N°d'ordre : 11/2013-14/inf

UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE HOUARI BOUMEDIENE (USTHB)

FACULTE D'ELECTRONIQUE ET D'INFORMATIQUE

MÉMOIRE

Présenté pour l'obtention du diplôme de :

MAGISTER

en Informatique

Option : Informatique Mobile

Par :

Mlle ZERROUKI HAYET

Sujet:

LES PROTOCOLES MAC POUR LES RÉSEAUX VÉHICULAIRES

Soutenue publiquement le 02/07/ 2013, devant le jury composé de :

Mme M.BOUKALA	**Professeur (L'USTHB)**	**Présidente**
Mme S. MOUSSAOUI	**Professeur (L'USTHB)**	**Directrice de mémoire**
Mlle N.SALMI	**Maître de Conférence/A (L'USTHB)**	**Examinatrice**
Z.DOUKHA	**Maître Assistante/A (USTHB)**	**Invitée**

A la mémoire de nos chers professeurs: *Mme BENHADID HAYET*, et *Mme AHLEM BENCHENNAF Ep. ZAOUCHE ;*

Allah Yarhamhoum;

A dieu nous appartenons, à lui nous retournons….

Remerciements

بسم الله الرحمان الرحيم

En premier lieu, je remercie Allah le tout puissant de m'avoir permis de mener à bien mon travail.

Avant de commencer la rédaction de ce mémoire, je souhaite vivement remercier et exprimer ma gratitude à :
Pr. Samira MOUSSAOUI, ma directrice de thèse, pour m'avoir donné la possibilité de travailler sur ce sujet de recherche très intéressant. Je la remercie pour le temps et l'attention qu'elle a bien voulu consacrer au bon déroulement de ce travail.

J'adresse aussi mes très sincères remerciements au Pr. Malika BOUKALA de me faire L'honneur de s'intéresser à ce travail et d'avoir présidé le jury. Je tiens à la remercier pour tous les efforts et le temps consacrés malgré les lourdes charges de son travail.

J'exprime ma plus profonde gratitude aux membres du Jury : Dr. Nabila SELMI, Mme Zouina DOUKHA qui ont accepté de rapporter cette thèse malgré leur emploi du temps surchargé.

Je remercie énormément mes très chers parents et mes frères, ma tente, et mes oncles, qui m'ont soutenu vivement durant toutes mes études. Leur amour et leurs conseils m'ont été extrêmement précieux durant toutes ces années.

Mes remerciements s'adressent également à Mr Nabil ZERROUKI, Mr Khaled LAKEHAL, Mme. Zouina DOUKA, Mr Noureddine HOUARI, Djeffal Marwa, Kenza MEKLICHE, Raouia, … pour leur aide et leur gentillesse.

Merci également à Hadia MESTGANEMI pour ses discussions et ses encouragements.

Mes remerciements vont aussi à tous ceux qui ont contribué de prés ou de loin à la concrétisation de ce travail. Qu'ils trouvent tout le témoignage de ma gratitude et ma parfaite considération.

Sommaire

Introduction générale

Les réseaux mobiles véhiculaires sont vus comme un type particulier de MANETS (Mobile Ad Hoc NETworks) du fait qu'ils utilisent les mêmes technologies sans fil en termes de moyens de communication (tels que les ondes radio, le bluetooth, l'infrarouge ainsi que les antennes WIFI directionnelles ou omnidirectionnelles), mais aussi en termes de standards : le plus populaire étant le standard IEEE 802.11. Néanmoins, les réseaux véhiculaires se distinguent principalement par leur modèle de mobilité: le déplacement des véhicules se heurte à des contraintes dues à l'infrastructure routière, au code de la route, à la qualité du trafic, à la vitesse et à la direction des véhicules ainsi qu'à la destination du conducteur. Ceci fait des réseaux mobiles ad hoc véhiculaires un environnement problématique quant au développement d'applications.

Le principal bénéfice des communications véhiculaires est dans les systèmes de sécurité des passagers grâce aux messages échangés entre les véhicules. D'autres applications et services privés sont également employés, pour encourager le déploiement des réseaux véhiculaires (Techniques, normes, et applications) car l'existence des équipements pour la norme IEEE 802.11 avec des prix abordables, encourage son utilisation dans ce type d'application. (Hartenstein & Laberteaux, 2010) (Huang & Chen, 2010)

Pour utiliser efficacement le spectre limité sans fil et les canaux DSRC, et pour garantir la qualité de service (QoS) aux applications véhiculaires, le contrôle d'accès au medium (MAC : Medium Access Control) constitue l'un des défis principaux dans les réseaux véhiculaires.

En effet, l'importance et le besoin d'améliorer la couche MAC est démontré par le fait que le temps où deux véhicules restent dans la même portée de communication peut être inférieur à 30s pour une vitesse des véhicules allant jusqu'à 120 km/h dans des directions opposées avec une portée de communication allant jusqu'à 1000 m. (Booysen, Zeadally, & Rooyen, 2011). En revanche, gérer et allouer des ressources dans un réseau IEEE 802.11 sont des objectifs très difficiles à obtenir étant donné la nature intrinsèque du protocole CSMA/CA. La difficulté provient donc de l'incapacité à pouvoir estimer d'une part le nombre de flux actifs dans le réseau, et d'autre part le volume de trafic de chaque flux. C'est dans cette optique que la norme 802.11p (802.11p, 2012) est apparue spécialement pour les réseaux véhiculaires ad-hoc (VANETs).

Le tableau suivant récapitule certains axes de recherches dans VANET qui ont été récemment étudiés, en introduisant le nombre de publications (obtenues à partir de la base de données d'IEEE à titre d'exemple). Comme le montre le tableau 1, nous remarquons que l'axe de recherche : MAC dans VANETs n'a pas eu vraiment un niveau d'attention élevé comparé aux autres axes dans VANETs. Les protocoles de la couche MAC n'ont pas été suffisamment développés surtout pour les communications V2V car plusieurs défis restent à relever.

VANET topic	IEEE Xplore publications
broadcasting	646
routing	253
evaluation of existing wireless technologies (cellular, Wi-Fi and WiMAX)	98
security	153
MAC	38

Tableau 1-1 Les articles de recherches IEEE de VANET récemment publiés. **(Booysen, Zeadally, & Rooyen, 2011)**

Dans ce qui suit, nous nous intéresserons au contrôle de congestion dans les réseaux véhiculaires car le standard 802.11p dédié aux VANETs, en sa version actuelle ne prévoit aucun contrôle de congestion spécifique à l'environnement véhiculaire, pourtant les nœuds constituant ces réseaux qui sont les véhicules n'ont pas de problème d'énergie ou bien un problème de capacité de stockage. De ce fait, ils peuvent être équipés facilement par des dispositifs hardware et des plateformes software.

La première partie de cette thèse est une étude bibliographique sur les protocoles MAC dédiés ou adaptés pour les réseaux véhiculaires. Les différentes approches proposées dans la littérature pour contrôler l'accès au canal dans l'environnement véhiculaire peuvent être classées en trois catégories comme : des approches basées sur la planification (free-contention), des approches basées sur la contention (based-contention), et des approches hybrides. La première catégorie qui se base sur la planification, comporte essentiellement les mécanismes: TDMA, FDMA, et STDMA (Bénédicte, Julien, Arnaud, Eric, & Laurent, 2002) (Booysen, Zeadally, & Rooyen, 2011). Le mécanisme CSMA/CA définit dans le standard 802.11 est le cœur de la deuxième catégorie. La troisième catégorie combine entre un ou plusieurs mécanismes based-contention et free-contention (Booysen, Zeadally, & Rooyen, 2011). Dans cette partie, nous avons recensé ces approches en présentant les principaux travaux et protocoles de chaque catégorie, détermin » leurs avantages et inconvénients, ainsi que leurs niveaux d'adaptation à l'environnement véhiculaire.

De nombreuses solutions basées sur le standard 802.11p et qui font l'objet des publications et communications récentes s'intéressent à l'adaptation de la fenêtre de contention et à l'algorithme back-off afin d'améliorer les performances du réseau. Dans ce mémoire, nous avons présenté les principaux travaux existants dans la littérature. Notre étude de cette question, nous a permis de proposer une classification inspirée du travail de (Stanica, 2011) en se basant sur la métrique utilisée pour adapter la valeur de la fenêtre de contention. Ces travaux ont donc été classés en cinq catégories en se basant sur l'un de ces paramètres suivants, à savoir: la densité (Barbosa, Bessa, Sérgio, Rober, & Jùnior, 2011) (Alapati, 2010) (Calì, Conti, & Gregori, 2000), le taux de collision, la taille de la file d'attente, le taux d'occupation du canal, ou un autre aspect aléatoire. Nous avons complété ce travail, en

proposant une seconde classification basée sur la modélisation utilisée, et en considérant d'autres approches comme (Huang & Liao, 2007) (Lin, Jia, Han, & De, 2007)... .

Nos travaux nous ont permis de proposer un mécanisme d'adaptation de la fenêtre de contention avec un nouvel algorithme de backoff dédié aux réseaux véhiculaires appelé NN-ACW (Neural Network based Approach for Adjusting the Contention Window). En effet, nous avons proposé dans un premier temps un modèle intelligent formel pour estimer le niveau de contention dans le réseau. En se basant sur cette valeur estimée, nous avons implémenté un algorithme d'adaptation dynamique de la fenêtre de contention selon l'état du trafic. Ce mécanisme tente de maximiser le débit et de diminuer les délais de transmissions. Nous avons proposé aussi une stratégie qui vise à réduire l'overhead du réseau lorsqu'il est congestionné, en se basant sur la probabilité de transmission. Cette stratégie permet de diminuer la probabilité de collision, et d'augmenter le trafic de données lorsque le réseau est saturé. Contrairement aux travaux précédents, notre solution utilise plusieurs paramètres du réseau et d'environnement pour estimer le niveau de congestion. Nous avons établi des priorités entre ces paramètres qui changent en fonction de l'ancienneté, la certitude, et l'influence de chaque paramètre. Le but de ce mécanisme est d'avoir une meilleure estimation de l'état de congestion autour du nœud.

D'ailleurs, les résultats de simulation obtenus dans ce travail montrent l'intérêt de ce genre de technique dans les réseaux véhiculaires, où les charges de trafic peuvent être très variables selon l'application souhaitée.

Ce mémoire est structuré en sept chapitres et trois parties: le premier chapitre, présente les généralités sur les réseaux véhiculaires, leurs caractéristiques et leurs moyens de communications. Le reste des chapitres peuvent être regroupés en trois parties :

Partie 1: dans cette partie, nous étudions les Protocoles de la couche MAC pour les réseaux véhiculaires, elle comporte trois chapitres.

- le deuxième chapitre définit la couche MAC dans les réseaux véhiculaires et décrit plusieurs méthodes d'accès au canal ;
- le troisième chapitre présente les standards MAC dédiés pour les réseaux véhiculaires;
- le quatrième chapitre présente quelques protocoles hybrides pour les réseaux véhiculaires, nous terminons cette première partie par une synthèse sur l'axe de recherche MAC pour les réseaux véhiculaires.

Partie 2: Etude de la Fenêtre de Contention (CW) et Algorithme BACKOFF pour Réseaux véhiculaires

- dans le cinquième chapitre, nous spécifions notre cadre de travail à l'algorithme de back-off et nous présentons les différentes méthodes d'adaptation de la taille de la fenêtre de contention existantes dans la littérature;

Partie 3: NN-ACW : Un nouveau mécanisme d'adaptation de la fenêtre de contention pour les réseaux VANET.

- le sixième chapitre présente nos propositions concernant l'adaptation de la fenêtre de contention et la gestion de congestion dans le réseau ;

  et, le septième et dernier chapitre, présente l'environnement de tests ainsi qu'une analyse des résultats obtenus.

Nous terminons ce mémoire par une conclusion générale.

Chapitre 1
Les réseaux véhiculaires

1. Introduction

L'introduction des MANETs dans plusieurs domaines de notre vie tels que le sauvetage, et la téléconférence a fait émergé un nouveau type de réseaux mobiles ad hoc où les équipements mobiles sont remplacés par des véhicules : il s'agit des réseaux véhiculaires.

Ces derniers connaissent de plus en plus d'intérêt aussi bien en recherche qu'en développement. Grâce à des équipements informatiques embarqués dans les véhicules et intégrés dans des stations le long des routes et autoroutes, les véhicules peuvent communiquer les uns avec les autres et avec des équipements fixes ou mobiles. Les applications des VANETs sont nombreuses. Ces applications incluent notamment la gestion du trafic, la signalisation d'accident ou de congestion de trafic et l'obtention d'informations via Internet pendant que les véhicules sont en mouvement.

Dans ce chapitre nous allons définir les réseaux VANETs, les caractéristiques, les types de communications, les applications, et les équipements utilisés dans les réseaux mobiles ad hoc véhiculaires (ou VANETs).

2. Les réseaux VANETs (Vehicular Ad-hoc NETworks)

Les réseaux VANETs (Vehicular Ad-hoc NETworks) désignent les réseaux spontanément créés par un ensemble de véhicules. C'est un réseau sans infrastructure ; où la communication est établie directement entre des nœuds mobiles (véhicules) sans l'intervention d'un serveur centralisé de contrôle ou de gestion. Outre la topologie ad hoc du réseau, les nœuds sont très dynamiques, ce qui provoque des changements très fréquents de la topologie du réseau. (Hartenstein & Laberteaux, 2010)

Les réseaux VANETs sont actuellement utilisés dans les systèmes de transport intelligents pour prévenir les véhicules des dangers de collisions ou pour diffuser des informations sur le trafic routier. Ce type d'application est assuré grâce à des messages de petite taille diffusés aux véhicules selon leurs localisations actuelles et leurs destinations. (Harbouche & Moussaoui, 2009)

3. Les équipements utilisés dans les réseaux VANETs

Dans les VANETs, les équipements dont sont dotés les véhicules d'une part et les routes d'autre part, permettent la localisation grâce aux systèmes de géo-localisation utilisant les satellites ainsi que la communication entre les éléments de ces réseaux. Ils peuvent aussi être dotés de capteurs spéciaux permettant d'informer le véhicule sur son environnement immédiat tels que les caméras. (Moustafa & Zhang, 2009):

3.1. Les systèmes de localisation

Il existe beaucoup de techniques de localisation du véhicule tel que: les détecteurs infrarouges, les caméras, les détecteurs piézo-électriques, Filoguidage, les boucles magnétiques, Aimant ou magnet, le GNSS, LE GPS, toutes ces techniques permettent de connaître la position de chaque véhicule du réseau.

3.2. Les systèmes de communication

Un système de communication du réseau désigne tous les éléments capables de véhiculer de l'information (audio, des données informatiques ou vidéo) d'une source vers une destination. Il est possible de distinguer deux types de communication : La communication radio telle que les systèmes de radiodiffusion, les systèmes cellulaires, le Bluetooth IEEE 802.15, le Wifi 802.11, et la communication optique telle que les systèmes de communication par infrarouge :

- **Le WIFI (Wireless Fidelity): 802.11**

En 2001, le premier standard international pour les réseaux locaux sans fil WLAN (Wireless Local Area Network) ou l'IEEE 802.11, est publié. C'est la norme des communications WIFI qui fera l'objet de notre étude dans le troisième chapitre. (Hartenstein & Laberteaux, 2010)

- **Le Bluetooth : IEEE 802.15**

Le groupe IEEE 802.15 intitulé WPAN (Wireless Personal Area Networks) a été mis en place en mars 1999 pour normaliser des réseaux d'une portée d'une dizaine de mètres. Au niveau d'un véhicule, cette norme peut être utilisée pour établir des communications avec l'ordinateur de bord de l'automobile. Le Bluetooth exploite la bande des 2,45 GHz sans licence d'utilisation. (Hartenstein & Laberteaux, 2010)

- **L'Infra Rouge(IR)**

La lumière infra rouge a quasiment les mêmes propriétés que la lumière visible. Un véhicule peut être équipé d'un système de communication par IR pour l'analyse et la gestion du trafic. La communication avec le véhicule est possible jusqu'à 70 Km/h. (Hartenstein & Laberteaux, 2010)

- **Le GSM (Global System for Mobile Communication)**

La Norme de téléphonie mobile Européenne est devenue un standard mondial. Plus d'une centaine de pays l'ont adoptée à travers le monde. Elle utilise 2 fréquences, 900 MHz et 1,8 GHz (1,9 GHz aux USA) (Hartenstein & Laberteaux, 2010) (Huang & Kung, 2009)

4. Architecture des réseaux véhiculaires

Les avancées technologiques et le besoin de sécuriser les routes(Harbouche & Moussaoui, 2009) ont poussé l'industrie automobile et les recherches gouvernementales à se concentrer sur le

déploiement des réseaux véhiculaires. Ces tendances d'avancement dans ces réseaux permettent un certain nombre d'architectures pour le déploiement des réseaux véhiculaires, dans les environnements d'autoroute, ruraux, ou urbains. De telles architectures devraient permettre la communication entre les véhicules (V2V) et entre les véhicules et les équipements fixes de bord de la route (V2I). (Tchepnda, 2008) (Hartenstein & Laberteaux, 2010) (Moustafa & Zhang, 2009)**.**

Le projet Car 2 Car (CAR 2 CAR Communication Consortium Manifesto version 1.1, 2007) classifie les applications VANETs en se basant sur le type de communication, qu'elles soient V2V (Vehicle to Vehicle), V2I (Vehicle to Infrastructure), I2V (Infrastructure to Vehicle), saut unique/multi-saut, ou sens unique/double sens.

4.1. Les réseaux véhiculaires à infrastructure

Les déploiements les plus actifs des réseaux véhiculaires sont dans des architectures de réseaux à infrastructure. Il s'agit dans la plupart des cas d'une réutilisation des technologies des réseaux mobiles de télécommunications dans l'implémentation de certaines applications ou certains services spécifiques aux réseaux véhiculaires.

4.2. Les réseaux véhiculaires ad-hoc

Les réseaux véhiculaires ad-hoc, plus connus sous la dénomination VANET (Vehicular Ad-hoc Networks), reprennent les mêmes principes architecturaux que les MANETs. Ils permettent une communication véhiculaire autonome (V2V) sans employer l'infrastructure,

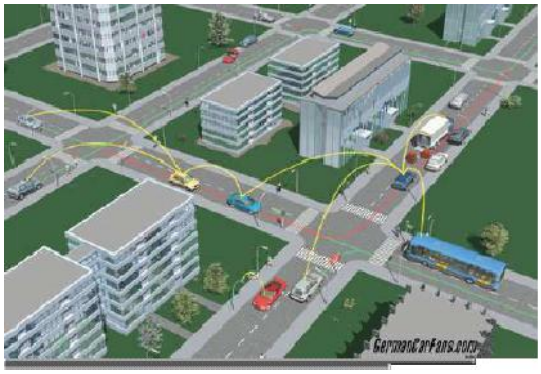


Figure 1-1 Communication V2V.

4.3. Les réseaux véhiculaires ad-hoc hybrides

Les réseaux hybrides ou réseaux ad-hoc hybrides, sont des réseaux sans fil ayant une organisation duale regroupant à la fois celle des réseaux à infrastructure et celle des réseaux ad-hoc. Cette architecture ne se base pas sur une infrastructure fixe d'une façon constante, mais elle peut être exploitée pour une meilleure production et pour entretenir l'accès quand elle est disponible. En effet, l'architecture V2I inclut implicitement la communication V2V.

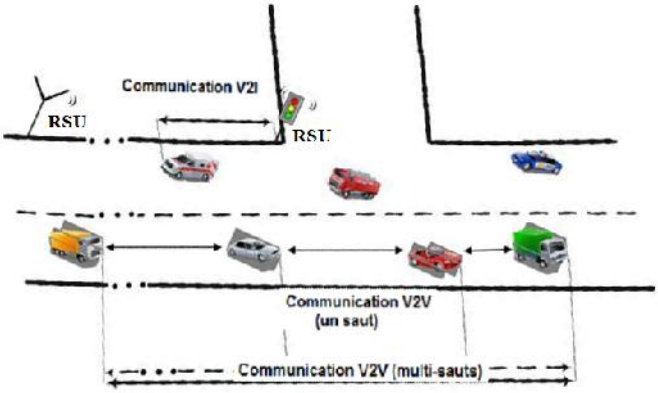


Figure 1 -2 Exemple des réseaux véhiculaires.

5. Propriétés et problématiques des réseaux VANETs

Le réseau VANET n'est qu'un type particulier des réseaux Mobile Ad-hoc. Cependant, les travaux de recherche réalisés dans le domaine des MANETs ne peuvent pas être directement appliqués dans le contexte des réseaux de véhicules à cause de leurs spécificités. Les protocoles et solutions doivent donc les prendre en considération. (Hartenstein & Laberteaux, 2010) (Moustafa & Zhang, 2009)

Voici quelques propriétés et challenges qui distinguent les réseaux véhiculaires des autres types de réseau (Hartenstein & Laberteaux, 2010) (Moustafa & Zhang, 2009) :

- ***Capacité de traitement***

Contrairement aux réseaux mobiles MANETs où les terminaux mobiles ont des contraintes de taille et de poids. Le matériel qu'on peut embarquer dans une voiture est très différent des terminaux mobiles dans les MANETs. Il est possible d'intégrer plusieurs interfaces de communication, comme Wi-fi, WiMax, et le Bluetooth…

- ***Energie et stockage suffisants***

Les nœuds dans les VANETs possèdent une énergie suffisante, et une grande puissance de calcul (y compris stockage et traitement), puisque les nœuds sont des voitures au lieu de petits dispositifs tenus dans la main.

- ***Environnement de déplacement et modèle de mobilité***

Les environnements dans les réseaux ad hoc sont souvent limités à des espaces ouverts. Les déplacements des véhicules, quant à eux, sont liés aux infrastructures routières (routes, autoroutes). Les trajectoires peuvent donc être prédictibles et l'environnement peut être urbain, rural ou autoroutier. Les contraintes imposées par ce type d'environnement, affectent le modèle de mobilité.

- ***Topologie du réseau et connectivité***

A la différence des réseaux mobiles ad hoc classiques, les VANETs sont caractérisés par une plus forte mobilité, liée à la vitesse des véhicules, en particulier sur l'autoroute. Un nœud peut rejoindre le réseau et le quitter en un temps très court, ce qui rend les changements de topologie très fréquents. Une des grandes problématiques dans ces réseaux est liée au partitionnement ou la fragmentation du réseau.

- ***Sécurité et anonymat dans le réseau***

Le problème de sécurité de la communication est important, par exemple, un message d'urgence doit pouvoir être validé ou ignoré s'il est envoyé par un nœud malicieux. Il doit y avoir un mécanisme pour s'assurer de la source de l'information et éliminer l'anonymat.

6. Les Applications des VANETs

La raison d'être des VANETs consiste à munir les voitures et les routes de capacités de communication permettant de rendre la route plus sûre et de rendre le temps passé sur les routes plus convivial. Actuellement, les systèmes de transport intelligents (ITS, Intelligent transportation System) (Annexe A) intègrent l'ensemble des applications et services permettant d'atteindre cette qualité dans le trafic routier. Il est possible de distinguer deux types d'applications avec les réseaux de véhicules, les applications de confort et les applications de sécurité routière. Les contraintes de ces applications sont différentes : Dans le cas d'un accident, il faut prévenir les usagers dans un bref délai alors que la diffusion de publicités n'a pas cette contrainte de temps, mais elle sera par contre plus consommatrice de bande passante. Nous allons donc décrire dans les paragraphes suivants quelques applications. (Hartenstein & Laberteaux, 2010) (Moustafa & Zhang, 2009) (Layouni, Weslem, Raphael, & Tran, 2010)

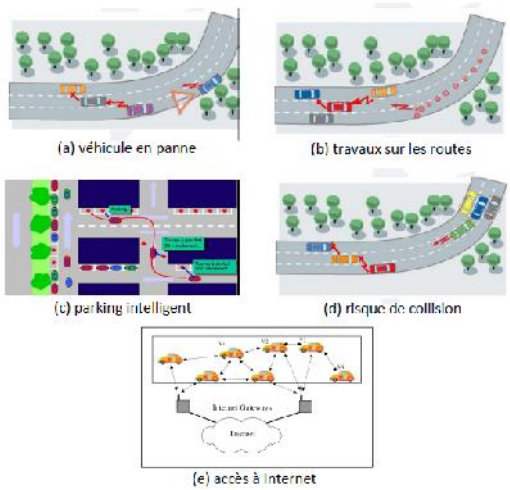


Figure 1-3 Des applications dans les réseaux VANETs. (Layouni, Weslem, Raphael, & Tran, 2010)

6.1. Applications de sécurité routière

Dans le cadre de la sécurité routière, plusieurs incidents sont possibles : accident, ralentissement anormal (bouchon, travaux, intempéries,…), évènements naturels.

Les applications de sécurité routière permettent, dans ce cas d'avertir les véhicules en cas d'incident ou d'accident. Si le conducteur est informé suffisamment à temps, il peut éviter d'être dans une situation dangereuse. (Moustafa & Zhang, 2009) (Layouni, Weslem, Raphael, & Tran, 2010):

6.2. Applications de confort

Aujourd'hui, les hotspots (zone wifi à accès Internet) sont de plus en plus développés dans les villes, en particulier avec les initiatives des communautés et les opérateurs de télécommunication. Les passagers des voitures ou des transports collectifs pourront ainsi jouer en réseaux, ou encore même naviguer sur Internet. (L'information passe d'une voiture à une autre jusqu'au point d'accès internet le plus proche).

Outre l'utilisation d'internet sur la route, il existe d'autres applications aussi importantes telles que '*la gestion des espaces libres dans les parkings*', Ce service permet de rassembler des informations sur la disponibilité de places libres de stationnement dans les parkings et les guider jusqu'au point de stationnement le plus proche par exemple. (Moustafa & Zhang, 2009) (Huang & Kung, 2009)

7. Conclusion

Les réseaux VANETs attirent de plus en plus l'attention des chercheurs ces dernières années. Les applications de communication dans ces réseaux sont nombreuses telles que l'amélioration de la sécurité routière, l'accès à Internet, le désengorgement de la circulation ...etc.

Les réseaux de véhicules sont donc une des réponses à ce nouveau besoin grâce à un faible coût et un gain de temps. Nous avons défini dans ce chapitre les réseaux véhiculaires, leurs caractéristiques, leurs applications, et leurs technologies les plus utilisées.

Dans ce qui suit, nous allons introduire notre problématique liée au contrôle d'accès au medium MAC dans les réseaux véhiculaires, les différentes méthodes utilisées, et les protocoles et les standards existants.

Chapitre 2
MAC pour les réseaux VANETs

1. Introduction

VANETs est un réseau distribué dans lequel les nœuds partagent les mêmes ressources comme le spectre de la communication radio. Mais, si tous les mobiles émettent en même temps, il y a de grandes chances pour que les signaux interfèrent et donc ne peuvent être décodables (on peut faire une analogie avec les êtres humains : si tout le monde parle en même temps dans une pièce, il y a peu de chance pour que les gens se comprennent (Lassous, 2008). Il est donc important de contrôler l'accès au médium radio. Ce mécanisme de contrôle est appelé protocole de la couche MAC.

Le rôle d'un protocole MAC est de déterminer qui peut parler, quand et où. Un protocole MAC permet donc à plusieurs nœuds de se connecter au même canal pour transmettre leurs données. Ce canal doit être partagé de manière à ce que la communication soit rapide, fiable et en diminuant les collisions, mais pour atteindre ces objectifs, plusieurs défis et problèmes de conception doivent toujours être adressés au niveau MAC. Ces défis seront discutés dans la prochaine section.

Dans la littérature, nous distinguons plusieurs protocoles de la couche MAC, qui ont été proposés pour les MANETs. Ces protocoles fonctionnent dans certaines situations et certains scénarios, mais ils ont toujours une certaine faiblesse, particulièrement quand les nœuds sont fortement mobiles, comme dans les réseaux VANETs. En plus, les réseaux MANETs diffèrent des réseaux VANETs par les contraintes et les caractéristiques, comme par exemple, la contrainte d'énergie qui est considérée principale dans les approches proposées pour MANETs, n'est pas une contrainte pour les VANETs. De ce fait, les réseaux VANETs ont besoin de leurs propres protocoles qui considèrent seulement les caractéristiques des environnements véhiculaires.

Le but de ce chapitre est de mettre en évidence l'importance de la couche MAC dans les communications inter véhiculaires V2V et entre véhicule et infrastructure V2I, et de montrer les problèmes et les défis MAC dans les réseaux véhiculaires. Ainsi nous allons recenser les principales solutions protocolaires récentes qui peuvent être utilisées dans un contexte des réseaux véhiculaires.

2. Définitions

Nous allons présenter quelques définitions liées à la couche MAC dans un réseau sans fil :

Les collisions Quand deux ou plusieurs trames sont émises simultanément sur le support radio, et elles se heurtent, les collisions surviennent car les données deviennent inexploitables et doivent être abandonnées. Les collisions engendrent des retards dans les livraisons des

messages au niveau des nœuds: source et destination suite aux retransmissions. Tous les protocoles MAC essayent à leur manière d'éviter les collisions, soit par conception (répartition fixe) ou par des procédures appropriées pour éviter les collisions comme CSMA/CA. Les collisions concernent plutôt les protocoles MAC avec contention. Toutes ces approches vont être développées dans ce chapitre. (Terre, 2007) (Kacimi, 2009)

L'overhead des paquets de contrôle l'envoi, la réception, et l'écoute des paquets de contrôle consomment de la bande passante. Comme les paquets de contrôle ne transportent pas directement des données, ils réduisent également le débit utile actif. (Kacimi, 2009)

3. Défis et problèmes MAC

Les défis les plus importants de la couche MAC pour les VANETs sont (Booysen, Zeadally, & Rooyen, 2011) (Hartenstein & Laberteaux, 2010) (Hartenstein & Laberteaux, 2010) (Moustafa & Zhang, 2009):

- **Manque du contrôle centralisé**

Dans les scénarios V2I, des méthodes MAC centralisées pourraient être utilisées, puisque l'infrastructure ou **RSU** (Road Side Unit) pourrait agir en tant que coordonnateur. Cependant, dans les scénarios V2V purs, aucune coordination centralisée n'est disponible pour contrôler et coordonner l'accès au medium. Le principal défi est de déterminer qui assure le contrôle d'accès au medium dans le mode ad hoc et comment les slots de temps et les canaux sont partagés entre les véhicules qui sont dans la même portée de communication afin de partager le canal d'une manière efficace et distribuée.

- **Besoin des protocoles spécifiques pour les VANETs**

Le but principal des réseaux VANETs est d'améliorer la sécurité routière et le confort des conducteurs. Ces réseaux, comme précédemment dit, bien qu'ils se dérivent des réseaux MANETs, ils ont leurs propres caractéristiques. Donc, ils ont besoin de leurs propres protocoles de communication pour bien fonctionner. Ces protocoles jouent un rôle important dans les réseaux à diffusion, où tous les utilisateurs sont susceptibles d'émettre et de recevoir à n'importe quel moment.

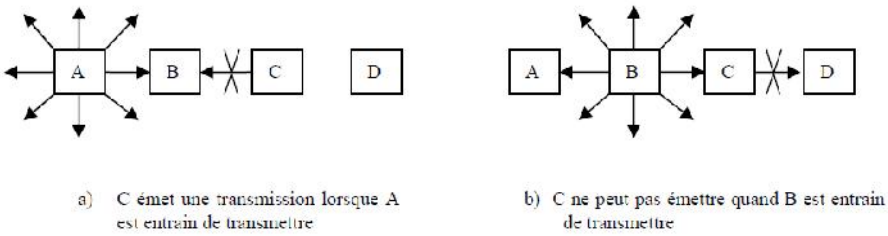
- **Le problème des stations cachées**

Ce problème se produit quand deux stations ne peuvent pas s'entendre du fait que la distance qui les sépare est trop grande ou bien un obstacle les empêche de communiquer mais elles ont des zones de couverture qui se recouvrent. Si les stations A et C ne sont pas en mesure de s'entendre, elles vont s'autoriser à émettre des paquets en même temps à une station B située dans l'intersection des zones de couverture, il va y avoir donc une collision entre les paquets, donc le nœud B ne pourra recevoir aucune donnée des communications. On dit que les stations A et C sont cachées l'une par rapport à l'autre. (Voir la figure 2.1.a)

- **Le problème des stations exposées**

Ce problème arrive dans le cas où une station B transmet des données à une station A. Si une station C écoute le canal radio, elle peut entendre une communication en cours. Elle conclut

par la suite qu'elle ne peut pas transmettre des paquets à une station D (qui n'est pas dans la portée du nœud A), donc si C transmettait le paquet, cela créerait des collisions seulement dans la région entre B et C et non dans les régions où D et A se situent. D'où les transmission entre A et B d'une part et entre C et D d'autre part peuvent se réaliser sans risque de collision (Voir la figure 3.1.b)



a) C émet une transmission lorsque A est entrain de transmettre

b) C ne peut pas émettre quand B est entrain de transmettre

Figure 2-1 Problème de la station cachée et de la station exposée (Hung-Cuong, 2008)

- **Largeur de bande**

Le spectre radio est considéré comme une ressource critique ayant une largeur de bande très limitée. Cette largeur de bande devrait être employée efficacement pour diminuer le contrôle d'overhead.

- **Qualité de service**

Le médium radio ne présente pas les mêmes caractéristiques qu'un médium filaire, car ce n'est pas possible d'accroître indéfiniment la bande passante allouée aux communications radios contrairement au monde filaire. Il est donc nécessaire d'avoir des solutions de qualité de service performantes et adaptées aux spécificités de ce type de réseaux. La qualité de service est l'un des principaux problèmes des réseaux sans fils. Les conditions de QoS pour des messages de sûreté sont différentes de ceux des médias .Il faut garantir que les messages de sécurité seront envoyés de telle façon à ce que le récepteur ait suffisamment de temps pour répondre. Par contre, dans les applications multimédia, il est suffisant de garantir une QoS qui permet une livraison claire et déchiffrable à l'utilisateur

Les premières normes 802.11 commercialisées (802.11a b et g) ne gèrent aucune priorité. Une nouvelle norme 802.11 intégrant la qualité de service est apparue, c'est la norme 802.11e, elle représente la base de la norme 802.11p, cette dernière est le sujet de notre étude et elle va être présentée dans le chapitre suivant. (KSENTINI, 2005)

- **Synchronisation**

La synchronisation entre les nœuds dans un réseau sans fil est très importante. Dans un réseau centralisé, la synchronisation est facile à contrôler puisque le réseau a une horloge commune qui est l'horloge de l'infrastructure centralisée. Ce n'est pas le cas pour les réseaux VANETs qui sont totalement distribués, mais puisque les véhicules peuvent être équipés des systèmes de positionnement, tels que le GPS, qui peut fournir une horloge commune dans le réseau, la synchronisation peut être ainsi assurée.

- **Mobilité des nœuds**

Si les nœuds n'étaient pas mobiles dans les VANETs, l'établissement d'un protocole d'accès au canal serait fait d'une façon statique où le medium est assigné à l'avance aux nœuds communicants. Mais dans les réseaux ads-hoc véhiculaires, tous les nœuds sont mobiles et leur mobilité est élevée. Il n'est donc pas possible de connaitre le nombre de véhicules qui partagent le canal.

- **Collision**

Puisque les émetteurs et les récepteurs sans fil ne peuvent pas transmettre et recevoir simultanément, la collision n'est pas détectée directement lors de l'émission, et comme il se produit souvent que les nœuds dans un même voisinage essayent d'accéder au canal en même temps, la probabilité de collision est tout à fait élevée dans les MANETs, comme dans les VANETs. Ainsi, le rôle d'un protocole MAC est de réduire autant que possible ces collisions car les collisions et les interférences dégradent sévèrement les performances du système de communication.

- **Partage équitable du canal**

La couche MAC doit assurer le partage équitable du canal entre toutes les stations sans fil et offrir l'accès prévisible au medium partagé.

- **Passage à l'échelle**

Les réseaux VANETs ont besoin d'être 'scalable', et d'assurer le fonctionnement du réseau dans les cas d'une densité véhiculaire faible ou élevée.

4. Les méthodes d'accès au medium pour les réseaux VANETs

Un des aspects principaux d'un protocole de communication dans un réseau est la couche MAC. Elle détermine le nœud qui accède au medium physique. Les protocoles d'accès au medium sont basés sur deux mécanismes d'allocation : statique et dynamique. Un mécanisme d'allocation statique attribue un canal de communication de façon permanente, comme la méthode FDMA, tandis que le mécanisme dynamique est capable de s'adapter à l'environnement. (Bénédicte, Julien, Arnaud, Eric, & Laurent, 2002) .Actuellement, un mécanisme statique seul n'est plus utilisé.

Les mécanismes MAC ont pu être classés par catégorie comme basé-contention (contention-based) et contention-libre (free-contention). Les approches basées contention se basent sur l'écoute du signal (de la porteuse), les backoffs et les tentatives de retransmettre en cas de collision, tandis que les approches free-contention s'appuient sur les attributions alternatives de ressources (temps et bande passante) et sur la synchronisation de temps (qui est généralement divisée en périodes). Les mécanismes MAC pourraient également être classés selon l'entité qui contrôle l'accès au médium. (Booysen, Zeadally, & Rooyen, 2011)

Les travaux de recherche dans les protocoles d'accès au canal pour les réseaux VANETS ont pour but la minimisation du temps de latence et l'augmentation de la fiabilité du réseau.

Au début, les solutions proposées pour les réseaux VANETs se concentraient seulement à la sécurité routière, d'où la bande passante était moins importante car dans les applications de sécurité, seulement des messages de petites tailles seront envoyés mais ces messages doivent être transmis rapidement et avec un taux de perte minimum. Actuellement, les chercheurs considèrent les autres types d'application des VANETs comme étant le déploiement futur de ces réseaux véhiculaires, ils proposent donc des solutions MAC qui visent à augmenter la qualité de service pour des applications multimédias (partage de son et de vidéo,…).

