Introduction

Le but de cette thèse est de faire avancer l'état de l'art des communications IP (notamment IPv6) vers des solutions prenant en charge la mobilité à grande échelle de réseaux de réseaux. Cette problématique s'intègre dans une vision de réseaux du futur, plus connus sous la terminologie "Future Internet" (F.I.). En effet, les chercheurs de ce domaine soutiennent que l'évolution d'Internet depuis son origine a suivi une direction qui a amené une certaine complexité et un manque de transparence sur la vision globale de l'architecture. En conséquence, il est de plus en plus difficile d'intégrer des solutions novatrices et utiles (telles que Mobile IPv6, Multicast, Multihoming et plus) dans l'architecture globale sans violer les principes de base sur lesquels repose cette construction, plus particulièrement le principe du "End-to-End design". L'initiative a été prise par des projets NSF (aux USA), FP7 (en Europe) et nationaux au Japon de faire des propositions selon deux méthode afin de permettre une avancée dans le domaine des réseaux du future: (1) Des approches évolutives, qui prennent un certain héritage de l'architecture actuelle d'Internet tout en évoluant sur des problèmes ciblés tels que la mobilité, le multihoming ou le multicast. (2) Des approches révolutionnaires (Feuille blanche, ou Clean Slate en Angl.), où il s'agit de proposer des solutions (architectures complètes) traitant de sujets spécifiques, techniques (routage avec des noms plats, sécurité des contenus ou autre) ou moins techniques (donner une plus grande liberté à l'utilisateur, favoriser la concurrence entre les fournisseurs d'accès Internet ou autre) sans forcément proposer des solutions de compatibilité avec l'architecture actuelle.

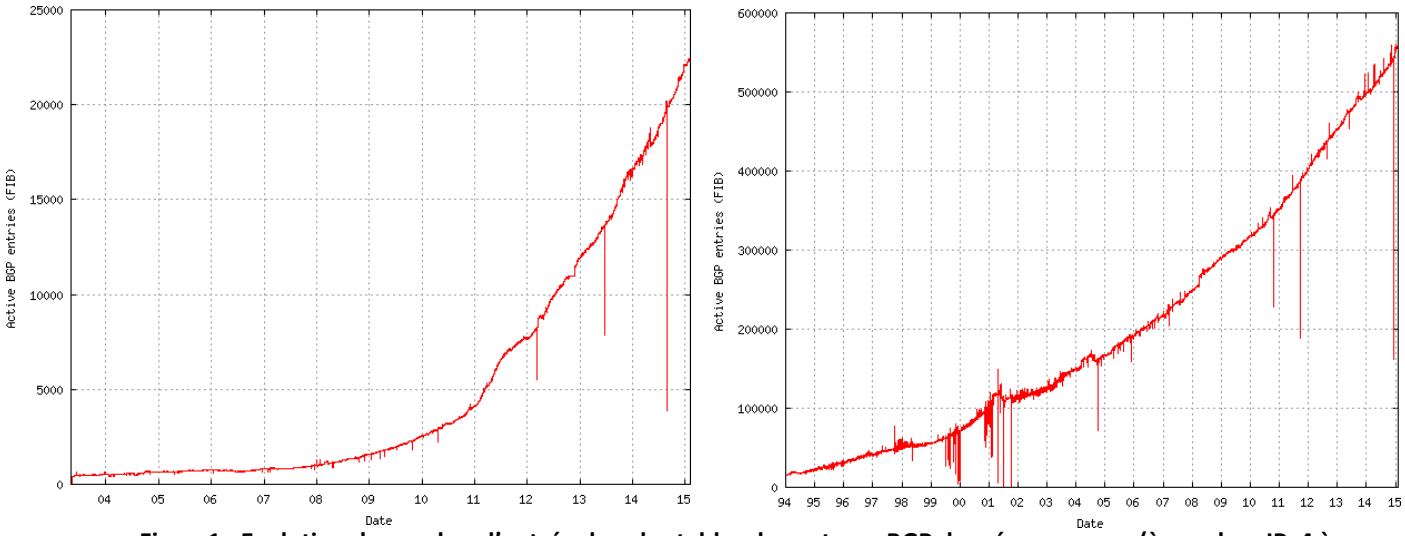

Figure1 : Evolution du nombre d'entrée dans les tables de routages BGP des réseaux cœur (à gauche : IPv4 à droite : IPv6)

La figure 1 illustre le problème du point de vue des opérateurs. En effet, les fournisseurs d'accès Internet utilisent le protocole BGP dans le cœur du réseau afin de router le trafic IP vers sa destination finale. Ces dernières années le nombre d'entrées dans ces tables de routage a explosé de manière exponentielle. Les craintes des opérateurs par rapport à la scalabilité de leurs réseaux ont été exprimées notamment au Workshop 2006 sur le nommage et l'adressage organisé par l'Internet Architechture Board (IAB). Ce workshop est le point de départ pour des propositions du Future Internet compatibles avec l'architecture passée (solutions dites « évolutionnaire ») ainsi que des approches de rupture (dites « révolutionnaires »).

