Contrôle dynamique des communications dans un environnement v2v et v2i

Thiwiza Bellache-Sayah

université PARIS-SACLAY

NNT : 2018SACLV011

Thèse de doctorat

UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES

université PARIS-SACLAY

Contrôle dynamique des communications dans un environnement V2V et V2I

Thèse de doctorat de l'Université Paris-Saclay
préparée à l'Université de Versailles Saint-Quentin-EN-Yvelines

École doctorale n°580
Sciences et Technologies de l'Information et de la communication (STIC)
Spécialité de Doctorat : Informatique

Thèse présentée et soutenue à INRIA-Paris, le 08 Février 2018, par

Mme. Thiwiza BELLACHE-SAYAH

Composition du Jury :

ANDRE-LUC BEYLOT Professeur, ENSEEIHT à Toulouse	Président
JALEL BEN OTHMAN Professeur, Université Paris 13	Rapporteur
RAMI LANGAR Professeur, Université Paris-Est Marne la vallée	Rapporteur
PAUL MULHLETHALER Directeur de Recherche, INRIA Rocquencourt	Examinateur
SONDES KALLEL Maître de conférences, Université de Versailles (UVSQ)	Co-Directeur de thèse
OYUNCHIMEG SHAGDAR Docteur, VeDeCOM	Co-Directeur de thèse
SAMIR TOHME Professeur, UVSQ & VeDeCOM	Directeur de thèse
CHRISTINE TISSOT Chef de projet, RENAULT- France	Invité

Université Paris-Saclay
Espace Technologique / Immeuble Discovery
Route de l'Orme aux Merisiers RD 128 / 91190 Saint-Aubin, France

université PARIS-SACLAY
ÉCOLE DOCTORALE
Sciences et technologies de l'information et de la communication (STIC)

Titre : Contrôle dynamique des communications dans un environnement V2V et V2I.

Mots clés: ITS, IEEE 802.11p, GeoNetworking, Congestion du canal, DCC, Mobile IP.

Résumé : Les systèmes de transport intelligents coopératifs permettent la communication des véhicules entre eux ainsi qu'avec l'infrastructure, afin d'assurer la disponibilité des informations d'une manière plus fiable sur les véhicules, leurs positions et les conditions de la route. Cet échange d'informations pertinentes permet d'améliorer la sécurité routière, réduire les incidents du trafic et d'assurer l'efficacité de la mobilité des véhicules. IEEE 802.11p est standardisé comme la technologie par défaut pour les communications des véhicules. Dans ce contexte, le standard européen ETSI s'attaque en particulier aux applications de la sécurité routière. Pour ce faire, il standardise plusieurs types de messages comme CAM (Cooperative Awareness Message) et DENM (Decentralised Event Notification Message). Les CAMs sont des messages de diffusion à un seul-saut, envoyés par chaque véhicule contenant des informations sur sa position, sa vitesse, sa direction, etc., afin d'assurer une coopération lucide entre les autres usagers de la route (y compris les véhicules). Les DENMs sont envoyés à la détection d'un événement sur la route, comme le cas d'un accident, embouteillages, etc. Si nécessaire, une communication multi-saut, exploitant des algorithmes de routage standardisés, est mise en œuvre pour disséminer ces messages au-delà de la portée du transmetteur. La faiblesse de 802.11p réside dans la congestion du canal radio due à la bande passante limitée (5.9 GHz). Afin de pallier à cela, ETSI a proposé un cadre pour le contrôle de la congestion appelé DCC (Distributed Congestion Control). Celui-ci permet l'échange d'informations, en particulier l'état du canal radio, entre les couches de la pile protocolaire. Ainsi, chaque protocole de communication contrôle ses propres paramètres pour éviter la congestion du canal. Par ailleurs beaucoup d'approches de contrôle de la congestion DCC existent pour les messages CAM tel que le contrôle de la période de génération des CAMs sur la couche Facilities. Le contrôle de la puissance de transmission ou le débit sur la couche Accès, etc. En revanche, peu de travaux ont été faits sur DENMs. A cet égard, nous avons proposé une approche DCC sur la couche GeoNetworking qui contrôle les paramètres de routage en se basant sur l'état du canal radio. Une évaluation du dual-DCC, à savoir CAM sur Facilities et DENM sur GeoNet, a démontré l'efficacité de l'approche proposée. En outre, certaines applications tel que la gestion d'une flotte de véhicules, ont besoin d'un centre de contrôle localisé sur Internet qui communique avec la flotte. Pour ce type d'échange, une communication hybride (IP et Géo) est nécessaire. De plus pour assurer la fluidité de la communication, la gestion de la mobilité est primordiale. Tout en restant dans le cadre de l'architecture Mobile IP, nous proposons une approche qui constitue une adresse IP routable avec une adresse de géographique, permettant à une entité fixe de communiquer avec des véhicules circulant dans une zone géographique particulière. Contrairement à Mobile IP, notre approche permet de réduire la surcharge de la signalisation, grâce au partitionnement de la route en zones de routage (RA) de telle sorte que l'accès à Internet se fait via une passerelle RSU-FA qui contrôle la RA. Chaque RA regroupe un certain nombre de RSUs.

Title: Dynamic control of communications in a V2V and V2I environment.

Keywords: ITS, IEEE 802.11p, GeoNetworking, Channel Congestion, DCC, Mobile IP.

Abstract: Cooperative intelligent transport systems allow vehicles to communicate with each other as well as with the infrastructure in order to ensure the availability of information in a more reliable way about vehicles, their positions and the road conditions. This exchange of relevant information improves road safety, reduces traffic incidents and ensures efficient mobility of vehicles. IEEE 802.11p is standardized as the default technology for vehicle communications. In this context, the European ETSI standard addresses in particular road safety applications. To do this, it standardizes several types of messages such as CAM (Cooperative Awareness Message) and DENM (Decentralized Event Notification Message). CAMs are single-hop broadcast messages, sent by each vehicle containing information on its position, speed, direction, etc., to improve awareness of vehicles about other vehicles in their surroundings. The DENMs are sent when there is a detection of an event on the road, as in the case of an accident, traffic jams, etc. If necessary, multi-hop communication, using standardized routing algorithms, is implemented to disseminate these messages beyond the scope of the transmitter. The weakness of 802.11p lies in congestion of the radio channel due to the limited bandwidth (5.9 GHz). In order to compensate for this, ETSI proposed a framework for congestion control called DCC (Distributed Congestion Control). This allows the exchange of information, in particular the state of the radio channel, between the layers of the protocol stack. Thus, each communication protocol controls its own parameters to avoid congestion of the channel. In addition, many DCC congestion control approaches exist for CAM messages such as the control of the CAM generation period on the Facilities layer. The control of the transmission power or data rate on the Access layer, etc. On the other hand, little works have been done on DENMs. In this regard, we proposed a DCC approach on the GeoNetworking layer which controls the routing parameters based on the state of the radio channel. An evaluation of the dual-DCC, namely CAM on Facilities and DENM on GeoNet, demonstrated the effectiveness of the proposed approach.
In addition, some applications such as managing a fleet of vehicles require a localized control center that communicates with the fleet. For this type of exchange, a hybrid communication (IP and Geo) is necessary. Moreover, to ensure the fluidity of data transmission, mobility management is paramount. While remaining the framework of the Mobile IP architecture, we propose an approach that constitutes a routable IP address with a geonetworking address, enabling a fixed entity to communicate with vehicles driving in a particular geographic area. Compared to Mobile IP, our approach reduces the signaling overhead, by partitioning the road into routing area (RA) in such a way that the access to the Internet is via a RSU-FA (Road Side Unit) gateway that controls the RA. Each RA regroups a number of RSUs.

Université Paris-Saclay
Espace Technologique / Immeuble Discovery
Route de l'Orme aux Merisiers RD 128 / 91190 Saint-Aubin, France

Remerciements

Je souhaite remercier en premier lieu mon directeur de thèse, M. SAMIR TOHME, je lui suis également reconnaissante pour le temps conséquent qu'il m'a accordé, ses qualités pédagogiques et scientifiques, sa franchise et sa sympathie. J'ai beaucoup appris à ses côtés et je lui adresse ma gratitude pour tout cela.

Je tiens à adresser ma profonde gratitude à mes encadrantes : Mme. OYUNCHIMEG SHAGDAR et Mme. SONDES KALLEL qui ont dirigé mes travaux. Merci pour tout le temps consacré, les conseils et le soutien que vous m'avez apporté tout au long de ma thèse.

Je voudrais remercier les rapporteurs de cette thèse M. JALEL BEN OTHMAN, Professeur à l'université Paris 13 et M. RAMI LANGAR, Professeur à l'université Paris-Est Marne la vallée, pour l'intérêt qu'ils ont porté à mon travail.

Je remercie également M.PAUL MULHLETHALER, Directeur de Recherche à l'INRIA Rocquencourt et Mme. CHRISTINE TISSOT, Chef de projet, RENAULT, d'avoir accepté de faire partie de mon jury de thèse et M. ANDRE-LUC BEYLOT, Professeur à l'université de Toulouse, d'avoir accepté la présidence de mon jury de thèse.

Un grand merci à tous les membres du laboratoire LI-PARAD de l'université de Versailles, en particulier Farah, Hanane, Meriem, Asma, ainsi que mes collègues à l'institut VEDECOM en particulier Pierre et Ahmed. J'ai eu vraiment beaucoup de plaisir à y côtoyer les gens et à travailler avec eux. Les échanges ont toujours été source d'enrichissement et dans un respect mutuel.

Enfin, un immense merci à mes chers parents, à mon mari Omar et mes frères (Cherif & Lyes) et sœurs (Fatima & Yasmine), pour leur soutien, leur confiance en moi et leurs encouragements sans faille.

Résumé

Les systèmes de transport intelligents coopératifs permettent la communication des véhicules entre eux ainsi qu'avec l'infrastructure, afin d'assurer la disponibilité des informations d'une manière plus fiable sur les véhicules, leurs positions et les conditions de la route. Cet échange d'informations pertinentes permet d'améliorer la sécurité routière, réduire les incidents du trafic et d'assurer l'efficacité de la mobilité des véhicules. IEEE 802.11p est standardisé comme la technologie par défaut pour les communications des véhicules. Dans ce contexte, le standard européen ETSI s'attaque en particulier aux applications de la sécurité routière. Pour ce faire, il standardise plusieurs types de messages comme CAM (Cooperative Awareness Message) et DENM (Decentralised Event Notification Message). Les CAMs sont des messages de diffusion à un seul-saut, envoyés par chaque véhicule contenant des informations sur sa position, sa vitesse, sa direction, etc., afin d'assurer une coopération lucide entre les autres usagers de la route (y compris les véhicules). Les DENMs sont envoyés à la détection d'un événement sur la route, comme le cas d'un accident, embouteillages, etc. Si nécessaire, une communication multi-saut, exploitant des algorithmes de routage standardisés, est mise en œuvre pour disséminer ces messages au-delà de la portée du transmetteur.

La faiblesse de 802.11p réside dans la congestion du canal radio due à la bande passante limitée (5.9 GHz). Afin de pallier à cela, ETSI a proposé un cadre pour le contrôle de la congestion appelé DCC (Distributed Congestion Control). Celui-ci permet l'échange d'informations, en particulier l'état du canal radio, entre les couches de la pile protocolaire. Ainsi, chaque protocole de communication contrôle ses propres paramètres pour éviter la congestion du canal. Par ailleurs beaucoup d'approches de contrôle de la congestion DCC existent pour les messages CAM tel que le contrôle de la période de génération des CAMs sur la couche Facilities. Le contrôle de la puissance de transmission ou le débit sur la couche Accès, etc. En revanche, peu de travaux ont été faits sur DENMs. A cet égard, nous avons proposé une approche DCC sur la couche GeoNetworking qui contrôle les paramètres de routage en se basant sur l'état du canal radio. Une évaluation du dual-DCC, à savoir CAM sur Facilities et DENM sur GeoNet, a démontré l'efficacité de l'approche proposée.

En outre, certaines applications tel que la gestion d'une flotte de véhicules, ont besoin d'un centre de contrôle localisé sur Internet qui communique avec la flotte. Pour ce type d'échange, une communication hybride (IP et Géo) est nécessaire. De plus pour assurer la fluidité de la communication, la gestion de la mobilité est primordiale. Tout en restant dans le cadre de l'architecture Mobile IP, nous proposons une approche qui constitue une adresse IP routable avec une adresse de géographique, permettant à une entité fixe de communiquer avec des véhicules circulant dans une zone géographique particulière. Contrairement à Mobile IP, notre approche permet de réduire la surcharge de la signalisation, grâce au partitionnement de la route en zones de routage (RA) de telle sorte que l'accès à Internet se fait via une passerelle RSU-FA qui contrôle la RA. Chaque RA regroupe un certain nombre de RSUs.

Mots-clés : ITS, IEEE 802.11p, GeoNetworking,Congestion du canal, DCC, Mobile IP, Simulation, Modélisation.

Abstract

Cooperative intelligent transport systems allow vehicles to communicate with each other as well as with the infrastructure in order to ensure the availability of information in a more reliable way about vehicles, their positions and the road conditions. This exchange of relevant information improves road safety, reduces traffic incidents and ensures efficient mobility of vehicles. IEEE 802.11p is standardized as the default technology for vehicle communications. In this context, the European ETSI standard addresses in particular road safety applications. To do this, it standardizes several types of messages such as CAM (Cooperative Awareness Message) and DENM (Decentralized Event Notification Message). CAMs are single-hop broadcast messages, sent by each vehicle containing information on its position, speed, direction, etc., to improve awareness of vehicles about other vehicles in their surroundings. The DENMs are sent when there is a detection of an event on the road, as in the case of an accident, traffic jams, etc. If necessary, multi-hop communication, using standardized routing algorithms, is implemented to disseminate these messages beyond the scope of the transmitter.

The weakness of 802.11p lies in congestion of the radio channel due to the limited bandwidth (5.9 GHz). In order to compensate for this, ETSI proposed a framework for congestion control called DCC (Distributed Congestion Control). This allows the exchange of information, in particular the state of the radio channel, between the layers of the protocol stack. Thus, each communication protocol controls its own parameters to avoid congestion of the channel. In addition, many DCC congestion control approaches exist for CAM messages such as the control of the CAM generation period on the Facilities layer. The control of the transmission power or data rate on the Access layer, etc. On the other hand, little works have been done on DENMs. In this regard, we proposed a DCC approach on the GeoNetworking layer which controls the routing parameters based on the state of the radio channel. An evaluation of the dual-DCC, namely CAM on Facilities and DENM on GeoNet, demonstrated the effectiveness of the proposed approach.

In addition, some applications such as managing a fleet of vehicles require a localized control center that communicates with the fleet. For this type of exchange, a hybrid communication (IP and Geo) is necessary. Moreover, to ensure the fluidity of data transmission, mobility management is paramount. While remaining the framework of the Mobile IP architecture, we propose an approach that constitutes a routable IP address with a geonetworking address, enabling a fixed entity to communicate with vehicles driving in a particular geographic area. Compared to Mobile IP, our approach reduces the signaling overhead, by partitioning the road into routing area (RA) in such a way that the access to the Internet is via a RSU-FA (Road Side Unit) gateway that controls the RA. Each RA regroups a number of RSUs.

Keywords: ITS, IEEE 802.11p, GeoNetworking, Channel Congestion, DCC, Mobile IP, Simulation, Modeling.

Table des matières

Liste des tableaux

Table des figures

Abréviations

AoRA : Address Of Routing Area.
CoA : Care Of Address.
C2V : Center To Vehicle.
C-V2V : Cellular vehicle to vehicle.
CBR : Channel Busy Ratio.
CCH : Control Channel.
CBF : Contention Based Forwarding.
CBF-RT : Contention Based Forwarding with Retransmission Threshold.
CBF2Cv1 : Contention Based Forwarding with Congestion Control version 1.
CBF2Cv2 : Contention Based Forwarding with Congestion Control version 2.
CAM : Cooperative Awareness Message.
CN : Corresponding Node.
DCC : Decentralized Congestion Control.
DENM : Decentralised Event Notification Message.
DSRC : Dedicated Short Range Communication.
E2ED : End To End Delay.
ETSI : European Telecommunications Standards Institute.
FA : Foreign Agent.
GF : Greedy Forwarding.
IP : Internet Protocol.
IPv6 : Internet Protocol version 6.
ITS : Intelligent Transportation Systems.
ITS-S : ITS station.
HA : Home Agent.
HoA : HOme Address.
MAC : Media Access Control.
MANET : Mobile Adhoc Networks.
MIPv6 : Mobile IP version6.
MN : Mobile Node.
MAG : Mobile Access Gateway.
MN : Mobile node (vehicle).
PDR : Packet Delivery Ratio.
PMIPv6 : Proxy Mobile IP version 6.
PMIPv6 : Proxy Mobile IP version 6.
LMA : Local Mobility Anchor.
LLC : Logical Link Control.
RC : Retransmission Count.
RC_{Th} : Retransmission Count Threshold.
RSU : Road Side Unit (En Anglais).
RSU-FA : Road Side Unit- Foreign Agent (Passerelle).

RA : Routing Area.
SCH : Service Channel.
UBR : Unité bord de route (En Français).
VANET : Vehicular Adhoc Networks.
V2V : Vehicle To Vehicle.
V2I : Vehicle To Infrastructure.
V2X : Vehicle To vehicle / Infrastructure / Central System .
V2C : Vehicle To Central System.
WT : Wait Time (timer, temporisateur ou compte à rebout).
WAVE : Wireless Access in Vehicular Environment.

Chapitre 1

Introduction Générale

1.1 Introduction Générale

1.1.1 Contexte et problématique

Les VANETs (Vehicular Ad-hoc NETwork) comprennent les véhicules équipés d'un dispositif sans fil pour communiquer avec d'autres. Chaque véhicule a une portée de transmission limitée à quelques centaines de mètres et assure une communication multi-sauts dans le cas d'une diffusion sur une grande distance. Ce dispositif permet aussi une communication entre le véhicule et les équipements de la route (ex. RSU). Les réseaux VANETs constituent une classe spéciale des réseaux MANETs (Mobile ad-hoc Network) et ils sont caractérisés par le changement fréquent de la topologie en raison de la forte mobilité des véhicules. Tous les véhicules partagent le même canal menant à la congestion du canal dans des réseaux très denses. L'architecture décentralisée de ces réseaux exige de nouveaux protocoles de diffusion des messages. De plus, la déconnexion fréquente des liens de communication et le changement rapide des véhicules voisins demandent de nouvelles approches pour assurer une communication fiable.

Le standard IEEE (Institute of Electrical and Electronics Engineers) normalise la technologie 802.11p pour les communications entre véhicules ou entre véhicules et infrastructure (V2X). En Europe, cinq canaux de 10 MHz sont attribués dont la bande de fréquences est de 5.9 GHz pour les communications véhiculaires basées sur IEEE 802.11p[37]. L'un des cinq canaux est défini comme canal de contrôle (CCH) dédié aux applications de la sécurité et de la gestion du trafic routier (road safety and efficiency).

Par ailleurs le standard ETSI (European Telecommunications Standardization Institute) a spécifié plusieurs ensembles de messages pour les applications de sécurité routière, notamment le message de sensibilisation coopérative (CAM) et le message décentralisé de notification d'événement (DENM) [40]. Les CAM sont des messages de diffusion (broadcast) à un seul saut, envoyés par chaque véhicule contenant des informations sur la position du véhicule, sa vitesse, sa direction etc., afin que les autres utilisateurs de la route (y compris les véhicules) puissent être au courant de la présence du véhicule. Les DENM sont, d'autre part, envoyés lors

de la détection d'événements, tels que des accidents, et peuvent être transmis sur plusieurs sauts si nécessaire. En effet, un certain nombre d'applications de DENM, telles que les notifications lors d'un freinage d'urgence, accidents, embouteillage etc., nécessitent un transfert multi-sauts de ces messages DENM. Un certain nombre de schémas d'acheminement des paquets en multi-sauts sont proposés dans le contexte des communications véhiculaires, en particulier GeoNetworking [70, 64, 68, 48, 47, 66], et certains sont inclus dans la norme ETSI [46], à savoir la transmission basée sur la contention (CBF et CBF-RT) et des algorithmes de Greedy forwarding (GF).

Dans la première partie de cette thèse, on se concentrera davantage sur la communication entre véhicules. Particulièrement sur le transfert multi-saut des paquets DENM quand le canal radio est partagé entre les deux types de messages (CAM et DENM). Le contrôle de la congestion est primordial, d'une part en raison des ressources limitées (5.9 GHz) lors des communications V2X basées sur le 802.11p et d'autre part, la charge importante créée par chaque véhicule. Notre objectif étant de réaliser une dissémination en Geobroadcast de ces messages sur une zone géographique, tout en optimisant l'utilisation de la ressource radio (autrement dit, éviter la congestion du canal), minimisant la perte de données et la totalité du temps de parcours entre le véhicule émetteur et la destination.

Des applications V2I nécessitant un contrôle par une entité située sur Internet sont de plus en plus utiles pour les conducteurs sur la route. Néanmoins, ce schéma d'échange exige une communication hybride qui utilise des informations géographiques et IP (Internet Protocol). Un des défis est d'assurer la fluidité de la communication entre les différentes entités, plus spécifiquement, entre les véhicules roulant dans certains zones géographiques et une entité fixe sur Internet. Dans ce cas, la gestion de la mobilité est nécessaire pour ces nouveaux types d'applications. Notre deuxième contribution consiste à proposer un nouveau mécanisme d'adressage permettant à une entité dans Internet d'accéder au véhicule en mouvement sur la route, tout en restant dans le contexte de Mobile IP. En plus de cela, notre nouvelle approche (GeoMIP) s'adapte plus à la forte mobilité des véhicules qui introduit beaucoup de surcharge en termes de signalisation échangée avec Internet.

1.1.2 Contributions

1.1.2.1 Contrôle de la congestion distribué (DCC) au niveau GeoNetworking sur DENM :

En Europe, 50 MHz de bande passante sur une plage de 5.855 à 5.905 GHz [37] a été allouée pour les applications critiques de la sécurité routière (road safety) et de la gestion du trafic routier (traffic efficiency). Deux types de canaux coexistent, à savoir un canal de contrôle (CCH) et un/ou plusieurs canaux de service (SCH). Le canal de contrôle CCH est utilisé par les applications critiques de la sécurité routière. Alors que, SCH sera aussi utilisé par les applications de la sécurité routière mais aussi de la gestion de trafic routier (safety and traffic efficiency). Plusieurs types de messages partagent le CCH basé sur la technologie 802.11p, ce qui mène au problème de surcharge du canal radio (la congestion) vu que les ressources radio sont limitées dans 802.11p. Un framework DCC d'ETSI a été conçu pour faire face à ce problème de la congestion du canal radio, des algorithmes DCC ont été proposés

particulièrement au niveau de la couche Accès et Facilities.

Dans un premier temps, nous proposons une amélioration de la transmission multi-sauts basée sur la contention (CBF) par une fonctionnalité de contrôle de la congestion. Plus précisément, nous proposons un algorithme de transfert de paquets, CBF2Cv1, qui est conçu pour s'adapter au framework DCC. Afin d'utiliser efficacement le canal, l'algorithme CBF2Cv1 adapte le nombre de retransmission en fonction de l'état de la charge du canal. Des simulations étendues sur l'évaluation des performances de la communication et l'utilisation du canal sont réalisées, ciblant des scénarios lorsque le canal sans fil est partagé par les messages DENMs et CAMs simultanément. Les performances de CBF2Cv1 sont comparées à celles de l'algorithme Flooding version améliorée (FloodingAdv), et d'autres schémas de transmission multi-sauts normalisés par le standard européen ETSI, à savoir CBF et CBF-RT. De plus, deux cas, avec et sans contrôle de congestion de taux de génération des CAMs, sont pris en compte dans les évaluations de performance.

Par ailleurs, la seconde contribution est une amélioration de notre premier algorithme CBF2Cv1, nommée CBF2Cv2, qui contrôle deux paramètres de transmission de l'algorithme CBF-RT, à savoir, le temps d'attente maximal (Wait-Time maximum) et le seuil de nombre de retransmission (RC_{th}), l'objectif est d'assurer un contrôle de la congestion et d'éviter les collisions, avec un court délai de transmission (E2ED) comparant à CBF2Cv1 et CBF-RT.

À l'aide du simulateur réseau NS3, les performances de CBF2Cv1, CBF2Cv2 sont comparées à celles de l'approche Flooding améliorée, CBF et de l'algorithme CBF-RT, ciblant des scénarios, où les messages DENMs et CAMs partagent le canal sans fil. Deux cas, avec et sans DCC sur le taux de génération des messages CAMs, sont pris en compte dans nos simulations. Les résultats de simulation montrent les avantages du dual contrôle de la congestion (dual-DCC).

Les protocoles de communication véhiculaire dans le contexte de réseau de véhicules (VANET) se basent sur des modèles de simulation et cela est dû à l'impossibilité d'avoir des expérimentations réelles (la difficulté et le coût).

Pour évaluer les performances de nos propositions, un développement a été fait en C++. Ceci a inclut l'implémentation de l'algorithme Flooding, CBF, CBF-RT et notre solution CBF2C et l'amélioration de Flooding dans un simulateur réseau NS3. On s'est basé sur des traces générées par le simulateur de trafic routier SUMO afin d'introduire la mobilité des véhicules dans nos simulations. Des scripts perl et Shell ont été également écrit pour les traitements des résultats de simulations avec et sans la mobilité des véhicules.

1.1.2.2 Un schéma d'adressage pour les communications Unicast (CN vers Véhicule) et géocast (serveur vers une zone géographique) :

Comme à la deuxième contribution, nous avons proposé une approche qui étend Mobile IP au réseau de véhicules pour les applications ITS qui exigent une dissémination d'informations vers une zone géographique à partir d'un serveur sur Internet.

Notre proposition GeoMIP consiste à appliquer la solution de Mobile IP (ou MIP) par zone de routage, ce qui va permettre à un nœud fixe dans Internet de communiquer avec les véhicules sur une zone géographique utilisant les réseaux IP et géographiques.

Un schéma d'adressage hybride (IP et Géographique) est proposé pour permettre aux

véhicules d'auto-configurer des adresses routables afin d'assurer une communication avec une entité sur Internet. Ainsi qu'un mécanisme qui permettra de localiser un seul ou un ensemble de véhicules à temps réel. Comme notre approche (GeoMIP) se base sur MIP, GeoMIP reste applicable pour les applications qui nécessitent une dissémination d'informations en unicast vers un véhicule à partir d'un nœud (ex. serveur) sur Internet.

Via une modélisation, nous montrons que la nouvelle approche, GeoMIP, assure de meilleures performances que Mobile IP. Une comparaison entre GeoMIP et Mobile IP est basée sur une modélisation de cellules (portées des RSUs) en files d'attente.

1.1.3 Organisation du manuscrit

Cette thèse est organisée comme suit :

Les chapitres 1 et 2 présentent un aperçu du contexte et les principaux objectifs de notre travail.

Le chapitre 3 est dédié au problème de la congestion lors des communications en Géobroadcast entre véhicules. Un état de l'art et nos contributions sur le contrôle de la congestion distribuée sur des messages de notifications DENM au niveau de la couche réseau est présenté.

Le chapitre 4 traite le problème d'accessibilité des véhicules dans VANET à partir d'une entité dans Internet. Un état de l'art sur la gestion de la mobilité dans VANET est défini. Ce chapitre présente GeoMIP, notre proposition pour une communication hybride (Géo et IP) basée sur le schéma de Mobile IP.

Le chapitre 5 conclut ce travail de thèse en résumant nos contributions et nous présentons les perspectives de notre travail.

1.1.4 Publications

Ce travail de thèse a abouti aux publications suivantes :

— Thiwiza Bellache, Oyunchimeg Shagdar and Samir Tohme, An alternative congestion control using an enhanced contention based forwarding for vehicular networks, in 13th Annual Conference on Wireless On-demand Network Systems and Services,WONS, Feb. 2017, pp. 81-87.

— Thiwiza Bellache, Oyunchimeg Shagdar, Sondes Kallel and Samir Tohme, Reducing Channel Load by Enhanced Contention based Forwarding in Vehicular Networks, in International Conference on Selected Topics in Mobile & Wireless Networking, MoWNET,May. 2017.

— Thiwiza Bellache, Oyunchimeg Shagdar and Samir Tohme, DCC-enabled Contention based Forwarding Scheme for VANETs, in 13th International Conference on Wireless and Mobile Computing, Networking and Communications, WiMob, Oct. 2017.

— Thiwiza Bellache, Sondes Kallel , Oyunchimeg Shagdar and Samir Tohme, GeoMIP : A Novel Mobility Management Solution for Internet and VANET Communication using Geographic Partition in Mobile IP, in 10th Wireless Days Conference, WD, April. 2018.

Chapitre 2

VANET (Vehicular Adhoc NETworks)

2.1 Introduction

La communication dans les applications de la sécurité routières peut se faire en utilisant plusieurs types de transmission y compris la transmission en GeoBroadcast avec ou sans un passage par l'infrastructure (RSU ou Internet). Afin d'aborder les limites et les points fort de chaque type de communications ceci s'appuie sur une étude approfondie sur ce sujet.

Dans ce qui suit, nous présentons le contexte globale de l'architecture ITS avec les différentes classes d'application dédiées à la sécurité routière. Ensuite, un aperçu de la pile protocolaire de ETSI est illustré, en particulier nous détaillons la couche réseau et transport.

2.2 L'architecture ITS

Les systèmes de communication coopératifs ITS (Intelligent Transportation Systems) permettent d'échanger des données entre véhicules ou avec l'infrastructure routière communicant(e)s, etc. Cet échange de données a pour objectif d'améliorer à la fois la sécurité routière et l'efficacité du trafic routier. Grâce à ces systèmes, un ensemble d'informations sur les véhicules ou des informations sur les conditions de la route (ex : les zones à danger etc.) devient disponible pour les utilisateurs de la route (ex : véhicules) et les gestionnaires de la route etc. Les standards dits ITS-coopératifs reposent tout d'abord sur une architecture de référence connue sous le nom de ITS-station. Ceci est indispensable pour garantir l'interopérabilité des systèmes déployés dans les véhicules, l'infrastructure routière, etc.

Les systèmes de transport intelligents (ITS) offrent un ensemble de standards pour les communications entre les véhicules. Les activités de recherche, au sein d'ITS ciblent principalement le développement de la sécurité, l'efficacité du trafic et l'info-divertissement liés aux applications. Les communications V2V et V2I sont les principaux objectifs de la recherche d'ITS. Parmi ces architectures y a deux les plus populaires qui sont IEEE/WAVE (Wireless Access in Vehicular Environment) [53], [19], [55], [54], [56], [52] et ETSI (European Telecommunications Standards Institute).

Dans notre étude, nous se basons sur l'architecture ETSI, le standard européen ne se limite pas aux communications V2V à un seul-saut, il prend en charge la communication multi-sauts à travers GeoNetworking (GeoNet), au niveau de la couche réseau & transport.

2.3 Les types de communications dans VANETs

L'environnement ITS comprend des stations ITS (ITS-S) qui peuvent communiquer directement comme suit : V2V (Véhicule à Véhicule), V2C (Véhicule à un système Central). Ces applications sont principalement axées sur plusieurs types de communications dans une bande de fréquence dédiée aux communications V2X. En outre, l'infrastructure ITS est accessible via une station ITS fixe au bord de la route.

2.3.1 Les communications (véhicule à véhicule - V2V)

La communication véhicule à véhicule s'appuie sur un réseau entièrement distribué et il n'exige pas de coordination avec l'infrastructure. Les véhicules forment un réseau ad hoc où chaque véhicule s'auto-configure automatiquement et communique avec leurs véhicules voisins lorsqu'une liaison sans fil existe. Cette architecture distribuée porte sur des communications à courte portée et peut atteindre une latence faible. Les performances se dégradent dans un réseau dense (un grand nombre de véhicules ou fréquence de transmission élevée) en surchargeant le réseau. La communication V2V est avantageuse lors d'un échange d'informations d'intérêt local (comme illustré sur la figure 2.1, à temps réel et sur une petite zone géographique [67].

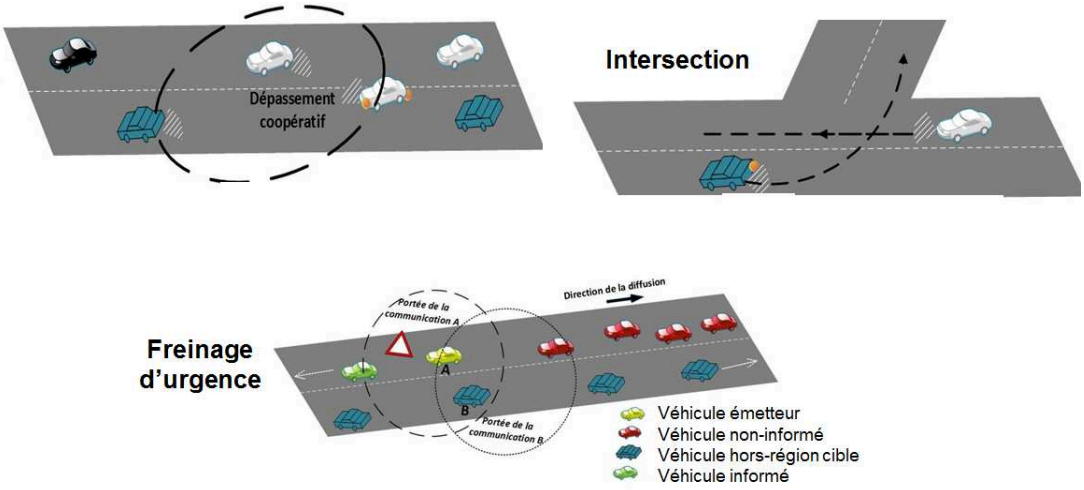

FIGURE 2.1 – Exemple d'applications en V2V

2.3.2 Les communications (Véhicule à un système central - V2C)

La communication de type véhicule à un serveur central comme illustrée sur la figure 2.2, peut être réaliser en passant par des réseaux cellulaires, des communications de type véhicule à Infrastructure (V2I) ou des communications de type Infrastructure à un serveur central (I2C).

Sachant qu'une communication de type V2I est simplement un échange entre une station ITS et les feux au bord de la route. La communications V2C s'appuie sur des points d'infrastructure (ex : Unité bord de route ou un serveur central), afin d'accéder par exemple à Internet pour faire un diagnostic, etc. La latence dans une architecture centralisée dépend du réseau d'accès (ex. structure hiérarchique) qui peut atteindre plusieurs centaines de millisecondes (100 ms). Par contre, dans des zones larges les performances sont meilleures grâce aux grandes portées de communications. La communication reste réalisable même dans un réseau dense. Cette architecture assure de meilleurs résultats lors d'un échange d'informations sans exigences strictes en termes de délai du bout en bout, sur une zone géographique large.

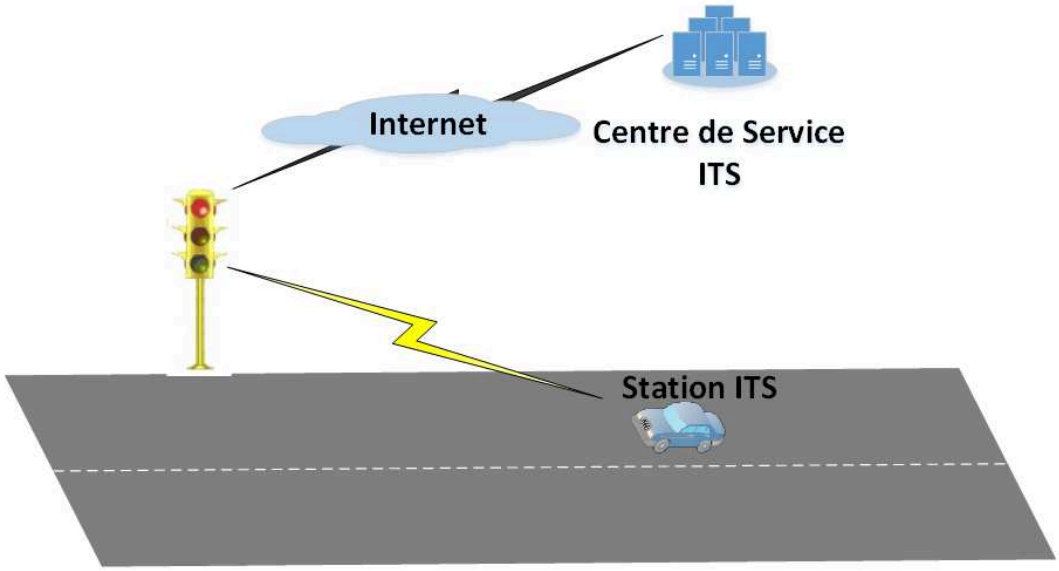

FIGURE 2.2 – Exemple d'application en V2C réalisé par V2I et I2C

La combinaison des différentes architectures de communications, permet d'obtenir des communications hybrides très intéressantes.

2.4 L'architecture de référence ETSI

ETSI est l'organisme de normalisation pour ICT (Information Communication Technologies) en Europe. La grande nouveauté de cette architecture est qu'elle introduit une nouvelle couche appelée la couche facilities et deux autres couches horizontales management et sécurité. L'architecture ITS se compose de six éléments principaux. Dans le plan de données (au milieu de la figure 2.3), l'architecture de la station ITS dispose de quatre couches qui exécutent des tâches différentes. Du bas vers le haut (Figure 2.3) les couches, Access, Réseau&Transport, Facilities et Application sont empilées. Les couches adjacentes sont connectées via SAP (Service Access Point). Les entités management et sécurité sont connectées à toutes les couches via SAPs. La séparation en couche dans ETSI, permet d'assurer une certaine portabilité sur des plateformes matérielles et logicielles différentes, mais surtout de changer des technologies dans les couches basses indépendamment des couches supérieures.

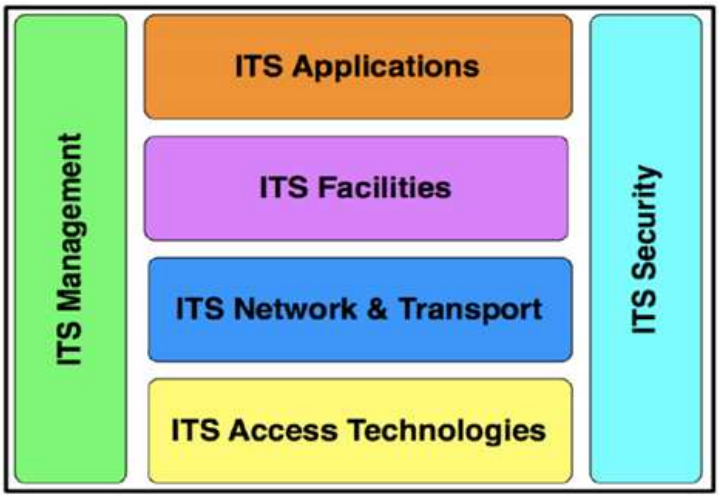

FIGURE 2.3 – La pile protocolaire ITS d'ETSI (ETSI EN 302 636-3)

La couche Access permet une communication transparente sur plusieurs technologies d'accès radio coexistant. L'architecture intègre donc des mécanismes pour sélectionner dynamiquement l'interface (sans fil ou filaire) la plus appropriée. Celles déjà supportées aujourd'hui, sont le WiFi véhiculaire (ex. IEEE 802.11p), le cellulaire (2G, 3G, 4G) etc.

Dans cette thèse, nous étudions la norme 802.11p pour les applications de sécurité dans VANET. Afin de communiquer en utilisant VANETs, IEEE a travaillé sur IEEE802.11p (WAVE Wireless Access in Vehicular Environments) et le standard des protocoles 802.11 pour DSRC (Dedicated Short Range Communication). Le DSRC a été conçu à l'aide d'un système multi-canal. (Figure 2.4)

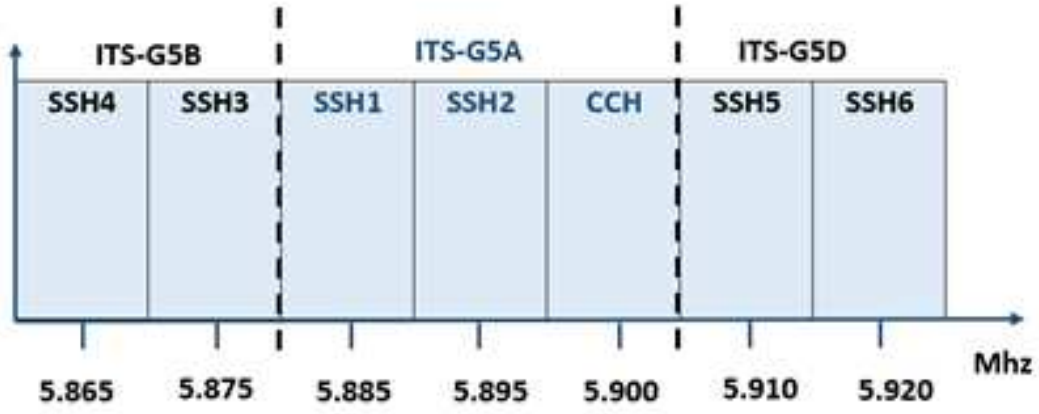

FIGURE 2.4 – Allocation des fréquences en Europe pour les applications de sécurité et la gestion de trafic routier [20]

Le spectre est divisé en sept canaux, chacun est de 10-20 Mhz. Dans le quel six ont été identifiés comme canal de service(SCH) et un en tant que canal de control (CCH). La figure

ci-dessous montre l'attribution des canaux pour DSRC sur la bande de fréquence allouée pour les ITS coopératifs. Pour rappel, les messages CAM et les DENMs doivent être transmis dans un canal ITS-G5A [44] réservé aux applications de la sécurité routière.

La couche réseau et transport (ITS Networking & Transport layer) contient les différents blocs de protocoles réseau et de transport nécessaires pour assurer des communications locales dédiées aux échanges directs V2V ou V2I (ex. ETSI GeoNetworking), et des communications distantes vers une entité plus éloignée (ex. IPv6). Le protocole IPv6 est spécifié dans [22], Le protocole GeoNetworking est spécifié dans le standard [46].

Geonetworking permet une communication multi-saut dans un réseau véhiculaire ad-hoc (VANET). C'est un bloc de protocole de la couche Réseau & Transport, basé sur des communications véhicule à véhicule (V2V) et des communications véhicule à infrastructure (V2I) afin de répondre aux exigences des applications ITS de la sécurité routière. Un message lié à la sécurité exige une communication sûre, fiable et d'une faible latence. Le routage d'informations se base sur la position géographique de la station ITS ou une UBR (Unité Bord de Route) et supporte des communications multi-saut. Les paquets peuvent être communiqués vers des zones géographiques spécifiques.

La couche Facilities (services) est un composant qui fournit des fonctions, des informations ou des services aux applications ITS. Elle échange des données avec les couches inférieures et avec la couche Management et la couche sécurité. La couche facilities peut être classée en deux catégories selon [45] :

1. Facilities Communes (Common facilities) : fournir des services de base pour assurer un fonctionnement fiable d'une station ITS et l'interopérabilité des applications. Un des exemples de Facilities Communes est le service de positionnement.
2. Facilities Domaine (Domain facilities) : fournit des services et des fonctions pour une ou plusieurs applications spécifiques telles que le service de base DEN (Decentralized Environmental Notification basic service) pour les applications d'avertissement coopératif de danger routier. Facilities domaine est commun pour une ou plusieurs applications. Il peut devenir facultatif ou ne pas être utilisé pour d'autres applications.

Des applications telles que l'alerte d'accident (accident warning), alerte de freinage d'urgence, alerte dépassement d'un véhicule, alerte changement de sens de la conduite doivent générer des messages déclenchés par un événement particulier (ex., accident). Une fois déclenché par cet événement, l'application continue souvent à générer des messages de façon périodique jusqu'à ce que l'événement se termine. ETSI défini des messages de notification (DENM) pour supporter de telles applications. À la demande d'une application, DENM est généré au niveau de la couche facilities. La diffusion de message DENM persiste tant que l'événement est présent. DENM peut être disséminé en multi-saut pour communiquer l'information à une zone plus large.

La couche verticale management permet l'échange d'informations en cross-layer entre les couches horizontales. La gestion des fonctionnalités internes de la station ITS comprennent la sélection dynamique des technologies d'accès disponibles, la gestion de la capacité, des autorisations et des priorités de transmission, des mécanismes du contrôle de congestion, etc.

La couche Application, contient toutes les applications. Ces applications doivent faire connaître leurs besoins de communication en fournissant à l'entité de gestion les exigences

de chacun information transmise par l'application.

Finalement, **la couche sécurité** est un bloc qui implémente les services de sécurité pour la communication de la pile protocolaire et l'entité management afin d'assurer la sécurisation des communications (authentification, chiffrements etc.).

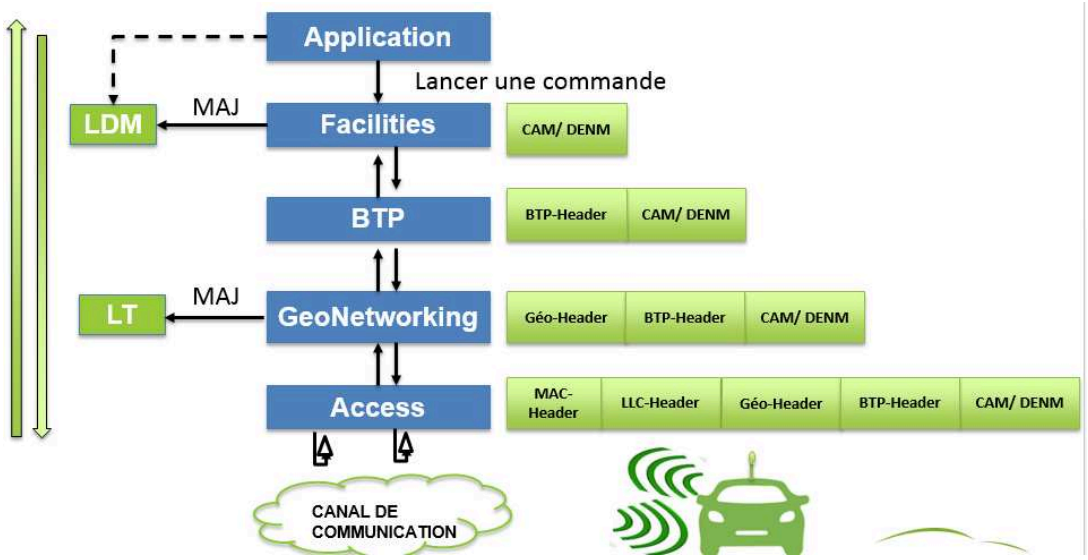

FIGURE 2.5 – Communication à travers la pile ETSI

D'une manière générale, la communication à travers la pile protocolaire est présentée sur la figure 2.5. Lors de la détection d'un événement sur la route, la couche Application décide d'envoyer une demande de génération d'un message DENM, entre temps des informations sont fournies à la couche Facilities. Cette dernière envoie une demande à la couche Réseau&Transport concernant le mode de transmission du message DENM ensuite la couche Facilities envoie les exigences de l'application et le message DENM à la couche Réseau&Transport. Ainsi donc, les couches basses procèdent au traitement de message DENM à sa réception et construit le paquet à transmettre en broadcast. Le LDM est basé sur une carte dynamique pour maintenir la topologie du réseau dynamique de la zone autour d'une station. Le LDM [39] (Local dynamic map) est mis à jour à la réception de ces messages DENM et CAM, etc. La table de localisation (LT) est mise à jour au niveau de la couche réseau. Le paquet envoyé est composé de plusieurs champs (données et en-têtes ajoutés à chaque niveau de la pile). Cette procédure se fait de la même manière lors d'une émission.

Notre contribution est au niveau de la couche Réseau&Transport de la pile protocolaire ITS d'ETSI. Mais avant, il est nécessaire de comprendre l'architecture du réseau ITS. Plus précisément, nous spécifions l'architecture du réseau pour les communications dans les systèmes de transport Intelligent coopératifs (ITS-C). Sachant que cette architecture n'est pas limitée à une communication entre véhicules. Cette dernière assure une large gamme d'applications ITS pour la sécurité routière, la gestion du trafic routier (traffic efficiency) ainsi que pour Informations et divertissement (infotainment). Ensuite, un aperçu de l'architecture protocolaire est décrit avec les différentes options d'usage du protocole GeoNetworking en combinaison avec les protocoles transport et les protocoles IP.

2.5 Les classes d'applications ITS

L'efficacité de la sécurité et de trafic sont les aspects les plus importants d'ITS. Ces applications sont organisées en trois catégories. La première comprend les applications de la sécurité (Safety), la deuxième est celle de l'efficacité de trafic (Traffic efficiency) et la troisième est les applications divertissement (Infotainment). Le tableau 2.1 illustre les caractéristiques de ces trois catégories d'applications, en termes de latence, portée de transmission, etc [75].

TABLE 2.1 – Les catégories d'applications C-ITS [75]

Catégorie d'application	Latence	Portée	Exigence en termes de délai (cas d'usage)
Sécurité routière (Road safety)	faible	locale	Pre-crash sensing (50 ms) ou Collision risk warning (100 ms)
Efficacité de trafic routier (Traffic efficiency)	moyenne	moyenne	Traffic information (500 ms)
Divertissement (Infotainment)	faible	moyenne	Map download update/Point of interest notification (500 ms)

Sécurité routière (Safety) : Les applications de sécurité sont essentiellement impliquées dans les avantages de la sécurité d'un véhicule sur une route. Dans le cas d'alerte d'un accident ou un évènement dangereux sur une route, ceux-ci sont pris en considération par les applications liées à la sécurité afin d'éviter la collision entre les véhicules.

Efficacité de trafic routier (Traffic Efficiency) : elles sont essentiellement utilisées pour améliorer l'efficacité du transport, en fournissant des informations relatives au trafic d'un ou plusieurs véhicules. Un exemple de ces applications est l'avertissement des conditions de trafic routier (Avertissement de condition de la circulation).

Divertissement (Infotainment) sont utilisées pour offrir aux conducteurs le confort. Ces applications sont généralement considérées comme des applications non-safety. L'exemple de ce type d'application est d'informer de la présence d'un service locale ou des points d'intérêt (ex : restaurant) à la proximité, en fournissant des informations telles que les heures d'ouverture, les prix, le temps d'attente, la salle disponible, les promotions, etc.

De plus en plus, les véhicules deviennent plus sûrs, et plus intelligents. Divers capteurs et systèmes d'assistance à la conduite permettent aux véhicules de surveiller leur environnement. Par des moyens d'échange d'informations entre les véhicules, ainsi que entre les véhicules et l'infrastructure, les véhicules se transforment d'un système autonome aux systèmes coopératifs. La communication entre véhicule est fondamentale pour ITS (ou C-ITS).

Dans cette thèse, nous nous intéressons plus particulièrement aux applications de la sécurité routières pour la transmission multi-saut. Ces dernières utilisent des messages de notification décentralisé (DENM) pour informer les conducteurs d'un événement sur la route. L'événement peut être un événement annoncé par un véhicule sur la route dans ce cas la dissémination peut se faire entre les véhicules sans passer par l'infrastructure (communication V2V). Dans le

cas où l'événement est annoncé par l'infrastructure (ex. CN, serveur central sur Internet etc.), deux types de communications se pressentent : de CN vers véhicule (via une communication en Unicast) ou du serveur vers un ensemble de nœuds localisé dans une zone géographique spécifique (via une communication en Geocast).

Les messages DENMs peuvent être utilisés pour signaler une localisation dangereuse, un danger local (ex. embouteillage, brouillard etc.) ou un comportement anormal sur la route (figure 2.6), en informant les véhicules de tout lieu dangereux, soit temporairement ou à long terme. L'objectif est de réduire le risque d'accident qui pourrait être causé par un endroit dangereux. Dans ce cas, quand un événement dangereux est détecté par une entité sur la route, un message de notification DENM est envoyé via une communication V2X, où chaque véhicule a la capacité de recevoir et d'envoyer en unicast, broadcast ou geocast etc. ces messages d'une manière périodique avec une fréquence maximale de 10 Hz. Les véhicules concernés (ex : sur la même route) doivent être capables de recevoir et de traiter ces messages DENMs.

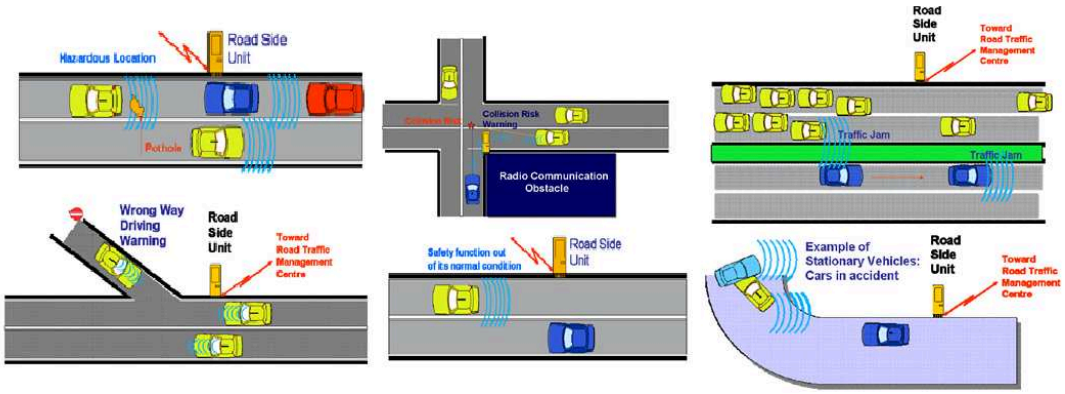

FIGURE 2.6 – Cas d'usages pour les applications d'avertissement de danger routier [40]

En raison d'une impossibilité d'une communication locale directe entre véhicules dans certaines situations, une RSU (Road Side Unit) peut détecter un risque de collision entre les véhicules et de diffuser des messages DENMs. Les véhicules concernés à leurs tours doivent analyser les DENMs reçus et prendre des mesures pertinentes.

Une unité bord de route (UBR ou RSU) peut fournir (aux véhicules) et collecter (des véhicules), des données via Internet pour assister les conducteurs à la conduite (l'assistance à la conduite) grâce aux échanges entre les véhicules qui sont de passage ou en stationnement et les RSUs locales. Quelques cas d'usages sont cités ci-dessous et illustrés sur la figure 2.7 :

— Pour réaliser des échanges locaux ou globaux entre véhicules, un service global de messagerie instantanée peut être réalisé en utilisant une RSU connectée à Internet.
— Pour qu'un conducteur soit toujours connecté à ses données personnelles, une unité bord de route qui possède des capacités d'accès à Internet peut jouer le rôle d'un routeur IPv6 ou passerelle et les véhicules concernés doivent à leurs tour assurer une configuration d'une adresse IPv6 globale et valide, pour assurer un échange des données en toute transparence entre les véhicules et Internet / leurs systèmes distants (par exemple, à la maison, au bureau etc.).

Pour ces cas d'usages, IPv6 est requis pour accéder à Internet. Pour les services basés

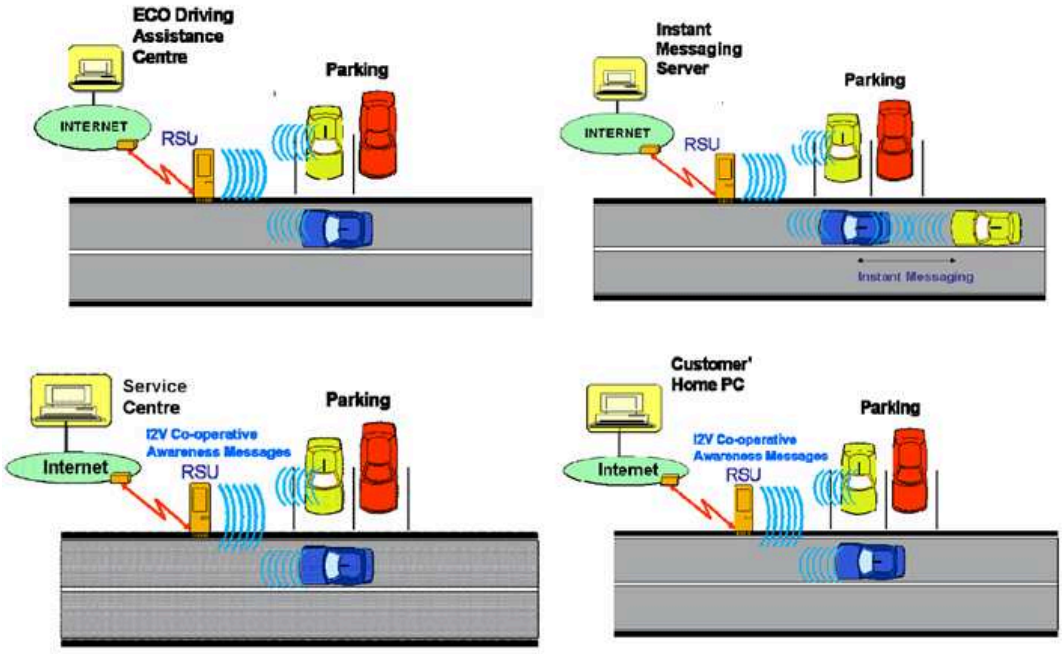

FIGURE 2.7 – Cas d'usages pour les applications de type I2V (ou V2C) [40]

sur une communication en unicast, ceci exige de fournir un adressage IPv6 global valide. Dans ITS 5.9 GHz, le protocole GeoNetworking combiné avec IPv6 étend la portée des RSUs. Ces cas d'usages exigent qu'une RSU broadcast sa capacité d'offrir un service tel que places de parking à proximité et des serveurs d'applications connus (ex. inclut dans les messages CAMs). La RSU peut agir comme un routeur IPv6 (ou passerelle) au réseau. Des applications spécifiques peuvent être exécutées au niveau de la RSU ou au niveau des serveurs d'applications. Ces applications assurent une connexion avec tout véhicule qui a besoin de l'assistance à la conduite. D'un autre côté, les véhicules concernés à recevoir ces messages de sensibilisation à la coopération traitent et configurent une adresse IPv6 pour qu'ils puissent se connecter à des serveurs annoncés ou connus et créer une communication en unicast pour assister entièrement la conduite des conducteurs sur la route.

