afin

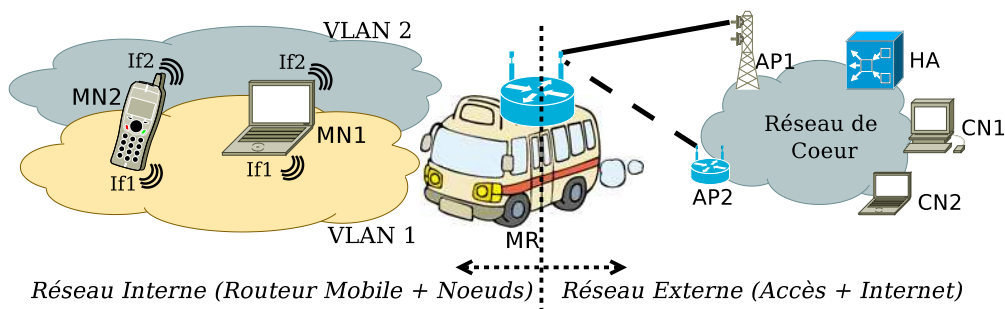


FIG. 2 – Un réseau mobile avec notre architecture : côté routeur un sous-réseau (VLANx) par interface externe et côté nœud une interface (Ifx) par sous-réseau.

de simplifier la lecture, nous définissons ici des abréviations présentes dans le tableau et qui seront utilisées par la suite :

- BU : Message « Binding Update » envoyé par le routeur mobile vers son agent mère pour la gestion de la mobilité (RFC6275, Perkins et al. (2011));
- Pref-IP : Préfixe IP communiqué par le routeur et utilisé par les noeuds pour configurer une adresse IP (RFC4861, Narten et al. (2007));
- Pour la gestion de l'association SCTP (RFC4960, Stewart (2007)) :
 - SCTP-ChangePrim : Envoi d'un chunk ASCONF requérant le changement du chemin primaire de l'association SCTP ;
 - SCTP-AddIP : Envoi d'un chunk ASCONF ajoutant une adresse IP à l'association SCTP ;
 - SCTP-RemIP : Envoi d'un chunk ASCONF supprimant une adresse IP à l'association SCTP ;

Des mécanismes non-présents dans le tableau peuvent aussi être envisagés afin d'améliorer les performances du système :

- Le changement de réseau est imminent : génération d'un RA avec le futur préfixe à utiliser et préparation des associations (RFC4861, Narten et al. (2007));
- Le chemin est stable : considérer l'utilisation de l'optimisation de route si possible.

Ces mécanismes sont intéressants mais leurs mises en place sont plus difficiles que les mécanismes présentés dans le tableau 2. Dans les deux cas il est nécessaire d'anticiper l'état des connexions dans un futur proche et une mauvaise anticipation revient à une perte de performances inutile.

Pour la mise en place de notre architecture, nous avons choisi d'utiliser les messages RA et RS introduits en 2.3. Ce choix est justifié par le fait que ces messages sont déjà utilisés par le routeur lors de la connexion d'un nouveau nœud mobile pour la transmission des préfixes IP du

Evènement	Mécanismes existants	Nouvelles Actions
Connexion MN-MR	Connexion niveau Liaison Transmission des préfixes IP	Signaler Pref-IP prioritaire Configuration interfaces
Nouveau AP Dispo	Connexion au point d'accès Envoi d'un BU	Signaler Nouveau Pref-IP SCTP-AddIP
Changement de Réseau en cours	Envoi d'un BU avec le chemin à utiliser	Signaler Pref-IP prioritaire SCTP-ChangePrim
Ancien AP indisponible	Envoi d'un BU sans l'ancien AP	Signaler Pref-IP inutile SCTP-RemIP
Aucun AP disponible	Mise en attente des données Interruption des connexions	Signaler Pref-IP inutiles Recherche autre réseau

TAB. 2 – Décisions et actions provoquées par la mobilité (Existantes et Nouvelles).

réseau mobile. Ces messages comportant de nombreuses options, il est possible de mettre en place notre architecture en respectant le standard c.-à-d. sans rajouter de nouvelles options et en utilisant les champs existants correctement. D'après le standard défini dans Narten et al. (2007), le champ d'option « Prefix Information » permet de transmettre les informations relatives aux sous-réseaux et contient :

- « Prefix Length » le nombre de bits valides dans le préfixe ;
- « Prefix » valeur de l'adresse IP ou du préfixe de l'adresse IP ;
- « Valid Lifetime » durée de validité du préfixe ;
- « Preferred Lifetime » durée pendant laquelle les adresses IP générées sont préférées.