Locator/Identifier Separation Protocol (LISP)

Dans la catégorie « évolutionnaire » prenant en charge la compatibilité avec spécification IP passée, le protocole Locator Identifier Separation Protocol (LISP) est le plus connu. Dans cette approche [1], les auteurs reprochent à la spécification de l'Internet Protocol de confondre les fonctionnalités de nom et de localisateur dans l'adresse IP. En effet, dû au manque d'outils réseaux, les ingénieurs ont utilisé dans leur protocoles compatibles IP les fonctionnalités de nom et d'adresse de manière interchangeable : l'adresse IP sert à identifier les correspondant (et donc de différencier les interlocuteurs) et de les localiser (pour leur acheminer le trafic). Cette confusion a pour résultat indirect d'augmenter les tailles des tables de routage BGP dans le cœur du réseau Internet.

Afin de répondre à ce besoin de séparation, les auteurs de LISP définissent l'architecture dans la Figure 2. Un site LISP est définit par son lot d'adresses EID qu'il utilise comme identifiant. Les sites LISP sont interconnectés par des routeurs de type ITR/ETR qui encapsulent le trafic originaire et à destination d'un autre site dans un tunnel. Pour ce faire, un autre lot d'adresses localisent ces ITER/ETR, des adresses dites RLOC. La correspondance entre les adresses de type EID (pour l'intérieur d'un site LISP) et RLOC (pour les routeurs externes ITR/ETR) est maintenue dans un table de correspondance globale : le mapping system (MS). Avant de transmettre un trafic dans le tunnel qui sépare un ITR d'un ETR, le routeur ITR qui se trouve dans le site à l'origine de ce trafic, doit faire correspondre l'adresse RLOC en effectuant une demande de correspondance au MS.

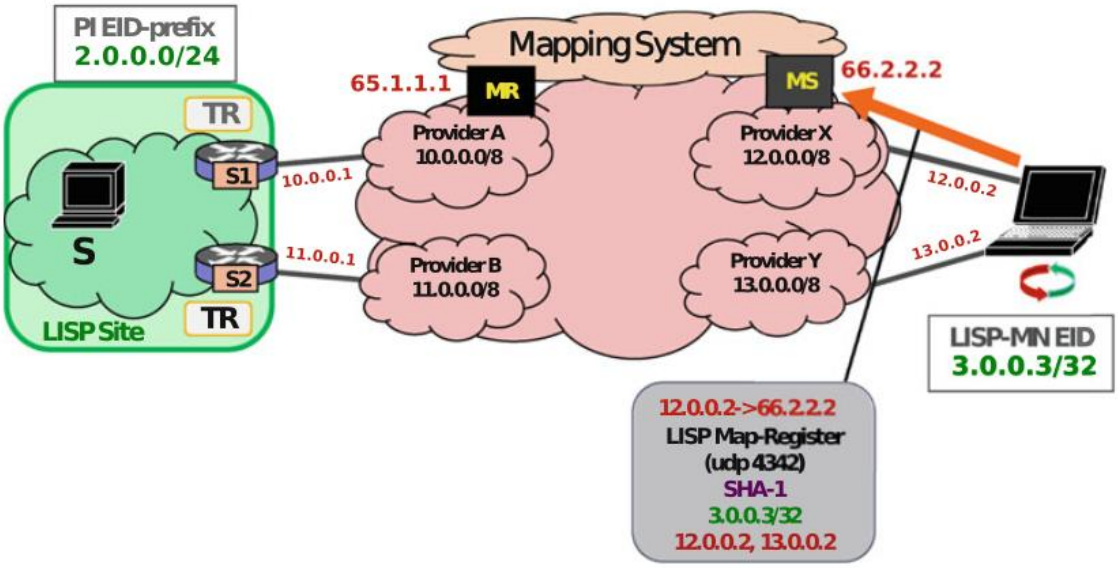

Figure2 : Architecture de référence pour le protocole LISP

Communications Véhicule-à-Internet

Dans le cadre de ce protocole LISP, au cours de cette thèse, une attention particulière est donnée au contexte des communications IPv6 pour réseaux véhiculaires, qui est adapté à la problématique du nommage et d'adressage englobée dans ce qui est décrit plus haut. En effet, les communications dans ce domaine sont proposées dans une configuration Vehicle-Infrastructure, Vehicle-Vehicle et plus récemment de cluster de véhicules dans le cadre d'applications surtout en relation avec la sécurité routière. L'un des objectifs de cette thèse sera de traiter le cas des communications IPv6 de Vehicule(s) à Véhicule à Infrastructure pour des applications plus diversifiées tout en gardant des objectifs de scalabilité et d'extension de l'existant.

Afin d'illustrer les cas d'usages faisant appel aux communications Véhicule-à-Internet, deux scénarios ont été étudiés dans cette thèse : e-Santé (eHealth) et le véhicule électrique (FEV, Angl. Fully-electric Vehicle). La e-Santé est une discipline en plein essor qui a profité des dernières évolutions d'Internet de termes de débit, d'utilisation et de mobilité. Elle comprend l'ensemble des technologies médicales connectées qui permettent de surveiller l'état d'un patient à distance. Ces appareils médicaux peuvent utiliser des technologies sans fil de courte portée (Bluetooth, Zigbee, Wifi) et s'appuient ensuite sur des routeurs connectés à Internet afin de transmettre les signaux vitaux relevés sur le patient. Le problème de la plateforme adéquat supportant les communications e-Santé depuis le véhicule se pose alors.