Nous présentons dans cette partie les deux catégories des protocoles d'accès au canal, à savoir free-contention et based-contention pour les réseaux sans fil et plus particulièrement pour les réseaux véhiculaires VANETs.

4.1. Les mécanismes d'allocation du support planifiés (Scheduled ou free-contention

4.1.1. Méthode FDMA : Frequency Division Multiple Access

C'est la technique la plus ancienne, elle était la seule lorsque le téléphone était purement analogique, elle consiste à effectuer un découpage fréquentiel du spectre. On obtient ainsi plusieurs porteuses contenues dans la bande de fréquence allouée. Chacune de ces porteuses reçoit une communication (et une seule à un moment donné). Deux signaux pouvant collisionner doivent être émis dans des porteuses différentes. Il faut donc être en mesure d'allouer intelligemment les porteuses aux mobiles concernés. Les différentes porteuses ainsi modulées sont juxtaposées et l'ensemble transmis sur le canal. A la réception, des filtres sélectifs isolent les différentes porteuses qui sont démodulées.

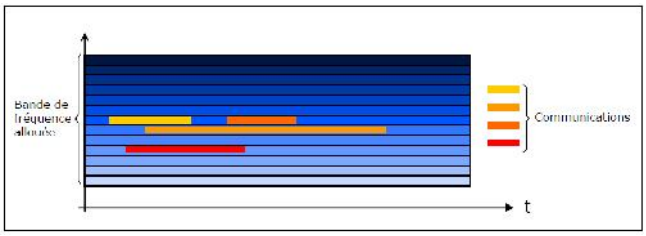


Figure 2-2 La méthode FMDA. (Bénédicte, Julien, Arnaud, Eric, & Laurent, 2002)

Ce mécanisme est surtout utilisé pour transmettre les signaux TV sur le câble, ou sur les canaux Hertziens et par le satellite. Il présente quelques inconvénients, comme:

- Chaque utilisateur monopolise une porteuse et ce même lors des phases de silence.
- Si une gamme de fréquences présente des zones d'ombre, le client perd toute la communication. (Bénédicte, Julien, Arnaud, Eric, & Laurent, 2002) (Mohamed, 2009)

4.1.2. Méthode TDMA : Time Division Multiple Access

Ce mode d'accès fonctionne sur un partage de la ressource physique dans le temps : chaque porteuse est découpée en éléments temporels appelés Slots (Slot-Time). Un slot

représente (BADIS, 2005) le temps nécessaire pour détecter la transmission d'un paquet par une autre station. Donc, il dépend fortement de la couche physique, délais de propagation et le temps pour signaler l'état du canal à la couche MAC. La trame TDMA est définie comme étant égale à huit slots. Lorsqu'un client accède au réseau, un slot lui est assigné (porteuse fixe et numéro de slot, de 1 à 8, dans la trame). Ce client conserve ce slot sur cette fréquence durant toute la durée de sa communication.

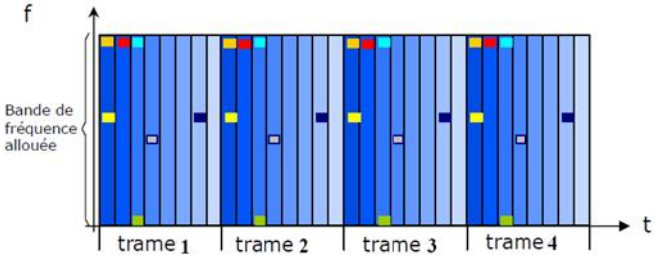


Figure 2-3 Le mécanisme TDMA. **(Bénédicte, Julien, Arnaud, Eric, & Laurent, 2002)**

Un nœud ne peut pas accéder au canal pendant l'intervalle de temps réservé à un autre. De ce fait, il n'y a jamais de collision dans ce type de protocole MAC. Cependant, il faut toujours avoir un ou plusieurs nœuds coordinateurs qui attribuent les intervalles de temps aux autres. Pour que TDMA puisse bien fonctionner, il faut une bonne synchronisation entre les nœuds. Quand la topologie du réseau change, il faut changer aussi les intervalles de temps attribués aux nœuds (Hung-Cuong, 2008).

Cette technique est bien plus intéressante que FDMA en termes de taux d'utilisation du canal. Elle a été utilisée par le GSM jusqu'en 2000 (aujourd'hui, dans la nouvelle norme GSM, les paquets propres à une communication changent de fréquence à chaque trame, ce qui assure une meilleure qualité de service moyenne : chaque utilisateur profite de l'ensemble de la gamme de fréquence).
Cependant, l'attribution des intervalles de temps de TDMA est effectuée d'une manière statique. Si un nœud se voit attribuer un intervalle de temps et qu'il n'a pas de données à transmettre, il ne peut pas laisser cet intervalle de temps à quelqu'un d'autre. C'est aussi un gaspillage de la bande passante et du temps. D'ailleurs, l'approche centralisée de TDMA nous semble moins adaptée aux réseaux véhiculaires, car nous voulons une gestion totalement distribuée pour un réseau à grande échelle. (Hung-Cuong, 2008) (Bénédicte, Julien, Arnaud, Eric, & Laurent, 2002)

4.1.3. Méthode CDMA : Code Division Multiple Access

Dans la méthode d'accès CDMA, tous les utilisateurs ont accès simultanément à la totalité de la bande passante. Cependant, dans les protocoles d'accès multiple, par écoute de porteuse, lorsque plusieurs nœuds transmettent en même temps dans la même portée, il y aura une collision, et le récepteur reçoit seulement un bruit. Ce n'est plus le cas dans CDMA où différentes trames peuvent se chevaucher de façon linéaire, En effet, chaque utilisateur est différencié des autres utilisateurs par un code qui lui a été alloué au début de sa communication.

Pour transmettre les données, le message A de l'émetteur 1 est multiplié par son code alloué CA, ce qui donne la séquence A*CA à envoyer dans le support de communication. Ce code doit être orthogonal au reste des codes liés aux autres utilisateurs, pour que plusieurs trames de données puissent se chevaucher sans perte de données, ce qui veut dire que les codes sont choisis tels que le produit scalaire entre deux codes CA et CB (CA*CB) des messages A et B respectivement, soit nul et CA.CA soit maximum (ie, codes orthogonaux = produit scalaire nul). (ACCES MULTIPLE A REPARTITION PAR CODE (CDMA), 2003)

Le récepteur utilise le code de son transmetteur pour déchiffrer les trames. En utilisant le code de l'émetteur, tous les bruits créés par les autres transmetteurs sont détruits et le récepteur peut recevoir une bonne trame de données, même s'il y a des interférences. (ACCES MULTIPLE A REPARTITION PAR CODE (CDMA), 2003)

4.1.4. Méthode SDMA : Space Division Multiple Access

Space Division Multiple Access (SDMA) utilise les antennes directionnelles afin de permettre à une station de transmettre vers une direction où elle ne risque pas d'interférer avec d'autres.
Dans cette méthode, les utilisateurs sont répartis dans l'espace et la communication entre le mobile et la station de base se fait par le biais d'un faisceau unique rayonné par l'antenne de cette dernière.
Le principe du SDMA repose sur le concept d'antenne intelligente, appelée ainsi par opposition aux antennes ayant un diagramme de rayonnement fixe, qu'il soit omnidirectionnel ou sectoriel. Les différents utilisateurs sont donc séparés grâce aux diagrammes de rayonnement formés par l'antenne. L'espace autour du nœud est divisé à des différents angles. La station de base forme ainsi un faisceau dans la direction du mobile utile et des zéros vers les interférents. L'implantation d'une antenne réseau permet d'augmenter la capacité du système. En effet, le signal de transmission est concentré seulement dans la direction du récepteur. Cela permet d'augmenter la gamme de couverture et la réutilisation spatiale et de réduire les interférences et les collisions lors des transmissions.
Dans la pratique, le SDMA est utilisé en combinaison avec une ou plusieurs techniques d'accès multiple. Même si le concept du SDMA existe depuis plusieurs années, il n'est pas encore utilisé à grande échelle pour des applications publiques à cause de la complexité des calculs requise par son établissement. (Mazen, 2009)

4.2. Les méthodes d'accès aléatoires (based-contention)

4.2.1. ALOHA pour les communications sans-fil

Le protocole ALOHA pur (original) a été développé en 1971. Le mot ALOHA, qui veut dire tout simplement Hello explique son fonctionnement.

Dans ALOHA, dès qu'un paquet arrive à la couche MAC, il est immédiatement transmis sur le support physique. S'il y a eu une collision, l'émetteur renvoie le paquet après un temps aléatoire, afin d'éviter les collisions répétées. De plus, quand la station de base reçoit un paquet, elle vérifie que le code correcteur contenu dans le paquet, est correct, dans ce cas elle

envoie un accusé de réception à l'émetteur. (Bénédicte, Julien, Arnaud, Eric, & Laurent, 2002) (Ksentini, 2005)

L'avantage principal du protocole ALOHA est sa simplicité, car il ne nécessite pas de synchronisation. En revanche, la probabilité élevée de collisions réduit le débit effectif d'ALOHA pur. (Bénédicte, Julien, Arnaud, Eric, & Laurent, 2002) (Ksentini, 2005)

4.2.2. Le protocole slotted ALOHA

Cette version améliore ALOHA pur en partageant le temps en éléments appelés « slots ». L'émetteur ne commence sa transmission qu'au début d'un slot, ce qui permet de réduire les collisions partielles. La synchronisation est effectuée grâce à un signal périodique (Beacon) envoyé par la station de base. Deux paquets n'entrent en collision que s'ils sont prêts à être émis dans le même slot. En fonction du type de transmission sélectionnée (CDMA…), le traitement des collisions diffère. (Bénédicte, Julien, Arnaud, Eric, & Laurent, 2002) (Ksentini, 2005)

4.2.3. Le protocole CSMA

CSMA / CA

Les mécanismes de détection de collisions CSMA/CD s'avèrent adaptés pour un réseau local câblé; ils ne le sont pas, en général, pour les réseaux radio.

Plusieurs raisons pour cela:

- Dans un environnement sans fil, on ne peut pas être sûr que toutes les stations s'entendent entre elles (ce qui est l'hypothèse de base du principe de détection de collision), et le fait que la station voulant transmettre teste si le support est libre, ne veut pas forcément dire que le support est libre autour du récepteur.

- Le problème des stations cachées et le problème des stations exposées.

Pour résoudre ces problèmes, la norme 802.11 utilise le mécanisme d'évitement de collision (Collision Avoidance) appelé CSMA/CA. CSMA/CA est une méthode d'accès de la même famille que CSMA/CD (Carrier Sense Multiple Access with Collision Detection. Dans CSMA/CA, les collisions ne peuvent pas être détectées comme dans le CSMA/CD, un nœud essaie d'éviter les collisions (sans pouvoir les éviter à 100%). Ceci est à cause de l'effet d'aveuglement du médium sans fil (Near Far Effect) qui empêche une entité de recevoir quand elle est entrain d'émettre. (Chalhoub, 2010)

Généralement, nous distinguons trois types de CSMA :

- 1-persistent CSMA, qui consiste à continuer à écouter le canal et émettre immédiatement lorsque le canal se libère.
- p-persistent CSMA, qui consiste à continuer à écouter le canal et émettre immédiatement avec une probabilité p.
- non-persistent CSMA, qui consiste à attendre un temps aléatoire avant d'émettre. (Ksentini, 2005)

L'algorithme de bachoff

Le mécanisme de tirage aléatoire (Random Backoff) du délai d'attente est utilisé dans le mécanisme CSMA/CA. Cette procédure permet de diminuer la probabilité de collision qui augmente lorsque le canal se libère. Elle est appliquée lorsque le canal devient occupé alors que d'autres stations sont en attente pour transmettre ou bien lors d'une collision.
Il s'agit, donc, de tirer un nombre n dans un intervalle de temps appelé fenêtre de contention [0,CW] selon la formule suivante :

$$BackoffTime = Random(0,CW) * SlotTime.$$

Lorsque le canal devient libre, la station attend de nouveau un temps DIFS *(à présenter dans la section suivante)* avant de décrémenter son Backoff slot par slot jusqu'à ce que ce dernier atteigne la valeur zéro ou que le canal devienne occupé.
Dans ce dernier cas, le processus est arrêté et reprendra lorsque le médium devient, à nouveau, libre i.e. la station devra attendre de nouveau un temps fixe DIFS et son nouveau Backoff correspondra au nombre de slots restants lors de l'arrêt du processus. Une fois que le Backoff atteint la valeur nulle, le paquet peut être émis par la station. Si la transmission échoue, elle sera ainsi différée et le processus est réitéré mais en doublant la valeur de la fenêtre de contention CW.
Après un certain nombre de tentatives de transmissions échouées, le processus est abandonné et les couches supérieures sont informées de l'incident.
Grâce à cet algorithme, les stations auront la même probabilité d'accéder au support. (Siad, 2007) (Nehdi, 2005)

5. Conclusion

Dans ce chapitre, nous avons montré l'importance de la couche MAC dans les réseaux véhiculaires, et les principaux défis et conflits MAC. Nous avons présenté les principales approches MAC : à savoir les approches basées contention (based-contention), et les approches aléatoires (free-contention).
Nous allons présenter dans le chapitre suivant, les normes et standards liés aux réseaux véhiculaires VANETs, à savoir le WAVE, DSRC, 802.11 et plus précisément 802.11p et la série P1609.x (1-4).

Chapitre 3
Les standards MAC pour VANETs

1. Introduction

Les systèmes de transport intelligents sont en développement depuis les années 1990. Leur but est d'automatiser les interactions entre les véhicules et l'infrastructure pour atteindre des niveaux élevés de sécurité, de confort et d'efficacité. Les communications, en général, et les gestions de réseaux en particulier, ont été des éléments essentiels dans l'évolution de ces systèmes.

La norme IEEE a mis au point une architecture de système connue sous le nom WAVE pour fournir un accès sans fil dans des environnements véhiculaires.

Dans ce chapitre, nous passons en revue les différents standards et normes proposés afin d'assurer les communications véhiculaires. Nous commençons tout d'abord par une présentation de la bande DSRC. Ensuite, nous étudions la norme IEEE 802.11 dans le cadre des réseaux véhiculaires. Nous aborderons après le mode WAVE, la norme 802.11p ainsi que la série des standards P1609, et ETSI.

2. DSRC : Dedicated Short Range Communication

DSRC est le nom de la bande passante allouée aux communications des systèmes de transports intelligents ou ITS (Intelligent Transport System).

DSRC est une norme de communication de courte à moyenne portée (1000 m), qui permet d'échanger des données des applications de sécurité routière publique et privée en utilisant les communications V2I et V2V tout en offrant un taux de transfert de données important. DSRC utilise la bande de fréquence de 5.850GHz à 5.925GHz. En Amérique du nord, le spectre DSRC se compose de 8 canaux (un canal de 5MHz pour utilisation future, et 7 canaux de 10MHz). (Moustafa & Zhang, 2009).

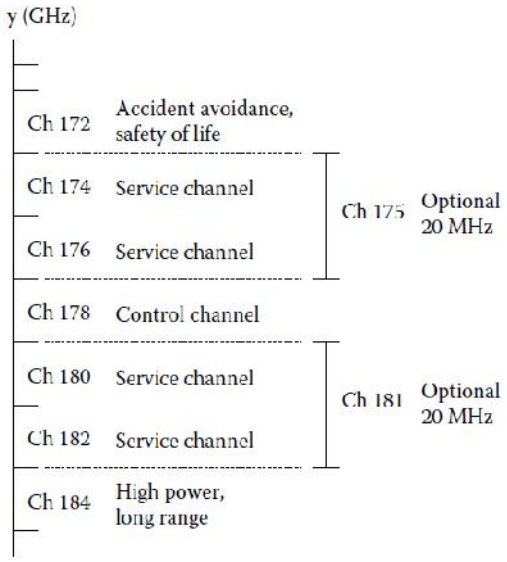


Figure 3-1 Allocation de DSRC en Amérique du Nord (Moustafa & Zhang, 2009)

3. IEEE 802.11

L'IEEE a lancé vers le début des années 90 (1993), le projet de définition d'un standard décrivant les caractéristiques d'un réseau local sans fil (WLAN). C'est la norme IEEE 802.11 qui est en réalité la norme initiale offrant des débits de 1 ou 2 Mbps. Des révisions ont été apportées à la norme originale afin d'optimiser le débit (c'est le cas des normes 802.11a, 802.11b, 802.11g et 802.11p). Son objectif principal est de développer une couche physique et une couche MAC permettant d'offrir une connexion sans fil à toute station aussi bien fixe que mobile. (Siad, 2007) (Nehdi, 2005)**.**

3.1. Modes de fonctionnement

Les réseaux compatibles au standard 802.11 s'organisent suivant deux architectures de réseaux : Ad Hoc et Infrastructure.

a) Le mode infrastructure

Dans ce mode, le réseau sans fils est constitué d'un point d'accès AP connecté à un réseau fixe, et d'un ensemble de stations clients sans fil. Cette configuration est basée sur une architecture cellulaire. Dans la norme 802.11, chaque cellule (appelée aussi **ensemble de service de base ou Basic Service Set : BSS**) est contrôlée par une station de base (**AP**).Les stations dans une BSS exécutent le même protocole Mac, et ils sont en concurrence pour accéder au même support de transmission. (Siad, 2007).

b) Le mode Ad Hoc

A la différence d'un réseau avec infrastructure, un réseau Ad Hoc ne comporte aucun point d'accès et fonctionne de manière totalement distribuée. La norme 802.11, désigne par IBSS (**Independent Basic Service Set**) l'ensemble des stations sans fil à portée radio mutuelle. Par conséquent, une station en dehors de la portée radio ne peut pas être atteinte par une transmission directe. (Siad, 2007)

Pour prévoir une large couverture, plusieurs BSSs sont employés. Pour les connecter, leurs points d'accès sont reliés par un système distribué **(DS : Distribution System).** Le tout interconnecté (au moins deux BSSs et un point d'accès et le DS) est vu comme étant un réseau logique IEEE 802 au niveau de la couche LLC, et il s'appelle l'ensemble prolongé de service (**ESS : Extended Service Set).** (Labiod, Afifi, & Detantis, 2007)

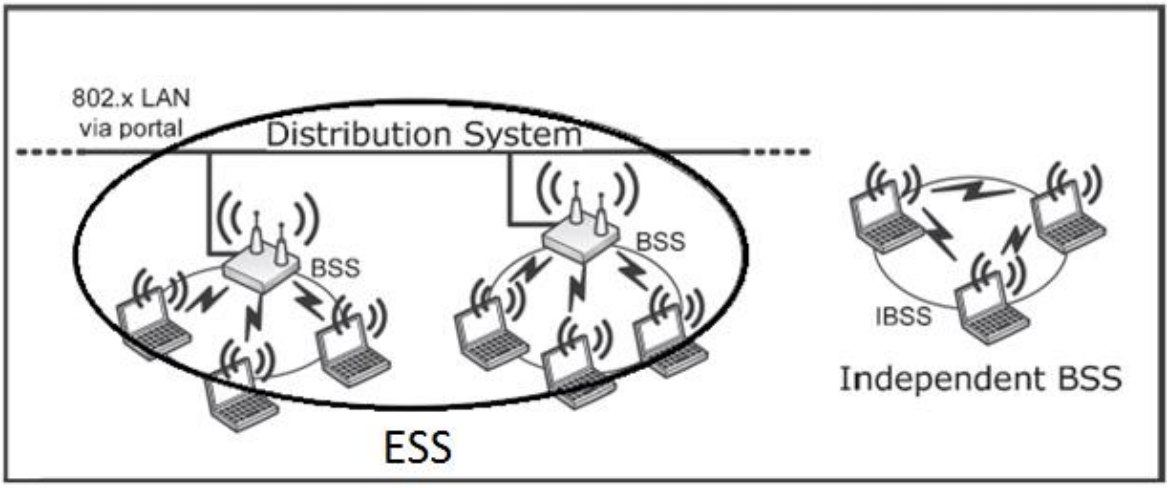


Figure 3-2 Le mode infrastructure et le mode ad hoc de 802.11. (Labiod, Afifi, & Detantis, 2007)

3.2. Description des couches

La norme IEEE 802.11, comme toute autre norme IEEE 802, concerne les deux dernières couches basées du modèle ISO (interconnection of the open systems), la couche physique PHY et la couche liaison de données qui contient les deux sous couches : couche MAC et la couche LLC comme illustré dans la figure suivante.

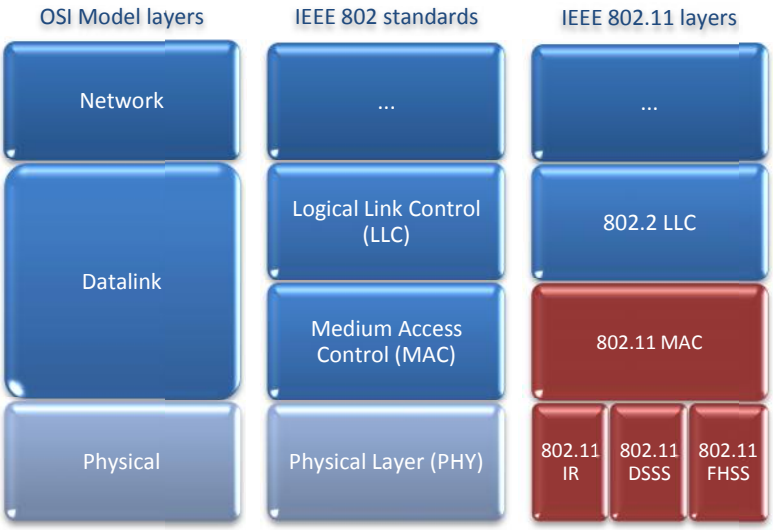


Figure 3-3 La norme 802.11 dans la pile réseau.

La couche physique se charge des transmissions des trames de la couche MAC dans le support sans fil, elle utilise des techniques de modulation et d'encodage binaire. La couche MAC est décrite par la représentation de différentes fonctions (l'association, la fragmentation, le contrôle d'accès, etc.) et la structure de la trame MAC 802.11.

Le standard IEEE 802 définit la même sous couche LLC pour tous les réseaux LANs, c'est la sous couche LLC 802.2.

IEEE 802.11 définit donc seulement la couche MAC et la couche physique.

3.2.1. La couche physique

La couche physique (PHY) définit la modulation des ondes radio- électriques et les caractéristiques de la signalisation pour la transmission de données.
La norme IEEE 802.11 définit deux sous-couches physiques : la sous couche **PMD (Physical Media Dependant)** et la sous couche **PLCP (Physical Layer Convergence Procedure).** La sous-couche PMD gère l'encodage des données et la modulation, tandis que la sous-couche PLCP s'occupe de l'écoute du support, elle est directement reliée à la couche MAC pour lui indiquer l'état du support (libre ou non). (Tibi & Tabbana, 2005). (Dridi, 2011)
Sur les deux bandes (ISM 'industriel, scientifique, et médical' et la bande des 5 GHz), on trouve essentiellement quatre techniques de transmission:

a) La technique FHSS : Frequency Hoping Sprend Spectrum

Elle offre un débit de 1 ou 2 Mbps. La bande passante utilisée est entre 2,4 et 2,483 GHz de l'ISM (Industrial, Scientific, Medical). Le principe de cette technique consiste à découper la bande passante en sous canaux (75 sous canaux de 1 MHz). Pour transmettre les données, l'émetteur et le récepteur s'accordent sur une séquence prédéfinie de sauts. Les avantages de FHSS sont nombreux. En effet, elle empêche la perte totale du signal et permet de réduire les risques de collision. En contre partie, cette technique limite le débit à 2 Mbps. (Siad, 2007) (Labiod, Afifi, & Detantis, 2007)

b) La technique DSSS Direct Sequence Sprend Spectrum

Cette technique utilise la bande de fréquence 2,4-2,4835 GHz. Elle divise la bande de fréquence en 14 sous canaux de 22 MHz. La transmission ne se fait que sur un sous canal. La largeur de la bande ISM étant égale à 83.5 MHz, il est impossible d'y placer 14 canaux adjacents de 20 MHz. Donc, les canaux se recouvrent. (Siad, 2007)
Comme la transmission ne se fait que sur un canal, les systèmes DSSS sont plus sensibles aux interférences que les systèmes FHSS, qui utilisent toute la largeur de la bande.

c) La technologie Infrarouge IR (Infra Red)

L'utilisation des ondes infrarouges est une autre solution pour envoyer des données dans un réseau 802.11. Cependant, la nature lumineuse de ces ondes ne permet pas de traverser des obstacles (tel qu'un mur). De plus, cette technologie a une faible portée (environ 10m),et elle ne permet pas d'atteindre des débits extrêmement élevés. (Siad, 2007) (Labiod, Afifi, & Detantis, 2007)

d) La technique OFDM : Orthogonal Frequency Division Multiplexing

La couche physique utilisant la technique OFDM a été définie dans la bande des 5.2 GHz. Son principe est basé sur un multiplexage fréquentiel de sous-porteuses. L'objectif de concevoir de telles techniques est de répondre aux nouveaux besoins en terme de débit pour atteindre jusqu'à 54 Mbits/s. (Siad, 2007)

Pour atteindre cet objectif, l'approche traditionnelle consiste à réduire la durée d'un symbole, mais cela augmente aussi les problèmes de chemins multiples. OFDM propose donc d'utiliser des symboles plus longs, mais envoyés en parallèle. En résumant cette méthode, « l'agrégation d'un certain nombre de canaux lents donne de meilleurs résultats que l'utilisation d'un seul canal très rapide, en présence de chemins multiples, à débit total équivalent ». (Ksentini, 2005) (Labiod, Afifi, & Detantis, 2007)**.**

3.2.2. La sous-couche MAC dans IEEE 802.11

La couche liaison de données de la norme 802.11, se compose essentiellement de deux sous-couches : la couche liaison de données notée LLC (Logical Link Control) et la couche MAC (Medium Access Control).

La sous-couche LLC de 802.11 définit les mêmes propriétés que la sous-couche LLC de 802.2.

La sous-couche MAC, quant à elle, est spécifique à 802.11. Elle définit, entre autres, la méthode d'accès, et l'interface entre le bus de la machine et la couche physique. Elle offre d'avantage de fonctions par rapport à une couche MAC classique (allocation du support, adressage, formatage des trames). Ces fonctions supplémentaires offertes sont généralement confiées aux protocoles supérieurs, comme les sommes de contrôle Cyclic Redundancy Check (CRC), la fragmentation et le réassemblage (très utile car le support radio a un taux d'erreurs important), les retransmissions de paquets et des accusés de réception.

Cela ajoute de la robustesse à la couche MAC 802.11 (Ksentini, 2005).

Plusieurs **services MAC** sont fournis par la norme:

• Le service MAC de base qui est un service d'échange de trames MAC de type BE (best-effort) sans connexion. Ce service permet de délivrer un paquet sans garantie de service. (Technique DCF).

• Le service de livraison de trames MAC plus adapté au trafic de données de type temps réel, ce service est un service optionnel du standard. (Technique PCF).

• Le service de confidentialité fourni par l'algorithme **Wired Equivalent Privacy (WEP)** qui permet la confidentialité, l'authentification, le contrôle d'accès et la gestion de couche.

• Le service de reséquencement qui permet, si nécessaire, de remettre en ordre les trames MAC reçues (Cavagna & Nuaymi, 2004) (Dridi, 2011)**.**

Le standard 802.11 est particulier, en effet, il définit deux méthodes d'accès extrêmement différentes au niveau de la sous-couche MAC. Le premier est le **DCF (**Distributed Coordination Function), qui correspond à une méthode d'accès assez similaire à celle des réseaux traditionnels supportant le best-effort. Le DCF a été conçu pour prendre en charge le

transport de données asynchrones, dans lequel tous les utilisateurs qui veulent transmettre des données ont la même chance pour accéder au support.

Le second mécanisme d'accès est le Point Coordination Function (PCF). Il se base sur l'interrogation à tour de rôle des terminaux, ou polling, sous le contrôle du point d'accès.
La méthode PCF est conçue essentiellement pour la transmission de données sensibles, qui demandent une gestion de la QoS. PCF est utilisé pour les applications temps réel, telles que la voix ou la vidéo.

Un réseau en mode ad-hoc utilise uniquement le DCF, tandis qu'un réseau en mode infrastructure utilise à la fois le DCF et le PCF (Ksentini, 2005).

a) La méthode d'accès DCF

DCF est un mécanisme de couche MAC distribué. Il est basé sur le protocole CSMA/CA. Pour contrôler l'accès au support et les transmissions contiguës, les stations séparent les trames par des intervalles de temps appelés entre-trames, ou **Inter-Frame Spacing (IFS),** qui correspondent à l'intervalle de temps entre deux transmissions successives du même nœud. Les intervalles IFS sont des périodes d'inactivité sur le support de transmission. Les valeurs des différents IFS sont calculées par la couche physique.
Le standard définit quatre types d'IFS:

- Short IFS (SIFS): c'est le plus petit des IFS, il est utilisé pour séparer les transmissions au sein d'un même dialogue (entre une trame émise et son acquittement par exemple ou entre plusieurs fragments d'une même trame).

- Point Coordination IFS (PIFS): ce type est utilisé par le point d'accès dans le mode PCF de IEEE 802.11 pour accéder avec priorité au support car PIFS < DIFS. Le PIFS correspond à la valeur du SIFS, auquel on ajoute un temps. Le PIFS est calculé de la façon suivante :

$$PIFS = SIFS + Slotime$$

- DCF IFS (DIFS): est utilisé dans le mode DCF de IEEE 802.11, il représente le temps minimal d'attente avant chaque transmission. Il est calculé comme suit :

$$DIFS = SIFS + 2\times Slotime$$

- Extended IFS (EIFS) : est utilisé par les stations opérantes en mode DCF. Il est supérieur au DIFS. Il est utilisé en cas de collision, pour éviter des collisions en série. Sa valeur est donnée par la formule suivante :

$$EIFS = 8 * tACK + SIFS + DIFS + tMAC + tPLCP$$

Avec : tACK : Durée de l'émission d'un acquittement
tMAC : Durée d'une encapsulation de la couche MAC

tPLCP : Durée d'une encapsulation de la couche PLCP (Tibi & Tabbana, 2005) (Siad, 2007).

Le fonctionnement du protocole :

- *Mécanisme de détection virtuelle*

La première opération effectuée par la station avant d'initialiser l'envoi d'une trame est de vérifier la disponibilité au préalable du support. Deux mécanismes sont utilisés à cet effet. Le premier est appelé **PCS (Physical Carrier Sense**). Il s'agit de détecter physiquement la porteuse en écoutant les signaux sur le canal.

Les stations utilisent un autre mécanisme appelé **VCS (Virtual Carrier Sense).** Il permet à celles-ci de réserver le canal pendant une période de temps fixe qui est mentionnée sur la trame de données. Cette information est exploitée par toutes les stations à portée de communication et elle est mise à jour et recopiée dans le vecteur d'allocation de réseau **NAV (Natwork Allocator Vector)** pour informer les autres stations que le canal est occupé. Le vecteur NAV contient, donc, l'estimation, par la station émettrice, du temps d'occupation du canal par la transmission en cours. Cette valeur est décrémentée à la fin de chaque période (slot) jusqu'à atteindre la valeur zéro, à ce moment, le canal est considéré comme libre.

Ces deux mécanismes sont utilisés de manière complémentaire. Une station voulant émettre vérifie d'abord la valeur de son NAV. S'il est nul, une deuxième vérification (PCS) est effectuée afin de confirmer si le canal est vraiment libre. Si l'écoute pendant un temps DIFS a confirmé que le canal est libre, alors la station peut envisager de transmettre. Lorsque les stations en écoute constatent une émission, ils déclenchent pour une durée fixée leur indicateur de **Virtual Carrier Sense (VCS) ou NAV**. Ils utiliseront cette information pour retarder toute transmission prévue. (Voir la figure suivante) (Tibi & Tabbana, 2005)

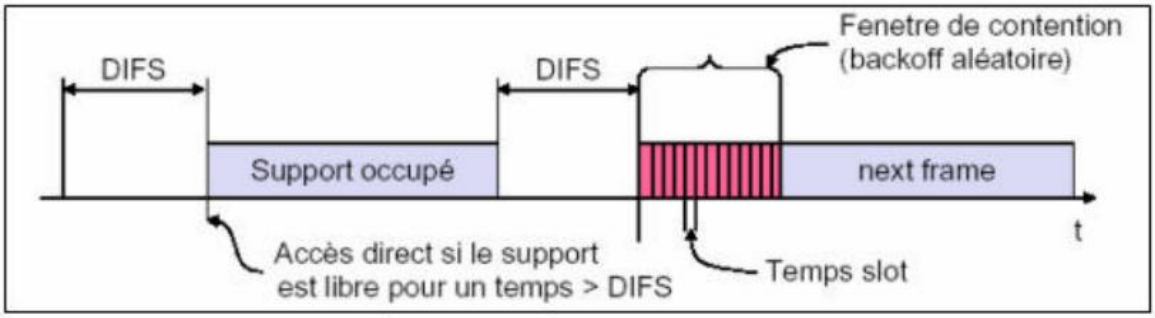


Figure 3-4 Le mécanisme DCF. (Tibi & Tabbana, 2005)

Dans le cas contraire (i.e NAV différent de zéro), la transmission est différée jusqu'à la libération du canal même si le canal est réellement libre. Au moment où la station trouve le canal occupé, le processus de backoff est initialisé, la station calcule un intervalle de temps aléatoire appelé **backoff timer** uniformément distribué entre 0 et la taille actuelle de la fenêtre de contention **CW**.

A la fin du temps '**backoff timer'**, la station peut accéder au canal s'il se libère, une collision peut avoir lieu si deux ou plusieurs stations (à portée de communication) ont commencé à transmettre en même temps, dans le cas contraire, un acquittement est envoyé à l'émetteur pour accuser la réception. Le récepteur, à son tour attend pendant un temps SIFS après la

réception correcte des données et vérifie le **CRC** de la trame reçue avant d'envoyer son ACK. Puisqu'un SIFS est plus petit qu'un DIFS, le récepteur n'a pas besoin d'écouter, préalablement le canal de transmission avant d'envoyer son acquittement. Si l'émetteur ne reçoit pas d'acquittement (Ksentini, 2005), il considère que la trame envoyée a été perdue et doit la retransmettre, il entame donc le processus backoff à nouveau. Pour réduire la probabilité de collisions, après chaque échec de transmission, la fenêtre de contention est doublée jusqu'à une valeur maximale prédéfinie CWmax :

$$CW = (CWmin \times 2^{i}) - 1$$

La fenêtre de contention est réinitialisée à une valeur minimale fixe CWmin, après chaque transmission avec succès.
Par ailleurs et, dans le but de résoudre le problème des stations cachées, le standard 802.11 définit dans la couche MAC un mécanisme optionnel de type RTS/CTS. (Ksentini, 2005) (Siad, 2007) (Tibi & Tabbana, 2005)

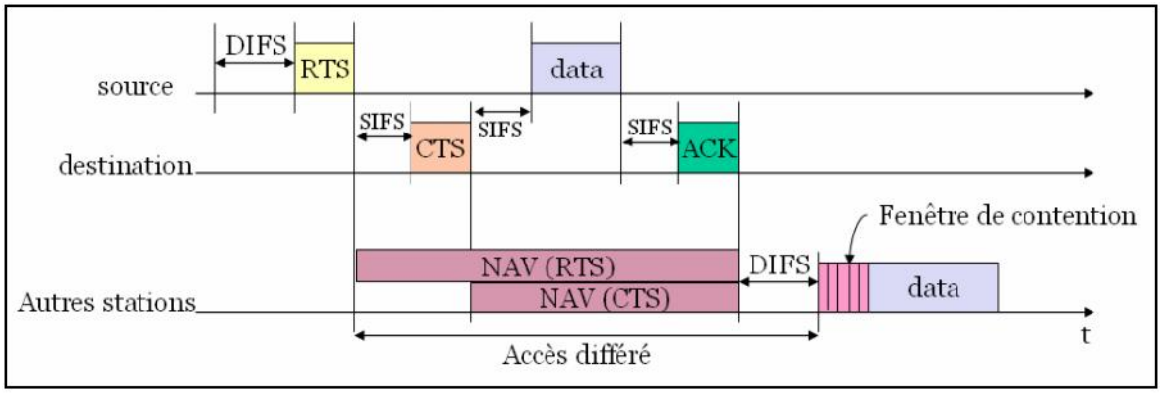


Figure 3-5 Le mécanisme RTS/CTS (Tibi & Tabbana, 2005)

Lorsque cette fonction est utilisée, une station émettrice transmet un RTS et attend en réponse un CTS. Toutes les stations du réseau recevant soit le RTS, soit le CTS, déclencheront pour une durée fixée leur indicateur NAV pour retarder toutes les transmissions prévues (Figure 3.12). La station émettrice peut alors transmettre et recevoir son accusé de réception sans aucun risque de collision.
Le mécanisme RTS/CTS est particulièrement performant si la taille des paquets de données est grande. Or, si ces derniers sont petits alors le mécanisme RTS/CTS surcharge le réseau. Pour savoir si un échange RTS/CTS doit avoir lieu, le standard définit un seuil nommé **RTS_Threshold**, si la taille de la trame est plus grande que ce seuil, alors un échange RTS/CTS doit être effectué avant l'envoi de la trame. (Ksentini, 2005) (Siad, 2007) (Tibi & Tabbana, 2005)

b) La méthode d'accès PCF

La méthode PCF est spécifique au mode cellulaire nécessitant les points d'accès ou stations de base pour gérer l'accès au canal radio de toutes les stations qui lui sont reliées. Elle se base sur un algorithme centralisé permettant de transmettre des données synchrones. Le point d'accès prend le contrôle et choisit les stations qui peuvent transmettre leurs données. Il

définit pour cela un **PC (Point Coordinator)** qui lui permet de communiquer avec les stations dans le BSS.
Dans cette méthode, le temps est divisé en trames (Superframe), chacune contient une période sans contention ou Contention-Free Period (CFP) suivie d'une période avec contention ou Contention Period (CP) comme illustré dans la figure suivante.
Durant la période PCF, le point d'accès ou AP maintient une liste des stations enregistrées et interroge chaque station l'une après l'autre suivant sa liste. Aucune station n'a le droit de transmettre tant qu'elle n'a pas été interrogée. (Tibi & Tabbana, 2005) (Ksentini, 2005)

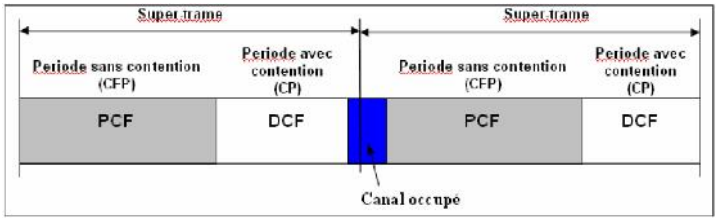


Figure 3-6 Succession de deux super-trames PCF (Tibi & Tabbana, 2005)

Le point d'accès AP écoute d'abord le canal pendant un intervalle PIFS, ensuite il commence une période CFP en diffusant un message Beacon en broadcast. Toutes les stations rajoutent à la valeur NAV la durée CFP_Maxduration (qui représente la durée maximale pour une période CFP), ce qui permet d'informer les stations que le réseau est sous contrôle du point d'accès (AP) pendant une période CFP. Le AP peut mettre fin à la période CFP à n'importe quel moment en transmettant un paquet CF-end, ce cas peut arriver quand le réseau est légèrement chargé. (Tibi & Tabbana, 2005) (Ksentini, 2005)

c) Fragmentation et Réassemblage

Dans la norme IEEE 802.11, il est possible de gérer la fragmentation des trames de données ou de gestion en plusieurs trames de taille inférieure pour des transmissions point à point. Cette solution augmente la fiabilité des transmissions. Elle réduit le besoin de retransmettre des données notamment lorsqu'il s'agit des données volumineuses, elle augmente ainsi les performances globales du réseau, car dans les environnements radio, plus la taille d'une trame est importante, plus la chance de la perte augmente.
Pour savoir si une trame doit être fragmentée, le standard 802.11 définit un seuil appelé **Fragmentation_Threshold**, si la taille de la trame atteint ce seuil, alors elle sera fragmentée. Les fragments ont une taille égale à la valeur du seuil Fragmentation_Threshold, sauf pour le dernier, qui peut avoir une taille plus petite.
Le champ **More_Frag** présent dans le champ de contrôle des trames IEEE 802.11 permet d'indiquer si la trame est fragmentée. Si le bit More Frag est positionné à 1, la trame est fragmentée.

