THÈSE

En vue de l'obtention du

DOCTORAT DE L'UNIVERSITÉ DE TOULOUSE

Délivré par :

Université Toulouse 3 Paul Sabatier (UT3 Paul Sabatier)

Présentée et soutenue par :
Lionel Bertaux

le jeudi 26 septembre 2013

Titre :

Architecture Réseau pour Véhicule de Transport en Commun Communiquant

---

École doctorale et discipline ou spécialité :
EDSYS : Informatique 4200018

Unité de recherche :
LAAS-CNRS

Directeur(s) de Thèse :

Thierry Gayraud
Pascal Berthou

Jury :
Toufik Ahmed, Rapporteur
Francis Lepage, Rapporteur
Michel Diaz
Olivier Alphand
Khaled Boussetta

Remerciements

Je remercie sincèrement mes rapporteurs, Monsieur Toufik Ahmed, Professeur au LaBRI et Monsieur Francis Lepage, Professeur au CRAN pour leur travail de relecture et les remarques qui en ont découlé. Merci à Messieurs Olivier Alphand et Khaled Boussetta, respectivement Maître de Conférences à l'INP Grenoble et Maître de Conférences à Paris XIII, pour avoir accepté de participer à mon jury de thèse ainsi que pour leurs remarques pertinentes. Enfin, je remercie chaleureusement Michel Diaz, Directeur de Rechercher au LAAS-CNRS, pour avoir présidé mon jury de thèse ainsi que pour son analyse critique et son expérience. A l'ensemble du jury, je tiens à dire merci pour le temps qu'ils ont su consacrer à l'étude de mes travaux et pour les discussions que nous avons ainsi pu avoir lors de la soutenance.

Les recherches effectuées dans de cette thèse n'auraient pu voir le jour sans Monsieur Thierry Gayraud, Professeur au LAAS-CNRS, et Monsieur Pascal Berthou, Maître de Conférences au LAAS-CNRS. Je les remercie pour avoir respectivement dirigé et co-encadré ma thèse ainsi que pour les différents échanges que nous avons eus. Leurs conseils ainsi que leur vision critique m'ont permis de réaliser les travaux présents dans cette thèse, durant laquelle j'ai eu l'opportunité de participer à deux projets en collaboration avec des entreprises. J'en profite pour saluer les personnes rencontrées dans le cadre de ces projets. Merci Thierry et Pascal pour la confiance que vous m'avez accordée.

J'adresse mes remerciements à Messieurs François Vernadat et Khalil Drira, qui m'ont accueilli dans leurs entités de recherche, respectivement le groupe de recherche OLC et l'équipe de recherche SARA au sein du LAAS-CNRS. Je remercie de même Monsieur Raja Chatilla, feu Monsieur Jean-Louis Sanchez et Monsieur Jean Arlat, directeurs du LAAS-CNRS pendant ma thèse pour m'avoir accueilli au sein de leur laboratoire et d'avoir ainsi permis la réalisation de cette thèse.

Merci à tous les membres de l'équipe SARA pour leur soutien ainsi que leurs remarques. Ils ont ainsi pu m'apporter une vision externe indispensable à la réalisation d'une thèse. Je salue plus particulièrement Yann, Philippe et Carolina.

Je remercie également l'ensemble du département EEA de l'Université Paul Sabatier. Plus particulièrement, je remercie Monsieur Jean-Claude Pascal pour m'avoir permis d'enseigner dans son département ainsi que les enseignants avec qui j'ai enseigné. Ils ont su me faire partager leur expérience de même que leur passion pour l'enseignement.

Je tiens à saluer les doctorants que j'ai côtoyés au cours de cette thèse, que ce soit lors de matchs de basket, des réunions plénières du vendredi ou tout simplement autour d'un café, vous avez su me soutenir et me conseiller. Pour cela, je vous remercie amicalement et vous souhaite bon courage pour la suite.

Merci aussi aux personnes qui étaient présentes en dehors du laboratoire notamment mon binôme, mes amis d'enfance, ma famille et ma belle-famille pour leur soutien et leur amitié.

Enfin, je remercie ma compagne Laurence pour son amour et le soutien qu'elle m'a apporté tout au long de cette thèse. A elle, ainsi qu'à notre enfant Adrien, je dédie ce travail.

Table des matières

Acronymes

Acronyme	Signification
AP	Access Point
API	Application Programming Interface
BA	Binding Acknowledgement
BBM	Break Before Make
BDP	Bandwidth Delay Product
BU	Binding Update
CBR	Constant Bit Rate
CN	Corresponding Node
CoA	Care-of-Address
CRA	Constant Rate Assignment
DAMA	Demand Assign Multiple Access
DHCP	Dynamic Host Configuration Protocol
DTN	Delay-Tolerant Network ou Disruption-Tolerant Networking
FA	Foreign Agent
FDMA	Frequency Division Multiple Access
FMIPv6	Fast Handover mobile IPv6
FTP	File Tranfer Protocol
GPS	Global Positioning System
GRPS	General Packet Radio Service
GW	GateWay
HA	Home Agent
HMIPv6	Hierarchical mobile IPv6
HO	Handover
HTTP	HyperText Transfer Protocol
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
LFN	Local Fixed Node
LMN	Local Mobile Node
MBB	Make Before Break
mCoA	Multiple Care-of-Address
MF-TDMA	Multiple Frequency Time Division Multiple Access
MIPv6	mobile IPv6
MN	Mobile Node
MNP	Mobile Network Prefix
MPTCP	Multipath TCP
MR	Mobile Router
NAR	New Access Router
NBMA	Non-Broadcast Multicast-Access
NCC	Network Control Center
NEMO	Network Mobility
PAR	Previous Access Router
PI	Prefix Information
QdS / QoS	Qualité de Service / Quality of Service
RA	Router Advertisement
RBDC	Rate-Based Dynamic Assignment
RFC	Request For Comment
RS	Router Solicitation
SCTP	Stream Control Transmission Protocol
TCP	Transmission Control Protocol

TDMA	Time Division Multiplie Access
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
VoIP	Voice over IP
Wi-Fi	Wireless Fidelity

Liste des figures

Liste des tableaux

Résumé du manuscrit

Les appareils mobiles de type tablettes, téléphones intelligents ou ordinateurs portables sont aujourd'hui omniprésents. Leur principale utilisation étant la consultation de contenu sur Internet ou la connexion à des réseaux sociaux, les utilisateurs sont de plus en plus demandeurs d'accès mobile (par la 3G par exemple). A bord des véhicules de transport en commun, cet accès peut être plus difficile à obtenir : absence de réseau entre deux villes, faible performance lors d'un déplacement à grande vitesse, présence d'obstacles… Afin de pallier à ces inconvénients, il est envisageable que les véhicules de transport en commun offrent une connexion à leurs passagers avec de meilleures performances qu'un appareil mobile ou avec d'autres moyens de communication. Des équipements plus performants et de plus grande taille pouvant être embarqués et partagés.

Le véhicule de transport en commun agit alors comme un routeur mobile possédant plusieurs interfaces réseaux : certaines dites « de sortie » permettant de se connecter aux points d'accès extérieurs et certaines dites « internes » servant de points d'accès aux utilisateurs. L'autonomie énergétique de ces véhicules ainsi que l'espace disponible permet d'envisager l'utilisation d'autres technologies de communication (Wi-Fi, 3G, satellite…) en plusieurs exemplaires ou avec des antennes plus performantes (plus grande taille, multidirectionnelles…). Afin de tirer profit de chaque connexion disponible, la solution de mobilité implantée dans le routeur doit être capable d'utiliser en permanence le réseau offrant les meilleures performances et doit pour cela effectuer régulièrement des changements de point d'accès. Lors du basculement d'un point d'accès vers un autre, les phénomènes suivants peuvent apparaitre:

- Changement de l'adresse IP du routeur,
- Introduction de latences dues aux configurations au niveau Liaison et au niveau Réseau,
- Modification des caractéristiques du réseau (bande passante, délai, congestion…),
- Réception désordonnée de paquets,

La couche Transport étant chargée de transmettre les données, ses performances sont fortement impactées par les phénomènes sus-cités. Le changement d'adresse IP peut entraîner directement la rupture de communications puisqu'un protocole de Transport comme TCP utilise l'adresse IP pour identifier la connexion. Un gestionnaire de mobilité est alors nécessaire pour passer outre cette modification par la mise en place d'un tunnel par exemple. Mobile IPv6 permet de ne pas rompre la connexion. L'introduction de latences ralentit la communication : le protocole de Transport détectant que le lien est inactif, il arrête d'émettre de nouvelles données. Si cette inactivité persiste, elle peut même conduire à la rupture de la connexion. Des extensions à MIPv6 permettent de réduire cette latence (HMIPv6, FMIPv6).

La modification des caractéristiques du réseau et la réception désordonnée de paquets vont avoir un impact différent sur les communications. La plupart des protocoles de Transport ayant été développé pour des réseaux filaires, ils sont incapables de s'adapter rapidement aux caractéristiques d'un nouveau réseau et interprètent ces phénomènes avec des mécanismes conçus pour des liens fixes, ce qui peut les induire en erreur. De plus, l'utilisation d'un gestionnaire de mobilité rend le changement de réseau transparent, ni les terminaux ni les protocoles de Transport ne peuvent alors être informés des phénomènes qui vont se produire. Il s'en suit alors souvent une dégradation des performances pouvant conduire à une perte de connectivité.

Au cours de cette thèse, différents phénomènes pouvant impacter les performances des applications dans un tel contexte ont été étudiés et nous avons proposé des solutions permettant de réduire l'impact de la mobilité et du changement de réseau.

La première contribution décrite dans ce manuscrit porte sur le protocole de Transport SCTP qui est comparé au protocole de Transport de référence : TCP. L'objectif était de déterminer si les performances de SCTP lui permettaient de rivaliser avec TCP sur un réseau contraignant tel qu'un réseau de communication par satellite comportant un mécanisme d'allocation de ressources (i.-e. d'attribution de bande passante) et une architecture avec Qualité de Service (QdS). Ce type de réseau est très contraignant pour les protocoles de Transport car la bande passante disponible change régulièrement et l'apparition de flux prioritaires va congestionner le réseau. Pour réaliser cette étude, nous avons utilisé le simulateur d'évènements orienté réseau Network Simulator 2 et un modèle de réseau de communication par satellite permettant l'allocation dynamique de la bande passante auquel nous avons ajouté l'architecture QdS et les mécanismes d'encapsulation.

Nous avons pu constater que SCTP était aussi efficace que TCP sur ce type de réseau et qu'il était « TCP-friendly » ; introduit avec l'omniprésence de TCP, ce concept signifie que le protocole n'est pas plus agressif que ne le serait une connexion TCP. Le comportement des deux protocoles en présence de congestion est similaire : ceci s'explique par l'utilisation de mécanismes de contrôle de congestion proches l'un de l'autre (fenêtre de congestion). Notamment, plusieurs secondes sont nécessaires pour atteindre le débit maximal (particulièrement s'il est élevé) car la fenêtre de congestion nécessite plusieurs RTT avant d'atteindre sa valeur optimale. Cette comparaison se faisant uniquement sur la capacité du protocole à transmettre des données, la multi-domiciliation n'a pas été utilisée. SCTP serait donc potentiellement plus efficace si celle-ci était activée, TCP ne permettant pas de communiquer sur plusieurs interfaces simultanément.

Dans un contexte mobile, plusieurs points d'accès sont souvent disponibles et les technologies de communication utilisées peuvent être hétérogènes. Des changements de réseau sont alors nécessaires impactant les communications. Le projet SAT-PERF visait à étudier les performances des protocoles de Transport dans un tel contexte. Nous alors choisi d'étudier le comportement de SCTP en présence de changements de réseau entre satellite et Wi-Fi et l'avons pour cela évalué à l'aide d'un émulateur de lien satellite. Deux cas d'études ont été choisis : un réseau hybride où le changement de réseau est transparent pour nœuds hôtes de la communication et un réseau multi-domicilié où le nœud hôte connait les différents chemins disponibles. Dans les deux cas, nous émulons la découverte de points d'accès Wi-Fi par un nœud circulant dans la zone de couverture d'un réseau satellite. Lorsque ces réseaux Wi-Fi sont détectés, un changement de réseau est effectué afin de profiter de leurs meilleures performances tant en terme de débit que de délai. Dans le premier cas, nous avons pu déterminer que SCTP est aussi efficace que TCP Compound ; la meilleure version de TCP ; leur adaptation étant suffisamment rapide pour les performances de l'application ne soient pas trop dégradées. Pour l'étude du deuxième cas, nous avons utilisé un point d'accès Wi-Fi réel en plus de l'émulateur afin d'évaluer les performances de SCTP en multi-domiciliation. Les résultats obtenus montrent un bien meilleur comportement comparé au cas hybride. Le design de SCTP lui permet d'évaluer rapidement le nouveau réseau en utilisant les valeurs initiales pour la fenêtre de congestion, le SRTT, le RTO… Les évaluations faites par SCTP ne sont donc pas faussées par un historique et les performances sont identiques à l'initiation d'une connexion.

En se basant sur l'étude de SCTP dans un contexte multi-domicilié, notre contribution vise à appréhender le changement de réseau à l'aide de la géo-localisation. Dans le contexte des transports en commun, la présence de GPS sur le véhicule et le parcours de trajets prédéfinis permettent de savoir quels réseaux seront présents à quels instants. Il suffit pour cela de posséder une carte de couverture de

ces réseaux. Il devient alors possible de prévoir les zones d'ombre de la 3G ou du satellite ainsi que l'apparition d'un réseau Wi-Fi. En appréhendant la présence d'un réseau Wi-Fi, il devient possible de configurer une interface réseau et de communiquer la nouvelle adresse IP au nœud distant avant que le réseau ne soit détecté. La seule contrainte est la possession d'une adresse IP fixe dans les réseaux traversés. Un tel mécanisme permet de diminuer le temps écoulé entre la détection d'un réseau et l'envoi de données sur celui–ci. Notre contribution permet de diminuer ce temps de 1 seconde en moyenne (1,8s au lieu de 2,8s). En considérant une zone de couverture Wi-Fi d'une cinquantaine de mètres et un véhicule allant à 50km/h, la durée de la connexion au réseau Wi-Fi est augmentée de plus de 10%. De plus, la connaissance des réseaux traversés permet d'estimer la durée avant la connexion à un réseau Wi-Fi. Il devient alors possible de choisir entre transmettre des données non-critiques sur un réseau 3G ou attendre la connexion à un réseau Wi-Fi et ainsi conserver de la bande passante pour les applications critiques.

Les études précédentes permettent de montrer que SCTP est un protocole de Transport capable de rivaliser avec TCP en termes de performances et que la multi-domiciliation lui permet de supporter le changement de réseau idéalement. Néanmoins, un changement de réseau réalisé par un routeur embarqué dans le bus va être transparent pour les nœuds mobiles et il n'est pas possible de tirer partie de la multi-domiciliation offerte par le protocole de Transport.

La dernière contribution est une architecture qui vise à limiter l'impact du changement de réseau transparent pour un nœud connecté à un routeur mobile. Le principe de base pour atteindre cet objectif est le partage d'informations détenues par le routeur avec les nœuds qui lui sont connectés, par exemple pour prévenir les protocoles de Transport présents dans les terminaux des utilisateurs lorsqu'un changement de réseau est réalisé. En utilisant un protocole de Transport adapté, celui-ci peut alors interpréter correctement les évènements suivant un changement de réseau et ne pas subir de pertes de performances. Pour la mise en place de cette architecture, nous proposons d'étendre la multi-domiciliation du routeur vers les nœuds mobiles en se basant sur deux principes : (i) le routeur mobile définit un sous-réseau par interface sortante (du routeur vers les points d'accès) et (ii) les nœuds mobiles se connectent à chaque sous-réseau avec une adresse IP différente. Un sous-réseau est désigné par le routeur comme préférentiel et les nœuds doivent communiquer sur celui-ci. Le protocole de Transport présent dans le nœud final est alors connecté de manière multi-domiciliée. Lorsqu'un changement de réseau intervient au niveau du routeur mobile, celui-ci demande aux nœuds mobiles de changer de sous-réseau, déclenchant alors des mécanismes de changement de réseau propres aux protocoles de Transport multi-domiciliés. L'impact du changement de réseau peut ainsi être diminué, ces mécanismes permettant une meilleure évaluation du nouveau réseau et étant plus robustes à la réception de données non ordonnées.

Les études et expériences faites au cours de cette thèse permettent de mieux cerner certaines problématiques relatives à la mobilité. L'étude approfondie du changement de réseau a permis une meilleure compréhension de cet événement et comment il peut influencer les performances des protocoles de Transport. Nos contributions visent à réduire l'impact du changement de réseau avec deux approches différentes : en diminuant la latence introduite par le changement de réseau et en limitant l'impact du changement des caractéristiques du réseau.

Chapitre I Les Transports en Commun comme Points d'accès

La gestion des réseaux mobiles est un sujet vaste qui reprend les problématiques de base de la mobilité : garantir une connexion stable et performante, effectuer des changements de réseau sans coupure et sans latence, localiser le nœud… L'ajout de contraintes comme le nombre de nœuds dans le réseau ou la prise en compte de l'impact des changements de réseau transparents rend plus complexe encore la gestion et l'optimisation des réseaux mobiles. Dans cette thèse, nous avons essayé d'avoir une vision globale de la problématique pour aborder le contexte des réseaux mobiles. Pour cela, nous avons étudié l'influence de la mobilité sur les différentes couches protocolaires puis nous nous sommes focalisés sur la couche Transport. Celle-ci étant en charge de la transmission des données, elle est directement responsable des performances des applications, même si elle est impactée par le comportement des couches inférieures.

Cette section introduit la problématique de la thèse en décrivant le contexte et les caractéristiques des transports en commun. Un exemple d'utilisation des transports en commun est donné avec les projets AMIC-TCP et DIESEL net qui visent à offrir un accès aux passagers, le premier avec une connexion permanente et le second avec un réseau tolérant au délai ou « Delay Tolerant Network » (DTN). Les descriptions données dans ce chapitre sont voulues de « haut niveau » et ne rentrent pas dans les détails techniques, ceci étant fait dans l'état de l'art.

I Introduction

L'évolution des technologies de communication et la démocratisation des « nouvelles technologies » ont permis aux appareils mobiles de faire partie de notre vie quotidienne. Depuis plusieurs années, le nombre de téléphones intelligents, tablettes et ordinateurs portables croit exponentiellement. Pour les particuliers, les ventes d'ordinateurs portables étaient déjà devant les ventes d'ordinateurs de bureaux avant 2011. Mais en 2011, l'explosion des tablettes conjuguée au recul des ventes de PC fixes a bouleversé le marché. Avec 1,45 million d'appareils vendus en France, les tablettes dépassent les machines fixes vendues à 1,24 million contre 1,46 en 2010 [11]. Les us et coutumes informatiques sont donc en train de changer et cette évolution a un impact sur l'utilisation des réseaux d'accès. Les appareils mobiles ayant une capacité limitée et visant surtout à la consultation de contenu, une connexion à Internet ou un autre réseau de grande taille est donc nécessaire pour exploiter au mieux leurs fonctionnalités.

Dans un contexte nomade, trouver un point d'accès est relativement aisé. La distribution de box par les fournisseurs d'accès permet à tout domicile connecté à Internet de posséder un point d'accès Wi-Fi. Les entreprises sont souvent munies de points d'accès sécurisés pour leurs employés et ouverts pour les visiteurs. De nombreux lieux de restauration et cafés sont aussi pourvus de bornes Wi-Fi réservées à leurs clients. Ces différents moyens de connexions sont apparus au cours des années 2000 avec la démocratisation des ordinateurs portables et permettent d'obtenir une connexion à un emplacement « fixe ». A l'opposé, les téléphones intelligents et les tablettes sont faits pour être utilisés dans un contexte mobile et l'obtention d'une connexion passe alors par l'utilisation de la 3G/UMTS. Si cette technologie permet de couvrir une zone vaste avec des performances acceptables, elle est limitée par les obstacles et engendre une dépense énergétique importante, diminuant ainsi l'autonomie de l'appareil. En effet, le maintien d'une connexion active et le rétro éclairage de l'écran sont les facteurs de consommation les plus importants des appareils mobiles et conduisent l'utilisateur à les recharger

quotidiennement. Un autre frein à l'utilisation de la 3G est son coût financier : les opérateurs facturent l'accès par des frais supplémentaires ou un forfait autorisant un quota mensuel de données. Une fois le quota dépassé, l'utilisateur est restreint à une connexion GPRS qui se révèle quasi inutile pour le transfert de données.

Le besoin de connexion dans le contexte mobile est donc toujours présent malgré la disponibilité de réseaux 3G et les véhicules de transports en commun sont adaptés pour répondre à cette demande. En agissant comme des points d'accès mobiles, les transports en commun peuvent fournir une multitude de services sur les appareils de leurs usagers : consultation des horaires en temps réel, consultation des mails, visionnage d'émissions en streaming, accès au web, lecture de magazines et de journaux gratuits de manière dématérialisée… De son côté le gérant de la flotte a lui aussi un besoin de connexion pour échanger avec le véhicule et obtenir des informations qui sont actuellement récupérées lors du retour au parking. La Figure 1 tirée du projet AMIC-TCP auquel nous avons participé illustre les différents composants d'un autocar moderne et les systèmes permettant des échanges avec le gérant y sont visibles : le comptage de passagers et la vision de la caméra sont des données pouvant être récupérées, les affichages extérieurs de destination ou d'informations (les girouettes) peuvent être commandés à distance.

Avoir des véhicules connectés peut donc être utile pour le consommateur mais aussi pour le gérant de la flotte. Si l'exemple donné ici est un autobus, tous les types de transports en commun sont éligibles pour être des points d'accès mobiles même s'ils ne sont pas identiques et n'ont pas le même comportement. Les solutions de mobilité utilisées doivent être adaptées mais les problématiques restent les mêmes quel que soit le véhicule. Par exemple, un train a besoin d'une technologie de communication avec une grande zone de couverture et assurant une connexion fiable à haute vitesse mais peut nécessiter une autre technologie lors du passage dans un tunnel ou lors de l'arrivée en gare.

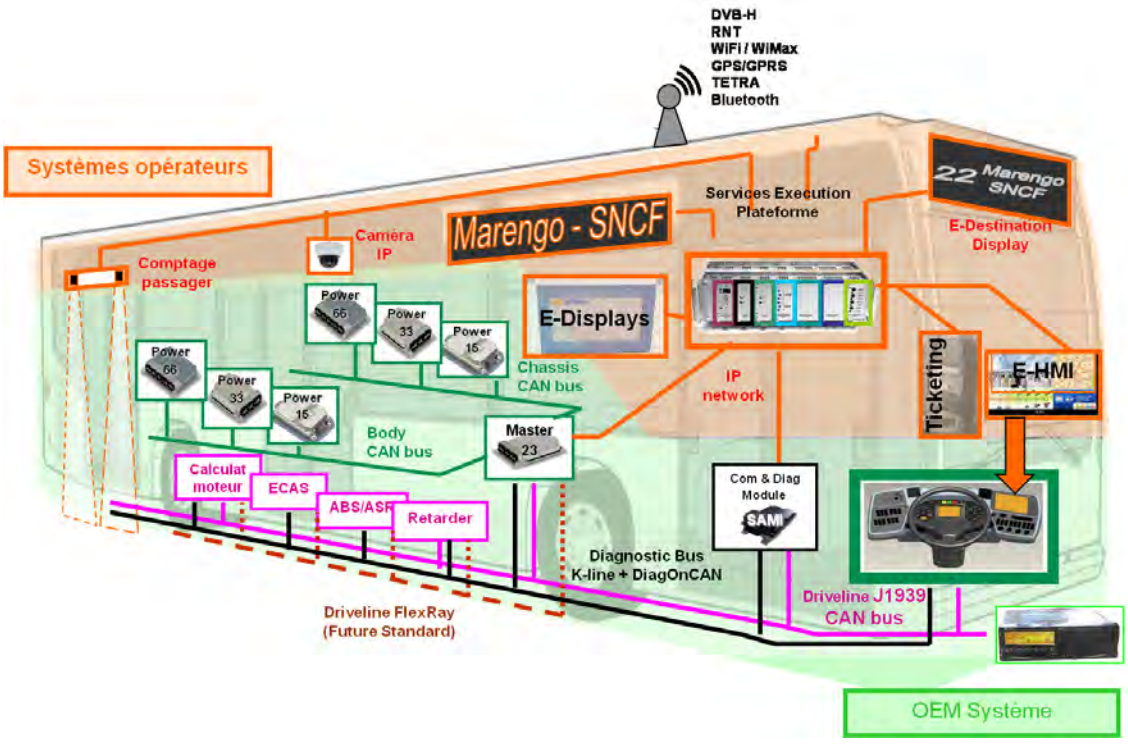


Figure 1 – Composants internes de l'autobus connecté conçus dans le projet AMIC-TCP.

II Les Caractéristiques des Transport en Commun

Les véhicules de transport en commun peuvent facilement devenir des points d'accès mobiles très prometteurs de par leurs caractéristiques et l'environnement dans lequel ils évoluent. Comparés à des véhicules particuliers, ils possèdent certaines spécificités :

- Connaissance du trajet à l'avance (peu amené à changer),
- Présence de moyens de localisation précis (GPS et odomètres),
- Autonomie conséquente en énergie (proportionnelle à la taille du véhicule),
- Espace à bord plus important (plus de place pour les antennes par exemple),
- Flux en présence très variés (critiques et non-critiques, usager et gérant de la flotte).

La connaissance du trajet permet de déterminer plusieurs éléments clés dans la mobilité du véhicule comme les zones de couverture traversées ou les obstacles rencontrés (tunnel, grands immeubles, arbres…). Le gestionnaire de mobilité peut donc être adapté pour améliorer la qualité des communications. Les Figure 2 et Figure 3 illustrent le déplacement d'un véhicule au travers de différentes zones de couverture. Le nombre de réseaux disponibles varie le long du trajet. La courte portée des réseaux Wi-Fi ne permet pas techniquement d'établir une connexion de longue durée si le véhicule continue à avancer : à 50km/h, 100m sont parcourus en moins de 8 secondes. Pour compenser

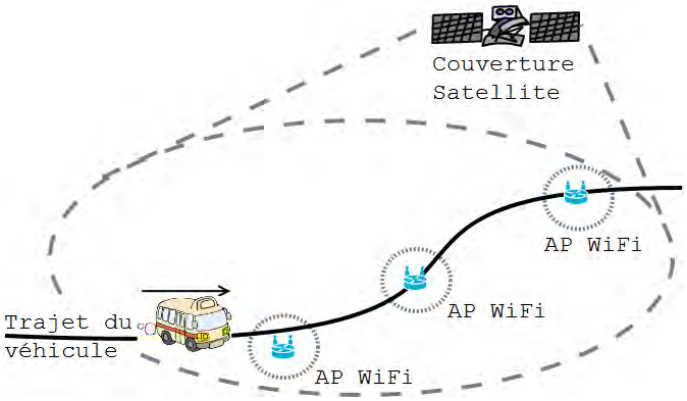


Figure 2 – Trajet d'un véhicule dans la zone de couverture d'un satellite et passant à proximité de points d'accès Wi-Fi.

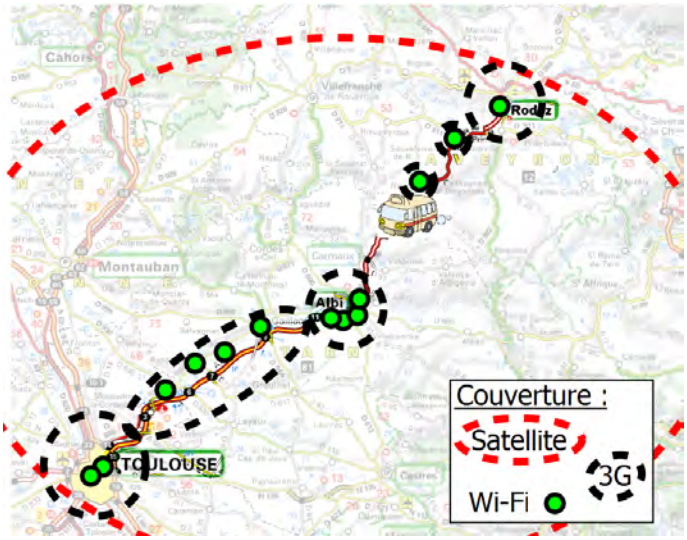


Figure 3 – Exemple d'une ligne de bus urbaine et intra-urbaine sur la N88: Rodez-Albi-Toulouse.

cette faible portée, le temps passé dans la zone de couverture peut être augmenté en plaçant des points d'accès aux arrêts ou par exemple dans le cas d'un autobus au niveau des feux tricolores. La section III.2 présente brièvement une étude sur le positionnement des bornes sur une carte dans le cadre d'un réseau tolérant au délai. La Figure 3 est le plan d'une ligne de bus suivant la nationale 88 entre Rodez et Toulouse. Les zones couvertes par les différentes technologies sont tracées à titre d'exemple, aucun test n'ayant été mené pour mesurer le signal satellite ou 3G. Néanmoins, on peut ainsi illustrer la taille des zones de couverture ainsi que la disponibilité des technologies de communication. Entre Rodez et Albi par exemple, le paysage est plutôt vallonné et les agglomérations sont rares, il est difficile d'y obtenir une connexion 3G stable. Au contraire entre Albi et Toulouse, l'autoroute traversant la plaine et étant proche de plusieurs agglomérations permet d'avoir un signal 3G quasi stable. Néanmoins, il

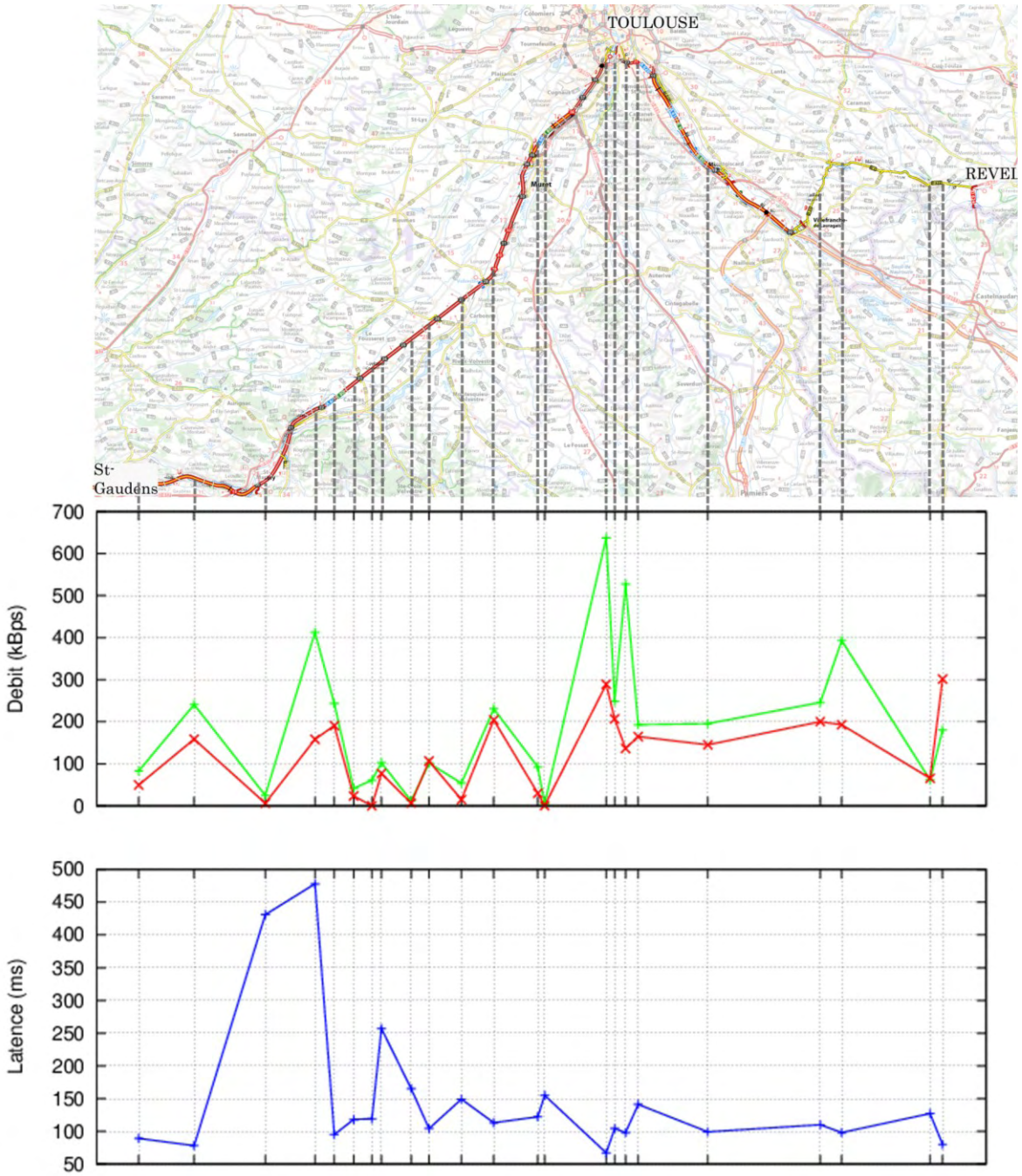


Figure 4 - Débits montants/descendants (vert/rouge) et latence mesurée entre un appareil mobile et un serveur fixe sur un trajet de Saint-Gaudens à Revel traversant Toulouse.

faut aussi prendre en compte la vitesse de déplacement qui diminue la qualité de la connexion.

Pour se faire une idée de l'influence de la vitesse de déplacement sur les communications, nous avons mené une expérience qui permet d'évaluer la qualité d'une connexion 3G pendant un déplacement en Haute-Garonne entre Saint-Gaudens et Revel passant par Toulouse. La Figure 4 représente les résultats obtenus le long de ce trajet avec les débits montant et descendant ainsi que la latence. Les résultats obtenus sont évidents : hors agglomération la bande passante disponible est plus faible. La latence quant à elle ne permet pas de tirer de conclusion, certaines mesures donnant un débit plus que correct avec une latence très élevée. On remarque que dans Toulouse, le débit atteint est beaucoup plus élevé que partout ailleurs et permet largement de rivaliser avec une connexion filaire située en campagne : plus de 600Ko/s sur la 3G contre un débit maximum de 350Ko/s aux environs de Revel avec l'ADSL.

Ces mesures ont été réalisées avec un téléphone intelligent connecté en 3G sur le réseau d'un fournisseur d'accès mobile français. L'application « SpeedTest.net » a permis de réaliser les tests de bande passante et de délai en se connectant à un serveur situé à Paris. La fiabilité de ces mesures est donc relative, l'application n'étant pas entièrement contrôlée par nos soins. Néanmoins le goulet d'étranglement étant localisé au niveau du point d'accès, les débits peuvent être observés à titre indicatif. De plus, pour avoir utilisé cette application à de maintes reprises, les résultats obtenus sont assez proches de ceux obtenus par des moyens plus traditionnels comme TCPDUMP ou Wireshark [90].

En Novembre 2012, un bilan a été dressé par l'Autorité de Régulation des Communications Electroniques et des Postes (ARCEP) sur la couverture et la Qualité de Service (QdS) des réseaux mobiles en France métropolitaine. Si les résultats de cette étude permettent de connaître la couverture dans des cas stationnaires, aucune mesure n'est faite à bord de véhicules ou dans les bâtiments. Par exemple, le chemin parcouru en Haute-Garonne pendant l'expérience précédente est signalé comme étant desservi par, au minimum 3 réseaux 2G et 3 réseaux 3G mais sans précisions sur la qualité du signal, que nous estimons très variable. Il faut tout de même noter la volonté de l'ARCEP d'obtenir des résultats pour ces situations par l'approfondissement de simulations ou la prise en compte de mesures complémentaires (proposition 6 et 7 du rapport [1]). L'accès à Internet à bord des trains est abordé pour illustrer la mauvaise réception du signal à bord des véhicules et une piste est donnée en répétant le signal à l'intérieur du véhicule ou en installant des bornes Wi-Fi.

Les moyens de localisation présents dans un véhicule de transport en commun permettent une précision de l'ordre du mètre : le « Global Positionning System » (GPS) peut en effet être amélioré par l'utilisation des odomètres. Cette localisation peut être utilisée de différentes manières. Le gérant de la flotte peut situer son véhicule à tout moment et ainsi améliorer la précision des horaires en temps réel ou même évaluer le trafic routier suivant l'heure de la journée en se basant sur des statistiques. La localisation peut aussi être utilisée par le gestionnaire de mobilité pour déterminer les réseaux prochainement disponibles, ceux bientôt hors de portée ou encore la panne d'un point d'accès (absence d'un réseau à un endroit normalement couvert). Pour cela, il est nécessaire de posséder une carte des réseaux disponibles qui peut être établie avec les passages successifs de véhicules de transport en commun. Notre proposition décrite dans le Chapitre IV utilise ce type de carte afin d'améliorer la mobilité avec mSCTP.

L'autonomie des véhicules de transport en commun est très importante comparée avec l'autonomie d'un nœud utilisateur et la taille du véhicule permet de posséder une ou plusieurs interfaces réseaux pour chaque technologie de communication disponible. Ce contexte où le nœud peut être connecté à plusieurs réseaux simultanément est appelé « multi homing » ou multi-domiciliation (voir Chapitre II,

section I.2). Les avantages à la multiplication des technologies de communication disponibles sont réels :

- Augmenter la connectivité du nœud avec une plus grande zone de couverture,
- Améliorer la stabilité du lien en choisissant la technologie la plus adaptée (obstacles…),
- Obtenir de meilleures performances (délai, débit, gigue, pertes…),
- Maximiser la bande passante disponible (répartition de la charge de données),
- Diminuer les temps de latence lors du basculement entre des réseaux d'accès (« Make Before Break »).

Les deux derniers points peuvent aussi être obtenus en utilisant plusieurs interfaces d'une même technologie. Les supports de communication Wi-Fi, 3G/UMTS et satellite sont décrits dans le Chapitre II, section II avec leurs impacts sur les communications et leurs spécificités.

La dernière caractéristique des points d'accès mobiles n'est pas un avantage mais plutôt une contrainte. Il s'agit de la diversité des flux présents : comme pour un réseau d'accès fixe, le nombre de nœuds connectés va influencer cette diversité : flux de données, streaming, voix sur IP, applications critiques du gestionnaire.... Pour distinguer les différents types de communication, certains critères comme les performances requises ou l'aspect critique de l'application sont évidents mais le possesseur du flux peut aussi être pris en compte. Une application non-critique appartenant à l'opérateur peut par exemple être privilégiée. Cette diversité va influencer le comportement du réseau en impactant les performances mais il est aussi envisageable de choisir le réseau d'accès en fonction des flux ou au contraire bloquer certains flux sur certains supports. En effet, il peut être préférable de « freiner » certains flux de données sur des connexions onéreuses comme le satellite dans l'attente de la présence d'une connexion Wi-Fi.

III Exemple d'un Banc de Test grandeur nature avec des véhicules de Transport en Commun

Si les expériences faites en simulation ou en émulation permettent de tester des systèmes et de concevoir les réseaux de demain, un banc de test réel permet l'obtention de résultats prenant en compte tous les facteurs de l'environnement. Le banc de test « Diverse Outdoor Testbed Environment » (DOME) [2] a été construit dans ce but là par le département des sciences informatiques de l'université du Massachussetts (UMass Department of Computer Science) et en coopération avec le « National Science Foundation's Global Environment for Network Innovation » (NSF GENI). DOME est composé de 35 bus et d'un réseau maillé construit avec la coopération de la ville d'Amherst dans le Massachussetts. Les véhicules sont équipés d'un ordinateur, d'une interface réseau Wi-Fi, d'un point d'accès Wi-Fi interne au véhicule, d'un modem 3G, d'une interface radio 900MHz et d'un GPS. Diverses expériences ont été menées depuis le lancement du banc de test en 2004 et les mesures effectuées ont permis de tirer plusieurs conclusions sur le domaine mobile. Nous nous intéresserons ensuite à une expérience menée avec un réseau tolérant au délai, « Delay-Tolerant Networking » ou « Disruption-Tolerant Networking » (DTN), et à la disposition de « boîtiers » améliorant leurs performances.

III.1 Etudes des mesures faite sur DOME

Entre janvier 2005 et décembre 2008, DOME a permis de recueillir une grande quantité de données, notamment des traces de mobilité et de connectivité. Leur analyse permet d'apprendre certains faits sur les réseaux dans une agglomération. Il faut néanmoins garder à l'esprit que la configuration dans

une autre agglomération peut être différente et les résultats peuvent donc changer suivant le contexte. Une analyse globale de ces données est faite dans [3] [1]et les auteurs soulignent cinq remarques intéressantes :

1. *« Les réseaux Wi-Fi publics fournissent une couverture suffisante dans l'environnement de DOME pour les applications envoyant des paquets relativement petits ou n'étant pas affectées par le débit. »*
2. *« L'accroissement du nombre de points d'accès Wi-Fi n'a pas été accompagné par une chute significative du nombre de points d'accès ouverts (relativement au nombre total). »*
3. *« Malgré la densité des points d'accès disponibles dans le banc d'essai DOME (considérée haute par les auteurs), il n'a pas été possible de démontrer significativement les effets négatifs des interférences. »*
4. *« Afin d'atteindre le débit global fourni par la 3G, il serait nécessaire d'avoir une couverture Wi-Fi offrant une connexion active sur quasiment 90% du trajet. »*
5. *« La plus grande partie des contacts avec les réseaux publics est faite lorsque le véhicule est à l'arrêt. »*

Les résultats 1, 2 et 5 portent sur les réseaux Wi-Fi publics et permettent de tirer plusieurs conclusions. Le premier résultat est logique étant donné que les réseaux publics offrent des connexions de très faible débit. L'utilisation des points d'accès publics est envisageable pour certains flux et peut permettre ainsi de soulager d'autres interfaces actives. De plus, il est intéressant de noter que les points d'accès détectés au cours de plusieurs années de mesures comportent sensiblement la même proportion de réseaux en libre accès. Il est possible de tabler sur ces réseaux pour certains types de flux de débit faible ou peu exigeants. Néanmoins, le résultat 5 modère les deux conclusions précédentes : les connexions avec les réseaux publics s'établissent plus facilement si le véhicule est à l'arrêt. Ceci est dû au temps de connexion nécessaire pour de tels réseaux. Au vu de ces trois résultats, les réseaux publics peuvent être utilisés comme points d'accès secondaires lors des arrêts à des feux ou des stations.

Les résultats 3 et 4 sont des hypothèses plus générales sur les réseaux Wi-Fi. Dans un environnement urbain, le problème des interférences dûes au nombre élevé de réseaux est souvent abordé, celui-ci pouvant altérer les communications. Pourtant, les relevés effectués sur le banc d'essai DOME tendent à montrer que ces interférences sont limitées et qu'il est difficile de démontrer leur impact sur les performances. Il faut quand même noter que les interférences dans l'environnement urbain peuvent aussi provenir d'obstacles ou d'émissions radios autres que Wi-Fi mais intervenant à la même fréquence.

La concurrence entre 3G et Wi-Fi dans l'environnement urbain est intéressante et il s'agit d'un sujet récurrent dans le domaine des réseaux mobiles. Toujours d'après les mesures effectuées avec DOME, la faible bande passante offerte par la 3G est largement compensée par sa disponibilité. Le taux de couverture à atteindre avec du Wi-Fi pour transférer la même quantité de données est difficilement atteignable.

III.2 Un DTN fait de véhicules de transport en commun

Le réseau tolérant au délai ou DTN est un concept basé sur une architecture visant à limiter l'impact d'un manque de connectivité dans les réseaux hétérogènes. Récemment, le terme « Disruption-Tolerant Networking » soit réseau tolérant aux perturbations est devenu courant avec les projets supportés par la « Defense Advanced Research Projects Agency » (DARPA). Deux standards [7], [8] ont été publiés en 2007 dans l'optique d'harmoniser les architectures et permettre l'interfaçage entre

différentes implémentations. Les utilisations envisagées des DTN sont diverses : environnements mobiles, réseaux spatiaux et liaisons interplanétaires [9], conditions extrêmes de communication (limites de couverture, nœuds en densité faible, économie d'énergie,…). Le banc de test DOME est donc adapté aux DTN avec ses bus de ville disséminés le long d'un trajet.

Ce banc de test a servi à plusieurs études sur les DTN : la résolution de problèmes de routage [4], le déploiement de boîtiers-relais [5], la réduction de la consommation électrique [6]… Le routage dans les DTN possède une contrainte très forte : l'absence de connexion directe entre le nœud émetteur et le nœud destinataire. La métrique utilisée est généralement le délai de livraison dans le pire cas ou le pourcentage de paquets livrés avant un temps limite. Le protocole de routage présenté dans [4] propose de traiter le routage comme une allocation de ressource afin de déterminer comment les paquets doivent être répliqués dans le réseau.

Le déploiement de boîtiers-relais est intéressant car il permet d'améliorer les performances du réseau en améliorant la connectivité, ce qui permet notamment d'augmenter la capacité globale du réseau pour un faible coût [5]. Une étude est faite sur le placement de ces boitiers en fonction de leur type et du schéma de mobilité. Dans le cas des transports en commun, l'amélioration apportée par les boitiers est important car la mobilité des nœuds est « régulière » (passage à des emplacements précis et à intervalle régulier). Le déploiement des boitiers est aussi facilité par l'utilisation d'algorithmes de placement basés sur les opportunités d'établir le contact et éventuellement les informations sur le trafic.

Les boitiers disposés le long du trajet ne sont pas alimentés et leur autonomie énergétique repose uniquement sur leur batterie. Une proposition est faite dans [6] pour diminuer leur consommation électrique. Comparé à une interface radio à ondes longues, une interface Wi-Fi consomme plus d'énergie et a une portée plus faible. En partant de ce constat, une étude a été menée où l'interface Wi-Fi des bornes est éteinte si aucun véhicule n'est à portée. L'interface radio est utilisée pour détecter l'arrivée prochaine d'un véhicule dans la zone de couverture Wi-Fi et, lors de l'arrivée d'un véhicule, l'interface Wi-Fi est allumée durant le temps de la communication. Cette étude est intéressante car l'utilisation de plusieurs technologies de communication ne vise pas à augmenter les performances mais permet de réduire la consommation électrique des boîtiers.

Chapitre II La mobilité dans les réseaux de communication

Les performances des applications dans les réseaux de communication sont influencées par de nombreux facteurs : la mobilité, le support physique, le comportement de la couche réseau, le protocole de Transport utilisé et plus généralement le contexte. Dans cette section, nous allons détailler ces différents facteurs, en ciblant notamment l'impact de la mobilité sur plusieurs couches du modèle OSI (voir Tableau 1). Dans un premier temps, nous introduirons les différentes problématiques de la mobilité que nous avons abordées ou rencontrées au cours de cette thèse. Ensuite, une description de différents supports physiques sera faite avec leurs caractéristiques et leur impact sur les communications. Enfin, les mécanismes de mobilité niveau Réseau et niveau Transport seront présentés avec leur définition issue des documents de référence et des études menées sur les solutions proposées.

I Introduction aux problématiques de la mobilité et des réseaux sans-fils

La mobilité est définie par le dictionnaire comme une *«Propriété, caractère de ce qui est susceptible de mouvement, de ce qui peut se mouvoir ou être mû, changé de place, de fonction ».* Dans un réseau informatique, la mobilité ne désigne pas uniquement la capacité d'un nœud à se déplacer, elle englobe toutes les problématiques qui lui sont liées : la localisation du nœud, le changement de point d'accès, les possibilités de multi-domiciliation… De plus, les contraintes de la communication sans-fil doivent aussi être prises en compte : atténuation du signal, présence d'un nœud caché, dégradation du signal à cause de l'environnement, influence du support…. Leur impact est très important et influence les performances des applications sur un réseau sans-fil. Dans la suite de cette section, nous allons nous intéresser aux problématiques de la mobilité tout en considérant certaines caractéristiques des réseaux sans-fils.