Dans ce cas par exemple, un serveur central (ex. centre de monitoring) peut avoir les capacités de communiquer des informations à un ensemble de véhicules qui se trouvent dans une certaine zone géographique, comme illustré sur la figure 2.8.

Pour réaliser un tel échange d'informations, ce serveur doit envoyer une requête à un serveur de localisation pour obtenir des informations (adresse IP des RSU qui couvrent la zone concernée) qui permettent une communication avec la RSU, ensuite cette dernière à son tour doit être capable de localiser les véhicules à temps réel et relayer les données à ces véhicules appartenant à la zone de destination. Les véhicules dans la zone de destination doivent être capable à leurs tour de configurer une adresse IPv6 valide afin d'assurer une communication avec le serveur ou Internet.

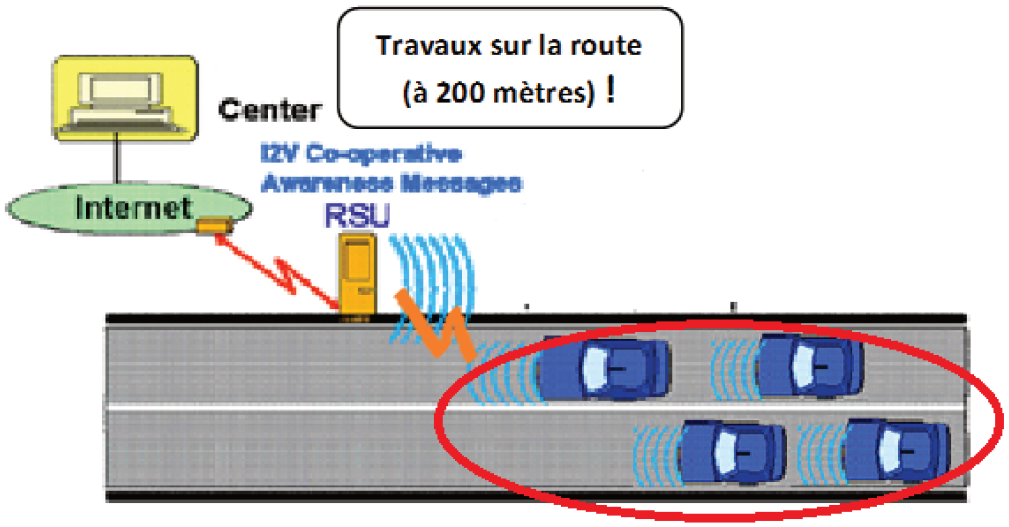

FIGURE 2.8 – Cas d'usage pour les applications de type serveur vers une zone géographique (V2C) [40]

2.6 Les applications d'avertissement de danger routier

L'application d'avertissement de danger routier RHW (Road Hazard Warning) améliore la sécurité routière en assistant les utilisateurs ITS dans leurs conduite en fournissant des informations sur les risques qui peuvent se produire sur la route. L'événement est caractérisé par une position, une durée, son impact sur la sécurité routière et son évolution en termes de temps et d'espace.

Des messages DENM sont principalement utilisés et disséminés par cette application RHW coopérative pour alerter les utilisateurs de la route des événements détectés sur la route. Selon le type d'événement détecté sur la route, la diffusion des messages DENM peut être réalisée par la même station ITS, d'une manière temporaire par une ou plusieurs stations ITS, ou relayée par une ou plusieurs stations ITS. A ce jour, treize cas d'usages ont été définis par ETSI [43] avec des exemples sur les conditions de déclenchement et de terminaison de la diffusion des messages DENM pour chaque cas d'usage. Deux scénarios peuvent être décrits pour les cas d'usage de l'application RHW :

— Un véhicule qui détecte un événement dangereux pour la route.
— Un équipement au bord de la route qui détecte ou qui est programmé pour signaler un événement dangereux sur la route.

Un message DENM fournit des informations relatives à un événement qui a un impact potentiel sur la sécurité routière. En outre, un message DENM peut être utilisé dans des cas d'usages pour l'efficacité du trafic routier (traffic efficiency). Dans une telle situation, un cas d'usage peut nécessiter la diffusion d'un message DENM sur une longue distance ou vers une station centrale ITS, comme pour le routage entre véhicules ou la gestion du trafic routier (traffic management).

En général, chaque événement se caractérise par le type d'événement, la position

géographique ou les coordonnées géographiques de la zone, le moment de sa détection et sa durée. Ces attributs peuvent changer au fil du temps. Un message DENM, qui concerne le même événement, peut être délivré par plusieurs stations ITS (ITS sources) se trouvant à différentes positions, la diffusion persiste même après que ces dernières (ITS sources) s'éloignent de l'événement détecté. Par conséquent, cet événement détecté peut être indépendant des stations ITS sources. En outre, la fiabilité des informations fournies relatives au même événement détecté peut varier dans les différentes stations ITS (ITS sources), selon la capacité de détection de chaque station ITS.

Comme mentionné précédemment, l'application RHW est composée de plusieurs cas d'usage. Généralement, la procédure de traitement d'un cas d'usage est défini par le standard comme suit :

1. Lors de la détection d'un événement qui correspond à un cas d'usage de RHW, la station ITS diffuse immédiatement les messages DENM à d'autres stations ITS situées dans une zone géographique et qui sont concernées par l'événement.
2. La transmission d'un message DENM se répète avec une certaine fréquence.
3. Cette diffusion des DENM persiste aussi longtemps que l'événement est présent.
4. La fin de la diffusion des messages DENM est automatiquement effectuée une fois l'événement disparaît après un temps d'expiration prédéfini ou par une station ITS qui génère un autre DENM spécial pour informer de la disparition de l'événement.
5. Les stations ITS, qui reçoivent les DENM, traitent les informations qu'elles trouvent pertinentes et décident de retransmettre des avertissements aux autres utilisateurs de la route.

Le PDU (Protocol Data Unit) de DENM est composé d'un en-tête (ITS-PDU) commun et de contenu de DENM. L'en-tête inclut des informations de base y compris la version du protocole, le type de message (CAM ou DENM) et le temps de génération du message, cet en-tête est sur 8 octets. Un DENM se compose de trois parties : la gestion du conteneur (management container) sur $13\ octets$, la situation du conteneur (situation container) sur $3\ octets$ et la localisation du conteneur (location container) qui sont définies et spécifiées par l'application RHW avec des tailles variables sur $13\ octets$ (sans le champ de zone de pertinence). La structure sémantique générale d'un DENM est illustrée dans la figure 2.9.

La gestion de conteneur contient des informations pour gérer un message DENM en indiquant par exemple l'évolution de l'événement ainsi que sa fin. Les informations incluses dans ce conteneur de gestion doivent permettre à la station ITS de distinguer les différentes stations ITS source de l'événement et les différents événements sans ambiguïté.

La situation du conteneur comprend des informations qui décrivent l'événement détecté ainsi que son impact potentiel sur la sécurité de la route et sur le trafic routier. Par exemple, l'effet du flux du trafic est l'une des données incluse dans ce conteneur et permet de fournir l'état du flux du trafic causé par l'événement. C'est-à-dire que l'événement a causé un embouteillage, un trafic dense ou n'a pas d'impact sur le trafic. D'autres informations supplémentaires peuvent être incluses pour indiquer le type de véhicule restrictif, si l'état du trafic est uniquement dédié à un type de véhicule spécifique.

La localisation du conteneur se compose principalement de trois informations : *la position de l'événement, le référencement de la localisation et la zone de pertinence*.

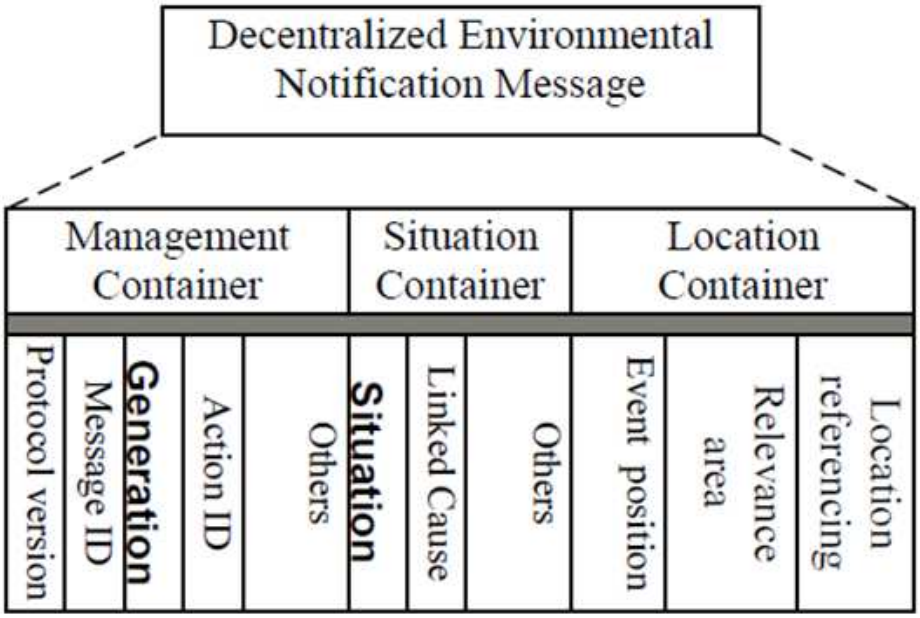

FIGURE 2.9 – La structure générale du message DENM [43]

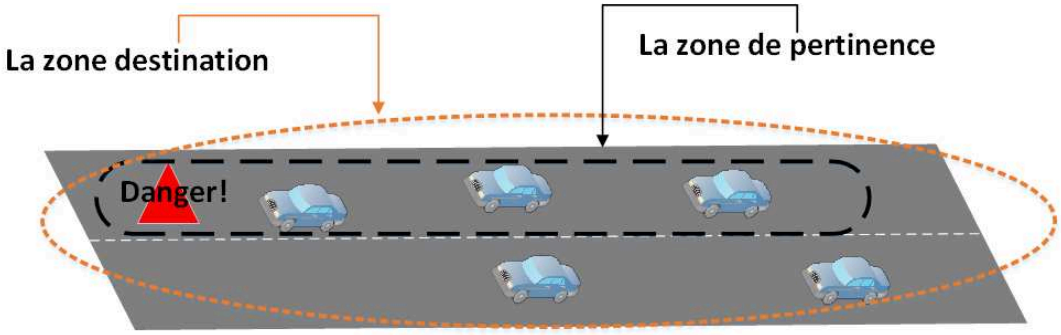

FIGURE 2.10 – Exemple d'une zone de pertinence et d'une zone de destination : cas d'autoroute

1. ***La position de l'événement*** : décrit la position géographique de l'événement détecté. Il peut être représenté comme une position géographique lorsque l'événement se trouve à une position géographique spécifique (Par exemple, la position courante d'un véhicule ITS en cas d'accident), une zone géographique lorsque l'événement couvre toute une zone ou une section de la route.
2. ***La zone de pertinence*** : la zone de pertinence décrit une zone géométrique (Geographical area), une topologie routière (Road topology) et/ou une direction spécifique de la dissémination du trafic (Dissemination traffic direction), dans laquelle on y trouve des stations ITS situées dans cette zone et elles sont concernées par l'événement. La zone de pertinence indique les frontières minimales dans lesquelles les messages DENM devraient être diffusés et la direction de transmission des DENM le long de la route. Chaque message DENM doit être diffusé à autant de stations ITS que possible localisées ou entrant dans la zone de pertinence. La zone de pertinence est incluse dans le message

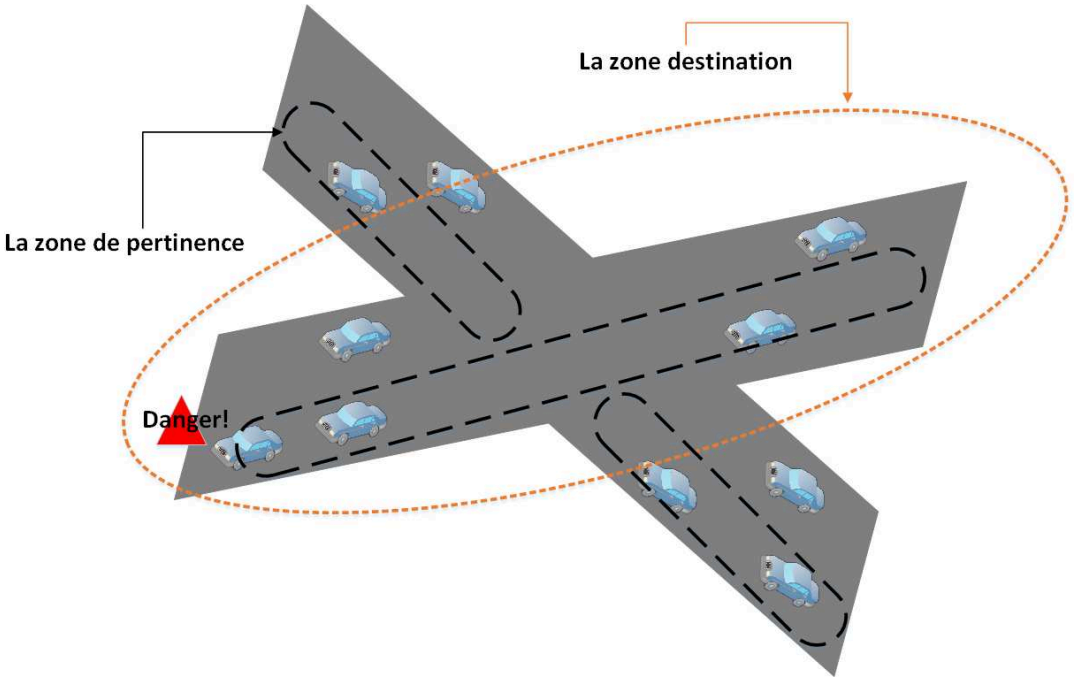

FIGURE 2.11 – Exemple d'une zone de pertinence et d'une zone de destination : cas d'intersection

DENM, où chaque station ITS se base sur une information pertinente pour réaliser la vérification de la pertinence et gérer les informations relatives à l'événement. La zone de pertinence est définie dans l'application RHW pour chaque cas d'usage [43]. Selon les exigences d'un cas d'usage, la zone de pertinence peut être décrite de plusieurs façons :

— *La zone géographique* : la zone de pertinence est décrite par une forme géométrique. Elle peut être combinée avec d'autres éléments tels que la distance. Par exemple, pour un accident sur une autoroute, la zone de pertinence du DENM liée à l'accident du véhicule se trouve à une certaine distance de la position de l'accident.
— *La topologie routière* : la zone de pertinence est décrite par un ou plusieurs identificateurs de segments de la route. Par exemple, Pour un travail routier, la zone de pertinence du DENM liée à la route peut être une ou plusieurs sections routières qui sont influencée(s) par les travaux routiers.
— *La direction de la dissémination du trafic* : la zone de pertinence est décrite par une direction de la circulation selon laquelle DENM est diffusé. Par exemple, pour un embouteillage sur une autoroute, la zone de pertinence du DENM liée à l'embouteillage est la direction en amont de ce bouchon.

La zone de destination peut être définie par des formes géométriques différentes. Trois formes sont actuellement définies selon [41] : la forme *circulaire, rectangulaire et elliptique*. La zone de pertinence n'est pas nécessairement identique à la zone de destination utilisée au niveau de la couche réseau et transport de ITS. Cependant, la zone de destination doit couvrir la zone de pertinence. Et une conversion de la zone de pertinence vers la zone de destination devrait se faire. Des exemples de la zone de

pertinence et la zone de destination sont illustrés sur les figures 2.10 et 2.11.

3. ***Le référencement de la localisation*** : il fournit des informations sur la position de l'événement. Plusieurs mécanismes de localisation peuvent être utilisés en fonction des exigences de chaque cas d'usages. Un mécanisme de localisation peut être utilisé pour l'utilisation des cas d'usages de RHW est la localisation par traces, en fournissant une liste des positions des points d'acheminement qui mènent vers la position de l'événement. Ce type de localisateur est défini et fourni par la station ITS initiatrice.

2.7 L'architecture réseau pour les stations ITS

L'architecture réseau comprend les réseaux internes et externes (Figure 2.12). Un réseau interne interconnecte les différents composants d'une station ITS. Les réseaux externes interconnectent des stations ITS entre-elles ou des stations ITS à d'autres entités du réseau. Les réseaux externes identifiés par [16] sont :

— Le réseau ad hoc ITS
— Le réseau d'accès (réseau d'accès ITS, réseau d'accès public, réseau d'accès privé)
— Le réseau cœur (ex. Internet).

En outre, une station ITS peut avoir un réseau interne qui permet l'interconnexion des composants de cette station ITS. Ces différents réseaux doivent supporter au moins un des cas d'usage (use case) de la sécurité routière (road safety), de la gestion du trafic routier (traffic efficiency), et d'informations et divertissement. Cependant, la communication avec un seul réseau ne peut pas répondre à toutes les exigences des applications et les cas d'usage. En revanche, une combinaison de ces réseaux est envisagée, dans laquelle de multiples technologies d'accès et de réseau sont utilisés.

— Réseau ad hoc ITS : permet la communication entre les véhicules, unité bord de route (RSU) et autres station ITS. Cette communication est basée sur des technologies sans fil qui assurent des communications à courte portée (short-range wireless technology) et qui permettent la mobilité des stations ITS sans avoir recours à coordonner la communication avec l'infrastructure. Par exemple : le réseau de véhicules et l'unité bord de route (RSU) sont interconnectés par la technologie sans fil ITS-G5 dans ce réseau.
— Réseau d'accès ITS : permet l'accès à des services et applications ITS spécifiques et il peut être exploité par un opérateur routier ou d'autres opérateurs. Ce réseau permet aussi l'interconnexion et la communication des RSUs entre-elles ainsi qu'entre les véhicules ITS via des RSUs qui sont interconnectées dans ce réseau d'accès ITS. Ce réseau local permet d'assurer une communication entre les véhicules ITS via une unité bord de route (RSU) au lieu d'utiliser directement le mode ad hoc. Par exemple : ce réseau d'accès ITS peut connecter des RSUs le long de la route avec une station centrale (ex. centre de gestion du trafic routier). Dans le cas où la communication via les RSUs est assurée par des technologies d'accès sans fil à courte portée, la connectivité au réseau d'accès ITS est alternative.
— Réseau d'accès public : assure un accès aux réseaux publics.
— Réseau d'accès privé : fournit des services à un groupe d'utilisateurs fermé pour un

accès sécurisé à un autre réseau. Par exemple : ce réseau peut connecter les véhicule ITS à l'Intranet d'une société.

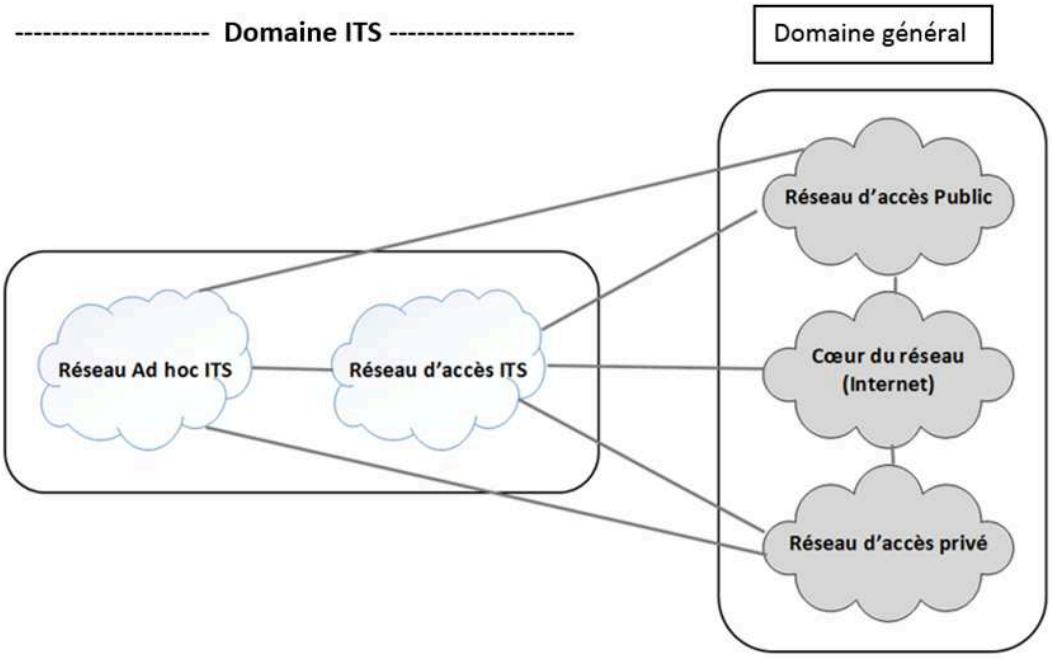

FIGURE 2.12 – les réseaux externes dans l'architecture ITS et ses interconnexions

Le réseau d'accès et le réseau cœur fournissent des accès à plusieurs services, à savoir :

— Les services traditionnels (ex. WWW, email etc.).
— Les services ITS fournis par les centres de gestion du trafic routier.
— Les services ITS nécessaires pour faire fonctionner des ITS, comme les services de sécurité.

Le composant cœur de l'architecture est la station ITS, qui a deux rôles principaux : son premier rôle, la station ITS est un nœud source (ex. transmetteur de données) dans le réseau (ex. le réseau ad hoc ITS) lors d'une communication. Son second rôle, la station ITS est placée dans l'edge de réseau et assure la connexion des différents réseaux via le réseau interne de la station ITS (ITS station internal network). Une station ITS doit pouvoir communiquer via l'un de ces moyens : réseau ad hoc ITS, réseau d'accès ITS, réseau d'accès public, réseau d'accès privé ou via un des réseaux d'accès au réseau cœur (ex. Internet).

Le composant principal de l'architecture réseau est la station ITS comme spécifiée dans [EN 302 665], cette dernière peut être : un véhicule ITS, une station ITS personnelle, l'unité bord de route ou une station ITS centrale. En plus, il existe d'autres composants réseau liés à la communication IPv6, à savoir : le routeur ad hoc, le routeur mobile, le routeur d'accès et la passerelle d'accès au réseau comme spécifié dans [7].

2.7.1 La pile protocolaire de la station ITS

La couche réseau et transport de ITS comprend plusieurs protocoles réseau et transport (figure 2.13), qui sont :

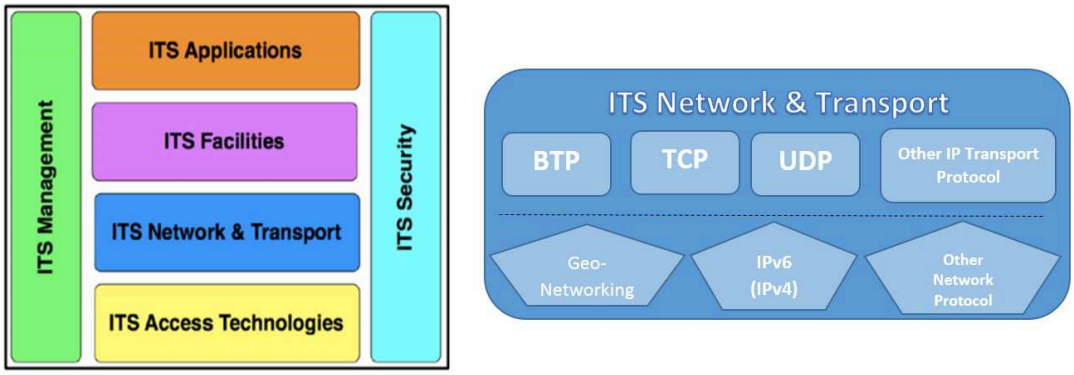

FIGURE 2.13 – les protocoles réseaux et transport de ITS

— Le protocole GeoNetworking,
— Les protocoles de transport au dessus de GeoNetworking, comme BTP (Basic Transport Protocol) défini dans [3].
— Le protocole internet IP version 6 défini dans [6], avec le support de la mobilité comme spécifié dans [8] et optionnellement, le support de la mobilité de réseau (NEMO) comme défini dans [9] ou dans d'autres approches qui dépendent du scénario déployé.
— Le protocole internet IP version 4 pour la transition vers IP version 6 tel que spécifié dans [11].
— UDP (User Datagram Protocol) comme défini dans [10].
— TCP (Transmission Control Protocols) comme spécifié dans [12].
— Autres protocoles réseaux.
— Autres protocoles de transport, comme SCTP.

Nous allons décrire en détail la pile GeoNetworking et celle d'IPv6.

2.7.2 La pile protocolaire GeoNetworking

La pile de protocole GeoNetworking peut être assemblée avec le protocole GeoNetworking ou avec des protocoles de transport spécifiques tels que prévus dans [3], un exemple de ces protocoles est le protocole BTP qui se situe en dessus de GeoNetworking comme illustré sur la figure 2.14 (la pile GeoNet dans la station ITS).

1. **Le protocole GeoNetworking :** permet d'assurer plusieurs modes de routage des paquets (geo-Unicast, geo-Broadcast et geo-Anycast) dans un réseau ad hoc basé sur l'adressage géographique. La couche supérieure de GeoNetworking peut être Basic Transport Protocol (BTP) décrit dans [21] ou aussi IPv6 (TCP/UDP) dans [22]. IPv6 permet d'assurer une transmission de paquets quelles que soient les technologies localement disponibles.

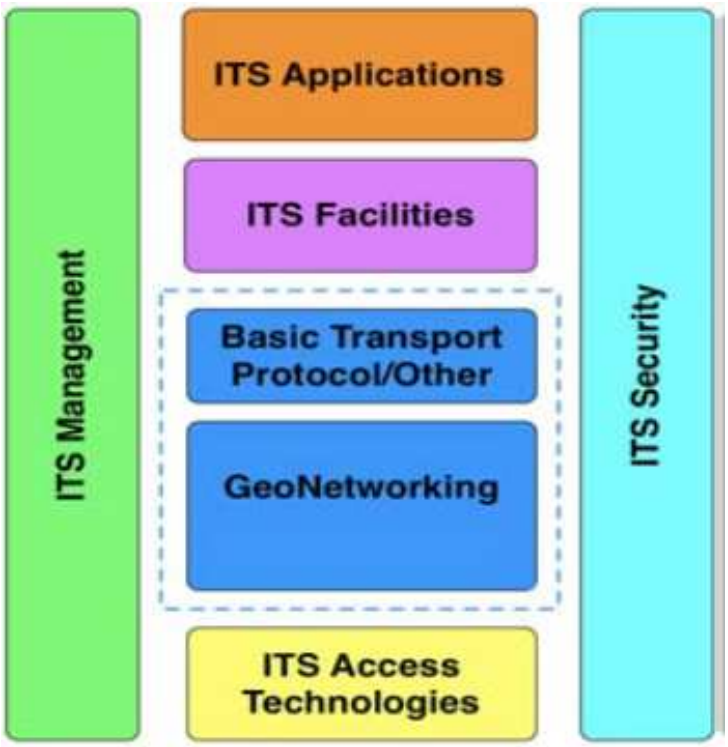

FIGURE 2.14 – les protocoles réseau et transport de ITS [16]

GeoNetWorking est un protocole de routage qui permet la dissémination des paquets de données dans un réseau ad-hoc sans coordination avec l'infrastructure. Il utilise la position géographique pour l'adressage et pour la transmission. L'envoi du paquet à une station ITS se fait en utilisant sa position géographique ou bien les coordonnés de la zone cible [1]. L'adressage dans GeoNetworking désigne la manière d'intégrer les données géographiques dans le mécanisme d'adressage. Le format de l'adresse GeoNetworking est composé de quatre champs (voir la figure 2.15).

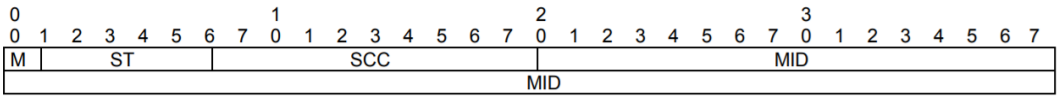

FIGURE 2.15 – Format d'une adresse GeoNetworking [EN 302 636-4-1]

M : le type de la configuration (automatique / manuelle).

ST : le type de la station ITS (Ex. bus, voiture, etc.)

SCC : le code du pays d'une station ITS.

MID : l'adresse de la couche liaison (LL-adresse).

Le routage désigne les concepts de base de dissémination des paquets avec la description de la zone géographique. La structure du paquet GeoNetworking est présentée dans la figure 2.16.

L'en-tête GeoNetworking est décomposé en deux champs :

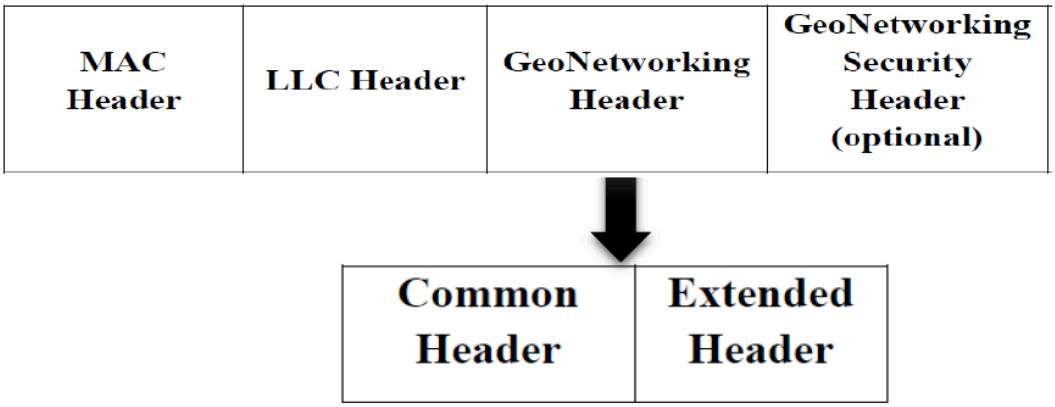

FIGURE 2.16 – Structure de l'en-tête GeoNetworking [EN 302 636-4-1]

Common Header : l'en-tête commun contient des informations comme :

- Le type de l'en-tête GeoNetworking : Beacon, GeoUnicast, GeoAnicast, etc.
- les différentes classes de trafic (AC ou Access Category) : AC_{BE} (AC Best Effort), AC_{BK} (AC BacKground), AC_{VI} (AC VIdeo) et AC_{VO} (AC VOice) [42].
- Le nombre maximum de saut.
- Next Header (NH) : BTP-A, BTP-B, IPv6, etc.

Extended Header : il dépend de la fonctionnalité, par exemple : GeoUnicast, GeoBroadcast, etc.

GeoNetWorking supporte cinq mode de transmission de paquets : *geo-unicast, geo-broascast, geo-anycast, single-hop broadcast et topologically-scoped broadcast*. *Geo-broadcast* est utilisé pour la dissémination des messages de notification DENMs. *Single-hop broadcast* est utilisé périodiquement pour le type de messages CAMs. GeoNetWorking permet de forwarder les paquets *on the fly* sans l'établissement et la maintenance des routes. Le standard de GeoNetWorking [EN 302 636-4-1] spécifie plusieurs algorithmes pour la dissémination des paquets en toute efficacité. Trois algorithmes ont été spécifiés pour le géo-broadcast des paquets : L'approche *Flooding (simple géo-broadcast)* limite le rebroadcast en se basant sur des frontières géographiques de la zone cible. La détection des paquets en duplications se fait en se basant sur l'identifiant de la source et le numéro de séquence des paquets. L'algorithme *Contention based forwarding* (CBF) buffer le paquet et la décision de transmission est faite au niveau du récepteur : chaque nœud candidat à la transmission déclenche un timer (le plus petit timer correspond au nœud le plus proche de la destination). Le nœud avec un timer plus petit retransmet le paquet. Les nœuds qui écoutent la retransmission annule leurs timers et abandonne la transmission du paquet. L'algorithme *Advanced forwarding* (également appelé *Greedy Forwarding*) combine CBF avec le principe de sélection d'un next-hop selon un critère.

2. **Le protocole BTP (Basic Transport Protocol) :** BTP (EN302 636-5-1) multiplexes ou dé-multiplexes des messages (ex. CAM, DENM) et permet de transporter des paquets de

bout en bout sans connexion similaire au protocole UDP, avec peu de fiabilité. Il adopte la notion de ports et attribue des ports bien connus pour les différents types de messages au niveau de la couche Facilities. Par exemple : pour les messages CAM, BTP attribue le port numéro 2001 (EN 302 637-2). Pour les messages de notification DENM, BTP affecte le port numéro 2002 (EN 302 637-3).

2.7.3 La pile protocolaire IPv6

La pile IPv6 peut être assemblée avec le protocole IPv6 et des protocoles de transport comme UDP définis dans [10].

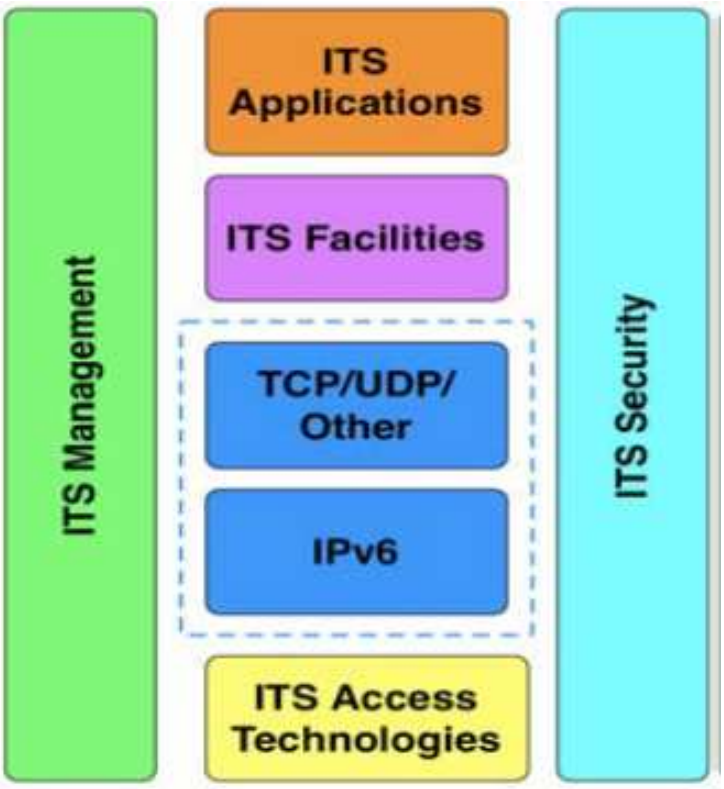

FIGURE 2.17 – les protocoles réseaux et transport de ITS [16]

2.7.3.1 Le protocole Mobile IP (MIP)

L'IETF a élaboré une première version de Standard mobile IP en 1996. Plus tard, l'IETF a développé le Mobile IPv4 [RFC3344] et Mobile IPv6 [RFC3775] en 2002 et 2004, respectivement. En 2010, la norme mobile IPv4 a été révisée [RFC5944]. En 2009, une double pile Mobile IPv4 [RFC5454] était standardisée pour permettre à un nœud d'utiliser les deux types d'adresses (IPv4 et IPv6) et de se déplacer entre IPv4 et le réseau des infrastructures.

Le protocole de mobilité IP permet le routage de paquets IP sur Internet indépendamment de l'emplacement. Chaque nœud itinérant est identifié par son adresse personnelle (home address), quel que soit son emplacement actuel sur Internet. Avec MIP, chaque nœud mobile

(MN) possède deux adresses IP différentes : une adresse mère (HoA) qui permet de l'identifier et une adresse temporaire (CoA) pour le localiser. L'adresse mère du nœud mobile est une adresse configurée par son agent mère(HA), l'agent mère est un routeur qui se trouve au niveau du réseau mère (home network). La CoA est une adresse attribuée par une passerelle (agent étranger, FA), le FA est un routeur situé au niveau du réseau visité. Quand le nœud mobile se déplace de son réseau mère vers un réseau visité, il effectue le handover en échangeant des messages de mise à jour de son association avec le HA (home binding update). Ce nœud mobile informe l'agent mère (HA) et le nœud correspondant (CN) de sa position courante, qui est présentée par son adresse temporaire (CoA). Il se peut que ce nœud mobile reçoit un paquet envoyé avec une HoA de nœud mobile (de cette CoA), dans ce cas le HA et CN peuvent transmettre ce paquet car ils possèdent à leurs niveaux l'association (HoA, CoA).

Mobile IP existe sous deux (02) versions, une pour les réseaux IP en version 4 et une autre pour les réseaux IP version 6. Dans ce qui suit, nous allons présenter les notations qui seront utilisées tout au long de ce chapitre.

Le protocole Mobile IPv4

Mobile IP définit les entités suivantes [77] :

— Le nœud mobile (Mobile node, MN) : une hôte ou un routeur qui modifie son point d'attachement d'un réseau ou d'un sous-réseau à un autre au cours de son déplacement.

— L'agent mère (ou Home Agent, HA) : un routeur sur le réseau mère d'un nœud mobile qui maintient l'information de localisation actuelle du mobile et il sert d'intermédiaire entre le nœud mobile et l'agent étranger (FA).

— L'agent étranger (ou Foreign Agent, FA) : Un routeur sur le réseau visité du nœud mobile qui fournit des services de routage au nœud mobile lors de son enregistrement. L'agent étranger sert d'intermédiaire entre le nœud mobile et l'agent mère.

Dans mobile IP, un nœud mobile a une adresse statique dans son réseau mère nommé adresse personnelle (home address ou HoA en anglais) et elle ne change pas tant que le nœud mobile reste dans le même réseau (domaine d'administration). A chaque fois que le nœud mobile change du réseau et se connecte à un réseau visité, il sollicite l'agent étranger et il obtient une adresse temporaire (care-of address ou CoA en anglais), cette dernière change à chaque fois que le nœud mobile se connecte à un nouveau réseau visité.

Les étapes suivantes fournissent une vue d'ensemble du fonctionnement du protocole IP mobile :

Lors d'une première tentative de communication entre un nœud correspondant (CN) et le nœud mobile, le CN envoie le paquet avec une adresse IP mère (HoA), qui est une adresse connue par le HA. Dans le cas où, le nœud mobile n'est pas connecté à son réseau mère, Le home agent encapsule le paquet avec une autre adresse pour l'envoyer au FA. Cette encapsulation est nommée Tunneling, elle permet la transmission des paquets dans un réseau visité sans modifier le paquet IP d'origine. Autrement dit, un tunnel est créé entre les deux entités (FA, HA) et le paquet encapsulé arrive au bout du tunnel au FA qui le décapsule et l'envoie au nœud mobile comme illustré sur la figure 2.18 . Sachant que ce paquet a une adresse de destination HoA. A partir de cet échange, le nœud mobile peut communiquer directement avec le nœud correspondant (CN). Dans un contexte de mobilité, il est claire que

la communication down (CN vers nœud mobile) est plus compliquée qu'une communication en up (nœud mobile vers CN).

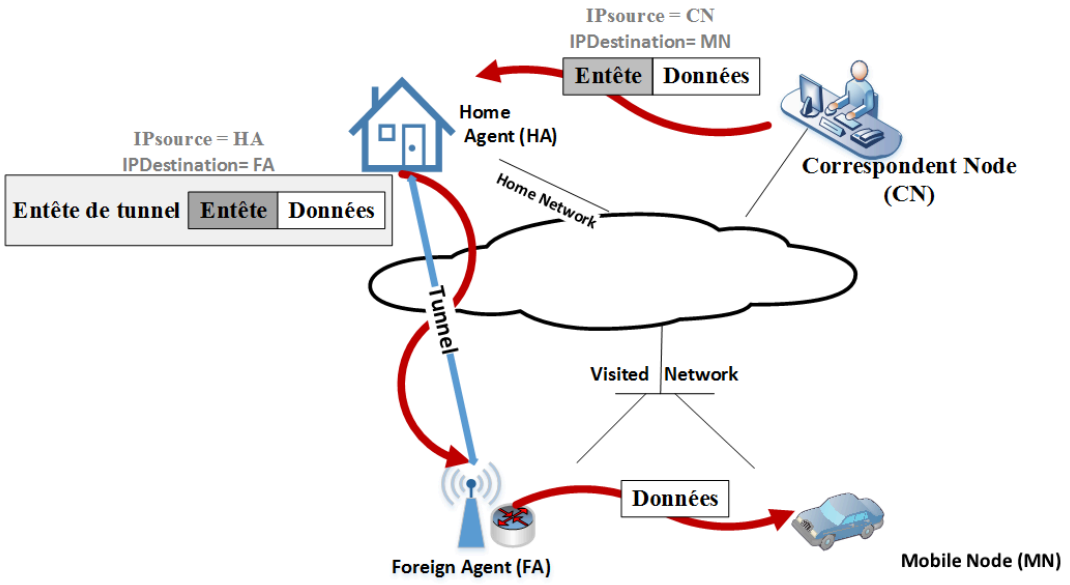

FIGURE 2.18 – Principe deMobile IPv4

Pour pouvoir assurer un bon fonctionnement du réseau dans le contexte de la mobilité, les services suivants sont définis pour Mobile IP :

- Découverte de l'agent (Agent Discovery) : chaque agent de mobilité (i.e., agent étranger et agent mère) annonce sa présence via des messages d'avertissement [ref RFC-1256-1991]. Un nœud mobile peut éventuellement solliciter un message d'avertissement de n'importe quel agent attaché localement à ce nœud mobile, à travers un message de sollicitation (Agent Solicitation message).
- Enregistrement (Registration) : cette procédure d'enregistrement permet au nœud mobile d'informer son agent mère de sa position courante.
  Lorsque le nœud mobile s'éloigne de son réseau mère , il enregistre une adresse temporaire (obtenue par le message d'avertissement) en envoyant une demande d'inscription (registration request) soit directement auprès de son agent mère, soit par l'intermédiaire d'un agent étranger qui transmet l'inscription (enregistrement) à l'agent mère. Une fois l'enregistrement est réussi, l'agent mère peut intercepter les paquets à destination du nœud mobile , puis l'envoyer à l'agent étranger via un tunnel entre l'agent mère et l'agent étranger (figure 2.18).

Dans mobile IPv4, la transmission des paquets doit passer par le home agent, ce qui génère de long délai d'échange entre le nœud mobile et le nœud correspondant. Dans ce qui suit, nous allons présenter le protocole Mobile IPv6 qui permet de maintenir la communication entre le nœud mobile et le nœud correspondant sans sollicitation d'une entité intermédiaire qui est l'agent étranger.

Le protocole Mobile IPv6

Pour réduire le délai de bout en bout de transit, Mobile IPv6 introduit la notion d'association qui permet de relier une adresse ip temporaire (CoA), celle donnée par le réseau visité, avec l'adresse IP mère (HoA) par le réseau mère. Dans Mobile IPv6, la notion de l'agent étranger ainsi que le problème de routage triangulaire n'existent pas. Le protocole Mobile IPv6 étend le protocole IPv6 en introduisant de nouvelles options [62]. Cette amélioration est conçue principalement pour la mobilité et elle comporte quatre options, qui sont binding update, binding acknowledgement, binding request, et l'option d'adresse mère (home address option). La figure 2.19 illustre le principe du protocole Mobile IPv6.

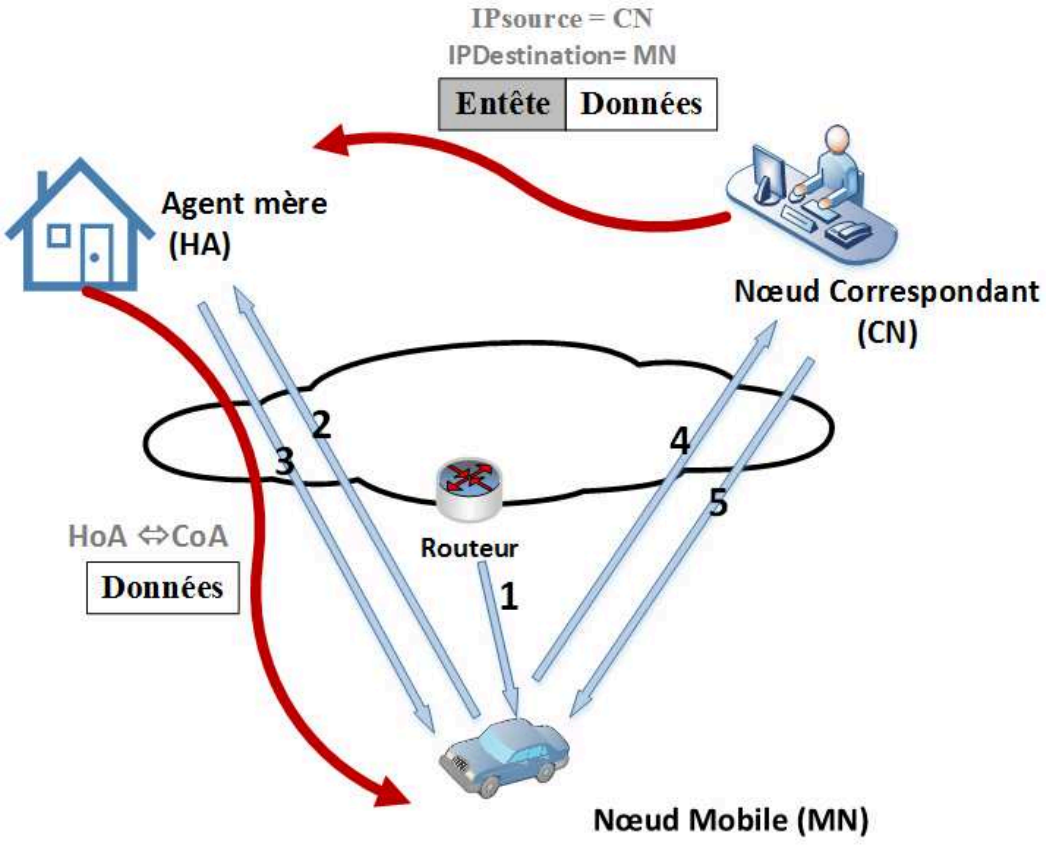

FIGURE 2.19 – Principe de Mobile IPv6

1 : Auto-configuration IPv6 du nœud mobile (MN) qui acquiert une adresse temporaire (CoA).

2 : Le nœud mobile (MN) envoie à son agent mère (HA) son adresse temporaire (CoA) (envoi d'un message Binding Update ou BU).

3. Le HA enregistre l'association (HoA, CoA) (message Binding ACK noté BA), un tunnel est établi entre le HA et MN.

4 : Le MN envoie un BU (contient son CoA) au nœud correspondant (CN).

5. Le CN envoie ses paquets directement au MN (optimisation de route).

— Binding update (Mise à jour de l'association) :

L'option de Binding update est utilisée par un nœud mobile pour annoncer qu'il a changé son point d'attachement à Internet ou pour renouveler une liaison existante qui est sur le point d'expirer. Cette option est l'équivalent du message de demande d'enregistrement dans IPv4 mobile. L'opération de Binding update est utilisée par le nœud mobile pour annoncer au nœud correspondant ou à l'agent mère son point d'attachement actuelle.

— Binding Acknowledgement (Acquittement de l'association) :
Le Binding Acknowledgement est utilisé pour confirmer la réception d'une mise à jour d'une liaison (Binding Update).

— Binding Refresh Request (Requête de mise à jour de l'association) :
Une requête de rafraîchissement d'une liaison (Binding Refresh Request) est utilisée par un nœud correspondant pour demander à un nœud mobile de rétablir sa liaison avec le nœud correspondant. Ce message est généralement utilisé pour rafraîchir son association avec le nœud mobile.

— Adresse mère (Home address) :
Cette option est utilisée par un nœud mobile pour informer le CN de son home of address (HoA). Les nœuds correspondants sont alors capables de substituer l'adresse temporaire (CoA) par l'adresse mère du nœud mobile.

Le protocole Mobile IPv6 permet la gestion de la mobilité, lors d'une mobilité rapide des nœuds qui entrainent des déconnexions de communications lors du changement de réseau, le problème de Mobile Ip réside dans son long délai d'échange de messages avec le réseau mère, ce qui n'est pas approprié dans le contexte de la sécurité routière où les applications sont critiques et à temps réel.

2.7.3.2 Proxy mobile IP (PMIP)

Mobile IP est la première approche proposée pour obtenir la mobilité sur Internet. Une de ses faiblesses est le délai de signalisation d'handover qui est très long vu qu'il faut remonter jusqu'à l'agent mère pour mettre à jour son adresse temporaire (CoA), ce qui convient pas aux applications de la sécurité routière dont le temps est critique.

La solution Proxy Mobile IP (PMIP) [RFC5213] est proposée en 2006 pour assurer une mobilité complètement transparente aux périphériques mobiles (le délai de signalisation lors d'handover est plus optimal). Proxy Mobile IP introduit deux types d'entité réseau, à savoir : Local Mobility Anchor (LMA) et Mobile Access Gateway (MAG), qui permettent de supporter la mobilité des nœuds mobiles sans intervention de ces derniers. Un LMD (local mobility domain) est un réseau où le proxy Mobile IP est active et LMD est constitué d'une LMA et plusieurs MAG.

LMA : joue le rôle d'agent mère local et attribue des identifiants (ex. adresse MAC de mobile) et des préfixes (Home Network Prefix) dans un domaine LMD aux mobiles. Elle assure l'acheminement de tout trafic vers ou depuis le mobile. LMA maintient aussi l'ensemble des routes pour chaque mobile connecté à un LMD.

MAG : gère les événements tel que l'attachement et le détachement du mobile en envoyant des messages de mise à jour (Proxy Binding Update) à LMA lors d'handover sans que le mobile participe à la signalisation. Pour que le mobile se connecte à une entité sur

Internet ou dans un domaine (LMD) à travers un réseau (3G , 4G etc), il utilise une MAG comme premier routeur d'accès. Chaque MAG possède une adresse (Proxy CoA). LMA utilise Proxy CoA comme adresse de destination pour encapsuler les paquets destinés à un mobile.

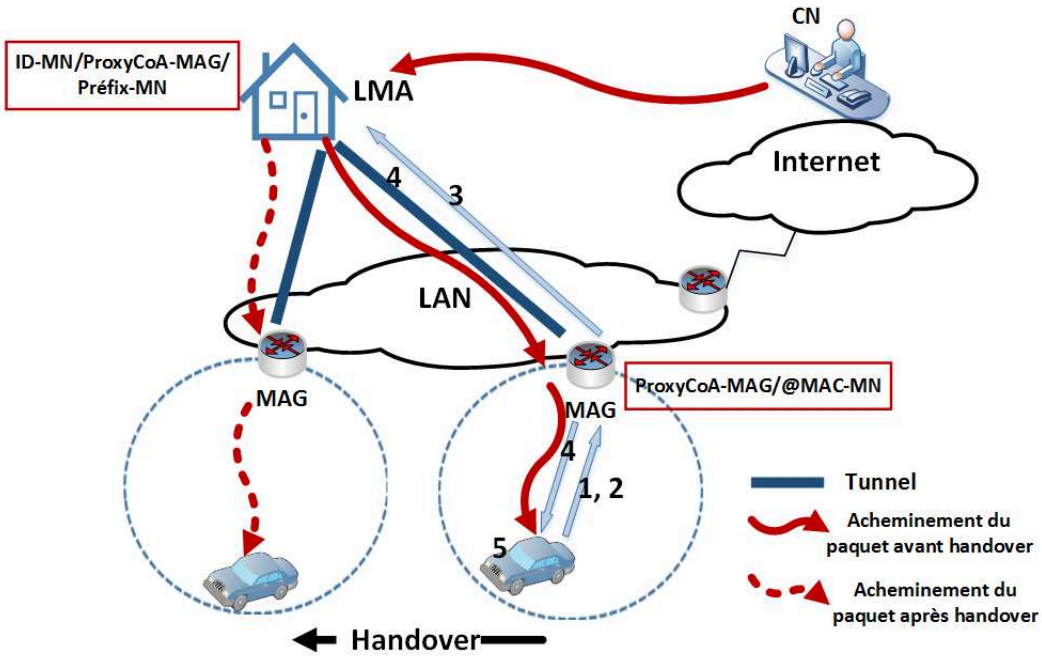

FIGURE 2.20 – Principe de protocole Proxy Mobile IP

Quand un mobile joint un domaine (LMD) et s'attache à une MAG, la procédure de Proxy Mobile IP est illustrée sur la figure 2.20 et elle est décrite comme suit :

(1) le mobile établit une connexion au niveau de la couche liaison (ex. adresse MAC), ensuite MAG identifie et autorise ou pas le mobile à configurer une adresse. dans le cas où le mobile est autorisé,

(2) le mobile envoie au MAG une demande d'attribution d'un préfixe IPv6,

(3) MAG envoie une demande (PBU) à LMA afin d'avoir un préfixe pour ce mobile,

(4) MAG répond au mobile via un message PBA, et un tunnel bi-directionnel (IPv6-in-IPv6) sera établi entre les deux entités MAG et LMA,

(5) le mobile configure une adresse en se basant sur le préfixe reçu de la part de son MAG.

Dans ce cas, le routage des paquets entre un CN et le mobile se fait en passant par LMA ensuite MAG. Autrement, la transmission des paquet entre deux mobiles qui se trouvent sous une même MAG va se faire en passant juste sur MAG (route plus courte).

L'introduction des deux entités (MAG et LMA) permet d'assurer un handover en toute transparence. Par contre avec cette solution, LMA doit attribuer un prefixe à chaque MAG pour chaque mobile ce qui rend la procédure d'adressage couteuse en termes de délai et signalisation. Par ailleurs, la gestion des préfixes aux niveaux de LMA ainsi qu'au niveau du mobile nécessite l'exécution de la procédure DAD pour éviter les collisions à chaque attribution d'un nouveau préfixe.

2.7.4 La Combinaison des deux protocoles GeoNetworking et IPv6

Dans cette pile protocolaire qui combine les deux piles précédentes, IP doit s'exécuter au dessus de GeoNetworking comme défini dans [4] ou bien directement au dessus des technologies d'accès ITS. figure 2.21

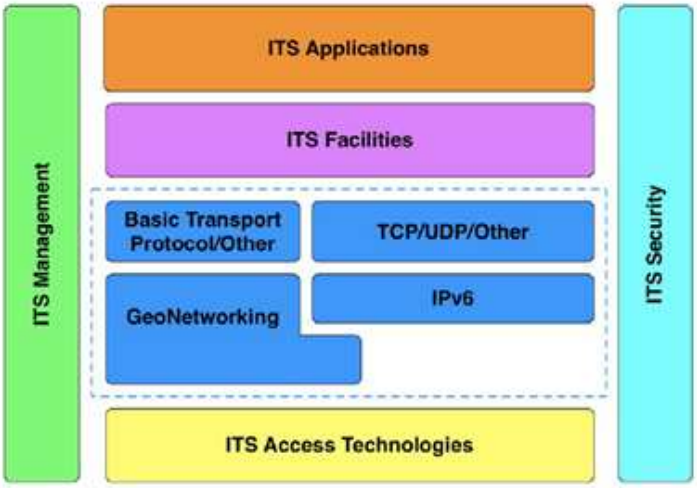

FIGURE 2.21 – Combinaison de la pile GeoNetworking et IPv6 dans une station ITS [16]

Une alternative de BTP est GN6 [22] qui permet la transmission multi-saut des paquets IPv6 sans modifications de IPv6. Il adapte l'auto-configuration d'adresse SLAAC (stateless address auto-configuration)[87] déja connue dans IPv6 et étend le concept de lien IPv6 à des zones géographiques qui sont associées à un point d'attachement IPv6. GN6 introduit une sous-couche d'adaptation, nommée GN6ASL (GeoNetworking to IPv6 Adaptation Sub-Layer).qui présente une topologie de réseau plate à IP [23].

Le réseau ad hoc ITS doit assurer l'acheminement des paquets IPv6 amélioré par GeoNetworking pour assurer la communication entre les stations ITS. L'envoi des paquets IPv6 peut se faire par exemple par l'encapsulation de ces paquets IPv6 au niveau de l'entête du paquet GeoNetworking, le routage de ces paquets encapsulés se fait par le protocole GeoNetworking. Pour la couche IPv6, les stations ITS apparaissent attachées au même lien IPv6. L'accès à l'infrastructure (ex. communication avec des nœuds IPv6 sur Internet) nécessite des mécanismes spécifiques qui permettent la configuration d'une adresse IPv6.