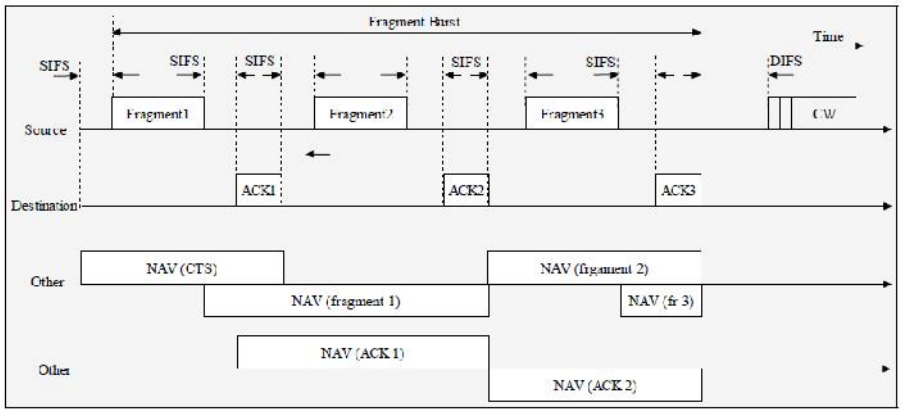


Figure 3-7 Exemple de mécanisme de fragmentation. (Ksentini, 2005)

Lors d'une fragmentation, tous les fragments sont transmis de manière séquentielle. Le support n'est libéré qu'une fois que tous les fragments sont transmis avec succès ou bien dans le cas où la station source ne reçoit pas l'acquittement d'un fragment transmis. La station 'destination' acquitte chaque fragment reçu avec succès en envoyant un ACK à la station source. La station source garde le contrôle du support et attend la réception de l'ACK durant l'intervalle SIFS, après la réception d'un ACK, la station reprend sa transmission. Mais si le message ACK n'est pas correctement reçu, la station source arrête la transmission et essaie d'accéder de nouveau au support. Lorsque la station source accède au support, elle commence à transmettre à partir du dernier fragment non acquitté.
La transmission d'une trame fragmentée peut se faire avec ou sans l'utilisation des messages RTS/CTS. Si les stations utilisent ce mécanisme, seul le premier fragment envoyé utilise les trames RTS/CTS pour réserver le support. Les autres stations dans le BSS maintiennent leur NAV en mettant l'information de durée de vie dans les différents fragments et ACK.
La Figure 3.7 illustre le processus suivi par l'émetteur pour transmettre une suite de fragments provenant d'une même trame. La trame est assemblée lorsque la station destination a reçu tous les fragments de la station source (Tibi & Tabbana, 2005) (Ksentini, 2005) (Cavagna & Nuaymi, 2004).

d) Les trames MAC

Le standard 802.11 définit trois types de trames (nommés aussi paquets dans ce mémoire) :

- les trames de données, utilisées pour la transmission des données.
- les trames de contrôle, utilisées dans la procédure d'accès au canal, par exemple RTS, CTS et ACK.
- les trames de gestion, pour l'échange d'informations de gestion au niveau MAC, ces trames restent au niveau MAC (trames Beacon contenant les informations de synchronisation). (Tibi & Tabbana, 2005)

i. La trame de données MAC 802.11

Une trame de données MAC 802.11 est constituée de trois parties :

- Entête MAC.
- Données MAC : Données reçues des couches supérieures et à encapsuler.

- CRC (Cyclic Redundancy Check) : champ de 32 bits contenant la somme de contrôle de la trame.

ii. La trame de contrôle MAC 802.11

La norme a considéré d'autres formats pour les trames de contrôle, en particulier les trames RTS, CTS et ACK. Les trames RTS et CTS sont utilisées pour la réservation virtuelle du support physique. La trame ACK est utilisée pour acquitter les transmissions réussies. Elle est envoyée par une station réceptrice, ayant correctement reçu une trame de données, à la station source.
Les trames RTS, CTS et ACK sont constituées chacune par un FCS (Frame CheckSequence) et un entête MAC.
L'entête MAC comporte quelques différences suivant qu'il s'agisse de trames RTS, CTS ou ACK :

- **L'entête de la trame RTS :** Elle comprend les champs suivants :

  - Frame Control : comme le champ de la trame de données MAC.
  - Duration : Durée à réserver.
  - RA : Adresse de la station réceptrice.
  - TA : Adresse de la station émettrice.

- **L'entête de la trame CTS** : Elle comprend les même champs que les message RTS, excepté le champ TA. Le champ RA étant recopié à partir du champ TA de la trame RTS reçue.

- **L'entête de la trame ACK :** Elle possède un format similaire à celui de CTS. L'adresse RA est recopiée à partir du champ Adresse 2 de la trame MAC à acquitter. (Tibi & Tabbana, 2005)

3.3. Les différentes versions de la norme IEEE 802.11

Le standard IEEE 802.11 a vu le jour en 1997. Depuis, il a été amélioré périodiquement par des draft issus des groupes de travail 802.11. C'est notamment le cas des normes 802.11a, 802.11b et 802.11g, appelées normes 802.11 physiques. D'autres normes comme la norme 802.11i a été proposée afin de préciser des éléments permettant d'assurer une meilleure sécurité ou la 802.11e pour une meilleure interopérabilité. (Nehdi, 2005)
Les différentes versions 802.11x diffèrent par leurs fréquences de fonctionnement, leurs débits et leurs portées.

Nous allons aborder ci-après un aperçu rapide des différentes normes existantes ou en développement.

- **La norme 802.11a**

La norme 802.11a permet d'obtenir un haut débit (54 Mbps théoriques, 30 Mbps réels). 802.11a spécifie 8 canaux radio dans la bande de fréquence des 5 GHz. (Nehdi, 2005)

- **La norme 802.11b**

Elle propose un débit théorique de 11 Mbps (6 Mbps réels) avec une portée pouvant aller jusqu'à 300 mètres dans un environnement dégagé. La plage de fréquence utilisée est la bande des 2.4 GHz. (Nehdi, 2005)

- **La norme 802.11c**

La norme 802.11c n'a pas d'intérêt pour le grand public. Il s'agit uniquement d'une modification de la norme 802.11d afin de pouvoir établir un pont avec les trames 802.11 (niveau liaison de données). (Nehdi, 2005)

- **La norme 802.11d**

La norme 802.11d est un supplément à la norme 802.11 dont le but est de permettre une utilisation internationale des WLAN 802.11. Son but est de permettre aux différents équipements d'échanger des informations sur les plages de fréquence et les puissances autorisées dans le pays d'origine du matériel. (Nehdi, 2005)

- **La norme 802.11e**

La norme 802.11e est conçue pour permettre le transfert des vidéos ou sons pour les applications multimédia, sans créer d'énormes bouchons lors de l'accès au canal, ainsi que pour les applications temps réel. Elle vise à donner des possibilités en matière de qualité de service en définissant les besoins des différents paquets en termes de bande passante et de délai de transmission. (Nehdi, 2005)

- **La norme 802.11f**

La norme 802.11f est une recommandation à l'intention des vendeurs de point d'accès pour une meilleure interopérabilité des produits.

Elle propose le protocole Inter-Access point roaming protocol permettant à un utilisateur itinérant de changer de point d'accès de façon transparente lors d'un déplacement, quelles que soient les marques des points d'accès présentes dans l'infrastructure réseau. Cette possibilité est appelée itinérance (ou roaming). **(Nehdi, 2005)**

- **La norme 802.11g**

La norme 802.11g offrira un haut débit (54 Mbps théoriques, 30 Mbps réels) sur la bande de fréquence des 2.4 GHz. La norme 802.11g a une compatibilité ascendante avec la norme 802.11b, ce qui signifie que des matériels conformes à 802.11g pourront fonctionner en 802.11b **(Nehdi, 2005)**

- **La norme 802.11h**

La norme 802.11h vise à rapprocher 802.11 du standard Européen (HiperLAN 2, d'où le h de 802.11h) et à être en conformité avec la réglementation européenne en matière de fréquence et d'économie d'énergie. (Nehdi, 2005)

- **La norme 802.11i**

La norme 802.11i a pour but d'améliorer la sécurité des transmissions (gestion et distribution des clés, chiffrement et authentification). Cette norme s'appuie sur l'AES (Advanced

Encryption Standard) et propose un chiffrement des communications pour les transmissions utilisant les technologies 802.11a, 802.11b et 802.11g. (Nehdi, 2005)

- **La norme 802.11r**

La norme 802.11r a été élaborée de telle manière à utiliser des signaux infra-rouges. Cette norme est considérée dépassée techniquement. (Nehdi, 2005)

- **La norme 802.11j**

La norme 802.11j est à la réglementation japonaise, ce que le 802.11h est à la réglementation européenne. (Nehdi, 2005)

- **La norme 802.11p**

Elle est dédiée pour les communications véhiculaires**,** on va l'aborder plus en détail dans la suite de ce chapitre.

4. Wireless Access in Vehicular Environments (WAVE) & IEEE P1609.x\802.11p

4.1. Le mode WAVE

WAVE est un mode de fonctionnement employé par les dispositifs IEEE 802.11 pour fonctionner sur la bande DSRC.
Il est basé sur la série de standards IEEE P1609, qui définissent l'architecture, les modèles de communication, la structure de gestion, la sécurité et les dispositifs d'accès physique aux communications véhiculaires.
Les composants architecturaux primaires sont les *Road-Side Units* (RSUs), les *OnBoard Units* (OBUs), et l'interface de WAVE. (Urmeneta, 2010)

WAVE décrit une implémentation d'IEEE 802.11p en définissant un ensemble minimum de paramètres. Ces paramètres assurent l'interopérabilité exigée entre les dispositifs sans fil pour communiquer dans les conditions des réseaux véhiculaires précédemment mentionnées. C'est ce qu'on appelle le mode WAVE. (Voir la figure suivante) (Urmeneta, 2010) (Calzada, Juny 2011)
La pile protocolaire du WAVE se compose de deux parties, le plan de données et le plan de gestion.

Le plan de données (ou Data plane) : Il comprend les protocoles de transmission, de communication et les hardwares pour le transfert de données. Il transporte le trafic de données entre les entités du plan de gestion de deux dispositifs ou entre des applications et les entités du plan de gestion. Il supporte le protocole UDP; le protocole TCP est optionnel (Huang & Chen, Telematics Communication Technologies and Vehicular Networks: Wireless Architectures and Applications, 2010)
Le plan de gestion (ou management plane)

Le plan de gestion est un ensemble de fonctions appliquées dans les protocoles de communications fournis par le plan de donnée. Il dispose de différentes entités pour les couches : l'entité PLME **(Physical Layer Management Entity) pour la couche physique,** l'entité **MLME (MAC Layer Management Entity) pour la couche MAC,** et l'entité **WME (WAVE Management Entity) pour la couche réseau et transport.**
Il fournit les services suivants : l'enregistrement d'application, la gestion de l'ensemble des services de base du WAVE (WBSS), le contrôle d'utilisation du canal, la configuration IPv6, le contrôle de l'indicateur de la puissance reçue du canal (la gestion de **RCPI : Received Channel Power Indicator**), et la maintenance de la base de gestion d'information (**the Management Information Base (MIB) maintenance**) (Huang & Chen, 2010)

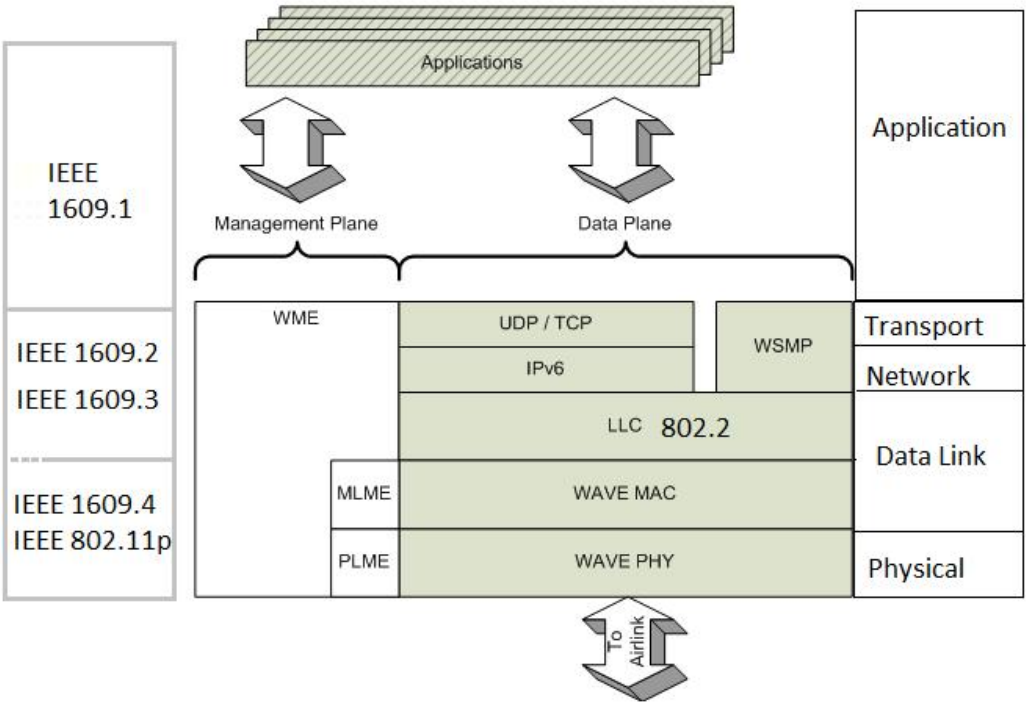


Figure 3-8 La pile du protocole WAVE.

4.2. La norme 802.11p

La notion de l'ensemble de services de base (BSS) est remplacée dans 802.11p par **WAVE-BSS (WBSS)**.
L'ensemble de services de base du mode WAVE (WBSS) dans IEEE 802.11p augmente les fonctions IEEE 802.11 MAC pour les communications rapides.
Une station mobile en mode WAVE devient membre d'un WBSS. Elle peut être comme étant fournisseur de WBSS (WBSS provider) ou bien utilisateur de WBSS (WBSS user).
Les stations mobiles en mode WAVE se déplacent beaucoup plus rapidement que les stations mobiles en mode infrastructure ou en mode ad-hoc dans un BSS. Alors comment assurer que les stations dans WAVE puissent joindre le réseau véhiculaire et puissent transmettre ou recevoir des données aussi rapidement que possible ? Pour cela, le WBSS n'exige pas l'authentification et l'association de sous-couche MAC avant de transmettre des données contrairement au réseau traditionnel IEEE 802.11 (a / b / g). Ce qui veut dire qu'après

l'écoute d'un message beacon ou la trame d'annonce de service **WSA** (**WBSS Service Announcement**) d'un fournisseur WBSS, un nouvel utilisateur peut joindre le réseau. Dans un WBSS, un utilisateur WBSS doit seulement recevoir la trame d'annonce de service **WSA** (**WBSS Service Announcement**) d'un fournisseur WBSS avant de commencer les transmissions. La trame **WSA** contient toutes les informations nécessaires pour joindre un WBSS (on détaillera cette partie par la suite). (Booysen, Zeadally, & Rooyen, 2011)
L'autre type de BSS est **le WAVE Independent Basic Service Set (WIBSS),** qui comprend les communications peer-to-peer. La communication peut se faire entre n'importe quelles paires d'utilisateurs à portée mutuelle. Les WIBSS dans la norme 802.11p est comme l'ensemble de services de base indépendant (IBSS) défini dans la norme 802.11 traditionnelle (a / b / g). La principale différence entre eux est que le WIBSS exclut explicitement l'utilisation de messages beacon dans son fonctionnement, tandis que le second (IBSS) les utilise pour synchroniser les horloges des nœuds.

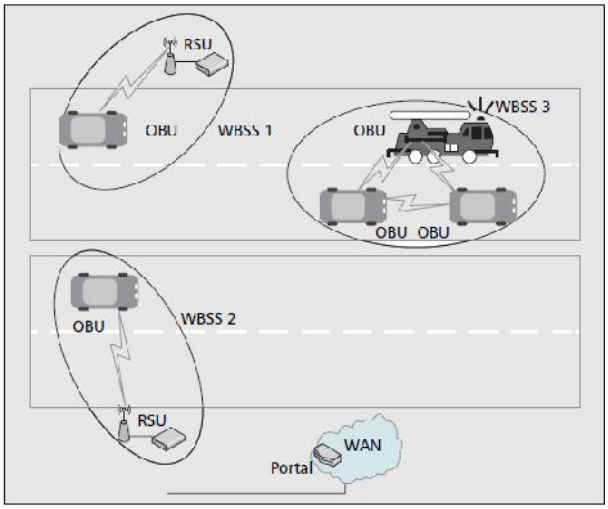


Figure 3-9 Exemple d'un système WAVE

Une station mobile en mode WAVE utilise **CCA (Clear Channel Assessment),** qui est un test sur le médium pour connaître l'état d'occupation du canal radio avec précision. En effet, le CCA est essentiel pour le fonctionnement de l'algorithme CSMA/CA de la couche MAC. La couche physique est capable d'effectuer trois modes de CCA :

- La détection d'un signal avec une puissance reçue **RSSI (Received Signal Strength Indicator)** supérieure à un certain seuil.
- La détection d'un signal conforme à la modulation de la couche physique.
- La détection d'un signal qui répond aux deux conditions.

Le standard IEEE 802.11(p)/1609 gère la bande passante en combinant FDMA et TDMA. IEEE 802.11p utilise le protocole **Enhanced Distributed Channel Access** (**EDCA**), dérivé de la norme IEEE 802.11e afin d'assurer la qualité de service QoS :

❖ *Qualité de service*

MAC 802.11e intègre deux mécanismes permettant la gestion de priorité :
- EDCA (Enhanced Distribution Channel Access)
- HCCA (Hybrid Coordination Function Controlled Channel Access).

- L'EDCA est une amélioration du mode de communication traditionnel DCF (*Distribution Coordination Function*) de la norme 802.11. Ce protocole introduit le concept de catégorie d'accès ou **AC pour "*Access Category*".**

- Le mécanisme HCCA s'appuie sur le mode de communication PCF (*Point Coordination Function*) qui est un mode de fonctionnement optionnel existant dans la norme 802.11.

Contrairement au protocole EDCA, le mécanisme HCCA n'a jamais été utilisé par aucun constructeur. Notre étude est limitée au mécanisme distribué EDCA car le mécanisme HCCA (mécanisme centralisé) n'est pas adapté aux réseaux VANETs (architecture distribuée).

Le mécanisme EDCA (Enhanced Distribution Channel Access)

Le protocole MAC (*media access control*) d'origine pour le standard 802.11 ne fait pas de distinction entre les différents types de trafics, d'où le rendement n'était pas adapté aux applications pour lesquelles une certaine priorité est nécessaire. Pour cela, le protocole EDCA qui est une évolution de DCF a été introduit comme étant le premier outil qui différencie les services au niveau de la couche MAC (DCF et PDF ne font pas de distinction entre les différents types de trafics). Cette technique attribue à chaque trafic une catégorie d'accès (AC) contenant des valeurs bien définies pour les paramètres d'accès DCF. L'accès au canal se fait donc selon la catégorie d'accès associée au flux à transmettre, toujours en faisant intervenir les espaces inter-trames. La norme 802.11e a défini ces quatre catégories d'accès notées AC (access category) :

- *AC_VO* : pour les applications temps réels.
- *AC_VI* : pour les applications vidéo.
- *AC_BE* : pour le trafic « Best Effort ».
- *AC_BK* : pour le trafic Background.

L'EDCF définit huit niveaux de priorités (entre 0 et 7) par l'intermédiaire des catégories d'accès (AC) ou *(Trafic Category*). Les espaces inter-trames ne sont plus identiques pour toutes les trames de données. EDCF introduit en effet le AIFS *(Arbitration IFS) selon* la classe de trafic : à chaque catégorie de trafic (TC) correspond un AIFS donné, il est de plus en plus petit afin d'augmenter le degré de priorité. La valeur minimale de AIFS correspond au DIFS.
Différents facteurs d'incrémentation (PF: Persistance Factor) de *backoff* sont introduits pour différentes priorités. De la même manière, les tailles limites de la fenêtre de contention CWmin et CWmax diffèrent selon la catégorie de trafic. Chaque catégorie de trafic TC possède une file d'attente FIFO où l'accès au canal se fait en mode DCF, avec AIFS [TC] au

lieu de l'habituel DIFS, et (CWmin[TC], CWmax [TC]) au lieu des (CWmin, CWmax). (Voir la figure suivante)

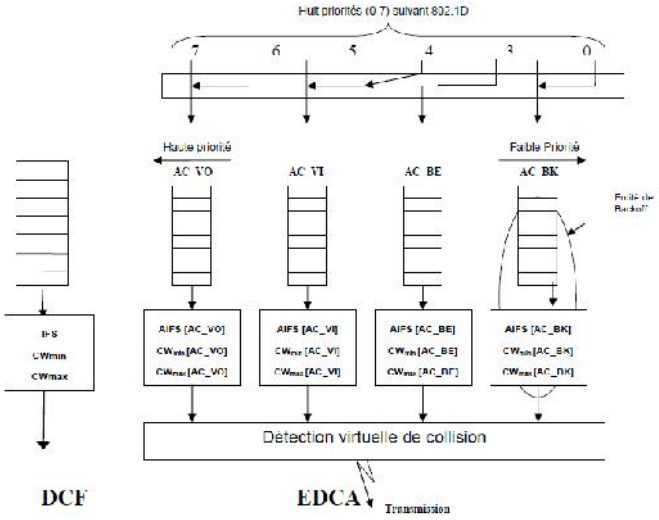


Figure 3-10 Différentiation de services au niveau de la couche MAC EDCA /DCF

Le délai d'attente d'une station devient ainsi une fonction de ces paramètres :

Backoff_Timer [*AC*] *=f(AIF* [*AC*] *, CWmin* [*AC*] *, CWmax* [*AC*] *,PF* [*AC*] *)*

avec :

- *AIF* [*AC]* est le délai inter-trame de la catégorie d'accès *(AC).*
- *CWmin* [*AC]* est la fenêtre minimale de *AC.*
- *CWmax* [*AC]* est la fenêtre maximale de *AC.*
- *PF* [*AC]* est un facteur de persistance (Persistence Factor) utilisé pour réduire encore la probabilité de collision de *TC.*
- *TXOPLimit [AC] (*Transmission Opportunity), période pendant laquelle la station a le droit d'envoyer ces données. (Hartenstein & Laberteaux, 2010)

Le tableau 3.1 illustre les valeurs d'accès, pour chaque catégorie d'accès,

Access category index	AIFSN	CW_{min}	CW_{max}
0	6	7	15
1	9	15	1023
2	3	3	7
3	2	3	7

Tableau 3.1. Paramètres d'accès pour chaque AC en mode EDCA dans un BSS (Hartenstein & Laberteaux, 2010)

- Au sein d'une même station, les files de priorités inférieures laissent l'accès à celles des priorités supérieures.
- Lorsque deux trames de deux files d'attente différentes entrent en collision, c'est la trame de priorité supérieure qui aura l'opportunité de transmission.

- Le facteur de persistance (PF) permet d'augmenter la taille de la fenêtre de contention (CW) après chaque collision selon l'équation suivante :

$$CWmin[i] = ((CWold[i] + 1)*PF-1$$

Quand PF est grand, la fenêtre de contention est grande en moyenne, par la suite il y'a moins de chance d'accéder au canal, d'où le débit utile sera réduit.

4.3. IEEE P1609.1

La norme IEEE P1609.1 décrit les éléments clés de l'architecture du système WAVE, elle définit les flux de données et les ressources aussi bien que les formats de message de commande et les formats de stockage des données. Elle spécifie également les types de dispositifs qui peuvent être supportés par les OBUs et traite le gestionnaire de ressources WAVE.

Cette norme décrit une application spécifique de WAVE comprenant :

- le gestionnaire de ressource : Resource Manager (RM)
- le processeur de contrôle de ressource : the Resource command processor (RCP),
- et l'application de gestion de ressource : Resource Manager Application (RMA).

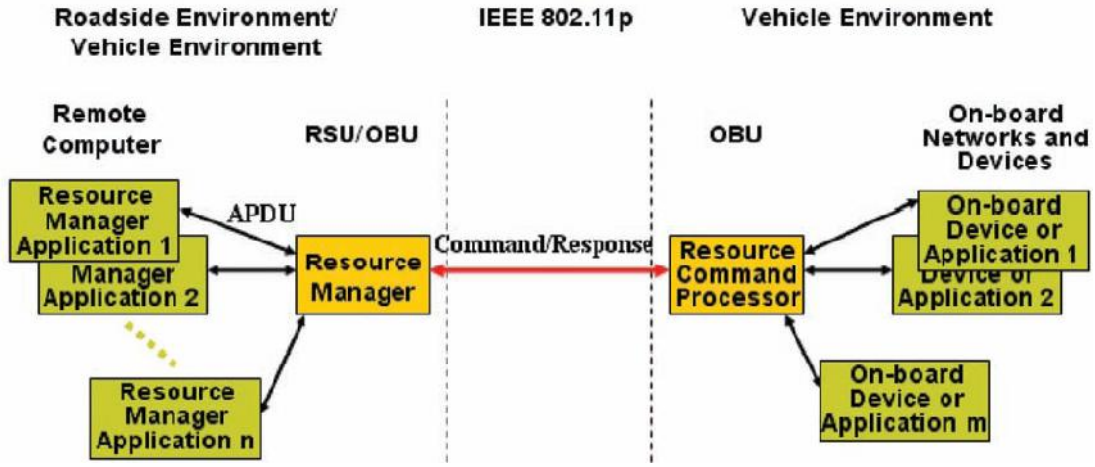


Figure 3-11 Composants adressés dans IEEE 1609.1 (IEEE 1609.1TM, 2006) (Huang & Chen, 2010)

Le RCP réside sur un OBU et le RM peut résider sur un RSU ou un OBU (comme le montre la figure 3.11). Le RM (ou le fournisseur) transmet par relais des commandes reçues du RMA au RCP (ou à l'utilisateur). Alternativement, le RCP exécute les commandes qu'il reçoit du RMA et renvoie des réponses au RMA par l'intermédiaire du RM. Le RM fournit les services qui permettent au RMA d'accéder à la mémoire et à l'interface utilisateur dans l'OBU aussi bien qu'aux interfaces des équipements de bord de la route commandées par le RCP. Le RM agit comme s'il était une couche d'application à un RMA. En général, les RMAs communiquent avec un ou plusieurs RMs sur un réseau câblé sécurisé, tandis qu'un RM communique avec un RCP sur une liaison sans fil qui peut ne pas être sécurisée. Le RM

multiplexe les sessions de communication de plusieurs RMA, ce qui permet à chaque RMA de communiquer de bout en bout avec les RCP (Alapati, 2010)
Comme représenté dans la figure, le transfert de données se fait en deux phases : l'encapsulation d'information transmise du RMA au RM contenu dans l'APDU (unité de données de protocole d'application), et le mode commande/réponse en général de RM au RCP. (Huang & Chen, 2010) (Alapati, 2010) (Calzada, Juny 2011)

4.4. IEEE P1609.2

IEEE P1609.2 traite les Services de Sécurité pour les Applications et les Messages de contrôle. Il définit les formats de message et de traitement sécurisés ainsi que les circonstances d'utilisation des échanges de messages sécurisés. (Harbouche & Samira, 2009)

4.5. IEEE P1609.3

IEEE P1609.3 traite les services réseaux. Il définit les services de la couche réseau et transport, y compris l'adressage et le routage.
Le système WAVE supporte les applications IP et non-IP. Les communications pour des applications non-IP sont basées sur le protocole **WSMP (WAVE short message protocol)** qui décrit également les **WAVE Short Messages (WSM) (figure 3.12)**, fournissant une alternative efficace à l'IP (WAVE-spécifique permettant de diminuer la taille du paquet de 52 octets au minimum pour un paquet UDP/IPv6 à une taille qui dépasse rarement 20octects). Le WSM peut être directement supporté par les applications VANET. Il permet également à l'application de contrôler directement les paramètres de la couche physique, tels que le numéro de canal et / ou la puissance de l'émetteur et il est conçu pour minimiser la capacité du canal. (Huang & Chen, 2010) (Harbouche & Samira, 2009)
L'ensemble de stations WAVE WBSS se compose d'un seul **fournisseur WBSS**, et soit d'aucun ou de plusieurs **utilisateurs WBSS**. Dans le mode WAVE, il ya 6 canaux de service et un seul canal de contrôle, ce concept multi-canal est défini par le standard 1609.4 que l'on va voir dans la section suivante.
Les applications basées sur le protocole WSMP peuvent initialiser le WBSS pour allouer un canal de service, mais ceci n'est pas exigé puisque les messages WSM peuvent être échangés sur le canal de contrôle. Donc, lorsque le WBSS n'est pas employé, les messages WSMs pourrait employer seulement le canal CCH. Si une application échange des données avec un WBSS, elle peut envoyer les informations en employant le protocole WSMP ou Pv6 sur un canal de service. Les applications basées IP sont assurées par le protocole IPv6 et les paquets IP ne peuvent être envoyés que sur un canal de service (plus de détails dans la section suivante). (Huang & Chen, 2010)

Le PSID

le PSID (**Provider Service Identifier : PSID**) qui est sur 4 octets, identifie le service dont le message WSM est associé. Chaque application possède un identificateur PSID unique qui sert donc à distinguer les applications. (Boix & Mecklenbräuker, 2008)

Le dispositif crée une liste d'identificateurs PSIDs actifs et lorsque le message WSM arrive, il vérifie si le PSID du message se trouve sur cette liste afin de le transmettre. De cette façon,

le PSID joue un rôle semblable au port TCP /UDP. Les identificateurs PSIDs sont dirigés par l'Autorité d'inscription IEEE. (Huang & Chen, 2010) (Harbouche & Samira, 2009)

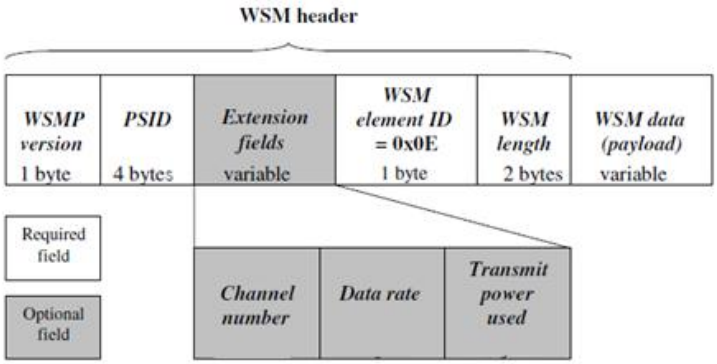


Figure 3-12 La structure du message WSM (WAVE Short Message)

Ce standard traite également la base de gestion d'information : **Management Information Base (MIB**) de l'entité de gestion WAVE (**WAVE Management Entity : WME**). Il dispose également des fonctions de la couche LLC. (Harbouche & Moussaoui, 2009) (Huang & Chen, 2010)

WAVE Management Entity (WME)

L'entité WME fournit une interface de gestion à toutes les entités du plan de données. WME échange les informations avec les applications et avec l'entité de gestion de la couche MAC **(MLME : MAC subLayer Management Entity)** en utilisant les primitives. (Voir la figure suivante) Ces primitives sont employées pour l'échange de communications entre les entités de couches adjacentes. Les **SAPs : Service Access points** (les points d'accès de service) supportent les communications entre les entités WAVE de gestion de réseaux et les autres entités WAVE dans un même dispositif. Il y a quatre types de primitives : Demande, Confirmation, Indication et Réponse.

L'entité de gestion WAVE donnerait l'accès au canal selon le niveau de priorité de l'application. Les droits d'accès sont attribués et contrôlés par la couche MAC. (Boix & Mecklenbräuker, 2008)

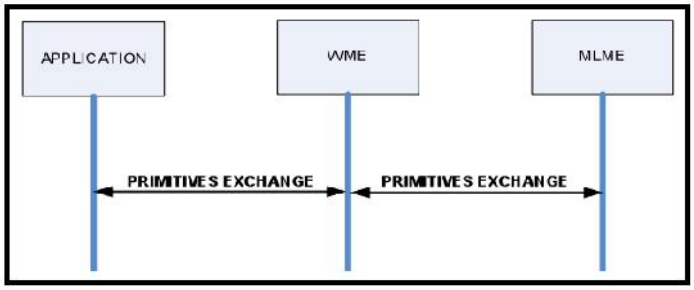


Figure 3-13 La communication entre les entités. (Boix & Mecklenbräuker, 2008)

Management Information Base (MIB)

Le WME contient la base d'information de gestion (**MIB : Management Information Base**). Dans cette base, les paramètres d'application (organisés en structures) seront enregistrés.

Quand une application est enregistrée, les informations d'enregistrement sont mises dans cette structure de données.

4.6. IEEE P1609.4

IEEE P1609.4 (IEEE 1609.4TM, 2006) décrit les améliorations du MAC 802.11 pour supporter le mode WAVE. Cette norme est applicable lorsque DSRC fonctionne dans un environnement multi-cana. Elle définit un mécanisme qui permet à la station ayant une ou plusieurs canaux radios de commuter de manière efficace entre les différents canaux. Elle peut être considérée comme une extension à la couche MAC, avec une instance logique IEEE 802.11p MAC fonctionnant dans chaque canal.

Le but de l'IEEE 1609.4 est de définir un mécanisme dont les dispositifs commutent entre les canaux pour qu'ils puissent communiquer. La norme implique deux concepts : la division du temps et le canal de "rendez-vous":

- La synchronisation de réseau est réalisée en divisant le temps à des périodes de 100 ms. Dans chaque intervalle de temps, deux types de canaux sont utilisés: un canal de contrôle (**CCH**) et un canal de service (**SCH**). On parle alors de l'intervalle CCH et de l'intervalle SCH.
- le concept de ' rendez-vous' définit un canal dans la bande DSRC, comme étant un canal spécial dans lequel les dispositifs l'accorderont de façon régulière. Dans IEEE 1609.4, ce canal est le canal de contrôle (CCH).

La synchronisation est assurée en supposant que tous les nœuds ont accès à une horloge commune : **Universal Coordinated Time (UTC).** Cette horloge est disponible dans le signal GPS. Un nœud sans récepteur de GPS pourrait potentiellement se synchroniser avec UTC, en recevant des signaux de synchronisation d'un autre nœud.

Le canal CCH est employé principalement pour deux types de messages :

•Les **Messages de sécurité** qui sont sous le format WSM (WAVE short message).
• et Les **Annonces de service de WAVE (WSAs)** qui sont employés pour annoncer la disponibilité d'un ou de plusieurs services de WAVE dans le prochain intervalle de service SCH.

Le canal CCH est alloué seulement aux messages WSM et WSA. Aux USA, le canal 178 est désigné comme CCH et les six autres canaux de DSRC sont désignés comme SCHs (voir la figure suivante).

