République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université A.MIRA-BEJAIA

Faculté des Sciences Exactes
Département d'Informatique
Unité de recherche LaMOS

THÈSE

EN VUE DE L'OBTENTION DU DIPLOME DE DOCTORAT

Domaine : Mathématiques et Informatique Filière : Informatique
Spécialité : Réseaux et Systèmes Distribués

Présentée par
Yani-Athmane BENNAI

Thème

Contrôle d'accès et routage avec qualité de service dans les réseaux VANETs

Soutenue le : 31/03/2022 **Devant le Jury composé de :**

Nom et Prénom	**Grade**		
Mr AÏSSANI Djamil	Professeur	Univ. de Bejaia	Président
Mme BOUALLOUCHE Louiza	Professeur	Univ. de Bejaia	Rapporteur
Mme YESSAD Samira	M.C.B	Univ. de Bejaia	Co-Rapporteur
Mr SAYAD Lamri	M.C.A	Univ. de M'Sila	Examinateur
Mr AISSANI Sofiane	M.C.A	Univ. de Bejaia	Examinateur
Mme BOULAHROUZ Djamila	M.C.A	Univ. de Bejaia	Examinatrice

Année Universitaire : **2021/2022**

Remerciements

Je tiens à adresser en premier lieu mes remerciements et ma profonde gratitude à ma directrice de thèse Mme BOUALLOUCHE-MEDJKOUNE Louiza pour m'avoir permis d'intégrer son équipe de recherche au sein du laboratoire LaMOS et avoir dirigé mes travaux de thèse. Je la remercie pour son encadrement extrêmement professionnel, son aide précieuse et sa confiance sans lesquels ce travail n'aurait pas été possible.

Mes remerciements s'adressent également à Mme YESSAD Samira Epse OUYAHIA pour avoir co-dirigé ce travail, pour ses critiques, ses précieux conseils, et surtout pour sa disponibilité tout au long de ces années.

Je remercie chaleureusement l'ensemble des membres du jury pour l'intérêt qu'ils ont porté à notre travail. Je remercie Monsieur AISSANI Sofiane, docteur à l'Université de Béjaia, Monsieur SAYAD Lamri, docteur à l'Université de M'Sila et Madame BOULAHROUZ Djamila, docteur à l'Université de Béjaia, de nous avoir honorés en acceptant la charge de travail qu'implique la lecture critique de ce manuscrit. Je remercie également Monsieur AÏSSANI Djamil, Professeur à l'Université de Béjaia pour l'honneur qu'il m'a fait en acceptant de présider le jury.

Je remercie également, de façon plus générale, tous les membres du laboratoire LaMOS ainsi que du laboratoire LIMED avec qui j'ai pu échanger et travailler.

Dédicaces

Je dédie ce travail :

À Mon défunt père, qui m'a encouragé et m'a éclairé par ses conseils bienveillants.

À ma chère mère et mon cher frère pour leur soutien indéfectible durant ces années.

Aux membres de ma famille et mes amis qui m'ont, de près ou de loin, aidé par leur présence à mes côtés.

Table des matières

Table des figures

Liste des algorithmes

Liste des tableaux

Liste des abréviations

A-STAR : Anchor-based Street and Traffic Aware Routing

AAA : Advanced Activity Aware multi-channel operations

ABF : Adaptive Broadcast Frame

ACK : ACKnowledgement

AIFS : Arbitration Inter-Frame Space

AODV : Ad-hoc On-demand Distance Vector

ATSA : Adaptative TDMA Slot Assignment

AU : Applications Unit

BCH : Basic Channel

BP : Beacon Period

CAHMAC : Cooperative AdHoc MAC

CBMAC : Cluster Based Medium Access Control

CBMCS : Clustering Based MultiChannel Communication System

CBT : Cluster-Based Tdma

CCH : Control Channel

CCRV-MAC : Cooperation in Cognitive Radio-based Vehicular Ad-hoc NETworks

CDS : Connected Dominating Sets

CEA : Centralized Enhancement Algorithme

CH : Cluster Head

CFR : Collision Free Reservation

CRP : Contention-based Reservation Period

CSMA/CA : Carrier Sense Multiple Access / Collision Avoidance

CSMA/CD : Carrier Sense Multiple Access / Collision Detection

CTB : Clear-To-Broadcast

CTS : Clear To Send

CTT : Connection Terminaison Time

CW : Contention Window

D-MAC : Directionnal MAC

DCF : Distributed Coordination Function

DCI : Dynamic CCH Interval

DEA : Distributed Enhancement Algorithme

DGR : Directional Greedy Routing

DIFS : Distributed Inter Frame Spacing

DMMAC : Dedicated Multi-channel MAC

DSRC : Dedicated Short-Range Communication Protocol

DTB-MAC : Dynamic Token-Based MAC

DYMO : DYnamic MANET On demand

EDCA : Enhanced Distributed Channel Access

EIFS : Extended Inter Frame Spacing

FI : Frame Information

FSP : Fuzzy Slot Priority

GINS : Geographic Information and Node Selfish-based routing

GPS : Global Positioning System

GPCR : Greedy Perimeter Coordinator Routing

GPSR : Greedy Perimeter Stateless Routing

GRUV : Geocast Routing in Urban Vehicular ad hoc networks

GSR : Global State Routing

GyTAR : Greedy Traffic Aware Routing

HN : Helper Nodes

HRV : Hybrid Routing in VANETs

ICA : Imperialist Competitive Algorithme

ICH : Intersection Cluster Head

IDVR : Intersection Dynamic VANET Routing

IEEE : Institute of Electrical and Electronic Engineering

ITS : Intelligent Transportation Systems

IVC : Inter-Vehicle Communication

LLC : Logical Link Control

LSR : Link State Routing

LREP : Location Reply

LREQ : Location Request

M-GEDIR : Multi-metric GEographic DIRectionnal routing

MAC : Medium Access Control

MANET : Mobile Ad hoc Network

MCCM-MAC : Mobility-Caused Collision Mitigation MAC

MCTRP : Multi Channel Token Ring Protocol

MPR : Multi-Point Relay

MSM : Mixed-Service-Mobility Model

MST : Minimum Spanning Tree Algorithm

NA-MAC : Neighbor Association-based MAC

NC-MAC : Network Coding-based Medium Access Control

OBU : On Board Unit

OFDM : Orthogonal Frequency Division Multiplexing

OLSR : Optimized Link State Routing

PNC : Physical-layer Network Coding

RMAC : Roundabout MAC

PDGR : Predictive Directional Greedy Routing

PDVR : Position-based Directional Vehicular Routing

PSCAR : Proactive-optimal-path Selection with Coordinator Agents assisted Routing

PSO : Particle Swarm Optimization

PSID : Provider Service Identifier

RR-ALOHA : Reliable Reservation ALOHA

RTB : Request-To-Broadcast

SAT : Slot Allocation Table

SCH : Service Channel

SCMAC : Slotted Contention-based Media Access Control

SIFS : Short Inter-Frame Space

SNAP : Sub-Network Access Protocol

SP : Safety Period

STDMA : Self-organized Time-Division Multiple Access

STI : Systèmes de Transport Intelligents

UTC : Universal Time Coordinated

QCH-MAC : Qos-aware Centralized Hybrid MAC

QoS : Quality of Service

RLNC : Random Linear Network Coding

RLR : Randomized Link Repair

ROVER : RObust VEhicular Routing

RREQ : Route REQuest

RSU : Road Side Unit

RTS : Request To Send

TA : Trusted Authority

TDMA : Time Division Multiple Access

UAV : Unmanned Aerial Vehicles

UMB : Urban Multi-hop Broadcast protocol

V2I : Vehicle to Infrastructure

V2V : Vehicle to Vehicle

VANET : Vehicular Ad Hoc Network

V-MESH : Vehicular MESH

VMMAC : Vanet Multi-channel MAC

VRCP : Vehicle to vehicle and Road to vehicle Collaborative Protocol

WAVE : Wireless Ability in Vehicular Environments

WLAN : Wireless Local Area Network

W-HCF : WAVE-based Hybrid Coordination Function

W-UIM : WBSS User Initiation Mode

Liste des contributions

Dans le cadre de nos recherches, nous avons réalisé les contributions scientifiques suivantes :

1. Une synthèse sur les principaux protocoles MAC proposés pour les VANETs, qui a fait l'objet d'une présentation dans les doctoriales avec actes de recherche opérationnelle 2018, organisées par l'unité de recherche LaMOS [1].

2. Un protocole de contrôle d'accès avec qualité de service pour les réseaux véhiculaires, qui a fait l'objet d'une publication dans une revue internationale indexée dans la base Scopus [2].

3. Un protocole de routage dédié aux autoroutes et basé sur la stabilité des liens de communication, qui a donné lieu à une présentation dans une conférence internationale avec actes [3].

[1] **Yani-Athmane Bennai, Samira Yessad, and Louiza Bouallouche-Medjkoune. Synthèse sur les principaux protocoles MAC proposés pour les VANETs. Doctoriales de Recherche Opérationnelle 2018, Université de Béjaia, 2018.**

[2] **Yani-Athmane Bennai, Samira Yessad, and Louiza Bouallouche-Medjkoune. A flexible and adaptive medium access control protocol for improving quality of service in vehicular ad-hoc networks. International Journal of Computers and Applications, pages 1–10, 2021.**

[3] **Yani-Athmane Bennai, Samira Yessad, and Louiza Bouallouche-Medjkoune. Link stability based routing protocol for highway scenarios in vehicular networks. 6^{th} IEEE International Conference on Recent Advances and Innovations in Engineering, Malaysia, 2021.**

Introduction générale

Durant ces dernières années, le nombre de véhicules en circulation sur les routes a connu une augmentation exponentielle partout dans le monde. Cette augmentation a poussé la communauté scientifique à travailler sur des moyens efficaces pour gérer ce trafic routier, dans le but d'offrir des services utiles aux conducteurs, tout en garantissant leur sécurité. Pour ce faire, il était nécessaire de définir un nouvel environnement afin de répondre à ces nouveaux besoins, c'est pour cela que dès les années 90, la notion de systèmes de transport intelligents "STI" (ou en anglais ITS pour Intelligent Transportation Systems) a été introduite. Ces systèmes utilisent les technologies de l'information et de la communication en les intégrant aux infrastructures de transport et aux véhicules dans le but de partager des données permettant d'améliorer l'efficacité des systèmes de transport.

Pour la mise en œuvre pratique de ces systèmes de transport intelligents, il était nécessaire de concevoir un nouveau type de réseaux Ad Hoc qui pourrait refléter le caractère très dynamique du trafic routier, ce qui a donné naissance aux VANETs (Vehicular Ad Hoc Networks). Dans ce contexte, plusieurs efforts de normalisation ont été déployés afin de tirer le meilleur parti de cette nouvelle idée de réseaux de véhicules. Parmi ces normes, 802.11p proposée par l'IEEE a suscité beaucoup d'intérêt chez les chercheurs et spécialistes. Elle est actuellement le standard le plus utilisé que ce soit pour les tests en conditions réelles ou les simulations sur machines.

Les enjeux principaux des différentes études conduites par le passé et celles en cours concernent : l'implémentation physique de ces réseaux dans un avenir proche, la garantie de la qualité de service et de la sécurité des données, l'assurance d'un accès efficace au canal, un routage et une dissémination de messages efficaces, etc. Mais pour l'instant, il existe énormément de verrous scientifiques et économiques à lever avant d'y parvenir.

Comme pour les autres types de réseaux Ad Hoc, le routage et l'accès au canal au sein des VANETs sont deux mécanismes sur lesquels il est crucial de se concentrer lorsqu'on a pour objectif de garantir une bonne qualité de service dans le réseau pour principalement éviter la perte de paquets de service et de sécurité critiques. Cette qualité de service est d'autant plus difficile à fournir dans le contexte des réseaux véhiculaires de par leur topologie très instable.

Dans ce travail, nous nous sommes intéressés aussi bien à l'accès au médium qu'au routage dans les VANETs, en apportant deux contributions majeures.

L'accès au canal qui est géré par le protocole MAC, s'effectue en programmant les transmissions en fonction du temps, de la fréquence, et en utilisant des codes uniques pour distinguer les différents utilisateurs. Dans la littérature, nous pouvons distinguer deux types principaux de protocole MAC : les protocoles MAC non-déterministes et déterministes. Dans les protocoles à accès non-déterministe, l'accès au support est aléatoire et basé sur un système de compétition. Contrairement au deuxième type, où un contrôleur central peut répartir les ressources entre toutes les stations nécessitant un accès et qui seront autorisées à émettre dans les limites d'un certain délai. Après une étude critique des différents protocoles MAC proposés pour les VANETs [1], nous avons constaté que les protocoles MAC déterministes sont plus adaptés aux topologies de réseaux centralisées, alors que dans les réseaux distribués tels que les VANETs, le protocole MAC doit être distribué et doit s'adapter en permanence à l'évolution du trafic de données et de la densité du réseau. En constatant que le protocole MAC non-déterministe 1609.4 de la norme IEEE 802.11p répond en partie à ces contraintes de conception des protocoles MAC pour les VANETs, nous avons choisi de l'étudier et de l'améliorer et ainsi proposer une version plus flexible et adaptative aux besoins du réseau en ajoutant trois mécanismes à la version originale [2]. Ces améliorations assurent une communication plus fiable et avec qualité de service, et comportent : un algorithme d'équité conçu pour faciliter l'accès au canal aux véhicules ayant des difficultés à transmettre (à cause d'une vitesse de déplacement élevée par exemple), une adaptation dynamique de l'intervalle SCH en fonction du taux d'échecs des transmissions de paquets de service dans le but d'optimiser l'allocation du temps sur le canal et de mieux répondre aux besoins du réseau. Pour finir, nous avons conçu un mécanisme d'urgence utilisable dans les cas où un évènement dangereux survient sur la route et que la transmission de paquets de sécurité critiques devient hautement prioritaire. Les nombreuses simulations que nous avons effectuées afin de comparer les performances de nos contributions avec celles du protocole d'origine ainsi que le protocole MAC "AAA", montrent une nette amélioration pour plusieurs métriques de performances fondamentales, en termes de qualité de service, à savoir : le taux de perte, le débit et le taux de réussite des paquets de sécurité critiques.

Ces simulations montrent également une meilleure adaptation à l'augmentation de la vitesse des véhicules dans notre contribution.

Dans la deuxième partie de notre recherche, nous avons étudié les principaux protocoles de routage dédiés aux réseaux véhiculaires. Nous avons constaté qu'il y a très peu de protocoles dédiés exclusivement aux environnements autoroutiers, c'est-à-dire des protocoles conçus pour fonctionner dans des conditions de vitesse extrêmes. Et il en existe encore moins qui sont basés sur le concept de stabilité des liens de communication, alors que cette notion est prioritaire dans le contexte des autoroutes, vu la grande mobilité des véhicules qui y circulent. Ainsi, nous avons proposé un nouveau protocole de routage conçu spécialement pour les scénarios d'autoroutes, et exploitant le concept de stabilité des liens de communication [3]. Ce protocole est adapté aux réseaux dans lesquels la vitesse de déplacement des véhicules est particulièrement élevée. Nous avons conduit des simulations pour comparer les performances de notre contribution avec celles de deux autres protocoles de routage adaptés aux environnements ouverts (GPSR et PDGR). Ces simulations ont permis de montrer que le fait de mettre l'accent sur la stabilité des liens permet de réduire de manière très efficace la perte de paquets tout en améliorant le débit global du réseau. Les résultats obtenus montrent aussi que notre solution permet de réduire la dégradation des performances avec l'augmentation de la vitesse des véhicules.

Ce manuscrit est organisé en cinq chapitres :

Le premier chapitre présente une vue d'ensemble des réseaux véhiculaires en mettant l'accent sur les standards, les notions théoriques et les principaux composants des VANETs.

Le second chapitre comprend un état de l'art sur les différents travaux réalisés dans le domaine de l'accès au canal pour les réseaux véhiculaires. Ces travaux sont brièvement décrits puis critiqués dans un tableau comparatif.

Le troisième chapitre comprend notre deuxième état de l'art, dédié aux travaux réalisés dans le domaine du routage pour les VANETs. Comme pour le deuxième chapitre, ces travaux sont résumés et critiqués.

Le quatrième chapitre présente notre contribution à l'accès au canal avec qualité de service dans les réseaux véhiculaires. Nos trois principaux apports y sont détaillés, à savoir :

— Un algorithme d'équité visant à uniformiser au maximum les chances d'accès au canal pour les nœuds en favorisant ceux ayant du mal à transmettre.

— Une adaptation dynamique de l'intervalle SCH en fonction du taux d'échec de transmission des paquets dans le but d'apporter de la flexibilité au protocole de base.

— **Un mécanisme d'urgence visant à offrir plus de réactivité dans le cas d'évènements dangereux soudains sur la route.**

Dans le cinquième chapitre, notre contribution au routage est présentée, avec un nouveau protocole destiné aux scénarios d'autoroute et basé sur le concept de stabilité des liens de communications. Ce protocole a été conçu pour offrir les transmissions les plus fiables possible dans des conditions de vitesse extrêmes, et améliorer ainsi la qualité de service pour les applications de sécurité routière.

Notre manuscrit se termine par une conclusion générale qui présente une synthèse de l'ensemble de nos contributions et quelques perspectives.

Chapitre I

Réseaux Véhiculaires, Caractéristiques et Architecture

Introduction

Dans ce premier chapitre, nous allons passer en revue les notions de base concernant les réseaux véhiculaires. Ces notions comportent les standards, quelques définitions, les mécanismes de fonctionnement et les caractéristiques qui définissent ce type de réseaux. Ceci est dans le but de définir l'environnement sur lequel nous avons effectué nos recherches et développé nos contributions, qui sont détaillées dans les prochains chapitres.

I.1 Les MANETs (Mobile Ad Hoc Networks)

Contrairement aux réseaux sans fil avec infrastructure, où chaque utilisateur communique directement avec un point d'accès ou une station de base, un réseau mobile Ad Hoc, ou MANET, ne dépend pas d'une infrastructure fixe pour son fonctionnement. Le réseau est une association de nœuds mobiles qui communiquent entre eux par des liaisons sans fil. Les nœuds qui se trouvent à portée de transmission les uns des autres peuvent communiquer directement et sont chargés de découvrir leurs voisins dynamiquement. Afin de permettre la communication entre des nœuds qui ne sont pas directement à portée de transmission les uns des autres, les nœuds intermédiaires agissent comme des routeurs qui relaient vers leur destination les paquets générés par d'autres nœuds. Ces derniers sont souvent des appareils à contrainte énergétique, c'est-à-dire à piles, dont les capacités sont très variées. En outre, les appareils sont libres de rejoindre ou de quitter le réseau et ils peuvent se déplacer de manière aléatoire, ce qui peut entraîner des changements de topologie rapides et imprévisibles. Dans cet environnement à énergie limitée, dynamique et distribué à sauts multiples, les nœuds doivent s'organiser de manière dynamique afin de

fournir les fonctionnalités de réseau nécessaires en l'absence d'infrastructure fixe ou d'administration centrale [4].

I.2 Les VANETs (Vehicular Ad Hoc Networks)

Les réseaux Ad Hoc véhiculaires (VANETs), reposent sur le même fonctionnement que les réseaux mobiles, à l'exception prés que les nœuds sont ici représentés par des véhicules dits intelligents. Ces derniers sont équipés de capteurs et de calculateurs et sont caractérisés, entre autres, par leur forte mobilité. Ils se composent aussi de deux autres types d'unités majeurs, les équipements de bord de route (RSU, Road Side Unit) ainsi que les infrastructures de contrôle et de gestion. Cet ensemble constitue ce qu'on appelle un système de transport intelligent (ITS) qui est dédié à la satisfaction d'un certain nombre d'objectifs que nous développerons ultérieurement [5].

I.3 Les caractéristiques des VANETs

Les réseaux véhiculaires présentent, de par leur forte mobilité entre autres, des caractéristiques qui leur sont propres.

I.3.1 Mobilité des véhicules

Le paramètre principal permettant de distinguer les réseaux VANETs des autres réseaux Ad Hoc est le déplacement très fréquent de leurs nœuds. Ainsi, la topologie est fortement dynamique dans ce type de réseaux, ce qui fragilise les liens de communication entre ses nœuds [6].

I.3.2 Mémoire et énergie

C'est une contrainte qui pose généralement problème dans les réseaux de capteurs sans fil par exemple. Mais grâce aux batteries embarquées dans les véhicules, la contrainte de consommation d'énergie n'est pas un souci dans les réseaux véhiculaires [6].

I.3.3 Nécessité de garantir un haut niveau de performances

À cause du caractère parfois urgent des paquets circulant dans un réseau VANET (alertes d'accidents ou d'événements dangereux), il est nécessaire de garantir un niveau de performances minimum en termes de délais et de perte de paquets [5].

I.3.4 Environnement de communication

Le fait que ce type de réseaux soit implémenté dans des routes automobiles implique une grande diversité en termes d'environnement de communication. En effet, les VANETs peuvent passer d'un environnement autoroutier dégagé avec des vitesses de circulation élevées et très peu d'obstacles, à des scénarios urbains beaucoup plus denses contenant des obstacles [5].

I.3.5 Les Stratégies de transmission

Les VANETs étant un sous-type de réseaux Ad Hoc, on y trouve plusieurs stratégies de transmission de paquets, allant de L'Unicast au Broadcast en passant par le Multicast (voir Figure I.1). Cependant, en raison de la nature des messages envoyés le plus souvent dans les VANETs, à savoir des messages d'information ou d'avertissement destinés à des groupes de nœuds, il s'avère que le Broadcast suivi de l'Unicast sont les deux modes de transmission dominants [5].

La transmission par Unicast

Dans ce type de transmissions, le paquet voyage d'un nœud source vers un seul nœud destinataire, en passant par d'éventuels nœuds intermédiaires qui servent de relais. L'Unicast est très largement utilisé dans les réseaux Ad Hoc classiques, mais plusieurs propositions d'adaptation pour les VANETs peuvent être trouvées dans la littérature [7].

La transmission par Broadcast

Avec cette méthode, les paquets circulent pour atteindre tous les nœuds visés et inclus dans le domaine de diffusion. Elle est largement utilisée dans tous les types de réseaux et donc aussi dans les réseaux véhiculaires. Le fait qu'un paquet puisse être retransmis par plusieurs nœuds du réseau augmente la probabilité que ce dernier arrive à destination, mais cela peut aussi engendrer une sur-consommation de la bande passante à cause de la réplication de paquets. Certains protocoles proposent que les nœuds qui identifient les paquets répliqués, les détruisent au lieu de les relayer [7].

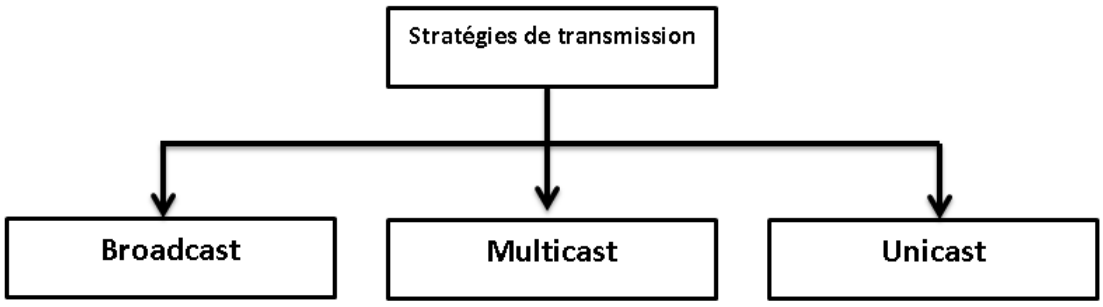

FIGURE I.1 – Stratégies de transmission

I.4 Les applications des VANETs

Les applications des VANETs peuvent se résumer en trois grandes catégories, les applications de sécurité routière, de gestion du trafic routier et les applications d'info-divertissement.

I.4.1 La sécurité routière

Ce type d'applications vise à réduire la probabilité qu'un accident de la route se produise et minimiser ainsi le nombre de victimes qu'elles soient des conducteurs ou des piétons. Les usagers de la route sont informés de tous risques potentiels ou événements dangereux grâce au partage d'informations telles que des données concernant les intersections, les zones à risque, l'état de la chaussée, le positionnement des véhicules, etc. La transmission de ces informations peut se faire suivant deux modes de communications principaux : communication entre véhicules et communication de véhicule à infrastructure, qui seront détaillées dans ce premier chapitre.

Quelques exemples d'applications spécifiques :

- **Prévention des collisions dans les intersections**
- **Assistance de changement de file**
- **Prévention des risques de collisions lors des dépassements**
- **Signalement de véhicules d'urgence et prioritaires**
- **Signalement pré-crash**
- **Feu de freinage électronique d'urgence**
- **Avertisseur de mauvais sens de conduite**
- **Avertisseur de véhicule arrêté ou en panne**
- **Avertisseur sur l'état du trafic**
- **Avertisseur de violation de signal**

— **Avertisseur de zone de danger sur la route**

— **Avertisseur de perte de contrôle du véhicule**

I.4.2 La gestion du trafic routier

Ces applications servent de soutien aux automobilistes en les guidant dans leur circulation. En effet, elles coordonnent les usagers de la route en utilisant les informations de trafic routier en temps réel afin de leur fournir les meilleurs itinéraires possibles. Elle utilise la position géographique des véhicules, l'état des routes et la densité de ces dernières en termes de véhicules. Bien que les objectifs soient nombreux, nous pouvons distinguer deux groupes majeurs dans ce type d'applications [8].

— **La gestion de la vitesse : le but ici est d'assister le conducteur afin d'optimiser la vitesse à laquelle il circule, et trouver un équilibre entre un rythme qui lui permettra de gagner du temps sans pour autant se mettre en danger.**

— **La circulation coopérative : qui vise tout simplement à faire communiquer les véhicules entre eux, cet échange d'informations doit permettre de satisfaire un maximum de membres du réseau.**

I.4.3 L'info-divertissement

Ces applications remplissent un rôle moins crucial comparé aux deux autres, et visent avant tout à améliorer la qualité de l'expérience utilisateur. Elles offrent des services de confort, d'information et de divertissement sous la forme de jeux en ligne, bulletins météo et streaming audio et vidéo par exemple. Il existe deux types d'applications d'info-divertissement, les applications locales et celles qui puisent directement d'internet.

I.5 Composants des réseaux véhiculaires

Dans les réseaux véhiculaires, comme le montre la Figure I.2, on trouve trois principaux composants :

I.5.1 Unités embarquées (On Board Unit, OBU)

Une OBU est un équipement embarqué sur les véhicules qui a pour fonction de permettre à ces derniers d'établir des communications directes avec d'autres véhicules (V2V), ou avec des infrastructures telles que les RSU (V2I). Cet équipement est généralement constitué d'une carte réseau, une antenne radio, une interface utilisateur ainsi qu'un processeur.

I.5.2 Unités de bord de route (Road Side Unit, RSU)

Ce sont des ponts réseau installés sur les bords des routes qui permettent aux nœuds du réseau d'établir une connexion à internet [6]. Les fonctions principales des RSU sont :

- **Elargir la couverture réseau du VANET et ainsi rendre possible l'échange de données avec les équipements embarqués.**
- **Servir de source d'informations pour le réseau.**
- **Permettre aux OBU de se connecter à internet.**

I.5.3 Autorités de confiance (Trusted Authority, TA)

C'est la partie du réseau qui permet d'assurer sa sécurité. En effet, pour que deux véhicules puissent communiquer de manière confidentielle au sein du VANET, chacun d'eux doit posséder une copie de l'accrédité (liste d'autorisations) de l'autre sous forme d'un certificat signé par l'autorité de confiance [8]. Les TA ont pour principales fonctions :

- **La génération de clés pour le cryptage des messages.**
- **La gestion des listes des véhicules autorisés.**
- **Le traçage de la source des messages pouvant créer des problèmes dans le réseau.**
- **L'identification des attaques.**

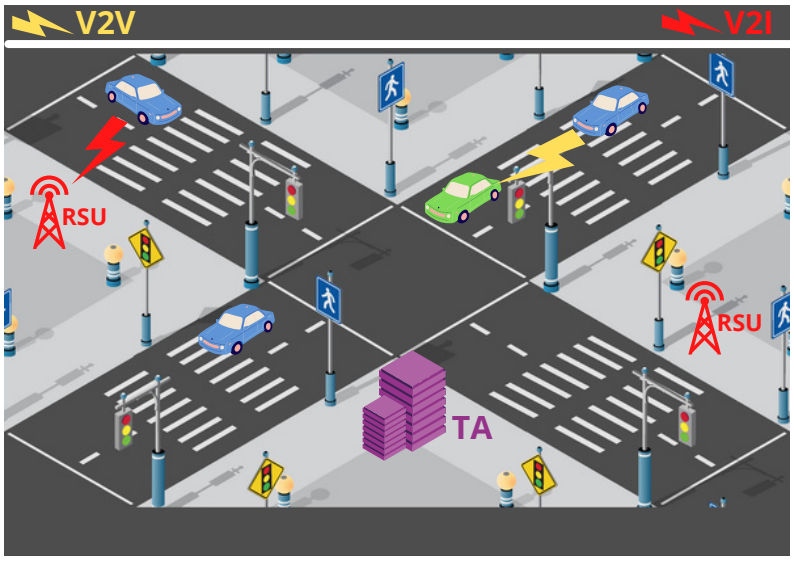

FIGURE I.2 – Structure générale des VANETS.

I.6 Architecture et schémas de communication

Les communications dans les VANETs peuvent être de deux types, véhicule à véhicule ou véhicule à infrastructure :

I.6.1 Communication de type Véhicule à Véhicule (V2V)

La communication V2V fait référence à l'échange d'information de manière directe entre les nœuds du réseau sans passer par un relais intermédiaire non véhiculaire. Ce mode de communication est surtout utilisé pour l'envoi de paquets de sécurité critiques, telles que les alertes d'accidents ou d'événements dangereux sur la route (voir Figure I.3). Pour ce faire, les nœuds du réseau doivent être équipés de capteurs et d'une carte réseau implantée dans l'OBU et avoir à leur disposition des informations concernant la position des autres nœuds grâce au service de positionnement global (GPS). Un nœud souhaitant découvrir son voisinage utilise généralement des messages de type HELLO diffusés périodiquement, ceci permet au nœud d'avoir une idée de la topologie locale. La communication V2V peut être effectuée par Unicast ou par Multicast. Unicast décrit l'envoi de paquets depuis un nœud source vers un seul nœud destinataire. Multicast décrit l'envoi vers un groupe composé de plusieurs destinataires [9].

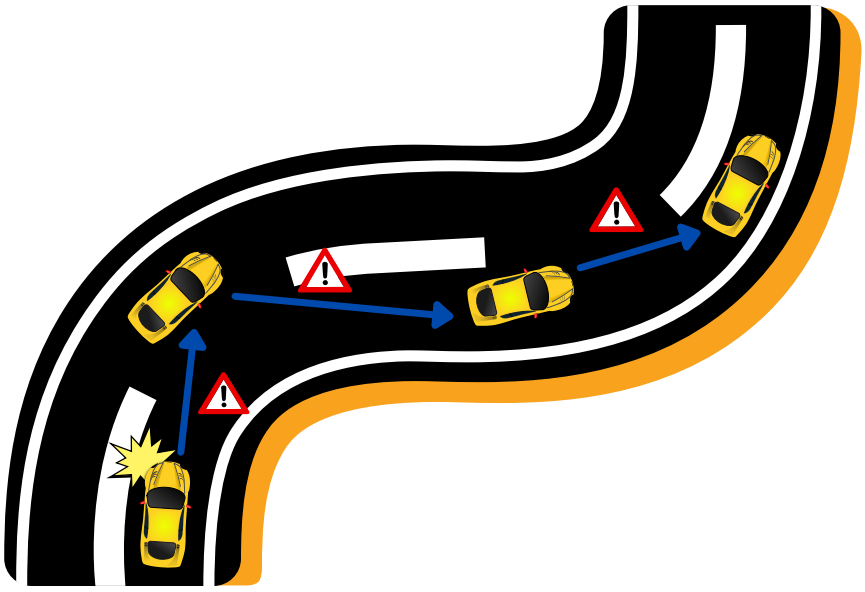

FIGURE I.3 – Communication de type véhicule à véhicule.

I.6.2 Communication de type Véhicule à Infrastructure (V2I)

La communication entre les unités de bord de route et les véhicules se fait dans la plupart des cas sans nœuds intermédiaires (voir Figure I.4). La RSU utilise des diffusions (Broadcast) afin d'atteindre les véhicules qui sont à l'intérieur de sa zone de couverture. Dans les environnements routiers denses (villes et métropoles), il est intéressant de placer des unités de bord de route à intervalles réguliers et séparées par de courtes distances. Ceci vise à offrir une couverture satisfaisante du réseau, ainsi qu'une bande passante suffisante pour répondre à la forte charge imposée par ses nœuds.

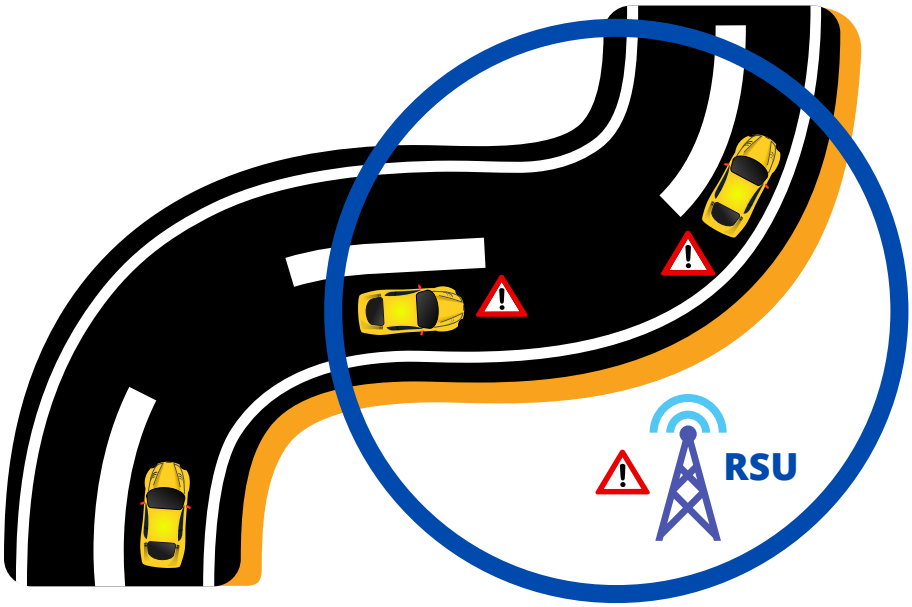

FIGURE I.4 – Communication de type véhicule à infrastructure.

I.7 Contraintes de conception

Le développement d'applications et protocoles pour les réseaux véhiculaires est rendu difficile par la nature très particulière de ce type de réseaux. Il existe certaines contraintes de conception, c'est-à-dire certains paramètres auxquels il est nécessaire de faire attention afin d'assurer le bon fonctionnement des VANETs.

I.7.1 La congestion dans le réseau

La congestion est causée par un surplus de données qu'un lien de communication ne peut pas transmettre car ce dernier est déjà saturé. Elle se traduit par une baisse de performances du réseau. Une solution pour faire face à ce problème réside dans l'utilisation de la mémoire tampon (Buffer), les paquets surnuméraires y sont ainsi placés en attendant que le temps de saturation se termine. Dans le cas où cette saturation se maintient trop longtemps, les nouveaux paquets arrivants seront automatiquement détruits, car ces derniers ne peuvent ni être transmis ni placés dans le Buffer. Ceci peut constituer un sérieux problème dans le cas du transport de données critiques [10].

I.7.2 La latence

La latence peut être définie par la durée de temps séparant l'émission et la réception d'un paquet dans le réseau, c'est-à-dire son délai de transmission. Elle dépend de la propagation, de la qualité des équipements et des retards éventuels. Au-delà du problème évident lié à une trop longue attente à cause de la latence, l'augmentation des temps de réponse de certaines applications peut s'avérer très gênante dans le cadre de l'amélioration de la qualité de service (QoS) [8].

I.7.3 La perte de paquets

Le taux de perte de paquets est le pourcentage de paquets n'ayant pas atteint leur destination lors de la transmission de données. Il s'agit d'un critère de qualité de service dans les réseaux Ad Hoc en général, et donc aussi les VANETs. Cette perte peut être causée par la congestion du réseau, une défaillance dans les équipements matériels ou alors une anomalie au sein du support de transmission. Minimiser ce taux revient donc à améliorer la qualité de service générale du réseau [8].

I.7.4 La sécurité

Comme pour tout réseau informatique, un VANET doit pouvoir garantir un certain niveau d'étanchéité afin de se protéger des attaques externes ou internes. Bien que de toute évidence la confidentialité et le respect de la vie privée des utilisateurs (automobilistes) doivent être un objectif, le plus important en ce qui concerne les applications de sûreté routière reste la résistance aux attaques visant à ralentir ou créer un dysfonctionnement dans le réseau (déni de service). La prévention ainsi que la réactivité sont donc primordiales si l'on veut garantir une bonne qualité de service [11].