Par ailleurs, dans un contexte de mobilité, l'accès d'une station ITS à une information au niveau de l'infrastructure de communication (ou l'inverse) nécessite que le concept d'IPv6 sur GeoNetworking soit amélioré pour supporter la mobilité IP.

2.8 Conclusion

Dans ce chapitre, nous avons résumé les études connexes qui ont été proposées dans le domaine des réseaux de véhicules par le standard européen ETSI et plus particulièrement (a) cette architecture est commune pour ETSI et ISO ([38] et ISO 21217 :2010) avec les différentes

applications (b) et les communications géographiques et IP à travers la pile protocolaire d'ETSI. Plusieurs types d'applications ITS ont été abordés par le standard ETSI et leurs exigences ont été spécifiées. Nous avons étudié le principe de Mobile IP et Proxy Mobile IP dédiés à la gestion de la mobilité.

Dans ce travail, nous nous sommes principalement intéressés aux applications de la sécurité routières qui nécessitent des mécanismes bien particuliers. Nous contribuons plus spécialement aux mécanismes de transmission multi-sauts au niveau de la couche réseau avec un contrôle de la congestion, ensuite à l'adressage hybrides (Géographique et IP) pour la gestion de la mobilité dans VANET.

Chapitre 3

Mécanismes de contrôle de la congestion décentralisé (DCC) dans GeoNetworking

3.1 Introduction

Dans ce chapitre, nous adressons le problème de la dissémination en géobroadcast dans les réseaux à forte densité. Nous proposons, un protocole de routage géographique CBF2C, qui assure la transmission multi-saut des paquets avec un certain nombre de retransmission en se basant sur l'état de la congestion du canal radio. Motivé par cela, dans un premier temps, nous abordons la congestion du canal lors du transfert de paquets DENM. Ensuite, nous nous sommes intéressés à l'étude de la congestion du canal lorsque les paquets CAM et DENM partagent la ressource sans fil avec et sans DCC sur les messages CAMs. Ensuite, nous proposons d'améliorer le mécanisme CBF avec un contrôle de la congestion distribuée sur les messages DENMs (nommé CBF2C).

D'abord, dans la section 3.2 nous présentons le contexte globale et nous expliquons la problématique étudiée. Un état de l'art sur DCC est présenté dans la section 3.3. Dans la section 3.4 une étude des algorithmes de transmission multi-saut proposés dans le cadre de ETSI, qui permet de motiver notre travail. Elle décrit le principe de chaque algorithme de transmission multi-sauts avec leurs points forts et leurs faiblesses. Dans les sections 3.5 et 3.6 nous décrivons nos approches CBF2Cv1 et CBF2Cv2. Ensuite, nous présentons une évaluation de performances pour la validation de nos propositions dans les sections 3.9 , 3.8 et 3.7. Enfin, nous résumons nos contributions en conclusion de ce chapitre.

3.2 Contexte global et Problématique

De nombreuses applications ITS nécessitent un transfert multi-sauts du message de notification DENM. Les algorithmes de transmission multi-sauts sont conçus sans considération du problème de la congestion et ils ont un impact négatif sur les systèmes de véhicules IEEE 802.11p, qui souffrent déjà de la congestion du canal causée, par exemple, par

les messages de sensibilisation coopérative (CAM).

En raison du fait que la ressource du canal soit limitée dans la bande de 5.9 GHz, la congestion du canal est l'un des problèmes clés du système réseau véhiculaire 802.11p. Le problème de congestion du canal causé par les CAM est bien connu [17, 83, 28]. Les études précédentes montrent que le PDR (taux de paquets reçus) peut se réduire à 50% et que le délai de la transmission de bout en bout (E2ED) peut augmenter à 1 seconde lorsque chaque véhicule diffuse périodiquement des messages CAM à 10 Hz avec une densité de 50 à 400 véhicules/Km^2 [83]. Ce niveau de qualité de la communication ne peut évidemment pas satisfaire les exigences des applications de sécurité routière critiques à temps réel.

En ce qui concerne ce problème de la congestion du canal, ETSI a spécifié un framework de contrôle de la congestion distribuée (DCC) [17], une architecture qui permet aux stations ITS (nœuds) de contrôler leurs paramètres de communication au niveau de la couche accès, réseau ou facilities, comme illustré sur la Fig. 3.1. Un certain nombre d'efforts ont été fournis pour le contrôle de la congestion du canal en adaptant quelques paramètres au niveau de la couche facilities (en particulier la fréquence de transmission des CAM) et au niveau de la couche accès (y compris la puissance d'émission, contrôle de débit (Data rate control)et contrôle du seuil de détection de porteuse (carrier sense threshold) [26]. Cependant, au mieux de nos connaissances, il n'y a pas beaucoup de travaux pour le contrôle de la congestion au niveau de la couche réseau, approprié au framework ETSI.

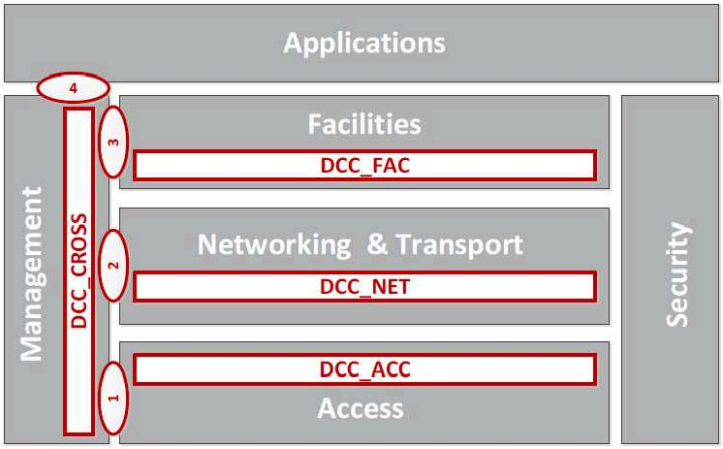

FIGURE 3.1 – L'architecture DCC d'ETSI [17]

Nous pouvons facilement imaginer que, le schéma d'acheminement des messages DENM le plus simple, est Flooding, créant un problème d'inondation du réseau (Broadcast Storm Problem), son impact sur la congestion du canal doit être important, en particulier lorsque le canal de contrôle (CCH) souffre déjà de la transmission des messages CAM. Dans ce qui suit, nous tentons de répondre aux questionnements suivants :

(a) Les algorithmes tels que CBF, qui évitent de créer des retransmissions redondantes, contribuent-ils à la congestion du canal ?

(b) Est-il possible que les messages DENM et CAM obtiennent des performances suffisantes lorsqu'ils partagent la même ressource sans fils (canal CCH) ?

En outre, si un contrôle de la congestion du canal est nécessaire pour les messages DENM,

alors quelles approches devraient être appliquées. Malgré le fait que les messages DENM puissent exploiter les efforts déjà réalisés sur les messages CAM, nous pensons qu'une attention particulière est nécessaire, notamment au niveau de la couche réseau. En effet, bien que les algorithmes DCC qui adaptent les paramètres MAC/ Physique s'appliquent aux messages DENM, ils ne conduisent pas nécessairement aux résultats souhaités. Par exemple, la réduction de la puissance de transmission et l'augmentation du débit de données raccourcissent la portée de transmission, ce qui augmente le nombre de sauts, entraînant une augmentation de la charge du canal.

3.3 État de l'art

3.3.1 Normalisation : Le mécanisme DCC

ETSI a défini un Framework DCC [17] qui assure le contrôle de la congestion distribuée dans les stations ITS (véhicules et RSUs). Il permet de contrôler la charge transmise sur le canal radio afin d'assurer le bon fonctionnement du système. L'architecture du mécanisme DCC est illustrée sur la figure 3.1. Ce mécanisme DCC est composé de DCC-ACC qui est introduit au niveau de la couche Access, DCC-NET introduit au niveau de la couche Networking, DCC-FAC introduit au niveau de la couche Facilities, et, DCC-CROSS introduit au niveau de la couche Management, ce dernier assure l'échange d'informations entre différentes couches et calcule les métriques communes.

L'objectif principal de l'algorithme DCC dans une station ITS est de calculer en fonction des paramètres actuellement en entrée, la limite de ressources autorisée sur le canal. Quatre configurations possibles de l'architecture DCC ont été identifiées selon le mode de fonctionnement de la station ITS (canal unique ou plusieurs canaux), ainsi que la configuration des paramètres d'entrée de l'algorithme DCC (local ou local& global). Le tableau 3.1 décrit les différentes configurations possibles [17].

La spécification du comportement du DCC-CROSS demeure dans sa capacité à supporter l'interopérabilité entre les différentes configurations DCC. Pour toutes les configurations, ils supposent qu'une mesure de la charge du canal (CL) est fournit par le composant radio ITS-G5. Cette dernière constitue l'entrée principale de l'algorithme DCC. L'entité DCC traite l'information concernant la charge du canal (CL) et fournit à l'algorithme DCC un taux d'occupation du canal radio (CBR). Toutes les configurations DCC énumérés dans le tableau 3.1, fournissent la valeur locale de CBR et supportent une opération à canal unique. Dans les configurations DCC 2 et 4, des paramètres globaux sont également disponibles [42]. En utilisant des paquets SHB (Single-Hop Broadcast) du protocole GeoNetWorking, la station ITS peut diffuser des informations sur son CL local, le CL le plus élevé reçu de ses stations voisines , son taux actuel de messages , sa puissance de sortie, etc. Lorsque ces paramètres d'entrée globaux sont disponibles, ceux-ci sont enregistrés dans la table de localisation du protocole GeoNetWorking. Ci-après les configurations DCC sont détaillées.

DCC configuration-1 : Dans cette configuration, la station ITS utilise un seul canal de communication et reçoit en entrée des paramètres locaux de DCC . Le calcul des ressources

TABLE 3.1 – Les différentes configurations de l'architecture DCC (ETSI TR 101 612)

	Canaux supportés		Paramètres en entrée	
	Unique	Multi	Local	local&global
DCC configuration-1	X		X	
DCC configuration-2	X		X	X
DCC configuration-3	X	X	X	
DCC configuration-4	X	X	X	X

disponibles sur le canal est basé seulement sur la mesure de la charge du canal (CL). La valeur CL mesurée est transformée à un paramètre DCC et transférée à la couche Access et la couche Facilities. Cette dernière attribue des niveaux de priorité aux différents paquets.

DCC configuration-2 : La station ITS utilise un seul canal de communication, mais elle a accès à des paramètres d'entrées locales et globales. L'ajout des paramètres DCC globaux permet d'aligner les différents paramètres de l'algorithme DCC au reste des stations ITS dans la même couverture de transmission. Ces paramètres globaux sont sauvegardés dans une table de voisinage au niveau de la couche Networking&Transport [42].

DCC configuration-3 : Dans ce cas, la station ITS a la capacité de basculer entrer les différents canaux mais elle n'a accès qu'aux informations DCC locales. Lors du déploiement des configurations multi-canaux, quand la charge autorisée d'un canal est dépassée, les mécanismes DCC peuvent inclure le déchargement des messages d'un canal congestionné vers autre moins chargé. Sachant que, cela nécessite un monitoring sur tous les canaux.

DCC configuration-4 : La station ITS a la capacité de basculer entre les différents canaux, avec un accès aux différentes informations DCC globales.

Contrairement à l'évaluation du paramètre DCC à canal unique, la table de voisinage, telle que la table de GeoNetWorking, contient les paramètres DCC globaux pour chaque canal monitoré. Les paramètres DCC internes sont évalués pour chaque canal en se basant sur des paramètres DCC globaux.

Les types d'algorithmes DCC

D'après le standard ETSI, diverses approches pour le contrôle de la congestion décentralisée (DCC) existent. Parmi-eux celles qui utilisent CBR comme paramètre d'entrée. D'une manière générale, deux types de classes DCC peuvent être identifiées, appelées réactives et adaptatives.

Les algorithmes DCC réactifs : Le cas d'un algorithme réactif, comme illustré sur la figure 3.2 une fonction DCC utilise directement CBR pour déterminer la valeur actuelle d'une ou plusieurs variables de contrôle, tel que le taux des messages, la puissance de transmission, etc. Ces variables influent sur le comportement de la communication, ainsi donc sur la valeur de CBR. La valeur de CBR observée par une station ITS est une fonction d'agrégation de

comportement de la communication de toutes les autres stations autour d'elle. Une fonction DCC compare la valeur actuelle de CBR à une valeur cible, puis utilise la différence entre ces deux, l'erreur d'adaptation, pour régler une ou plusieurs variables de contrôle.

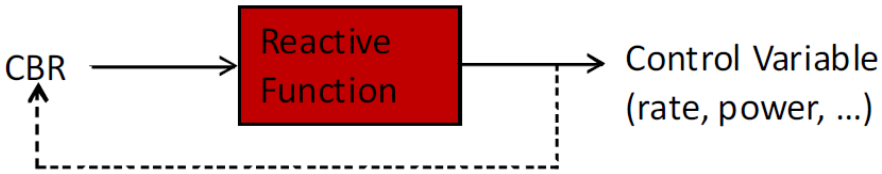

FIGURE 3.2 – Fonction DCC Réactive [17]

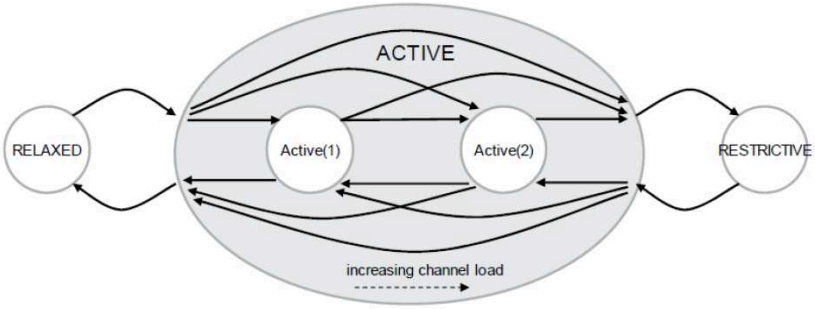

FIGURE 3.3 – Les états du mécanisme réactif DCC

Comme illustré sur la figure 3.3, le DCC réactif définit les différents états pour la charge du canal [26], à savoir relaxed, actif, et restrictif, où la métrique de charge du canal (CL) est la plus petite pour un état relaxed et la plus grande pour un état restrictif. L'état actif peut être divisé en plusieurs états. La charge du canal est mesurée en tant qu'un canal occupé (CBR), qui est le rapport du temps pendant lequel le canal est aperçu comme occupé pendant l'intervalle de monitoring. Dans le cas où le taux des CAMs est le paramètre de communication cible du reactif DCC, dans ce cas, la valeur de l'intervalle des CAMs est définie pour chaque état de charge du canal, comme représenté dans le tableau 3.4.

Les algorithmes DCC adaptatifs : Dans la classe des mécanismes DCC adaptatifs , deux catégories d'algorithmes adaptatifs existent : le Contrôle Binaire (Binary Control) et le Contrôle Linéaire (Linear Control). Ce label se réfère à la manière dont l'erreur d'adaptation est utilisée afin de modifier les variables de communication. Le contrôle binaire ne considère que le signe arithmétique de l'erreur, c'est-à-dire si le CBR est supérieur ou inférieur à la valeur de CBR cible. Un contrôle linéaire utilise la précision complète de l'erreur d'adaptation, à la fois le signe et la grandeur. Contrairement à la fonction réactive, la fonction adaptative utilise non seulement l'erreur d'adaptation, mais aussi le contrôle préalable des valeurs des variables comme illustré sur la figure 3.4.

De nombreux exemples d'algorithmes de contrôle adaptatif binaire existent. L'algorithme le plus connu est AIMD (Additive Increase Multiplicative Decrease) [86], dont une variante fait

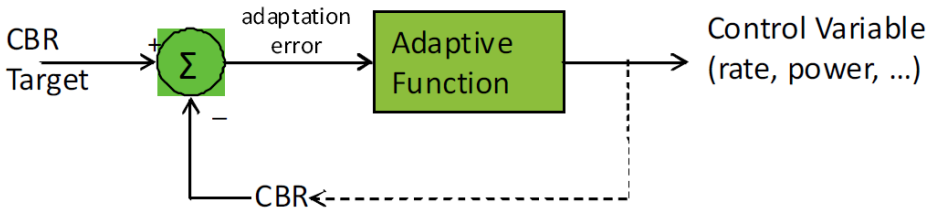

FIGURE 3.4 – Fonction DCC adaptative [17]

partie du protocole TCP (Transmission Control Protocol). Dans l'algorithme AIMD, si l'erreur est positive (CBR_{target}> CBR (t)), il est souhaitable que la valeur de CBR augmente, donc la variable de contrôle est élevée par un décalage additif (AI) indépendant de la valeur actuelle. Dans le cas d'une valeur d'erreur négative, la valeur de CBR devrait diminuer et la variable de contrôle est réduite à une fraction donnée (MD) de sa valeur actuelle. Le principe AIMD est illustré dans l'équation 3.1, pour le cas où un périphérique j adapte sa variable de fréquence R_{tx} (t) au fil du temps :

$$\begin{aligned} si : CBR(t) \leq CBR_{target} : R_{tx}(t+1) &= R_{tx}(t) + AI \\ sinon : R_{tx}(t+1) &= MD \times R_{tx}(t) \end{aligned} \tag{3.1}$$

Un exemple de contrôle adaptatif linéaire est l'algorithme LIMERIC [29], qui se base sur l'équation 3.2 de mise à jour pour le taux r(t) au périphérique j avec α, β comme paramètres de l'algorithme.

$$R_{tx}(t+1) = (1-\alpha) \times R_{tx}(t) + \beta \times (CBR_{target} - CBR(t)) \tag{3.2}$$

Comme mentionné précédemment, le framework DCC de ETSI permet aux stations ITS (ITS-S) d'adapter leurs paramètres de communication comme le taux de génération des messages CAM, la puissance de transmission et le taux de transmission des données, le seuil de la porteuse (carrier sense threshold) basé sur le taux d'occupation du canal radio mesuré par CBR. Un certain nombre d'algorithmes DCC incluant Reactive-DCC [17, 26], LIMERIC [29] et le contrôle adaptatif (AIMD) [86] ont été proposés pour contrôler le taux de génération des messages CAM au niveau de la couche Facilities. La principale différence entre les algorithmes réside dans leur façon de contrôler le taux de génération des CAMs. Le réactif DCC contrôle le taux de génération des CAMs suivant des paramètres dans une table. Le contrôle de taux de génération des CAMs avec LIMERIC est basé sur un algorithme d'adaptation linéaire. L'algorithme AIMD contrôle le taux de génération des CAMs d'une manière similaire à TCP.

3.3.2 Contrôle de la Congestion Distribuée : DCC

Le problème de la congestion du canal dans les systèmes IEEE 802.11p a été bien abordé dans la littérature. Un certain nombre d'études ont rapporté que la diffusion périodique des messages CAM par véhicule peut facilement conduire au problème de la congestion du canal

[26, 82, 18, 29]. Comme mentionné précédemment, ETSI a spécifié un framework de contrôle de la congestion distribuée (DCC), dans lequel chaque station ITS (ITS-S, nœud dans le réseau de véhicules) mesure la charge du canal en fonction du taux de charge du canal (CBR) et adapte les paramètres de communication tels que le taux de génération des messages CAM, la puissance d'émission et le débit, carrier sense threshold, etc. [17]. Il a été démontré que seul le contrôle du taux de génération des messages CAMs peut atténuer la congestion du canal [18, 29, 83]. Cependant, étant donné qu'une grande réduction du taux de génération CAM peut avoir un impact négatif sur la sécurité routière, il est souhaitable de contrôler d'autres paramètres en parallèle.

Les auteurs de [26] ont comparé les impacts de contrôle des différents paramètres et ont montré qu'en ajoutant un contrôle sur le taux de génération des messages CAMs et la puissance de transmission, ceci peut considérablement réduire la charge du canal radio. Lorsqu'il est nécessaire d'envoyer les paquets DENM, les DENMs introduisent encore plus de charge au canal sans fil et, par conséquent, il faut prendre en compte le contrôle de la congestion du canal lorsque les deux messages DENM et CAM partagent le canal sans fil.

Les algorithmes qui contrôlent les paramètres au niveau de la couche accès, tels que la puissance de transmission, le débit, carrier sense threshold, etc., [26] sont également applicables aux paquets DENM. Cependant, comme mentionné précédemment, ces algorithmes n'entraîneraient pas nécessairement un impact positif sur la transmission des paquets DENM, qui nécessitent souvent un transfert sur plusieurs sauts. Par exemple, le contrôle de la puissance de transmission ou le débit de données réduirait la portée de communication (par saut) et donc augmente le nombre de sauts pour les messages DENM qui peuvent entraîner par conséquent une charge plus élevée et des performances plus faibles. Par conséquent, nous pensons que pour les paquets DENM, il est important de considérer la congestion du canal lors de la conception du mécanisme d'acheminement de ces messages DENM. Sachant que, très peu d'efforts ont été faits au niveau de la couche réseau. En effet, comme dans [84], la majorité des efforts existants sur DCC y compris ceux de la couche d'accès, sont conçus dont l'idée est de cibler les messages CAMs et pour évaluer de telles applications.

Les auteurs de [82] ont classé les mécanismes de contrôle de la congestion en trois classes. La première classe est un contrôle de congestion réactif qui utilise des informations sur l'état de la congestion du canal pour décider si et comment une action doit être prise. La deuxième classe est un contrôle de congestion proactif qui utilise des modèles, qui se basent sur des informations telles que le nombre de nœuds, etc. Les auteurs estiment les paramètres de transmission qui ne conduiront pas à congestionner le canal . La troisième classe est le contrôle de la congestion hybride qui combine les avantages des approches proactives et réactives.

Au niveau de la couche Accès, Aygun et al. [27] propose un algorithme adaptatif de contrôle de la puissance, qui détermine la puissance de transmission pour un environnement routier donné. L'algorithme est combiné avec le LIMERIC [29] afin que les messages CAM soient contrôlées à la fois au niveau de la couche Facilities et au niveau de la couches Accès.

Andreas et al. [25] ont proposé un algorithme DCC qui utilise le DCC-gatekeeper, qui réside entre les couches réseau et la couche Accès et qui permet de contrôler la fréquence de transmission des paquets. Contrairement à notre schéma proposé, CBF2C, qui repose sur la couche réseau en contrôlant directement les paramètres d'acheminement en fonction de l'état de charge du canal.

3.3.3 Protocoles de routage dans VANET

Outre la mobilité, les topologies de réseau trop sparse ou trop denses créent de grands défis dans la transmission d'un paquet. La manière la plus simple pour la transmission des paquets est la diffusion en broadcast, ce qui mène au problème de broadcast storm plus particulièrement dans un réseau dense. Pour atténuer à ce problème de broadcast storm, dans [89], les auteurs ont étendu le protocole de routage AODV (Ad hoc on demand vector routing) pour inclure le mécanisme de broadcast et étudient comment le réseau se comporte sous différentes densités de trafic. Ils ont proposé trois techniques de suppression probabiliste et basées sur un compteur (timer-based broadcast) : le schéma weighted p-persistence, slotted 1-persistance et slotted p-persistence. La probabilité de transmission du paquet est calculée en fonction de la distance relative entre les nœuds ou bien de la force du signal reçu (RSS) du paquet et la portée moyenne de transmission.

Le protocole Pro-AODV (Proactive AODV) [63] est également proposé, ce dernier utilise des informations de la table de routage de AODV et un schéma probabiliste où la probabilité p (la probabilité de suppression du paquet) est calculée à partir d'une densité locale n (nombre de nœuds). Ce schéma a l'inconvénient que p est basé sur un paramètre statique comme le nombre de voisins. Dans [80], les auteurs proposent un mécanisme dans lequel les nœuds avec un espace tampon (buffer) plus important, sont sélectionnés comme nœuds transmetteurs. dans le cas où, l'espace de mémoire tampon (buffer) d'un nœud est suffisant, le message est transmis à ce dernier, autrement le message ne sera pas envoyé.

En raison du changement rapide de la topologie dans les réseaux de véhicules, Le transfert multi-saut (routage) a toujours été un sujet de recherche difficile. Un certain nombre d'algorithmes *carry-and-forward* incluant TBD [61], VADD [93] et DiRCoD [81], proposés pour des topologies de réseau sparse permettant aux véhicules de grader les paquets jusqu'à ce qu'ils rencontrent d'autres véhicules afin de leur transmettre les paquets reçus. Les approches de type *carry-and-forward* ne sont pas adaptées aux applications avec des exigences strictes en terme de délai, telles que le freinage d'urgence. Évidemment, si le réseau est trop sparse, la congestion du canal ne serait pas un problème. La congestion de canal devient un problème dans des topologies de réseau connectées (dense) qui nécessitent des mécanismes de type *carry-and-forward*. Le mécanisme de type *carry-and-forward* le plus simple et probablement le plus robuste est Flooding, dans lequel chaque nœud qui se trouve géographiquement entre la source et la destination retransmet le paquet [76, 89]. Le problème majeur de Flooding réside dans sa génération d'un grand nombre de retransmissions redondantes menant au problème d'inondation (broadcast storm problem) du réseau (c'est-à-dire au problème de congestion du canal) [76, 89].

Un grand nombre d'algorithmes d'acheminement sont proposés et peuvent être classés en deux catégories basant sur la décision de transmission du paquet soit prise au niveau de l'expéditeur ou du récepteur. Les algorithmes incluant GPSR [64], GPCR [70], ToGo [68] appartiennent au groupe, dans lequel les expéditeurs sélectionnent les prochains nœuds transmetteurs en fonction de la position des nœuds [64] et de la topologie routière [70, 68], en utilisant les messages de contrôle (beacon) échangés entre les véhicules. Les mécanismes de transfert multi saut basés sur la contention (CBF) [48, 47, 66, 50] se comportent de manière plus opportuniste dans le sens où ils ne nécessitent pas de nœud pour identifier

leurs voisins, car ce sont les nœud récepteurs qui décident de transférer ou non le paquet en utilisant un compte à rebours (Wait-Time). Gonzalez et Al. [50], proposent PDB (Preset Delay Broadcast protocol), un protocole de diffusion avec un délai fixe pour les véhicules tentant de retransmettre un message d'avertissement, ce qui offre une diffusion rapide et fiable. Ils ont montré que, en réglant de manière adéquate le temps d'attente pour les nœuds candidats relais, les performances peuvent être significativement améliorées, tout en préservant une bonne fiabilité.

Dans [69] GeOpps (Geographical Opportunistic Routing for Vehicular Networks) , les auteurs proposent un nouvel algorithme de routage avec délai toléré (DTN). Cet algorithme exploite la disponibilité des informations à partir du système de navigation (SN) pour acheminer d'une façon opportuniste un paquet de données à un certain emplacement géographique. L'avantage de SN est le fait qu'il sélectionne les véhicules intermédiaires les plus proches de la destination pour porter l'information. Une fonction est utilisé pour estimer le temps minimum pour que le paquet atteigne la destination en passant par le véhicule qui est considéré comme un le point le plus proche de la destination. Ce protocole dépend de la topologie du réseau.

Dans [71] (Opportunistic Geocast in Disruption-Tolerant Networks) ils se concentrent sur le transfert geocast d'un message vers une zone ciblée. Ce routage se base sur la mobilité statistique. L'approche Flooding simple est remplacée par l'estimation de temps de séjour afin de permettre aux nœuds de choisir les meilleurs transporteurs vers la zone de destination. En d'autres termes, un message de geocast n'est remis qu'au nœud ayant un plus grand taux de séjour vers leurs régions de destination. L'idée de base est d'utiliser une approche de routage SCF (multi-copy-based) pour délivrer le message geocast à la région de destination. Dans le but de surmonter l'incertitude de la mobilité de nœud et le changement de topologie.

Bien que ces algorithmes de transfert des paquets en multi-sauts créent de la charge relativement faible par rapport à Flooding, aucun d'entre eux n'est intentionnellement conçu pour contrôler la congestion du canal.

Nous nous sommes intéressés au problème de la congestion du canal lorsque les paquets DENM et CAM partagent le canal sans fil. Ciblant ces scénarios, nous proposons d'améliorer l'algorithme de transfert des paquets standardisés par ETSI, à savoir CBF, en introduisant un mécanisme de contrôle de la congestion distribué (DCC) du canal, conçu pour s'adapter à l'architecture ETSI-DCC [17]. Dans les sections 3.5 et 3.6, plus précisément, nous proposons nos algorithmes de transmission multi-sauts, nommés CBF2Cv1 et CBF2Cv2, qui sont des versions améliorées de l'algorithme CBF, qui adaptent le nombre de retransmissions redondantes en fonction de l'état de charge du canal.

3.4 Préliminaires

3.4.1 Aperçu du scénario

Nous supposons que des données sont envoyées d'Internet vers des zones géographiques en passant par des unités bord de route (RSU). Les véhicules à porté des RSUs et qui se trouvant dans ces zones concernées, à leurs tour vont disséminer ces données aux véhicules voisins.

Comme l'illustre la Figure 3.5, de nombreuses applications ITS nécessitent des transmissions de messages DENM, y compris l'information sur le trafic, les changements brusques de la météo, les collisions, etc. La majorité de ces types d'informations nécessitent un transfert multi-sauts des paquets DENM. Dans ce chapitre, nous introduisons des algorithmes d'acheminement de paquets en multi-saut qui peuvent être utilisés pour la diffusion de paquets DEMN dans VANET. Pour ce faire nous étudions différents algorithmes de routage pour la transmission multi-saut des paquets DENMs qui sont standardisés par ETSI, afin d'identifier leurs points forts et leurs faiblesses.

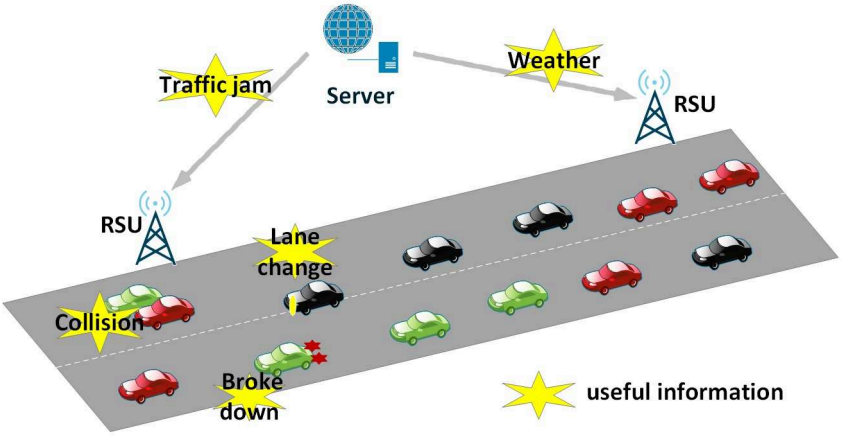

FIGURE 3.5 – Description du scénario

3.4.2 Flooding et Flooding amélioré

Parmi les schémas de transmission des paquets en multi-saut, y a l'approche Flooding , dans laquelle chaque nœud situé entre le nœud source et le nœud destination retransmet le paquet, est extrêmement robuste dans les topologies de réseaux dynamiques. Cet avantage provient de sa simplicité et de ses retransmissions redondantes. La création d'un nombre important de duplications de paquets constitue le déficit majeur de l'approche Flooding, entraînant des collisions et la congestion dans les réseaux à forte densité.

Une analyse de l'impact des retransmissions redondantes sur la couverture additionnelle a été faite. Dans [76], dans un premier temps, les auteurs calculent le nombre de nœuds qui bénéficient d'une retransmission du paquet, basant sur un scénario où un nœud B retransmit le paquet reçu de nœud A (3.6). Les résultats montrent qu'une retransmission peut apporter jusqu'à 61% de couverture supplémentaire par rapport à celle déjà couverte par la transmission précédente (en moyenne 41%). La seconde étude illustrée sur la figure 3.6, où le paquet de nœud A est retransmis par B (1ère transmission), puis par C (2ème retransmission), etc. La couverture supplémentaire attendue par la K ième retransmission du paquet est inférieure à 5% lorsque $k \geqslant 4$.

L'augmentation du nombre de retransmissions redondantes influence sur la couverture additionnelle qui se dégrade et sur la probabilité des collisions qui augmente. Selon l'état du canal, la probabilité de collision est de 100% dans le cas d'un canal en repos et de 50% quand

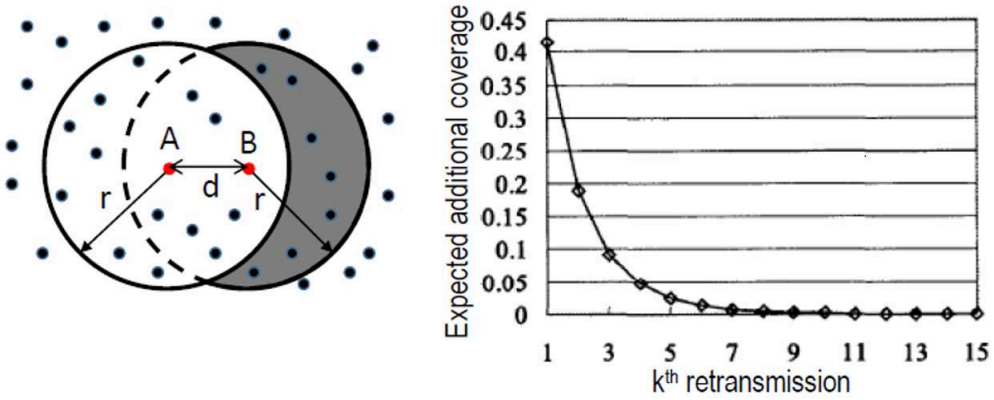

FIGURE 3.6 – Couverture additionnelle [76]

ce dernier est occupé.

L'approche Flooding crée également des accès synchronisés au canal, c'est-à-dire des collisions entre les paquets. Cela est du au fait que plusieurs nœuds reçoivent et renvoient le même paquet simultanément . Le problème est sévère, en particulier lorsque le réseau est sparse où le protocole MAC (Medium Access Control) prend immédiatement la procédure d'accès au canal, c'est-à-dire l'accès au canal sans invoquer le backoff [57] .

Ce dernier problème peut être facilement résolu en utilisant une minuterie de compte à rebours (wait time) afin d'asynchroniser les opérations de transmission d'un paquet en optant pour l'approche FloodingAdv (Flooding amélioré), où chaque nœud situé géographiquement entre la source et la destination, s'il reçoit les données, il retransmet le paquet de données après l'expiration de sa minuterie (la fonctionnalité de FloodingAdv est décrite dans Algorithme 1).

Algorithme 1 : L'algorithme FloodingAdv

- Le nœud N reçoit un paquet pour la première fois
Si (N est positionné entre la source et la zone de destination) **alors**
  Le nœud N déclenche un compte à rebours avec une valeur wt tirée au hasard dans l'intervalle [0, WT_{max}].
Fin si
Si (wt expiré) **alors**
  re-transmission du paquet()
Fin si

La figure 3.7 illustre la fonctionnalité de FloodingAdv. Dans l'exemple, deux nœuds $N1$ et $N2$ reçoivent un paquet de la source au même temps. Au lieu de le retransmettre directement (le principe de Flooding), avec FloodingAdv (comme on le voit dans l'Algorithme 1), les deux nœuds déclenchent des temps d'attente différents et ils retransmettent le paquet à l'expiration de leurs temps d'attente. De cette façon, la collision entre les paquets transférés de N1 et N2 est évitée.

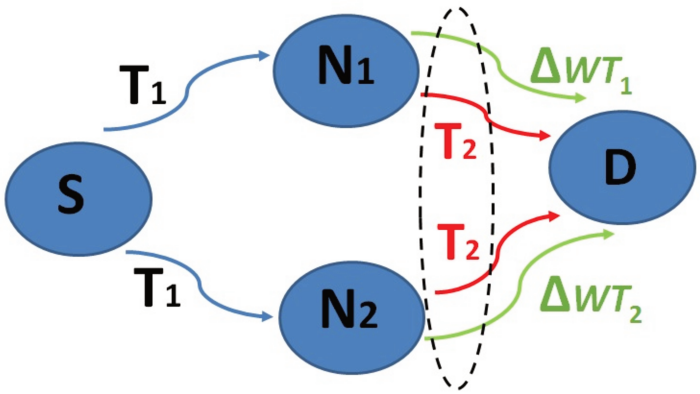

FIGURE 3.7 – Exemple avec FloodingADV

3.4.3 CBF et CBF-RT

ETSI a standardisé d'autres algorithmes de routage multi-saut basés sur la contention, à savoir CBF (Contention Based Forwarding) et l'amélioration de CBF nommé CBF-RT (Contention Based Forwarding with Retransmission Threshold).

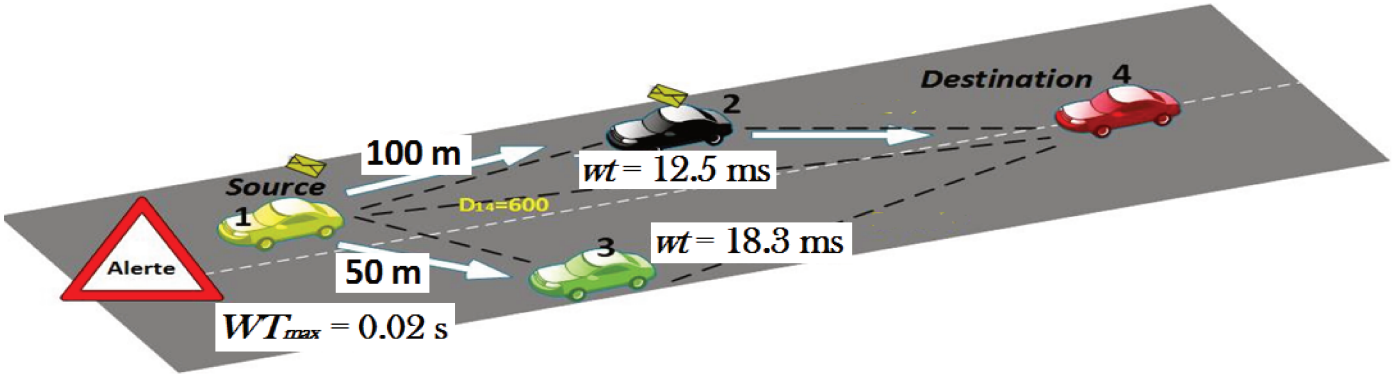

FIGURE 3.8 – Exemple avec CBF

La retransmission des paquets basée sur la contention, comme CBF [66], utilise un compte à rebours (countdown timer) pour éliminer les retransmissions redondantes, évitant ainsi le problème d'inondation du réseau (broadcast storm problem). Lors de la réception d'un paquet, chaque nœud candidat à la retransmission mets en place une minuterie (wait time) avant l'envoi du paquet, et seul le nœud, dont la minuterie a expiré en premier, envoie le paquet, tandis que d'autres nœuds abandonnent la retransmission dès qu'ils détectent que le paquet a été déjà retransmis par un nœud voisin. La valeur de la minuterie est définie de telle sorte que le nœud le plus éloigné de la source émette le premier, par exemple :

$$wt = WT_{max}(1 - \frac{d_{SN}}{d_{SD}}). \tag{3.3}$$

Le WT_{max} est le temps d'attente maximum, d_{SN} et d_{SD} sont les distances entre le nœuds source et le nœuds récepteur, ainsi que la source et la destination, respectivement.

L'algorithme CBF est sans procédure de Beaconing c'est à dire que les nœuds n'envoient pas des informations sur leurs positions. En plus, la décision de transmission du paquet est faite au niveau de récepteur autrement dit, chaque nœud décide s'il envoi ou pas.

Un exemple sur la figure 3.8 illustre le principe de l'algorithme CBF. Un véhicule source 1 qui détecte un obstacle sur la route calcule deux timers (un pour le véhicule 2 et l'autre pour le véhicule 3) en se basant sur la formule 3.3 où WT_{max} = A = 0.02 secondes, d_{SD} = 600 mètres, etc., pour le véhicule 2 le timer obtenu est de 12.5 ms et 18.3 ms pour le véhicule 3. Dans cet exemple, le timer calculé pour le véhicule 2 (qui est le plus proche de la destination) expire en premier et donc, c'est à ce dernier de retransmettre le paquet reçu de la source. Le véhicule 3 écoute la retransmission de la part du véhicule 2 et abandonne le paquet.

Dans un cas idéal, CBF peut parfaitement éliminer le renvoi redondant, évitant ainsi la congestion. Cependant, cela signifie également que, puisqu'il n'y a pas de redondance, CBF est extrêmement sensible aux pertes de paquets. Notre intention est alors de proposer une approche qui profite à la fois des avantages des deux approches Flooding et CBF tout en tenant compte de l'état du canal.

Algorithme 2 : l'algorithme CBF-RT

```
- le nœud N reçoit un paquet
Si (N est positionné entre la source et la zone de destination) alors
  Si si c'est la première fois que le paquet est reçu alors
    RetransmissionCount=0
    déclenche un compte à rebours wt suivant l'équation 3.3.
  sinon
    RetransmissionCount++
    Si RetransmissionCount > RC_th alors
      annule le compte à rebours ; supprime le paquet
    Fin si
  Fin si
Fin si
Si (wt expiré) alors
  re-transmission du paquet ()
Fin si
```

Les auteurs de [66] ont proposé une approche CBF améliorée, appelée CBF-RT (renvoi basé sur la contestation avec l'introduction d'un seuil de retransmission). Comme décrit dans l'algorithme 2, dans CBF-RT, durant le compte à rebours (le temps d'attente) , le nœud compte le nombre de retransmissions du même paquet effectué par ses nœuds voisins. Si le nombre de retransmissions atteint le seuil RC_{th}, le nœud annule la minuterie (timer) et arrête la transmission du paquet. Enfin, il convient de mentionner que les deux algorithmes CBF et CBF-RT sont adoptés comme des protocoles GeoNetworking dans ETSI.

3.5 Proposition : CBF2Cv1

Nous proposons un algorithme de transmission multi-saut, CBF2Cv1, qui étend l'algorithme CBF avec la fonctionnalité de contrôle de la congestion. Plus précisément, CBF2Cv1 contribue au contrôle de la congestion suivant le Framework ETSI- DCC illustré dans la Figure 3.1. Identique aux autres algorithmes DCC [26, 18, 29], CBF2Cv1 surveille l'état de la charge du canal et adapte le nombre de retransmissions redondantes (le nombre de retransmissions). Le taux d'occupation du canal (Channel Busy Ratio) est une métrique commune utilisée pour caractériser la charge du canal [18]. CBR est le rapport du temps pendant lequel le canal était occupé pendant l'intervalle de surveillance du canal (ex. 100 ms), calculé comme suit :

$$CBR_N = \frac{T_{busy}}{T_{monitor}}. \tag{3.4}$$

Le CBR est mesuré localement par chaque nœud, CBR local, qui peut être échangé entre les nœuds pour calculer le CBR dans la zone de voisinage, CBR global [17]. Alors que le CBR global nécessite des communications entre les nœuds (consomme de la ressource radio, ajoute de la charge au canal). A ce jour, les avantages de CBR global par rapport au CBR local ne sont pas encore clairement identifiés. Pour cette raison, dans notre approche, nous appliquons le CBR local. L'approche CBF2Cv1 se compose de deux niveaux de contrôle :

La fonction du contrôle de seuil du nombre de retransmissions, le seuil du nombre de retransmissions, RC_{th}, est adapté suivant l'algorithme 3 :

Algorithme 3 : CBF2Cv1 avec la fonction de contrôle du seuil du nombre de retransmissions

- Le protocole CBF2Cv1 est informé de la valeur courante de CBR
Si ($CBR > CBR_{max}$) **alors**
  RC_{th}=MAX(1,RC_{th}-1)
sinon Si ($CBR < CBR_{min}$) **alors**
  RC_{th}=MIN(RC_{max},RC_{th}+1)
Fin si

Comme on le voit dans l'algorithme 3 et la figure 3.9, lorsque le taux d'occupation du canal (CBR) dépasse un seuil maximum RC_{max}, impliquant que le canal est saturé (congestionné), le nœud réduit le nombre des retransmissions redondantes (retransmissions redondantes). Si la valeur de CBR est inférieure à un seuil minimum RC_{min}, le nœud augmente le nombre de retransmissions. Sachant que le nombre de retransmissions, RC_{th}, prend une valeur dans l'intervalle [1, RC_{max}]. Par ailleurs, les auteurs de [76, 89] ont étudié l'impact des retransmissions redondantes sur la couverture supplémentaire en supposant que les nœuds ne transmettent pas en même temps (pas de collisions). Les résultats montrent que lorsqu'un certain nombre de retransmissions est supérieur à 4, la couverture supplémentaire attendue est inférieure à 5%, ce qui implique que plus de 4 retransmissions à chaque saut n'est pas nécessaire pour la transmission multi saut. Sur la base de cette étude, il semble que fixer RC_{max} à 4 est suffisant. Alors que la distance relative est généralement considérée pour calculer le temps

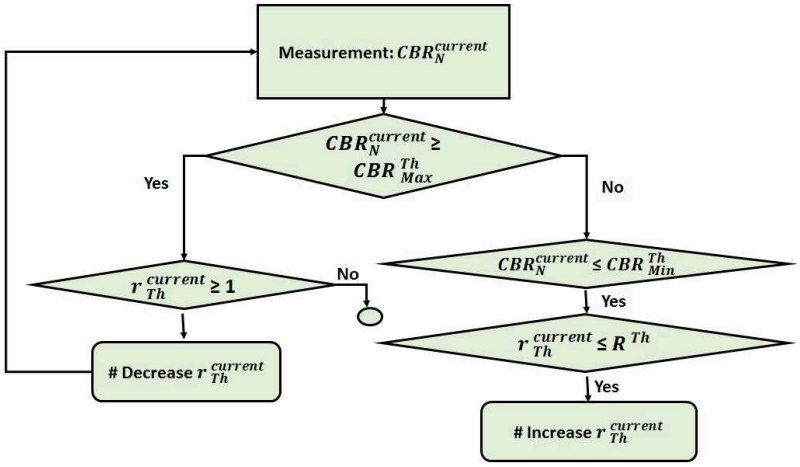

FIGURE 3.9 – La fonction du contrôle de seuil du nombre de retransmissions (Threshold Control Function)

d'attente (Wait Time) des nœud transmetteurs, l'équation peut conduire aux cas, où les nœuds qui se trouvent à proximité obtiennent un même temps d'attente (même valeur de timer) qui expire en même temps.

Par conséquent, nous proposons d'améliorer encore l'algorithme de sorte que le calcul du temps d'attente ne soit pas uniquement basé sur les distances entre le nœud et la source, ainsi que la source et la destination (voir (3.3), mais aussi sur le nombre des nœuds voisins, n, qui sont à une distance de Δd, comme suit :

$$wt = WT_{max}(1 - \frac{d_{SN}}{d_{SD}}) + \tau k. \tag{3.5}$$

Où k est un nombre entier pris au hasard dans l'intervalle [0, n] et τ est une valeur de temps fixe. Enfin, l'algorithme de transmission multi-sauts CBF2Cv1 est identique à celui de l'Algorithme 2 (CBF-RT), sauf que le RC_{th} se calcule en se basant sur l'algorithme 3 et que wt est calculé en se basant sur l'équation 3.5.

Contrôle de la retransmission, lors de la réception d'un nouveau paquet à transmettre, le nœud déclenche une minuterie de compte à rebours suivant (l'équation 3.5). Pendant le processus de compte à rebours (wt), le nœud compte le nombre de paquets reçus en double ($N_{duplicate}$) de la part de ses nœuds voisins. Dans le cas où la valeur de $N_{duplicate}$ est supérieure au nombre maximal des retransmissions permises ($r_{current}^{Th}$), le nœud abandonne la retransmission du paquet et annule sa minuterie. Sinon, le nœud attend l'expiration de sa minuterie et transmet le paquet. Ce contrôle du nombre de retransmissions se trouve à la Figure 3.10 Comme décrit précédemment, l'algorithme proposé applique une minuterie pour éviter le renvoi synchronisé et un nombre excessif de transmissions du paquet en double, tout en exploitant de la redondance tant que l'état du canal le permet. L'algorithme est décrit dans la figure 3.10.

Dans la section 3.6, nous proposons une amélioration de notre précédente approche, CNF2Cv1. Le schéma proposé, nommé CBF2Cv2, adapte les paramètres de transmission de

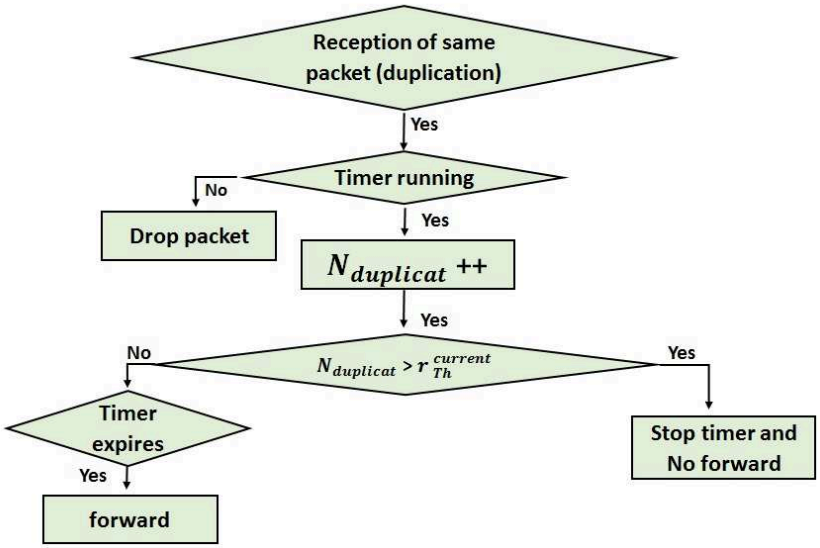

FIGURE 3.10 – L'approche CBF2Cv1

l'algorithme CBF-RT (à savoir, le wait time) en tenant compte de l'état de charge du canal.

3.6 Proposition : CBF2Cv2

3.6.1 Problématique : CBF2Cv1

Pour rappel, les auteurs de [65] proposaient le protocole CBF-RT (Contention Based Forwarding with Retransmission Threshold), une approche de transmission basée sur la contention avec un certain seuil de retransmissions, dans lequel la décision d'acheminement des paquets est prise suivant l'algorithme 2. Lors de la réception d'un paquet, chaque candidat destiné à la transmission définit un compte à rebours (wt) suivant la formule 3.5.

Dans cette approche, le WT_{max} est un paramètre fixe définissant le délai maximal de transfert du paquet. Les d_{SN} et d_{SD} sont respectivement, les distances entre la source et le nœud récepteur (candidat à la transmission du paquet), la source et la destination. Durant le processus de compte à rebours de la minuterie (wt), le nœud candidat compte le nombre de retransmissions du même paquet effectué par ses nœuds voisins. Si le nombre de retransmissions atteint une valeur d'un seuil fixe donné, le nœud annule son compteur à rebours (wt) et arrête la retransmission du paquet. Autrement, le nœud transmet le paquet. Dans un cas idéal, à chaque saut RC_{th} les nœuds les plus proches de la destination retransmettent le paquet. CBF-RT peut avoir une charge de canal très faible si RC_{th} est configuré sur une petite valeur et la charge augmente lorsque RC_{th} est réglé sur une grande valeur. De toute évidence, si RC_{th} est très petit, le protocole ne peut pas être assez robuste dans un réseau avec un fort changement de topologie, d'autre part, si RC_{th} est grand, le protocole peut induire à une énorme surcharge du canal (à la congestion).

Motivé par cela, dans [85] (avec CBF2Cv1), nous avons proposé un mécanisme DCC sur GeoNetworking au niveau de la couche réseau de la pile protocolaire ETSI ciblant CBF-RT,

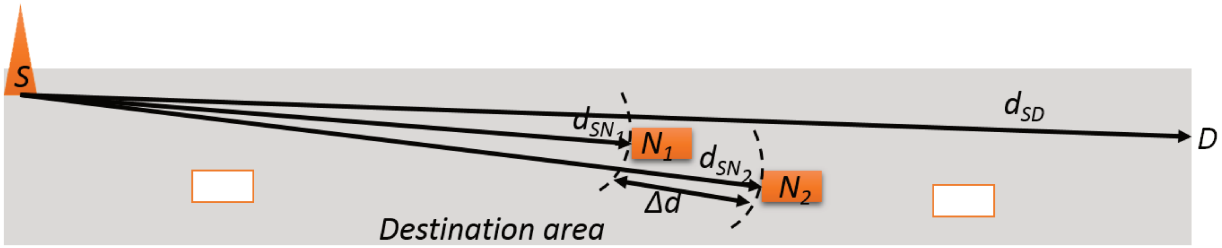

FIGURE 3.11 – Illustrant le calcul de wt à deux nœuds, N_1 et N_2.

dont le but est de contrôler le RC_{th} en fonction de l'état de la charge du canal. Suivant le Framework DCC, CBF2Cv1 adapte le nombre de retransmissions redondantes, RC_{th}, en fonction de CBR mesurée. Comme illustré dans l'algorithme 3, si la valeur de CBR dépasse un seuil maximum CBR_{max}, ce qui signifie que le canal est saturé, le nœud réduit le nombre de retransmission. Si la valeur de CBR est inférieure à un seuil CBR_{min}, le nœud incrémente le nombre de retransmissions. La valeur RC_{th} est contrôlée dans l'intervalle de [1, CBR_{max}]. Pour rappel, selon [76, 89], il semble suffisant de fixer CBR_{max} à 4, puisque la couverture supplémentaire qui fournit plus de quatre retransmissions est aussi faible que 5%. Une autre contribution avec notre précédente approche CBF2Cv1 était de réduire la probabilité de collision en utilisant une formule modifiée pour le calcul de wt illustrée dans l'équation 3.5. Bien que la motivation derrière cette modification soit déjà expliquée dans la section précédente, dans ce qui suit, la motivation est justifiée par la formulation du problème. Considérons que deux nœuds, $N1$ et $N2$, ont reçu un paquet DENM à transférer entre une source et une destination donnée. Dans le cas où les deux nœuds ($N1$ et $N2$) calculent le délai d'attente (wt) avant le transfert du paquet suivant l'équation 3.3, la différence entre les délais de transmission est calculée comme suit :

$$\Delta wt = WT_{max}\frac{d_{SN_1} - d_{SN_2}}{d_{SD}} \equiv WT_{max}\frac{\Delta d}{d_{SD}}, \tag{3.6}$$

Où d_{SN_1} (resp. d_{SN_2}) est la distance entre la source et le nœud N1 (resp. N2), N_1 (resp. N_2) et $\Delta d \equiv d_{SN_1} - d_{SN_2}$ (voir la figure 3.11). Afin de réduire efficacement le nombre de retransmissions dupliquées ainsi que d'éviter les collisions entre les paquets, Δwt ne doit pas être plus petit que le délai de transmission d'un paquet, τ . Par conséquent, afin d'éviter les collisions et la retransmission redondante, il est nécessaire que :

$$\Delta d > d_{SD}\frac{\tau}{WT_{max}}. \tag{3.7}$$

Avec WT_{max} à 20 ms et τ à 1 ms (ce qui correspond à peu près au délai de transmission d'une donnée de 600 octets en utilisant un taux par défaut de 6 Mbps de l'IEEE 802.11p), nous constatons que la condition est $\Delta d > 50$ m si $d_{SD} = 1000$ m. Cela implique que si deux ou plusieurs nœuds sont a une distance de 50 m (l'un de l'autre, voir la figure 3.11) reçoivent un message DENM, ils retransmettront le paquet presque simultanément, entraînant des collisions et des redondances inutiles. Dans les scénarios routiers à moyenne densité [17], nous pouvons facilement trouver deux véhicules dans la portée de 50 m (dans le système de coordonnées

polaires, dont le pôle est la position de la source). Malgré la faible densité de la route, si cette dernière comporte deux voies ou plus, deux ou plusieurs véhicules sont peut-être trouvés dans cette portée. Par conséquent, il existe une forte probabilité que la condition (3.7) se rencontre, de sorte que les retransmissions redondantes et / ou les collisions ne puissent être évitées dans des scénarios réalistes, si les paramètres mentionnés ci-dessus sont appliqués à l'équation 3.3.

Dans notre précédente approche CBF2Cv1 [85], le deuxième composant dans l'équation 3.5 est donc ajouté pour éviter les collisions des paquets et pour réduire les retransmissions redondantes. Plus précisément, le candidat à la transmission du paquet désynchronise le délai de transmission du paquet en ajoutant un délai aléatoire de τk à l'équation 3.3, sachant que , τ est une valeur fixe pour le délai de transmission d'un paquet et k est une valeur aléatoire prise dans l'intervalle de [0, n], où n est le nombre de voisins sur une distance de Δd.

Cette modification combinée avec l'algorithme 3 réduit efficacement les collisions de paquets et améliore les performances en terme de PDR par rapport à CBF-RT [85], comme l'équation 3.5 le montre, l'algorithme peut augmenter le délai de bout en bout (E2ED).