Le dernier champ est intéressant pour notre architecture, il signifie que lors de la génération de plusieurs adresses IP, l'une d'entre elles est marquée comme adresse préférée et sera utilisée pour les communications. Dans notre architecture, cette option va être utilisée par le routeur pour forcer les nœuds à communiquer via l'adresse IP voulue. Lors de l'envoi d'un RA, le routeur mobile règle la durée de préférence du préfixe choisi à une valeur élevée et à une valeur plus faible pour les autres préfixes. Un changement de réseau entraîne alors la génération d'un RA avec de nouvelles durées de préférence.

Si une association SCTP est déjà établie lors de la réception d'un RA et que le nœud détecte un changement dans les durées de préférence, celui-ci doit demander à l'association en cours de changer de chemin prioritaire et d'utiliser le chemin correspondant à l'adresse avec la durée de préférence la plus élevée. Les nouvelles communications sont établies avec l'adresse IP

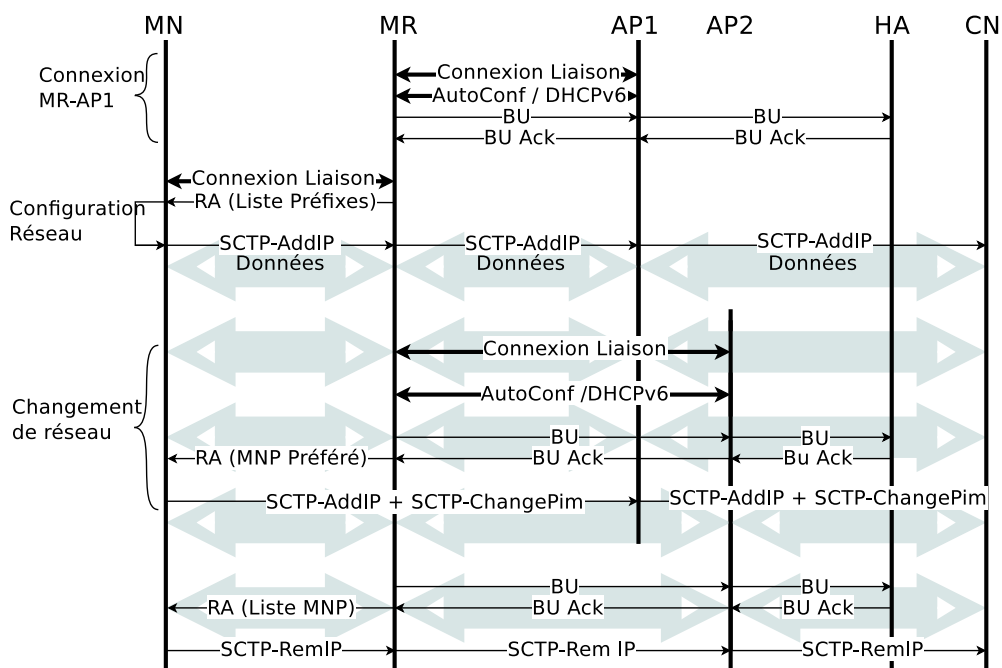


FIG. 3 – Messages échangés pendant plusieurs changements de réseau.

ayant la durée de préférence la plus élevée.

L'utilisation des messages RA et de la durée de préférence présente un autre avantage en plus d'être compatible avec les standards. Un nœud mobile connecté au routeur mobile mais qui souhaiterait utiliser l'une de ces interfaces pour communiquer directement avec un point d'accès peut le faire en configurant une adresse IP avec une durée de préférence plus élevée. Le gestionnaire de mobilité du nœud mobile peut alors choisir librement quelle interface utiliser.

La figure 3 est une représentation temporelle du fonctionnement de notre architecture reprenant les données du tableau 2. Il est clairement visible que chaque événement est suivi par une action et notamment le changement de réseau provoquant la modification du chemin primaire utilisé par SCTP. La section suivante détaille l'impact de notre architecture sur le comportement des protocoles de Transport.

4 Analyse

Comme expliqué en 2.2, la modification des conditions du réseau due aux changements de réseaux peut avoir un impact important sur les protocoles de la couche Transport. Notre architecture vise à diminuer cet impact en informant les protocoles de Transport qu'un changement de réseau est réalisé, leur permettant ainsi de réagir correctement aux différents événements qui suivent un changement de réseau. Dans cette section, nous allons analyser l'apport que peut avoir notre architecture en étudiant l'impact du changement de réseau sur une communication SCTP dans deux cas :

- Réseau Hybride : le changement de réseau est transparent pour les nœuds finaux ;
- Réseau Multi Domicilié : les nœuds réalisent le changement de réseau grâce à la multi domiciliation de SCTP.