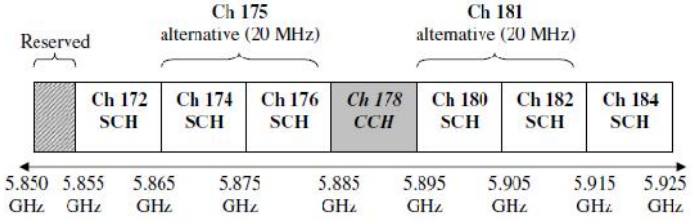


Figure 3-14 Désignations des canaux de la bande DSRC à l'USA. (Hartenstein & Laberteaux, 2010)

La figure 3.15 illustre le concept de base de la division de temps défini dans IEEE 1609.4. Le temps est divisé en périodes de 100 ms. Chaque intervalle CCH ou SCH (de 50ms chacun) commence par un intervalle de garde de 4 ms (guard interval) qui est employé par le nœud pour commuter d'un contrôle MAC (canal) à un autre. Il sert aussi lors des petites erreurs ou décalages de synchronisation.

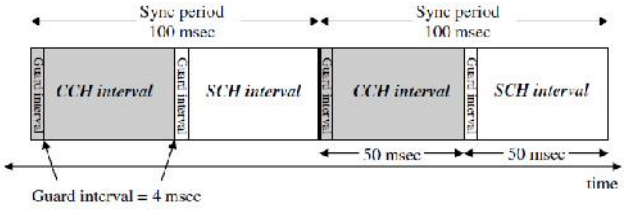


Figure 3-15 Division de temps dans des intervalles de CCH et des intervalles de SCH. (Hartenstein & Laberteaux, 2010)

Mutation au canal de service SCH:

Pendant l'intervalle CCH. Si un nœud reçoit une ou plusieurs annonces de services(WSA), et qu'il s'intéresse par un service annoncé, il commutera au canal SCH approprié à la fin de l'intervalle CCH.

Généralement, à la fin de l'intervalle CCH, le nœud est systématiquement commuté au canal de service SCH sélectionné dans l'intervalle précédent. Mais il existe deux cas où un nœud peut rester sur le canal CCH pendant l'ntervalle prévu pour SCH (ie, il accède au canal de commande CCH durant les deux intervalles au lieu de commuter du canal CCH au canal SCH à la fin du premier intervalle), ces deux cas sont :

(1) - Lorsque le nœud ayant une seule interface radio peut ne pas entendre une annonce de service pour y accéder.

(2) - Ou bien lorsque le nœud perd temporairement la synchronisation avec l'UTC, ainsi que sa capacité de discerner les limites entre les intervalles de CCH et de SCH. Le nœud doit donc rester sur le canal CCH jusqu'à sa synchronisation.

Dans le premier cas, le nœud qui utilise le canal CCH pendant l'intervalle SCH peut transmettre et recevoir des trames limitées uniquement aux informations non essentielles puisque les nœuds voisins utilisent les canaux de service SCH. En général, l'information essentielle devrait être envoyée seulement dans l'intervalle prévu pour le canal CCH, c'est le moment des rendez-vous, où on s'attend à ce que tous les nœuds écoutent le canal de transmission.

Actuellement, les protocoles IEEE 1609 ne permettent pas à un nœud de savoir combien de radios peut avoir un voisin, ainsi le nœud doit supposer qu'au moins certains voisins ont une seule radio. C'est important pour déterminer comment employer la deuxième radio, par exemple. (Hartenstein & Laberteaux, 2010)

IEEE 1609.4 définit les règles d'agissement pour un dispositif de WAVE (c-à-d un OBU et un RSU). Le nœud peut avoir une seule radio (radio simple) ou plusieurs (multiples radios).

Si le dispositif a de multiples radios, alors le rendez-vous sur le canal CCH peut se faire par une des deux radios et la deuxième radio pourrait être accordée au canal CCH afin de donner au nœud plus de chance pour entendre les messages broadcast, ou bien elle pourrait être accordée à un canal SCH.
Dans le protocole de commutation courant de l'IEEE 1609.4, l'utilisation principale de la deuxième radio permet à un nœud d'accéder à deux services simultanément, sur deux canaux SCHs différents durant l'intervalle SCH. Les chercheurs étudient activement la question d'améliorer l'utilité de la deuxième radio. (Hartenstein & Laberteaux, 2010)

Issues de collision de trames: Il existe deux sortes de collisions pour une communication en utilisant la norme 1609.4.
Le premier type est 'une collision synchronisée 'synchronized collision' qui est relativement facile à éviter. Le second type est la collision due à la congestion 'congestion collision' qui est susceptible de devenir un vrai problème lors d'une intensité élevée. (Hartenstein & Laberteaux, 2010)

- *Collision synchronisée 'synchronized collision'*

L'objectif des réseaux véhiculaires est dans les applications de sureté. Alors, si les couches supérieures ignorent la synchronisation de temps, il y a environ une probabilité de 46% pour que le message soit mis en file d'attente pendant l'intervalle CCH, et une probabilité d'environ 54% pour qu'il soit mis en file d'attente au moment où le message ne peut pas être immédiatement envoyé. La norme 1609.4 suppose que n'importe quelle trame mise en file d'attente pour transmission sur le canal CCH pendant l'intervalle SCH traitera le canal comme étant occupé initialement. La trame déclenche ainsi le mécanisme backoff. Ce problème est relativement simple à éviter si la fonction de génération de message dans les couches les plus élevées est équipée d'un signal indiquant le début d'une période de synchronisation. Il sera donc possible de mettre le message dans la file d'attente pendant l'intervalle CCH de 46 millisecondes. Cependant, la station peut trouver le canal occupé, mais aux charges raisonnables du réseau, il est moins probable d'avoir une collision.
La norme 1609.4 recommande, mais n'exige pas un dispositif pour prendre des mesures afin d'éviter ce phénomène. (Hartenstein & Laberteaux, 2010)

- *Collision due à la congestion 'congestion collision'*

Le modèle de communication de sûreté suppose que chaque véhicule envoie un message de sûreté par période de synchronisation de 100 millisecondes, mais l'utilisation est limitée seulement à 46 millisecondes (l'intervalle CCH). Néanmoins, puisque nous sommes en première phase de déploiement, cette limitation n'est pas susceptible d'être significative puisque seulement quelques véhicules sont équipés par le DSRC.

Ce problème peut être montré par un simple calcul: supposant que le canal est toujours utilisé pour les messages de sûreté, et que chaque message de sûreté est de 3000 bits, et que la couche PHY de DSRC emploie un débit de 6 Mbps. Par conséquent, le canal CCH ne peut pas supporter plus de 2000 messages par seconde, ou 200 véhicules envoyant des messages toutes

les 100msec. Mais réellement, 46 millisecondes sont réservés aux messages de sûreté dans une période de 100msec, cela diminue le nombre de véhicules envoyant des messages toutes les 100msec de 200 à 92 véhicules par période. (Hartenstein & Laberteaux, 2010)

Le protocole CSMA/CA possède un nombre croissant de collisions lorsque la charge est importante, ainsi en réalité, le nombre de véhicules dans une même portée de communication est limité à moins de 92 véhicules. (Hartenstein & Laberteaux, 2010)

5. ETSI TC ITSS

ETSI TC ITS (ETSI EN 302 637-2 Draft V.0.0.5, 2012)sont des normes développées dans le projet COMeSafety et publiées dans (European ITS Communication Architecture: Overall Framework and Proof of Concept Implementation, 2010). C'est une norme européenne responsable de la normalisation des applications routières.

Figure 3-16 La norme ETSI TC ITS. (Sjöberg, 2013)

Il existe quelques différences entre la norme européenne ETSI TC ITS et le standard WAVE des Etats-Unis. Dans la figure suivante, les piles protocolaires des deux normes sont présentées. Les protocoles des couches inférieures PHY, MAC et LLC, sont identiques. Le mécanisme IEEE P1609.4 pour le fonctionnement multi canal est ajouté au mode WAVE, tandis que l'utilisation des différents canaux attribués en Europe est expliquée dans le mécanisme DCC.
Les principales différences entre les deux standards se trouvent au niveau des couches supérieures.
Dans la couche réseau/transport, le mode WAVE utilise le protocole WSMP pour les communications à un saut, alors que le standard ETSI utilise le protocole GeoNetworking (routage géographique) pour les communications multi-sauts. L'emploi de P1609,3 (WSMP) pour les annonces de service n'a pas été abordé dans la pile protocolaire européenne. (Sjöberg, 2013)

La couche d'installation (facilities), introduite par l'ETSI TC ITS n'est pas présente dans le standard WAVE. La norme J2735 dans le mode WAVE spécifie des types de messages tels que BSM, qui est un type également présent dans l'ETSI sous le nom CAM.

Des spécifications plus détaillées pour le déploiement des applications sont spécifiées dans la couche d'installation de l'ETSI TC ITS qui sont présentes aussi dans la couche d'application du WAVE.

ETSI TC ITS a également précisé trois types applications de sécurité pour la circulation routière contenant plusieurs cas d'utilisation. Jusqu'à présent, aucune précision n'a été faite aux Etats-Unis, sauf que des exigences minimales de performance sont en cours de développement au sein de SAE dans le document J2945.1. (Sjöberg, 2013)

Figure 3-17 Différence entre WAVE et ETSI TC ITS**.** (Sjöberg, 2013)

6. Conclusion

L'objectif de ce chapitre est de présenter les différents standards pour les réseaux véhiculaires. En premier lieu, nous avons introduit la bande DSRC dédiée aux systèmes de transport intelligents. En deuxième lieu, nous avons présenté les notions de base concernant les réseaux locaux sans fil de type IEEE 802.11 avec ses deux couches : physique et liaison de données. Ensuite, nous avons abordé les mécanismes d'accès au médium sans fil pour la norme IEEE 802.11, à savoir le mode distribué DCF et le mode centralisé PCF, ainsi que la fragmentation et le réassemblage, les trames MAC 802.11, et les différentes versions de la norme 802.11.

A partir des limites des deux méthodes DCF et PCF en terme de qualité de service et vu la nature spécifique des réseaux VANET, nous avons introduit, en troisième lieu, le standard WAVE comprenant la norme des réseaux véhiculaires 802.11p avec sa méthode d'accès EDCF (qui a été introduite au départ pour la norme 802.11e), nous avons arboré aussi la série de standards P1609.x, en particulier la norme P1609.4 qui améliore MAC 802.11 afin de supporter le mode WAVE. Nous avons également mentionné les différences entre la norme américaine WAVE et la norme européenne ETSI TC ITS. Nous n'avons pas détaillé la norme

européenne, car elle possède les mêmes protocoles des couches basses que la norme américaine.
Dans le chapitre suivant, nous allons présenter les principaux protocoles MAC hybrides dédiés aux réseaux véhiculaires.

Chapitre 4
Les protocoles MAC hybrides

1. Introduction

Après avoir présenté les challenges de la couche MAC pour les réseaux VANETs et les approches MAC basées et non basées sur la contention au niveau du deuxième chapitre, et les différents standards pour les réseaux véhiculaires au niveau du troisième chapitre. Ce chapitre parvient afin de présenter les protocoles MAC hybrides qui combinent deux ou plusieurs protocoles planifiés (frree-contention) ou aléatoires (based-contention). On va présenter quelques protocoles MAC (non standard) dédiés spécialement pour les réseaux VANET et qui ont été récemment proposés dans la littérature.

2. Le protocole CBMMAC : Cluster-Based Multichannel MAC

Afin de bien utiliser les canaux DSRC, les chercheurs dans (Kim, Jung, & Lee, 2009) ont proposé un schéma de communication basé sur les clusters (le groupement) en intégrant des groupes dans les protocoles MAC basés contention.

Dans ces protocoles, le véhicule chef du groupe "cluster-head" (CH) joue le rôle de coordinateur pour collecter et délivrer les messages de sécurité dans son groupe en temps réel, et les envoyer à ses voisins. Il contrôle également les transmissions de données entre les membres de son groupe qui ne sont pas en temps réel.

Ce protocole utilise les mécanismes TDMA/broadcast dans le cluster (groupe), et la norme IEEE 802.11 MAC entre les véhicules CH ("cluster-head"), pour assurer une livraison de messages en temps réel. Il suppose aussi que chaque véhicule possède deux radios.

Le but de ce protocole est de considérer la qualité de service et d'augmenter le nombre de flux de sortie pour des communications non-temps-réel (augmenter le débit). Pour réaliser ces buts, les chercheurs ont développé un schéma de communication multi canaux qui se base sur la bande DSRC. Ils ont défini donc des fonctions particulières pour les 7 canaux DSRC dans le schéma de ce protocole MAC. Ces fonctions sont présentées dans le tableau suivant :

Channel Name	*Channel Abbreviations*	*DSRC Channel Numbers*
Intercluster control	ICC	178
Intercluster data	ICD	174
Cluster range control	CRC	172
Cluster range data	CRD	176,180,182,184

Tableau 4-1 Définition des canaux DSRC pour le protocole CBMMAC (Moustafa & Zhang, 2009)

Chaque cluster-head se charge des communications à l'intérieur de son cluster et maintient les informations de routage lui permettant de joindre les autres cluster-heads. De plus, comme les

cluster-heads ne sont pas forcément reliés, des nœuds intermédiaires ou passerelles sont aussi élus et utilisés pour les communications entre cluster-heads.
Le protocole définit l'algorithme de groupement (de clustering) dans les deux phases MAC : basé contention et contention-free, utilisé respectivement dans les communications inter-cluster et intra-custer. (Moustafa & Zhang, 2009) (Kim, Jung, & Lee, 2009) (Booysen, Zeadally, & Rooyen, 2011)

Le fonctionnement du protocole
Les véhicules qui sont à proximité les uns des autres, forment un groupe (cluster). Ce groupe contient un seul véhicule chef noté CH (c'est le véhicule cluster head) qui est sélectionné par des règles prédéfinies. Chaque véhicule CH communique via le canal CRC en utilisant MAC free-contention TDMA avec les véhicules appartenant à son groupe (véhicules membres du même groupe), pour recevoir et envoyer les messages de sécurité (comme les messages de contrôle). Le canal ICC est utilisé par le véhicule CH pour communiquer avec les autres véhicules CH, les message de sécurité en utilisant le schéma MAC 802.11.
Chaque véhicule membre du cluster (qui n'est pas CH et appartient au groupe) échange des messages via le canal CRD avec les autres véhicules de son groupe. (Moustafa & Zhang, 2009)
Le canal ICD peut être utilisé pour les communications non temps réels entre les membres des clusters voisins. (Véhicule membre et non pas CH).

Pour réaliser ces communications, trois protocoles sont développés dans cette approche : le protocole de configuration des clusters, le protocole de communication inter cluster, et le protocole de communication et de coordination intra cluster.
Le premier protocole : **protocole de configuration de cluster** utilise MAC based-contention sur le canal ICC pour la gestion de clusters (tel que joindre ou quitter un cluster, l'élection du cluster-head). Le deuxième protocole : **le protocole de transmission d'inter cluster** est responsable de l'échange des messages de sûreté et du trafic non-temps-réel sur les canaux ICC et ICD respectivement. Le troisième protocole : **le protocole de communication et de coordination intra cluster** utilise le protocole MAC multicanaux pour contrôler la communication entre le véhicule CH et les véhicules appartenant à son cluster. (Moustafa & Zhang, 2009)

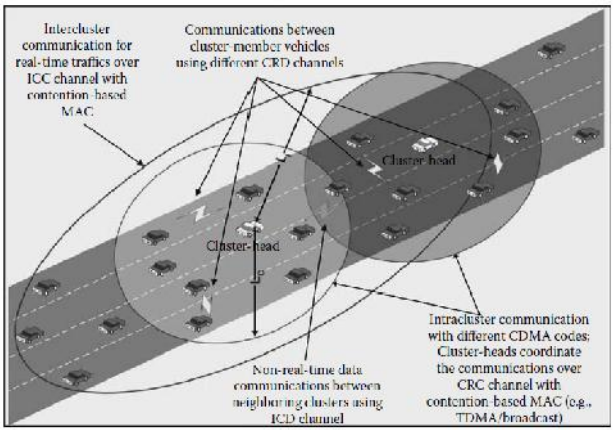


Figure 4-1 Illustration d'une communication en utilisant le protocole **CBMMAC** (Moustafa & Zhang, 2009)

	Transceiver	Channel	MAC method
cluster head (CH)	1	CRC	contention-free TDMA and broadcast
	2	ICC	contention-based (e.g. IEEE 802.11)
cluster member	1	CRC	contention free TDMA and Broadcast
	2[a]	CRD	contention-free (allocated channels)
		ICD	contention-based (e.g. IEEE 802.11)
non-member	1	ICC	contention-based (e.g. IEEE 802.11)

Tableau 4-2 L'attribution des canaux DSRC dans le protocole CBMMAC. (Booysen, Zeadally, & Rooyen, 2011)

Le protocole de coordination et de communication est basé sur le protocole MAC multicanaux, où chaque véhicule CH utilise le canal CRC, pour rassembler ou diffuser des messages de sûreté et pour coordonner les véhicules membres afin qu'ils puissent transférer des données non-temps-réel à l'intérieur ou entre les clusters. Le protocole de communication inter cluster transmet deux types de messages,

(1) les messages de sûreté, en temps réel sur le canal ICC ;

(2) et les messages non-temps-réel sur le canal ICD ;

Les clusters-heads, quasi-cluster-heads, et quasi-cluster-members utilisent les protocoles basés contention (IEEE 802.11) pour accéder au canal ICC. Puis, les véhicules CH rassemblent les messages de sûreté de leurs propres clusters, ils essaient ensuite d'accéder au canal ICC pour envoyer les données fusionnées aux véhicules CH voisins.

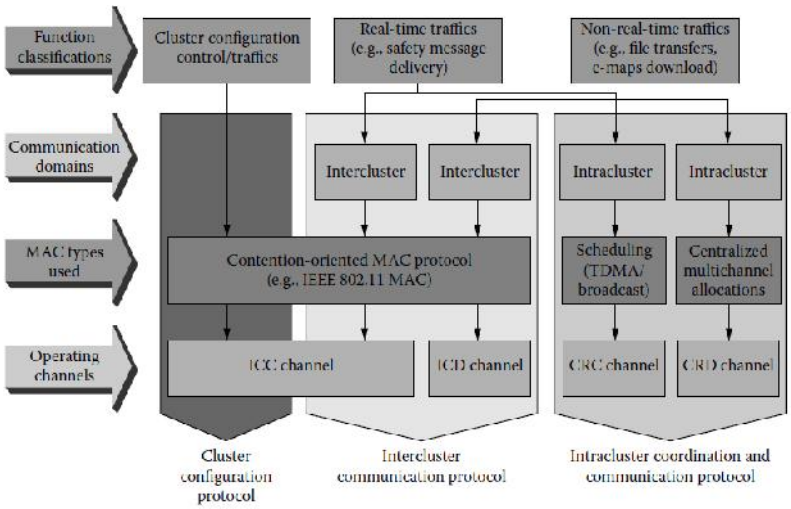


Figure 4-2 Diagramme de structure du schéma CBMMAC. **(Moustafa & Zhang, 2009)**

Les résultats de simulation et d'analyse obtenus dans ce travail prouvent que ce protocole peut réaliser non seulement une livraison opportune des messages de sûreté, mais également il

augmente le flux de sortie pour le trafic non-temps-réel. (Booysen, Zeadally, & Rooyen, 2011)

3. STDMA : self-organising TDMA

La méthode self-organising TDMA : STDMA (TDMA à organisation automatique) a été évaluée par Bilstrup et al (Bilstrup, Uhlemann, Strom, & U, 2009) dans un environnement véhiculaire. Son but est de garantir un temps de livraison opportun des messages critiques. Elle est actuellement utilisée dans l'aviation et la communication entre les bateaux en tant qu'élément du système automatique d'identification (AIS) (Booysen, Zeadally, & Rooyen, 2011)
STDMA applique le principe de R-ALOHA, elle fournit une coordination décentralisée, et presque basée free-contention. Elle divise le temps en trames de même durée et la trame en slots, la trame est considérée comme une séquence répétée d'un nombre fixe de slots. Les trames ne sont pas synchronisées et chaque nœud synchronise ses slots par rapport au temps GPS (Booysen, Zeadally, & Rooyen, 2011)

*Le principe de STDMA :*Au départ, un nœud commence par déterminer le taux de rapport (report rate ie le nombre de slots employés pendent une trame). Puis, quatre phases vont se suive : *l'initialisation, l'entrée du réseau, la première trame, et le processus périodique*. Lors de l'initialisation, le nœud se met à l'écoute du canal, pendant une trame, pour déterminer l'affectation des emplacements (ie, quels sont les slots occupés, et quelles sont les positions des nœuds qui les utilisent). Dans la phase d'entrée dans le réseau, le nœud détermine ses propres slots de transmission dans la trame d'après les règles suivantes:

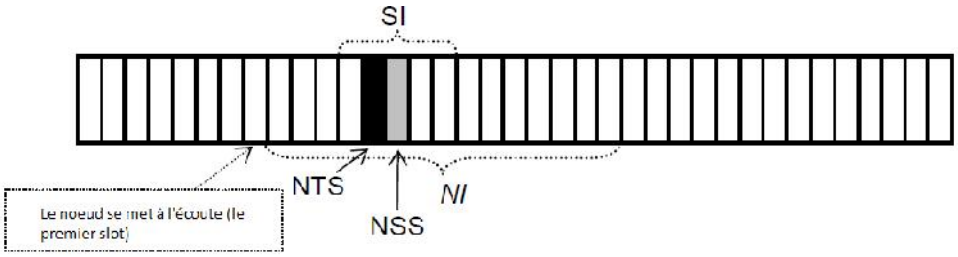


Figure 4-3 La structure du message STDMA. (Bilstrup, Uhlemann, Strom, & U, 2009)

(i) : Calculer NI :(nominal increment) en divisant le nombre de slots sur le taux de rapport,
(ii) : Sélectionner au hasard un premier slot (NSS), entre l'emplacement actuel et le NI (cet emplacement sera le début de la trame pour le nœud et donc chaque nœud possède son propre NSS),
(iii) Déterminer un intervalle de sélection de slots (SI) qui représente 20 % de la période Ni et qui est autour du slot NSS comme le montre la figure 4.3,
(iv) Une fois la trame est déterminée, le nœud à chaque fois sélectionne de manière aléatoire un slot NTS à partir de l'intervalle SI, si le NTS choisi au hasard est occupé, alors le slot libre le plus proche dans l'intervalle SI sera choisi. Si tous les slots dans SI sont occupés, alors le slot utilisé le plus loin sera sélectionné. (Bilstrup, Uhlemann, Strom, & U, 2009)

Cette méthode possède quelques insuffisances si elle est considérée comme solution pour diverses applications et scénarios de VANET. STDMA AIS a été développée et normalisée pour des bas débits, elle est utilisée seulement pour annoncer les positions des nœuds.

Cette solution n'est pas adéquate pour transmettre des données volumineuses comme des vidéos (multimédia en général) car elle utilise la méthode TDMA dans laquelle un slot est gaspillé à chaque fois qu'un nœud ne transmet pas de données. Par contre, cette méthode est plus appropriée pour un trafic véhiculaire sur des autoroutes que pour un trafic urbain car il y a moins de changement de direction et de la vitesse entre les nœuds sur l'autoroute.

En conséquence, cette approche a été dédiée et évaluée sur des autoroutes pour des applications de sécurité qui emploient des messages courts et exigent une fiabilité élevée. Ce système doit toujours être relié au GPS, et il utilise seulement un des sept canaux disponibles de WAVE. Dans le cas de surcharge de réseau, les slots sont également en surcharge, donc ils ne seront pas bien séparés, et cela produira des collisions qui peuvent retarder les transmissions. (Booysen, Zeadally, & Rooyen, 2011)

4. VeSOMAC: self-organizing collision-free TDMA approach

Une approche : self-organising contention-free TDMA MAC appelée VeSOMAC est développée et évaluée par Yu et Biswas (Yu & Biswas, 2007).

Le but de cette recherche est de développer une méthode MAC distribuée basée contention-free afin d'augmenter le transfert de données entre les véhicules dans un scénario d'autoroute. Dans l'approche VeSOMAC, les nœuds sont synchronisés via le GPS, ou bien avec les autres (auto-synchronisation).

La trame représente essentiellement une période pour un nœud (voir la figure suivante). Toutes les trames ont la même durée T_{trame}.. Par conséquent, le taux assigné à un véhicule est $\lambda_{alloc} = 1/T_{trame}$ trame/sec. (Booysen, Zeadally, & Rooyen, 2011)

VeSOMAC peut fonctionner en mode synchrone et asynchrone. En mode synchrone, tous les véhicules sont synchronisés, et donc, ils ont les mêmes limites des trames et des slots. En mode asynchrone, les véhicules maintiennent leurs propres limites de trames et donc les slots sont également asynchrones (ie deux trames de deux nœuds différents peuvent être décalées comme montré dans la figure 4.4).

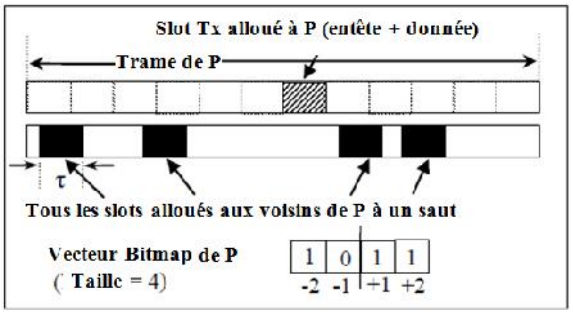


Figure 4-4. Le vecteur Bitmap pour des opérations asynchrones. (Yu & Biswas, 2007)

Dans cet exemple, le vecteur Bitmap est à 4 bits, chaque bit représente l'état d'occupation de deux slots autour du nœud P car un slot d'un nœud voisin peut occuper partiellement deux slots en mode asynchrone.
Les valeurs (-2, -1, +1, +2 : représentent dans la figure les positions des slots par rapport au slot P, comme par exemple +1 est le slot juste après le slot P). Le '1' dans l'emplacement "+1" i indique qu'au moins un des deux slots qui se trouve juste après le slot p est entièrement ou partiellement occupé.
La longueur du vecteur Bitmap est un paramètre de conception dont la valeur maximale est le nombre de slots dans une trame. Dans la figure 4.4, la taille de la trame est 12, tandis que la longueur du vecteur Bitmap est 4, ce qui empêche le nœud P de savoir l'état du slot extrême gauche. (Le vecteur donne les informations d'occupation de seulement 8 slots). (Yu & Biswas, 2007)

- **Allocation d*e slot***

  Les slots de deux nœuds qui peuvent communiquer en un saut ou bien en deux sauts, ne doivent pas se chevaucher afin d'éviter les collisions et le problème des nœuds cachés.
  En utilisant ce vecteur bitmat dans l'en-tête de paquet, le véhicule informe sans interruption ses voisins directs au sujet des slots occupés. D'autre part, en écoutant les vecteurs Bitmap de tous les paquets reçus, le véhicule peut détecter les slots de ses voisins à 1-hop et à 2-hop. Cette information peut alors être employée pour choisir un slot libre pour transmettre des données. (Yu & Biswas, 2007)

Ce travail n'a pas mentionné comment un nœud combine les vecteurs bitmap qui ne sont pas synchronisés pour choisir un slot, bien que ce choix dépend de la synchronisation (Booysen, Zeadally, & Rooyen, 2011)
La relocalisation de slots est faite au moyen d'un mécanisme de résolution de collisions. Quand un nœud détecte à plusieurs reprises que ses voisins ne reconnaissent pas son slot, il suppose qu'une collision a lieu et il réapproprie son slot. (Booysen, Zeadally, & Rooyen, 2011)

5. Le protocole multicanal token-ring (MCTRP)

Le protocole multicanal token-ring est proposé pour les réseaux VANET par Bi et al (Bi Y. , Liu, Cai, & Shen, 2009) Son but est de développer un protocole MAC basé free-contention dans lequel les nœuds s'organisent de manière autonome en utilisant la technique de jeton et en supposant une topologie en anneaux. Cette solution, a été proposée afin de minimiser le temps de latence pour les messages critiques et d'augmenter, le taux de trafic (nombre de messages) dans le réseau pour les applications non-critiques.
Le fonctionnement de ce protocole se base sur le groupement des nœuds en anneaux. Chaque groupe possède un chef (leader).
Le schéma token-passing TDMA (TDMA en utilisant le jeton), est utilisé pour contrôler l'accès au medium pour les transmissions des données intra-ring (à l'intérieur de l'anneau) et le CSMA/CA est utilisé pour contrôler l'accès au medium pour transmettre les données inter-ring (entre les anneaux), ie les informations urgentes et les transmissions de configuration et d'administration des anneaux. (Booysen, Zeadally, & Rooyen, 2011)

Chaque nœud est équipé de deux radios. La première radio est accordé de manière permanente au canal 178 du WAVE pour les communications de données inter-ring, ie les messages critiques inter-ring et la configuration de l'anneau (ring setup).

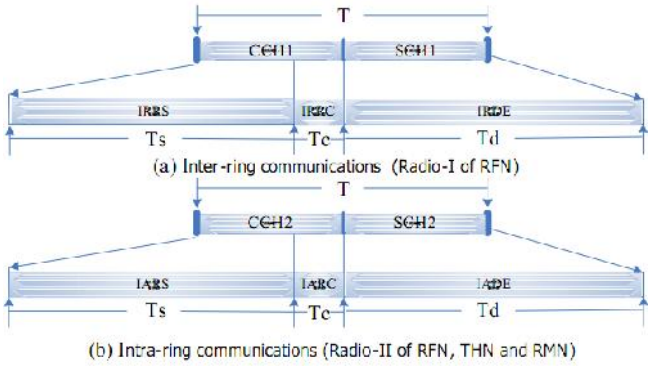


Figure 5-5 Les intervalles de communication dans le protocole multicanal token-ring. (Bi, Liu, & Shen, 2008)

La deuxième radio est allouée à un des six canaux restants du WAVE. Chaque anneau l'utilise pour les transmissions intra-ring des messages critiques, de coordination, et les données.
MCTRP se synchronise via le GPS et il divise le temps en segments égaux. Chaque segment T est réparti en trois périodes, comme illustré dans la figure 4.5, la première période pour la sécurité (Ts), la deuxième pour la coordination (Tc) et la dernière pour l'échange de données (Td).
La livraison du jeton se produit dans l'intervalle IARC ou IADE. Le jeton attribue le droit de transmission des paquets de données non urgentes d'intra-anneau aux nœuds membres de l'anneau sur la Radio-II.
Dans MCTRP, le jeton est livré selon l'état du buffer IADE du nœud qui a le jeton. Dans un premier cas, si le buffer n'est pas vide au début de la période Td, le nœud ayant le jeton transmettra ses paquets jusqu'à la fin de Td. Après, il livrera le jeton à son successeur dans la prochaine période Tc et attendra l'accusé. Une fois que ce nœud reçoit l'accusé de son successeur, il deviendra un nœud membre d'anneau. Autrement, le nœud chef (qui maintient le jeton) retransmettra le jeton jusqu'à ce qu'il obtienne un accusé ou le temps de retransmission atteint une valeur maximale Tmax. Dans ce dernier cas, on considère que son successeur a quitté l'anneau, alors le nœud chef le redonnera au nœud créateur d'anneau qui effectuera une opération de suppression (pour plus de détails, voir la section III de (Bi, Liu, & Shen, 2008)**)** (Booysen, Zeadally, & Rooyen, 2011)

Dans le deuxième cas (ie si le buffer de paquet est vide), le nœud chef déclenche un temporisateur (timer), et lorsque le temps du timer s'achève, il transmettra le jeton à son successeur dans l'intervalle IADE. Ceci assure que les nœuds ayant des paquets à transmettre pourraient acquérir le jeton aussitôt que possible. Par conséquent, le flux de sortie dans le réseau peut être augmenté d'une manière significative.
Chaque nœud dans l'anneau maintient une liste d'identificateurs des nœuds appartenant au même anneau (ID, MAC ADDRESS). Quand la couche MAC au niveau d'un nœud reçoit un paquet de la couche supérieure, elle vérifie si l'adresse de destination de ce paquet existe dans cette liste. Si l'adresse n'est pas dans la liste, le paquet sera transmis en utilisant la Radio I

suivant le protocole MAC IEEE802.11 (car il s'agit d'une communication inter-ring); dans le cas contraire, le nœud attendra le jeton pour envoyer le paquet (il s'agit d'une communication de données d'intra-anneau). (Bi, Liu, & Shen, 2008)

L'initialisation d'anneau se fait quand un nœud annoncera le message de création d'anneau dans l'intervalle IRRC en utilisant la Radio I, il déclenche ainsi un temporisateur de création d'anneau. Le message annoncé inclut le numéro SCH pour des communications de données d'intra-anneau. Si un anneau est déjà créé dans le canal spécifié, le chef d'anneau répond à ce nœud (l'initiateur) et l'invite à joindre son anneau à condition que le nombre de ses membres soit inférieur à un certain seuil Nmax ; Dans le cas contraire (i.e., l'anneau est complet), le chef d'anneau informera le nœud dissociatif pour changer son numéro SCH afin de créer un autre anneau avec un autre canal SCH pour ne pas avoir de collisions. Si le nœud dissociatif ne répond pas et le temps du temporisateur se termine, un nouvel anneau sera créé. (Bi, Liu, & Shen, 2008) (Booysen, Zeadally, & Rooyen, 2011)

6. Le protocole MAC multicanal DMMAC

Le protocole MAC multicanal DMMAC (Dedicated Multi-channel MAC) a été proposé pour réduire les délais de livraison des messages critiques en utilisant un mécanisme de diffusion (broadcasting) adapté.
Contrairement à plusieurs approches proposées, ce protocole utilise seulement une seule radio par véhicule. Il utilise la structure de WAVE en divisant chaque segment de temps de 100ms en deux intervalles de 50 ms chacun : l'intervalle CCH et l'intervalle SCH. L'intervalle CCH possède deux parties : la première partie a une longueur variable adaptée à la trame de diffusion (Adaptive Broadcast Frame : ABF), elle se compose de plusieurs slots TDMA free-contention, la deuxième partie est l'intervalle CRP : Contention-based Reservation Period (c'est la période de réservation de l'intervalle SCH, elle est basée sur la contention). (Booysen, Zeadally, & Rooyen, 2011)

L'intervalle SCH, utilisé pour la transmission non-critique, est appelé trame d'application non-critique : Non-Safety Application Frame (NSAF).
En résumant, L'intervalle ABF est utilisé pour les transmissions des messages de sûreté et temps-critiques, alors que l'intervalle CRP est employé pour coordonner l'attribution des ressources (canal et temps) pour les applications non-critique. Chaque nœud informe ses voisins à un saut des attributions des slots de tous les voisins à chaque fois qu'il transmet des données (les états libre/occupé des slots et les identificateurs des slots occupés). Un nouveau nœud peut de ce fait déterminer quels sont les slots de l'intervalle ABF qui ne sont pas employés par les voisins à deux sauts, et il peut employer l'intervalle CRP pour réserver un slot de l'intervalle NSAF. La confirmation de l'attribution du slot est faite par les transmissions des nœuds voisins. (Booysen, Zeadally, & Rooyen, 2011)

Dans ce protocole (décrit dans l'article (Lu, Ji, Liu, & Wang, 2010)**),** les processus de réservation de slot pendant les intervalles CRP et SCH ne sont pas expliqués, et les

simulations réalisées sont basées sur des scénarios limités et simples. L'approche proposée a donc quelques inconvénients (Booysen, Zeadally, & Rooyen, 2011) :

- En effet, le fait de rendre l'intervalle ABF plus petit n'a pas vraiment de sens, puisqu'il libère une largeur de bande inutilisée.
- Malheureusement ce temps est utilisé seulement dans la négociation et la période de coordination (CRP) au lieu qu'il soit utilisé dans la période de NSAF.
- Le nombre de slots pendant NSAF est fixe, ceci mènera à une sous- utilisation dans le cas d'une charge de circulation dense.
- Les auteurs de cette approche ne discutent pas ce qui se produit si un nœud sort de la gamme, et comment le slot assigné sera libéré.
- Si tous les nœuds réapproprient les slots au début de l'intervalle ABF, les nouveaux nœuds n'auront pas de slots disponibles.