I.1 Le changement de réseau horizontal et vertical

Le changement de réseau ou « handover » (HO) est l'un des phénomènes le plus influent de la mobilité. Que ce soit en sortant d'une zone de couverture, à cause d'obstacles ou pour obtenir de meilleures performances, il est obligatoire de changer de points d'accès régulièrement (fréquence dépendant de la taille de la zone de couverture et de la mobilité). Basculer entre deux réseaux de même technologie est un changement de réseau dit horizontal. Si la technologie est différente, le changement de réseau est dit vertical. Nous nous focalisons ici sur la modification de l'identifiant réseau lors du changement de réseau, la latence introduite par le basculement et la modification des

Tableau 1 – Modèle OSI (à gauche) et sa version simplifiée dite modèle TCP/IP (à droite)

Type de PDU	Modèle OSI	Numéro	Modèle TCP/IP
Donnée	Application	7	Application
	Présentation	6	
	Session	5	
Segments	Transport	4	Transport
Paquet/Datagramme	Réseau	3	Réseau
Trame	Liaison	2	Liaison
Bit	Physique	1	Physique

caractéristiques du réseau.

I.1.1 La modification de l'identifiant réseau

A l'origine, les réseaux informatiques ont été conçus pour faire communiquer des nœuds fixes. Un identifiant invariable était donc attribué à chaque appareil. Avec la démocratisation des technologies sans-fil, les nœuds sont amenés à changer de points d'accès et deviennent alors des nœuds mobiles. Avec Internet Protocol version 4 (IPv4), la connexion à un nouveau point d'accès provoque l'attribution d'un nouvel identifiant réseau (adresse IP). Les protocoles de Transport se basant sur cet identifiant pour communiquer, le modifier conduit à la rupture de la connexion. Plusieurs solutions ont été proposées pour contourner la modification de l'adresse et ainsi garantir le support de la mobilité.

Les solutions de mobilité au niveau Réseau se basent pour la plupart sur la mise en place d'un tunnel entre le nœud et une entité dans le réseau de cœur, permettant ainsi de garder la connexion active contre une perte de performances (voir Chapitre II, section III). La définition d'IPv6 a permis de limiter le changement d'identifiant par la disponibilité d'un nombre quasi illimité d'adresses. Théoriquement, il est possible d'attribuer $3{,}4 * 10^{38}$ adresses soit plus de 667 millions de milliards d'adresses par millimètres carré sur toute la surface du globe. La mobilité avec IPv6 permet donc de garder l'identifiant mais les autres problématiques liées au changement de réseau sont toujours présentes.

Au niveau Transport, des solutions de mobilité ont été proposées notamment pour pallier à la durée de mise en place d'IPv6. Ces solutions reposent sur l'ajout d'un autre identifiant permettant aux nœuds de reconnaître une communication en cours même si l'adresse IP a changé. L'avantage de ces solutions est l'absence de modifications dans le réseau d'accès ou le réseau de cœur. Néanmoins, la présence du protocole de Transport adéquat est nécessaire dans les terminaux ainsi que son support dans les nœuds intermédiaires.

I.1.2 La latence introduite par le changement de réseau

L'association d'un nœud mobile à un point d'accès implique plusieurs niveaux du modèle OSI : le niveau Liaison intervient dans la connexion « physique » entre les deux entités et le niveau Réseau permet la connexion « logique » avec la configuration de l'interface réseau. La latence introduite par ces configurations est souvent importante comparée au délai des communications et varie suivant le matériel utilisé.

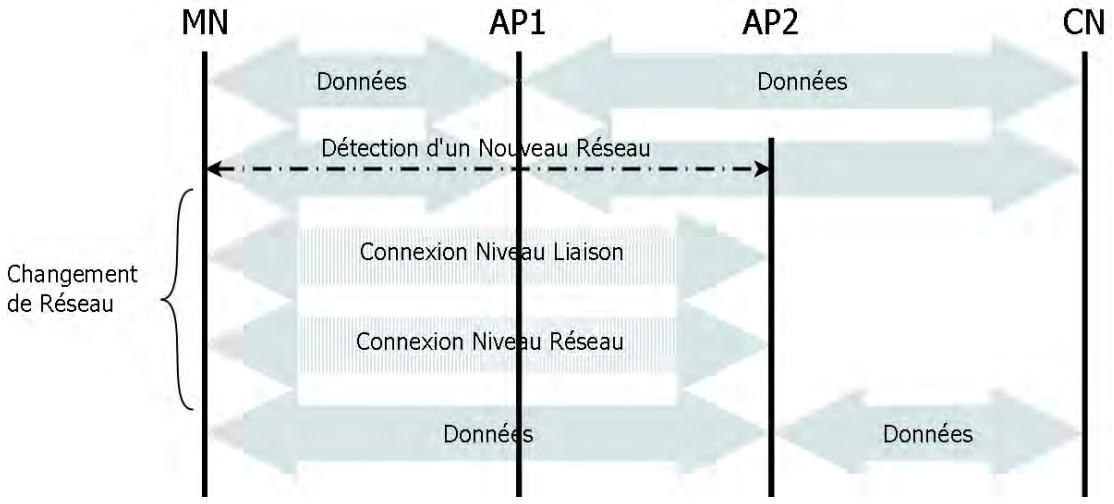


Figure 5 – Echanges entre nœud mobile et point d'accès lors d'un changement de réseau.

La Figure 5 illustre les échanges entre un nœud mobile ou « Mobile Node » (MN) et deux points d'accès ou « Access Points » (AP) lors d'un changement de réseau. Le MN est en communication avec un nœud correspondant ou « Corresponding Node » (CN) lorsqu'un nouveau réseau est détecté. Le temps écoulé entre l'envoi de la dernière donnée sur l'ancien lien et l'envoi de la nouvelle donnée sur le nouveau lien est appelé durée du changement de réseau ou « Handover delay ». Aucune donnée n'est envoyée ou reçue pendant ce délai nécessaire à l'établissement de la connexion et à la configuration de l'interface réseau.

La durée du changement de réseau est fortement dépendante du gestionnaire de mobilité utilisé. Si celui-ci doit contacter une entité extérieure pour mettre en place un nouveau tunnel, la durée peut être augmentée. Néanmoins, la plupart des solutions de mobilité visent à réduire cette latence en faisant du « Make Before Break » (MBB) au lieu du « Break Before Make » (BBM), c'est-à-dire en se connectant au nouveau réseau avant de rompre la connexion à l'ancien réseau et non l'inverse.

Au niveau applicatif, la latence introduite par le changement de réseau peut être gênante pour l'utilisateur : une coupure de plusieurs secondes au milieu d'une communication Voix sur IP ou Voice over IP (VoIP) est difficilement tolérable. Nous verrons par la suite que les recommandations en termes de délai et gigue pour les applications dites multimédia ne tolèrent pas une latence excessive (voir Chapitre II, section I.3).

I.1.3 Changement des caractéristiques du réseau d'accès

Le comportement des flux applicatifs dépend en grande partie des caractéristiques du réseau et des services proposés par le point d'accès. La bande passante, le délai, la gigue, la congestion ou encore la Qualité de Service ou « Quality of Service » (QdS/QoS) sont des caractéristiques qui impactent fortement les communications. Leurs valeurs autant que leurs variations influent sur la Qualité d'Expérience ou « Quality of Experience » (QdE/QoE). L'impact des caractéristiques du réseau sur un lien stable dépend principalement du support utilisé par la communication. L'influence du support physique est discutée dans le Chapitre II, section II avec la présentation des trois technologies : le Wi-Fi, les réseaux cellulaires et les réseaux de communication par satellite. La discussion porte ici sur la modification brutale de ces caractéristiques et l'impact sur les communications.

Lorsqu'un nœud mobile change de point d'accès, le chemin utilisé par la communication est différent et ses caractéristiques sont brusquement modifiées. Les performances des applications peuvent être impactées de manière critique : perte de données, diminution du débit, augmentation du délai... Ces changements sont immédiats et peuvent être de grande ampleur. Si l'utilisation d'une solution de mobilité permet de réaliser le changement de réseau en résolvant les contraintes introduites précédemment (modification de l'identifiant réseau et introduction d'une latence), cette solution rend aussi souvent le changement de réseau transparent pour les protocoles de Transport situés dans les terminaux des utilisateurs. Si la mobilité est gérée par un routeur en amont, le nœud mobile est même incapable de détecter le changement de réseau.

Les protocoles de Transport gèrent les communications de bout-en-bout entre nœuds et sont donc en charge de transférer les données. Afin d'obtenir des performances optimales, ces protocoles utilisent des mécanismes tels que la gestion du flux et la prévention de la congestion. Ils permettent aux protocoles de Transport d'évaluer les conditions de la communication et de s'y adapter en se basant sur l'évaluation des caractéristiques du réseau et leur évolution. Ces fonctionnalités se révèlent particulièrement efficaces dans les réseaux filaires. Les liens utilisés pour les communications étant stables, la modification des caractéristiques du réseau perçues par la communication se fait en général de manière progressive et est souvent liée à l'apparition d'une congestion dans le réseau. L'impact sur

les communications est alors limité car les protocoles de Transport sont en mesure de prévenir la congestion et de prendre des décisions permettant de la limiter.

La modification drastique des caractéristiques du réseau a un impact différent sur les protocoles de Transport. Immédiatement après le changement de réseau, les évaluations faites par le protocole de Transport ne sont plus valables et les mécanismes permettant d'améliorer les communications sur un lien stable vont alors être induits en erreur. Le temps nécessaire au protocole pour s'adapter au nouveau réseau est alors dépendant du support physique et du protocole de Transport utilisés, certains ayant été conçus pour supporter des modifications importantes des caractéristiques.

L'impact du changement de réseau transparent sur un protocole de Transport comme TCP est discuté dans le Chapitre II, section V.1.2 avec la présentation d'études démontrant la faiblesse des mécanismes actuels et comment les améliorer avec de nouvelles versions de TCP ou des mécanismes inter-couches. Le Chapitre V présente une de nos propositions qui permet de prévenir la dégradation de performances lors de la modification brutale des caractéristiques dans le contexte d'un réseau mobile en informant le nœud mobile lorsque le routeur mobile effectue un changement de réseau.

I.2 La multi-domiciliation pour faciliter la mobilité

Ces dernières années, les avancées scientifiques ont permis une évolution des réseaux de communication et surtout de leur utilisation. La miniaturisation des composants électroniques permet aux appareils mobiles de posséder plusieurs interfaces réseaux et la diversité des technologies de communication permet d'obtenir plusieurs moyens de connexion. Un nouveau concept est alors né : la multi-domiciliation ou « multi homing ». Il s'agit de l'activation simultanée de plusieurs interfaces réseaux pour se connecter à des points d'accès et permettre la mise en place de chemins multiples. Cette technique est appelée à devenir courante notamment avec les protocoles de Transport de nouvelles génération dont l'architecture est adaptée à la gestion de plusieurs chemins. En 2008, les documents [27] et [28] présentent les motivations poussant vers la multi-domiciliation et discutent de sa généralisation. Les bénéfices sont notamment l'augmentation de la connectivité, de la fiabilité ou encore de la bande passante. Nous allons voir que la multi-domiciliation peut aussi être utilisée pour améliorer la mobilité.

En utilisant plusieurs interfaces, il est possible de se connecter à un nouveau réseau tout en restant connecté à l'ancien réseau. L'impact de la mobilité est alors grandement réduit en réalisant un « Make

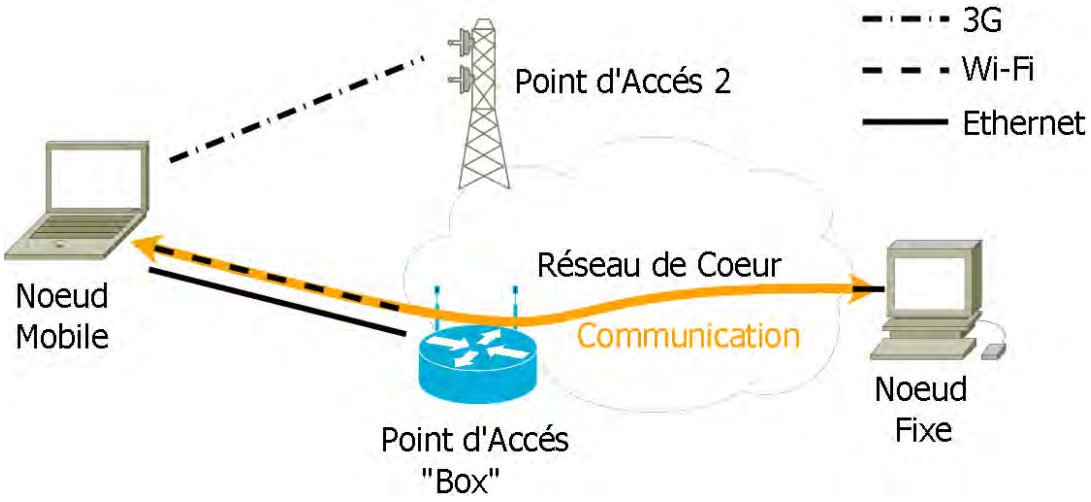


Figure 6 – Exemple d'un nœud multi-domicilié possédant des interfaces de 3 technologies de communication différentes : 3G, Wi-Fi et Ethernet.

Before Break » entre plusieurs interfaces. Un avantage de cette technique est la possibilité de garder plusieurs interfaces actives pour basculer instantanément de l'une à l'autre. Certaines des solutions de mobilité présentées dans le Chapitre II, section III et section V, comportent des extensions utilisant la multi-domiciliation pour améliorer leurs performances.

La multi-domiciliation est appelée à devenir courante dans les réseaux de demain. Néanmoins, certaines contraintes doivent être considérées pour ne pas diminuer les performances des applications. Un des préceptes de base de la multi-domiciliation est que deux chemins ne doivent pas partager de goulet d'étranglement ou « bottle-neck ». En effet, cela reviendrait à rendre « dépendants » les deux chemins : une amélioration sur un chemin induirait donc obligatoirement une dégradation sur l'autre. Dans un réseau, un potentiel goulet d'étranglement est un nœud dont la bande passante sortante est inférieure à la bande passante entrante. Dans un réseau sans-fil Wi-Fi par exemple, le point d'accès est considéré comme le goulet d'étranglement dans le sens réseau Wi-Fi vers réseau de cœur.

La Figure 6 présente un nœud multi-domicilié connecté à un réseau de cœur via la 3G, le Wi-Fi et une connexion Ethernet. Dans le cas d'un particulier, les connexions Ethernet et Wi-Fi sont fournies par le même équipement, le point d'accès au réseau de cœur est donc unique. Il est donc clair que sur ce schéma, les chemins Wi-Fi et Ethernet ne sont pas indépendants et les utiliser comme tel irait à l'encontre des recommandations. Ceci est correct car le point d'accès est connecté au réseau de cœur par un lien unique. Nous verrons plus tard que si le routeur est multi-domicilié, il devient possible de considérer les chemins comme indépendants en associant chaque technologie interne à un chemin externe.

I.3 Réseaux sans-fils, Mobilité et Contraintes Temporelles

Les réseaux sans-fils présentent de nombreuses caractéristiques qui les différencient des réseaux filaires. Le temps de propagation et l'environnement sont des contraintes fortes qui influencent le délai, la gigue, la bande passante, le taux de pertes… Dans un contexte mobile, les latences dues au changement de réseau ainsi que des possibles interruptions viennent s'ajouter. L'objectif des architectures mobiles est d'offrir aux applications une connexion stable et fiable.

Dans un réseau d'accès, les flux en présence sont très variés et ont des priorités différentes : débit important, délai ou variation de délai faible, faible taux de pertes… Les applications multimédias sont considérées comme étant les plus contraignantes car elles nécessitent un débit stable parfois conséquent tout en ayant un délai faible. Les recommandations de l' « International Telecommunication Union » (ITU) pour ces flux sont présentées dans le Tableau 2 issu de [29]. Si les performances demandées sont relativement faciles à atteindre dans un réseau filaire, il devient difficile de les égaler avec un réseau sans-fil. Nous verrons dans la partie IIque certaines technologies de communication ne sont pas en mesure d'atteindre certains objectifs comme le délai de préférence et devront se contenter de rester en dessous du délai considéré comme limite.

Tableau 2 – Recommandations de l'ITU-T pour les délais, débits, gigues et taux de pertes.

Medium	Application	Degree of symmetry	Typical data rates (Kb/s)	Key performance parameters and target values			
				One-way delay	Delay variation	Information loss (Note 2)	Other
Audio	Conversational voice	Two-way	4-64	<150 ms preferred <400 ms limit	< 1 ms	< 3% packet loss ratio (PLR)	
Audio	Voice messaging	Primarily one-way	4-32	< 1 s for playback < 2 s for record	< 1 ms	< 3% PLR	
Audio	High quality streaming audio	Primarily one-way	16-128	< 10 s	<< 1 ms	< 1% PLR	
Video	Videophone	Two-way	16-384	< 150 ms preferred <400 ms limit		< 1% PLR	Lip-synch: < 80 ms
Video	One-way	One-way	16-384	< 10 s		< 1% PLR	

II L'influence du support physique

Le support physique a une influence primordiale sur les performances atteignables dans les réseaux de communication car il peut fixer certaines contraintes. Le temps de propagation et la fréquence utilisée déterminent respectivement un délai et un débit d'émission qui sont alors immuables. D'autre part, la méthode d'accès au médium (niveau 2 du modèle OSI, voir Tableau 1) peut varier d'un réseau à l'autre pour le même support et impacte plusieurs facteurs : temps d'accès au support, gestion de la QoS, … Dans cette section, nous allons détailler les caractéristiques et les performances de trois technologies très différentes : les réseaux de communication par satellite, les réseaux Wi-Fi et les réseaux dits « cellulaires » 3G/UMTS ou GPRS.

II.1 Les Réseaux de Communication par Satellite

La deuxième moitié du 20° siècle a été marquée par la guerre froide et la rivalité est-ouest. La volonté d'observation des deux blocs les pousse dans une course à l'espace qui commence par la mise en orbite de satellites. Les recherches étant financées en grande partie par l'armée, les premières applications seront essentiellement militaires. Mais les avancées technologiques apportées dans le domaine des télécommunications ouvrent la voie à de nouvelles technologies. En 2007, plus de 5500 satellites ont été placés en orbite depuis le début de la conquête de l'espace et 700 étaient encore actifs d'après [10].

Le premier satellite mis en orbite est « Spoutnik I » en octobre 1957, sa seule utilité était d'émettre un bip sur les fréquences 20,005MHz et 40,002MHz [12]. Les premiers satellites non-militaires apparaissent en 1960 : « TIROS-1 » est dédié à l'observation météorologique et « Echo » permet de retransmettre des signaux sans amplification. Il a fallu attendre 1962 pour que soit mis en orbite un satellite régénérant les signaux et capable de les amplifier : « Telstar-1 ». Une antenne d'une dizaine de mètres est nécessaire pour recevoir le signal mais il s'agit là du début des télécommunications par satellite.

Suivant leur taille et leurs fonctionnalités, les satellites sont placés sur des orbites différentes et ne sont pas soumis aux mêmes contraintes. De nombreuses dénominations existent pour différencier les orbites entre elles [13], les plus connues sont :

- « Low Earth Orbit » : orbite basse au dessus de l'atmosphère terrestre, altitude comprise entre 80km et 2000km, révolution de 90min.
- « Middle Earth Orbit » : orbite circulaire intermédiaire, altitude comprise entre 2000km et 35786km, révolution entre 2h et 12h.
- « Geosynchronous Orbit » : ou orbite de Clarke, altitude 35786km, révolution de 1 jour exactement. L'orbite est dite géostationnaire si l'inclinaison est de 0°.

Ces caractéristiques sont prises en compte pour l'utilisation des satellites comme réseaux de communication. Le Tableau 3 résume les caractéristiques de ces familles de satellites d'un point de vue réseau. Le délai minimal donné correspond à deux fois le temps de propagation, soit le temps pour

Tableau 3 – Caractéristiques des différentes familles de satellite

	Délai minimal (aller-retour)	**Exemple d'application**
LEO	~10ms	Voix, Vidéos Conférences…
MEO	~100ms	Voix, Données…
GEO	250ms	Télévision, Données…

un paquet de monter au satellite et de revenir sur Terre. Il faut donc multiplier ce temps par 2 pour obtenir le RTT entre deux hôtes communiquant via satellite. Il est clair que chaque type de satellite ne se destine pas aux mêmes applications, les satellites proches de la Terre paraissent plus adaptés aux flux multimédia critiques tandis que les satellites les plus éloignés sont mieux adaptés pour des transferts de données ou des applications multimédia non-critiques. Par exemple, au vu des recommandations de l'ITU présentées dans le Tableau 2, il parait difficile d'établir une communication audio de type VoIP via des satellites géostationnaires. Néanmoins, la rapidité de révolution des satellites en orbite basse les rend plus complexes à utiliser pour les télécommunications, le basculement entre différents satellites étant obligatoire pour garder une connexion stable. A l'opposé, les satellites géostationnaires couvrent une zone fixe sans changement de satellite. Les réseaux satellites étudiés dans cette thèse étant considérés géostationnaires, la suite de cette section présente leurs particularités.

Les satellites géostationnaires présentent deux inconvénients majeurs pour l'utilisateur : un délai élevé et une obligation de partager la bande passante. Différentes normes et architectures réseau sont apparues depuis la mise en place des satellites de communications permettant de réduire l'impact de ces particularités. La différentiation des flux permet de concevoir une architecture avec des services de QdS et ainsi se soumettre aux contraintes temporelles des applications critiques. L'allocation de la bande passante dans le sens montant permet d'obtenir un partage équitable et neutre entre les différents terminaux. Dans le sens descendant, le partage n'est pas obligatoire, le débit global étant très élevé (>60Mbps).

La division de la bande passante se fait en deux étapes : une division fréquentielle « Frequency Division Multiple Access » (FDMA) suivi par une division temporelle « Time Division Multiplie Access » (TDMA). L'agrégation de ces deux techniques est le « Multi-Frequency Time Division Multiple Access » (MF-TDMA). L'utilisation de plusieurs porteuses permet d'augmenter considérablement le nombre de canaux. Ces canaux sont divisés en intervalles temporels qui peuvent être alloués aux différents terminaux satellites. La méthode d'allocation utilisée pour répartir

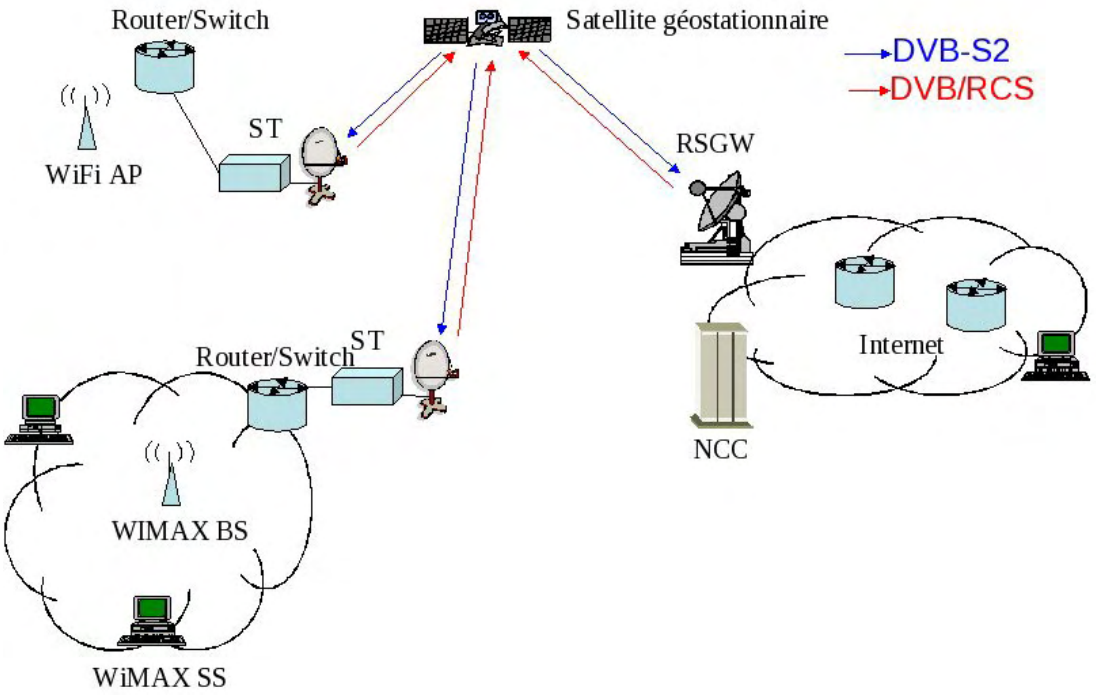


Figure 7 – Un réseau de communication par satellite avec le NCC et la GW sur le même réseau.

équitablement ces intervalles entre terminaux est le protocole « Demand Assignment Multiple Access » (DAMA). Il distribue les intervalles temporels de manière statique « Constant Rate Assignement » (CRA) ou dynamique « Rate Based Dynamic Capacity » (RBDC) et « Volume Based Dynamic Capacity » (VBDC). Les terminaux satellites ou « Satellite Terminals » (ST) envoient des informations sur leurs files d'attente au Network Control Center (NCC). Ce dernier calcule les débits nécessaires pour chaque station et en déduit un nombre d'intervalle qu'il envoie aux terminaux. La Figure 7 illustre un réseau de télécommunication par satellite. Les différentes entités sont présentes : les terminaux avec leurs réseaux d'accès, le satellite, le NCC et la passerelle ou GateWay (GW). Le placement du NCC dans le schéma est arbitraire, il peut être dans un terminal, dans le réseau de cœur (Internet) ou plus simplement avec la passerelle (GW).

Les protocoles de l'exemple de la Figure 7 sont le « Digital Video Broadcasting by Satellite 2 » (DVB-S2) et le « Digital Video Broadcast – Return Channel via Satellite » (DVB-RCS) aujourd'hui remplacé par sa nouvelle version DVB-RCS2. Ces protocoles sont des héritages de la diffusion de la télévision par satellite. En effet, les différentes normes ont été adaptées pour permettre la convergence vers le tout IP à l'aide de fragmentation et d'encapsulation en ATM dans le sens montant et en MPEG2-TS dans le sens descendant.

II.2 Les Réseaux Wi-Fi

Si la possession d'une connexion à Internet à domicile a commencé à se démocratiser à la fin des années 90, les années 2000 ont vu la disparition des modems basiques au profit de boitiers plus complets. Ces « *-Box » des fournisseurs d'accès ont permis de faire entrer le Wi-Fi dans tous les foyers possédant une connexion ADSL. En effet, la connexion filaire à domicile a quasiment disparu, les téléphones intelligents et même certains ordinateurs portables ne possédant pas de prise Ethernet. Les fournisseurs d'accès proposent même d'interconnecter leurs différents appareils avec le Wi-Fi (entre Box et boîtier TV par exemple). Dans le cadre professionnel, cette technologie est omniprésente, la plupart des entreprises proposent un point d'accès chiffré pour leurs employés et souvent un deuxième point d'accès ouvert pour les invités, ce qui permet aux administrateurs réseau de définir plusieurs niveaux de sécurité.

Si à l'origine les performances de cette technologie étaient limitées, les derniers standards permettent d'atteindre des débits plus que satisfaisants. En effet, la norme 802.11 a hérité de plusieurs améliorations au fil des années dans le but d'améliorer les performances des réseaux Wi-Fi. Les différentes variations regroupées dans le Tableau 4 ne sont pas toutes de simples augmentations de débits. Les réseaux Wi-Fi étant soumis à des nombreuses perturbations et leurs utilisations étant très variées, certaines normes introduisent de nouveaux services comme le chiffrement des communications, la Qualité de Service ou encore l'itinérance. Ces différents services sont nés du besoin des utilisateurs et certains sont présents dans les normes récentes. Au vu des performances prometteuses de la norme 802.11n, il est clair que la seule limite restante des réseaux Wi-Fi est leur zone de couverture restreinte qui dépend de plusieurs facteurs :

- La puissance d'émission du point d'accès,
- Les antennes utilisées : taille, forme, fonctionnalités, …
- L'environnement : obstacles, interférences, …
- Les protocoles de routage utilisés

Tableau 4 –Différentes versions du Wi-Fi et leurs caractéristiques

Norme	Fréquence	Débit théorique	Particularité
802.11a	5GHz	54Mbps	--
802.11b	2,4GHz	11Mbps	Portée de 300m théorique
802.11e	--	--	Ajout Qualité de Service
802.11f	--	--	Ajout de l'itinérance
802.11g	2,4GHZ	54Mbps	Compatible 802.11b
802.11n **802.11i**	2,4Ghz et/ou 5GHz --	300Mbps --	Possibilité de combiner des canaux Ajout du chiffrement AES

La puissance d'émission d'un nœud est limitée par la réglementation française à 100mW même si certains logiciels permettent de l'augmenter au delà de ces limites ; des « firmwares » ou micro programmes ouverts pour points d'accès Wi-Fi laissent libre à l'administrateur la gestion de cette puissance (voir Openwrt ([15] ou DD-WRT [16]).

L'antenne utilisée pour émettre le signal a un impact majeur sur la puissance du signal reçu et la zone de couverture. Il est possible d'en distinguer deux types : omnidirectionnelles et directionnelles. Les premières sont présentes dans la majorité des appareils et diffusent le signal dans toutes les directions. Les secondes sont plus rares et permettent de cibler et concentrer la diffusion du signal. Différents modèles existent, par exemple les antennes tubulaires dites « shotguns » permettant de viser un endroit fixe ou les antennes sélectives permettant de choisir une direction dynamiquement et éviter les interférences inutiles. La Figure 8 illustre l'utilisation d'une antenne tubulaire. En orientant l'antenne, le signal est envoyé uniquement vers le nœud récepteur. Le nœud tiers est alors libre de communiquer sur la même fréquence avec d'autres nœuds. Les études menées sur les antennes directionnelles sont nombreuses et ont différents objectifs : amélioration de la capacité du réseau, meilleur support de la mobilité ou encore découverte de la position des nœuds voisins. Par exemple, l'étude menée dans [17] vise à démontrer le potentiel des antennes directionnelles dans un réseau multi-bonds. Il est démontré qu'il est possible d'améliorer la qualité du signal reçu tout en maintenant constante la puissance totale émise par l'ensemble des nœuds du réseau.

Au contraire des réseaux filaires, les réseaux sans-fil ont besoin de protocoles de routage réactifs et si possible dynamiques. Les réseaux mobiles « Mobile Area Networks » (MANETs) et surtout les réseaux véhiculaires « Vehicular Ad-Hoc Networks » (VANETs) sont en constante évolution : la mobilité des nœuds qui les composent résulte dans une permanente modification des liens possibles entre nœuds. La détermination de ces liens ainsi que la mise en place de routes avec plusieurs bonds

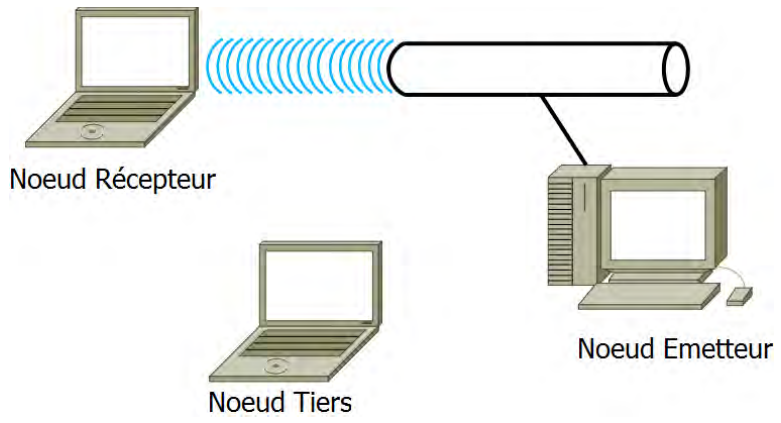


Figure 8 – Exemple d'utilisation d'une antenne directive de type dit « shotgun », seul le nœud récepteur perçoit la communication.

ou « multi-hops » est une problématique adressée par de nombreuses études. Dans [18], les auteurs proposent une technique de routage basée sur la prédiction du mouvement des nœuds dans un réseau véhiculaire appelée « Movement Prediction-based Routing Protocol » (MOPR). En prenant en compte la position des nœuds et leur mouvement, le protocole cherche à déterminer la route la plus « stable » c.à.d. la route qui restera active le plus longtemps. La comparaison avec le protocole de routage « Ad-Hoc On-Demand Distance Vector » (AODV) montre que si MOPR permet d'obtenir une augmentation de la bande passante dans le réseau et de limiter les erreurs de liens, la communication de la position aux nœuds voisins ajoute 20% d'utilisation de bande passante.

II.3 Les Réseaux de téléphonie mobile

Depuis la démocratisation de la téléphonie mobile à la fin des années 90, les appareils mobiles ont évolués pour proposer plus que le simple service d'appel. La miniaturisation ayant permis aux téléphones de devenir des ordinateurs de poche, les réseaux cellulaires permettent l'accès à des services à ceux accessibles à domicile via un équipement fixe. Nous ne détaillerons pas ici la première génération (1G) de téléphonie mobile qui était analogique, encombrante et qui a disparu en 2000.

La seconde génération (2G) marque le passage de l'analogique au numérique avec le « Global System for Mobile Communications » (GSM). Il était alors possible de transmettre des données autre que la voix : le protocole « Wireless Application Protocol » (WAP) pour accéder à Internet, l'envoi de messages textes « Short Message Service » (SMS) et même de messages multimédia «Multimédia Messaging Service » (MMS) contenant des photographies, des enregistrements audio ou vidéo. Néanmoins, le faible débit proposé (9,05kb/s) limite fortement les possibilités d'utilisation. Le développement de réseaux de téléphonie proposant une meilleure connexion fut alors nécessaire. La norme « General Packet Radio Service » (GPRS) est une extension du GSM pour la transmission de paquets et permet de fournir une connectivité IP. Cette norme se situe entre la seconde génération et la troisième génération, elle est donc souvent appelée 2,5G.

La troisième génération de téléphonie mobile (3G) est définit par la norme « Universal Mobile Telecommunications System » (UMTS) qui permet d'atteindre des débits bien supérieurs (2Mbps en théorie). Contrairement au GPRS qui utilisait les mêmes antennes que le GSM, l'UMTS n'est pas compatible et le coût relatif au déploiement d'antennes a freiné certains opérateurs à l'étranger, ceux-ci préférant passer directement aux réseaux de quatrième génération (4G). La France peut être considérée comme une exception, les opérateurs ayant opté pour la 3G dans les années 2000, la 4G est installée moins rapidement.

Les réseaux « Long Term Evolution Advanced» (LTE-Advanced) sont considérés comme les réseaux mobiles 4G et devraient permettre un débit de 1Gbps à l'arrêt est de 100Mbps en mouvement. Les implémentations de ces réseaux sont en cours et les téléphones les plus récents sont compatibles.

Les réseaux de téléphonie étant conçus pour supporter la mobilité, nous allons surtout traiter dans cette partie leurs performances et leur capacité à fournir des services de QdS. Les descriptions faites dans cette partie étant tirées des normes, il est plus difficile de savoir ce qui est réellement implémenté, les opérateurs installant leur propre infrastructure. La seule information disponible sur les réseaux déployés est la couverture, qui ne révèle ni les débits réellement atteignables ni les services disponibles.

II.3.1 Le GPRS

La norme GPRS est l'amélioration du GSM pour permettre la transmission de paquets. Comme pour tout réseau d'accès, les données qui sont amenées à y circuler possèdent des caractéristiques et des

contraintes différentes. La norme GPRS doit donc être en mesure d'apprendre les caractéristiques de ces flux et de respecter leurs contraintes. Les besoins des applications des abonnés sont déterminés lors de l'utilisation du service. Le terminal de l'utilisateur communique à l'entité en charge du réseau un profil de QdS souhaité. Le serveur répond alors avec un profil adapté à la disponibilité du réseau. Les types de trafic sont triés en classes suivant plusieurs critères :

- Classes de priorité : haute, normale ou basse,
- Classes de fiabilité de la transmission : dépendant des probabilités de pertes, de duplication, de l'ordre d'arrivée et de corruption des paquets,
- Classes de délai : garantissant un délai moyen suivant le service utilisé,
- Classes de débit : limité en moyenne (octets par heure) ou limité en pointe maximale (octets par seconde).

La prise en compte en compte des interférences présentes sur le réseau (obstacles, autres terminaux,….) permet la définition de profils précis répondant aux contraintes des applications dans la mesure du possible. Une fois le profil déterminé, le serveur d'accès peut alors allouer la bande passante aux différents utilisateurs en assignant un nombre d'intervalles temporels. Si le réseau est en surcharge, certains intervalles peuvent être partagés entre utilisateurs à condition que leurs demandes le permettent. Inversement, un seul abonné peut obtenir jusqu'à 8 slots. La bande passante disponible est alors définie en fonction du schéma de codage utilisé, soit pour 1 slot et 8 slots :

- CS1: 9.05kb/s/72kb/s,
- CS2: 13.6kb/s/108.8kb/s,
- CS3: 15.7kb/s/125.6kb/s,
- CS4: 21.4kb/s/171.2kb/s.

Le choix se fait en fonction notamment des conditions météorologiques, les débits les plus faibles permettant des taux de pertes moins élevés. En général, le schéma de codage est établi par le gérant du réseau et les terminaux doivent s'adapter.

Le principal avantage du GPRS est sa grande disponibilité, partout en France et avec un signal très fort en zone urbaine. Mais les différents services ainsi que le coût sont déterminés par le fournisseur et dépendent du contrat établi. Pour pouvoir établir une QoS sur GPRS, il faut donc se renseigner sur ce qui est implémenté sur le réseau, ce qui peut être utilisé et à quel prix.

II.3.2 La 3G

L'organisme 3GPP (3rd Generation Partnership Project) visait à standardiser la 3° génération de téléphonie mobile. La spécification technique 23.107 [19] traite des concepts et de l'architecture QoS. La technologie utilisée est UMTS (Universal Mobile Telecommunications System) qui est un dérivé de W-CDMA (Wideband Code Division Multiple Access).

Les « UMTS Bearer Services » sont définis pour l'accès au support radio et le réseau de cœur, ils ne prennent pas en compte l'architecture des terminaux. Les paquets sont triés dans 4 classes correspondant à 4 besoins différents:

- Conversation: délai et gigue faible (voix, VoIP,…),
- Streaming Vidéo: gigue faible (Streaming Vidéo),
- Interactif: transfert de données (WebBrowsing requête/réponse),
- Background: transfert de données sans limitation dans le temps (télémétrie, emails).

Les attributs des différents services donnés aux applications sont nombreux, débit maximum et débit garanti, SDU maximum, ordre d'arrivée respecté ou non… Comme pour le GPRS, les attributs des différents services permettent d'avoir une définition précise pour le fournisseur sur le type de trafic et pour l'utilisateur sur le comportement que va avoir la connexion.

II.3.3 La 3G+

Basé sur la technologie HSDPA (High Speed Downlink Packet Access), ce protocole pour la téléphonie mobile est censé offrir des performances 10 fois supérieures à la 3G.

Il s'agit d'une amélioration du lien descendant par rapport à UMTS, le DCH (Dedicated CHannel) qui était utilisé par un seul utilisateur est maintenant partagé. Les voies montantes et descendantes utilisent des nouveaux canaux physiques: UHS-DPCCH (Uplink High Speed Dedicated Physical Control CHannel) et HS-PDSCH (High Speed Physical Downlink Shared Channel). Les canaux de transport définissent dans le sens descendant sont: HS-DSCH (High Speed Dedicated Shared CHannel) pour la transmission des données et HS-SCCH (Shared Control CHannel) pour la signalisation. L'architecture QoS de HSDPA reprend les services définis dans UMTS, en ciblant particulièrement le streaming, l'interactif et le background.

II.3.4 La 4G

La 4° génération de réseau cellulaire est celle qui doit permettre d'atteindre le très haut débit et permettre l'utilisation de nouvelles applications. La différence majeure par rapport aux générations précédentes est la disparition du mode commuté pour les appels, ceux-ci reposant uniquement sur la voix sur IP. Le rapport [20] publié par l'ITU-R définit les pré-requis pour qu'un système soit « International Mobile Telecommunications-Advanced » (IMT-Advanced). Par exemple, les temps d'interruptions lors d'un changement de station de base sont définis : 27.5ms lorsque le changement intervient dans la même fréquence et 40ms lorsque le changement se passe entre 2 fréquences différentes (60ms si la bande spectrale diffère aussi). Deux technologies sont actuellement déployées et commercialisées : « Mobile Wimax » (IEEE802.16e) et « Long Term Evolution » (LTE). Elles sont tous les deux estampillés 4G même si les performances qu'elles proposent restent en-dessous des recommandations de l'ITU-R qui sont 1Gb/s en position stationnaire et 100Mb/s à haute vitesse. Mobile Wimax et LTE atteignent respectivement 128Mb/s et 100Mb/s sur le lien descendant. Une amélioration du réseau LTE appelée LTE-Advanced permet d'atteindre 300Mb/s.

III La mobilité au niveau Réseau

Dans cette section, nous allons voir des mécanismes permettant de gérer la mobilité de bout-en-bout ainsi que certains concepts permettant de les améliorer. La terminologie relative à la mobilité est dense et une grande partie de ce vocabulaire est défini dans un document de l'IETF à caractère informatif [26]. Les termes et acronymes relatifs à la mobilité utilisés dans cette section et par la suite de cette thèse sont issus de ce document.

Avec la croissance du nombre de nœuds sur Internet, l' « Internet Protocol » (IP) évolue vers sa nouvelle version IPv6 qui permet la gestion d'une plus grande quantité d'adresses IP. Comme la mobilité n'était pas incluse dans IPv4, de nombreux travaux sur la mobilité se sont tournés vers IPv6, ce qui laisse penser que la gestion de la mobilité est incluse dans le déploiement d'IPv6. Nous ne présenterons donc pas ici la mobilité avec IPv4 mais directement avec IPv6.

III.1 Mobile IPv6

Mobile IPv6 (MIPv6) est un ensemble de mécanismes et de recommandations permettant la mobilité d'un nœud. La première définition date de 2004 [21], elle a été rendue obsolète en 2011 par [22]. Ces documents décrivent trois entités : le terminal mobile ou « Mobile Node » (MN), l'agent mère ou « Home Agent » (HA) en charge de rediriger les paquets à destination du MN (et le localiser si nécessaire) et le terminal correspondant ou « Correspondent Node » (CN) en communication avec le MN. Ces trois entités vont pouvoir appartenir à trois réseaux et sont mis en scène dans la Figure 9 :

- Le réseau mère ou réseau de domicile : réseau d'origine du MN,
- Le réseau correspondant contenant le CN,
- Les réseaux visités ou réseaux extérieurs : réseaux temporaires dans lequel le MN se déplace.

Une adresse mère permanente HoA (Home Address) est attribuée au MN afin qu'il soit toujours joignable. Lorsqu'il visite un réseau, il se voit attribué une adresse temporaire CoA (Care-of Address). Lors de son arrivée dans un réseau visité, le MN va solliciter le routeur pour récupérer une CoA et

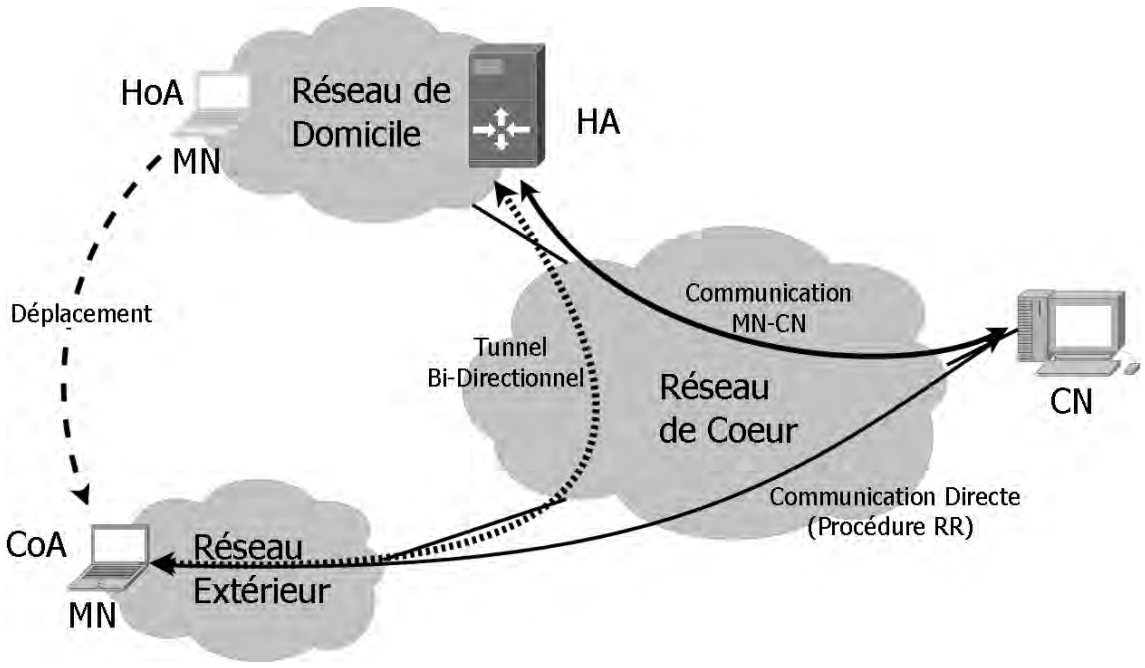


Figure 9 – Exemple d'utilisation de Mobile IPv6 : un Nœud Mobile (MN) change de point d'accès en gardant active la connexion avec le Nœud Correspondant (CN).

utiliser le mécanisme d'auto-configuration IPv6. Le terminal va ensuite enregistrer sa CoA auprès de son HA avec les messages BU/BA « Binding Update / Binding Acknowledgement ». Le HA va alors pouvoir transmettre les paquets à destination du MN. Pour le CN, ce changement de réseau est transparent, un tunnel bidirectionnel étant mis en place entre le HA et le MN. Le délai de communication est alors important puisque tout le trafic est obligé de transiter par le réseau mère.

Une amélioration importante de mobile IPv6 est la possibilité qui est donnée au MN de signaler au CN le changement d'adresse temporaire. Le terminal mobile va alors envoyer les messages BU/BACK directement au CN. La communication va alors se faire directement entre le MN et le CN sans passer par le HA, évitant de surcharger le réseau mère et permettant d'améliorer les performances de la communication. Pour des questions de sécurité, une procédure RRT (Return Routability Test) a aussi été ajoutée afin qu'un terminal tiers ne puisse prendre la main dans la connexion en se faisant passer pour le MN. D'autres améliorations proposent un échange de clefs, ce qui est plus performant et permet l'établissement d'un tunnel directionnel directement entre le MN et le CN.

Néanmoins, une latence est toujours présente lors du changement de réseau et peut entrainer des pertes de paquets, ce qui est pénalisant surtout pour les applications temps réel. Les principales causes sont:

- Le délai de connexion de niveau 2 (changement de point d'accès et association),
- La configuration de la nouvelle CoA,
- Les échanges BU/BACK avec le HA ou le CN.

Un autre point sensible de cette solution est le HA, la centralisation de la gestion de l'itinérance en un seul point résulte dans des interruptions de communication en cas de dysfonctionnement et des problèmes de congestion suivant le nombre de MN associés avec le HA.

III.2 Fast Mobility IPv6

L'amélioration de mobile IPv6 nommée FMIPv6 (Fast Mobility IPv6) [23] propose de réduire le délai du changement de réseau en améliorant le temps de détection du mouvement du MN et le temps d'enregistrement de la CoA. FMIPv6 introduit pour cela de nouveaux mécanismes :

- Configuration d'une adresse IPv6 pour le prochain réseau avant le déplacement,
- Envoi des paquets dès que le nouveau lien est détecté,
- Réception des paquets dès que le nouveau routeur a détecté l'attachement.

Ces mécanismes sont compatibles avec MIPv6 et d'autres protocoles gérant la mobilité IPv6. Le meilleur cas sera la réduction du temps d'interruption à la valeur du temps nécessaire à la réassociation de niveau 2. De nouveaux éléments sont aussi définis, le PAR (Previous Access Router) et le NAR (New Access Router) sont les routeurs d'accès avant et après la procédure de handover. Le MN va posséder deux adresses temporaires, la PCoA (Previous CoA) et la NCoA (New CoA) correspondant aux adresses temporaires fournies par le PAR et le NAR. Tout en restant connecté au PAR, le MN va pouvoir lui demander des informations sur les points d'accès qu'il détecte en indiquant leurs identifiants. Avec la réponse de son PAR, le MN est alors capable de se connecter au NAR grâce à sa NCoA. Suivant sa configuration en mode prédictif ou réactif, le MN peut anticiper la déconnexion ou attendre celle-ci avant de s'associer avec le NAR. Le changement de réseau peut aussi être géré par le réseau, le PAR envoie un message non-sollicité au MN en lui spécifiant les paramètres nécessaires à la création d'une NCoA pour le NAR.