I.8 La pile de protocoles WAVE

De nombreux efforts de recherche visent à standardiser et améliorer les performances globales des réseaux véhiculaires et les ITS [12] [13] puisque ces derniers représentent l'avenir du trafic routier. Parmi ces normes, celle proposée par la IEEE demeure celle qui mobilise la plus grande partie de la communauté scientifique. 802.11p [12] est une partie importante de la pile WAVE (voir Figure I.6) (Wireless Access in Vehicular Environments) proposée par la IEEE. 802.11p utilise la distribution d'accès au canal avancée présente dans la méthode MAC de l'EDCA [14], qui est elle-même une amélioration de la fonction de coordination distribuée (DCF) [15] utilisée dans la norme 802.11. Aux États-Unis, 75 MHz ont été consacrés exclusivement aux communications au sein des réseaux VANET (DSRC) [16]. La Figure I.5 montre la division de la bande passante, avec un total de sept canaux alloués [17]. Un canal de contrôle appelé CCH (Control Channel) que les véhicules ou les infrastructures utilisent pour échanger des informations de sécurité critiques ou bien des messages périodiques de sécurité. Six canaux de service appelés SCH (Service Channels) qui sont utilisés pour partager des données de service non critiques (divertissement et information) [18].

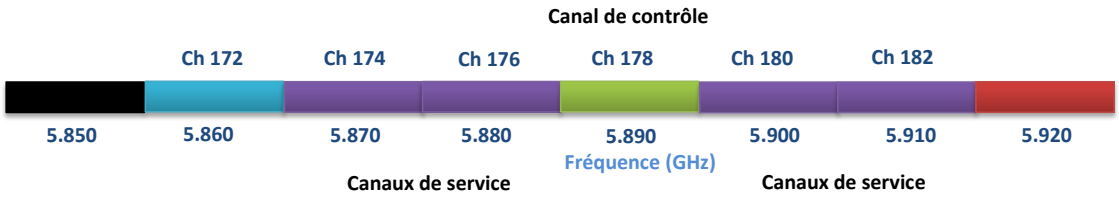

FIGURE I.5 – Distribution des fréquences

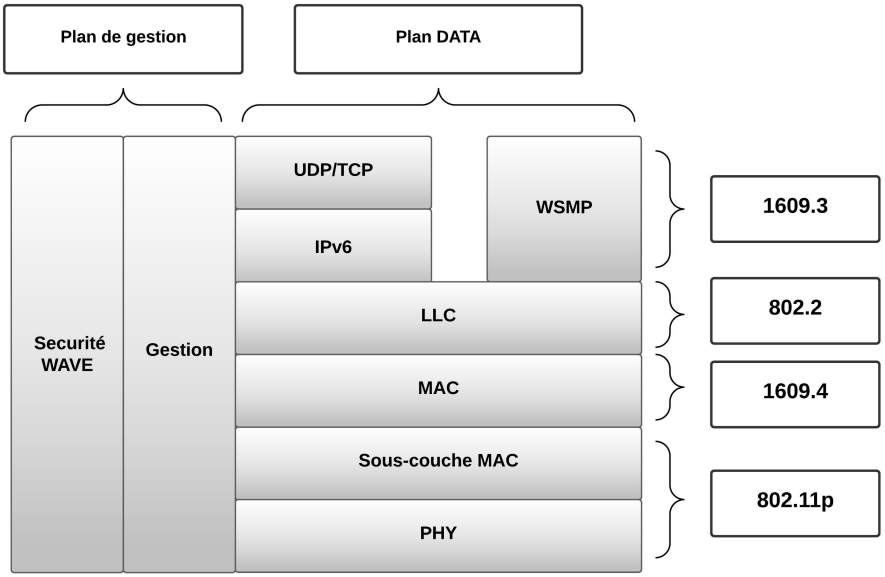

FIGURE I.6 – Pile de protocoles WAVE

La partie supérieure de la pile de protocoles WAVE est assez similaire au modèle TCP/IP traditionnel, avec les trois couches application, transport et réseau, tandis que la norme 802.2 regroupe les protocoles de la sous-couche LLC. La partie inférieure contient le standard 802.11p, on y trouve la couche physique et la couche MAC qui sont indissociables car elles font communiquer plusieurs protocoles dont 1609.4, qui gère l'accès au canal dans le réseau.

Dans 1609.4, le temps sur le canal est divisé en segments périodiques de 100 ms, et chaque segment est lui-même divisé en deux intervalles de 50 ms chacun (CCH et SCH, voir Figure I.7). Une période de temps nommée Guard est ajoutée au début de chaque intervalle pour résoudre les problèmes de désynchronisation entre les nœuds, sa durée varie entre 4 ms et 6 ms [19].

Le protocole 1609.4 utilise CSMA/CA (avec évitement de collisions)[20]. Un nœud souhaitant émettre sur le canal commence d'abord par effectuer une écoute, il envoie ses données s'il constate que ce dernier est libre. Cependant, si le canal est occupé, le nœud devra exécuter la procédure d'attente aléatoire avant d'essayer de transmettre à nouveau, l'accès aux canaux est donc basé sur un système de compétition.

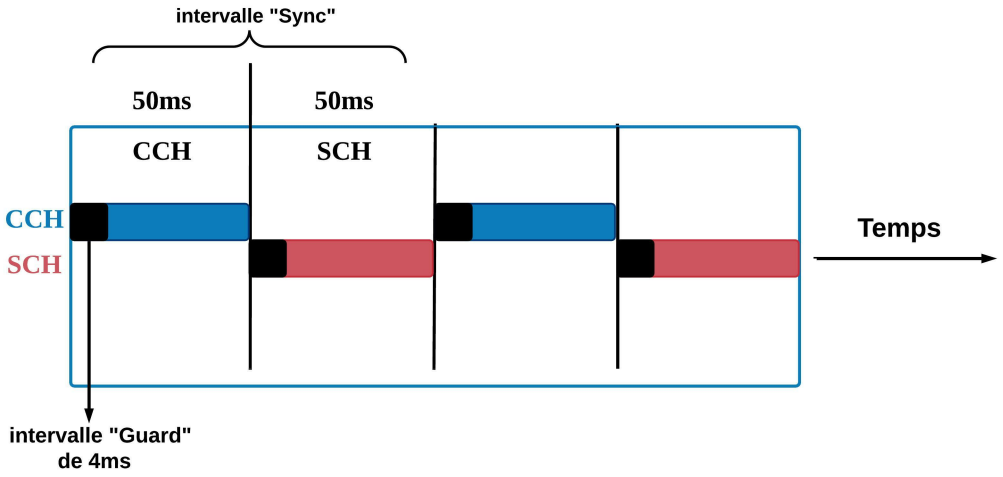

FIGURE I.7 – Intervalle SYNC

Ce système de compétition soulève des questions sur le protocole et notamment sa capacité à garantir de bonnes performances en matière de transmission de messages de sécurité critique [21]. Ces dernières sont très sensibles aux temps d'attente en raison de la nature très urgente de leurs paquets. D'un autre côté, la configuration statique des intervalles CCH et SCH n'offre pas la souplesse nécessaire pour s'adapter à la nature dynamique des VANETs. Par exemple, si la route ne présente pas de dangers majeurs à signaler, le fait que l'intervalle CCH soit fixé à 50 ms devient un handicap pour les performances du réseau. En effet, le nombre de paquets de sécurité à envoyer est limité et il y aura inévitablement un gaspillage de bande passante qui pourrait être exploité par des applications non critiques. D'autre part, dans les scénarios où un événement dangereux se produit sur la route, le nombre de paquets de sécurité critiques à envoyer augmente, et la limitation de l'intervalle CCH à 50 ms devient un handicap pour l'acheminement des informations urgentes.

I.8.1 La couche physique

La couche physique de la pile WAVE est détaillée par la IEEE dans [12]. Cette couche s'appuie sur un mécanisme de multiplexage par répartition orthogonale de la fréquence (Orthogonal Frequency Division Multiplexing, OFDM) pour prendre en charge différents débits de données qui sont déterminés par le taux de codage et le type de modulation. La largeur de bande de 75 MHz dans le spectre de 5,9 GHz est divisée en 7 canaux d'opération plus petits, chacun d'une largeur de bande de 10 MHz. Le canal 178 est utilisé comme canal de contrôle (CCH) tandis que les canaux 174, 176, 180 et 182 sont utilisés comme

canaux de service (SCH). Les canaux 184 et 172 sont mis de côté pour une utilisation future. Les dispositifs à couches physiques multiples fonctionnent généralement avec un CCH et au moins un SCH simultanément, tandis que les dispositifs à couche physique unique doivent basculer entre le CCH et le SCH. Dans ce cas et afin de s'adapter à cette capacité limitée, la synchronisation est nécessaire pour garantir que tous les dispositifs WAVE surveillent le CCH durant la même période de temps [22]. Dès qu'un groupe de dispositifs WAVE est synchronisé, ils peuvent simultanément surveiller et/ou utiliser le canal de contrôle. La norme WAVE actuelle [23] suit un mécanisme de synchronisation simple dans lequel tous les dispositifs WAVE alignent leur ressource radio sur une horloge globalement précise à chaque période [24].

Le spectre de fréquences disponible est divisé en sous canaux plus étroits (sous-porteuses). Le flux de données à haut débit est divisé en un certain nombre de flux de données à plus faible débit transmis simultanément sur un certain nombre de sous-porteuses, chaque sous-porteuse étant munie d'une bande étroite. Il y a en tout 52 sous-porteuses, 48 sont utilisées pour les données et 4 sont des sous-porteuses pilotes. La couche PHY supporte trois canaux de fréquence différents : 5 MHz, 10 MHz et 20 MHz. 802.11p utilise des canaux de 10 MHz alors que le WLAN utilise habituellement des canaux de 20 MHz. La fréquence de la sous-porteuse est déterminée en fonction de la largeur des canaux, c'est-à-dire que le nombre de sous-porteuses est fixe. Voir le tableau I.1 pour plus de détails.

Paramètre	20 MHz	10 MHz	5 MHz
Subcarrier Frequency Spacing	0.3125 MHz	0.15625 MHz	0.078125 MHz
OFDM	4 μs	8 μs	16 μs
Intervalle de garde	0.8 μs	1.6 μs	3.2 μs

TABLE I.1 – Distribution des fréquences au niveau de la couche Physique

I.8.2 La sous-couche LLC (Logical Link Control)

La couche liaison de données est partagée en deux sous-couches LLC et MAC. Cette séparation permet de surmonter les différences dans les techniques d'accès au canal. LLC fournit par l'intermédiaire du protocole d'accès au sous-réseau appelé SNAP la possibilité de différencier les différents protocoles de la couche réseau par le biais de ce qu'on appelle les protocoles EtherTypes. Dans la Figure I.8, les en-têtes LLC et SNAP sont présentées. L'en-tête LLC a une taille de 3 octets et l'en-tête SNAP de 5 octets. Lorsque SNAP est présent, l'en-tête LLC contient des valeurs par défaut indiquant cette présence. La partie ID

du protocole de l'en-tête SNAP contient également une valeur par défaut pour indiquer la présence d'un EtherType. L'EtherType est un identifiant unique à un protocole réseau qui peut être reçu par la IEEE après le dépôt d'une demande [25].

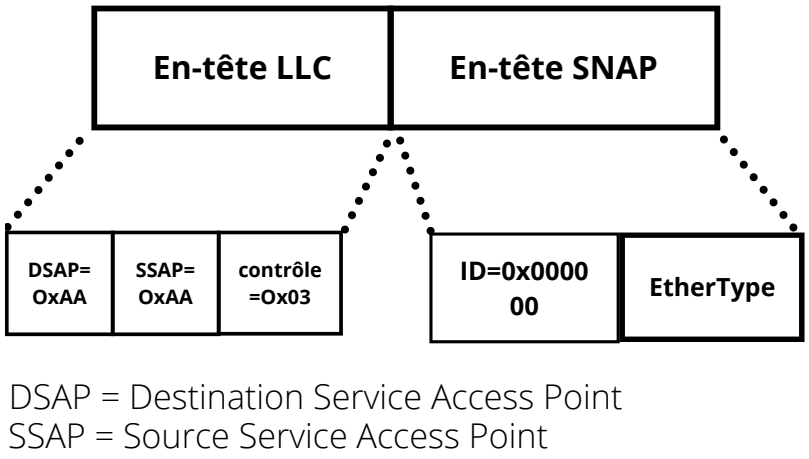

FIGURE I.8 – En-têtes LLC et SNAP

I.8.3 La sous-couche MAC

Le protocole MAC, qui réside dans la couche liaison de données, est responsable de la gestion de l'accès au canal pour le partage de données sous forme de paquets MAC (voir la figure I.9). Cette gestion s'effectue en programmant les transmissions en fonction du temps, de la fréquence, et en utilisant des codes uniques pour distinguer les différents utilisateurs. La recherche sur les protocoles MAC est vaste et remonte au milieu des années 70. Nous pouvons distinguer deux types principaux : Les protocoles MAC non-déterministes et déterministes, qui peuvent fournir un accès aléatoire ou pré-réservé au canal. En ce qui concerne les protocoles à accès non-déterministe, les stations se disputent l'accès au support et le délai d'accès au canal n'est pas prévisible. Contrairement au deuxième type, où l'accès est garanti et les délais d'attente sont bornés et peuvent donc être connus. Dans ce cas, toutes les stations seront

autorisées à émettre dans les limites d'un certain délai, quel que soit le nombre de stations, et l'accès au canal peut ainsi être rendu pseudo équitable (l'équité parfaite est difficile à obtenir). L'accès au canal est plus facilement garanti dans une topologie de réseau centralisée, où un contrôleur central, par exemple un point d'accès, peut répartir les ressources entre toutes les stations nécessitant un accès. Dans les réseaux distribués tels que les VANETs, le protocole MAC appliqué ne doit pas seulement être distribué, il doit aussi s'auto-organiser de telle sorte qu'il s'adapte en permanence à l'évolution du trafic de données et de la densité du réseau. Ainsi, dans la norme IEEE, le protocole MAC est basé sur CSMA dont le principe est expliqué dans ce qui suit.

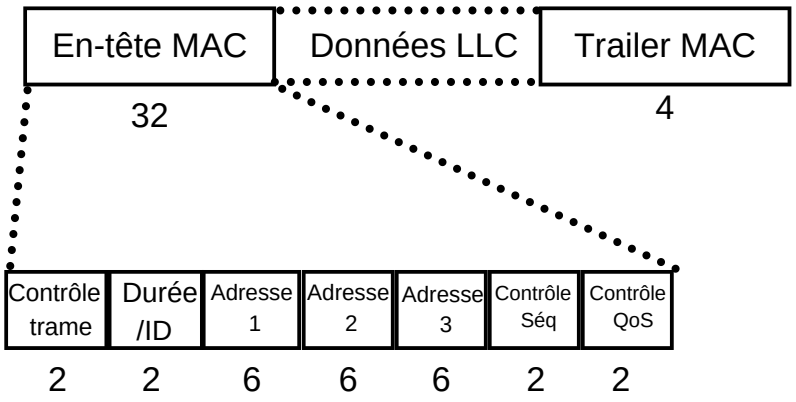

FIGURE I.9 – Format d'un paquet MAC

CSMA

Il existe deux méthodes possibles pour l'accès au canal dans le cadre de la norme 802.11 en utilisant CSMA : l'accès au canal distribué amélioré (EDCA) et la fonction de coordination distribuée (DCF). DCF est le mécanisme d'accès de base, sans prise en charge de la qualité de service. Il maintient une seule file d'attente pour tous les types de trafic de données. Pour les réseaux véhiculaires, EDCA a été choisie comme méthode MAC par défaut en raison des besoins particuliers de ce type de réseaux en termes de qualité de service. EDCA garantit la qualité de service par les moyens suivants : gérer le trafic de données au niveau de la couche MAC en plaçant les paquets dans l'une des quatre files d'attente différentes, chacune d'elles avec sa propre période d'écoute prédéterminée, son inter-frame space (AIFS) et ses réglages de fenêtres de contention.

Dans CSMA, chaque station initie une tentative de transmission en écoutant le canal pendant une période d'écoute prédéterminée. Si la détection est

négative, c'est-à-dire qu'il n'y a pas d'activité détectée sur le canal, la station transmet directement. Si le canal est occupé ou devient occupé pendant l'écoute, la station doit effectuer une procédure d'attente aléatoire (Backoff), c'est-à-dire qu'elle doit reporter son envoi suivant une durée de temps aléatoire.

Une fois qu'un canal occupé devient libre, toutes les stations doivent écouter sur ce dernier pendant la période prédéterminée avant que la décrémentation de la valeur de Backoff ne puisse reprendre. En mode Unicast, un ACK est envoyé en réponse à un paquet reçu avec succès. Si l'émetteur ne reçoit pas d'ACK la procédure peut être invoquée plusieurs fois pour le même paquet. L'échec de la transmission peut se produire si :

- **Le destinataire n'a pas reçu le paquet et n'a donc pas envoyé l'ACK**
- **Le destinataire n'a pas pu décoder le paquet et n'a donc pas envoyé l'ACK**
- **Le destinataire a pu décoder le paquet, a envoyé l'ACK mais ce dernier n'a pas été reçu par l'émetteur**
- **Le destinataire a pu décoder le paquet, a envoyé l'ACK, ce dernier a été reçu par l'émetteur mais n'a pas pu être décodé**

L'échec de la réception ou du décodage des paquets peut être dû à une perte de chemin (signal faible en raison d'une grande distance entre l'émetteur et le récepteur) ou de transmissions simultanées (par exemple dans le cas du problème du terminal caché). Pour chaque tentative de transmission d'un paquet spécifique en mode Unicast, la fenêtre de contention CW est augmentée jusqu'à ce qu'elle atteigne sa valeur maximale, c'est-à-dire en partant de la valeur minimale CWmin jusqu'à ce que la valeur CWmax soit atteinte. La couche physique détermine la valeur de ces paramètres, en l'occurrence : CWmin = 15 et CWmax = 1023. Dans la Figure I.10, l'augmentation de la fenêtre de contention est illustrée. Ceci implique que pour la première procédure de Backoff, il y a 16 valeurs à sélectionner [0..15], pour la deuxième tentative d'émission il y aura 32 valeurs à sélectionner [0..31] et ainsi de suite, jusqu'à ce que la taille maximale de la fenêtre de contention(CWmax) ait été atteinte (1023). Si la transmission du paquet est réussie, un ACK est envoyé en réponse, CW est remis à sa valeur initiale, qui est CWmin, pour préparer la prochaine transmission de paquets.

Dans EDCA, chaque station maintient des files d'attente avec des périodes d'écoute (AIFS), des paramètres et des tailles de fenêtres de contention différentes dans le but de garantir que les données prioritaires soient toujours transmises avant les données de basse priorité. Pour assurer la qualité de service, le trafic de données dans 802.11p a été segmenté en 4 types qui ont 4 niveaux de priorité différents. À chaque type de donnée est associé une AC (Access Category) et les priorités sont ordonnées par le choix du paramétrage de départ pour chaque AC (voir le tableau I.2), la priorité la plus faible est 0 et la priorité la plus élevée est 3.

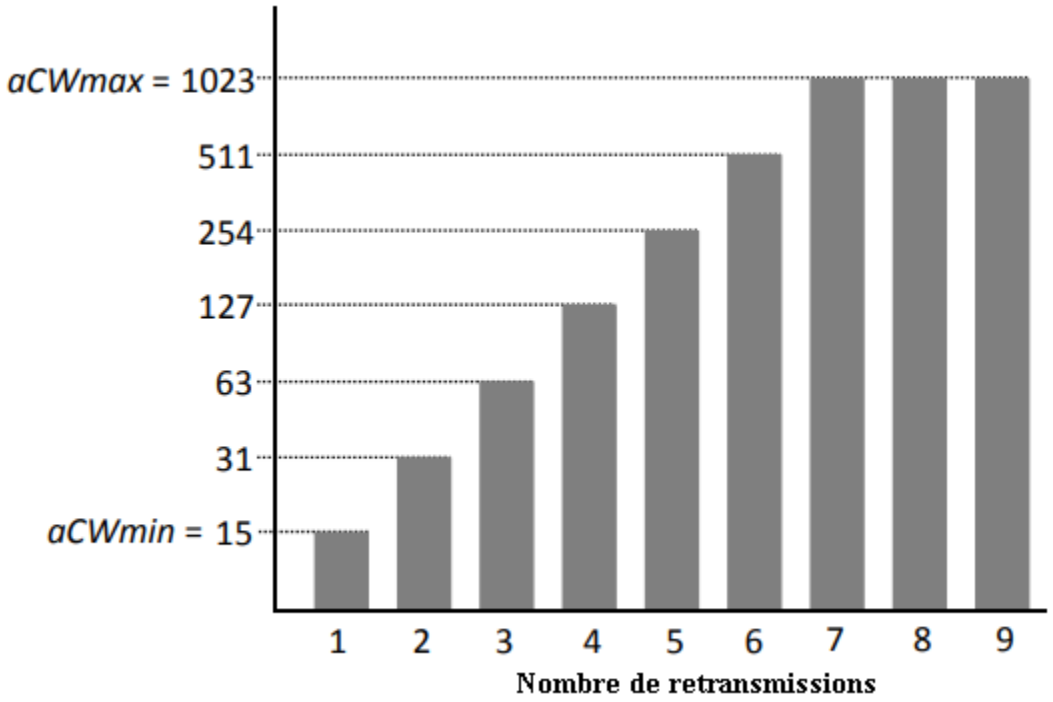

FIGURE I.10 – Augmentation des valeurs de CW selon le nombre de retransmissions

Catégorie	Abréviation dans 802.11p
Background	AC-BK
Best effort	AC-BE
Video	AC-VI
Voice	AC-VO

TABLE I.2 – Les catégories AC dans la norme 802.11p

Le tableau I.3 montre le paramétrage concernant chaque AC. Évidemment plus la priorité de l'AC est élevée, plus les paramètres de départ tels que les fenêtres de contention et AIFSN sont réduits dans le but d'avoir des temps d'attente minimaux et ainsi garantir l'accès au canal pour cette catégorie. À noter que AIFS qui est la période d'écoute d'un nœud avant de transmettre est calculée selon la formule suivante, cette formule utilise les constantes générées par la couche physique : $AIFS = AIFSNXaSlotTime + aSIFSTime$**.**

AC	CWmin	CWmax
AC-BK	15	1023
AC-BE	15	1023
AC-VI	7	15
AC-VO	3	7

TABLE I.3 – Valeurs des fenêtres de contention selon les catégories AC

Le tableau I.4 montre les valeurs des paramètres par défaut générés par la couche physique.

Paramètre	Valeur
aSlotTime	13 μs
aSIFSTime	32 μs
aCWmin	15
aCWmax	1023

TABLE I.4 – Valeurs de base des paramètres PHY

Sur la Figure I.11, la procédure d'accès au canal pour le mode Unicast et le mode Broadcast est décrite pour le mécanisme EDCA. Rappelons qu'en mode diffusion, il n'y a pas d'augmentation exponentielle de la taille de la fenêtre de contention Cw, car la procédure de Backoff ne peut être déclenchée qu'une seule fois et ce lors de la détection initiale. Toutefois, en mode Unicast la procédure de Backoff peut être invoquée à la fois lors de l'écoute initiale du canal et à chaque fois qu'un ACK n'est pas reçu par l'émetteur. Par conséquent, la taille de la fenêtre Cw continue d'augmenter de manière exponentielle à chaque nouvelle tentative de transmission. De plus, il y a un compteur associé à chaque paquet qui est incrémenté à chaque nouvelle tentative d'envoi, et lorsque ce compteur atteint sa valeur maximale pour un paquet particulier, le paquet est rejeté (détruit). Enfin, il y a une durée de vie attachée à chaque paquet entrant dans la couche MAC et lorsque ce compteur de durée de vie est dépassé, le paquet est également détruit. Ces rejets de paquets internes sont toujours signalés aux couches supérieures. Lorsque EDCA est utilisé dans une topologie Ad Hoc où tous les nœuds ont une connectivité complète, c'est-à-dire que tous les nœuds sont à portée, la procédure est prévisible. Cependant, dans un VANET, où les stations ne disposent pas d'une connectivité complète avec toutes les autres stations, la procédure EDCA n'est plus prévisible.

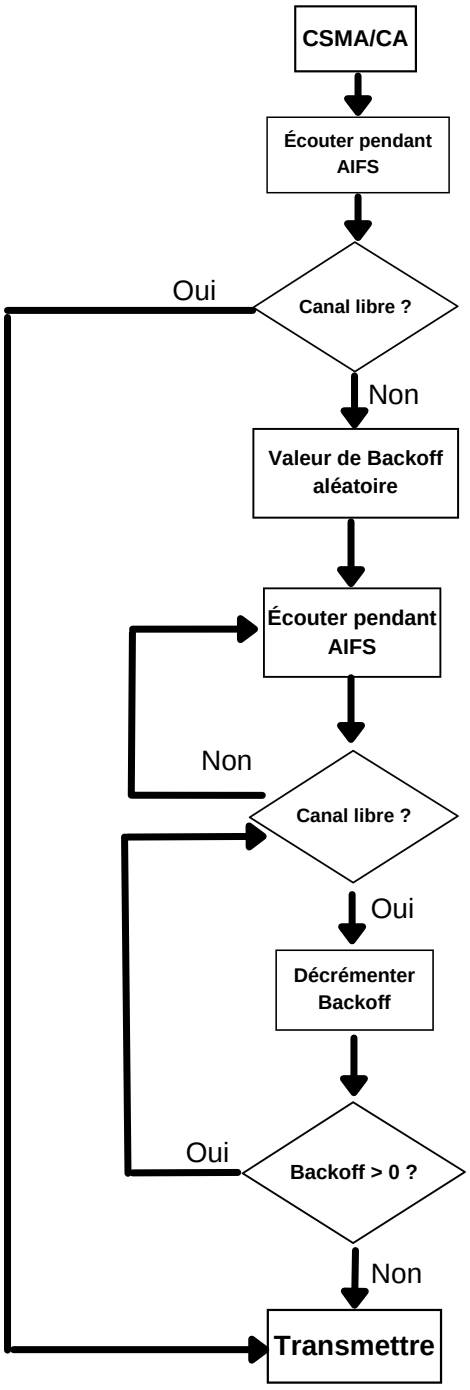

FIGURE I.11 – Fonctionnement du protocole CSMA

I.8.4 Les couches transport et réseau

Les couches réseau et transport partagent un protocole commun appelé WAVE Short Message Protocol(WSMP) [26]. Il a été développé pour minimiser la surcharge dans le réseau et ne supporte pas le routage, ce qui implique qu'il ne gère qu'un saut entre l'émetteur et le récepteur. L'Overhead minimal créé pour WSMP est de 5 octets et il dépasse rarement 20 octets par rapport à une transmission IPv6/UDP qui atteint des Overhead de 55 octets. Les messages de type "annonce de services WAVE" (Wave Service Announcement, WSA) se trouvent dans cette partie de la pile de protocoles. Il s'agit d'un cadre de gestion qui est transmis pendant l'intervalle CCH et qui contient des informations sur les services offerts sur les différents SCHs. Les services peuvent aller de la publicité aux informations utiles pour le conducteur. Il est prévu que ce soit les unités de bord de route (RSU) qui proposent des services (WSA), bien que les stations ITS mobiles (véhicules) ne soient pas interdites d'en offrir également.

L'opération de routage qui consiste à trouver comment acheminer des paquets de la source à la destination peut se faire de deux façons différentes. Dans le routage de type source, toutes les informations sur la façon d'arriver de la source à la destination sont d'abord recueillies au niveau du nœud émetteur, qui les place dans les paquets qu'il va envoyer vers la destination. Le rôle des nœuds intermédiaires est simplement de lire ces informations de routage et d'agir en conséquence. Dans le routage saut-par-saut, la source n'est pas censée avoir toutes les informations sur comment se rendre vers la destination. Il suffit que la source sache seulement comment atteindre le prochain saut, ou par exemple un réseau intermédiaire vers lequel il existe un lien de communication, et ainsi de suite jusqu'à ce que la destination soit atteinte. Les nœuds intermédiaires ont donc plus de responsabilité, car ils n'ont que l'adresse de la destination à leur disposition plutôt qu'une spécification complète de l'itinéraire par la source avec laquelle déduire le meilleur saut suivant pour chaque paquet [27].

Dans les VANETs, plusieurs protocoles de routage ont été développés. Dans ce qui suit, nous présentons une classification de ces protocoles. Un état de l'art détaillé de ces protocoles est le sujet du troisième chapitre.

I.9 Les types de protocoles de routage

Les protocoles de routage proposés dans les VANETs peuvent être de deux types, basés sur la position géographique ou basés sur la topologie. Cette classification est illustrée par la figure I.12 et expliquée dans ce qui suit.

I.9.1 Basés sur la position géographique

Ces protocoles utilisent les informations de positionnement des nœuds pour le routage des paquets, c'est-à-dire que l'adresse du destinataire est déterminée par sa position géographique plutôt que par une adresse codée prédéfinie. Les nœuds utilisent pour cela la technologie GPS pour avoir l'équivalent d'une table d'adresses géographiques correspondant à chaque membre du réseau. Lorsqu'un nœud souhaite envoyer un paquet, il inclut généralement dans l'en-tête de ce dernier les informations de position du destinataire, afin que tous les nœuds intermédiaires (ceux qui se trouvent sur la route du paquet) puissent connaître le prochain saut à effectuer. L'avantage avec cette technique est que les nœuds ne sont pas obligés de connaître les informations sur la topologie du réseau, et la phase de découverte de route n'est également pas nécessaire. De ce fait, ce type de protocoles est particulièrement adapté aux réseaux véhiculaires, à cause de la forte mobilité de leurs nœuds et de leur topologie très dynamique [7].

Les protocoles tolérants aux délais

Comme leur nom l'indique, ces protocoles agissent sur des réseaux où il y a un fort risque de longs délais, de fréquentes pertes de connexions et une bande passante limitée. Les nœuds dans ce type de réseaux ont une portée d'envoi assez faible, ils sont toutefois chargés de relayer les paquets qu'ils reçoivent, c'est de là que viennent les délais imprévisibles. Puisqu'il n'y a aucune garantie sur la stabilité de la connexion durant l'acheminement d'un paquet, les nœuds intermédiaires peuvent stocker ce dernier pour éviter qu'il soit définitivement perdu. Quelques protocoles proposés : MOV,VADD [7].

Les protocoles non tolérants aux délais

C'est un sous-type des protocoles à position géographique. Dans ce cas, on suppose que le problème de déconnexions entre les nœuds est inexistant, c'est-à-dire qu'un paquet trouvera toujours des nœuds intermédiaires à portée afin de le relayer. Les protocoles non tolérants aux délais sont donc plus adaptés aux réseaux à forte densité. Un nœud ayant reçu un paquet qui ne lui est pas destiné se contente de le transmettre au nœud voisin le plus proche géographiquement, ce qui peut poser problème lorsque justement ce nœud est isolé et ne trouve aucun voisin. Plusieurs protocoles tentent d'optimiser ceci et sont présentés dans l'état de l'art. Quelques protocoles proposés : GPCR,SPSR [7].

Quelques limitations des protocoles à position géographique

Bien que le fait que ces protocoles permettent de se passer d'une table de routage car ils ne se basent pas sur des adresses réseau, ils présentent néanmoins certaines contraintes et limitations qui les rendent parfois difficilement applicables. L'une des plus évidente est la dépendance totale qu'ont ces protocoles par rapport à la précision des informations de position, car leurs performances peuvent baisser considérablement dans le cas où les informations GPS récoltées sont incorrectes ou non précises. Comme indiqué précédemment, l'un des autres obstacles que peuvent rencontrer ces protocoles est l'indisponibilité des nœuds proches du nœud destinataire, ce qui rend la transmission impossible et peut donc engendrer la perte du paquet.

I.9.2 Basés sur la topologie

Largement utilisés dans les réseaux mobiles, ces protocoles se distinguent des protocoles à position géographique par le fait qu'ils tiennent à jour ce qu'on appelle des tables de routage. Elles servent à stocker des informations sur les adresses des différents nœuds du réseau, afin que l'acheminement des paquets puisse se faire en partant d'un nœud source à un nœud destinataire. Nous pouvons distinguer trois sous-types majeurs pour ces protocoles [7].

Les protocoles pro-actifs

Dans ces protocoles, les nœuds se servent des tables de routage pour déterminer les chemins que doivent suivre les paquets. Chaque entrée dans ces tables correspond en effet au prochain saut pour se rapprocher de la destination d'un paquet. Cette table doit par conséquent être mise à jour et communiquée périodiquement à l'ensemble des nœuds, ceci se fait par diffusion (Broadcast) et a pour but de décrire avec précision la topologie actuelle du réseau. L'inconvénient avec cette technique est qu'elle peut conduire à des surcoûts (Overhead), mais elle offre l'avantage de la disponibilité des chemins à tout moment, c'est-à-dire que les routes seront toujours connues en cas de besoin. L'algorithme du plus court chemin est très souvent utilisé par ce type de protocoles afin de déterminer la meilleure route à suivre pour atteindre un nœud destinataire. Quelques protocoles proposés : OLSR,FSR [7].

Les protocoles réactifs

En opposition aux pro-actifs, les protocoles réactifs ne génèrent les routes à suivre que lorsqu'un nœud en a besoin, ce qui permet de réduire considéra-

blement le surcoût. Ce même nœud déclenche la procédure de découverte de chemin en diffusant une demande de route à travers tout le réseau s'il trouve que son destinataire n'est actuellement pas atteignable (aucun chemin n'est disponible). Cette demande, lorsqu'elle est réceptionnée par le nœud possédant la route demandée, obtiendra une réponse destinée au demandeur, sous forme d'Unicast. Cela est utile lorsqu'on souhaite appliquer ce type de protocoles sur les réseaux véhiculaires, car la topologie de ces derniers est fortement dynamique et change constamment. Quelques protocoles proposés : AODV, DSR [7].

Les protocoles basés sur la topologie hybrides

Comme leur nom l'indique, ces protocoles tentent de profiter des avantages des deux types précédemment présentés, et de contourner leurs limitations. Ils ont donc pour but de réduire les temps de calcul lors de la recherche de route utilisée dans les protocoles réactifs, tout en réduisant le surcoût généré par l'utilisation des tables de routage permanentes dans les protocoles pro-actifs. Afin de faire fonctionner les deux méthodes, les protocoles hybrides proposent de diviser le réseau en deux parties, c'est-à-dire que chaque nœud gère deux zones distinctes : une zone dite proche qui regroupe les nœuds à proximité et une zone plus éloignée. Il utilise alors la méthode pro-active (avec table de routage) pour les transmissions au sein de la zone proche, et la méthode réactive (avec découverte du chemin) pour les transmissions en dehors de cette zone [7].

Quelques limitations des protocoles basés sur la topologie

Bien que ce type de protocoles permette d'établir à l'avance les liens de communications entre les nœuds, d'éviter la phase de découverte de route et ainsi de réduire les délais d'initialisation des transmissions, ils présentent néanmoins quelques inconvénients. Le principal est le sur-coût dû à une charge plus importante comparée aux protocoles géographiques. Ceci est à cause de la nécessité de maintenir des tables de routage, d'avoir une vision globale du réseau et donc d'échanger des paquets de contrôle supplémentaires entre les nœuds.

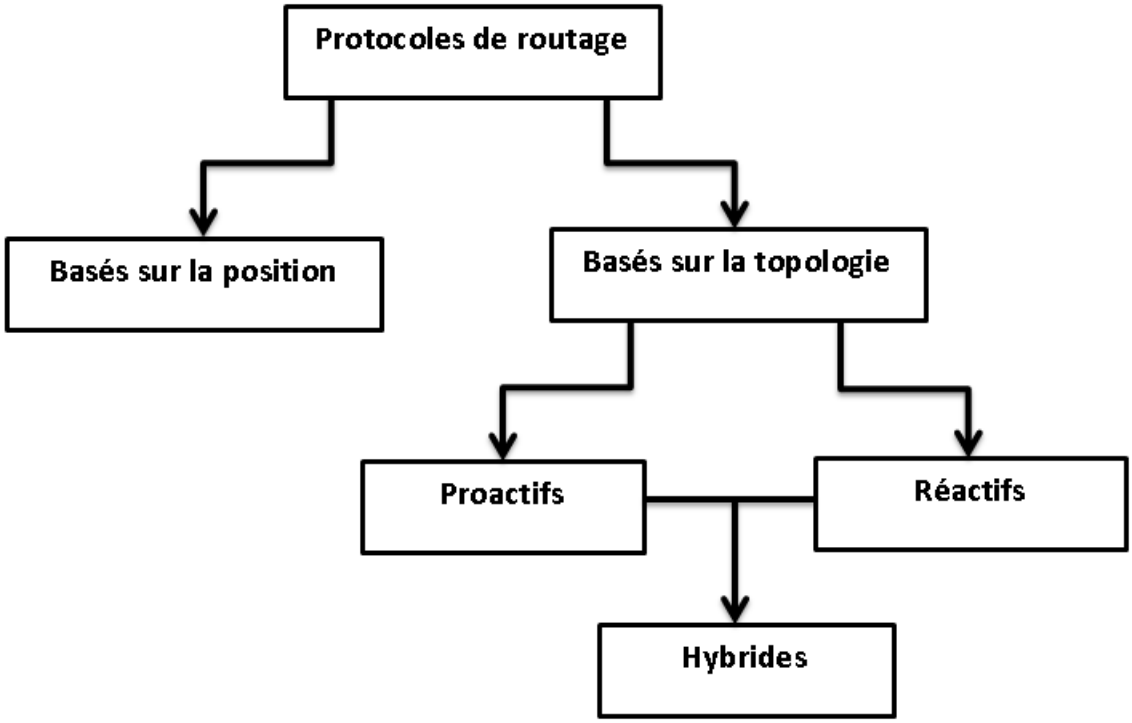

FIGURE I.12 – Types de protocoles de routage

I.10 Conclusion

Dans ce premier chapitre, nous avons défini les réseaux véhiculaires, présenté leurs principales caractéristiques ainsi que leur principe de fonctionnement. Nous avons vu que ce type de réseaux, de par la grande mobilité de ses nœuds, présente plusieurs contraintes de conception lorsqu'il s'agit de la création de protocoles.