7. Synthèse sur les protocoles MAC dans VANET

Le protocole MAC est le noyau de partage du medium sans fil avec une largeur de bande limitée et un environnement fortement dynamique. Nous avons présenté dans les trois chapitres précédents, un aperçu sur de diverses approches MAC qui ont été proposées dans la littérature pour permettre le partage efficace du medium sans fil pour les réseaux véhiculaires. Aucune solution proposée n'est parfaite, chacune possède des avantages ainsi que des inconvénients et parfois des scénarios spécifiques adaptés. Un des avantages des approches d'accès aléatoires et des méthodes basées sur la contention est qu'elles nécessitent peu de coordination. Ces méthodes sont donc plus robustes aux changements de configuration de réseau et elles ont des overheads plus petits par rapport aux méthodes basées free-contention. Cependant, les performances de ces méthodes se détériorent de manière significative lorsque le trafic est important car les collisions augmentent avec l'augmentation de la charge de circulation des messages. En plus, n'importe quelle méthode basée sur la contention peut également engendrer des retards illimités dans les délais d'accès au medium.
Par contre, les méthodes free-contention sont avantagées car elles peuvent garantir la qualité de service (QoS), et leurs performances sont meilleures lorsque le trafic est important. Cependant, elles exigent plus de coordination pour l'attribution et l'allocation du support, particulièrement lors des changements rapides dans la configuration de réseau. (Booysen, Zeadally, & Rooyen, 2011) Il a été démontré et largement accepté que les méthodes MAC contention-free permettent une meilleure utilisation du canal et elles sont plus fiables que la méthode CSMA**.** (Booysen, Zeadally, & Rooyen, 2011)

Critères / Catégorie	Coordination	Overheads	Trafic chargé	Temps d'accès	QoS	Fiabilité	Adéquats? pour VANETS
Les protocoles basés-contention	nécessitent peu de coordination donc plus robustes	Peu	Dégradation des performances dans un trafic chargé (à cause de l'augmentation de collisions)	peuvent faire face à des retards illimités dans les délais d'accès au medium.	Qualité de service n'est pas garantie	Faible	OUI Car le Nombre de nœuds imprévisible
Les protocoles free-contention	Exigent plus de coordination pour l'attribution et l'allocation du support	Beaucoup	Meilleures performances dans le cas où le trafic est chargé.	L'accès au canal est garanti pour un réseau statique	Qualité de service garantie pour réseau satique	Elevée	NON Difficulté de coordination car : mobilité, vitesse, nombre de nœuds, V2V

Tableau 2-3 Tableau comparatif des protocoles non basés et basés contention

Bien que le protocole Cluster-Based Multichannel MAC (CBMMAC) soit soigneusement fait, il a également quelques insuffisances : le système est exclusivement conçu pour le trafic d'autoroute, en effet, ce protocole est désigné lorsque la densité de la route est élevée pour permettre les communications inter-cluster. L'approche dépend intensément (Booysen, Zeadally, & Rooyen, 2011) du véhicule cluster-head, et de la coordination dans le cluster. Ce protocole est bien efficace lorsque la mobilité est relativement faible pour permettre la coordination, et les échanges de messages. Un avantage principal d'employer des clusters est l'utilisation des sept canaux dans un cluster, ceci mènera à l'utilisation élevée du canal, mais seulement lorsque les groupes ne se chevauchent pas et ne sont pas près les uns des autres, car les collisions augmentent lorsque les groupes sont à proximité. Chaque véhicule maintient deux radios et le GPS (beaucoup de ressources pour communiquer). (Booysen, Zeadally, & Rooyen, 2011)

La méthode STDMA qui a été développée pour des bas débits est utilisée seulement pour annoncer les positions des nœuds. Cette solution n'est pas adéquate pour transmettre des données volumineuses comme des vidéos (multimédia en général), car elle utilise la méthode TDMA dans laquelle un slot est gaspillé à chaque fois que le nœud n'a pas besoin de transmettre des données. Par contre, elle est plus appropriée pour le trafic des autoroutes que pour un trafic urbain car les changements de vitesse et de direction entre les véhicules sont moins fréquents. (Booysen, Zeadally, & Rooyen, 2011)

L'approche VeSOMAC, basée sur un vecteur binaire permet d'être mis en application avec ou sans la synchronisation. Bien que dans la version asynchrone, l'efficacité du vecteur Bitmap est légèrement réduite à cause de la contrainte qu'un bit représente l'occupation de deux slots au lieu d'un seul ; dans

le cas synchrone, cet inconvénient n'existe pas. *Le VeSOMAC* asynchrone est efficace pour des déploiements distribués sans besoin de synchronisation à travers le réseau. Cette approche a quelques imperfections, en effet, le système est conçu et évalué seulement pour des scénarios d'autoroute. Il est très probable que les performances du système se dégradent de manière significative dans des environnements urbains avec de nombreux véhicules roulant dans plusieurs directions. Le papier rapporte un retard de livraison plus long que celui de IEEE 802.11p à cause des horloges relatives dans chaque véhicule. Il existe également une perte de temps significative dans le système, puisque chaque nœud doit occuper un slot, même s'il n'a aucune donnée à transmettre. En plus, la taille de la trame en étant un paramètre de conception, ne permet pas un nombre très élevé de véhicules dans un groupe. La trame devrait donc être conçue pour une capacité maximale à tout moment, menant à la sous utilisation seulement si quelques nœuds sont présents. En outre, dans cette solution, il n'y a aucune disposition pour utiliser les canaux multiples assignés par la FCC. (Yu & Biswas, 2007) (Booysen, Zeadally, & Rooyen, 2011)
Donc, cette solution doit être modifiée, il est possible de combiner entre cette approche et celle des clusters par exemple, en effet, on peut garder le principe du vecteur Bitmap à l'intérieur d'un groupe car le nombre de nœuds est limité dans un groupe à un moment donné, et utiliser le principe du WAVE 802.11p pour les communications intra groupe.

Bien que le protocole multi canal token-ring nous semble efficace, la topologie d'anneau qui est formée par les nœuds chefs rend le système fortement dépendant de ces nœuds. Si le nœud chef d'anneau quitte l'anneau, il faudra réinitialiser l'association d'anneaux, Ceci rend ce schéma plus adapté aux scénarios où il existe une tendance de mobilité en groupe, plutôt qu'une mobilité imprévisible. (Booysen, Zeadally, & Rooyen, 2011) (Bi, Liu, & Shen, 2008)
La topologie d'anneaux est également assez statique puisque la taille de l'anneau est fixe.
Etant donnés la topologie d'anneau, la taille fixe, et le seuil de la vitesse des nœuds, il est probable que beaucoup de nœuds ne peuvent pas joindre les anneaux. Le système se base sur la connectivité entre tous les nœuds dans l'anneau, puisque le jeton doit circuler entre les nœuds ; et le nœud chef doit rendre compte de toutes les interactions. Ce scénario est idéal et non probable en raison de la mobilité élevée des véhicules.
MCTRP emploie CSMA / CA pour des messages critiques et TDMA tokenpassing pour les transferts de données. Ceci mène à un scénario où les messages critiques pourraient faire face à des retards illimités sous une lourde charge du réseau.
MCTRP dépend de deux radios par véhicule et tous les slots de transmission sont employés quoiqu'un nœud peut ne pas transmettre. (Bi, Liu, & Shen, 2008) (Booysen, Zeadally, & Rooyen, 2011)
L'efficacité du protocole MAC EDCA actuellement utilisé pour WAVE afin de réduire le nombre de collisions se base sur **le mécanisme backoff** qui consiste en une large sélection aléatoire des périodes de backoff afin d'écarter les retransmissions dans le temps. De ce fait réduire la probabilité que les mêmes trames produisent de nouvelles collisions. Ce protocole permet de donner des possibilités en matière de qualité de service. Les modifications introduites au niveau de la couche MAC assurent un traitement spécifique pour chaque type de trafic.
Les recherches et les simulations réalisées prouvent que cette différenciation garantit une meilleure transmission de la voix et de la vidéo. Mais plusieurs problèmes se posent, à savoir la dégradation des trafics à faible priorité. En effet, au moment où seulement un trafic best effort circule, sa transmission avec une faible priorité engendre un temps d'attente supplémentaire dans la file d'attente. (Huang & Chen, Telematics Communication Technologies and Vehicular Networks: Wireless Architectures and Applications, 2010) (Moustafa & Zhang, 2009) (Nehdi, 2005) En plus, les messages envoyés sur le canal CCH doivent être traités avec différentes priorités selon l'aspect critique

du message. Cependant, EDCA ne traite pas cette condition. En effet, il n'établit pas des priorités strictes, (Barradi, Hafid, & Gallardo, 2010) mais seulement, il avantage relativement quelques types de messages par rapport à d'autres messages (ie il impose seulement une différence dans les services pour les différents types de messages). (Barradi, Hafid, & Gallardo, 2010). Cela soulève d'autres problèmes :

(1) Un message ayant une faible priorité, peut heurter un message plus prioritaire pendant sa transmission, cela cause la perte des deux transmissions, même si le deuxième message est très critique ;
(2) un message de faible priorité peut réussir à accéder au canal et emporter le temps précieux nécessaire pour la transmission des messages prioritaires. (Barradi, Hafid, & Gallardo, 2010)

Un autre problème est que, une fois les messages sont diffusés (broadcasting) sur le canal CCH, il n'y a aucune réponse ; ceci signifie qu'il n'est pas possible de savoir si une transmission est réussie ou pas, or, cette information diminue l'utilisation exponentielle de la technique backoff afin de réduire les congestions. (Barradi, Hafid, & Gallardo, 2010)

En conclusion, La norme IEEE 802.11p devrait aborder plusieurs challenges, tels que les fréquentes déconnexions et le 'handoff'. Il est important de montrer aussi au moins par simulation et analyse, si la norme 802.11p garantit les conditions de fiabilité et le minimum de temps de latence des applications sécuritaires de DSRC pour les réseaux véhiculaires. (Moustafa & Zhang, 2009)

Cette norme ne s'adresse pas d'une manière adéquate aux applications imposées par les réseaux VANET, puisqu'elle emploie une approche basée sur la contention. La qualité de service QoS ne peut pas être garantie pour les messages critiques de sécurité et les transmissions en temps réel. (Booysen, Zeadally, & Rooyen, 2011)

Ce tableau récapitule les principales approches MAC proposées et discutées ci-dessus.

Tableau 4-4 Les approches MAC récemment proposées pour les réseaux VANETs. **(Booysen, Zeadally, & Rooyen, 2011)**

Protocoles / Paramètres	WAVE MAC	STDMA	VeSO-MAC	MCTRP	CBM-MAC	DMMAC
Buts des approches alternatives MAC	Assurer l'interopérabilité entre dispositifs sans fil & mode opératoire pour fonctionner dans DSRC.	Eviter les collisions maritimes	Améliorer les flux de données	Diminuer la latence des messages d'urgence et Augmenter le flux de sortie non temps réel	Garantir la livraison de message de sécurité tout en supportant les données non-critiques	Collision-libre et Délais de livraison avec adaptation de flux de données
Destiné et Simulé pour scénarios d'autoroute	Oui	Partiellement	Oui	Oui	Oui	Oui
Destiné et Simulé pour scénarios Urbains	Oui	Partiellement	Non	Non	Non	Non
Délais liés à la transmission temps-critique	Non	Partiellement	Partiellement	Oui	Oui	Oui
Coordination en temps et indépendance du nœud chef	Oui	Oui	Oui	Non	Non	Oui
Auto-synchronisation (independent du GPS)	Non	Non	Oui	Non	Oui	Non
Conformité à la synchronisation WAVE (intervalle CCH& SCH)	-	Non	Non	Non	Non	Oui
L'attribution de la bande passante adaptée à la demande	Non	Partiellement	Non	Non	Non	Partiellement
Exploitation multi-canal (canaux WAVE)	-	Non	Non	Oui	Oui	Oui
Nombre de radios par véhicule	-	1	1	2	2	1
Complexité (Niveau de coordination et de gestions requises)	Simple	Assez simple	Assez simple	Assez complexe	Assez complexe	Complexe

Dans cette première partie, nous avons présenté les différents protocoles de la couche MAC dédiés ou adaptés pour les réseaux véhiculaires. Nous avons soulevé notre synthèse sur les différentes approches. Reste maintenant le choix de la méthode à améliorer dans ce travail. Est ce que nous optons pour une solution basée: free-contention, basée-contention, ou hybride ?

Ce que nous avons remarqué est que le standard 802.11p est bien installé, et tôt ou tard, il constituera le noyau principal des communications véhiculaires. Il faut proposer donc une solution qui s'intègre facilement au standard existant ; plutôt que de changer l'existant pour notre solution, et le standard 802.11p étant le plus populaire, connait de plus en plus d'intérêt dans plusieurs projets, ainsi que dans la communauté industrielle comme le projet SAE J2945.1 (Stanica, 2011)

Certes, ce standard MAC 802.11p possède beaucoup d'insuffisances pour être déployé et généralisé dans nos routes. C'est ce qui nous a motivé à nous intéresser aux travaux récents qui ont pour but l'amélioration de ce standard.

Dans le tableau suivant, nous avons soulevé la tendance des travaux récents autour de la norme 802.11p et le mode WAVE.

Des travaux récents d'amélioration du standards 802.11p & WAVE	
Axes de recherche (802.11p & WAVE)	**Quelques travaux**
Amélioration de 802.1p & WAVE pour les applications de sécurité et de non-sécurité (confort).	(Amadeo, Campolo, & Molina, 2012)
Amélioration des transmissions des messages beacons pour permettre une collecte rapide et efficace des informations	(Vales-Alonso, Vicente-Carrasco, & Alca, 2011)
Amélioration des stratégies de Transmissions multi sauts & Broadcasting (diffusion) dans la norme 802.11p	(Vinel, Campolo, Petit, & Koucheryavy, 2011)
Modélisation du standard 1609.4 **Synchronisation et mutation entre les canaux WAVE (canal de contrôle et les canaux de service)**	(Wang, Leng, Fu, & Zhan, 2010) (Ameixieira, Matos, Moreira, Cardote, Oliveira, & Sargento, 2011)
La transmission d'accusés de réception pour minimiser les collisions	(Barradi, Hafid, & Gallardo, 2010)
L'étude des priorités entre les différentes catégories d'accès	(Barradi, Hafid, & Gallardo, 2010)
Amélioration de l'algorithme backoff (adaptation dynamique)	(Barbosa, Bessa, Sérgio, Rober, & Jùnior, 2011)

Tableau 4-5 Quelques travaux récents d'amélioration du standards 802.11p & WAVE.

8. Conclusion

Nous avons parcouru dans ce chapitre les principaux protocoles MAC hybrides récemment développés pour les réseaux véhiculaires.

Nous avons terminé ce chapitre et cette première partie par une synthèse où nous avons discuté les approches présentées précédemment et tiré des conclusions.

Chapitre 4
Les protocoles MAC hybrides

9. Introduction

Après avoir présenté les challenges de la couche MAC pour les réseaux VANETs et les approches MAC basées et non basées sur la contention au niveau du deuxième chapitre, et les différents standards pour les réseaux véhiculaires au niveau du troisième chapitre. Ce chapitre parvient afin de présenter les protocoles MAC hybrides qui combinent deux ou plusieurs protocoles planifiés (frree-contention) ou aléatoires (based-contention). On va présenter quelques protocoles MAC (non standard) dédiés spécialement pour les réseaux VANET et qui ont été récemment proposés dans la littérature.

10. Le protocole CBMMAC : Cluster-Based Multichannel MAC

Afin de bien utiliser les canaux DSRC, les chercheurs dans (Kim, Jung, & Lee, 2009) ont proposé un schéma de communication basé sur les clusters (le groupement) en intégrant des groupes dans les protocoles MAC basés contention.

Dans ces protocoles, le véhicule chef du groupe "cluster-head" (CH) joue le rôle de coordinateur pour collecter et délivrer les messages de sécurité dans son groupe en temps réel, et les envoyer à ses voisins. Il contrôle également les transmissions de données entre les membres de son groupe qui ne sont pas en temps réel.

Ce protocole utilise les mécanismes TDMA/broadcast dans le cluster (groupe), et la norme IEEE 802.11 MAC entre les véhicules CH ("cluster-head"), pour assurer une livraison de messages en temps réel. Il suppose aussi que chaque véhicule possède deux radios.

Le but de ce protocole est de considérer la qualité de service et d'augmenter le nombre de flux de sortie pour des communications non-temps-réel (augmenter le débit). Pour réaliser ces buts, les chercheurs ont développé un schéma de communication multi canaux qui se base sur la bande DSRC. Ils ont défini donc des fonctions particulières pour les 7 canaux DSRC dans le schéma de ce protocole MAC. Ces fonctions sont présentées dans le tableau suivant :

Channel Name	*Channel Abbreviations*	*DSRC Channel Numbers*
Intercluster control	ICC	178
Intercluster data	ICD	174
Cluster range control	CRC	172
Cluster range data	CRD	176,180,182,184

Tableau 4-1 Définition des canaux DSRC pour le protocole CBMMAC (Moustafa & Zhang, 2009)

Chaque cluster-head se charge des communications à l'intérieur de son cluster et maintient les informations de routage lui permettant de joindre les autres cluster-heads. De plus, comme les

cluster-heads ne sont pas forcément reliés, des nœuds intermédiaires ou passerelles sont aussi élus et utilisés pour les communications entre cluster-heads.
Le protocole définit l'algorithme de groupement (de clustering) dans les deux phases MAC : basé contention et contention-free, utilisé respectivement dans les communications inter-cluster et intra-custer. (Moustafa & Zhang, 2009) (Kim, Jung, & Lee, 2009) (Booysen, Zeadally, & Rooyen, 2011)

Le fonctionnement du protocole
Les véhicules qui sont à proximité les uns des autres, forment un groupe (cluster). Ce groupe contient un seul véhicule chef noté CH (c'est le véhicule cluster head) qui est sélectionné par des règles prédéfinies. Chaque véhicule CH communique via le canal CRC en utilisant MAC free-contention TDMA avec les véhicules appartenant à son groupe (véhicules membres du même groupe), pour recevoir et envoyer les messages de sécurité (comme les messages de contrôle). Le canal ICC est utilisé par le véhicule CH pour communiquer avec les autres véhicules CH, les message de sécurité en utilisant le schéma MAC 802.11.
Chaque véhicule membre du cluster (qui n'est pas CH et appartient au groupe) échange des messages via le canal CRD avec les autres véhicules de son groupe. (Moustafa & Zhang, 2009)
Le canal ICD peut être utilisé pour les communications non temps réels entre les membres des clusters voisins. (Véhicule membre et non pas CH).

Pour réaliser ces communications, trois protocoles sont développés dans cette approche : le protocole de configuration des clusters, le protocole de communication inter cluster, et le protocole de communication et de coordination intra cluster.
Le premier protocole : **protocole de configuration de cluster** utilise MAC based-contention sur le canal ICC pour la gestion de clusters (tel que joindre ou quitter un cluster, l'élection du cluster-head). Le deuxième protocole : **le protocole de transmission d'inter cluster** est responsable de l'échange des messages de sûreté et du trafic non-temps-réel sur les canaux ICC et ICD respectivement. Le troisième protocole : **le protocole de communication et de coordination intra cluster** utilise le protocole MAC multicanaux pour contrôler la communication entre le véhicule CH et les véhicules appartenant à son cluster. (Moustafa & Zhang, 2009)

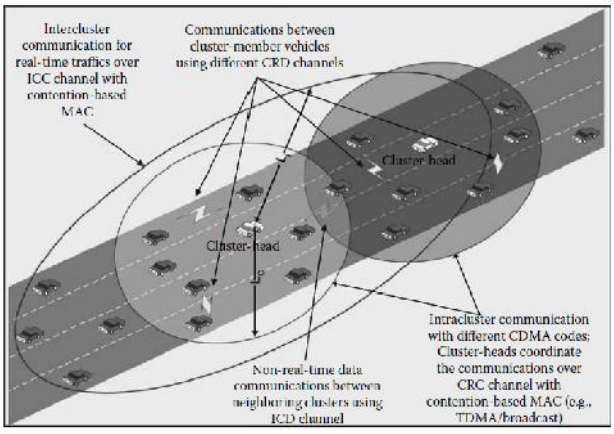


Figure 4-1 Illustration d'une communication en utilisant le protocole **CBMMAC** (Moustafa & Zhang, 2009)

	Transceiver	Channel	MAC method
cluster head (CH)	1	CRC	contention-free TDMA and broadcast
	2	ICC	contention-based (e.g. IEEE 802.11)
cluster member	1	CRC	contention free TDMA and Broadcast
	2[a]	CRD	contention-free (allocated channels)
		ICD	contention-based (e.g. IEEE 802.11)
non-member	1	ICC	contention-based (e.g. IEEE 802.11)

Tableau 4-2 L'attribution des canaux DSRC dans le protocole CBMMAC. (Booysen, Zeadally, & Rooyen, 2011)

Le protocole de coordination et de communication est basé sur le protocole MAC multicanaux, où chaque véhicule CH utilise le canal CRC, pour rassembler ou diffuser des messages de sûreté et pour coordonner les véhicules membres afin qu'ils puissent transférer des données non-temps-réel à l'intérieur ou entre les clusters. Le protocole de communication inter cluster transmet deux types de messages,

(3) les messages de sûreté, en temps réel sur le canal ICC ;

(4) et les messages non-temps-réel sur le canal ICD ;

Les clusters-heads, quasi-cluster-heads, et quasi-cluster-members utilisent les protocoles basés contention (IEEE 802.11) pour accéder au canal ICC. Puis, les véhicules CH rassemblent les messages de sûreté de leurs propres clusters, ils essaient ensuite d'accéder au canal ICC pour envoyer les données fusionnées aux véhicules CH voisins.

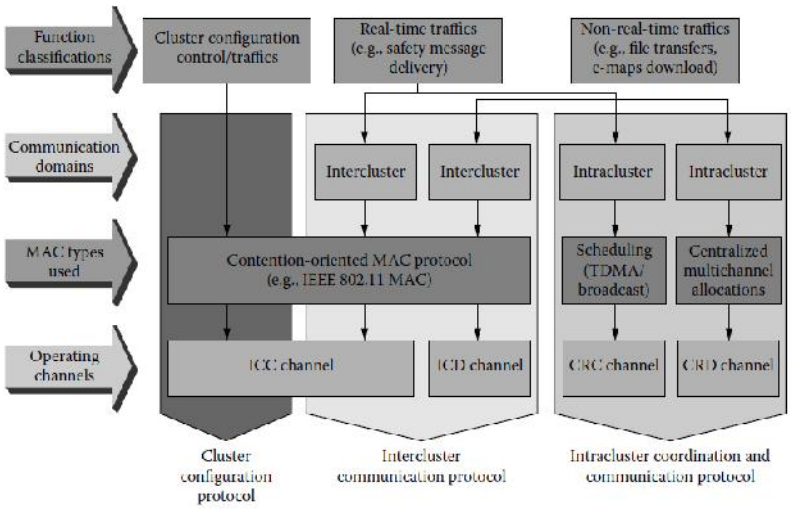


Figure 4-2 Diagramme de structure du schéma CBMMAC. **(Moustafa & Zhang, 2009)**

Les résultats de simulation et d'analyse obtenus dans ce travail prouvent que ce protocole peut réaliser non seulement une livraison opportune des messages de sûreté, mais également il

augmente le flux de sortie pour le trafic non-temps-réel. (Booysen, Zeadally, & Rooyen, 2011)

11. STDMA : self-organising TDMA

La méthode self-organising TDMA : STDMA (TDMA à organisation automatique) a été évaluée par Bilstrup et al (Bilstrup, Uhlemann, Strom, & U, 2009) dans un environnement véhiculaire. Son but est de garantir un temps de livraison opportun des messages critiques. Elle est actuellement utilisée dans l'aviation et la communication entre les bateaux en tant qu'élément du système automatique d'identification (AIS) (Booysen, Zeadally, & Rooyen, 2011)
STDMA applique le principe de R-ALOHA, elle fournit une coordination décentralisée, et presque basée free-contention. Elle divise le temps en trames de même durée et la trame en slots, la trame est considérée comme une séquence répétée d'un nombre fixe de slots. Les trames ne sont pas synchronisées et chaque nœud synchronise ses slots par rapport au temps GPS (Booysen, Zeadally, & Rooyen, 2011)

*Le principe de STDMA :*Au départ, un nœud commence par déterminer le taux de rapport (report rate ie le nombre de slots employés pendent une trame). Puis, quatre phases vont se suive : *l'initialisation, l'entrée du réseau, la première trame, et le processus périodique*. Lors de l'initialisation, le nœud se met à l'écoute du canal, pendant une trame, pour déterminer l'affectation des emplacements (ie, quels sont les slots occupés, et quelles sont les positions des nœuds qui les utilisent). Dans la phase d'entrée dans le réseau, le nœud détermine ses propres slots de transmission dans la trame d'après les règles suivantes:

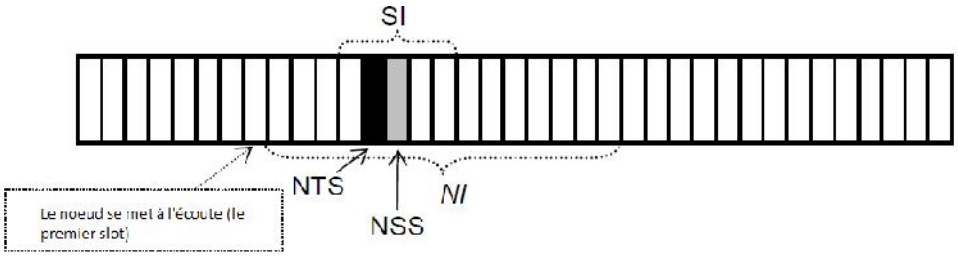


Figure 4-3 La structure du message STDMA. (Bilstrup, Uhlemann, Strom, & U, 2009)

(i) : Calculer NI :(nominal increment) en divisant le nombre de slots sur le taux de rapport,
(ii) : Sélectionner au hasard un premier slot (NSS), entre l'emplacement actuel et le NI (cet emplacement sera le début de la trame pour le nœud et donc chaque nœud possède son propre NSS),
(iii) Déterminer un intervalle de sélection de slots (SI) qui représente 20 % de la période Ni et qui est autour du slot NSS comme le montre la figure 4.3,
(iv) Une fois la trame est déterminée, le nœud à chaque fois sélectionne de manière aléatoire un slot NTS à partir de l'intervalle SI, si le NTS choisi au hasard est occupé, alors le slot libre le plus proche dans l'intervalle SI sera choisi. Si tous les slots dans SI sont occupés, alors le slot utilisé le plus loin sera sélectionné. (Bilstrup, Uhlemann, Strom, & U, 2009)

Cette méthode possède quelques insuffisances si elle est considérée comme solution pour diverses applications et scénarios de VANET. STDMA AIS a été développée et normalisée pour des bas débits, elle est utilisée seulement pour annoncer les positions des nœuds.

Cette solution n'est pas adéquate pour transmettre des données volumineuses comme des vidéos (multimédia en général) car elle utilise la méthode TDMA dans laquelle un slot est gaspillé à chaque fois qu'un nœud ne transmet pas de données. Par contre, cette méthode est plus appropriée pour un trafic véhiculaire sur des autoroutes que pour un trafic urbain car il y a moins de changement de direction et de la vitesse entre les nœuds sur l'autoroute.

En conséquence, cette approche a été dédiée et évaluée sur des autoroutes pour des applications de sécurité qui emploient des messages courts et exigent une fiabilité élevée. Ce système doit toujours être relié au GPS, et il utilise seulement un des sept canaux disponibles de WAVE. Dans le cas de surcharge de réseau, les slots sont également en surcharge, donc ils ne seront pas bien séparés, et cela produira des collisions qui peuvent retarder les transmissions. (Booysen, Zeadally, & Rooyen, 2011)

12. VeSOMAC: self-organizing collision-free TDMA approach

Une approche : self-organising contention-free TDMA MAC appelée VeSOMAC est développée et évaluée par Yu et Biswas (Yu & Biswas, 2007).

Le but de cette recherche est de développer une méthode MAC distribuée basée contention-free afin d'augmenter le transfert de données entre les véhicules dans un scénario d'autoroute. Dans l'approche VeSOMAC, les nœuds sont synchronisés via le GPS, ou bien avec les autres (auto-synchronisation).

La trame représente essentiellement une période pour un nœud (voir la figure suivante). Toutes les trames ont la même durée T_{trame}.. Par conséquent, le taux assigné à un véhicule est $\lambda_{alloc} = 1/T_{trame}$ trame/sec. (Booysen, Zeadally, & Rooyen, 2011)

VeSOMAC peut fonctionner en mode synchrone et asynchrone. En mode synchrone, tous les véhicules sont synchronisés, et donc, ils ont les mêmes limites des trames et des slots. En mode asynchrone, les véhicules maintiennent leurs propres limites de trames et donc les slots sont également asynchrones (ie deux trames de deux nœuds différents peuvent être décalées comme montré dans la figure 4.4).

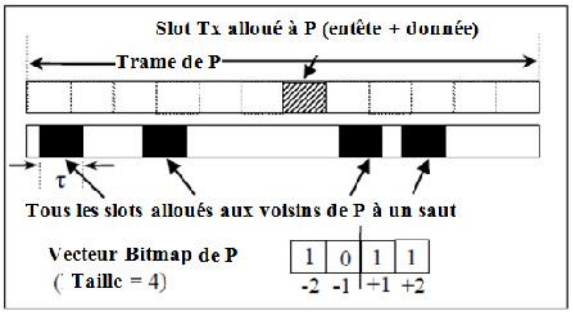


Figure 12-4. Le vecteur Bitmap pour des opérations asynchrones. (Yu & Biswas, 2007)

Dans cet exemple, le vecteur Bitmap est à 4 bits, chaque bit représente l'état d'occupation de deux slots autour du nœud P car un slot d'un nœud voisin peut occuper partiellement deux slots en mode asynchrone.
Les valeurs (-2, -1, +1, +2 : représentent dans la figure les positions des slots par rapport au slot P, comme par exemple +1 est le slot juste après le slot P). Le '1' dans l'emplacement "+1" i indique qu'au moins un des deux slots qui se trouve juste après le slot p est entièrement ou partiellement occupé.
La longueur du vecteur Bitmap est un paramètre de conception dont la valeur maximale est le nombre de slots dans une trame. Dans la figure 4.4, la taille de la trame est 12, tandis que la longueur du vecteur Bitmap est 4, ce qui empêche le nœud P de savoir l'état du slot extrême gauche. (Le vecteur donne les informations d'occupation de seulement 8 slots). (Yu & Biswas, 2007)

- **Allocation d*e slot***

  Les slots de deux nœuds qui peuvent communiquer en un saut ou bien en deux sauts, ne doivent pas se chevaucher afin d'éviter les collisions et le problème des nœuds cachés.
  En utilisant ce vecteur bitmat dans l'en-tête de paquet, le véhicule informe sans interruption ses voisins directs au sujet des slots occupés. D'autre part, en écoutant les vecteurs Bitmap de tous les paquets reçus, le véhicule peut détecter les slots de ses voisins à 1-hop et à 2-hop. Cette information peut alors être employée pour choisir un slot libre pour transmettre des données. (Yu & Biswas, 2007)

Ce travail n'a pas mentionné comment un nœud combine les vecteurs bitmap qui ne sont pas synchronisés pour choisir un slot, bien que ce choix dépend de la synchronisation (Booysen, Zeadally, & Rooyen, 2011)
La relocalisation de slots est faite au moyen d'un mécanisme de résolution de collisions. Quand un nœud détecte à plusieurs reprises que ses voisins ne reconnaissent pas son slot, il suppose qu'une collision a lieu et il réapproprie son slot. (Booysen, Zeadally, & Rooyen, 2011)

13. Le protocole multicanal token-ring (MCTRP)

Le protocole multicanal token-ring est proposé pour les réseaux VANET par Bi et al (Bi Y. , Liu, Cai, & Shen, 2009) Son but est de développer un protocole MAC basé free-contention dans lequel les nœuds s'organisent de manière autonome en utilisant la technique de jeton et en supposant une topologie en anneaux. Cette solution, a été proposée afin de minimiser le temps de latence pour les messages critiques et d'augmenter, le taux de trafic (nombre de messages) dans le réseau pour les applications non-critiques.
Le fonctionnement de ce protocole se base sur le groupement des nœuds en anneaux. Chaque groupe possède un chef (leader).
Le schéma token-passing TDMA (TDMA en utilisant le jeton), est utilisé pour contrôler l'accès au medium pour les transmissions des données intra-ring (à l'intérieur de l'anneau) et le CSMA/CA est utilisé pour contrôler l'accès au medium pour transmettre les données inter-ring (entre les anneaux), ie les informations urgentes et les transmissions de configuration et d'administration des anneaux. (Booysen, Zeadally, & Rooyen, 2011)

Chaque nœud est équipé de deux radios. La première radio est accordé de manière permanente au canal 178 du WAVE pour les communications de données inter-ring, ie les messages critiques inter-ring et la configuration de l'anneau (ring setup).

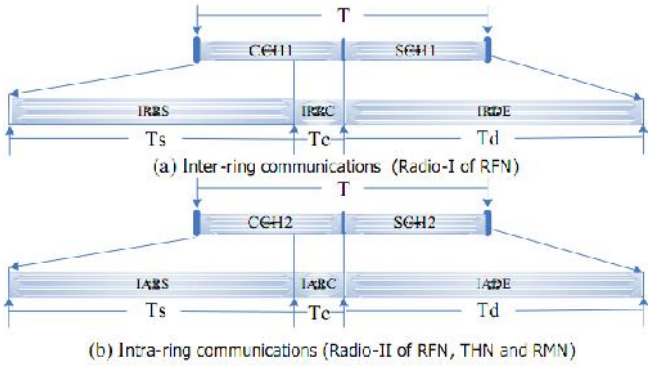


Figure 13-5 Les intervalles de communication dans le protocole multicanal token-ring. (Bi, Liu, & Shen, 2008)

La deuxième radio est allouée à un des six canaux restants du WAVE. Chaque anneau l'utilise pour les transmissions intra-ring des messages critiques, de coordination, et les données.
MCTRP se synchronise via le GPS et il divise le temps en segments égaux. Chaque segment T est réparti en trois périodes, comme illustré dans la figure 4.5, la première période pour la sécurité (Ts), la deuxième pour la coordination (Tc) et la dernière pour l'échange de données (Td).
La livraison du jeton se produit dans l'intervalle IARC ou IADE. Le jeton attribue le droit de transmission des paquets de données non urgentes d'intra-anneau aux nœuds membres de l'anneau sur la Radio-II.
Dans MCTRP, le jeton est livré selon l'état du buffer IADE du nœud qui a le jeton. Dans un premier cas, si le buffer n'est pas vide au début de la période Td, le nœud ayant le jeton transmettra ses paquets jusqu'à la fin de Td. Après, il livrera le jeton à son successeur dans la prochaine période Tc et attendra l'accusé. Une fois que ce nœud reçoit l'accusé de son successeur, il deviendra un nœud membre d'anneau. Autrement, le nœud chef (qui maintient le jeton) retransmettra le jeton jusqu'à ce qu'il obtienne un accusé ou le temps de retransmission atteint une valeur maximale Tmax. Dans ce dernier cas, on considère que son successeur a quitté l'anneau, alors le nœud chef le redonnera au nœud créateur d'anneau qui effectuera une opération de suppression (pour plus de détails, voir la section III de (Bi, Liu, & Shen, 2008)**)** (Booysen, Zeadally, & Rooyen, 2011)

Dans le deuxième cas (ie si le buffer de paquet est vide), le nœud chef déclenche un temporisateur (timer), et lorsque le temps du timer s'achève, il transmettra le jeton à son successeur dans l'intervalle IADE. Ceci assure que les nœuds ayant des paquets à transmettre pourraient acquérir le jeton aussitôt que possible. Par conséquent, le flux de sortie dans le réseau peut être augmenté d'une manière significative.
Chaque nœud dans l'anneau maintient une liste d'identificateurs des nœuds appartenant au même anneau (ID, MAC ADDRESS). Quand la couche MAC au niveau d'un nœud reçoit un paquet de la couche supérieure, elle vérifie si l'adresse de destination de ce paquet existe dans cette liste. Si l'adresse n'est pas dans la liste, le paquet sera transmis en utilisant la Radio I

suivant le protocole MAC IEEE802.11 (car il s'agit d'une communication inter-ring); dans le cas contraire, le nœud attendra le jeton pour envoyer le paquet (il s'agit d'une communication de données d'intra-anneau). (Bi, Liu, & Shen, 2008)

L'initialisation d'anneau se fait quand un nœud annoncera le message de création d'anneau dans l'intervalle IRRC en utilisant la Radio I, il déclenche ainsi un temporisateur de création d'anneau. Le message annoncé inclut le numéro SCH pour des communications de données d'intra-anneau. Si un anneau est déjà créé dans le canal spécifié, le chef d'anneau répond à ce nœud (l'initiateur) et l'invite à joindre son anneau à condition que le nombre de ses membres soit inférieur à un certain seuil Nmax ; Dans le cas contraire (i.e., l'anneau est complet), le chef d'anneau informera le nœud dissociatif pour changer son numéro SCH afin de créer un autre anneau avec un autre canal SCH pour ne pas avoir de collisions. Si le nœud dissociatif ne répond pas et le temps du temporisateur se termine, un nouvel anneau sera créé. (Bi, Liu, & Shen, 2008) (Booysen, Zeadally, & Rooyen, 2011)

14. Le protocole MAC multicanal DMMAC

Le protocole MAC multicanal DMMAC (Dedicated Multi-channel MAC) a été proposé pour réduire les délais de livraison des messages critiques en utilisant un mécanisme de diffusion (broadcasting) adapté.
Contrairement à plusieurs approches proposées, ce protocole utilise seulement une seule radio par véhicule. Il utilise la structure de WAVE en divisant chaque segment de temps de 100ms en deux intervalles de 50 ms chacun : l'intervalle CCH et l'intervalle SCH. L'intervalle CCH possède deux parties : la première partie a une longueur variable adaptée à la trame de diffusion (Adaptive Broadcast Frame : ABF), elle se compose de plusieurs slots TDMA free-contention, la deuxième partie est l'intervalle CRP : Contention-based Reservation Period (c'est la période de réservation de l'intervalle SCH, elle est basée sur la contention). (Booysen, Zeadally, & Rooyen, 2011)

L'intervalle SCH, utilisé pour la transmission non-critique, est appelé trame d'application non-critique : Non-Safety Application Frame (NSAF).
En résumant, L'intervalle ABF est utilisé pour les transmissions des messages de sûreté et temps-critiques, alors que l'intervalle CRP est employé pour coordonner l'attribution des ressources (canal et temps) pour les applications non-critique. Chaque nœud informe ses voisins à un saut des attributions des slots de tous les voisins à chaque fois qu'il transmet des données (les états libre/occupé des slots et les identificateurs des slots occupés). Un nouveau nœud peut de ce fait déterminer quels sont les slots de l'intervalle ABF qui ne sont pas employés par les voisins à deux sauts, et il peut employer l'intervalle CRP pour réserver un slot de l'intervalle NSAF. La confirmation de l'attribution du slot est faite par les transmissions des nœuds voisins. (Booysen, Zeadally, & Rooyen, 2011)

Dans ce protocole (décrit dans l'article (Lu, Ji, Liu, & Wang, 2010)**),** les processus de

Chapitre 6 : Principes de Conception du Mécanisme NN-ACW

1. Introduction

Dans le chapitre précédent, nous avons présenté les différentes approches d'adaptation de la taille de la fenêtre de contention. Nous avons présenté deux classifications et on a rajouté une nouvelle catégorie à la deuxième classification. Cette classe fait l'objet de notre travail.