III.3 Hierarchical Mobile IPv6

Les mécanismes de MIPv6 se révèlent peu efficaces lorsque le déplacement du MN se fait à l'intérieur d'un domaine, surtout si la distance de déplacement est faible en comparaison avec les distances MN/HA et MN/CN. Chaque déplacement nécessite l'échange de messages entre le MN et son HA, ce qui peut résulter dans une charge du réseau et une latence due à la distance du réseau mère par rapport à la distance entre les deux réseaux visités.

Hierarchical Mobile IPv6 [23] a été proposée pour optimiser les déplacements à l'intérieur d'un domaine en ayant une gestion plus hiérarchique de la mobilité. Le protocole propose l'utilisation d'une nouvelle entité : le MAP (Mobility Anchor Point), qui gère la mobilité dans son domaine. Il est utilisé comme un « agent mère local » : si le MN se déplace en restant dans le domaine géré par le MAP, la signalisation concernant la mobilité se fait uniquement dans le domaine et est transparente pour le HA et le CN. Pour cela, HMIPv6 définit deux nouvelles adresses temporaires : la Regional CoA allouée par le MAP et la Local CoA allouée par le routeur d'accès courant auquel le MN est rattaché. Le MN prévient alors le nouveau MAP de l'association avec un message LBU (Local Binding Update), puis prévient aussi son HA et éventuellement son CN avec un BU/BA contenant la LCoA.

Cette solution est intéressante, mais il faut prendre en compte que l'utilisation d'une adresse locale oblige l'encapsulation des paquets entre le MAP et le MN, ce qui peut être pénalisant suivant le support sans fil utilisé. Tout comme pour FMIPv6, HMIPv6 est compatible avec MIPv6, et le MN peut choisir de l'utiliser ou pas. De plus HMIPv6 peut être utilisé sans HA, les différents routeurs MAP serviront alors de HA successifs.

Si HMIPv6 est avantageux pour des déplacements dans un même domaine, les déplacements inter-domaines génèrent un échange supplémentaire de LBU/BACK entre le MN et le MAP. Pour éviter cela, il est possible d'envoyer la nouvelle LCoA dans un LBU vers l'ancien MAP, celui-ci pourra alors transmettre les paquets vers la nouvelle destination. Ce principe rejoint le fonctionnement de FMIPv6, ce qui a conduit à des propositions combinant les deux solutions. Une proposition a été formulée dans [25] mais reste sous la forme « Draft ». Connue sous le nom de F-HMIPv6, cette combinaison propose la mise en place d'un tunnel de plusieurs manières :

- Entre le PAR et le NAR ce qui entraine un double passage par le lien PAR-NAR,
- Entre le MAP et le NAR.

La deuxième solution est la plus intéressante et permet de tirer parti des deux protocoles. Dans un même domaine, les associations ne sont mises à jour qu'avec le MAP et en déplacement inter-domaines le passage PAR/NAR va éviter le double échange de LBU.

III.4 La multi-domiciliation et Mobile IPv6

Comme expliqué brièvement dans le Chapitre II, section I.2, la multi-domiciliation peut améliorer la mobilité d'un nœud en facilitant le « Make Before Break ». Le document [30] définit les règles et mécanismes indispensables à l'utilisation de plusieurs interfaces réseaux avec mobile IPv6. Ce document reprend les règles définies par MIPv6 mais au lieu de déclarer une seule adresse IP CoA à son « Home Agent », le nœud mobile envoie un BU avec une liste de ses adresses IP actives, ce sont les « multiple Care-of-Addresses » (mCoA). Le nœud mobile et son HA s'accordent sur l'adresse à utiliser en priorité et l'interface correspondante est alors dédiée aux communications. Néanmoins, si les échanges d'adresses sont définis, aucune précision n'est faite sur la détermination du chemin à utiliser c.à.d. l'interface réseau à utiliser pour communiquer. Cette faille dans les définitions peut mener à un mauvais fonctionnement dépendant de l'implémentation si le chemin optimal n'est pas sélectionné en priorité.

Une étude des performances d'une application multimédia sur mCoA est faite dans [31]. Trois cas sont choisis MIPv6 classique, mCoA avec une interface choisie aléatoirement pour communiquer et mCoA avec plusieurs interfaces. Les simulations sont faites pour un nœud bougeant à 3km/h puis 30km/h et les paramètres analysés sont le « Mean Opinion Score » (MOS) de VoIP et les taux de pertes. Il est démontré que mCoA peut améliorer les performances, notamment en diminuant les pertes à haute vitesse. De plus, l'utilisation simultanée de plusieurs interfaces permet de diminuer encore le taux de pertes. Ces deux résultats étaient attendus ; ils permettent de soutenir l'intérêt croissant des chercheurs pour la multi-domiciliation.

Dans un contexte mobile, la bande passante offerte par un point d'accès varie suivant la distance entre le nœud mobile et la borne. En effet, pour pallier aux erreurs de transmission dues aux perturbations, plus la distance entre nœuds est importante, plus le codage utilisé est fort réduisant ainsi le débit maximal atteignable. Il est donc nécessaire de choisir le point d'accès en fonction des performances et pas seulement de changer de réseau en sortant de la zone de couverture. Ce cas est étudié dans [32], où il est montré par la simulation que choisir le lien en fonction de la bande passante permet d'obtenir un meilleur débit global et aussi moins de variations dans le débit. Effectivement, en ne communiquant pas en « bordure » de zone de couverture, le débit minimal est plus élevé.

La gestion de la mobilité par MIPv6 présentant certaines lacunes, ses extensions FMIPv6 ou HMIPv6 sont souvent implémentées car elles proposent de meilleures performances. Les améliorations à MIPv6 sont donc souvent conçues de manière à être compatibles avec les extensions d'IPv6. Néanmoins, il arrive que le comportement particulier de ces extensions revienne à dégrader les performances des communications. Avec FMIPv6, l'utilisation de plusieurs interfaces réseau couplée avec l'établissement du tunnel entre le nœud mobile et le NAR provoque de nombreuses réceptions désordonnées. L'article [33] propose de nouveaux mécanismes permettant de supprimer cette dégradation en spécifiant l'interface réseau utilisée pour établir le tunnel.

Les possibilités introduites par la multi-domiciliation sont nombreuses et ne se limitent pas à faciliter la mobilité. La multi-domiciliation permet aussi la mise en place de nouveaux mécanismes. Le document [34] définit des mécanismes permettant de lier un flux à une interface réseau particulière et introduit de nouvelles opportunités :

- Grouper les flux avec des contraintes identiques sur les technologies adaptées,
- Limiter les changements de réseau non obligatoires pour les flux critiques,
- Améliorer les performances de certains flux en les privilégiant (mise à disposition d'une interface pour un seul flux).

Les objectifs visés avec ces mécanismes concernent la QdS mais diffèrent légèrement entre eux. Ils correspondent à proposer différents niveaux de QdS directement liés aux chemins disponibles ou encore à éviter l'introduction de latences inutiles pouvant impacter les flux critiques. La définition de la QdS va dépendre du nombre d'interfaces réseaux et des technologies de communication disponibles : par exemple le Wi-Fi pour les applications demandeuses en débit ou le satellite pour les applications nécessitant une connexion permanente. Il a été vu dans les parties précédentes qu'un changement de réseau peut provoquer de nombreux événements. Il peut être judicieux de ne pas soumettre une application critique à un changement brutal des caractéristiques du réseau tout en permettant aux applications non-critiques d'augmenter leur débit en les basculant temporairement sur un autre réseau proposant une bande passante plus large. Enfin, privilégier certains flux revient à établir une politique d'accès au réseau : en limitant le nombre de flux suivant les connexions disponibles, il est possible de « réserver » une certaine quantité de bande passante voire une interface

complète pour un flux particulier. Nous reviendrons sur une implémentation de « Flow Binding » dans la partie suivante qui traite de la mobilité des réseaux.

IV Le support des réseaux mobiles

Les solutions présentées précédemment proposent des réponses aux problématiques présentées dans le Chapitre II, section I.1 pour un nœud mobile seul. Néanmoins, ces solutions ne permettent pas la mobilité d'un réseau entier : il est nécessaire pour cela de mettre en place des mécanismes supplémentaires. En 2002, la démocratisation des réseaux sans-fil et le développement des appareils mobiles ont poussé l'Internet Engineering Task Force (IETF) à ouvrir le groupe de travail Network Mobility (NEMO). Son objectif est la gestion de la mobilité d'un réseau entier et la gestion de l'accessibilité de ce réseau. Le vocabulaire relatif à NEMO utilisé ici et dans la suite de cette thèse est issu du document à caractère informatif [35] qui définit la terminologie à employer, nous en présentons les termes les plus courants dans cette section.

IV.1 NEtwork Mobility (NEMO)

Défini en 2005 dans [36], NEMO repose sur des mécanismes similaires à MIPv6 et permet la mobilité d'un réseau avec IPv6. L'utilisation de techniques proches a deux avantages majeurs: il est possible de s'inspirer des avancées faites pour la mobilité des nœuds simples et la démocratisation des solutions est facilitée (déploiement, implémentation, …). Plusieurs propositions d'extensions à NEMO sont des adaptations des extensions de MIPv6. La Figure 10 présente un réseau comportant des entités similaires à celles introduites dans le Chapitre II, section III.1Chapitre IIIII.1 pour MIPv6 et adaptées pour la mobilité d'un réseau :

- « Mobile Router » (MR): Routeur mobile offrant une connexion entre le réseau mobile et le réseau de cœur,
- « Local Mobile Node » (LMN): Nœud connecté au MR pouvant changer de réseau d'accès,
- « Local Fixed Node » (LFN): Nœud connecté au MR ne pouvant changer de point d'accès,
- « Home Agent » : Entité gérant l'accessibilité du routeur mobile,
- « Correspondent Node » : Nœud communicant avec un des nœuds locaux, qu'il soit fixe ou mobile.

Il est à noter que les nœuds fixes sont distingués des nœuds mobiles dans la terminologie. De plus, il est possible pour un nœud mobile d'être lui-même routeur mobile, on va alors parler de « sub-NEMO » et de « parent –NEMO » pour respectivement le réseau fils et le réseau père. L'ensemble de

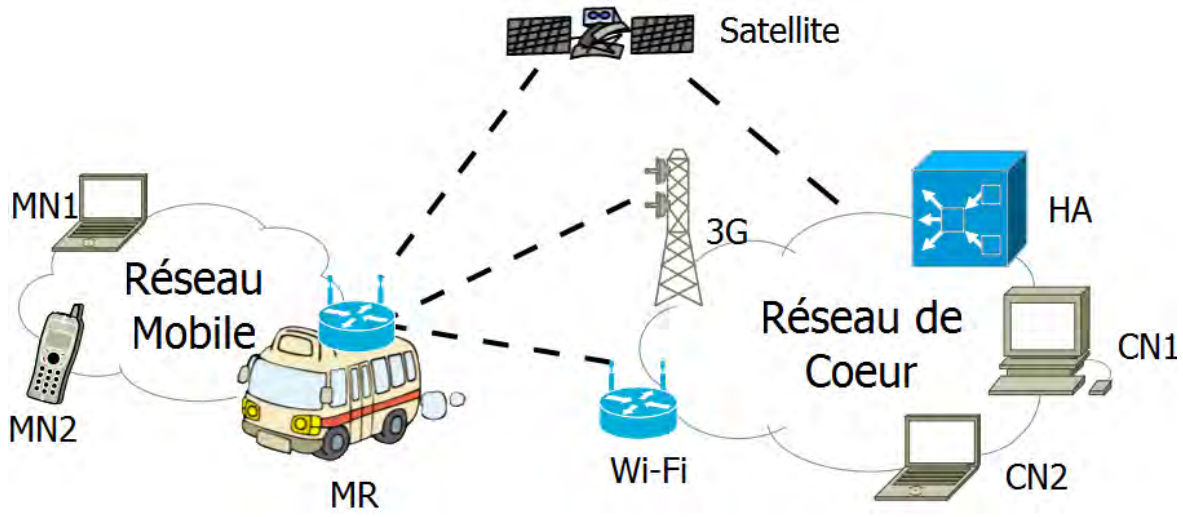


Figure 10 – Exemple d'un réseau comportant les entités définies par NEMO : le réseau mobile est connecté à des points d'accès via le routeur mobile (MR).

ces deux réseaux est alors dit imbriqué, ou « Nested-NEMO ».

Afin de permettre la mobilité du réseau et surtout son accessibilité, le HA est informé de l'adresse utilisée par le routeur pour se connecter au point d'accès (AP) via un « Binding Update » (BU). Une fois la réception confirmée avec un « Binding Acknowlegdement » (BA), le HA met en place une route vers le MR et ce tunnel sera utilisé pour toute communication entrante ou sortante du réseau mobile. Le routeur mobile peut aussi inclure dans le BU son (ou ses) préfixe(s) d'adresse IP ou « Mobile Network Prefix » (MNP).

En 2005, des chercheurs ont utilisé le réseau déployé pour une réunion du projet « Widely Integrated Distributed Environment » (WIDE) [39] pour tester NEMO. Le réseau mobile était symbolisé par un routeur Wi-Fi situé derrière plusieurs points d'accès et auquel les participants de la réunion pouvaient se connecter. La mobilité du réseau était provoquée par le routeur qui changeait régulièrement de point d'accès. Le nombre élevé de participants (presque 250) a permis l'obtention de résultats pertinents sans le problème de mise à l'échelle de nombreuses expérimentations. Les résultats exposés dans [40] sont assez succincts mais permettent de mettre en avant un inconvénient majeur de NEMO : lors du changement de réseau, les nœuds du réseau sont incapables de communiquer pendant une durée relativement longue. Par contre, ce phénomène n'affecte pas les flux émis par le routeur mobile qui est régi par MIPv6 dans sa version basique (voir la suite de cette section pour un autre exemple). Afin d'améliorer les performances, les auteurs proposent l'utilisation de l'extension mCoA pour NEMO.

Une étude de performances sur NEMO est aussi menée dans [37] ; les auteurs se basent sur une plateforme comprenant trois points d'accès 802.11b et un nœud émulant Internet. Les mesures effectuées permettent de déterminer plusieurs points faibles de NEMO qui sont induits par les changements de réseau:

- Le délai nécessaire au changement de réseau est élevé (supérieur à 2s) et n'est pas conforme aux exigences d'applications critiques comme la Voix-sur-IP,
- L'utilisation supplémentaire de la bande passante induite par NEMO lors d'un changement de réseau peut conduire à une dégradation des performances.

Le délai introduit par le changement de réseau est un problème qui peut être en partie résolu avec les extensions FMIPv6 et HMIPv6. Néanmoins, l'utilisation d'une seule interface réseau oblige une rupture temporaire de la connexion. Afin d'éliminer cette latence et de ne pas rompre la connexion, les auteurs suggèrent l'utilisation de plusieurs interfaces réseaux et ainsi réaliser un changement de réseau en MBB (« Make Before Break »). La section suivante porte sur l'utilisation de routeurs mobiles multi-domiciliés.

L'utilisation supplémentaire de la bande passante par NEMO dépend de sa configuration et du contexte. La version de base de NEMO oblige les flux provenant du réseau à utiliser le tunnel entre le routeur mobile et son agent tandis les flux émis par le routeur sont régis par les règles de MIPv6 et n'ont pas à utiliser le tunnel. Lorsque la connexion est stable, les paquets provenant du routeur sont encapsulés et une sur-utilisation de la bande passante existe. En contrepartie, un changement de réseau va induire moins d'échange d'information car seul le tunnel routeur-agent est modifié. Il est possible « d'inverser » la situation en autorisant des connexions directes entre les nœuds du réseau mobile et leurs nœuds correspondants. Afin d'obtenir les meilleures performances dans les deux cas, la configuration suivante est utilisée dans le réseau mobile : les nœuds fixes (LFN) utilisent le tunnel et les nœuds mobiles (LMN) peuvent communiquer directement avec leurs nœuds correspondants en se servant de leurs propres solutions de mobilité pour établir les routes.

IV.2 NEMO et la multi-domiciliation

Le Chapitre II, section III.4 présente les améliorations relatives à la multi-domiciliation dans MIPv6 qui permettent d'utiliser les multiples interfaces réseaux d'un nœud mobile. Au vu de la dégradation de performances lors du changement de point d'accès avec un routeur mobile, des chercheurs ont suggéré d'ajouter le support de la multi-domiciliation à NEMO. L'extension mCoA pour MIPv6 ayant été proposée alors que le groupe de travail NEMO était encore actif, des propositions similaires ont été effectuées pour les réseaux mobiles. Un document du groupe de travail discute des différents scénarios envisageables pour la multi-domiciliation dans un réseau mobile (voir [41]). Les scénarios sont distingués suivant la configuration du réseau : nombre de réseaux d'accès, nombre de routeurs mobiles présents dans le réseau mobile et nombre de préfixes d'adresse IP définis dans le réseau mobile. Deux cas sont particulièrement intéressants pour nous :

- Cas classique : 1 Routeur, multiples interfaces réseaux, 1 préfixe.
- Cas avec sous-réseaux : 1 Routeur, multiples interfaces réseaux, multiples préfixes.

Le premier cas correspond à un réseau mobile multi-domicilié de base et correspond à la topologie étudiée dans le Chapitre III, section III. Le second cas est celui utilisé dans notre proposition du Chapitre V.

Suite à l'expérience décrite dans [40] et présentée précédemment, une expérience avec NEMO et mCoA dans des conditions réelles a été réalisée en 2006 lors d'une conférence du projet WIDE [39]. Les mesures effectuées sont présentées dans [42] et comparées à celles faites l'année précédente sur un réseau NEMO mono-domicilié [40] (détaillée dans IV.1). La mobilité dans ce contexte n'est pas réelle mais elle est « simulée » en changeant le point d'accès utilisé par le routeur. Les conclusions de cette expérience sont prévisibles : l'utilisation de plusieurs interfaces réseaux permet de réduire le délai nécessaire au changement de réseau, les pertes sont limitées lors du basculement (de 30% à moins de 10%) et la Qualité d'Expérience (QdE) ne semble pas affectée par la pseudo-mobilité. Afin de déterminer la QdE, les auteurs ont demandés aux utilisateurs s'ils avaient ressenti le changement de point d'accès. Il en est ressorti que seulement 10% des participants avaient remarqué certains basculements.

Une autre expérience sur un banc de test réel a été réalisée dans [43]. Ici, les auteurs visent à comparer la version basique de NEMO avec sa version multi-domiciliée lors de la réalisation de changements de réseaux. Les résultats sont sans équivoque : la latence introduite par le changement de réseau est de 13s avec NEMO et de 75ms en utilisant la multi-domiciliation. L'impact sur les communications est donc largement moins important, le débit et l'évolution des numéros de séquence étant peu affectés.

En même temps que pour mobile IPv6, la possibilité de lier un flux à une interface est définie dans [34]. Cette fonctionnalité est encore plus intéressante dans un réseau mobile car le nombre de flux en présence est beaucoup plus élevé qu'avec un nœud mobile unique. La mise en place de mécanismes de différenciation de flux est alors plus rentable et il est possible de mettre en place une vraie politique d'admission ce qui revient à définir des services de QdS.

Une implémentation de « Flow Binding » est faite dans [43] en se basant sur une implémentation de Nemo appelée « Nemo BS Implementation for Linux » (NEPL) [46] ; NEPL est aujourd'hui remplacée par UMIP [47] qui propose une implémentation de MIPv6 et de NEMO. L'étude faite sur le « Flow Binding » permet de déterminer deux moyens pour améliorer le débit des connexions TCP : en répartissant les flux entre les interfaces actifs et en définissant un seul chemin pour la connexion (données et acquittements). La première technique se base logiquement sur des mécanismes de partage de la charge. Avec la seconde technique, les auteurs présentent une solution à une faille de la multi-domiciliation : si les accords ne sont pas bien faits entre le routeur et son agent, un flux peut emprunter un tunnel pour les données et un autre tunnel pour les acquittements. Si les deux tunnels ne possèdent

pas les mêmes caractéristiques, les performances de TCP peuvent être affectées car les paquets de données et les acquittements ne vont pas être soumis aux mêmes contraintes, ce qui peut entrainer un déséquilibre.

V Protocoles de Transport et mobilité

Les solutions présentées dans la section précédente permettent de gérer la mobilité au niveau Réseau. Les changements de réseau sont alors totalement transparents pour les applications et la couche Transport. Néanmoins, le changement de point d'accès revient à changer les caractéristiques du lien utilisé pour les communications, ce qui affecte les performances des protocoles de Transport (voir le Chapitre II, section I.1.3). Nous reviendrons sur ce point dans cette section en détaillant l'impact du changement de réseau transparent sur TCP. La plupart des solutions de mobilité intervenant au niveau de la couche Transport présentées dans cette section proposent de meilleures performances à la suite du changement des caractéristiques du réseau. De plus, le principal avantage de ces solutions est le faible besoin d'implémentation dans les réseaux d'accès. En effet, les solutions de la couche Réseau nécessitent des entités de type « Home Agents ». Il est donc nécessaire d'avoir une architecture spécifique et de choisir le fournisseur d'accès en fonction des services proposés. D'un autre côté, les solutions de la couche Transport ont seulement besoin d'être implémentées dans les terminaux. En contrepartie, il peut être nécessaire d'utiliser un protocole de Transport particulier ou une version spécifique ce qui peut rendre difficile le déploiement mais aussi l'utilisation suivant les entités traversées dans le réseau (pare-feux par exemple).

Dans cette section, deux protocoles de Transport ayant des approches différentes de la mobilité sont présentés. Transmission Control Protocol (TCP) est le protocole de Transport le plus commun et des versions adaptées à la mobilité existent. Nous décrirons la gestion de la communication de bout-en-bout qui est faite par TCP, puis nous introduirons les mécanismes permettant la mobilité qui ont été implémentés dans ces différentes versions. Nous présenterons ensuite Multipath TCP (MPTCP), un protocole de Transport basé sur TCP et permettant la multi-domiciliation.

V.1 Le protocole TCP et ses variantes pour la mobilité

TCP a été développé dans les années 1970 et la définition de son standard date de 1981 [45]. Malgré son âge, il reste aujourd'hui le protocole de Transport le plus utilisé. Il offre des services de fiabilité, de livraison ordonnée, de gestion du flux et de prévention de la congestion. De nombreuses versions sont apparues avec l'évolution des réseaux et de leur utilisation : certaines spécifiques à des contextes précis sont restées peu utilisées alors que d'autres ont apporté des mécanismes aujourd'hui indispensables comme par exemple les acquittements sélectifs. Les sous-sections suivantes présentent d'un part la prévention de la congestion et le contrôle du flux avec TCP et d'autre part des versions de TCP qui facilitent le changement de réseau.

V.1.1 Prévention de la congestion et contrôle du flux

Dans un réseau, la prévention de la congestion et le contrôle du flux sont indispensables. TCP est d'ailleurs né du besoin de « contrôler » les communications afin de garantir une utilisation équitable de la bande passante entre les flux, limiter les débordements des files d'attente et ainsi éviter des pertes et retransmissions inutiles. Un protocole de Transport utilisant équitablement la bande passante est d'ailleurs dit « TCP-Friendly » s'il n'est pas plus agressif que ne le serait une connexion TCP. Afin d'obtenir un respect mutuel entre les protocoles de Transport, il est demandé que tous soient « TCP-Friendly ».

Les réactions du protocole face aux événements réseaux ont évolué avec les versions de TCP mais le mécanisme principal reste identique : l'utilisation d'une « fenêtre de congestion » qui correspond à la quantité de données en vol (données envoyées mais pas acquittées pour l'instant). Les différents

algorithmes régissant cette fenêtre sont définis dans [48] pour les mécanismes basiques, puis dans les extensions pour les améliorations:

- « Threshold » : Seuil déterminant le passage d'un algorithme vers un autre. Mis à jour en cas de reprise à la moitié de la dernière bonne valeur de la fenêtre,
- « Slow Start » : utilisé lorsque la fenêtre est inférieure au « threshold ». La fenêtre est augmentée d'au plus un « Sender Maximal Segment Size » (SMSS) à chaque réception d'acquittement.
- « Congestion Avoidance » : utilisé lorsque la fenêtre est supérieure au « threshold ». La fenêtre est augmentée d'au plus d'un SMSS par RTT.
- « Fast Retransmit / Fast Recovery » : utilisé après la réception de 3 acquittements reportant des réceptions de données non ordonnées. Permet la retransmission des paquets reportés manquants sans délai.

Le dernier point correspond à des mécanismes introduits par TCP New Reno [49], ces trois algorithmes sont présents sur la Figure 11 qui illustre une simulation faite sous ns-2 avec TCP NewReno. Les algorithmes Slow Start et Congestion Avoidance proviennent de la version basique de TCP, ils permettent d'obtenir un équilibre entre performances et prévention de la congestion. Le Slow Start permet une croissance rapide au début de la communication jusqu'au « threshold » et, ensuite, le Congestion Avoidance garantit un accroissement plus faible mais régulier. Le seuil « threshold » entre les deux algorithmes doit être défini à une valeur très élevée en début de communication afin que l'estimation de la bande passante disponible se fasse correctement. Lorsque les algorithmes Fast Retransmit / Fast Recovery sont utilisés, la fenêtre de congestion est réduite de manière à être légèrement supérieure au seuil. Les données reportées manquantes sont retransmises en même temps

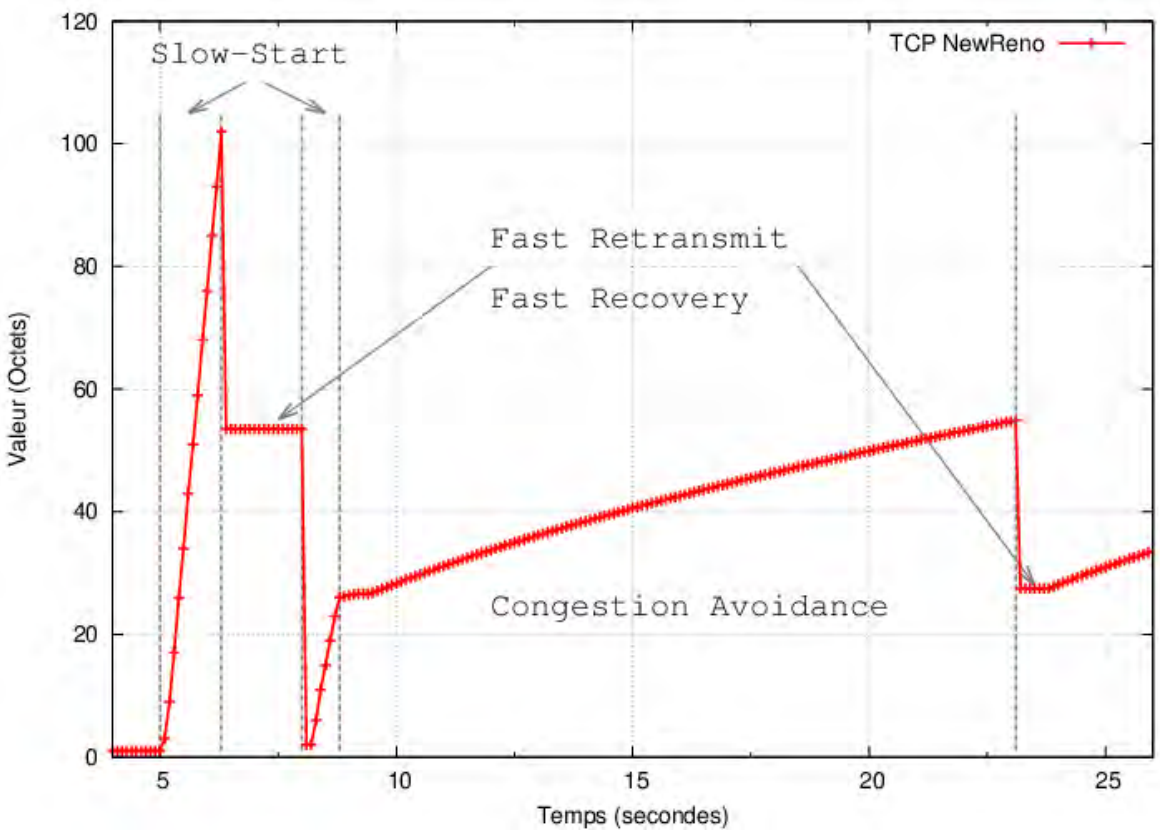


Figure 11 – Différents algorithmes utilisés par la fenêtre de congestion de TCP NewReno : Slow-Start, Congestion Avoidance et Fast Retransmit / Fast Recovery.

que de nouvelles données si la taille de la fenêtre le permet. Une fois que ces données ont été transmises correctement (réception d'acquittements les déclarant arrivées), la taille de la fenêtre est réglée égale au seuil et l'algorithme Congestion Avoidance est utilisé. L'algorithme Slow Start ne sera réutilisé que si la phase Fast Retransmit / Fast Recovery échoue. Sur la Figure 11, un échec de cet algorithme est visible à 8s (reprise à la valeur initiale) et une utilisation réussie est visible à 23s (reprise en « congestion avoidance »). Ces mécanismes permettent à la fenêtre de se stabiliser en approchant la valeur optimale dépendante de la bande passante disponible sur le lien et aussi des autres flux en présence.

Si cette gestion de la communication est efficace, il en existe d'autres adaptées à des situations particulières. Par exemple TCP Hybla [50] est une version conçue pour les communications par satellite. En modifiant la fenêtre de congestion pour que celle-ci envoie des rafales de données, Hybla permet d'obtenir de meilleures performances qu'un TCP classique sur les réseaux à faible débit et long délai que sont les réseaux de communication par satellite. Ces envois par rafale sont particulièrement efficaces pour les petites quantités de données comme les communications « HyperText Transfer Protocol » (HTTP).

Les réseaux à large bande passante sont aussi un problème pour TCP. Ce protocole a été développé pour contrôler son taux d'émission mais il a été montré que si la bande passante est suffisamment importante, TCP n'arrive pas l'utiliser correctement car la taille de la fenêtre de congestion ne grandit pas assez vite. Une approche modifiant les paramètres d'augmentation et diminution de la taille de la fenêtre a été faite dans [51] pour améliorer les performances des connexions TCP à large fenêtre de congestion. Une approche plus intéressante est faite par Compound TCP (CTCP) dans [52] et [53]. En plus des erreurs et des pertes, cette version de TCP estime le délai subi par les paquets pour réguler son taux d'émission. Pour cela, CTCP définit sa fenêtre de congestion comme étant la somme de la fenêtre de TCP classique et d'une seconde fenêtre basée sur l'observation du RTT. Pour la première, les mécanismes de New Reno sont utilisés de manière normale dans toutes les phases. En revanche, la seconde fenêtre est modifiée uniquement durant la phase de congestion avoidance. Ce comportement permet au protocole de rester « TCP-Friendly » tout en proposant une utilisation plus efficace de la bande passante. CTCP fait partie des versions de TCP déployées par Microsoft dans ses systèmes d'exploitation les plus récents comme Windows Vista, Windows 7 ou Windows Server 2008 mais est aussi disponible sur les anciennes versions. Sous Linux, l'utilisation de cette version n'est plus possible depuis le noyau 2.6.17 ce qui pourrait limiter son déploiement. De plus, même si CTCP est déployé dans des systèmes d'exploitation, son implémentation reste obscure, aucun standard n'étant disponible.

TCP CUBIC [54] utilise une approche plus « mathématique » avec une fenêtre de congestion basée sur une fonction cubique prenant pour point d'inflexion la valeur de la fenêtre de congestion avant le dernier événement de congestion. L'évolution de la fenêtre de congestion est alors divisée en deux phases : une concave avant le point d'inflexion et une convexe après. Dans la phase concave, la taille de la fenêtre de congestion augmente rapidement puis ralentit en approchant de la taille enregistrée avant le dernier événement de congestion. Dans la phase convexe, la fenêtre commence par augmenter lentement puis accélère jusqu'à provoquer un nouvel évènement de congestion. Contrairement à un TCP classique, l'évolution de la fenêtre n'est alors plus basée sur la réception d'acquittements mais sur le temps écoulé depuis le dernier événement de congestion. Cette version est incluse dans les noyaux Linux récents, TCP CUBIC peut donc être considéré comme un concurrent à Compound TCP.

V.1.2 TCP face aux changements de réseau

Dans le Chapitre II, section IChapitre III, il a été introduit que la mobilité pouvait détériorer les performances des protocoles de Transport. Le changement de point d'accès provoque deux

phénomènes pouvant entraîner une dégradation : l'apparition d'une latence durant laquelle aucune communication n'est possible et la modification des caractéristiques du réseau. Nous avons vu que la réduction de la latence était possible grâce à MIPv6 et ses extensions dans le cas d'un nœud mobile simple. Dans le cas d'un réseau mobile, l'utilisation de NEMO permet aussi de réduire cette latence, notamment si la multi-domiciliation est utilisée. Nous allons voir dans cette section que la modification des caractéristiques du réseau est un problème plus difficile à résoudre.

TCP ayant été conçu pour être utilisé sur des réseaux filaires, il ne prend pas en compte les particularités des réseaux sans fil et peut être grandement affecté par la modification des caractéristiques du chemin utilisé par la communication. La section précédente présente les différents mécanismes utilisés par TCP pour contrôler le flux et limiter la congestion afin d'améliorer ses performances. En se basant sur l'évaluation des caractéristiques du réseau et sur un historique de ces évaluations, TCP peut normalement réagir de manière optimale aux différents événements pouvant se produire au cours d'une communication. Si les caractéristiques évaluées sont modifiées brutalement, l'historique utilisé par le protocole se retrouve faussé et ses réactions sont alors inadaptées.

Une étude de l'impact de ces modifications sur les performances de TCP est réalisée dans [55]. Les auteurs se focalisent sur la réception non ordonnée de paquets et sur la modification du produit délai – bande passante ou « Bandwidth Delay Product » (BDP). Il est démontré dans cet article que ces phénomènes introduisent les mauvaises réactions suivantes de la part du protocole de Transport :

- Réception non ordonnée : envoi de rafales de segments,
- Augmentation du BDP : remplissage des mémoires au niveau du point de congestion,
- Diminution du BDP : sous utilisation de la bande passante disponible.

L'impact du changement de réseau vertical est aussi étudié dans [56] avec l'exemple des trains à haute vitesse et l'utilisation d'un réseau hybride satellite - Wi-Fi. Plusieurs versions de TCP sont simulées (NewReno, WestWood, BIC, CUBIC et Vegas) et les problèmes rencontrés sont similaires à l'étude précédente faite dans [55]. Dans ces expériences, le dépassement du RTO est la plus grande cause de dégradation des performances. Les auteurs proposent d'améliorer son évaluation après le changement de réseau en injectant le seuil « threshold » utilisé par la fenêtre de congestion et en fixant la valeur maximale de la fenêtre.

Freeze TCP [57] propose de « bloquer » la valeur de la fenêtre de congestion pendant le changement de réseau. En temps normal, les acquittements contiennent la quantité de mémoire disponible coté récepteur pour recevoir des paquets (fenêtre de réception), appelée « advertised window » (AWND). Cette valeur fixe la taille maximale de la fenêtre de congestion utilisée par l'émetteur. Avec Freeze TCP, un nœud récepteur perdant bientôt la connexion va envoyer un acquittement avec AWND = 0. Le nœud émetteur va alors rester dans un état d'attente durant lequel il n'enverra aucun paquet de données mais seulement des requêtes pour savoir si la connexion est toujours active. Les échecs de ces requêtes diminuant moins la fenêtre que des échecs de paquets de données, Freeze TCP permet de garder une taille de fenêtre plus élevée. Lorsque le nœud récepteur est prêt, il envoie simplement un acquittement avec une valeur d'AWND supérieure à 0 et la communication peut reprendre. Néanmoins, cette version de TCP ne permet pas de s'adapter rapidement aux conditions du nouveau réseau puisque les anciennes valeurs sont reprises.

Afin d'améliorer l'adaptation après le changement de réseau, « Vertical handoff Aware TCP » (VA-TCP) [58] se base sur une estimation dynamique de la bande passante et du délai dans le nouveau réseau. En utilisant la méthode « Packet-Pair » [59], VA-TCP estime le BDP du nouveau réseau. Cette méthode consiste à envoyer deux paquets à la suite et à mesurer le temps écoulé entre leurs arrivées. En se basant sur cette estimation du BDP, VA-TCP fixe des valeurs pour la fenêtre de congestion, le

seuil du Slow Start, le délai aller-retour et les compteurs de retransmission. Ainsi, VA-TCP est capable d'atteindre directement les performances optimales sans phase d'estimation et de sous utilisation du réseau.

Si les solutions présentées dans cette section permettent de réduire l'impact du changement de réseau sur les communications, elles se basent sur l'utilisation de versions spécifiques de TCP. Cet avantage peut alors se transformer en handicap sur un lien stable, sans compter la nécessité de déployer ces versions. En effet, l'utilisation de versions spécifiques nécessite leur présence dans les deux hôtes de la communication, aussi bien dans les serveurs que dans les nœuds des utilisateurs et peut alors nécessiter une installation préalable à l'établissement de la communication. De plus, les mécanismes d'intrusion utilisés (notamment l'injection de valeurs) peuvent être considérés comme passant outre les définitions des standards originels de TCP.

V.2 Multipath TCP : le TCP nouvelle génération ?

Avec l'augmentation du nombre de points d'accès et l'intégration de plusieurs technologies réseau dans les terminaux, les hôtes ont souvent la possibilité de se connecter à Internet via différents chemins. Pourtant, un protocole de Transport comme TCP ne permet pas d'en tirer parti. MPTCP (Multi Path Transmission Control Protocol) est un lot d'extensions pour TCP qui permet d'obtenir un protocole de Transport multi chemin. Ce protocole est toujours au stade de la conception, la description faite dans cette partie est tirée du document réalisé en 2010 : « Architecture Guidelines for Multipath TCP development » [60]. Les recommandations faites dans ce document concernent MPTCP mais certaines sont aussi valables pour les autres protocoles multi-chemins. Les objectifs de ce nouveau protocole de Transport sont :

- Augmenter la connectivité en utilisant le plus de chemins possibles,
- Améliorer l'état des ressources du réseau en répartissant la charge,
- Etre au moins aussi performant qu'une connexion TCP mono-chemin.

Multipath TCP a été conçu suivant le concept des protocoles de Transport de nouvelle génération (Tng). Introduit dans [61] (voir Figure 12), ce concept vise à diviser la couche Transport en plusieurs sous-couches :

- La couche supérieure « Semantic » contenant la sémantique et l'interaction avec l'application, utilisée dans les terminaux.
- Les couches inférieures « Flow Regulation» et « End Point », gérant les connexions et présentes dans les terminaux mais aussi dans les nœuds intermédiaires (routeurs ou pare-feux

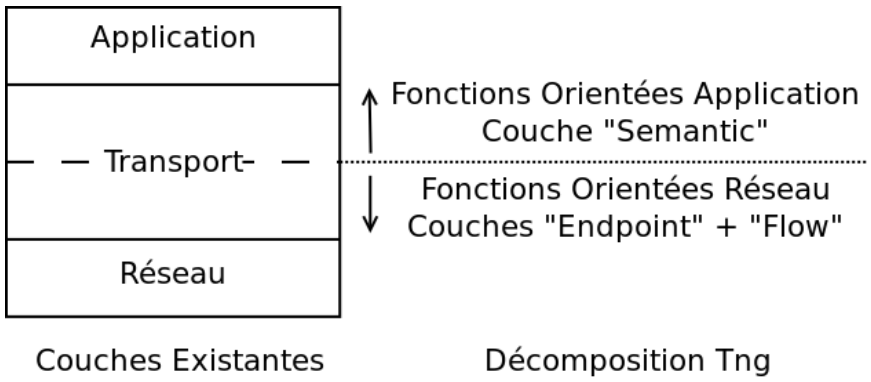


Figure 12 – Décomposition des fonctions de la couche Transport dans le Tng

par exemple).

Les bénéfices espérés d'une telle architecture sont nombreux même si certains restent discutables Parmi ces avantages, les suivants nous paraissent les plus importants : la segmentation des chemins permet la spécialisation par rapport aux caractéristiques du réseau et l'amélioration des performances en réduisant le RTT, les communications multi-chemins sont possibles au niveau du flux sans modifier la sémantique du protocole de Transport et enfin l'agrégation de flux permet de reprendre l'état d'un contrôle de congestion ou encore d'obtenir une meilleure équité entre les flux.

Avec une approche similaire (voir Figure 13), Multipath TCP est basé sur le protocole de Transport TCP : une session MPTCP est composée de plusieurs connexions TCP (les sous-flux), chacune correspondant à un chemin. Dans la décomposition décrite ci-dessus, MPTCP correspond à la couche supérieure et les sous-flux composent la couche inférieure. Cette architecture permet de tirer parti des fonctions de base de TCP comme la fiabilité et le contrôle de congestion mais aussi de ses extensions, notamment en ce qui concerne la sécurité de la connexion. Comme TCP, MPTCP garantit différents services aux applications : fiabilité de la connexion, livraison ordonnée des données, contrôle du flux, prévention de la congestion et ajoute aussi la gestion de plusieurs chemins. Ces différents mécanismes sont décrits au travers de fonctions : « Path Management » pour la gestion des chemins, « Packet Scheduling » et « SubFlow » pour l'ordonnancement des paquets.

La fonction « Path Management » permet la détection des différents chemins entre les hôtes, l'échange des adresses et la mise en place des sous-flux. Pour déterminer ces chemins, Multipath TCP utilise les adresses IP des deux hôtes, les chemins étant identifiés à l'aide d'un quadruplet TCP : adresse/port destination et source. Afin d'être le plus efficace possible, MPTCP doit être capable de prendre en compte des liens qui sont apparus au cours de la connexion.

Les fonctions « Packet Scheduling » et « Subflow » permettent le transfert des données : l'ordonnanceur est en charge de partager le flux de données venant de l'application en segments et de les transmettre aux sous-flux. Ceux-ci enverront ces données sur le réseau en agissant comme de simples connexions TCP. Pour que les données puissent être réassemblées par l'hôte distant, MPTCP se charge de numéroter les segments. Néanmoins une seconde numérotation par les sous-flux est nécessaire, car sans cela les nœuds intermédiaires détecteraient des « trous » dans le flux de données.

Le contrôle de la congestion avec un protocole de Transport multi-domicilié aborde des problématiques similaires au contrôle de la congestion dans un contexte mono-domicilié et notamment le respect de l'équité au niveau des points de congestion. Afin d'agir en amont de chaque sous-flux, le standard [62] définit un algorithme de contrôle de congestion pour protocoles multi-domiciliés qui va gérer le flux de données en provenance de l'application. Les mécanismes proposés permettent de

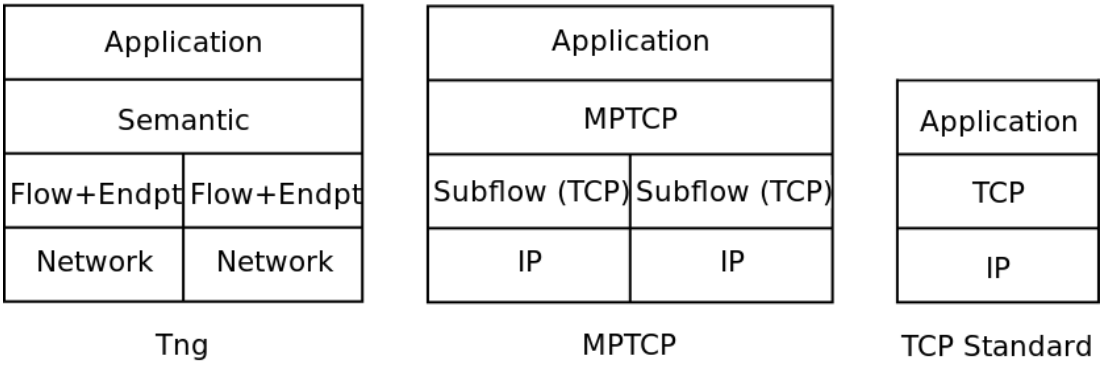


Figure 13 – Représentation en couche de plusieurs modèles : protocole de Transport de future génération (Tng), Multi-Path TCP et TCP classique.

coupler les fonctions d'incrémentation des sous-flux afin de contrôler l'agressivité du flux multi-chemins. De plus, l'algorithme de contrôle de congestion permet aussi de répartir les données entre les sous-flux suivant la congestion sur le chemin emprunté. Il est logique qu'un chemin peu congestionné doive être utilisé pour transférer plus de données.

L'implémentation de l'architecture de MPTCP soulève néanmoins certains problèmes :

- Avec TCP, les connexions sont identifiées grâce à un quintuplé (adresse/port source/destination et numéro de protocole), ce qui est impossible avec MPTCP. Les propositions sont d'utiliser un identifiant par hôte ou alors le quintuplé du premier sous-flux.
- Dans un protocole de Transport fiable, le buffer de réception permet de stocker les données qui ne sont pas reçues dans l'ordre. Une perte dans un sous-flux ne devant pas handicaper les autres sous-flux, MPTCP nécessite un buffer de taille importante : sum(BW_i)*RTT_max contre BW*RTT pour TCP (avec BW_i la bande passante sur le chemin i, et RTT_max le plus grand RTT de tous les chemins). Il en va de même pour la taille du buffer d'émission.
- La signalisation nécessaire à MPTCP pendant une connexion n'a pas été précisée. Pour l'instant, MPTCP utilise les options de TCP pour passer des informations (notamment lors de l'initiation de la connexion pour savoir si le protocole est supporté).

La sécurité de la transmission est aussi importante ; au cours d'une connexion MPTCP, des échanges sont nécessaires pour ajouter ou supprimer une adresse ou initier un sous-flux, et il ne faut pas qu'un hôte malicieux puisse intervenir. Le protocole de Transport doit proposer des mécanismes sûrs permettant d'effectuer ces opérations en toute confiance : le nœud récepteur doit être en mesure de déterminer avec certitude le nœud émetteur de ces requêtes et ne les accepter que si ce dernier est bien l'hôte distant.

Pour l'instant, MPTCP dans sa version basique ne supporte pas la mobilité, même si le « Working Group » MPTCP précise que le protocole a été conçu pour la supporter. Au travers d'une expérience sur un banc de test réel, les travaux réalisés dans [63] démontrent que la mobilité peut être gérée par MPTCP. L'implémentation est réalisée en utilisant une adresse IP permanente pour l'hôte de la communication et des adresses IP temporaires utilisées localement. L'adresse IP permanente sert alors d'identifiant pour la connexion MPTCP. Les résultats avancés permettent de conclure que le débit moyen est amélioré par rapport à une connexion TCP mono domiciliée et que la latence introduite lors d'un changement de réseau peut même être réduite par rapport à mobile IPv6. De l'aveu même des auteurs, cette solution n'est pas forcément l'implémentation parfaite de la mobilité avec MPTCP, il faut considérer cette expérience comme une preuve de faisabilité.

VI Conclusion

Les réseaux mobiles comportent de nombreuses contraintes ; particulièrement lors du changement de réseau : modification de l'identifiant réseau, introduction de latences, changement des caractéristiques du chemin utilisé par la communication... Nous avons vu dans cet état de l'art que des solutions étaient proposées, notamment au niveau Réseau pour réduire ou supprimer la modification de l'identifiant et obtenir des latences les plus faibles possibles en préparant la configuration de l'interface réseau. Dans le cas d'un réseau mono domicilié, la latence introduite par le changement d'adresse réseau ne peut cependant pas descendre en dessous d'une certaine valeur : l'établissement du lien au niveau Liaison. La solution qui nous parait la plus pertinente pour supprimer définitivement cette latence est l'utilisation de plusieurs interfaces réseau. En effet la multi-domiciliation permet d'effectuer toute les configurations préalables sur une interface réseau tout en continuant la communication sur une autre interface. Lorsque la nouvelle interface est configurée, la communication peut alors basculer vers celui-ci sans latences.