Le développement des véhicules électriques reste très dépendant du développement des batteries afin de garantir au chauffeur d'atteindre une destination arbitraire sans tomber en panne de batterie. Le projet européen Eco-FEV a pour but de mettre en commun les infrastructures routières (constructeur, autoroute, centre de recharge) dans une architecture unifiée où des serveurs suivent l'état du véhicule électrique pendant son trajet et lui conseillent notamment des chemins où il croisera un centre de recharge. Les problèmes de mobilité IPv6 et de continuité des communications se posent alors.

La plateforme e-Santé véhiculaire (l'ambulance connectée)

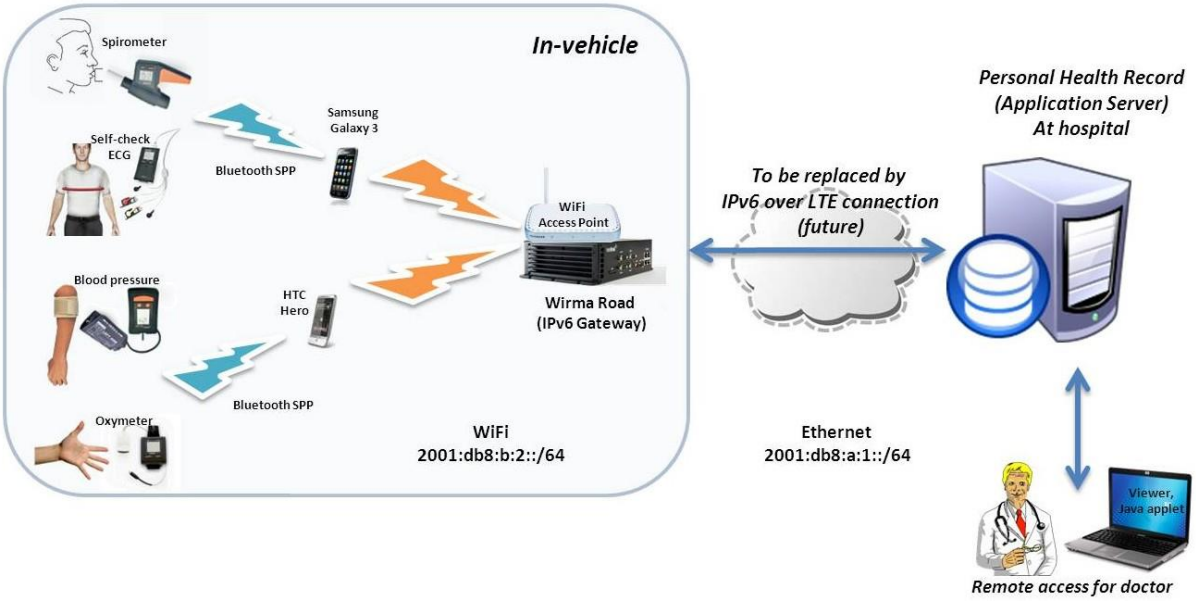

Figure3 : Plateforme e-Santé embarquée – l'ambulance connectée

La Figure 3 illustre notre proposition de plateforme e-Santé représentant le modèle d'une ambulance connectée. Cette plateforme comprend des appareils capables de communiquer en Bluetooth (spiromètre, électrocardiogramme, tension sanguine, oxymètre) vers une application contenue dans un appareil Android (application vidavo Vida24). Ces données sont ensuite transmises à travers une connexion IPv6 qui passe par notre routeur mobile connectée à l'Internet en 3G/IPv6. Ce routeur transmet plus tard les données vers un serveur localisé sur Internet. Ces données peuvent être accédées à tout moment par le médecin traitant et un diagnostic peut être posé ou une chambre de soins peut être préparée, selon les cas.

Le routeur mobile embarqué dans le véhicule annonce un préfixe IPv6 qu'il a récupéré auparavant d'Internet (DHCPv6 prefix delegation) ou d'un serveur local dans son Home Network (Network Mobility for Mobile IPv6).