Dans ce chapitre, nous présentons notre contribution ainsi que les principaux points qui résultent de nos choix. C'est pourquoi dans un premier temps nos principaux objectifs et motivations sont décrits. Dans un deuxième temps, nous aborderons en détail notre proposition. Une partie importante sera consacrée au modèle d'estimation de l'état du réseau. Ensuite, nous insisterons en particulier sur les effets de l'algorithme back-off en proposant deux solutions d'amélioration pour ajuster la taille de la fenêtre de contention.

2. Motivation et Objectifs

Quelles contraintes des Réseaux véhiculaires ?

Un réseau véhiculaire contrairement à un réseau Mobile ad hoc offre plus d'avantages pour le déploiement des applications. En effet, il n'y a pas de contrainte d'énergie, ni limitation de stockage. Cependant, un tel réseau est sujet à un nombre de caractéristiques qui rendent son déploiement très complexe. On peut citer essentiellement : la mobilité élevée des nœuds, les contraintes du médium radio, l'absence d'une administration centralisée dans les scénarios V2V. Ces caractéristiques influent sur la qualité de service aussi bien que sur les délais d'attente. Pour cela, un protocole de communication doit être rapide, efficace et spécifique à l'environnement véhiculaire.

Pourquoi la couche mac?

Nous avons choisi d'agir au niveau de la couche MAC pour plusieurs raisons. Premièrement, il existe peu de solutions mac dédiées aux réseaux véhiculaires. Le standard mac dédié aux réseaux véhiculaires en sa version actuelle ne prévoit pas un protocole d'adaptation selon l'environnement. En plus, la couche physique est liée à la technologie et au matériel, tandis que les couches 3, 4 et plus dépendent de la couche mac.

Pourquoi un modèle formel et une approche mathématique ?

En raison de la complexité de ce type de réseaux, il existe peu de modèles mathématiques qui établissent une relation entre les performances du protocole et les paramètres du réseau. De même, on apprend qu'il existe une relation proportionnelle inverse entre la taille optimale de

la fenêtre de contention et la densité des véhicules. D'où notre but est d'établir une relation entre les paramètres du réseau et la probabilité de collision d'une part, et entre la valeur minimale de la fenêtre de contention et l'état du réseau d'autre part.
La plupart des approches existantes proposent des algorithmes probabilistes en se basant sur des tests statiques (par exemple : si un certain paramètre est supérieur à un certain seuil, alors on augmente la taille). Cependant, l'algorithme statique n'est pas approprié au réseau véhiculaire et à n'importe quel scénario. Cela donne de bons résultats dans certains cas mais ce n'est pas facile de généraliser. C'est pourquoi nous avons pensé à une approche formelle basée sur l'apprentissage. Cela rend l'algorithme dynamique et évolutif.

Pourquoi une nouvelle solution ?

Le fait d'utiliser l'algorithme CSMA/CA rend le comportement du réseau non déterministe. Ce non déterminisme peut provoquer une instabilité dans le réseau et peut changer ses performances.

En plus, peu d'études se sont intéressées aux capacités du passage à l'échelle du protocole IEEE 802.11p et à des scénarios caractérisés par une densité élevée.

Dans notre travail, nous considérons que fournir l'efficacité de l'algorithme de backoff est plus important que fournir l'équité surtout quand le réseau est surchargé ou bien quand il n'y a pratiquement pas de charge dans le réseau (ie dans les cas extrêmes). L'équité n'est pas notre objectif principal.

Cependant, il y a une nécessité d'avoir de nouvelles solutions qui peuvent être facilement intégrées dans la norme IEEE 802.11p et qui peuvent améliorer les performances de la méthode d'accès au canal sous une charge importante. Une grande communauté chercheurs et d'industrie travaille actuellement sur la question.

Nous voulons comme but dans ce travail que chaque véhicule réagisse de manière différente des autres véhicules, quoi que cet algorithme assure cette contrainte en agrandissant l'intervalle de la fenêtre de contention, mais cette méthode aléatoire n'est pas la méthode optimale afin d'assurer la qualité de service et un temps d'attente acceptable pour un tel réseau, qui est entièrement différent d'un autre réseau sans fil.
En outre, un autre objectif principal est de proposer une technique afin d'avoir une bonne estimation de l'état du trafic dans le réseau, en utilisant des informations disponibles et sûres, et non pas exiger un échange permanent des messages de contrôle ou l'existence obligatoire des RSU. Ces objectifs ont été tracés pour que notre solution puisse être mise en œuvre facilement.

3. Environnement et hypothèses

Nous considérons un réseau véhiculaire composé de nœuds mobiles qui communiquent entre eux en utilisant la simple communication V2V et sans aucun

recours aux points d'infrastructures vu que les solutions V2V sont plus scalables et peu coûteuses. Nous supposons que les véhicules sont équipés avec des antennes omnidirectionnelles ayant la même portée de transmission, des PC intégrés, des receveurs GPS pour les localiser géographiquement. Les communications entre les véhicules sont supposées bidirectionnelles et sont basées sur la diffusion de messages. L'utilisation des messages RTS (Ready To Send) et CTS (Clear To Send) est essentielle dans la solution proposée pour régler le problème du nœud caché et du nœud exposé.

La densité et les distances sont obtenues par le simulateur, car notre but n'est pas d'utiliser les messages beacon, mais d'estimer ces informations, malheureusement le simulateur ne donne pas des scénarios réalistes pour pouvoir déduire la densité à partir de la vitesse ou des points d'arrêt.

4. Contribution et Principes de base

Notre contribution se compose de plusieurs parties, un modèle intelligent pour estimer le niveau de contention dans le réseau. Il est implémenté comme un nouveau module du simulateur, et deux stratégies d'adaptation de la valeur de la fenêtre de contention (cw). La première stratégie est une adaptation dynamique de la valeur CW en fonction des informations instantanées des paramètres du réseau, la deuxième stratégie permet de diminuer la probabilité de collision et d'augmenter le trafic de données lorsque le réseau est saturé.

Le schéma suivant montre les différentes parties de notre solution, ainsi que les liens entre eux.

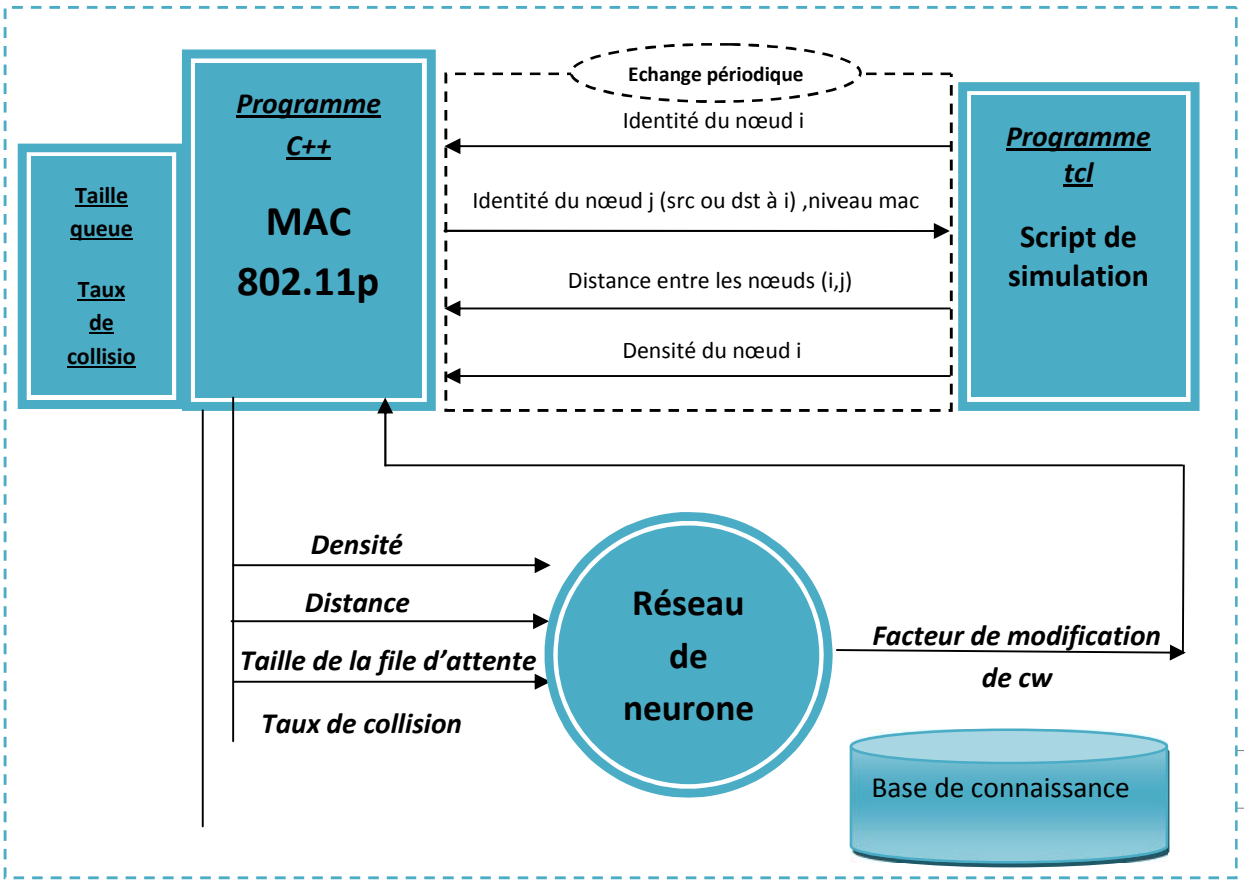


Figure 6-1 L'échange d'informations entre les différents modules du système

❖ Méthode formelle

La contribution principale de ce travail consiste en une méthode formelle qui adapte l'intervalle de la fenêtre de contention pour réduire les collisions et les congestions tout en garantissant la qualité de service et réduire les délais d'attente supplémentaires. Cette nouvelle technique pour estimer le niveau de congestion dans le réseau est basée sur les réseaux de neurones comme modèle d'estimation de la probabilité de transmission. Chaque nœud possède son propre réseau de neurones qui s'exécute en arrière plan et de manière périodique. Ce modèle est en interaction permanente avec l'instance MAC 802.11p du nœud par le biais des entrées et des sorties du réseau de neurone.

❖ Le choix des paramètres

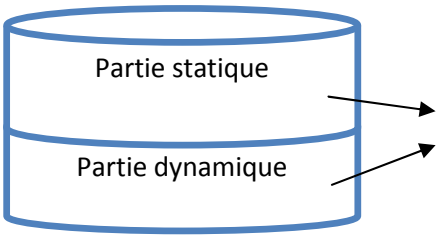
Nous proposons un mécanisme adaptatif de l'algorithme back-off basé sur plusieurs facteurs qui influencent la probabilité de collision. Le premier facteur est le nombre de stations actives. Il joue un rôle important dans la sélection de la valeur optimale de la fenêtre de contention. Le deuxième facteur est la longueur de la file d'attente du nœud qui est une information localement disponible au niveau du nœud. Il est capable de refléter l'état de congestion au niveau du nœud. Le troisième facteur est le taux de collision. Il est calculé périodiquement par le nœud. Plusieurs recherches utilisent ce paramètre pour l'adaptation. Leurs résultats montrent une meilleure performance par rapport à la solution statique. Le dernier facteur utilisé est la distance entre l'émetteur et le récepteur. Ce paramètre n'a pas été utilisé auparavant pour l'adaptation des paramètres du réseau, pourtant il influence fortement la probabilité de collision. En effet, si la distance séparant l'émetteur du récepteur est grande, la probabilité des collisions augmente car le signal s'atténue avec la distance. En plus la distance peut être facilement estimée à partir de la puissance reçue du dernier message. Outre, la probabilité d'avoir des nœuds intermédiaires entre l'émetteur et le récepteur augmente avec l'augmentation de la distance.

Le but de l'utilisation de plusieurs paramètres dans notre travail est d'augmenter la fiabilité sur l'état du canal. Cependant, la densité et le taux de collision ayant une grande importance sur l'adaptation peuvent être des informations moins sûr, ou anciennes. Du fait, il est possible en utilisant les réseaux de neurones d'attribuer des priorités à ces paramètres en fonction de l'ancienneté et de la disponibilité de l'information, ainsi que leurs impacts sur la probabilité de collision. Cette priorité est assurée en utilisant les poids des paramètres, en fonction de leurs positions, et en fonction de la base d'apprentissage choisie ; ces facteurs sont classés du plus prioritaire au moins prioritaire.

❖ La base de connaissance ou d'apprentissage

La base de connaissance est initialisée de manière intuitive et après plusieurs tests afin de choisir les bonnes valeurs vu qu'elle influence directement sur les performances du réseau.

Cette base de connaissance est limitée à cause de la limitation de la machine pour avoir un temps d'exécution acceptable. Chaque exemple de cette base est constitué du vecteur d'entrée et du vecteur de sortie approprié. Elle se divise en deux parties : une partie statique initialisée au départ, et une partie dynamique modifiée régulièrement dans le cas où les valeurs d'entrée et de sortie arrivent à diminuer considérablement le taux de collisions.



L'entrée désirée				Sortie désiée
Densité	**Taille queue**	**Taux de collision**	**Distance**	**Sortie**

Figure 6-2 Le format de la base d'apprentissage

❖ Algorithme d'invocation du réseau de neurones

L'algorithme d'invocation du réseau de neurone (RDN) s'exécute périodiquement au niveau du nœud. Il met à jour les valeurs d'entrée du RDN qu'il récupère à partir de l'instance MAC. Il vérifie la différence entre le taux de collision ancien et le nouveau, si elle est importante, il met à jour la base de connaissance, puis il lance le réseau de neurones. Il récupère ensuite la valeur de sortie et il l'envoie à l'instance mac. L'algorithme suivant résume ces étapes.

Algorithme périodique d'invocation du réseau de neurone pour le nœud i

Début

Ligne_ancienne = (d,q,col,dis,sortie)

- Calculer la densité **d**
- Calculer la distance **dis** entre l'émetteur i et le récepteur j ou le contraire
- Calculer la taille **q** de la file d'attente du nœud i
- Enregistrer le taux de collision **col**

Si (taux_collisi_nouveau - taux_collisi_ancien > seuil1)

début

Ajouter **Ligne_ancienne** à la base de connaissance à la place de la ligne la plus ancienne , puis initialisation à 0

Fsi

- Appeler réseau de neurone **RDN(d,dis,q,col)**
- Envoyer la sortie du RDN à l'instance MAC802.11p

Fin

Dans la prochaine section, nous allons détailler notre perceptron multi couches et les bases mathématiques utilisées dans ce modèle.

4.1. L'utilisation du Réseau de neurones

Nous utilisons dans cette section les références suivantes: (Stricker, 2000) (TOUZET, 1992) (MAIDI, TEMGLIT, & ACHOUR, 2001), pour présenter la constitution et les définitions des éléments du réseau de neurones. (Boix & Mecklenbräuker, 2008)

Les réseaux multicouches sont aujourd'hui les modèles les plus employés. Ils permettent une approximation de n'importe quelle fonction par une combinaison linéaire de fonctions d'activation (sigmoïde, tangente hyperbolique ou fonction de Heaviside). Ainsi chaque neurone est doté de cette fonction et chaque lien entre les neurones est pondéré suivant le problème à résoudre). Ils sont autant capables de résoudre le cas du "ou exclusif" (cf Perceptron). Les différentes couches de traitement permettent de réaliser des associations non linéaires entre l'entrée et la sortie.

La propriété d'approximation universelle a été démontrée par Cybenko en 1989 et Funahashi, en 1989 et peut s'énoncer de la façon suivante (Stricker, 2000) :

Toute fonction bornée suffisamment régulière peut être approchée uniformément, avec une précision arbitraire, dans un domaine fini de l'espace de ses variables, par un réseau de neurones comportant une couche de neurones cachés en nombre fini, possédant tous la même fonction d'activation, et un neurone de sortie linéaire.

Cette propriété justifie l'utilisation de l'architecture présentée précédemment. Comme le montre ce théorème, le nombre de neurones cachées doit être choisi convenablement pour obtenir la précision voulue. (Stricker, 2000)

- **Architecture**

L'architecture de notre réseau de neurone multi couches est montré dans la figure 3 où xi désigne l'entrée du réseau et yj désigne la sortie du réseau. Elle comporte trois couches :

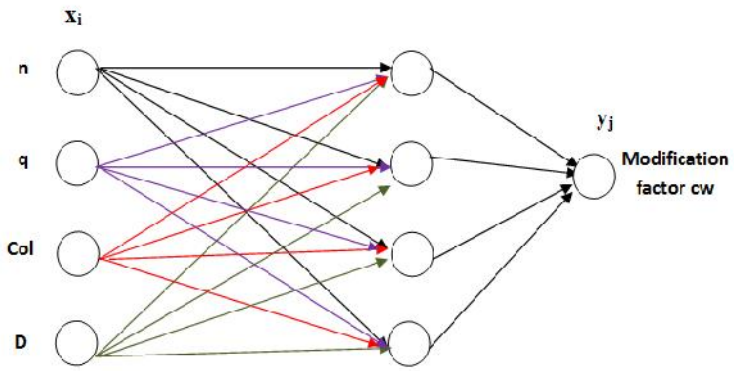


Figure 6-3 L'architecture du réseau de neurones.

- Une couche d'entrée qui reçoit les informations provenant de l'instance MAC 802.11p. Elle se compose des quatre paramètres issus du protocole Mac 802.11p (densité, longueur de la queue, le taux de collision, et la distance). Ils influencent le choix de la valeur optimale de la fenêtre de contention. Chaque neurone de cette couche se contente de transmettre un paramètre sans faire de traitement.

- Une couche intermédiaire, (ou couche cachée), l'information de la couche d'entrée est traitée par la couche cachée. L'utilité de cette couche est d'augmenter la puissance de calcul ainsi que la précision de l'estimation. Après plusieurs tests, le nombre de neurones de cette couche a été fixé à 4 car cette configuration fourni un bon compromis entre la précision et les performances du système.

- Une couche de sortie, le taux de modification de la fenêtre de contention ou probabilité de collision est utilisé comme la seule unité de cette couche.

- **Le fonctionnement des neurones**

Chaque neurone de la couche cachée et de la couche de sortie forme une somme pondérée de l'entrée de la couche précédente à laquelle il est directement connecté. La valeur de sortie est une simple fonction non linéaire de cette somme (voir la figure suivante).

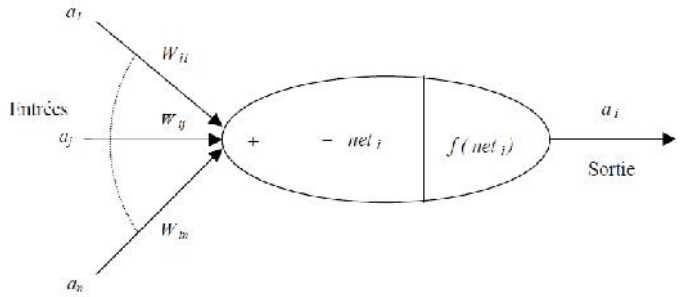


Figure 4.1 Fonctionnement du réseau de neurone.

Cette valeur est calculée à partir de l'équation suivante :

$$Y_j^{\,p} = f\left(\sum_i Wij\ xj^p\right) \qquad (1)$$

où, Wij est le poids positif ou négatif reliant le neurone i au neurone j, P représente le numéro de l'itération. f est la fonction d'activation qui est une fonction sigmoïde. Elle est décrite par l'équation suivante :

$$f(x) = \frac{1}{1+e^{-x}} \qquad (2)$$

En raison de la restriction de la fonction sigmoïde, les valeurs d'entée et de sortie doivent être comprise entre 0 et 1, ainsi ces paramètres sont normalisées.

$$n = \frac{\text{number of station}}{\text{n\_ max}} \qquad (3)$$

$$col = \frac{\text{collision rate}}{\text{max collision rate}} \qquad (4)$$

$$q = \frac{\text{queue length}}{\text{max queue length}} \qquad (5)$$

$$d = \frac{\text{distance}}{\text{transmission range}} \qquad (6)$$

Où, n_max and max collision rate sont fixés par la simulation dans un scenario très dense. La valeur de sortie étant une probabilité, elle est comprise entre 0 et 1.

- **L'apprentissage**

L'algorithme d'apprentissage utilisé dans ce travail est un algorithme de rétro-propagation. Il s'agit d'un algorithme itératif de gradient, son but est de minimiser l'erreur quadratique moyenne entre la sortie réelle du réseau qui est calculée par propagation et une réponse désirée. Cette minimisation est réalisée par une configuration appropriée des poids. D'ailleurs le but d'apprentissage est d'ajuster les coefficients du modèle de telle manière que les sorties calculées soient aussi proches que possible des sorties désirées.

« Des recherches bibliographiques ont montré que la rétropropagation s'agit en fait d'une redécouverte. Son principe est la minimisation d'une fonction dépendante de l'erreur. En effet, l'algorithme consiste à considérer l'apprentissage comme la recherche sur la surface de coût de la position de coût minimal. A chaque configuration de poids correspond un coût. Le gradient est une estimation locale de la pente de la surface. La minimisation du gradient permet de parcourir cette surface orthogonalement aux courbes de niveau d'un pas fixé. »

Dans notre cas, il s'agit d'un problème de classification supervisée, il s'agit de déterminer une surface de séparation entre 3 classes : faible congestion, forte congestion, et congestion moyenne.

Afin d'obtenir le vecteur de sortie correct quel que soit l'exemple présenté, il est nécessaire de définir cette fonction d'erreur (on choisit en général l'erreur quadratique moyenne). Cette fonction est :

$$E = 1/N \sum_{i \in S} (di - ai)^2 \qquad (7)$$

Où di est la valeur désirée, ai est la valeur de sortie, et N est le nombre d'éléments dans la base d'apprentissage.

Le processus de calcul de la sortie est répété jusqu'à l'obtention de toutes les valeurs de sortie de toutes les couches. Lorsque l'erreur de tous les neurones est déterminée, l'algorithme retrace le chemin inverse. Les valeurs d'erreur sont propagées vers l'arrière pour ajuster ces poids (voir la figure).

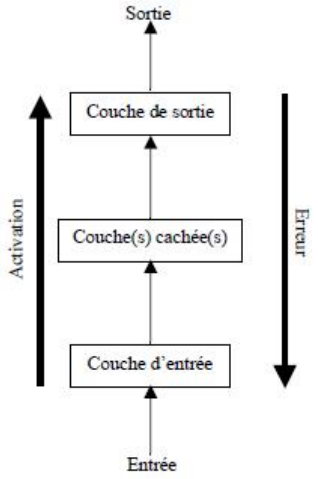


Figure 4.1 Calcul de sorties et retro-propagation.

L'équation de mise à jour des poids est la règle delta (ou Widrow et Hoff règle), elle calculé comme suit :

$$\Delta wij = -\eta \frac{\partial E}{\partial Wij} \qquad (8)$$

Où, E est la fonction d'erreur, η : est l'itération d'apprentissage. Wij est le poids synaptique reliant le neurone i au neurone j de la couche précédente.
L'apprentissage est effectué jusqu'à ce que l'erreur entre la sortie calculée et la valeur désirée est acceptable, il faut trouver un bon compromis entre l'erreur et le temps d'exécution. Pour cela un seuil d'erreur et définit et ajusté par des tests. L'algorithme suivant résume ces étapes.

Algorithme 1

Étape 1: Initialiser les poids avec des valeurs aléatoires entre -0,5 et 0,5.

Etape 2: introduire les paramètres d'entrée du nœud à partir de l'instance mac 802.1p et injecter le vecteur dans la couche d'entrée du réseau.

Étape 3: Calculer les sorties de chaque couche en utilisant la propagation.

Etape 4: Comparaison de la sortie calculée à la sortie désirée, et déterminer l'erreur.

Etape 5: rétro-propagation de l'erreur de la sortie à l'entrée du réseau.

Étape 6: Mise à jour des poids: soit en augmentant ou en diminuant leurs valeurs,

Etape 7: Si l'erreur entre la sortie obtenue et la valeur de sortie désirée est acceptable, alors fin de l'apprentissage, sinon, répéter le processus de 3 à 7.

Étape 8: Enregistrer l'état final du réseau de neurones qui représentent le taux de modification de cw.

L'algorithme d'apprentissage est simple à implanter, mais un certain savoir-faire est nécessaire pour une utilisation efficace.

En effet, de multiples variables sont à ajuster précisément en fonction du problème traité. Parmi ces variables à fixer,

- les paramètres apparaissants dans les différentes équations (gain de la procédure de gradient (μ), pente de la fonction sigmoïde (Ò), ..),
- la sélection des exemples pour l'apprentissage et le test,
- l'ordre de présentation et les distributions relatives des exemples dans la base d'apprentissage,
- le choix du codage des informations en entrée et en sortie, la structure du réseau
- limitation pratique du nombre de couches,
- taille de la couche cachée,
- configuration initiale des poids,
- le nombre d'itérations d'apprentissage, ...

4.2. Adaptation dynamique de la fenêtre de contention

Dans cette partie, nous proposons un nouvel algorithme d'adaptation dynamique de la fenêtre de contention (CW) qui a pour but d'augmenter la probabilité de réception d'une transmission.

Notre solution consiste en l'augmentation et la diminution automatique de l'intervalle de la fenêtre de contention CW. Il n'est pas nécessaire d'attendre la dégradation du réseau pour faire quelque chose. La taille de la fenêtre de contention utilisée par chaque station est en fonction de la probabilité de collision. Comme nous avons précédemment discuté, cette probabilité regroupe plusieurs paramètres typiques qui influencent sur le choix de cette valeur.

Contrairement aux approches existantes, notre approche se base non pas sur un seul paramètre, mais regroupe plusieurs paramètres. Chaque paramètre est doté par une priorité qui change au fur et à mesure. Nous accordons une grande priorité à un paramètre qui a une forte influence sur la fenêtre de contention et les performances du réseau et dont sa valeur est récente et plus sûre.

Notre mécanisme appelé Neural Network based Adaptive Contention Window NN-ACW consiste à modifier quelques concepts ; ces derniers se résument en une translation de l'intervalle de sélection de la valeur de la fenêtre de contention selon l'état du réseau.

L'intervalle de sélection devient [cw inf ;cwsup] au lieu de [0, cw] come le montre la figure suivante , si un nœud constate une collision, il faut au moins s'assurer que la nouvelle valeur de cw soit supérieure à la valeur actuelle.

Algorithm : backoff window updating mechanism for vehicle v_i

$T_i = \theta_i * cw$

if ($\theta_i <$ **threshold**$_{1)}$ **backoff range = [0, (1-** θ_i**)*cw]**

else if ($\theta_i >$ **threshold**$_{2)}$ **backoff range = [**T_i**, cw*2+** T_i**]**

else if ($\theta_i >$ **threshold3**$_{)}$ **backoff range = [0, cw +** T_i**]**

else if backoff range = [0, cw]

0	cw-1	Cas 1 : Forte contention
0	cw-1	Cas 2 : Contention moyenne
0	cw-1	Cas 3 : Faible contention

Figure 4.16 Nouveaux intervalles de la fenêtre de contention.

L'utilisation de plusieurs paramètres peut diminuer la probabilité de collision, car dans un même voisinage, si on se base seulement sur la densité, les nœuds tendent à choisir une valeur de cw dans une même plage, or que notre but est de distinguer entre les intervalles de sélection afin de diminuer la probabilité qu'une même collision se reproduise. Si on se base seulement sur la densité, les nœuds voisins vont utiliser le même intervalle qui sera en plus réduit comme le font plusieurs travaux existants. Cela ne diminue pas la probabilité de collision, pour cette raison, nous avons choisi d'utiliser la distance et la densité afin de

représenter l'environnement du réseau, et la taille de la file et le taux de collision pour représenter l'état du trafic au niveau du nœud.

En fonction de la valeur calculée de la probabilité de collision, nous modifions l'intervalle de sélection de CW comme le montre l'algorithme suivant

Il existe 4 cas, lorsque la contention est très faible, le nœud sélectionne une petite valeur tout en gardant l'aspect aléatoire. Du coup, on élimine les retard supplémentaire en choisissant une grande valeur. Lorsque la contention est très importante ou le réseau est saturé ou presque, le nœud sélectionne une grande valeur sans diminuer la taille de l'intervalle défini par le standar mais en excluant les valeurs proche de 0. Nous attribuont moin de priorité à cette communication, car elle a une grande chance de produire une collision. Vu que le trafic est important dans le réseau, d'autre communications aurons lieu.

Lorsque la contention est moyenne vers importante, le nœud sélectionne une valeur aléatoire mais en augmentant juste l'intervalle de sélection. Dans ce cas, on n'exclut pas les valeurs petites, mais on augmente la probabilité de choisir une grande valeur. Le dernier cas est lorsque le trafic est moyen, nous laissons l'intervalle tel qu'il est défini par la norme.

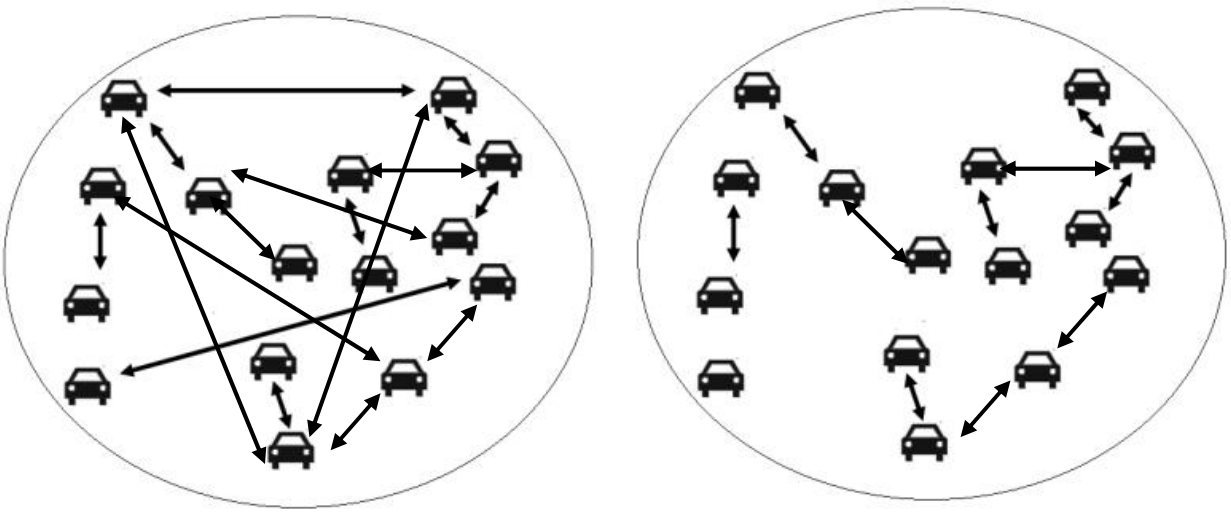
Les nouvelles bornes de la fenêtre de contention ne sont pas sauvegardées. C'est-à-dire que la valeur de la fenêtre de contention ne ne change que s'il y a une collision, elle est doublée et bornée par CW max. Apres une transmission avec succès, elle est initialisée à CWmin. Notre algorithme intéragit juste au moment de la selection.

Le mécanisme NN-ACW a plusieurs avantages: il est adapté lorsque la charge de trafic augmente en raison de l'augmentation des collisions. Il est approprié pour les deux communications V2V et V2I.

En utilisant la densité, le taux de collision, la longueur de queue, et la distance pour régler la fenêtre de collision, le réseau peut maintenir sa stabilité.

4.3. Adaptation du trafic dans des conditions de saturation du réseau

La nature des réseaux de véhicules avec des changements fréquents crée une topologie très dynamique et peut entraîner une dégradation des performances du réseau si le protocole n'est pas conçu pour gérer de telles situations. Pour cette raison, et afin d'assurer l'évolutivité et la scalabilité, un mécanisme supplémentaire pour gérer le réseau lorsque le niveau de congestion est élevé est nécessaire. D'où, l'intérêt de notre seconde contribution. Elle consiste à gérer le réseau quand il est saturé. Nous utilisons la sotie du réseau de neurones comme indicateur de congestion. Si le nœud constate que ce paramètre dépasse un certain seuil, il retarde certaines communications en se basant sur la distance, qui peut être estimée à partir de la puissance d'émission. La valeur de la fenêtre de contention est doublée si la distance entre la source et la destination est grande. Nous attribuons plus de priorité aux communications de courte à moyenne distance entre la source et la destination, car la probabilité de réception diminue avec l'augmentation de la distance, ce qui peut entraîner des collisions.



(a) (b)

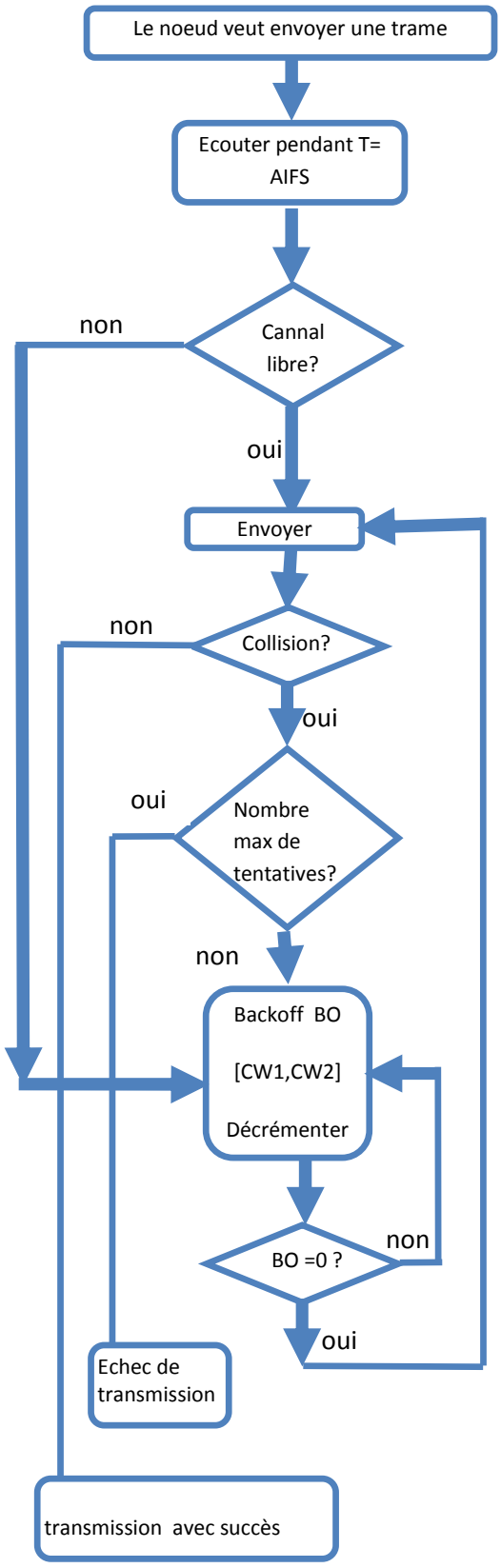
Figure 6-7 (a) : Exemple de trafic, (b) : les communications ayant plus de priorité.

Dans cette proposition, il n'est pas nécessaire d'échanger des messages de contrôle entre les nœuds. Toutefois, en se basant sur la distance, le message peut ne pas arriver en intégrité. Cela rend notre proposition plus approprié pour des messages non critiques plutôt que pour des messages critiques pour deux raisons. La première est qu'un message critique est plus sensible à la collision par sa taille généralement petite. La deuxième raison est que, généralement un message non critique qui peut être soit video ou son n'est pas aussi sensible aux collisions, et son contenu peut être lisible même s'il ya quelques pertes.

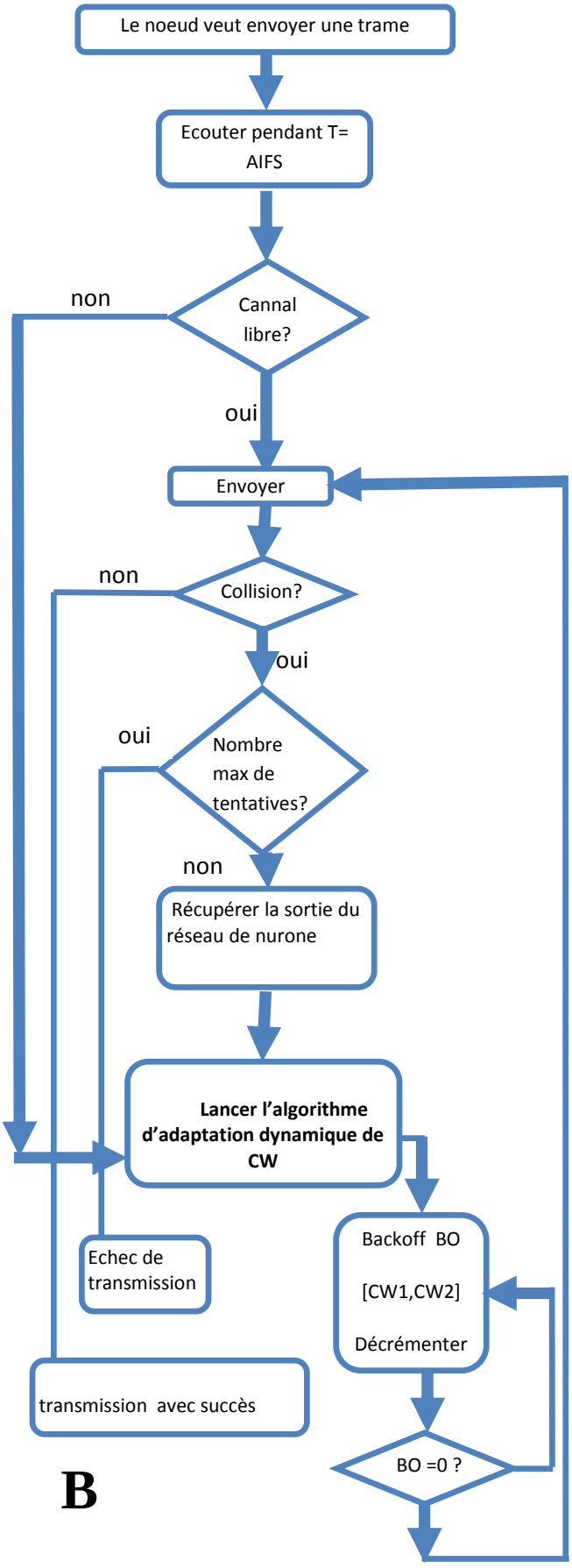
En outre, tous les nœuds n'ont pas les mêmes chances de transmettre leurs données, mais le plus important est d'améliorer les performances du réseau en réduisant les collisions et les retards et en augmentant le débit. En plus, la norme 802.11p basée sur la sélection aléatoire ne garantit pas le partage équitable du medium.