Le changement des caractéristiques du chemin utilisé pour les communications est plus difficile à prendre en compte. En effet, la couche Transport est directement impactée et les mécanismes classique de gestion du flux sont inefficaces pour prévenir ce phénomène. Pire, les évènements introduits peuvent conduire le protocole de Transport en erreur car celui-ci se base sur ses précédentes évaluations pour prendre les décisions alors que celles-ci ne sont plus valables. Nous avons vu précédemment l'impact sur TCP, le protocole de Transport le plus utilisé de nos jours. Si l'utilisation de versions spécifiques permet de diminuer cet impact, elles restent réservées à des cas exceptionnels. Une solution pourrait venir de MPTCP qui propose la multi-domiciliation mais il est difficile à ce jour de savoir quelles seront ces réelles capacités en terme de mobilité. Pour ces raisons, il nous semble clair que TCP n'est pas le protocole de Transport adéquat dans notre contexte.

Comme nous avons pu le voir dans ce chapitre, aucune précision exacte n'est donnée dans le standard sur le support de la mobilité par MPTCP. Pour cette raison, nous avons choisi d'étudier un autre protocole de Transport multi-domicilié : SCTP. Ce protocole de Transport reprend les services classiques proposés par TCP aux applications et introduit le support de la multi-domiciliation et du multi flux. Nous verrons par la suite que la gestion de la multi-domiciliation par SCTP permet de réduire l'impact du changement des caractéristiques. De plus, ses extensions (présentes dans toutes les implémentations) permettent de gérer la mobilité directement avec SCTP, ce qui peut être avantageux si aucune solution de mobilité n'est implémentée.

Chapitre III SCTP : un véritable concurrent à TCP ?

Stream Control Transmission Protocol (SCTP) est un protocole de Transport offrant des fonctionnalités modernes non-présentes dans les versions « basiques » de TCP. Dans cette section, nous allons démontrer que SCTP peut rivaliser avec TCP et être même plus performant dans certains contextes grâce à ses fonctionnalités innovantes.

Afin de déterminer si SCTP peut véritablement concurrencer TCP, il est nécessaire de comparer leurs comportements et leurs performances. Dans un premier temps, nous allons présenter SCTP avec sa gestion des données, ses fonctionnalités de multi homing et de multi streaming ainsi que ses extensions permettant la mobilité. Nous nous attacherons lors de cette description à le positionner par rapport à TCP.

L'étude des deux protocoles se fera en deux temps. Tout d'abord, nous nous intéresserons à leur contrôle du flux et leur prévention de la congestion en étudiant les mécanismes utilisés puis en simulant les protocoles sur un réseau de communication par satellite mono domicilié ayant une architecture avec QdS. Ensuite, nous regarderons l'impact de la mobilité sur ces deux protocoles de Transport et plus particulièrement l'impact de la modification des caractéristiques du réseau. Dans cette deuxième étude, nous nous concentrerons d'abord sur un réseau mono domicilié où la mobilité est transparente pour les terminaux. Dans un tel contexte, les protocoles de Transport peuvent uniquement subir le changement de réseau et la modification des caractéristiques du chemin utilisé par la communication. Nous tâcherons ensuite d'utiliser au mieux les nouvelles fonctionnalités de SCTP en étudiant sa gestion de la mobilité sur un réseau multi-domicilié. Le protocole sera alors informé des changements de réseau et nous verrons comment il s'adapte aux changements des caractéristiques du réseau.

Avant de poursuivre, il est nécessaire de faire un point sur les techniques qui seront utilisées pour réaliser les expériences illustrant ces études. L'émulation et la simulation sont souvent comparées car ce sont deux méthodes d'expérimentation n'utilisant pas tous les éléments réels du réseau étudié. En simulation, aucun composant de l'expérience n'est réel et la fiabilité des résultats va dépendre de la qualité de la modélisation. Des abstractions sont souvent nécessaires afin d'obtenir une simulation ne nécessitant pas de super calculateur pour être exécutée. Si la simulation facilite la conception en ne présentant quasiment aucune contrainte dans la réalisation d'un protocole ou la prise de mesures, il peut être plus difficile de réaliser certaines actions lors de la mise en œuvre sur un système réel. Entre réalité et simulation, l'émulation propose de coupler l'utilisation de composants physiques et de composants modélisés : la plupart du temps les terminaux sont réels et les communications traversent un nœud tiers chargé d'ajouter l'impact de la technologie de communication et/ou du phénomène étudié. Ces deux méthodes d'étude ne présentent donc pas les mêmes caractéristiques. Si l'émulation est plus proche de la réalité, la simulation permet de faciliter le passage à l'échelle et reste indispensable pour tester des technologies et des protocoles. L'émulation est aussi plus difficile à mettre en œuvre car elle nécessite plus de ressources et l'implémentation d'un « vrai » protocole ou programme est souvent plus complexe que dans une simulation. Dans les deux cas, il est nécessaire de posséder des informations précises sur le système réel, soit pour le modéliser précisément, soit pour configurer la partie émulée de l'expérience avec des valeurs correctes.

I SCTP : un protocole de Transport supportant la mobilité

Stream Control Transmission Protocol (SCTP) est un protocole conçu au début des années 2000 dans l'objectif de transmettre des données de signalisation. Ses fonctionnalités ainsi que ses performances ont permis d'en faire un protocole de Transport à part entière. Les mécanismes du protocole ainsi que le vocabulaire relatif à SCTP sont définis dans le standard [64]. Les termes suivants sont indispensables à la compréhension du protocole :

- Association : communication établie au niveau Transport avec SCTP, équivalent une connexion TCP,
- « Chunks » ou morceaux : suites d'octets formés d'une en-tête et de données composants un paquet SCTP,
- « Path » ou Chemin : route utilisée pour transmettre les paquets et établie entre deux interfaces réseaux distantes (une locale et une distante).

Le Tableau 5 compare les fonctionnalités de SCTP, TCP et UDP. Il est à noter que certaines versions de TCP peuvent proposer plus de services mais il s'agit ici d'une comparaison avec des versions classiques de type New-Reno ou Vegas. Tous les services proposés par TCP sont repris par SCTP qui propose en plus une transmission partiellement fiable ou la livraison non ordonnée des données. Mais les véritables améliorations de SCTP sont la résistance aux attaques SYN flooding, le support de la multi-domiciliation ou « multi homing » et la gestion du multi flux ou « multi-streaming ». Ces fonctionnalités sont permises grâce à la structure même de SCTP.

La résistance aux attaques de type SYN flooding vient de l'établissement de la connexion en 4 temps (voir Figure 14). Lors de la réception d'une demande de connexion, un cookie est généré par le serveur et envoyé avec l'acquittement d'initiation; aucune ressource n'est réservée à cet instant là. Seule la validité du cookie reçu dans le « cookie echo » permet la réservation de ressource et la mise

Tableau 5 – Services fournis par SCTP, TCP et UDP.

SERVICES	SCTP	TCP	UDP
Orienté connexion	Oui	Oui	Non
Full Duplex	Oui	Oui	Oui
Transmission fiable	Oui	Oui	Non
Transmission partiellement fiable	Optionnel	Non	Non
Arrivage ordonné des données	Oui	Oui	Non
Arrivage non ordonné des données	Oui	Non	Oui
Contrôle du flux et de la congestion	Oui	Oui	Non
Support d'ECN	Oui	Oui	Non
Acquittement sélectifs	Oui	Optionnel	Non
Découverte du Path MTU	Oui	Oui	Non
Empaquetage/fragmentation des PDU	Oui	Oui	Non
Multi streaming	Oui	Non	Non
Multi homing	Oui	Non	Non
Protection contre les attaques SYN flooding	Oui	Non	--
Autorisation de connections semi-fermées	Non	Oui	--
Vérification de l'accessibilité	Oui	Oui	Non

en place de la communication. A partir de là, l'association est établie côté serveur et des données peuvent être envoyées avec l'acquittement du cookie.

Pour un protocole de Transport, le multi homing est la capacité à gérer de multiples interfaces réseaux dans la même communication. SCTP utilise cette fonctionnalité pour établir plusieurs chemins entre deux hôtes d'une communication. Lors de l'initiation d'une association, les nœuds échangent les adresses IP actives qui vont servir à déterminer les chemins disponibles. Chaque hôte possède alors un jeu d'adresses de destination correspondant à des interfaces réseaux actives appartenant à l'hôte distant c.à.d. à un chemin permettant de communiquer. Le chemin qui a servi à l'initiation de l'association est considéré comme primaire et est utilisé pour transférer les données, les autres sont considérés comme secondaires et peuvent avoir trois états :

- « Idle » (en attente) : aucun chunk permettant de mettre à jour le RTT n'a été envoyé sur ce lien et son état est incertain,
- Actif : des chunks ont été envoyés sur ce lien et un acquittement a été obtenu,
- Inactif : le nombre de chunks envoyés sur ce lien et non acquittés pendant le RTO égale ou dépasse la valeur de 'Path.Max.Retrans'.

L'état des chemins peut être déterminé à l'aide de deux types de messages différents : les messages de données transportant le flux applicatif ou des messages envoyés périodiquement par l'association appelés « Heart Beats » (HB) et permettant d'actualiser la liste des chemins secondaires. Lorsque le chemin primaire est déclaré comme inactif suite à l'échec de plusieurs retransmissions, le premier chemin secondaire actif devient alors le nouveau chemin primaire.

Dans sa version de base [64], SCTP ne peut modifier dynamiquement les adresses IP utilisées par une association et un nœud ne peut demander à l'hôte distant d'utiliser un chemin particulier. Nous verrons par la suite que l'introduction de ces deux fonctionnalités dans des extensions à SCTP permet la gestion de la mobilité.

Nous avons vu dans le Chapitre II, section I.1.3, que le changement de réseau était responsable d'une modification brutale des caractéristiques du réseau. SCTP étant multi-domicilié, des changements de réseaux peuvent intervenir et il faut que ceux-ci dégradent les performances à cause d'une mauvaise estimation. Pour cela, SCTP utilise un jeu de paramètres (fenêtre de congestion, SRTT, RTO…) par chemin et ne prend donc pas en compte l'historique en arrivant sur un nouveau chemin. Les caractéristiques du nouveau réseau sont estimées à partir des valeurs initiales, ce qui permet d'atteindre plus rapidement les performances optimales.

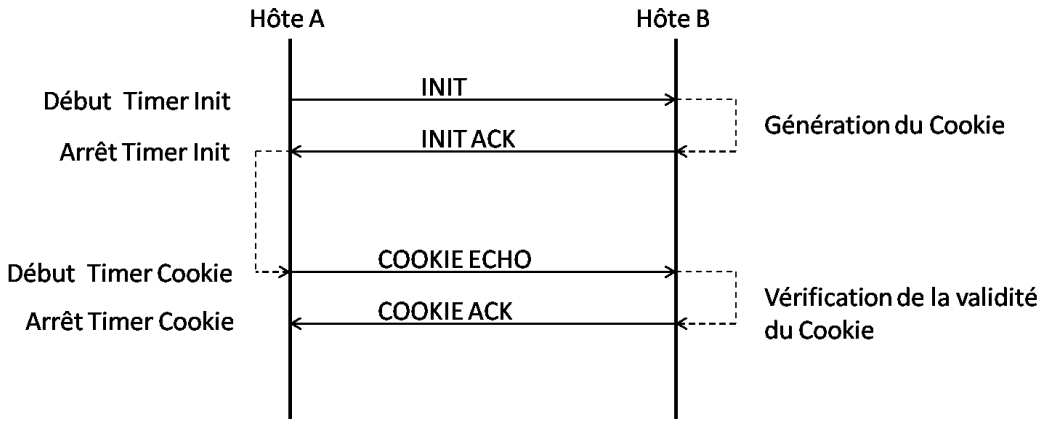


Figure 14 – Initiation en quatre temps d'une connexion avec SCTP.

Le multi-streaming permet d'avoir plusieurs flux dans une seule association SCTP, chacun de ces flux pouvant avoir différentes propriétés (par exemple livraison ordonnée ou non ordonnée). Le nombre de flux par association est négocié lors de l'initialisation de l'association, les chunks INIT et INIT ACK contiennent le nombre souhaité de flux en sortie et le nombre supporté de flux en entrée. Si le nombre de flux entrants de l'hôte distant est inférieur au nombre de flux en sortie de l'hôte local, celui-ci va limiter son nombre de flux sortants et peut notifier la couche supérieure. La couche supérieure peut alors décider d'annuler l'association si les ressources proposées sont insuffisantes. Les champs « Transmission Serial Number » (TSN) utilisés pour différencier les chunks sont communs à l'association contrairement aux champs « Stream Sequence Number » (SSN) qui dépendent du flux et correspondent à l'ordre des messages : les chunks sont donc délivrés dans l'ordre pour chaque flux le nécessitant. La perte d'un chunk de SSN x dans un flux devant être ordonné ne va pas influencer directement les autres flux, les chunks de SSN supérieur à x sont gardés dans le buffer de réception en attendant la retransmission. Pendant ce temps là, les chunks des autres flux sont délivrés sans retard, seule la taille de la fenêtre de réception (rwnd) va être diminuée et influencer ainsi la taille de la fenêtre de congestion. Pour obtenir le même résultat avec TCP, les hôtes sont obligés d'établir plusieurs connexions et donc d'ouvrir plusieurs sockets.

I.1.1 Transmission des messages avec SCTP

Comme indiqué précédemment, les paquets ou « Packet Datagram Units » (PDU) générés par SCTP ont une composition particulière : ces paquets comportent un en-tête commun et un ou plusieurs chunks (littéralement des « morceaux »). La structure des paquets SCTP est illustrée par la Figure 15 ci-dessous, l'en-tête commun contient le port source et le port destination, une étiquette de vérification et un checksum pour vérifier la validité du paquet. L'étiquette de vérification est un entier sur 32 bits, choisi lors de l'initiation, qui permet de vérifier l'émetteur du paquet.

Les chunks permettent de transporter des données mais aussi les messages de contrôle. La Figure 16 présente l'en-tête commun des chunks et la structure des paramètres de taille variable. Suivant son type, un chunk peut contenir un ou plusieurs paramètres de taille variable. L'en-tête d'un chunk

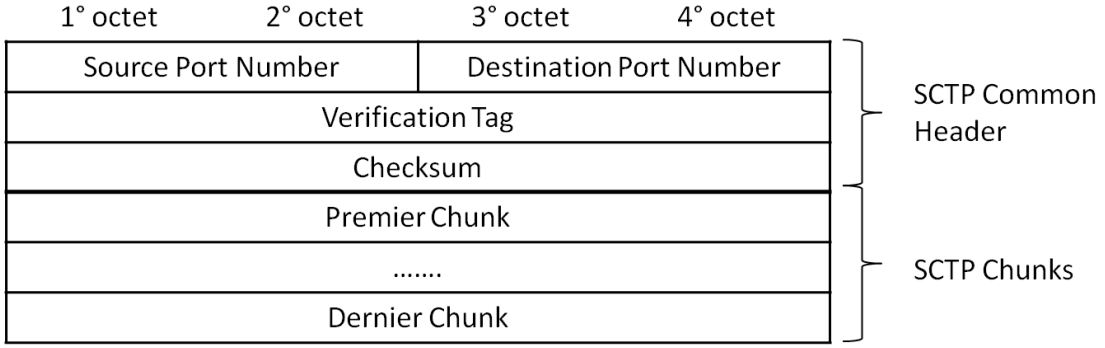


Figure 15 – Structure d'un paquet (PDU) SCTP : En-tête commune suivie par les différents morceaux ou « chunks » (voir liste Tableau 6).

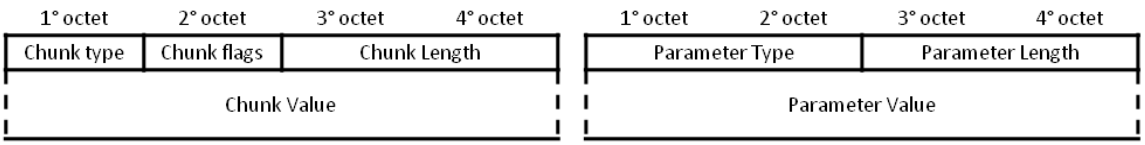


Figure 16 - En-tête commun à tous les chunks SCTP (à gauche) et structure d'un paramètre optionnel de taille variable pouvant être inclus dans un chunk (à droite).

Tableau 6 – Morceaux ou « chunks » utilisés par SCTP pour la transmission de données et les messages de contrôle.

Identifiant	Référence	Description
0	DATA	Données
1	INIT	Initiation de l'association
2	INIT ACK	Acquittement d'initiation
3	SACK	Acquittement sélectif
4	HEARTBEAT	Requête d'Heart Beat
5	HEARTBEAT	Acquittement d'Heart Beat
6	ABORT	Annulation de l'association
7	SHUTDOWN	Requête d'arrêt de l'association
8	SHUTDOWN ACK	Acquittement de l'arrêt
9	ERROR	Erreur lors d'une opération
10	COOKIE	Cookie d'état
11	COOKIE ACK	Acquittement d'un cookie
14	SHUTDOWN COMPLETE	Acquittement certifiant l'arrêt

contient son type, un champ réservé pour certains drapeaux dépendant du type, la taille du chunk et les valeurs qu'il transporte. Les différents types de chunks et leurs identifiants sont listés dans le Tableau 6. L'ensemble de ces chunks permet la gestion d'une communication avec ses différentes phases : initiation, transfert des données et fermeture. Il est à noter que SCTP ne permet pas de communication semi-ouverte, d'où la définition d'acquittements pour l'arrêt de l'association et pour certifier que cet arrêt a été pris en compte.

SCTP est un protocole de Transport fiable avec contrôle du flux et prévention de la congestion. Pour cela, il utilise une fenêtre de congestion similaire à celle utilisée par TCP ainsi qu'une numérotation des données. Comme expliqué précédemment, la numérotation des données se fait par flux (SSN) et par association (TSN). La fenêtre de congestion s'intéresse uniquement aux TSN, ce qui permet une gestion globale des flux en multi streaming. Les différents algorithmes utilisés par SCTP sont similaires à TCP : Slow Start, Congestion Avoidance et Fast Retransmit / Fast Recovery. Ses performances sont donc très proches d'un TCP New Reno, nous y reviendrons par la suite avec la comparaison des performances de SCTP et de TCP.

I.1.2 Mobile-SCTP : regroupement d'extensions pour la mobilité

De par sa structure et ses fonctionnalités, SCTP est rapidement apparu comme un protocole de Transport prometteur, notamment grâce au multi homing. Dans un contexte mobile, l'utilisation de plusieurs chemins permet d'effectuer des changements de réseaux sans pertes et de manière douce (on parle alors de « soft handover »). La seule contrainte est la définition statique des adresses IP lors de l'initiation de l'association. Pour pallier à cet inconvénient, deux extensions à SCTP ont été définies : l'une définissant de nouveaux chunks et autorisant la modification dynamique des adresses ainsi que le choix du chemin primaire [65], l'autre permettant l'authentification des chunks [66]. Leur implémentation dans SCTP est regroupée sous l'appellation « mobile SCTP » (mSCTP) et chaque extension est détaillée dans la suite de cette section.

Dans sa version originale, SCTP authentifie les chunks en se basant uniquement sur l'étiquette de vérification présente dans l'en-tête. Pour permettre la mobilité, une authentification plus robuste est nécessaire afin d'éviter qu'un hôte malicieux ne puisse détourner l'association en demandant l'ajout de son adresse IP. L'extension [66] apporte des mécanismes à SCTP pour authentifier les chunks en utilisant des clés partagées. Plusieurs composants sont nécessaires pour mettre en œuvre cette technique : de nouveaux paramètres, un nouveau chunk et une nouvelle cause d'erreur ont été

introduits. Ces paramètres doivent être présents dans les chunks INIT ou INIT ACK si leur émetteur souhaite utiliser l'authentification :

- « Random Parameter » (RANDOM), utilisé pour transporter un nombre aléatoire,
- « Chunk List Parameter » (CHUNKS), précise les types de chunks devant être authentifiés (nécessaire uniquement pour la réception de chunks authentifiés),
- « Requested HMAC Algorithm Parameter » (HMAC-ALGO), liste des identifiants HMAC que peut utiliser l'hôte dans l'ordre de préférence (par exemple basé sur SHA-1 ou SHA-256).

Les chunks INIT, INIT ACK, SHUTDOWN COMPLETE et AUTH ne peuvent pas être authentifiés et ne doivent pas être listés dans le paramètre listant les chunks ; s'ils le sont, leur type est ignoré.

L' « Authentification Chunk » (AUTH, type=0x0F) introduit par l'extension reprend l'en-tête commune des chunks définie dans la partie I.1.1, elle est composée d'un identifiant décrivant la paire de clés partagées qui est utilisée, l'identifiant de l'algorithme utilisé, le résultat du calcul HMAC et un remplissage (pour avoir un chunk de la taille d'un multiple de quatre octets). Ce chunk doit être présent une seule fois dans tout paquet transportant des chunks authentifiés. Tous les chunks de contrôle ou de données situés après ce chunks sont considérés comme étant authentifiés. Ceux placés avant ne le sont pas, les chunks de contrôle devant absolument être placés avant ceux de données. Avant d'envoyer un paquet SCTP contenant des chunks authentifiés, l'émetteur utilise l'algorithme souhaité par le récepteur et la clé partagée pour calculer le HMAC. Les données utilisées pour ce calcul contiennent le chunk AUTH avec le champ HMAC à 0 et tous les chunks suivants contenus par le paquet. Lors de la réception d'un paquet SCTP contenant des chunks authentifiés, le nœud va vérifier que l'identifiant de l'algorithme HMAC contenu dans le chunk AUTH corresponde aux paramètres spécifiés dans le INIT ou le INIT ACK. Si ce n'est pas le cas, le paquet est ignoré et un chunk ERROR est envoyé contenant la nouvelle cause d'erreur : 'Unsupported HMAC Identifier'.

L'extension à SCTP permettant la mobilité [65] introduit de nouveaux chunks et permet la modification des adresses de destination utilisées par l'association sur l'hôte local mais aussi sur l'hôte distant. Le protocole de Transport SCTP va alors pouvoir utiliser des interfaces devenus actifs au cours de l'association. L'utilisation de l'authentification présentée plus haut est obligatoire. Deux nouveaux chunks sont introduits par cette extension : ASCONF et ASCONF ACK (« Address Configuration Change Chunk »). Leur structure est identique à celle des autres chunks avec un en-tête commun, un numéro de séquence et des paramètres de taille. Le numéro de séquence est initialisé à la même valeur que le TSN initial, et est incrémenté de un à chaque envoi. De nouveaux paramètres de taille variable ont aussi été introduits pour être utilisés dans ces chunks :

- « Add IP Address », permet d'ajouter une adresse IP de destination dans le jeu d'adresses de l'hôte distant,
- « Delete IP Address », permet d'enlever une adresse IP de destination dans le jeu d'adresses de l'hôte distant,
- « Set Primary Address », demande à l'hôte distant de prendre l'adresse donnée comme adresse de destination primaire,
- « Error Cause Indication », renvoyé dans un ASCONF ACK pour justifier un échec,
- « Success Indication », renvoyé dans un ASCONF ACK pour indiquer un changement correctement effectué.

En plus des paramètres précédents qui sont indispensables pour l'utilisation de l'extension, des informations doivent être échangées entre les nœuds lors de l'initiation. Les paramètres suivants peuvent être présents dans les chunks INIT et INIT ACK :

- « Set Primary Address », permet de choisir l'adresse de destination initiale utilisée par l'hôte distant,
- « Supported Extensions », permet de spécifier les extensions supportées par l'émetteur du chunk,
- « Adaptation Layer Indication », définit dans la RFC mais pas utilisé par l'extension, ce paramètre permet de passer des informations aux couches supérieures lors de l'initialisation.

Les demandes de reconfiguration ne pouvant pas toujours être appliquées par l'hôte distant, de nouvelles causes d'erreur ont aussi été ajoutées pour être utilisées dans l'acquittement :

- « Request to delete last remaining IP address », signalant une tentative d'enlever de l'association la seule adresse IP de destination existante,
- « Operation refused due to resource shortage », problème d'allocation de ressources sur l'hôte distant,
- « Request to delete source IP address », signale une tentative d'enlever l'adresse source de la requête,
- « Association aborted due to illegal ASCONF ACK », chunk invalide (par exemple adresse déjà présente dans l'association),
- « Request refused – no authorization », échec de l'authentification ou extension absente/inactive.

Un acquittement considéré comme illégal peut conduire à l'annulation de l'association si son numéro de séquence est plus grand que celui attendu ; dans ce cas la cause d'erreur sera incluse dans un chunk ABORT. Un acquittement ayant un numéro de séquence inférieur à celui attendu est silencieusement ignoré. La création de ces erreurs permet d'avoir une réponse plus précise lors du refus de la nouvelle reconfiguration et d'envisager une nouvelle requête.

Les mécanismes apportés par cette extension permettent à un nœud itinérant de changer de chemin sans avoir à subir un certain nombre de pertes conduisant au changement de lien primaire. Si le changement de lien est effectué suffisamment en avance, la communication ne va subir aucune perte. L'inconvénient majeur du changement de réseau étant la localisation du nœud mobile par un hôte distant, cet aspect est à prendre en compte pour obtenir une solution complète de mobilité et doit être implémenté en plus des extensions décrites dans ce document.

Les implémentations de mSCTP fournissent uniquement les interfaces de programmation ou « Application Programming Interface » (API) permettant de gérer dynamiquement le jeu d'adresses IP de l'association et le chemin primaire. La gestion de la mobilité à proprement parler doit être réalisée par le développeur de l'application SCTP. Lors de la présentation de l'application SCTP développée au cours de cette thèse, nous verrons comment simplifier la tâche des développeurs en concevant un agent gérant la mobilité de SCTP compatible avec n'importe quelle application (voir le Chapitre III, section III.2). La section suivante présente une implémentation en module d'application SCTP gérant la mobilité.

I.1.3 Gestion de la mobilité avec SCTP

Mobile SCTP ne fournissant pas de gestionnaire pour la mobilité, il était nécessaire de proposer un schéma de mobilité. Dans [67], il est proposé un module mSCTP-DAC permettant de gérer la mobilité en se basant sur les l'état des liens et certains événements réseaux. L'implémentation de cette solution est faite en C sous Linux. Le nœud mobile possède deux interfaces réseaux et le reste du réseau est émulé. Le schéma de mobilité utilisé pour cette expérience est simple et est illustré par la Figure 17 :

1. Une association est établie sur l'interface If1,
2. Un nouveau réseau est détecté par l'interface If2,
3. Le nœud se connecte au nouveau réseau (niveau Liaison et niveau Réseau),
4. La nouvelle adresse est communiquée au nœud correspondant avec un ASCONF-ADD IP,
5. Une requête pour changer de chemin primaire peut être faite (ASCONF-Change Prim) et sera effective une fois le chemin vérifié avec un Heart Beat.
6. L'adresse est supprimée une fois la connexion perdue.

Dans cette expérience, la requête de changement d'adresse primaire se fait un certain temps après l'ajout de l'adresse IP (1 seconde, 2 secondes et 4 secondes). Néanmoins, cette requête peut aussi se faire en même temps que l'ajout. Le meilleur moment pour changer va dépendre des technologies de communication utilisées et de l'environnement : se connecter à un réseau en limite de couverture peut dégrader les performances. Plutôt qu'un temps fixe à attendre, il est alors plus pertinent de comparer la qualité ou la puissance des signaux pour choisir le chemin primaire.

Au vu de la Figure 17, il est clair que la durée nécessaire au changement de réseau avec l'algorithme mSCTP-DAC est fortement dépendante de la durée nécessaire à la connexion de niveau Liaison et niveau Réseau. Notamment, la méthode utilisée pour configurer l'adresse IP va fortement influencer la durée nécessaire à son obtention. Si une détermination autonome est relativement rapide, l'envoi de requêtes DHCP peut nécessiter plusieurs secondes. Nous verrons dans le Chapitre IV que même une configuration de manière statique peut prendre un temps conséquent par rapport au temps de connexion disponible.

Une comparaison des performances entre MIP, SIP et mSCTP est faite dans [68]. Le changement de réseau vertical entre UMTS et WLAN est étudié sur le simulateur OPNET. Les auteurs démontrent que MIP et mSCTP sont plus performants que SIP, notamment en proposant de plus faibles latences lors du changement de réseau. Une remarque intéressante est aussi faite en se basant sur les relevés de l'expérience. Une grande partie du délai de changement de réseau étant due à la configuration de l'adresse IP avec DHCP, l'utilisation de points d'accès de plus haut débit permet de réduire de 50% la

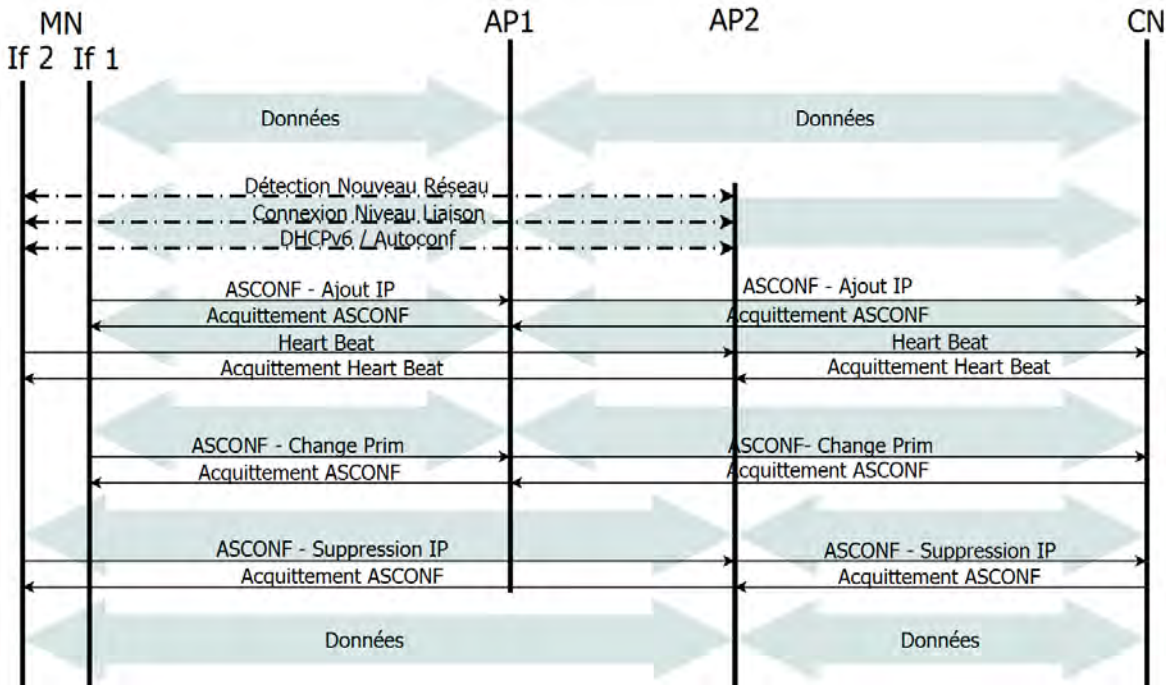


Figure 17 – Changement de réseau avec l'algorithme mSCTP-DAC.

latence introduite par le changement de réseau.

II Performances de SCTP sur un réseau satellite avec architecture à Qualité de Service

Comme TCP, SCTP est un protocole de Transport offrant le contrôle du flux et la prévention de la congestion. Les mécanismes utilisés par les deux protocoles sont similaires : une fenêtre de congestion gère la quantité de données en vol et évolue suivant différents algorithmes dépendant de la situation : « Slow-Start », « Congestion Avoidance », « Fast Retransmit/Fast Restart »… Ces algorithmes ont été conçus avec l'évolution des réseaux filaires et sont intégrés dans TCP et ses différentes versions (Reno, New Reno, …). Il est logique qu'un protocole de Transport conçu au début des années 2000 se base sur les mêmes techniques pour maitriser son flux de données.

Sur un réseau mono domicilié en mono flux, les deux protocoles devraient donc avoir un comportement proche, leur gestion des données étant quasi identique. Pour vérifier cela nous avons choisi de les comparer sur un réseau de communication par satellite avec une architecture QdS. Ce type de réseau est particulièrement contraignant pour les protocoles de Transport puisque le délai subi est important et la bande passante disponible varie régulièrement.

II.1 Modèle utilisé et configuration de la simulation

Les télécommunications par satellite géostationnaire présentent des contraintes pouvant dégrader les performances des protocoles de Transport : long délai (autour de 250ms) et débit souvent faible et variable (dépendant de la méthode d'allocation de bande passante). De plus, certains réseaux de communication par satellite possèdent une architecture avec Qualité de Service (QdS). La différentiation des flux impacte les communications en priorisant certains flux lors de leur introduction. La bande passante disponible pour les flux diminue alors brutalement, ce qui va aussi augmenter le délai subi à cause du remplissage des files d'attente dans le point d'accès au réseau satellite (point de congestion). Les protocoles de Transport étant rudement mis à l'épreuve sur ce type de support, il est intéressant de comparer les performances de TCP et SCTP sur un tel réseau.

La comparaison des performances de ces deux protocoles a été faite en simulation avec un simulateur événements discrets pour les réseaux de communication : Network Simulator 2 (ns-2) [79]. Ce logiciel est né en 1989 comme une variante du simulateur réseau REAL [80]. Depuis, ns-2 a su évoluer notamment grâce à sa conception modulaire qui permet de facilement incorporer et partager une nouvelle implémentation. Sa conception en modules a permis d'incorporer les modifications et nouveautés au fur et à mesure de leur apparition.

Les liens de communication par satellite sont simulables avec ns-2 mais des fonctionnalités doivent être ajoutées. La méthode d'accès implémentée de base est le protocole « Unslotted Aloha » ou « Pure Aloha » qui a été conçu dans les années 70 à Hawaï [81]. Une méthode d'accès de type TDMA-DAMA correspondant plus à la réalité actuelle a été implémentée dans [82], son code disponible en tant que patch nous a servi de base pour notre implémentation. Nous avons rajouté à ce modèle une différenciation des flux au niveau IP et au niveau MAC afin d'obtenir une architecture avec QdS similaire à celle présentée sur la Figure 18. Au niveau IP, les files « Expedited Forwarded » (EF), « Assured Forwarded » (AF) et « Best Effort » (BE) permettent de faire une première séparation entre les flux. An niveau MAC, les files « Real-Time » (RT) et « non Real-Time » (NRT) permettent de différencier les flux critiques des autres. Lors de l'envoi des trames, les paquets sont prélevés en priorité dans la file RT ; un pourcentage maximal de la bande passante peut aussi être déterminé pour permettre à la file NRT de se vider. Pour être plus précis au niveau de l'utilisation de la bande passante, nous avons aussi ajouté l'impact de l'encapsulation et de la fragmentation causé par l'utilisation du protocole AAL5 dans le sens montant (des terminaux vers le satellite). En effet, les mesures effectuées permettent de montrer que ces mécanismes engendrent 10% de débit supplémentaire ce qui est conséquent sur un lien à faible bande passante. Des détails sur la conception et les expériences faites avec TCP sur ce modèle sont présents dans [83].

Ce modèle nous a permis de faire une comparaison entre les performances de SCTP et TCP [84]. Le réseau satellite simulé correspond à l'illustration donnée par la Figure 19, il comporte :

- Un satellite géostationnaire,
- Un Network Control Center connecté à une passerelle (GW),
- Deux terminaux satellites (ST) chacun fournissant un accès à deux nœuds utilisateurs (n5 à

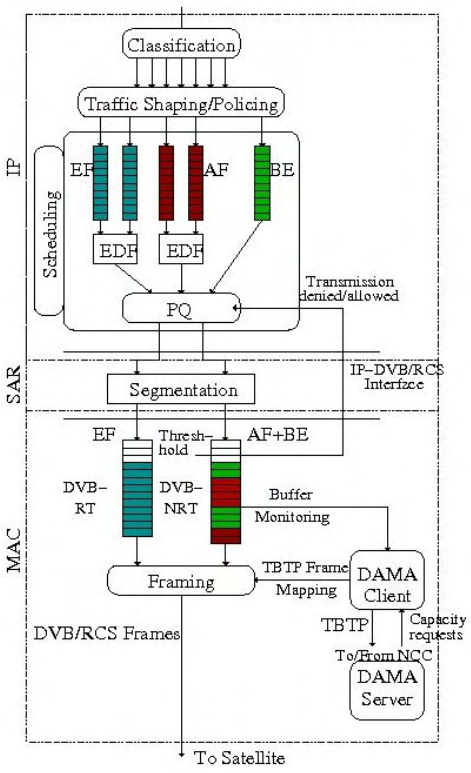


Figure 18 – Exemple d'une architecture réseau avec Qualité de Service utilisée dans les réseaux de communication par satellite et implémentée dans notre modèle.

n8).

Les connexions des deux terminaux au réseau satellite sont similaires : leur bande passante est allouée en TDMA-DAMA et ils peuvent requérir indépendamment l'un de l'autre au maximum 256kb/s (32ko/s), 128kb/s (16ko/s) étant alloués en CRA (Allocation d'un taux de transmission constant, « Constant Rate Assignment ») et 128kb/s en RBDC (Allocation basée dynamiquement sur le taux de transmission du flux, «Rate-Based Dynamic Capacity »). Pour que les deux protocoles de Transport ne s'influencent pas, les sources sont placées derrière des terminaux différents, dans les nœuds n5 et n7. Afin de soumettre les protocoles à de plus fortes contraintes, des flux à débits constants de plus haute priorité sont rajoutés derrière chaque terminal, dans les nœuds n6 et n8. Ces flux « Constant Bit Rate » (CBR) sont envoyés avec le protocole de Transport « User Datagram protocol » (UDP) qui ne possède pas de mécanisme de contrôle de congestion. Le débit est donc uniquement fixé par le flux CRA situé dans la couche supérieure, il est réglé égal à 128kb/s. La connexion TCP et l'association SCTP vont transporter des données d'applications type « File Transfer Protocol » (FTP) simulée par des sources infinies avec ns-2.

Le scénario simulé est un cas typique de QdS : une application prioritaire est lancée alors qu'un transfert de fichier est en cours et l'architecture QdS va favoriser les flux de plus haute priorité, obligeant les autres flux à s'adapter.

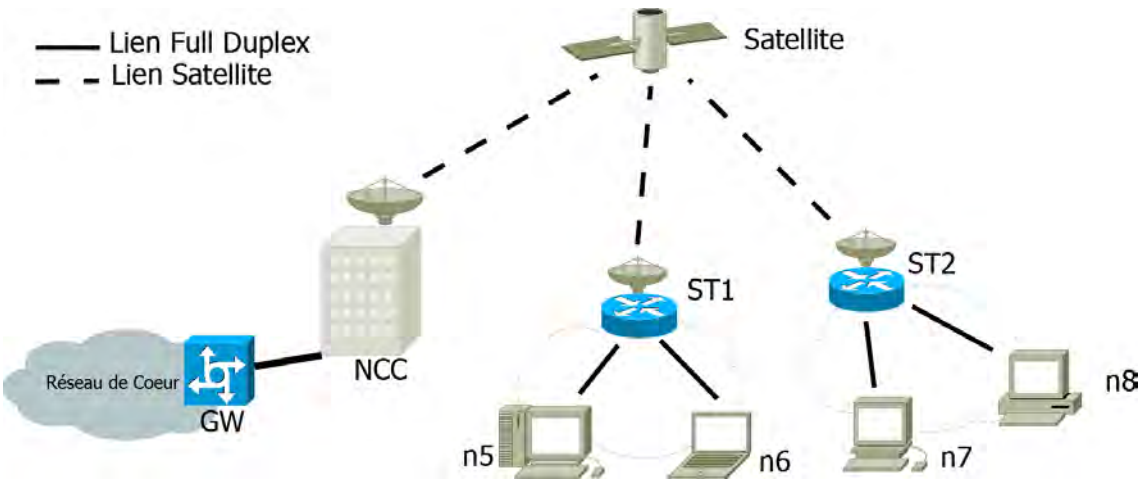
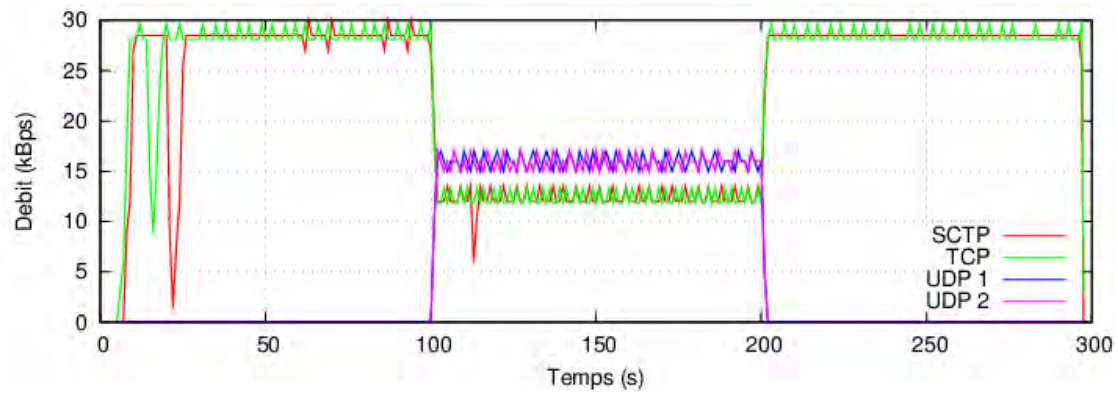


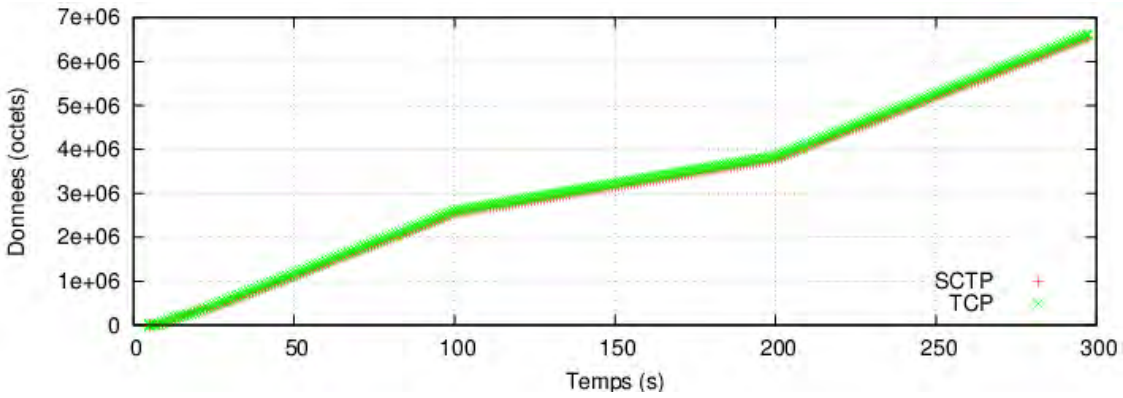
Figure 19 – Réseau satellite simulé pour la comparaison entre SCTP et TCP : 2 terminaux avec 2 nœuds utilisateurs et le point d'accès vers l'extérieur (GW).

II.2 Résultats

La Figure 20 présente le débit des flux (a) ainsi que la quantité cumulée de données reçues (b). Ces deux courbes permettent d'illustrer la capacité des protocoles à transmettre des données et il est clair que, de ce point de vue là, les performances de SCTP et TCP sont similaire. La bande passante disponible est entièrement utilisée avec un débit aux alentours de 30Ko/s, les 2Ko/s restants étant nécessaires à l'encapsulation et à la fragmentation des paquets IP. Lors de l'apparition des flux concurrents, l'adaptation se fait rapidement et sans dégradation importante. Aucune coupure n'apparait dans le flux de données et les trois phases de la simulation sont visibles : avant, pendant et après la présence du flux concurrent. Logiquement, la quantité cumulée de données reçues augmente plus lentement en présence du flux CBR entre 100s et 200s.



(a) Débit de chaque flux en Ko/s.

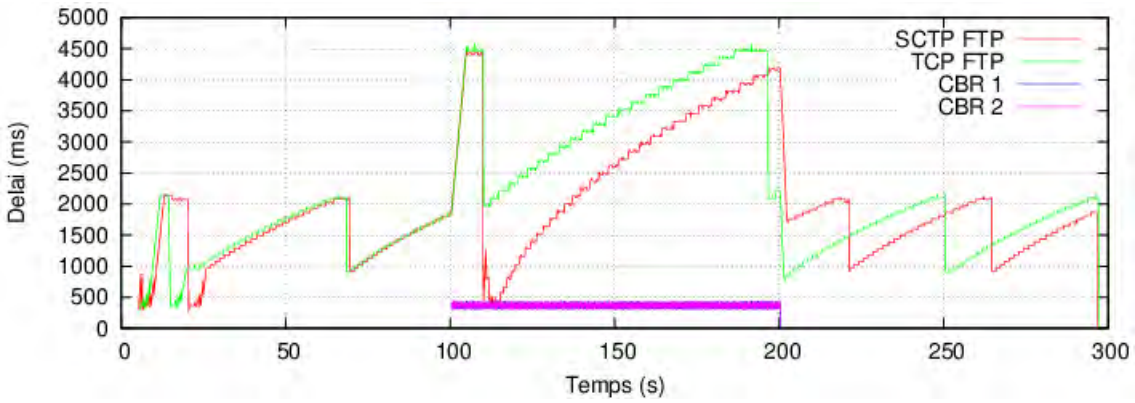


(b) Données reçues en octets.

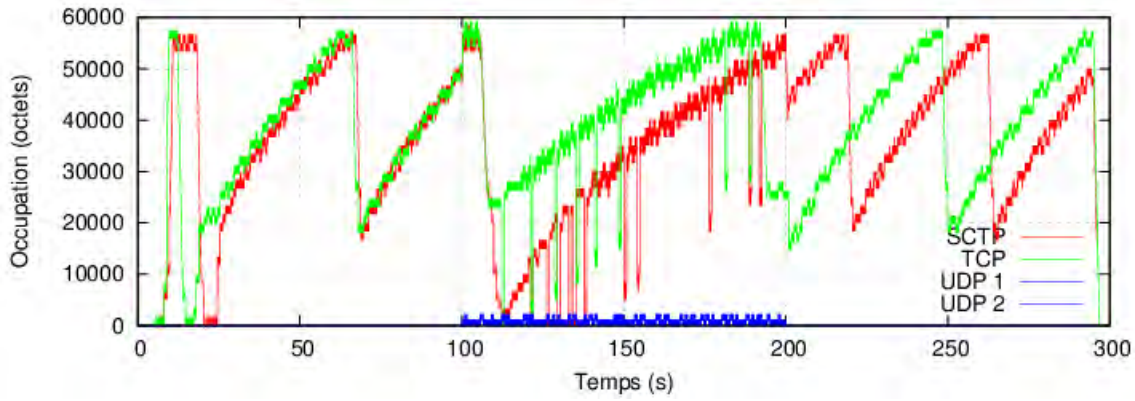
Figure 20 – Performances de SCTP et TCP sur un lien satellite et mise en concurrence avec des flux UDP entre 100s et 200s (débit et données reçues).

Sur la Figure 21, les mesures suivantes sont présentées : le délai (a), le niveau d'occupation des files d'attente traversées par les flux (b) et la fenêtre de congestion de la connexion TCP et de l'association SCTP. Ces mesures permettent de comprendre le comportement des protocoles de Transport et de vérifier que celui-ci est correct par rapport à ce qui est attendu (respect des standards et du comportement théorique).