La section suivante est consacrée à ce problème et propose une amélioration de CBF2Cv1, nommée CBF2Cv2.

3.6.2 Principe de l'algorithme CBF2Cv2

La modification proposée de CBF2Cv1 dans l'équation 3.5 est établie afin de réduire les collisions entre les paquets, mais pas nécessairement avec l'esprit de contrôle de la congestion. Une autre faiblesse de la modification, comme on peut le voir facilement en comparant l'équation 3.5 avec 3.3, en raison de l'ajout du deuxième composant dans l'équation 3.5, le délai de transfert (E2ED) des paquets peut être plus long.

Dans cette section, nous proposons un algorithme CBF2C amélioré, nommé CBF2Cv2, qui contrôle deux paramètres de transmission de l'algorithme CBF-RT, à savoir, le délai d'attente maximal (WT_{max}) et le seuil du nombre de retransmissions (RC_{th}), pour les deux objectifs qui sont le contrôle de la congestion et l'évitement de collision, tout en assurant un délai de transmission plus court ou égal à celui obtenu avec l'algorithme CBF-RT.

En effet, nous notons qu'au lieu d'ajouter le deuxième composant de l'équation 3.5, un objectif similaire peut être obtenu en adaptant dynamiquement la valeur de WT_{max} (voir l'équation 3.3) en fonction de la valeur de CBR, contribuant à DCC. L'algorithme CBF2Cv2 est illustré dans la Figure 3.12 et représenté dans l'algorithme 4.

Comme illustré sur la figure, CBF2Cv2 a trois états opérationnels qui correspondent à l'état de charge du canal à savoir *léger*, *normale* et *congestionné*. La charge du canal est considérée comme légère, lorsque le CBR mesuré est inférieur à un seuil CBR_{min} donné. Lorsque l'état du canal est détecté comme étant *léger*, le nombre de retransmissions RC_{th} est incrémenté (RC_{th}= MIN(RC_{th}+1, $maxRC$)) pour permettre une redondance plus élevée et WT_{max} est réduit (WT_{max}=MAX($\beta \times WT_{max}$, $minWT$), avec $\beta \in]0, 1[$ pour un délai de transmission plus court. Lorsque l'état du canal est *normale*, c'est-à-dire que le CBR mesuré est dans l'intervalle [CBR_{min}, CBR_{max}], les valeurs WT_{max} et RC_{th} réelles sont conservées, étant donné qu'elles sont appropriées. Enfin, si le canal est considéré saturé, c'est-à-dire que le CBR mesuré dépasse le CBR_{max}, l'algorithme réduit le seuil de nombre de retransmission (RC_{th}= MAX(RC_{th}-1, 1)) et augmente le WT_{max} (WT_{max}=MIN($\alpha \times WT_{max}$, $maxWT$), $\alpha > 1$) pour éviter les

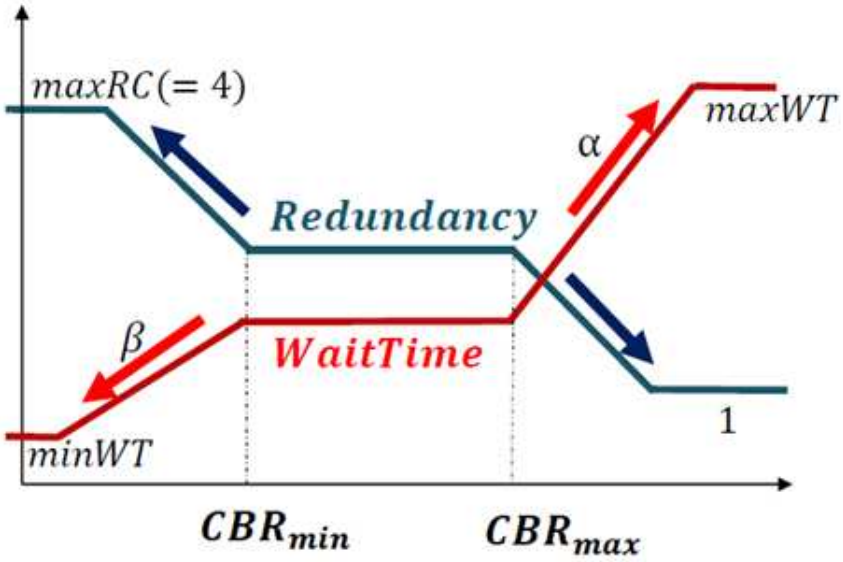

FIGURE 3.12 – Contrôle des paramètres de transfert.

collisions et les retransmissions redondantes.

Algorithme 4 : CBF2Cv2 avec le contrôle de nombre de retransmissions (RC_{th}) et la valeur de contention (WT_{max})

- CBF2Cv2 est informé de la valeur courante de CBR

Si ($CBR > CBR_{max}$) **alors**

- Congestionné : réduire la redondance, augmenter le temps d'attente (WT_{max})

RC_{th}=MAX(1,RC_{th}-1)

WT_{max}=MIN($maxWT$, α * WT_{max})

// α >1

sinon Si ($CBR < CBR_{min}$) **alors**

- Légère : augmenter la redondance, réduire le temps d'attente (WT_{max})

RC_{th}=MIN(RC_{max},RC_{th}+1)

WT_{max}=MAX($minWT$, β * WT_{max})

// 0 < β < 1

Fin si

Il convient de noter que le délai réel de transfert des paquets est calculé en utilisant l'équation 3.3, qui est en fonction de la distance et de WT_{max} (ce dernier est adapté en fonction de la valeur de CBR).

Afin de comprendre l'effet du CBF2Cv2 sur le délai de transmission, dans ce qui suit, nous comparons le temps d'attente, wt, calculé par chaque nœud récepteur et candidat à la retransmission pour chaque algorithme CBF2Cv1 et CBF2Cv2. Nous considérons une route à 6 lignes (3 voies par direction) défini dans [17] pour trois types de densité de véhicules, (0.01, 0.02 et 0.06 véhicules / m / voie) qui correspondent à des scénarios sparse, moyens et denses,

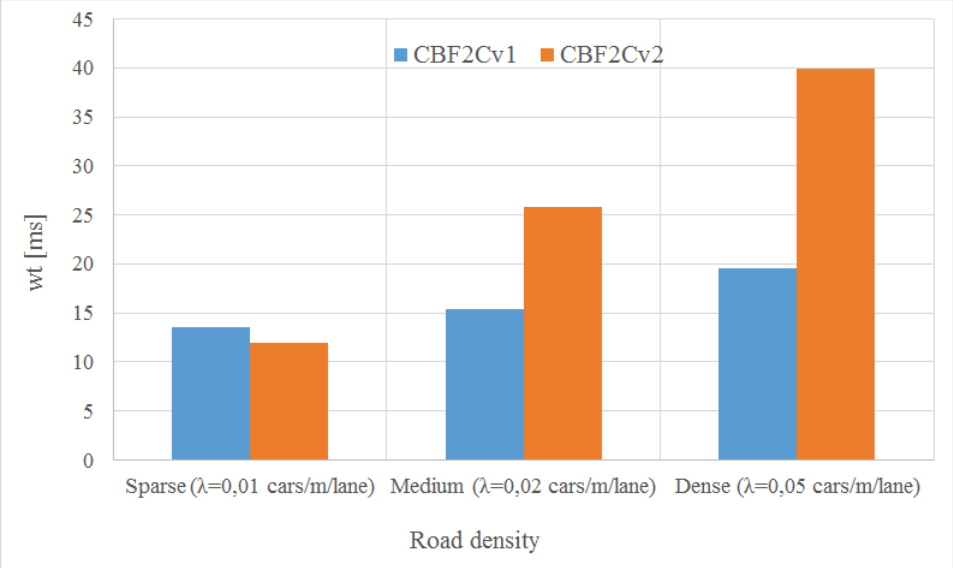

FIGURE 3.13 – Délai de transfert du nœud candidat à la transmission avec les algorithmes CBF2Cv1 et CBF2Cv2. d_{SD} = 1 Km, d_{SN} = 200 m.

respectivement [17]. Nous considérons que la distance entre la source et la destination, d_{SD}, est de 1 Km, et la source et le nœud candidat à la transmission, d_{SN}, est de 200 m. Le WT_{max} pour CBF2Cv1 à 20 ms, le wt moyen calculé en utilisant l'équation 3.5 est respectivement de 17.5, 19 et 23 millisecondes pour les scénarios sparse, moyens et denses. Notez que le wt calculé par l'équation 3.5 prend différentes valeurs pour différentes densités de route en raison du nombre variable de nœuds voisins, n dans l'intervalle de Δd (qui prend 50 m pour d_{SD} = 1 Km).

Le wt de CBF2Cv2 est calculé en utilisant l'équation 3.3, où WT_{max} varie en fonction de l'état du canal. Nos résultats de simulation révèlent que le CBR moyen prend 0.4, 0.7 et 0.8 pour les scénarios sparse, moyens et denses, respectivement, lorsqu'il n'y a pas de DCC sur les paquets CAM (voir la figure 3.26). Nous considérons alors que CBR prend une valeur dans la portée de ±0.2 autour des valeurs mentionnées ci-dessus pour dix (10) mesures consécutives et calcule le wt moyen pour CBF2Cv2 pour les différents types de densité. Le WT_{max} initial est à 0.03 s, WT_{min} et WT_{max} sont respectivement à 0.02 et 1 seconds. α et β sont fixés respectivement à 1.2 et 0.3.

La figure 3.13 compare wt du nœud candidat à la transmission pour CBF2Cv1 et CBF2Cv2. Comme le montre la figure, contrairement à CBF2Cv1, wt pour CBF2Cv2 prend des valeurs significativement différentes pour les scénarios sparse, moyens et denses, indiquant que l'algorithme prend clairement en compte l'état de charge du canal. L'impact sur l'état du canal est significatif vu que CBF2Cv2 contrôle à la fois WT_{max} et RC_{th}.

3.7 Évaluation de performances de CBF2Cv1 avec les messages DENM

Dans cette section, nous évaluons les performances de deux approches CBF2Cv1 et l'amélioration de Flooding (FloodingADV), en les comparant avec l'approche CBF. Dans cette première étude, nous considérons que les messages DENMs, sont échangés sur le canal radio sans l'introduction des CAMs. La mobilité des véhicules n'est pas introduite sous l'hypothèse que l'échelle de temps de transmission des messages est plus grande que celle du mouvement des véhicules.

3.7.1 Paramètres de simulation

Dans nos simulations, nous utilisons le simulateur réseau NS3. Les performances du schéma proposé (CBF2C) sont comparées à celles des deux algorithmes FloodingAdv et CBF. Suite à la suggestion de ETSI pour les évaluations des algorithmes de contrôle de la congestion décentralisée [17], une autoroute à 6 voies de 1 kilomètre avec les densités de véhicules de 11, 23, 51 et 101 véhicules/voie, est utilisée comme scénario de simulation (voir la Figure 3.18 et Tableau 3.2). La table. 3.3 répertorie les autres paramètres de simulation.

Dans les simulations, nous supposons qu'il a cinq RSUs (Road Side Unit), qui sont installées sur la ligne médiane de la route, séparées avec une distance de 200 mètres et diffusant des DENMs tous les 100 ms. La zone d'intérêt (RoI) pour les DENMs est l'ensemble de l'autoroute. Le CBR_{Max} et CBR_{Min} de l'algorithme CBF2C sont fixés respectivement à 70% et 55% [83]. Nous supposons que le nombre maximal de retransmissions R_{Th} est égal à 4 [76]. Le temps d'attente WT dans FloodingAdv est défini sur 5 ms et dans les approches CBF et CBF2C est fixé à 20 ms. Quatre paramètres de performance sont étudiés : taux moyen de paquets reçus (PDR), délai de transmission de bout en bout (E2ED), Surcharge (overhead) et taux d'occupation du canal radio (CBR), permettent de comparer les performances des trois algorithmes.

TABLE 3.2 – Paramètres du scénario routier

Classe	Inter-distance	Densité (Nœuds/Km)
Sparse	100 m inter-distance (3 lignes/ 2 directions)	11
Medium	45 m inter-distance (3 lignes/ 2 directions)	23
Dense	20 m inter-distance (3 lignes/ 2 directions)	51
Extreme	10 m inter-distance (3 lignes/ 2 directions)	101

TABLE 3.3 – Paramètres du simulation

Paramètres	Valeur
Scénario simulé	Autoroute
Zone simulée	$1000 \times 18 \ m^2$
Largeur de la voie	3 m
Bande passante du canal	10 Mhz
Inter-distance	10 - 100 m
Puissance de transmission	23 dBm
Modèle de propagation	Log-distance
L'exposant du modèle de propagation	2
Intervalle de surveillance de CBR	100 ms
Nombre de RSU	5

3.7.2 CBF2Cv1 avec CBF et Flooding amélioré

3.7.2.1 Le taux moyen de paquets reçus (PDR)

Le PDR (Packet Delivery Ratio) est défini comme le rapport des paquets qui sont envoyés avec succès à une destination dans la région d'intérêt (RoI) par rapport au nombre des paquets qui ont été envoyés par les sources. La figure 3.14 montre la PDR des trois algorithmes pour des densités de véhicules différentes. Comme on peut s'y attendre, en raison de l'augmentation de la charge du canal, la PDR obtenue par les trois protocoles diminue avec l'augmentation de la densité des véhicules. Néanmoins, CBF2C montre un PDR plus élevé par rapport aux algorithmes conventionnels, ce qui est possible grâce à la retransmission asynchrone et à la permission d'un certain niveau de redondance des transmissions. L'approche FloodingAdv montre un PDR élevé dans un scénario sparse, mais les résultats de PDR se dégradent dans des scénarios plus denses. C'est évidemment, en raison du problème de broadcast storm (broadcast storm problem).

3.7.2.2 Le délai de bout en bout (E2ED)

La deuxième métrique de performance, le délai de bout en bout (E2ED) qui se réfère au temps moyen pris pour une transmission de paquets de la source jusqu'à la destination. La figure 3.15 illustre l'impact de la variation de la densité du réseau sur le délai moyen de bout en bout . Afin d'éliminer les retransmissions redondantes, CBF a un temps d'attente relativement important WT_{max} (0,02 secondes) qui génère un long délai de transmission. En revanche, FloodingAdv utilise la minuterie (un temps d'attente) uniquement pour une retransmission asynchrone et, par conséquent, WT_{max} est configuré sur une petite valeur (0,005 secondes), ce qui entraîne un faible délai de communication. Enfin, alors que CBF2C a une configuration identique de WT_{max}, assure un délai plus court que celui de CBF. Il est concevable que c'est

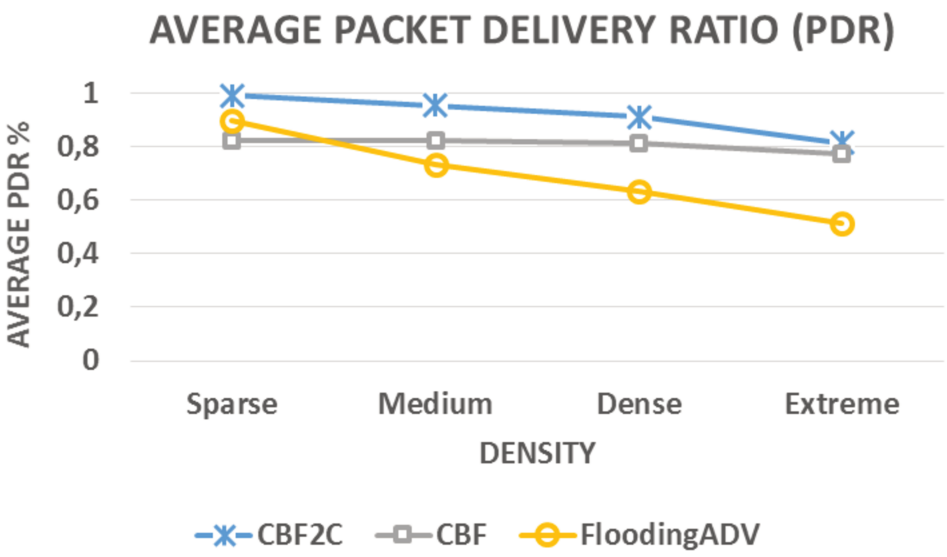

FIGURE 3.14 – Le taux moyen de paquets reçus

grâce à l'autorisation d'un certain niveau de redondance avec l'approche CBF2C.

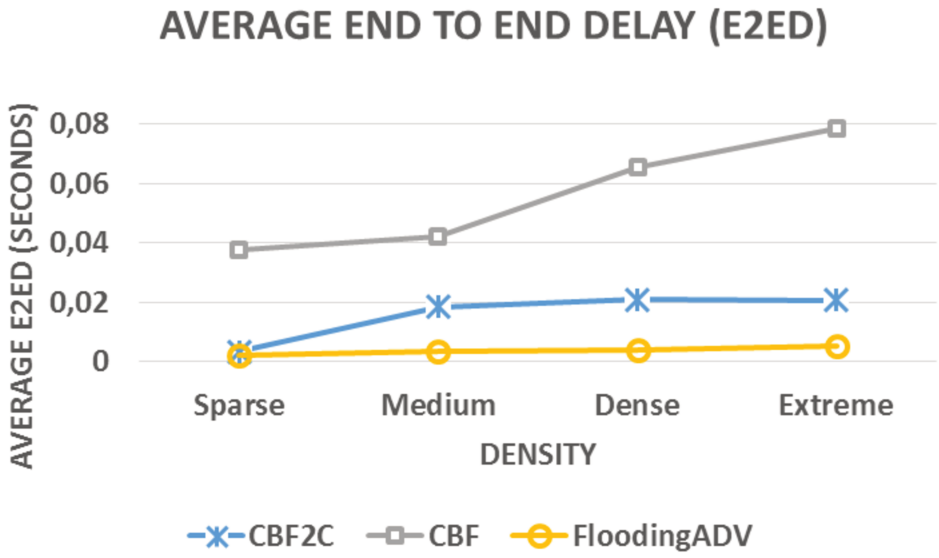

FIGURE 3.15 – Le Délai moyen

3.7.2.3 La surchage (Overhead)

La troisième métrique utilisée dans nos évaluations est la surcharge (overhead), qui est définie comme le nombre total de retransmissions durant le temps de simulation. La figure 3.16 compare les surcharges de chaque approche de transmission multi-sauts pour des densités de

réseau variables. tel qu'anticipé, CBF montre une faible surcharge. En revanche, FloodingAdv a une surcharge significativement élevée en raison de la redondance excessive utilisée au niveau de chaque véhicule (qui est le comportement idéal de Flooding). Enfin, l'approche CBF2C affiche une faible surcharge car elle permet un certain niveau de redondance se basant sur le contrôle du nombre de retransmissions en fonction de l'état du canal. Il convient de souligner que CBF2C offre d'excellentes performances en termes de PDR et de délai avec moins de surcharges.

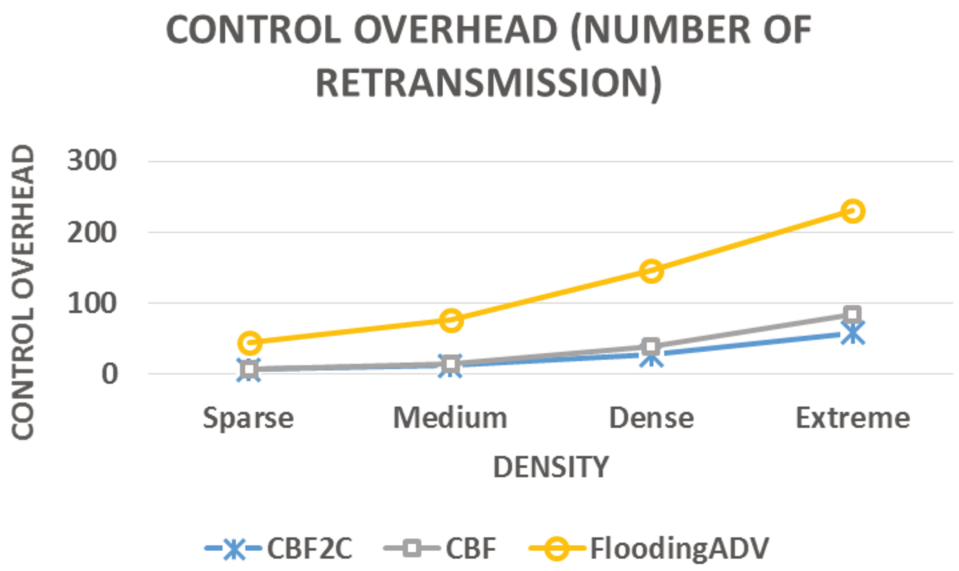

FIGURE 3.16 – Le contrôle de la surcharge

3.7.2.4 Le taux d'occupation du canal (CBR)

La quatrième métrique d'évaluation de performance est le taux d'occupation du canal (Channel Busy Ratio), CBR. La figure 3.17 compare le CBR moyen pour les trois algorithmes. Il faut d'abord noter que le CBR est une conséquence de la surcharge (overhead). En d'autres termes, une augmentation de la surcharge entraîne un accroissement de CBR jusqu'à ce que le canal devienne saturé, où CBR prend sa valeur maximale. FloodingAdv montre un CBR plus élevé, ce qui s'accroît avec l'augmentation de la densité du réseau, jusqu'à ce que le canal atteigne l'état de saturation. Enfin, CBF et CBF2C montrent des niveaux acceptables en terme de CBR.

Motivé par le manque d'efforts sur le contrôle de la congestion pour la diffusion à plusieurs sauts des messages DENM , nous avons proposé un algorithme de transfert nommé CBF2C qui prend en considération les performances de la communication telles que l'utilisation éfficace du canal. Plus précisément, CBF2C exploite les avantages des approches Flooding et CBF tout en tenant compte de l'état de congestion du canal. Les résultats de la simulation montrent que, contrairement à CBF et FloodingAdv, l'approche proposée offre des performances améliorées en termes de PDR , ainsi que de délai (E2ED) et évite la congestion du canal (CBR, overhead).

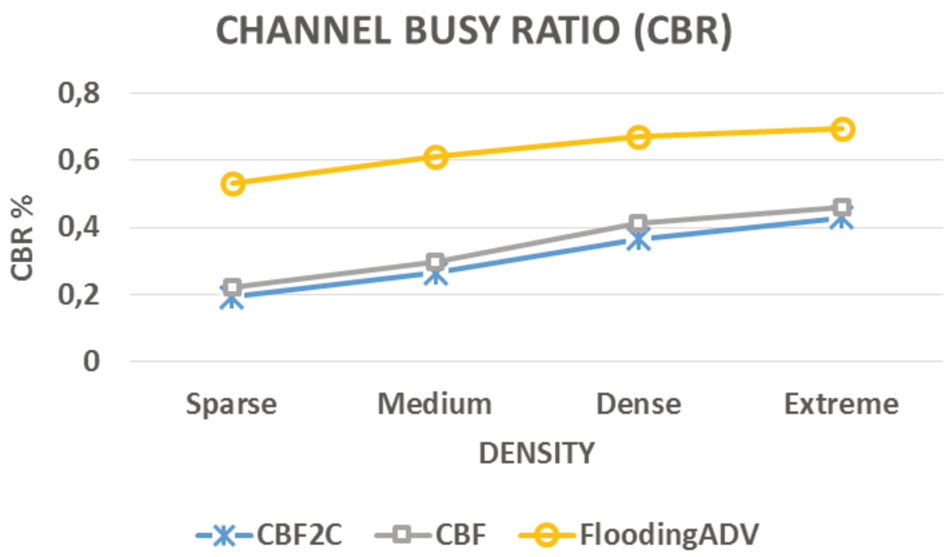

FIGURE 3.17 – Le taux d'occupation du canal

La section suivante 3.8 comprend l'évaluation des différents schémas pour des scénarios dans le cas où les deux types de messages CAM et DENM coexistent. En outre, des évaluations dans le cas, d'un dual-DCC (DCC sur CAM et DCC sur DENM), seront également effectuées.

3.8 Évaluation de performances de CBF2Cv1 sans la mobilité

Dans cette partie, nous évaluons les performances des approches CBF2Cv1, l'amélioration de Flooding (FloodingADV) et CBF-RT. Dans cette étude, nous considérons que le canal est partagé par deux types de messages qui sont les messages DENMs et CAMs. Un dual-DCC, à savoir CAM sur la couche Facilities et DENM sur la couche GeoNet a été considéré.

3.8.1 Paramètres de simulation

Dans cette section, nous comparons les performances de CBF2CV1 avec FloodingAdv et CBF-RT pour des scénarios lorsque les paquets DENM et CAM partagent le même canal. Nous évaluons d'abord les performances des paquets CAM et DENM pour les différents algorithmes, lorsque le taux de génération des CAMs n'est pas adapté (sans DCC sur CAM). Ensuite, nous évaluons les performances des paquets CAM et DENM, lorsque le taux de génération des CAMs est contrôlé (avec DCC sur CAM) suivant l'algorithme DCC réactif asynchrone (asynchronous reactive DCC algorithm) [83], qui règle le taux de génération des CAMs d'une manière asynchrone comme défini dans le tableau 3.4.

Les étapes de la simulation suivent les recommandations de standard ETSI pour l'évaluation des algorithmes de contrôle de la congestion [17].

TABLE 3.4 – Table des valeurs de contrôle de DCC Reactive

États	CBR (%)	T_{off} (ms)	R^{ms} (Hz)
$Relaxe$	[0,19[	60	16.7
$Active_1$	[19,27[	100	10.0
$Active_2$	[27,35[	180	5.6
$Active_3$	[35,43[	260	3.8
$Active_4$	[43,51[	340	2.9
$Active_5$	[51,59[	420	2.4
$restrictif$	[59,100]	460	2.2

Plus précisément, comme l'illustre la Figure 3.18, les véhicules sont répartis sur une autoroute avec 6 voies. La longueur de l'autoroute est de 1 km et la largeur de chaque voie est de 3 mètres. On considère trois types de densités routières, sparse, moyennes et denses, où la distance entre les véhicules (inter-distance) est respectivement de 100, 45 et 20 mètres (voir tableau 3.5).

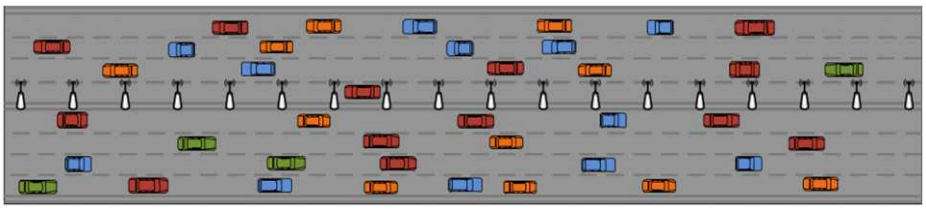

FIGURE 3.18 – Scenario d'autoroute (ETSI TR 101 612)

TABLE 3.5 – Paramètres du scénario routier

Classe	Inter-distance	Densité des nœuds (Nœuds/Km)
Sparse	100 m inter-distance (3 lignes/ 2 directions)	11
Medium	45 m inter-distance (3 lignes/ 2 directions)	23
Dense	20 m inter-distance (3 lignes/ 2 directions)	51

Les paramètres de communication sont présentés dans le tableau 3.6. Comme on peut le voir dans le tableau, chaque véhicule diffuse périodiquement des paquets CAM d'une taille de 400 octets tous les 10 Hz (par défaut). Les RSUs diffusent 500 octets de paquets DENM tous les 10 Hz. La zone de destination des paquets DENM est une route de (1 km x 18 m). Les transmissions de paquets DENM ont une priorité plus élevée que les paquets CAM, en particulier, les DENM sont envoyés à l'aide de la catégorie d'accès de type Vidéo tandis que

les CAM sont envoyés à l'aide d'une catégorie d'accès de type Background. Les CBR_{max} et CBR_{min} sont fixés à 70% et 55% respectivement dans CBF2C. RC_{Th} est de 2 pour CBR-RT [66]. Le WT_{max} est de 5 ms pour l'approche Flooding et de 20 ms pour CBF-RT et CBF2C (CBF2Cv1). La valeur de τ dans l'équation 3.5 est de 1 ms.

TABLE 3.6 – Les paramètres de la simulation

Paramètres	Valeur
Bande passante du canal	10 Mhz
Puissance de transmission	23 dBm
Modèle de propagation	Log-distance
Intervalle de surveillance du CBR	100 ms
Nombre de RSUs	5
Sources des DENM	RSUs
Taux de génération des DENM	10Hz
Taille des DENM	500 octets
Zone destination des DENM	route [1000m x 18m]
Taux de défaut de génération des CAM	10 Hz
Taille des CAM	400 octets
Catégorie d'accès (Access category) CAM/DENM	BK/VI

3.8.2 CBF2Cv1 avec CAMs et DENMs

3.8.2.1 Le taux moyen de paquets reçus (PDR)

Les figures 3.19 et 3.20 montrent le taux moyen des paquets DENM reçus (PDR) dans les cas avec et sans DCC sur le taux de génération des messages CAM, respectivement. Le PDR pour DENM est calculée sur chaque véhicule dans la route pour tous les DENMs transmis par les RSUs. En comparant les deux figures, on peut dire que les performances des DENM sont similaires pour les cas avec et sans contrôle de la congestion des CAMs avec chaqu'un des algorithmes. Ceci est dû au fait que les paquets DENM sont assignés avec une plus grande priorité contrairement aux CAMs, Cette priorité permet de protéger les DENM de la congestion du canal. D'autre part, il est clair que l'algorithme CBF2Cv1 montre de meilleures performances en terme de PDR suivi par le CBF-RT. Plus précisément, le PDR de CBF2Cv1 ne se dégrade pas lorsque le contrôle de congestion CAM est effectué.

Les figures 3.21 et 3.22 montrent le PDR moyen des paquets CAM sans et avec DCC sur les taux de génération des CAM, respectivement. Le PDR des CAM est calculé à chaque véhicule pour toutes les CAM diffusées par leurs véhicules voisins dans une portée de 400 mètres. Par rapport à la figure 3.22, la figure 3.21 montre clairement que lorsqu'il n'y a pas de

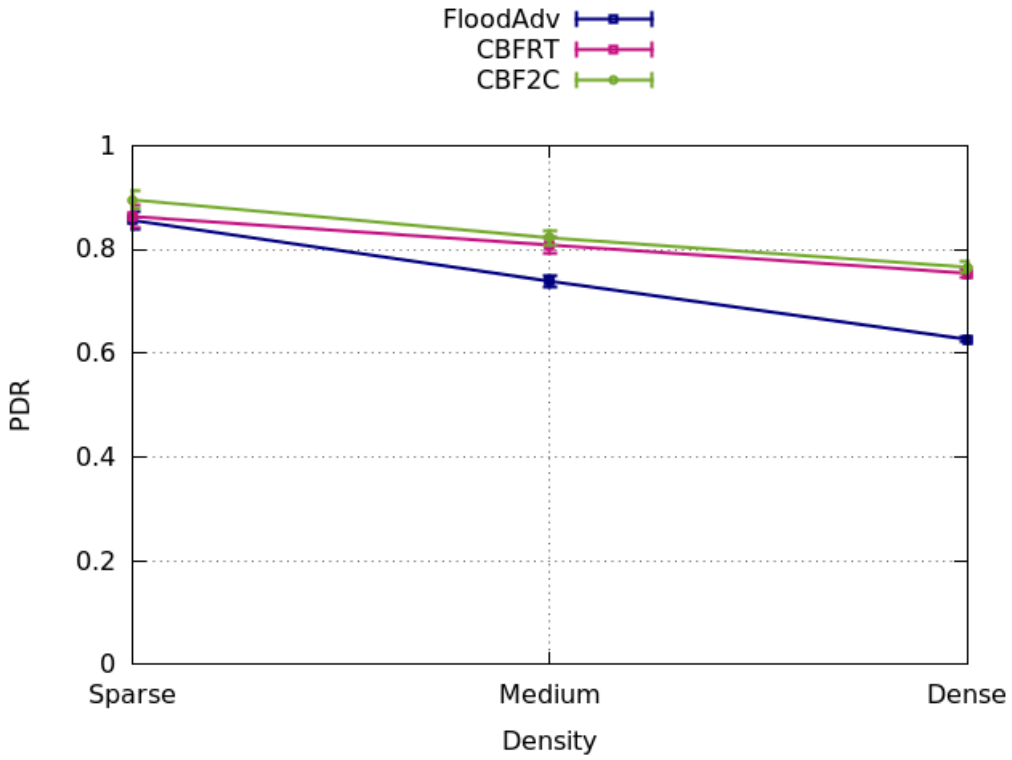

FIGURE 3.19 – Le taux moyen de paquets (PDR) DENM reçus sans DCC sur CAMs.

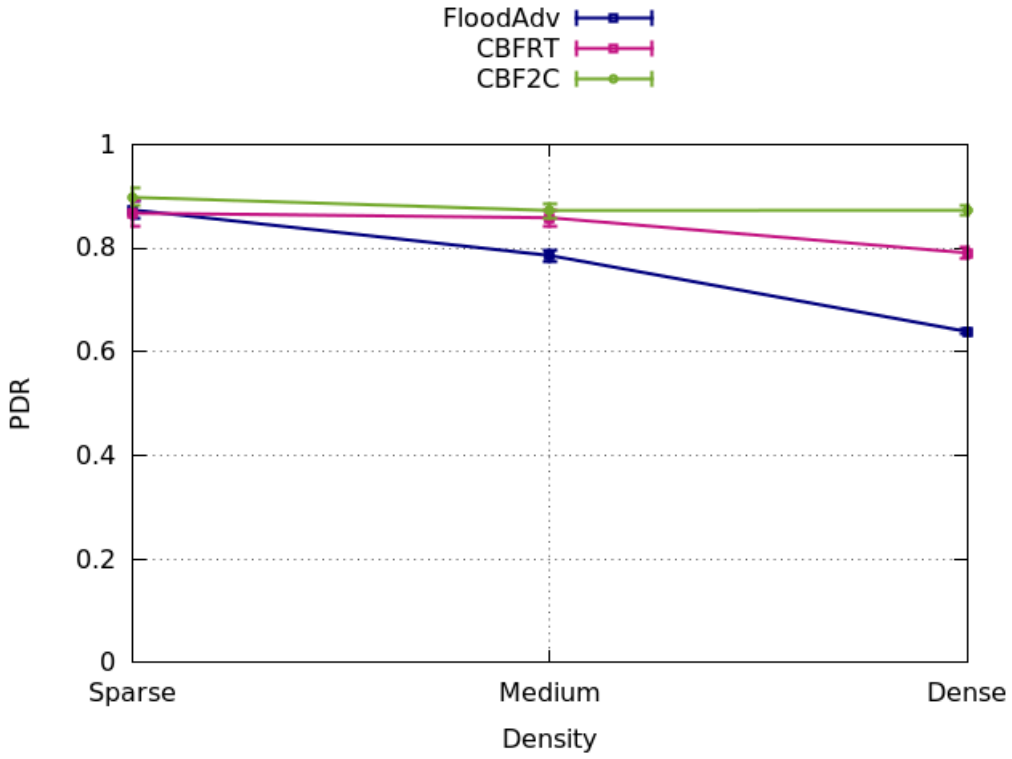

FIGURE 3.20 – Le taux moyen de paquets (PDR) DENM reçus packets avec DCC sur CAM.

DCC sur le taux de génération des CAMs, les performances en terme de PDR se dégradent avec l'augmentation de la densité routière. Ceci est particulièrement important si nous comparons les performances par rapport au PDR des paquets DENM (Figure 3.19), ce qui indique que le trafic de données avec une catégorie d'accès faible paie la congestion du canal. D'autre part, quand le DCC est utilisé sur les CAMs, le PDR des paquets CAMs est en grande partie amélioré.

L'amélioration est significative pour CBF2Cv1, qui fournit un contrôle de la congestion sur les paquets DENM. Les figures 3.20 et 3.22 montrent clairement l'avantage du double contrôle de la congestion sur les paquets CAM et sur les DENM.

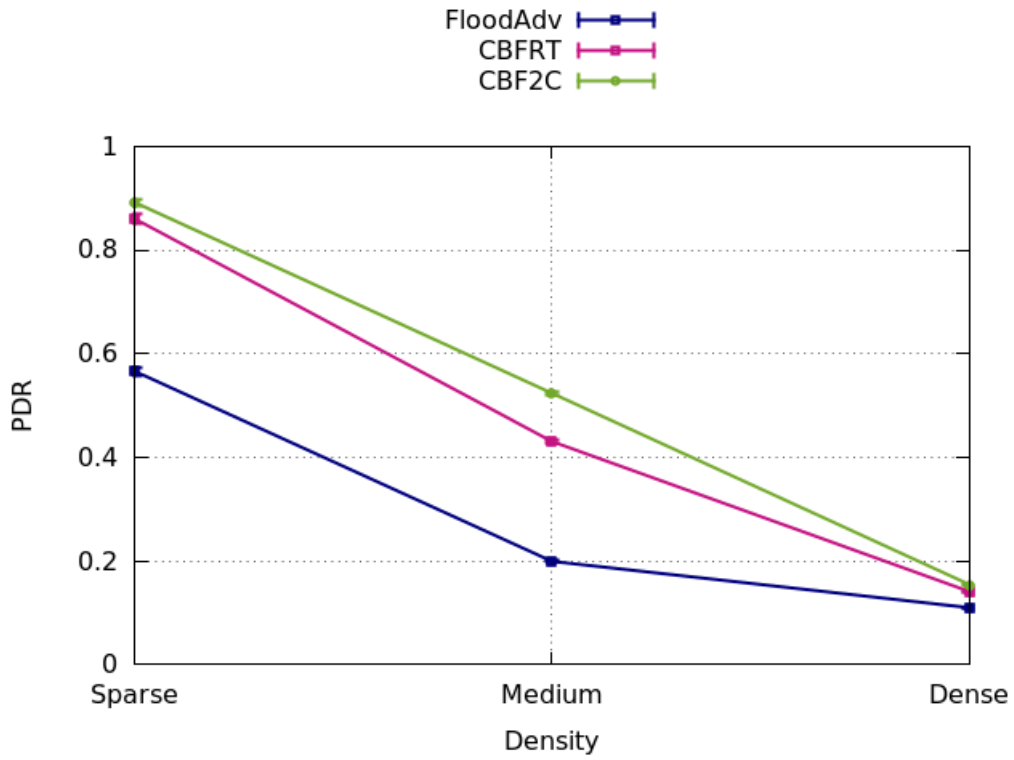

FIGURE 3.21 – Le taux moyen de paquets (PDR) CAM reçus sans DCC sur CAMs.

3.8.2.2 L'intervalle moyen de réception des paquets

Les figures 3.23 et 3.24 représentent l'intervalle moyen de réception des paquets CAM sans et avec DCC sur les CAMs, respectivement. L'intervalle de réception des paquets est le temps entre les deux CAM consécutives arrivant du même émetteur. L'intervalle de réception des paquets augmente en raison des pertes de paquets ou du DCC sur les CAM. La figure 3.23 montre que s'il n'y a pas de DCC sur les CAM, l'intervalle de réception des CAM est important surtout lorsque l'approche améliorée de flooding (appelé FloodADV) est utilisée pour les paquets DENM. D'autre part, l'intervalle est beaucoup plus court lorsque CBF2Cv1 et CBF-RT sont utilisés pour la transmission des paquets DENM. Nous comparons maintenant les résultats des Figures 3.23 et 3.24. dans l'ensemble, les résultats présentés dans les figures 3.23 et 3.24 sont similaires, sauf le cas de CBF2Cv1 dans le scénario dense (l'intervalle est

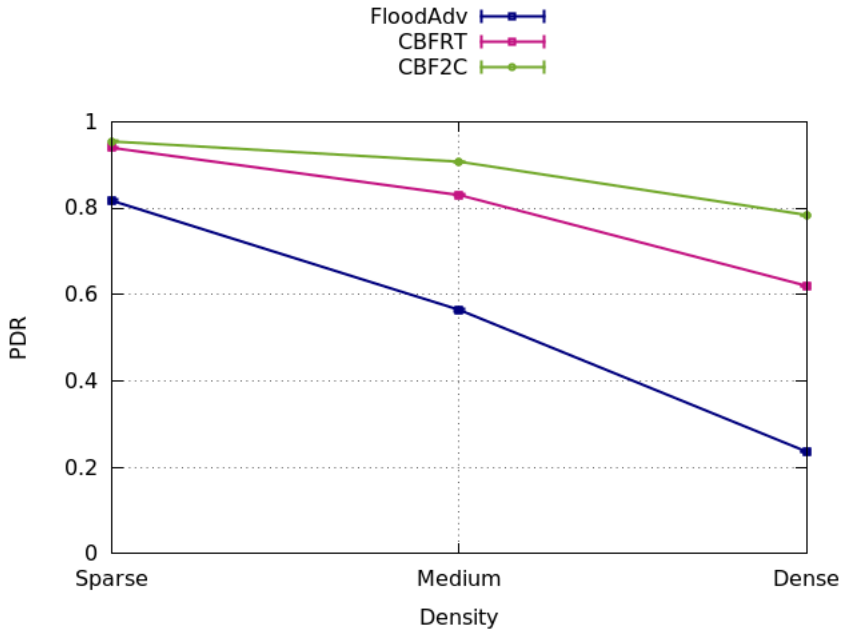

FIGURE 3.22 – Le taux moyen de paquets (PDR) CAM reçus avec DCC sur CAMs.

de 300 ms, plus court dans la figure 3.24). Néanmoins, en considérant les Figures 3.21 et 3.22, les observations faites peuvent être ignorées. En général, grâce au contrôle DCC sur les CAM, moins de CAMs seront perdus, ce qui est important lorsque CBF2Cv1 est utilisé pour les DENM. Néanmoins, le niveau de conscience coopérative (intervalle de réception de l'information) est similaire pour les cas avec et sans DCC sur CAM , en particulier pour les deux approches flooding améliorée et CBF-RT. Lorsque le contrôle de congestion est effectué pour CAM et DENM (c.-à-d. CBF2Cv1), un niveau plus élevé de la sensibilisation coopérative est atteint.

3.8.2.3 La surcharge (overhead)

La figure 3.25 compare le nombre de retransmissions redondante (ou overhead) créées par chaque algorithme lorsque DCC est appliqué sur les CAM. Notez que presque les mêmes résultats sont obtenus pour le cas où aucun DCC n'est introduit sur CAM. le nombre de retransmissions (ou overhead) créées est mesuré par le nombre de copies transmises par paquet DENM par une source pour diffuser les paquets à destination. Comme le montre la figure, une approche Flooding améliorée crée un grand nombre de retransmissions. En revanche, le nombre de retransmissions avec CBF2Cv1 est significativement faible, indépendamment de la densité du réseau. l'algorithme CBF-RT montre un nombre de retransmissions plus élevé par rapport à notre approche CBF2Cv1.

3.8.2.4 Le taux d'occupation du canal (CBR)

Enfin, les figures 3.26 et 3.27 comparent le taux d'occupation du canal (CBR) pour les cas sans et avec DCC sur CAMs, respectivement. Dans la figure 3.26, s'il n'y a pas de DCC

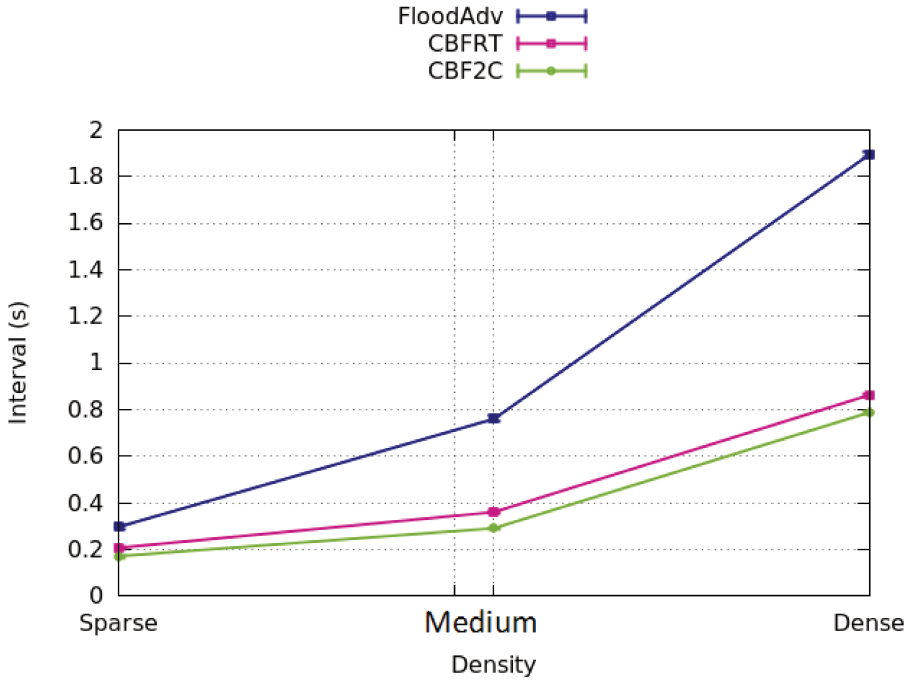

FIGURE 3.23 – L'intervalle de réception des paquets CAM sans DCC sur CAM.

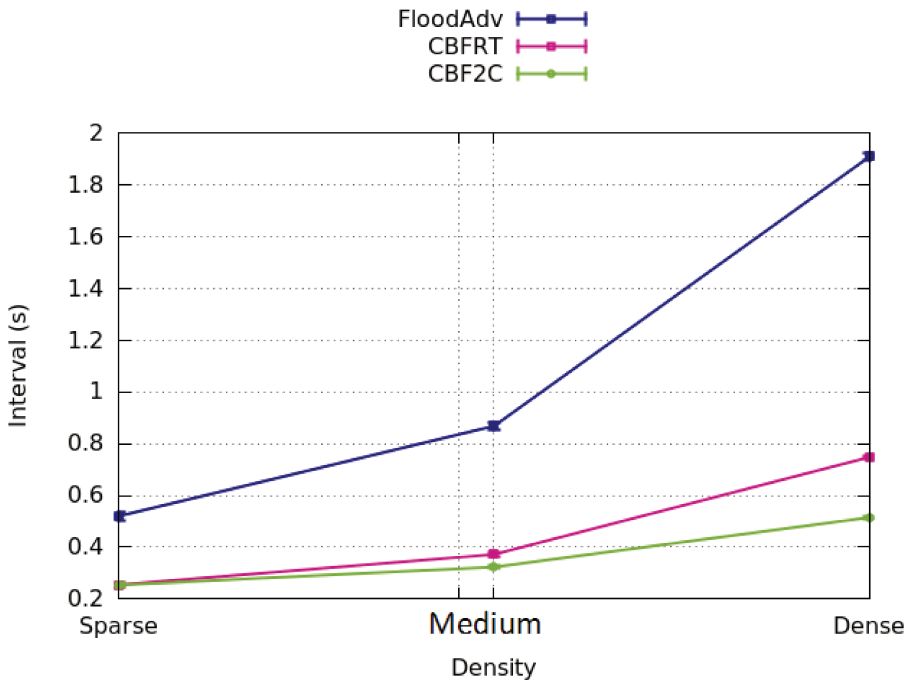

FIGURE 3.24 – L'intervalle de réception des paquets CAM avec DCC sur CAM.

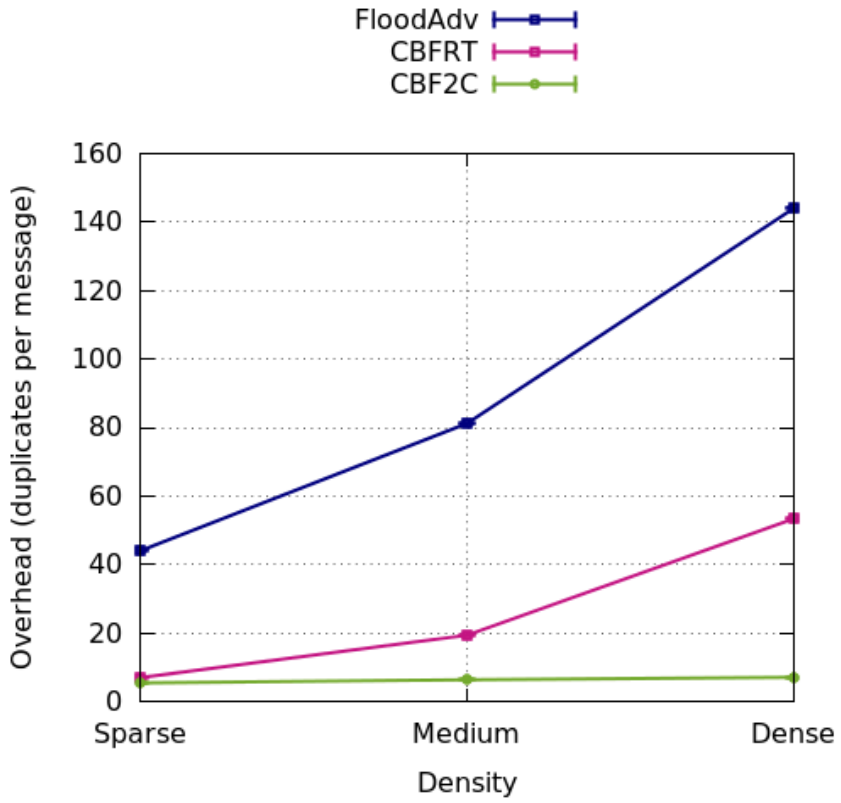

FIGURE 3.25 – Communication overhead c'est à dire, nombre de retransmissions redondantes pour différents algorithmes par message

sur CAM, le CBR dépasse 60% indépendamment de l'approche de transmission utilisée pour les DENM, et le canal est quasiment constamment saturé pour l'approche flooding améliorée (FloodAdv). En revanche, le CBR est faible pour CBF2Cv1 suivie de CBF-RT, en particulier si DCC sur CAM est effectué.

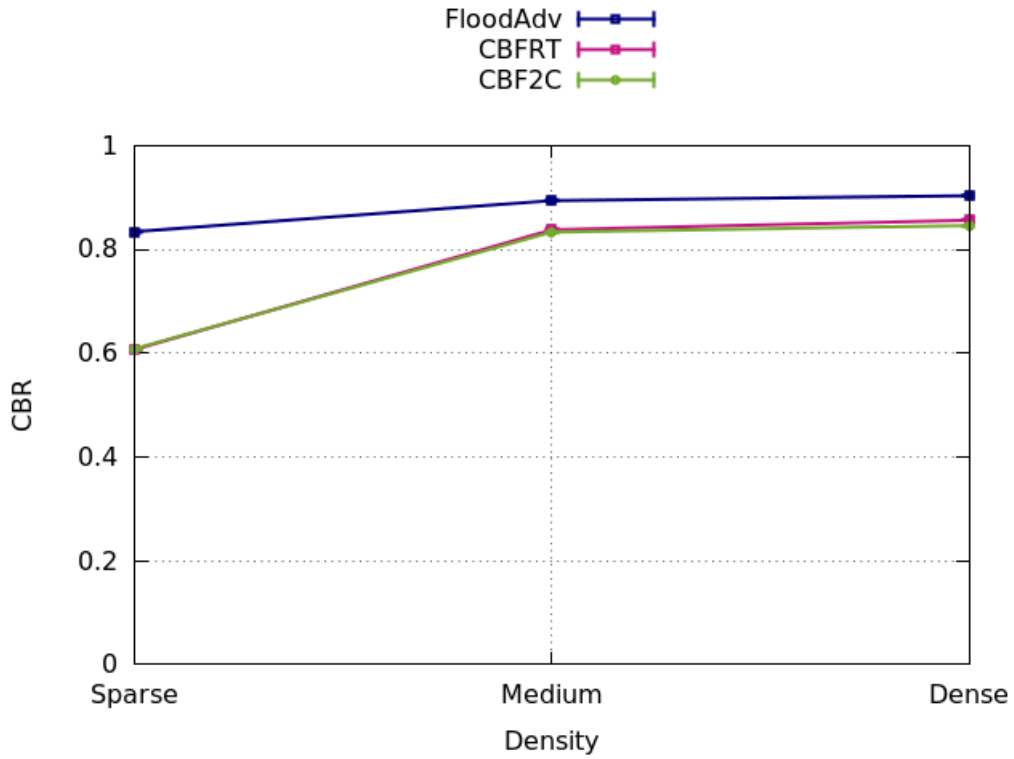

FIGURE 3.26 – Le taux d'occupation du canal (Channel Busy Ratio) sans DCC sur CAM.

Enfin, d'après les figures 3.20, 3.22, 3.24, 3.25, et 3.27, nous pouvons conclure que l'impact de DCC sur CAM est significatif, et DCC sur DENM peut améliorer davantage les performances de la communication.

Motivée par l'absence d'efforts effectués sur le contrôle de la congestion pour la diffusion multi-hop des DENM, nous avons proposé un algorithme de transmission CBF2Cv1 qui tient compte à la fois des performances de communication et de l'utilisation du canal. CBF2Cv1 est conçu pour s'adapter à l'architecture DCC de ETSI : il adapte le nombre de retransmissions en fonction de l'état de chargement du canal. Une évaluation approfondie de CBF2Cv1 est faite par rapport à flooding améliorée et CBF-RT, lorsque le canal est partagé avec les messages CAM. Dans les simulations, nous considérons les cas avec et sans contrôle de la congestion sur les CAMs. Les conclusions obtenues sont les suivantes : l'accès avec priorité au canal peut largement protéger les paquets avec la priorité la plus élevée (dans notre étude, ce sont les messages DENM) et les paquets à priorité moins élevée souffrent en grande partie de la congestion du canal, surtout s'il n'y a pas de contrôle (DCC) sur les messages CAM ainsi que sur les messages DENM. Le contrôle de la congestion sur CAM offre de grands avantages sur les performances des CAMs et DENMs, et le contrôle de la congestion sur DENM améliore davantage les performances.

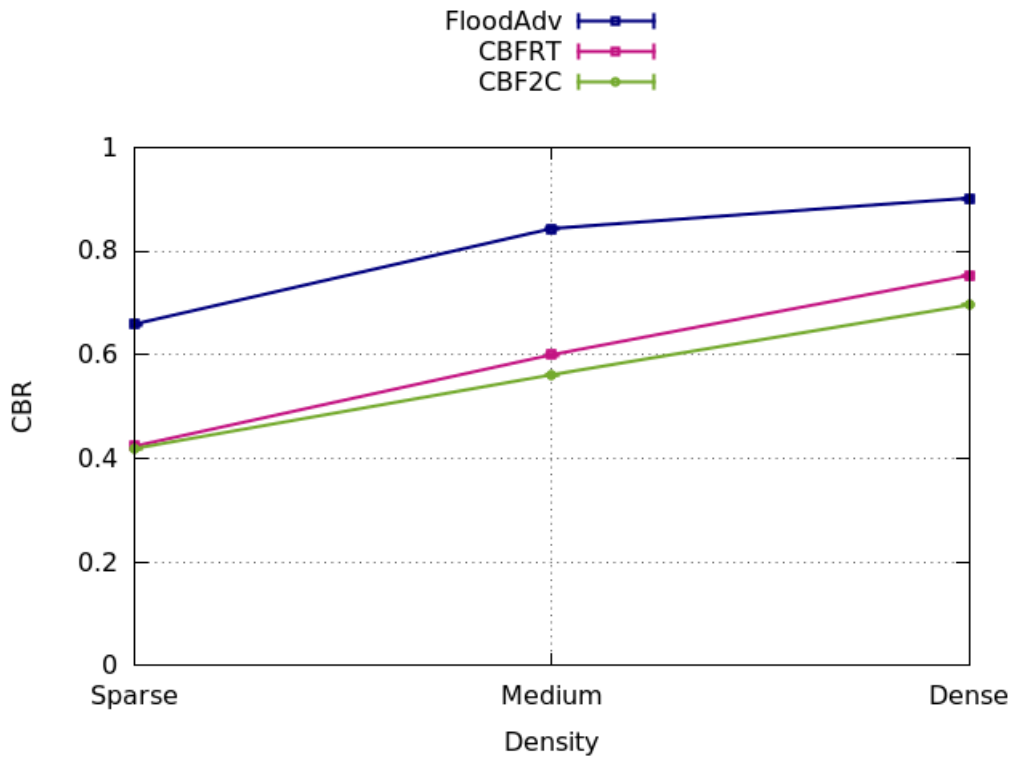

FIGURE 3.27 – Le taux d'occupation du canal (Channel Busy Ratio) avec DCC sur CAM.

Dans la section 3.9, notre prochaine étude comprend l'évaluation des schémas pour des scénarios avec la considération de la mobilité des véhicules.

3.9 Évaluation de performances de CBF2Cv2 avec la mobilité

Dans cette section, nous comparons les performances des différentes approches CBF2Cv2, CBF2Cv1, l'amélioration de Flooding (FloodingADV) et CBF-RT. La mobilité des véhicules est introduite.

3.9.1 Paramètres de simulation

Nous évaluons les performances de CBF2Cv2, CBF2Cv1, CBF-RT et FloodingAdv en utilisant le simulateur de trafic SUMO [15] et le simulateur réseau NS3 [13]. Comme le montre l'Algorithme 1, avec FloodingAdv, lors de la réception d'un paquet, le candidat met en place une minuterie et envoi le paquet lorsque cette dernière expire.