Afin de réaliser cette étude, nous avons mis en place un banc de test permettant d'effectuer un changement de réseau entre deux technologies de communication : satellite et Wi-Fi. Les sous-sections suivantes présentent le banc de test ainsi que le scénario utilisé puis les résultats obtenus sont présentés et analysés.

4.1 Banc de test et scénario

Pour réaliser cette étude dans un cadre le plus proche possible de la réalité, il a été choisi de ne pas recourir à la simulation. En effet, la simulation ne permet pas de prendre en compte tous les paramètres et les implémentations des protocoles peuvent différer par rapport à un système d'exploitation réel, ce qui pourrait fausser les résultats obtenus. Nous avons donc utilisé un banc de test composé des éléments suivants :

- Deux ordinateurs portables sous Ubuntu 10.10 possédant chacun une interface Ethernet et une interface Wi-Fi ;
- Un émulateur de lien satellite SATEM capable de réaliser un changement de réseau transparent pour les nœuds finaux ;
- Un point d'accès Wi-Fi pour le réseau multi domicilié.

Les ordinateurs portables sont les hôtes de la communication SCTP. Ils utilisent pour cela la librairie `lk-sctp` présente par défaut dans Ubuntu et utilisé aussi par Fedora et Debian. La génération du trafic, la gestion des chemins (mSCTP) ainsi que l'observation des paramètres

de l'association (fenêtre de congestion, SRTT, RTO, ...) se fait grâce à une application que nous avons développée.

Dans le cas hybride, les liens satellite et Wi-Fi sont émulés par SATEM qui est capable d'effectuer un changement de réseau entre les deux. Dans le cas multi domicilié, le lien satellite est émulé par SATEM et la connexion Wi-Fi est obtenue grâce à un point d'accès réel. Le changement de réseau entre les deux est réalisé directement par notre application en utilisant les API de mobile SCTP.

Le scénario choisi pour réaliser cette étude correspond à un cas réel : celui d'un véhicule de transport en commun connecté à un réseau d'accès avec un grande couverture (satellite) et qui passe à portée d'un point d'accès de couverture moindre mais offrant de meilleures performances (Wi-Fi). Il est alors judicieux de communiquer au travers de la connexion la plus performante tant que celle-ci est à portée. La réalisation de ce scénario sur notre banc de test se déroule ainsi dans le cas hybride et dans le cas multi domicilié :

- 0s : Les deux hôtes initient la communication SCTP sur le lien satellite ;
- 20s : Un changement de réseau est réalisé entre satellite et Wi-Fi ;
- 40s : Un changement de réseau est réalisé entre Wi-Fi et satellite.

Ainsi, il est possible d'observer le changement de réseau dans les deux sens. Les caractéristiques suivantes ont été choisies pour la configuration des liens émulés :

- Lien satellite : délai de 250ms et bande-passante de 512 kbps ;
- Lien Wi-Fi : délai de 20ms et bande-passante de 10 Mbps ;

L'application générant un trafic avec un débit constant à 300 kbps, aucune congestion ne doit apparaître sur le lien Wi-Fi. Dans le cas multi-domicilié, le délai et la bande-passante sont similaires, garantissant des performances proches.

Ces expériences sont illustrées par les figures 4 et 5. La figure 4 présente l'évolution de la fenêtre de congestion pour un réseau hybride avec un changement de réseau transparent pour les nœuds finaux. La figure 5 présente l'évolution de la fenêtre de congestion sur le réseau multi domicilié avec mSCTP comme solution de mobilité. L'utilisation d'un jeu de valeurs différent est clairement visible suivant que le chemin primaire soit le satellite ou le Wi-Fi.

En observant l'évolution de la fenêtre de congestion, deux différences sont visibles entre ces deux figures : les valeurs optimales sur le lien Wi-Fi et les comportements après le second changement de réseau. Les origines et les impacts de ces différences sont discutés dans les sous-sections suivantes.

4.2 Comportement de la fenêtre de congestion

En premier lieu, il est important de noter que le comportement des deux fenêtres est similaire avant le premier changement de réseau, c.-à-d. avant 20s. Pour effectuer le changement de réseau, l'association SCTP en multi domicilié change de chemin primaire et utilise donc une nouvelle fenêtre de congestion qui se stabilise autour de 26000 octets. Sur le réseau hybride, le premier changement de réseau est suivi immédiatement par une diminution de moitié de la fenêtre de congestion puis une légère augmentation jusqu'à 30000 octets.