Architecture intégrée pour les services IP du véhicule électrique

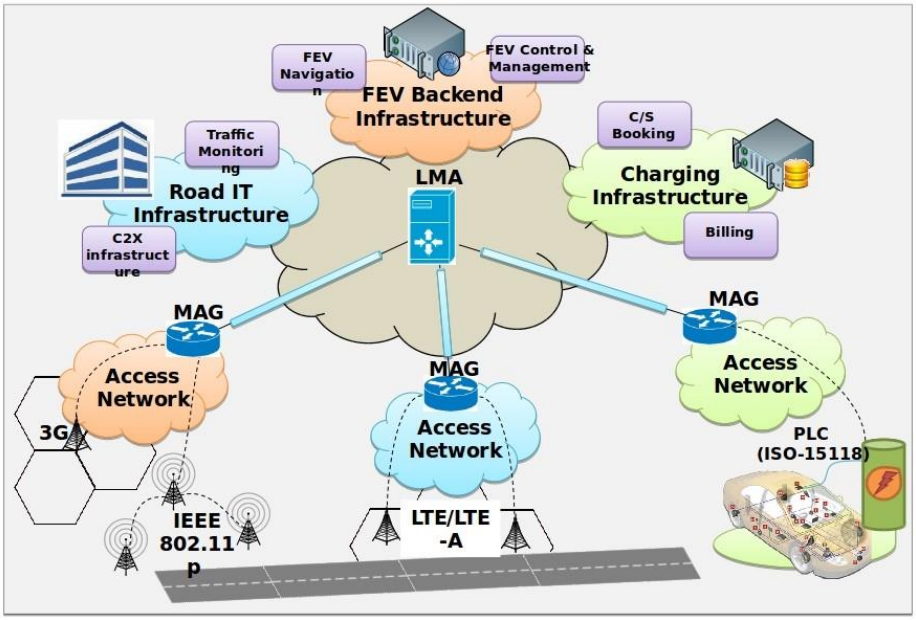

Figure4 : Architecture unifiée pour les services IP du véhicule électrique

La Figure 4 illustre la vue globale de l'architecture de mobilité PMIPv6 (Proxy Mobile IPv6, RFC5213) intégrant l'infrastructure de la route avec d'autres acteurs utiles au bon fonctionnement du véhicule électrique. Dans cette architecture, le véhicule dispose d'un identifiant unique (le numéro identifiant du véhicule, VIN) et qui permet de lui attribuer les mêmes adresses IP/IPv6 quelle que soit l'interface utilisée (PLC, WiFi, LTE). Cette identification unique permet de garantir que les applications IPv6 sur Internet restent activent et continuent de surveiller l'état du véhicule sans déconnexions (continuité de session IPv6). Les services IP peuvent annoncer des perturbations sur le chemin, conseiller le véhicule sur des trajets alternatifs et indiquer sur une carte la localisation des points de recharge les plus proches.

Ces deux cas d'usage de communications Véhicule-à-Internet illustrent les besoins en mobilité d'adressage IPv6, continuité de session pour les applications et l'importance d'architectures sacalables supportant un nombre important d'utilisateurs.

Les protocoles de gestion de mobilité

L'IETF (Internet Engineering Task Force) définie et normalise plusieurs protocoles de gestion de mobilité selon les besoins des opérateurs mobiles, notamment. Depuis la couche réseau du modèle OSI, on peut classer les protocoles de mobilité comme indiqué sur le Tableau 1.

		Anchoring function	
		Centralized	**Distributed**
Location Update	**Host-based**	**Mobile IPv6, LISP-MN**	**Client-DMM**
	Network-based	**PMIPv6**	**Network-DMM**

Tableau 1 : Classification des approches de gestion de mobilité de la couche réseau

Les protocoles de gestion de mobilité comprennent 3 fonctions importantes :

- La fonction d'ancrage ; qui permet de centraliser les échanges IP dans un point unique de l'architecture et attribuer les adresses/préfixes IPv6
- La base de données de localisation ; qui permet de suivre l'état de mobilité des utilisateurs et de mettre à jour leur localisations. Elle fait donc appel à un protocole de mise à jour de localisation.
- La fonction de transfert ; qui permet de faire suivre le trafic destiné à un utilisateur mobile selon sa localisation.

Le Tableau 1 illustre la classification des protocoles de mobilité selon le placement de ces fonctions dans l'architecture. Pour notre comparaison des protocoles centralisés et distribués, nous prenons le cas des protocoles MIPv6, PMIPv6, et N-DMM. Nous proposons aussi d'étendre le protocole N-DMM d'une extension de mobilité de réseaux, N-DMM-NEMO (Figure 5).

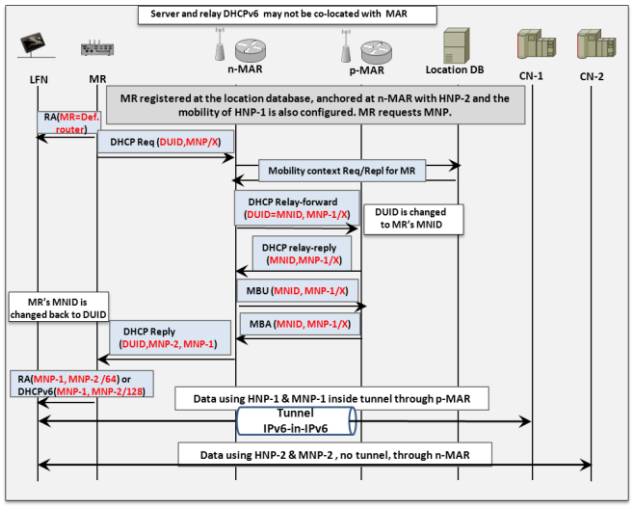

Figure5 : Extension NEMO pour le protocole N-DMM

Cette extension étend la proposition de Network DMM avec le support de la mobilité de réseaux IPv6. Dans notre proposition après que le routeur mobile s'attache au réseau et reçoive un préfixe du nouveau MAR (Mobility Anchor Router), le n-MAR demande à la base de localisation des utilisateurs du réseau de mettre à jour la nouvelle localisation du MR. Le contexte de mobilité du routeur mobile est ainsi transféré au n-MAR qui demande ensuite au précédant MAR (p-MAR) d'étendre la période validité du préfixe du MR dans son domaine et de transférer tout trafic vers sa nouvelle localisation. Un tunnel est établi entre les deux MARs, le trafic vers les utilisateurs CN-1 et CN-2 peut se poursuivre vers la nouvelle localisation du MR.