La configuration des paramètres de la simulation suit les recommandations de l'ETSI pour évaluer les schémas DCC pour un modèle routier défini dans [17]. Comme l'illustre la figure 3.28, l'autoroute comporte 6 voies (3 voies par direction) avec une longueur de 10 km.

Nous considérons trois scénarios de différentes densités de trafic (sparse, moyenne et

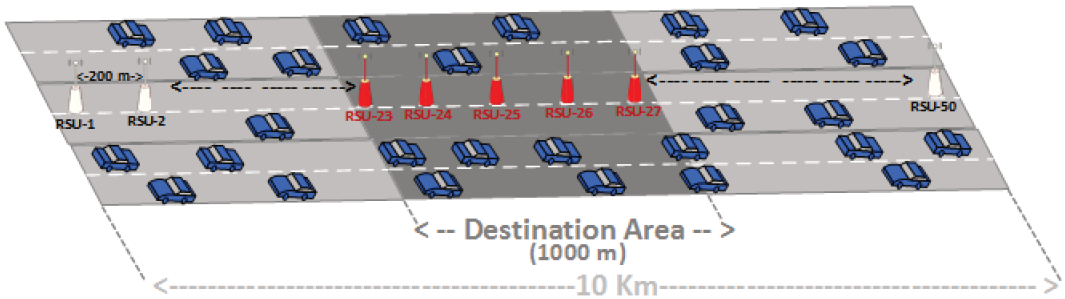

FIGURE 3.28 – Scénario simulé : 6-Lignes 10 Km Autoroute. Taux arrivées des véhicules : Erlang(k, λ), où k = 1, λ est 20, 9, et 2 secondes pour les scénarios sparse, medium, et dense, respectivement.

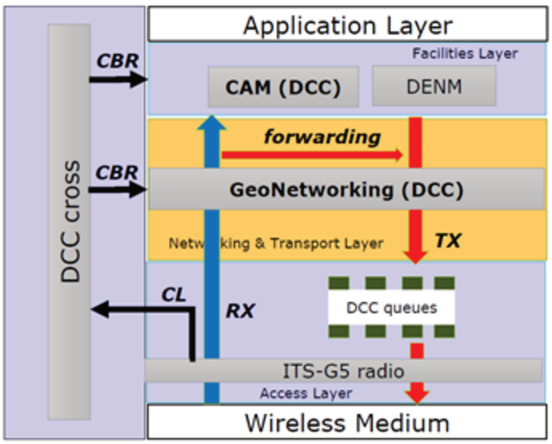

FIGURE 3.29 – Le framework DCC

dense), dans lesquelles les véhicules entrent dans les voies routières individuelles avec le taux d'arrivée d'Erlang(k, λ), Où k = 1 et λ prend une valeur de 20, 9 et 2 secondes (temps inter-distance) pour les scénarios sparse, moyens et denses, respectivement. Comme le montre la figure 3.28, les RSUs sont déployées sur la ligne médiane de la route à chaque 200 m (total de 50 RSU), dont cinq RSU au centre (les RSU en rouge sur la figure) diffusent des DENMs à une fréquence de 10 Hz. Les DENMs doivent être (re)transmises par les véhicules (en utilisant CBF2Cv2, CBF2Cv1, CBF-RT ou FloodingAdv) pour être diffusés dans la zone de destination de 1000 m×18 m (voir la figure 3.28). Par ailleurs, tous les véhicules sur la route diffusent des paquets CAM avec un taux par défaut de 10 Hz, et donc les CAM et les DENM partagent un canal de contrôle commun (plus précisément, dans la zone centrale de la route). En particulier, nous évaluons les performances des paquets CAM et DENM pour les différents algorithmes d'acheminement mentionnés ci-dessus, avec et sans DCC sur le taux de génération des CAM. Lorsque le module DCC-CAM est introduit (voir la figure 3.29), le taux de génération des CAM est contrôlé suivant l'algorithme réactif asynchrone de DCC [83], dans lequel chaque véhicule ajuste l'intervalle de génération des CAM suivant la table de paramètres 3.4.

Les paramètres de communication sont listés dans le tableau 3.7 , qui sont essentiellement

identiques à ceux dans [17]. Les tailles de données de CAM et DENM sont respectivement de 400 et 500 octets. Les DENMs sont transmis à l'aide de la catégorie d'accès VIDÉO, tandis que les CAMs sont transmis à l'aide de la catégorie d'accès Background access (c'est-à-dire que les DENMs ont une priorité plus élevée). La valeur de la minuterie (WT_{max}) pour floodingAdv, CBFRT, CBF2Cv1 est de 5 ms, 80 ms, 20 ms, respectivement. Dans CBF2Cv2, WT_{max} prend une valeur dans l'intervalle de [0.02 s, 1 s] avec les paramètres α = 1.2 et β = 0.3. τ dont CBF2Cv1 est fixé à 1 ms. RC_{max} est de 2 pour CBFRT et prend une valeur dans l'intervalle de [2,4] pour les approches CBF2C. Enfin, CBR_{min} et CBR_{max} de CBF2Cv2 sont respectivement de 55% et 70%.

TABLE 3.7 – Paramètres de simulation

Paramètres	Valeur
Inter-distance RSU	200 m
Taille du véhicule	5 m ×2 m
Bande passante du canal	10 MHz
Puissance de transmission	23 dBm
Modèle de propagation	Log-distance
Intervalle de surveillance du canal	100 ms
Taux de génération des DENM	10 Hz
Taille d'un DENM	500 Octets
Zone destination des DENMs	[1000m x 18m] route
Taux par défaut des CAMs	10 Hz
Taille d'un CAM	400 Octets
Catégorie d'accès CAM/DENM	BK/VI

3.9.2 CBF2Cv2 avec la mobilité, DCC sur CAM et DENM

3.9.2.1 Le taux moyen de paquets reçus (PDR)

Les figures 3.30 et 3.31 montrent le PDR moyen des paquets CAM sans et avec l'introduction de DCC sur le taux de génération des CAMs, respectivement. Le PDR des CAMs est calculé pour chaque véhicule pour tous les CAMs diffusés par ses véhicules voisins dans la portée de 400 mètres. En comparant les deux figures, il est clair que, lorsqu'aucun DCC n'est appliqué sur le taux de génération des CAM, le PDR des CAM est très faible (moins de 20%, voir la figure 3.30). En revanche, le PDR des CAM peut être largement amélioré par l'introduction du mécanisme DCC sur CAM (prenant des valeurs supérieures à 60%, voir la figure 3.31). Les deux figures montrent également que les performances en terme de PDR des CAM, qui sont impactées par le mécanisme de transmission multi-saut appliqué sur les

paquets DENM. Particulièrement, les deux figures montrent que de très basses valeurs de PDR sont obtenues lorsque Flooding est utilisée, tandis que des valeurs plus élevées de PDR sont obtenues lorsque CBF2Cv2 est utilisée pour les DENM. Par conséquent, nous pouvons dire que la plus grande amélioration est obtenue avec CBF2Cv2 qui introduit le mécanisme DCC en utilisant deux paramètres de CBF, à savoir WT_{max} et RC_{th}.

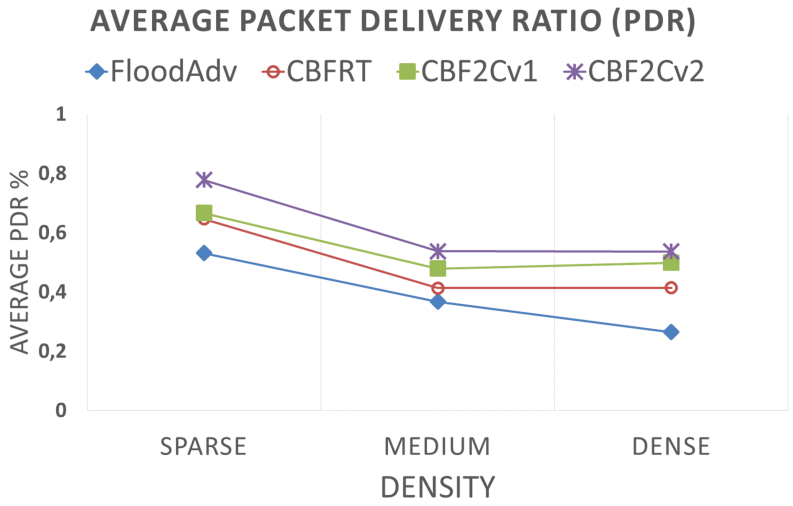

FIGURE 3.30 – Taux moyen de paquets CAM reçus sans DCC sur CAM.

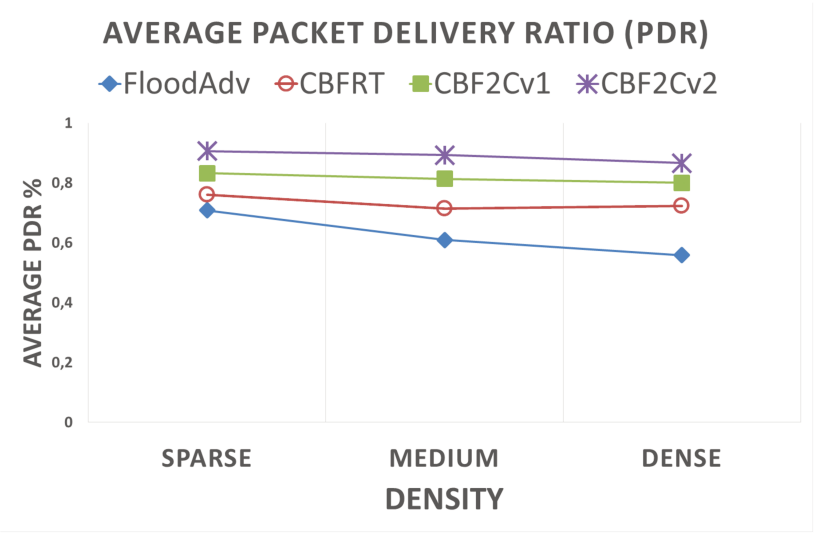

FIGURE 3.31 – Taux moyen de paquets CAM reçus avec DCC sur CAMs.

Les figures 3.32 et 3.33 représentent les performances en terme de PDR des paquets DENM sans et avec DCC sur le taux de génération des CAM, respectivement. Les résultats indiquent la valeur moyenne de PDR (le rapport du nombre de paquets DENM reçus sur le nombre de DENM transmis par les 5 RSU) calculé au niveau de chaque véhicule pour la période au cours de laquelle les véhicules se trouvaient dans la zone de destination. En comparant les deux

figures, nous remarquons que, contrairement à ce que nous avons vu précédemment dans les figures 3.30 et 3.31 l'impact de DCC sur CAM n'est pas significatif pour les performances de PDR pour les DENM, les paquets DENM obtiennent de meilleures performances en terme de PDR que celles des paquets CAM indépendamment du mécanisme DCC sur les CAMs. Cela est dû au fait que les paquets DENM sont assignés avec une plus haute priorité par rapport aux CAM, cette priorité permet de protéger les DENM, tandis que les inconvénients de la congestion du canal se répercutent sur les CAMs. D'autre part, tous les algorithmes CBF assurent de meilleures performances que l'algorithme Flooding, et l'amélioration est significative pour les algorithmes CBF2C qui contrôlent les paramètres de transfert en fonction de l'état de charge du canal.

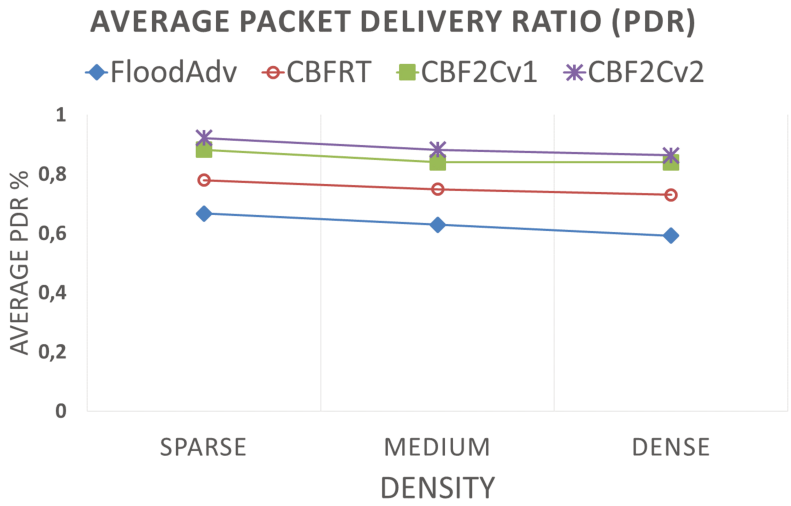

FIGURE 3.32 – Taux moyen de paquets DENM reçus sans DCC sur CAMs.

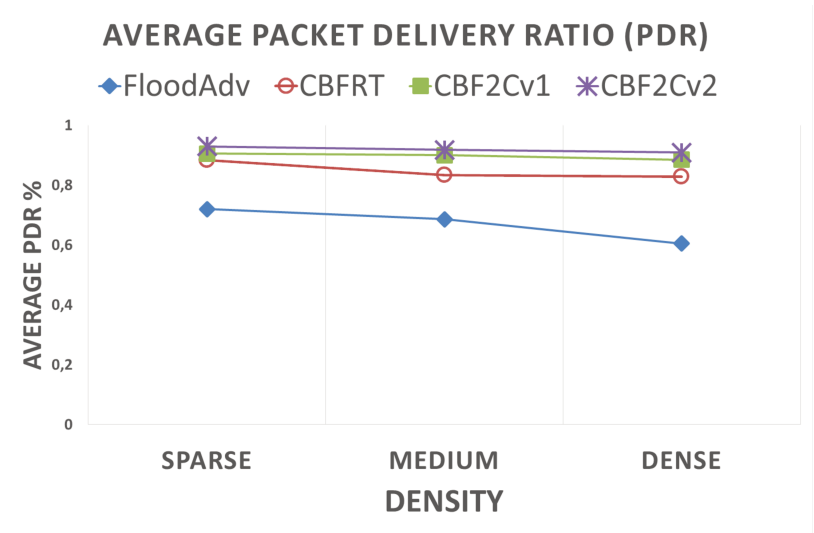

FIGURE 3.33 – Taux moyen de paquets DENM reçus avec DCC sur CAMs.

3.9.2.2 Le délai de bout en bout (E2ED)

Les figures 3.34 et 3.35 montrent le délai moyen de bout en bout (E2ED) pour les paquets DENM sans et avec DCC sur CAM, respectivement. Le E2ED d'un DENM est le temps moyen écoulé depuis le moment où le paquet DENM est généré par la source (RSU) jusqu'à ce qu'il soit reçu par les véhicules dans la zone de destination. De la même manière que les résultats de PDR pour DENM (figures 3.32 et 3.33), DCC sur CAM n'impacte pas beaucoup le E2ED des DENM. Nous constatons cependant les impacts des schémas d'acheminement des DENM. Actuellement, parmi tous les schémas d'acheminement, seul le CBF2Cv2 est capable d'ajuster dynamiquement ses paramètres, en particulier WT_{max} dans une plage donnée, par exemple [0.02 s, 1 s]. Les autres algorithmes d'acheminement nécessitent un réglage manuel de leurs paramètres qui sont statiques (WT_{max}) . Par conséquent, nous avons défini manuellement WT_{max} à 0.005, 0.08 et 0.02 millisecondes pour les algorithmes Flooding, CBF-RT et CBF2Cv1, respectivement, qui représentent en quelque sorte le plus petit WT_{max} fournissant des PDR relativement les plus élevés (figures 3.32 et 3.33).

Par conséquent, si nous réduisons le WT_{max} dans CBR-RT pour, par exemple, 0.02 millisecondes, le PDR diminue considérablement en raison de collisions accrues et des retransmissions redondantes. En raison de ceci, il est pratiquement artificiel de comparer l'E2ED des algorithmes, mais nous pouvons encore conclure que, grâce à son auto-adaptabilité, CBF2Cv2 peut afficher un E2ED significativement court, sans dépendre énormément de la densité de la route et sans nécessiter des paramétrages manuels.

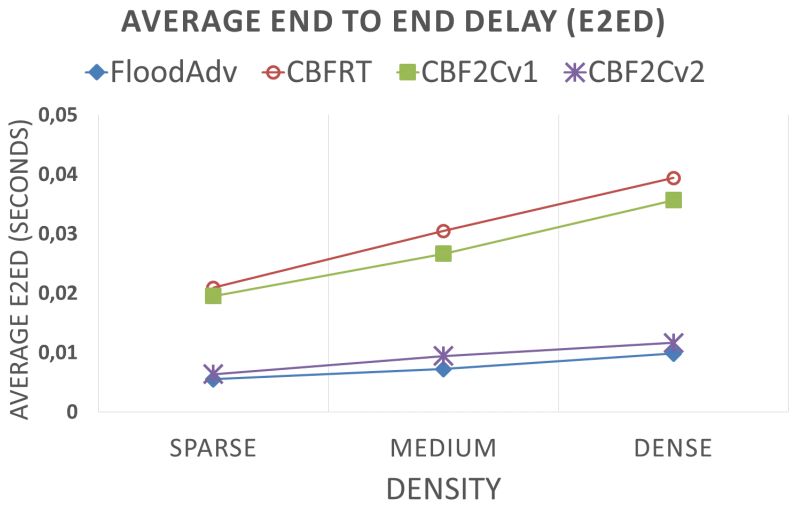

FIGURE 3.34 – Délai de bout en bout (E2ED) sans DCC sur CAM.

3.9.2.3 La surcharge (overhead)

La figure 3.36 compare la surcharge créée lors de la communication par les algorithmes d'acheminement individuellement lorsque DCC est introduit sur le taux de génération des CAMs. Notez que presque les mêmes résultats sont obtenus pour le cas où aucun DCC n'est effectué sur CAM. La surcharge créée est mesurée par le nombre de copies transmises par

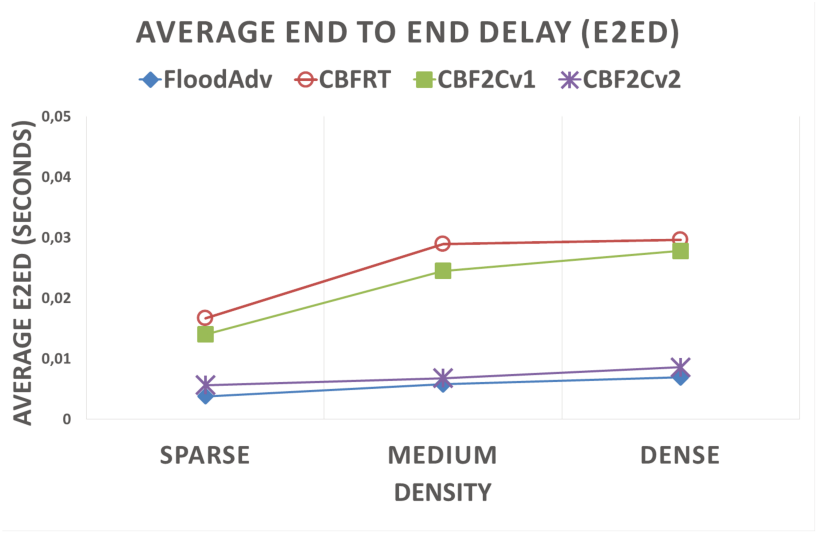

FIGURE 3.35 – Délai de bout en bout (E2ED) avec DCC sur CAM.

paquet DENM. Comme le montre la figure et comme éventuellement escompté, l'approche Flooding crée une grande surcharge. En revanche, la surcharge créée par les schémas CBF sont significativement faibles, la charge (nombre de retransmission) sont particulièrement faibles pour CBF2Cv2.

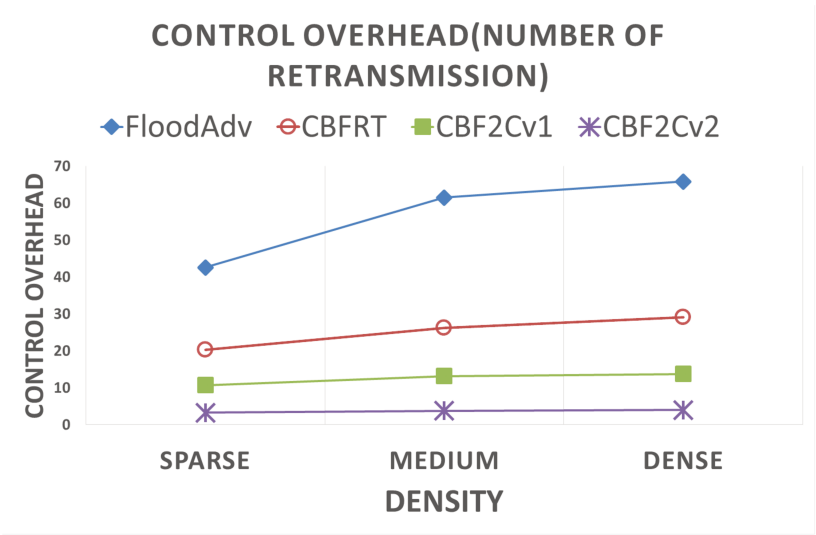

FIGURE 3.36 – Surcharge (Communication overhead) c'est à dire, nombre de paquets en duplication par message.

3.9.2.4 Le taux d'occupation du canal radio (CBR)

Les figures 3.37 et 3.38 illustrent le taux d'occupation du canal (CBR) pour le cas sans et avec DCC sur les CAM, respectivement. Dans la figure 3.37, s'il n'y a pas de DCC sur CAM, le CBR dépasse 60% indépendamment de l'approche de transmission utilisée pour DENM, et

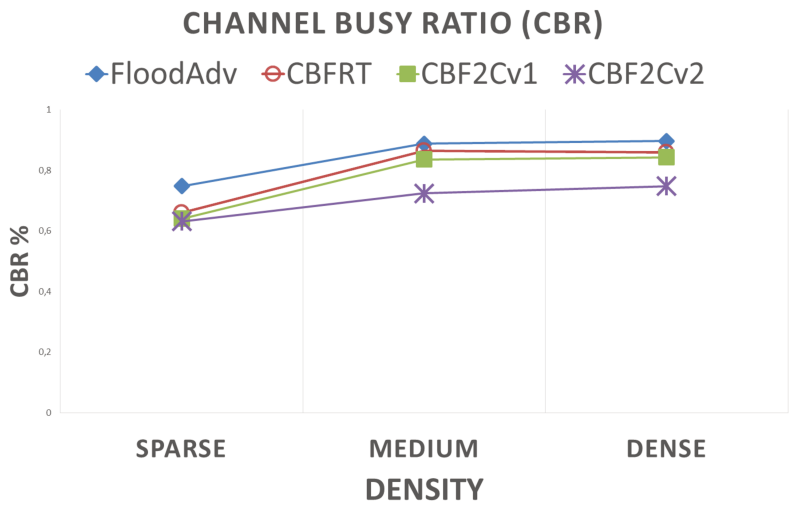

FIGURE 3.37 – Taux d'occupation du canal (Channel busy ratio) avec DCC sur CAM.

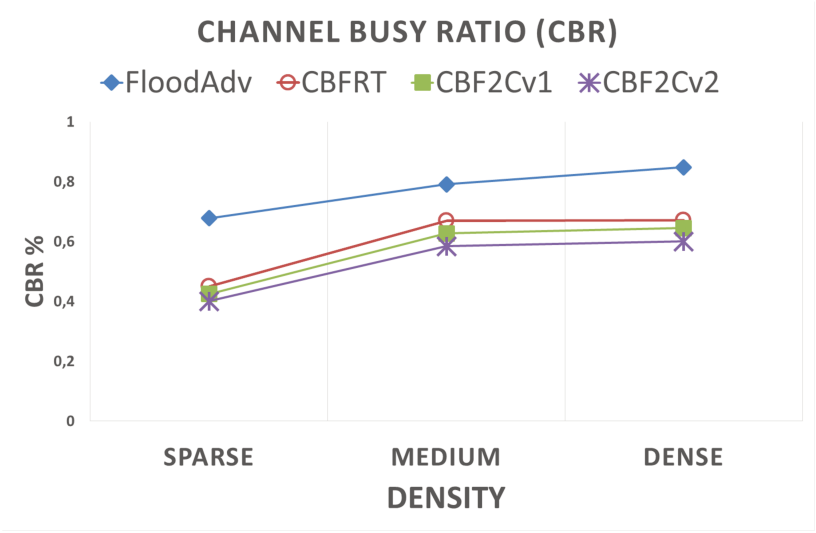

FIGURE 3.38 – Taux d'occupation du canal (Channel busy ratio) sans DCC sur CAM.

l'état du canal est quasiment toujours saturé pour Flooding. En revanche, le CBR est faible pour CBF2Cv2 suivi de CBF2Cv1, en particulier lorsque DCC sur CAM est effectué.

3.10 Conclusion

Nous avons proposé un algorithme CBF2C amélioré, CBF2Cv2, qui contrôle les paramètres de transmission de l'algorithme CBF, à savoir, le temps d'attente avant la retransmission des paquets et le seuil de nombre de retransmissionss en fonction de l'état de chargement du canal.

En utilisant des simulations, les performances de notre algorithme CBF2Cv2 sont comparées à celles des algorithmes CBF2Cv1, CBF-RT, et Flooding, lorsque les messages

CAMs et DENMs partagent le même canal radio. Dans nos simulations, le DCC au niveau de la couche Facilities contrôle le taux de génération des CAMs et qui est également étudié avec la combinaison de notre algorithme DCC proposé au niveau de la couche réseau, CBF2C (DCC sur DENM).

A partir des résultats de la simulation, nous pouvons conclure que l'impact de DCC sur CAM est significatif, et DCC sur DENM, en particulier CBF2Cv2, peut améliorer encore mieux les performances de la communication.

Chapitre 4

Gestion de la Mobilité dans VANET

4.1 Introduction

Dans ce chapitre, nous abordons le problème d'accessibilité d'un véhicule (ou tous les véhicules appartenant à une zone géographique) à partir d'une entité dans Internet. Un des défis majeurs est de permettre la fluidité des communications entre les entités communicantes. En particulier, un mécanisme de gestion de la mobilité adapté au réseau de véhicules est nécessaire. Cela nécessite d'une part, la mise en place d'une communication hybride (IP et Géographique) permettant aux véhicules de configurer une adresse routable, et d'autre part, un mécanisme permettant de réduire la surcharge de la signalisation. Ciblant ces objectifs, nous proposons une approche (GeoMIP) qui gère la mobilité des véhicules dans le contexte de Mobile IP (MIP).

Ce chapitre est organisé en plusieurs sections, la section 4.2 introduit la problématique étudiée avec une description des notions de base nécessaires dans notre étude. La section 4.3 porte sur une étude des travaux existants sur la gestion de la mobilité dans le contexte des VANETs. Dans la section 4.4 nous décrivons dans un premier temps nos motivations avec l'intégration des notions discutées dans les sections précédentes, puis nous expliquons l'architecture proposée (GeoMIP) dans ses détails dans les sections 4.6, 4.7 et nous citons les scénarios d'application de notre nouvelle architecture dans la section 4.5. En se basant sur un ensemble d'hypothèses, une analyse de notre solution est faite dans la section 4.8. Dans les sections 4.11, 4.10 et 4.9 nous présentons une étude analytique pour la validation de notre proposition (GeoMIP), suivi d'une évaluation de performances. Enfin, nous résumons nos contributions en conclusion de ce chapitre.

4.2 Problématique

Pour gérer la mobilité, il est essentiel de permettre un nomadisme transparent et une connexion continue à Internet. La question fondamentale consiste à comment envoyer des données à un récepteur en mouvement (autrement dit, à un ou plusieurs véhicule(s)). Pour qu'une entité sur Internet (ex. Nœud Correspondant ou un serveur) puisse envoyer des données au mobile, le CN ou le serveur doit avoir des moyens d' obtenir la dernière adresse IP

valide du mobile ou bien être en mesure d'atteindre le mobile en utilisant une information stable (c-à-d celle qui ne change pas lors du mouvement du mobile) [95]. Parmi les solutions existantes, quelques-unes utilisent le DNS (système des noms de domaine) comme moyen de fournir au CN ou au serveur les adresses IP actuelles des mobiles. D'autres fournissent une fonction qui permet d'atteindre le mobile lors du changement de sa localisation, en se basant sur un identifiant inchangé connu par le CN ou le serveur. Essentiellement trois composants sont impliqués dans les solutions de la gestion de la mobilité : un identifiant stable pour le mobile, un localisateur qui représente la localisation courante du mobile (ex. adresse IP), et une correspondance (mapping) entre les deux concepts (identifiant et localisateur).

En effet , chaque hôte possède un identifiant indépendant de sa localisation alors que son adresse reflète son point d'attachement. Par conséquent, dans le cas d'un réseau fixe où l'hôte est statique, son identifiant et son adresse peuvent être utilisés de manière interchangeable, contrairement au cas d'un réseau mobile où l'hôte mobile change son adresse à chaque fois qu'elle s'attache à un nouveau domaine d'administration. un hôte mobile possède une adresse personnelle (HOme Address ou HoA) qui dépend du domaine d'administration du nœud mobile. Dans le même domaine, cet hôte mobile obtient une autre adresse qui est une adresse temporaire (care of address ou CoA). Cette dernière (CoA) est utilisée par l'agent mère (HA) pour la transmission des paquets à ce nœud mobile.

Pour pouvoir envoyer des paquets d'une source à une destination (C2V), il est nécessaire de localiser la destination. L'envoi peut être soit vers un seul véhicule (une communication unicast) ou bien vers une zone géographique où se trouve un ensemble de véhicules qui sont en générale concernés par un même événement (une communication GeoBroadcast).

En effet, l'une des parties importantes dans la gestion de la mobilité au niveau de la couche réseau est le protocole de mise à jour de la localisation (location update protocol) : l'acheminement des paquets à leurs destinations se base sur la table de localisation de chaque nœud mobile. La mise à jour de ces informations de localisation se fait de deux manières : basée sur le nœud, ou basée sur le réseau. Dans le premier cas, c'est le nœud mobile qui interagit directement avec son point d'attachement actuel au réseau, dans ce cas les protocoles de mobilité sont des protocoles basés sur l'hôte (Host-based) comme par exemple les approches Mobile IP, HMIP [30], NEMO, etc.. Dans le deuxième cas, le cas d'inexistence d'interactions avec le nœud mobile, les protocoles de la mobilité sont donc basés sur le réseau (Network-based), comme dans l'approche Proxy Mobile IP dans LTE [24], Proxy Mobile IP-NEMO.

Dans notre étude, nous nous intéressons à la mobilité au niveau de la couche réseau, particulièrement au protocole Mobile IP [95]. Le Mobile IPv6 est une solution qui permet de gérer la mobilité sur Internet, au niveau de la couche réseau (IP). La mobilité IP, proposée par Mobile IPv6, permet aux utilisateurs de rester connectés avec le monde extérieur (ex. Internet) d'une manière permanente. Ceci implique que toute entité sur Internet peut les joindre à tout moment ainsi que leur correspondant en utilisant une adresse IP valide.

Toutes ces solutions font face à deux problèmes communs. Le premier est de savoir comment mener à bien la tâche de transfert, étant donné que le paquet d'origine est envoyé par le CN avec l'adresse personnelle (HoA) du mobile comme destination. L'autre problème est de savoir comment éviter le routage triangulaire entre le CN ou le serveur, l'agent mère et le mobile.

Dans cette thèse, nous somme intéressés au problème d'adressage hybride (de IP vers une

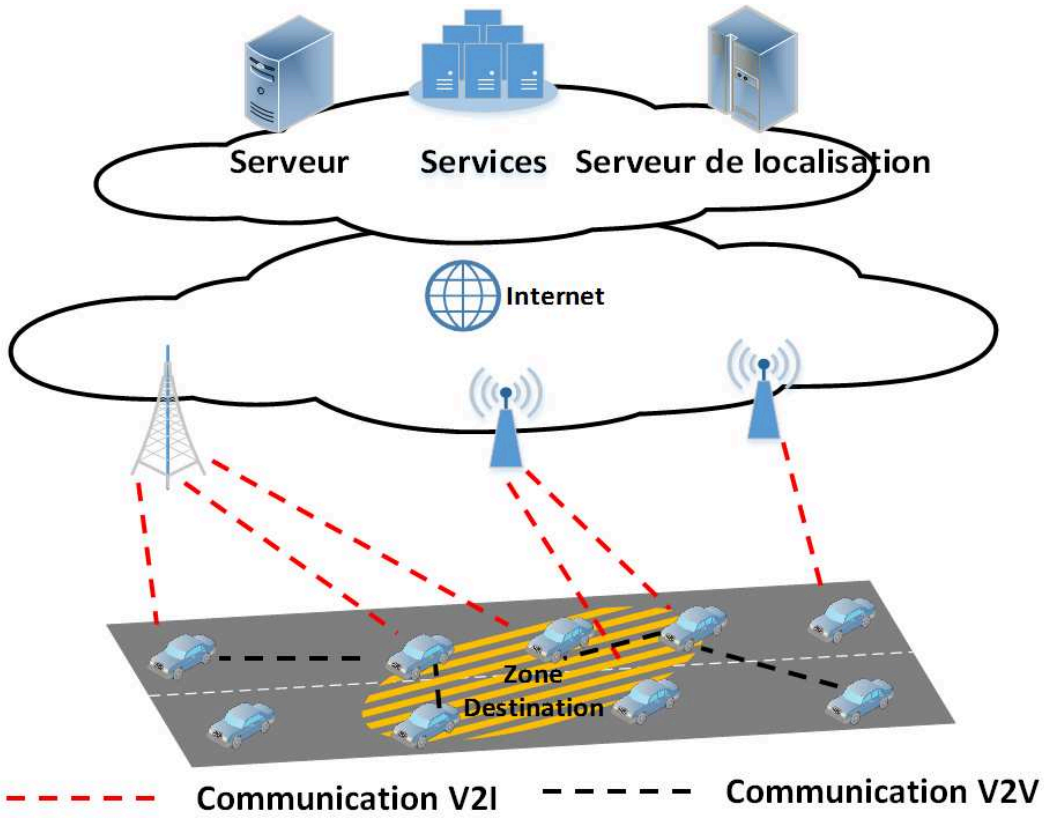

FIGURE 4.1 – Communications V2V2I (ou V2X)

zone géographique), en proposant une solution qui permet d'introduire IP (Internet Protocol) dans le réseau de véhicules. Basant sur le protocole IP pour la gestion de la mobilité, nous proposons une approche qui permet d'envoyer des données en unicast ou à partir d'une entité sur Internet vers une zone géographique, tout en optimisant la signalisation et la latence entre VANET et une entité qui gère la mobilité sur Internet (ex. Home agent), et tout en restant dans un contexte de mobile IP (Mobile IP).

Un réseau ad-hoc hybride permet au réseau de véhicules non seulement d'assurer la connectivité entre eux mais aussi d'accéder à Internet en passant par l'infrastructure. La figure 4.1 montre une architecture d'un réseau ad-hoc hybride dans une autoroute. Les points d'accès qui sont représentés par des RSUs (Road Side Unit), sont répartis le long de la route avec une certaine densité. Ces RSUs peuvent communiquer grâce aux réseaux filaire qui les relient ou via la radio. Un véhicule (nœud mobile) accède à Internet en passant par une ou plusieurs unités bord de route (RSUs ou OBUs).

Dans notre étude nous nous intéressons aux échanges entre une entité sur Internet (centre de service) et le réseau VANET. Les données peuvent être destinées à tous les véhicules appartenant à la zone géographique (la zone destination) ou à un sous-ensemble de véhicules (sous zone de la zone destination). Le problème de la gestion de la mobilité dans les réseaux de véhicules, en particulier concernant l'adressage ainsi que la surcharge lors de Handover sont abordés.

4.3 État de l'art

L'un des défis des réseaux véhiculaires est d'assurer une communication entre Internet et le réseau de véhicules, cela requière d'assurer certaines fonctionnalités, pour se faire il faut identifier et localiser les véhicules. Cela nécessite la capacité des véhicules à auto-configurer une adresse globale et valide, un mécanisme de mobilité (localisation) doit être aussi adapté aux scénarios des véhicules afin d'assurer la gestion de la mobilité des véhicules. Dans cette section, nous nous intéressons aux problèmes d'accès (a) aux services déployés sur Internet et (b) à un/ensemble de véhicules à partir d'une entité sur internet (ex. centre de monitoring).

En effet, il existe un nombre important de protocoles de gestion de la mobilité, cependant, ces protocoles restent inadaptés dans un environnement de véhicules à cause du changement rapide de la topologie dû à la forte mobilité des véhicules. Dans ce qui suit, nous citons quelques travaux qui abordent les problèmes liés à l'adressage et à la gestion de la mobilité.

L'une des caractéristiques de VANET est la forte mobilité des véhicules dont les communications multi-sauts (entre véhicules sans ou avec un passage par des RSU(s)), ce qui ne facilite pas la tâche de la configuration d'adresses IP. L'auto-configuration traditionnelle IP ne peut pas être utilisée pour attribuer des adresses IP uniques aux véhicules car elle s'appuie sur des algorithmes basés sur des fonctions aléatoires. Ce qui ramène à générer des adresses redondantes, bien entendu une procédure DAD (Duplicate Address Detection) est mise en place pour supprimer la redondance. Par contre, ces schémas d'auto-configuration utilisés dans les réseaux ad hoc (Mobile Ad hoc Networks, MANETs) causent de longs délais de configuration d'adresses IP, ce qui n'est pas souhaité pour VANETs. La configuration d'adresse IP dans VANETs est un problème clé dans la recherche. Pour assurer un bon mécanisme d'auto-configuration d'adresses IP pour les applications VANET basées sur Internet il faut respecter les exigences suivantes :

- La réduction de la surcharge (signalisation) vu que la ressource radio est une ressource rare surtout sur le canal de contrôle (CCH),
- Prise en compte de la détection de mouvement de véhicules vu la mobilité dans VANET.
- Assurer une meilleure sélection de passerelle pour le véhicule ou le serveur sur Internet (dans le cas où plusieurs passerelles (RSUs) sont accessibles pour l'une des entités communicantes),
- La configuration d'un adresse globale valide pour qu'elle soit routable sur Internet.

4.3.1 Gestion de la mobilité Internet vers VANET

Dans le contexte des applications basées sur Internet, pour supporter la mobilité dans les réseaux de véhicules, l'utilisation des informations géographiques dans Mobilité IP ou l'intégration d'adresses géographiques et adresses IP reste une piste de recherche ouverte [32]. Dans ce qui suit, nous donnons un aperçu des travaux de recherche existants.

4.3.1.1 Mobile IPv6 NEMO

NEMO basic support protocol (NEMO-BSP) [35] est la solution de gestion de la mobilité sur le réseau (Network-based) proposée par IETF (Internet Engineering Task Force). Dans ce

cas, un réseau mobile se compose de routeurs mobiles (MR) et nœuds de réseau mobile (MNN) où les MRs sont chargés de la gestion de la mobilité des MNNs.

Mobile IPv6 [78] est une solution de la gestion de la mobilité basée sur la hôte (Host-based), qui permet au mobile de grader son adresse mère (HoA) tout en changeant son point d'attachement à Internet. Une correspondance entre cette adresse (HoA) et une adresse temporaire (CoA) est établie à chaque fois que le mobile change son point d'attachement. Cette extension de Mobile IPv6 (NEMO-BSP) permet une association d'une adresse temporaire (CoA) à un pool de préfixes mère IPv6 (a pool of IPv6 home prefixes) nommés préfixes des nœuds mobiles (the Mobile Network Prefixes - MNP). L'idée derrière le concept de NEMO (Network mobility) (RFC 3963) est d'assurer la connectivité de ces MNNs à Internet et de gérer leurs mobilité via une entité unique, nommée router mobile (MR), au lieu de gérer chaque hôte mobile séparément.

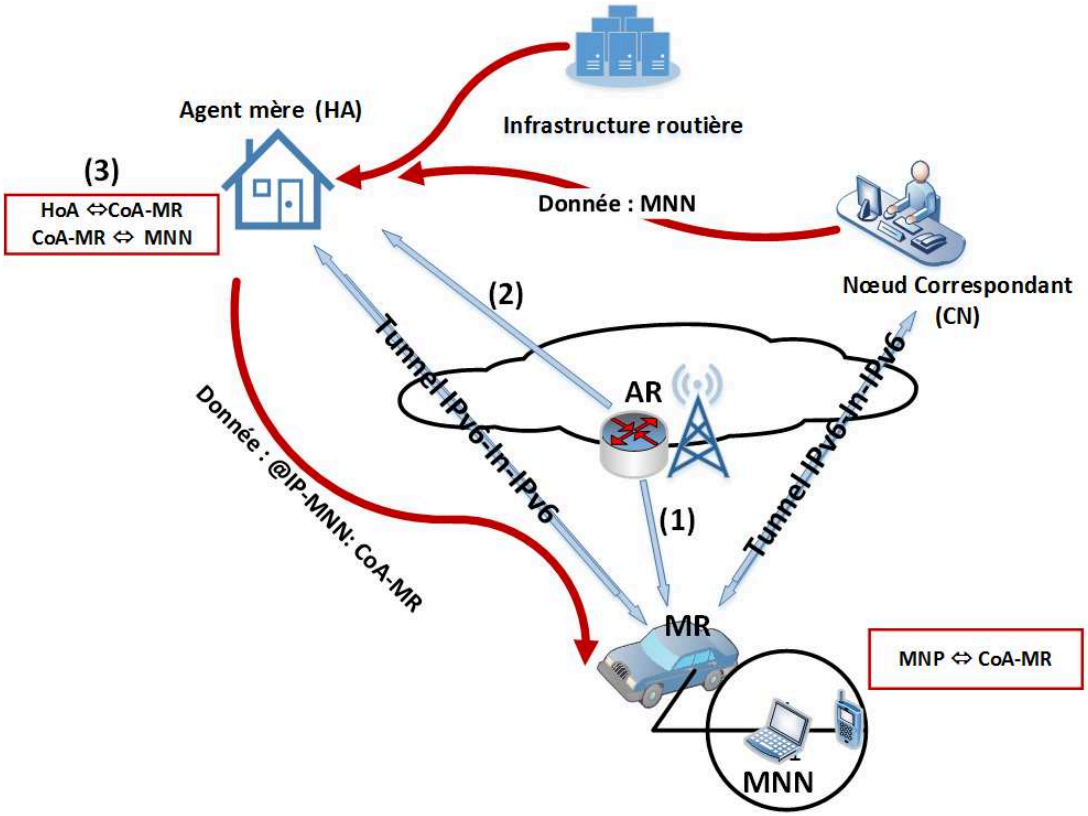

FIGURE 4.2 – NEMO dans Mobile IP (NEMO-BSP)

Comme illustré sur la figure 4.2 : (1) le MR s'attache à un point d'accès (AR), qui lui fournit une CoA. (2) Le MR informe son agent mère (HA) de sa nouvelle CoA et son rôle comme MR (indiqué par un label R) via un message BU (Binding Update) . (3) Le HA met à jour l'association CoA, MNP appartenant au MR et envoi un message d'acquittement BA (Binding Acknowledgment) à ce dernier. Ensuite, un tunnel bi-directionnel (IPv6-to-IPv6) se crée entre les deux entités.

Lorsqu'un nœud correspondant (CN) sans Internet souhaite échanger des paquets avec les MNNs dans le MR. Le CN envoi le paquet avec l'adresse IP du MNN, comme cette adresse

appartient au réseau mère, le paquet est acheminé vers le HA qui connait la liaison (CoA, MNP). Le HA envoi le paquet au MR via le tunnel (IPv6-to-IPv6). Le MR décapsule le paquet reçu et transmet au MNN. Les mêmes étapes s'appliquent dans le sens d'une transmission de MNN vers CN (MNN -> MR -> HA -> CN).

4.3.1.2 Proxy Mobile IPv6 NEMO

Le Proxy Mobile IPv6 (PMIPv6) [51] est une solution pour la gestion de la mobilité sur le réseau (network-based) d'IETF, où la mobilité IP est transparente pour le nœud mobile. Basé sur Mobile IPv6, Proxy Mobile IPv6 introduit un proxy qui effectue la signalisation de la mobilité à la place de l'hôte mobile. Le PMIPv6 définit deux nouveaux éléments fonctionnels :

- LMA (Local Mobility Anchor) : effectue la fonction de l'agent mère de Mobile IPv6, qui attribue l'adresse temporaire (CoA) aux mobiles.

- MAG (Mobile Access Gateway) : est un routeur d'accès responsable de la signalisation de la mobilité. MAG détecte les mouvements de l'hôte et participe aux opérations de mise à jour de la localisation.

Afin de permettre au mobile de changer dynamiquement son point d'attachement lors de handover entre différents points d'accès, les opérations de transmission sont partagées entre les deux entités LMA et MAG. LMA et MAG créent un tunnel bidirectionnel, lorsque l'hôte change de point d'attachement, LMA et la nouvelle MAG créent un nouveau tunnel tout en conservant la connectivité IP avec l'hôte.

PMIPv6 attribue un préfixe HNP (Home Network Prefix) au mobile (MR), ce préfixe ne peut pas être utilisé par les MNN pour attribuer une adresse pour eux-mêmes. Ce préfixe HNP peut être utilisé par le mobile pour auto-configurer une seule adresse. Dans ce cas, les applications IP entre MNN et CN sont impossibles car les MNNs ne possèdent pas d'adresses roulables, car une seule adresse est fournie au MR.

NEMO-BSP qui est une extension de Mobile IPv6 héritant les mêmes limites de ce dernier, telles que le problème d'optimisation de routes (suboptimal route), surcharge lors de tunneling (tunneling overhead) et la latence de transfert (handoff latency) des paquets entre HA, MNN et MR. Plusieurs extensions existent dans NEMO pour supporter la mobilité d'un réseau avec Proxy Mobile IPv6, comme le mécanisme de délégation de préfixes [94] et d'autres solutions qui ne sont pas encore normalisées par IETF [33].

4.3.1.3 Communication Véhicule vers Internet avec le protocole GeoNetworking

Dans [88], les auteurs évaluent les performances du protocole ETSI-GN (GeoNetworking) comme spécifié dans [2] lors de la connectivité Internet aux véhicules dans VANET en analysant les résultats des simulations. Ils déterminent les causes des mauvaises performances lorsque les véhicules communiquent avec Internet et ils identifient des mécanismes pour les améliorer. Pour ce faire, ils ont introduit Greedy Forwarding au niveau réseau, l'analyse des résultats de simulation montrent que :

— Plus le nombre de véhicules qui communiquent avec le nœud correspondant (CN) est élevé, plus le trafic total de données dans le réseau augmente et dans ce cas les ressources doivent être partagées entre tous les véhicules, diminuant le taux de paquets reçus (PDR).

Plus précisément, la valeur de PDR dans les deux directions (internet-VANET et VANET-Internet) est basse. Cette perte élevée de paquets est due à deux raisons : La première, c'est que les paquets sont supprimés au niveau de la couche MAC des nœuds (perte des paquets) lorsque l'algorithme de transmission des paquets (Greedy forwarding) sélectionne des voisins invalides comme prochain saut, la deuxième c'est que les paquets sont rejetés dans le sens Internet-VANET au niveau de la couche MAC de la RSU car sa file d'attente est pleine. Cela signifie qu'une RSU ne peut pas transmettre tout le trafic qu'elle reçoit d'Internet (perte des paquets à la congestion).

La transmission des paquets dans les deux sens (Internet-VANET et VANET-Internet) assure un délai de bout en bout (E2ED) très long. Plus le nombre de véhicules qui communique avec le CN est élevé, plus le trafic de données échangées dans un canal sans fil partagé est important, augmentant le délai de bout en bout. Des améliorations ont été proposées telles que, la sauvegarde des nœuds voisins dite plus stable (vérifiant la formule : $t < R$ (portée)/ v (vitesse), qui suppose t est le temps de traversée de la portée de la RSU) comme prochain saut dans une table de localisation et la prédiction des prochains sauts en se basant sur leurs position, vitesse etc. L'objectif étant d'éviter le problème de la sélection invalide des prochains sauts, dû à la forte mobilité des véhicules. Cette solution s'appuie sur une forte hypothèse où les véhicules se déplacent avec une vitesse constante.

4.3.2 Configuration d'adresse IP pour les scénarios hybrides

La configuration basée sur la position géographique se fait via l'auto-configuration d'adresse (stateless address auto-configuration) et la procédure de détection des adresses en double (Duplicate Address Detection ou DAD) [14] afin de vérifier l'unicité des adresses. Pour introduire IP dans le réseau de véhicules : il faut que le véhicule soit capable d'auto-configurer une adresse IP valide, d'introduire de nouveaux mécanismes plus adaptés , et d'introduire des mécanismes pour une transmission de datagrammes IP d'une manière efficace dans le réseau de véhicules.

IPv6 fournit un mécanisme standard pour auto-configurer des adresses IPv6. Comme défini dans Stateless Address Auto-Configuration (SLAAC) [87], les nœuds reçoivent un préfixe réseau (network prefix advertisement) envoyé par des points d'accès (routeur) qui fournissent une connectivité Internet. Ce préfixe est fusionné avec l'identifiant MAC pour calculer une adresse IPv6 valide. Une procédure de détection d'adresse en duplication (Duplicate Address Detection, DAD) est lancée pour vérifier l'unicité de chaque adresse. La solution IPv6 SLAAC est conçue pour les communications à un seul saut (entre le nœud mobile et le point d'accès). Donc, cette solution n'est pas souhaitable pour les communications multi-sauts.

Dans [73], deux approches principales ont été adaptées pour intégrer IP dans un réseau de véhicules multi-sauts. (a) La première approche consiste à faire en sorte que la couche IP soit pleinement consciente de la nature du multi-saut dans VANETs. (b) La deuxième approche consiste à masquer la nature du multi-saut dans VANET de la couche IP. Dans la première approche, VANET est défini comme un ensemble de routeurs IP (points d'accès) interconnectés par plusieurs liens IP. Le changement rapide de chaque lien individuel contribue fortement à la surcharge liée à la gestion d'adressage et au routage. Dans la seconde approche, le concept de lien IPv6 est étendu à l'ensemble des nœuds qui pourraient ne pas être directement accessibles

via un seul saut. La sous couche située sous IP assure que le lien soit perçu par la couche IP comprenant tous les nœuds y compris ceux qui ne sont pas directement accessibles à un seul saut, ceci est réalisé sans même introduire des modifications dans les mécanismes d'auto-configuration d'adresse IP.

Pour assurer une communication multi-saut entre VANET et le réseau d'infrastructure, les paquets issus d'un nœud émetteur ne souffrent pas des encapsulations supplémentaires au niveau des nœuds intermédiaires et donc permettent d'éviter le passage à travers plusieurs agents mères (HA) avant d'atteindre le nœud correspondant (CN). Pour atteindre le réseau fixe via le multi-saut, un routage ad-hoc sous-IP est utilisé pour transférer des paquets IP via le chemin multi-saut, de manière à créer un lien virtuel entre le véhicule et le AR, sans traitement des en-têtes IP sur les véhicules intermédiaires. Les paquets sont ensuite transmis de AR au bon HA et puis livré au CN. La solution MANET-Centric [31] utilise le routage géographique sous-IP. Une fois le nœud routeur (MR) encapsule un paquet, la sous-couche IP construit un en-tête géo (geo-header) pointant le routeur d'accès (AR). Cet en-tête est utilisé pour transmettre le paquet jusqu'à ce que l'AR soit atteint. Par conséquent, du point de vue de la couche IP, cette configuration est cachée, imitant un lien direct entre l'AR et le MR.

Dans [91] propose la solution MHVA (mobility handover vehicular ad hoc networks) pour VANET basée sur IPv6. Dans MHVA, un véhicule est toujours identifié par son adresse IPv6 mère (HoA) et il reste en communication avec d'autres véhicules sans utilisation d'une adresse temporaire (CoA) durant le processus de mobilité. Le schéma proposé utilise le mécanisme de tunnels pour réaliser le handover lors de la mobilité, ce qui permet au véhicule de recevoir des paquets de la part du point d'accès servi durant le processus de handover lors de sa mobilité. Le principe de MHVA est décrit comme suit :

— Le point d'accès (AP) envoie au routeur d'accès (AR) un message de mise à jour (Update message), contenant l'adresse IPv6 du véhicule et celle du prochain point d'accès (Next associated AP).
— Une fois le message de mise à jour est reçu par AR, il vérifie la table de routage (contenant les véhicules à sa portée) et met à jour l'adresse IPv6 de AP dans l'entrée correspondante avec l'adresse IPv6 du prochain AP.
— Le processus de handover se termine.

La solution MHVA complète les opérations de handoff au niveau de la couche réseau avant les opérations de handoff au niveau de la couche liaison et dans ce cas le véhicule maintient sa connectivité au niveau de la couche liaison durant le processus de handover, ce qui réduit d'une manière significative la perte de paquets. Néanmoins, le tunneling augmente le délai de handover et l'insuffisance de MHVA réside dans la nécessité de solliciter un véhicule voisin pour lancer ce processus avancé de handover lors de changement de sous réseau.

Vehicular Address Auto-configuration (VAC) [72] est une solution pour l'environnement VANET qui exploite un service DHCP avec une amélioration qui consiste à élire des véhicules headers pour fournir une configuration rapide et fiable de l'adresse IP. Le véhicules header est celui qui possède la plus petite adresse et une procédure de construction et de maintenance de la chaine des headers basée sur la distance entre eux (un véhicule normal devient header si la distance qui le sépare d'un header est supérieure à une valeur maximale) .

VAC organise des têtes (headers) (figure 4.3) dans une chaîne connectée, de sorte que chaque véhicule se trouve dans la portée de communication d'au moins un head. Cette

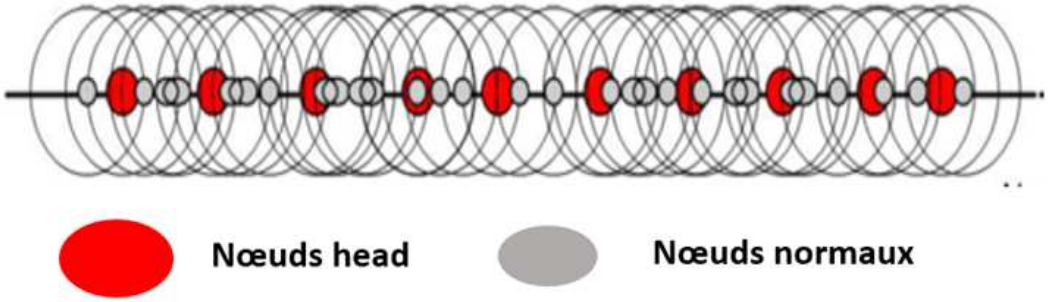

FIGURE 4.3 – Organisation du réseau (nœuds tête (head) et normaux avec VAC) [72]

organisation hiérarchique permet de gérer l'adressage avec moins de signalisation. Seuls les véhicules headers communiquent entre eux pour maintenir l'information de mise à jour sur les adresses configurées dans le réseau. Ces headers agissent comme des serveurs d'un protocole DHCP distribué et les autres véhicules non-headers demandent aux véhicules headers de leurs attribuer une adresse IP valide à chaque fois qu'ils en ont besoin. La limite de cette solution est la supposition (forte hypothèse) qu'il y ait une topologie linéaire avec le mouvement groupé de véhicules, ce qui limite l'application de cette solution à d'autres schémas où la topologie est différente de celle présentée sur la figure 4.3 , et la surcharge due à la gestion explicite de la signalisation (ex. entre vehicules headres).

La solution GeoSAC [79] adapte le mécanisme IPv6 SLAAC dans [87] à l'adressage géographique en introduisant la notion de lien géographique virtuel (Geographical Virtual Link). Ce dernier est défini comme une zone géographique restreinte (GVL) où le protocole GeoNet délivre des paquets multicast à tous les nœuds qui sont à l'intérieur de cette zone, au moyen de la diffusion Géo-broadcast, ainsi tous les nœuds à l'intérieur de la zone de ce lien géographique virtuel appartiennent au même sous réseau IPv6. Autrement dit, cette solution consiste à adapter le mécanisme existant d'auto-configuration d'adresses IP à l'adressage géographique.