Cette chute est due à la réception de données non-ordonnées lors du changement de réseau entre satellite et Wi-Fi. Le délai sur le lien satellite étant élevé, les données envoyées sur le lien Wi-Fi arrivent plus vite à destination et les acquittements signalent les données encore en vol comme des trous dans la communication. Si les mêmes données sont signalées manquantes 3 fois, l'algorithme Fast Retransmit est utilisé par l'émetteur : la fenêtre de congestion

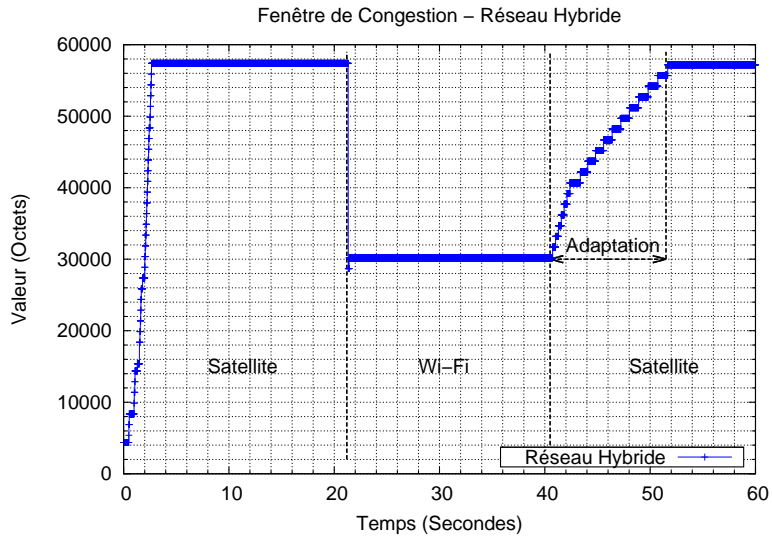


FIG. 4 – Comportement de la fenêtre de congestion lors de changements de réseau entre satellite et Wi-Fi sur un réseau hybride.

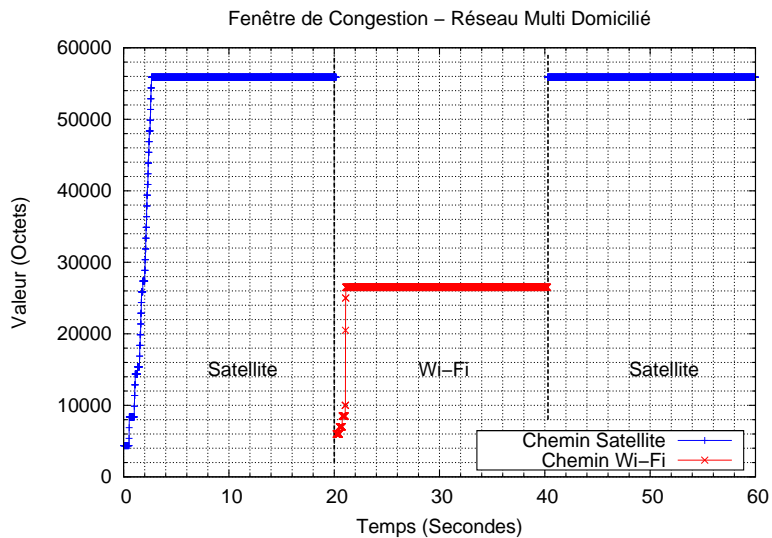


FIG. 5 – Comportement de la fenêtre de congestion lors de changements de réseau entre satellite et Wi-Fi sur un réseau multi-domicilié.

est diminuée de moitié et les données signalées sont retransmises. En quittant l'état Fast Retransmit, la fenêtre de congestion est en « congestion avoidance » et se stabilise quand elle est suffisamment grande pour envoyer toute la quantité de données générées par l'application.

Après le changement de réseau entre Wi-Fi et satellite à environ 40 s, le délai grandit et la fenêtre de congestion doit s'adapter. Dans le cas hybride, l'utilisation de l'algorithme « congestion avoidance » sur un lien satellite conduit à une période d'adaptation de plusieurs secondes. Dans le cas multi domicilié, les paramètres utilisés précédemment sur le lien satellite sont repris et la fenêtre de congestion repart donc avec sa valeur optimale.

L'adaptation sur un réseau hybride est conduite en erreur par des mécanismes internes aux protocoles de Transport comme les algorithmes « Fast Retransmit/Fast Recovery » ou « congestion avoidance ». Dans le contexte multi domicilié, l'adaptation se fait naturellement, des paramètres indépendants étant utilisés. L'impact sur les communications est détaillé dans la section suivante.