Comparaison entre les protocoles centralisés et distribués

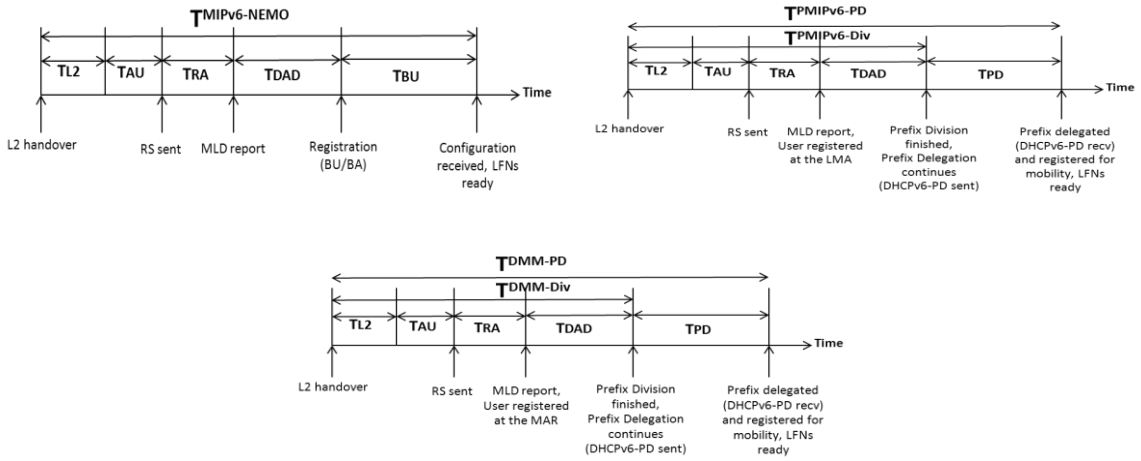

Figure6 : Configuration d'adresses pour les protocoles MIPv6, PMIPv6 et DMM (respectivement).

La Figure 6 illustre les phases de la configuration d'adresses IPv6 suivies dans les protocoles MIPv6, PMIPv6 et DMM pour l'extension NEMO. Dans les 3 protocoles, une phase d'authentification est nécessaire avant l'établissement de connexion, l'annonce de préfixe (Router Advertisement) et l'exécution de l'algorithme de détection de collision. Les 3 protocoles ensuite se distinguent lors de la phase de mobilité de préfixes. Pour MIPv6, un échange BU/BA est nécessaire et suffisant pour obtenir un préfixe du Home Network. Pour PMIPv6 et DMM, un échange DHCPv6 Prefix Delegation est nécessaire afin d'obtenir un préfixe HNP. Cette phase peut déclencher plusieurs messages, notamment si la mobilité est inter-sites et pas seulement à l'intérieur du même site.

Afin de comparer la performance des approches précédente, nous proposons d'utiliser un modèle analytique dont nous montrons seulement les résultats ici.

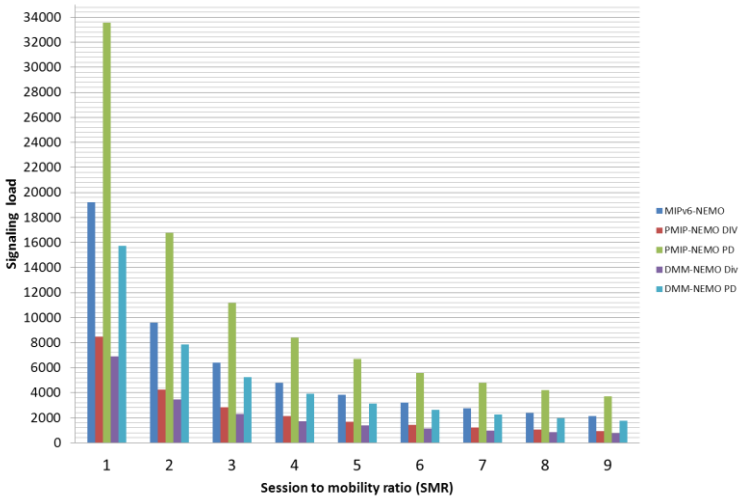

Figure7 : Impact du ratio session-à-mobilité sur l'évolution du coût de signalisation.

La Figure 7 illustre l'impact du ratio session-à-mobilité (SMR) sur l'évolution de la charge en signalisation. Le SMR représente le taux communications par rapport à celui de la mobilité d'un hôte IPv6 : si le (SMR >> 1), le nœud est alors presque statique, alors que (SMR<=1) signifie que la mobilité de l'utilisateur est plus importante. Nous observons sur le graphe que le taux de signalisation baisse avec la faible mobilité de l'utilisateur et qu'elle augmente avec son augmentation (SMR proche de 1). La tendance est que les approches centralisées (MIPv6-NEMO et PMIPv6-NEMO PD) provoquent plus de signalisation et coutent donc plus en charge que l'approche DMM-NEMO PD distribuée.

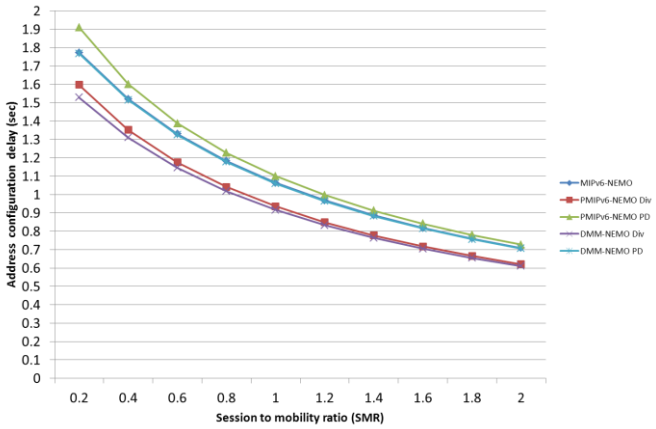

Figure8 : Impact du ratio session-à-mobilité sur l'évolution du délai de configuration d'adresses.