5. L'organigramme

L'organigramme suivant montre la différance entre le mécanisme CSMA défini par le standard (le schéma A), et la version modifiée du CSMA proposée dans ce travail (le schéma B).


Le noeud veut envoyer une trame
Ecouter pendant T= AIFS
Cannal libre?
non
oui
Envoyer
Collision?
non
oui
Nombre max de tentatives?
oui
non
Backoff BO
[CW1,CW2]
Décrémenter
BO =0 ?
non
oui
Echec de transmission
transmission avec succès

A


Le noeud veut envoyer une trame
Ecouter pendant T= AIFS
Cannal libre?
non
oui
Envoyer
Collision?
non
oui
Nombre max de tentatives?
oui
non
Récupérer la sortie du réseau de nurone
Lancer l'algorithme d'adaptation dynamique de CW
Echec de transmission
Backoff BO
[CW1,CW2]
Décrémenter
transmission avec succès
BO =0 ?

B

6. Adaptation au mode WAVE et faisabilité de la solution

Notre solution a été conçue essentiellement pour le mode WAVE. Sachons qu'il existe sept canaux différents dont un est un canal de contrôle et les six autres sont des canaux de service.

L'intervalle de synchronisation de 100ms est divisé en deux sous intervalles : un sous intervalle CCH dans lequel le nœud échange les messages de sécurité et de contrôle via le canal de contrôle CCH, et un autre intervalle de service pour échanger les messages non critiques sur un canal de service.

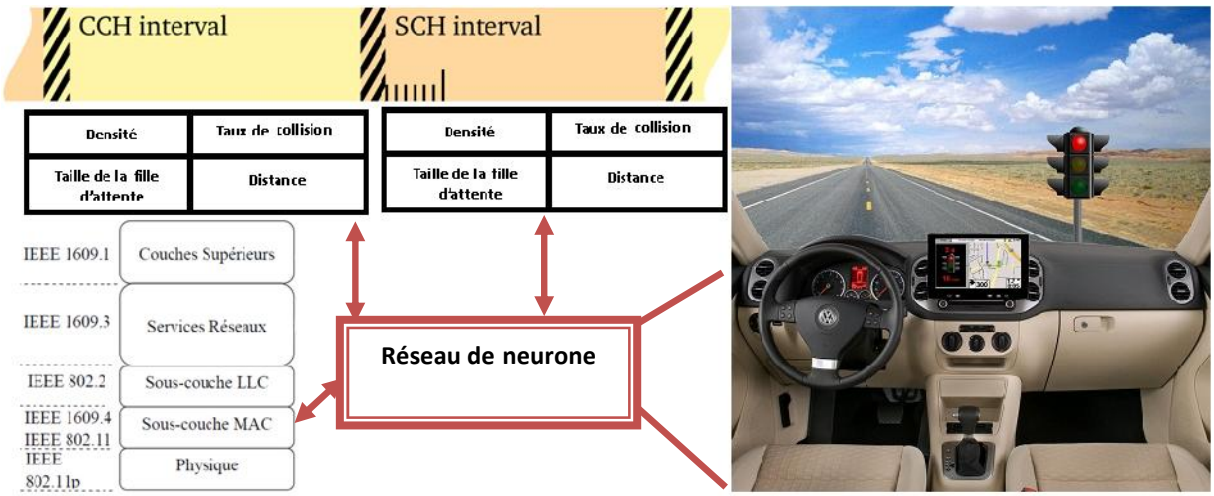


Figure 6-8 Adaptation au mode WAVE.

Les quatre paramètres indicateurs diffèrent dans la manière et les périodes de leurs calculs. Dans cette section, nous allons discuter et montrer la faisabilité et les différents changements appliqués à nos idées en mode WAVE.

Densité : Il existe plusieurs méthodes pour l'estimer. L'utilisation des messages beacon s'avère nécessaire pour plusieurs applications notamment dans le routage et la dissémination de l'information. Il est plus intéressant d'estimer ce paramètre en utilisant les informations localement disponibles comme la vitesse et le temps d'arrêt des véhicules comme abordé dans (Artimy, 2007) et (Shirani & Hendessi, 2009). Cela augmentera le trafic des données.

On s'attend dans un futur proche que les véhicules de demain aient accès au GPS et peuvent se localiser. Le réseau routier ne cesse de se développer. Il est possible d'imaginer qu'un véhicule peut savoir la nature du segment de route à tout instant. D'où la vitesse est un indice significatif dans une autoroute alors que dans une route urbaine, la vitesse étant limitée, il est difficile d'estimer la densité. Cependant, l'infrastructure dans la ville est bien présente, elle peut diffuser périodiquement la densité au niveau d'une intersection par exemple. Il résulte par cela que cette information peut être facilement disponible lorsque le réseau véhiculaire sera déployé.

Le Taux de collision est estimé par le nœud en se basant sur les messages ACK. Cependant, il existe plusieurs problèmes là-dessus. Il y a des applications qui n'utilisent pas les ACK. En

plus, le nœud, lorsqu'il est entrain d'envoyer, ne peut pas recevoir en même temps. Pour cela, nous pouvons suggérer d'utiliser deux antennes sur la même fréquence pour pouvoir écouter et envoyer en même temps, vu que ces dispositifs ne sont pas chers. La valeur du taux de collision calculée périodiquement et indépendamment sur chaque canal CCH et SCH est plus exacte pendant l'intervalle CCH que pendant l'intervalle SCH car pendant l'intervalle SCH, le nœud peut commuter entre plusieurs canaux SCH, d'où il est difficile d'estimer le taux d'erreur d'un canal. Dans ce cas là, il est plus intéressant d'utiliser le taux d'occupation du canal et de proposer un service dans un canal où la charge est moins importante.

Il résulte que ce paramètre n'est pas exact, nous attribuons moins de priorité à ce paramètre pendant l'intervalle de service SCH, et lorsque les messages ACK ne sont pas utilisés. Le test de mise à jour de la base de connaissance ne sera pas fait dans ces deux cas là.

La Taille de la file d'attente une information exacte et disponible. Il ya 4 files d'attente correspondante à quatre catégories d'accès. Pendant chaque intervalle SCH ou CCH, nous considérons que les files d'attente des catégories dédiées à cet intervalle là.

La Distance est estimée à partir de la puissance de réception du dernier message reçu. Vue la mobilité élevée et selon la longueur du message, cette information peut ne pas être exacte, mais sa valeur reste significative, car il est possible de savoir si le véhicule source s'approche ou s'éloigne de la destination ; il est préférable de favoriser le premier cas (lorsqu'ils s'approchent) pour augmenter la chance d'avoir moins de perte de données et un échange de messages sans collisions (cas idéaliste). Dans la littérature, il existe plusieurs formules pour avoir la distance séparant la source et la destination en fonction de la puissance reçue. Par exemple, la formule utilisée dans (Dib & Stancil, 2009) est :

$$D = \frac{\lambda \sqrt{G \cdot Pt}}{4\pi \sqrt{Pr}}$$

Où, Pt est la puissance d'émission du signal, Pr est la puissance de réception du signal, λ est la longueur d'ondes du signal transmis.

7. Conclusion

Nous avons proposé dans ce chapitre notre contribution. La solution proposée se compose de deux parties, un modèle mathématique permettant d'estimer le niveau de congestion au près du nœud et un nouveau mécanisme de backoff adapté à l'environnement. Notre proposition suit le même principe que les travaux antécédents mais elle diffère dans la manière d'estimer le niveau de congestion et la stratégie choisie.

Notre mécanisme nécessite peu de modifications dans le standard mac. Il permet facilement le passage à l'échange. L'évaluation de ses performances fait l'objet du chapitre suivant. Nous utilisons pour cela le simulateur ns2.

réservation de slot pendant les intervalles CRP et SCH ne sont pas expliqués, et les simulations réalisées sont basées sur des scénarios limités et simples. L'approche proposée a donc quelques inconvénients (Booysen, Zeadally, & Rooyen, 2011) :

- En effet, le fait de rendre l'intervalle ABF plus petit n'a pas vraiment de sens, puisqu'il libère une largeur de bande inutilisée.
- Malheureusement ce temps est utilisé seulement dans la négociation et la période de coordination (CRP) au lieu qu'il soit utilisé dans la période de NSAF.
- Le nombre de slots pendant NSAF est fixe, ceci mènera à une sous- utilisation dans le cas d'une charge de circulation dense.
- Les auteurs de cette approche ne discutent pas ce qui se produit si un nœud sort de la gamme, et comment le slot assigné sera libéré.
- Si tous les nœuds réapproprient les slots au début de l'intervalle ABF, les nouveaux nœuds n'auront pas de slots disponibles.

15. Synthèse sur les protocoles MAC dans VANET

Le protocole MAC est le noyau de partage du medium sans fil avec une largeur de bande limitée et un environnement fortement dynamique. Nous avons présenté dans les trois chapitres précédents, un aperçu sur de diverses approches MAC qui ont été proposées dans la littérature pour permettre le partage efficace du medium sans fil pour les réseaux véhiculaires. Aucune solution proposée n'est parfaite, chacune possède des avantages ainsi que des inconvénients et parfois des scénarios spécifiques adaptés. Un des avantages des approches d'accès aléatoires et des méthodes basées sur la contention est qu'elles nécessitent peu de coordination. Ces méthodes sont donc plus robustes aux changements de configuration de réseau et elles ont des overheads plus petits par rapport aux méthodes basées free-contention. Cependant, les performances de ces méthodes se détériorent de manière significative lorsque le trafic est important car les collisions augmentent avec l'augmentation de la charge de circulation des messages. En plus, n'importe quelle méthode basée sur la contention peut également engendrer des retards illimités dans les délais d'accès au medium.
Par contre, les méthodes free-contention sont avantagées car elles peuvent garantir la qualité de service (QoS), et leurs performances sont meilleures lorsque le trafic est important. Cependant, elles exigent plus de coordination pour l'attribution et l'allocation du support, particulièrement lors des changements rapides dans la configuration de réseau. (Booysen, Zeadally, & Rooyen, 2011) Il a été démontré et largement accepté que les méthodes MAC contention-free permettent une meilleure utilisation du canal et elles sont plus fiables que la méthode CSMA**.** (Booysen, Zeadally, & Rooyen, 2011)

Critères / Catégorie	Coordination	Overheads	Trafic chargé	Temps d'accès	QoS	Fiabilité	Adéquats? pour VANETS
Les protocoles basés-contention	nécessitent peu de coordination donc plus robustes	Peu	Dégradation des performances dans un trafic chargé (à cause de l'augmentation de collisions)	peuvent faire face à des retards illimités dans les délais d'accès au medium.	Qualité de service n'est pas garantie	Faible	OUI Car le Nombre de nœuds imprévisible
Les protocoles free-contention	Exigent plus de coordination pour l'attribution et l'allocation du support	Beaucoup	Meilleures performances dans le cas où le trafic est chargé.	L'accès au canal est garanti pour un réseau statique	Qualité de service garantie pour réseau satique	Elevée	NON Difficulté de coordination car : mobilité, vitesse, nombre de nœuds, V2V

Tableau 2-3 Tableau comparatif des protocoles non basés et basés contention

Bien que le protocole Cluster-Based Multichannel MAC (CBMMAC) soit soigneusement fait, il a également quelques insuffisances : le système est exclusivement conçu pour le trafic d'autoroute, en effet, ce protocole est désigné lorsque la densité de la route est élevée pour permettre les communications inter-cluster. L'approche dépend intensément (Booysen, Zeadally, & Rooyen, 2011) du véhicule cluster-head, et de la coordination dans le cluster. Ce protocole est bien efficace lorsque la mobilité est relativement faible pour permettre la coordination, et les échanges de messages. Un avantage principal d'employer des clusters est l'utilisation des sept canaux dans un cluster, ceci mènera à l'utilisation élevée du canal, mais seulement lorsque les groupes ne se chevauchent pas et ne sont pas près les uns des autres, car les collisions augmentent lorsque les groupes sont à proximité. Chaque véhicule maintient deux radios et le GPS (beaucoup de ressources pour communiquer). (Booysen, Zeadally, & Rooyen, 2011)

La méthode STDMA qui a été développée pour des bas débits est utilisée seulement pour annoncer les positions des nœuds. Cette solution n'est pas adéquate pour transmettre des données volumineuses comme des vidéos (multimédia en général), car elle utilise la méthode TDMA dans laquelle un slot est gaspillé à chaque fois que le nœud n'a pas besoin de transmettre des données. Par contre, elle est plus appropriée pour le trafic des autoroutes que pour un trafic urbain car les changements de vitesse et de direction entre les véhicules sont moins fréquents. (Booysen, Zeadally, & Rooyen, 2011)

L'approche VeSOMAC, basée sur un vecteur binaire permet d'être mis en application avec ou sans la synchronisation. Bien que dans la version asynchrone, l'efficacité du vecteur Bitmap est légèrement

réduite à cause de la contrainte qu'un bit représente l'occupation de deux slots au lieu d'un seul ; dans le cas synchrone, cet inconvénient n'existe pas. *Le VeSOMAC* asynchrone est efficace pour des déploiements distribués sans besoin de synchronisation à travers le réseau. Cette approche a quelques imperfections, en effet, le système est conçu et évalué seulement pour des scénarios d'autoroute. Il est très probable que les performances du système se dégradent de manière significative dans des environnements urbains avec de nombreux véhicules roulant dans plusieurs directions. Le papier rapporte un retard de livraison plus long que celui de IEEE 802.11p à cause des horloges relatives dans chaque véhicule. Il existe également une perte de temps significative dans le système, puisque chaque nœud doit occuper un slot, même s'il n'a aucune donnée à transmettre. En plus, la taille de la trame en étant un paramètre de conception, ne permet pas un nombre très élevé de véhicules dans un groupe. La trame devrait donc être conçue pour une capacité maximale à tout moment, menant à la sous utilisation seulement si quelques nœuds sont présents. En outre, dans cette solution, il n'y a aucune disposition pour utiliser les canaux multiples assignés par la FCC. (Yu & Biswas, 2007) (Booysen, Zeadally, & Rooyen, 2011)
Donc, cette solution doit être modifiée, il est possible de combiner entre cette approche et celle des clusters par exemple, en effet, on peut garder le principe du vecteur Bitmap à l'intérieur d'un groupe car le nombre de nœuds est limité dans un groupe à un moment donné, et utiliser le principe du WAVE 802.11p pour les communications intra groupe.

Bien que le protocole multi canal token-ring nous semble efficace, la topologie d'anneau qui est formée par les nœuds chefs rend le système fortement dépendant de ces nœuds. Si le nœud chef d'anneau quitte l'anneau, il faudra réinitialiser l'association d'anneaux, Ceci rend ce schéma plus adapté aux scénarios où il existe une tendance de mobilité en groupe, plutôt qu'une mobilité imprévisible. (Booysen, Zeadally, & Rooyen, 2011) (Bi, Liu, & Shen, 2008)
La topologie d'anneaux est également assez statique puisque la taille de l'anneau est fixe.
Etant donnés la topologie d'anneau, la taille fixe, et le seuil de la vitesse des nœuds, il est probable que beaucoup de nœuds ne peuvent pas joindre les anneaux. Le système se base sur la connectivité entre tous les nœuds dans l'anneau, puisque le jeton doit circuler entre les nœuds ; et le nœud chef doit rendre compte de toutes les interactions. Ce scénario est idéal et non probable en raison de la mobilité élevée des véhicules.
MCTRP emploie CSMA / CA pour des messages critiques et TDMA tokenpassing pour les transferts de données. Ceci mène à un scénario où les messages critiques pourraient faire face à des retards illimités sous une lourde charge du réseau.
MCTRP dépend de deux radios par véhicule et tous les slots de transmission sont employés quoiqu'un nœud peut ne pas transmettre. (Bi, Liu, & Shen, 2008) (Booysen, Zeadally, & Rooyen, 2011)
L'efficacité du protocole MAC EDCA actuellement utilisé pour WAVE afin de réduire le nombre de collisions se base sur **le mécanisme backoff** qui consiste en une large sélection aléatoire des périodes de backoff afin d'écarter les retransmissions dans le temps. De ce fait réduire la probabilité que les mêmes trames produisent de nouvelles collisions. Ce protocole permet de donner des possibilités en matière de qualité de service. Les modifications introduites au niveau de la couche MAC assurent un traitement spécifique pour chaque type de trafic.
Les recherches et les simulations réalisées prouvent que cette différenciation garantit une meilleure transmission de la voix et de la vidéo. Mais plusieurs problèmes se posent, à savoir la dégradation des trafics à faible priorité. En effet, au moment où seulement un trafic best effort circule, sa transmission avec une faible priorité engendre un temps d'attente supplémentaire dans la file d'attente. (Huang & Chen, Telematics Communication Technologies and Vehicular Networks: Wireless Architectures and Applications, 2010) (Moustafa & Zhang, 2009) (Nehdi, 2005) En plus, les

messages envoyés sur le canal CCH doivent être traités avec différentes priorités selon l'aspect critique du message. Cependant, EDCA ne traite pas cette condition. En effet, il n'établit pas des priorités strictes, (Barradi, Hafid, & Gallardo, 2010) mais seulement, il avantage relativement quelques types de messages par rapport à d'autres messages (ie il impose seulement une différence dans les services pour les différents types de messages). (Barradi, Hafid, & Gallardo, 2010). Cela soulève d'autres problèmes :

(3) Un message ayant une faible priorité, peut heurter un message plus prioritaire pendant sa transmission, cela cause la perte des deux transmissions, même si le deuxième message est très critique ;
(4) un message de faible priorité peut réussir à accéder au canal et emporter le temps précieux nécessaire pour la transmission des messages prioritaires. (Barradi, Hafid, & Gallardo, 2010)

Un autre problème est que, une fois les messages sont diffusés (broadcasting) sur le canal CCH, il n'y a aucune réponse ; ceci signifie qu'il n'est pas possible de savoir si une transmission est réussie ou pas, or, cette information diminue l'utilisation exponentielle de la technique backoff afin de réduire les congestions. (Barradi, Hafid, & Gallardo, 2010)

En conclusion, La norme IEEE 802.11p devrait aborder plusieurs challenges, tels que les fréquentes déconnexions et le 'handoff'. Il est important de montrer aussi au moins par simulation et analyse, si la norme 802.11p garantit les conditions de fiabilité et le minimum de temps de latence des applications sécuritaires de DSRC pour les réseaux véhiculaires. (Moustafa & Zhang, 2009)
Cette norme ne s'adresse pas d'une manière adéquate aux applications imposées par les réseaux VANET, puisqu'elle emploie une approche basée sur la contention. La qualité de service QoS ne peut pas être garantie pour les messages critiques de sécurité et les transmissions en temps réel. (Booysen, Zeadally, & Rooyen, 2011)
Ce tableau récapitule les principales approches MAC proposées et discutées ci-dessus.

Tableau 4-4 Les approches MAC récemment proposées pour les réseaux VANETs. **(Booysen, Zeadally, & Rooyen, 2011)**

Protocoles / Paramètres	WAVE MAC	STDMA	VeSO-MAC	MCTRP	CBM-MAC	DMMAC
Buts des approches alternatives MAC	Assurer l'interopérabilité entre dispositifs sans fil & mode opératoire pour fonctionner dans DSRC.	Eviter les collisions maritimes	Améliorer les flux de données	Diminuer la latence des messages d'urgence et Augmenter le flux de sortie non temps réel	Garantir la livraison de message de sécurité tout en supportant les données non-critiques	Collision-libre et Délais de livraison avec adaptation de flux de données
Destiné et Simulé pour scénarios d'autoroute	Oui	Partiellement	Oui	Oui	Oui	Oui
Destiné et Simulé pour scénarios Urbains	Oui	Partiellement	Non	Non	Non	Non
Délais liés à la transmission temps-critique	Non	Partiellement	Partiellement	Oui	Oui	Oui
Coordination en temps et indépendance du nœud chef	Oui	Oui	Oui	Non	Non	Oui
Auto-synchronisation (independent du GPS)	Non	Non	Oui	Non	Oui	Non
Conformité à la synchronisation WAVE (intervalle CCH& SCH)	-	Non	Non	Non	Non	Oui
L'attribution de la bande passante adaptée à la demande	Non	Partiellement	Non	Non	Non	Partiellement
Exploitation multi-canal (canaux WAVE)	-	Non	Non	Oui	Oui	Oui
Nombre de radios par véhicule	-	1	1	2	2	1
Complexité (Niveau de coordination et de gestions requises)	Simple	Assez simple	Assez simple	Assez complexe	Assez complexe	Complexe

Dans cette première partie, nous avons présenté les différents protocoles de la couche MAC dédiés ou adaptés pour les réseaux véhiculaires. Nous avons soulevé notre synthèse sur les différentes approches. Reste maintenant le choix de la méthode à améliorer dans ce travail. Est ce que nous optons pour une solution basée: free-contention, basée-contention, ou hybride ?

Ce que nous avons remarqué est que le standard 802.11p est bien installé, et tôt ou tard, il constituera le noyau principal des communications véhiculaires. Il faut proposer donc une solution qui s'intègre facilement au standard existant ; plutôt que de changer l'existant pour notre solution, et le standard 802.11p étant le plus populaire, connait de plus en plus d'intérêt dans plusieurs projets, ainsi que dans la communauté industrielle comme le projet SAE J2945.1 (Stanica, 2011)

Certes, ce standard MAC 802.11p possède beaucoup d'insuffisances pour être déployé et généralisé dans nos routes. C'est ce qui nous a motivé à nous intéresser aux travaux récents qui ont pour but l'amélioration de ce standard.

Dans le tableau suivant, nous avons soulevé la tendance des travaux récents autour de la norme 802.11p et le mode WAVE.

Des travaux récents d'amélioration du standards 802.11p & WAVE	
Axes de recherche (802.11p & WAVE)	**Quelques travaux**
Amélioration de 802.1p & WAVE pour les applications de sécurité et de non-sécurité (confort).	(Amadeo, Campolo, & Molina, 2012)
Amélioration des transmissions des messages beacons pour permettre une collecte rapide et efficace des informations	(Vales-Alonso, Vicente-Carrasco, & Alca, 2011)
Amélioration des stratégies de Transmissions multi sauts & Broadcasting (diffusion) dans la norme 802.11p	(Vinel, Campolo, Petit, & Koucheryavy, 2011)
Modélisation du standard 1609.4 **Synchronisation et mutation entre les canaux WAVE (canal de contrôle et les canaux de service)**	(Wang, Leng, Fu, & Zhan, 2010) (Ameixieira, Matos, Moreira, Cardote, Oliveira, & Sargento, 2011)
La transmission d'accusés de réception pour minimiser les collisions	(Barradi, Hafid, & Gallardo, 2010)
L'étude des priorités entre les différentes catégories d'accès	(Barradi, Hafid, & Gallardo, 2010)
Amélioration de l'algorithme backoff (adaptation dynamique)	(Barbosa, Bessa, Sérgio, Rober, & Jùnior, 2011)

Tableau 4-5 Quelques travaux récents d'amélioration du standards 802.11p & WAVE.

16. Conclusion

Nous avons parcouru dans ce chapitre les principaux protocoles MAC hybrides récemment développés pour les réseaux véhiculaires.

Nous avons terminé ce chapitre et cette première partie par une synthèse où nous avons discuté les approches présentées précédemment et tiré des conclusions.

Chapitre 7: Evaluation des performances

1. Introduction

Dans ce chapitre, nous allons évaluer les performances de nos deux propositions. Pour cela, nous avons implémenté nos deux solutions en utilisant l'environnement de simulation. Nous avons comparé notre solution NN-CWA avec le protocole de base 802.11p défini par le standard. La comparaison est réalisée à travers des résultats de simulation selon plusieurs critères.
Dans un premier temps, nous allons présenter le simulateur choisi, et mettre le point sur l'environnement de simulation. En suite, nous allons présenter les résultats des deux solutions et les interpréter.

2. Le choix du simulateur

Pour évaluer les performances de nos solutions, nous utilisons un simulateur car les tests réels ne sont pas possibles. La simulation s'agit d'utiliser un modèle simplifié du système à l'aide d'un logiciel de simulation adéquat qui représente le comportement du système à évaluer de manière réaliste. Elle permet la visualisation des résultats sous forme de graphes faciles à analyser et à interpréter. Cependant, elle n'est pas une méthode exacte, mais elle permet l'étude du système en variant ses divers paramètres. (Benaidja & Moussaoui, 2010)

Beaucoup de simulateurs de réseaux sans fil ont été développés comme OPNET, OMNET, NS2, J-SIM …etc. Nous choisissons NS2 (The Network Simulator - ns-2) pour implémenter nos solutions parce qu'il est gratuit et contient beaucoup de protocoles dans les différentes couches. Il est extensible puisque il permet facilement d'ajouter de nouveaux protocoles. La norme 802.11e a été développée dans ns2 par smalko (802.11e)**.** D'où peu de changements sont nécessaires pour implémenter la norme 802.11p. Le réseau de neurones proposé est développé en c++ comme un module supplémentaire à NS-2.

Nous n'avons pas combiné nos deux solutions, c'est pour voir l'impact de chacune indépendamment, donc les résultats de simulation correspondent à une solution indépendamment de l'autre.

3. Présentation du simulateur NS2

NS-2 est un logiciel de simulation open source, gratuit, à évènements discrets. Il est développé dans le cadre du projet VINT qui regroupe plusieurs laboratoires de recherche comme AT&T institut de recherche à Berckeley (ACIRI), Xerox PARC et Sun Microsystems.

Ce simulateur est développé en C++ et OTCL, il utilise le langage TCL pour créer des scénarios de simulation.
Il supporte les réseaux sans fil et filaires, avec plusieurs protocoles des différentes couches (Physique, MAC, réseaux, transport … etc.). Par sa possibilité d'extension, NS2 est le simulateur le plus utilisé dans le domaine de recherche pour les tests des nouveaux protocoles proposés. Pour plus d'information sur NS2 ou sur son installation, veuillez consulter (Benaidja & Moussaoui, 2010)

4. Critère de performances

Afin d'évaluer les performances de notre solution, nous avons utilisé les métriques suivantes :

Taux de perte

La perte de paquets affecte directement la qualité de l'application. Elle compromet l'intégrité des données et perturbe le service. Dans le réseau, la perte de paquets peut être causée par la congestion du réseau, qui a comme conséquence des paquets rejetés. Pour évaluer cette métrique, nous utilisons le taux de perte moyen qui est le rapport entre le nombre de paquets de données reçus par les destinations et le nombre de données émies par les sources;

Throughput

Le 'average throughput' ou le flux de sortie moyen ou débit moyen est défini par la quantité de données en bits transmis avec succès par une station après avoir parcouru un temps bien déterminé (le temps nécessaire pour cette transmission). Il décrit l'état du flux de données dans le réseau. Ce paramètre est calculé comme suit :

$$\text{Débit effectif} = (\sum \text{Paquets reçus}) / \text{délais (bits/s)}$$

Délai de bout en bout

Le délai de bout en bout (E2ED) ou la latence est le temps écoulé entre l'envoi d'un paquet par un émetteur et sa réception par le destinateur ; il comporte aussi les temps d'attente et de traitement dûs à la chaine de transmission ;

$$\text{E2ED} = [\text{Temps d'arrivée} - \text{Temps de départ}] \text{ (s)}$$

Délais moyen = Somme des délais E2ED de tous les Paquets / Nombre total des paquets reçus

Nous utilisations la moyenne de ces délais comme indicateur de performance dans notre simulation.

Densité

Nous avons mesuré cette métrique en faisant varier le nombre de nœuds pour montrer son impact sur le mécanisme backoff et sur les performances du réseau.

5. Scénarios et paramètres de simulation

Afin d'évaluer les performances de la solution proposée. Nous utilisons plusieurs scenarios de simulation. Nous considérons que le réseau est en mode Ad hoc avec la prise en charge de la mobilité. Nous avons généré des scénarios en utilisant le simulateur de mobilité **SUMO** (***S**imulation of **U**rban **Mo**bility*) (SUMO - Simulation of Urban Mobility)**,** c'est un simulateur open source codé en C++. Il génère des simulations routières microscopiques selon un modèle de poursuite routière. Ce simulateur est accompagné d'un outil programmé en JAVA appelé **MOVE** (***Mo**bility model generator for **Ve**hicular network*) (Laboratory for Experimental Network And System (LENS)), qui permet de convertir les mouvements créés par SUMO en un langage utilisé par le simulateur NS2.

Les cartes routières simulées peuvent être générés manuellement ou importés depuis des bases de données. Ce simulateur comporte une interface graphique pour faciliter la simulation. Le principal inconvénient du SUMO est que l'itinéraire des véhicules est calculé avant le début de la simulation, c'est-à-dire que les véhicules ne pourront pas changer d'itinéraire suite à des informations reçues par le réseau au cours de la simulation. (Benaidja & Moussaoui, 2010)

Dans notre simulation, nous considérons que les véhicules circulent dans une route à deux directions, chaque direction possède trois voies. La vitesse de déplacement d'un véhicule varie entre une valeur minimale de 1 m/s et une valeur maximale de 20m/s. Le comportement du réseau est testé sur différentes densités. Nous présentons quelques exemples de topologie de réseau dans la figure suivante. Ce sont des petits tronçons de la route utilisée.

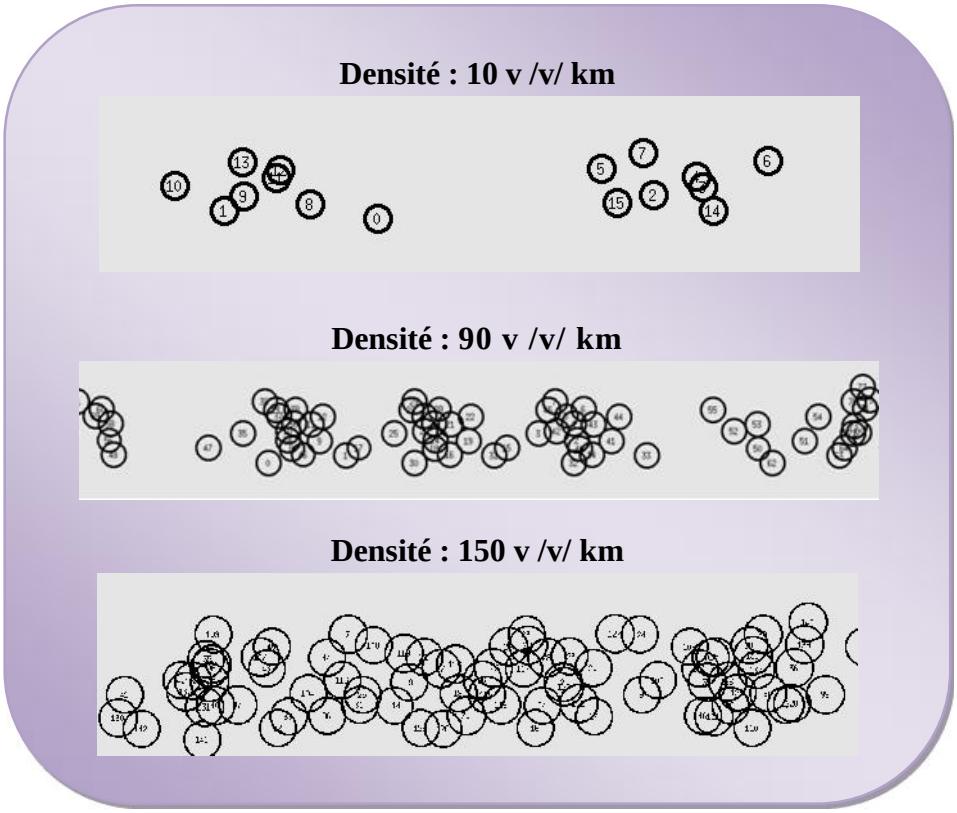


Figure 7-1 Exemples de quelques scénarios utilisés.

Les performances de notre solution d'adaptation dynamique de CW et notre solution adaptation basée sur la distance sont comparées avec la norme IEEE 802.11p en utilisant plusieurs métriques. Nous étudions l'impact de variation de ces paramètres sur chaque protocole proposé.

Les messages de contrôle RTS/CTS sont utilisés pour éviter les collisions dûes au problème de nœud caché. Nous considérons que chaque véhicule génère un trafic CBR chaque 0.15 seconde, la taille du paquet est de 512 bytes. Pour prévoir la possibilité de congestion du réseau, nous avons limité arbitrairement la taille des files d'attentes des nœuds à 50 paquets. Cette limitation permet la génération des paquets perdus (dropped or lost packets) similaire au cas d'un réseau réel lorsque l'ordonnanceur dépasse la limite de sa capacité.

Le tableau suivant résume les principaux paramètres de configuration de l'environnement de simulation.

Density of vehicles	10, 20, 40, 70, 90, 130, 150 Vehicle / Lane / Km
Maximum vehicle speed	30 m/s
Channel Frequency	5.9 GHz
Channel Width	10 MHz
Simulation time	120s
packet size	512 Bytes
CWmin	15
CWmax	1024
Catégorie de priorité	3
Threshold 1	0.21
Threshold 2	0.71
Threshold 3	0.52
generation rate	4 packets per second

Tableau 7-1 Les paramètres de simulation.

6. Résultats de simulation

6.1. Adaptation dynamique de CW

a) Délais de bout en bout

La figure 7.2 illustre la comparaison entre notre solution d'adaptation dynamique de la taille de la fenêtre de contention avec le protocole 802.11p de base en termes de délais de bout en bout en fonction de la densité. La figure montre que les délais d'attente augmentent dans les deux méthodes d'accès avec l'augmentation de la densité. Cela est à cause de l'augmentation dans la taille de la fenêtre de contention et l'augmentation des nœuds contendants pour accéder au canal. En effet, si la densité est importante, les collisions sont nombreuses et très fréquentes. De ce fait, le nœud à chaque fois double la taille de la fenêtre de contention et choisit une valeur aléatoire. La probabilité de choisir une grande valeur est grande notamment lorsque la densité est très élevée. Cette confirmation est assez intuitive en raison des compétitions pour accéder au canal qui devient gigantesque.

Ce qu'on peut remarquer aussi à partir de ce graphe, est que, plus la valeur CW est grande, plus le temps de backoff est grand, et les délais seront larges. On peut constater aussi que plus la densité est grande, plus le temps d'occupation du canal est important, d'où le temps d'attente est aussi important puisque les délais de bout en bout incluent également les temps d'attentes des transmissions.

Nous pouvons remarquer en second lieu, que la vitesse d'augmentation (traduit dans le graphe par la pente) est différente d'une plage de densité à une autre. Lorsque la densité est très faible, entre 10 et 20v/km/voie, nous remarquons une légère diminution, cela paraît étrange, mais çà a une explication. Vu que nous calculons les délais de bout en bout, et nous considérons toute sorte de collisions ou pertes ; si la densité est inférieure à 20v/voie/km, sachant que nous avons fixé le rayon de transmission à 250m, il y a beaucoup de perte à cause du manque des nœuds relais pour acheminer le message. D'où, nous pouvons avoir des retards supplémentaires. A partir de la valeur de densité égale à 20v/voie/km, selon la pente, nous distinguons trois cas : une légère augmentation (de 20 à 70 v/voir /km), suivie par une augmentation plus importante (de 70 à 130 v/voie/km), après il ya une augmentation très élevée de (130 à 150 v/voie/km). Ce qu'on peut déduire par cela est qu'entre 70 et 130v/v/km, on parle d'une congestion élevée, et au delà de 130 v/v/km, la communication devient quasi impossible. C'est ce qui nous a motivé à proposer notre deuxième contribution.