4.3 Impact sur les Communications

L'algorithme Fast Retransmit est utilisé par l'émetteur si des données sont reçues dans le désordre. Dans un environnement sans perte, il fonctionne correctement et dans notre expérience, il permet de s'adapter rapidement aux caractéristiques du nouveau réseau. Néanmoins, son utilisation peut avoir un impact négatif sur les communications : la perte d'un paquet retransmis pendant l'utilisation de l'algorithme force la fenêtre de congestion à sa plus faible valeur (=1 paquet) et le passage en « congestion avoidance » ralentit les estimations faites par la suite.

Perte d'un paquet retransmis avec Fast Retransmit. Dans l'expérience illustrée par la Figure 4, 50 kilo-octets de données sont en vol lorsque le premier changement de réseau est effectué. Retransmettre ces données prend 110 ms sur un lien Wi-Fi émulé ayant une bande passante raisonnable (soit supérieure à 4 Mbps). Dans un contexte réel, le début de la communication sur le lien Wi-Fi correspond à l'arrivée à portée sur point d'accès. Le nœud est donc à la limite de la zone de couverture et la probabilité de perdre un paquet est donc plus forte qu'à proximité du point d'accès. Si un paquet retransmis est perdu, la fenêtre de congestion est forcée à 1 MTU (« Maximum Transmission Unit ») et utilise l'algorithme « congestion avoidance » pour grandir.

Le Tableau 3 est un calcul théorique de la fenêtre de congestion après la perte d'un paquet dans l'état Fast Retransmit. Ce tableau comporte aussi les données acquittées et les données envoyées à chaque RTT ainsi que la quantité totale de données envoyées. La fenêtre de congestion commence à 1500 octets (1 MTU) et 240 ms sont nécessaires pour envoyer 44 kilo-octets de données. Comparées au 110 ms nécessaires à l'envoi de ces données avec une fenêtre de congestion optimale, le temps de transmission est doublé.

Adaptation en « Congestion Avoidance » sur un réseau satellite. Après l'utilisation du Fast-Retransmit, l'algorithme « congestion avoidance » est utilisé pour agrandir la fenêtre de congestion et il est toujours utilisé lors du second changement de réseau entre satellite et Wi-Fi. À ce moment-là les caractéristiques du réseau changent brutalement : le débit disponible est fortement réduit et le délai est décuplé. La fenêtre de congestion s'adapte à cette situation

en augmentant afin d’atteindre sa valeur optimale. L’algorithme « congestion avoidance » étant prévu pour éviter la congestion, l’adaptation de la fenêtre de congestion se fait lentement. Le temps nécessaire à cette adaptation dépend du délai du réseau et de la différence entre fenêtre initiale et fenêtre optimale ; respectivement 30 kilo-octets et 57 kilo-octets dans la figure 4. En théorie, la fenêtre peut augmenter de 1 MTU à chaque RTT, la durée de cette phase peut donc être exprimée ainsi :

$$T = \Delta_{Donnees} * \frac{RTT}{MTU} \tag{1}$$

En prenant un RTT de 500ms pour le lien satellite et un MTU de 1500octets, au moins 9 secondes sont nécessaires pour atteindre la valeur optimale. Sur le réseau satellite émulé dans notre expérience, entre 11 et 12 secondes sont nécessaires pour réaliser cette adaptation.

Durant cette phase d’adaptation, la valeur de la fenêtre de congestion étant inférieure à sa valeur optimale, la quantité maximale de données en vol est inférieure à la quantité optimale et le débit peut donc être inférieur à la bande-passante disponible. Dans notre expérience, l’impact sur les communications est amoindri par la faible bande passante disponible (64kilo-octets). La bande-passante disponible est alors entièrement utilisée et l’accroissement de la fenêtre de congestion est uniquement du au délai très grand du réseau satellite. Si des pertes apparaissent au cours de cette phase d’adaptation, l’impact sur les communication est plus important : la valeur de la fenêtre de congestion est alors divisée par deux et il sera plus difficile d’atteindre le débit optimal.

La figure 6 présente la quantité de données reçues au cours de la communication sur le réseau hybride. La courbe encadrée focalise sur la quantité de données reçue juste après le second changement de réseau. Il est clairement visible que les paquets sont reçus en rafales après 40 s et ce pendant environ 2s. Suivant le type d’application, ce comportement peut être perturbant, puisque les paquets ne sont plus reçus régulièrement et obligent l’application à attendre avant de lire plusieurs paquets à la fois.