La figure 8 illustrant l'effet du SMR sur le délai de configuration d'adresses confirme aussi les résultats de la Figure 7. Ceci est notamment visible quand le SMR est proche de 1 (haute mobilité) où nous observons que le délai de configuration d'adresses est plus court pour DMM que MIPv6 et

PMIPv6. Les deux résultats montrent donc un protocole plus efficace dans le cas de DMM pour deux métriques (charge en signalisation et délai de configuration d'adresses) dû aussi à une architecture modifiée plate.

Communications Véhicule-à-Internet avec VIN6

Les approches Future Internet telles que LISP proposent de séparer l'identifiant du localisateur dans la fonction d'adressage. Nous proposons ici l'utilisation d'un identifiant propre aux réseaux véhiculaires, le Vehicle Identification Number (VIN) et de le convertir en adresse IPv6. Nous proposons ensuite d'intégrer cette proposition dans l'architecture de LISP-MN en introduisant le concept d'opérateur véhiculaire.

Numéro d'Identification de Véhicules (VIN)

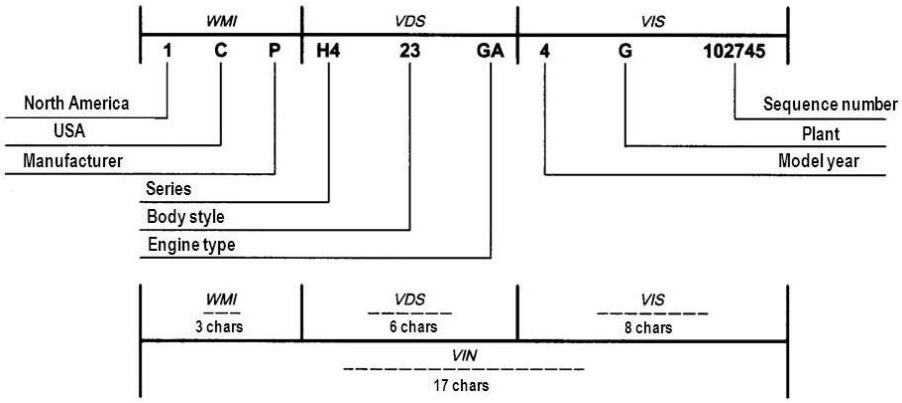

Figure9 : Illustration des sections d'un numéro d'identification de véhicules.

Le VIN est un code alphanumérique à 17 caractères découpé en 3 sections. Le WMI identifie le constructeur, le VDS donne une description de la catégorie du véhicule et le VIS donne le numéro de série du véhicule chez le constructeur et l'identifie de manière unique. Les sections WMI et VIS sont seules nécessaires afin d'identifier le véhicule de manière unique. Ces deux codes sont convertis grâce à l'algorithme illustré dans la Figure 10 en une adresse IPv6 et un préfixe unique appartenant au véhicule. Le résultat de cette conversion est utilisé par la suite afin d'adresser les appareils embarqués à l'intérieur du véhicule grâce au routeur mobile. Ce préfixe est aussi utilisé dans le réseau du constructeur automobile afin de distinguer les adresses de chaque véhicules et de les associer à leur identifiants.

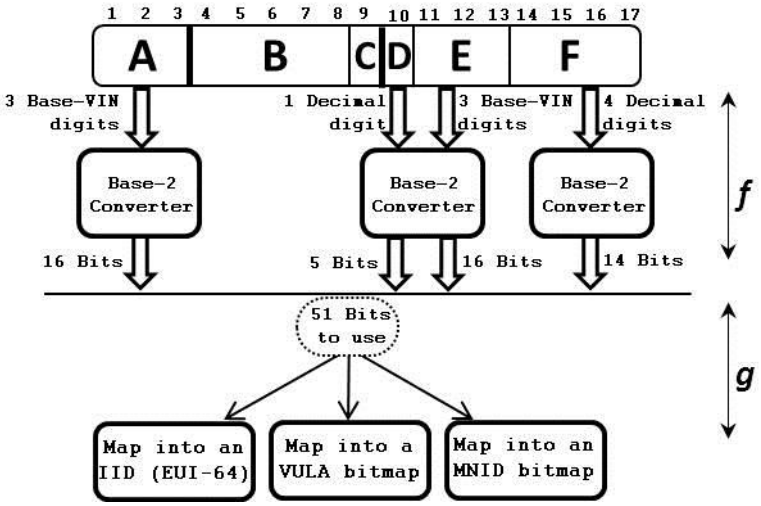

Figure10 : Algorithme de conversion du VIN en adresse et préfixe IPv6.

La Figure 11 montre l'intégration du résultat de conversion de l'algorithme à l'architecture LISP-MN. Dans cette architecture l'opérateur véhiculaire supportant des services IPv6 pour le véhicule et le connectant à l'Internet en suivant sa mobilité est responsable de l'annonce des préfixes VIN6 contenant le WMI dans les tables BGP. Ceci sert les autres opérateurs du réseau à joindre le véhicule à tout moment à travers son opérateur véhiculaire. L'opérateur véhiculaire va ensuite délivrer les paquets destinés au véhicule selon sa localisation la plus récente obtenue grâce au protocole de gestion de mobilité LISP-MN (dont le fonctionnement est proche de MIPv6).