Nous présenterons dans le chapitre II un état de l'art des différents protocoles d'accès au canal proposés pour les VANETs.

Chapitre II

État de l'art des protocoles d'accès au canal pour les VANETs

II.1 Introduction

Dans ce deuxième chapitre, nous présentons un état de l'art sur les protocoles d'accès au canal proposés dans la littérature. Ces protocoles sont classifiés selon la méthode utilisée pour l'attribution de cet accès, à savoir : les protocoles déterministes sans compétition, les protocoles non déterministes avec compétition et pour finir les protocoles hybrides. Une brève critique de ces travaux avec leurs principaux avantages et inconvénients est présentée à la fin de ce chapitre.

II.2 Les protocoles MAC déterministes

Les protocoles MAC déterministes sont les protocoles qui se basent essentiellement sur TDMA. Le principe de base est d'allouer des slots de temps dans une trame pour les nœuds souhaitant transmettre des paquets. Ainsi, chaque nœud commence sa transmission dès que son tour sur la trame arrive. Plusieurs protocoles MAC basés sur TDMA sont proposés pour les VANETs. Nous les classons en deux sous-types, les protocoles fondateurs et les protocoles récents, et nous présentons quelques protocoles de chaque sous-type.

II.2.1 Les protocoles fondateurs

Dans [28], F.Borgonovo et al. ont proposé un nouveau protocole MAC destiné aux VANETs nommé RR-ALOHA, et qui est une poursuite du travail fait sur R-ALOHA. Ce protocole vise à réaliser le mécanisme TDMA d'une manière décentralisée, chaque nœud du réseau doit ainsi sélectionner un canal de

base sur lequel il souhaite émettre, qui est en fait un slot numéroté qui se répète périodiquement dans chaque trame. Pour pallier au problème du terminal caché, RR-ALOHA permet aux nœuds d'avoir une vision globale des transmissions faites dans un rayon de deux voisins. Pour cela, on impose à tout véhicule émetteur sur son canal d'inclure ses informations de trame "FI" (Frame Information) qui contiennent le statut des N derniers slots sur la trame précédente. Chaque trame est divisée en N slots numérotés et pendant chaque durée de trame, les véhicules écoutent les transmissions de leurs voisins et mettent à jour leur FI après chaque réservation de slot réussie.

Dans [29], un protocole d'accès au canal basé sur TDMA est proposé. ATSA (Adaptative TDMA Slot Assignment) est destiné aux réseaux ayant des populations non équilibrées, c'est-à-dire lorsque le nombre de véhicules circulant sur deux voies opposées varie. Pour cela, le protocole divise les trames de temps en deux intervalles gauche et droite, quand un véhicule souhaite transmettre, il requiert un slot de temps disponible pour son côté de la route. La gestion de ces slots de temps se fait suivant un mécanisme d'arbre binaire, c'est-à-dire que les informations concernant l'allocation des slots sont stockées dans un arbre comptant n niveaux suivant la population du réseau. Les branches se trouvant sur le côté gauche de l'arbre représentent ainsi le côté gauche du slot, et pareillement pour le côté droit.

Dans [30], une nouvelle méthode d'accès au canal visant à résoudre le problème du terminal caché est présentée. Les nœuds se trouvant à portée sont ici groupés en Clusters sans pour autant élire de CH (Cluster Head), et le temps sur le canal est divisé en trames périodiques. Chaque nœud du réseau est garanti d'accéder au canal au moins une fois par trame, et se voit ainsi allouer un slot au sein de cette trame qui est appelé par les auteurs Basic Channel (BCH). Chaque nœud doit aussi diffuser périodiquement à ses voisins à deux sauts les informations concernant ses réservations de slots pour pallier au problème du terminal caché.

Dans [31], Bi et al. ont proposé un protocole utilisant des anneaux et jetons sur plusieurs canaux de communication (multi-canal) appelé MCTRP (Multi Channel Token Ring Protocol). Le but de ce protocole est de concevoir une méthode MAC déterministe qui puisse gérer de manière autonome l'organisation des nœuds du réseau en anneaux afin de maximiser la bande passante et réduire les temps de latence. Pour la communication, chaque nœud est équipé de deux radios : La première est constamment connectée au canal WAVE 178 et dédiée aux transmissions inter-anneaux. La deuxième radio est quant à elle connectée à un des six canaux WAVE restants et est dédiée aux communications au sein de chaque anneau quel que soit le type de message transmit (message de sécurité, de coordination ou de données).

STDMA (Self-organized Time-Division Multiple Access) [32] est une méthode MAC basée sur le très répandu TDMA dont le but est de garantir de bons délais de transmission pour ce qui est des messages de sécurité critiques.

Elle propose des communications présentant peu de risques de collisions. Un nombre défini de slots forment une trame et le service GPS est utilisé afin de synchroniser les slots pour les nœuds du réseau. Chaque nœud choisit ainsi un ensemble de slots auxquels il pourra potentiellement accéder. La méthode suit ensuite le fonctionnement standard de TDMA. Une fois que les slots ont été affectés, chaque nœud transmet ses données ainsi qu'un message d'urgence (optionnel) durant le slot qui lui est affecté.

Gunter et al. proposent dans [33] un nouveau protocole d'accès au canal nommé CBMAC (Cluster Based Medium Access Control). Il vise notamment à résoudre le problème du nœud caché en octroyant aux chefs de Clusters la responsabilité de gérer la bande passante allouée aux nœuds présents dans leurs Clusters respectifs. Le protocole utilise des trames TDMA structurées en slots, le premier slot est réservé aux chefs de Clusters qui doivent transmettre des avertissements périodiques pour indiquer le début des trames. Le deuxième slot est aussi réservé pour les chefs de Clusters, ils y transmettent les informations relatives à la réservation des autres slots, c'est-à-dire quels sont ceux qui sont déjà réservés et quels nœuds les ont réservé. Les prochains slots sont alloués aux nœuds les ayant réservés afin de transmettre leurs données, et pour finir, les derniers slots représentent la phase de réservation pour la prochaine trame TDMA. A noter que la barrière entre la phase d'envoi de données et la phase de réservation est flexible.

Dans [34], un schéma de réservation coopératif de l'intervalle SCH est proposé, il vise à utiliser l'intervalle CCH afin d'envoyer des informations sur l'occupation des canaux de service et ce en utilisant des trames WSA. Pour ce faire, deux méthodes sont proposées dans CRaSCH : Proactive Gossiping et Reactive Gossiping.

Dans [35], les auteurs proposent une méthode appelée W-UIM (WBSS User Initiation Mode) visant à minimiser au maximum les collisions de paquets. La méthode se base sur un système de sollicitation et utilise ce que les auteurs ont appelé "Polling Scheme" qui est une méthode de réservation par vote. Les utilisateurs peuvent solliciter des trames de données afin de les recevoir, et ce en les demandant à un "WBSS Provider" (fournisseur) par scrutin (Poll).

II.2.2 Quelques protocoles récents

Dans [36], un système coordonné, adaptatif et fiable de contrôle d'accès multimédia pour VANETs (VCAR-MAC) est présenté. Un nouveau système d'accès multiple par division temporelle (TDMA) qui tient compte des conditions environnementales permet d'identifier chaque véhicule rapidement de sorte qu'un slot sur l'intervalle CCH puisse être alloué efficacement pour une transmission fiable des messages de sécurité. Pour l'intervalle SCH, les auteurs utilisent une méthode qui adapte de manière dynamique la réservation des slots afin d'utiliser pleinement la bande passante du canal. La taille initiale des

fenêtres de contention est optimisée pour maximiser le nombre de réservations réussies sur SCH, maximisant ainsi le débit des messages de service.

Dans [37], un protocole MAC déterministe, nommé I-MAC, est proposé. Il vise à minimiser les collisions dues aux hautes densités parfois présentes dans les réseaux véhiculaires. I-MAC exploite la méthode DIFS pour s'assurer que les nœuds ne choisissent pas de transmettre au même moment juste après avoir trouvé le canal libre, les auteurs ont ainsi augmenté cette durée d'attente qui précède la transmission car plus la population augmente, plus la chance que deux véhicules (ou plus) choisissent une durée d'attente similaire et causent ainsi une collision.

Dans [38], un protocole MAC distribué basé sur TDMA avec atténuation des collisions causées par la mobilité (MCCM-MAC, Mobility-Caused Collision Mitigation MAC) est présenté. Le protocole utilise un nouveau mécanisme pour détecter les collisions dues aux fusions de routes et les atténuer en évitant les collisions d'accès résultantes. Chaque véhicule vérifie le statut de ses slots à chaque réception. Si le véhicule détecte un slot perdu à un moment donné, il doit en acquérir un nouveau grâce à un mécanisme de suggestion de slots développé par les auteurs.

Dans [39], une approche axée sur les conditions du trafic routier (TA-TDMA), qui améliore le protocole VeMAC pour répondre aux exigences en temps réel est présentée. Le protocole repose sur la prévision du trafic dans un futur proche pour affecter les ressources appropriées à chaque zone du réseau. À chaque voie est assigné un ensemble différent de slots réservables, et pour réserver un slot, les véhicules envoient une demande d'allocation à leurs CHs respectifs. Le CH maintient un tableau d'informations sur les slots assignés à sa zone (direction et segment), qui contient leurs états. Une fois qu'une demande est reçue, il transmet une liste des créneaux disponibles au véhicule.

Dans [40], les auteurs proposent une amélioration des diffusions de messages périodique de type Beacon, étant donné leur grande importance pour l'amélioration de la sécurité routière et la prévention des situations dangereuses dans les VANETs. Dans NC-MAC (Network Coding-based Medium Access Control), le temps sur le canal est divisé en créneaux de même durée, et la bande passante disponible est divisée en plusieurs sous-canaux. Chaque véhicule envoie son propre message original et une combinaison linéaire indépendante de son propre message original (Beacon) et des Beacons reçus d'autres véhicules qui doivent être retransmis sur la première et la deuxième possibilité de transmission respectivement.

Dans [41], une méthode MAC visant à réguler la transmission des messages « Beacon » périodiques durant l'intervalle CCH est présentée. Son but est d'augmenter la fiabilité et l'évolutivité au sein de la norme 802.11p. TDMA est utilisé pour l'accès au canal et les auteurs proposent deux principes de fonctionnement : « Cooperative Beaconing » et « Proactive Slot Reservation ». Les nœuds ayant réservé un slot deviennent «en ligne» et sont responsables d'in-

former les nœuds environnants du statut des autres slots (vides ou réservés).

Dans [42], les auteurs proposent une amélioration de la méthode TDMA nommée NA-MAC (Neighbor Association-based MAC). Dans cette méthode, le temps sur le canal est divisé en unités plus petites appelées slots, qui sont eux-mêmes divisés en 3 segments distincts ayant 3 tâches : détection de canaux, acquisition de créneaux et transmission de données. Au cours de la première phase, un nœud souhaitant transmettre écoute le canal à la recherche de slots libres. Une fois trouvé, la phase d'acquisition de slots est déclenchée par l'échange de paquets de contrôle nommés RTB (Request-To-Broadcast) et CTB (Clear-To-Broadcast). Puis une fois que le slot a été acquis par le nœud, la phase de transmission peut commencer.

Dans [43], les auteurs proposent un mécanisme d'allocation des slots basé sur TDMA. Ce mécanisme utilise une fonction appelée "Fuzzy Slot Priority (FSP) Function" pour l'attribution des slots aux nœuds d'un même cluster. Cette fonction est calculée en utilisant des paramètres tels que la longueur de la file d'attente de transmission des nœuds et l'estimation des délais d'envoi de leurs paquets pour obtenir une attribution de slots optimisée.

Dans [44], Hassan Aboubakr Omar et al. ont présenté un protocole MAC multicanaux déterministe nommé VeMAC. Il vise à garantir des liaisons point à point et multipoint efficaces, avec un faible taux de collisions. Chaque nœud est équipé de deux récepteurs radio, le premier est constamment connecté au canal de contrôle (c0), tandis que le second peut être connecté à chacun des m canaux de service (c1..cm) et la synchronisation se base sur le signal GPS. Les paquets transmis sur le canal de contrôle sont constitués de quatre champs : L'en-tête, l'annonce de service (AnS), l'acceptation de service (AcS) et le champ "High Priority Short Applications". Lors de sa transmission sur c0, chaque message doit contenir dans son en-tète les slots réservés par tous les voisins à un saut du nœud émetteur afin d'éviter le problème du terminal caché, cela permet au récepteur de connaître tous les slots de temps utilisés par les voisins et ainsi déterminer quels sont ceux qu'il pourra réserver (ceux qui sont libres). La désignation de slots sur les canaux de service est effectuée par le fournisseur. On appelle fournisseur tout nœud offrant un service sur un canal de service donné dans le champ AnS sur c0, et on appelle utilisateur tout nœud ayant reçu cette offre et ayant décidé de s'en servir (utiliser le service), c'est donc la responsabilité du fournisseur d'allouer les slots à tous les utilisateurs.

Dans [45], les auteurs présentent un protocole MAC visant à offrir des transmissions de messages de sécurité critiques sans aucune compétition. Pour ce faire, les nœuds envoient des requêtes de réservation pendant une phase spécifique de l'intervalle SCH. Les RSUs s'occupent ensuite de programmer les transmissions lors des futurs intervalles CCH suivant ces réservations, selon la disponibilité de la bande passante.

Dans [46], un protocole MAC coopératif basé sur la méthode TDMA est présenté. Dans CAHMAC (Cooperative AdHoc MAC), lorsqu'un échec de trans-

mission se produit, certains nœuds voisins du nœud ayant des difficultés à transmettre appelés HNs (Helper Nodes) servent de relais pour retransmettre les paquets en question. Ceci permet d'éviter la perte de ces paquets et d'améliorer la bande passante pour les applications de service non-critiques.

Dans [47], un protocole MAC déterministe est proposé. Le réseau est ici divisé en Clusters gérés par des CHs. Ces CHs sont responsables de la réservation de slots pour tous les nœuds de leurs Clusters respectifs. Les auteurs proposent aussi un algorithme d'élection de CH peu gourmand en ressources, afin de réduire la charge sur le réseau. Les messages de type Unicast dont les nœuds source et destinataire se trouvent dans des Clusters différents sont aussi gérés par les CHs.

Dans [48], un protocole MAC à division de temps est présenté. Dans CBT (Cluster-Based Tdma), le réseau est divisé en Clusters et les véhicules connaissent leur position et celle de leurs voisins grâce au service GPS. Les communications inter et intra-Cluster sont gérées par des nœuds spécifiques appelés VC (VANET Coordinator). Le premier slot de chaque trame est réservé à l'allocation des slots respectifs pour chaque nœud ayant des données à transmettre (cette allocation est gérée par les VC), et le reste des slots est utilisé pour le transfert de ces données.

Dans [49] et [50], les auteurs proposent un protocole MAC basé sur TDMA et ayant pour but d'exploiter les unités de bord de route pour optimiser la bande passante. Chaque RSU récolte des informations concernant l'état du canal de transmission ainsi que la vitesse de déplacement des véhicules à sa portée. La première information est utilisée pour fournir la meilleure réservation de slots possible et ainsi augmenter la bande passante du réseau. La seconde information est quant à elle utilisée pour garantir que tous les nœuds aient un accès équitable au canal quelles que soient leurs vitesses.

Dans [51], les unités de bord de route sont utilisées pour gérer l'allocation de slots basé sur TDMA. Un sous-réseau est formé au niveau de chaque RSU dans le but d'avoir une gestion personnalisée des slots qui s'adapte à la densité du sous-réseau en question. Les RSUs ont donc pour rôle d'éviter d'avoir trop de slots inutilisés dans les cas de faible densité, ou au contraire de ne pas avoir assez de slots disponibles dans les cas de forte densité.

Dans [52], Zou et al. présentent un nouveau protocole basé sur la division de temps nommé CFR (Collision Free Reservation). Comme son nom l'indique, le but de ce protocole est d'avoir des transmissions sans collisions en réglant le problème de la fusion de voies de circulation. La réservation des slots se fait en se basant sur le protocole VeMAC, en prenant en compte la population, la direction et la vitesse des véhicules. Comme pour ATSA, les slots sont divisés en un côté gauche et un côté droit, reflétant ainsi les deux voies de circulation. Cependant dans CFR, chaque côté du slot est divisé en trois segments pour caractériser les différentes vitesses des véhicules, forte vitesse, moyenne vitesse et basse vitesse.

II.3 Les protocoles MAC non-déterministes

Dans les protocoles MAC non-déterministes, l'accès au canal est basé sur un système de compétition. Il n'y a pas de garanties sur les durées exactes que les nœuds doivent attendre avant de pouvoir accéder au canal, car cet accès n'est pas réservé à l'avance contrairement à ce qui se fait dans la méthode TDMA. Nous classons ici quelques protocoles non-déterministes proposés dans la littérature en deux sous-types, les protocoles fondateurs et les protocoles récents.

II.3.1 Les protocoles fondateurs

Dans [53], les auteurs proposent un nouveau protocole d'accès au canal pour la pile WAVE nommé V-MESH (Vehicular MESH). Le protocole vise à optimiser la réservation de ressources au sein de l'intervalle de service SCH. Ceci se fait grâce à la division de l'intervalle CCH en deux segments distincts. Le premier appelé BP (Beacon Period) est utilisé par les nœuds pour transmettre des informations relatives à leurs futures intentions. LE deuxième, appelé SP (Safety Period) sert quant à lui à l'échange de paquets de sécurité critiques.

Un protocole MAC basé sur le Clustering est proposé dans [54], les Cluster Heads effectuent des diffusions contenant ce que les auteurs appellent des listes d'utilisation de canaux. Ces listes permettent aux nœuds souhaitant émettre de connaître la disponibilité des canaux de communication. Un nœud source doit aussi envoyer une requête de canal à son Cluster Head. Ce dernier peut ensuite soit lui indiquer que le canal en question est libre et que les données peuvent être acheminées, soit que le canal est occupé. Dans ce cas, le nœud source effectuera une retransmission de la requête de canal. Cette méthode permet de réduire les délais de bout en bout et d'augmenter le pourcentage de paquets arrivés avec succès.

Dans [55], les auteurs proposent un nouveau protocole d'accès au canal avec Clustering destiné aux trois types de données circulant dans les VANETs (sécurité critique, données de circulation périodiques et info-divertissement). Comme dans la plupart des protocoles utilisant le Clustering, les Cluster Heads ont pour responsabilité de gérer la diffusion des paquets de sécurité critique au sein de leurs Clusters respectifs, ainsi que les communication inter-clusters. La création des Clusters se fait suivant la direction dans laquelle circulent les véhicules. Les auteurs proposent de regrouper les véhicules se dirigeant dans la même direction et de leur assigner un Cluster Head. Le Cluster a ainsi plus de chance de rester groupé et survivre dans le temps.

Dans [56], les auteurs proposent un protocole MAC conçu pour éviter le gaspillage de la bande passante. Ceci peut se produire lorsque plusieurs canaux de transmission dédiés aux applications de service restent inoccupés alors que

des messages de sécurité critiques sont en attente de diffusion. Pour ce faire, le protocole propose une utilisation simultanée des deux types de canaux et les véhicules sont constamment connectés à des unités de bord de route afin d'avoir en temps réel l'état de ces canaux. Le temps sur le réseau est divisé en intervalles de synchronisation. Chaque nœud souhaitant émettre choisit un des sept canaux disponibles sans se soucier du type de données ou de la nature du canal en question. Pour les paquets de première priorité, le véhicule source envoi un message d'urgence à la RSU la plus proche. Cette dernière diffuse sur tous les canaux (service et sécurité) le message pour atteindre les autres nœuds du réseau.

Dans [57], VMMAC (Vanet Multi-channel MAC) est proposé. Ce protocole exploite les antennes directionnelles afin d'élargir la zone de transmission des véhicules tout en minimisant le nombre de sauts nécessaire pour aller du nœud source au nœud destinataire. Comme la plupart des méthodes basées sur des antennes, des rayons de transmission sont utilisés sur les sept canaux (un par canal), et l'état de ces rayons est partagé entre les véhicules du réseau afin de former des tables de rayons. Un rayon peut soit être occupé soit libre, un nœud souhaitant émettre commence par envoyer une requête de canal dans un rayon spécifique, cette requête contient des identifiants uniques pour la source et la destination ainsi que la table de rayons que le nœud a à sa disposition. Pour les transmissions SCH, la traditionnelle méthode du Handshake en quatre étapes est utilisée. Tandis que pour CCH, un simple acquittement après l'envoi direct des données suffit à cause du caractère urgent des messages envoyés sur CCH.

Dans [58], les auteurs proposent D-MAC (Directionnal MAC), qui est un protocole d'accès au canal se basant sur des antennes directionnelles. Pour fonctionner, D-MAC requiert que tous les nœuds connaissent avec exactitude leur position géographique ainsi que celle de leurs voisins, ce qui peut être fait en utilisant la technologie GPS (Global Positioning System). Un nœud voulant transmettre commence par exécuter une poignée de main (Handshake), suivant le mécanisme RTS/CTS (Request To Send/Clear To Send). Le fait d'utiliser ces antennes directionnelles peut considérablement réduire le risque de collisions.

Dans [59], Y.Wang et al. proposent deux algorithmes visant à améliorer le débit pour le protocole MAC de la norme IEEE 802.11p. En effet, ce dernier peut subir des baisses importantes de performances suivant les changements du nombre de véhicules émetteurs sur le réseau. Ceci est dû au choix statique des paramètres MAC du protocole 1609.4. Le premier algorithme, appelé Centralized Enhancement Algorithme(CEA) a pour but de calculer la fenêtre de contention optimale adaptée au nombre de véhicules transmettant sur le réseau. Le deuxième algorithme nommé Distributed Enhancement Algorithme(DEA) est utilisé pour obtenir une estimation du nombre de nœuds émettant simultanément des messages et adapter la taille de la fenêtre.

Dans [60], Y.Wang et al. proposent une méthode d'accès au canal modifiée qui donne plus d'importance à l'intervalle SCH, dans le sens où cette dernière

est augmentée mais ceci au détriment de l'intervalle CCH. Un nœud reste donc plus longtemps sur les canaux de service et ce temps est déduit du temps alloué aux messages de contrôle.

II.3.2 Quelques protocoles récents

Dans [61], un protocole MAC non-déterministe est proposé. Son principal objectif est d'améliorer la transmission de paquets de sécurité pendant l'intervalle CCH dans les réseaux à haute densité. Les auteurs ont introduit le concept d'intervalle CCH dynamique (DCI, Dynamic CCH Interval) qui est donc flexible et s'adapte en temps réel aux conditions du réseau. L'intervalle SCH est divisé en slots plus petits qui s'adaptent à la population actuelle dans le réseau.

Dans [62], les auteurs proposent un nouveau protocole d'accès au canal axé sur la coopération entre les nœuds. Le but est de garantir une qualité de service satisfaisante pour les applications de sécurité routière. CCRV-MAC (Cooperation in Cognitive Radio-based Vehicular Ad-hoc NETworks) encourage la collaboration entre les véhicules pour échanger des rapports sur l'état des canaux en vue d'un changement de canal proactif en cas d'apparition d'utilisateurs prioritaires qui portent des paquets urgents.

Dans [63], un protocole de contrôle d'accès pour une transmission fiable et rapide des messages de sécurité est proposé. Les auteurs mettent l'accent sur les délais de transmission des paquets critiques vu le caractère urgent de ces derniers. Le concept de valeur des paquets est intégré à la latence des différents messages déterminée par l'intervalle d'attente des paquets dans une file d'attente. En cas de congestion des canaux, un modèle de jeu coopératif inter-véhicules multicouche basé sur l'utilité optimale locale des participants est construit.

Dans [?], les auteurs proposent une nouvelle approche par l'utilisation d'un contrôle coopératif des véhicules sans compromettre la sécurité de ces derniers. Des unités de bord de route placées au niveau des ronds points permettent de gérer les changements de voies des véhicules entrants et sortants de ces ronds points. Ceci est fait dans le but d'optimiser le débit au niveau de ces scénarios spécifiques. RMAC (Roundabout MAC) utilise un ensemble de messages avec un système de priorisation différent qui se traduit par une meilleure utilisation de spectre de fréquence.

Dans [64], une amélioration de la méthode CSMA est proposée, avec pour principal objectif l'amélioration des transmissions multi-sauts pour les VANETs à forte densité. Le protocole commence par une première phase de construction d'une architecture en Clusters dans laquelle, chaque nœud désigne un père et un fils pour construire des liens visant à atteindre le chef de Cluster. Dans la seconde phase, chaque nœud enregistre pour chaque paquet une durée de vie calculée grâce au Minimum Spanning Tree Algorithm (MST). Le but de cet

algorithme est de résoudre le problème des interconnexions entre nœuds lors du routage des données.

Dans [65], les auteurs présentent une méthode visant à réduire les délais de transmission pour les applications non critiques dans les scénarios autoroutiers. Cette méthode ajuste dynamiquement les valeurs des fenêtres de contention dans 802.11p pour les différents services en fonction des conditions de circulation. Chaque véhicule tient une liste d'utilisation de l'intervalle SCH qui stocke les emplacements disponibles sur chaque SCH de l'intervalle de synchronisation suivant. Les nœuds peuvent ensuite négocier et réserver les canaux SCHs en utilisant des messages de type poignée de main WSA/RFS pour l'intervalle de synchronisation suivant.

Dans [66], les auteurs ont proposé une méthode de communication coopérative qui vise à limiter la dégradation des performances associée à la grande mobilité dans les réseaux de véhicules. Les RSU coopèrent avec les OBUs en s'échangeant des messages « Coop ». Ces messages contiennent de nouveaux champs de données tels que PSID (Provider Service Identifier), Data Rate et PMET (Path Maintenance Expectation Time). L'objectif est de permettre la sélection des meilleurs nœuds relais et d'améliorer les performances en termes de perte de paquets et de débit.

Dans [67], une méthode de contrôle de la congestion à l'intérieur de l'intervalle de service SCH est proposée. Les auteurs ont appliqué la stratégie « Taguch » afin de déduire un paramétrage optimal pour un meilleur flux de communication dans les scénarios autoroutiers. Cette méthode réduit les délais de transmission et peut être intégrée à d'autres protocoles MAC pour diminuer le taux de perte des paquets (PLR).

Dans [68], les auteurs ont proposé une solution axée sur la transmission de paquets de service nommée Mixed-Service-Mobility Model (MSM). Cette solution vise à offrir des performances satisfaisantes à la fois pour les applications tolérantes aux retards et pour celles qui doivent être gérées en temps réel. Les fenêtres de contention sont ici ajustées dynamiquement en fonction des variations de vitesse des nœuds du réseau.

Dans [69], les auteurs proposent une méthode coopérative visant à garantir des communications V2V et V2I avec qualité de service, et accroître la fiabilité et l'efficacité des transmissions sur le réseau. Le protocole s'appuie sur les liaisons V2V pour établir des échanges de données V2I modélisés pour satisfaire les contraintes de distance et de perte de paquet. Les métriques de performance visées par les auteurs sont : les délais de transmission et le taux de paquets de service envoyés avec succès.

Dans [70], les auteurs ont proposé une amélioration du protocole 1609.4 nommée AAA (Advanced Activity Aware Multi-Channel Operations). L'idée principale est d'utiliser les délais de transmission des BSMs (Message de sécurité de base) et le nombre de ces BSMs afin de calculer des valeurs adaptatives pour les intervalles SCH et CCH. Ce calcul est effectué par une RSU qui doit

collecter les informations communiquées par les nœuds du réseau et calculer ensuite une nouvelle valeur CCH au début de chaque seconde (UTC, Universal Time Coordinated). Cette information comprend le nombre moyen de BSM envoyés par véhicule, et le délai moyen des BSMs reçus par ce dernier. Ainsi, la RSU calcule le nouvel intervalle CCH en multipliant le nombre de BSMs par le délai moyen.

Dans [71], les auteurs ont proposé une solution au Coupon Collector's Problem présent au niveau MAC de la IEEE 802.11p. En effet, en raison du caractère aléatoire de l'accès au canal au sein du protocole de base, la collecte des informations concernant chaque véhicule du réseau peut s'avérer coûteuse en temps. H.Seo et al ont alors proposé d'exclure les nœuds WAVE ayant pu accéder avec succès au canal lors de la tentative précédente des prochains intervalles de messages de sécurité périodiques.

Dans [72], les auteurs ont proposé un algorithme de priorités strictes pour 802.11p. L'idée principale dans leur algorithme est de prolonger la durée du paramètre AIFS pour les trames de faible priorité pour ainsi réduire la compétition pour les trames prioritaires et donc améliorer les performances pour ce type de transmissions.

Dans [73], les auteurs proposent une optimisation de la bande passante en appliquant un "Vehicular Channel Access Scheme" appelé VCAS. L'idée ici est que tous les véhicules doivent écouter le canal pendant l'intervalle CCH pour recevoir des trames WAVE qui contiennent des informations WSA, qui seront ensuite diffusées par les RSUs pendant le même intervalle. Les véhicules ayant des taux de transmission similaires seront ensuite regroupés pour émettre sur le même SCH, et la taille des groupes est contrôlée afin de garantir l'équité. Les auteurs ont aussi proposé un modèle d'utilité marginal afin de trouver un compromis entre le débit et l'équité dans le réseau.

Dans [74], les auteurs proposent un protocole basé sur la détection. Un mécanisme RTS/CTS est utilisé dans le but de détecter la congestion dans le réseau par l'échange de messages périodiques et ainsi prédire le nombre de nœuds en compétition. Pour ensuite faire en sorte que ces nœuds adaptent leurs paramètres de contention (Window Values) de manière dynamique en se basant sur ces prédictions.

II.4 Les protocoles MAC hybrides

Les protocoles hybrides ont pour but d'exploiter les points forts des protocoles déterministes et non-déterministes. Ils se composent généralement de deux phases, l'une étant basée sur la réservation de slots (similaire à la méthode TDMA), et la seconde basée sur un système de compétition (similaire à la méthode CSMA). Nous présentons ici les protocoles hybrides fondateurs, ainsi que quelques protocoles récents.

II.4.1 Les protocoles fondateurs

Dans [75], les auteurs proposent un protocole MAC multi-canal. Il vise à garantir la prise en charge des hauts débits de données nécessaires pour l'acheminement des services d'info-divertissement (en utilisant plusieurs canaux simultanément), sans pour autant nuire à la transmission des messages de sécurité critiques. Le protocole utilise des points de coordination qui sont composés d'un point d'accès et d'un ou plusieurs fournisseurs de services non liés à la sécurité suivant les besoins du réseau. Les auteurs proposent ainsi de diviser le temps sur le canal en segments égaux nommés périodes de répétition. Chaque segment est lui-même divisé en deux parties distinctes ; une partie avec compétition pour l'accès au canal et une autre sans compétition. Dans un premier temps, le point de coordination procède à un tirage au sort par diffusion entre les véhicules ayant des émissions urgentes à effectuer et détermine ainsi un ordre de priorité durant la partie sans compétition. Les véhicules n'ayant pas été choisis lors de cette première phase entrent donc en compétition lors de la deuxième partie.

Dans [76], Lu et al. ont proposé un protocole d'accès au canal pour les réseaux véhiculaires basé sur la pile WAVE appelé DMMAC (Dedicated Multichannel MAC). Ce protocole vise avant tout à garantir un accès sans collisions au canal pour la transmission des messages de sécurité sur l'intervalle de temps CCHI (chaque intervalle de synchronisation est divisé en deux parties : CCHI pour le canal de contrôle et SCHI pour les canaux de service). DDMAC utilise une combinaison entre TDMA et CSMA/CA. L'intervalle SCHI est dédié aux messages d'information, tandis que CCHI est consacré aux messages de sécurité. CCHI est divisé en deux sous-intervalles, ABF (Adaptive Broadcast Frame) et CRP (Contention-based Reservation Period), qui sont séparés par une frontière flexible qui s'adapte au nombre de nœuds. ABF est utilisé pour la diffusion (multipoint) de messages de sécurité (similaire au CCH dans WAVE), à la différence près que pour ABF, des transmissions sans collisions peuvent être réalisées grâce à l'utilisation de TDMA. Les nœuds ont accès à des slots d'1 ms chacun. Une fois qu'un nœud a pu acquérir un slot il devra alors envoyer une trame d'information (IF) qui contient son identifiant (ID), des informations qui permettront à ses voisins de calculer la frontière entre ABF et CRP, ainsi que sa table d'allocation des slots (SAT, Slot Allocation Table). CRP est quant à lui utilisé pour prétendre à un slot et un canal pour la transmission des messages d'information. Les demandes durant l'intervalle CRP sont basées sur une authentification en trois étapes entre deux nœuds, une requête puis une réponse puis un acquittement. Les deux nœuds peuvent ainsi se mettre d'accord sur un slot et un canal pour commencer la transmission.

Dans [77], Ding et al. présentent CBMCS (Clustering Based MultiChannel Communication System). C'est un protocole basé sur le Clustering et qui a pour but de privilégier la transmission des messages de sécurité au détri-

ment des messages de service. Pour ce faire, on alloue six canaux de contrôle et un seul canal de service contrairement à 802.11p qui alloue un canal de contrôle et six canaux de service. Dans CBMCS, les canaux de contrôle utilisent CSMA pour l'accès au canal, pour le canal de service, TDMA est utilisé pour garantir des transmissions sans collisions. Après avoir choisi un chef de Cluster, tous les nœuds doivent lui envoyer périodiquement des informations relatives à leur vitesse et leur position durant la phase TDMA sur le canal de service. Le protocole inclut aussi ce que les auteurs appellent VAAM (Vehicle Accident Avoidance Mechanism) qui pousse les véhicules témoins d'un événement dangereux sur la route à informer leurs voisins et ainsi tenter d'éviter les accidents.

Dans [78], un protocole MAC hybride est proposé. VRCP (Vehicle to vehicle and Road to vehicle Collaborative Protocol) se compose de deux modes de communication. Le premier nommé MODE-A (Ad Hoc Mode) est utilisé lorsque l'unité de bord de route est hors de portée, et la méthode CSMA est privilégiée pour l'accès au canal. Le second mode nommé MODE-I est utilisé lorsque la RSU est à portée, et c'est la méthode TDMA qui est privilégiée dans ce cas. Dans VRCP, les RSUs s'échangent entre elles des informations concernant les "Message Data Slots" (MDS) afin de former un réseau centralisé au niveau de ces RSUs.

II.4.2 Quelques protocoles récents

Dans [79], les auteurs présentent SCMAC (Slotted Contention-based Media Access Control), qui est un protocole MAC hybride. Son but est de s'adapter aux changements fréquents de densité dans les VANETs, ainsi qu'aux différentes conditions des canaux de communication en temps réel. Chaque slot est divisé en deux périodes, la première est dédiée à la phase de réservation et la seconde à la transmission. La première phase est non-déterministe, c'est-à-dire que les nœuds entrent en compétition pour acquérir des slots encore libres. Tandis que durant la seconde phase, les collisions sont minimisées grâce à l'absence de compétition.

Dans [80], un nouveau protocole MAC adaptatif est présenté, avec deux objectifs principaux, améliorer l'allocation des slots pour les diffusions tout en garantissant un accès rapide au canal pour les autres types de transmission. Ceci est fait grâce à un schéma de trames adaptatif sur le canal de contrôle et les canaux de service. L'intervalle CCH est divisé en période de diffusion et période de négociation. La période de diffusion est composée de slots égaux en durée, et le nombre de slots change de manière adaptative suivant les densités de trafic pour permettre aux véhicules d'émettre des messages de statut périodiquement.

Dans [81], les auteurs présentent un protocole MAC basé sur les jetons pour des communications V2V fiables dans les VANETs. DTB-MAC (Dyna-

mic Token-Based MAC) met en œuvre une approche d'échange de jetons en plus d'un protocole MAC à accès aléatoire pour éviter autant que possible la congestion des canaux, améliorant ainsi la fiabilité des transmissions de messages de sécurité. Il offre automatiquement des possibilités de retransmission pour permettre aux véhicules de transmettre avec succès leurs Beacons avant la génération du message périodique suivant, chaque fois que le temps et la largeur de bande le permettent.

Dans [82], les auteurs proposent une amélioration de la méthode EDCA présente dans la norme 802.11p. En introduisant le principe de réservation de slots défini dans TDMA, QCH-MAC (Qos-aware Centralized Hybrid MAC) vise à améliorer la qualité de service en réduisant la perte de paquets et en augmentant le débit. Le temps d'accès est divisé en deux périodes : une période de transmission (TP) et une période de réservation (RP). TP se compose d'un ensemble de slots TDMA appelés Tslots, tandis que la période RP utilise le protocole EDCA avec deux classes. La période RP est uniquement utilisée par les véhicules entrants dans le réseau pour réserver leurs créneaux horaires parmi ceux du set des Tslot.

Dans [83], une solution MAC hybride est présentée, elle vise à améliorer la diffusion des messages basiques de sécurité (BSMs). Cette solution est basée sur la méthode DSRC, elle est partiellement centralisée et partiellement distribuée. Ceci permet non seulement de réduire efficacement les collisions, mais aussi de maintenir la compatibilité avec la norme IEEE 802.11p. Les auteurs ont également proposé l'utilisation du codage au niveau de la couche physique (PNC, Physical-layer Network Coding) et du codage de réseau linéaire aléatoire (RLNC, Random Linear Network Coding) afin de renforcer la fiabilité et l'efficacité de la diffusion des BSMs.