Temps écoulé (s)	Fenêtre de Congestion	Données acquittées	Données envoyées	Données totales
0.00	1500	0	1000	0
0.04	2500	1000	2000	1000
0.08	4000	2000	4000	3000
0.12	7000	4000	7000	7000
0.16	11500	7000	11000	14000
0.20	19000	11000	19000	25000
0.24	32500	19000	32000	44000

TAB. 3 – Evolution de la fenêtre de congestion théorique après des pertes en Fast Retransmit (fenêtre et quantité de données en octets).

Wi-Fi

Satellite

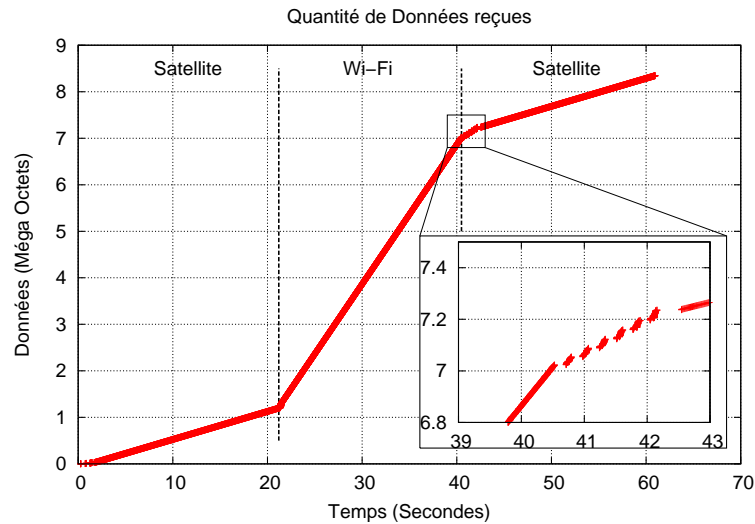


FIG. 6 – Evolution de la quantité de données reçues lors du changement de Wi-Fi à satellite sur un réseau hybride.

4.4 Impact sur l'évaluation de l'état du réseau

Le « Smoothed Round Trip Time » (SRTT) ou temps aller-retour lissé est une des variables utilisée par l'émetteur pour évaluer l'état du réseau. Plus précisément, le SRTT permet d'évaluer le temps d'un trajet aller-retour entre deux hôtes. En utilisant le SRTT et la variation du dernier temps aller-retour mesurée, l'émetteur calcule la valeur du temporisateur de retransmission « Retransmission Time Out » (RTO). Lors de l'envoi d'un paquet, ce temporisateur est lancé et s'il arrive à 0 avant que le paquet ne soit acquitté, alors celui-ci est considéré comme perdu et doit être retransmis. Ces deux paramètres ont une influence très importante sur les communications :

- Si le RTO est trop faible : des paquets peuvent être retransmis inutilement ;
- Si le RTO est trop élevé : les pertes ne sont pas détectées assez vite ;

Les figures 7 et 8 présentent respectivement le SRTT et le RTO pour les expériences décrites précédemment. Comme pour l'évolution de la fenêtre de congestion, l'évolution du SRTT avant le premier changement de réseau est similaire pour le réseau hybride et pour le réseau multi domicilié. Il en est de même pour le RTO.

À 20s le changement de réseau entre satellite et Wi-Fi est réalisé. Sur le réseau multi domicilié, il est clairement visible que le SRTT et le RTO repartent avec leur valeurs initiales car un nouveau jeu de paramètres est utilisé pour ce chemin. Sur le réseau hybride, l'adaptation se fait rapidement grâce au faible délai aller-retour sur le lien Wi-Fi. Seulement quelques secondes sont nécessaires pour avoir des valeurs proches entre réseau hybride et réseau multi domicilié.

Après le second changement de réseau (40 s), les comportements diffèrent : sur le réseau multi domicilié, les anciennes valeurs sont reprises tandis que sur le réseau hybride l'adaptation