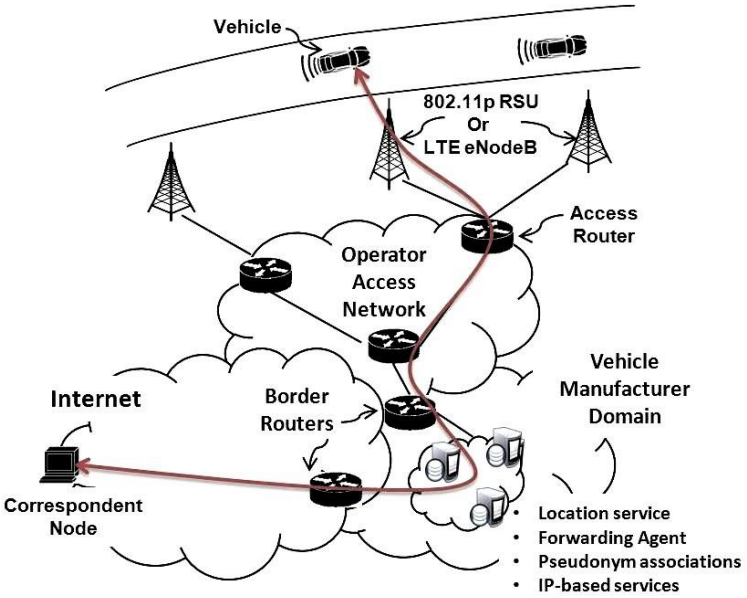

Figure11 : Architecture intégrée VIN6 et LISP-MN.

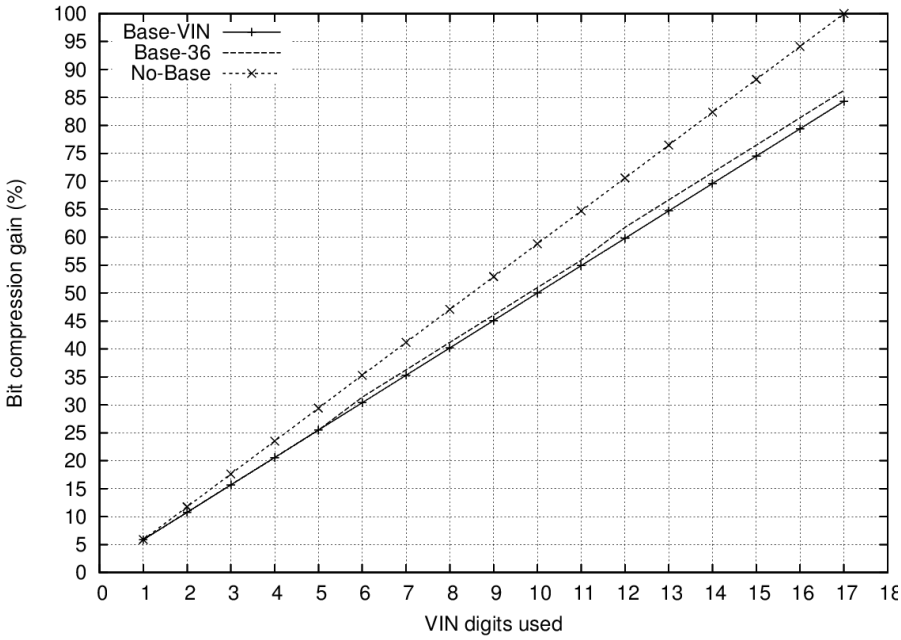

Figure12 : Taux de compression de l'algorithme de conversion VIN vers IPv6 comparé à l'état de l'art.

Dans la figure 12, nous illustrant l'efficacité de l'algorithme de conversion du VIN vers des adresses IPv6 et préfixes comparés aux approches de l'état de l'art. Notre algorithme basé sur la base numérique appelée VIN permet comme illustré sur le graphe un gain de 2% (2 bits supplémentaires) par rapport à l'approche dite BMW (Base-36) et un gain de 16% (presque 16 bits) par rapport à l'approche dite Samsung (No-Base). Notre approche est aussi la seule à garantir l'unicité et la non collision des identifiants obtenues lorsque l'on les convertit en IPv6.

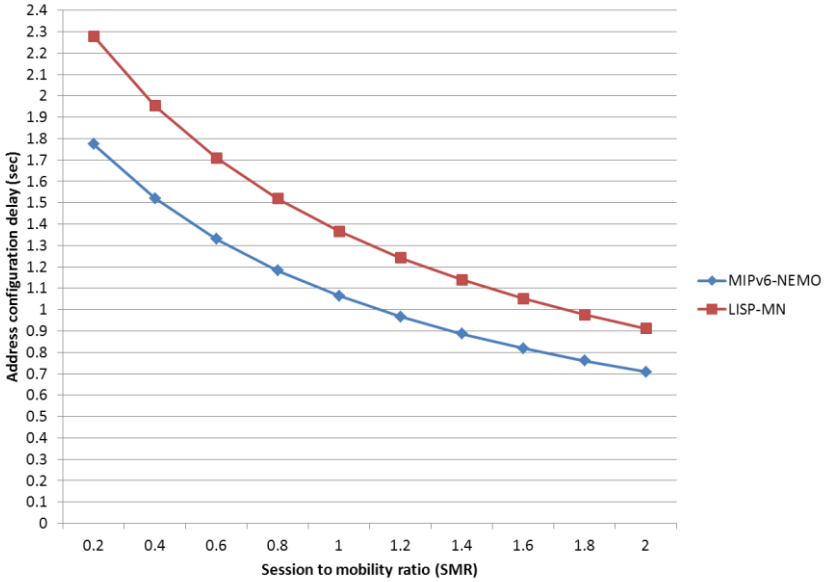

Figure13 : Délai de configuration d'adresse en utilisant MIPv6 et LISP-MN pour la gestion de mobilité.