Comme illustré sur la figure 4.4, cette approche se base sur un partitionnement en zones géographiques (GVL) où chaque RSU est responsable d'une GVL en assurant une sorte de correspondance entre une GVL et une adresse IP d'un routeur d'accès (RSU), tout en utilisant une extension de serveur DNS , ce dernier connait la localisation de chaque RSU avec leurs préfixes unicast. Dans cette approche, les paquets qui arrivent à une RSU destination sont disséminés en géo-broadcast dans une zone géographique donnée. L'avantage de cette approche, est le non chevauchement des partitions de VANETs (portée de RSU), le préfixe IPv6 annoncé par une RSU est exclusivement assigné à cette zone, ce qui assure l'unicité des adresses, par conséquent le mécanisme DAD (Duplicate Address Detection) n'est pas obligatoire. L'inconvénient réside dans la nécessité d'une signalisation afin de configurer une adresse géographique multicast ainsi que le fait que la zone de destination doit être la même que la zone de routage, autrement dit, cette approche ne permet pas d'assurer une dissémination de paquets vers une sous-zone de la GVL. Le problème avec la solution GeoSAC est que pendant la configuration d'une nouvelle adresse IPv6 (le temps de configuration), le véhicule ne peut pas communiquer et donc doit reporter ses communications en cours jusqu'à ce qu'une

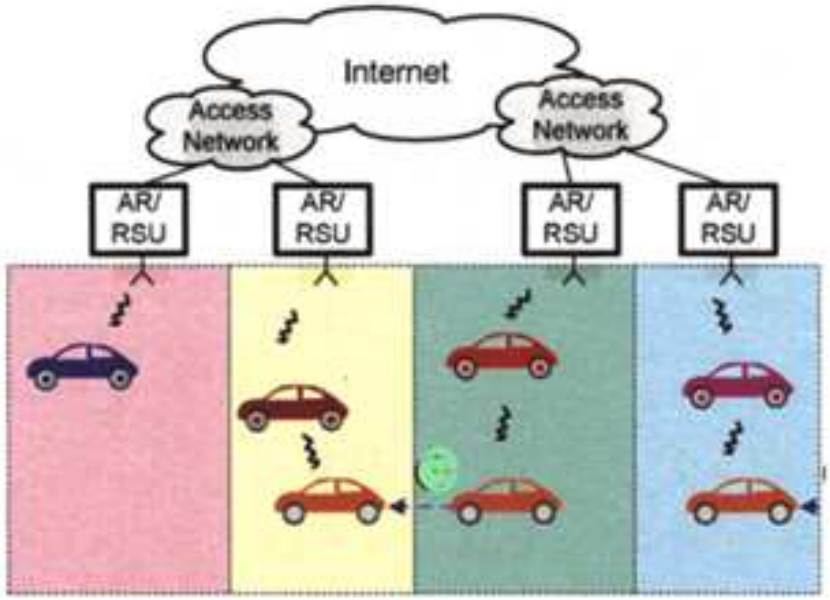

FIGURE 4.4 – Partitionnement de la zone avec GeoSAC [87]

nouvelle adresse IP valide et utilisable soit configurée. D'autres optimisations ont été proposées au mécanisme IPv6 SLAAC tel que [74] où une station ITS peut prévoir les informations concernant les préfixes des zones GVL voisines.

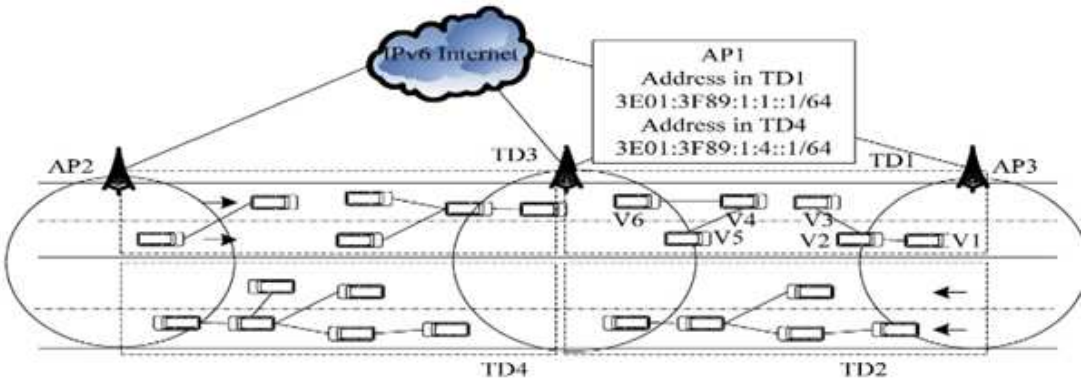

FIGURE 4.5 – L'architecture proposée ([92])

La solution dans [92] utilise le point d'attachement (RSU) du véhicule pour lancer le processus avancé de handover au lieu d'utiliser les véhicules voisins comme est le cas dans [90]. L'amélioration se base sur le concept de construction de groupes de vehicules sous forme d'un arbre (vehicule tree (VTs)) comme illustré sur la figure 4.5. Le but est de réduire la latence de la configuration d'adresses en effectuant une seule opération par groupe (VT), cette opération se fait par le véhicule tête (head). Le schéma de configuration d'adresse IPv6 proposée se base sur des informations de localisation où chaque AP diffuse (broadcast) d'une manière périodique des messages (BasicSafetyMessage) à un seul saut, ces messages incluant des informations sur

leurs adresses IPv6, leurs coordonnées géographiques, des intervalles prédéfinis d'identifiants pour les véhicules (vehicle ID space), handover flag, et root flag etc. Lorsque le flag d'un véhicule est égal à 1, cela signifie que le véhicule est la racine d'un VT. L'architecture adoptée consiste à partager la route en domaines (TD) dans le but de réduire efficacement la fréquence de configuration d'adresse des véhicules. La gestion de la mobilité dans cette approche est basée sur la création d'adresse manuellement, elle n'intègre pas IPv6 et la gestion de la mobilité ne suit pas Mobile IP, en conséquence le véhicule ne peut pas être joignable de l'extérieur (ex. Internet).

4.4 Motivations et Hypothèses

Il existe des applications pour les systèmes de transport intelligents nécessitant une entité dans Internet qui communique avec une flotte de véhicules. Plus particulièrement, on peut mentionner la remontée des informations sur les positions , la recherche dans une base de données centralisée (ex. Serveur de localisation), etc. Pour cette raison il y a un grand intérêt de lier les réseaux de véhicules à l'infrastructure, plus particulièrement à Internet.

Cette nouvelle liaison (communication hybride) permet d'offrir un grand nombre de services pour les passagers de la route. Ces services sont offerts soit par les constructeurs d'automobiles, soit par les installateurs de l'infrastructure. Afin d'assurer la fluidité des échanges entre les entités communicantes, la gestion de la mobilité est nécessaire. Néanmoins, la configuration d'adresses reste un processus coûteux en terme d'échange de messages de contrôle ainsi qu'en terme de délai requis à la configuration de ces adresses.

Avant d'entamer quelques cas d'usages de ce type d'applications qui s'appuie sur la communication hybride, nous émettons quelques hypothèses dans notre étude :

— Cela suppose qu'il n' y ait pas de couverture globale entre les RSUs, c'est-à-dire les RSUs peuvent ne pas être régulièrement espacées.
— Le serveur, une entité fournissant des services sur internet (ex. centre de monitoring, le système de supervision de SANEF, etc.), ne connait pas les RSUs, plus exactement les RSU-FA.
— Le serveur de localisation s'occupe seulement de la gestion de la localisation et de l'adressage IP des RSU-FA.
— L'agent mère (Home Agent) ne connait pas la localisation et les adresses IP des RSUs.
— Chaque nœud mobile (véhicule) porte deux adresses (CoA, HoA) et chaque agent étranger (RSU-FA) possède un préfixe réseau sur 16 octets.

Motivée par la sûreté routière et la gestion du trafic routier (ex. réduction d'embouteillages), deux types d'applications ont été visés dans cette étude, à savoir, les applications IP Unicast et les applications ITS-GeoNetworking.

4.5 Cas d'usage

4.5.1 Applications ITS- Geocast

Motivée par ce type d'applications, qui sont des applications ITS- GeoNetworking pour les cas d'une communication en Géobroadcast. L'application de la gestion du trafic (Traffic management) fait partie de ce type d'applications, où un serveur (ex. système de supervision de SANEF) dans Internet offre un service tel que l'échange d'informations concernant un bouchon, travaux sur la route, vitesse contextuelle, etc. avec les usagers de la route.

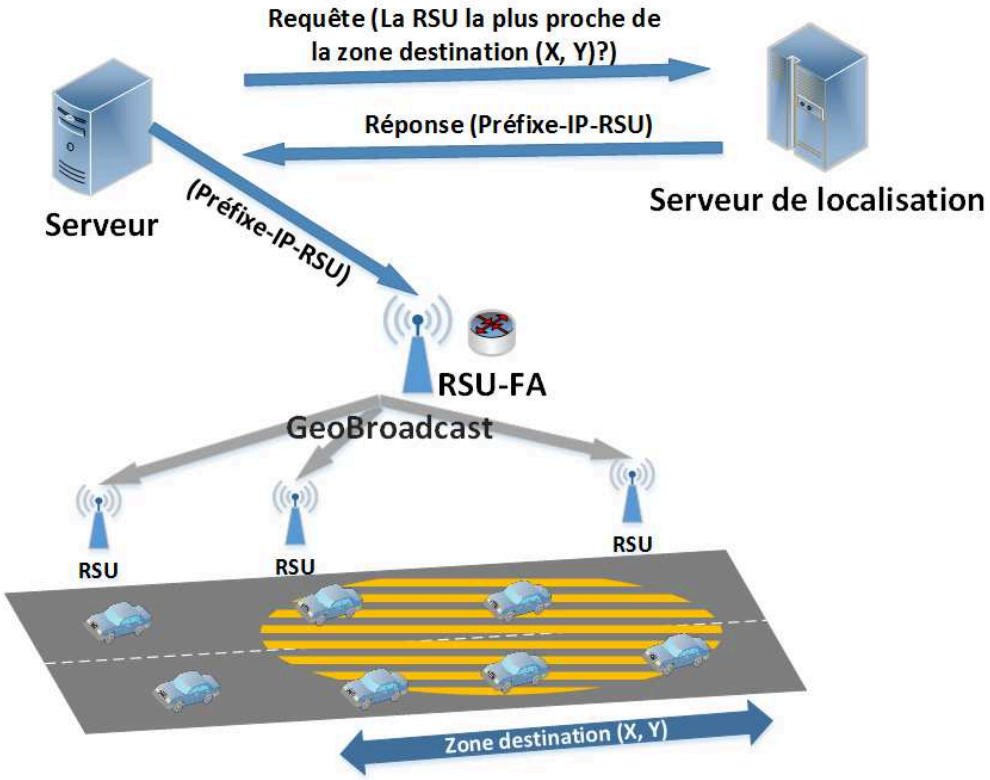

FIGURE 4.6 – Une communication en Geocast

Comme illustré dans la figure 4.6, un serveur sur Internet veut envoyer des données via une communication en Géobroadcast à une zone géographique (VANET) définie par des coordonnées géographique (X, Y). Pour réaliser l'envoi, le serveur envoie une requête de localisation au serveur de localisation pour obtenir l'adresse de la RSU-FA qui s'occupe de la zone (X, Y) concernée par l'évènement. Une fois le serveur de localisation répond en envoyant l'adresse IP (le préfixe) de la RSU-FA, le serveur encapsule les données via ce préfixe, ensuite la RSU-FA envoie à son tour les données reçues de serveur à la zone de destination (X,Y) via une transmission en broadcast.

Dans le cadre du projet PACV2X, nous nous intéressons à un cas d'usage qui est la vitesse contextuelle où un serveur centralisé de l'opérateur routier SANEF avec un système de supervision de la vitesse des véhicules dans des zones à danger (présence de la pollution,

accidents, travaux sur la route). Les entités qui constituent ce cas d'usage sont : un serveur de SANEF centralisé qui définit pour certaines zones des vitesses maximales, un serveur de localisation qui est un superviseur à VeDeCOM, distribue des informations aux RSUs qui sont liées à ce dernier via la 4G. Des RSUs au bord de la route, et des véhicules.

Nous nous intéressons à définir : -le format des messages échangé par le serveur de SANEF et le serveur de localisation. -le contenu des base de données au niveau des serveurs et les RSU.

4.5.2 Applications IP Unicast

Motivée par le cas de la navette. Cette dernière nécessite beaucoup de communications en UpLink et parfois des communications en DownLink, en effet ;

— La navette remonte (UL) ses informations (ex : nombre passagers, direction, vitesse etc.) au centre de monitoring,en général chaque 100 à 500 ms. Périodiquement, la navette envoie au centre de monitoring (HA) des informations (ex. position, vitesse). Dans ce cas , l'adresse de destination est l'adresse IP du centre de monitoring et l'adresse de la source est l'adresse temporaire (CoA) de la navette.

— Le centre de monitoring envoie (DL) des ordres : changement de trajets, informations aux passagers sur le trafic routiers (ex : problème gare des chantiers), et demandes des vidéos (ex : camera devant la navette pour la surveillance).

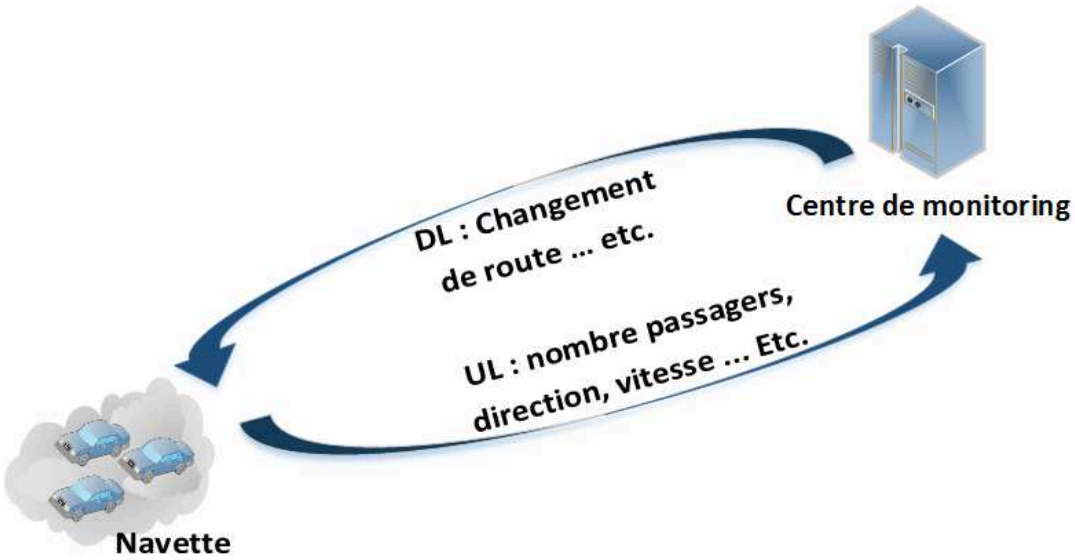

FIGURE 4.7 – Une communication en IP Unicast

La figure 4.7 illustre le scénario de la navette qui utilise MIPv6 pour communiquer avec le serveur avec les différents échanges.

Une solution telle que, Mobile IP (MIP) classique, n'est pas adaptée à des applications Unicast, telle que la localisation de la navette au niveau du centre de monitoring à temps réel vu la latence de la configuration d'adresses (sollicitation de l'agent mère à chaque changement d'une RSU) lors des handovers.

La solution de Mobile IP reste applicable sur ce type d'applications, où chaque RSU (point d'accès) est vue comme RSU-FA. Dans ce cas, à chaque instant t_i l'agent mère (HA) est sollicité à chaque changement de position de la navette, pour que l'agent mère mette à jour l'association adresse temporaire et adresse de domicile BU/BA (CoA, HoA) du nœud mobile (navette), saturant rapidement le réseau lorsque le nombre des nœuds mobiles augmente (la figure 4.8).

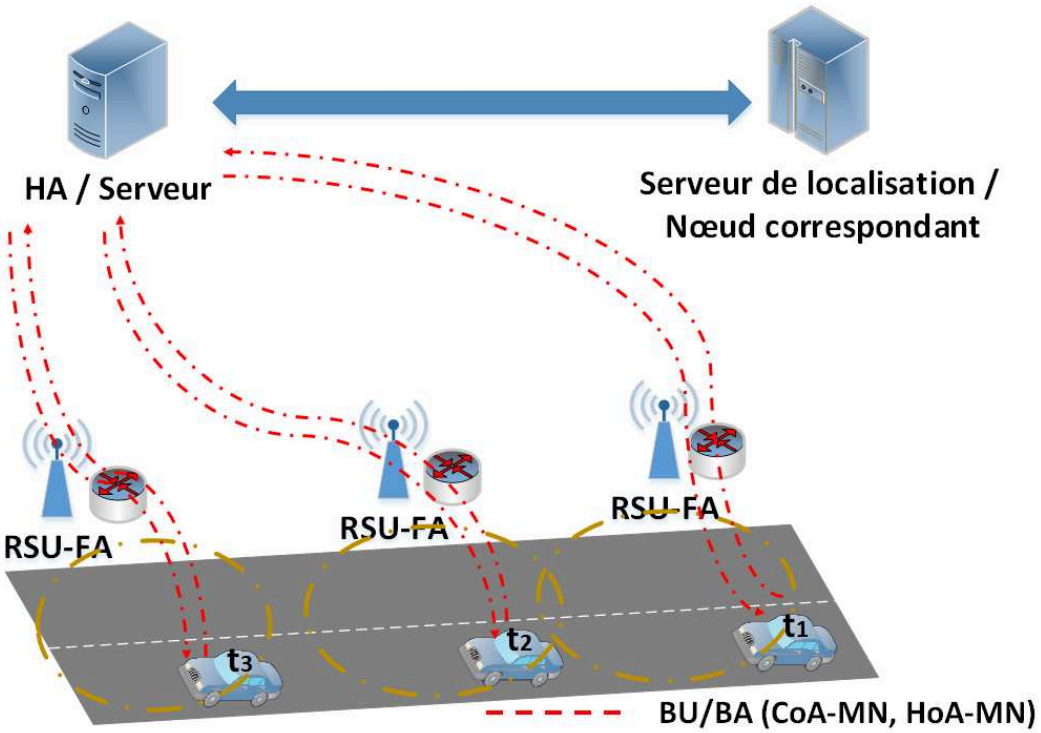

FIGURE 4.8 – Le problème de surcharge du réseau avec MIPv6

Néanmoins, la solution que nous allons proposer reste applicable sur ce type d'application c-à-d aux communications Unicast, et l'avantage avec la solution proposée (GeoMIP) est qu'elle permet de réduire la signalisation et donc la surcharge dans le réseau, tout en assurant une dissémination de données vers des zones ou sous-zones de la RA.

4.6 Approche proposée GeoMIP

Comme illustré sur la figure 4.9, la route est partitionnée en zones de routage, chaque zone de routage (RA) est considérée comme domaine d'administration avec une passerelle qui est la RSU-FA (porte les fonctionnalités de l'agent étranger). Les RSUs appartenant au même domaine d'administration (réseau) sont groupés sous une seule RSU-FA formant une zone de routage (Routing Area,nommée RA). Cette RSU-FA est un point d'accès qui se trouve géographiquement au milieu de la zone de routage (RA). La RSU-FA assure la communication entre les véhicules et le monde extérieur (par exemple, Internet). Lors de l'envoi des messages d'une entité sur Internet vers une destination géographique, ces messages peuvent passer

par plusieurs RSUs, si la destination (qui peut être soit, un seul véhicule ou toute une zone géographique) est dans la portée d'une RSU qui est différente de la RSU considérée comme passerelle (RSU-FA).

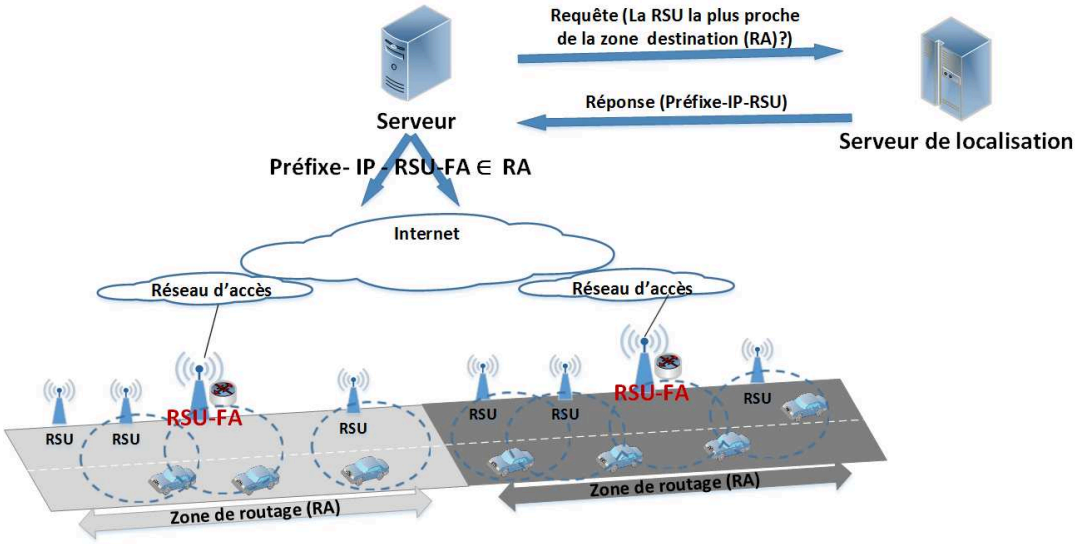

FIGURE 4.9 – Le partitionnement géographique (en RAs) avec la solution proposée (GeoMIP)

Nous nous sommes basés sur le principe de MIPv6 où l'établissement des adresses temporaires (CoA) se fait au niveau de chaque nœud mobile (véhicule) d'où l'absence d'une entité qui porte les fonctionnalités de l'agent étranger (RSU-FA). Nous avons améliorer MIPv6, en introduisant une entité (RSU-FA) afin d'assurer un handover avec un minimum de perte de paquets. Un hard handover (une seule RSU capte le nœud mobile) est utilisé dans GeoMIP avec une RSU-FA qui porte des fonctions qui permettent d'assurer la coopération entre les RSUs afin de réaliser des échanges avec un minimum de perte. En plus, Les RSU-FA se coordonnent pour un moment (durée) au niveau du réseau, ce qui permet d'assurer un handover plus efficace. La solution que nous avons adoptée a pour objectif de remplacer le soft handover, autrement dit, un hard handover avec une fonction de coopération reste moins évolué qu'un soft handover mais cela permettra d'éviter la perte élevée des paquets. La RSU-FA permet aussi d'assurer les mécanismes de sécurité avec le monde extérieur.

Notre contribution (GeoMIP) consiste à introduire GeoNetworking dans Mobile IP, notre approche d'adressage est une amélioration de la solution GeoSAC [79]. Avec la solution GeoSAC, chaque portée d'une RSU est considérée comme une RA, ce qui ne permet pas à une entité sur Internet d'envoyer des données vers des sous-zones de RA, contrairement à notre nouvelle solution GeoMIP où l'envoi peut se faire vers des sous-zones de RA. Faire adapter MIPv6 au réseau ad-hoc hybride (dans ce cadre d'applications véhiculaires) nécessite l'intégration de mécanismes supplémentaires.

4.6.1 Combinaison de l'adresse IP avec l'adresse Géographique

Le nœud mobile (MN) peut être atteint via deux modes d'adressage :

— Adresse unicast (adresse IP) : via une adresse temporaire (CoA) et au niveau de la micro mobilité, une adresse locale routable (adresse of routing area, nommée AoRA) a été introduite pour que le nœud mobile ne change pas d'adresse temporaire (CoA) tant qu'il reste dans le même domaine d'administration (Routing Area).
— Adresse Broadcast (adresse géographique) : dans le cas où la destination est une zone géographique, et la source peut être soit,
  — Un véhicule : dans ce cas, le protocle GeoNetworking est appliqué entre les véhicules. (plusieurs solutions ont été proposées dans la partie communication V2V).
  — Une infrastructure : dans ce cas, l'adresse destination est composée d'une partie IP et d'une autre partie géographique.

  L'infrastructure peut être :
  — Un passage par le cellulaire (ex. Un opérateur Orange),
  — 4G LTE privé (réseau privé),
  — RSU (ITS-G5).

Dans cette section, nous nous focalisons sur le problème de la localisation de la navette à temps réel, plus particulièrement à quel(les) RSU(s) la navette est attachée. Pour ce faire, notre contribution est au niveau inférieur (VANET), c-à-d au niveau du domaine ITS (figure 2.12). L'architecture proposée a pour objectif de permettre aux nœuds mobiles de garder leurs adresses temporaires (CoA) même s'ils changent de points d'accès (RSUs) appartenant au même domaine (RA), ceci évite de solliciter l'agent mère à chaque déplacement et donc d'éviter de surcharger le réseau.

Pour rappel, notre solution consiste à partitionner les zones géographiques en Routing Area (RAs). Chaque RA possède une RSU-FA qui joue le rôle d'une passerelle et les autres RSUs jouent le rôle de point d'accès, liées à cette RSU-FA qui se trouve dans leurs RA. Pour assurer un échange entre une entité sur Internet et le(s) véhicule(s) dans la RA, notre approche constitue une adresse IP routable avec une adresse GeoNet. Pour ce faire, la partie qui reste de l'adresse IP sera une adresse géographique (Géo-Adresse) comme illustré sur la figure 4.10. sachant que, la partie hôte peut être :

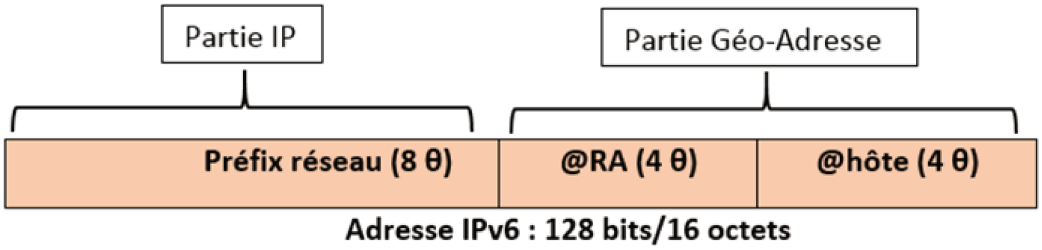

FIGURE 4.10 – Format d'addresse (128 bits/16 octets)

— Un seul véhicule (Unicast),
— Toute la zone RA (Broadcast),
— Une sous zone de RA (calculée en se basant sur les coordonnées de la zone de couverture et l'addresse MAC d'une RSU).

D'après le standard ETSI [2], l'adresse MAC d'une entité (véhicule ou de la RSU) est sur 6 $octets$. Les coordonnées géographiques (X,Y) d'une zone (geoArea) est sur 14 $octets$, comme spécifié dans [1] d'où la nécessité d'utiliser une fonction de hachage : Hash (14 octets) = 4 octets et Hash (6 octets) = 4 octets.

La fonction de hachage $H()$ prend N attributs géographiques de la zone de routage RA_i (par exemple : pour une zone géographique rectangulaire : Les attributs géographiques (A_i) représentent la longitude et la Latitude du centre), exprimé comme suit :

$$\text{H}(A_1,A_2 \ldots\ldots A_N) = (h_1,h_2 \ldots\ldots h_n) \text{ où } h_i \in \{0,1\}$$

Chaque véhicule ou RSU génère une valeur de hachage comme illustré sur la figure 4.11 et au niveau du serveur de localisation, une valeur est générée à partir des coordonnées géographique de chaque zone de routage comme illustré sur la figure 4.12.

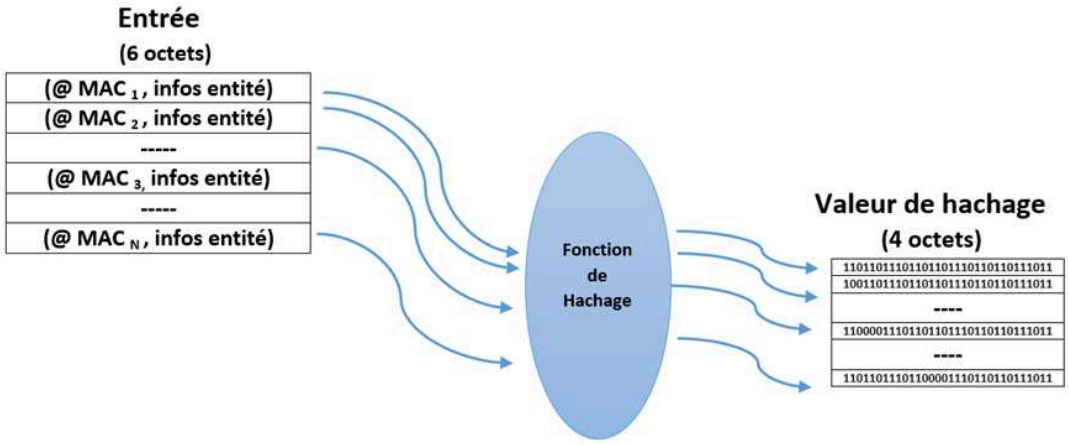

FIGURE 4.11 – Fonction de hachage pour l'addresse MAC

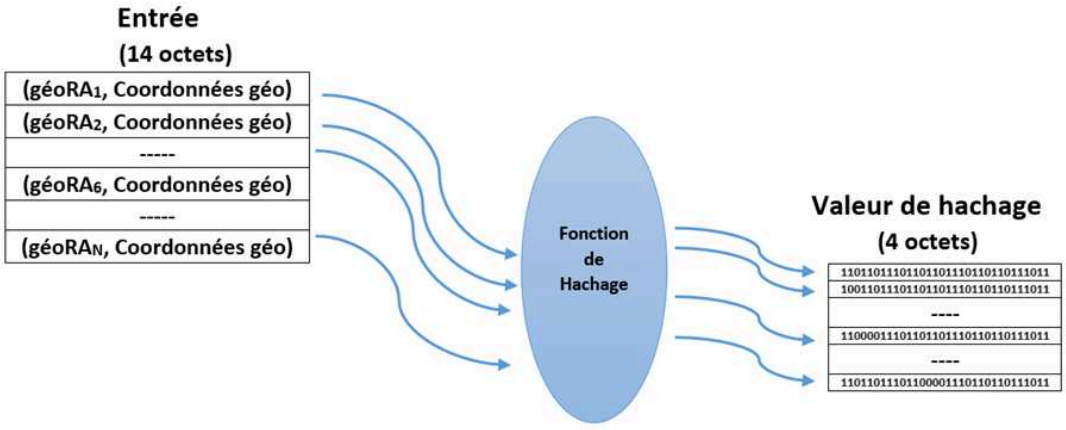

FIGURE 4.12 – Fonction de hachage pour la zone de routage (RA)

Pour mettre en œuvre ces opérations de hachage, une des fonctions de hachage qui peut être utilisée est la fonction FNV [5], cette dernière permet un hashage simple et garantit l'unicité de l'adresse, qui est déjà assurée par notre architecture d'adressage.

La figure 4.13 illustre l'adressage proposé avec notre architecture :

— Un nœud mobile (MN) porte deux adresses :
  - Adresse temporaire CoA sous la forme : PrefixRéseau.@RA.@MAC-MN, cette adresse permet de localiser le mobile au niveau du réseau (macro). Pour rappel, cette adresse ne change pas tant que le mobile reste dans la même RA. Cela permet d'éviter de solliciter le HA quand un véhicule traverse des RSUs appartenant à la même RA.
  - Adresse locale routable AoRA sous la forme : PrefixRéseau .@RA. [@MAC-RSU+@MAC-MN], cette adresse permet de localiser le véhicule au niveau de chaque RSU (assurer la mobilité au niveau micro) et permet aussi une communication en unicast avec le véhicule.
— Chaque RSU (y compris la RSU-FA) porte différentes adresses, qui sont :
  - Un préfixe Unicast de la RSU-FA, connu par le serveur de localisation qui est sous forme :
    PrefixRéseau.@RA.
  - Une adresse de diffusion (Broadcast) au niveau de la RSU-FA sous forme :
    PrefixRéseau.@RA.255, dans le cas où la destination est toute la RA.
  - Une adresse Unicast de la RSU, sous forme :
    PrefixRéseau.@RA.[@CG+@MAC-RSU], dans le cas où la destination est une sous-zone de la RA.
  - Une adresse de diffusion au niveau de la RSU (Geocast), sous forme :
    PrefixRéseau.@RA.@CG, dans le cas où la destination est une sous-zone de la RA.

4.6.2 Méthode proactive

Comme mentionné précédemment, cette nouvelle architecture est conçue pour la remontée des informations vers une entité sur Internet ou bien pour qu'une entité sur Internet puisse communiquer à temps réel avec le(s) véhicules sur l'autoroute. Ces informations transitent en passant par une passerelle, cette dernière représente dans notre architecture une RSU-FA. Chaque RSU-FA a une table de localisation qui porte les entrées suivantes :

— CoA-MN : ne change pas quand le nœud mobile (MN) reste dans la même RA. Elle change quand le MN se déplace d'une RA à une autre.
— L'adresse des RSUs : change avec la mobilité d'un nœud mobile. L'objectif étant de localiser le nœud mobile.
— AoRA -MN (adresse local routable) : change d'une RSU à une autre.

La table au niveau de la RSU-FA contient les nœuds mobiles qui sont attachés à chaque RSU en temps réel, ce qui permet de localiser les nœuds mobiles à tout moment. Cette table est mise à jour d'une manière proactive.

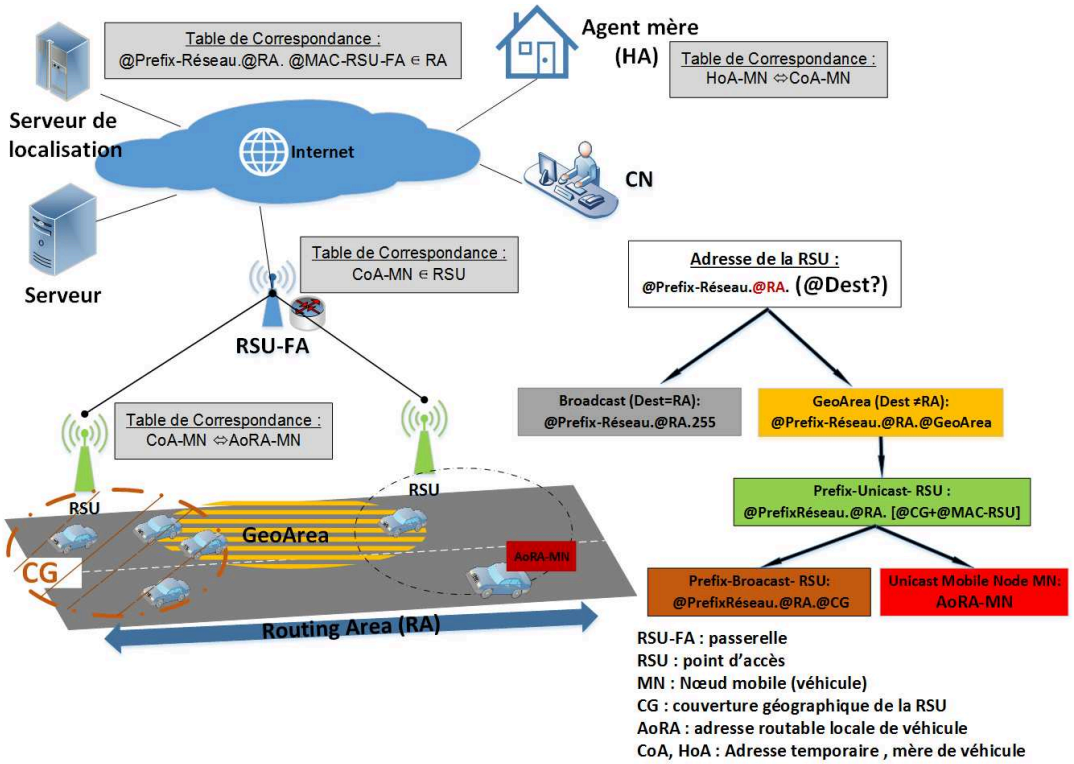

FIGURE 4.13 – Adressage hiérarchique proposé

4.6.3 Groupement des RSUs sous une seule zone de routage (RA)

La zone géographique est partitionnée géographiquement en zones de routage (RA) où chaque RA est un domaine d'administration. Le groupement des RSUs sous une seule RSU-FA se fait par zones de routage. Autrement dit, une seule RSU-FA par RA.

4.6.3.1 GeoMIP avec la zone de routage comme destination (Geobroadcast)

Due à l'apparition de la latence et à la surcharge (signalisation) du réseau avec la solution Mobile IPv6. Notre solution consiste à introduire la notion de zone de routage (RA) représentée par une passerelle (RSU-FA) qui assure la liaison avec le monde extérieur ainsi qu'avec les RSUs qui se trouvent dans cette RA.

La figure 4.14 illustre l'échange des messages lors d'une communication entre un serveur vers une zone géographique (DL). Cette dernière représente toute la zone de routage (RA). Un serveur qui veut s'adresser à la zone de routage (RA) demande la localisation de la RSU-FA responsable de cette RA au serveur de localisation. Ce dernier lui répond avec l'adresse IP de la RSU-FA. Ensuite, le serveur envoie le paquet à la RA en passant par la RSU-FA via l'adresse IP de la RSU-FA.

4.6.3.2 GeoMIP avec une sous zone de RA comme destination (Geocast)

La figure 4.15 illustre l'échange de messages lors d'une communication avec une sous zone de RA, cette zone est représentée par la couleur orange dans le schéma et qui concerne dans

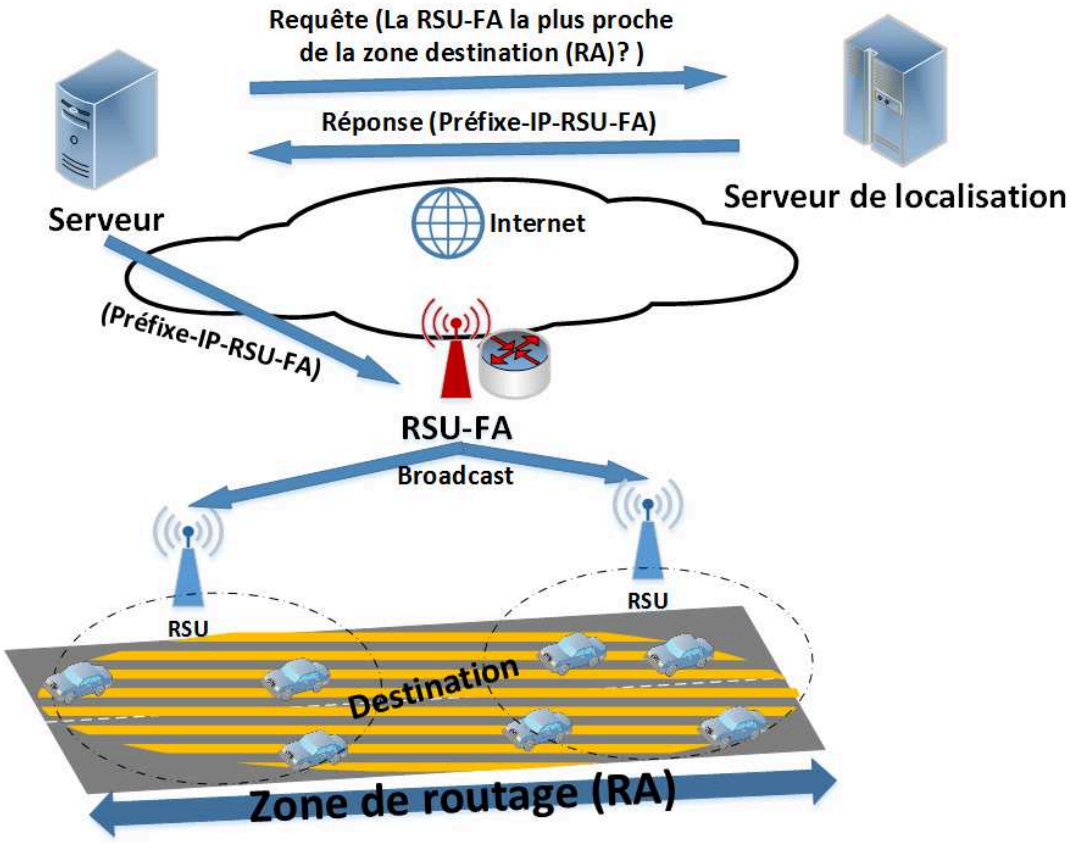

FIGURE 4.14 – GeoMIP : Geocast avec la RA comme destination

notre cas deux RSUs le 1 et 2 où le serveur demande la localisation de la RSU-FA (responsable de la RA) au serveur de localisation. Ce dernier répond avec l'adresse IP de la RSU-FA. En suite, le serveur envoie le paquet à cette RSU-FA via l'adresse IP de la RSU-FA. Cette dernière renvoie ce paquet au (x) RSU(s) qui couvrent cette sous zone destination, où chaque RSU, à son tour diffuse le paquet dans sa zone de couverture.

4.6.3.3 GeoMIP dans le cas d'une communication en IP-Unicast

L'avantage de cette nouvelle solution est qu'un nœud mobile sollicite une seule fois l'agent mère pour obtenir une adresse temporaire (CoA), tant qu'il ne change pas de zone de routage (RA). Autrement dit , l'opération de Binding Update (CoA, HoA) dans Mobile IPv6 est appliquée une seule fois par zone de routage(RA) pour chaque nœud mobile. De cette manière, tant que le nœud mobile ne change pas de RA, Il communique directement avec le CN sans solliciter l'agent mère comme illustré sur la figure 4.16.

La notion de la zone de routage reste applicable pour une communication en unicast avec moins de surcharge que la solution Mobile IPv6.

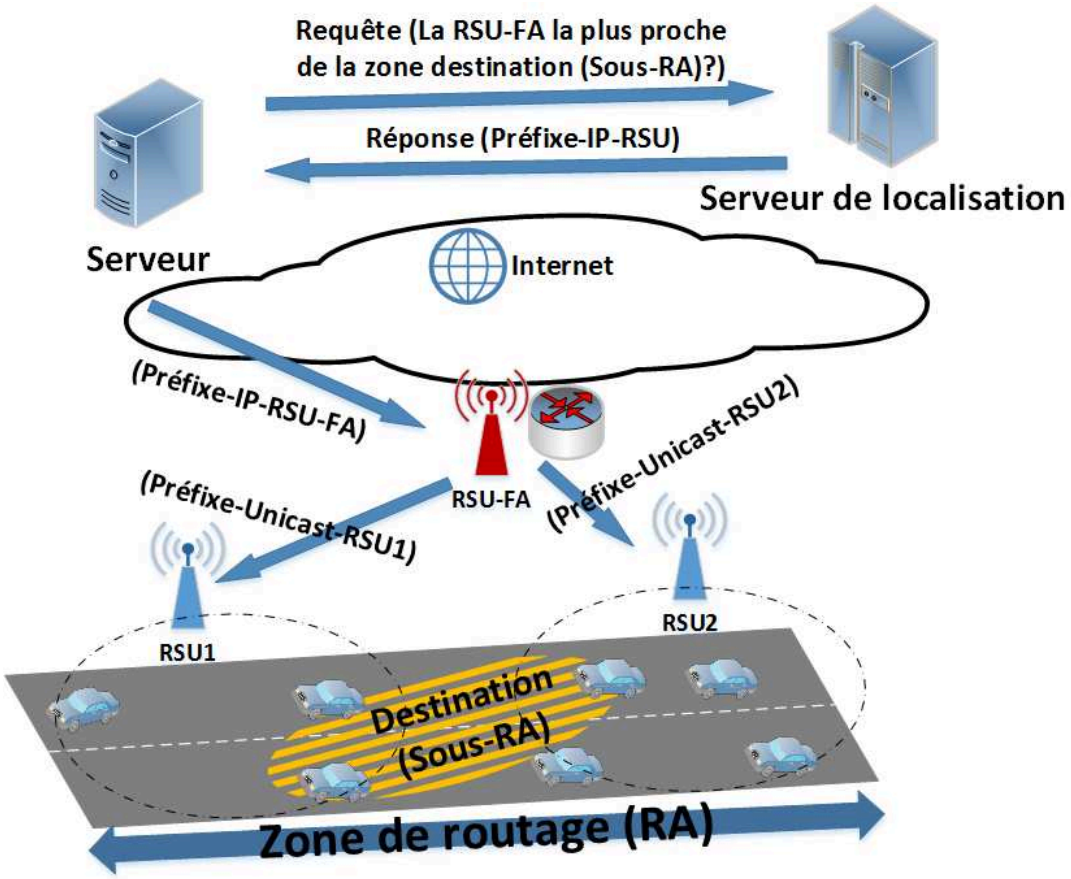

FIGURE 4.15 – GeoMIP : Geocast avec sous-zone de la RA comme destination

4.6.4 Coopération au niveau des RSU-FA

Au niveau de la RSU-FA, il y a une intelligence qui va permettre d'assurer une connectivité avec Internet. La RSU-FA porte des fonctions afin de coopérer avec d'autres RSUs et afin de communiquer avec eux tout en minimisant la perte des paquets lors d'un handover. Les figures 4.17, 4.18 montrent les étapes d'échanges lors de l'envoi des paquets de la part de CN vers un véhicule qui est sur le point de changer son point d'attachement (RSU), où le véhicule s'apprête à quitter la RSU1 pour s'attacher à la RSU2, sachant que les RSUs communiquent via le réseau filaire ou la radio.

Dans un premier temps, le paquet est transmis au RSU-FA, ce dernier se focalise sur sa table pour envoyer le paquet vers la bonne RSU (la RSU sous laquelle se trouve le véhicule). Etant donné que le véhicule est sur le point de quitter la zone de couverture de l'ancienne RSU, grâce à la coopération entre les RSUs , l'ancienne RSU va envoyer ce paquet à la nouvelle RSU et enfin cette dernière garde le paquet destiné au véhicule dans une file d'attente afin de le retirer (dépiler) de la file quand le véhicule s'accroche à elle.

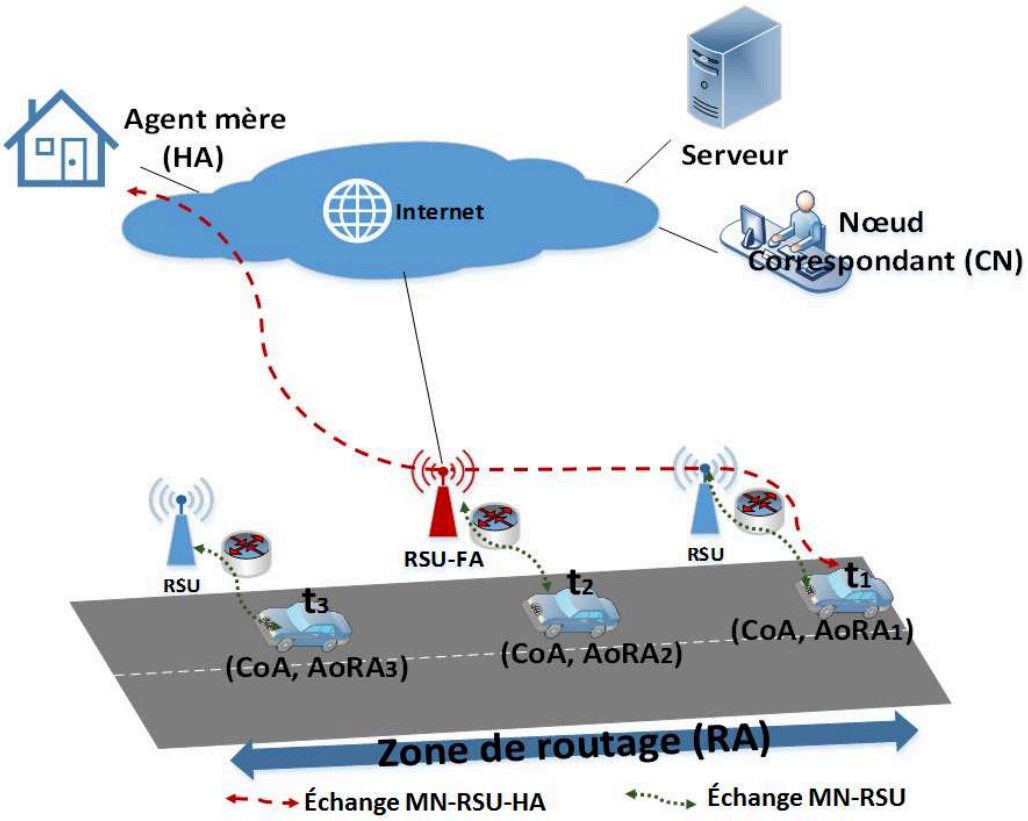

FIGURE 4.16 – GeoMIP : communication IP Unicast

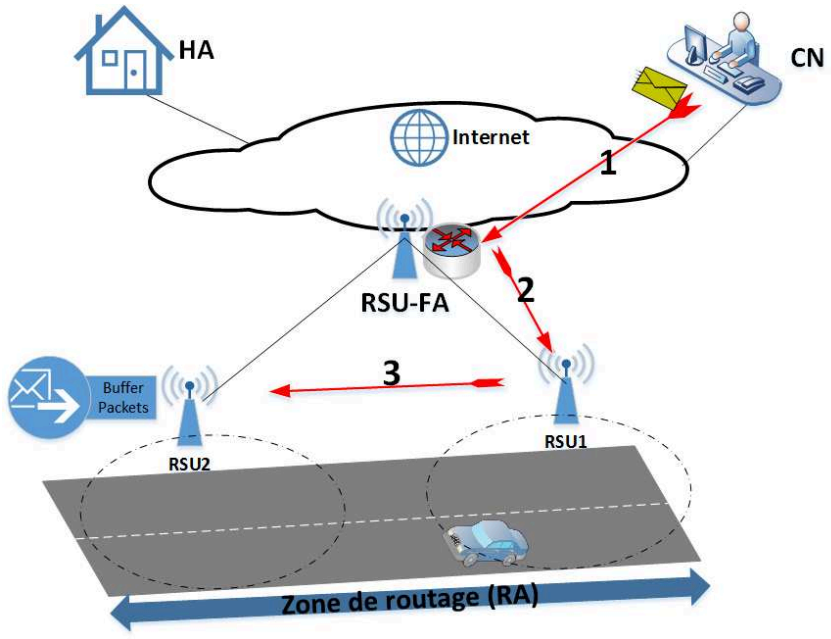

FIGURE 4.17 – Fonction de coopération entre RSUs : Buffer le paquet

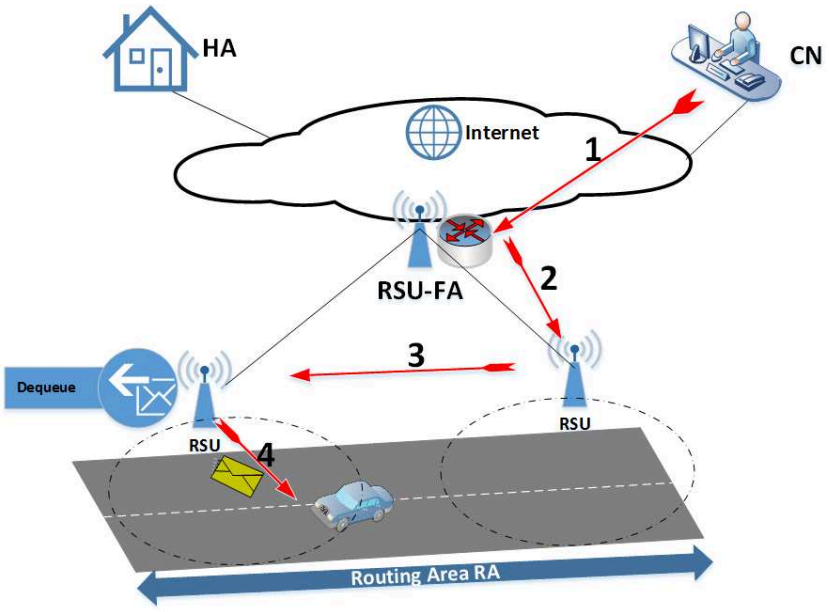

FIGURE 4.18 – Fonction de coopération entre RSUs : Dequeue le paquet

4.6.5 Aspects Sécurité et Hypothèses

Comme les applications de la sécurité routière sont critiques, particulièrement en terme de délai de communication, nous supposons que l'authentification se fait une seule fois, en supposant qu'il y ait un accord entre les réseaux opérés afin de réduire la latence lors des communications. Pour rappel, une RSU est désignée comme passerelle (RSU-FA) dans chaque domaine d'administration (RA). Ce dernier, assure la connectivité avec le monde extérieur (ex.Internet) et s'occupe des aspects liés à la sécurité (par exemple l'authentification, etc.) de telle sorte que :

— Un contrat soit établi une seule fois entre les véhiucles et l'agent mère. Ce qui assure l'économie de renégociation du contrat vu que les RSUs se coordonnent.

— Au niveau des RSUs qui s'occupent de cette négociation :

- La sécurité se règle à l'entrée dans une nouvelle RA.
- Les aspects de sécurité se passent sur le réseau filaire, ce qui soulage la charge au niveau radio.

4.7 Mécanismes d'échanges avec GeoMIP

Avec notre solution (GeoMIP), afin de localiser les véhicules lors de leurs mouvements, une gestion de leurs adresses est primordiale. Pour ce faire, chaque entités possède une table de localisation avec leurs entrées décrits ci-après.

Au niveau du nœud correspondant (CN) : l'adresse domicile (HoA) et l'adresse temporaire (CoA) de chaque nœud mobile (MN) sont connues, comme illustrée sur la table ci-dessous.

HoA-MN	CoA-MN

Au niveau du serveur de localisation : il maintient les informations sur la RSU-FA (son adresse et sa position géographique) et les informations sur le partitionnement géographique (en plusieurs RA) de la route. Grâce à cette table de correspondance montrée ci-après, le serveur de localisation pourrait répondre aux sollicitations de l'agent mère (demande de l'adresse de la RSU-FA responsable de la RA destination).

Adresse IP de la RSU-FA	Les coordonnées géo de la RSU-FA	les coordonées géo de la zone de routage (RA)

Au niveau de l'agent mère (HA) : l'agent mère possède une table d'association (HoA, CoA) de chaque nœud mobile (MN), qu'il met à jour à chaque fois que le MN entre dans une nouvelle RA.

HoA-MN	CoA-MN

Au niveau de l'agent étranger ou passerelle (RSU-FA) : selon la décomposition de la zone géographique en RA, chaque passerelle (RSU-FA) possède une vision globale des autres points d'accès (RSU) de son domaine (RSUs appartenant à la même RA). Grâce aux entrées de cette table, la RSU-FA suit le mouvement de chaque véhicule dans la RA, c-à-d elle connait l'adresse temporaire de chaque véhicule et elle sait sous quelle couverture de RSU (RSU_i) le véhicule (MN_j) se trouve à temps réel.

CoA-MN_j	Le $MN_j \in RSU_i$

Au niveau de la RSU_i (points d'accès) : chaque RSU possède une vision locale des nœuds mobiles sous sa zone de couverture. Autrement dit, la RSU connait l'adresse locale routable du mobile (AoRA-MN_j) mappée avec son adresse temporaire (CoA-MN_j).

CoA-MN_j	AoRA-MN_j

4.7.1 GeoMIP : cas de la macro mobilité

La figure 4.19 illustre l'échange lors de la marco mobilité basée sur le principe de MIP. Rappelons que la macro mobilité est le passage d'une RA vers une autre. Périodiquement, chaque point d'accès (RSU) diffuse un message d'avertissement contenant son adresse MAC et les coordonnées géographiques de sa zone de routage (étape 1). Pour la marco mobilité, le nœud mobile (véhicule) auto configure une adresse IPv6 (CoA) en se basant sur le message d'avertissement envoyé par son point d'attachement (étape 2). Ce nœud mobile communique cette adresse (CoA) à son point d'attachement(étape 3) et son agent mère (HA) via un message de mise à jour de l'association Binding Update (étape 4), l'agent mère enregistre cette association via un échange de message Binding Acknowledgement (étapes 5,6). Dans notre solution, le HA communique par la suite cette CoA au Nœud Correspondant (étape 7). De cette manière , un tunnel direct bi-directionnel est établi entre le MN et le CN

Contrairement à MIPv6, avec notre solution GeoMIP, chaque véhicule exécute les étapes illustrés sur la figure 4.19 une seule fois par RA, ce qui éviter la sollicitation de HA à la traversée des RSUs du même RA.

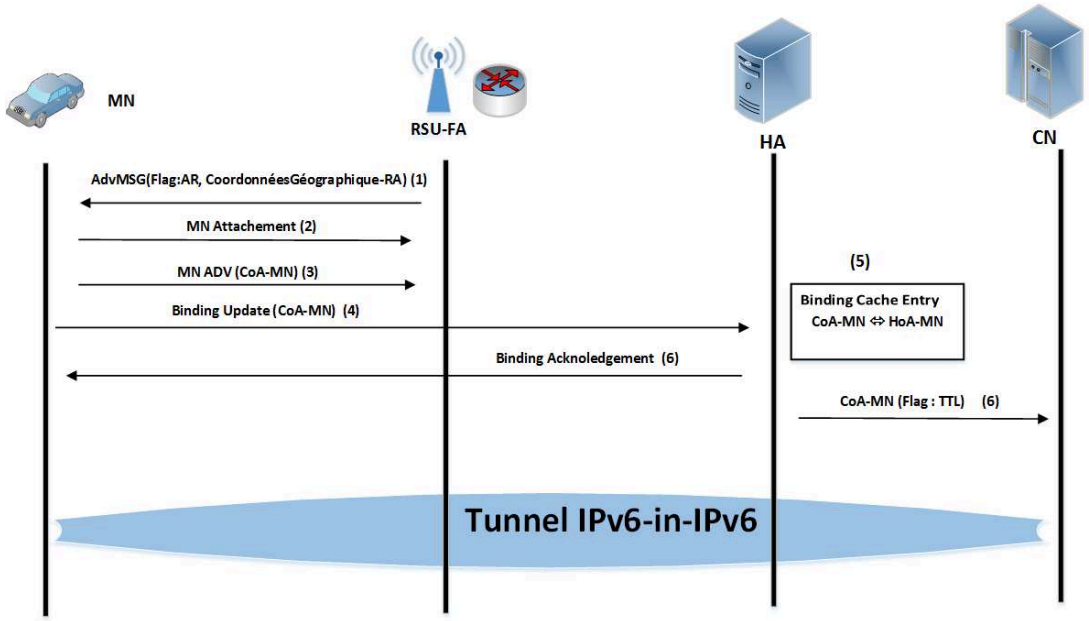

FIGURE 4.19 – GeoMIP : Marco mobilité

4.7.2 GeoMIP : cas de la micro mobilité

La gestion de la mobilité se fait aussi au niveau local (la micro mobilité), le diagramme d'échange est illustré sur la figure 4.20. A la réception du message d'avertissement de la RSU (étapes 1,2), le véhicule configure une autre adresse locale routable nommée AoRA. Cette adresse est communiquée à son point d'attachement (étapes 3-6). Cette RSU peut être différente de la passerelle (RSU-FA). Dans ce cas (RSU différente de RSU-FA), la RSU communique le CoA du nœud mobile en se basant sur une table de correspondance à son niveau (cette table contient l'association CoA, AoRA) à la RSU-FA (étapes 7-9). Au niveau de la RSU-FA, une table de correspondance existe, elle contient le CoA du nœud mobile avec l'adresse de son point d'attachement (RSU) à chaque déplacement du nœud mobile.