Dans [84], les auteurs contribuent à améliorer la détection en temps réel des évènements potentiellement dangereux sur la route afin d'augmenter la sécurité de ses usagers. Pour ce faire, un protocole distribué est proposé qui assure à la fois la couverture et la connectivité du réseau. Il permet la détection des dangers potentiels, et ce même en cas de défaillance des nœuds capteurs.

Dans [85], les auteurs proposent de diviser le réseau en cellules, et que les nœuds de chaque cellule partagent une bande de fréquence qui leur soit unique. Le temps d'accès au canal est divisé en deux périodes RS (Reservation Slot) et TS (Transmission Slot). Dans la période RS, les nœuds entrent en compétition en utilisant la méthode CSMA. Il s'échangent des messages de type « WAVE SHORT », tout en émettant des requêtes de réservation pour la prochaine période TS. Cette dernière utilise quant à elle la méthode TDMA et sert à la transmission de données plus volumineuses.

Dans [86], les auteurs proposent d'allier les deux méthodes TDMA et CSMA pour garantir un accès au canal sans collisions pour les messages de sécurité critiques. Le protocole utilise la réservation de slots et l'intervalle CCH est divisé en deux périodes. La première est dédiée à la réservation de slots et la

seconde à la transmission. Durant la phase de réservation, chaque nœud se voit allouer un slot qui lui sera unique pour une durée de temps limitée, c'est-à-dire que ce nœud utilisera le même slot pendant cette durée. Durant la phase de transmission, des messages de type HELLO, SWITCH et WSA/RES/ACK sont échangés dans le réseau.

Dans [87], CS-TDMA est présenté. C'est un protocole MAC qui vise à fournir des diffusions fiables à un saut, en combinant les trois méthodes CSMA, TDMA et SDMA. Dans CS-TDMA, les intervalles CCH et SCH sont ajustés de manière dynamique en fonction de la densité du réseau. C'est-à-dire que plus le nombre de nœuds est important, plus la durée de l'intervalle CCH est augmentée pour répondre aux besoins du réseau en termes de transmissions de paquets de sécurité critiques. Dans le cas où la population est moins importante, c'est l'intervalle SCH qui est augmenté au détriment de CCH afin de fournir une meilleure bande passante pour les applications de service non critiques.

Dans [88], les auteurs proposent de diviser l'accès au canal en deux segments distincts. Le but est de réduire le taux de collisions entre les messages périodiques et les messages non planifiés (spontanés). Le premier segment est donc dédié à la réservation de slots, et sert à allouer des slots spécifiques aux nœuds pour la transmission de messages périodiques. Le second segment est dédié à la compétition pour l'accès au canal, et sert à la transmission de messages spontanés.

Dans [89], les auteurs ont proposé une amélioration de la qualité de service pour les applications d'information et de divertissement en optant pour une alternation entre un accès au canal centralisé et distribué pour l'intervalle SCH. Ce protocole appelé W-HCF (WAVE-based Hybrid Coordination Function) vise aussi à ajuster la bande passante pour les applications qui ne sont pas affectées par les restrictions de qualité de service. C'est-à-dire qu'une partie de l'intervalle SCH est réservée aux applications affectées par la qualité de service et l'accès y est centralisé. Tandis que l'autre partie est réservée aux applications non sensibles à la qualité de service et l'accès y est donc distribué.

II.5 Synthèse et analyse critique sur les protocoles MAC présentés

La Table II.1 présente une analyse critique des protocoles MAC présentés dans ce chapitre. Nous avons donné dans cette table pour chaque protocole un avantage principal et inconvénient principal.

Analyse critique sur les protocoles MAC présentés			
Protocole	**Type**	**Avantages**	**Inconvénients**

RR-ALOHA [28]	**Déterministe**	**Très peu de collisions**	**Temps d'attente élevés.**
ATSA [29]	**Déterministe**	**Temps sur le canal réparti de façon équitable entre les véhicules**	**S'adapte mal aux fortes populations.**
[30]	**Déterministe**	**Permet aux nœuds d'avoir une vision globale des réservations de slots de leurs voisins, et règle ainsi le problème du terminal caché**	**Les diffusions entre voisins augmentent la charge sur le réseau.**
MCTRP [31]	**Déterministe**	**Les temps d'attente pour l'accès au canal sont très courts**	**Très dépendant des Ring Leaders.**
STDMA [32]	**Déterministe**	**Réduit les collisions et donc la perte de paquets**	**Les cas où des slots sont alloués mais pas utilisés se produisent assez souvent.**
CBMAC [33]	**Déterministe**	**Bonne bande passante et problème du nœud caché résolu**	**Non adapté aux réseaux déployés en ville.**
W-UIM [35]	**Déterministe**	**Faible taux de perte de paquets**	**Dépendant des "WBSS providers".**
VCAR-MAC [36]	**Déterministe**	**Adapté aux transmissions multimédia telle que la vidéo.**	**Inadapté aux scénarios d'accidents.**
I-MAC [37]	**Déterministe**	**Nombre de collisions faible.**	**Inadapté aux transmissions urgentes.**

[41]	**Déterministe**	**Faible taux de collision**	**Inadapté aux applications en temps réel.**
[42]	**Déterministe**	**Faible taux de collisions**	**Inadapté aux applications en temps réel.**
[43]	**Déterministe**	**Faible taux de perte de paquet**	**Délais de bout en bout élevés.**
VeMAC [44]	**Déterministe**	**Faible taux de perte de paquets**	**Cause une forte charge sur le réseau.**
[45]	**Déterministe**	**Améliore le taux de transmissions réussies pour les paquets de sécurité critiques**	**Dépendant des RSU qui sont très coûteuses à installer.**
CAHMAC [46]	**Déterministe**	**Diminue la perte de paquets et augmente la bande passante sur l'intervalle SCH**	**Les HNs (Helper Nodes) peuvent utiliser pour les retransmissions des slots dont auraient besoin d'autres véhicules du réseau.**
[47]	**Déterministe**	**Fonctionne très bien dans des environnements dégagés**	**S'adapte mal aux fortes populations.**
CBT [48]	**Déterministe**	**Transmissions stables au sein du même Cluster**	**Le choix des VC ne se base pas sur des paramètres prenant en compte le caractère dynamique des VANETs.**
[49] [50]	**Déterministe**	**Améliore les transmissions de type V2I**	**Très coûteux à déployer.**

[51]	**Déterministe**	**Protocole adaptatif au caractère dynamique des VANETs**	**Très coûteux à déployer.**
CFR [52]	**Déterministe**	**Très adaptatif au caractère mobile des VANETs**	**Inadapté aux environnements urbains.**
V-MESH [53]	**Non-Déterministe**	**Améliore la bande passante pour les applications de service non-critiques**	**Cette amélioration se fait au détriment des transmissions de sécurité critiques.**
[54]	**Non-Déterministe**	**Faible taux de perte de paquets**	**S'adapte mal aux fortes populations.**
[55]	**Non-Déterministe**	**Adaptatif aux fortes vitesses des véhicules**	**S'adapte mal si les véhicules changent fréquemment de voies.**
[56]	**Non-Déterministe**	**Fournit une bonne bande passante dans le réseau**	**Très dépendant d'une bonne connexion V2I.**
VMMAC [57]	**Non-Déterministe**	**S'adapte bien aux fortes populations**	**L'installation des antennes omnidirectionnelles serait très coûteux.**
D-MAC [58]	**Non-Déterministe**	**Perte de paquets réduite**	**Coût de déploiement élevé.**
[61]	**Non-Déterministe**	**Transmission de paquets de sécurité améliorée.**	**Inadapté au trafic multimédia.**
[65]	**Non-Déterministe**	**Délais de transmission courts**	**Charge élevée sur le réseau.**
[66]	**Non-Déterministe**	**Débit élevé**	**Dépendant de certains nœuds clés.**

[67]	**Non-Déterministe**	**Faible taux de perte de paquets**	**Inadapté aux réseaux à haute densité.**
MSM [68]	**Non-Déterministe**	**Protocole adapté à plusieurs types de données transmises**	**Requiert des informations précises en temps réel sur la vitesse des nœuds.**
[69]	**Non-Déterministe**	**Faible taux de collisions**	**Nombre de paquets échangés élevé.**
[70]	**Non-Déterministe**	**Délais de bout en bout réduits**	**La fréquence de mise à jour des nouveaux intervalles calculés n'est pas assez élevée pour s'adapter à la grande mobilité des nœuds.**
[71]	**Non-Déterministe**	**Charge sur le réseau réduite**	**Peut engendrer des délais d'attente importants pour certains nœuds.**
[73]	**Non-Déterministe**	**Bonne utilisation de la bande passante**	**Dépendant des unités de bords de route, et utilise l'inondation qui augmente la charge sur le réseau.**
[74]	**Non-Déterministe**	**Permet de garantir un certain niveau d'équité entre les nœuds**	**Le système de prédiction ne fonctionne pas en cas de déconnexion de certains nœuds.**

[75]	**Hybride**	**Adapté aux applications de service non-critiques**	**Non adapté aux diffusions critiques en cas d'accidents ou d'événements dangereux.**
DMMAC [76]	**Hybride**	**Transmissions stables avec peu de perte de paquets pour les applications de sécurité**	**S'adapte mal aux fortes populations.**
CBMCS [77]	**Hybride**	**Adapté aux diffusions de messages de sécurité critiques**	**Inadapté aux environnements urbains.**
VRCP [78]	**Hybride**	**Adaptatif en temps réel aux conditions du réseau**	**Même si le Mode-A existe, le protocole reste dépendant des RSUs.**
SCMAC [79]	**Hybride**	**Faible taux de collisions.**	**Inadapté aux transmissions urgentes.**
[80]	**Hybride**	**Débit élevé pour les applications de service.**	**Inadapté aux transmissions urgentes.**
[85]	**Non-Déterministe**	**Offre une bonne bande passante et une faible charge sur le réseau**	**Ne s'adapte pas aux changements de population et à la forte mobilité des nœuds.**
[86]	**Hybride**	**Réduit les collisions sur l'intervalle CCH**	**Fonctionne mal dans les réseaux à forte population.**

[87]	**Hybride**	**Augmente la fiabilité des transmissions de sécurité critiques pour les réseaux à forte population**	**La population n'est pas un paramètre suffisant pour le choix de la durée de l'intervalle CCH.**
[88]	**Hybride**	**Réduit la perte de paquets**	**S'adapte mal aux réseaux à forte population.**
[89]	**Hybride**	**Qualité de service améliorée pour l'info-divertissement**	**Dépendant de certains nœuds distributeurs.**

TABLE II.1: Analyse critique des protocoles MAC

II.6 Conclusion

Nous avons vu dans ce chapitre les principaux protocoles d'accès au canal proposés pour les VANETs dans la littérature.

Nous pouvons constater que les propositions d'amélioration de l'accès au canal ont tendance à se concentrer sur un type de données en se préoccupant peu de l'autre type. En effet, les articles qui visent à améliorer les transmissions de paquets de service (information ou divertissement) ont tendance à négliger les transmissions de messages de sécurité critiques, et vice-versa.

Dans le prochain chapitre, nous nous intéressons aux différents travaux proposés dans la littérature qui visent à améliorer le routage dans les réseaux véhiculaires.

Chapitre III

État de l'art des protocoles de routage pour les VANETs

III.1 Introduction

Dans ce chapitre, nous allons passer en revue les principaux protocoles de routage proposés pour les réseaux véhiculaires. Ces derniers peuvent être de nouvelles solutions ou bien des améliorations de travaux déjà existants. Nous avons opté pour une classification basée sur la méthode utilisée pour la sélection des nœuds constituant les routes choisies. Nous présentons donc les protocoles géographiques basés sur la position, puis les protocoles topologiques avec leurs trois sous types (proactif, réactif et hybride). Une critique de ces travaux est présentée à la fin du chapitre.

III.2 Protocoles Géographiques (basés sur la position)

Les protocoles basés sur la position exploitent les informations fournies par le service GPS pour prendre des décisions sur le routage des paquets, et les nœuds ne disposent généralement pas d'informations sur la topologie du réseau. Nous présentons ici les principaux protocoles fondateurs présents dans la littérature, ainsi que quelques protocoles récents.

III.2.1 Les protocoles fondateurs

Dans [90], les auteurs proposent d'utiliser des nœuds désignés (distributeurs) pour stocker les paquets qui doivent être envoyés dans une zone Multicast. Bien sûr, le nœud lui-même doit faire partie de cette zone, et les paquets transportés par les nœuds désignés doivent être envoyés à d'autres nœuds s'ils sont sur le point de quitter la zone. Le choix de ces nœuds se fait selon deux

critères qui sont la vitesse du véhicule (favorisant les basses vitesses) et la position (favorisant les nœuds proches du centre de la zone Multicast). Ceci permet à un distributeur de conserver ce rôle le plus longtemps possible.

Dans [91], les auteurs proposent un protocole de routage qui se base sur un système de stockage puis de retransmission de paquets. Donc, un nœud enregistre le paquet qu'il reçoit jusqu'à ce qu'un autre nœud entre dans sa zone de transmission, il lui envoie alors le paquet. Ceci permet de s'adapter au caractère très mobile et à la topologie dynamique des réseaux véhiculaires, et d'offrir une solution au problème de déconnexions fréquentes. Le protocole utilise la prédiction des mouvements des véhicules en évaluant le type de la route empruntée, ce qui est utile aux nœuds pour déterminer leurs prochains sauts. Le protocole calcule ensuite la route optimale en termes de temps de transmission, pour envoyer les paquets. Pour maintenir la continuité des transmissions, chaque nœud s'enregistre en tant que saut déjà visité avant de transférer un paquet. De cette manière, tous les nœuds auront à leur disposition des informations sur les sauts précédents par lesquels est passé le paquet, et éviteront donc de le renvoyer à un nœud l'ayant déjà reçu. Le problème de la boucle de routage est donc évité.

Dans [92], un protocole de routage qui prend en compte les temps de transmission prédits à l'avance pour déterminer les chemins à suivre par les paquets est proposé. Les nœuds sont choisis par rapport à leur disposition à router rapidement ces paquets. Les véhicules utilisent les informations GPS pour avoir une estimation de leurs trajectoires, ils connaissent aussi les adresses des autres nœuds. Ils utilisent ensuite ces informations pour estimer le meilleur chemin possible en prenant en compte la position GPS du destinataire par rapport à leur future position (calculée via la trajectoire).

Dans [93], les auteurs présentent un protocole de routage géographique utilisant les transmissions Multicast nommé ROVER (RObust VEhicular Routing). Pour fonctionner, ROVER fait circuler de manière périodique des paquets de contrôle à travers le réseau, et les nœuds peuvent envoyer des paquets destinés à des zones géographiques ciblées. Dans ce protocole, tous les nœuds sont supposés avoir un identifiant unique, ainsi que des informations précises sur le positionnement des autres nœuds du réseau. La transmission d'un paquet se fait comme suit, le nœud émetteur commence par diffuser une demande de route dans toute sa zone géographique, à l'intérieur de laquelle il doit inclure son identifiant, sa position et un numéro spécial attribué au chemin demandé. Ce paquet sera retransmis par tout nœud l'ayant reçu et se trouvant dans la zone géographique, ce même nœud enverra aussi son identifiant et le numéro de la route demandée à tous ses voisins à un saut.

Dans [94], les auteurs proposent un protocole de routage géographique appelé Greedy Perimeter Stateless Routing (GPSR). Dans GPSR, les nœuds diffusent leur position via des messages périodiques, et lorsqu'un nœud a des données à transmettre, il utilise l'un des deux modes de transmission propo-

sés : Greddy Forwarding et Perimeter Routing. Dans Greedy Forwarding, un nœud désireux de transmettre des paquets commence par chercher le chemin le plus court vers la destination (dont la position exacte est censée être connue grâce à un service de localisation) et envoie le paquet. Il y a cependant un cas où aucun des voisins de l'expéditeur n'est plus proche de la destination que l'expéditeur lui-même, c'est dans ce cas que le second mode de transmission est utilisé. Dans le routage périmétrique, un lien virtuel entre le nœud source et le nœud destinataire est créé à l'aide d'un graphe planaire, les paquets suivront alors ce lien. Ce qui signifie que les nœuds les plus proches de cette ligne virtuelle sont élus comme sauts suivants.

Dans [95], Lochert et al. ont proposé GPCR (Greedy Perimeter Coordinator Routing). C'est un protocole de routage se basant sur des nœuds coordinateurs pour transmettre les paquets à travers leur chemin, et la retransmission des paquets vise toujours les nœuds qui sont géographiquement proches de la destination. GPCR fournit ses meilleures performances lorsqu'il est implémenté sur des réseaux comptant peu d'obstacles (dégagés), et avec un positionnement uniforme des nœuds.

Dans [96], Santos et al. ont présenté un protocole de routage basé sur la localisation. Ce protocole fonctionne avec un système de Clusters. Chaque nœud peut devenir chef de Cluster, nœud passerelle ou bien simple membre d'un Cluster. Chaque Cluster ne peux avoir qu'un seul chef au maximum, et comme leur nom l'indique les nœuds passerelles servent de lien entre deux Clusters, ils sont donc connectés à plus d'un Cluster. La transmission de paquets se fait suivant la méthode Greedy Routing. Si le nœud source ne connaît pas la position du destinataire, il va suivre la même procédure présente dans le protocole AODV. C'est-à-dire envoyer une requête LREQ (Location Request), qui sera normalement suivie d'une réponse LREP (Location Reply). A noter que ces deux messages spéciaux ne peuvent être acheminés que par les chefs de Clusters et les nœuds passerelles.

Dans [97], les auteurs proposent un nouveau protocole géographique dédié à la diffusion de paquets dans les scénarios autoroutiers. Dans ce protocole, les groupes cibles de diffusion ou de Multicast sont déterminés en fonction de trois paramètres : direction, vitesse et position des véhicules. Les auteurs proposent également d'utiliser un système de minuterie pour acheminer les messages d'un saut à l'autre, et les véhicules doivent écouter les émissions périodiques afin de connaître la topologie actuelle du réseau.

Dans [98], une solution au problème du minimum local est proposée. Si un véhicule ne trouve pas de nœud relais pour ses paquets qui soit plus proche de la destination que lui-même, il le stocke dans une mémoire cache. Ensuite, il doit le transmettre dans le futur le plus proche possible, par exemple, après un changement de topologie. Les auteurs ont également proposé un nouveau mécanisme de sélection des meilleurs voisins basé sur les informations concernant les changements de voisinage précédents collectées par les nœuds du réseau.

Dans [99], A-STAR (Anchor-based Street and Traffic A ware Routing) est présenté. C'est un protocole de routage géographique dédié aux environnements urbains et basé sur la technique de Greedy Forwarding. Afin de sélectionner les meilleures routes possibles, les auteurs ont proposé d'utiliser les informations relatives au trafic routier récoltées sur les voies parallèles (dédiées aux transports en commun tels que les Bus). En effet, après avoir récolté ces informations, les meilleures routes sont désignées. Ces dernières sont celles comptant le plus grand nombre de "bonnes" intersections. C'est-à-dire des intersections ayant un nombre suffisant de véhicules afin d'assurer une bonne connectivité.

Dans [100], les auteurs présentent un protocole de routage géographique adapté aux réseaux installés en ville. GyTAR (Greedy Traffic Aware Routing) utilise les informations relatives à la vitesse et la direction des véhicules (récoltées par GPS + capteurs) afin de sélectionner les routes les plus stables. L'objectif affiché pour ce protocole est d'optimiser la bande passante en réduisant la charge causée pas les messages de contrôle circulant sur le réseau.

Dans [101], un protocole de diffusion visant à réduire la perte de paquets est proposé. UMB (Urban Multi-hop Broadcast protocol) se déroule en deux phases distinctes. Dans la première, appelée "diffusion directionnelle", le nœud source choisit un nœud se déplaçant dans la direction de la zone de distribution pour servir de relais, sans pour autant prendre en considération quelconque information sur la topologie. La seconde phase se déroule quant à elle au niveau des intersections et consiste en la diffusion des paquets vers toutes les directions.

III.2.2 Quelques protocoles récents

Dans [102], un nouveau protocole de routage géographique est présenté. Ce protocole est conçu pour la transmission de messages multimédia dans les environnements denses. Les auteurs proposent d'exclure les nœuds se trouvant derrière des obstacles (murs, bâtiments, etc.) de la liste des prochains sauts potentiels pour un paquet donné.

Dans [103], un algorithme de routage nommé GINS (Geographic Information and Node Selfish-based routing) est présenté. Il exploite une combinaison des informations de position disponibles et échangeables par les nœuds, et des intentions de transmission de ces nœuds dans le futur proche afin de maximiser les chances d'établir le contact avec le véhicule destinataire. L'algorithme calcule un score de relais pour chaque nœud pouvant être un saut potentiel dans la route d'un message. Puis, selon la disponibilité au niveau de la mémoire tampon de chaque nœud, une décision de transmission est prise en résolvant ce que les auteurs ont appelé le 0-1 knapsack problem.

Dans [104], un protocole de routage dédié à la diffusion de paquets d'urgence est présenté. Il est particulièrement adapté aux réseaux couvrant une grande surface. Un système de zones de transmission est utilisé afin d'amener les paquets vers des concentrations de nœuds pouvant assurer la retransmission. Ceci est fait dans le but d'éviter les retransmissions inutiles et donc de réduire également le taux de collisions des diffusions d'urgence.

Dans [105], M-GEDIR (Multi-metric GEographic DIRectionnal routing) est présenté. Ce protocole se base sur deux métriques pour la sélection des prochains sauts. Il utilise l'estimation de la puissance du signal et la prédiction des futures positions des véhicules. Le but est d'éviter la sélection de nœuds relais non atteignables et donc aussi des routes condamnées à disparaître.

Dans [106], un algorithme basé sur les Clusters est proposé. Son objectif est d'assurer une diffusion de paquets de sécurité critiques efficace, pour ainsi éviter au maximum les accidents. Les Clusters sont formés de telle sorte que les collisions entre véhicules soient minimisées, et l'élection de Cluster Heads permet d'éviter les intrusions inter-Cluster. Les auteurs ont proposé d'utiliser un protocole MAC déjà existant pour la dissémination de messages d'urgence dans des délais raisonnables.

Dans [107], ZHANG et al. proposent un protocole géographique nommé GRUV (Geocast Routing in Urban Vehicular ad hoc networks). Il vise à améliorer la qualité des diffusions de paquets en zones urbaines car cette dernière est généralement rendue difficile par le caractère très mobile des réseaux véhiculaires, et par les nombreux obstacles potentiels sur les routes qui peuvent causer des pertes de connexion et des ruptures de liens entre les nœuds. Pour ce faire, GRUV classe ces nœuds selon leur position par rapport à la route. C'est-à-dire que le protocole fait une distinction entre les véhicules se trouvant au milieu d'une route et ceux se trouvant aux intersections. Les zones de routage sont ensuite choisies dynamiquement selon ces positions et une des trois méthodes de transmission proposées est privilégiée.

Dans [108], les auteurs proposent un protocole de routage pour les réseaux véhiculaires, qui vise à résoudre le problème des ruptures de liens qui est fréquent pour les protocoles géographiques. Ce problème survient lorsque les informations stockées concernant un (ou plusieurs) nœud(s) sont obsolètes (elles n'ont pas été mises à jour). Le protocole utilise les informations GPS récoltées pour estimer les prochaines positions d'un véhicule suivant sa trajectoire. Les nœuds commencent par vérifier qu'au moins un voisin est disponible pour transférer un paquet. Si plusieurs nœuds voisins sont disponibles il choisit alors la meilleure option en se basant sur les informations de mobilité récoltées.

Dans [109], les auteurs ont proposé un protocole de routage se basant sur la retransmission par diffusion de paquets en utilisant des voisins qui sont déterminés suivant leur position géographique. Les autres nœuds voisins n'ayant pas reçu un ordre de retransmission après une certaine durée prédéfinie (un temps d'attente) exécutent la rediffusion du paquet. Afin de fonctionner correctement,

le protocole a besoin d'un balisage permanent du réseau, pour avoir des informations nécessaires tels que la position des véhicules, leur état de connectivité, leur vitesse, etc.

Un protocole de routage pour les environnements ouverts appelé Directional Greedy Routing (DGR) a été proposé par Gong et al. dans [110]. Ce protocole s'appuie sur les données et les cartes GPS pour recueillir des informations sur la position des véhicules, ainsi que sur des services de localisation pour obtenir la position exacte des nœuds destinataires. Chaque nœud est également censé enregistrer sa propre vitesse et sa propre direction à l'aide de capteurs internes, et utiliser ces données pour acheminer les paquets de la meilleure façon possible. DGR utilise un compromis entre la distance séparant les relais potentiels du nœud destinataire et la direction de ces relais. Dans [111], les auteurs ont proposé une amélioration de DGR nommée PDGR (Predictive Directional Greedy Routing). Comme dans DGR, les véhicules doivent communiquer la position de leurs voisins aux autres nœuds, mais dans PDGR, cette information est utilisée pour transmettre des paquets aux relais en utilisant une technique prédictive. C'est-à-dire que les nœuds relais sont sélectionnés en fonction des positions futures calculées ou estimées.

Dans [112], les auteurs proposent d'utiliser la prévision de mouvements pour estimer les futures positions des véhicules et garantir ainsi une plus grande efficacité lors du choix des groupes Multicast. Les véhicules vérifient de manière autonome s'ils font ou non partie du groupe de destination d'un message envoyé. Pour ce faire, ils utilisent un nouveau format de paquet contenant leur position et leur vitesse, de sorte qu'ils puissent également décider si leurs voisins font partie de ces groupes destinataires via l'échange de messages de type HELLO. L'idée est de regrouper les véhicules les plus susceptibles de se trouver dans la même zone géographique à l'avenir pour former des groupes Multicast stables.

Dans [113], les auteurs proposent un algorithme qui peut être utilisé comme complément aux protocoles de routage et vise à prédire avec précision la position des nœuds destinataires. Pour être opérationnel, cet algorithme doit recueillir des informations relatives au mouvement des véhicules ; la vitesse du véhicule (V-Speed), la direction du déplacement (V-Dir), la position actuelle (V-Pos) et la position finale (V-Final). Notez que cette dernière information n'est pas toujours exacte à 100%. La façon dont fonctionne l'algorithme est qu'il commence par estimer la future position d'un nœud en utilisant simplement les trois premières mesures de données présentées ci-dessus. Puis une vérification est faite pour savoir si la position estimée est correcte (en utilisant des paquets de type Query-Acquittal ou requête-acquittement). S'il s'avère que l'estimation n'est pas exacte, une seconde estimation est effectuée à l'aide du paramètre V-Final afin d'obtenir une prévision plus précise.

Dans [114], les auteurs proposent un protocole géographique se basant sur la portée de transmission des nœuds pour la sélection des prochains sauts.

Contrairement aux protocoles utilisant le Greddy Forwarding (comme GPSR), les auteurs ont opté pour le choix des routes comptant des véhicules séparés de distances assez courtes pour garantir des transmissions radio de qualité et éviter la perte de signal. Pour ce faire, le protocole compte trois phases principales ; prédiction du prochain saut, choix du prochain saut et planification par priorité.

Dans [115], un protocole de routage géographique est proposé par les auteurs. PDVR (Position-based Directional Vehicular Routing) vise à sélectionner les prochains sauts en se basant sur deux critères principaux. Le prochain saut doit avoir une vitesse proche de celle du nœud source (les véhicules sont supposés utiliser les informations GPS pour récupérer les données de vitesse et de position), et ce même prochain saut doit se diriger vers le nœud destinataire (directions de mouvement similaires). Le but de ces deux critères est de garantir la sélection de relais ayant le plus de chance de ne pas perdre les paquets reçus, et le plus de chance de rapprocher ces paquets de leurs destinataires.

Dans [116], HRV (Hybrid Routing in VANETs) est présenté. C'est un protocole de routage géographique basé sur la coopération. En effet, les auteurs proposent d'allier la force de calcul des unités de bord de route afin de déduire les meilleurs relais pour la transmission des paquets. Ces calculs se basent sur la prédiction des futures positions des véhicules. L'une des particularités de HRV et que certaines tâches sont confiées à certains nœuds individuels dans le but d'optimiser les ressources du réseau.

III.3 Protocoles basés sur la topologie

Ces protocoles se basent sur un ensemble d'informations stockées dans des tables de routage, qui contiennent notamment les adresses des différents nœuds du réseau. Nous avons classé ces protocoles en trois sous-types, les protocoles proactifs, réactifs et hybrides, nous présentons pour chaque sous-type les protocoles fondateurs, et quelques protocoles récents.

III.3.1 Protocoles proactifs

Les protocoles fondateurs

Dans [117], les auteurs utilisent l'algorithme du plus court chemin de Dijkstra, afin de calculer les chemins optimaux qu'un paquet doit suivre pour atteindre le nœud destinataire. Dans GSR (Global State Routing), qui est un protocole proactif, chaque nœud maintient une table décrivant la topologie du réseau, l'adresse de ses voisins et celle de ses prochains sauts. En plus, on a dans la table, la liste des distances séparant les nœuds, qui est utilisée pour appliquer l'algorithme de Dijkstra. Ces tables doivent être mises à jour de manière périodique via des diffusions de contrôle afin de refléter de manière fidèle

les changements dans le réseau (changements de topologie, de distance entre les nœuds, etc.).

Un protocole de routage basé sur la diffusion d'urgence a été présenté dans [118]. BROADCOMM est destiné aux réseaux implémentés en autoroute et fonctionne suivant un système de hiérarchie. Le réseau est divisé en cellules, les nœuds se trouvant dans une cellule sont ainsi considérés au sommet de la hiérarchie, et les autres nœuds sont appelés nœuds réflecteurs. Ces nœuds réflecteurs ont pour mission d'agir comme des chefs de Clusters et ainsi transmettre les messages urgents entre les nœuds d'une même cellule.

Dans [119], Clausen et al. proposent une amélioration de la méthode Link State Routing (LSR). Ils introduisent la notion de nœuds relais multipoint (MPR, Multi-Point Relay), et le protocole s'adapte à la topologie dynamique des réseaux véhiculaires. En effet, dans OLSR (Optimized Link State Routing) les adresses des nœuds du réseau ainsi que l'état des liens de communication sont enregistrés dans des tables de routage, et les changements de topologie sont tout de suite signalés à certains nœuds désignés. Ces nœuds sont choisis pour servir de relais et éviter d'utiliser la méthode d'inondation de paquets dans le but de réduire la charge sur le réseau. Les auteurs ont également proposé de modifier le format des paquets de contrôle afin de réduire l'Overhead, en y incluant les liens de communication reliant les nœuds du réseau aux nœuds relais (MPR).

Quelques protocoles récents

Dans [120], les auteurs présentent un protocole de routage proactif avec Clusters pour les VANETs utilisant un nouveau schéma d'adressage dans lequel chaque nœud reçoit une adresse en fonction de sa mobilité actuelle. La technique de « Hamming » est ensuite utilisée pour cloisonner le réseau d'une manière centrée sur l'adresse. Les Clusters sont gérés par un seul chef et des méthodes adaptatives sont utilisées pour chacune des trois situations : le CH quitte son Cluster, un nœud non enregistré intègre le Cluster, un lien de communication est rompu au sein d'un Cluster.

Dans [121], les auteurs proposent PSCAR (Proactive-optimal-path Selection with Coordinator Agents assisted Routing), un protocole de routage proactif basé sur la sélection de chemins optimisés en utilisant des agents coordinateurs. Ces nœuds coordinateurs sont placés aux intersections dans le but d'améliorer les performances de routage et de faire face aux obstacles radio (bâtiments, arbres, etc.). Ils sont statiques et ont à leur disposition la position de tous les autres nœuds coordinateurs du réseau. PSCAR essaye donc toujours d'envoyer les paquets vers le coordinateur le plus proche de la destination.

Dans [122], un nouveau protocole de routage proactif intelligent est présenté. Les auteurs ont opté pour un échange d'informations intensif dans le but de fournir rapidement à tous les véhicules du réseau des informations en temps réel concertant l'état des liens de communication et l'utilisation des canaux. Le protocole vise ainsi à garantir des transmissions causant le moins de congestion possible et réduire le taux de rupture des liens.

Dans [123], les auteurs proposent d'utiliser le concept de PSO (Particle Swarm Optimization) dans le but de garantir un routage proactif avec qualité de service. En modélisant le comportement d'un groupe de particules, le protocole évalue la meilleure solution possible au problème de sélection de la meilleure route. Les paramètres pris en compte pour nourrir l'algorithme d'optimisation sont la position relative des véhicules et leur vitesse à un instant t. Comme toutes les instances de PSO, le protocole passe par de nombreuses itérations afin d'affiner le processus de sélection.

Dans [124], Un protocole de routage nommé IDVR (Intersection Dynamic VANET Routing) est proposé. Un réseau centralisé est utilisé pour récolter des informations de trafic routier en temps réel et les envoyer vers les intersections qui sont gérées par des chefs appelés ICH (Intersection Cluster Head). Ces ICH sont responsables de sélectionner les meilleures routes en se basant sur la durée de vie des liens et la position du nœud destinataire. Tout ceci dans le but d'augmenter la stabilité des transmissions et le débit pour les topologies en grille.

Dans [125], les auteurs ont proposé un nouveau schéma d'acheminement de paquets optimisé pour les VANETs. Pour pallier au caractère instable des routes de transmission dans ce type de réseaux, ils ont opté pour l'union de deux méthodes qui sont l'approche système multi-agent et les algorithmes PSO (Particle Swarm Optimization).

Dans [126], une amélioration de la dissémination de paquets dans les réseaux véhiculaires est proposée. Les auteurs proposent de se baser sur certaines unités de bord de route dans le but d'améliorer la fiabilité des transmissions et diminuer les risques d'attaques internes. Un système de détection à deux niveaux est utilisé. Dans le premier niveau, les nœuds voisins calculent le niveau de confiance individuellement. Au second niveau, un consortium est utilisé et est basé sur une "Blockchain" avec des unités RSUs autorisées comme valideurs.

Dans [127], les auteurs présentent un protocole de diffusion utilisable dans les scénarios à très haute vitesse. Une méthode appelée CDS (Connected Dominating Sets) est couplée à un mécanisme d'élimination de voisins pour suppri-

mer les instances de diffusion redondantes. Le protocole se base sur l'échange d'informations via des messages périodiques transmis entre voisins à deux sauts. Chaque nœud maintient deux tables de routage nommées R et NR, R contient la liste des voisins ayant déjà reçu les paquets de la diffusion, et NR contient tous les autres. Le nœud exécute donc une diffusion si la liste NR est non-vide.

Dans [128], la notion de Link Residual Lifetime est introduite par les auteurs. Ce paramètre représente le temps restant pendant lequel un lien de communication peut encore fournir un service de transmission satisfaisant. Les auteurs proposent donc d'utiliser cette nouvelle métrique pour créer une méthode d'adaptation proactive aux changements de topologie très fréquents dans les réseaux véhiculaires. Cette méthode consiste à utiliser des informations collectées sur deux couches différentes relatives au mouvement des véhicules et à la propagation radio. Ces informations servent à déterminer les meilleures voies de transmission possibles en fonction de la durée de vie des liens de communication.

Dans [129], les auteurs proposent un nouveau protocole de routage destiné à améliorer la qualité des transmissions et réduire les pertes de paquets dues à l'instabilité de la topologie des réseaux véhiculaires. La méthode consiste à sélectionner des itinéraires qui offrent un compromis intéressant entre un bon nombre de sauts et une bonne durée de vie des liens de communication. À cette fin, les auteurs proposent de formuler le problème sous la forme d'un problème de flux à coût minimal.

III.3.2 Protocoles réactifs

Les protocoles fondateurs

Dans [130], le protocole de routage DYMO (DYnamic MANET On demand) est présenté. L'objectif principal est de garantir des chemins de transmission dénués de boucles. DYMO fonctionne de manière réactive, il possède donc les deux phases principales de ce type de protocole. A savoir, la découverte de routes et la maintenance de ces dernières. La particularité de ce protocole réside dans le fait que lors de la première phase, les informations concernant tous les nœuds intermédiaires présents sur la route doivent être enregistrées.

In [131], les auteurs proposent une nouvelle méthode de sélection des sauts suivants pour les protocoles de routage réactifs. Les auteurs soulignent que la technique classique de redirection "Greedy" ne tient pas compte de la qualité des liens de communication formée lors de la sélection d'un nouveau saut. Pour

palier à ce problème, ils proposent donc d'utiliser la durée de vie de ces liens comme paramètre pour faciliter le choix des routes les plus durables et les plus fiables pour la transmission. Cette méthode est basée sur l'exploitation des informations fournies par le service GPS. afin que les nœuds puissent prédire les positions futures et les vitesses relatives de leurs voisins directs, ils utilisent l'échange de messages de contrôle périodiques. Chaque nœud a ainsi une vue claire de son voisinage à un saut et peut donc choisir le meilleur saut suivant en termes de qualité du lien de communication.

Quelques protocoles récents

Dans [132], les auteurs présentent CBQoS-Vanet, un nouveau protocole de routage adapté aux scénarios autoroutiers. Ce protocole est basé sur l'utilisation de deux techniques. Une technique de Clustering qui organise et optimise l'échange d'informations relatives à l'acheminement des paquets. Un algorithme inspiré des colonies d'abeilles, qui calcule les meilleurs itinéraires d'une source à une destination en fonction de critères de qualité de service (QoS) donnés. Les Clusters sont formés autour de chefs qui sont eux-mêmes élus en fonction de considérations de QoS. Les critères de QdS sont basés sur les deux catégories de métriques : métriques QoS et métriques de mobilité.

Dans [133], les auteurs se basent sur un système d'inondation de paquets qui réagit automatiquement à chaque variation de topologie tout en surmontant les obstacles lors de l'échange de données. Pour cela, des drones communément appelés véhicules aériens sans pilote (UAV, Unmanned Aerial Vehicles) sont utilisés. Le but est de sélectionner les routes fournissant une connectivité intéressante en termes de durée de vie en se basant sur le volume de trafic routier et le temps d'expiration de chaque chemin découvert.