En utilisant le modèle analytique précédant, nous avons comparé l'utilisation du protocole LIP-MN et MIPv6 pour la configuration d'adresse. Dû à une architecture comprenant un niveau supplémentaire d'indirection (le Mapping System), l'approche LISP-MN provoque un délai supplémentaire pour la configuration d'adresse. Ce délai est surtout visible pour un SMR proche de 1, i.e. une haute mobilité et un changement fréquent de point de connexion au réseau.

Conclusion

Le but de cette thèse est de faire avancer l'état de l'art des communications IP (notamment IPv6) vers des solutions prenant en charge la mobilité à grande échelle de réseaux de réseaux. Cette problématique s'intègre dans une vision de réseaux du futur, plus connus sous la terminologie "Future Internet" (F.I.). Nous avons pris l'initiative dans cette thèse de considérer le cas des communications véhiculaires à Internet, représentatif de cette problématique et non traité du point de vue des communications IPv6.

Notre première activité fût d'illustrer les besoins de tels scénarios par des cas pratiques : la e-Santé et le cas des véhicules électriques. Nous avons notamment pu observer que, certes ces cas sont différents de par leurs besoins, mais nécessitent tous deux un support de la mobilité des hôtes et un adressage IPv6 à l'intérieur du véhicule et à l'extérieur. C'est donc vers la comparaison des approches de gestion de mobilité que nous nous sommes orientés. Ces approches se distinguent de par la centralité ou la distribution du point d'ancrage ainsi que l'implication de l'hôte dans la fonction de mise à jour de localisation IPv6. Les protocoles MIPv6, PMIPv6 et N-DMM ont été considérés pour une comparaison par modèle analytique afin de juger de leur scalabilité et leurs délais d'adressage. L'approche DMM a montré notamment qu'elle était meilleure dans les deux cas.

Pour notre activité suivante nous nous sommes concentrés sur l'utilisation d'une approche de Future Internet dans notre architecture. Notre choix s'est porté sur LIP et LISP-MN pour la mobilité. Nous avons proposé notamment d'intégrer grâce à un algorithme de conversion VIN vers IPv6 préservant l'unicité, nos adresses VIN6 à l'architecture LISP et d'introduire le concept d'opérateur véhiculaire. Les performances du protocole LISP-MN comparé à MIPv6 pour le délai de configuration d'adresses montre que des améliorations peuvent être envisagées. LISP-MN est cependant mieux programmé pour le support de millions d'utilisateurs, grâce à son Mapping System (au prix d'un délai supplémentaire en configuration).

Quelques pistes supplémentaires peuvent être envisagées à la fin de cette thèse, notamment le support de la mobilité de groupe et de clusters.

Références

[1] E. Baccelli, T. Clausen, and R. Wakikawa. "IPv6 operation for WAVE; Wireless Accessin Vehicular Environments". In: IEEE Vehicular Networking Conference (VNC). 2010,pp. 160–165. doi: 10.1109/VNC.2010.5698260.

[2] Bernardos, CJ. and de la Oliva, A. and Giust, F. "An IPv6 Distributed Client Mobility Management approach using existing mechanisms (Internet Draft)". In: IETF (2014).

[3] Pravin Bhagwat, Satish Tripathi, and Charles Perkins. "Network layer mobility: an architecture and survey". In: IEEE Personal Communications 3.3 (1996), pp. 54 –64. issn: 1070-9916. doi: 10.1109/98.511765.

[4] H. Chan. "Problem statement for distributed and dynamic mobility management (Internet draft)". In: IETF (2011).

[5] J. Day. "Patterns in Network Architecture, a return to fundamentals". In: ed. by Prentice Hall. Prentice Hall, 2008. Chap. 5, "Background on Naming and Addressing", pp. 141–183.

[6] D. Farinacci et al. "RFC 6830 - Locator/ID Separation Protocol (LISP) (Internet Draft)". In: IETF (2013).

[7] Gerla, Mario and Kleinrock, Leonard. "Vehicular Networks and the Future of the Mobile Internet". In: Comput. Netw. 55.2 (Feb. 2011), pp. 457–469. issn: 1389-1286. doi: 10. 1016/j.comnet.2010.10.015. url: http://dx.doi.org/10.1016/j.comnet.2010.10.015.

[8} Giust, F. and Bernardos, C.J. and De La Oliva, A. "Analytic Evaluation and Experimental Validation of a Network-Based IPv6 Distributed Mobility Management Solution". In: IEEE Transactions on Mobile Computing 13.11 (2014), pp. 2484–2497. issn: 1536-1233. doi: 10.1109/TMC.2014.2307304.