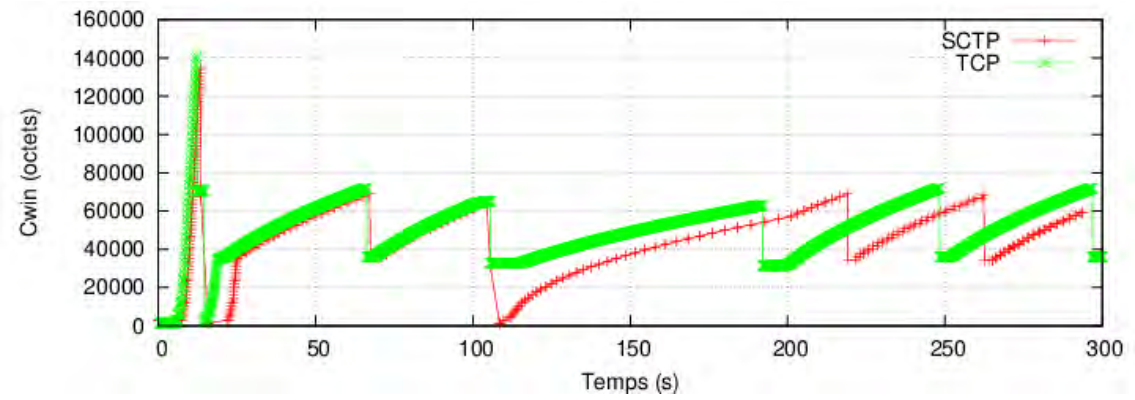
Dans le meilleur des cas, le délai subi par les communications sur un lien satellite géostationnaire est d'environ 300ms (temps de propagation montant et descendant). Au vu des résultats de la Figure 21



(a) Délai subi par chaque flux en ms.



(b) Niveau d'occupation des files traversées par chaque flux en octets.



(c) Fenêtres de congestion en octets.

Figure 21 – Performances de SCTP et TCP sur un lien satellite et mise en concurrence avec des flux UDP entre 100s et 200s (délai, occupation des files d'attente et fenêtre de congestion).

(a), les délais subis par les flux FTP sont largement supérieurs à 500ms contrairement aux flux CBR qui restent en dessous de 500ms. La différence entre les deux types de flux est due à deux facteurs : l'architecture avec QdS priorise les flux CBR par rapport aux FTP et les flux CBR ont un débit constant inférieur à la bande passante disponible. En effet, l'important délai subi par les flux FTP est du à la mise en attente des données au niveau du terminal.

La Figure 21 (b) présente la taille des files d'attente dans les terminaux et il est clairement visible que seulement 1 ou 2 paquets UDP sont stockés au même instant. En revanche, les quantités de données correspondant aux flux transportés par SCTP et TCP varient en permanence et remplissent complètement la file à plusieurs reprises, conduisant à la suppression de nouvelles données entrantes. Ce comportement est en accord avec les fenêtres de congestion des deux protocoles, présentées sur la Figure 21 (c). Dans ce cas, la quantité de données en vol correspondant à la fenêtre de congestion est donc majoritairement stockée dans la file d'attente du terminal.

Le phénomène que nous venons de décrire permet d'expliquer les variations et les valeurs importantes du délai pour les protocoles SCTP et TCP, celui-ci correspondant principalement au temps passé dans la file d'attente au niveau du terminal.

II.3 Conclusion

Cette étude permet de confirmer l'hypothèse avancée en début de section : SCTP et TCP ont un comportement similaire en ce qui concerne la gestion de données. L'utilisation des mêmes mécanismes pour contrôler le flux de données et prévenir la congestion explique cette ressemblance et induit forcément des performances similaires. Lors de la mise en concurrence avec un nouveau flux, leurs réactions différent pourtant légèrement, TCP arrivant à redémarrer après un passage en « Fast Retransmit » tandis que SCTP voit sa fenêtre diminuée au minimum. Néanmoins, l'impact sur les performances est minime, le débit des flux restant optimal.

Les performances de SCTP et TCP sont similaires, SCTP peut donc rivaliser avec TCP sur un réseau mono-domicilié tel qu'un réseau de communication par satellite avec architecture de QdS. Cette étude ne comparant que des fonctionnalités existant dans les deux protocoles, SCTP semble potentiellement plus performant. En effet, l'utilisation de la multi-domiciliation dans un contexte mobile doit amener des bénéfices. Dans la section suivante, nous allons continuer l'étude de SCTP et TCP sur un lien mono domicilié mais qui sera cette fois soumis à des changements de réseau transparents pour les terminaux. Il va ainsi être possible d'analyser la réaction de ces deux protocoles de Transport face à des variations importantes des caractéristiques du réseau. Dans un second temps, nous étudierons SCTP sur un réseau équivalent multi-domicilié.

III Impact du changement de réseau sur les protocoles de Transport et mobilité avec SCTP

Dans la section précédente, nous avons vu que les comportements de SCTP et de TCP étaient similaires sur un réseau mono domicilié avec un lien fixe. Ceci venait conforter notre hypothèse de départ : les deux protocoles se basant sur les mêmes mécanismes pour gérer leur flux de données et prévenir la congestion, leurs comportements sont forcément proches et leurs performances équivalentes.

Après avoir étudié le comportement de SCTP et de TCP sur un réseau satellite, nous allons nous intéresser à un phénomène pouvant perturber les protocoles de Transport : la modification des caractéristiques du réseau suite à un changement de réseau. Nous avons vu dans le Chapitre II, section V.1.2, que TCP pouvait être impacté. L'étude faite ici va déterminer dans quelle mesure SCTP est impacté par le changement de réseau et s'il le supporte mieux que TCP. Pour que cette étude soit plus complète, nous prendrons en compte plusieurs versions de TCP.

L'étude de l'impact du changement de réseau sur SCTP va se faire en plusieurs temps. Tout d'abord, nous étudierons comment le protocole est affecté par un changement de réseau transparent effectué sur un réseau mono domicilié. Les nouvelles fonctionnalités de SCTP ne sont alors pas utilisées et il est ainsi possible de faire une comparaison avec TCP. Pour commencer, nous décomposerons le changement de réseau en ne modifiant qu'un paramètre à la fois et en observant son influence. L'étude d'un changement de réseau complet permettra alors de comprendre l'origine des différents phénomènes intervenant après celui-ci. L'un des atouts principaux de SCTP étant le support de la multi-domiciliation, nous étudierons ensuite le changement de réseau sur un réseau multi-domicilié avec une gestion de la mobilité par mSCTP. Nous déterminerons l'apport de la multi-domiciliation face à la modification des caractéristiques du réseau induites par un changement de réseau.

La mise en pratique de cette étude se fait sur un banc de test permettant d'émuler le changement de réseau. Ce banc de test a été utilisé pour le projet SAT-PERF qui est décrit dans la section suivante suivi par la configuration des expériences. La section III.2 présente l'application que nous avons développée pour générer le trafic SCTP, relever des paramètres de l'association et gérer la mobilité avec SCTP. La suite de cette partie sera consacrée à l'étude de SCTP : la section III.3 pour les cas mono-domicilié et la section III.4 pour le cas multi-domicilié.

III.1 Le projet SAT-PERF : intérêts, plateforme et protocole de test

Le projet SAT-PERF vise à l' « Amélioration des performances applicatives dans un contexte hybride réseau terrestre / satellite ». Il s'agit d'une étude Recherche et Technologie (R&T) dirigée par le Centre National d'Etude Spatial (CNES) [85] et réalisée par le Laboratoire pour l'Analyse et l'Architecture des Systèmes (LAAS) [87] et ASTRIUM [86]. Cette étude se focalise plus précisément sur l'impact du changement de réseau sur les performances des protocoles de Transport. Deux approches ont été choisies : une portant sur le court terme avec des solutions existantes comme TCP et ses différentes versions, une autre portant sur un plus long-terme avec un protocole moderne comme SCTP.

Les changements de réseaux sont connus pour affecter les performances des applications et pour perturber le comportement des protocoles de Transport en changeant brutalement les caractéristiques du chemin utilisé pour la communication. Pour un changement de réseau horizontal, l'impact est moindre ; deux liens de même technologie sont plus à même d'avoir des caractéristiques proches. En revanche dans le cas d'un changement de réseau vertical, il peut y avoir un rapport de 10 entre les

caractéristiques des deux liens : un exemple est la différence de délai entre un réseau satellite et un réseau Wi-Fi. L'impact de ce phénomène a déjà été introduit dans le Chapitre II, section I.1.3, et détaillé dans le Chapitre II, section V.1.2, avec l'exemple de TCP.

Les scénarios envisagés dans cette étude sont divers mais peuvent être classés dans deux familles : ceux mettant en œuvre un réseau hybride et ceux utilisant un réseau multi-domicilié. Dans le cas hybride, le nœud mobile possède une seule interface réseau et le changement de réseau n'est pas perçu directement par le protocole de Transport, la gestion de la mobilité étant réalisée par exemple au niveau Réseau avec MIPv6. Avec un réseau multi-domicilié, le nœud mobile possède plusieurs interfaces réseaux, le changement de réseau se fait d'une interface à l'autre. Dans les deux cas, un changement de réseau est effectué sur le chemin utilisé par la communication.

La réalisation de cette étude est faite avec un émulateur de lien satellite développé par ASTRIUM. SATellite EMulator (SATEM) consiste en un ordinateur sous Ubuntu comportant plusieurs interfaces réseau Ethernet. La reproduction du délai et du débit d'un réseau particulier est faite avec Netem comme illustré dans la Figure 23. Netem est un émulateur réseau sous Linux qui permet la réalisation de files d'attente ainsi que l'ajout de délais. Une étude est faite dans [88] avec le test de plusieurs de ces fonctionnalités. Lors de leur arrivée dans SATEM, les paquets sont marqués en modifiant le champ Type of Service (ToS) de l'en-tête du paquet IP. Cette valeur va permettre de classer le paquet dans une file correspondant au lien actuel et appliquant les caractéristiques voulues. Si un changement

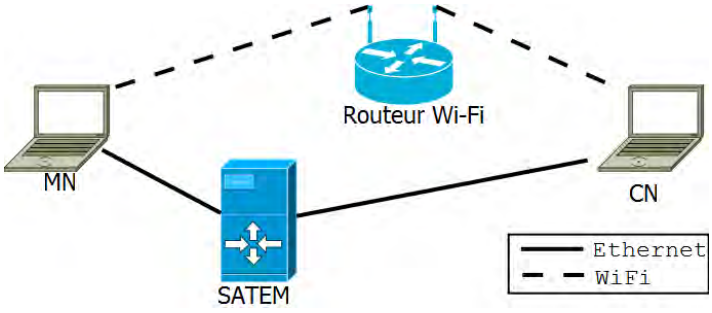


Figure 22 – Plateforme de test pour le réseau multi-domicilié : émulateur de lien satellite en Ethernet d'un côté et routeur Wi-Fi de l'autre.

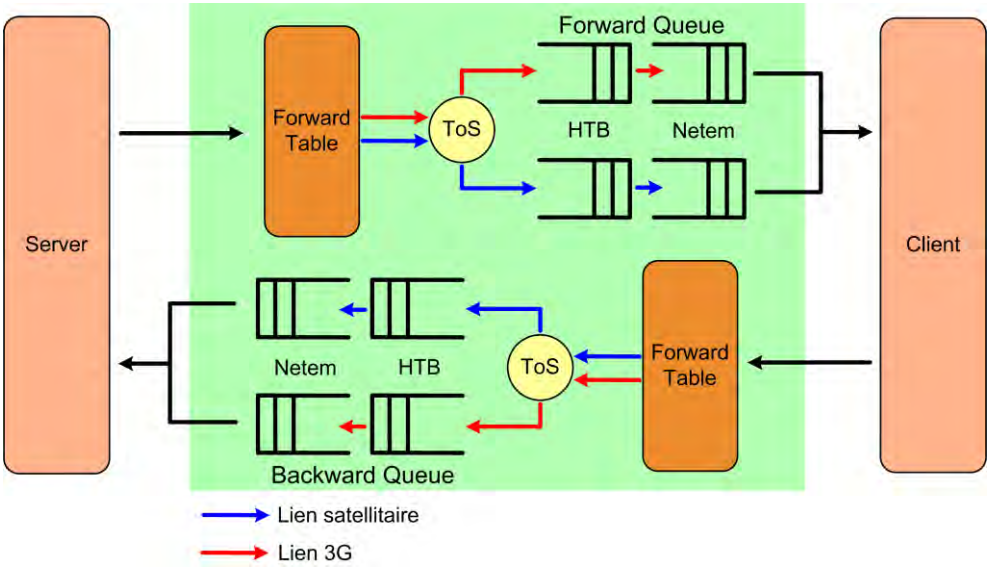


Figure 23 – Composants de l'émulateur de lien satellite SATEM d'ASTRIUM basé sur l'utilisation de files d'attentes et de NETEM.

de réseau est effectué, les nouveaux paquets sont marqués avec une nouvelle valeur et vont dans l'autre file. L'émulation du changement de réseau est alors proche de la réalité, chaque file d'attente correspondant à un lien différent. Il est ainsi possible de reproduire des mécanismes naturels comme la réception non ordonnée de paquets due aux données toujours en vol lors du changement de réseau.

La Figure 22 représente la plateforme utilisée pour les expériences sur le réseau multi-domicilié : d'un côté SATEM et de l'autre un point d'accès Wi-Fi réel tournant sous Openwrt. Les terminaux sont des ordinateurs portables sous Ubuntu et utilisant la librairie lk-sctp. La plateforme pour le réseau hybride est identique mais seul SATEM est utilisé, le changement de réseau étant effectué en interne par l'émulateur comme décrit plus haut. Les différentes mesures prises au niveau applicatif et au niveau Transport sont faites à l'aide de l'application présentée par la suite (Chapitre III, section III.2). Les mesures prises à des niveaux inférieurs sont faites avec Wireshark [90] à chaque extrémité du réseau.

Afin de pouvoir comparer les protocoles de Transport entre eux, il est nécessaire de définir une méthode de test répondant aux besoins de l'étude. L'approche choisie est de décomposer le changement de réseau en étudiant indépendamment l'impact du changement de délai et celui du changement de débit. Ensuite, l'analyse d'un changement de réseau complet (délai et débit) doit permettre de retrouver l'influence des deux caractéristiques. L'impact des caractéristiques d'un réseau étant différent suivant leur évolution (augmentation ou diminution), il est nécessaire d'observer le changement de réseau dans les deux sens : du satellite vers le Wi-Fi et du Wi-Fi vers le satellite. Enfin, nous souhaitons observer deux phases dans la communication : l'adaptation après le changement de réseau et le régime stable. Pour répondre à ces contraintes, le scénario suivant est utilisé :

1. Temps 0s : Initiation de la communication via le lien satellite,
2. Temps 20s : Changement de réseau vers le lien Wi-Fi,
3. Temps 40s : Changement de réseau vers le lien satellite,
4. Temps 60s : Fin de la communication.

Cette expérience est donc réalisée en changeant uniquement le délai, puis uniquement le débit et enfin en modifiant les deux comme lors d'un changement de réseau classique entre satellite et Wi-Fi. Les jeux de valeurs choisis pour les deux technologies sont :

- Satellite : 250ms en délai aller et 512kb/s (64ko/s) en bande passante,
- Wi-Fi : 20ms en délai aller et 2Mb/s (250ko/s) en bande passante.

Dans les expériences ne modifiant qu'une seule caractéristique lors du changement de réseau, la valeur de la caractéristique fixe est choisie pour ne pas affecter les résultats : le délai est fixé à 20ms dans l'expérience sur la bande passante et la bande passante est fixée à 2MBps dans l'expérience sur le délai.

Les expériences faites avec le réseau multi-domicilié suivent le même protocole de test. Seul le Wi-Fi aura une configuration légèrement différente car déterminé par un équipement réel et l'environnement. Néanmoins, les différences par rapport au réseau émulé sont suffisamment faibles pour être négligeables.

III.2 Développement d'un générateur de trafic SCTP supportant la mobilité et la prise de mesures

Pour l'étude de SCTP, le choix a été fait de développer notre propre application permettant de générer du trafic, gérer la mobilité et enregistrer les différents paramètres utilisés par les associations. Ce choix est né de deux constatations, SCTP n'est pas inclus de base dans le générateur de trafic Iperf [91]

utilisé pour mener les expériences du projet faites sur TCP et aucun gestionnaire de mobilité n'est implémenté dans SCTP ; seules les API sont fournies. Lors de la conception de cette application, nous nous sommes attachés à garder distinctes ses différentes fonctionnalités : d'une part la génération du trafic avec prise de mesures sur le flux et d'autre part la gestion de la mobilité avec observation des paramètres de l'association. L'architecture de l'application est représentée par la Figure 24. Trois entités majeures sont visibles dans l'espace utilisateur :

- Le générateur de trafic SCTP qui initie l'association avec le nœud distant et génère les données,
- L'agent qui a le contrôle sur l'association SCTP et mesure des paramètres internes à l'association,
- L'observateur qui scrute les évènements réseau.

Ces trois entités ont été implémentées en trois applications séparées pour deux raisons principales : l'utilisation de différents processus permet de limiter les inter-blocages et le générateur de trafic peut être remplacé par une autre application SCTP. Ces applications ont été développées sous Ubuntu 10.10 avec la librairie lk-sctp qui est la version installée par défaut sur Ubuntu et de nombreux systèmes d'exploitation Linux. Le générateur de trafic SCTP a été implémenté en C, l'observateur et l'agent ont été implémentés en C++. Les différentes classes et leurs interactions sont décrites sous la forme d'un diagramme UML sur la Figure 25.

Le générateur de trafic permet d'envoyer et de recevoir des données avec SCTP. Les arguments passés en paramètres lors du lancement permettent une configuration très précise du flux de données généré :

- Sens de la communication :
  - Emission
  - Réception,
- Paramétrage du flux de données :
  - Débit,
  - Taille des paquets,
  - Temps inter-départ,

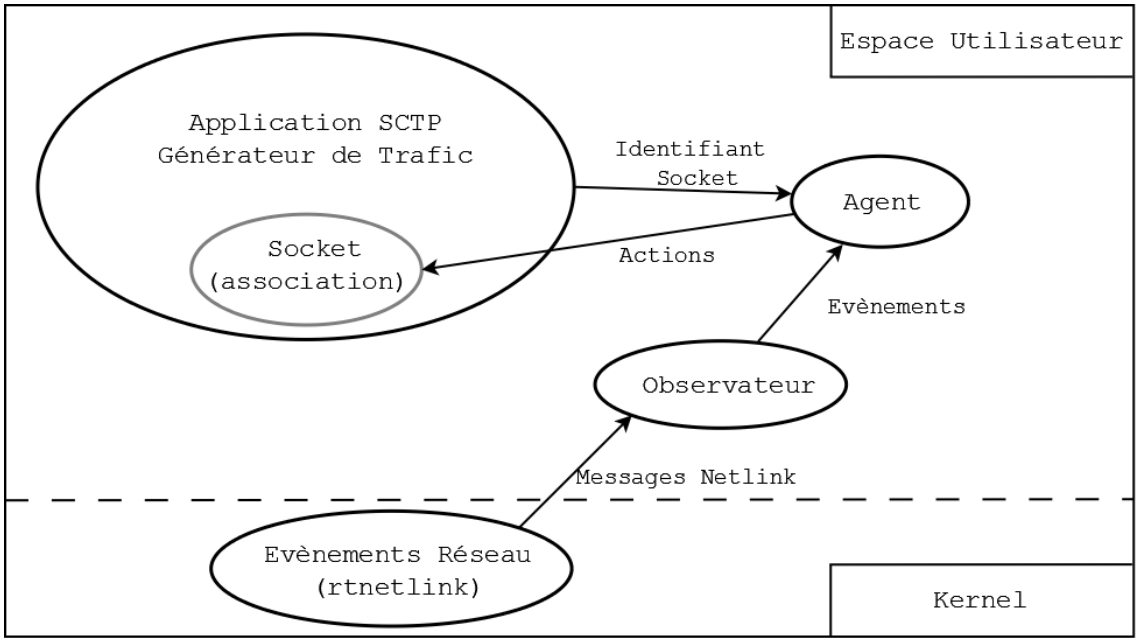


Figure 24 –Implémentation de l'application SCTP

    - Durée de l'envoi,
    - Nombre de paquets à envoyer…
- Enregistrements des temps d'émission et de réception des paquets ainsi que leur taille dans un fichier,
- Paramètres pour l'initiation de la connexion :
    - Adresse IP locale à utiliser,
    - Adresse IP distante à utiliser,
    - Port à joindre.
- Activation / Désactivation de l'agent.

Les paramètres qui ne sont pas spécifiés lors du lancement de l'application sont attribués par défaut ou déduits des autres paramètres (par exemple, le débit et la taille des paquets permettent de déduire le temps inter-départs).

L'enregistrement des temps de réception et d'émission permet d'obtenir plusieurs informations indispensables à un générateur de trafic : le débit de l'application, le délai subi par les paquets, la gigue, les pertes ou les réceptions non ordonnées. Le calcul du débit est fait simplement à partir des enregistrements. Le calcul de délai en revanche nécessite de synchroniser les deux hôtes avant la communication. Pour cela, nous utilisons le protocole « Network Time Protocol » (NTP) [89] qui permet la synchronisation de parcs de machines. Lors de la génération d'un paquet de données, l'émetteur met une étiquette temporelle dans le champ de données et complète le reste pour obtenir la taille adéquate. La comparaison de cette étiquette avec le temps courant lors de la réception du paquet permet de déduire le délai du flux au niveau applicatif (appelé délai applicatif par la suite).

L'observateur de la Figure 24 est chargé de guetter les évènements réseau qui pourraient être pertinents pour le gestionnaire de mobilité. Il va effectuer un premier filtre parmi la multitude d'informations que peuvent contenir les messages « netlink », comme par exemple le changement de l'adresse IP d'une interface réseau, la détection d'un nouveau réseau, l'établissement d'une connexion au niveau Liaison, la modification de la table de routage… Ces informations sont alors mises sous la forme d'un évènement daté avec la classe « Event Descriptor » et transmises à l'agent via une file de type FIFO.

L'agent est le composant « intelligent » de notre implémentation, il est en charge de la gestion de la mobilité et de l'enregistrement des paramètres des associations. Lors de l'initiation d'une association, l'application SCTP transmet l'identifiant du socket à l'agent via une file UNIX. Cette manœuvre n'est possible que si l'application utilise un socket non-bloquant car, dans le cas contraire, l'agent ne pourra jamais prendre la main. Une fois l'identifiant du socket en sa possession, l'agent est alors capable d'interagir avec l'association SCTP avec les API et ainsi obtenir certaines informations ou effectuer des actions. Périodiquement, l'agent va ainsi aller vérifier l'état de l'association, ce qui permet d'avoir accès à l'état des chemins et aux variables suivantes pour le chemin principal :

- Etat des différents chemins (primaire, actif, en attente de détermination…),
- Taille de la fenêtre de congestion, variable CWND,
- « Smoothed Round Trip Time », variable SRTT,
- « Retransmission Time Out », variable RTO.

L'enregistrement des paramètres de l'association en complément du débit et du délai permet d'obtenir une analyse plus profonde de la communication et ainsi de comprendre le comportement de SCTP dans certaines situations. La seconde fonction de l'agent est la gestion de la mobilité, il va se baser pour cela sur les évènements réseau remontés par l'observateur. Toujours en utilisant les API de SCTP, l'agent est capable d'effectuer les actions suivantes :

- Ajout/Suppression d'une adresse IP à l'association pour l'hôte local et l'hôte distant,
- Changement du chemin prioritaire du flux de données,
- Envoi d'un Heart Beat sur un chemin.

Le changement de réseau peut alors se faire entièrement avec SCTP et sans action extérieure. Afin d'obtenir un comportement adéquat de l'agent, il est néanmoins nécessaire de lui fournir une certaine base de connaissances. Par exemple, la connexion à un réseau peut entrainer la configuration de l'adresse IP de différentes manières : statique, autonome ou avec DHCP.

Le diagramme de séquence de la Figure 26 présente les réactions de l'observateur et de l'agent après la détection d'un nouveau réseau. Deux phases sont visibles : la détection du nouveau réseau qui entraine la configuration d'une nouvelle adresse IP puis la notification d'une adresse IP configurée qui entraine l'ajout de cette adresse à l'association et le changement du chemin primaire. Cette séquence correspond donc exactement à un changement de réseau avec mSCTP.

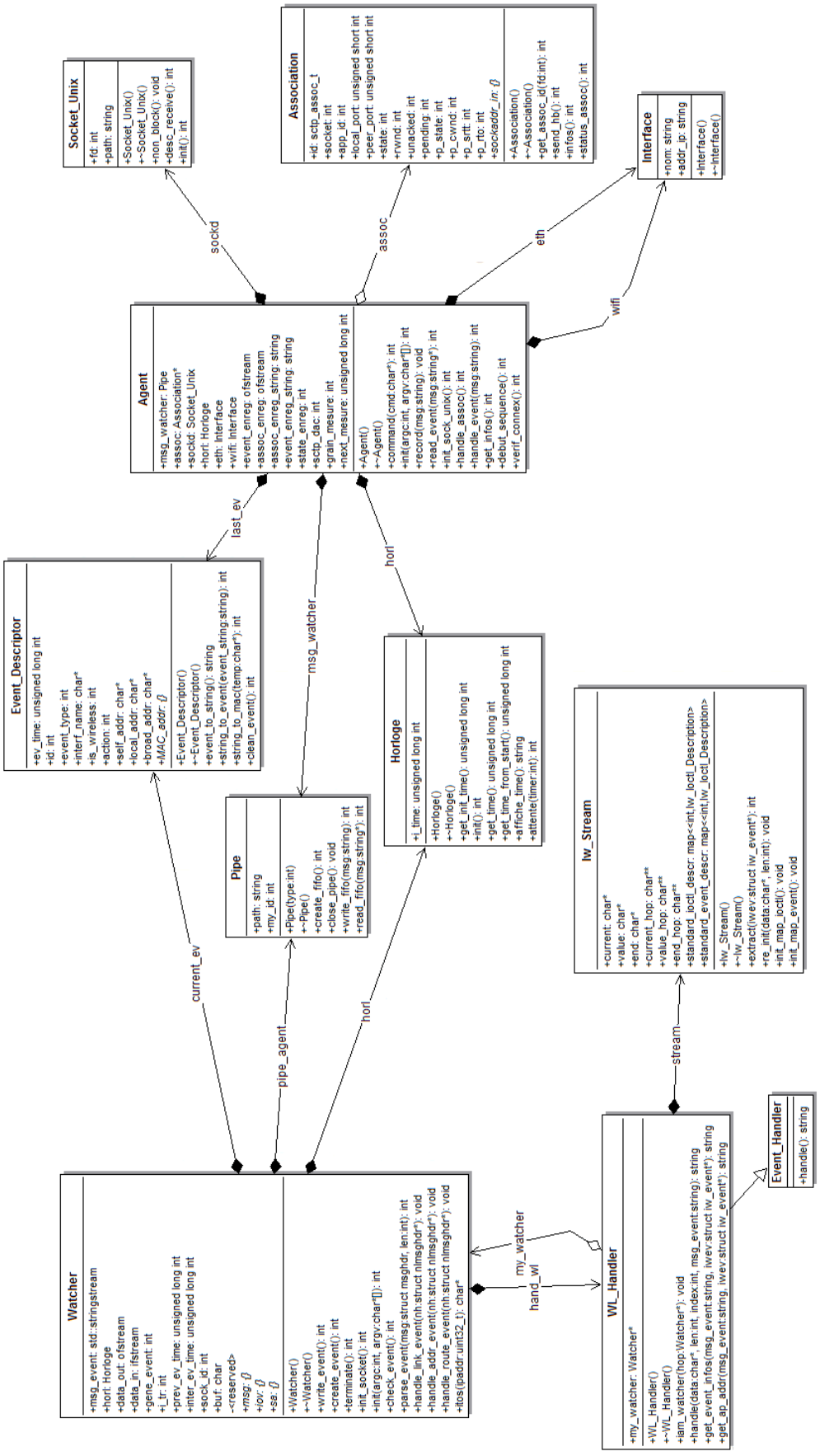


Figure 25 – Diagramme UML de l'observateur et de l'agent utilisés dans l'application SCTP.

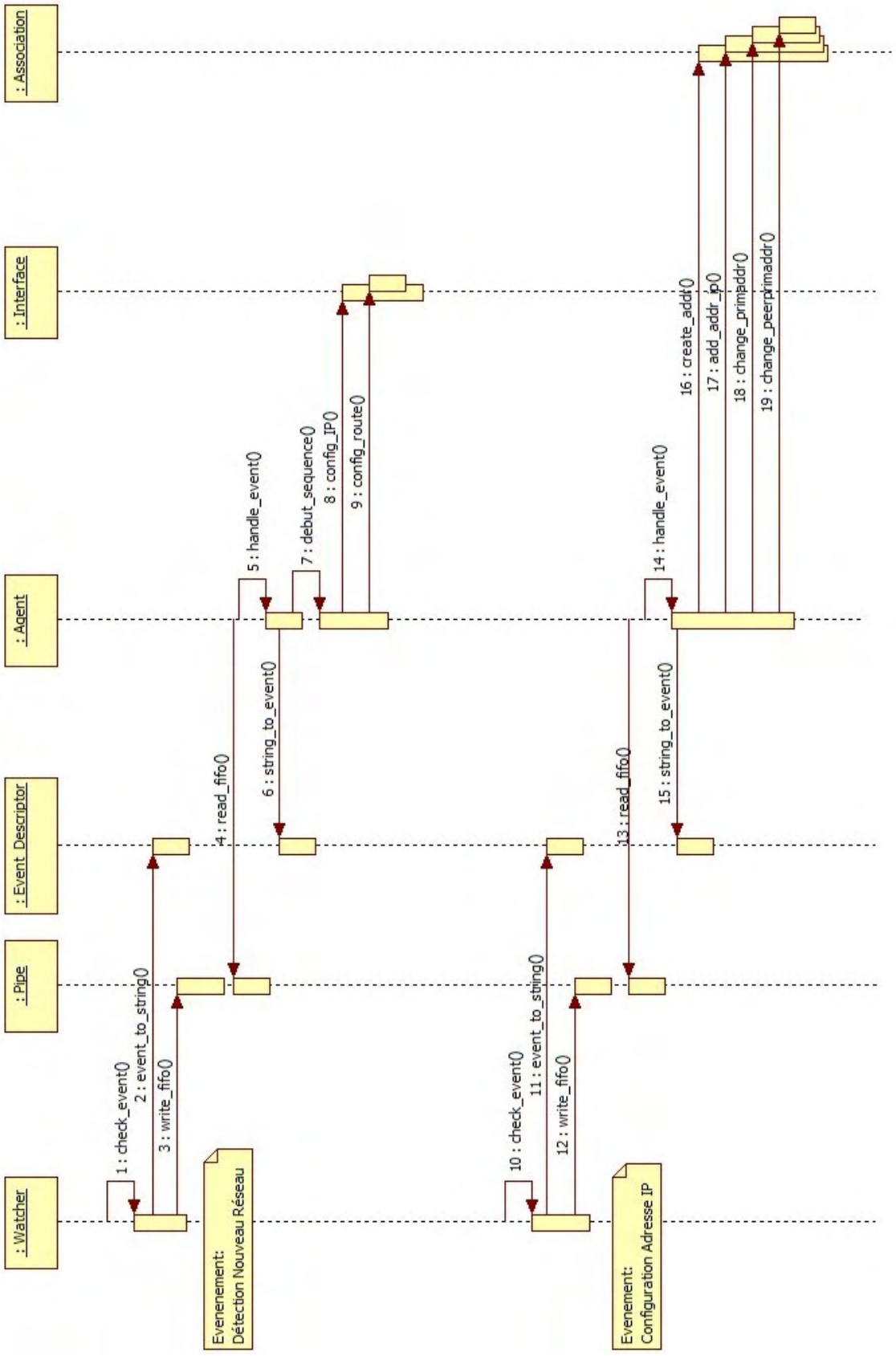


Figure 26 – Diagramme de séquence décrivant les réactions suivant la détection d'un nouveau réseau : configuration d'une nouvelle adresse et ajout à l'association.

III.3 SCTP face au changement de réseau dans un contexte hybride

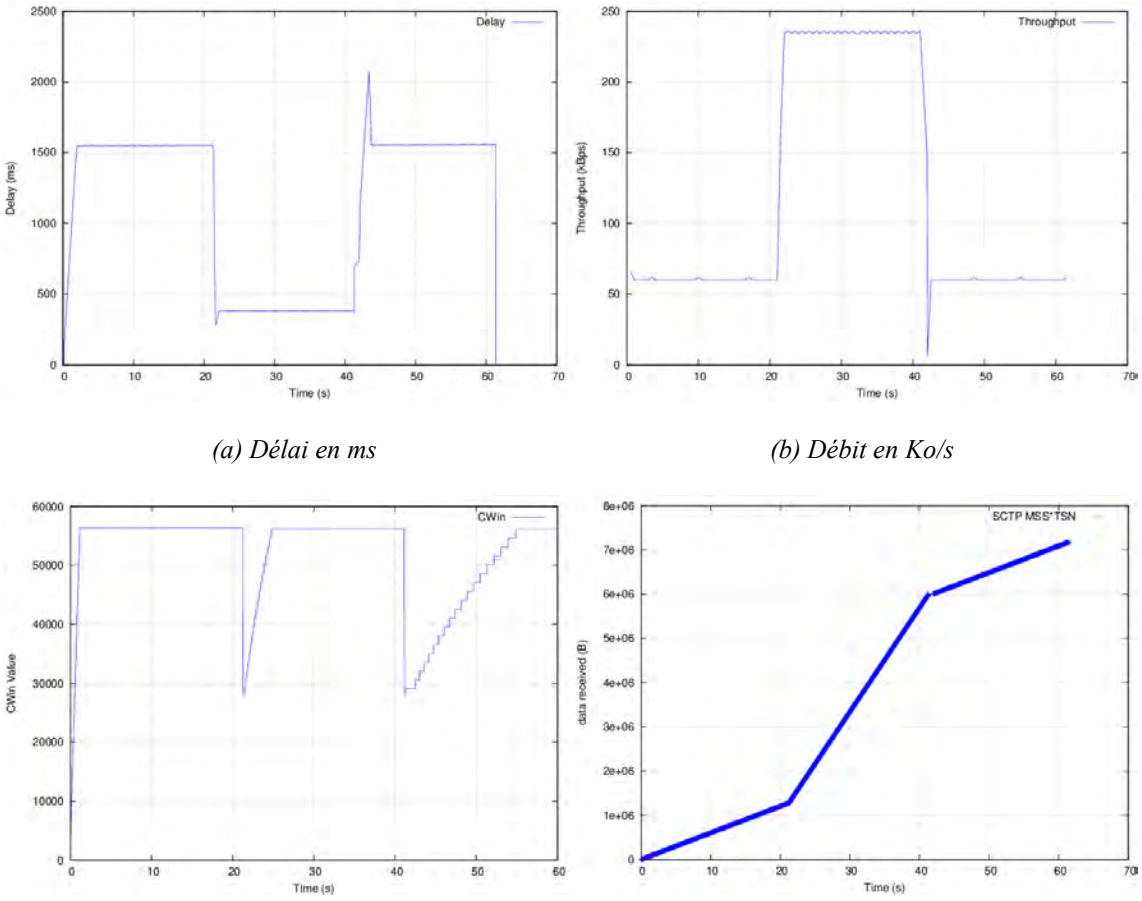
Comme indiqué précédemment, nous avons étudié l'impact du changement de réseau en le divisant en trois études distinctes : bande passante, délai et les deux réunis. Ces expériences reprennent le protocole de test décrit en III.1.

III.3.1 Changement de débit

Dans cette étude, le délai de propagation est fixé à 20ms pour le lien satellite et le lien Wi-Fi. Seule la bande passante change de 64ko/s à 250ko/s. La Figure 27 présente les mesures prises au cours de cette expérience : le délai applicatif (a), le débit de l'application (b), la fenêtre de congestion de l'association (c) et la quantité de données reçues depuis le début (d).

Un phénomène intéressant se produit dans cette expérience : même si le délai de propagation est fixé à 20ms, il est clairement visible que le délai applicatif est largement supérieur, spécialement sur le réseau satellite. D'un autre côté, la mesure du débit applicatif permet de conclure que la bande passante maximale est atteinte. Il y a donc une congestion qui se crée sur le réseau et celle-ci se traduit par un stockage des données dans les files d'attente. La bande passante sur le réseau satellite étant plus faible que sur le réseau Wi-Fi, plus de paquets sont stockés et le délai applicatif est plus important.

La limitation de la bande passante a un impact sur les communications mais il pourrait sembler logique que la fenêtre de congestion vienne corriger cet impact en limitant son débit d'émission.



(a) Délai en ms *(b) Débit en Ko/s*

(c) Fenêtre de congestion en octets *(d) Données reçues en octets*

Figure 27 – Mesures faites sur le réseau hybride avec un changement de réseau uniquement sur le débit de satellite vers Wi-Fi (20s) puis Wi-Fi vers satellite (40s).

Pourtant il n'en est rien : la fenêtre de congestion sur le réseau satellite augmente rapidement jusqu'à atteindre sa valeur maximale même si le lien a un faible délai et une faible bande passante. Les files d'attente étant capable de stocker toutes les données envoyées, il n'y a pas de suppression de paquets et la fenêtre reste stable.

La Figure 28 se focalise sur l'évolution de la fenêtre de congestion pendant les deux premières secondes de l'expérience. Deux autres valeurs sont aussi présentes : la quantité de données en vol calculée à partir des relevés et une estimation théorique de l'évolution de la fenêtre de congestion. Les valeurs prises pour cette estimation sont calculées à partir du comportement de la fenêtre décrit dans la RFC de SCTP [64] et visibles dans le Tableau 7. Il s'agit de l'algorithme « Slow Start » : lors de la réception d'un acquittement si des données sont en attente, la fenêtre de congestion est augmentée du minimum entre un MTU et la quantité de données acquittées. Les résultats obtenus lors de cette expérience sont donc en accord avec l'estimation : la fenêtre de congestion grandit rapidement puis se stabilise. La fenêtre de congestion estimée est affichée en utilisant la date d'arrivée réelle des acquittements et la valeur estimée correspondante ; la première arrivée correspond à la première valeur et ainsi de suite.

Lors de l'augmentation ou de la diminution du débit (temps 20s et 40s), la fenêtre de congestion est diminuée puis augmente lentement jusqu'à atteindre sa valeur précédente. Ce comportement est typique de la réception de paquets non ordonnés et du déclenchement de l'algorithme Fast Retransmit / Fast Recovery. Lors de cette expérience, seule l'association étudiée est présente sur le réseau ; les files d'attente du nouveau réseau après le basculement sont donc entièrement vides. Les délais de propagation étant ici fixés à la même valeur pour le satellite et le Wi-Fi, les paquets traversant le nouveau réseau vont donc subir un délai plus faible pendant que les files d'attente de l'autre réseau se vident. Une fois que les paquets signalés non ordonnés ont été reçus correctement, la fenêtre passe en mode « Congestion Avoidance ». L'accroissement est alors plus lent sur le réseau satellite car dans ce régime la fenêtre augmente de 1 MTU par RTT et non à chaque réception d'acquittements (le RTT plus grand du satellite est du dans ce cas à la faible bande passante et au remplissage des files).

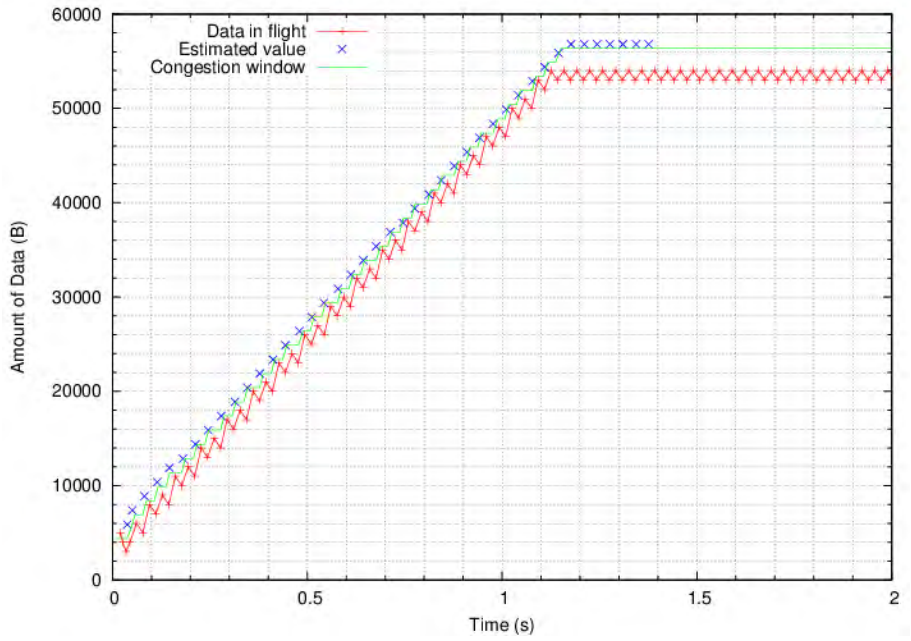


Figure 28 – Fenêtre de congestion mesurée et calculée théoriquement comparées à la quantité de donnée en vol durant les 2 premières secondes.

Tableau 7 – Calcul théorique de la valeur de la fenêtre de congestion après l'initiation de la connexion (premières séries d'acquittements sélectifs).

Sack	Données acquittées (Octets)	Temps	Taille de la fenêtre (Octets)
sack1	2 000	t0+RTT	5 880
sack1	2 000	t0+RTT	7 380
sack2	2 000	t0+2*RTT	8 880
sack2	2 000	t0+2*RTT	10 380
sack2	2 000	t0+2*RTT	11 880
sack2	1 000	t0+2*RTT	12 880
sack3	2 000	t0+3*RTT	14 380
…	…	…	…
sack3	2 000	t0+3*RTT	21 880
sack4	2 000	t0+4*RTT	23 380
…	…	…	…
sack4	1 000	t0+4*RTT	37 880
sack5	2 000	t0+5*RTT	39 380
…	…	…	…
sack5	2 000	t0+5*RTT	49 880
sack5	2 000	t0+5*RTT	51 380
sack5	2 000	t0+5*RTT	52 880
sack5	2 000	t0+5*RTT	54 380
sack5	2 000	t0+5*RTT	55 880
sack5	2 000	t0+5*RTT	56 800
sack5	2 000	t0+5*RTT	56 800
…	…	…	…
sack5	1 000	t0+5*RTT	56 800

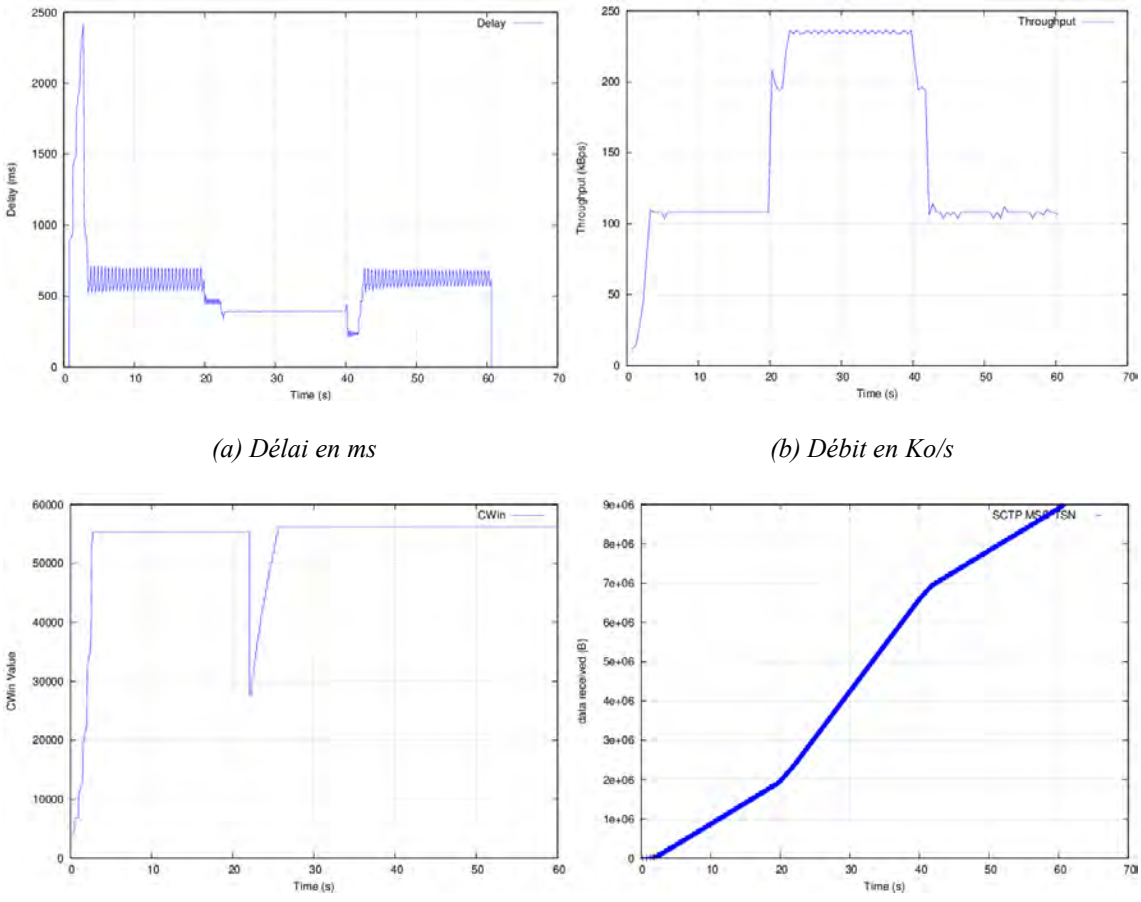
III.3.2 Changement de délai

Dans cette étude, la bande passante allouée pour chaque lien est fixée à 2Mbps, le délai à 20ms pour le W-Fi et à 250ms pour le satellite. Les mesures effectuées sont présentées par la Figure 29. Plusieurs remarques peuvent être faites à la vue de ces courbes :

- Le délai subi par l'application ne varie pas énormément entre satellite et Wi-Fi même si le délai de propagation est très différent,
- Le débit de l'application semble limité à 110 Ko/s sur le lien satellite alors la bande passante est de 2Mbps,
- La fenêtre de congestion diminue lors du changement de délai puis remonte pour reprendre la valeur atteinte sur le réseau satellite,
- Le flux de donnée côté récepteur est régulier et ne présente pas de coupure aux changements.

La faible différence de délai entre les deux technologies est déductible de la première expérience : sur le réseau Wi-Fi la présence de congestion implique un remplissage des files alors que sur le réseau satellite il n'y a plus de congestion car le débit mesuré est inférieur à la bande passante disponible. Cette remarque est donc en lien avec la seconde : le débit sur le lien satellite semble limité autour de 110Ko/s.

Ce débit maximal est du à la valeur limite de la fenêtre de congestion fixée par la librairie lk-sctp. Dans cette expérience comme dans la précédente, la fenêtre ne dépasse pas 57000 octets. Le RTT sur



(a) Délai en ms *(b) Débit en Ko/s*

(c) Fenêtre de congestion en octets *(d) Données reçues en octets*

Figure 29 – Mesures faites sur le réseau hybride avec un changement de réseau uniquement sur le délai, de satellite vers Wi-Fi (20s) puis Wi-Fi vers satellite (40s).