Dans [134], une approche de routage réactive a été proposée pour VANETS. Cette approche vise à résoudre le problème des ruptures fréquentes des liens de communication causées par la grande mobilité des véhicules. Le protocole maintient de multiples routes entre la source et la destination pour la transmission des données. Le concept de temps de terminaison de connexion (CTT, Connection Terminaison Time) est utilisé pour sélectionner les deux trajectoires les plus disjointes. Le nœud source utilise d'abord le chemin principal pour la transmission de données et enregistre le chemin dérivé pour une utilisation ultérieure au cas où le chemin principal devient indisponible.

Dans [135], les auteurs se basent sur la méthode Greedy dans leur protocole de routage réactif pour les VANETs. Le but est de sélectionner les routes les plus efficaces en termes de consommation d'énergie entre les nœuds du réseau.

Le protocole estime ainsi l'énergie dont chaque route pourrait avoir besoin en additionnant les besoins énergétiques des nœuds intermédiaires qui la constituent, la route la plus optimale est donc ensuite choisie.

Dans [136], un protocole de routage réactif basé sur une amélioration de AODV (Ad-hoc On-demand Distance Vector) est présenté. Il exploite une méthode de réparation aléatoire de liens (Randomized Link Repair ,RLR) pour réduire la congestion dans le réseau qui est causée par les diffusions de paquets de requête de routes. Lorsqu'une rupture de lien se produit, les auteurs proposent d'utiliser plusieurs paquets de « réponse de route » à travers des chemins alternatifs.

Dans [137], une amélioration du protocole de routage AODV a été présentée. Cette méthode se base sur la réduction du nombre de paquets échangés nécessaires à son fonctionnement, ceci est fait dans le but de réduire la charge globale sur le réseau. En utilisant des paquets de données dupliqués au lieu des messages RREQ (Route REQuest) pour créer un chemin alternatif.

Dans [138], les auteurs proposent une méthode d'acheminement basée sur l'estimation de la vitesse de déplacement des véhicules afin d'assurer des transmissions fiables. Il s'agit ici d'utiliser la vitesse moyenne d'un groupe de véhicules sur une période donnée pour prévoir la vitesse individuelle des membres de ce groupe. Selon les auteurs, cette vitesse globale reflète le comportement actuel et futur des véhicules. Les auteurs proposent ensuite d'utiliser la méthode Fuzzy pour prédire la stabilité d'un lien de communication en utilisant la vitesse relative des nœuds. Puis, cela est couplé au choix des chemins de transmission comptant le moins de sauts pour la transmission des paquets.

III.3.3 Protocoles hybrides

Les protocoles fondateurs

Dans [139], une nouvelle méthode de diffusion adaptative est proposée. Dans DECA, les nœuds sont censés disposer d'informations concernant la densité locale de leur voisinage direct grâce à la transmission de messages périodiques. Ces informations sont ensuite utilisées par ces nœuds pour prendre des décisions autonomes sur les prochains sauts à privilégier. Un nœud souhaitant diffuser choisit donc le voisin qui est entouré par le plus de véhicules. C'est-à-dire le voisin ayant la meilleure densité locale. Les nœuds récepteurs vérifient alors s'ils ont été choisis pour retransmettre le paquet, si ce n'est pas le cas, ces nœuds stockent le paquet pour d'éventuelles retransmissions futures.

Dans [140], les auteurs proposent une solution de diffusion intelligente qui tient compte de la densité du voisinage afin de choisir le mode de transmission le plus approprié. L'idée de base est de proposer trois méthodes différentes pour les trois différents degrés de densité définis par les auteurs. Le schéma de persistance pour les voisinages considérés comme très denses. La retransmission à l'aide d'informations sur la direction des véhicules pour les voisinages moins denses. Enfin, la technique Carry and Forward pour les voisinages déconnectés (isolés).

Dans [141], les auteurs ont proposé un protocole de routage visant à offrir des Clusters stables afin de s'adapter aux caractéristiques particulières des réseaux véhiculaires (topologie dynamique, grande mobilité des nœuds, etc.). La particularité de ce protocole réside dans la phase de sélection des Cluster Heads, qui s'effectue en s'adaptant non seulement aux mouvements actuels des véhicules mais aussi à la prévision de leurs futures positions. Contrairement à ce qui se fait dans les techniques classiques de Clustering comme l'utilisation d'identificateurs de nœuds (IDs).

Quelques protocoles récents

Dans [142], les auteurs proposent d'utiliser la conscience situationnelle (CS), et un algorithme basé sur le système de colonie de fourmis pour développer un routage avec qualité de service multi-contraintes adapté pour les VANETs. Les routes potentielles sont évaluées et comparées suivant un certain nombre de contraintes liées à la qualité de service, les meilleures routes sont alors sélectionnées pour les transmissions.

Dans [143], un protocole de routage basé sur le Clustering est introduit. Les nœuds sont groupés en fonction des informations de mouvement telles que l'angle et la vitesse des véhicules au moyen de l'algorithme impérialiste compétitif (ICA, Imperialist Competitive Algorithme). Ensuite, le chef de cluster est sélectionné en utilisant l'algorithme de réseau de neurone à base radiale en fonction de la quantité de mémoire tampon libre et du nombre de transmissions attendues.

Dans [144], un nouveau protocole de routage hybride est proposé. Il exploite une version modifiée de l'algorithme K-Means et des réseaux de Hopfield continus. Les paramètres d'entrée de base de l'algorithme K-Means, tels que le nombre de Clusters et de leurs chefs, ne sont pas choisis au hasard, mais plutôt en résolvant le problème du Maximum Stable Set (MSS). L'affectation des véhicules aux Clusters est effectuée selon le modèle de fiabilité de liens en tant que métrique. Le chef de Cluster est sélectionné par une fonction de poids et selon la quantité de mémoire tampon libre ainsi que de la vitesse.

Dans [145], les méthodes Fuzzy et Cuckoo sont utilisées dans un protocole de routage hybride. Le but est de sélectionner les routes les plus stables possibles. La phase de découverte de route est réduite de manière intelligente grâce à l'approche Fuzzy, et ce en limitant les messages de requête de route initiaux. La méthode Cuckoo est quant à elle utilisée pour choisir les routes les plus optimales en termes de stabilité en calculant ce que les auteurs ont appelé Enhanced Fitness Function (EFF).

Dans [146], les auteurs proposent d'exploiter les informations GPS pour permettre aux nœuds faisant partie d'une route sélectionnée de partager leur position exacte. Ces informations sont récoltées par des unités nommées LVS qui sont installées dans les stations de base. Ces LVS sont également responsables de diffuser les informations vers les nœuds à portée afin que ces derniers puissent mettre à jour leurs tables de routage. Ce système permet d'éviter les cas de véhicules malicieux qui pourraient partager de fausses informations de position et ainsi dégrader les performances du réseau.

Dans [147], les auteurs ont utilisé l'ontologie et ont divisé le réseau en groupes (Clusters) selon leur position géographique. Chaque groupe est géré par un seul chef de Cluster et les deux types de routage (proactif et réactif) sont utilisés selon le type de communication (intra-Cluster et inter-Cluster).

III.4 Synthèse et analyse critique sur les protocoles de routage présentés

La Table III.1 présente une analyse critique des protocoles de routage présentés dans ce chapitre. Nous avons donné dans cette table pour chaque protocole un avantage principal et inconvénient principal.

Analyse critique sur les protocoles de routage présentés			
Protocole	**Type**	**Avantages**	**Inconvénients**

[90]	**Position**	**Le protocole garantit la fiabilité des transmissions Multicast en sélectionnant les meilleurs nœuds relais possibles pour cette tâche.**	**Les transmissions sont totalement dépendantes de certains nœuds désignés et peuvent donc être interrompues si ces nœuds deviennent indisponibles en raison de déconnexions par exemple.**
[91]	**Position**	**Les auteurs proposent 4 variantes pour la transmission de paquets, ce qui offre beaucoup de flexibilité**	**Certaines de ces variantes peuvent causer des boucles de routages et une haute consommation de bande passantes dans le cas ou plusieurs copies du même paquet existent simultanément.**
[92]	**Position**	**Le choix des routes de routage se fait de manière efficace et ne sollicite que les nœuds désignés**	**Puisque il est dépendant des informations de localisation, les performances du protocole peuvent varier suivant la fiabilité des GPS.**

ROVER [93]	**Position**	**Diffusions efficaces dans les scénarios à haute mobilité**	**Comme beaucoup de protocoles de routage utilisant la diffusion, il présente un haut risque d'Overhead.**
GPSR [94]	**Position**	**Protocole simple et peu coûteux en ressources**	**Peut conduire à un mauvais choix de routes, à des nœuds isolés et à de longs délais de transmission.**
GPCR [95]	**Position**	**Ne dépend pas des informations GPS pour fonctionner**	**Dépend en revanche fortement de la fiabilité des liens entre les nœuds, si certains de ces liens sont faibles ou inexistants (ce qui peut arriver), le protocole est moins performant.**
[96]	**Position**	**Fonctionnement simple et peu coûteux**	**Absence de mécanisme de choix d'un nouveau chef de Cluster en cas de défaillance de l'actuel CH.**

[97]	**Position**	**Le protocole fournit une vue globale de la topologie du réseau**	**Les prévisions de changements de vitesse futures dans un environnement aussi instable qu'une autoroute peuvent parfois conduire à des inexactitudes.**
[98]	**Position**	**Le protocole permet de résoudre efficacement les cas où un nœud est isolé et ne trouve pas de relais**	**Choisir le futur saut sur la base d'informations recueillies à partir des variations de voisinage antérieures ne reflète pas vraiment la nature très dynamique des VANETs**
A-STAR [99]	**Position**	**Bande passante très intéressante grâce au choix des intersections ayant une bonne connectivité**	**Délais de transmission élevés.**
GyTAR [100]	**Position**	**Taux de succès de transmission des paquets de service élevé**	**Délais de transmission élevés.**
UMB [101]	**Position**	**Offre une méthode fiable pour la diffusion en zones urbaines**	**Coût de déploiement très élevé car chaque intersection requiert l'installation de récepteurs spéciaux.**

[102]	**Position**	**Faible taux de perte de paquets**	**Les informations concernant les obstacles doivent arriver immédiatement, sinon le protocole est inefficace.**
GINS [103]	**Position**	**Nombre de sauts nécessaires réduit**	**Pas de mécanisme de retransmission.**
[104]	**Position**	**Faible taux de collisions pour les diffusions d'urgence**	**Inadapté aux réseaux à haute densité.**
M-GEDIR [105]	**Position**	**Sélection de routes durables.**	**Délais de transmission élevés.**
[106]	**Position**	**Diffusion des messages de sécurité efficace.**	**Fonctionne mal lorsque la distance entre les véhicules augmente.**
GRUV [107]	**Position**	**Principe de fonctionnement simple, ne génère pas beaucoup d'Overhead**	**Vulnérable car il dépend de certains nœuds désignés (non réactif aux défaillances).**
[108]	**Position**	**Les auteurs ont atteint leur objectif de réduire les ruptures de liens qui sont fréquentes dans les protocoles géographiques**	**La détermination de la position géographique dans ce protocole n'est pas toujours fiable (obstacles et perte de signal).**
POCA [109]	**Position**	**Adapté aux réseaux urbains avec beaucoup de trafic**	**Risque de congestion élevé.**

DGR [110], PDGR [111]	**Position**	**Peut offrir des temps de transmission relativement courts.**	**La direction de mouvement est relativement facile à prévoir, mais pas les changements futurs de la vitesse des véhicules, ce qui peut conduire à de mauvais choix de routes à long terme.**
[112]	**Position**	**Réduit la perte de paquets en groupant les nœuds destinataires pour le Multicasting.**	**Le nombre élevé des messages de contrôle échangés peut entraîner une augmentation de la charge du réseau.**
[113]	**Position**	**Permet des transmissions fiables et réduit la perte de paquets.**	**Le protocole dépend du paramètre de position final "V-Final" qui n'est pas toujours disponible.**
[114]	**Position**	**Transmissions stables et perte de paquets réduite**	**Ne prend pas en considération la direction des véhicules et les délais de transmission sont élevés.**

PDVR [115]	**Position**	**Permet des relais stables dans les environnements dégagés**	**Fonctionne mal dans les routes ayant des virages serrés ou carrés (90 degrés). Le protocole est donc mal adapté aux environnements urbains.**
HRV [116]	**Position**	**Faible taux de perte de paquets pour les transmissions Unicast**	**Dépendant des RSU qui sont coûteuses à déployer.**
[117]	**Topologie**	**Les routes choisies sont souvent fiables**	**Nécessite beaucoup de paquets périodiques**
BROACOMM [118]	**Topologie**	**Adapté à la gestion des situations d'urgence (accidents ou événements dangereux)**	**C'est un parti pris des auteurs plus qu'une limitation, mais le protocole se concentre sur les transmissions de sécurité critiques par rapport aux messages de service.**
[119]	**Topologie**	**Faible charge sur le réseau**	**Délais de transmission élevés**
[120]	**Topologie**	**Délais de bout en bout réduits.**	**Débit assez faible.**
[122]	**Topologie**	**Liens de communication stables.**	**Délais de bout en bout élevés.**
[123]	**Topologie**	**Liens de communication stables.**	**Temps de sélection de routes très élevé.**

IDVR [124]	**Topologie**	**Débit élevé.**	**Dépendant des ICHs, utilisable uniquement pour un type spécifique de topologie.**
[125]	**Topologie**	**S'adapte bien aux vitesse élevées en termes de PLR**	**Délais de bout en bout élevés.**
[126]	**Topologie**	**Sûreté des transmissions augmentée**	**Nécessite un nombre élevé de paquets échangés.**
[127]	**Position**	**Charge sur le réseau réduite**	**Non adapté aux diffusions d'urgence car les délais de transmissions sont trop longs.**
[128]	**Topologie**	**Le protocole permet des transmissions fiables avec un faible taux de perte de paquets**	**Les temps de transmission peuvent être longs et la collecte de données sur deux couches peut entraîner une lourde charge sur le réseau.**
[129]	**Topologie**	**Le protocole augmente le débit et réduit la perte de paquets.**	**Le nombre de calculs nécessaires au fonctionnement du protocole le rend relativement gourmand en termes de messages de contrôle.**

DYMO [130]	**Topologie**	**Courts délais de transmissions**	**L'enregistrement des informations concernant tout les nœuds intermédiaires de chaque route augmente la charge sur le réseau.**
[131]	**Position**	**Améliore la méthode de transmission "Greedy" en termes de qualité des liens de communication sélectionnés**	**Le choix de nouveaux relais basé sur chaque saut ne reflète pas une vision globale de la topologie du réseau.**
[132]	**Topologie**	**Adapté aux réseaux à forte mobilité.**	**Nécessite l'échange d'un nombre important de paquets.**
[133]	**Topologie**	**Connectivité du réseau élevée.**	**Les drones autonomes sont coûteux à déployer.**
[134]	**Topologie**	**Fiabilité des transmissions élevée.**	**Le maintient de plusieurs routes par paquet augmente la charge.**
[135]	**Topologie**	**Routes optimales en termes d'énergie.**	**Nécessite un nombre élevé de paquets échangés.**
[136]	**Topologie**	**Faible congestion dans le réseau.**	**Débit faible.**
[137]	**Topologie**	**Faible charge sur le réseau**	**Taux de paquets transmis relativement faible**

[138]	**Topologie**	**L'utilisation de la méthode Fuzzy permet d'estimer de manière relativement précise la durée de vie d'un lien de communication.**	**La vitesse individuelle d'un véhicule ne reflète pas toujours la vitesse moyenne du groupe auquel il appartient.**
DECA [139]	**Hybride**	**Permet d'atteindre plus de nœuds avec des diffusions.**	**Choisir le meilleur prochain saut ajoute un retard supplémentaire à la transmission des messages diffusés.**
[140]	**Hybride**	**Le protocole est très polyvalent grâce à ses trois modes de transmission différents**	**Si le réseau oscille entre deux états de densité différents dans un court laps de temps, cela peut conduire à des performances sous-optimales en raison de changements rapides dans le mode de transmission.**

[141]	**Hybride**	**Le protocole s'adapte bien aux vitesses élevées des véhicules**	**Pour être opérationnel, le protocole nécessite de nombreux messages de contrôle et prédictions pour l'organisation des Clusters, ce qui augmente la charge sur le réseau.**
[142]	**Hybride**	**Adapté aux topologies hautement dynamiques.**	**Délais de transmission élevés.**
[143]	**Hybride**	**Faible taux de perte de paquets.**	**Très gourmand en ressources.**
[144]	**Hybride**	**Adapté aux réseaux à haute vitesse.**	**Charge élevée sur le réseau.**
[145]	**Hybride**	**Communications stables et routes durables.**	**Génère beaucoup d'Overhead.**
[146]	**Hybride**	**Permet la sélection de routes sûres.**	**Coûteux à déployer.**
[147]	**Hybride**	**Faible taux de perte de paquets**	**Initiation des transmission coûteuse en temps.**

TABLE III.1: Analyse critique des protocoles de routage

III.5 Conclusion

Nous avons vu dans ce chapitre les principaux protocoles de routage présents dans la littérature et dédiés aux réseaux véhiculaires. Nous pouvons constater que tous les types de routages sont assez bien représentés, mais il existe un manque qui a attiré notre attention et orienté nos travaux : Il y a très peu de

protocoles dédiés exclusivement aux environnements autoroutiers. C'est-à-dire des protocoles conçus pour fonctionner dans des conditions de vitesse extrêmes avec des véhicules circulant en ligne droite la plupart du temps. Et il en existe encore moins qui sont basés sur le concept de stabilité des liens de communication. Cette notion est prioritaire dans le contexte des autoroutes, vu la grande mobilité des véhicules qui y circulent.

Nous présentons dans le prochain chapitre notre contribution à l'accès au canal dans la norme 802.11p, avec des méthodes visant à améliorer la qualité de service pour ce standard.

Chapitre IV

Contrôle d'accès avec qualité de service

IV.1 Introduction

Dans le deuxième chapitre, nous avons passé en revue les principaux travaux visant à améliorer les protocoles d'accès au canal déjà existants, et ceux proposant de nouveaux protocoles originaux. Dans ce chapitre, nous allons présenter notre contribution à la couche MAC, qui est un ensemble d'améliorations du protocole d'accès au canal 1609.4 présent dans la pile de protocoles WAVE de la IEEE.

IV.2 Problématique et Motivation

Au cours des dernières années, plusieurs efforts de normalisation ont été déployés par la IEEE en association avec la communauté scientifique dans le but de concevoir des réseaux de véhicules offrant des performances satisfaisantes pour les applications critiques sans négliger les applications d'information et de divertissement. Les protocoles MAC sont particulièrement difficiles à concevoir pour les VANETs, ceci est dû à la nature très instable de ce type de réseaux par rapport aux réseaux Ad Hoc classiques (vitesse élevée des nœuds, changements de position qui entraînent des déconnexions et des pertes de signal, etc.). Nous avons toutefois remarqué que les travaux disponibles dans la littérature avaient tendance à se concentrer sur un type d'applications et négliger l'autre. Il s'agit soit d'améliorer les transmissions de sécurité critiques et négliger les transmissions utilitaires soit le contraire. Nous avons donc tenu à proposer des améliorations qui puissent permettre de ne négliger aucun type de transmissions. Dans notre thèse, nous proposons des mécanismes visant à améliorer la qualité de service et, dans l'ensemble, les performances du protocole d'accès au canal 1609.4 inclus dans la pile de protocoles WAVE [2]. Ces mécanismes

sont présentés sous la forme d'un algorithme d'équité qui, comme son nom l'indique, vise à répartir les chances d'accès au canal de manière plus juste entre les nœuds, d'un algorithme d'adaptation de l'intervalle SCH aux besoins du réseau et d'un mécanisme d'urgence qui vise à garantir l'acheminement des paquets de sécurité critiques en cas d'événements dangereux sur la route.

IV.3 Algorithme d'équité

L'une des principales caractéristiques des réseaux véhiculaires est la grande mobilité des nœuds qui induit inévitablement des turbulences et des pertes de signal en raison de la vitesse élevée des véhicules. Par conséquent, les VANETs sont plus susceptibles d'avoir des problèmes liés à l'équité entre les nœuds du réseau parce qu'un véhicule plus rapide aura plus de difficulté à gagner l'accès aléatoire au canal pour acheminer ses paquets jusqu'à leur destination.

Algorithm 1 Algorithme d'équité

```
//Algorithme exécuté par chaque nœud du réseau dès le début de l'intervalle SYNC
//N est l'approximation du nombre de nœuds dans le réseau, communiquée par le nœud calculateur
//Wait : Temps attendu par un nœud depuis le dernier accès réussi au canal (en secondes)
// ω : le seuil auquel le temps d'attente d'un nœud est comparé, pour décider si ce temps d'attente est suffisamment élevé pour favoriser le nœud
//Backoffcur : Valeur de Backoff courante
//Backoffinit : Valeur de Backoff initiale

if Transmission réussie then
   Wait = 0
end if
chaque seconde :
incrémenter "Wait"
if  Wait > ω et Backoffcur > Backoffinit/3  then
   // réajuster les paramètres pour favoriser ce nœud

   Backoffcur = (Backoffcur + N)/wait
end if
```

Pour pallier à ce problème d'équité, nous proposons l'Algorithme 1. Ce dernier est basé sur un système de temps d'attente. Chaque véhicule tient un compteur "wait" qui enregistre la période pendant laquelle ce dernier n'a pas pu accéder au canal, ce compteur est réinitialisé après chaque transmission

réussie du véhicule. L'objectif est d'éviter les cas où une partie de la population du réseau monopolise la bande passante et qu'une autre partie se trouve ainsi négligée. Dès qu'un certain seuil "ω" est dépassé, le véhicule en question apporte des modifications à la valeur de son Backoff. L'objectif de ces modifications est de favoriser le véhicule et de l'aider à avoir une meilleure possibilité d'accéder au canal lorsqu'il essaye à nouveau et donc améliorer l'équité dans le réseau. Notez (comme vous pouvez le voir dans l'Equation IV.2) que cette diminution est proportionnelle au temps d'attente "wait", c'est-à-dire que plus le temps d'attente est important, plus les paramètres de contention du nœud seront réduits et, par conséquent, le nœud sera plus favorisé pour ses prochaines tentatives. Il est également important de noter que lors de l'élaboration de l'Algorithme 1, nous avons veillé à ce qu'il n'influe pas sur la transmission des messages prioritaires, c'est-à-dire que les véhicules munis de paquets urgents à transmettre auront toujours un accès plus rapide au canal. La valeur de la fenêtre de contention augmente aussi proportionnellement au nombre de véhicules dans le réseau, car le risque de collisions augmente avec la croissance de la population. Il fallait donc éviter d'avoir des valeurs trop faibles pour Backoffcur lorsque le réseau est encombré. C'est pourquoi, nous avons aussi comme paramètre dans l'Equation IV.2 le nombre de nœuds dans le réseau N.

Ainsi, les nœuds qui ont atteint le temps d'attente "ω" vérifient leurs valeurs de Backoff. Sachant que la valeur de "ω" a été déterminée, comme pour d'autres paramètres empiriques utilisés dans nos travaux, par les centaines de sessions de simulation que nous avons effectuées. Sa valeur optimale a pour but d'avantager les véhicules ayant accumulé un retard, tout en maintenant la priorité des véhicules ayant des paquets urgents à transmettre. Pour ce faire, nous avons surveillé le taux de réussite des transmissions de paquets critiques tout en ajustant la valeur du paramètre "ω". Par exemple, une valeur de "ω" inférieure à 5 secondes aurait eu pour effet d'inclure plus de véhicules dans l'algorithme d'équité, et donc d'augmenter le risque de collisions.

Nous savons que dans la norme 802.11p, la valeur du Backoff est calculée selon la formule de [148] :

$$Backoff = Random(0, CW) * SlotTime \tag{IV.1}$$

Où Random est un nombre généré aléatoirement dans l'intervalle [0, CW] et SlotTime est une valeur générée par la couche PHY.

Notre première idée était d'utiliser cette valeur de Backoff pour que le nœud puisse extraire le nombre aléatoire initialement généré et si ce nombre généré s'avérait être élevé et très proche de la borne supérieure de l'intervalle [0, CW], cela aurait pu en partie expliquer pourquoi le nœud a des difficultés à accéder au canal. Mais cette méthode ne permet pas de connaître concrètement le nombre de fois que le nœud a trouvé le canal libre mais n'a pas pu transmettre

à cause d'une valeur de Backoff non nulle. Nous avons donc décidé d'opter pour une deuxième méthode. Cette dernière consiste à comparer la valeur initiale de Backoff d'un nœud générée par l'Equation IV.1, et la valeur de Backoff courante de ce dernier, afin de déterminer s'il faut aider ce nœud à accéder au canal. La norme stipule qu'un nœud qui souhaite transmettre des données mais qui se trouve dans la période de Backoff doit écouter le canal et décrémenter cette valeur chaque fois que le canal est trouvé libre, et le nœud pourra transmettre lorsque la valeur sera égale à 0. En comparant la valeur de Backoff courante avec la valeur initiale, nous pouvons savoir combien de fois le nœud a eu l'opportunité de la décrémenter et combien de fois le nœud devra trouver que le canal est libre avant d'être autorisé à transmettre. Si le nœud constate que la valeur courante de son backoff est toujours proche de sa valeur initiale et que la période d'attente a atteint le seuil "ω", cela signifie que non seulement il vient de passer un temps anormalement long à attendre, mais qu'il est encore loin d'être en mesure de transmettre dans un futur proche. Pour notre cas, nous aidons un tel nœud si la valeur courante du Backoff est supérieure à 1/3 de sa valeur initial. Cette condition est due au fait que nous avons constaté par simulation que lorsque la valeur courante est inférieure à 1/3 du Backoff, le nœud parvient généralement à accéder au canal dans un délai raisonnable et n'a donc pas besoin d'être favorisé. Alors, si la valeur du Backoff du nœud vérifie cette condition, il doit faire une modification sur ses paramètres de contention selon l'Equation IV.2 suivante afin d'améliorer sa probabilité de transmission :

$$Backoffcur = (Backoffcur + N)/wait \tag{IV.2}$$

IV.4 Algorithme d'adaptation de l'intervalle SCH

Selon la norme IEEE 802.11p [12], le temps sur le canal est divisé en deux sous-intervalles appelés CCH et SCH, et la durée de ces deux intervalles est fixée à 50 ms chacun. CCH est destiné à la transmission de messages de sécurité critiques ou de messages périodiques, tandis que pendant l'intervalle SCH, les nœuds peuvent échanger des messages de service non critiques. Évidemment, ce paramétrage statique a été étudié pour garantir une bonne performance globale pour le plus grand nombre de scénarios possibles, mais elle n'est pas adaptée à la nature très dynamique des VANETs et aux changements très fréquents dans le comportement de ses nœuds (changement de direction, de vitesse ou réaction à des événements inattendus sur la route). Pour pallier à ce problème, plusieurs solutions proposent d'adapter ces intervalles en augmentant l'intervalle CCH au détriment de l'intervalle SCH. Ceci permet d'optimiser la transmission des

messages de sécurité critiques en négligeant les transmissions utilitaires ou de service. Cependant, quand il n'y a pas de danger ou d'accident sur la route, les transmissions utilitaires doivent être optimisées pour améliorer les performances du réseau [149]. Motivés par cette étude, nous avons étudié par simulation le taux d'échecs des transmissions en fonction de la vitesse maximale des véhicules avec différentes valeurs de l'intervalle SCH. Les résultats présentés dans le graphe de la figure IV.1 montrent que l'augmentation de l'intervalle SCH réduit considérablement le taux d'échecs et l'augmentation de ce dernier avec l'augmentation de la vitesse des véhicules.

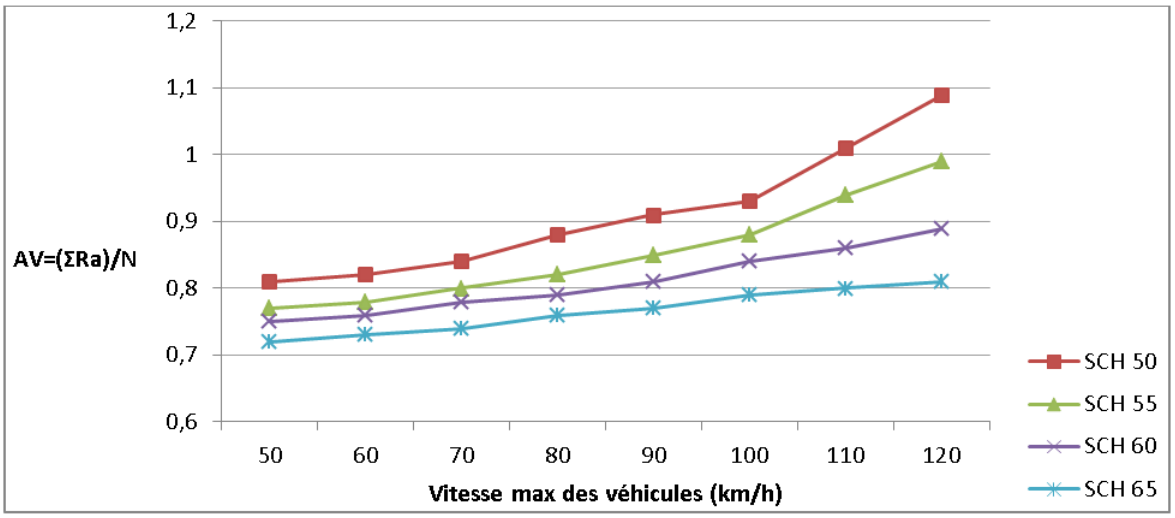

FIGURE IV.1 – «AV» vs. Vitesse pour différents intervalles SCH

Suite à ces simulations, nous proposons ici l'Algorithme 2 qui gère le segment périodique de 100 ms et ajuste dynamiquement les valeurs des intervalles CCH et SCH en s'adaptant au comportement et aux besoins des nœuds du réseau.

Nous avions conscience lors de l'élaboration de l'Algorithme 2 de l'importance de l'intervalle CCH vu qu'il sert à transmettre des messages de sécurité critiques, c'est pourquoi, nous proposons également un mécanisme d'urgence (présenté dans la section IV.5) pour garantir la transmission des messages de sécurité dans de bonnes conditions en cas d'événements urgents ou dangereux sur la route. Nous avons également pris en considération la limite de réduction de CCH dans les conditions normales où il n'y a pas d'accidents ou d'événement dangereux, comme expliqué à la fin de cette section.

Algorithm 2 Algorithme d'adaptation de l'intervalle SCH

begin
//Su : Nombre de transmissions réussies
//Fa : Nombre de transmissions échouées
//N est le nombre estimé de nœuds dans le réseau
//Ra est le rapport entre les transmissions échouées et réussies au sein d'un nœud
//Av est la valeur moyenne calculée de tous les ratios du réseau

Tant que non finSCH

if Transmission réussie **then**
  incrémenter Su
else
  incrémenter Fa
end if

finSCH = True

//Au début de l'intervalle CCH
Calcul du ratio : $Ra = Fa/Su$
Envoyer la valeur de Ra via le champ de paquet spécial par unicast au CN
Su=0, Fa=0
if n'a pas reçu d'ACK de la part du CN **then**
  retransmettre le paquet spécial
end if

//exécutée par le CN dans la seconde moitié de l'intervalle CCH

Calcul du nombre estimé de nœuds N (en utilisant le nombre de paquets reçus contenant des valeurs de Ra)
Calcul de la valeur moyenne du rapport : Av = $(\sum Ra)/N)$
Calcul de la nouvelle valeur de l'intervalle SCH :

$$newSCH = \frac{\beta + (AV * N * \beta)}{N * 10^{-1}} * 10^{-3} Seconds$$

$NewCCH = (100 - newSCH) * 10^{-3} Seconds$
Diffuser par Broadcast la nouvelle valeur de SCH vers les autres nœuds
end

L'idée principale de l'Algorithme 2 est de permettre à certains nœuds désignés pour collecter périodiquement des informations relatives à l'activité sur le réseau afin de calculer les valeurs optimales pour l'intervalle SCH en se basant sur ces données récoltées, puis de déduire la durée de l'intervalle CCH. Ces nœuds désignés sont appelés nœuds calculateurs (Computer Nodes, CN). Nous supposons dans notre travail que les nœuds du réseau sont dotés de mécanismes permettant d'élire ces nœuds calculateurs (semblable à ce qu'on peut trouver dans les réseaux avec Clusters par exemple).

La première phase est la phase de collecte d'informations, au cours de laquelle chaque nœud tient deux compteurs pendant l'intervalle SCH : Su (pour "Successful") qui est incrémenté à chaque fois que le nœud a transmis avec succès un paquet , et Fa (pour "Failed") qui est incrémenté chaque fois qu'un nœud a un paquet à envoyer mais qu'il a échoué lors de sa tentative d'accès.

Pendant l'intervalle CCH, chaque nœud calcule Ra (pour "Ratio"), qui est le résultat de la division :

$$Ra = Fa/Su \tag{IV.3}$$

Après ce calcul, le résultat sera envoyé par Unicast au nœud calculateur (CN) à l'aide d'un nouveau champ que nous avons ajouté au paquet MAC pour stocker la valeur de Ra. Et puisqu'il s'agit d'un Unicast, le nœud émetteur attendra un ACK, s'il ne le reçoit pas, le paquet sera envoyé à nouveau.

Au cours de la deuxième phase, le calcul de la nouvelle valeur de l'intervalle SCH et de la nouvelle valeur de CCH est effectué. Après avoir reçu les valeurs de Ra, le nœud calculateur calcule la valeur moyenne de tous les ratios reçus AV **comme suit :**

$$AV = (\sum Ra)/N) \tag{IV.4}$$

Ensuite, le nœud calculateur fixe la nouvelle valeur optimale pour l'intervalle SCH, qui augmente proportionnellement avec le taux d'échec de la transmission des paquets de service, selon la formule IV.5 présentée dans l'Algorithme 2

$$NewSCH = \frac{\beta + (AV * N * \beta)}{N * 10^{-1}} * 10^{-3} \tag{IV.5}$$

La valeur de β **a été ajustée suite aux simulations que nous avons effectuées. Le but est de trouver un équilibre en augmentant l'intervalle SCH autant que possible sans endommager les transmissions de paquets de sécurité critiques. Ceci a été fait en surveillant le taux d'échec des paquets envoyés pendant l'intervalle CCH tout en réglant le paramètre** β**. Cela signifie que la formule a été ajustée en fonction des résultats des centaines de simulations que nous avons réalisées. Cette version finale est donc celle qui a donné les meilleures**

performances pour les scénarios présentés. Le paramètre β a été introduit afin de rendre la formule plus flexible, nous avons trouvé que pour notre réseau la valeur optimale pour ce paramètre est 6, parce que la valeur du paramètre AV variait entre 0,81 et 1,09. Comme nous avons trouvé que dans des conditions normales, la diminution de la durée de l'intervalle CCH ne commence à nuire à l'efficacité des transmissions de paquets de sécurité critiques qu'à partir de 35 ms, c'est-à-dire que lorsque l'intervalle CCH est supérieur à cette valeur, aucun impact significatif n'est à signaler. Ces résultats sont présentés dans les figures IV.1 et IV.2. Le graphe de la figure IV.1 montre les valeurs de l'Intervalle SCH calculées par le CN en fonction de la variation des valeurs de AV et le graphe de la figure IV.2 illustre l'impact de la réduction de l'intervalle CCH, dans des conditions normales où il n'y a pas d'accidents de la route ou d'événements dangereux à signaler, sur l'efficacité des transmissions de paquets de sécurité critiques.

Cela signifie que β nous permettrait d'ajuster la formule pour un autre réseau où la valeur de AV serait très différente de celle de notre réseau, c'est-à-dire, obtenir un intervalle SCH suffisamment long pour répondre aux besoins du réseau sans trop réduire l'intervalle CCH au point de nuire à la transmission des paquets de sécurité critiques.

Notre formule IV.5 permet donc à l'intervalle SCH d'augmenter avec l'augmentation de la valeur du paramètre AV, parce que l'augmentation de AV signifie une augmentation du ratio Ra et donc une augmentation du taux d'échec Fa par rapport à Su. Ceci est dans le but de répondre aux nouveaux besoins du réseau en offrant ainsi plus de temps aux nœuds pour l'échange de messages de service non-critiques.

Après le calcul de la valeur de l'intervalle SCH, le nœud calculateur va calculer aussi la nouvelle valeur de l'intervalle CCH et diffuser ces nouvelles valeurs, de sorte que tous les autres nœuds du réseau puissent les utiliser pendant le prochain segment de 100 ms.