Architecture Multi Domiciliée dans les Réseaux Mobiles

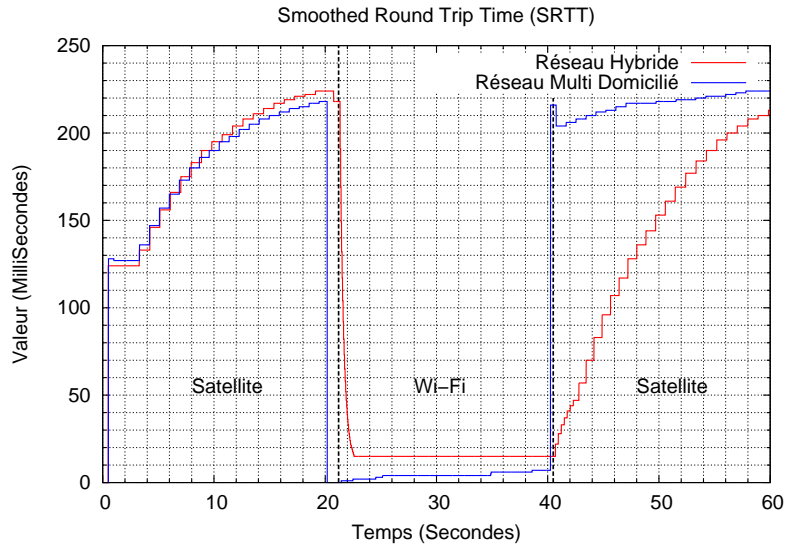


FIG. 7 – Variation du SRTT lors de changements de réseau entre satellite et Wi-Fi.

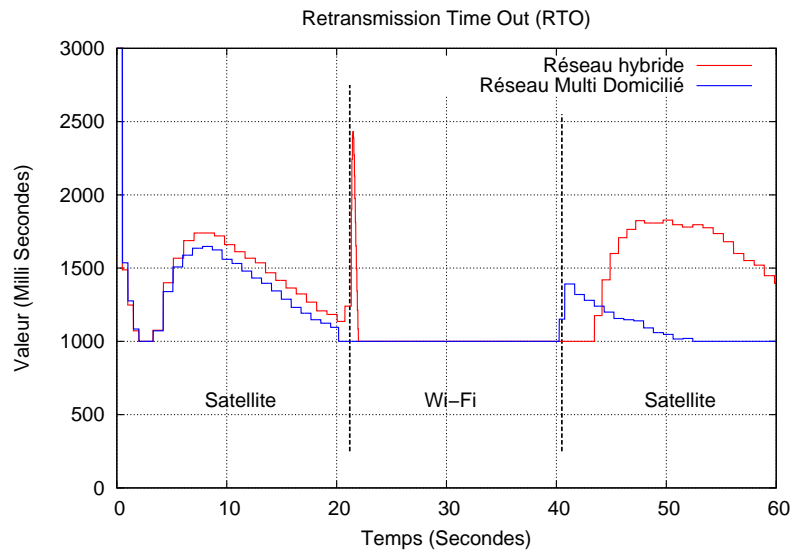


FIG. 8 – Evolution du RTO lors de changement de réseau entre satellite et Wi-Fi.

se fait plus lentement. Le délai aller-retour sur le lien satellite étant conséquent (supérieur à 500 ms), 20 secondes sont nécessaires pour que le SRTT atteigne la valeur atteinte avant le premier changement de réseau. Dans le même temps, le RTO sur le réseau hybride augmente jusqu'à dépasser 1.5 s puis diminue à partir de 50 s.

Un point intéressant est relevé par ces mesures : sur le réseau hybride, l'adaptation du SRTT au lien satellite est faite 2 fois, après l'initiation et après le second changement de réseau (retour sur le lien satellite). À l'opposé, l'adaptation du SRTT sur le réseau multi domicilié ne se fait qu'une fois par technologie de communication : lors du retour sur le lien satellite l'ancienne valeur est reprise. Dans cette expérience, le temps passé à s'adapter au réseau est donc 2 fois plus important dans le cas du réseau hybride.

4.5 Bilan

L'utilisation de la multi domiciliation permet aux associations SCTP d'utiliser des fenêtres de congestion indépendantes pour chaque chemin. En arrivant sur un nouveau réseau, l'utilisation de valeurs initiales permet de s'adapter correctement. En revenant sur un réseau connu, l'utilisation des anciennes valeurs permet d'atteindre immédiatement les performances optimales. Néanmoins, des dégradations peuvent intervenir si les conditions du réseau ont changées : apparition de congestion ou diminution de la bande passante causée par une allocation dynamique. L'analyse de cette expérience montre que l'utilisation de la multi domiciliation permet d'améliorer la précision des évaluations faites par les protocoles de Transport après un changement de réseau.

5 Conclusion

L'architecture introduite dans ce papier se base sur la fonctionnalité de multi-domiciliation de SCTP et sur des mécanismes de mIPv6. Les protocoles de Transport n'étant pas adaptés aux réseaux mobiles avec changement de réseau transparent, cette architecture vise à améliorer leurs performances en augmentant le partage d'informations entre le routeur mobile et les nœuds qui y sont connectés.