Dans la gestion de la mobilité, il est nécessaire de décrire les échanges dans plusieurs cas à savoir quand un Nœud Correspondant (CN) veut communiquer avec un véhicule (cas de IP-Unicast) et dans le cas où le Nœud Correspondant envoie un message vers une zone géographique (RA ou sous zone de RA). Sachant que, le deuxième type présente un cas particulier, le cas d'une destination différente de RA, est le cœur de notre contribution.

4.7.3 GeoMIP : CN vers un véhicule (IP-Unicast)

Le CN qui envoie pour la première fois le paquet connait seulement l'adresse HoA du véhicule. Le HA prévient le CN de l'adresse temporaire (CoA) du véhicule avec une durée de vie dans le but d'éviter le routage triangulaire. Rappelons que le routage triangulaire a été décrit dans le chapitre 2.

Quand un CN envoi des données à un véhicule, lors du premier envoi, le CN encapsule le paquet de données avec l'adresse HoA et il sera envoyé à son HA (étape 1), ensuite ce

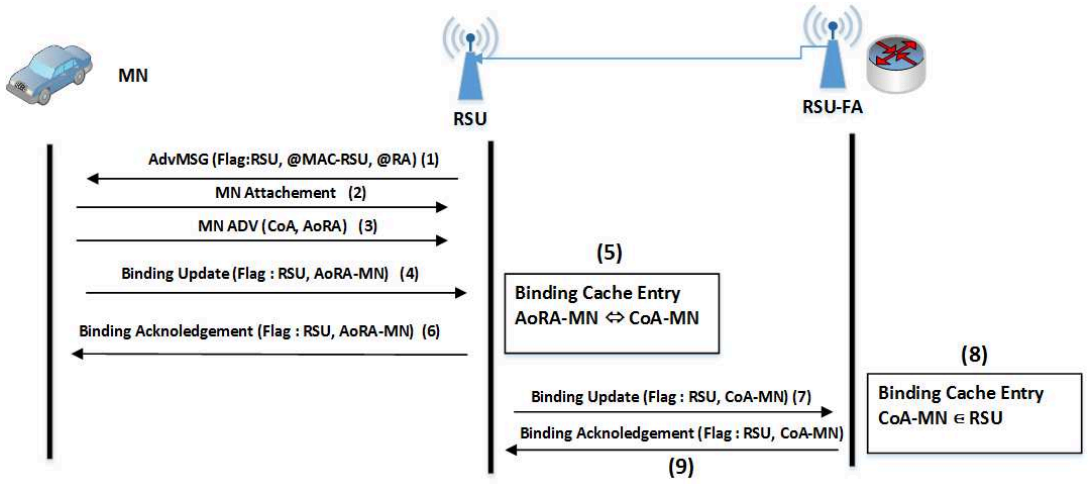

FIGURE 4.20 – GeoMIP : Micro mobilité

dernier encapsule le paquet avec l'adresse temporaire du véhicule (CoA) et envoie à la RSU-FA responsable de la RA où se trouve le véhicule (étape 3). Grâce à la table de correspondance entre l'adresse temporaire CoA et l'adresse locale routable AoRA, la RSU-FA encapsule le paquet avec AoRA et l'envoie à la RSU où se trouve le véhicule (étapes 4,5). A partir du deuxième envoi, l'échange se fait directement entre le véhicule et le CN via son CoA (étape 6). Voir la figure 4.21.

4.7.4 GeoMIP : Serveur vers une zone géographique

Deux cas se présentent, dans le cas où la zone de destination représente toute la zone de routage (RA), comme illustré sur la figure 4.22, le serveur envoie une requête de demande de localisation de la RSU-FA au serveur de localisation (étape 1), ensuite ce dernier répond (étape 2) avec le préfixe unicast de la RSU-FA (la RSU-FA qui se trouve dans cette RA). A partir de cet échange, le serveur envoie le paquet directement à la RSU-FA (étape 3). Une fois le paquet est arrivé au niveau de la RSU-FA, cette dernière encapsule le paquet avec l'adresse broadcast où toutes les RSUs à sa portée (dans sa RA) reçoivent le paquet (étape 4), ensuite chaque RSU à son niveau diffuse en Broadcast (PrefixRSU=@FA.@RA.CG) le paquet dans sa zone de couverture (étape 5).

Dans le cas où la zone destination est une sous zone de la zone de routage (RA), comme illustré sur la figure 4.23, le serveur envoie une requête de localisation de la RSU-FA au serveur de localisation (étape 1). Ensuite, ce dernier répond avec le préfixe unicast de la RSU-FA appartenant à cette RA (étape 2). A partir de cet échange, le serveur envoie le paquet directement à la RSU-FA (étape 3). Une fois le paquet est arrivé au niveau de la RSU-FA et comme cette dernière connait la position et l'adresse IP de chaque RSU se trouvant à sa portée, cette fois-ci, la RSU-FA encapsule le paquet avec le préfixe unicast de la RSU (étape 4) responsable de la sous-zone destination. Deux cas se présentent, le cas où la RSU à son niveau Broadcast le paquet dans toute sa zone de couverture (CG), ou bien la RSU envoie en unicast à un véhicule en utilisant son adresse locale routable (AoRA) (étape 5).

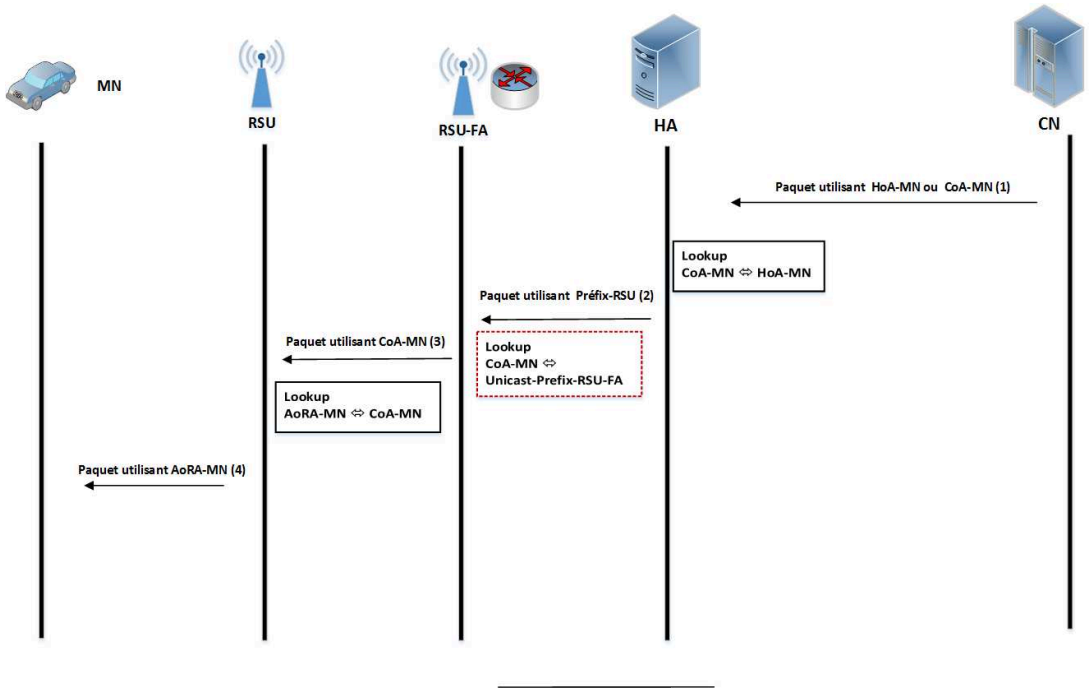

FIGURE 4.21 – GeoMIP : CN vers véhicule (IP-Unicast)

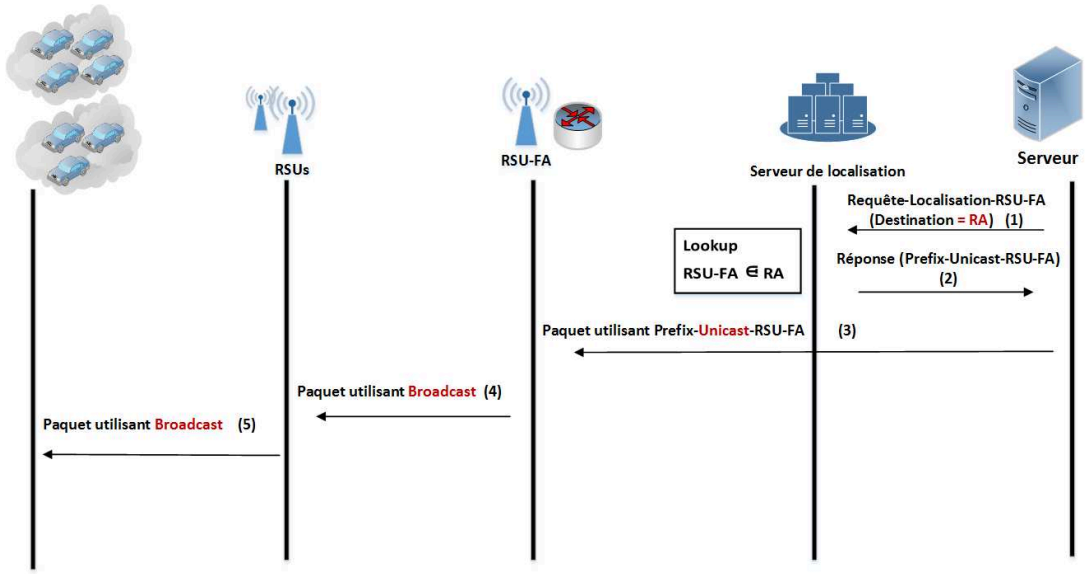

FIGURE 4.22 – GeoMIP : Serveur vers une zone géographique (destination est la RA)

Pour rappel, ce deuxième cas présente le cœur de notre contribution. Le serveur peut envoyer des paquets à une sous zone de la zone de routage (RA), contrairement à la solution GeoSAC [79] où la zone destination ne peut être que toute la RA.

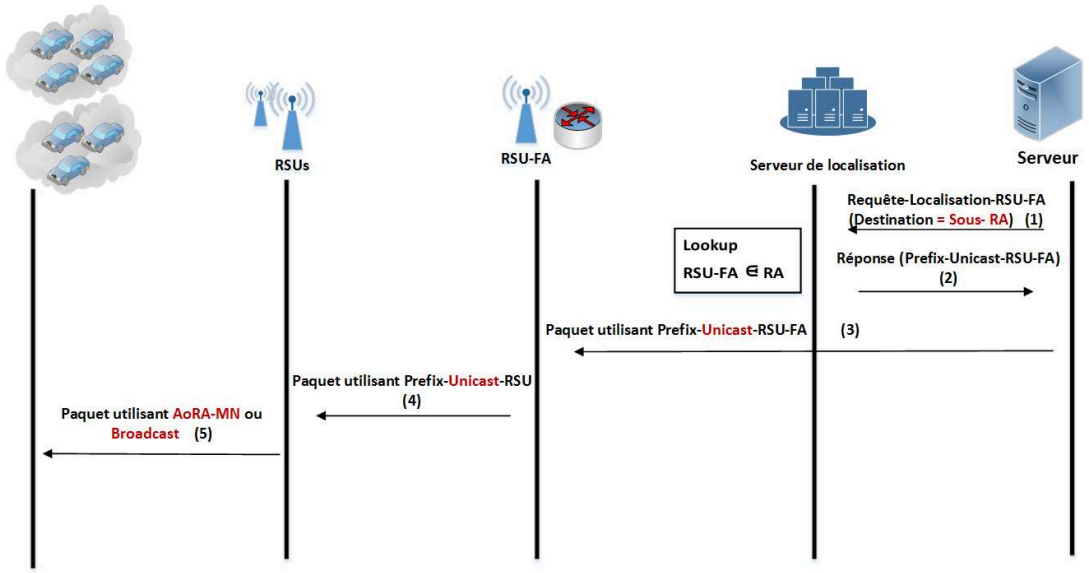

FIGURE 4.23 – GeoMIP : Serveur vers une zone géographique (destination est une sous-zone de la RA)

N'oublions pas que le véhicule est susceptible de changer sa position. Deux cas se présentent : le premier, quand le véhicule change de RA,le deuxième, quand le véhicule change de RSU mais reste dans la même RA.

4.7.4.1 GeoMIP : Changement de RA

La figure 4.24 montre le diagramme d'échange lors du changement de zone de routage (RA) avec un hard handover (transfert anticipé). Quand le CN envoie le paquet (destiné au véhicule) à la RSU-FA qui se trouve dans l'ancienne RA, sachant que le MN est sur le point de quitter l'ancienne RA et d'entrer à la nouvelle RA. Une des méthodes qui permet d'optimiser le déplacement du véhicule est d'utiliser le hard handover où la connexion à l'ancienne RSU-FA est rompue avant (ou au même moment) l'établissement de la liaison avec la nouvelle RSU-FA. Une fois le MN configure une nouvelle CoA dans sa nouvelle RA. Il communique cette adresse à son ancienne RSU-FA (étape 1). Dans ce cas, l'ancienne RSU-FA qui reçoit le paquet de la part de CN (étape 2), envoie le paquet encapsulé avec la nouvelle CoA de MN à la nouvelle RSU-FA (étape 3). Une fois le MN est enregistré dans la nouvelle RSU-FA (obtient une nouvelle CoA dans la nouvelle RA), la RSU-FA transmet le paquet au véhicule directement avec la nouvelle CoA sans passer par l'ancienne RSU-FA.

4.7.4.2 GeoMIP : Changement des RSUs dans la même RA

La figure 4.25 illustre le diagramme d'échange lorsqu'un véhicule change de RSU appartenant à la même RA avec un message envoyé par le CN vers ce véhicule comme

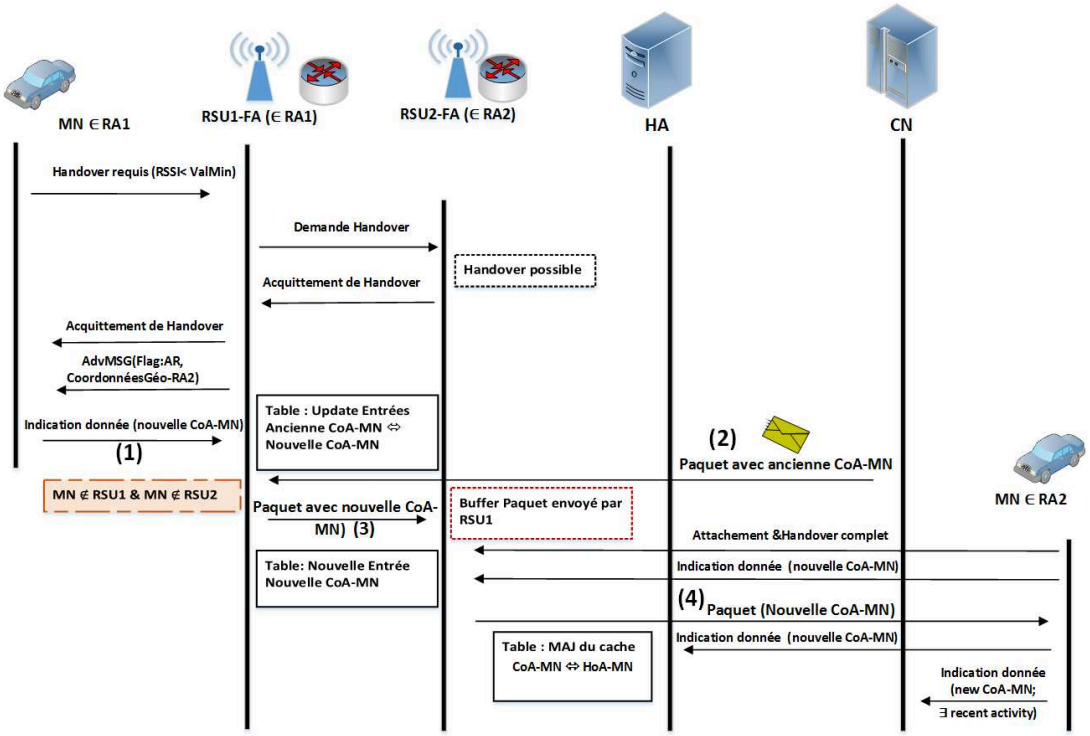

FIGURE 4.24 – GeoMIP : Changement de RA

destination. Sachant que, ce nœud mobile va se retrouver pour un moment en dehors de la portée des deux RSUs.

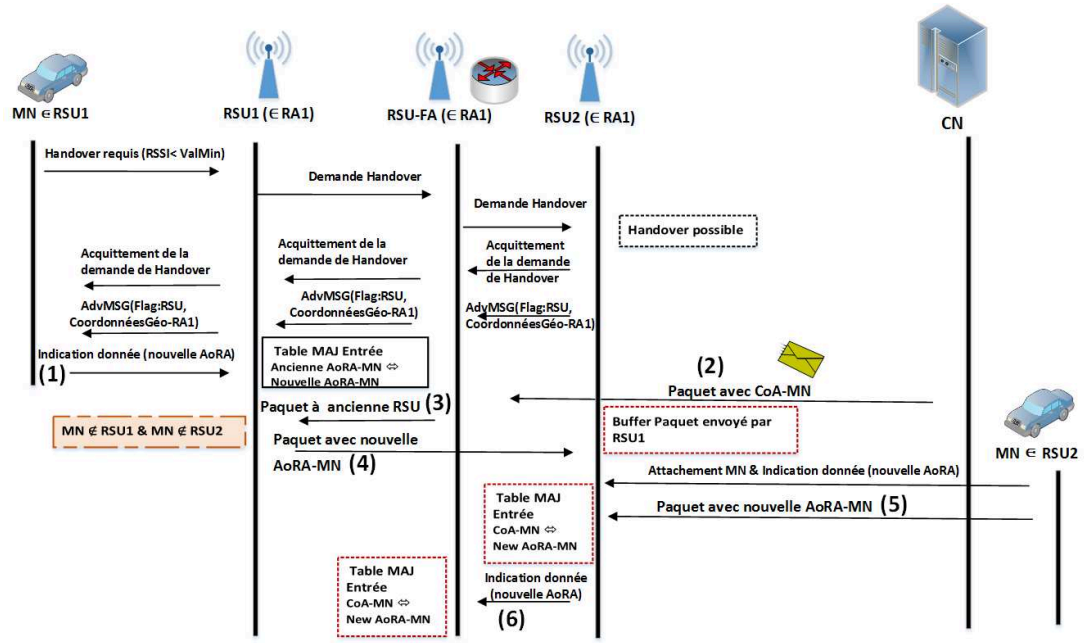

FIGURE 4.25 – GeoMIP : Changement des RSUs dans la même RA

Quand le CN envoie le paquet à l'ancienne RSU passant par la RSU-FA, sachant que le MN est sur le point de quitter la portée de cette RSU et d'entrer dans la portée d'une nouvelle RSU. Un hard handover est appliqué où la connectivité du véhicule avec l'ancienne RSU est rompue avant (ou au même moment) l'établissement de la liaison avec la nouvelle RSU. Au niveau local, une fois le véhicule configure une nouvelle adresse routable locale (AoRA) avec sa nouvelle RSU , il communique cette adresse à son ancienne RSU (étape 1). A cet instant, quand la RSU-FA reçoit un paquet avec le CoA de véhicule (CoA-MN) de la part de CN (étape 2), la RSU-FA envoie ce paquet à l'ancienne RSU (étape 3). Comme le véhicule ne se trouve pas dans la portée de l'ancienne RSU, cette dernière envoie le paquet avec la CoA-MN à la nouvelle RSU (en passant par la RSU-FA) (étape 4). La nouvelle RSU garde le paquet jusqu'à ce que le véhicule s'attache à elle (étape 5). Enfin, la nouvelle RSU informe la RSU-FA de la nouvelle adresse routable (AoRA-MN) du véhicule (étape 6), ce qui permet à la RSU-FA de localiser le véhicule au niveau micro d'où l'intérêt d'une adresse locale (AoRA).

4.8 Analyse de la solution

4.8.1 Description du système

Nous supposons que l'on a un réseau véhiculaire sur une route à plusieurs voies (autoroute) composée de plusieurs RSUs. La route est partitionnée sur plusieurs domaines et chaque domaine est constitué de plusieurs cellules. Dans chaque domaine une seule RSU joue le rôle de RSU-FA. Afin de comprendre la différence avec MIPv6, les schémas 4.26, 4.27 montrent bien qu'une RA n'est plus une seule cellule avec une seule RSU mais plusieurs cellules contrôlées par une RSU-FA, , où N est le nombre totale de cellules et m est le nombre de cellules par domaine.

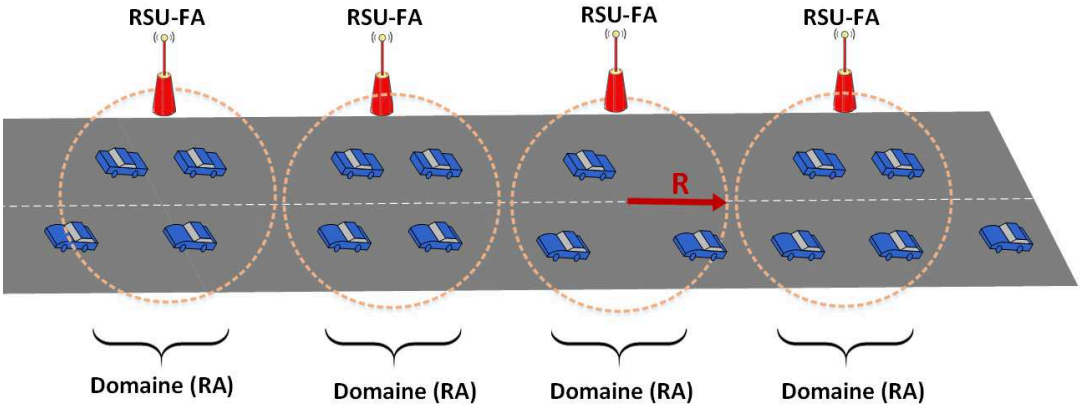

FIGURE 4.26 – Cas de Mobile IP (MIP)

Quand le véhicule se déplace , il peut changer de domaines (RA) ou de cellules. Il est donc nécessaire de suivre cette mobilité. Pour ce faire, un des schéma d'échange de messages de signalisation (BU/BA) décrit ultérieurement dans la section 4.7 est déclenché. Cela introduit un coût en terme de surcharge et de délais. En effet, le nombre de nouvelles adresses (CoA,

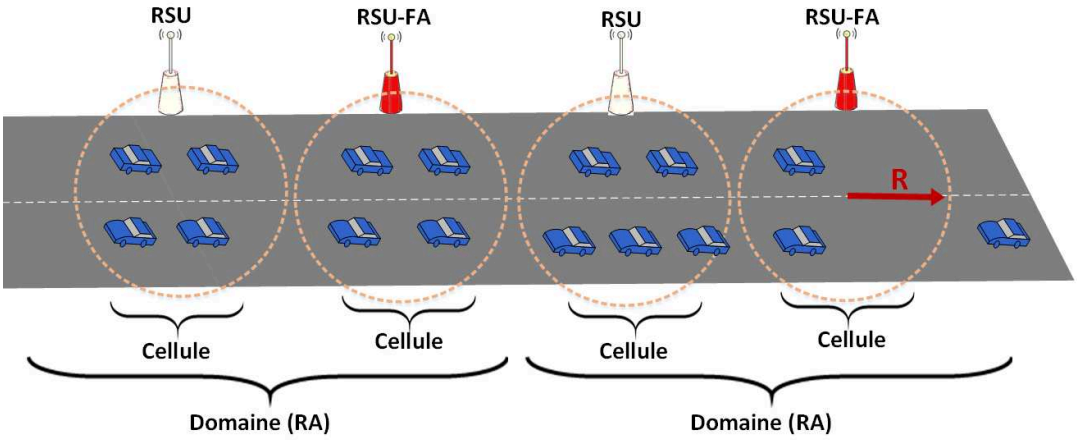

FIGURE 4.27 – Cas de la solution proposée (GeoMIP)

AoRA) détermine le nombre de RSU-FA /RSU impliquées précédemment, ce qui influe sur le coût de signalisation.

En se basant sur le MIPv6 conventionnel, le véhicule configure une nouvelle adresse dans chaque cellule visitée (pour rappel, dans MIPv6 une cellule est un domaine et chaque RSU est une RSU-FA). Ce comportement est à l'opposé de la solution que nous proposons (GeoMIP), où précisément les RSUs sont regroupées sous une seule RSU-FA (agent étranger) et la même adresse IP temporaire (CoA) est utilisée par le nœud mobile dans toutes les cellules de la même zone de routage (c'est à dire du même domaine où rappelons le, un domaine est composé d'un ensemble de cellules).

Tant que le véhicule se déplace dans des cellules appartenant au même domaine et ne le quitte pas, il pourrait utiliser la même adresse IP temporaire (CoA) configurée dans toutes les cellules appartenant au même domaine. Pour gérer la micro mobilité, le véhicule configure une adresse locale routable (AoRA) qui change en changeant de RSU sans solliciter l'agent mère (HA). Par conséquent, un aspect clé de notre analyse des coûts est le coût lié à la signalisation du changement d'adresse en tenant compte du nombre moyen de véhicules et le nombre de handover qui dépend du nombre de cellules (ou domaines).

Afin d'évaluer les performances de notre proposition (GeoMIP), il est important d'estimer le coût de cette signalisation. Pour ce faire, nous allons dans ce qui suit, modéliser le système décrit ci-dessus.

4.8.2 Formulation du problème et hypothèses

Afin d'évaluer le coût de la signalisation d'un système appliquant notre solution GeoMIP, nous émettons quelques hypothèses.

Chaque RSU a un rayon de couverture R et chaque domaine est composé de plusieurs cellules. Afin d'estimer le volume du trafic de contrôle échangé au niveau d'une RSU, définie comme couverture de la zone desservie par une RSU. L'objectif étant de calculer le nombre moyen de véhicules dans une cellule.

— Les RSUs sont déployées comme suit, une RSU couvre une cellule avec une forme

circulaire de rayon R formant un sous réseau (portée-RSU). la route est découpée en domaines d'administration (ou zones de routage) nommés RA (Routing Area).

— Les RSUs et la RSU-FA peuvent communiquer entre elles via le réseau filaire ou radio.

— Avec notre solution GeoMIP (figure 4.27), chaque domaine est composé de m cellules dont une seule RSU dans chaque domaine porte la fonctionnalité de l'agent étranger (RSU-FA).

— Avec le MIPv6 conventionnel (figure 4.26) , chaque cellule est un domaine et la configuration de l'adresse change lorsque le véhicule se déplace entre les RSUs (toutes les RSU sont des RSU-FA). Ce qui n'est pas notre cas.

Pour mener à bien l'estimation du coût, nous allons définir les paramètres suivants :

— Le nombre total de cellules est : N.

— Le nombre de domaines pour les approches est calculé comme suit :
  - N dans le cas de MIP, car il y a autant de domaines que de cellules.
  - $\lceil \frac{N}{m} \rceil$ dans le cas de la solution proposée, où m est le nombre de cellules par domaine.

— H_{HA}^{CN} : c'est le nombre moyen de sauts entre l'agent mère (HA) et le nœud correspondant (CN). Nous supposons que le CN est à la même distance de HA que du serveur de localisation que de la RSU-FA. C'est à dire : H_{HA}^{CN}=$H_{serveur}^{CN}$=H_{RSU-FA}^{CN}=H_{RSU-FA}^{HA}

— On suppose que le MN est directement attaché à la RSU et que l'on pas besoin de passer par un autre nœud pour y accéder. C'est à dire : H_{MN}^{RSU} = 1.

— H_{MN}^{RSU-FA}=1 si RSU-FA=RSU sinon H_{MN}^{RSU-FA} est la moyenne du nombre de saut entre les deux entités.

— C_u^d, C_u^c : Le coût de traitement lors d'une mise à jour de la liaison (BU/BA) (voir les figures 4.19 et 4.20) dans un domaine, dans une cellule respectivement.

— T_{L2}, T_{AU} : c'est la durée de traitement au niveau de la couche liaison (L2) et celle du processus d'authentification.
  Il est à noter que l'opération liée à ces deux paramètres ne dépend pas du protocole de la mobilité au niveau de la couche 3. En effet, l'élément précédent est lié à la technologie sans fil déployée, alors que l'authentification est liée aux mécanismes de sécurité utilisés, qui ne sont pas forcément étroitement liés à la mobilité [49]. En outre, nous supposons que ces deux paramètres sont négligés dans l'analyse des deux approches.

— M_{msg} : la taille du message échangé, il s'agit de la taille du paquet de données. On suppose qu'elle est la même pour GeoMIP et pour MIP.

— $T_{Radv-min}$, $T_{Radv-max}$: la valeur minimale, maximale respectivement des temporisateur d'avertissement pour les messages d'avertissement (Router Advertisement messages). Ils sont définis dans le RFC 6275. Ces paramètres sont utiles pour calculer la durée de configuration d'une adresse.

4.9 Modèle de la mobilité

Notre objectif est d'analyser lors d'un handover le volume du trafic de contrôle échangé, qui peut être soit local et qui correspond à la signalisation entre le véhicule et la RSU, soit global et qui correspond à la signalisation entre le véhicule et son agent mère. Il est à noter que

ce volume est corrélé sur une durée. Il existe deux types de handover :

Le handover vertical (entre domaines) :

La variabilité de la vitesse de la traversée de la cellule conduit à modéliser le temps de séjour par une distribution Exponentielle. Les arrivées exogènes suivent le processus de Poisson. Ces hypothèses conduisent à un modèle d'attente Markovien au niveau de la cellule.

Un handover entre domaines donne un temps de séjour sur les m cellules des deux domaines qui est une somme d'exponentiel qui donne $Erlang$ d'ordre m dans un domaine composé de m cellules.

Dans notre étude, la traversée de deux domaines revient à la traversée de deux cellules avec un volume de trafic de contrôle différent à savoir local (cas des cellules du même domaine) et global (cas des cellules appartenant à deux domaines différents). Ceci nous a mené à modéliser les cellules comme une file d'attente sans considérer les domaines.

Le handover horizontal (entre cellules du même domaine) :

Il s'agit du changement de cellules dans un même domaine, le processus est Markovien. La traversée des cellules appartenant à un même domaine (RA) génère un trafic local. Dans ce qui suit nous allons modéliser ce handover entre les cellules, en utilisant la théorie des files d'attente. L'objectif est de calculer $E(V)$, le nombre moyen de véhicules dans une cellule (desservie par une seule RSU).

Le modèle considéré est un réseau de files d'attente en série (Figure 4.28). Ce réseau est régi par une arrivée de véhicules extérieure suivant une loi de Poisson et des temps de service exponentiellement distribués général et indépendant.

Nous avons supposé que dans notre système il y a uniquement une seule classe de mobile. Dans ce contexte mono-classe le temps de traitement est similaire que le véhicule soit de type voiture, navette ou camion, etc. Ainsi, peut-on généraliser notre modèle de réseaux de file d'attente à forme produit par un réseau BCMP avec des nœuds de type M/GI/∞. Le système présente une variabilité de temps de traitement dans la cellule, ce qui correspond à des modèles M/GI/∞ où nous avons considéré en particulier le cas $GI = M$ ce qui amène à un réseau de Jackson [60] ouvert.

Soit N_1,N_2,...,N_n, le nombre de véhicules respectivement dans la file 1,2,...n. Le réseau est défini par les valeurs de P (N_1,N_2,....N_n, t) : probabilité d'être au temps t dans l'état N_1, N_2,...N_n (cette probabilité est appelée probabilité jointe). Notre modèle représente bien une chaîne de Markov à temps continu avec un espace d'état C^n.

A l'état stationnaire (état d'équilibre), notre réseau de files d'attente peut s'exprimer sous forme produit comme suit :

$$P\{N_1 = i_1, N_2 = i_2 ... N_n = i_n\} = \prod_{j=1}^{n} P\{N_j = i_j\} \tag{4.1}$$

i_j : le nombre de véhicules dans une cellule j.

n : le nombre de cellules total.

$P\{N_j = i_j\}$: la probabilité d'avoir i_j véhicules dans la cellule j.

— Chaque cellule est considérée comme une file d'attente car les arrivées et les sorties des véhicules suivent le processus de Poisson avec un serveur qui est la cellule. Où :

— La capacité dans chaque cellule est limitée, qui est C et qui correspond au nombre maximum de véhicules dans une cellule.
— Le processus d'arrivée des véhicules est distribué selon un processus de Poisson de paramètre λ.
— Le processus de temps de service (service iid) est indépendant du processus d'arrivée et suit la loi exponentielle de paramètre μ.
— On considère un seul serveur qui correspond à la RSU dans une cellule.
— Les cellules ont le même rayon (R), et la vitesse moyenne des véhicules est de S'.
— Le temps de la traversée de la cellule (séjour) est l'intervalle de temps qui sépare l'instant d'entrée à la cellule et de la sortie de cette dernière, qui est lié à la vitesse moyenne des véhicules.
— Le taux d'utilisation du premier serveur ($j = 1$) est donné par :

$$\rho_1 = 1 - \sum_{\substack{i_j \\ i_j \neq i_1}} P\{N_1 = 0, N_2 = i_2, N_3 = i_3, ..., N_n = i_n\} \tag{4.2}$$

Une généralisation de la formule ci-dessus, nous permet de déterminer le taux d'utilisation des autres serveurs du réseau ($\rho_{j,j=2,3...,n}$).
— Le nombre moyen de véhicules dans la première cellule ($j = 1$) est donné par :

$$E(V_1) = \sum_{i_1=0}^{C} i_1 \times \sum_{\substack{i_j \\ i_j \neq i_1}} P\{N_1 = i_1, N_2 = i_2, N_3 = i_3, ..., N_n = i_n\} \tag{4.3}$$

Une généralisation de la formule ci-dessus, nous permet de récupérer le nombre moyen de véhicules dans d'autres cellules (files) du réseau ($E(Vi, i = 2, 3..., n)$).Le nombre moyen de clients dans tout le réseau est :

$$E(V) = \sum_{i_2, i_3, ..., i_n} E(V_i) \tag{4.4}$$

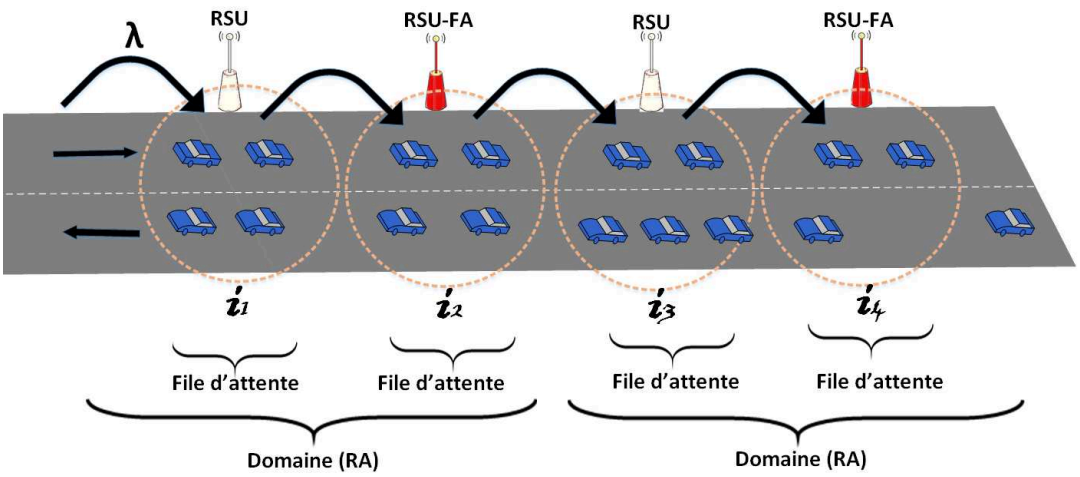

FIGURE 4.28 – Modélisation des cellules avec des files d'attente en série

Les réseaux de Jackson Markoviens à forme produit peuvent contenir aussi bien des files de type M/M/1, M/M/∞ ou M/M/m. Dans les réseaux d'infrastructures routières, on peut considérer deux cas : le premier cas correspond au cas où les véhicules évoluent dans une route où il est interdit d'effectuer un dépassement, le deuxième cas ou il s'agit d'une route où le dépassement est toléré. Nous allons considérer ces deux cas et nous allons les modéliser en utilisant les réseaux de Jackson Markoviens.

a- Cas d'une route tolérant le dépassement :

Notre système est modélisé comme un réseau de files d'attente en série avec des files M/M/∞. Ce modèle est sans attente avec un temps de service identique au temps de séjour dans la cellule (file). Le temps de séjour correspond au temps de la traversée de la cellule qui est lié à la vitesse spatiale des véhicules.

Une modélisation en file M/M/∞ permet à un véhicule dans la cellule de dépasser un autre. Une route où le dépassement est toléré peut être modélisé par une file M/M/∞ en effet l'ordre d'entrée et de sorties des véhicules n'est pas préservé ceci peut se traduire par des dépassement, des arrêts (c-à-d : S = 0 m/s) de véhicules (par exemple : accidents, etc.). En effet, dans ce cas un véhicule qui entre en premier dans une cellule n'est pas forcement celui qui va quitter en premier cette même cellule.

Dans notre système , nous nous intéressons à une autoroute. Dans ce cas précis, le nombre de handover coïncide avec le nombre moyen de véhicules dans une cellule. Tout véhicule qui quitte la zone de couverture desservi par une RSU à laquelle il est attaché doit forcément procéder à un handover et s'attacher à la nouvelle RSU qui dessert la zone dans laquelle il rentre.

Sachant que dans notre cas d'étude, toutes les cellules se comportent de la même manière c'est à dire les taux d'entrée dans une cellule n'influencent pas sur le taux de sortie dans l'autre. Cette caractéristique rend notre système symétrique, nous permettant de se limiter au calcul du nombre moyen de véhicules dans une seule cellule. Dans le cas d'une file M/M/∞ le facteur d'utilisation (ou la charge de service) est le nombre moyen de serveurs occupés. Ce dernier est égal au nombre moyen de véhicules dans la cellule puisqu'il n'y a pas d'attente.

La charge en terme de nombre moyen de véhicules dans une cellule vaut donc :

$$E(V) = \rho = \frac{\lambda}{\mu} \tag{4.5}$$

Nous sommes dans un cas de processus stochastique avec une charge ρ égale à λ/μ, avec $\rho \leq 1$. Sachant qu'à cause de la variabilité du processus poisson, la variabilité dans la cellule est constante. Cela est du aux freinages et au fait que les véhicules se suivent, ce qui implique un temps de séjour variable (plus long ou plus court). Cette variabilité à l'arrivée des véhicules mène à la congestion qui dépend du nombre de véhicules dans une cellule. Cette dernière a un impact sur le temps de traversée de la cellule (μ). Deux cas se présentent :

1- Cas d'un trafic fluide : ceci est traduit par une charge $\rho < 50$ % de la charge totale.

2- Cas d'un trafic congestionné (encombré) : ceci correspond à une charge $\rho \geq 50$ % de la charge totale.

b- Cas d'une route où les dépassements sont interdits :

Dans le cas où les véhicules ne sont pas autorisés à effectuer un dépassement, la modélisation de handover entre les cellules peut se baser sur une modélisation de file d'attente de type M/M/1. Rappelons que l'objectif est de déterminer le nombre moyen de véhicules dans une cellule desservie par une RSU et que l'on a noté $E(V)$.

Les véhicules arrivent dans la cellule avec un taux λ qui suit une loi poisonnienne (arrivées suivent la loi poisson). Le système décrit et les hypothèses émises ci-dessus nous permettent de modéliser une cellule par une file d'attente M/M/1/C où :

M : indique la loi de probabilité des instants d'arrivées qui est exponentielle.

M : indique la loi de probabilité de la durée du service.

1 : un seul serveur est considéré et qui correspond à la RSU qui dessert tous les véhicules qui lui sont attachés.

C : La capacité totale du système qui correspond au nombre maximal de véhicules dans la cellule. Notons que cette capacité est finie. Ainsi dans le cas où le dépassement est interdit les arrivées et sorties des véhicules suivent une loi poissoniennes. Un seul serveur est considéré. où :

- Le temps de traversé de la cellule suit la loi exponentielle du paramètre : μ (1-ρ).
- Le temps d'attente n'existe pas (virtuel) : E(W) = E(S)- (1/μ)
  avec E(S) = 1/(μ-λ) = (1/μ) / (1-ρ).
- On préserve l'ordre FIFO, un véhicules qui arrive en premier quittera en premier la cellule car il n'y a pas de dépassement.
- Le temps de séjour qui compte correspond au temps de traversée moyenne de la cellule : E(S) = μ- λ.

La moyenne du nombre de véhicules dans la cellule est calculée comme suit :

$$E(V) = \begin{cases} \frac{\rho}{1-\rho} \times \frac{1-(C+1)\times\rho^{C}+C\times\rho^{C+1}}{(1-\rho^{C+1})} & \text{si } \mu \neq \lambda \\ \frac{C}{2} & \text{si } \mu = \lambda \end{cases} \tag{4.6}$$

Rappelons qu'il y a N cellules au total et m cellules par domaine (GeoMIP), la traversée de la cellule déclenche un handover entre les cellules et la traversée de cellules appartenant à des domaines différents (c-à-d qui sont des frontières des domaines), déclenchant un handover entre les domaines. Dans ce qui suit, ces cas sont considérés :

- Intra domain handover (handover horizontal) : changement des RSUs dans un même domaine (RA). Dans ce cas, l'adresse temporaire (CoA) ne change pas et l'adresse locale routable (AoRA) change d'une RSU à une autre.
- Inter domain handover (handover vertical) : changement de RSUs qui appartiennent à des domaines différents, l'adresse (CoA) est mise à jour.
- La coopération entre RSUs et RSU-FA dans le même domaine permet d'assurer une transmission des paquets entre les RSUs dans un domaine lors d'un handover (voir la section 4.7.3).
- La coopération entre des domaines (RA) différents.

Il est important de faire la différence entre ces différents cas, car de ceux-ci que dépend le coût de la signalisation.

4.10 Paramètres de performances

Dans cette section, nous allons analyser le coût de la solution Mobile IP (MIP) et notre proposition GeoMIP ainsi que le gain en termes du volume de trafic échangé, du délai de la configuration des adresses (CoA, AoRA), du délai de bout en bout (E2ED) et du type de la liaison entre les RSUs et RSU-FAs (radio ou filaire). Rappelons que notre solution tient compte des schémas d'optimisation de la configuration d'adresses. En particulier, nous étudierons deux cas, le premier, est celui de la solution MIPv6, où une RSU joue le rôle d'une passerelle (RSU-FA), par conséquent chaque cellule est un domaine. La seconde, est notre solution dans laquelle nous regroupons les RSUs d'un même domaine (zone de routage) sous une seule RSU-FA. Pour mesurer les différents paramètres de performance du système, nous devrons tenir compte du nombre de handover et de la densité des véhicules, principales causes de la signalisation dans la mobilité.

Dans cette étude, nous considérerons que la cause du handover est du au fait qu'un véhicule quitte la cellule et non pas la dégradation du signal à l'intérieur de la cellule ou la surcharge des nœuds dans la cellule.

Dans notre étude analytique, nous nous intéressons aux métriques de performances suivantes :

— **Le volume de la signalisation échangée (C^d_{total}, C^C_{total})** : c'est le volume du trafic de contrôle échangé au niveau local (micro) et global (marco) entre les différentes entités du réseau. On entend par signalisation locale le trafic échangé lié à la configuration de l'adresse lors de la traversée d'une nouvelle cellule dans le même domaine (signalisation locale) et par signalisation globale l'obtention d'une nouvelle adresse lors du changement de cellules appartenant à des domaines différents.
Avec MIP, le volume de trafic échangé est lié à la configuration et à l'obtention d'une nouvelle adresse à chaque traversée d'une nouvelle cellule où chacune est considérée comme un domaine, cette solution de la gestion de la mobilité représente le cas limite où il y a que de la macro mobilité. Notons que C^d_{total}, C^C_{total} représentent la signalisation totale du domaine et celle de la cellule respectivement.
Notons par C^{GeoMIP}_{total} , C^{MIP}_{total} les coûts totaux de la signalisation obtenue en appliquant l'architecture proposée (GeoMIP) et MIP respectivement. Ce coût total dépend du nombre total de cellules noté N, du nombre total de domaine noté $\lceil \frac{N}{m} \rceil$ et m le nombre total de cellules par domaine.

— **Le délai de la configuration d'adresse (T^d_{total}, T^C_{total})** : c'est la durée nécessaire pour configurer une adresse valide. C'est l'intervalle entre le moment où le véhicule effectue le handover au niveau de la couche 2 et le moment où le véhicule reçoit une adresse dans la nouvelle cellule/ domaine de rattachement. Le délai total lors du changement de domaine est noté T^d_{total} et lors du changement de la cellule (local) est T^C_{total}. Autrement dit , c'est le **temps d'exécution du handover**, qui représente le temps de traitement du handover du point de vue du véhicule à deux niveaux : au niveau de la macro mobilité et au niveau de la micro mobilité.
Notons que T^{GeoMIP}_{total} , T^{MIP}_{total} sont les délais moyens totaux de la configuration d'adresse avec l'architecture proposée (GeoMIP) et MIP respectivement.

— **Le délai de bout en bout ($E2ED^d_{total}$, $E2ED^c_{total}$)** : c'est la durée entre l'envoi du

paquet de la part du véhicule et son arrivée à l'autre extrémité (CN), nous appellerons cette durée pour le cas du domaine $E2ED^{d}_{total}$ et celui de la cellule $E2ED^{c}_{total}$.
Sachant que, $\boldsymbol{E2ED^{GeoMIP}_{total}}$, $\boldsymbol{E2ED^{MIP}_{total}}$ sont les délais moyens totaux de bout en bout dans l'architecture proposée (GeoMIP) et MIP respectivement.

4.10.1 Estimation du volume total de la signalisation échangée

Pendant la mobilité du véhicule, le maintien de la mise à jour de sa table de localisation est primordiale indépendamment de l'approche utilisée (MIP, GeoMIP). Tout au long de son déplacement (traversée de la cellule ou de la zone de routage), le véhicule génère des messages de contrôle pour la configuration de ses adresses.

Afin d'estimer le coût(en terme de volume) de la configuration et du maintien de la connectivité du véhicule pendant sa mobilité en temps réel, nous considérons le cas où le domaine contient une seule cellule (cas limite) ou plusieurs (au moins deux cellules) et celui de MIP où la cellule est un domaine. Pour calculer le volume de signalisation, il est nécessaire de définir un certain nombre de paramètres. Ces derniers sont définis dans le tableau 4.7.

Le coût total pour chaque approche peut être exprimé comme suit :

Cas du MIPv6 :

Comme mentionné précédemment, avec la solution MIP, chaque cellule est un domaine. Le coût total de la signalisation engendré par l'approche MIP est exprimé par la formule ci-dessous :

$$C^{MIP}_{total} = N \times E(V) \times C^{d}_{total} \tag{4.7}$$

Remarquons que ce coût dépend d'une part, du nombre moyen de véhicules dans une cellule ($E(V)$) qui correspond dans notre cas au nombre de handovers (HO) qui vont être déclenchés dans un seul domaine. Ce dernier est calculé en se basant sur une modélisation d'une file d'attente de type M/M/∞. D'autre part, Ce coût dépend du nombre de domaines (N) pour obtenir le coût total lors de la traversée de tous les domaines. où, C^{d}_{total} est le coût de la signalisation d'une mise à jour lors de la traversée d'un domaine c'est à dire lors d'un handover vertical.

Cas de la solution proposée (GeoMIP) :

Le coût de signalisation lors d'un handover (HO) horizontal dépend d'une part, du coût de la traversée de la cellule (C^{c}_{total}). D'autre part, il dépend du nombre moyen de véhicules dans cette cellule ($E(V)$) qui représentent le nombre de handovers déclenchés dans la cellule. Ce coût total d'un handover horizontal est exprimé comme suit :

$$C^{HO-Horizontal}_{total} = E(V) \times C^{c}_{total} \tag{4.8}$$

Tandis que dans le cas d'un handover vertical, ou le changement de domaines revient au changement de deux cellules appartenant à des domaines différents. Le coût de signalisation dépend d'une part, du coût de la traversée d'un domaine (RA) (C^{d}_{total}). D'autre part, il dépend du

nombre moyen de véhicules dans cette cellule ($E(V)$) qui représentent le nombre de handovers déclenchés dans la cellule. Ce coût total d'un handover vertical est exprimé comme suit :

$$C_{total}^{HO-Vertical} = E(V) \times C_{total}^{d} \tag{4.9}$$

D'une manière plus générale, à savoir, un nombre total de cellules noté $\boldsymbol{N}$, un nombre total de domaines noté $\lceil \frac{N}{m} \rceil$ et $\boldsymbol{m}$ comme nombre total de cellules par domaine. Le coût total de la signalisation avec l'architecture proposée (GeoMIP), où les RSUs de la même zone de routage (RA) sont regroupées sous une seule RSU-FA, est exprimée par la formule ci-dessous :

$$C_{total}^{GeoMIP} = E(V) \times [N \times C_{total}^{c} + \lceil \frac{N}{m} \rceil \times C_{total}^{d}] \tag{4.10}$$

Sachant que,

C_{total}^{c} : le coût de signalisation d'une mise à jour pour un handover horizontal.

C_{total}^{d} : le coût de signalisation d'une mise à jour lors d'un handover vertical.

Il nous reste à définir le coût de la signalisation globale $\boldsymbol{C_{total}^{d}}$ et le coût de la signalisation locale $\boldsymbol{C_{total}^{c}}$.

4.10.1.1 Le volume total de la signalisation globale échangée (C_{total}^{d})

Pour rappel, la signalisation globale consiste à traverser le domaine. Pour ce faire, le véhicule s'enregistre à un nouveau domaine pour configurer une adresse IP (CoA) valide.

Pour obtenir cette adresse, la passerelle (RSU-FA) et l'agent mère (HA) échangent deux types de messages : BU/BA (nous avons décrit l'échange de messages dans la section 4.7).

La configuration de cette adresse (CoA) nécessite la détection de sortie de la cellule et de détachement du point d'accès, l'authentification et la réception des messages d'avertissement (M_{Radv}) de la part de la RSU.

Une fois l'adresse configurée, le véhicule doit enregistrer son nouveau attachement au niveau de son agent mère afin d'associer ses deux adresses HoA et CoA. L'enregistrement entre le véhicule et son agent mère (HA) se fait par l'intermédiaire de RSU-FA (passerelle).

Avec GeoMIP, le véhicule peut ne pas être lié directement à la RSU-FA, ce qui nécessite de faire passer les messages à travers les RSUs du domaine avant s'atteindre la RSU-FA. Ainsi, il est nécessaire de définir la moyenne maximale du nombre de sauts entre le véhicule (v) et la RSU-FA noté $\boldsymbol{H_{v}^{RSU-FA}}$ qui correpond à la distance en nombre de sauts entre le véhicule et la RSU-FA.

L'agent mère contrôle $E(V)$ véhicules dans un domaine avec une complexité des opérations de mise à jour de $O(Logn)$, étant donné que la structure des données est arborescente. Nous supposons que la détection de mouvements lors de la sortie de la cellule et l'authentification du véhicule sont les mêmes pour les deux approches et donc omises dans notre analyse. Le coût de la signalisation globale à la traversée d'un domaine est calculé par la formule suivante :

$$\begin{aligned} C_{total}^{d} &= M_{Radv} + 2 \times M_{BU}^{d} + 2 \times (M_{BU}^{d} \times H_{v}^{RSU-FA}) + 2 \times (M_{BU}^{d} \times H_{RSU-FA}^{HA}) + C_{u/F}^{d} + C_{u}^{d} \\ H_{v}^{RSU-FA} &= \frac{(m-1)}{2} \\ C_{u}^{d} &= f \times log(E(V)) \end{aligned} \tag{4.11}$$

Où :

H_v^{RSU-FA} qui est la distance en nombre de sauts entre le véhicule et la RSU-FA.

C_u^d est le coût du traitement d'une mise à jour de liaison (BU/BA) entre les RSUs pour configurer une adresse globale (CoA) dans un domaine (RA).

$C_{u/F}^d$ est le coût du traitement d'une mise à jour de liaison (BU/BA) entre RSU-FA et HA pour configurer une adresse globale (CoA) dans un domaine (RA).

Avec :

f= α : dans le cas où les RSUs (y compris la RSU-FA) sont reliées par la radio.

f= β : dans le cas où les RSUs (y compris la RSU-FA) sont reliées par un réseau filaire.

$C_{u/F}^d = \beta \times log(E(V))$.

4.10.1.2 Le volume total de la signalisation locale échangée (C_{total}^C)

Lors de la traversée des cellules dans un même domaine (RA), le véhicule échange avec le point d'accès (RSU) auquel il est attaché deux messages (BU/BA).

Le véhicule configure une adresse IP locale routable (AoRA) dans chaque cellule. La configuration de cette adresse routable localement nécessite la détection du mouvement de la traversée de la cellule et la réception des messages d'avertissement (M_{Radv}) de la part de la RSU (point d'attachement).

Une fois l'étape de la configuration est achevée, le véhicule enregistre une nouvelle liaison au niveau de la RSU (qui peut être différente de la RSU-FA) pour associer son AoRA avec son CoA. Etant donné que le mobile reste dans le même domaine, sa CoA reste inchangée même s'il traverse différentes cellules. Cela implique que le handover s'exécute en évitant de solliciter l'agent mère. L'intérêt de notre solution GeoMIP qui consiste à grouper des RSUs de la même RA sous une seule passerelle RSU-FA est d'introduire une adresse routable localement (AoRA) pour la gestion de la micro mobilité. Le coût de la signalisation à la traversée des cellules dans un même domaine est calculé par la formule suivante :

$$\begin{aligned} C_{total}^C &= M_{Radv} + 2 \times M_{BU}^C + C_u^C \\ C_u^C &= \alpha \times E(V) \end{aligned} \tag{4.12}$$

Où, C_u^C est le coût du traitement d'une mise à jour de liaison (BU/BA) pour configurer une adresse locale (AoRA) dans une cellule.

4.10.2 Modélisation du délai moyen de la configuration d'adresse

Ce délai représente le délai moyen de l'exécution du handover au niveau de la macro mobilité et de la micro mobilité. De la même manière, nous définissons le délai moyen total de configuration d'adresse pour les deux approches comme suit :

Cas du MIPv6 :

Comme mentionné précédemment, avec la solution MIP, chaque cellule est un domaine (RA). Le délai moyen de la configuration d'une adresse globale appelée CoA peut être exprimé comme suit :

$$T^{MIP}_{total-Moyen} = T^{d}_{total} \tag{4.13}$$

Avec T^{d}_{total} est la durée de la configuration d'une adresse temporaire (CoA) lors de la traversée d'un domaine.

Cas de la solution proposée (GeoMIP) :

Le délai total de la configuration d'une adresse avec l'architecture proposée, où les RSUs d'une même zone de routage sont regroupées sous une seule entité RSU-FA, dépend de la durée de configuration d'une adresse locale (AoRA) pour un handover horizontal (entre cellules de même RA) appelé T^{C}_{total} et la durée T^{d}_{total} qui correspond au temps que prend le véhicule pour la configuration d'une adresse temporaire (CoA) lors de la traversée d'une RA, c'est à dire lors d'un handover vertical (entre domaines). Le délai total moyen est exprimé par la formule ci-dessous :

$$T^{GeoMIP}_{total} = T^{d}_{total} + T^{C}_{total} + (m-1) \times T^{C}_{total} \tag{4.14}$$

Le délai moyen est calculé comme suit :

$$T^{GeoMIP}_{total-Moyen} = \frac{1}{m} \times T^{d}_{total} + T^{C}_{total} \tag{4.15}$$

4.10.2.1 Le délai total de configuration de l'adresse globale (T^{d}_{total})

La figure 4.29 illustre le diagramme de temps pour la configuration de l'adresse lors du changement de domaine (Handover vertical), qui dépend de plusieurs paramètres qui sont :

T_{L2}, T_{AU} : qui sont la durée de la détection de la sortie d'une cellule et le processus d'authentification respectivement.