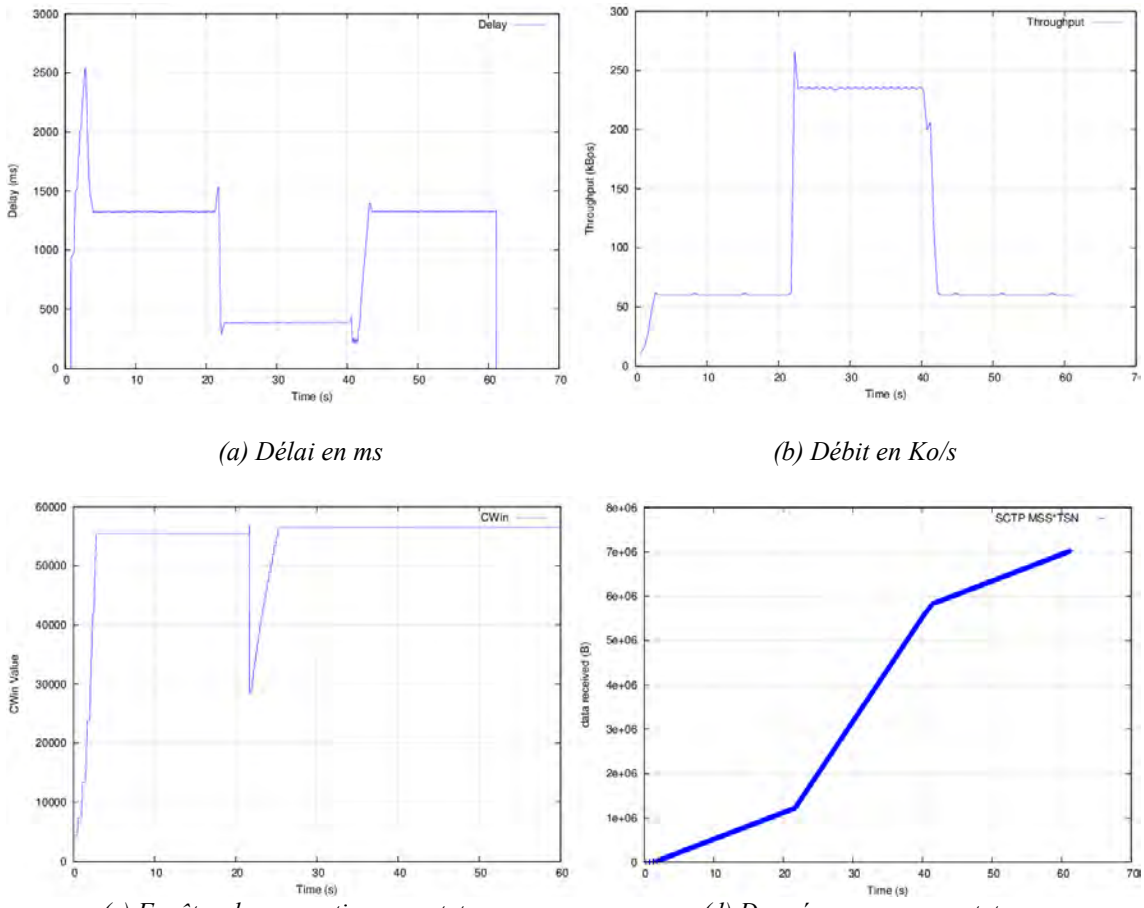
un lien satellite étant de 500ms, il est facile de déduire que le débit maximal sur un lien satellite ne peut dépasser les 110Ko/s. Si de prime abord une telle limite peut paraître insuffisante car elle empêche un flux d'utiliser toute la bande passante, il est peu probable qu'un seul flux ait autant de bande passante disponible sur un réseau satellite : plusieurs applications sont souvent actives en même temps et la bande passante offerte par une connexion satellite est bien en-dessous de 110Ko/s, particulièrement dans le sens montant (cas étudié ici).

Lors du passage du réseau satellite au réseau Wi-Fi, le comportement de la fenêtre de congestion est le même que dans l'expérience précédente : la réception de paquets non ordonnés provoque une chute puis une reprise en Congestion Avoidance. Ceci est normal puisque le délai sur le lien satellite est supérieur au délai sur le lien Wi-Fi. Par contre, il n'y a ici pas de réception de paquets non ordonnés lors du passage de Wi-Fi vers satellite : même en présence de congestion et de files remplies, le délai sur le lien Wi-Fi reste inférieur.

III.3.3 Changement de réseau complet (débit et délai)

Cette étude peut être vue comme la synthèse des deux précédentes. Lors du changement de réseau, les deux caractéristiques sont modifiées suivant les valeurs fixées par le protocole de test. La Figure 30 présente des mesures prises pendant cette expérience : délai (a), débit (b), fenêtre de congestion (c) et quantité de données reçues en fonction du temps (d).

Au vu des mesures, il est clair que les influences du débit et du délai étudiées dans les expériences précédentes sont visibles : les délais applicatifs sont largement au dessus des délais de propagation ce



(a) Délai en ms *(b) Débit en Ko/s*

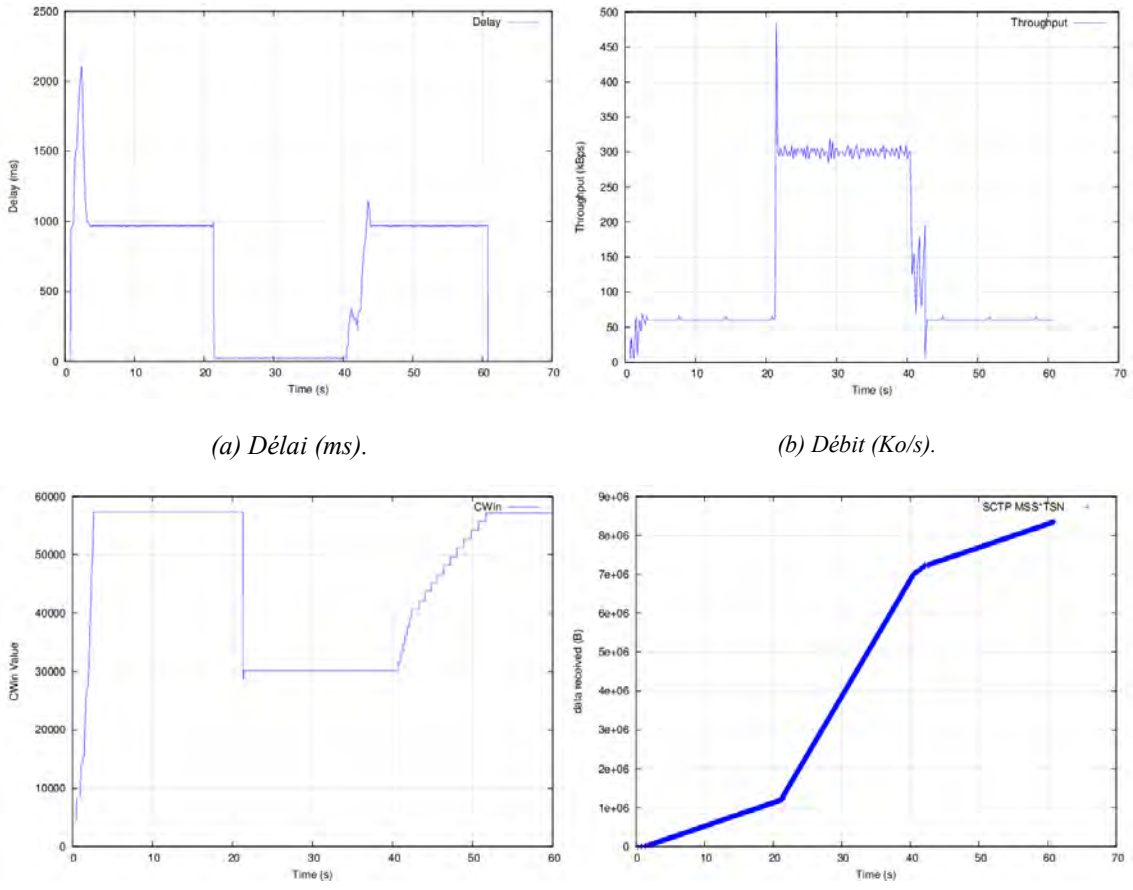
(c) Fenêtre de congestion en octets *(d) Données reçues en octets*

Figure 30 – Mesures faites sur le réseau hybride avec un changement de réseau complet de satellite vers Wi-Fi (20s) puis Wi-Fi vers satellite (40s) avec congestion sur le lien Wi-Fi.

qui dénote un fort remplissage des files d'attente. Comme prévu, la fenêtre de congestion grandit rapidement jusqu'à atteindre sa valeur maximale. Après le premier changement de réseau, des réceptions non ordonnées de paquets apparaissent et sont compensées par l'utilisation de l'algorithme Fast Retransmit / Fast Recovery suivi par une phase de congestion avoidance. Après le second changement de réseau, la fenêtre de congestion reste stable, les paquets étant tous reçus dans l'ordre.

Les expériences menées sur le changement du délai, du débit et des deux à la fois ont été faites sur un réseau Wi-Fi congestionné. En effet, le débit de l'application était de 300Ko/s alors que la bande passante était de 2Mbps soit 250Ko/s. Afin que les expériences faites en réseau hybride et réseaux multi-domiciliés puissent être comparés, nous avons exécuté le scénario à nouveau avec une bande passante de 10Mbps sur le lien Wi-Fi.

La Figure 31 présente les mesures faites au cours de cette expérience. Le délai sur le lien Wi-Fi est faible (autour de 20ms) et le débit atteint 300Ko/s. De plus la fenêtre de congestion a une valeur plus faible : 30000 octets environ contre 58000 octets dans le cas congestionné. Si cette valeur est proche du cas multi-domicilié (voir expérience suivante), la méthode utilisée pour la déterminer n'est pas adéquate. Lors du changement de réseau de Wi-Fi vers satellite, la réception de données non ordonnées conduit à l'utilisation de l'algorithme Fast Recovery / Fast Retransmit. La fenêtre de congestion est alors divisée et reprend en congestion avoidance. A ce moment-là, des données sont en attente d'être émises car la file entre l'application et le socket est plein (à cause de la congestion sur le lien satellite). La réception d'un acquittement provoque donc l'augmentation de la fenêtre de congestion. Après 1 RTT, les données en attente ont été envoyées et la réception d'un acquittement



(a) Délai (ms). *(b) Débit (Ko/s).*

(c) Fenêtre de congestion (B). *(d) Données reçues (B).*

Figure 31 – Mesures faites sur le réseau hybride avec un changement de réseau complet de satellite vers Wi-Fi (20s) puis Wi-Fi vers satellite (40s) sans congestion sur le lien Wi-Fi.

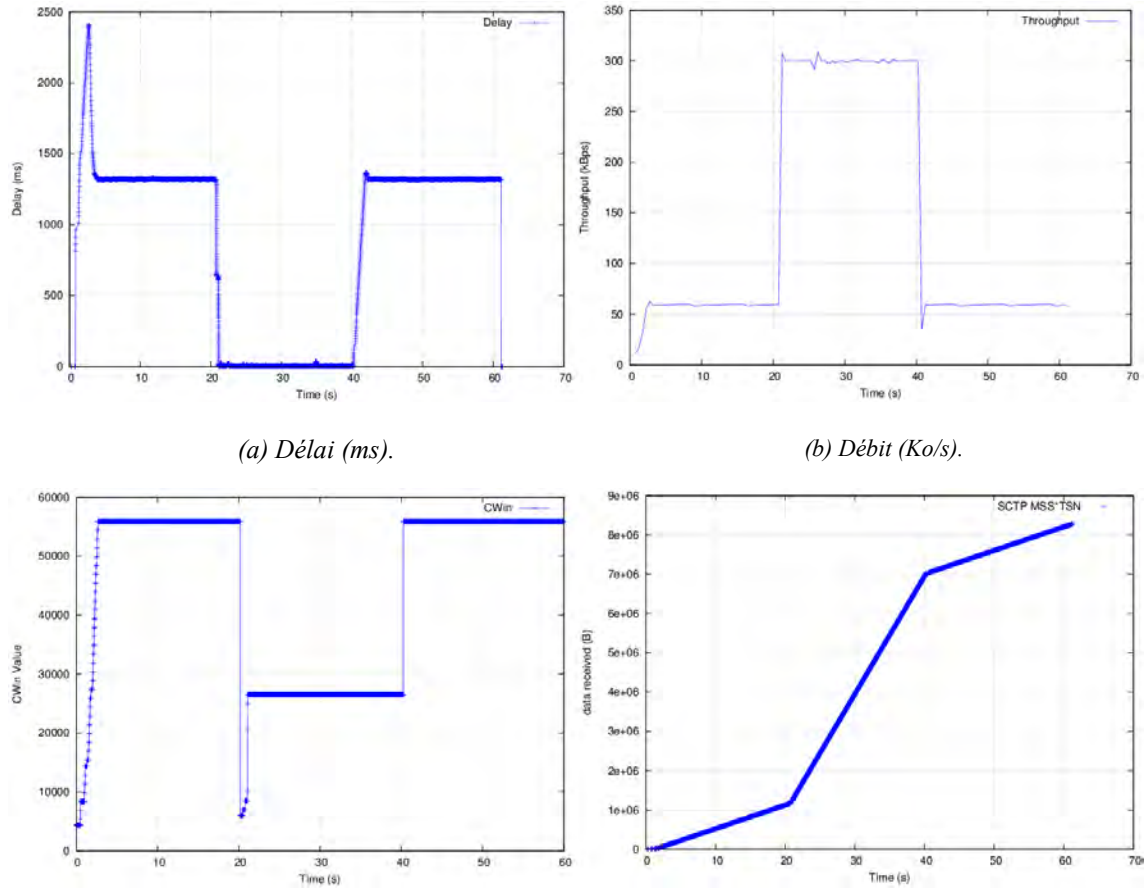
n'augmente plus la fenêtre, celle-ci étant suffisamment grande pour transmettre un flux à 300Ko/s. La fenêtre de congestion se stabilise donc à une valeur déterminée en grande partie par la diminution de moitié appliquée par l'algorithme Fast Recovery / Fast Retransmit.

III.4 Comportement de SCTP dans les réseaux multi-domiciliés

Les expériences menées dans cette sous-section utilisent les capacités de multi-domiciliation de SCTP. Le protocole de test défini précédemment est repris en utilisant un point d'accès Wi-Fi réel en plus de SATEM comme spécifié en III.1. En revanche, la bande passante du Wi-Fi n'étant pas limitée à 2Mbps, il n'y a ni congestion ni remplissage des files d'attente sur le lien Wi-Fi.

Comme détaillé dans le Chapitre III, section I, SCTP en multi-domicilié distingue chaque chemin en se basant sur les adresses de destination et calcule des paramètres réseaux pour chacun d'eux (CWND, SRTT, RTO, MTU…). Dans les courbes présentées par la suite, il est fondamental de distinguer les mesures faites sur le chemin Wi-Fi ou sur le chemin satellite. Pour cela, plusieurs résultats sont présentés en indiquant les points de mesures afin de distinguer une évolution rapide lors du passage à un autre jeu de paramètres.

La Figure 32 présente les mesures faites avec un nœud multi-domicilié : délai (a), débit (b), fenêtre de congestion (c) et quantité de données reçues au cours du temps(d).



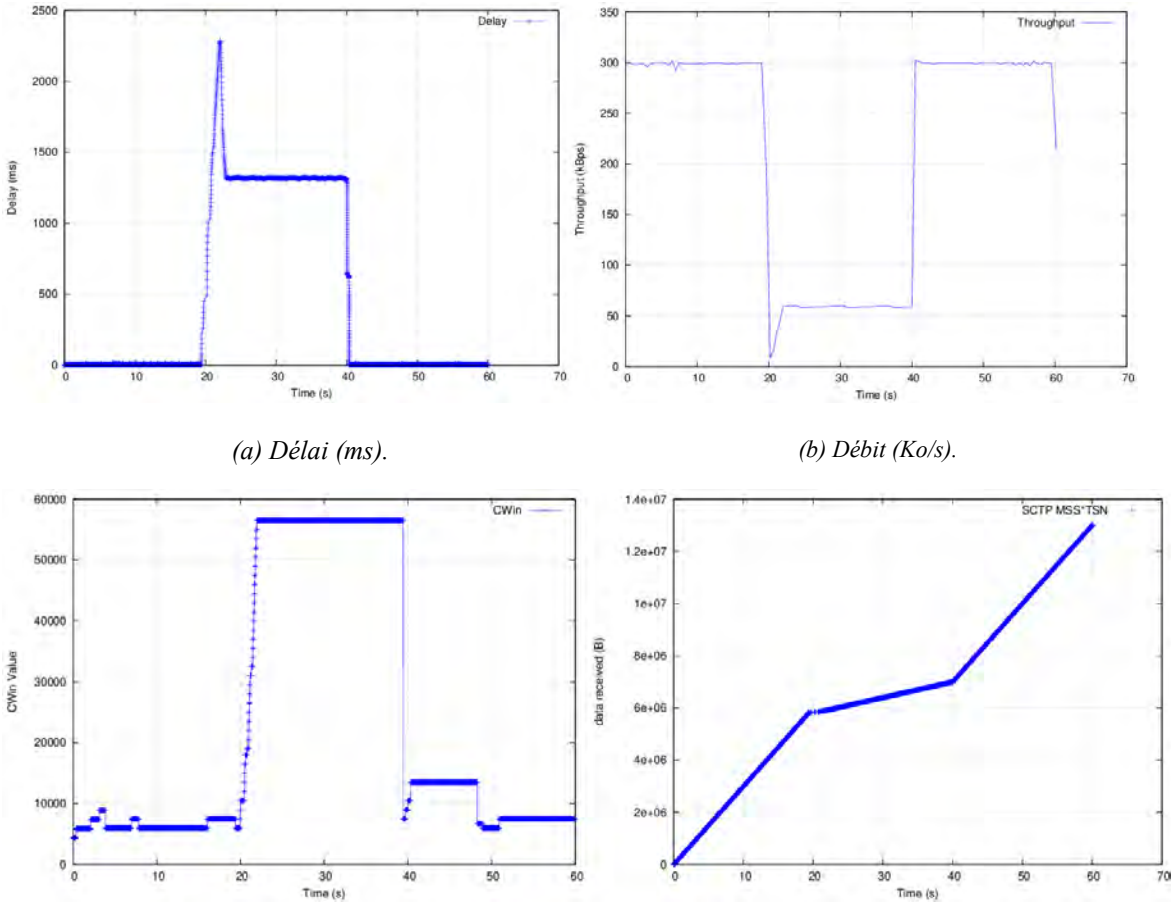
(a) Délai (ms). *(b) Débit (Ko/s).*

(c) Fenêtre de congestion (B). *(d) Données reçues (B).*

Figure 32 – Mesures faites sur le réseau multi-domicilié avec des changements de réseau complets de satellite vers Wi-Fi (20s) puis Wi-Fi vers satellite (40s).

Le comportement de la fenêtre de congestion est particulièrement intéressant. Lors du premier changement de réseau, un nouveau jeu de paramètres avec leurs valeurs initiales est utilisé. La fenêtre de congestion sur le réseau Wi-Fi reprend donc en-dessous de 10000 octets et se stabilise à 28000 octets. Il y a donc légèrement moins de paquets en vol et les files d'attente sont moins remplies que dans l'expérience sur le réseau hybride. Lors du second changement de réseau, la fenêtre de congestion reprend sa précédente valeur sur le réseau satellite et repart donc au régime stable directement.

La valeur de la fenêtre de congestion sur le réseau Wi-Fi est pourtant élevée comparé au délai de quelques dizaines de millisecondes subi par l'application. Afin de vérifier cette valeur, nous avons effectué une expérience avec le même banc de test multi-domicilié en initiant l'association sur le lien Wi-Fi. A 20s, un changement de réseau vers le lien satellite est réalisé, puis un autre à 40s pour revenir sur le réseau Wi-Fi. Les mesures faites pendant cette expérience sont visibles la Figure 33. Pour reprendre la remarque précédente, la fenêtre de congestion sur le réseau Wi-Fi est en dessous de 10000 octets après l'initiation de l'association. Après le second changement de réseau, cette valeur est reprise mais la fenêtre grandit jusqu'à 15000 octets pendant un peu moins de 10s avant de se stabiliser en dessous de 1000 octets. Cette augmentation après le passage sur le réseau satellite s'explique par la congestion qui y est présente : la bande passante est insuffisante comparée au débit de l'application, la file d'attente entre l'application et le socket se remplit. Une valeur supérieure de la fenêtre de congestion est alors nécessaire pour la vider. On peut en déduire que la taille relativement élevé de la



(a) Délai (ms). *(b) Débit (Ko/s).*

(c) Fenêtre de congestion (B). *(d) Données reçues (B).*

Figure 33 – Mesures faites sur le réseau multi-domicilié avec des changements de réseau complets de Wi-Fi vers satellite (20s) puis satellite vers Wi-Fi (40s).

fenêtre de congestion sur le lien Wi-Fi dans les expériences précédentes est aussi liée à ce phénomène.

Nous avons vu que SCTP utilise un nouveau jeu de valeurs lors du passage sur un nouveau réseau. Si ce comportement permet d'évaluer correctement les capacités du lien, cette expérience montre aussi un inconvénient majeur. Lors du changement entre Wi-Fi et satellite, le débit chute bien en dessous de sa valeur optimale pendant 2s. Il s'agit du temps nécessaire à la fenêtre de congestion pour atteindre sa valeur optimale sur le lien satellite, des valeurs initiales étant prises pour les paramètres.

III.5 Comparaison des différents protocoles

Cette section présente une brève comparaison entre plusieurs protocoles de Transport testés au cours du projet SAT-PERF : SCTP dans un réseau hybride et dans un réseau multi-domicilié, Cubic TCP, Compound TCP, Hybla TCP et TCP New Reno. Le point d'accès Wi-Fi utilisé pour le réseau multi-domicilié ne limitant pas la bande passante, SCTP en multi-domicilié va forcément réaliser de meilleures performances et sa présence dans cette comparaison est uniquement à titre indicatif.

La Figure 34 présente la quantité de données reçues en fonction du temps pour chaque protocole de Transport. Les trois phases des communications sont clairement visibles et permettent d'analyser le comportement des protocoles suivant la situation. Avant le premier changement de réseau, un protocole est clairement au dessus du lot : TCP Hybla a été conçu pour transmettre des données sur des liens satellites, ce qui se voit dans les mesures. SCTP et Compound TCP se comportent de manière similaire et sont réguliers. TCP New Reno et Cubic sont les plus affectés par le réseau satellite même si Cubic accélère à partir de 12s sans doute à cause de son comportement proche d'une fonction cubique.

Seulement trois protocoles ne semblent pas affectés par le changement de réseau : SCTP, Coumpound

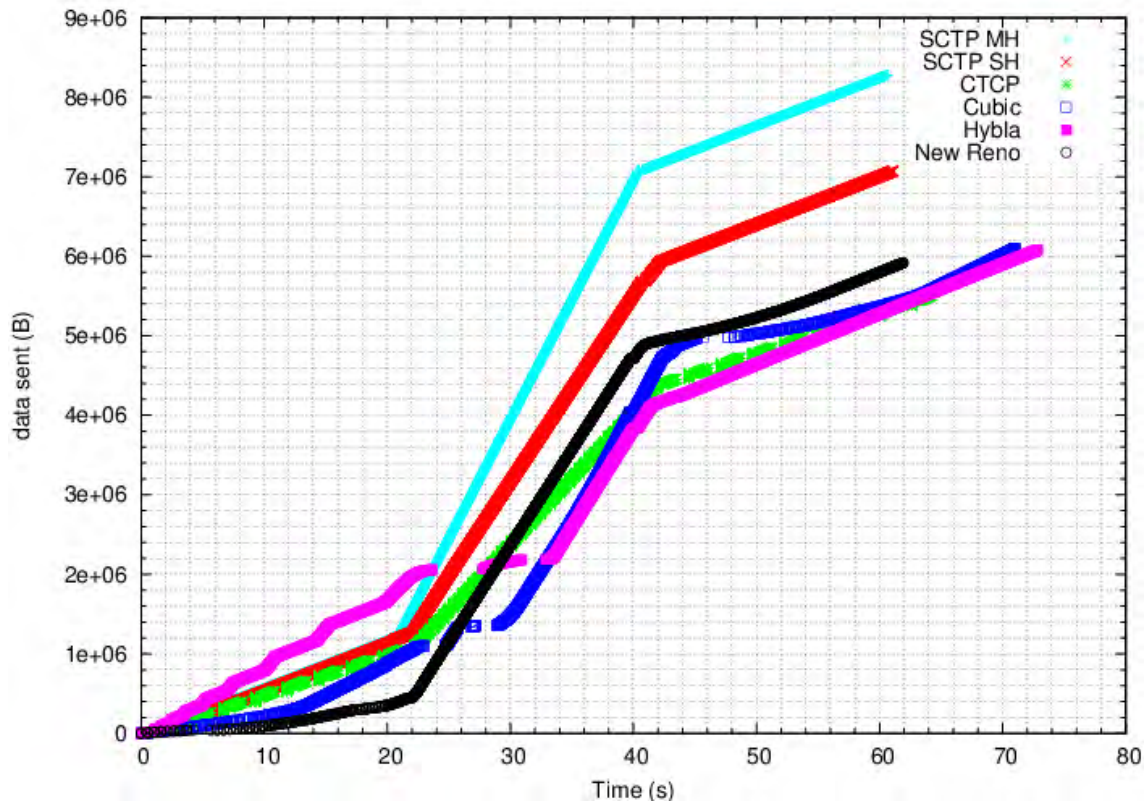


Figure 34 – Comparaison des données reçues pour différents protocoles de Transport.

TCP et New Reno. Aucun de ces protocoles ne présente de coupure apparente dans le flux de données ce qui signifie qu'ils sont peu impactés par le changement. Néanmoins, les performances de Compound pendant toute la durée de la communication sur le réseau Wi-Fi sont inférieures aux autres protocoles. Sa fenêtre basée sur l'estimation du temps peut être un frein après le changement de réseau. TCP Hybla et Cubic sont gravement affectés par le changement de réseau : environ 5s et 10s sont nécessaires respectivement à Cubic et à Hybla pour envoyer un flux régulier. De plus, le flux de données généré par Hybla est alors similaire au flux de New Reno, ce qui peut laisser penser que le protocole est repassé sur une fenêtre de congestion classique.

Le second changement de réseau affecte moins les communications : seul Cubic semble affecté. Par contre, il est important de remarquer que, même de retour sur le lien satellite, Hybla continue à émettre un flux régulier semblable à celui de New Reno.

La Figure 35 montre les débits sortants des nœuds mobiles pour chaque protocole de Transport. Les résultats observés sur le flux de données sont aussi visibles avec cette mesure. L'envoi par à-coups utilisé par TCP Hybla pour obtenir de meilleures performances sur satellite est seulement visible avant le premier changement de réseau, son comportement après le second changement de réseau étant complément différent. Compound n'est pas stable (envoi par à-coups) mais reste régulier contrairement à Cubic qui nécessite un certain temps pour atteindre des performances optimales. Les performances de New Reno sur le réseau satellite sont les moins bonnes mais il s'adapte très rapidement en arrivant sur le lien Wi-Fi. En fait, il s'agit du seul TCP atteignant le débit de SCTP sur le lien Wi-Fi.

Au vu de ces résultats, il semble que SCTP obtienne globalement de meilleures performances que les versions de TCP testées. Il faut quand même nuancer : sur satellite Hybla permet d'atteindre un meilleur débit et sur Wi-Fi New Reno atteint un débit similaire. Néanmoins, aucun des ces deux protocoles n'est vraiment performant sur l'autre technologie.

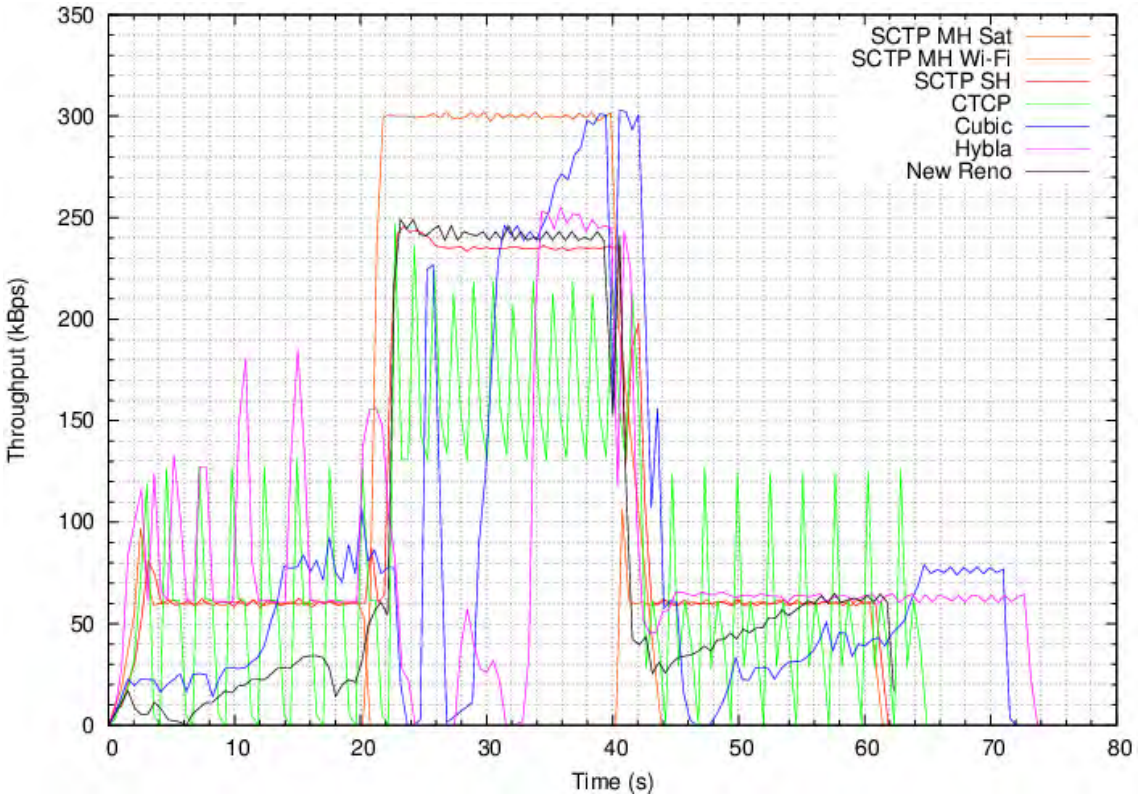


Figure 35 – Débit d'émission pour plusieurs protocoles de Transport.

IV Bilan de l'étude de SCTP et de ses performances

Dans ce chapitre, nous avons étudié le protocole de Transport SCTP dans différent contexte et l'avons comparé au protocole de Transport de référence TCP. Cette étude a été menée en deux temps. Dans un premier temps, nous avons étudié le comportement de SCTP sur un lien n'étant pas soumis aux contraintes de la mobilité. Dans un second temps, l'étude s'est portée sur l'impact du changement de réseau sur le protocole. En réalisant cette deuxième étude sur un réseau hybride et sur un réseau multi-domicilié, une vision globale des performances de SCTP peut être obtenue.

L'étude menée sur un lien fixe permet de mettre en avant les similarités qui existent entre SCTP et TCP. Dans le cas d'un flux simple, leurs mécanismes de gestion des données et de prévention de la congestion sont relativement proches. Il est donc normal que leurs comportements dans la première partie de notre étude soient similaires. Les performances des deux protocoles sont alors équivalentes : même sur un réseau contraignant possédant une différentiation des flux, le débit est toujours égal au maximum de la bande passante disponible. En analysant leur comportement, on constate même que ces protocoles possèdent le même point faible : ils remplissent les files d'attente pour évaluer la congestion. Ce comportement est typique des protocoles de Transport évaluant la congestion en se basant sur les pertes.

Les changements de réseau transparent soumettent les protocoles de Transport à des évènements particuliers. Le banc de test que nous avons mis en place nous a permis d'étudier l'impact de ce phénomène sur SCTP. En étudiant séparément deux des paramètres modifiés par le changement de réseau, nous avons pu déterminer l'origine de certains évènements mal interprétés par les protocoles de Transport, notamment la réception de données dans le désordre provoquée par la différence de délai entre les deux chemins. L'utilisation des capacités de multi-domiciliation de SCTP nous a permis d'étudier ses mécanismes de mobilité et de comparer les performances avec le cas hybride. Le principal gain est la bonne interprétation des conditions du nouveau réseau et une adaptation optimale à ce nouveau réseau.

La comparaison de SCTP en hybride et en multi-domicilié avec les différentes versions de TCP semble indiquer la supériorité de SCTP sur les deux technologies de communications. Le point le plus intéressant de cette comparaison est la régularité du flux de données de SCTP dans le contexte multi-domicilié par rapport aux autres protocoles. En effet, il est le seul à ne pas présenter de « cassure » ou de ralentissement après un changement de réseau.

Chapitre IV Amélioration de la mobilité de SCTP par la localisation

Dans le chapitre précédent, nous avons vu que les performances de SCTP lui permettaient d'être compétitif face à différentes versions de TCP, que le lien utilisé soit stable ou soumis à des fluctuations (différentiation de services, changements de réseau, …). Il a aussi été démontré que ces capacités de multi homing lui permettent d'être plus réactif et de mieux s'adapter aux nouveaux réseaux dans un contexte mobile. Dans cette section, nous proposons une amélioration de la mobilité avec SCTP qui permet de diminuer le temps nécessaire au changement de réseau en profitant des informations sur la localisation disponibles sur un grand nombre de véhicules de transport.

I Motivations

Lors de la présentation des problématiques liées à la mobilité, il a été montré que l'impact du changement de réseau entraîne plusieurs phénomènes : modification des caractéristiques du lien, changement de l'identifiant réseau, ajout d'une latence lors du basculement… La gestion de la mobilité avec mSCTP permet de supporter le changement de l'identifiant réseau en ajoutant dynamiquement la nouvelle adresse IP à l'association. Les mécanismes utilisés par mSCTP après un changement de réseau lui permettent de s'adapter plus facilement aux caractéristiques du nouveau réseau.

En revanche, un des points faibles de la mobilité avec mSCTP est la nécessité d'échanger la nouvelle adresse IP avec l'hôte distant avant de pouvoir communiquer avec celle-ci. Une latence peut alors être introduite comme pour mobile Ipv6, induite en partie par le temps de configuration de l'interface réseau. Ce temps de configuration peut être relativement important comparé au temps passé dans la zone de couverture du point d'accès. Par exemple, un bus circulant en ville à 50km/h (soit environ 14m/s) souhaitant se connecter à un point d'accès Wi-Fi ayant une portée de 100m va alors passer moins de 15s dans la zone de couverture. Pour obtenir le temps « utilisable » pour communiquer, il faut soustraire le temps d'établissement de la connexion au niveau Liaison et le temps de configuration de l'interface Réseau. Suivant la méthode utilisée, plusieurs secondes peuvent être nécessaires pour obtenir l'adresse IP, réduisant alors le temps de communication à seulement quelques secondes.

Dans le Chapitre I, nous avons vu que les transports en commun présentent certains avantages par rapport à des véhicules particuliers. La présence à bord du véhicule d'un système de localisation comme le GPS permet de connaitre une position dont la précision peut être améliorée grâce à l'utilisation des odomètres (capteurs mesurant la distance parcourue). Contrairement aux véhicules particuliers, les véhicules de transport en commun suivent un trajet défini à l'avance et similaire d'un jour à l'autre. Ces nœuds mobiles traversent donc toujours les mêmes réseaux et vont chercher à se connecter aux mêmes points d'accès. Dans un tel contexte, il est envisageable d'avoir une carte de la couverture de ces réseaux ainsi qu'une adresse IP fixe dans chacun de ces réseaux. Ces deux éléments couplés avec la localisation permettent d'effectuer des configurations en amont en anticipant les connexions disponibles. Nous allons étudier ici une implémentation de cette solution avec mSCTP que nous comparerons avec une gestion plus « classique » de la mobilité avec mSCTP.

II Présentation de la solution

Lors de la présentation du protocole de Transport mSCTP (voir Chapitre III, section I), une séquence appelée mSCTP-DAC [67] permettant d'effectuer un changement de réseau avec mSCTP a été présentée. Dans un premier temps, la nouvelle adresse IP du réseau rencontré est ajoutée à l'association puis celle-ci est choisie comme étant l'adresse primaire. Dans un contexte classique, l'attribution de l'adresse IP ne peut se faire qu'une fois la connexion établie entre le nœud mobile et le point d'accès. Afin de réduire le temps nécessaire au changement de réseau, nous allons anticiper cette connexion en configurant l'adresse IP et en la communiquant au nœud distant avant que le nouveau réseau soit détecté. Pour rappel, la durée écoulée entre la détection du réseau et l'envoi de données sur celui-ci dépend du temps nécessaire à l'établissement de la connexion au niveau Liaison et à la configuration de l'interface réseau (adresse IP, routes, …). La durée de configuration de l'interface est influencée par la méthode utilisée (DHCPv6, auto-configuration, …). En effectuant la configuration de l'interface en amont, nous espérons pouvoir réduire le temps nécessaire au changement de réseau. La section suivante propose une étude temporelle de cette proposition ainsi qu'une comparaison avec l'algorithme classique de gestion de la mobilité avec SCTP.

Notre proposition se basant sur la configuration de l'interface réseau avant la connexion au réseau, il est nécessaire de posséder une adresse IP statique pour chaque point d'accès traversé. Si cette hypothèse est inimaginable pour des nœuds ayant une mobilité irrégulière, le trajet fixe emprunté par les véhicules de transport en commun conduit à traverser les mêmes réseaux et il est donc possible d'avoir une adresse réservée à chaque point d'accès. De plus, il est aussi envisageable, connaissant le préfixe IP du futur réseau, de générer une adresse IP à l'aide de l'auto-configuration d'IPv6. En arrivant dans le nouveau réseau, il est alors nécessaire de vérifier la présence d'une adresse dupliquée.

III Étude temporelle et comparaison avec l'algorithme DAC

L'analyse faite dans cette section vise à démontrer l'intérêt de notre solution en ayant une approche logique basée principalement sur les temps de transfert des messages. Une comparaison est faite avec l'algorithme SCTP-DAC présenté dans le Chapitre III, section I.1.3, et décrit dans [67]. Afin de simplifier la compréhension des équations et d'alléger les schémas, les abréviations suivantes seront utilisées par la suite :

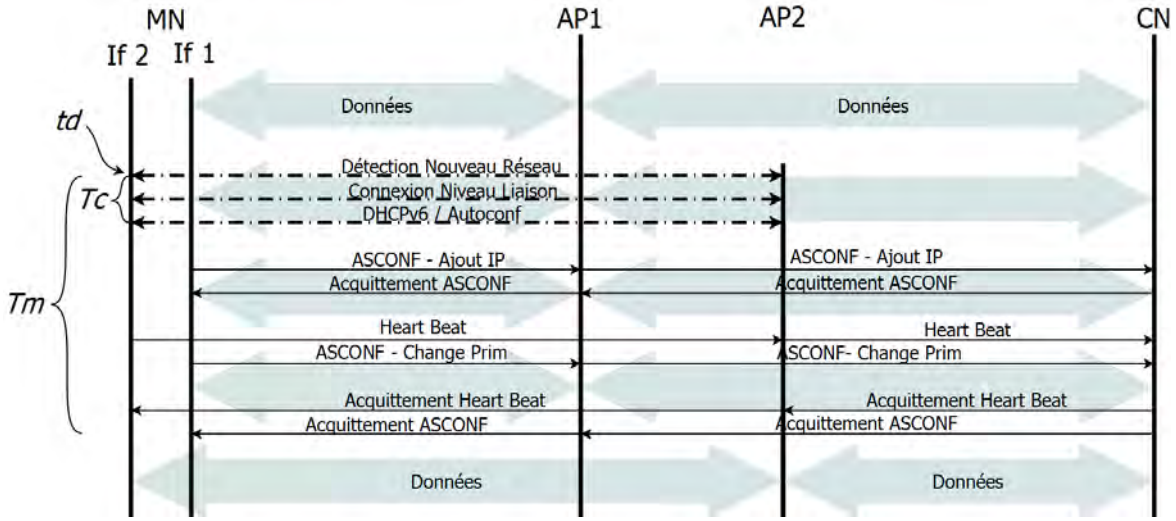
- T_c : Temps nécessaire pour configurer l'interface réseau, dépendant du matériel et de la méthode utilisée pour la configuration (DHCP, configuration autonome, …),
- Td_i : Délai de bout-en-bout entre les deux hôtes en prenant le chemin i,
- RTT_i : Temps aller-retour entre les deux hôtes sur le chemin i,
- t_d : Temps correspondant à la détection du nouveau réseau,
- t_0 : Temps correspondant au début de la séquence de configuration en avance,
- T_m : Durée du changement de réseau avec mSCTP-DAC (à partir de la détection),
- Ts_d, Ts_0 : Durée du changement de réseau avec notre solution à partir de la détection et à partir du début de la séquence.

Le vocabulaire utilisé ici est celui de SCTP, les définitions exactes étant données avec la présentation du protocole dans le Chapitre III, section I. Par exemple, la notion de chemin correspond ici à la vision de SCTP : il s'agit du trajet pris par les paquets entre deux adresses IP (une locale et une distante). SCTP émettant différents types de chunks suivant les informations à transmettre, des abréviations sont aussi utilisées pour désigner les messages de contrôle suivants :

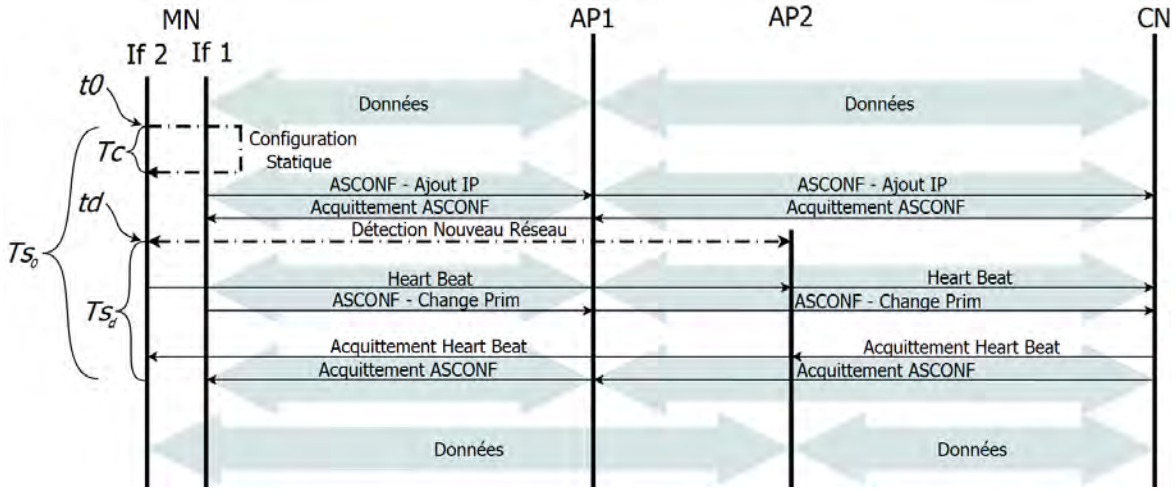
- $A - A_{Ack}$: Message ASCONF et acquittement d'un message ASCONF,
- $HB - HB_{Ack}$: Message « Heart Beat » et acquittement d'un message « Heart Beat ».

Les messages de données ne seront pas représentés ici puisque nous considérerons le changement de réseau fini lorsque les deux hôtes sont dans un état similaire : le nouveau chemin est considéré actif par les deux nœuds. Pour estimer ce moment précisément, il est nécessaire de prendre en compte le temps de transfert des acquittements. Cette durée est différente de la durée de perturbation provoquée par le changement de réseau, celle-ci correspondant au temps écoulé entre la réception du dernier paquet sur l'ancien chemin et la réception du premier paquet sur le nouveau chemin. Ces deux mesures sont équivalentes, l'unique différence étant l'échange d'un paquet de données supplémentaire dans chaque cas.

En se basant sur la définition de l'algorithme mSCTP-DAC de [67] et sur la définition donnée précédemment de notre algorithme, il est ainsi possible d'obtenir une représentation temporelle de ces définitions présentée sur la Figure 36. La principale différence entre les deux algorithmes est clairement visible : le protocole mSCTP-DAC fait la configuration de l'interface réseau après la détection du nouveau point d'accès contrairement à notre solution qui configure de manière statique l'interface en amont de la détection. Il est à noter que dans la configuration présentée, seul le nœud mobile est multi-domicilié, ce qui est le cas par exemple d'une connexion mobile vers un serveur web



(a) Echanges lors du changement de réseau avec SCTP-DAC.



(b) Echanges lors du changement de réseau avec configuration en avance.

Figure 36 - Schémas temporels représentant les échanges entre MN et CN lors d'un changement de réseau avec deux algorithmes différents : un réactif (mSCTP-DAC) et un préventif.

qui n'utilise alors qu'une seule interface (ce cas est supporté par le standard). Sur le diagramme les messages HB et ASCONF sont représentés un en-dessous de l'autre mais ils sont envoyés simultanément, cette représentation étant juste choisie pour plus de visibilité.

Ce diagramme temporel permet de déterminer plusieurs durées en fonction de temps de transferts des messages de contrôle. Le temps nécessaire au changement de réseau avec mSCTP-DAC s'exprime ainsi :

Équation 1 : $\boldsymbol{T_m = T_c + \max\left(Td_1(A) + Td_1(A_{Ack}), Td_2(HB) + Td_2(HB_{Ack})\right)}$

Équation 2 : $T_m = T_c + Td_1(A) + \max\left(Td_1(A_{Ack}), Td_2(HB) + Td_2(HB_{Ack})\right)$

Deux cas se distinguent avec mSCTP-DAC, soit le message de vérification du lien « Heart Beat » est envoyé par le nœud mobile en même temps que la requête ASCONF (Équation 1), soit le message de vérification est envoyé par le nœud correspondant lors de la réception de la requête ASCONF (Équation 2). Le cas représenté dans Figure 36 (a) correspond à l'envoi simultané des requêtes par le nœud mobile. Le temps nécessaire à notre solution pour effectuer le changement de réseau peut être exprimé à partir de deux instants : du début de la séquence t_0 ou de la détection du nouveau réseau t_d.

Équation 3 : $\boldsymbol{Ts_d = \max\left(Td_1(A) + Td_1(A_{Ack}), Td_2(HB) + Td_2(HB_{Ack})\right)}$

Équation 4 : $Ts_0 = T_c + Td_1(A) + Td_1(A_{Ack}) + Ts_d$

L'Équation 3 et l'Équation 4 expriment la durée nécessaire à notre solution pour effectuer le changement de réseau. Comme cette solution nécessite de configurer l'interface et d'échanger la nouvelle adresse entre le début de la séquence et la détection du réseau, il est nécessaire de respecter une condition pour que cette solution soit efficace. Il faut que le temps écoulé entre le début de la séquence et la détection du réseau soit suffisamment important pour permettre le déroulement de la séquence :

Équation 5 : $\boldsymbol{t_d - t_0 \geq T_c + Td_1(A) + Td_1(A_{Ack})}$

L'Équation 5 doit être vérifiée pour que l'Équation 3 soit vraie. Si elle ne l'est pas, on retombe alors dans une configuration de type mSCTP-DAC. Dans cette étude, la configuration de l'adresse IP est faite de manière statique, aucun échange n'est donc effectué avec une entité extérieure et le temps de configuration T_c est alors relativement faible. En revanche, le délai pris par l'échange de la nouvelle adresse avec l'hôte distant peut varier suivant le délai subi par la communication en cours. Dans les chapitres précédents, nous avons vu que le délai peut dépasser 2 voire 3 secondes, particulièrement sur un réseau de communication par satellite avec une architecture QoS. Néanmoins, notre solution permet facilement de prévoir le changement de réseau plusieurs secondes avant que celui-ci n'arrive, rendant l'Équation 5 une hypothèse réalisable.

L'expression de ces équations peut être simplifiée en considérant le délai aller-retour sur chaque technologie plutôt que le délai simple. Les équations suivantes correspondent aux durées écoulées entre la détection du réseau et les deux nœuds prêts à communiquer sur le nouveau chemin.

Équation 6 : $\boldsymbol{T_m = T_c + \max(RTT_1, RTT_2)}$

Équation 7 : $T_m = T_c + Td_1(A) + \max(Td_1(A_{Ack}), RTT_2)$

Équation 8 : $Ts_d = \max(RTT_1, RTT_2)$

Il devient alors possible de comparer facilement les performances de ces deux solutions. Il est clairement visible que notre solution permet au minimum de réduire le temps du changement de réseau d'un temps équivalent à la configuration de l'interface réseau (T_c). Ceci est valable pour le cas où le nœud mobile envoie la requête Heart Beat en même temps que la requête de changement de chemin

primaire. Si cette requête est envoyée par le nœud correspondant, les apports de notre solution dépendent alors du délai subi par les applications suivant les réseaux utilisés :

- $Td_1 > RTT_2 \; soit \; Td_1 > 2 * Td_2$: les bénéfices de notre solution sont alors équivalents à seulement le temps de configuration T_c.
- $2 * Td_2 > Td_1 > Td_2$: les bénéfices dépendent alors de la différence entre Td_1 et Td_2 mais peuvent être considérés équivalents à $T_c + RTT_2 - Td_1$ soit entre T_c et $T_c + Td_2$.
- $Td_1 \leq Td_2$: les bénéfices sont alors de $T_c + Td_1$.