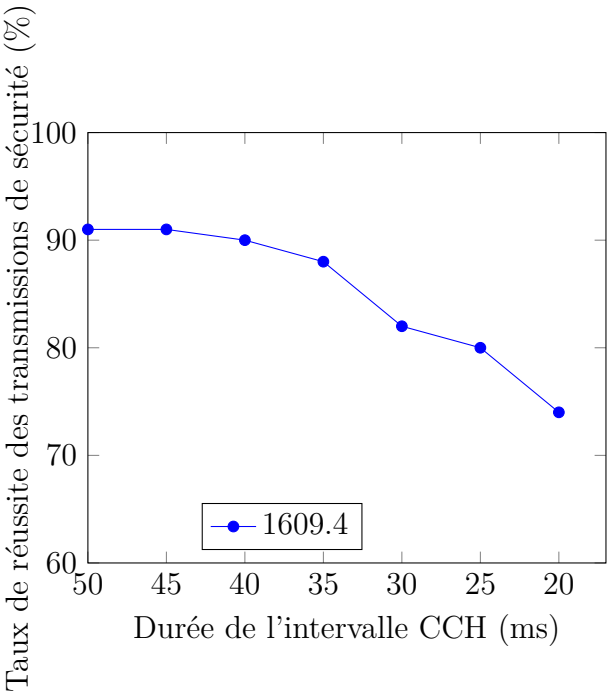

FIGURE IV.2 – Taux de réussite des transmissions de sécurité Vs Intervalle CCH

IV.5 Mécanisme d'urgence

Nous présentons ici notre mécanisme d'urgence, qui vise à gérer les situations où la transmission de messages de sécurité critiques sur l'intervalle CCH est cruciale et peut avoir d'énormes conséquences sur la vie des conducteurs et des piétons. Lorsqu'un événement significatif se produit (accident, danger sur la route ou toute autre situation pouvant être considérée comme dangereuse), le mécanisme d'urgence est déclenché. Le nœud qui a détecté l'événement transmet par Unicast un paquet de haute priorité (HP) au CN. Le paquet HP est un nouveau type de paquet prioritaire que nous avons ajouté, dont les paramètres de contention sont fixés à zéro, il n'est affecté par aucune procédure de Backoff ou de temps d'attente. Si le nœud ne reçoit pas d'ACK dans les 10 ms, il renvoie à nouveau le message. Ensuite, le nœud calculateur fait entrer le réseau dans une phase d'urgence en diffusant un paquet de même priorité (HP) afin d'informer tous les autres nœuds de la procédure. Chaque nœud qui a reçu cette diffusion devra envoyer un ACK au CN afin de spécifier qu'il est prêt à exécuter le mécanisme d'urgence (le CN a accès aux données concernant le nombre exact de nœuds dans le réseau grâce à la procédure d'échange d'informations présentée précédemment).

L'objectif de cette phase est d'avertir tous les nœuds du réseau qu'un danger

est présent sur la route, et que les transmissions ne doivent être dédiées qu'à l'échange de messages de sécurité critiques. Le segment initial de 100 ms, qui est à la base divisé en intervalles CCH et SCH, sera ainsi transformé en un segment "CCH-Only" de 200 ms renouvelable, comme le montre l'Organigramme IV.3. La responsabilité tombe alors sur le nœud calculateur pour gérer le reste du mécanisme. Le CN attendra les ACKs de tous les nœuds du réseau, entre temps, il continuera à envoyer des émissions HP pour renouveler le segment de 200 ms, parce qu'il y a encore des véhicules qui n'ont pas été informés du danger.

De leur côté, les autres nœuds ont également un rôle à jouer. Si un nœud reçoit un paquet qui n'est pas du type "sécurité critique", cela signifie qu'il provient d'un nœud qui vient d'entrer dans le réseau et qui n'est donc pas informé du mécanisme d'urgence. Un message informatif sera transmis au CN afin de l'informer que la phase d'urgence doit se poursuivre et que, par conséquent, le segment de 200 ms doit être renouvelé. Une fois que le CN a reçu tous les ACKs (le CN connaît la population actuelle du réseau, il compare donc le nombre d'ACKs reçus à cette population), il déclenche un délai d'attente de 5 secondes, pendant lesquelles il renouvellera automatiquement les segments de 200 ms, s'il ne reçoit aucun message l'informant que de nouveaux membres non-informés ont intégré le réseau pendant cette période. Il pourra alors diffuser un message indiquant aux nœuds que la phase d'urgence est terminée. Notez que les nœuds retourneront au segment classique de 100 ms (avec 50 ms pour les intervalles CCH et SCH respectivement) pour la première réutilisation, et que le mécanisme présenté dans la partie précédente (calcul de la durée de SCH optimale) sera activé à partir du segment suivant.

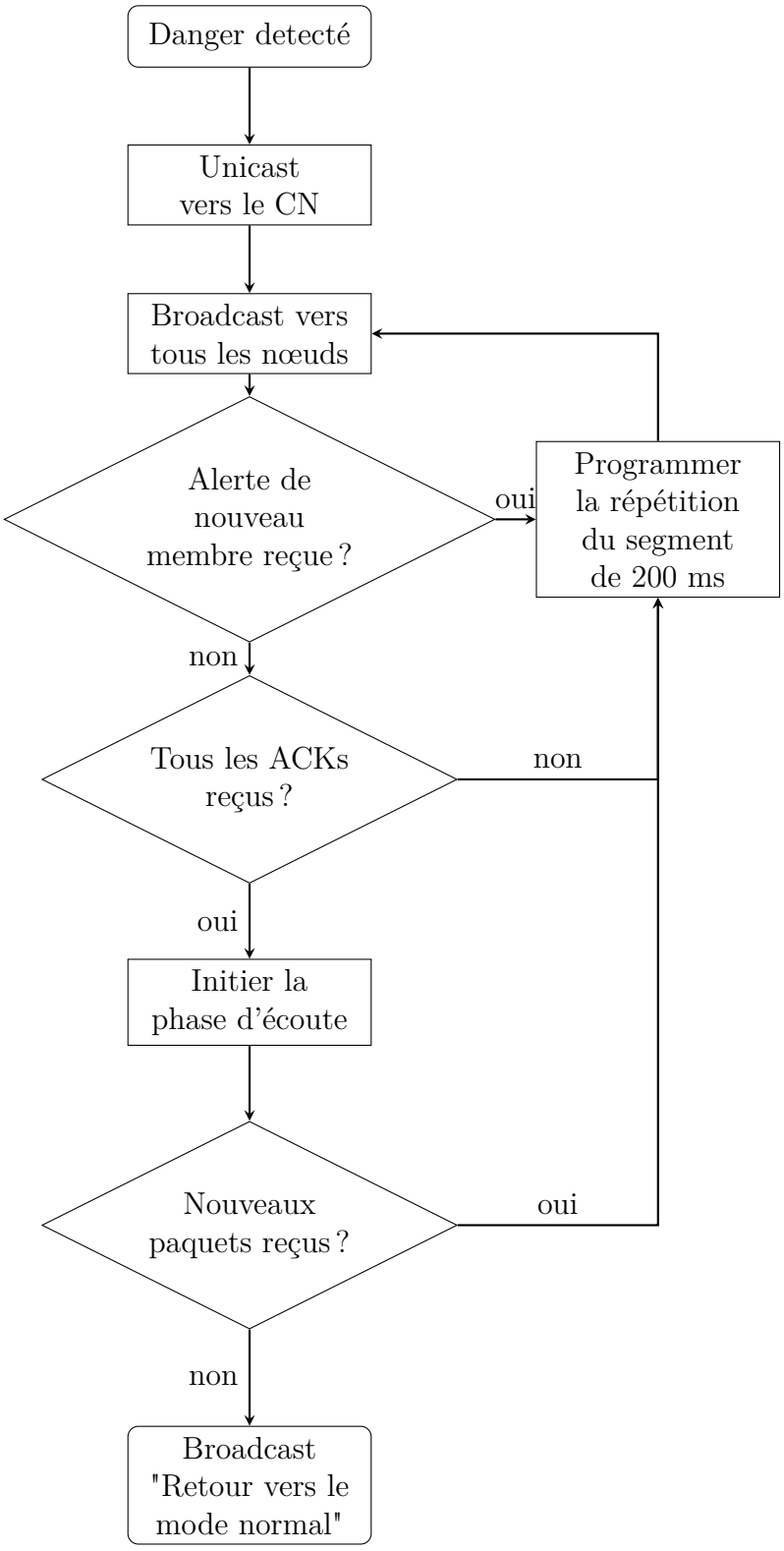

FIGURE IV.3 – Le mécanisme d'urgence

IV.6 Simulations et résultats

Pour montrer l'apport de notre solution pour l'accès au canal dans les réseaux véhiculaires, nous avons évalué et comparé les performances de notre solution par simulation avec celles du protocole MAC d'origine 1609.4 et AAA.

Dans cette section, nous présentons l'environnement et les paramètres de simulation puis les résultats de simulations obtenus lors de la comparaison des performances de nos mécanismes proposés avec les performances du protocole MAC original 1609.4 présent dans la norme IEEE 802.11p ainsi que l'amélioration AAA proposée dans [70]. Cette dernière est présentée dans le chapitre II, et est une amélioration du protocole 1609.4 qui utilise des intervalles CCH/SCH dynamiques afin d'améliorer sa qualité de service et réduire la perte de paquets, c'est pourquoi nous l'avons choisie pour la comparaison.

IV.6.1 Environnement et paramètres de simulation

Pour montrer les améliorations de la qualité de service, nous avons opté pour trois métriques : le débit, le taux de perte de paquets (PLR) et le taux de transmissions réussies pour les messages de sécurité critique.

Paramètre	Valeur
Durée SCH	50ms
Durée CCH	50ms
CWMin	15
CWMax	1023
Canaux SCH	4
Canaux CCH	1
Durée de la garde	4ms
Durée SIFS	32 μs
Durée SlotTime	13 μs

TABLE IV.1 – Paramètres de simulation

L'environnement de simulation est Omnet++ avec l'utilisation du Framework "Veins", et la mobilité des véhicules est gérée par SUMO. La carte choisie est une carte urbaine de 5 km de long et 5 km de large avec des intersections et des ronds-points. Les véhicules se déplacent le long de chemins générés aléatoirement par SUMO. 13 unités de bord de route ont été utilisées pour couvrir la surface de la carte. Trois scénarios pour trois limites de vitesse différentes ont été exécutés : 50 km/h (14 m/s), 80 km/h (22 m/s) et 120 km/h (33.5 m/s), ceci dans le but de montrer l'impact de la variation de vitesse [150], [151] sur les améliorations que nous proposons, le protocole original 1609.4 et

le protocole AAA. Nous supposons ici que les véhicules du réseau sont à portée (pas de nœuds isolés) et que le réseau est en situation de surcharge, c'est-à-dire que la file d'attente d'envoi de chaque nœud du réseau est toujours non vide. La durée de simulation est de 120 secondes et les paramètres choisis sont indiqués dans le tableau IV.1. Les valeurs choisies pour les paramètres ω et β sont respectivement $\omega = 5$, $\beta = 6$.

IV.6.2 Analyse des résultats de simulation

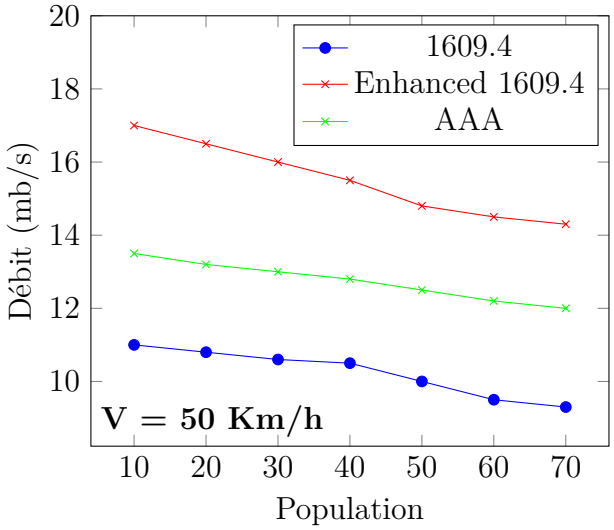

FIGURE IV.4 – Débit Vs Population (V=50 Km/h)

Les figures IV.4, IV.5 et IV.6 montrent le débit (en mb/s) dans le réseau en fonction de la population (ou le nombre de nœuds) pour comparer nos méthodes proposées avec le protocole original et AAA.

Nous pouvons constater une amélioration significative du débit dans les trois scénarios, variant de 36% à 81% de plus pour notre solution proposée par rapport au protocole original, et jusqu'à 25% par rapport à AAA. Cela s'explique par une utilisation plus optimale du temps sur le réseau grâce au système d'intervalle SCH adaptatif proposé. Lorsque les nœuds ont besoin de plus de temps pour envoyer des paquets de service non critiques, le protocole s'adapte automatiquement à cette demande pour le prochain segment de temps de 100 ms, ce qui donne un meilleur débit et une meilleure qualité de service sur le réseau.

AAA surpasse le protocole de base en termes de débit grâce aux intervalles CCH/SCH dynamiques implémentés par les auteurs. Cependant, les graphiques montrent que notre contribution garantit de meilleures performances, ceci pourrait être dû au fait que dans AAA, la durée optimale de l'intervalle

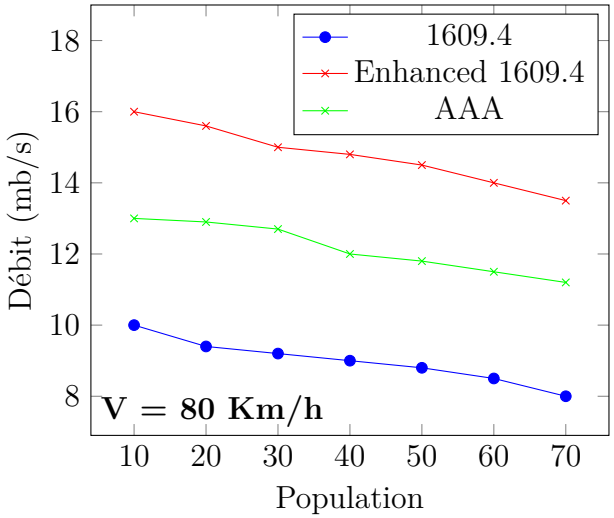

FIGURE IV.5 – Débit Vs Population (V=80 Km/h)

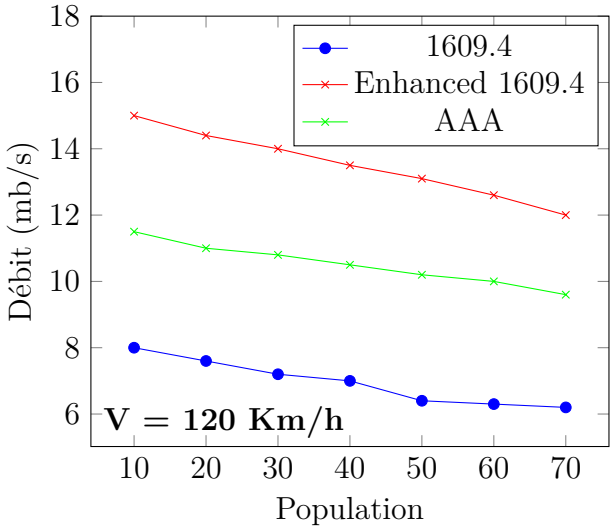

FIGURE IV.6 – Débit Vs Population (V=120 Km/h)

CCH est basée sur un calcul utilisant le nombre moyen de BSMs envoyés par un nœud ainsi que le délai moyen des BSMs reçus par ce dernier. Or, nous savons que dans les VANETs, la vitesse des véhicules varie beaucoup et donc les délais de transmission des paquets également, car la distance entre ces véhicules varie aussi rapidement. Les délais de transmission des paquets ne sont donc pas un paramètre assez fiable sur lequel se baser pour calculer les intervalles, notamment, lorsqu'on sait que la RSU exécute l'algorithme AAA toutes les secondes (UTC), ce qui représente l'équivalant de 10 intervalles SYNC dans 1609.4. La mise à jour des nouveaux intervalles calculés n'est donc pas faite assez fréquemment pour s'adapter à la nature très mobile des nœuds.

Il est également important de noter que lorsque la vitesse maximale des véhicules augmente, nous constatons une diminution des performances concernant le débit. Nous savons que l'un des principaux problèmes dans les VANETs vient de leurs soucis de stabilité, car la vitesse élevée de leurs nœuds encourage les déconnexions et les pertes de signal. Cette instabilité peut causer des pertes de paquets qui augmentent avec l'augmentation de cette vitesse, et donc causer une diminution du débit global du réseau. Nous pouvons également observer que cette baisse de performances liée à la vitesse est plus faible pour notre solution par rapport aux deux autres, avec une diminution de seulement 13% alors qu'elle atteint 40% pour le protocole original et 22% pour AAA. Nous pouvons donc conclure que notre proposition répond mieux à l'instabilité du réseau en termes de débit.

En effet, nous savons que dans les VANETs, l'augmentation de la vitesse des véhicules affecte la qualité des communications. Mais pour limiter la dégradation de la qualité de service au niveau de l'accès au canal (couche MAC) causée par cette augmentation de la vitesse des véhicules, il n'y a pas de paramètre explicite dans le protocole 1609.4, qui est directement lié à cette variable de vitesse, donc, nous avons agi sur deux axes :

— **Tout d'abord, nous nous sommes intéressés à l'équité au niveau de l'accès au canal. Partant du fait que les véhicules les plus rapides peuvent avoir moins de chances d'accéder au canal, puisque les véhicules ayant des déconnexions fréquentes en raison de leur vitesse auront naturellement plus de mal à écouter le canal et donc à décrémenter la valeur de leur Backoff. C'est pourquoi, nous avons proposé notre premier algorithme qui favorise les nœuds qui attendent depuis longtemps. Pour ce faire, nous avons surveillé le temps d'attente, le paramètre $wait$, et quand il atteint un certain seuil, le paramètre ω, et que la valeur courante du Backoff est supérieure au tiers de sa valeur initiale, nous réduisons la valeur courante du Backoff en fonction de la valeur de $wait$ et de la densité du réseau, N, pour réduire**

le risque de collisions.

— **Deuxièmement, nous avons évalué l'incidence de l'augmentation de l'intervalle SCH sur le taux de perte de paquets causé par l'augmentation de la vitesse des véhicules et les résultats montrent clairement que ce taux augmente moins rapidement avec un intervalle SCH plus grand, comme le montre la figure IV.1. Sur la base de ces résultats, nous avons proposé l'Algorithme 2 où nous adaptons l'intervalle SCH en fonction du taux d'échecs moyen, le paramètre Av et de la densité du réseau, le paramètre N. Cela signifie que plus la vitesse d'un nœud est élevée, plus la valeur de son paramètre Ra est élevée. Par conséquent, plus il y a de nœuds rapides dans le réseau, plus la valeur du paramètre AV sera élevée. La durée de l'intervalle SCH sera ainsi allongée et les nœuds rapides auront plus de chance de réduire leur taux d'échecs pour le segment de temps suivant.**

En résumé, nos algorithmes réagissent à tout ce qui augmente le taux de défaillance, et comme la plupart de ces défaillances sont causées par les vitesses élevées des nœuds, la dégradation des performances est moins importante comparé au protocole original et à AAA car dans les segments de temps suivants, les nœuds rapides auront plus de chance de transmettre. C'est pourquoi, nous avons utilisé le terme "adaptation", parce que nos algorithmes apportent des changements à certaines de leurs valeurs lorsque les véhicules augmentent leur vitesse.

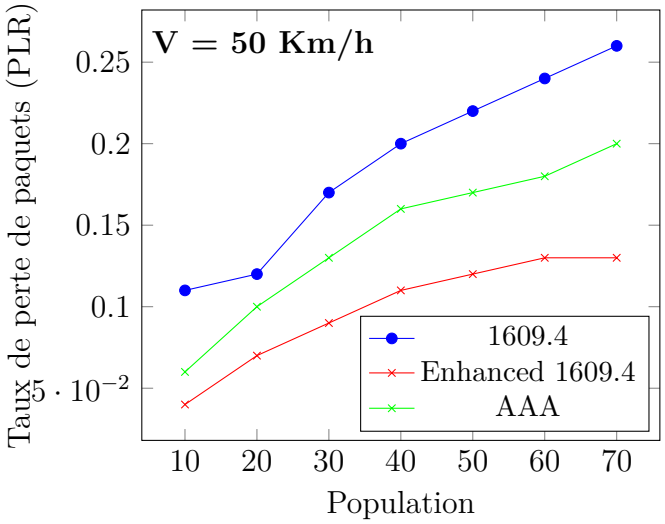

FIGURE IV.7 – Taux de perte de paquets Vs Population (V=50 Km/h)

Les figures IV.7, IV.8 et IV.9 mettent en évidence une autre métrique importante de la qualité de service, le taux de perte de paquets (PLR), qui est le rapport entre le nombre de paquets perdus par tous les nœuds et le nombre total de paquets envoyés. Nous pouvons constater que les mécanismes que nous

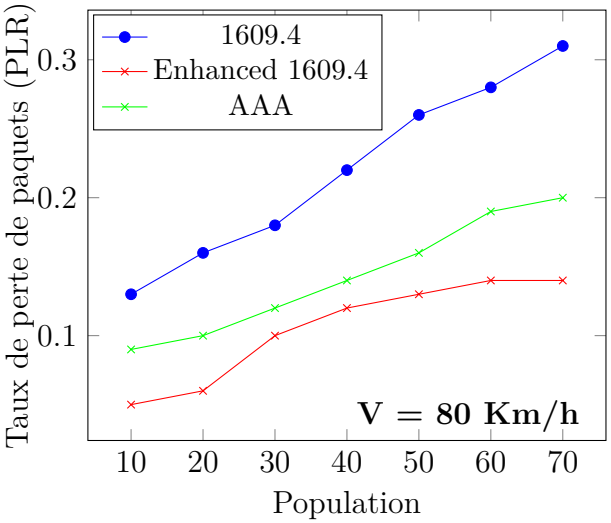

FIGURE IV.8 – Taux de perte de paquets Vs Population (V=80 Km/h)

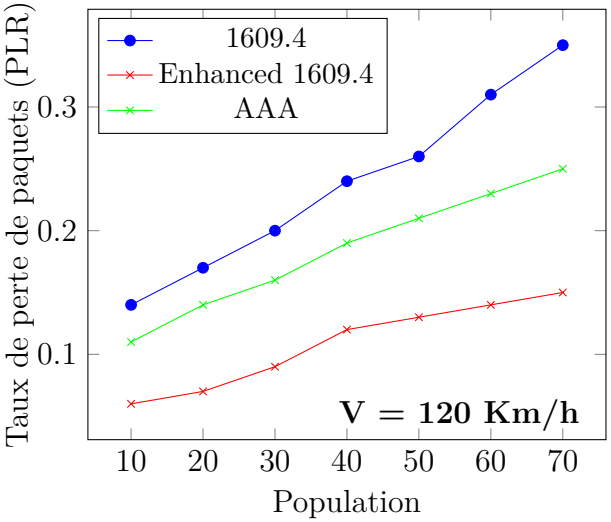

FIGURE IV.9 – Taux de perte de paquets Vs Population (V=120 Km/h)

proposons permettent une diminution significative du PLR sur le réseau par rapport au protocole original 1609.4 et à AAA, avec une amélioration allant de 48% à 72% par rapport au protocole original, et jusqu'à 55% par rapport à AAA selon les scénarios. En effet, le fait que l'intervalle SCH s'adapte dynamiquement aux besoins du réseau réduit la perte de paquets car les nœuds se verront allouer plus de temps pour envoyer leurs données durant chaque segment de 100 ms. Cette amélioration a un impact direct sur la qualité de service et notamment sur le transfert des paquets média, comme les fichiers audio, car nous savons que la qualité d'un signal audio, par exemple, est fortement impactée par la perte de paquets.

Il est intéressant de noter l'augmentation du PLR lorsque la vitesse maximale est augmentée. Cette baisse de performances est due aux mêmes raisons que celles mentionnées ci-dessus : la stabilité du signal dans le réseau est diminuée par l'augmentation de la vitesse. Ainsi, les transmissions sont moins fiables (paquets perdus parce que le récepteur s'est déconnecté, ou que l'émetteur a eu accès au canal mais s'est déconnecté juste après, etc). Nous notons également que cette baisse de performances peut aller jusqu'à 53% pour le protocole original (entre les scénarios de vitesse 50 km/h et 120 km/h) et 37% en moyenne pour AAA alors qu'elle ne dépasse pas 15% pour notre solution. Nous pouvons donc dire qu'elle s'adapte mieux aux variations de vitesse en termes de perte de paquets, grâce notamment à l'algorithme d'équité et à l'adaptation de la valeur de l'intervalle SCH qui crée plus d'équilibre entre les nœuds et donne plus de temps pour le transfert des paquets de service, et permet donc de réduire le taux global de perte de paquets.

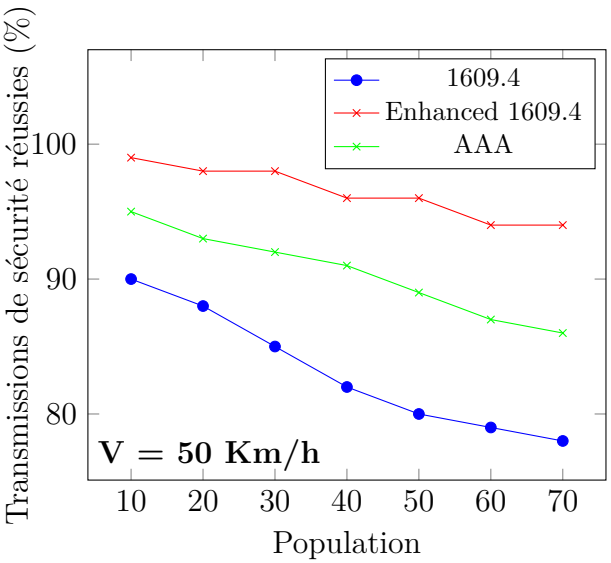

FIGURE IV.10 – Taux de réussites des paquets de sécurité Vs Population (V=50 Km/h)

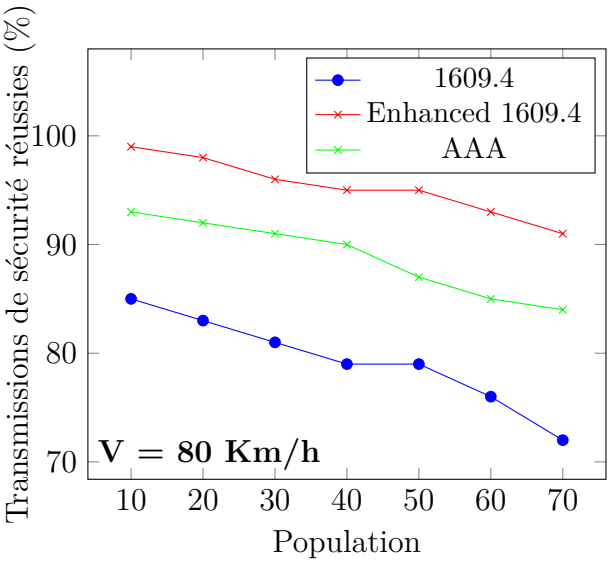

FIGURE IV.11 – Taux de réussites des paquets de sécurité Vs Population (V=80 Km/h)

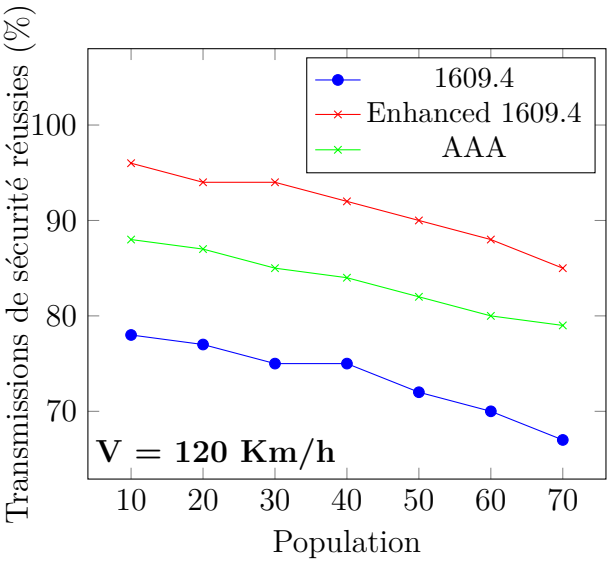

FIGURE IV.12 – Taux de réussites des paquets de sécurité Vs Population (V=120 Km/h)

Dans les figures IV.10, IV.11 et IV.12, nous avons montré l'impact de notre mécanisme d'urgence sur l'efficacité de la transmission des messages de sécurité critiques, et comparé ses performances avec le protocole original 1609.4 et AAA. Pour ce faire, un accident impliquant deux véhicules est déclenché à un moment aléatoire de la simulation. Les résultats présentés dans les figures sont une moyenne calculée après 50 itérations de la simulation pour chaque scénario.

La figure IV.10 montre une nette amélioration du taux de transmissions réussies pour les paquets de sécurité critiques pour notre mécanisme par rapport au protocole de base et à AAA. Ce pourcentage reflète le nombre de paquets de sécurité qui arrivent à destination par rapport au nombre total de paquets de sécurité envoyés. Cela s'explique assez facilement : notre mécanisme d'urgence reflète le parti pris que lorsqu'un événement potentiellement dangereux se produit sur la route, l'envoi de paquets de service non critiques devient secondaire et même handicapant car il prend du temps d'accès sur le canal de communication. Le fait de déclencher ce mécanisme d'urgence permet donc de concentrer toutes les communications sur la transmission des messages de sécurité critiques, et donc d'augmenter le taux de réussite pour ce type de paquets. L'amélioration va d'une différence de 12% (par rapport au protocole original) à 30% pour certains scénarios, et 10% par rapport à AAA. Les chiffres montrent également que l'augmentation de la vitesse des véhicules a un impact négatif sur le taux de réussite des transmissions critiques pour notre solution, le protocole original et AAA, mais comme pour les métriques précédentes, cette perte de performance due à la forte mobilité est plus faible pour notre solution.

IV.6.3 Récapitulatif des résultats de simulation

Pour donner une vue globale sur les résultats de simulation présentés précédemment, nous les résumons dans deux tableaux. Le tableau IV.2 présente une comparaison théorique et expérimentale de notre solution avec les deux protocoles simulés, 1609.4 et AAA. Le tableau IV.3 présente les taux moyens de dégradation des trois métriques de performances analysées par simulation des trois protocoles avec l'augmentation de la vitesse.

TABLE IV.2: Comparaison des protocoles

Protocole	Intervalles dynamiques	Paramètres de contention dynamiques	dépendant des RSUs	Garantit l'équité	Multi-canaux	Méthode utilisée	Fréquence de mise à jour des intervalles	Débit moyen	PLR moyen	Taux de réussites des paquets de sécurité
Original 1609.4	**Non**	**Non**	**Non**	**Non**	**Oui**	/	/	**8,86 mb/s**	**0,22**	**78,62%**
AAA	**Oui**	**Non**	**Oui**	**Non**	**Oui**	**Calculer les intervalles optimaux en fonction du nombre de paquets transmis et de leurs délais**	**Chaque seconde (UTC)**	**11,27 mb/s**	**0,17**	**85,62%**
Enhanced 1609.4	**Oui**	**Oui**	**Non**	**Oui**	**Oui**	**Calculer les intervalles optimaux en fonction des taux d'échec des paquets**	**Chaque 100 ms**	**13,97 mb/s**	**0,10**	**94,33%**

TABLE IV.3: Perte de performance moyenne entre 50km/h et 120km/h

	Débit	**PLR**	**Transmissions de sécurité réussies**
Original 1609.4	**39,19%**	**44.50%**	**14.67%**
AAA	**21.83%**	**37.21%**	**9.59%**
Enhanced 1609.4	**12.58%**	**15.05%**	**5.35%**

IV.7 Conclusion

Dans ce chapitre, nous avons présenté trois mécanismes pour améliorer la qualité de service dans le protocole MAC IEEE 1609.4. Nous avons proposé un algorithme d'équité, un algorithme d'intervalle SCH dynamique pour assurer une gestion plus adaptative des intervalles d'accès au canal, et un mécanisme d'urgence axé sur la transmission de messages critiques en cas d'événements dangereux. L'idée générale étant de garantir de bonnes performances lorsque le réseau est dans des conditions normales, tout en étant réactif et adaptatif à tout événement nécessitant la transmission de paquets de sécurité critiques. Les comparaisons avec le protocole original 1609.4 et le protocole AAA (Advanced Activity-Aware Multi-Channel Operations 1609.4) montrent que nos méthodes peuvent améliorer le débit, réduire le taux de perte de paquets et augmenter le pourcentage de paquets de sécurité critiques transmis lors d'événements dangereux. Dans le prochain chapitre, nous présentons notre contribution au routage dans les réseaux véhiculaires, avec un nouveau protocole basé sur le principe de stabilité des liens de communication.

Chapitre V

Routage avec qualité de service

V.1 Introduction

En raison des caractéristiques particulières des réseaux de véhicules (topologie dynamique, grande mobilité des nœuds, etc.), le routage dans les VANETs présente de nombreux défis. Plusieurs contributions ont été proposées dans la littérature au cours des deux dernières décennies, mais les protocoles de routage dédiés au trafic routier urbain ne sont pas nécessairement adaptés aux scénarios autoroutiers (différence de densité de véhicules, différence de vitesse maximale autorisée, etc.) Il est donc difficile de créer un protocole de routage adapté aux deux types de scénarios.

Nous avons remarqué que dans les scénarios autoroutiers, il est important de prendre en compte les particularités de la mobilité des véhicules car elles ont un impact sur la stabilité des liens de communication. Par conséquent, nous avons conçu un protocole de routage basé sur la stabilité des liens (LSRP, Link Stability Based Routing Protocol) [3] qui favorise la sélection de routes qui sont les plus susceptibles de maintenir leur structure et leur régularité en termes de distance entre les nœuds relais qui les composent. Nous avons agi en exploitant les voies de circulation définies sur les autoroutes. Ces voies sont généralement caractérisées par des vitesses de circulation différentes, et les véhicules circulant sur la même voie ont tendance à avoir des vitesses plus proches et des distances stables entre eux. Sur la base de ces constats, nous pouvons dire que le choix de chemins de routage ayant un grand nombre de véhicules circulant sur la même voie garantit non seulement des communications plus stables entre les nœuds dans le moment présent, mais aussi des liens potentiellement plus stables dans le futur proche. Par conséquent, nous avons proposé dans notre protocole de combiner ce concept avec les différences de vitesse des véhicules et la distance entre ces derniers pour la prédiction de la durée de vie des liens de communication afin de sélectionner les chemins de routage les plus optimaux

en termes de stabilité de ces liens, comme le montrent les résultats présentés dans ce chapitre.

V.2 Problématique et Motivation

Comme nous pouvons le constater dans notre étude de la littérature (chapitre 3), il y a un nombre limité de travaux récents qui abordent le problème du routage dans les autoroutes et encore moins qui prennent en compte la stabilité des liens de communication. Cependant, nous savons que les véhicules circulant sur une autoroute ont tendance à se déplacer à grande vitesse et par conséquent, beaucoup de liens de transmission entre ces véhicules sont très éphémères. Sur la base de ces remarques, nous présentons dans ce chapitre, notre protocole de routage basé sur la stabilité des liens, qui est dédié exclusivement à une utilisation en scénario d'autoroute. Vu que notre protocole vise à garantir des communications stables avec un minimum de rupture de liens, il est particulièrement adapté aux communications sensibles à la perte de paquets et aux déconnexions, comme le partage de média audio et vidéo avec qualité de service.

L'idée principale est assez simple, nous savons que dans une autoroute il y a plusieurs voies dédiées à la circulation des véhicules, et qu'en général, les véhicules souhaitant augmenter leur vitesse ont tendance à se diriger vers les voies de gauche (ou de droite, selon les pays). Un autre fait intéressant est que lorsqu'un véhicule modifie sa vitesse mais reste sur la même voie, les véhicules qui sont derrière lui ont tendance à adapter leur vitesse en conséquence, soit en accélérant soit en ralentissant. Ainsi, la distance entre les véhicules reste raisonnable. L'objectif de notre protocole est donc d'exploiter ces faits afin de maintenir des liens de communication aussi stables que possible, en privilégiant les routes qui présentent un compromis intéressant entre la durée de vie des liens et le nombre de véhicules consécutifs (voisins directs) qui se trouvent sur la même voie.

V.3 Collecte et échange d'information

On suppose ici que tous les véhicules du réseau sont équipés d'un système de positionnement global (GPS). Par conséquent, ils ont connaissance de leur propre position ainsi que celle de leurs voisins grâce à l'échange de messages périodiques. De plus, nous supposons que le réseau dispose d'un service de localisation qui permet aux nœuds de connaître la position géographique exacte de la destination de leurs paquets.

Notre protocole commence dans un premier temps par construire une vue globale du réseau en termes de position des nœuds et des liens de communication qui les relient. Pour ce faire, nous commençons par la découverte des voisins à un et deux sauts en utilisant des messages de type HELLO. Ensuite, pour le partage des informations (vitesse, direction, voisins, etc.) avec une charge minimale sur le réseau, nous optons pour une solution hiérarchique au lieu d'inonder le réseau avec des diffusions de contrôle contenant les données. Ainsi, dans notre solution, nous formons des Clusters et désignons des chefs de Clusters (CH) qui sont responsables de la collecte de ces données et de leur distribution. Ces chefs de Clusters doivent avoir un profil idéal pour être sélectionnés, c'est-à-dire que leur vitesse moyenne doit être proche de celle des véhicules formant le groupe auquel ils appartiennent, leur position doit aussi être proche du centre de ce groupe. Cependant, le chef de Cluster pourrait quitter la zone de couverture du réseau, laissant ainsi les nœuds au sein du Cluster sans distributeur pour leur fournir des mises à jour relatives à la topologie du réseau. Pour résoudre ce problème, nous utilisons une architecture à double chef de Cluster, où, au lieu d'en élire un seul, nous en choisissons deux, le principal et le secondaire qui remplace le premier s'il quitte la zone du Cluster.