Nous avons démontré que les erreurs des protocoles de Transport après un changement de réseau sont dues à une mauvaise interprétation des caractéristiques du réseau. À l'opposé, l'utilisation de protocole de Transport permettant la multi domiciliation avec notre solution résulte dans une meilleure interprétation des événements liés au changement de réseau et dans des prises de décisions plus adaptées à la situation.

Un aspect important lors de la conception d'une architecture est sa facilité de déploiement et sa compatibilité avec les systèmes déjà déployés. Notre architecture se basant sur des mécanismes définis dans les standards de mIPv6 et IPv6, son déploiement est facilité car les hôtes IPv6 possède les mécanismes nécessaires. Les modifications nécessaires à sa mise en place se situent uniquement dans le réseau mobile, il n'y a pas besoin de composants externes. De plus si l'utilisation d'un protocole de Transport multi domicilié est nécessaire pour profiter des apports de l'architecture, les nœuds utilisant un protocole de Transport mono domicilié peuvent établir la communication et auront des performances similaires à celles disponibles sur un réseau hybride.

Références

- Daley, G., B. Pentland, et R. Nelson (2003). Effects of Fast Router Advertisement on Mobile IPv6 Handovers. In *Proceedings. Eighth IEEE International Symposium on Computers and Communication, 2003. (ISCC 2003)*.
- Devarapalli, V., R. Wakikawa, A. Petrescu, et P. Thubert (2005). RFC3963 : Network Mobility (NEMO) Basic Support Protocol. Rfc, Internet Engineering Task Force.
- Ford, A., C. Raiciu, M. Handley, S. Barre, et J. Iyengar (2011). RFC6182 : Architectural Guidelines for Multipath TCP Development. Rfc.
- Ford, B. et J. Iyengar (2008). Breaking Up the Transport Logjam. In *Hot Topics in Networks, HOTNETS*.
- Hansmann, W. et M. Frank (2003). On things to happen during a TCP handover. In *28th Annual IEEE International Conference on Local Computer Networks, 2003. LCN '03. Proceedings.*, pp. 109–118. Ieee.
- Narten, T., E. Nordmark, W. Simpson, et H. Soliman (2007). RFC4861 : Neighbor Discovery for IP version 6 (IPv6). Rfc, Internet Engineering Task Force.
- Ng, C., T. Ernst, E. Paik, et M. Bagnulo (2007). RFC4980 - Analysis Of Multihoming in Network Mobility Support. Rfc, Internet Engineering Task Force.
- Perkins, C., D. Johnson, et J. Arkko (2011). RFC6275 : Mobility Support in IPv6. Rfc, Internet Engineering Task Force.
- Raiciu, C., M. Handly, et D. Wischik (2011). RFC6356 : Coupled Congestion Control for Multipath Transport Protocols. Rfc, Internet Engineering Task Force.
- Stewart, R. (2007). RFC4960 : Stream Control Transmission Protocol. Rfc, Internet Engineering Task Force.
- Stewart, R., Q. Xie, M. Tuexen, S. Maruyama, et M. Kozuka (2007). RFC5061 : Stream Control Transmission Protocol (SCTP) Dynamic Address Reconfiguration. Rfc, Internet Engineering Task Force.
- Sun, Y., Y. Cui, W. Wang, T. Ma, Y. Ismailov, et X. Zheng (2011). Mobility support in Multipath TCP. In *2011 IEEE 3rd International Conference on Communication Software and Networks*, pp. 195–199. Ieee.
- Tsirtsis, G., H. Soliman, N. Montavont, G. Giaretta, et K. Kuladinithi (2011). RFC6089 : Flow Bindings in Mobile IPv6 and Network Mobility Basic Support. Rfc, Internet Engineering Task Force.
- Tuexen, M., R. Stewart, P. Lei, et E. Rescorla (2007). RFC4895 : Authenticated Chunks for the Stream Control Transmission Protocol (SCTP). Rfc, Internet Engineering Task Force.
- Wakikawa, R., V. Devarapalli, G. Tsirtsis, T. Ernst, et K. Nagami (2009). RFC5648 : Multiple Care-of Addresses Registration. Rfc, Internet Engineering Task Force.

Summary

Mobile Routers provide all mobile nodes connected to them with a reliable connection and transparent mobility. Transport protocols can be impacted by such transparency since network state is changing without warning, affecting their evaluation of network conditions. Our architecture suggests to inform Transport protocols when a handover is made so impact on communications can be lowered. This solution is based on defining several network interfaces in mobile nodes and on using SCTP multi homing capabilities.