Les différents cas listés ci-dessus permettent d'envisager une diminution du temps nécessaire au changement de réseau au pire de T_c et au mieux de $T_c + Td_1$. Dans le cas où les deux réseaux ont des délais égaux, il est ainsi possible de réduire cette durée d'une valeur équivalente au délai de bout-en-bout et du temps de configuration soit plus de 30%.

Au vu de cette analyse temporelle, il apparait que le temps de configuration de l'interface réseau (variable T_c) a un impact très important sur l'apport de notre solution. Pour effectuer cette configuration, il est nécessaire de connaître la nouvelle adresse IP à attribuer à l'interface réseau. La détermination de cette adresse peut se faire de plusieurs manières :

- Statique : le réseau est connu et le nœud possède une adresse IP utilisable dans ce réseau.
- « Dynamic Address Discovery » définie dans « Neighbor Discovery » [69]: l'adresse est générée en se basant sur le préfixe communiqué par le routeur lors de la connexion à celui-ci. Des échanges peuvent ensuite avoir lieu pour vérifier que l'adresse ainsi déterminée ne soit pas déjà utilisée par un autre nœud.
- « Dynamic Host Configuration Protocol for IPv6 DHCPV6 » [76] : l'adresse IP est obtenue suite à l'échange d'informations entre un serveur DHCPv6 et l'hôte demandeur. L'obtention se fait en deux temps : un premier échange permet à l'hôte de connaître les serveurs disponibles, un deuxième échange permet l'obtention de l'adresse IP.

A l'opposé de la première méthode, les deux autres sont dynamiques et nécessitent des échanges entre le nœud et une entité du réseau (routeur ou serveur DHCPv6). Il est difficile de chiffrer la latence introduite par chaque configuration, la valeur étant fortement dépendante du matériel utilisé, tant du côté client que du côté serveur. En basant uniquement sur les temps de propagation, on peut les évaluer à deux fois et quatre fois le délai du réseau, soit 50ms et 100ms environ sur un réseau Wi-Fi. Toutefois, il faut aussi ajouter le temps de traitement côté serveur et côté client.

Dans le contexte étudié ici, la configuration de l'interface réseau se fait de manière statique pour les deux solutions. Le temps de configuration est alors minimal. La différence entre les deux solutions étant dépendante de ce temps de configuration, notre solution ne peut donc être que plus performante si elle est opposée à une configuration dynamique.

IV Banc de test et scénario

L'analyse temporelle réalisée dans la section précédente démontre les améliorations possibles de cette proposition. Afin de vérifier ces prévisions, nous avons choisi de réaliser une expérience avec des composants réels. En effet, la simulation ne permet pas de tenir compte de certaines contraintes comme la durée de configuration d'une interface réseau ou la mise en place des routes. Nous avons donc repris le banc de test du Chapitre III, section III.1, qui est composé de deux ordinateurs portables possédant chacun une interface Wi-Fi et une interface Ethernet. Pour rappel, ce banc de test est multi-domicilié et propose deux technologies permettant d'établir une connexion entre les nœuds :

- Lien satellitaire émulé par SATEM et utilisant les interfaces Ethernet de chaque nœud,
- Lien Wi-Fi obtenu grâce à un routeur Wi-Fi configuré en mode Infrastructure.

De même, l'application SCTP utilisée est celle présentée en Chapitre III, section III.2, qui permet de générer le trafic, d'observer les variables de l'association, de mesurer les performances de l'application et de gérer la mobilité avec mSCTP.

L'objectif de cette expérience est de prouver que la latence introduite par le changement de réseau peut être réduite grâce à notre solution. Nous avons donc fixé la génération de données à 100Ko/s, ce débit étant suffisamment élevé pour stresser correctement le réseau sans pour autant générer de congestion.

Le scénario choisi permet de connaitre le temps nécessaire à l'établissement de la connexion sur un nouveau réseau. Au début, l'association est établie sur le lien satellite et aucun réseau Wi-Fi n'est disponible. Au bout de 10 secondes, l'interface Wi-Fi du routeur est activée, représentant l'arrivée du nœud mobile à portée d'un point d'accès. Le nœud mobile se connecte alors au réseau Wi-Fi. Notre solution est comparée à l'algorithme mSCTP-DAC avec ce scénario. Notre solution effectuant des actions avant l'apparition du réseau Wi-Fi (soit avant 10s), les résultats obtenus doivent démontrer que le temps nécessaire au changement de réseau est minimisé.

V Analyse des résultats

Les résultats présents dans cette section proviennent d'expériences faites sur la plateforme décrite précédemment. La Figure 37 présente le délai applicatif lors de la réalisation d'un changement de réseau entre un lien satellite et un lien Wi-Fi. Ces courbes illustrent le scénario présenté plus haut pour l'algorithme mSCTP-DAC (a) et pour notre solution (b), le réseau étant détecté à 0s.

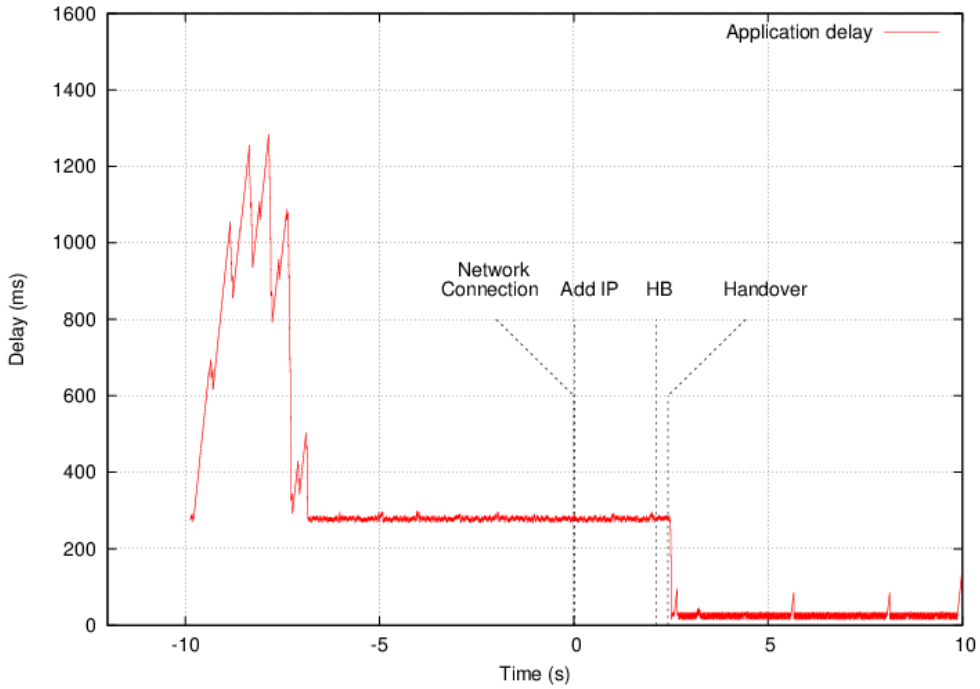
Avec l'algorithme mSCTP-Dac, l'adresse IP est ajoutée une fois le nœud connecté au réseau Wi-Fi et est ajoutée à l'association 20ms plus tard. S'en suivent alors les envois d'un HB pour vérifier le chemin et d'une requête pour effectuer le changement de chemin primaire. Il est important de préciser que dans cette expérience la configuration de l'adresse IP se fait de manière statique lors de la détection du nouveau réseau. Si l'adresse IP est obtenue par un mécanisme d'échange avec le point d'accès (comme DHCPv6 par exemple), des latences supplémentaires sont ajoutées et le temps de configuration (T_c) augmente.

Avec notre solution, l'ajout de l'adresse IP à l'association se fait en amont de la détection du réseau comme indiqué sur la Figure 37 (b). Lors de la connexion au réseau, aucune configuration d'interface réseau n'est nécessaire, l'émission du HB se fait immédiatement tout comme l'envoi de la requête pour le changement de chemin primaire.

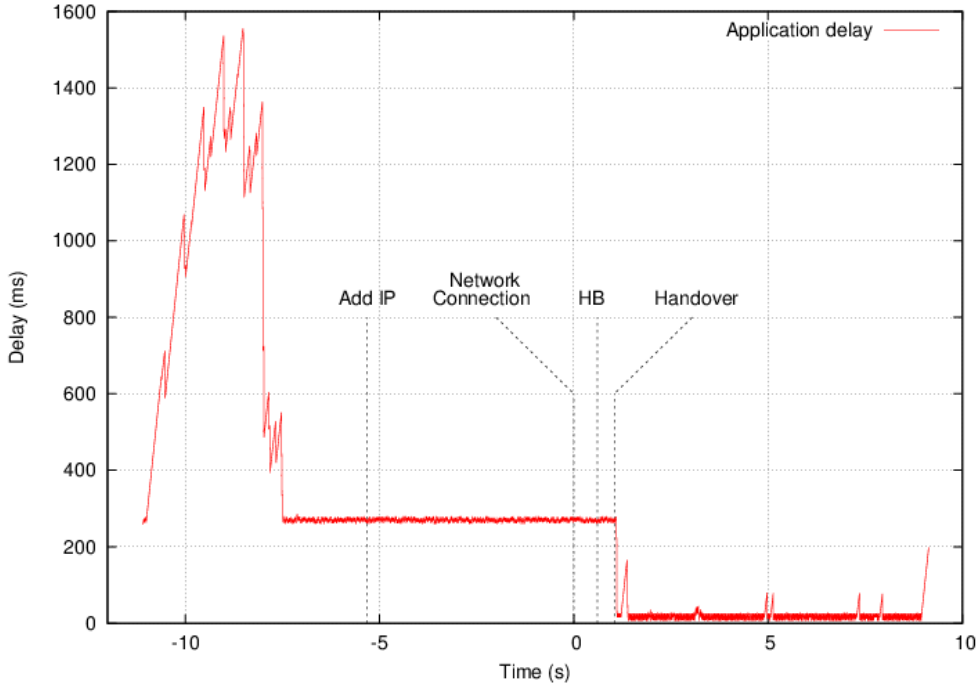
Afin d'évaluer plus précisément les différences entre ces deux solutions, nous avons répété ces deux expériences 12 fois chacune. Le Tableau 8 présente les latences moyennes lors de la réalisation de changements de réseau similaires à ceux présentés sur la Figure 37. Trois latences sont indiquées, il s'agit des temps écoulés entre la connexion au réseau et :

- L'envoi de données sur le nouveau lien marquant la fin du changement de réseau,
- L'envoi du HB vérifiant le nouveau chemin,
- La configuration de la route signalant l'interface prête à être utilisée.

Le temps écoulé entre la connexion au réseau et l'émission de données sur le nouveau lien correspond au temps nécessaire au changement de réseau. Ces résultats montrent que notre solution permet d'envoyer les données 900ms plus tôt. Dans un contexte urbain avec un véhicule circulant à 50km/h, 13m sont parcourus en 900ms. Si l'on considère qu'un point d'accès Wi-Fi a une portée d'une centaine de mètres, on peut ainsi augmenter la « zone utilisable » de 10%.



(a) Algorithme mSCTP-DAC.



(b) Configuration en avance.

Figure 37 – Délai applicatif lors de la réalisation d'un changement de réseau entre satellite et Wi-

Tableau 8 – Latences moyennes lors de la réalisation d'un changement de réseau.

	Temps nécessaire en secondes		
	Connexion au réseau > Emission de données	Connexion au réseau > Emission HB	Connexion au réseau > Configuration Route
Solution	1.86s	0.890s	0.889s
mSCTP-DAC	2.79s	1.84s	1.84s

En observant les autres latences du Tableau 8, on s'aperçoit que la différence entre les deux algorithmes provient principalement du temps nécessaire à la configuration de l'interface réseau et de la route. En effectuant ces configurations en avance, cette latence est divisée par deux.

Cette étude permet d'avoir des valeurs du temps nécessaires à la configuration de l'adresse IP et la connexion au réseau pour les deux algorithmes étudiés. Nous allons maintenant nous servir de ces valeurs pour paramétrer des simulations et effectuer ainsi une étude comportant plusieurs changements de réseau. Pour cela, nous avons choisi d'utiliser le simulateur réseau ns-2 car celui-ci inclut déjà SCTP et nous avons pu vérifier le bon fonctionnement de son implémentation dans ce simulateur.

VI Etude de performances en simulation

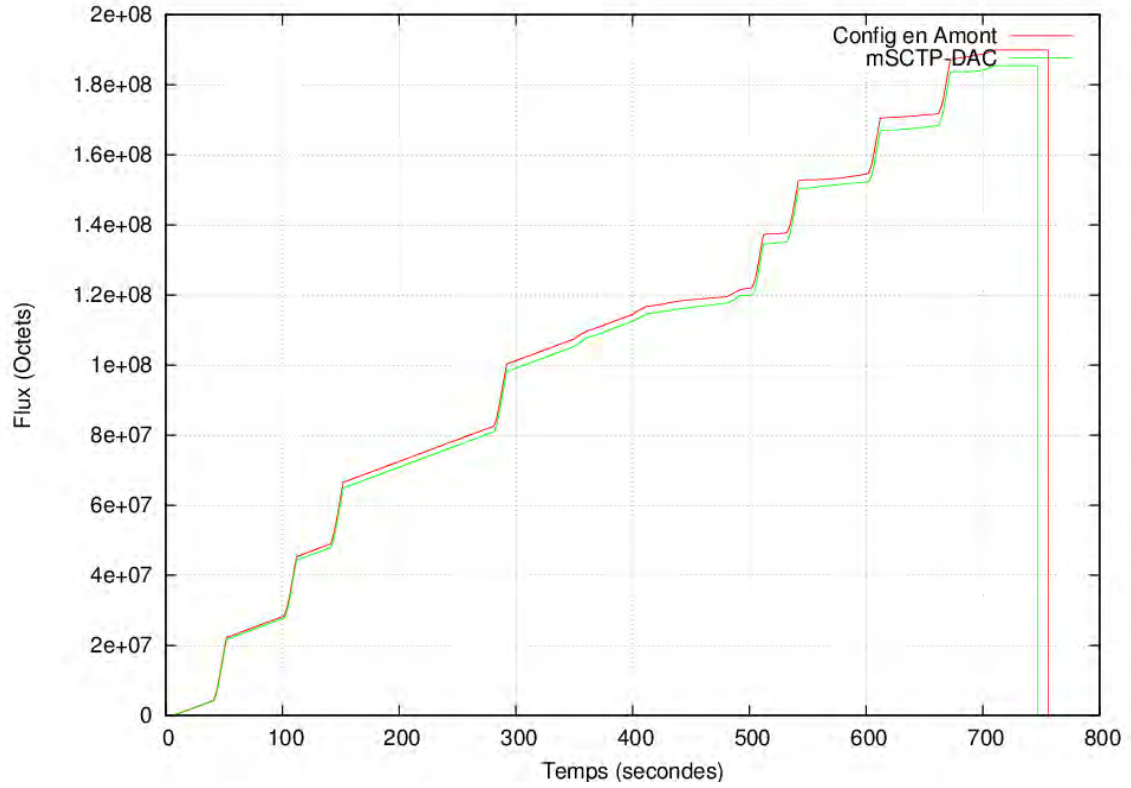
Le principal avantage de l'étude précédente est l'émulation, soit l'utilisation d'ordinateurs et de systèmes d'exploitation réels. Les valeurs ainsi obtenus dépendent de protocoles implémentés et déployés, elles peuvent alors être considérées plus fiables que les mêmes valeurs obtenues par le calcul ou la simulation (obtenir un temps de configuration par la simulation est tout simplement impossible). Cependant, la limite de l'émulation étant le passage à l'échelle, l'expérience précédente était limitée par le nombre de flux en présence, le nombre de changements de réseau…Il est alors plus simple de changer de méthode et d'utiliser la simulation en la configurant avec les valeurs obtenues par la simulation.

Le scénario simulé correspond au déplacement d'un véhicule dans la zone de couverture d'un point d'accès 3G. Il rencontre alors plusieurs point d'accès de type Wi-Fi et les utilise tant qu'il reste dans leurs zones de couverture. Le temps passé dans la zone de couverture du Wi-Fi est calculé à partir des données acquises par répétition de l'expérience précédente. Les temps de configuration sont listés dans le Tableau 9 avec dans chaque colonne le numéro de l'expérience et dans la dernière colonne la moyenne des valeurs pour chaque algorithme. Le temps passé dans la zone de couverture de chaque point d'accès évolue donc et certains temps de configuration avec notre solution sont plus élevés qu'avec l'algorithme DAC. Néanmoins, la moyenne étant avantageuse à notre solution, ce scénario doit permettre l'obtention de meilleures performances avec notre celle-ci.

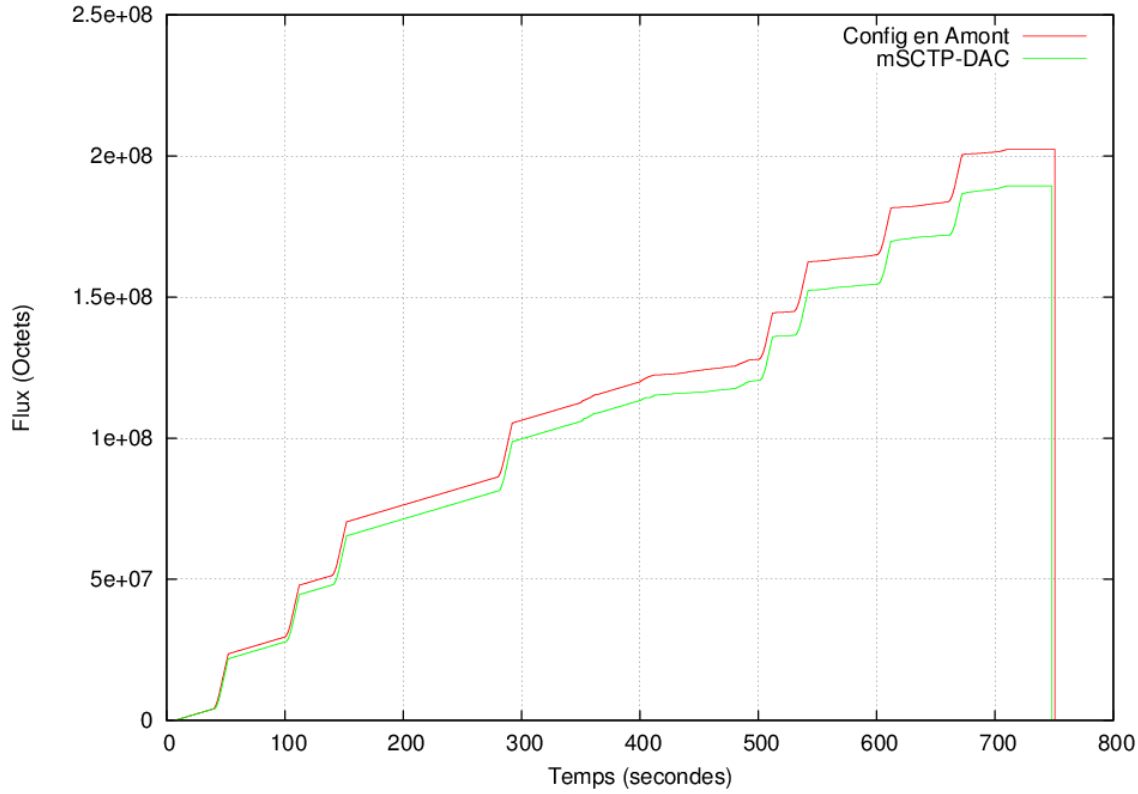
La configuration de la simulation est la suivante : 1Mbps pour la 3G et 20Mbps pour le Wi-Fi. Suivant les points d'accès, des flux entrent aussi en concurrence avec le flux SCTP principal qui est étudié. Entre 300s et 500s, les points d'accès Wi-Fi ont été congestionnés puis entre 400s et 700s le point d'accès 3G a été congestionné.

Tableau 9- Temps de configuration trouvés par l'émulation et repris dans la simulation.

Algo	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**Moy**
DAC	0.77	0.15	1.15	4.27	3.49	0.55	0.46	2.61	1.87	3.44	1.05	2.58	1.86
SOL	1.09	0.57	5.99	1.24	4.92	3.02	1.58	0.88	7.20	1.60	2.99	2.43	2.79



(a) Temps de configuration correspondant au valeur trouvées par émulation.



(b)Temps de configuration fixé à 1s.

Figure 38 – Quantité de données transférée par deux associations SCTP utilisant différents algorithmes avec de multiples changements de réseau.

La Figure 38 (a) présente la quantité de données transférée pour les deux algorithmes avec une association SCTP transportant un flux FTP. Les changements de réseau sont clairement visibles, la capacité de transfert étant plus importante sur le Wi-Fi, la courbe augmente plus rapidement. On remarque qu'à chaque changement de réseau, notre algorithme transfère légèrement plus de données que mSCTP-DAC.

Dans cette simulation, nous avons calculé le temps passé dans la zone de couverture du Wi-Fi en se basant sur les valeurs réelles, ce qui donne en moyenne 890ms d'écart entre les deux algorithmes. Si l'on considère que la configuration de l'adresse IP avec l'algorithme mSCTP-DAC ne se fait plus de manière statique, le temps nécessaire à cette configuration est alors plus grand. Nous avons refait une simulation en prenant 1s d'écart entre les deux algorithmes. La quantité de données transférée dans cette simulation est illustrée sur la Figure 38 (b). Le gain de performances apporté par notre solution est alors plus net puisqu'il est ici de 7% comparé à la simulation (a) où il était de 2.5% alors que le temps de configuration n'a été augmenté que de 100ms. Ce point est intéressant car il démontre que l'utilisation d'une méthode de configuration nécessitant un échange entre un nœud mobile et son point d'accès va diminuer les performances de la communication, même si la latence introduite est relativement faible.

Dans un second temps, nous avons changé l'application générant les données et utilisé un flux à débit constant paramétré à 32ko/s en reprenant les valeurs de temps de configuration trouvés lors de l'expérience en émulation. La Figure 39 présente la quantité de données transférée dans ce cas. L'apport de notre solution est toujours visible, équivalent à celui obtenu lors du transport d'un flux FTP.

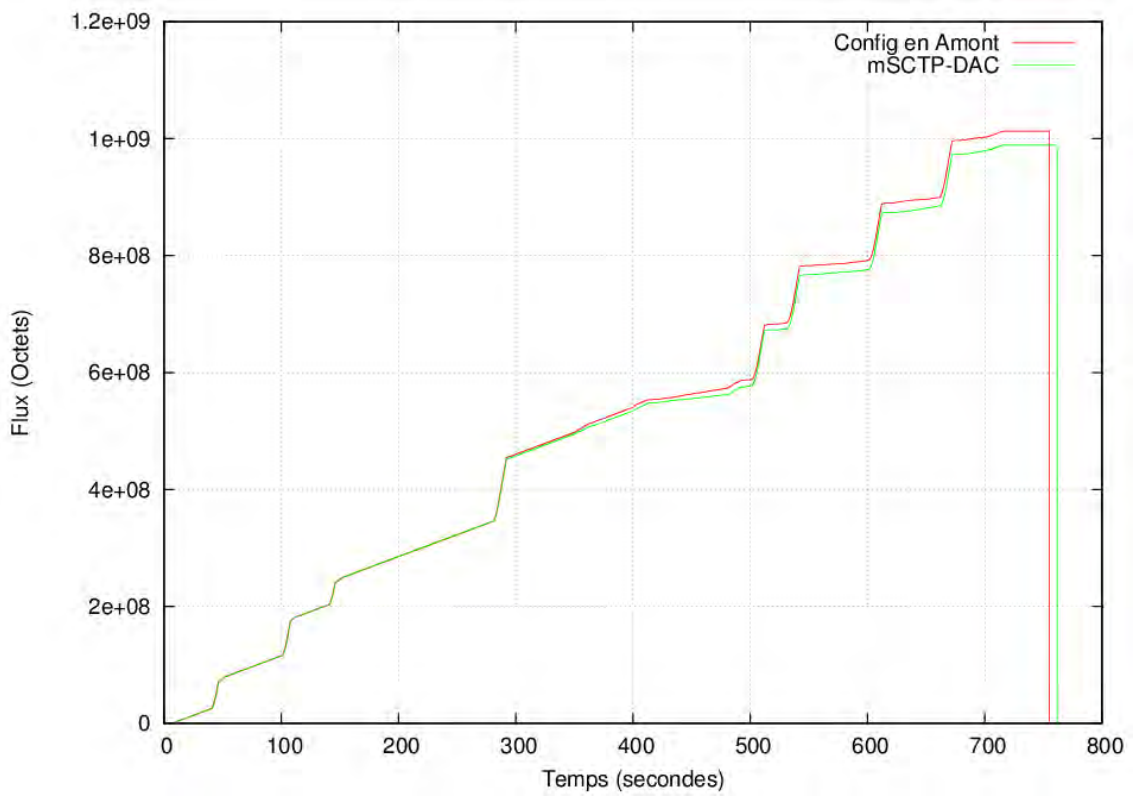


Figure 39 – Quantité de données transférée par deux associations SCTP transportant un flux CBR lors de multiples changements de réseau.

VII Bilan

Garantir une connexion à bord d'un véhicule de transport en commun nécessite de résoudre les pertes de connexions de niveau Transport lors des changements de réseau. De nombreuses solutions ont été conçues au niveau Réseau et au niveau Transport mais peu sont implémentées dans la réalité. En effet, la plupart de ces solutions se basent sur de nouveaux composants ou fonctionnalités qui ne peuvent être déployés dans les réseaux actuels à cause de leur architecture ou de leur administration privée. Notre solution se concentre sur la couche Transport et utilise les fonctionnalités de multi-domiciliation de SCTP avec la géo localisation pour prédire les changements de réseau et les réaliser plus rapidement. Un point fort de cette solution est l'absence de modifications nécessaires dans les réseaux d'accès, les seuls composants nécessaires sont internes au véhicule de transport en commun et n'impactent pas l'extérieur. Seule l'utilisation de SCTP pour communiquer est obligatoire, tout comme la connaissance des prochains réseaux traversés mais aucune configuration préalable de SCTP n'est nécessaire côté serveur.

Les résultats obtenus permettent de vérifier les améliorations prévues par l'analyse temporelle. Il est possible de diminuer la latence nécessaire au changement de réseau en effectuant des configurations en avance. En réduisant cette latence, le temps passé à portée du point d'accès est mieux rentabilisé puisqu'une plus grande partie de ce temps est utilisée pour transmettre des données. Dans un contexte urbain, l'apport peut être conséquent puisque les changements de réseau peuvent intervenir fréquemment avec des technologies de moyenne portée comme le Wi-Fi.

Les simulations configurées avec les valeurs trouvées par l'émulation permettent de vérifier cette hypothèse. Lorsque plusieurs changements de réseau sont effectués, notre solution permet d'améliorer la quantité de données transférée entre le nœud mobile et son nœud correspondant que ce soit pour une application FTP ou une application à débit constant. Des plus, on constate que l'introduction d'une latence correspondant à une configuration non-statique permet d'augmenter les performances de manière conséquente (5% de gain pour 100ms).

Chapitre V Architecture pour réseau mobile diminuant l'impact du changement de réseau

En introduction de cette thèse, nous avons présenté des véhicules de transport en commun qui agissent comme des routeurs mobiles. Dans un tel contexte, le véhicule gère la mobilité de tous les nœuds mobiles qui y sont connectés (terminaux des utilisateurs). Lorsque le routeur change de point d'accès, les terminaux n'ont rien à gérer mais ne sont pas informés non plus qu'un changement de réseau transparent est réalisé au niveau du routeur. L'impact de ce changement de réseau a déjà été introduit dans le Chapitre II et nous avons aussi pu observer son impact sur les communications dans le projet SAT-PERF lors de l'étude du réseau hybride (voir le Chapitre III, section III.3).

Pour rappel, un changement de réseau transparent intervient lorsqu'un gestionnaire de mobilité (mobile IP ou NEMO par exemple) réalise un changement de réseau sur le chemin utilisé par les communications. Dans le cas des réseaux mobiles, tout changement de point d'accès au niveau du routeur est un changement de réseau transparent. Nous avons vu dans l'état de l'art et l'étude précédente des évènements induits par le changement de réseau transparent, notamment la modification abrupte des caractéristiques du réseau et la réception désordonnée de paquets. Face à ces évènements, les réactions des protocoles de Transport ne sont pas adaptées car elles sont basées sur des mécanismes développés pour les réseaux filaires. Les interprétations erronées des protocoles de Transport peuvent même dans certains cas conduire à des pertes de performances.

L'approche que nous proposons pour limiter l'impact du changement de réseau transparent est d'informer le protocole de Transport lorsqu'un changement de réseau est effectué pour que celui-ci puisse réagir en accord avec la situation. Pour cela, il est nécessaire de mettre en place un échange entre le routeur mobile qui détient les informations et les nœuds mobiles qui gèrent les communications. Il est aussi indispensable d'avoir un protocole de Transport capable de prendre en compte ces informations et d'utiliser des mécanismes adaptés.

Dans ce chapitre, nous proposons une architecture qui permet de mettre en place cette solution tout en respectant les standards définis dans les réseaux mobiles. La première section détaille la conception de l'architecture avec 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. Une analyse est ensuite réalisée visant à démontrer les apports d'une telle architecture et de quelle manière les performances des protocoles de Transport peuvent être améliorées. Cette analyse se base notamment sur des expériences faites dans le cadre du projet SAT-PERF.

I Conception de l'architecture

I.1 Fonctionnement

Comme indiqué précédemment, notre architecture doit permettre à un routeur mobile de prévenir les protocoles de Transport situés dans les nœuds mobiles lorsqu'un changement de réseau est réalisé et qu'il leur faut réagir en fonction. Il faut donc un protocole de Transport supportant le changement de réseau. Nous avons vu dans les chapitres précédents qu'un protocole de Transport multi-domicilié comme mSCTP comporte une gestion de la mobilité et supporte le changement de réseau si celui-ci se produit au niveau d'un des hôtes de la communication. La solution que nous proposons est de « propager » le changement de réseau transparent réalisé au niveau du routeur jusqu'au nœud mobile. Pour cela, notre architecture se base sur deux principes:

- Définition d'un sous-réseau par interface possédée par le routeur et donnant vers l'extérieur,
- Obligation pour les nœuds mobiles de configurer une adresse IP par sous-réseau.

Le nœud mobile se retrouve alors connecté à autant de sous-réseaux que d'interfaces réseau sortantes du routeur. Si le nœud mobile possède suffisamment d'interfaces réseaux de la technologie demandée, il peut directement configurer une adresse IP par interface physique. Dans le cas contraire, le nœud mobile peut définir plusieurs adresses IP par interface réseau.

La Figure 40 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 via plusieurs interfaces réseaux ou la définition de plusieurs adresses par interface. Un protocole de Transport multi-domicilié est alors conscient de la présence de deux chemins.

En utilisant la fonctionnalité de multi-domiciliation de mSCTP, les nœuds mobiles connectés à plusieurs sous-réseaux sont capables de choisir une interface pour envoyer les données (chemin primaire de mSCTP) et peuvent basculer d'une interface vers une autre en changeant de chemin primaire. Avec notre architecture, le choix du chemin primaire est déterminé par le routeur mobile et un changement de réseau au niveau du routeur provoque un changement du chemin primaire au niveau de l'hôte de l'association SCTP. Nous verrons par la suite comment le routeur peut informer le nœud d'un changement de réseau et recommander à l'association SCTP un changement de chemin primaire.

I.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 les fonctionnalités suivantes (suivies des références des standards ou des articles) :

- NEMO ou un service équivalent permettant la mobilité du réseau (RFC3963 [36]),
- La gestion de la mobilité avec plusieurs interfaces (RFC5648 [30]),
- La définition de plusieurs préfixes IP permettant de définir les sous-réseaux (RFC4861 [69]),
- « Flow Binding » pour améliorer les performances (RFC6089 [34]).

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 (RFC4960 [64] et extensions [65], [66]):,

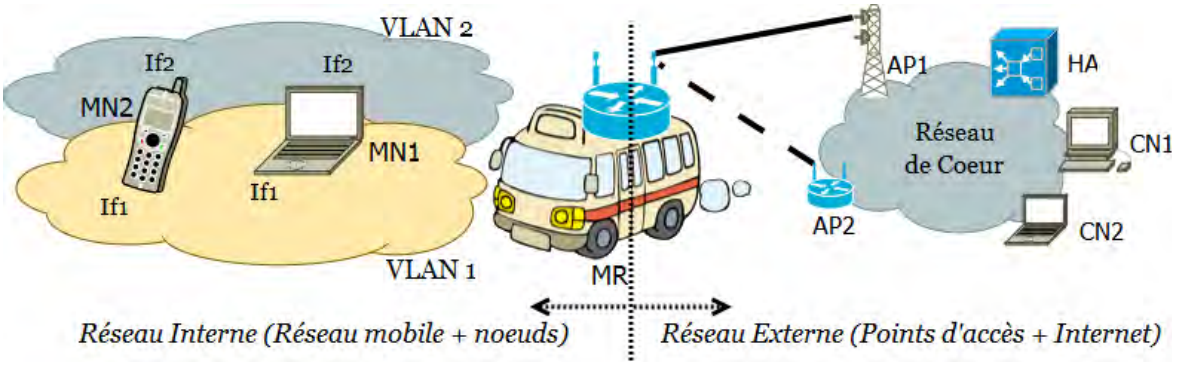


Figure 40 – Un réseau mobile avec notre architecture : côté routeur un sous-réseau VLANx par interface externe et côté nœud une interface Ifx par sous-réseau.

- La capacité de définir plusieurs adresses IP pour une seule interface (voir RFC4861 [69]).

Ces fonctionnalités étant déjà définies dans la littérature, la suite de cette section suppose leur implémentation dans les nœuds du réseau.

I.3 Partage d'informations entre le router mobile et ses nœuds

Afin de limiter l'impact du changement de réseau, notre architecture propose d'améliorer le partage d'informations entre le routeur et les nœuds qui lui sont connectés. Avant de définir les messages permettant ce partage, il est nécessaire d'établir précisément quelles informations sont pertinentes, de quels évènements elles découlent mais aussi quelles actions doivent être effectuées à la suite de ces évènements. Nous allons établir ici le fonctionnement précis de notre architecture en commençant par l'initialisation des nœuds mobiles.

Lors de l'arrivée d'un nœud mobile dans le réseau mobile, celui-ci va chercher à se connecter au routeur. Il établit alors la connexion au niveau Liaison et le routeur lui communique les préfixes IP des différents sous-réseaux définis. En même temps, il faut que le routeur signale quel sous-réseau doit être utilisé pour les communications. Le nœud mobile va alors générer une adresse IP correspondant à chaque préfixe et communiquer sur le sous-réseau demandé par le routeur. De plus, si une association SCTP est déjà en cours, il faut que le nœud mobile ajoute les nouvelles adresses IP et les communique à l'hôte distant.

Les autres évènements intéressants pour notre architecture sont induits par la mobilité et plus particulièrement par les changements de réseau : détection d'un nouveau point d'accès, changement de point d'accès, ancien point d'accès devenu indisponible et aucun point d'accès disponible. Une correspondance entre ces évènements et le déplacement d'un véhicule est donnée par la Figure 41. Le véhicule est connecté à un premier point d'accès puis traverse la zone de couverture d'un second point d'accès et termine dans une zone non-couverte.

Pour chacun de ces évènements, le gestionnaire de mobilité implémenté dans le routeur effectue des actions en se basant sur le standard adapté qu'il utilise. Pour la présentation de notre architecture, nous supposons que NEMO est la solution choisie pour gérer la mobilité au niveau du routeur. Lorsque des changements arrivent dans la liste des points d'accès disponibles, le routeur va donc générer des « Binding Update » (BU) en direction de son agent mère en signalant l'ajout ou la suppression d'un

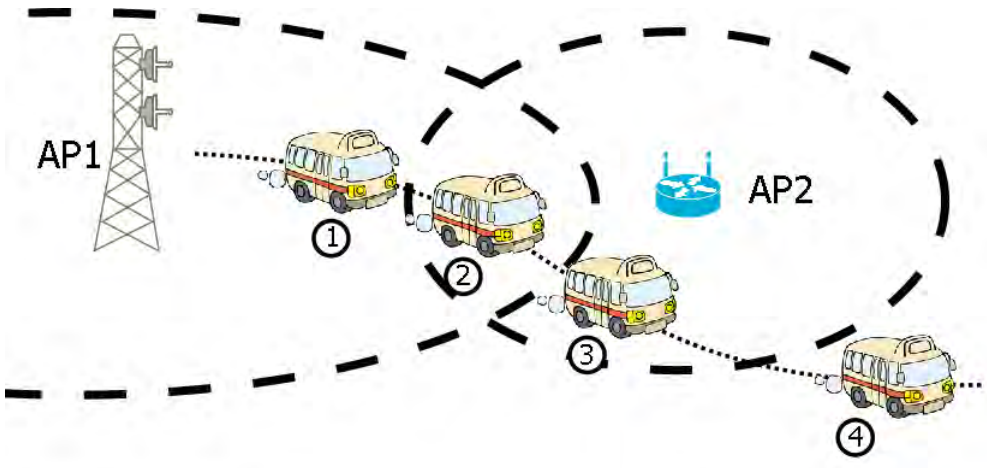


Figure 41 – Evènements se produisant dans un contexte mobile : (1) détection, (2) changement, (3) indisponibilité et (4) absence de réseau.

point d'accès. Une liste des évènements cités précédemment et des actions qui les accompagnent est donnée dans le Tableau 10 (1° et 2° colonnes).

Parallèlement, il est aussi possible de lister les actions à définir pour le bon fonctionnement de notre architecture. Si le routeur change de point d'accès, il doit répercuter ce changement de réseau en forçant les nœuds mobiles à changer de sous-réseau. Pour cela, il va signaler aux nœuds mobiles quel préfixe IP (et donc quel sous-réseau) ils doivent utiliser pour communiquer. Par conséquent, les associations SCTP actives doivent changer de chemin primaire. Les actions à ajouter pour chacun des évènements discutés au dessus sont listées dans le Tableau 10 (3° colonne).

Des abréviations ont été utilisées afin de faciliter la compréhension de ce tableau : Pref-IP correspond à préfixe IP, SCTP-AddIP, SCTP-ChangePrim et SCTP-RemIP correspondent respectivement à l'ajout d'une adresse IP, au changement de chemin primaire et à la suppression d'une adresse IP.

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,
- 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 10. 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. Par exemple, en anticipant le changement de réseau, il faut être certain que le réseau sera présent sinon la configuration aura été faite pour rien, introduisant un trafic de contrôle supplémentaire dans le meilleur des cas ou une tentative de connexion à un réseau absent dans le pire des cas.

Quel que soit l'évènement, les échanges introduits par notre architecture portent sur le signalement du sous-réseau à utiliser. Des messages permettant au routeur de signaler le préfixe à utiliser sont donc nécessaires. L'objectif de notre architecture n'étant pas l'ajout de nouveaux protocoles, nous nous sommes intéressés aux messages permettant la configuration des adresses IP dans un réseau IPv6. Dans la sous-section suivante, nous décrivons une partie du standard définissant ces messages et introduisons la manière de les utiliser pour partager des informations sur un changement de réseau.

Tableau 10 – Décisions et actions provoquées par la mobilité (Existantes et nouvelles).

Evènement	**Mécanismes existants**	**Nouvelles Actions**
Connexion MN-MR	Connexion niveau Liaison Transmission des préfixes IP	Signaler Pref-IP prioritaire Configuration des 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 d'un réseau autre

I.4 Configuration d'adresse et partage d'information dans les réseaux IPv6

Lors de son arrivée sur un nouveau réseau ou après l'évolution de celui-ci, un nœud a besoin de connaître le contexte dans lequel il va communiquer : identifiants à utiliser, routeurs disponibles, autres nœuds hôtes présents dans le réseau… Les mécanismes et échanges nécessaires à l'obtention de ces informations sont permis avec le protocole « Neighbor Discovery » pour IPv6 défini dans [69]. Ce document est complété par le standard [70] qui apporte des précisions sur le comportement de l'hôte. Ces ajouts ont été nécessaires suite à des implémentations incorrectes pouvant conduire à des failles de sécurité. La découverte des nœuds voisins s'applique à tous les types de liens excepté ceux ne permettant pas le multicast au niveau Liaison. Ces liens sont dits « Non-Broadcast Multi-Access » (NBMA) et les détails pour l'utilisation de la découverte des nœuds est faite dans [72]. Des exemples de liens NBMA sont présents dans les technologies cellulaires et 3G, l'utilisation de « Neighbor Discovery » est discutée respectivement dans [73] et [74]. Seuls des éléments adaptés aux réseaux locaux seront présentés ici.

Le protocole « Neighbor Discovery » propose des mécanismes permettant la résolution des problèmes relatifs aux interactions entre nœuds :

- Découverte du routeur : comment localiser le routeur local,
- Découverte du préfixe : comment découvrir le jeu de préfixes IP utilisé sur le réseau et défini par le routeur,
- Découverte des paramètres : apprentissage des paramètres de lien (MTU par exemple),
- Auto configuration de l'adresse : possibilité des nœuds à définir leurs adresses indépendamment,
- Résolution de l'adresse : détermination de l'adresse niveau Liaison d'un nœud,
- Détermination du prochain bond : comment trouver les nœuds à joindre pour atteindre la destination,
- Détection d'un voisin inaccessible : à quel moment un nœud est considéré inaccessible,
- Détection d'une adresse en double : comment savoir si une adresse est déjà utilisée,
- Redirection : comment prévenir un nœud qu'un meilleur premier bond existe.

L'auto configuration de l'adresse IP est abordée par le protocole mais uniquement comme un service, sa définition est faite dans [75]. La résolution des problèmes listés ci-dessus n'est possible qu'en partageant des informations dans le réseau. De nouveaux types de messages ont donc été ajoutés au protocole « Internet Control Message Protocol » (ICMP) [71] qui permet l'échange de messages de contrôle avec IPv6 :

- « Router Solicitation » (RS): permet à un nœud de demander la génération d'un RA,
- « Router Advertisement » (RA): utilisé par le routeur pour transmettre des informations,
- « Neighbor Solicitation » : utilisé entre nœuds pour connaitre l'adresse niveau Liaison, vérifier l'accessibilité ou vérifier la disponibilité d'une adresse,
- « Neighbor Advertisement » : réponse à un NS, peut aussi être envoyé spontanément pour signaler un changement
- « Redirect » : utilisé par les routeurs pour signaler qu'un meilleur bond est disponible.

Nous nous intéresserons ici aux messages échangés entre le routeur et les nœuds du réseau. Les formats des messages « Router Solicitation » (RS) et « Router Advertisement » (RA) sont représentés respectivement sur les Figure 42 et Figure 43. La première ligne de ces messages est l'en-tête commun à tout message ICMP : le type de message, un code dépendant du type (égal à 0 ici) et un « checksum » pour vérifier l'intégrité des données. Les messages du protocole « Neighbor Discovery »

sont numérotés de 133 à 137 et sont donc classés comme messages à caractère informatif par ICMP (valeur supérieure à 127). Le message RS est basique car il s'agit uniquement d'une requête, la seule option qu'il peut contenir est l'adresse source si celle-ci est déjà configurée. En revanche, les messages RA transportent des informations sur le routeur ou sur la configuration du réseau :

- « Cur Hop Limit » : Nombre de bonds à utiliser pour tout paquet IP sortant,
- « M » et « O » : Bits signalant que la configuration d'adresse est gérée par « Dynamic Host Configuration Protocol » (DHCP) [76],
- « Router Lifetime » : Durée de vie associée au routeur par défaut,
- « Reachable Time » : Durée pendant laquelle un nœud est supposé accessible après réception d'une confirmation de son accessibilité,
- « Retrans Timer » : Temps entre deux messages « Neighbor Solicitation ».

D'autres informations sont envoyées via les options : l'adresse source niveau Liaison, la taille maximale d'un paquet ou « Maximum Transmission Unit » (MTU) et le préfixe d'adresse IP du routeur « Prefix Information ». Cette dernière option contient les informations nécessaires aux nœuds pour effectuer une auto configuration de leurs adresses IP et peut être répétée dans un RA pour chaque préfixe du routeur, son format est représenté Figure 44. En plus du préfixe, les champs de cette option contiennent plusieurs valeurs :

- « Prefix Length » 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 (valide pour déterminer une adresse),
- « 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

Type	**Code**	**Checksum**
Reserved		
Options …		

Figure 42 - Format d'un message Router Solicitation (RS).

Type	**Code**			**Checksum**
Cur Hop Limit	M	O	Reserved	Router Lifetime
Reachable Time				
Retrans timer				
Options…				

Figure 43 - Format d'un message Router Advertisement (RA)

Type	**Length**	**Prefix Length**	**L**	**A**	**Reserved1**
Valid Lifetime					
Preferred Lifetime					
Reserved2					
Prefix					

Figure 44 – Format de l'option « Prefix Infomation ».

durée de préférence du préfixe choisi à une valeur élevée et à une valeur plus faible pour les autres préfixes. Un changement de réseau entraine 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 dont la durée de préférence est la plus élevée. Que ce soit avec SCTP ou un autre protocole de Transport, les nouvelles communications sont établies automatiquement avec l'adresse IP 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 tout en restant connecté au réseau mobile.

La Figure 45 est une représentation temporelle du fonctionnement de notre architecture reprenant les données du Tableau 10. Il est clairement visible qu'à chaque événement réseau correspond des actions, notamment pour le changement de réseau qui provoque la modification du chemin primaire utilisé par SCTP. La section suivante détaille l'impact de notre architecture sur le comportement des protocoles de Transport.

II Analyse

Notre architecture vise à diminuer l'impact du changement de réseau sur les protocoles de Transport en les informant qu'un changement de réseau est réalisé, leur permettant ainsi de réagir correctement aux différents évènements qui suivent un changement de réseau. Dans cette section, nous allons

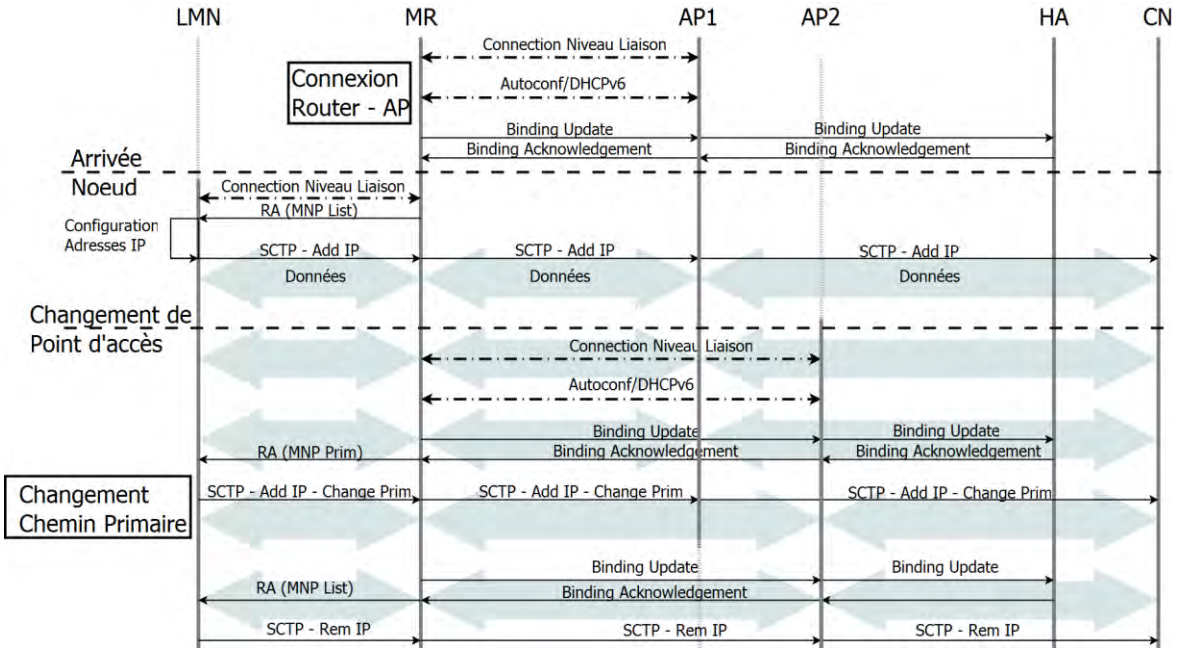


Figure 45 – Messages échangés pendant différents phases : connexion routeur – point d'accès, arrivée d'un nouveau nœud, changement de point d'accès et changement de chemin primaire.