Pour être un chef de Cluster, le nœud en question doit être dans une position centrale par rapport à la topologie du groupe, de sorte qu'il puisse atteindre tous les nœuds de son Cluster afin de partager avec ces derniers les informations nécessaires au fonctionnement du protocole. De plus, le chef de Cluster doit avoir une faible mobilité relative par rapport aux autres véhicules du réseau, car plus cette mobilité relative est faible, plus il est probable que le CH reste dans sa position centrale pendant une période plus longue et reste donc à la portée des autres nœuds du réseau. L'utilisation d'un deuxième CH a pour but de palier à une éventuelle défaillance du chef de Cluster principal (déconnexion, accident ou départ du réseau). Dans ce cas, le deuxième CH prendra alors les commandes et la procédure d'élection sera renouvelée pour trouver un autre chef de Cluster et ainsi remplacer celui qui n'est plus opérationnel. Le chef de cluster secondaire est également remplacé en cas de défaillance. Cette méthode de sélection de deux chefs de Cluster afin de distribuer l'information dans le réseau est présentée dans [152].

V.4 Définition des concepts

Avant de décrire le fonctionnement de notre protocole LSRP, nous présentons certains concepts que nous avons utilisés :

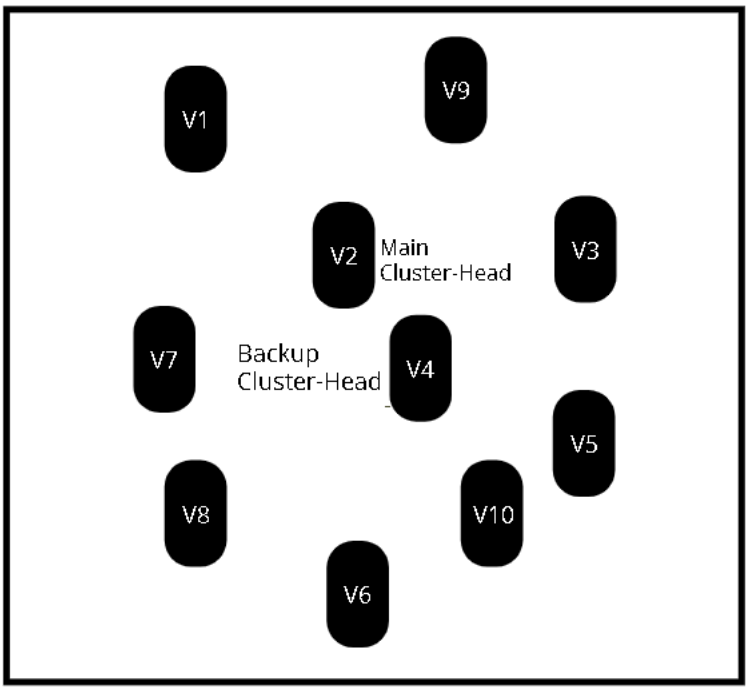

FIGURE V.1 – L'architecture à double chefs de Cluster

Nous utilisons dans notre protocole les concepts de Link Stability (stabilité des liens) et de Link Lifetime (durée de vie des liens). La stabilité d'un lien est la fiabilité de la liaison de communication à l'heure actuelle et dans un futur proche. Cela signifie qu'un lien est considéré comme stable s'il permet la transmission de données à une distance/vitesse idéale entre les nœuds qui le composent et s'il n'est pas susceptible de se rompre dans un avenir proche et d'entraver ainsi la transmission. La durée de vie d'un lien de communication représente le temps restant jusqu'à son expiration, c'est-à-dire la durée pendant laquelle la liaison restera fonctionnelle dans le futur. Ce paramètre est généralement calculé en utilisant la vitesse relative des nœuds, leur position relative ainsi que la portée de la transmission.

La durée de vie d'un lien dans notre travail actuel est notée LLT, ce paramètre dépend de la différence entre les vitesses des deux nœuds constituant ce lien, la distance qui les sépare et le rayon de la portée de communication. La durée de vie d'un lien de communication l est donc :

$$LLT_l = (R - d)/\Delta V \tag{V.1}$$

Où R est le rayon de la portée de communication, d est la distance entre les deux nœuds qui constituent le lien l et ΔV est la différence de vitesse entre ces deux nœuds. Les informations de vitesse et de position des véhicules sont partagées périodiquement par les chefs de Cluster en utilisant la méthode décrite précédemment.

V.5 Routage basé sur la stabilité des liens (LSRP)

Il est connu que le routage proactif n'est pas forcément adapté à la nature dynamique des VANETs, en particulier dans les scénarios à grande vitesse, en raison des changements fréquents de topologie. Cependant, nous avons remarqué que malgré le fait qu'il ne soit pas vraiment optimal d'établir de manière proactive des routes complètes allant du nœud source au nœud destinataire, il est possible et même intéressant d'établir proactivement des routes sur un certain nombre limité de sauts afin d'éviter le problème du maximum local et le risque de sélectionner des routes qui ne sont pas optimales en termes de stabilité et d'avoir des cas de nœuds relais complètement isolés.

Sur la base de ces constats, nous avons opté pour la conception d'un protocole de routage hybride qui est proactif sur un segment de dix (10) sauts et réactif lorsqu'il s'agit de choisir le futur segment de dix (10) sauts. Le choix d'utiliser des segments de 10 sauts pour le routage a été basé sur nos simulations sur des scénarios d'autoroute. Nous avons trouvé que ce nombre offrait le meilleur compromis, il est suffisamment élevé pour appliquer les principes de la stabilité des liens de communication, mais pas trop élevé au point d'affecter les transmissions de façon négative. C'est-à-dire que le temps de propagation entre le premier nœud du segment (position 1) et le dernier (position 10) est suffisamment court pour que les changements de topologie qui se déroulent pendant ce temps de propagation ne soient pas si importants qu'ils gênent les communications.

Un nœud source S souhaitant transmettre des paquets doit trouver tous les différents segments de routes à 10 sauts menant au nœud destinataire D, puis, il calcule le score de chacun de ces segments en fonction des informations relatives à la topologie du réseau. Le nœud S choisit le segment de 10 sauts ayant le score le plus élevé. Le score du segment est calculé sur la base de la formule :

$$SS(segmentscore) = ST + C \tag{V.2}$$

Pour être sélectionné, un segment X à 10 sauts doit avoir le score le plus élevé, ce score représente deux facteurs : le premier, noté ST dans l'Equation V.2, représente la qualité du segment en fonction de la durée de vie de ses dix liens de communication, et le second, noté C, est la plus longue séquence de

véhicules consécutifs (voisins directs) qui circulent sur la même voie. De façon précise, les deux paramètres peuvent être détaillés comme suit :

— Le paramètre ST d'un segment X représente le nombre de "bons" liens dans ce segment. Tout d'abord, les $LLTs$ des dix liens de communication du segment X sont calculés en utilisant l'Equation V.1 pour estimer la qualité de chacun d'entre eux, puis, le paramètre ST est incrémenté chaque fois qu'un "bon" lien est trouvé sur le segment X. Pour déterminer si un $n^{ième}$ lien l sur le segment X est considéré comme bon, on compare sa durée de vie $LLT_{l,n}$ au temps nécessaire pour qu'un paquet puisse être envoyé sur les n premiers liens du segment. Par conséquent, le $n^{ième}$ lien l a une bonne durée de vie s'il remplit la condition de l'équation V.3

$$LLT_{l,n} > TP * n \tag{V.3}$$

$LLT_{l,n}$ étant la durée de vie du lien l qui se trouve à la position n sur le segment X, et TP le temps de propagation moyen entre deux nœuds. Le but de cette condition est de vérifier si la durée de vie du lien l est suffisamment grande pour permettre aux paquets envoyés par S de passer par tous les liens qui précèdent le lien l avant que celui-ci n'expire ($TP * n$ est la somme des temps de propagation sur les liens allant de l'émetteur S au lien l).

— Le paramètre C est le nombre maximum de nœuds consécutifs qui se déplacent sur la même voie dans le segment tel qu'il est illustré sur la figure V.2. Ces nœuds ont plus de chances de conserver des vitesses proches à l'avenir car, comme expliqué précédemment, les changements de vitesse ont tendance à se produire en groupe lorsque les véhicules se trouvent sur la même voie, car ils essaient d'adapter leur vitesse à celle du véhicule qui les précède (si un véhicule ralentit ou accélère, les véhicules qui le suivent ont de fortes chances de faire de même pour maintenir une distance raisonnable).

Pour plus d'explications, la figure V.3 illustre un exemple de calcul du score de deux segments de 10 sauts. Évidemment, plus le score d'un segment est élevé, plus il a de chances d'être sélectionné pour le routage des données, car plus les paramètres ST et C sont élevés, plus les liens de communication sont considérés comme stables.

L'Algorithme 3 présente les étapes de sélection du segment optimal de 10 sauts pour acheminer les données en fonction de la stabilité des liens.

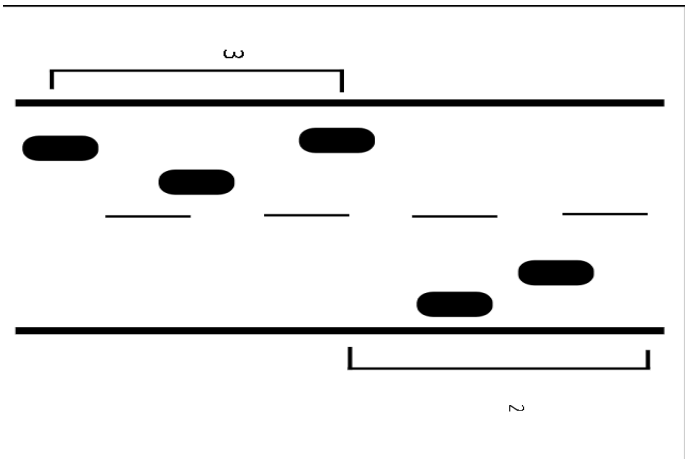

FIGURE V.2 – Véhicules consécutifs circulant sur la même voie

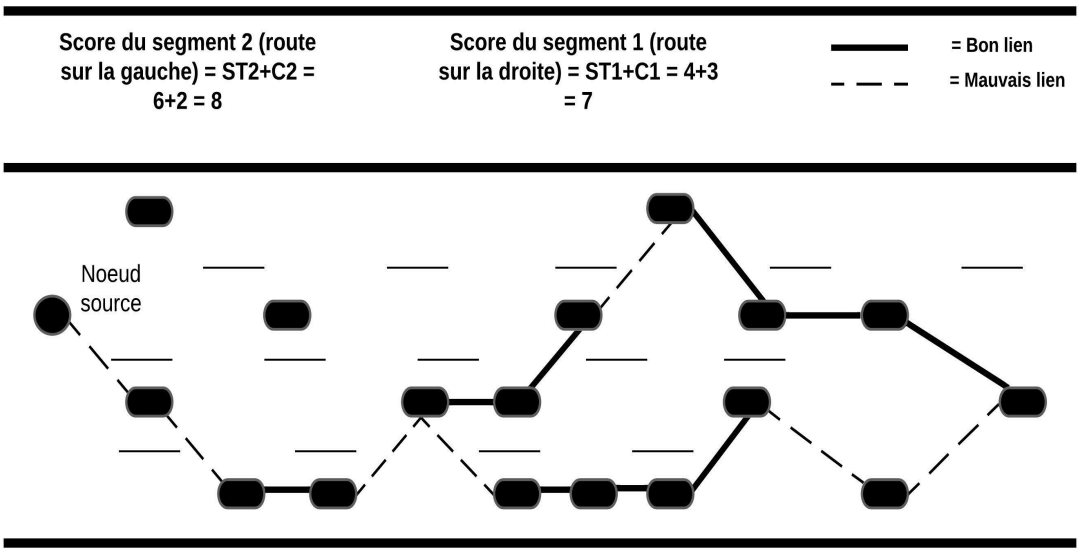

FIGURE V.3 – Exemple illustratif du calcul de score des segments

Algorithm 3 Algorithme LSRP

//Algorithme exécuté par chaque nœud ayant un paquet à envoyer
// C : Nombre maximal de véhicules consécutifs circulant sur la même voie (pour un segment X)
//ST : Représente la qualité du segment en fonction de la durée de vie des liens de communication qui le composent
//SS : Score de segment
//LLT : Durée de vie du lien

Le nœud S a un paquet à envoyer à la destination D :
Vérifier les chemins disponibles vers D
if Pas de routes complètes de S à D et pas de routes partielles **then**
  Le nœud S effectue un Carry-and-Forward pendant 5 secondes
end if
if Routes partielles trouvées **then**
  Le nœud S cible le nœud intermédiaire (le plus proche de D) et le marque comme nouveau nœud destinataire tout en mettant l'adresse du nœud D dans l'en-tête de données.
end if
if Routes complètes trouvées **then**
  le nœud S sélectionne un segment composé des 10 premiers sauts sur chacune de ces routes et effectue une comparaison de leurs scores.
end if
Pour chaque segment X :
Calculer C= Nombre maximal de véhicules consécutifs sur la même voie
Calculer ST= Nombre de bons liens sur un segment X
Calculer SS=ST+C
Le nœud S sélectionne ensuite le meilleur segment en comparant les scores de segment

Comment déterminer si deux nœuds se trouvent sur la même voie ?

Pour déterminer si deux véhicules se déplacent sur la même voie de l'autoroute, nous avons utilisé une méthode simple inspirée de celle présentée dans [153]. Les véhicules sont équipés du service GPS et de services de localisation et ont donc à leur disposition des cartes des routes sur lesquelles ils se déplacent. L'idée est d'utiliser ces cartes de la manière suivante (se référer à la figure V.4 pour illustration). Le véhicule 1 trace une ligne virtuelle L1 parallèle à la ligne formée par le côté de la route, tandis que le véhicule 2 trace une ligne virtuelle L2 qui est perpendiculaire à ce même côté de la route. Une troisième ligne est tracée entre les véhicules 1 et 2 et le croisement des trois lignes virtuelles forme ainsi un triangle carré. En utilisant l'angle α et le calcul de la tangente, nous pouvons déterminer si le véhicule 2 est suffisamment éloigné horizontalement

du véhicule 1 pour déduire qu'il se trouve sur une autre voie (on suppose ici que la largeur de la route est connue à l'avance). Nous savons que :

$$tan(\alpha) = d/b$$

donc

$$d = tan(\alpha) * b$$

Il nous suffit donc de calculer la valeur de d et de déterminer si elle est suffisamment grande (par rapport à la largeur de la route) pour affirmer que les véhicules 1 et 2 ne se trouvent pas sur la même voie.

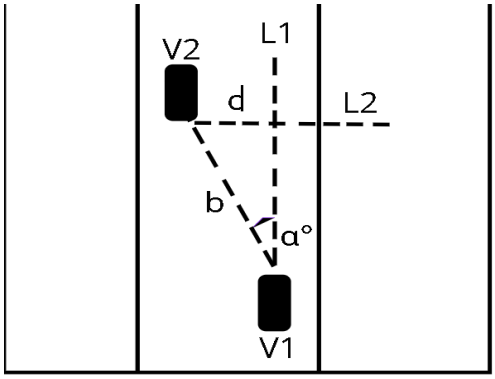

FIGURE V.4 – Déterminer si deux véhicules se trouvent sur la même voie

V.6 Simulation et résultats

Pour évaluer les performances de notre proposition (LSRP), nous l'avons implémentée avec deux autres protocoles de routage dans le simulateur OMNET++. Nous avons choisi de comparer les performances de LSRP avec celles des protocoles de routage GPSR et PDGR. GPSR est une référence pour le routage dans les réseaux à haute mobilité et est facile à déployer dans des environnements ouverts tels que les autoroutes. PDGR est également un protocole reconnu, il vise à assurer, comme le nôtre, des transmissions plus efficaces en réduisant les pertes de paquets et il est comme GPSR adapté aux environnements ouverts.

Il est supposé ici que les véhicules du réseau sont équipés d'un GPS et d'un service de localisation, la carte choisie est une autoroute de 15 km. Les véhicules choisissent leurs voies et procèdent aux changements de voie aléatoirement et ceci est généré par le moteur de mobilité SUMO. Nous avons opté pour une

Paramètre	Valeur
Surface du réseau	200m X 15000 m
Portée de communication	150 m
Nombre de véhicules	150
Vitesse maximale des véhicules	70 kph-120 kph
Intervalle de message périodique	0.8s
Protocole MAC	IEEE 1609.4
Nombre de voies	3
Taille des paquets	512 bytes

TABLE V.1 – Paramètres de simulation

variation progressive de la vitesse maximale des véhicules, allant de 70 km/h à 120 km/h afin de montrer l'impact de cette augmentation de la vitesse sur les performances des trois protocoles simulés et leur capacité à s'adapter à cette mobilité. Les autres paramètres de simulation sont présentés dans le tableau V.1.

Les métriques de performance que nous avons choisies d'évaluer pour les protocoles de routage étudiés sont les trois paramètres suivants : débit, taux de perte de paquets (PLR, Packet Loss Rate) et ratio de rupture de liens (LBR, Link Break Ratio).

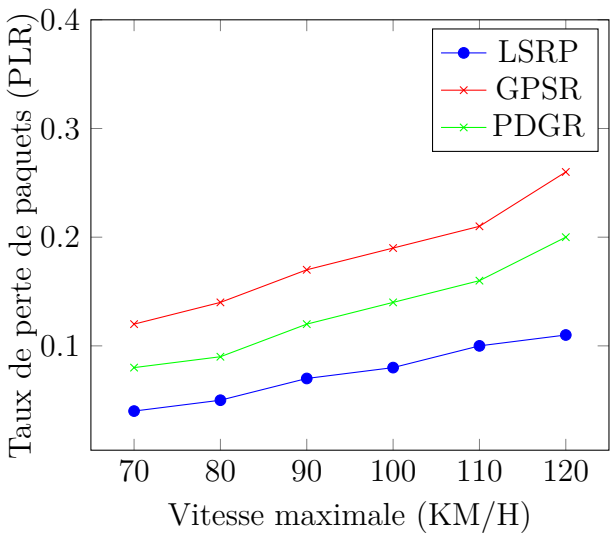

FIGURE V.5 – Taux de perte de paquets (PLR) Vs Vitesse

La figure V.5 montre les performances de notre protocole par rapport à GPSR et PDGR en termes de taux de perte de paquets. Les résultats montrent

que notre proposition garantit un meilleur PLR par rapport aux deux protocoles pour différentes raisons. Comme nous le savons, un nœud dans GPSR utilise des informations localement disponibles sur ses voisins directs, et envoie ses paquets à ceux qui sont géographiquement proches de la destination, mais si le nœud émetteur ne trouve pas de relais de ce type en raison du problème du maximum local, le protocole passe en mode périmètre, sauf que ce mode ne garantit pas de trouver un relais intéressant en une durée de temps raisonnable, et le paquet risque de s'éloigner du nœud destinataire et donc d'être détruit en raison des longs délais d'attente, ou simplement être perdu parce qu'il s'est isolé en raison du mauvais choix de l'itinéraire.

En ce qui concerne PDGR, le fait qu'il cause un PLR plus élevé par rapport à notre protocole peut s'expliquer par le fait que le protocole désigne les meilleurs nœuds relais en se basant sur les positions futures des véhicules. Bien que la direction soit facile à prévoir grâce aux cartes routières notamment sur les autoroutes, les futures variations de vitesse des véhicules ne le sont pas, et ces variations peuvent jouer un rôle important dans la formation des liens de communication. Par conséquent, choisir des itinéraires basés sur des prédictions qui sont exécutées saut par saut ne garantit pas une vision globale du réseau et donc une transmission optimisée.

Comme notre protocole vise à garantir des communications stables et des liens durables, les paquets voyageant sur l'itinéraire choisi ont une forte probabilité d'atteindre leur destination sans être perdus ou détruits. En effet, le fait de favoriser les liens de communication reliant des véhicules qui sont proches en vitesse et en distance et l'utilisation du Carry and Forward permet de réduire la perte de paquets. En favorisant des routes comptant plusieurs nœuds consécutifs circulant sur la même voie, nous augmentons la probabilité d'avoir une séquence de véhicules dont les vitesses ne diffèrent pas trop dans le présent et que cela reste le cas à l'avenir, ces derniers maintiendront donc des distances raisonnables entre eux dans le futur proche.

La figure montre un autre fait intéressant. Bien que les trois protocoles affichent une augmentation de la perte de paquets causée par l'augmentation de la vitesse maximale des véhicules (axe des abscisses), on remarque que cette augmentation est moins importante pour LSRP, c'est-à-dire qu'il réagit mieux à ces vitesses élevées. Cela est dû au choix des itinéraires basé sur la stabilité des liens, parce que plus la vitesse des véhicules augmente, plus les liens de communication sont faibles. Le fait que notre protocole favorise le choix de liens offrant une bonne distance entre les nœuds et des vitesses relatives intéressantes couplées avec le choix des nœuds se déplaçant sur les mêmes voies le rend plus adapté à des vitesses élevées et réduit l'impact de ces vitesses sur la perte de paquets.

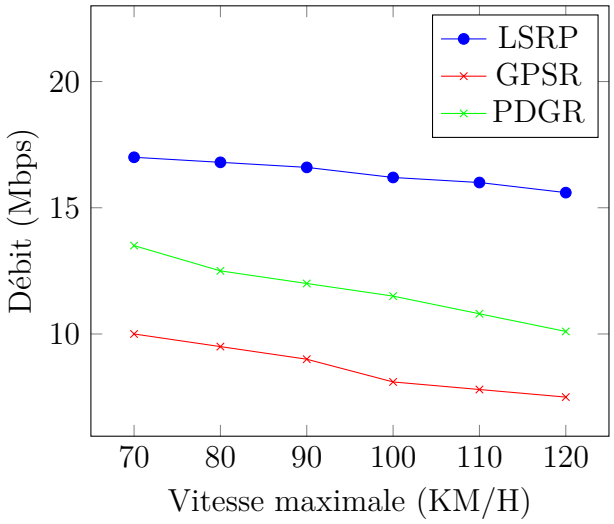

FIGURE V.6 – Débit (Mbps) Vs Vitesse

La figure V.6 présente une comparaison des performances en termes de débit, et comme nous pouvons le voir, notre protocole garantit un meilleur débit par rapport à PDGR et GPSR sous les mêmes conditions. Pour GPSR cela peut s'expliquer par le fait que lorsqu'un paquet entre en mode périmètre, il y a une probabilité qu'il passe beaucoup de temps et traverse beaucoup de nœuds relais avant d'atteindre sa destination, et peut parfois s'en éloigner, ce qui se traduit par une faible transmission de paquets par unité de temps et donc un faible débit de données envoyé. La méthode de planarisation de graphe est également une tâche difficile à réaliser dans un réseau de véhicules en raison de la grande mobilité de ses nœuds, ce qui peut provoquer la transmission d'un paquet sur une route non optimale, parce que, dans GPSR, il est impossible de savoir à l'avance si les paquets suivent le meilleur chemin possible.

Bien que PDGR prenne en compte la prédiction des futures positions des voisins, il ne considère pas de manière optimale le cas où un voisin est situé au bord de la zone de transmission du nœud émetteur, et puisque les routes ne sont pas choisies à l'avance, mais plutôt saut par saut, la possibilité qu'un nœud choisisse un mauvais relais avec qui l'émetteur crée un mauvais lien de communication est assez élevée dans le contexte des réseaux de véhicules en général et des scénarios autoroutiers en particulier en raison de la grande mobilité. Les prévisions faites dans PDGR peuvent également être entravées par la nature du trafic routier, par exemple si le nœud destinataire est loin derrière le nœud source, cela peut conduire à un choix d'itinéraire non optimisé. Toutes ces raisons entraînent une diminution du nombre de paquets pouvant être acheminés dans une unité de temps et donc une diminution du débit sur le réseau.

Pour notre protocole, en plus du fait que réduire la perte de paquets contribue à améliorer le débit, le fait que l'information topologique est disponible rapidement au niveau du nœud source signifie que les nœuds relais composant un itinéraire peuvent être choisis par segments, au lieu de le faire saut par saut. Cela évite de sélectionner de mauvaises routes et donc d'augmenter la chance que les paquets atteignent leur destination sans avoir à changer d'itinéraire, et au même temps de réduire le temps de sélection initiale de l'itinéraire, car les estimations topologiques sont faites à l'avance et périodiquement. Toutes ces raisons permettent d'avoir un taux intéressant de paquets transmis par unité de temps et d'améliorer le débit.

Notons que comme pour le taux de perte de paquet, la dégradation du débit avec l'augmentation de la vitesse est moins importante dans notre protocole que dans GPSR et PDGR.

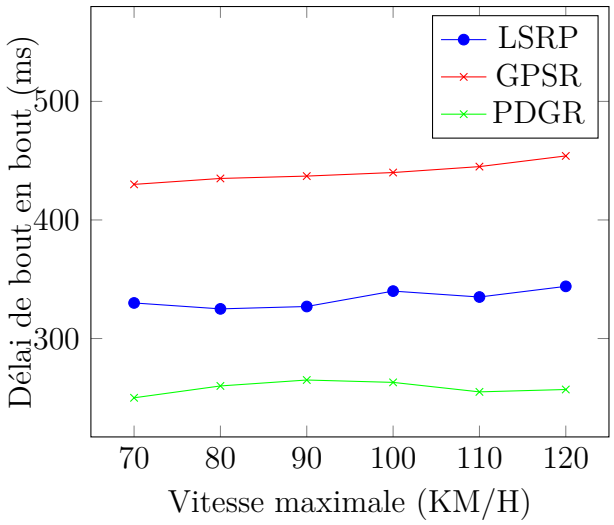

FIGURE V.7 – Délai de bout en bout moyen (ms) Vs Vitesse

Le graphe de la figure V.7 montre la performance des trois protocoles en termes de délais de bout en bout, qui représente le temps moyen en millisecondes nécessaire pour qu'un paquet traverse son chemin depuis le nœud source vers le nœud destinataire. Nous pouvons voir que notre protocole fournit un meilleur délai de bout en bout par rapport à GPSR, mais que PDGR est meilleur en ce qui concerne cette métrique de performance. GPSR utilise la planarisation de graphe en mode périmétrique qui est déclenchée dans les cas de maximum local. Ce mode de transmission conduit souvent les paquets à des itinéraires non optimaux en termes de délais, et peut même les éloigner géographiquement du nœud destinataire dans le cas des réseaux à faible densité, provoquant ainsi une augmentation du délai de bout en bout. PDGR offre

de meilleures performances que notre protocole, parce que son mode de transmission basé sur le choix de nœuds relais qui se déplacent en direction de la destination couplé à l'utilisation du système Carry and Forward dans le cas de nœuds isolés permet de minimiser le temps de routage des paquets. Ceci est dû au fait que PDGR vise à acheminer les paquets le plus rapidement possible sans tenir compte des risques de rupture des liens de communication contrairement à notre solution qui vise à choisir les routes les plus stables qui ne sont pas nécessairement les plus rapides. Notre parti pris a cependant un inconvénient, dans le sens où le choix des routes avec plusieurs nœuds à proximité circulant sur la même voie peut conduire à une augmentation du nombre de sauts requis avant d'atteindre la destination, et ces routes ne sont pas nécessairement les plus courtes en termes de distance, ce qui peut conduire à une augmentation des délais.

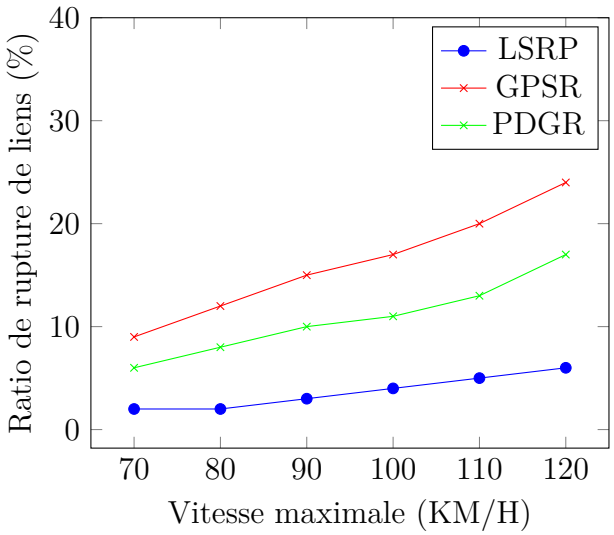

FIGURE V.8 – Ratio de rupture de liens Vs Vitesse

Puisque notre protocole vise à garantir que les routes soient constituées des liens de communication les plus stables possibles, il est intéressant d'étudier la fréquence avec laquelle ces liens sont rompus. La rupture d'un lien est habituellement causée par la distance croissante entre les deux nœuds qui le forment et amène ainsi l'un à quitter la portée de transmission de l'autre. La figure V.8 montre que notre protocole offre un meilleur ratio, ceci est dû au fait que les routes présélectionnées sont celles ayant les liens de communication les plus stables, de sorte qu'ils sont plus durables grâce à la courte distance et à la faible différence de vitesse entre les deux nœuds qui les composent. Le fait que ces routes comportent également un grand nombre de nœuds circulant sur la même voie signifie que des segments de plusieurs liens consécutifs ont de fortes chances de rester stables à l'avenir en cas de changements de vitesse

des nœuds. GPSR utilise la "Greedy Forwarding", qui ne tient compte que des informations géographiques lors de la sélection des sauts suivants, sans tenir compte des différences de vitesse et sans faire de prédictions basées sur une idée globale de la topologie du réseau, cela peut conduire un nœud à sélectionner un voisin positionné à la limite de sa portée de communication, et qu'un changement soudain de vitesse provoque la disparition du lien de communication et du paquet. Le mode périmètre peut aussi conduire à des choix de route non optimisés qui pourraient isoler les nœuds relais parce que l'information de densité n'est pas prise en compte. PDGR n'est pas immunisé contre la possibilité d'une mauvaise sélection de nœuds relais, car cette sélection prend en compte la vitesse et la direction de ces nœuds et la distance les séparant de la destination uniquement, ce qui peut conduire à des liens de communication excessivement longs (en distance) entre les nœuds relais et donc augmenter le risque qu'un de ces nœuds quitte la zone de transmission de l'émetteur en raison de changements brusques de vitesse. Comme GPSR, PDGR ne prend pas non plus de décisions de routage basées sur des informations concernant la densité globale, ce qui peut causer qu'un paquet soit envoyé à une zone de faible densité où Il est difficile de trouver des liens de communication stables.

V.7 Conclusion

Dans ce chapitre, nous avons présenté un nouveau protocole de routage hybride dédié aux scénarios d'autoroute, et basé sur le principe de la stabilité des liens entre les nœuds pour assurer des communications efficaces et durables. Cela a été fait en tenant compte des différences de vitesse entre les véhicules circulant sur des voies différentes ainsi que le fait qu'il soit possible de prévoir les changements de vitesse des véhicules circulant sur la même voie. Les résultats de nos simulations montrent que notre protocole fournit des communications plus stables par rapport à GPSR et PDGR, avec de meilleurs liens de communication, et de meilleurs taux de perte de paquets et de débit grâce à la minimisation des ruptures de liens. Comme travaux futurs, nous avons pour but d'améliorer notre proposition en prenant en compte des paramètres supplémentaires, et par la suite développer un nouveau protocole de routage dédié aux scénarios urbains à forte densité.

Conclusion générale et perspectives

Dans cette thèse, nous avons proposé des contributions visant à améliorer la qualité de service pour le routage et l'accès au canal dans les réseaux véhiculaires. En mettant l'accent sur l'adaptabilité aux hautes vitesses qui caractérisent ce type de réseaux, nous avons pu montrer qu'il était possible de réduire les effets néfastes de cette vitesse sur certaines métriques de performances, ce qui peut être extrêmement utile dans le contexte des applications sensibles à la perte de paquets en particulier et à la stabilité des communications en général.

Après avoir posé notre problématique, et défini nos principaux objectifs, nous avons réparti notre travail en deux parties distinctes, l'une dédiée au routage et l'autre à l'accès au canal.

Dans le cadre de l'accès au canal, notre étude des travaux existants nous a permis de constater un fait intéressant. Il s'agit de l'existence d'un certain déséquilibre dans ces travaux, c'est-à-dire que ces derniers favorisent souvent un certain type de transmissions au détriment de l'autre (transmissions des paquets de sécurité par opposition aux paquets de service et vice versa). Cela nous a incités à proposer des améliorations susceptibles de répondre aux besoins du réseau en matière de transmission de messages de service, sans pour autant négliger les paquets de sécurité critiques transmis en situations d'urgence. Afin d'évaluer les performances de ces améliorations, nous les avons comparées avec celles des protocoles 1609.4 original et AAA, qui est aussi une amélioration qui vise à offrir plus de flexibilité dans l'accès au canal. Les nombreuses simulations effectuées ont montré que nos contributions permettent d'améliorer les performances en considérant les métriques suivantes : Le taux de perte de paquets, le débit et le taux de transmission de paquets de sécurité critiques.

En ce qui concerne le routage, notre revue de littérature nous a permis de pointer du doigt un manque flagrant. En effet, il existe très peu de protocoles de routage dédiés exclusivement aux autoroutes (scénarios à grande vitesse) et encore moins ceux qui sont basés sur le principe de stabilité des communi-

cations. Or, nous savons que les vitesses élevées ont un impact négatif sur ces communications et que certaines applications sont très sensibles aux métriques telle que la perte de paquets. Cela nous a motivés à proposer un protocole de routage dédié aux autoroutes, basé sur le concept de stabilité des liens de communication et donc adapté aux grandes vitesses. La comparaison des performances de notre protocole avec celles de GPSR et PDGR a montré une amélioration significative en termes de perte de paquets, de débit et de taux de rupture de liens, ainsi qu'une meilleure adaptabilité à l'augmentation de la vitesse des véhicules. Néanmoins, notre protocole offre un délai de bout en bout moins intéressant que celui offert par PDGR pour des raisons citées dans le chapitre 3.

Notre travail sur trois couches protocolaires différentes (couche physique, liaison de données et réseau) nous a également permis de constater la pauvreté de la recherche actuelle en ce qui concerne les solutions multi-couches. De ce fait, l'une de nos motivations pour nos travaux futurs est de développer un protocole offrant une solution multi-couche garantissant la qualité de service dans le contexte des réseaux véhiculaires à haute vitesse. Nous avons comme autre perspective, de proposer des protocoles VANET dans le contexte IoT (Internet of Things) tant cette technologie semble s'installer comme le futur de nos villes, et donc de nos routes.

L'apprentissage automatique est également une discipline à laquelle nous comptons nous intéresser sur le court et moyen terme. En effet, la recherche actuelle dans le domaine de l'intelligence artificielle offre plusieurs opportunités d'intégrer ses concepts dans la conception de réseaux VANETs, pour par exemple améliorer la collaboration entre les véhicules, ou encore créer des systèmes de sûreté routière intelligents.

En ce qui concerne le long terme, nous comptons travailler sur la sécurité informatique dans les réseaux véhiculaires. En effet, l'utilisation de diffusions fréquentes, ainsi que le caractère critique de certaines communications véhiculaires, rendent ce type de réseaux très attractifs pour les pirates informatiques. Assurer une bonne étanchéité à ces attaques potentielles est donc crucial dans les réseaux VANETs.

Bibliographie

[1] Yani-Athmane Bennai, Samira Yessad, and Louiza Bouallouche-Medjkoune. Synthèse sur les principaux protocoles MAC proposés pour les VANETs. *Doctoriales de Recherche Opérationnelle 2018, Université de Béjaia*, 2018.

[2] Yani-Athmane Bennai, Samira Yessad, and Louiza Bouallouche-Medjkoune. A flexible and adaptive medium access control protocol for improving quality of service in vehicular ad-hoc networks. *International Journal of Computers and Applications*, pages 1–10, 2021.

[3] Yani-Athmane Bennai, Samira Yessad, and Louiza Bouallouche-Medjkoune. Link stability based routing protocol for highway scenarios in vehicular networks. *6th IEEE International Conference on Recent Advances and Innovations in Engineering, Malaysia*, 2021.

[4] Anas Abu Taleb. VANET routing protocols and architectures : An overview. *J. Comput. Sci.*, 14(3) :423–434, 2018.

[5] R Nithiavathy, E Udayakumar, and K Srihari. Survey on VANET and various applications of internet of things. In *Cloud-Based Big Data Analytics in Vehicular Ad-Hoc Networks*, pages 75–89. IGI Global, 2021.

[6] Saif Al-Sultan, Moath M Al-Doori, Ali H Al-Bayatti, and Hussien Zedan. A comprehensive survey on vehicular ad hoc network. *Journal of network and computer applications*, 37 :380–392, 2014.

[7] Marwa Altayeb and Imad Mahgoub. A survey of vehicular ad hoc networks routing protocols. *International Journal of Innovation and Applied Studies*, 3(3) :829–846, 2013.

[8] Michael Lee and Travis Atkison. VANET applications : Past, present, and future. *Vehicular Communications*, 28 :100–310, 2021.

[9] Ketut Bayu Yogha Bintoro. A study of V2V communication on VANET : Characteristic, challenges and research trends. *JISA (Jurnal Informatika dan Sains)*, 4(1) :46–58, 2021.

[10] Tarandeep Kaur Bhatia, Ramkumar Ketti Ramachandran, Robin Doss, and Lei Pan. Data congestion in VANETs : research directions and new trends through a bibliometric analysis. ***The Journal of Supercomputing***, pages 1–43, 2021.

[11] Al-Sakib Khan Pathan. ***Security of self-organizing networks : MANET, WSN, WMN, VANET***. CRC press, 2016.

[12] Fabio Arena, Giovanni Pau, and Alessandro Severino. A review on IEEE 802.11 p for intelligent transportation systems. ***Journal of Sensor and Actuator Networks***, 9(2) :1–22, 2020.