T_{Radv} : le délai de traitement d'un messages d'avertissement reçu d'une RSU.

T_{BU} : la Latence de traitement des opérations de mise à jour et de mapping (BU/BA).

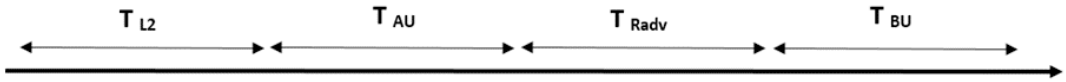

FIGURE 4.29 – Diagramme du délai de configuration de l'adresse

Le processus commence par l'exécution d'un handover au niveau de la couche 2 et se termine lorsque le véhicule reçoit son adresse (CoA) de la part de son agent mère. Ce processus contient l'étape de configuration de la CoA et l'établissement de la liaison (BU/BA) avec le HA.

Le délai total est calculé comme suit :

$$T^{d}_{total} = T^{d}_{CoA} + T^{d}_{BU} + T^{d}_{BA} \tag{4.16}$$

Le calcul de ce délai s'est inspiré du [59] où le temps de configuration de CoA est basé sur T_{Radv}, qui est la durée moyenne d'attente entre le moment où le véhicule entre dans une nouvelle RA (domaine) et le moment où le véhicule reçoit un message d'avertissement de la part de la RSU pour configurer son adresse. La durée moyenne est exprimée comme suit :

$$T_{Radv} = \frac{T^2_{Radv_{max}} + T^2_{Radv_{min}} + T_{Radv_{max}} \times T_{Radv_{min}}}{3 \times (T_{Radv_{max}} + T_{Radv_{min}})} \tag{4.17}$$

Nous nous intéressons au temps au niveau de la couche 3, nous négligeons le temps T_{L2} et aussi le temps d'authentification T_{AU}. Le temps de configuration d'adresse temporaire (CoA) est comme suit :

$$T_{CoA} = T_{Radv} \tag{4.18}$$

D'un autre côté, la mise à jour de liaison (BU/BA) dépend de la taille du message de contrôle et de la bande passante.

Le temps d'acheminement d'un message dépend du temps d'injection de ce dernier dans le réseau et son temps de propagation. Dans le cas où les RSUs et la RSU-FA sont liées par un réseau sans fil, le temps de propagation de ce message au niveau du réseau sans fil (radio), est exprimé comme suit :

$H^{RSU-FA}_{Vehicule} \times (\frac{M_{BU}}{B_{V2I}} + R_{V2I})$.

Le cas d'une communication entre les RSUs et la RSU-FA via le réseau filaire, le temps de propagation de ce message au niveau du réseau filaire, exprimé par :

$H^{RSU-FA}_{Vehicule} \times (\frac{M_{BU}}{B_f} + R_f)$.

Le temps de propagation est calculé comme suit :

$$T^d_{BU} = T^d_{BA} = (\frac{M_{BU}}{B_{V2I}} + R_{V2I}) + H^{RSU-FA}_{Vehicule} \times (\frac{M_{BU}}{B} + R) + H^{HA}_{RSU-FA} \times (\frac{M_{BU}}{B_f} + R_f) + 2 \times T_u \tag{4.19}$$

Où :

R : le temps de propagation sur la radio (R_{V2I}) ou filaire (R_f).

B : la bande passante des liens radio (B_{V2I}) ou filaire (B_f).

T_u : la latence de traitement des opérations de mise à jour d'un message BU ou BA.

Sachant que, le temps d'acheminement du message de contrôle du véhicule à la RSU-FA peut passer par des RSUs intermédiaires avec GeoMIP, dans le cas où le véhicule se trouve dans la portée d'une RSU qui est différente de la passerelle (RSU-FA). Ce qui amène à un temps de propagation de ce message exprimé par :

$H^{RSU-FA}_{Vehicule} \times (\frac{M_{BU}}{B} + R)$.

Le délai total de configuration de l'adresse temporaire (CoA) est exprimé comme suit :

$$T^d_{total} = T_{Radv} + 2 \times T^d_{BU} \tag{4.20}$$

Où : $T^d_{BU} = T^d_{BA}$.

4.10.2.2 Le délai total de configuration de l'adresse locale (T^C_{total})

Le temps de configuration d'une adresse locale routable (AoRA) est exprimé de la même manière que le temps de configuration d'une adresse temporaire (CoA). De ce fait, il est basé sur T_{Radv} calculé précédemment.

Rappelons que, la mise à jour de la liaison (BU/BA) dépend de la taille du message de contrôle et de la bande passante avec un temps d'acheminement d'un message qui dépend du

temps d'injection de ce dernier dans le réseau et son temps de propagation. Sachant que , pour un handover horizontal, ce temps de propagation est calculé en se basant sur la distance entre le véhicule et son point d'attachement (RSU), ce qui donne :

$$T_{BU}^{C} = T_{BA}^{C} = \left(\frac{M_{BU}}{B_{V2I}} + R_{V2I}\right) + T_{u} \tag{4.21}$$

Où : T_u est la latence de traitement des opérations de mise à jour d'un message BU ou BA.

Le délai total de la configuration de l'adresse locale routable (AoRA), autrement dit, le délai total nécessaire pour configurer une adresse valide lors du changement de cellules du même domaine, est exprimé comme suit :

$$T_{total}^{C} = T_{Radv} + 2 \times T_{BU}^{C} \tag{4.22}$$

Sachant que : $T_{Radv} = T_{AoRA}$

4.10.3 Le délai moyen de bout en bout (E2ED)

Le délai de bout en bout (E2ED) dépend de la bande passante, du délai de propagation, et de la distance entre les deux entités communicantes. Nous définissons le délai total moyen de bout en bout comme suit :

Cas du MIPV6 :

Le E2ED moyen avec la solution MIP est exprimé comme suit :

$$E2ED_{total}^{MIP} = E2ED_{total}^{d} \tag{4.23}$$

Avec $E2ED_{total}^{d}$ est la durée nécessaire pour acheminer le paquet de bout en bout, lors de la traversée d'un domaine (pour rappel, une cellule est un domaine avec MIP) c'est à dire lors d'un handover vertical.

Cas de la solution proposée (GeoMIP) :

Le E2ED moyen avec l'architecture proposée, où les RSUs de la même zone de routage sont regroupées par zone de routage (domaine), est exprimée par la formule ci-dessous :

$$T_{total}^{GeoMIP} = \frac{1}{m} \times E2ED_{total}^{d} + E2ED_{total}^{C} \tag{4.24}$$

Sachant que,

$E2ED_{total}^{C}$: la durée nécessaire pour acheminer le paquet de bout en bout, lors de la traversée d'une cellule, c'est à dire lors d'un handover horizontal (entre des cellules du même domaine (RA)).

$E2ED_{total}^{d}$: la durée nécessaire pour acheminer le paquet de bout en bout, lors de la traversée d'un domaine (pour rappel, un domaine (RA) est composé de m cellules) c'est à dire lors d'un handover vertical.

4.10.3.1 Le E2ED total lors d'un handover vertical ($E2ED_{total}^{d}$)

La figure 4.30 illustre le diagramme du temps pour le E2ED lors du changement de domaine (Handover vertical). Les paquets échangés entre un véhicule et une destination (CN)

sont d'abord encapsulés au niveau du véhicule avant qu'ils ne soient transmis au HA via la RSU-FA. Le HA décapsule l'en-tête lorsque le paquet arrive, avant de l'envoyer au CN (la destination). Le E2ED est alors exprimé comme suit :

$$\begin{aligned} E2ED^{d}_{Total} = (\frac{M_{Vehicule} + M_{Tunnel}}{B_{V2I}} + R_{V2I}) + \\ H^{RSU-FA}_{Vehicule} \times (\frac{M_{Vehicule} + M_{Tunnel}}{B} + R) + \\ H^{HA}_{RSU-FA} \times (\frac{M_{Vehicule} + M_{Tunnel}}{B_f} + R_f) + \\ H^{CN}_{HA} \times (\frac{M_{Vehicule} + M_{Tunnel}}{B_f} + R_f) \end{aligned} \tag{4.25}$$

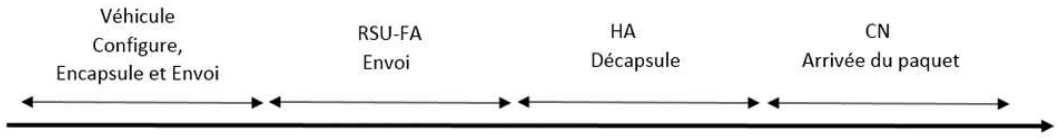

FIGURE 4.30 – Diagramme du délai cas du HO vertical (changement de domaine)

4.10.3.2 Le E2ED total lors d'un handover horizontal ($E2ED^{C}_{total}$)

Lors d'un handover horizontal, les paquets échangés entre un véhicule et son point d'attachement actuel (RSU) sont d'abord encapsulés (avec $AoRA$) au niveau du véhicule avant qu'ils ne soient transférés à la RSU. La RSU décapsule l'en-tête lorsque le paquet arrive, avant de le transférer à la RSU-FA (la destination). Dans ce cas , le E2ED est alors exprimé comme suit :

$$E2ED^{C}_{Total} = (\frac{M_{Vehicule} + M_{Tunnel}}{B_{V2I}} + R_{V2I}) \tag{4.26}$$

4.11 Évaluation de performances

Dans cette partie, nous allons analyser les deux approches (MIP, GeoMIP) en terme de coût de signalisation, du délai moyen de configuration d'adresse et du délai d'acheminement des données de bout en bout (E2ED) avec un temps de traitement exponentiel. Une variation du nombre de cellules par domaine et le nombre totale de cellules a été fait, deux types de communications entre les RSUs (y compris la RSU-FA) sont introduites, à savoir le cas d'une communication radio entre RSUs et le cas d'une communication via le réseau filaire entre ces dernières.

La Table 4.7 présente les valeurs numériques des paramètres du système. Nous allons décrire les résultats obtenus de notre analyse pour les paramètres de performance définis ultérieurement.

4.11.1 Le coût total de la signalisation

Les figures 4.31 , 4.32, 4.33 et 4.34 illustrent le coût total (volume du trafic de contrôle) de la signalisation des deux approches MIP et GeoMIP en variant le nombre total de cellules (N = {4,6,8,10,12}), le nombre total de cellules par domaine (m = {1, 2, 3, 4}) et la charge du réseau (en terme de nombre moyen de véhicules dans une cellule). Les figures montrent l'impact de la variation du nombre total de cellules sur le coût total de la signalisation.

Le véhicule change son point d'attachement (RSU) à chaque traversée d'une cellule. Cela introduit beaucoup de messages (comme la génération des BUs/BA) échangés entre les entités du réseau. Autrement dit, la signalisation élevée est une conséquence des sollicitations fréquentes d'une RSU avec ou sans sollicitation de l'agent mère (HA), à chaque changement de cellule. Néanmoins, le fait de regrouper plus de cellules par domaine (avec GeoMIP) diminue le volume du trafic échangé car l'agent mère n'est pas sollicité à la traversée de ces cellules appartenant au même domaine.

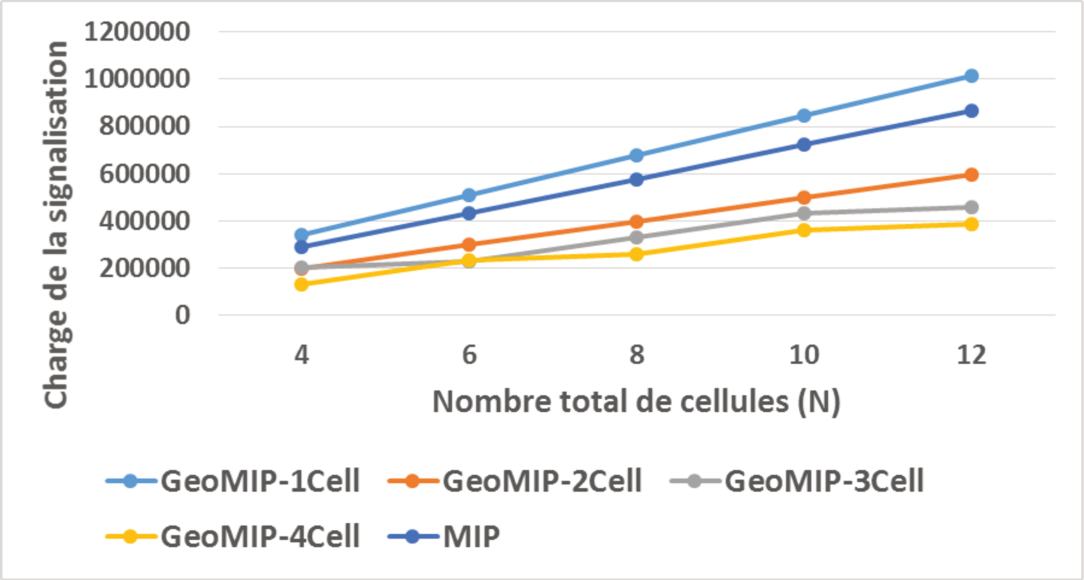

FIGURE 4.31 – Charge de la signalisation : cas d'une communication filaire et un trafic fluide

A partir de deux cellules par domaine, GeoMIP affiche un coût plus faible que MIP car l'approche MIP qui présente le cas limite où il y a que de la macro mobilité (handover vertical), introduit plus de volume de signalisation échangé avec le HA qu'avec notre approche GeoMIP. Pour un nombre maximum de 12 cellules où on regroupe 4 cellules par domaine (GeoMIP), le coût reste plus faible que MIP pour 4 cellules.

Autrement dit, MIP assure une forte charge de signalisation comparant à notre approche, ceci est dû à l'architecture centralisée de MIP (sollicitation de HA à chaque changement de sous-réseau). Contrairement à notre architecture qui regroupe les sous-réseaux (cellules) sous une seule passerelle (RSU-FA), par conséquence l'échange de messages entre le véhicule et l'agent mère se fait à chaque changement de domaine (RA) et non pas à chaque changement de cellule.

En revanche, en comparant notre solution GeoMIP avec MIP en terme de messages

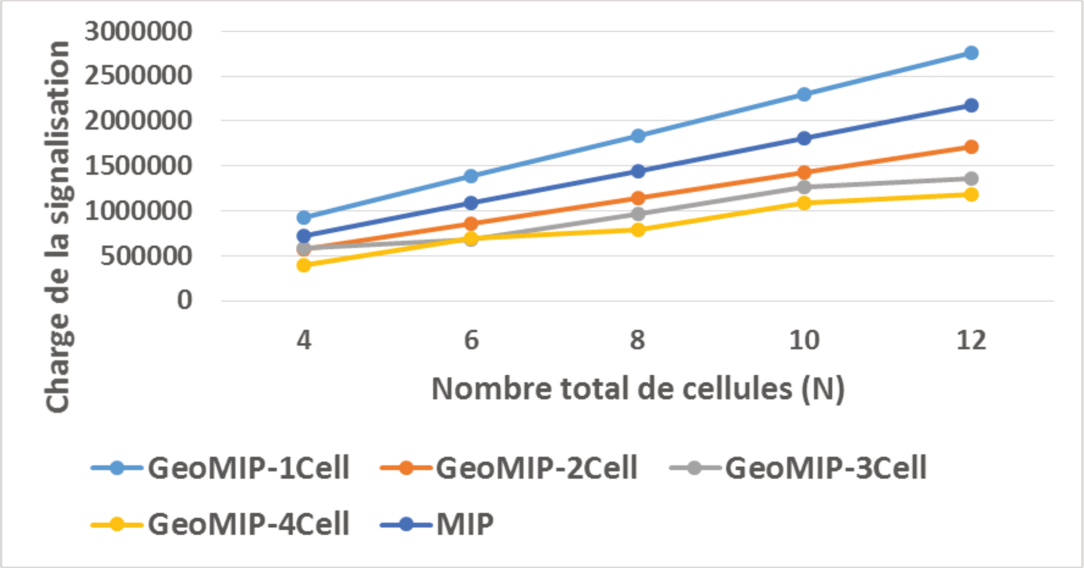

FIGURE 4.32 – Charge de la signalisation : cas d'une communication filaire et un réseau surchargé

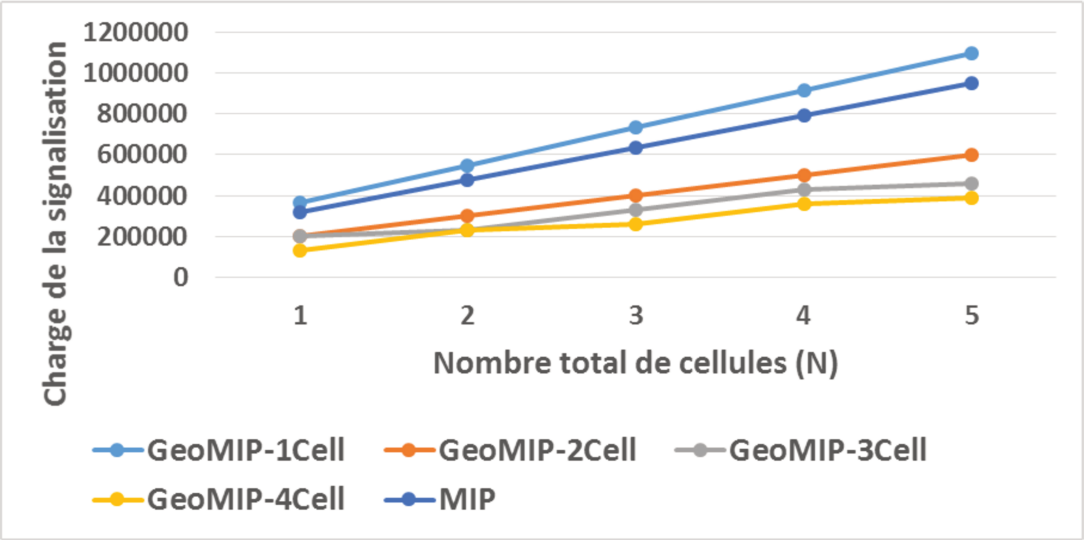

FIGURE 4.33 – Charge de la signalisation : cas d'une communication radio et un trafic fluide

échangés, GeoMIP avec une seule cellule (GeoMIP-1Cell) par RA (domaine) assure un coût de signalisation plus élevé que MIP en raison de la signalisation additionnelle liée à la configuration de l'adresse locale (AoRA) à chaque changement de RSU.

Enfin, nous remarquons que la charge de la signalisation sur le réseau radio est plus élevé que sur le filaire (les tables 4.1 et 4.2) pour les deux approches indépendamment de l'état du trafic routier. Le gain dépend du coût de traitement des messages échangés sur la radio ou le réseau filaire qui est calculé en fonction des coefficients (α, β) respectivement. Pour mieux visualiser l'apport de notre solution, nous définissons le gain du coût en se basant sur les formules précédentes. Le gain est exprimé comme suit :

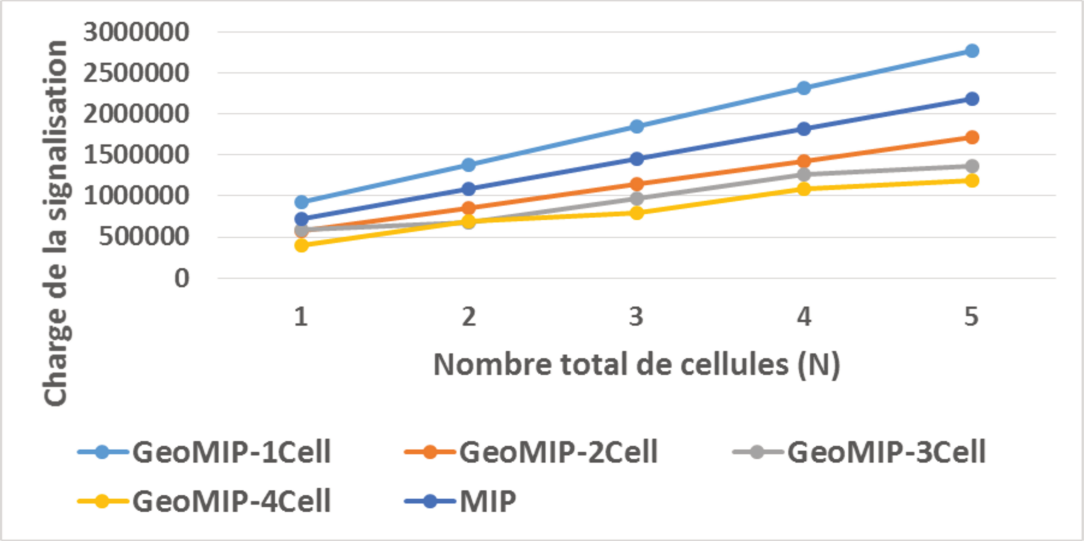

FIGURE 4.34 – Charge de la signalisation : cas d'une communication radio et un réseau surchargé

$$\Delta^{GeoMIP/MIP}_{Signalisation} = \Delta^{GeoMIP/MIP}_{Radio} - \Delta^{GeoMIP/MIP}_{Filaire} = \Delta^{GeoMIP/MIP}_{C^d_u} = (\alpha - \beta) \times log(E(V)) \quad (4.27)$$

TABLE 4.1 – Le gain en terme de la charge de la signalisation : cas d'un réseau chargé

Approche / Nombre total de cellules	4	6	8	10	12
$GeoMIP-1Cell$	2400	3600	4800	6000	7200
$GeoMIP-2Cell$	1200	1800	2400	3000	36000
$GeoMIP-3Cell$	1200	1200	1800	2400	2400
$GeoMIP-4Cell$	600	1200	1200	1800	1800
MIP	2400	3600	4800	6000	7200

Nous remarquons que indépendamment de l'approche utilisée (GeoMIP ou MIP), le gain dépend du nombre de véhicules par cellule ($E(V)$) et des facteurs du coût de traitement des message de liaisons (BU/BA) sur la radio (α) ou sur le filaire (β).

4.11.2 Le délai moyen total de configuration d'adresse

Le tableau 4.3 montre le délai moyen de configuration de l'adresse qui est le temps moyen d'exécution du handover à deux niveaux (macro et micro) sur le réseau filaire ou sur la radio, en fonction du nombre de cellules et de domaines. Le délai de configuration de l'adresse est élevé car le véhicule introduit de la signalisation à chaque changement de point d'attachement (RSU-FA) qui se fait de manière plus fréquente avec MIP qu'avec notre approche GeoMIP. Ce

TABLE 4.2 – Le gain en terme de la charge de la signalisation : cas d'un réseau à faible surcharge

Approche / Nombre total de cellules	4	6	8	10	12
$GeoMIP$ – $1Cell$	27648.98	41473.48	55297.97	69122.47	82946.96
$GeoMIP$ – $2Cell$	384.49	576.74	768.98	961.23	1153.48
$GeoMIP$ – $3Cell$	384.49	384.49	576.74	768.98	768.98
$GeoMIP$ – $4Cell$	192.24	384.49	384.49	576.74	576.74
MIP	27648.98	41473.48	55297.97	69122.47	82946.96

délai est une conséquence de la charge de signalisation, à chaque fois que ça nécessite d'autres messages à échanger. Cela implique une latence plus élevée. Nous constatons que l'intérêt de notre nouvelle architecture apparait quand le nombre de cellules par domaine est au moins égal à deux (à partir de deux cellules par domaine), GeoMIP avec une seule cellule par domaine assure un délai plus long que MIP. Ceci est dû à l'introduction d'un temps additionnel qui est le temps de configuration d'une adresse locale (AoRA).

TABLE 4.3 – Délai moyen de la configuration des adresses

Approche	Filaire (ms)	Radio (ms)
$GeoMIP$ – $1Cell$	1780.461818	1780.461818
$GeoMIP$ – $2Cell$	1149.941818	1171.957273
$GeoMIP$ – $3Cell$	939.7684848	969.1224242
$GeoMIP$ – $4Cell$	834.6818182	867.705
MIP	1262.1	1262,1

Néanmoins, MIP (de point de vue de la macro mobilité) souffre de délais longs vu la longue distance entre le véhicule et l'agent mère. Ce dernier est sollicité lors du changement des messages de mise à jour des adresses à chaque traversée d'une cellule du même domaine ou pas.

Contrairement à MIP, avec GeoMIP cette distance (véhicule - agent mère) est parcourue juste lors du changement de cellule qui n'appartiennent pas au même domaines (RA). Autrement dit, un délai court est assuré avec notre architecture grâce au changement de la distance empruntée par les messages (BU/BA) échangés par les entités réseau. C'est à dire, la distance entre le véhicule et l'agent mère est parcourue à chaque changement de domaine qui regroupe plusieurs RSUs tandis qu'avec MIP, elle est parcourue à chaque changement de cellule. Ainsi, la distance parcourue est celle entre le véhicule et la RSU-FA qui est plus courte avec GeoMIP.

Enfin, nous remarquons clairement que le délai nécessaire pour la configuration d'adresse

sur le réseau radio est plus élevé que sur le filaire (le tableau 4.4) pour GeoMIP avec ($m \geqslant 2$). Le gain dépend du délai de traitement des messages(BU/BA) échangés pour la mise à jour des adresses sur la radio ou le réseau filaire en fonction de la bande passante et du temps de propagation qui sont différents. Le gain est calculé comme suit :

$$\begin{aligned} \Delta_{Delai}^{GeoMIP/MIP} &= \Delta_{Radio}^{GeoMIP/MIP} - \Delta_{Filaire}^{GeoMIP/MIP} \\ = \Delta_{T_u^d}^{GeoMIP/MIP} &= [(\frac{M_{BU}}{B_{V2I}} + R_{V2I}) - (\frac{M_{BU}}{B_f} + R_f)] \times H_{Vehicule}^{RSU-FA} \end{aligned} \tag{4.28}$$

A partir de deux cellules par domaine (RA), nous notons que notre solution (GeoMIP) améliore le délai moyen de configuration de l'adresse d'un véhicule. Par contre, il n y a pas de gain pour MIP et GeoMIP (avec une seule cellule par domaine) car dans l'équation ci-dessus $H_{Vehicule}^{RSU-FA} = 0$, ce qui implique un $\Delta_{Delai}^{GeoMIP/MIP}$ nul.

TABLE 4.4 – Gain en terme de Délai moyen

Approche	Radio-Filaire (ms)
$GeoMIP-1Cell$	0
$GeoMIP-2Cell$	22.01545455
$GeoMIP-3Cell$	29.35393939
$GeoMIP-4Cell$	33.02318182
MIP	0

4.11.3 Le délai moyen de bout en bout (E2ED)

Comme illustré sur le tableau 4.5, en augmentant le nombre total de cellules, le E2ED moyen devient plus long. Le délai de bout en bout (E2ED) diminue quand le chemin de routage est raccourci, séparant ainsi le plan de contrôle du plan de données. Etant donné que cette approches d'optimisation du chemin de routage est appliquée avec GeoMIP, cette dernière assure de courts E2ED comparant à MIP à chaque fois qu'il y ait plus de cellules dans le domaine (ex. GeoMIP avec 3 cellules est meilleur que GeoMIP avec 2 cellules etc.).

$$\begin{aligned} \Delta_{E2ED}^{GeoMIP/MIP} &= \Delta_{Radio}^{GeoMIP/MIP} - \Delta_{Filaire}^{GeoMIP/MIP} \\ &= \Delta_{T_u^d}^{GeoMIP/MIP} \\ = [(\frac{M_{Vehicule} + M_{Tunnel}}{B_{V2I}} + R_{V2I}) &- (\frac{M_{Vehicule} + M_{Tunnel}}{B_f} + R_f)] \times H_{Vehicule}^{RSU-FA} \end{aligned} \tag{4.29}$$

Enfin, le tableau 4.6 montre le gain en terme de E2ED des deux approches dans le cas où les RSUs sont liées via la radio ainsi que dans le cas où elles sont liées via le réseau filaire.

TABLE 4.5 – E2ED moyen

Approche	Filaire (ms)	Radio (ms)
$GeoMIP - 1Cell$	230.4545455	230.4545455
$GeoMIP - 2Cell$	141.5863636	154.0909091
$GeoMIP - 3Cell$	111.9636364	128.6363636
$GeoMIP - 4Cell$	97.15227273	115.9090909
MIP	178.6363636	178.6363636

TABLE 4.6 – Gain en terme de E2ED moyen

Approche	Radio-Filaire (ms)
$GeoMIP - 1Cell$	0
$GeoMIP - 2Cell$	12.50454545
$GeoMIP - 3Cell$	16.67272727
$GeoMIP - 4Cell$	18.75681818
MIP	0

Le délai de bout en bout sur la radio est beaucoup plus long que sur le filaire pour les deux approches. La formule ci-dessus montre les paramètres liés à cette différence.

Par contre, il n' y a pas de gain pour MIP et GeoMIP (avec une seule cellule par domaine) car dans l'équation ci-dessus $H_{Vehicule}^{RSU-FA} = 0$, ce qui donne un $\Delta_{E2ED}^{GeoMIP/MIP}$ nul.

4.12 Conclusion

Dans ce chapitre, nous avons proposé une approche qui permet une communication entre une entité sur Internet et le(s) véhicule(s) dans les réseaux véhiculaires (VANET) en traitant le problème d'adressage hybride (IP, coordonnées géographiques) et le mécanisme de la gestion de la mobilité. Notre solution repose sur l'architecture du mobile IP (MIP) avec un objectif qui consiste à optimiser l'échange des messages entre les entités réseau communicantes responsables de la gestion des adresses. Notre approche comprend (1) un partitionnement géographique, (2) le regroupement des RSUs sous une seule RSU-FA (3) et un adressage hybride en se basant sur une fonction de hachage. Afin d'évaluer les performances de cette proposition, nous nous sommes basés sur une modélisation du système par un modèle M/M/∞. Nous avons fait varier le nombre de cellules et nous avons étudié l'impact de cette variation en termes de coût de la signalisation échangée lors d'un handover, du délai moyen de configuration d'adresse et du délai de bout en bout (E2ED). Les résultats ont montré que notre solution a permis d'améliorer ces différents paramètres de performances par rapport à MIP à partir du

regroupement de deux cellules par domaine (RA).

TABLE 4.7 – Paramètres du modèle

Paramètres	Description	Valeur
M_{Radv} ,M_{BU}, M_{BA}	Taille des messages d'avertissement ; Binding Update (BU), Binding Ack (BA)	80 octets, 56 octets, 56 octets
C	La capacité d'une cellule	dépend de la taille de véhicule, la portée de la RSU,etc. C = 120
m , N	Nombre de cellules dans chaque domaine et Nombre total de cellules respectivement	-
$\frac{N}{m}$	Nombre de domaines en considerons le découpage avec la solution proposée (GeoMIP)	$\lceil \frac{N}{m} \rceil$
$H_{Vehicule}^{RSU-FA}$	La moyenne du nombre de sauts entre le véhicule et la RSU-FA (passerelle)	$\frac{(m-1)}{2}$
H_{RSU-FA}^{HA} , H_{HA}^{CN}	Nombre moyen du saut entre la RSU-FA et l'agent mère, entre l'agent mère et le nœud correspondant	15, 10
$T_{Radv_{min}}$, $T_{Radv_{max}}$	le délai minimal et maximal entre deux messages d'avertissement (Router Advertisements) consécutifs	40, 70 ms (RFC 6275)
B_{V2I}, B_f	La bande passante des liens V2I (radio), Infrastructure fixe (filaire)	11, 100 Mps
R_{V2I}, R_f	Temps de propagation pour le V2I (radio), Infrastructure fixe (filaire) (comme temps de parcours)	27 Mbps (maximum pour le 802.11p), 100 Mbps, 40, 0.5 ms[58]
T_u	Latence de traitement des opérations de mise à jour et mapping d'un messgae BU ou BA	500 ms [34]
T_{BU}^d, T_{BA}^d,T_{BU}^C, T_{BA}^C	Latence de traitement des opérations de mise à jour et mapping dans une cellule , domaine respectivement	-
$M_{Vehicule}$, M_{Tunnel}	Taille de paquet de donnée envoyé par un véhicule, taille de tunnel d'encapsulation	90, 40 octets
α , β	Facteur de coût de traitement des messages BU/BA via la radio, Filaire respectivement	3, 2
ρ	Le facteur d'utilisation (ou la charge de service) dans la file (cellule) M/M/∞	Dépend de la valeur de λ et μ où $\rho = \lambda / \mu$
C_u^C, C_u^d	Le coût du traitement d'une mise à jour de liaison (BU/BA) dans une cellule, domaine respectivement	-

Chapitre 5

Conclusion générale

5.1 Bilan des contributions

La communication entre véhicules est le noyau des systèmes de transport intelligents (ITS), communément nommés ITS Coopératifs (C-ITS) ou communications V2X. Par ailleurs, l'échange d'informations entre les véhicules, ainsi qu'avec l'infrastructure au bord de la route est généralement considéré comme un moyen pour réduire les accidents et améliorer l'efficacité de la gestion du trafic routier. En effet, cet échange aide les usagers de la route à prendre conscience des autres véhicules, diffuser des messages d'avertissements sur les dangers de la route et fournir des informations en temps réel sur les conditions du trafic routier afin de régler la vitesse, changer de direction,.. etc. Dans cette thèse, nous nous sommes intéressés à l'étude de ces communications dans le contexte des applications de la sécurité routière. Généralement, elles reposent sur une connectivité via la technologie 802.11p entre les véhicules à proximité, y compris l'infrastructure lors de l'échange fréquent des données. La principale problématique de la technologie 802.11p est la bande passante limitée qui mène au problème de la congestion du canal radio lors d'échange des messages dans des scénarios à forte densité. Dans un premier temps, nous présentons un algorithme de transmission basé sur l'état du canal radio, appelé CBF2C. Les simulations réalisées à l'aide d'un simulateur de réseaux de véhicules (NS) et de la mobilité urbaine (SUMO), dans un contexte autoroutier ont montré la bonne utilisation de la ressource radio. Les résultats obtenus suscitent une possibilité d'exploiter des mécanismes de contrôle de la congestion sur des algorithmes de dissémination des messages afin de gérer au mieux la ressource radio. Une comparaison en termes de taux de perte, délai de bout en bout (E2ED), taux d'occupation du canal et la surcharge des communications, des différents algorithmes proposé par le standard ETSI et notre algorithme CBF2C, a été faite dans le chapitre 3. En outre, l'accès à des services sur Internet, comme le contrôle d'accès routier, la gestion du stationnement, etc. améliore la commodité de la conduite. Dans le chapitre 4, nous avons abordé le problème d'accessibilité du véhicule par un centre sur Internet. Nous avons proposé une approche d'adressage hybride (IP et Géographique), nommé GeoMIP, qui fabrique une adresse IP routable en utilisant en partie les coordonnées géographiques. GeoMIP était essentiellement conçu pour assurer la fluidité de la communication et réduire la surcharge de la signalisation, en introduisant le concept de zone de routage appelée RA. Ce concept est basé sur l'hypothèse que la route est divisée en zones géographiques (RAs) avec une RSU-FA

comme passerelle et d'autres RSUs comme points d'accès dans chaque RA.

Un modèle analytique du volume de trafic de la signalisation échangé lors de la gestion de la mobilité, du délai moyen de configuration d'adresse et du délai moyen de bout en bout (E2ED) est proposé. Par la suite, selon ce modèle, nous avons étudié le comportement des paramètres des deux protocoles dédiés à la gestion de la mobilité (MIP, GeoMIP) et nous avons soutiré une conclusion précise de l'intérêt du regroupement des RSUs sous une seule RSU-FA se trouvant dans la même RA.

5.2 Perspectives de recherche

Comme perspective pour le premier axe de recherche, consiste à considérer de nouveaux scénarios comme les intersections en milieu urbain afin d'évaluer notre mécanisme DCC sur DENM. Il serait intéressant de valider la robustesse de nos solutions dans un environnement où des obstacles peuvent entraîner des pertes de paquets, en réalisant des expérimentations dans un réseau réel.

Quant à notre second axe de recherche, nous pouvons envisager un cas plus réaliste pour l'application de notre mécanisme de la gestion de la mobilité (GeoMIP). Par exemple le cas de la vitesse contextuelle où les conducteurs doivent se déplacer avec une vitesse constante dans certaine zones. Dans ce cas, la limitation de la vitesse est liée aux conditions du trafic sur la route. Le serveur doit informer les véhicules dans la zone concernée, en passant par la RSU-FA responsable de cette zone, de la vitesse maximale ou minimale autorisée.

En plus, nous devons prendre en considération d'autres configuration de route (autre qu'une autoroute) afin de montrer l'intérêt de notre solution, ce qui incite à prendre en considération dans la modélisation, la variation de la vitesse des véhicules, du rayon de couverture des unités bord de route (RSUs), la probabilité de routage statistique (variation du taux d'entrées / sorties dans la cellule), etc. Dans ce cas, le handover ne sera plus en fonction du nombre moyen de véhicules dans la cellule mais dépendra de ces paramètres et du nombre moyen de véhicules dans tout le réseau (qui n'est pas homogène). Ce qui nécessite d'introduire des scénarios plus précis permettant de faire une analyse quantitative afin de quantifier le gain moyen sur l'ensemble des scénarios.

Une autre perspective, est que nos contributions CBF2C et GeoMIP peuvent être intégrées ensemble, en se basant sur des communications multi-vecteurs c'est à dire les unités bord de route supportent plusieurs technologies (par exemple : wifi-véhiculaire 802.11p, C-V2V, wifi, etc.).

D'une part, pour les applications de la sécurité routière à temps réel, le passage par GeoNetworking est plus recommandé vu sa rapidité. Dans le cas de manque de la couverture radio (déconnexion de côté V2V) et de saturation du côté de GeoNet (canal CCH congestionné), les unités bord de route peuvent basculer les flux vers un autre vecteur (ex. passage par eNodeB de LTE). Dans ce cas, LTE devient un réseau de débordement.

D'autre part, pour la diversité qui rentre dans le cadre des applications critiques, l'utilisation des paquets en duplication peut se faire pour corriger les paquets mal reçus, sans répéter la transmission de bout en bout. De cette manière une réception plus rapide et plus robuste des paquets est assurée. D'une manière générale, la communication via l'infrastructure (V2I) peut

être utilisée soit comme réseau de débordement ou bien pour la diversité.

Pour des raisons de scalabilité dans ce type d'environnement (réseau de véhicules), la technologie SDN (Software Defined Networks) [36] peut supporter la surcharge du trafic et contribue à améliorer la gestion de ce dernier. Dans notre cas d'étude, le contrôleur qui est une entité qui porte une intelligence, peut être une RSU-FA ou un serveur ITS sur Internet, dont l'intelligence consiste à orchestrer le réseau en ayant une vision du système, de définir les règles de routage, etc. Par exemple, une RSU-FA (qui correspond à une tête (head) dans chaque domaine (RA)) peut jouer le rôle d'un contrôleur SDN pour mesurer l'état du canal radio basé sur communication via le 802.11p et de décider ou pas de faire basculer les flux de données sur une autre technologie de communication. Les autres RSUs sur la route s'occupent juste de la partie données (plan data).

Bibliographie

[1] ETSI EN 302 931 (ITS) vehicular communications geographical area definition.

[2] ETSI TS 102 636-4-1 intelligent transport systems (its) vehicular communications geonetworking part 4 : Geographical addressing and forwarding for point-to-point and point-to-multipoint communications sub-part 1 : Media-independent functionality.

[3] Etsi ts 102 636-5-1 : Intelligent transport systems (its) vehicular communications geonetworking part 5 : Transport protocols sub-part 1 : Basic transport protocol.

[4] ETSI TS 102 636-6-1 : Intelligent transport systems (ITS) vehicular communications geonetworking part 6 : Internet integration sub-part 1 : Transmission of ipv6 packets over geonetworking protocols.

[5] FNV : http ://isthe.com/chongo/tech/comp/fnv/.

[6] IETF RFC 2460 : Internet protocol version 6 (ipv6) specification.

[7] IETF RFC 3753 - mobility related terminology.

[8] IETF RFC 3775 : Mobility support in ipv6.

[9] IETF RFC 3963 : Network mobility (nemo) basic support protocol.

[10] IETF RFC 768 : User datagram protocol.

[11] IETF RFC 791 : Internet protocol.

[12] IETF RFC 793 : Transmission control protocol.

[13] Ns3 network simulator, https ://www.nsnam.org/.

[14] RFC 4429 optimistic duplicate address detection (DAD) for IPv6.

[15] Simulator for urban mobility sumo, http ://sumo.dlr.de/wiki/simulation_of_urban_mobility_-_wiki.

[16] ETSI EN 3 - Intelligent Transport Systems (ITS) Vehicular Communications Geonetworking Part 3 : Network Architecture. 2014.

[17] ETSI TR 101 612 ; Intelligent Transport Systems (ITS) ; Cross Layer DCC Management Entity for operation in the ITS G5A and ITS G5B medium ; Report on Cross layer DCC algorithms and performance evaluation, Sep. 2014. V1.1.1.

[18] ETSI TR 101 613 ; Intelligent Transport Systems (ITS) ; Cross Layer DCC Management Entity for operation in the ITS G5A and ITS G5B medium ; Validation set-up and results, Sep. 2015. V1.1.1.

[19] IEEE standard for wireless access in vehicular environments–security services for applications and management messages. *IEEE Std 1609.2-2016 (Revision of IEEE Std 1609.2-2013)*, pages 1–240, 2016.

[20] ETSI EN 302 571 V2.0.0. Intelligent transport systems (ITS) ; Radio communications equipment operating in the 5 855 MHz to 5 925 MHz frequency band. 2016.

[21] ETSI EN 302 636-5-1 V1.2.0. Intelligent transport systems (ITS). vehicular communications ; geonetworking ; part 5 : Transport protocols ; sub-part 1 : Basic transport protocol. 2013.

[22] ETSI EN 302 636-6-1 V1.2.0. Intelligent transport systems (ITS). vehicular communications ; geonetworking ; part 6 : Internet integration ; sub-part 1 : Transmission of ipv6 packets over geonetworking protocols. 2013.

[23] A.Festag. Cooperative intelligent transport systems standards in europe. *IEEE Communications Magazine*, 52 :166 – 172, December 2014.

[24] T. Ali-Yahiya. *Understanding LTE and its Performance*. SpringerLink : Bücher. Springer New York, 2011.

[25] Festag Andreas, Kuhlmorgen Sebastian, and Maslekar Nitin. Decentralized congestion control for multi-hop vehicular communication. *23rd ITS World Congress*, (12), 2016.

[26] Alessia Autolitano, Claudia Campolo, Antonella Molinaro, Riccardo M Scopigno, and Andrea Vesco. An insight into decentralized congestion control techniques for vanets from etsi ts 102 687 v1. 1.1. In *Wireless Days (WD), 2013 IFIP*, pages 1–6. IEEE, 2013.

[27] B Aygun, Mate Boban, and Alexander M Wyglinski. Ecpr : Environment-and context-aware combined power and rate distributed congestion control for vehicular communications. *arXiv preprint*, 2015.

[28] Gaurav Bansal, Bin Cheng, Ali Rostami, Katrin Sjoberg, John B Kenney, and Marco Gruteser. Comparing limeric and dcc approaches for vanet channel congestion control. In *Wireless Vehicular Communications (WiVeC), 2014 IEEE 6th International Symposium on*, pages 1–7. IEEE, 2014.

[29] Gaurav Bansal, John B Kenney, and Charles E Rohrs. Limeric : A linear adaptive message rate algorithm for dsrc congestion control. *IEEE Transactions on Vehicular Technology*, 62(9) :4182–4197, 2013.

[30] P. Bhagwat, C. Perkins, and S. Tripathi. Network layer mobility : an architecture and survey. *IEEE Personal Communications*, 3 :54 – 64, 1996.

[31] B.Roberto, Z.Wenhui, F.Andreas, and L.Long. A manet-centric solution for the application of nemo in vanet using geographic routing. In *Proceedings of the 4th International Conference on Testbeds and Research Infrastructures for the Development of Networks & Communities*, pages 12 :1–12 :7, 2008.

[32] S. Cespedes, X. Shen, and C. Lazo. Ip mobility management for vehicular communication networks : challenges and solutions. *IEEE Communications Magazine*, 49(5) :187–194, May 2011.

[33] Ch.Jae-In, S.Won-Kyeong, and Ch.You-Ze. Efficient network mobility support scheme for proxy mobile ipv6. *EURASIP Journal on Wireless Communications and Networking*, page 210, Sept 2015.

[34] F. Coras, D. Saucez, L. Iannone, and B. Donnet. On the performance of the lisp beta network. In *2014 IFIP Networking Conference*, pages 1–9, 2014.

[35] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert. RFC 3963 - Network Mobility (NEMO) basic support protocol. *In : IETF*, 2004.

[36] Xiaoyu Duan, Yanan Liu, and Xianbin Wang. SDN Enabled 5G-VANET : Adaptive Vehicle Clustering and Beamformed Transmission for Aggregated Traffic. *IEEE*.

[37] ETSI EN 302 663 V1.2.0. Intelligent Transport Systems (ITS), Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band. 2012.

[38] ETSI EN 302 665 V1.1.1. Intelligent transport systems (ITS). communications architecture. 2010.

[39] ETSI EN 302 895 V1.0.0. Intelligent transport systems (ITS). vehicular communications ; basic set of applications ; local dynamic map (ldm). 2014.

[40] ETSI TR 102 638 V1.0.4. Intelligent Transport Systems (ITS) ; Vehicular communications ; Basic set of Applications. 2009.

[41] ETSI TS 102 636-4-1 V1.1.1. Intelligent transport systems (ITS). vehicular communications ; geonetworking ; part 4 : Geographical addressing and forwarding for point-to-point and point-to-multipoint communications ; sub-part 1 : Media-independent functionality. 2011.

[42] ETSI TS 102 636-4-2 V1.1.1. Intelligent transport systems (ITS). vehicular communications ; geonetworking ; part 4 : Geographical addressing and forwarding for point-to-point and point-to-multipoint communications ; sub-part 2 : Media-dependent functionalities for its-g5. 2013.

[43] ETSI TS 102 637-3 V1.1.1. Intelligent transport systems (ITS). vehicular communications ; basic set of applications ; part 3 : Specifications of decentralized environmental notification basic service. 2010.

[44] ETSI TS 102 724 V1.1.1. Intelligent transport systems (ITS).intelligent transport systems (its) ; harmonized channel specifications for intelligent transport systems operating in the 5 ghz frequency band. 2012.

[45] ETSI TS 102 894-1 V1.1.1. Intelligent transport systems (ITS). users and applications requirements ; part 1 : Facility layer structure, functional requirements and specifications. 2013.

[46] ETSI TS 102636-4-1 V1.1.1. Intelligent transport systems (ITS). geonetworking ; part 4 : Geographical addressing and forwarding for point-to-point and point-to-multipoint communications ; sub-part 1 : Media-independent functionality. 2011.

[47] Holger Füßler, Hannes Hartenstein, Martin Mauve, Wolfgang Effelsberg, and Jörg Widmer. Contention-based forwarding for street scenarios. In *1st International workshop in intelligent transportation (WIT 2004)*, number LCA-CONF-2004-005, 2004.

[48] Holger Füßler, Jörg Widmer, Michael Käsemann, Martin Mauve, and Hannes Hartenstein. Contention-based forwarding for mobile ad hoc networks. volume 1, pages 351–369, 2003.

[49] F. Giust, C. J. Bernardos, and A. de la Oliva. Analytic evaluation and experimental validation of a network-based ipv6 distributed mobility management solution. *IEEE Transactions on Mobile Computing*, 13(11) :2484–2497, Nov 2014.

[50] Salvador Gonzalez and Victor Ramos. Preset delay broadcast : a protocol for fast information dissemination in vehicular ad hoc networks (vanets). *EURASIP Journal on Wireless Communications and Networking*, 2016(1) :117, 2016.

[51] S. Gundavelli, K. Leung, K. Chowdhury, and B. Patil. RFC 5213 - Proxy Mobile IPv6. *In : IETF*, 2008.

[52] IEEE 1609 Working Group. Remote Management Service Working Group.

[53] IEEE 1609 Working Group. Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE) - Resource Manager, May 2006.

[54] IEEE 1609 Working Group. EEE Standard for Wireless Access in Vehicular Environments (WAVE) – Multi-Channel Operation, 2016.

[55] IEEE 1609 Working Group. IEEE Standard for Wireless Access in Vehicular Environments (WAVE) – Networking Services, 2016.

[56] IEEE 1609 Working Group. Standard for Wireless Access in Vehicular Environments (WAVE) - Communication Manager, 2016.

[57] IEEE 802.11 Working Group. IEEE Standard for Information Technology – Telecommunications and information exchange between systems – Local and metropolitan area networks –Specific requirements – Part 11 : Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 6 : Wireless Access in Vehicular Environments, July 2010.

[58] Sofiane Imadali, Arnaud Kaiser, and Fikret Sivrikaya. A review of network mobility protocols for fully electrical vehicles services. In *IEEE Intelligent Transportation Systems Magazine*, 2014.

[59] Sofiane Imadali, Véronique Vèque, and Alexandru Petrescu. Analyzing dynamic ipv6 address auto-configuration techniques for group ip-based vehicular communications. In *IEEE 39th Conference on Local Computer Networks*, pages 722–729, 2014.

[60] James R. Jackson. Jobshop-Like Queueing Systems. *Management Science*, 10(1) :131–142, 1963.

[61] Jaehoon Jeong, Shuo Guo, Yu Gu, Tian He, and David Du. Tbd : Trajectory-based data forwarding for light-traffic vehicular networks. In *Distributed Computing Systems, 2009. ICDCS'09. 29th IEEE International Conference on*, pages 231–238. IEEE, 2009.

[62] D. Johnson, C. Perkins, and J. Arkko. RFC 3775 - Mobility support in IPv6. *In : IETF*, 2004.

[63] T. Kabir, N. Nurain, and M. H. Kabir. Pro-aodv (proactive aodv) : Simple modifications to aodv for proactively minimizing congestion in vanets. pages 1–6, 2015.

[64] Brad Karp and H. T. Kung. GPSR : Greedy perimeter stateless routing for wireless networks. In *Proceedings of the sixth annual international conference on Mobile computing and networking MOBICOM, Boston, MA, USA.*, pages 243–254, 2000.

[65] S. Kuhlmorgen, I. Llatser, A. Festag, and G. Fettweis. Performance evaluation of ETSI GeoNetworking for vehicular Ad Hoc networks. In *IEEE 81st Vehicular Technology Conference (VTC Spring)*, pages 1–6, May 2015.

[66] Sebastian Kuhlmorgen, Ignacio Llatser, Andreas Festag, and Gerhard Fettweis. Performance evaluation of etsi geonetworking for vehicular ad hoc networks. In *2015 IEEE 81st Vehicular Technology Conference (VTC Spring)*, pages 1–6. IEEE, 2015.

[67] L Le, A Festag, A Mader, R Baldessari, M Sakata, T Tsukahara, and M Kato. Infrastructure-assisted communication for car-to-x communication. *18th ITS World Congress*, 2011.

[68] Kevin C Lee, Uichin Lee, and Mario Gerla. To-go : Topology-assist geo-opportunistic routing in urban vehicular grids. In *Wireless On-Demand Network Systems and Services, 2009. WONS 2009. Sixth International Conference on*, pages 11–18. IEEE, 2009.

[69] I. Leontiadis and C. Mascolo. Geopps : Geographical opportunistic routing for vehicular networks. In *IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks*, pages 1–6. IEEE, 2007.

[70] Christian Lochert, Martin Mauve, Holger Füßler, and Hannes Hartenstein. Geographic routing in city scenarios. *ACM SIGMOBILE mobile computing and communications review*, 9(1) :69–72, 2005.

[71] Y. Ma and A. Jamalipour. Opportunistic geocast in disruption-tolerant networks. In *IEEE Global Telecommunications Conference*, pages 1–5. IEEE, 2011.

[72] M.Fazio, S.Das, Claudio E. Palazzi, and M.Gerla. Vehicular address configuration. In *in Proc. of the 1st IEEE Workshop on Automotive Networking and Applications (AutoNet), GLOBECOM 2006*, 2006.

[73] M.Gramaglia, Carlos J. Bernardos, I.Soto, M.Calderon, and R.Baldessari. IPv6 address autoconfiguration in geonetworking-enabled VANETs : characterization and evaluation of the ETSI solution. *EURASIP Journal on Wireless Communications and Networking*, 2012 :19 :1–17, 2012.

[74] M.Gramaglia, I.Soto, Carlos J. Bernardos, and M.Calderon. Overhearing Assisted Optimization of Address Auto-Configuration in Position Aware VANETs. *IEEE Transactions on Vehicular Technology*, 60(7) :3332–3349, 2011.

[75] I. C. Msadaa, P. Cataldi, and F. Filali. A comparative study between 802.11p and mobile wimax-based v2i communication networks. In *Fourth International Conference on Next Generation Mobile Applications, Services and Technologies*, pages 186–191, 2010.

[76] Sze-Yao Ni, Yu-Chee Tseng, Yuh-Shyan Chen, and Jang-Ping Sheu. The broadcast storm problem in a mobile ad hoc network. In *The Fifth Annual ACM/IEEE International Conference on Mobile Computing and Networking MOBICOM, Seattle, Washington, USA.*, pages 151–162, 1999.

[77] C. Perkins. RFC 3344 - IP Mobility support for IPv4. *In : IETF*, 2002.

[78] C. Perkins, D. Johnson, and J. Arkko. RFC 6275 - Mobily Support in IPv6. *In : IETF*, 2011.

[79] R.Baldessari, J. Bemardos, and M.Calderon. GeoSAC scalable address autoconfiguration for vanet using geographic networking concepts. 2008.

[80] Musabe Richard and Larijani Hadi. Congestion aware spray and wait protocol : A congestion control mechanism for the vehicular delay tolerant network. *CoRR*, abs/1601.01527 :24–33, 2016.

[81] M. Rondinone and J. Gozalvez. Distributed and real time communications road connectivity discovery through vehicular adhoc networks. 2010.

[82] M. R. J. Sattari, R. M. Noor, and H. Keshavarz. A taxonomy for congestion control algorithms in vehicular ad hoc networks. In *IEEE International Conference on Communication, Networks and Satellite (ComNetSat)*, pages 44–49, 2012.

[83] Oyunchimeg Shagdar. Evaluation of Distributed Congestion Control -Reactive DCC. Research report, Inria, December 2014.

[84] Heecheol Song and Hwang Soo Lee. A survey on how to solve a decentralized congestion control problem for periodic beacon broadcast in vehicular safety communications. In *Advanced Communication Technology (ICACT), 2013 15th International Conference on*, pages 649–654. IEEE, 2013.

[85] Bellache Thiwiza, Shagdar Oyunchimeg, and Tohmé Samir. An alternative congestion control using an enhanced contention based forwarding for vehicular networks. In *13th Annual Conference on Wireless On-demand Network Systems and Services,WONS*, pages 81–87, Feb. 2017.

[86] Tessa Tielert, Daniel Jiang, Qi Chen, Luca Delgrossi, and Hannes Hartenstein. Design methodology and evaluation of rate adaptation based congestion control for vehicle safety communications. In *Vehicular Networking Conference (VNC), 2011 IEEE*, pages 116–123. IEEE, 2011.

[87] T.Narten and T.Jinmei and S.Thomson. IPv6 Stateless Address Autoconfiguration, sep 2007.

[88] V.Sandonis, I.Soto, M.Calderon, and M.Uruena. Vehicle to internet communications using the etsi its geonetworking protocol. October 2014.

[89] Nawaporn Wisitpongphan, Ozan K. Tonguz, Jayendra S. Parikh, Priyantha Mudalige, Fan Bai, and Varsha K. Sadekar. Broadcast storm mitigation techniques in vehicular ad hoc networks. *IEEE Wireless Commun.*, 14(6) :84–94, 2007.

[90] W.Xiaonan, L.Deguang, and C.Hongbin. Location-based ipv6 address configuration for vehicular networks. *Journal of Network and Systems Management*, 24(2) :257–284, 2016.

[91] W.Xiaonan and Q.Huanyan. A mobility handover scheme for ipv6-based vehicular ad hoc networks. *Wireless Personal Communications*, 70(4) :1841–1857, 2013.

[92] X.Wang, D.Wang, and S.Qi. Mobility support for vehicular networks based on vehicle trees. *Computer Standards & Interfaces*, 49(2) :1–10, 2017.

[93] Jing Zhao and Guohong Cao. Vadd : Vehicle-assisted data delivery in vehicular ad hoc networks. *IEEE transactions on vehicular technology*, 57(3) :1910–1922, 2008.

[94] X. Zhou, J.Korhonen, C.Williams, S.Gundavelli, and C.Bernardos. RFC 7148 - Prefix Delegation Support for Proxy Mobile IPv6. *IEEE Communications Magazine*, 27, Mar 2014.

[95] Z. Zhu, R. Wakikawa, and L. Zhang. RFC 6301 - A survey of mobility support in the internet. *In : IETF*, 2011.