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 terminaux,
- Réseau Multi-Domicilié : les nœuds réalisent le changement de réseau grâce à la multi-domiciliation de SCTP.

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

II.1 Banc de test et scénario

Le banc de test utilisé étant présenté en détail dans le Chapitre III, section III.1, seule une description succincte est faite ici à titre de rappel. Quatre éléments le composent : un émulateur de lien satellite capable de réaliser un changement de réseau transparent, un point d'accès Wi-Fi permettant la multi-domiciliation et deux ordinateurs portables hôtes de la communication SCTP. 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 l'application que nous avons développée et qui est présentée dans le Chapitre III, section III.2.

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 une 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 kb/s (64ko/s),
- Lien Wi-Fi : délai de 20ms et bande passante de 10 Mb/s (250ko/s).

L'application générant un trafic avec un débit constant à 300ko/s, aucune congestion ne doit apparaitre 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 Figure 46 (a) et (b). La Figure 46 (a) présente l'évolution de la fenêtre de congestion de SCTP avec une seule interface sur un réseau hybride avec un changement de réseau transparent pour les terminaux. La Figure 46 (b) présente quant à elle l'évolution de la fenêtre

de congestion sur le réseau multi-domicilié avec mSCTP comme solution de mobilité. L'utilisation d'une fenêtre de congestion différente est clairement visible selon que le chemin primaire soit le satellite ou le Wi-Fi.

En observant l'évolution de ces fenêtres de congestion, deux différences sont visibles : 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.

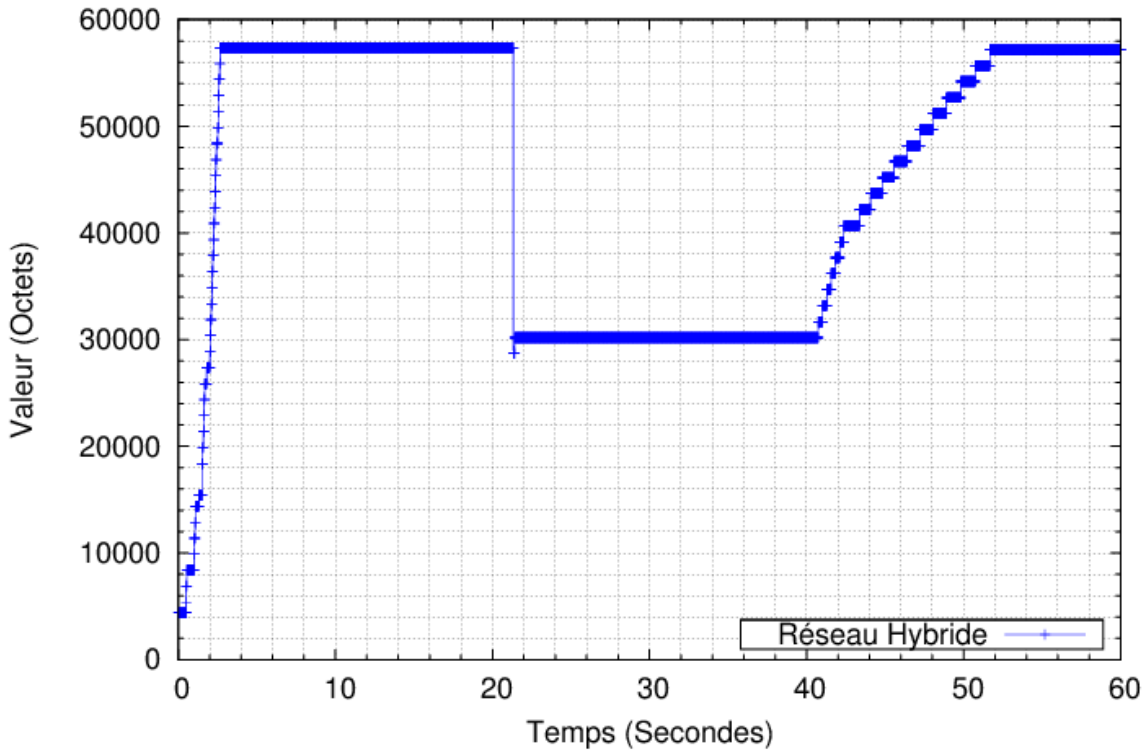
II.2 Comportement de la fenêtre de congestion

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-domiciliation 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.

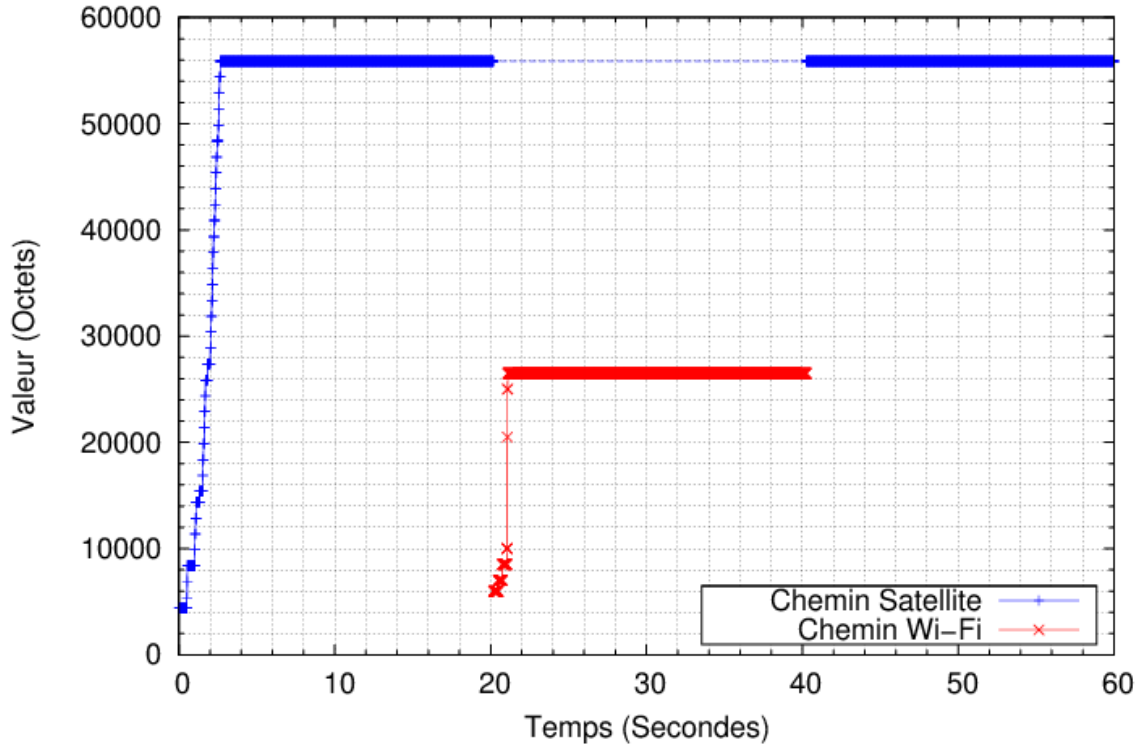
Cette chute est due à la réception de données non ordonnées lors du changement de réseau entre satellite et Wi-Fi. Le délai sur le lien satellite étant élevé, les données envoyées sur le lien Wi-Fi arrivent à destination avant les données en cours de transmission sur le lien satellite. Les données encore en vol sont alors considérées comme des trous dans la communication et signalées au nœud émetteur via les acquittements. Si les mêmes données sont signalées manquantes 3 fois, l'algorithme Fast Retransmit est utilisé par l'émetteur : la fenêtre de congestion est diminuée de moitié et les données signalées manquantes sont retransmises. Une fois les retransmissions effectuées, la fenêtre quitte l'état Fast Retransmit et entre en « congestion avoidance ». Elle se stabilise quand sa taille est suffisamment importante pour envoyer toute la quantité de données générée par l'application.

Après le changement de réseau entre Wi-Fi et satellite à environ 40s, 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 induite 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.



(a)Comportement de la fenêtre de congestion sur le réseau hybride.



(b) Comportement de la fenêtre sur le réseau multi-domicilié

Figure 46 – Comportement de la fenêtre de congestion lors de changement de réseaux entre satellite et Wi-Fi (20s) puis entre Wi-Fi et satellite (40s).

II.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 (soit égale à 1 paquet d'après le standard de SCTP).

II.3.1 Perte d'un paquet retransmis avec Fast Retransmit.

Dans l'expérience illustrée par la Figure 46, 50 Ko 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 du 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 « Slow Start » pour grandir.

Le Tableau 11 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 Ko de données. Comparées aux 110 ms nécessaires à l'envoi de ces données avec une fenêtre de congestion optimale, le temps de transmission est doublé.

II.3.2 Adaptation en « Congestion Avoidance » sur un réseau satellite.

Après l'utilisation du Fast-Retransmit suivant le premier changement de réseau, 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 sa taille afin d'atteindre sa valeur optimale. L'algorithme « congestion avoidance » étant prévu pour éviter la congestion, l'adaptation 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 Ko et 57 Ko dans la Figure 46 (a). En théorie, la fenêtre peut augmenter de 1 MTU à chaque RTT, la durée de cette phase peut donc être exprimée

Tableau 11 – Evolution de la fenêtre de congestion théorique après la perte de données retransmises avec l'algorithme Fast Retransmit (valeurs en octets).

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

ainsi:

Equation 9 : $$T = \Delta_{Données} * \frac{RTT}{MTU}$$

En prenant un RTT de 500ms pour le lien satellite et un MTU de 1500 octets, 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 (voir Figure 46 (a)).

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 capacité de transmission disponible (64Ko/s). La bande passante disponible est alors entièrement utilisée, l'accroissement de la fenêtre jusqu'à sa valeur maximale est uniquement dû au délai très élevé du réseau satellite et à la présence de file d'attente importantes : ce qui explique une grande quantité de données en vol. Si des pertes apparaissent au cours de cette phase d'adaptation, l'impact sur les communications 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.

Dans une communication, l'observation du flux de données à l'arrivée permet aussi de détecter certains comportements non optimaux. La Figure 47 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 40s et ce pendant environ 2s. Ce comportement est du à l'utilisation de l'algorithme « Congestion Avoidance » après la phase en « Fast-Retransmit » à 20s (premier changement de

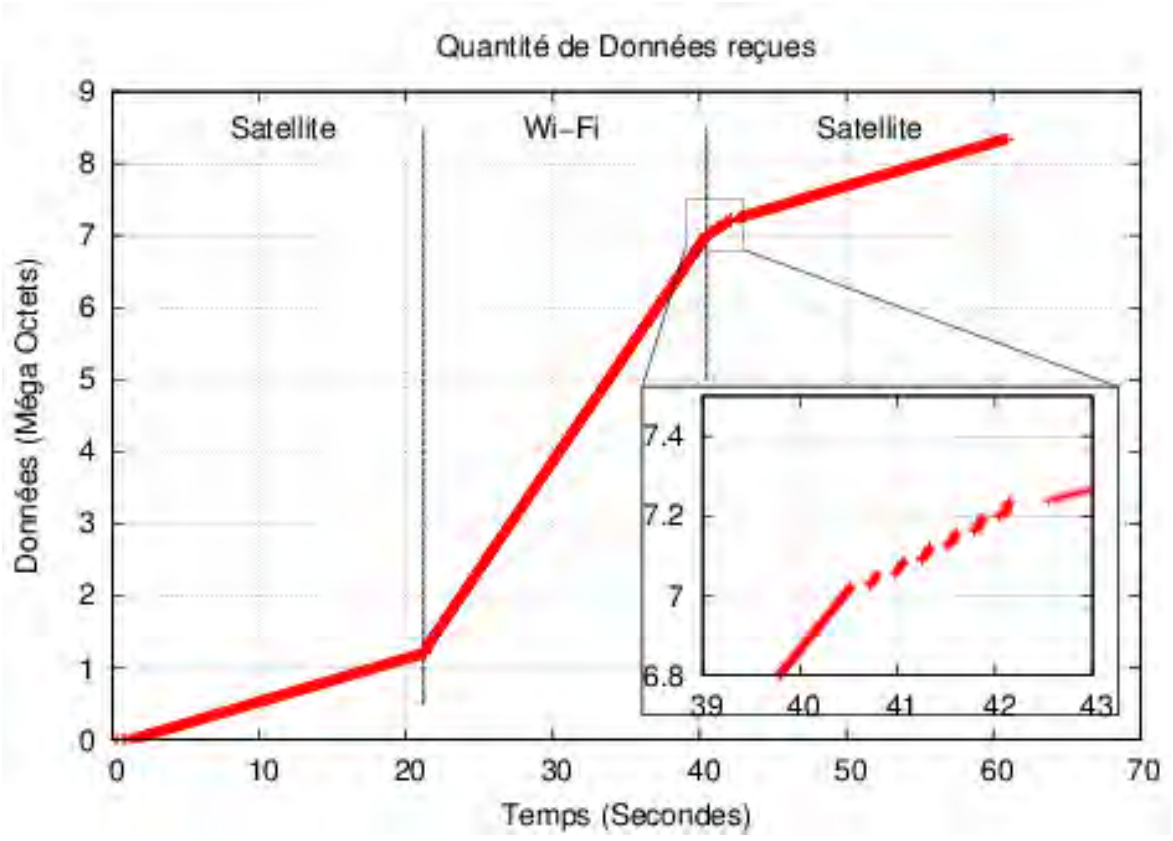


Figure 47 – Evolution de la quantité de données reçues sur un réseau hybride lors du changement de réseau entre satellite et Wi-Fi (20s) puis Wi-Fi et satellite (40s).

réseau). 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.

II.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 SCTP 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:

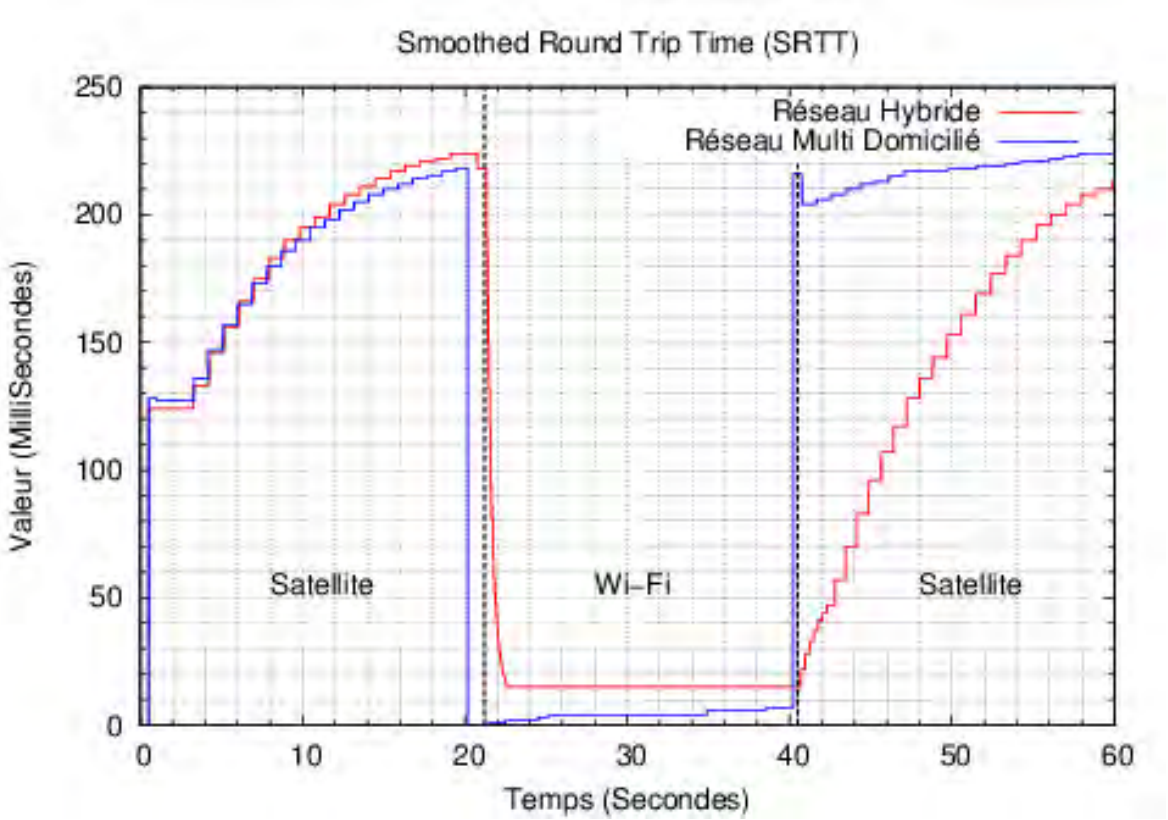
- Si le RTO est trop faible : des paquets peuvent être retransmis inutilement,
- Si le RTO est trop élevé : les pertes ne sont pas détectées assez vite.

Les Figure 48 (a) et (b) 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.

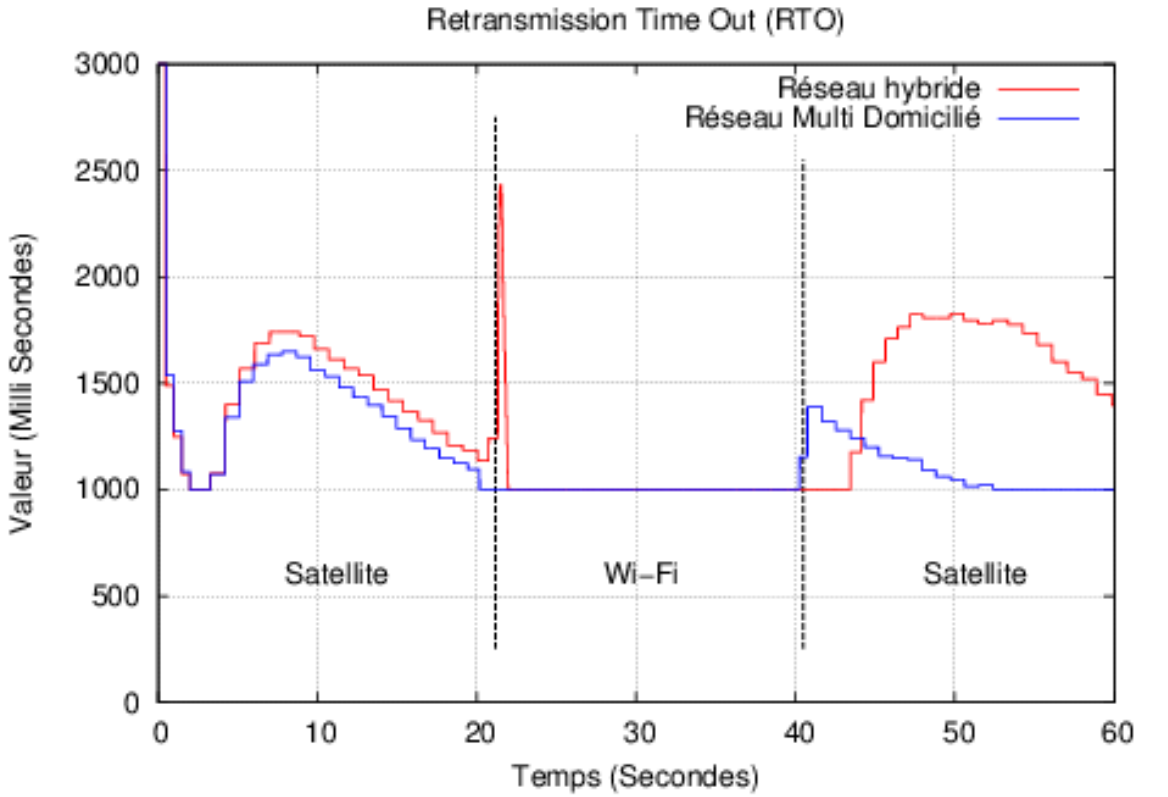
À 20s, le changement de réseau entre satellite et Wi-Fi est réalisé. Sur le réseau multi-domicilié, il est clairement visible que le SRTT et le RTO repartent avec leurs valeurs initiales car un nouveau jeu de paramètres est utilisé pour ce chemin. Sur le réseau hybride, l'adaptation se fait rapidement 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 (40s), les comportements diffèrent : sur le réseau multi-domicilié, les anciennes valeurs sont reprises tandis que, sur le réseau hybride l'adaptation 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 1.5s, puis diminue à partir de 50s.

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.



(a) SRTT : estimation du RTT entre les hôtes de la communication.



(b) RTO : valeur du temporisateur utilisé pour les retransmissions.

Figure 48 – Evaluation des latences faites par le protocole de Transport lors de changement de réseau entre satellite et Wi-Fi (20s) puis entre Wi-Fi et satellite (40s).

III 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 changé : 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.

L'architecture introduite dans ce papier est basée 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. A l'opposé, l'utilisation d'un 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.

La technique proposée pour la mise en œuvre de notre architecture revient à faire du cross-layer distribué entre le routeur mobile et les nœuds qui y sont connectés. En effet, des informations de la couche Liaison du routeur sont utilisées par la couche Transport des nœuds mobiles. Néanmoins, il ne s'agit pas là de véritable cross-layer puisque la communication d'informations se fait au moyen de la couche Réseau par la sélection du sous-réseau de préférence.

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 possèdent les mécanismes nécessaires. Les modifications nécessaires à sa mise en place se situant 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 ; ils ne seront pas impactés par notre solution.

Conclusion

Au cours de cette thèse, nous avons étudié une des principales problématiques de la mobilité : le changement de réseau. L'état de l'art nous a permis de déterminer que les solutions existantes permettent de résoudre certains impacts de ce changement de réseau mais la modification des caractéristiques sur le chemin utilisé pour les communications reste difficile à résoudre. L'influence de ce changement pouvant être ressenti même s'il n'a pas lieu directement au niveau du nœud mobile, il est difficilement prévisible et souvent indétectable. Pour essayer de résoudre cette problématique, nous nous sommes intéressés aux protocoles de Transport multi-domicilié et plus particulièrement à SCTP.

Dans un premier temps, il était nécessaire de vérifier que les performances d'un tel protocole soient correctes sur un lien fixe (ne présentant pas de changements de réseau). En effet, il est inutile de supprimer l'impact du changement des caractéristiques du réseau si le gain de performance qui en résulte est annulé par une chute des performances lorsque le lien est stable. Afin de vérifier le bon comportement de SCTP, nous l'avons comparé à TCP qui est le protocole de Transport de référence omniprésent de nos jours et avons démontré que les deux protocoles de Transport ont des performances similaires sur un lien fixe, même si celui-ci est contraignant. Forts de cette analyse, nous nous sommes alors intéressés à l'impact de la modification des caractéristiques du réseau et de quelle manière la multi-domiciliation pouvait le réduire. L'analyse faite du comportement de SCTP en mono-domicilié a permis de déterminer les causes des pertes de performances lors du changement de réseau, notamment les études séparées de l'impact du délai et de l'impact de la bande passante ont permis de relever l'influence de chaque paramètre. Enfin, nous avons constaté que la multi-domiciliation permet de limiter l'impact de la modification des caractéristiques en effectuant une meilleure évaluation du nouveau réseau notamment. Il est important de noter que cette différence est aussi visible par rapport à diverses versions de TCP en mono-domicilié. La multi-domiciliation au niveau du protocole de Transport permet donc de limiter la dégradation des performances dans un contexte mobile.

Partant du constat que les véhicules de transport en commun ont des caractéristiques particulières et que leur mobilité est différente des véhicules particuliers, nous avons proposé un nouvel algorithme pour la gestion de la mobilité avec mSCTP basé sur la configuration en avance des interfaces réseau. Les tests effectués en émulation et en simulation ont permis de vérifier les hypothèses émises ainsi que l'analyse temporelle. Il est possible de réduire la latence nécessaire à mSCTP pour changer de réseau et ainsi d'augmenter la capacité de transfert globale disponible le long du trajet du véhicule. L'un des avantages de cette solution est la facilité de déploiement, aucune entité supplémentaire n'est nécessaire dans le réseau ; seule la présence de mSCTP est indispensable. Dans le contexte des transports en commun, un gestionnaire de flotte a la possibilité de déployer une solution en modifiant uniquement ses véhicules et en ne touchant pas à l'infrastructure. Il n'est donc pas nécessaire d'utiliser une solution particulière à un fournisseur d'accès et implémentée sporadiquement.

L'étude faite sur l'impact du changement de réseau a permis d'affirmer l'apport de la multi-domiciliation. Néanmoins, la présence d'un changement de réseau transparent comme dans un réseau mobile par exemple ne permet pas d'utiliser la multi-domiciliation directement sur le nœud hôte de la communication, même si le routeur est multi-domicilié. Nous proposons une architecture qui permet de remédier à cela en étendant la multi-domiciliation jusqu'aux terminaux. Il est alors possible d'éviter une mauvaise interprétation des phénomènes suivant un changement de réseau en utilisant des mécanismes adéquats. L'analyse du comportement de SCTP dans le cas hybride et dans le cas multi-domicilié permet d'espérer des résultats intéressants avec une telle solution. Contrairement à la

proposition précédente, le routeur mobile peut utiliser ici le gestionnaire de mobilité qu'il souhaite, celui-ci n'intervenant pas directement dans les nouveaux mécanismes définis par notre architecture. L'utilisation d'un protocole de Transport multi-domicilié permet de lutter contre l'impact du changement de réseau mais apporte un second avantage. Un nœud mobile souhaitant utiliser ponctuellement l'un de ses interfaces pour communiquer peut le faire librement tout en restant connecté au routeur mobile. Les contraintes fixées par la connexion au routeur mobile sont donc minimes. De plus, un nœud ne possédant pas de protocole de Transport multi-domicilié peut utiliser l'un de ces protocoles et ne verra pas ses performances dégradées. Ses deux points permettent à notre architecture un meilleur respect des nœuds ne voulant pas utiliser notre solution et peut ainsi faciliter le déploiement.

Les contributions faites durant cette thèse ont permis de mettre en avant l'apport de la multi-domiciliation dans le contexte mobile. Deux voies différentes ont été choisies pour cela : réduire la latence nécessaire à la configuration des interfaces réseau d'un côté et limiter l'impact des changements de réseau transparent de l'autre. Dans les deux cas, l'utilisation de plusieurs interfaces permet d'améliorer les performances tout en garantissant des performances identiques sur un lien stable. La multi-domiciliation étant amenée à devenir courante dans les années à venir, il est intéressant d'explorer toutes les possibilités qu'elle pourra apporter dans les réseaux de communication, la résumer à l'augmentation de bande passante étant réducteur.

Perspectives

Les travaux réalisés au cours de cette thèse ouvrent des perspectives, que ce soit dans la continuité des solutions proposées ou en complément à celle-ci.

Lors de l'état de l'art, nous avons présenté MPTCP, qui est en quelque sorte le « TCP du futur ». MPTCP étant multi-domicilié et proposant des services similaires à SCTP, il serait intéressant d'étudier précisément leurs points communs en théorie de en pratique. Les propositions faites dans cette thèse qui sont basées sur SCTP pourraient alors être reprises avec MPTCP et il serait intéressant de voir l'apport de ce protocole. Toutefois, l'étude de MPTCP est pour l'instant difficile au vu du pauvre déploiement des ses fonctionnalités de mobilité.

Dans un contexte mobile, le point d'accès choisi pour communiquer influe fortement sur les communications, que le nœud mobile soit un routeur ou un nœud simple. Dans nos travaux, nous sommes partis du principe qu'à tout instant, le meilleur réseau était utilisé. La réalité est pourtant différente pour deux raisons : la notion de meilleur réseau est relative aux exigences et les méthodes de choix existantes sont limitées. Il serait donc intéressant d'établir une méthode de choix du point d'accès ne se basant pas simplement sur la qualité du signal ou sur la bande passante disponible mais plutôt sur un ensemble de critères dépendant des demandes des utilisateurs. Une méthode de choix pouvant regrouper l'ensemble de ces critères serait l'utilisation de diagrammes étoiles. En pondérant les critères les plus importants, un nœud pourrait alors déterminer le réseau qui les rempli au mieux.

L'architecture proposée dans la dernière contribution doit être implémentée sur des composants réels afin de pouvoir vérifier son apport et tester ses performances face une gestion classique des réseaux mobiles. Nous envisageons pour cela l'utilisation d'une plateforme d'émulation ou même l'utilisation d'un réseau cellulaire et d'une ligne de transport en commun. Cette architecture vise à diminuer l'impact du changement de réseau sur les protocoles de Transport. Il serait intéressant de compléter ses fonctionnalités en ajoutant le multi-chemin au niveau du routeur : il serait ainsi possible d'augmenter la bande passante globale disponible mais aussi de décider quels flux doivent changer de liens en se basant sur des critères prédéfinis (exigences QdS, …). Il serait ainsi possible d'effectuer une différentiation des flux tout en répartissant la charge sur les différentes technologies de communication disponibles.

L'application SCTP développée dans le cadre de cette thèse visait deux points : générer du trafic SCTP et gérer la mobilité en se basant sur des évènements du réseau. Son amélioration passe par deux points : permettre une meilleure vision du contenu existant et ajouter des fonctionnalités. Le premier point vise essentiellement à ajouter une interface graphique permettant le paramétrage de l'association, l'affichage des performances et surtout la gestion de la mobilité. Cette piste est en cours d'exploration et devrait être implémentée sous Qt. En ajoutant l'acquisition de la position avec un GPS, il devient possible de connaître et d'afficher la position du nœud mais aussi de créer une base de données des réseaux rencontrés. Enfin, il serait intéressant d'ajouter au générateur de trafic d'autres protocoles de Transport pour permettre une mise en concurrence des flux. L'ajout de MPTCP notamment peut permettre d'étudier sa gestion de la mobilité et son support des changements de réseau.

Bibliographie

[1] ARCEP, « Rapport sur la couverture et la qualité des services mobiles en France métropolitaine », Novembre 2012.

[2] UMass DOME Testbed, "A Mobility Testbed", http://prisms.cs.umass.edu/dome/, mars 2013.

[3] H. Soroush, N. Banerjee, A. Balasubramanian, M.D. Corner, B.N. Levine, and B. Lynn, "DOME : A Diverse Outdoor Mobile Testbed," *Proc. ACM Intl. Workshop on Hot Topics of Planet-Scale Mobility Measurements (HotPlanet)*, June 2009.

[4] A. Balasubramanian, B. N. Levine, and A. Venkataramani, "Replication Routing in DTNs: A Resource Allocation Approach," *IEEE/ACM Transactions on Networking*, vol. 18, no. 2, pp. 596–609, Apr. 2010.

[5] C. Computing, Y. Chen, and B. Levine, "Capacity Enhancement using Throwboxes in DTNs," *Proceedings of IEEE International Conf on Mobile Ad hoc and Sensor Systems (MASS)*, October 2006.

[6] N. Banerjee, M.D. Corner, and B.N. Levine, "Design and Field Experimentation of an Energy-Efficient Architecture for DTN Throwboxes," *IEEE/ACM Transactions on Networking*, April 2010.

[7] V. Cerf, S. Burleigh, A. Hooke, L. Togerson, R. Durst, K. Scott, K. Fall, and H. Weiss, "RFC4838 : Delay-Tolerant Networking Architecture," Apr. 2007.

[8] K. Scott and S. Burleigh, "RFC5050 : Bundle Protocol Specification," Nov. 2007.

[9] L. Wood, W. M. Eddy, W. Ivancic, J. Mckim, and C. Jackson, "Saratoga : a Delay-Tolerant Networking convergence layer with efficient link utilization," *Development*, pp. 168–172, Sep. 2007.

[10] Jacques Villain, *À la conquête de l'espace : de Spoutnik à l'homme sur Mars*, Vuibert Ciel & Espace, 2007.

[11] M. Amiot, « Les ménages français ont acheté plus de tablettes que de bons vieux PC de bureaux », http://archives.lesechos.fr/archives/2012/lesechos.fr/01/17/0201848007981.htm, Les Echos.fr, 17 janvier 2012.

[12] William J. Jorden, Soviet Fires Earth Satellite Into Space; It Is Circling the Globe at 18,000 M.P.H.; Sphere Tracked in 4 Crossings Over U.S. [archive], *The New York Times*.

[13] Ancillary Description Writer's Guide, 2012. Global Change Master Directory. National Aeronautics and Space Administration. [http://gcmd.nasa.gov/User/suppguide/].

[14] Autorité de Régulation des communications électroniques et des postes (ARCEP), « Réseaux Locaux radioélectriques ou RLAN (Wi-Fi) : les puissances d'émissions autorisées », http://www.arcep.fr/index.php?id=9272#c12931, mars 2008.

[15] OpenWrt, https://openwrt.org/.

[16] DD-WRT, http://www.dd-wrt.com/site/index.

[17] L. Dritsoula and C. B. Papadias, "On the Throughput Potential of Two-Dimensional Wireless Multi-Hop Networks Using Directional Antennas," in *69th Vehicular Technology Conference VTC Spring 2009*, 2009.

[18] H. Menouar, M. Lenardi, and F. Filali, "A Movement Prediction-based Routing Protocol for Vehicle-to-Vehicle Communications," *1st international Vehicle-to-Vehicle Communications Workshop San Diego USA*, Jul. 2005.

[19] 3rd Generation Partnership Project, "Quality of Service (QoS) concept and architecture", SP-56, 2012.

[20] ITU-R, "Report ITU-R M.2134 Requirements related to technical performance for IMT-Advanced radio interface(s)," Oct. 2008.

[21] D. Johnson, C. Perkins, and J. Arkko, “RFC3775 : Mobility Support in IPv6,” Jun. 2004.

[22] . Perkins, D. Johnson, and J. Arkko, “RFC6275 : Mobility Support in IPv6,” Jul. 2011.

[23] R. Koodli, “RFC5568 : Mobile IPv6 Fast Handovers,” Jul. 2009.

[24] H. Soliman, C. Castellucia, K. Elmalki, and L. Bellier, “RFC5380: Hierarchical Mobile IPv6 Mobility Management,” Oct. 2008.

[25] H. Jun, H. Soliman, S. J. Koh, and J. Y. Lee, “Draft: Fast Handover for Hierarchical MIPv6 (F-HMIPv6),” vol. 6, Apr. 2005.

[26] J. Manner and M. Kojo, “RFC3753 : Mobility Related Terminology,” Jun. 2004.

[27] T. Ernst, N. Montavont, R. Wakikawa, C. Ng, and K. Kuladinithi, “Motivation and Scenarios for Using Multiple Interfaces and Global Addresses,” May 2008.

[28] N. Montavont, R. Wakikawa, T. Ernst, and K. Kuladinithi, “Analysis of Multihoming in Mobile IPv6,” May 2008.

[29] International Telecommuniaction Union, “Series G: Transmission Systems and Media, Digital Systems and Networks, Quality of Service and Performance, End-user multimedia QoS Categories”, G.1010, novembre 2001.

[30] R. Wakikawa, V. Devarapalli, G. Tsirtsis, T. Ernst, and K. Nagami, “RFC5648 : Multiple Care-of Addresses Registration,” Oct. 2009.

[31] B. Sousa, K. Pentikousis, and M. Curado, “A study of multimedia application performance over Multiple Care-of Addresses in Mobile IPv6,” in *Computers and Communications (ISCC), 2011 IEEE Symposium on*, 2011.

[32] J.-Y. Pan, J.-L. Lin, and K.-F. Pan, “Multiple Care-of Addresses Registration and Capacity-Aware Preference on Multi-Rate Wireless Links,” in *Advanced Information Networking and Applications - Workshops, 2008. AINAW 2008. 22nd International Conference on*, 2008.

[33] M. K. Park, J. Y. Lee, B. C. Kim, and D. Y. Kim, “Design of fast handover mechanism for multiple interfaces mobile IPv6,” in *Wireless Pervasive Computing, 2008. ISWPC 2008. 3rd International Symposium on*, 2008.

[34] G. Tsirtsis, H. Soliman, N. Montavont, G. Giaretta, and K. Kuladinithi, “RFC6089 : Flow Bindings in Mobile IPv6 and Network Mobility Basic Support,” Jan. 2011.

[35] T. Ernst and H.-Y. Lach, “RFC4885 : Network Mobility Support Terminology,” Jul. 2007.

[36] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert, “RFC3963 : Network Mobility (NEMO) Basic Support Protocol,” Jan. 2005.

[37] H. Petander, E. Perera, S. Member, and K. Lan, “Measuring and Improving the Performance of Network Mobility Management in IPv6 Networks,” *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 9, pp. 1671–1681, Sep. 2006.

[38] K. Leung, G. Dommety, V. Narayanan, and A. Petrescu, “RFC5177 : Network Mobility (NEMO) Extensions for Mobile IPv4,” Apr. 2008.

[39] Widely Integrated Distributd Environment (WIDE) Project, http://www.wide.ad.jp/index.html.

[40] K. Shima and Y. Uo, “An operational demonstration of a mobile network with a fairly large number of nodes,” *International Symposium on Applications and the Internet Workshops, 2006. SAINT Workshops 2006.*, pp. 0–3, Jan. 2006.

[41] C. Ng, T. Ernst, E. Paik, and M. Bagnulo, “RFC4980 - Analysis Of Multihoming in Network Mobility Support,” Oct. 2007.

[42] K. Shima, Y. Uo, N. Ogashiwa, and S. Uda, “Operational Experiment of Seamless Handover of a Mobile Router using Multiple Care-of Address Registration,” *Journal of Networks*, vol. 1, no. 3, pp. 23–30, Jul. 2006.

[43] M. S. Hossain, M. Atiquzzaman, and W. Ivancic, "Performance evaluation of multihomed NEMO," in *2012 IEEE International Conference on Communications (ICC)*, 2012, pp. 5429–5433.

[44] T. Ropitault and N. Montavont, "Implementation of Flow Binding Mechanism," *2008 Sixth Annual IEEE International Conference on Pervasive Computing and Communications (PerCom)*, pp. 342–347, Mar. 2008.

[45] Information Sciences Institure, "RFC793 : Transmission Control Protocol," Sep. 1981.

[46] "NEPL (NEMO Platfrom for linux) HOWTO, http://www.nautilus6.org/doc/nepl-howto/nepl-howto.html, 2010.

[47] "UMIP.org", http://www.umip.org/, 2012.

[48] M. Allman, V. Paxson, and E. Blanton, "RFC5681 : TCP Congestion Control," pp. 1–19, Sep. 2009.

[49] T. Henderson, S. Floyd, A. Gurtov, and Y. Nishida, "RFC6582 : The NewReno Modification to TCP's Fast Recovery Algorithm," Apr. 2012.

[50] C. Caini and R. Firrincieli, "TCP Hybla: a TCP enhancement for heterogeneous networks," *International Journal of Satellite Communications and Networking*, vol. 22, no. 5, pp. 547–566, Sep. 2004.

[51] S. Floyd, "HighSpeed TCP for Large Congestion Windows," pp. 1–35, Dec. 2003.

[52] K. Tan and J. Song, "Compound TCP : A Scalable and TCP-Friendly Congestion Control for High-speed Networks," *in 4th International workshop on Protocols for Fast Long-Distance Networks (PFLDNet)*, 2006.

[53] K. Tan, J. Song, Q. Zhang, and M. Sridharan, "A Compound TCP Approach for High-Speed and Long Distance Networks," *Proceedings IEEE INFOCOM 2006. 25TH IEEE International Conference on Computer Communications*, pp. 1–12, Apr. 2006.

[54] S. Ha, I. Rhee, and L. Xu, "CUBIC : A New TCP-Friendly High-Speed TCP Variant," *ACM SIGOPS Operating Systems Review*, pp. 64–74, Jul. 2005.

[55] W. Hansmann and M. Frank, "On things to happen during a TCP handover," in *28th Annual IEEE International Conference on Local Computer Networks, 2003. LCN '03. Proceedings.*, 2003, pp. 109–118.

[56] G. Giambene, S. Marchi, and S. Kota, "TCP Performance in Hybrid Satellite - WiFi Networks for High-Speed Trains," in *Third International ICST Conference, PSATS 2011*, 2011.

[57] T. Goff, J. Moronski, and D. S. Phatak, "Freeze-TCP : A true end-to-end TCP enhancement mechanism for mobile environments," *INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, pp. 1537–1545, Mar. 2000.

[58] Y. Lin and H.-P. Chang, "VA-TCP : A Vertical Handoff-Aware TCP," *SAC '07 Proceedings of the 2007 ACM symposium on Applied computing*, pp. 237–238, Mar. 2007.

[59] S. Keshav, "A control-theoretic approach to flow control," *Proceedings of the conference on Communications architecture & protocols - SIGCOMM '91*, pp. 3–15, 1991.

[60] A. Ford, C. Raiciu, M. Handley, S. Barre, and J. Iyengar, "RFC6182 : Architectural Guidelines for Multipath TCP Development," Mar. 2011.

[61] B. Ford and J. Iyengar, "Breaking Up the Transport Logjam," in *Hot Topics for Networks*, 2008.

[62] C. Raiciu, M. Handly, and D. Wischik, "RFC6356 : Coupled Congestion Control for Multipath Transport Protocols," 6356, Oct. 2011.

[63] Y. Sun, Y. Cui, W. Wang, T. Ma, Y. Ismailov, and X. Zheng, “Mobility support in Multi-Path TCP,” in *2011 IEEE 3rd International Conference on Communication Software and Networks*, 2011, pp. 195–199.

[64] R. Stewart, “RFC4960 : Stream Control Transmission Protocol,” Sep. 2007.

[65] R. Stewart, Q. Xie, M. Tuexen, S. Maruyama, and M. Kozuka, “RFC5061 : Stream Control Transmission Protocol (SCTP) Dynamic Address Reconfiguration,” Sep. 2007.

[66] M. Tuexen, R. Stewart, P. Lei, and E. Rescorla, “RFC4895 : Authenticated Chunks for the Stream Control Transmission Protocol (SCTP),” Aug. 2007.

[67] D. P. Kim, S. J. Koh, and S. W. Kim, “mSCTP-DAC: Dynamic Address Configuration for mSCTP Handover,” *Ifip International Federation For Information Processing*, pp. 244–253, Aug. 2006.

[68] A. Mahmoud, A.-A. Al-Helali, M. Abu-Amara, T. Al-Kharobi, and T. Sheltami, “Comparative Performance Study for Integrated 3G / WLAN Networks Using Mobile IP , SIP , and m- SCTP Protocols,” *Vehicular Technology Conference (VTC 2010-Spring)*, May 2010.

[69] T. Narten, E. Nordmark, W. Simpson, and H. Soliman, “RFC4861 : Neighbor Discovery for IP version 6 (IPv6),” Sep. 2007.

[70] H. Singh, W. Beebee, and E. Nordmark, “RFC5942 : IPv6 Subnet Model : The Relationship between Links and Subnet Prefixes,” Jul. 2010.

[71] A. Conta, S. Deering, and M. Gupta, “RFC4443 : Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification,” *Network Working Group*, Mar. 2006.

[72] G. Armitage, P. Schulter, M. Jork, and G. Harter, “RFC2491 : IPv6 over Non-Broadcast Multiple Access (NBMA) networks,” *Network Working Group*, Jan. 1999.

[73] M. Wasserman, “RFC3314 : Recommendations for IPv6 in third Generation Partnership Project (3GPP) Standards,” *Network Working Group*, Sep. 2002.

[74] J. ARkko, G. Kuijpers, H. Soliman, J. Loughney, and J. Wiljakka, “RFC3316 : Internet Protocol Version 6 (IPv6) for Some Second and Third Generation Cellular Hosts,” Apr. 2003.

[75] S. Thomson, T. Narten, and T. Jinmei, “RFC4862 : IPv6 Stateless Address Autoconfiguration,” Sep. 2007.

[76] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, and M. Carney, “RFC3315 : Dynamic Host Configuration Protocol for IPv6 (DHCPv6),” *Network*, Jul. 2003.

[77] J. Kempf, M. M. Khalil, and B. Pentland, “Drat: IPv6 Fast Router Advertisement,” 2005.

[78] G. Daley, B. Pentland, and R. Nelson, “Effects of Fast Router Advertisement on Mobile IPv6 Handovers,” in *Proceedings. Eighth IEEE International Symposium on Computers and Communication, 2003. (ISCC 2003)*, 2003.

[79] Network Simulator 2 (ns-2), “http://nsnam.isi.edu/nsnam/index.php/Main_Page” Nsnam.

[80] REAL, “http://www.cs.cornell.edu/skeshav/real/overview.html”.

[81] N. Abramson, “THE ALOHA SYSTEM — Another alternative for computer communications,” in *AFIPS ’70 (Fall)*, 1968.

[82] A. Gotta, F. Potorti, and R. Secchi, “Simulating Dynamic Bandwidth Allocation on Satellite Links,” in *WNS2 ’06 Proceeding from the 2006 workshop on ns-2: the IP network simulator*, 2006.

[83] T. Gayraud, L. Bertaux, and P. Berthou, “A NS-2 Simulation model of DVB-S2 / RCS Satellite network,” in *15th Ka Band Conference*, 2009.

[84] L. Bertaux, T. Gayraud, and P. Berthou, "How is SCTP Able to Compete with TCP on a QoS-Aware Satellite Network?," in *Second International Conference on Advances in Satellite and Space Communications (SPACOMM)*, 2010.

[85] Centre National d'Etude Spatial (CNES), www.cnes.fr, mars 2013.

[86] ASTRIUM Toulouse, www.astrium.eads.net, mars 2013

[87] Laboratoire d'Analyse et d'Architecture des Systèmes (LAAS), www.laas.fr, mars2013.

[88] A. Jurgelionis, J.-P. Laulajainen, M. Hirvonen, and A. I. Wang, "An Empirical Study of NetEm Network Emulation Functionalities," in *Proceedings of 20th International Conference on Computer Communications and Networks (ICCCN)*, 2011.

[89] D. L. Mills, "Network Time Protocol (Version 3) Specification , Implementation and Analysis," Mar. 1992.

[90] Wireshark, GNU General Public License version 2, http://www.wireshark.org/, décembre 2012.

[91] Iperf, http://iperf.fr/, mars 2013.

Network Architecture for Connected Public Transports

With the growing popularity of mobile devices, Public Transport will have to evolve and will have to introduce new services to customers, like an Internet connection onboard for example. The vehicle will act as a mobile router providing its nodes with a reliable connection and therefore will be forced to stay connected to an access point at any time. Since network coverage area is restricted depending on communication technology and environment, performing handovers is mandatory, leading to network events affecting Transport protocols efficiency: latencies are introduced by network configuration, network parameters are changed brutally. This thesis studies such impact by focusing on its source before giving solutions aiming at lowering handover impact. Two means were chosen: lowering latencies introduced by network configuration and avoiding network parameters modification impact on Transport protocols.

Keywords : Mobiles Networks, Transport Protocols, Wi-Fi, 3G, Satellite Communication Networks, SCTP, TCP

AUTEUR : Lionel Bertaux

TITRE : Architecture Réseau pour Véhicule de transport en commun communiquant

DIRECTEUR DE THESE : Thierry Gayraud et Pascal Berthou

LIEU ET DATE DE SOUTENANCE : Toulouse, le 26 septembre 2013

Avec la démocratisation des appareils mobiles, les transports en commun sont amenés à proposer de nouveaux services à leur usagers et notamment une connexion à Internet. Le véhicule de transport en commun agit alors comme un routeur mobile fournissant une connexion fiable à ses nœuds et doit pour cela être connecté en permanence à un point d'accès. Les zones de couverture étant limitées par les technologies utilisées et par les obstacles, des changements de réseaux sont alors nécessaires et provoquant différents évènements pouvant impacter les performances des protocoles de Transport : introduction de latences dues à la configuration des interfaces, modification des caractéristiques du chemin utilisé par la communication.. Dans cette thèse nous étudions cet impact en déterminant son origine puis nous proposons des solutions visant à le réduire de deux manières : en réduisant les latences introduites par le changement de réseau et en diminuant l'impact de la modification des caractéristiques du réseau.

MOTS-CLES : Réseaux Mobiles, Protocoles de Transport, Wi-Fi, 3G, Réseaux de Communication par Satellite, SCTP, TCP.

DISCIPLINE ADMINISTRATIVE : Informatique

LAAS-CNRS, 7 avenue du colonel Roche, 31400 Toulouse Cedex 9