[13] Felipe Cunha, Guilherme Maia, Heitor S Ramos, Bruno Perreira, Clayson Celes, André Campolina, Paulo Rettore, Daniel Guidoni, Fernanda Sumika, Leandro Villas, et al. Vehicular networks to intelligent transportation systems. In ***Emerging Wireless Communication and Network Technologies***, pages 297–315. Springer, 2018.

[14] Sofiane Ouni, Narjes Boulila, and Bassam A Zafar. Enhanced EDCA with deterministic transmission collision resolution for real-time communication in vehicular ad hoc networks. ***Wireless Personal Communications***, 98(1) :311–335, 2018.

[15] Jungmin So and Ayinebyona Eliab. N-DCF : MAC overhead reduction using narrow channel contention in wireless networks. ***EURASIP Journal on Wireless Communications and Networking***, 2018(1) :1–19, 2018.

[16] IEEE 1609 Working Group et al. IEEE standard for wireless access in vehicular environments (WAVE)-multi-channel operation. ***IEEE Std***, pages 4–1609, 2016.

[17] Bechir Alaya, Rehanullah Khan, Tarek Moulahi, and Salim El Khediri. Study on QoS management for video streaming in vehicular ad hoc network (VANET). ***Wireless Personal Communications***, pages 1–33, 2021.

[18] C Tripti and MG Jibukumar. An enhanced synchronized multi-channel MAC scheme to improve throughput in VANET. ***International Journal of Communication Networks and Information Security***, 12(2) :153–161, 2020.

[19] Khondokar Fida Hasan, Yanming Feng, and Yu-Chu Tian. GNSS time synchronization in vehicular ad-hoc networks : Benefits and feasibility. ***IEEE Transactions on Intelligent Transportation Systems***, 19(12) :3915–3924, 2018.

[20] Xinquan Huang, Aijun Liu, and Xiaohu Liang. An analytical model of CSMA/CA performance for periodic broadcast scheme. In *2018 IEEE/CIC International Conference on Communications in China (ICCC)*, pages 475–479. IEEE, 2018.

[21] R Thenmozhi. Study on preventing data collision by enhanced safety or alert message broadcasting strategy in vehicular ad-hoc network (VANET). *Recent Developments in Engineering Research*, 11 :1–15, 2021.

[22] James Adu Ansere, Guangjie Han, and Hao Wang. A novel reliable adaptive beacon time synchronization algorithm for large-scale vehicular ad hoc networks. *IEEE Transactions on Vehicular Technology*, 68(12) :11565–11576, 2019.

[23] Khondokar Fida Hasan, Charles Wang, Yanming Feng, and Yu-Chu Tian. Time synchronization in vehicular ad-hoc networks : A survey on theory and practice. *Vehicular communications*, 14 :39–51, 2018.

[24] Shereen AM Ahmed, Sharifah HS Ariffin, and Norsheila Fisal. Overview of wireless access in vehicular environment (WAVE) protocols and standards. *environment*, 7 :1–8, 2013.

[25] Shubha R Shetty and DH Manjaiah. A comprehensive study of security attack on VANET. In *Data Management, Analytics and Innovation*, pages 407–428. Springer, 2022.

[26] Htoo Aung Win, Ram Dantu, and Pradhumna Shrestha. On-road performance evaluation of IEEE 802.11 p/WAVE in BSM signalling and video streaming using WSMP. In *2020 Wireless Telecommunications Symposium (WTS)*, pages 1–8. IEEE, 2020.

[27] Yugal Kumar, Pradeep Kumar, and Akash Kadian. A survey on routing mechanism and techniques in vehicle to vehicle communication (VANET). *International Journal of Computer Science & Engineering Survey (IJCSES)*, 2(1) :135–143, 2011.

[28] Flaminio Borgonovo, Antonio Capone, Matteo Cesana, and Luigi Fratta. RR-ALOHA, a reliable R-ALOHA broadcast channel for ad-hoc inter-vehicle communication networks. In *Proceedings of Med-Hoc-Net*, volume 2002, 2002.

[29] Akimitsu Kanzaki, Takahiro Hara, and Shojiro Nishio. An adaptive TDMA slot assignment protocol in ad hoc sensor networks. In *Proceedings of the 2005 ACM symposium on Applied computing*, pages 1160–1165. ACM, 2005.

[30] Flaminio Borgonovo, Antonio Capone, Matteo Cesana, and Luigi Fratta. Adhoc MAC : New MAC architecture for ad hoc networks providing efficient and reliable point-to-point and broadcast services. ***Wireless Networks***, 10(4) :359–366, 2004.

[31] Yuanguo Bi, Kuang-Hao Liu, Lin X Cai, Xuemin Shen, and Hai Zhao. A multi-channel token ring protocol for QoS provisioning in inter-vehicle communications. ***IEEE Transactions on Wireless Communications***, 8(11) :5621–5631, 2009.

[32] Katrin Bilstrup, Elisabeth Uhlemann, Erik Ström, and Urban Bilstrup. On the ability of the 802.11 p MAC method and STDMA to support real-time vehicle-to-vehicle communication. ***EURASIP Journal on Wireless Communications and Networking***, 2009(1) :1–13, 2009.

[33] Yvonne Gunter, Bernhard Wiegel, and Hans Peter Grossmann. Cluster-based medium access scheme for VANETs. In ***2007 IEEE Intelligent Transportation Systems Conference***, pages 343–348. IEEE, 2007.

[34] Claudia Campolo, Alessandro Cortese, and Antonella Molinaro. Crasch : A cooperative scheme for service channel reservation in 802.11 p/wave vehicular ad hoc networks. In ***2009 International Conference on Ultra Modern Telecommunications & Workshops***, pages 1–8. IEEE, 2009.

[35] Nakjung Choi, Sungjoon Choi, Yongho Seokt, Taekyoung Kwon, and Yanghee Choi. A solicitation-based IEEE 802.11 p MAC protocol for roadside to vehicular networks. In ***2007 Mobile Networking for Vehicular Environments***, pages 91–96. IEEE, 2007.

[36] Shengbin Cao and Victor CS Lee. A novel coordinated medium access control scheme for vehicular ad hoc networks in multichannel environment. ***IEEE Access***, 7 :84333–84348, 2019.

[37] Ghassan Samara. An improved CF-MAC protocol for VANET. ***arXiv preprint arXiv :1906.11922***, 2019.

[38] Muhammad Bilal Latif, Feng Liu, and Kai Liu. A TDMA-based MAC protocol for mitigating mobility-caused packet collisions in vehicular ad hoc networks. ***Sensors***, 22(2) :6–43, 2022.

[39] Oumaima El Joubari, Jalel Ben Othman, and Véronique Vèque. Ta-TDMA : A traffic aware TDMA MAC protocol for safety applications in VANET. In ***2021 IEEE Symposium on Computers and Communications (ISCC)***, pages 1–8. IEEE, 2021.

[40] Hamed Mosavat, Yue Li, Lin Cai, and Lei Lu. NCMAC : A distributed MAC protocol for reliable beacon broadcasting in V2X. *IEEE Transactions on Vehicular Technology*, 2021.

[41] Yi Cao, Haixia Zhang, Xiaotian Zhou, and Dongfeng Yuan. A scalable and cooperative MAC protocol for control channel access in VANETs. *IEEE Access*, 5 :9682–9690, 2017.

[42] Odilbek Urmonov and HyungWon Kim. Highly reliable MAC protocol based on associative acknowledgement for vehicular network. *Electronics*, 10(4) :3–82, 2021.

[43] Chakrapani Venkataramanan and Selvaraj M Girirajkumar. Markov fuzzy based MAC protocol for life time maximization of wireless sensor network. *International Journal of Computers and Applications*, 36(4) :133–139, 2014.

[44] Hassan Aboubakr Omar, Weihua Zhuang, and Li Li. VeMAC : A TDMA-based MAC protocol for reliable broadcast in VANETs. *IEEE transactions on mobile computing*, 12(9) :1724–1736, 2012.

[45] Yunmin Kim, Mingyu Lee, and Tae-Jin Lee. Coordinated multichannel MAC protocol for vehicular ad hoc networks. *IEEE Transactions on Vehicular Technology*, 65(8) :6508–6517, 2015.

[46] Sailesh Bharati and Weihua Zhuang. CAH-MAC : cooperative adhoc MAC for vehicular networks. *IEEE Journal on Selected Areas in Communications*, 31(9) :470–479, 2013.

[47] Mohammad S Almalag, Stephan Olariu, and Michele C Weigle. TDMA cluster-based MAC for VANETs (TC-MAC). In *2012 IEEE international symposium on a world of wireless, mobile and multimedia networks (WoWMoM)*, pages 1–6. IEEE, 2012.

[48] Tsang-Ling Sheu and Yu-Hung Lin. A cluster-based TDMA system for inter-vehicle communications. *J. Inf. Sci. Eng.*, 30(1) :213–231, 2014.

[49] Rongqing Zhang, Jinsung Lee, Xia Shen, Xiang Cheng, Liuqing Yang, and Bingli Jiao. A unified TDMA-based scheduling protocol for vehicle-to-infrastructure communications. In *2013 International Conference on Wireless Communications and Signal Processing*, pages 1–6. IEEE, 2013.

[50] Rongqing Zhang, Xiang Cheng, Liuqing Yang, Xia Shen, and Bingli Jiao. A novel centralized TDMA-based scheduling protocol for vehicular networks. *IEEE Transactions on Intelligent Transportation Systems*, 16(1) :411–416, 2014.

[51] Weijie Guo, Liusheng Huang, Long Chen, Hongli Xu, and Jietao Xie. An adaptive collision-free MAC protocol based on TDMA for inter-vehicular communication. In *2012 International Conference on Wireless Communications and Signal Processing (WCSP)*, pages 1–6. IEEE, 2012.

[52] Rui Zou, Zishan Liu, Lin Zhang, and Muhammad Kamil. A near collision free reservation based MAC protocol for VANETs. In *2014 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 1538–1543. IEEE, 2014.

[53] Yunpeng Zang, Lothar Stibor, Bernhard Walke, Hans-Jurgen Reumerman, and Andre Barroso. A novel MAC protocol for throughput sensitive applications in vehicular environments. In *2007 IEEE 65th Vehicular Technology Conference-VTC2007-Spring*, pages 2580–2584. IEEE, 2007.

[54] TaeOh Kim, SungDae Jung, and SangSun Lee. Cmmp : clustering-based multi-channel MAC protocol in VANET. In *2009 second international conference on computer and electrical engineering*, volume 1, pages 380–383. IEEE, 2009.

[55] Hang Su and Xi Zhang. Clustering-based multichannel MAC protocols for QoS provisionings over vehicular ad hoc networks. *IEEE Transactions on Vehicular Technology*, 56(6) :3309–3323, 2007.

[56] Kai Liu, Jinhua Guo, Ning Lu, Fuqiang Liu, Xinhong Wang, and Ping Wang. Ramc : A RSU-assisted multi-channel coordination MAC protocol for VANET. *IEICE transactions on communications*, 94(1) :203–214, 2011.

[57] Xu Xie, Benxiong Huang, Shaoshi Yang, and Tiejun Lv. Adaptive multichannel MAC protocol for dense VANET with directional antennas. In *2009 6th IEEE Consumer Communications and Networking Conference*, pages 1–5. IEEE, 2009.

[58] Hamid Menouar, Fethi Filali, and Massimiliano Lenardi. A survey and qualitative analysis of MAC protocols for vehicular ad hoc networks. *IEEE wireless communications*, 13(5) :30–35, 2006.

[59] Yi Wang, Akram Ahmed, Bhaskar Krishnamachari, and Konstantinos Psounis. IEEE 802.11 p performance evaluation and protocol enhancement. In *2008 IEEE International Conference on Vehicular Electronics and Safety*, pages 317–322. IEEE, 2008.

[60] SY Wang, CL Chou, KC Liu, TW Ho, WJ Hung, CF Huang, MS Hsu, HY Chen, and CC Lin. Improving the channel utilization of IEEE 802.11

p/1609 networks. In *2009 IEEE Wireless Communications and Networking Conference*, pages 1–6. IEEE, 2009.

[61] Vijay Kumar Singh and Rohit Kumar. Multichannel MAC scheme to deliver real-time safety packets in dense VANET. *Procedia computer science*, 143 :712–719, 2018.

[62] Jahnvi Tiwari, Arun Prakash, and Rajeev Tripathi. A novel cooperative MAC protocol for safety applications in cognitive radio enabled vehicular ad-hoc networks. *Vehicular Communications*, 29 :100–336, 2021.

[63] Jian Wang, Xinyu Guo, Xuejie Liu, and Yuming Ge. RPO-MAC : reciprocal partially observable MAC protocol based on application-value-awareness in VANETs. *Wireless Networks*, 27(4) :2509–2528, 2021.

[64] S Ouahou S Bah Z Bakkoury. Packets aggregation scheme with new designed CSMA/CA for VANET multi-hop network. *International Journal on "Technical and Physical Problems of Engineering" (IJTPE)*, 13(4) :186–193, 2021.

[65] Caixia Song, Guozhen Tan, Chao Yu, Nan Ding, and Fuxin Zhang. Apdm : An adaptive multi-priority distributed multichannel MAC protocol for vehicular ad hoc networks in unsaturated conditions. *Computer Communications*, 104 :119–133, 2017.

[66] Jin-Woo Kim, Jae-Wan Kim, and Dong-Keun Jeon. A cooperative communication protocol for QoS provisioning in IEEE 802.11 p/WAVE vehicular networks. *Sensors*, 18(11) :3–622, 2018.

[67] Shamsul J Elias, M Elshaikh, M Yusof Darus, Jamaluddin Jasmis, and Angela Amphawan. 802.11 p profile adaptive MAC protocol for non-safety messages on vehicular ad hoc networks. *Indonesian Journal of Electrical Engineering and Computer Science*, 12(1) :208–217, 2018.

[68] Lin Zhang, Yu Liu, Zi Wang, Jinjie Guo, and Yiding Huo. Mobility and QoS oriented 802.11 p MAC scheme for vehicle-to-infrastructure communications. *Telecommunication Systems*, 60(1) :107–117, 2015.

[69] Radwa Ahmed Osman, Xiao-Hong Peng, and MA Omar. Adaptive cooperative communications for enhancing QoS in vehicular networks. *Physical Communication*, 34 :285–294, 2019.

[70] Yassine Maalej, Ahmed Abderrahim, Mohsen Guizani, Bechir Hamdaoui, and Elyes Balti. Advanced activity-aware multi-channel operations1609. 4 in VANETs for vehicular clouds. In *2016 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6. IEEE, 2016.

[71] Hyundoc Seo, Sangki Yun, and Hyogon Kim. Solving the coupon collector's problem for the safety beaconing in the IEEE 802.11 p WAVE. In *2010 IEEE 72nd Vehicular Technology Conference-Fall*, pages 1–6. IEEE, 2010.

[72] Mohssin Barradi, Abdelhakim S Hafid, and Jose R Gallardo. Establishing strict priorities in IEEE 802.11 p WAVE vehicular networks. In *2010 IEEE Global Telecommunications Conference GLOBECOM 2010*, pages 1–6. IEEE, 2010.

[73] Shiann-Tsong Sheu, Yen-Chieh Cheng, and Jung-Shyr Wu. A channel access scheme to compromise throughput and fairness in IEEE 802.11 p multi-rate/multi-channel wireless vehicular networks. In *2010 IEEE 71st Vehicular Technology Conference*, pages 1–5. IEEE, 2010.

[74] Hung-Chin Jang and Wen-Chieh Feng. Network status detection-based dynamic adaptation of contention window in IEEE 802.11 p. In *2010 IEEE 71st Vehicular Technology Conference*, pages 1–5. IEEE, 2010.

[75] Tony K Mak, Kenneth P Laberteaux, Raja Sengupta, and Mustafa Ergen. Multichannel medium access control for dedicated short-range communications. *IEEE Transactions on Vehicular Technology*, 58(1) :349–366, 2008.

[76] Ning Lu, Yusheng Ji, Fuqiang Liu, and Xinhong Wang. A dedicated multi-channel MAC protocol design for VANET with adaptive broadcasting. In *2010 IEEE Wireless Communication and Networking Conference*, pages 1–6. IEEE, 2010.

[77] Ranran Ding and Qing-An Zeng. A clustering-based multi-channel vehicle-to-vehicle (V2V) communication system. In *2009 First International Conference on Ubiquitous and Future Networks*, pages 83–88. IEEE, 2009.

[78] Kaichi Fujimura and Takaaki Hasegawa. A collaborative MAC protocol for inter-vehicle and road to vehicle communications. In *Proceedings. The 7th International IEEE Conference on Intelligent Transportation Systems (IEEE Cat. No. 04TH8749)*, pages 816–821. IEEE, 2004.

[79] Shujing Li, Yanheng Liu, Jian Wang, and Zemin Sun. SCMAC : A slotted-contention-based media access control protocol for cooperative safety in VANETs. *IEEE Internet of Things Journal*, 7(5) :3812–3821, 2020.

[80] Zhiping Lin and Yuliang Tang. Distributed multi-channel MAC protocol for VANET : An adaptive frame structure scheme. *IEEE Access*, 7 :12868–12878, 2019.

[81] Ali Balador, Annette Böhm, Carlos T Calafate, and Juan-Carlos Cano. A reliable token-based MAC protocol for V2V communication in urban VANET. In *2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pages 1–6. IEEE, 2016.

[82] Narjes Boulila, Mohamed Hadded, Anis Laouiti, and Leila Azouz Saidane. QCH-MAC : A QoS-aware centralized hybrid MAC protocol for vehicular ad hoc networks. In *2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA)*, pages 55–62. IEEE, 2018.

[83] Minglong Zhang, GG Md Nawaz Ali, Peter Han Joo Chong, Boon-Chong Seet, and Arun Kumar. A novel hybrid MAC protocol for basic safety message broadcasting in vehicular networks. *IEEE Transactions on Intelligent Transportation Systems*, 21(10) :4269–4282, 2019.

[84] Rebiha Souadih and Fouzi Semchedine. Energy-efficient coverage and connectivity of wireless sensor network in the framework of hybrid sensor and vehicular network. *International Journal of Computers and Applications*, pages 1–11, 2020.

[85] Ghassan M Abdalla, Mosa Ali Abu-Rgheff, and Sidi-Mohammed Senouci. Space-orthogonal frequency-time medium access control (SOFT MAC) for VANET. In *2009 Global Information Infrastructure Symposium*, pages 1–8. IEEE, 2009.

[86] VanDung Nguyen, Thant Zin Oo, Pham Chuan, and Choong Seon Hong. An efficient time slot acquisition on the hybrid TDMA/CSMA multichannel MAC in VANETs. *IEEE communications letters*, 20(5) :970–973, 2016.

[87] Lin Zhang, Zishan Liu, Rui Zou, Jinjie Guo, and Yu Liu. A scalable CSMA and self-organizing TDMA MAC for IEEE 802.11 p/1609. x in VANETs. *Wireless Personal Communications*, 74(4) :1197–1212, 2014.

[88] Juan Luo, Junli Zha, Yi Xiao, and Renfa Li. H-MAC : a hybrid MAC protocol for VANET. In *China Conference on Wireless Sensor Networks*, pages 346–356. Springer, 2012.

[89] Marica Amadeo, Claudia Campolo, and Antonella Molinaro. Enhancing IEEE 802.11 p/WAVE to provide infotainment applications in VANETs. *Ad Hoc Networks*, 10(2) :253–269, 2012.

[90] Christian Maihöfer, Tim Leinmüller, and Elmar Schoch. Abiding geocast : time–stable geocast for ad hoc networks. In *Proceedings of the*

2nd ACM international workshop on Vehicular ad hoc networks, pages 20–29, 2005.

[91] 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.

[92] Ilias Leontiadis and Cecilia Mascolo. GeOpps : Geographical opportunistic routing for vehicular networks. In ***2007 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks***, pages 1–6. IEEE, 2007.

[93] Maria Kihl, Mihail Sichitiu, Ted Ekeroth, and Michael Rozenberg. Reliable geographical multicast routing in vehicular ad-hoc networks. In ***International Conference on Wired/Wireless Internet Communications***, pages 315–325. Springer, 2007.

[94] Brad Karp and Hsiang-Tsung Kung. GPSR : Greedy perimeter stateless routing for wireless networks. In ***Proceedings of the 6th annual international conference on Mobile computing and networking***, pages 243–254, 2000.

[95] 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.

[96] RA Santos, A Edwards, and O Alvarez. Towards an inter-vehicle communication algorithm. In ***2006 3rd International Conference on Electrical and Electronics Engineering***, pages 1–4. IEEE, 2006.

[97] Abdelmalik Bachir and Abderrahim Benslimane. A multicast protocol in ad hoc networks inter-vehicle geocast. In ***The 57th IEEE Semiannual Vehicular Technology Conference, 2003. VTC 2003-Spring.***, volume 4, pages 2456–2460. IEEE, 2003.

[98] Christian Maihofer and Reinhold Eberhardt. Geocast in vehicular environments : caching and transmission range control for improved efficiency. In ***IEEE Intelligent Vehicles Symposium, 2004***, pages 951–956. IEEE, 2004.

[99] Boon-Chong Seet, Genping Liu, Bu-Sung Lee, Chuan-Heng Foh, Kai-Juan Wong, and Keok-Kee Lee. A-STAR : A mobile ad hoc routing strategy for metropolis vehicular communications. In ***International conference on research in networking***, pages 989–999. Springer, 2004.

[100] Moez Jerbi, Rabah Meraihi, Sidi-Mohammed Senouci, and Yacine Ghamri-Doudane. Gytar : improved greedy traffic aware routing protocol for vehicular ad hoc networks in city environments. In *Proceedings of the 3rd international workshop on Vehicular ad hoc networks*, pages 88–89, 2006.

[101] Gökhan Korkmaz, Eylem Ekici, Füsun Özgüner, and Ümit Özgüner. Urban multi-hop broadcast protocol for inter-vehicle communication systems. In *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*, pages 76–85, 2004.

[102] Ahmad Mohamad Mezher and Mónica Aguilar Igartua. Multimedia multimetric map-aware routing protocol to send video-reporting messages over VANETs in smart cities. *IEEE Transactions on Vehicular Technology*, 66(12) :10611–10625, 2017.

[103] Fang Lu, Jianbo Li, Shan Jiang, Youmei Song, and Fushu Wang. Geographic information and node selfish-based routing algorithm for delay tolerant networks. *Tsinghua Science and Technology*, 22(3) :243–253, 2017.

[104] Daxin Tian, Chao Liu, Xuting Duan, Zhengguo Sheng, Qiang Ni, Min Chen, and Victor CM Leung. A distributed position-based protocol for emergency messages broadcasting in vehicular ad hoc networks. *IEEE Internet of Things Journal*, 5(2) :1218–1227, 2018.

[105] Ahmed Nazar Hassan, Abdul Hanan Abdullah, Omprakash Kaiwartya, Yue Cao, and Dalya Khalid Sheet. Multi-metric geographic routing for vehicular ad hoc networks. *Wireless Networks*, 24(7) :2763–2779, 2018.

[106] B Ramakrishnan, R Bhagavath Nishanth, M Milton Joe, and M Selvi. Cluster based emergency message broadcasting technique for vehicular ad hoc network. *Wireless Networks*, 23(1) :233–248, 2017.

[107] Guoqing Zhang, Wu Chen, Zhong Xu, Hong Liang, Dejun Mu, and Li Gao. Geocast routing in urban vehicular ad hoc networks. In *Computer and Information Science 2009*, pages 23–31. Springer, 2009.

[108] Min-Woo Ryu, Si-Ho Cha, Jin-Gwang Koh, Seokjoong Kang, and Kuk-Hyun Cho. Position-based routing algorithm for improving reliability of inter-vehicle communication. *KSII Transactions on Internet & Information Systems*, 5(8), 2011.

[109] Kulit Na Nakorn and Kultida Rojviboonchai. POCA : position-aware reliable broadcasting in VANET. In *2nd Asia-Pacific conference of information processing (APCIP)*, pages 17–18, 2010.

[110] Rupesh Kumar and SV Rao. Directional greedy routing protocol (DGRP) in mobile ad-hoc networks. In *2008 International Conference on Information Technology*, pages 183–188. IEEE, 2008.

[111] Jiayu Gong, Cheng-Zhong Xu, and James Holle. Predictive directional greedy routing in vehicular ad hoc networks. In *27th International Conference on Distributed Computing Systems Workshops (ICDCSW'07)*, pages 2–4. IEEE, 2007.

[112] Wouter Klein Wolterink, Geert Heijenk, and Georgios Karagiannis. Constrained geocast to support cooperative adaptive cruise control (CACC) merging. In *2010 IEEE Vehicular Networking Conference*, pages 41–48. IEEE, 2010.

[113] Marwane Ayaida, Lissan Afilal, Hacène Fouchal, and Haytem EL Mehraz. Improving the link lifetime in VANETs. In *2011 IEEE 36th Conference on Local Computer Networks*, pages 905–912. IEEE, 2011.

[114] Kevin C Lee, Uichin Lee, and Mario Gerla. TO-GO : Topology-assist geo-opportunistic routing in urban vehicular grids. In *2009 Sixth International Conference on Wireless On-Demand Network Systems and Services*, pages 11–18. IEEE, 2009.

[115] Daxin Tian, Kaveh Shafiee, and Victor CM Leung. Position-based directional vehicular routing. In *GLOBECOM 2009-2009 IEEE Global Telecommunications Conference*, pages 1–6. IEEE, 2009.

[116] Di Wu, Yuan Zhang, Lichun Bao, and Amelia C Regan. Location-based crowdsourcing for vehicular communication in hybrid networks. *IEEE transactions on intelligent transportation systems*, 14(2) :837–846, 2013.

[117] Tsu-Wei Chen and Mario Gerla. Global state routing : A new routing scheme for ad-hoc wireless networks. In *ICC'98. 1998 IEEE International Conference on Communications. Conference Record. Affiliated with SUPERCOMM'98 (Cat. No. 98CH36220)*, volume 1, pages 171–175. IEEE, 1998.

[118] Mimoza Durresi, Arjan Durresi, and Leonard Barolli. Emergency broadcast protocol for inter-vehicle communications. In *11th International Conference on Parallel and Distributed Systems (ICPADS'05)*, volume 2, pages 402–406. IEEE, 2005.

[119] Thomas Clausen, Philippe Jacquet, Cédric Adjih, Anis Laouiti, Pascale Minet, Paul Muhlethaler, Amir Qayyum, and Laurent Viennot. Optimized link state routing protocol (OLSR). 2003.

[120] Saeid Pourroostaei Ardakani. ACR : A cluster-based routing protocol for VANET. *International Journal of Wireless & Mobile Networks (IJWMN) Vol*, 10, 2018.

[121] Souaad Boussoufa-Lahlah, Fouzi Semchedine, Louiza Bouallouche-Medjkoune, and Nadir Farhi. PSCAR : a proactive-optimal-path selection with coordinator agents assisted routing for vehicular ad hoc networks. *International Journal of High Performance Computing and Networking*, 11(2) :129–144, 2018.

[122] Ghassan Samara. An intelligent routing protocol in VANET. *International Journal of Ad Hoc and Ubiquitous Computing*, 29(1-2) :77–84, 2018.

[123] Amir Javadpour, Samira Rezaei, Arun Kumar Sangaiah, Adam Slowik, and Shadi Mahmoodi Khaniabadi. Enhancement in quality of routing service using metaheuristic PSO algorithm in VANET networks. *Soft Computing*, pages 1–12, 2021.

[124] Ahmad Abuashour and Michel Kadoch. An intersection dynamic VANET routing protocol for a grid scenario. In *2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud)*, pages 25–31. IEEE, 2017.

[125] Samira Harrabi, Ines Ben Jaffar, and Khaled Ghedira. Novel optimized routing scheme for VANETs. *Procedia Computer Science*, 98 :32–39, 2016.

[126] Sowmya Kudva, Shahriar Badsha, Shamik Sengupta, Hung La, Ibrahim Khalil, and Mohammed Atiquzzaman. A scalable blockchain based trust management in VANET routing protocol. *Journal of Parallel and Distributed Computing*, 152 :144–156, 2021.

[127] Francisco J Ros, Pedro M Ruiz, and Ivan Stojmenovic. Reliable and efficient broadcasting in vehicular ad hoc networks. In *VTC Spring 2009-IEEE 69th Vehicular Technology Conference*, pages 1–5. IEEE, 2009.

[128] Nikoletta Sofra, Athanasios Gkelias, and Kin K Leung. Route construction for long lifetime in VANETs. *IEEE Transactions on Vehicular Technology*, 60(7) :3450–3461, 2011.

[129] Kalupahana Liyanage Kushan Sudheera, Maode Ma, and Peter Han Joo Chong. Link stability based optimized routing framework for software defined vehicular networks. *IEEE Transactions on Vehicular Technology*, 68(3) :2934–2945, 2019.

[130] Christoph Sommer and Falko Dressler. The DYMO routing protocol in VANET scenarios. In *2007 IEEE 66th vehicular technology conference*, pages 16–20. IEEE, 2007.

[131] Siddharth Shelly and AV Babu. Link residual lifetime-based next hop selection scheme for vehicular ad hoc networks. ***EURASIP Journal on Wireless Communications and Networking***, 2017(1) :1–23, 2017.

[132] Abderrahmane Lakas, Mohamed El Amine Fekair, Ahmed Korichi, and Nasreddine Lagraa. A multiconstrained QoS-compliant routing scheme for highway-based vehicular networks. ***Wireless Communications and Mobile Computing***, 2019, 2019.

[133] Omar Sami Oubbati, Noureddine Chaib, Abderrahmane Lakas, Salim Bitam, and Pascal Lorenz. U2RV : UAV-assisted reactive routing protocol for VANETs. ***International Journal of Communication Systems***, 33(10) :4–104, 2020.

[134] Pavan Kumar Pandey, Vineet Kansal, and Abhishek Swaroop. ALMR : Alternate link based multipath reactive routing protocol for vehicular ad hoc networks (VANETs). ***Adhoc & Sensor Wireless Networks***, 50, 2021.

[135] Thar Baker, Jose M García-Campos, Daniel Gutiérrez Reina, Sergio Toral, Hissam Tawfik, Dhiya Al-Jumeily, and Abir Hussain. GreeAODV : An energy efficient routing protocol for vehicular ad hoc networks. In *International Conference on Intelligent Computing*, pages 670–681. Springer, 2018.

[136] Sudesh Rani and Trilok C Aseri. Randomized link repair reactive routing protocol for vehicular ad hoc network. ***International Journal of Sensors Wireless Communications and Control***, 9(1) :64–79, 2019.

[137] Ayushi Pandey, Vikas Deep, and Purushottam Sharma. Enhancing AODV routing protocol for vehicular ad hoc networks. In *2018 5th International conference on signal processing and integrated networks (SPIN)*, pages 565–568. IEEE, 2018.

[138] Hui Wang, Wei Cheng, Xiaolin Lu, and Haoyang Qin. A improved routing scheme based on link stability for VANET. In *2019 14th IEEE Conference on Industrial Electronics and Applications (ICIEA)*, pages 542–546. IEEE, 2019.

[139] Nawut Na Nakorn and Kultida Rojviboonchai. DECA : density-aware reliable broadcasting in vehicular ad hoc networks. In ***ECTI-CON2010 : The 2010 ECTI International Confernce on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology***, pages 598–602. IEEE, 2010.

[140] Ozan K Tonguz, Nawaporn Wisitpongphan, and Fan Bai. DV-CAST : A distributed vehicular broadcast protocol for vehicular ad hoc networks. *IEEE Wireless Communications*, 17(2) :47–57, 2010.

[141] Jeremy Blum, Azim Eskandarian, and Lance Hoffman. Mobility management in IVC networks. In *IEEE IV2003 Intelligent Vehicles Symposium. Proceedings (Cat. No. 03TH8683)*, pages 150–155. IEEE, 2003.

[142] Mahmoud Hashem Eiza, Thomas Owens, Qiang Ni, and Qi Shi. Situation-aware QoS routing algorithm for vehicular ad hoc networks. *IEEE Transactions on vehicular technology*, 64(12) :5520–5535, 2015.

[143] Mojtaba Mohammadnezhad and Ali Ghaffari. Hybrid routing scheme using imperialist competitive algorithm and rbf neural networks for VANETs. *Wireless Networks*, 25(5) :2831–2849, 2019.

[144] Khalid Kandali, Lamyae Bennis, and Hamid Bennis. A new hybrid routing protocol using a modified k-means clustering algorithm and continuous hopfield network for VANET. *IEEE Access*, 9 :47169–47183, 2021.

[145] Shirin Rahnamaei Yahiabadi, Behrang Barekatain, and Kaamran Raahemifar. TIHOO : an enhanced hybrid routing protocol in vehicular ad-hoc networks. *EURASIP Journal on Wireless Communications and Networking*, 2019(1) :1–19, 2019.

[146] Waheeda Jabbar, Robert Malaney, and Shihao Yan. A location verification based hybrid routing protocol for VANETs. In *2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall)*, pages 1–6. IEEE, 2020.

[147] Hamza Toulni and Benayad Nsiri. A hybrid routing protocol for VANET using ontology. *Procedia Computer Science*, 73 :94–101, 2015.

[148] Ichiro Masaki. Machine-vision systems for intelligent transportation systems. *IEEE Intelligent Systems and their applications*, 13(6) :24–31, 1998.

[149] VanDung Nguyen, Chuan Pham, Thant Zin Oo, Nguyen H Tran, Eui-Nam Huh, and Choong Seon Hong. MAC protocols with dynamic interval schemes for vanets. *Vehicular Communications*, 15 :40–62, 2019.

[150] Antonio Guerrero-Ibanez, C Flores, Pedro Damian-Reyes, Antoni Barba, and Angelica Reyes. A performance study of the 802.11 p standard for vehicular applications. In *2011 Seventh International Conference on Intelligent Environments*, pages 165–170. IEEE, 2011.

[151] **Satya S Karanki and Mohammad S Khan. SMMV : Secure multimedia delivery in vehicles using roadside infrastructure. *Vehicular Communications*, 7 :40–50, 2017.**

[152] **Ghada H Alsuhli, Ahmed Khattab, and Yasmine A Fahmy. Double-head clustering for resilient VANETs. *Wireless Communications and Mobile Computing*, 2019, 2019.**

[153] **Leila Chelouah and Louiza Bouallouche-Medjkoune. Mécanismes de gestion de la localisation dans les réseaux de capteurs sans fil mobiles. *University of Bejaia, Algeria*, PhD Thesis, 2017.**

Résumé

L'explosion du nombre de véhicules circulant sur les routes lors des dernières années a causé un intérêt grandissant autour des Systèmes de Transport Intelligents (STI) et des réseaux Ad Hoc de véhicules (VANETs), tant ces derniers représentent le futur de nos transports. De nombreux standards et applications ont été développés autour de ce type de réseaux dans le but de satisfaire la qualité de service qui se dégrade à cause de la forte mobilité des nœuds constituant un réseau véhiculaire. Dans cette thèse, nous avons apporté différentes contributions visant à améliorer la qualité de service des communications, et pour les applications de sécurité routière, et pour celles de l'info-divertissement des VANETs tout en contournant le problème de forte mobilité des nœuds. Au niveau de la couche réseau, nous avons proposé un nouveau protocole de routage destiné aux autoroutes et basé sur la stabilité des liens. Au niveau de la couche liaison de données, nous avons proposé des méthodes et mécanismes ayant pour but d'offrir plus d'équité et de flexibilité dans le processus d'accès au canal. L'efficacité des deux contributions a été validée et prouvée par simulation.

Mots clés : STI, VANET, Qualité de service, MAC, Routage, Sécurité routière.

Abstract

The explosion in the number of vehicles on the roads in recent years has led to a growing interest in Intelligent Transportation Systems (ITS) and Vehicular Ad Hoc Networks (VANETs), which represent the future of transportation. Numerous standards and applications have been developed around this type of networks in order to satisfy the quality of service which is degraded because of the high mobility of the nodes constituting a vehicular network. In this manuscript, we present various contributions aimed at improving the quality of service of communications, both for road safety applications and for info-entertainment in VANETs, while solving the problem of high node mobility. At the network layer level, we have proposed a new routing protocol for highways based on link stability. At the data link level, we have proposed methods and mechanisms to provide greater equity and flexibility in the channel access process. The effectiveness of both contributions was validated and demonstrated by simulation.

Keywords : ITS, VANET, Quality of Service, MAC, Routing, Road safety.

ملخص

تسبب التزايد في عدد المركبات على الطرق في السنوات الأخيرة في اهتمام متزايد بأنظمة النقل الذكية (ITS) وشبكات المركبات (VANETs)، حيث تمثل هذه المركبات مستقبل النقل عبر العالم. وقد تم تطوير العديد من المعايير والتطبيقات حول هذا النوع من الشبكات من أجل ضمان نوعية الخدمة (QoS) التي تتدهور بسبب التنقل العالي للعقد التي تشكل شبكة المركبات. في هذه الأطروحة، قمنا بتقديم مساهمات مختلفة تهدف إلى تحسين نوعية خدمة الاتصالات، سواء كان لتطبيقات السلامة على الطرق، أو تلك المتعلقة بالإنفوتينمنت وفي نفس الوقت حل مشكلة التنقل العالي للعقد. في طبقة الشبكة (Réseau)، اقترحنا بروتوكول توجيه جديد للطرق السريعة مصمم على أساس استقرار روابط الاتصال. على مستوى طبقة وصلة البيانات (LLC)، اقترحنا آليات لتوفير المزيد من الإنصاف والمرونة في عملية الوصول إلى القناة. وقد تم التحقق من فعالية المساهمتين وإثباتها عن طريق المحاكاة.

الكلمات الدالة: VANET، ITS، جودة الخدمة، MAC، التوجيه، السلامة على الطرق.