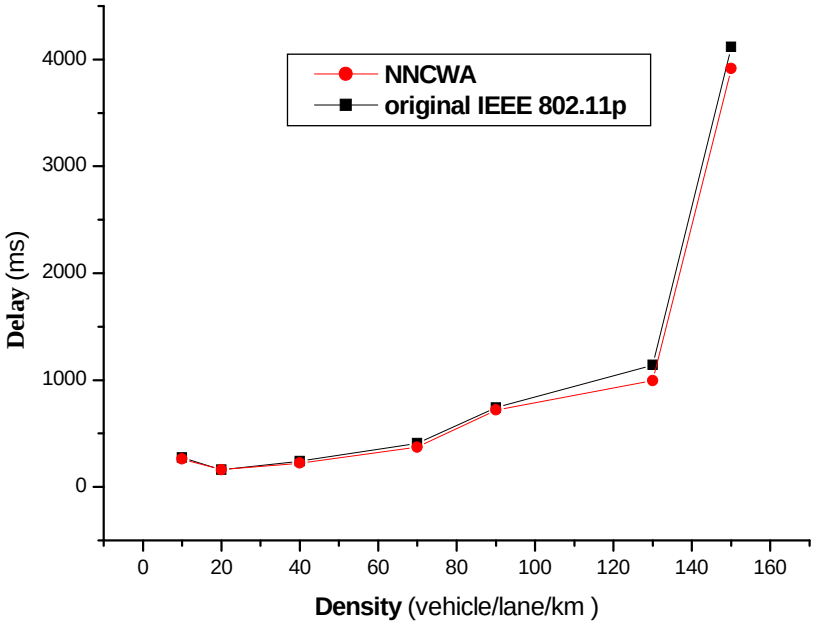


Figure 7-2 Délais de bout en bout. **7.2**

En outre, les délais de bout en bout sont inférieurs dans la solution proposée par rapport au protocole par défaut dans tous les cas (les sept scénarios). Comme nous pouvons voir dans la figure 7.2, il n'y a pas beaucoup de variation lorsque la densité est faible entre notre proposition et le standard parce que la différence entre les valeurs de CW est minime. En plus, il y a moins de collisions consécutives, de ce fait l'intervalle de la fenêtre de contention n'est pas large lorsque la densité est égale à 10,20, et 40v/v/km. A partir de 130 v /voie/km, nous remarquons un peu plus de différence. Ce qu'il faut indiquer est que : dans le cas des scénarios denses, notre approche d'adaptation tente à augmenter la valeur de la fenêtre de contention ; car les collisions deviennent très fréquentes et consécutives ; par cette augmentation, nous diminuons théoriquement la probabilité de collision.

b) Taux de collision

La figure 7.3 représente la variation du taux de collision en fonction de la densité. Nous remarquons la même constatation que dans la figure précédente, le taux d'erreur augmente avec l'augmentation de la densité. Nous remarquons bien les quatre cas distingués par la vitesse d'augmentation de la courbe. Lorsque la densité est inférieure à 20v/v/km, nous remarquons une légère diminution. Une légère augmentation suivie par une augmentation élevée, puis très élevée dans les intervalles : [20,70], [70,130], [130,150v/v/km] respectivement. Le taux de collision est amélioré dans tous les cas, l'amélioration du taux de collision est plus importante que l'amélioration des délais, notamment lorsque la densité est moyenne. De ce fait, le choix de la valeur de la fenêtre de contention influence considérablement sur le taux de collision. Ce comportement peut être expliqué en comprenant qu'une collision peut avoir des conséquences sur des transmissions simultanées. L'adaptation

adéquate de CW permet à chaque nœud l'opportunité de réduire les retransmissions simultanées. Malheureusement, si la taille de la fenêtre de contention est choisie assez petite, plusieurs nœuds vont se concurrencer pour les mêmes slots de transmissions, ce qui augmente la probabilité de collision. En choisissant, une grande valeur, plusieurs slots peuvent ne pas être utilisés pour une transmission. Donc pour avoir de performances optimales du système, un certain compromis est nécessaire entre garantir de meilleurs délais et assurer un taux de collision moins important. De ce fait, l'amélioration par rapport au standard n'est pas très importante concernant les délais de bout en bout et le taux de collision. Cependant, cette amélioration couvre différents scénarios allant d'une faible densité jusqu'à la saturation des routes.

Ce qui est important de noter aussi est qu'il est très difficile d'assurer de meilleurs résultats, et un grand écart comparé au protocole de base, lorsque nous considérons une densité faible et lorsqu'elle est très importante en même temps, cela a été constaté lors de l'ajustement des seuils de l'algorithme.

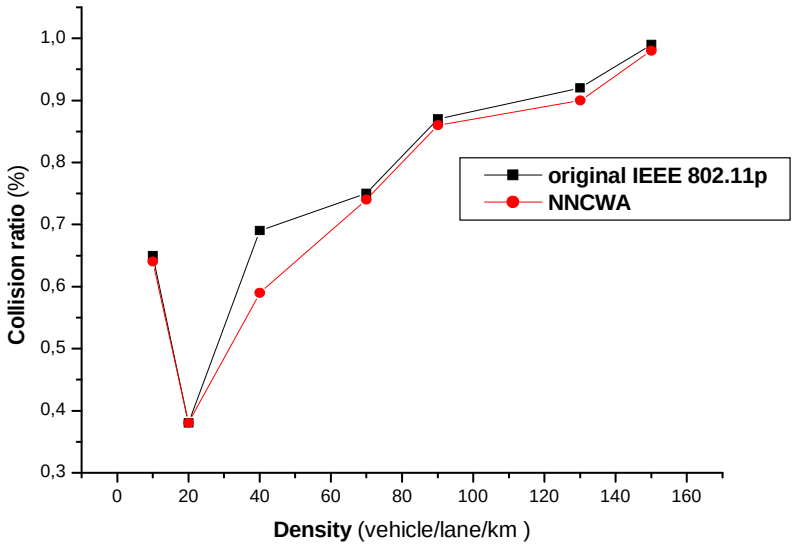


Figure 7-3 Taux de collision.

c) Le débit moyen

La figure 7.4 représente le flux de données moyen (Average throuthput) en fonction de la densité. A travers ce graphe, nous pouvons constater que notre solution arrive à surmonter cette troisième métrique très importante. Le flux de sortie est amélioré par rapport au standard de base dans tous les scénarios. Il existe cependant, quelques différences entre un scénario et un autre, cela est dû au non-déterminisme du protocole backoff et à la mobilité imprévisible des véhicules. Les même constatations que les deux métriques précédentes sont valables pour cette métrique. Rappelons qu'il existe une relation proportionnelle inverse entre le flux de sortie et la densité, contrairement aux deux métriques précédentes. Nous remarquons bien les quatre cas distingués par la vitesse de diminution du flux de sortie, comme présenté précédemment.

Le flux de sortie ou débit moyen a deux comportements différents conformément à la topologie du réseau. En effet, lorsque la densité des nœuds est faible, le débit est maximisé. Dans ce cas, les nœuds sont avantagés par la densité et ils ont tendance à transmettre de façon plus active, ayant une probabilité de collision relativement faible en raison d'un faible nombre de concurrents. Nous notons également que les valeurs de fenêtre de contention ont tendance à s'augmenter lorsque la densité des nœuds devient élevée.

L'impact de l'adaptation de la fenêtre de contention sur le flux de sortie est important. De minime changement dans les valeurs choisies de CW affectent considérablement le réseau. En outre, la saturation du flux de sortie dépend intensivement de la densité.

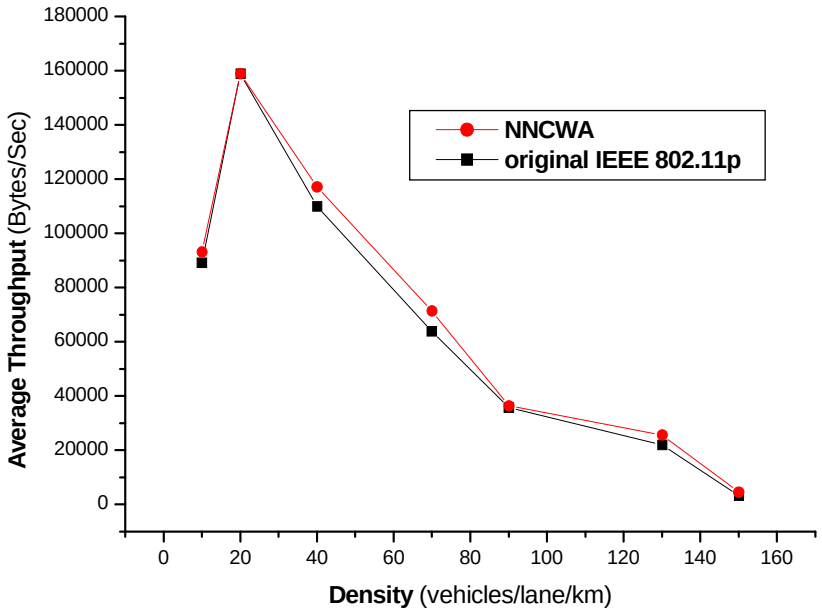


Figure 7-4 Average Throughput.

Nous allons montrer dans les graphes suivants (figure 7.5 et figure 7.6) un exemple de variation des valeurs CW choisies dans deux scénarios différents, un scenario dense de 130v/voie/km et un autre d'une densité très faible 20 v/voie/km. Les valeurs obtenues à partir de notre proposition et à partir du standard sont présenté dans les deux graphes. D'après ces deux graphes, nous pouvons remarquer que les valeurs de CW sont plus petites par rapport au standard dans le scénario de faible densité. Par contre, dans le scénario dense, les valeurs sont proches, il existe quelques pics dans notre proposition d'adaptation lors des collisions, Cependant la plage de CW dans le scénario dense est plus importante que la plage des valeurs dans un scénario de faible densité, malgré que l'aspect aléatoire est bien visible, puisque les valeurs ne sont pas fermées ; c'est ce qui peut diminuer la probabilité de collision.

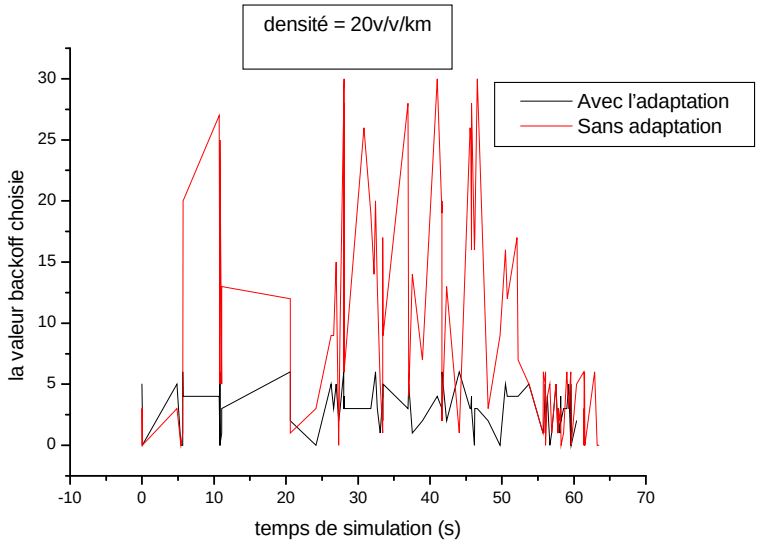


Figure 7-5 Variation des valeurs de CW choisies lorsque la densité 20v/v/km.7.5

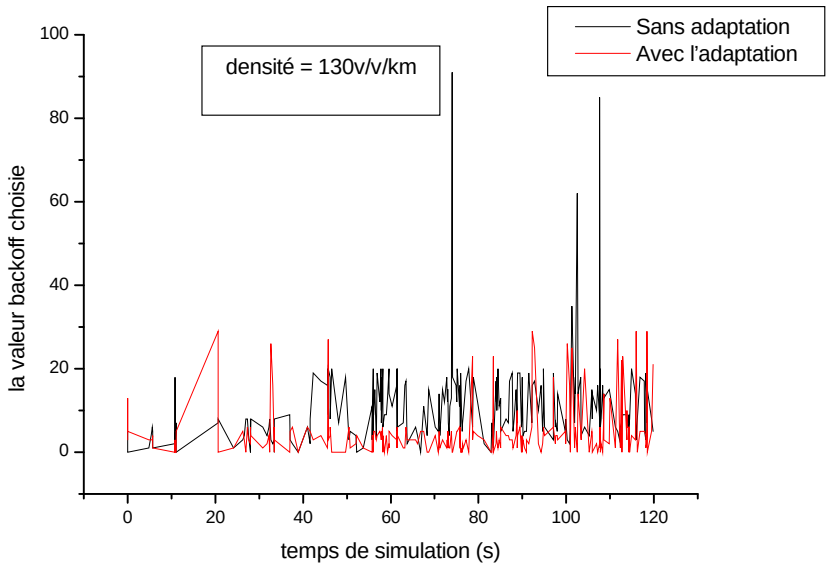


Figure 7-6 Variation des valeurs de CW choisies lorsque la densité 130v/v/km..7.6

D'après le graphe, bien que les valeurs de CW dans notre approche soient bien inférieures à celles du standard, nous ne constatons pas une grande différence de performances dans les délais illustrés dans la figure 7.2. La raison principale est qu'en diminuant la valeur CW, les collisions peuvent se produire fréquemment, car les même collisions peuvent se reproduire en choisissant le même nombre de slots de backoff (temps d'attente). Cela nécessite donc des retransmissions supplémentaires des paquets perdus. Ces retransmissions accroîtront les délais de bout en bout, et elles diminueront également le flux de sortie moyen.

Les trois métriques présentées précédemment sont des indicateurs de robustesse de notre proposition par rapport à la solution de base définie par le standard. Cela peut être observé à partir de tous nos résultats.

6.2. Adaptation de CW basée sur la distance et scalabilité

Dans ce qui suit, nous allons présenter les résultats de simulation de notre deuxième proposition. Il s'agit de l'adaptation de CW basée sur la distance entre l'émetteur et le récepteur afin de diminuer la saturation du réseau. Nous avons choisi d'utiliser plusieurs scénarios, particulièrement des scénarios denses, car ce mécanisme agit lorsque le seuil de congestion calculé par le réseau de neurones atteint une certaine valeur. Nous avons opté pour cinq densités différentes : 70, 90, 100, 130 et 150 véhicules/voie/km.

Le tableau suivant montre les différents paramètres fixés lors des tests :

Density of vehicles :	10, 20, 40, 70, 90, 130, 150 vehicle / lane / km
Maximum vehicle speed	30 m/s
Channel Frequency	5.9 GHz
Channel Width	10 MHz
generation rate	4 packets (512byte) per second

a) Les délais de bout en bout

La figure 7.7 montre la variation des délais de bout en bout en fonction de la densité de notre approche d'adaptation basée sur la distance, comparée au standard de base 802.11p. Ce qu'on peut constater est que notre seconde proposition arrive à réduire les délais dans tous les scénarios de simulation. Cependant l'apport de cette amélioration diffère d'un scénario à un autre. En effet, la mobilité joue aussi un rôle très important vu que les véhicules changent très rapidement leurs positions, ce qui rend la connectivité du réseau pas toujours assurée.

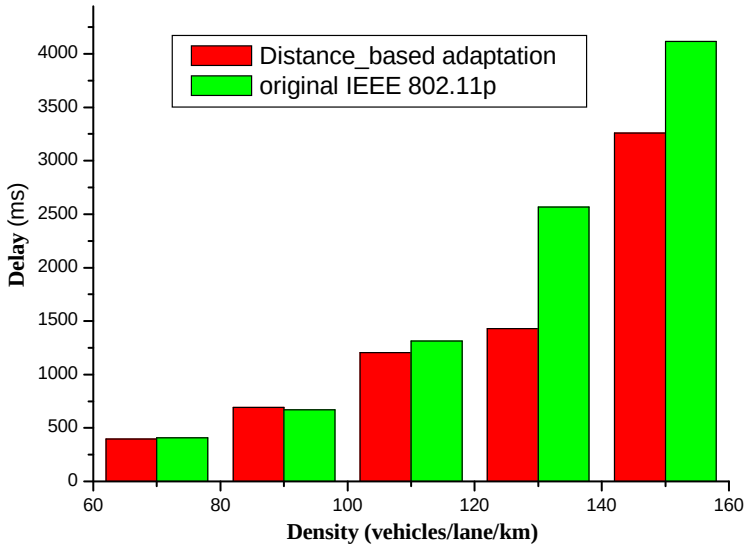


Figure 7-7 Délais moyens, en comparaison de notre approche basée distance, avec le standard de base.

Nous pouvons remarquer aussi que les variations des délais entre notre proposition et le standard est minime voir nulle lorsque la densité est inférieur à 110v/voie/km. La raison principale de cela est que le fait de se baser sur la distance afin de retarder quelques communications, pour alléger le réseau, et vue la mobilité élevée des véhicules, le message peut ne pas arriver en intégrité en un temps minimal, ie que les distances entre l'émetteur et le récepteur varient de manière imprévisible particulièrement dans le cas où les véhicules communiquants circulent dans deux directions opposées. Ce scénario est bien présent dans nos communications simulées afin d'avoir un comportement plus réaliste. De ce fait, les trames d'un même message n'ont pas la même chance d'accéder au canal surtout lorsque la distance varie de manière considérable pendant l'envoi du même paquet, ie que des trames mac seront perdues ou subissent des retard supplémentaires à cause de la distance importante entre les deux véhicules communicants au niveau mac, donc cela peut nécessiter des retransmissions complémentaires, ce qui augmentera les délais de réception de l'intégrité du paquet. Ce comportement rend notre approche plus adaptée aux applications de non-sécurité, car le message qui peut être soit de la vidéo ou de la musique possède une taille importante, et contrairement à un message de sécurité, ce message est moins sensible aux pertes car son contenu peut être lisible même avec quelque trames perdues.

Cependant, à partir de la densité égale à 130v/v/km où le réseau est saturé, les délais moyens sont plus stables dans notre solution contrairement au standard de base. Lorsque la densité est égale à 130v/v/km, notre solution arrive à diminuer les délais de 40%, et lorsqu'elle est égale à 150v/v/km, les délais sont améliorés de plus de 18%.

b) Débit moyen

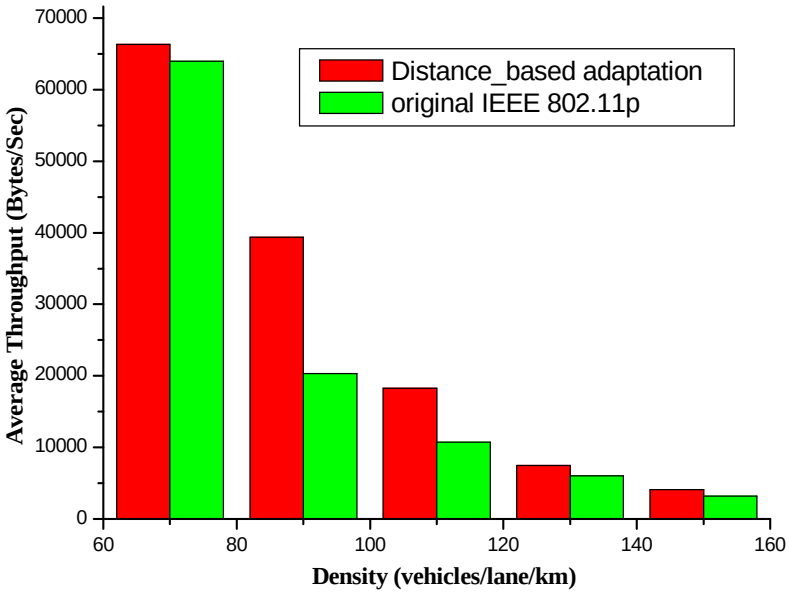


Figure 7-8 Débits moyens, approche basée distance.7.8

D'après le graphe illustré dans la figure 7.8, nous pouvons voir que les débits moyens sont améliorés dans notre approche basée sur la distance par rapport à la norme de base 802.11p. Le graphe montre l'effet de l'utilisation de la probabilité de collision estimée afin d'alléger le réseau. Cependant, lorsque la densité est supérieure ou égale à 130v/voie/km, l'apport de notre solution devient moins important car le réseau devient très saturé.

Les résultats de simulation ne se comportent pas de la même façon pour les débits que pour les délais, ce qui montre que l'algorithme Backoff dans l'environnement véhiculaire a un comportement impondérable.

c) Taux de collision

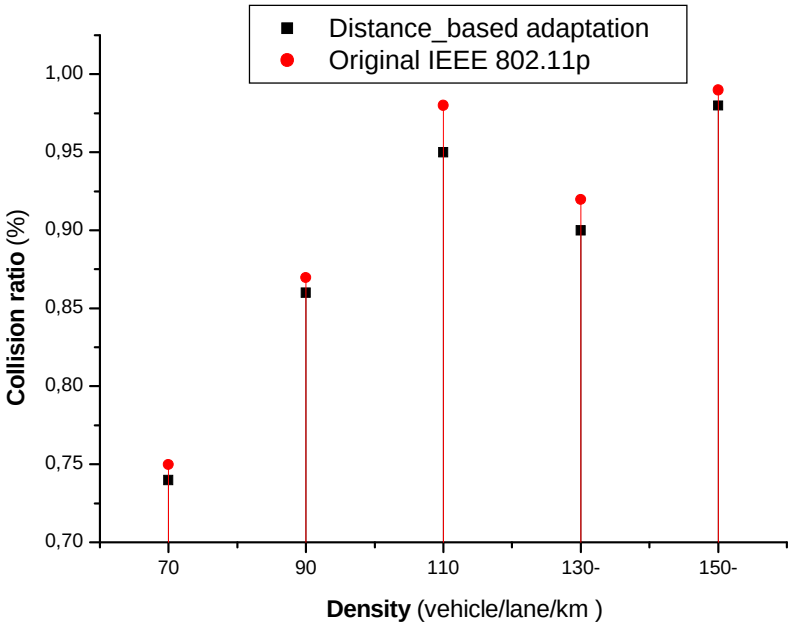


Figure 7-9 Taux de collision, approche basée distance.7.9

Le graphe donné en figure 7.9 montre le taux de collision moyen des véhicules en fonction de la densité. Nous pouvons remarquer que notre solution offre un taux de collision moins important que le standard de base dans tous les scénarios de simulations. C'est ce qui confirme que notre deuxième solution a répondu aux objectifs visés lors de sa conception.

7. Synthèse

Pour résumer, nous pouvons dire que, d'une part, une petite valeur de la fenêtre de contention encourage plus de transmissions concurrentes mais au détriment de plus de collisions. D'autre part, une grande valeur de la fenêtre de contention réduit la probabilité de collision, mais elle résulte des délais de bout en bout plus importants et empêche les transmissions simultanées de se produire, ce qui peut limiter la capacité du système.

Pour surmonter le manque de contrôle de congestion dans la norme 802.11p. Nous avons proposé une nouvelle approche pour estimer le niveau de congestion dans le réseau. En utilisant le réseau de neurones. L'approche est capable de combiner entre différents paramètres influençant sur la probabilité de collision afin de retarder une communication qui a une grande chance de produire une collision, ou bien, favoriser une communication qui a une faible chance de produire une collision. D'un autre côté, nous diminuons les délais de backoff s'il y a une faible congestion dans le réseau, en opposition, nous augmentons cet intervalle si le niveau de congestion est élevé, dans le but de diminuer les collisions consécutives, en diminuant la chance de choisir le même nombre de slots par les deux véhicules qui ont causé cette collision. D'un autre côté, Il faut noter que les performances du système sont dépendantes de l'interaction entre les différentes couches du réseau PHY/MAC/NETWORK.

Il est nécessaire au niveau MAC de prendre en considération les besoins des autres couches du réseau.

8. Conclusion

Dans ce chapitre, nous avons étudié un algorithme de backoff dans le but d'améliorer la QoS dans les réseaux véhiculaires. Nous avons évalué les deux solutions présentées dans le chapitre précédent. Les algorithmes proposés intègrent à la fois le suivi de l'état de congestion, et l'adaptation nécessaire à faire.

Le scénario d'autoroute mis en place, nous a permis de simuler un cas de réseau où plusieurs véhicules interagissent pour partager le même canal. Les résultats de simulation montrent bien qu'avec un minimum de changement dans CW, les performances du réseau sont améliorées. Ceci allège la charge du réseau tout en diminuant la probabilité des collisions. Nous avons aussi montré l'intérêt du changement dynamique de la fenêtre de contention sur les trois métriques importantes du réseau, les délais de bout en bout, le flux de sortie et le taux de collision.

Conclusion générale

Au terme de cette thèse, nous nous proposons de faire un récapitulatif de notre travail, d'analyser globalement les résultats obtenus et enfin dresser des perspectives que nous trouvons prometteuses et constituant la suite logique du présent travail.

Dans la première partie de ce travail, nous avons étudié et classer les différentes solutions d'adaptation de la fenêtre de contention après avoir mis le point sur les différentes solutions et standards MAC pour les réseaux véhiculaires. La deuxième partie présente nos solutions proposées avec les tests et les résultats de simulation.

Dans le chapitre 2 nous avons étudié les principaux protocoles de la couche MAC des réseaux véhiculaires qui ont été proposés dans la littérature. Dans le chapitre 3 nous avons présenté le standard IEEE 802.11p, son fonctionnement et les principales problématiques liées à la couche MAC de ce dernier. Le standard propose entre autres le mode WAVE permettant aux véhicules de se communiquer en prenant en considération la mobilité des nœuds. En effet nous avons pu constater dans ce chapitre que la couche MAC du standard IEEE 802.11p ne propose aucun mécanisme de contrôle de congestion spécifique aux réseaux véhiculaires.

Dans ce cadre, il existe différents mécanismes de contrôle de congestion pour ces réseaux. Parmi ces mécanismes, une grande communauté de recherche s'intéresse à l'amélioration du protocole BACKOFF lorsqu'il s'agit des réseaux dynamiques. Cet algorithme qui est le seul mécanisme de contrôle de congestion disponible dans la norme 802.11p, et qui a comme principe la sélection d'un nombre aléatoire de slots à attendre à partir d'un intervalle appelé fenêtre de contention lorsqu'il y a une collision ou lorsque le canal est occupé. Dans le but de minimiser les interférences et les collisions, la taille de la fenêtre de contention est doublée et elle est bornée par CWmax. Elle sera réinitialisée à CWmin après une transmission réussie (Nehdi, 2005).

L'intérêt de l'adaptation de la fenêtre de contention est très important pour améliorer les performances du réseau en termes de délais, débit, et taux de collisions. Nous avons donc étudié les différents travaux d'adaptation dynamique de la fenêtre de contention dans le cadre des réseaux véhiculaires.

Cette étude nous a permis de proposer une nouvelle stratégie NN-ACW d'adaptation de la fenêtre de contention pour le standard IEEE 802.11p, dont le but est de permettre l'auto-adaptation de la taille de la fenêtre de contention dans le protocole d'accès au canal afin d'offrir des performances optimales en terme d'utilisation de la bande passante.

L'étude menée dans ce mémoire montre l'apport de cette adaptation dans un réseau véhiculaire.

Par ailleurs, notre solution a comme particularité de ne pas être conditionnée par la présence obligatoire de l'infrastructure ou l'échange permanents des messages beacon ou de coordination pour maintenir à jour la densité véhiculaire, c'est-à-dire que le véhicule, selon les conditions observées et les informations disponibles et récentes, établit les priorités entre les quatre paramètres utilisés pour l'estimation de la congestion. C'est dans le but d'avoir une estimation proche de la réalité au sujet de l'état du trafic dans le réseau. Ceci évite d'avoir une mauvaise évaluation de l'état de congestion qui peut susciter une mauvaise décision d'adaptation.

Nous avons proposé une solution hybride qui regroupe globalement ces paramètres en utilisant les réseaux de neurones et l'apprentissage (Stricker, 2000). D'ailleurs, c'est ce qui permet au nœud d'être en interaction permanente avec l'état de congestion dans son environnement.

Nous avons pu constater à partir des résultats d'évaluation des performances que cet algorithme est fortement influencé par l'état du trafic et d'environnement. Les résultats obtenus montrent l'intérêt de ce genre de technique dans les réseaux véhiculaires où la charge de trafic peut être très variable selon l'application considérée. Ces résultats prouvent l'intérêt des solutions proposées et leurs capacité d'amélioration des performances du standard IEEE 802.11p et ceci en considérant différentes densités véhiculaires. Nous avons conclu que face aux différentes applications que doivent gérer les réseaux véhiculaires, il faut avoir un mécanisme d'auto adaptation gérant des paramètres du réseau.

Notre contribution a fait l'objet d'une publication dans une conférence internationale (Zerrouki, Moussaoui, & Doukha, 2013).

Comme perspective envisageable pour améliorer les performances de notre solution nous proposons de :

- Comparer notre solution à d'autres approches existantes dans le but de montrer l'avantage d'utiliser les réseaux de neurones et l'apprentissage par rapport à d'autres méthodes existantes comme par exemple les approches utilisant la logique floue.

- Mettre en place l'approche proposée en considérant les différentes catégories d'accès afin d'assurer la qualité de service.

- Penser à la manière de fixer les seuils autre que l'utilisation des tests, on pourrait penser à établir une formule mathématique reliant directement la sortie du réseau de neurones à la valeur instantanée de la fenêtre de contention.

- Utiliser des approches automatiques et formelles pour choisir de meilleures valeurs d'apprentissage, il faut peut être penser au Datamining.

Bibliographie

802.11-2012 - IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY). (2012, March 29). *IEEE Std 802.11-2012 (Revision of IEEE Std 802.11-2007)* .

802.11e. (n.d.). Retrieved from http://hpds.ee.ncku.edu.tw/~smallko/ns2/ns2.htm

ACCES MULTIPLE A REPARTITION PAR CODE (CDMA). L'IES institut d'électronique. unité mixte de recherche (2003).

Alapati, J. (2010). *MAC Layer Protocols for Broadcast Transmissions in Vehicular Networks.* Master of Technology in Communications and Signal Processing, Department of Electrical Engineering IndianInstitute of Technology, Bombay.

Alapati, J., Pandya, B., Merchan, S. N., & Desai, U. (2010, June). Back-off and Retransmission Strategies for Throughput Enhancement of Broadcast Transmissions in 802.11p Proceedings of the 21st IEEE Intellig. *Proceedings of the 21st IEEE Intelligent Vehicles Symposium (IV 2010)* , pp. 700-705.

Amadeo, M., Campolo, C., & Molina, A. (2012). Enhancing IEEE 802.11p/WAVE to provide infotainment applications in VANETs. *Ad Hoc Networks , 10*, 253–269.

Amamra, A. (2008). *Techniques d'Estimation de la Bande Passante Disponible de Réseaux Sans Fil.* Université Blaise Pascal – Clermont-Ferrand II.

Ameixieira, C., Matos, J., Moreira, R., Cardote, A., Oliveira, A., & Sargento, S. (2011). An IEEE 802.11p/WAVE Implementation with Synchronous Channel Switching for Seamless Dual-channel Access. *IEEE Vehicular Networking (VNC)* .

Artimy, M. (2007, September). Local Density Estimation and Dynamic Transmission-Range Assignment in Vehicular Ad Hoc Networks. *IEEE Transactions on Intelligent Transportation Systems , 8* (3), pp. 400-412.

Badis, H. (2005). *ÉTUDE ET CONCEPTION D'ALGORITHMES POUR LES RÉSEAUX MOBILES ET AD HOC.* Université Paris-Sud, CNRS 8623. France: Laboratoire de Recherche en Informatique.

Balador, A., & Movaghar, A. (2010, April 24-25). The Novel Contention Window Control Scheme for IEEE 802.11 Mac Protocol. *Second International Conference on Networks Security, Wireless Communications and Trusted Computing* , pp. 134 - 137.

Balon, N. (2006). *INCREASING BROADCAST RELIABILITY IN VEHICULAR AD HOC NETWORKS.* Master of Science, The University of Michigan.

Balon, N., & Guo, J. (2006, September). Increasing Broadcast Reliability in Vehicular Ad Hoc Networks. *Proceedings of the 3rd ACM International Workshop on Vehicular Ad Hoc Networks (VANET 2006)* , pp. 104-105.

Barbosa, A., Bessa, A. L., Sérgio, A., Rober, F. M., & Jùnior, J. C. (2011). An Adaptive Mechanism for Access Control in VANETs. *ICN 2011 : The Tenth International Conference on Networks* .

Barradi, M., Hafid, A. S., & Gallardo, J. R. (2010). Establishing strict priorities in IEEE 802.11p WAVE vehicular networks. *IEEE Globecom 2010 proceedings* .

Basic Set of Applications; Part 2: Specification of Cooperative Awareness, Intelligent Transport Systems (ITS). *Vehicular communications.*

Benaidja, A., & Moussaoui, S. (2010). *Les réseaux inter-véhiculaires : Application à la sécurité routière.* Thèse de magistère, Université des Sciences et de la Technologie Houari Boumediene, Alger.

Bénédicte, H., Julien, A., Arnaud, D., Eric, L., & Laurent, M. (2002). *Etude et comparaison des protocoles Slotted ALOHA et CPCH pour l'accès à un réseau UMTS.* Projet Opnet.

Bi, Y., Liu, K., Cai, L., & Shen, X. (2009). A multi-channel token ring protocol for QoS provisioning in inter-vehicle communications. *IEEE Trans , 8* (11), 5621–5631.

Bi, Y., Liu, K.-H., & Shen, X. (2008). A Multi-Channel Token Ring Protocol for Inter-Vehicle Communications. *IEEE* .

Bianchi, G., Luigi, F., & Oliveri, M. (1996, Octobre). Performance Evaluation and Enhancement of the CSMA/CA MAC Protocol for 802.11 Wireless LANs, Proceedings of the 7th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 1996), pp. *Proceedings of the 7th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 1996)* , pp. 392-396.

Bilstrup, K., Uhlemann, E., Strom, E., & U, B. (2009). On the ability of the 802.11p MAC method and STDMA to support real-time vehicle-tovehicle communications. *EURASIP J. Wirel* .

Boix, N. M., & Mecklenbräuker, C. (2008). *Design and development of an automated test environment for car-to-car and car-to-infrastructure communications based on IEEE 802.11p and IEEE 1609 WAVE standards.* FINAL PROJECT, TECHNISCHE UNIVERSITÄT WIEN INSTITUTE OF COMMUNICATIONS AND RADIO FREQUENCY ENGINEERING UNIVERSIDAD POLITÉCNICA DE VALENCIA ESCUELA TÉCNICA SUPERIOR DE INGENIEROS DE TELECOMUNICACIONES.

Booysen, M. J., Zeadally, S., & Rooyen, G.-J. v. (2011, March). Survey of media access control protocols for vehicular ad hoc networks. *IET Communications ISSN 1751-8628* .

Calì, F., Conti, M., & Gregori, E. (2000, December). Dynamic Tuning of the IEEE 802.11 Protocol to Achieve a Theoretical Throughput Limit. *IEEE/ACM Transactions on Networking , 8* (6), pp. 785-799.

Calzada, R. C. (Juny 2011). *PERFORMANCE EVALUATION OF REALISTIC SCENARIOS FOR VEHICULAR AD HOC NETWORKS WITH VANETMOBISIM AND NS2.* PROJECTE FINAL DE CARRERA, Enginyeria de Telecomunicació.

(2007). *CAR 2 CAR Communication Consortium Manifesto version 1.1.* Rapport technique CAR 2 CAR Communication Consortium (C2C-CC).

Cavagna, R., & Nuaymi, L. (2004). *Analyse de la norme IEEE 802.11.* ENST Bretagne.

Chalhoub, G. (2010). Clermont Université 44, Routage et MAC dans les réseaux de capteurs sans fil.

Dib, G., & Stancil, D. (2009). *Vehicle-to-Vehicle Channel Simulation in a Network Simulator*. THESIS of MASTERS OF SCIENCE, CARNEGIE MELLON UNIVERSITY.

Dridi, K. (2011). *Réseaux & Télécoms Spécification du Protocole MAC pour les Réseaux IEEE 802.11e à Différentiation de Services sous Contrainte de de Mobilité.* thèse de Doctorat, L'Université Paris Est, Informatique Spécialité, Paris.

(2010). *European ITS Communication Architecture: Overall Framework and Proof of Concept Implementation.* COMeSafety.

Harbouche, O., & Moussaoui, S. (2009). *La sécurité des communications véhiculaires.* Alger: USTHB.

Hartenstein, H., & Laberteaux, K. P. (2010). *VANET: Vehicular Applications and Inter-Networking Technologies Book.* (Ltd, Ed.)

Huang, C.-L., & Liao, W. (2007, JANUARY). Throughput and Delay Performance of IEEE 802.11e Enhanced Distributed Channel Access (EDCA) Under Saturation Condition. *IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS , 6* (1), pp. 136-145.

Huang, C.-M., & Chen, Y.-S. (2010). *Telematics Communication Technologies and Vehicular Networks: Wireless Architectures and Applications.* New York.

Huang, C.-M., & Kung, C. (2009). *Telematics Communication Technologies and Vehicular Networks: Wireless Architectures and Applications.* Hershey, New York: InformatIon scIence reference.

Hung-Cuong, L. (2008). *Optimisation d'accès au médium et stockage de données distribuées dans les réseaux de capteurs.* thèse de doctorat, l'Université de Franche-Comté.

Igartua, A. M., Frías, C. V., de la Cruz Llopis, L. J., & Gargallo, S. E. (2010). Dynamic framework with adaptive contention window and multipath routing for video-streaming services over mobile ad hoc networks. *Springer Science+Business Media* , pp. 379–390.

Jang, H. C., & Feng, W. C. (2010, May). Network Status Detection-Based Dynamic Adaptation of Contention Window in IEEE 802.11p . *Proceedings of the IEEE 71st Vehicular Technology Conference (VTC Spring 2010)* , pp. 1-5.

Jiang, L., & Walrand, J. (2010, June). A Distributed CSMA Algorithm for Throughput and Utility Maximization in Wireless Networks IEEE/ACM Transactions on Networking. *IEEE/ACM TRANSACTIONS ON NETWORKING , 18* (3), pp. 960-972.

Kacimi, R. (2009). *Techniques de conservation d'énergie pour les réseaux de capteurs sans fil.* l'Institut National Polytechnique de Toulouse. Toulouse: Unité de recherche : IRIT.

Kim, T. H., Marwitz, L., & Kim, D. K. (2003). Dynamic Offset Contention Window (DOCW) Algorithm for Wireless MAC in 802.11e Based Wireless Home Networks. *Springer* , pp. 162-172.

Kim, T. H., Ni, J., Srikant, R., & Vaidya, N. H. (2011, April). On the Achievable Throughput of CSMA under Imperfect Carrier Sensing. *the 30th IEEE Annual International Conference on computer Communications (INFOCOM 2011)* , pp. 1674-1682.

Kim, T., Jung, S., & Lee, S. (2009). CMMP : Clustering-Based Multi-Channel MAC Protocol In VANET. *Second International Conference on Computer and Electrical Engineering* .

Ksentini, A. (2005). *Quality of service (QoS) in IEEE 802.11-based Wireless Local Area Networks (WLAN) Qualité de Service (QoS) dans les réseaux locaux sans fil basés Sur la technologie IEEE 802.11*. thèse de doctorat, Laboratoire Informatique de Cergy-Pontoise (LICP) EA 2175.

Labiod, H., Afifi, H., & Detantis, C. (2007). (SPRINGER, Ed.) FRANCE: Springer Netherlands.

Laboratory for Experimental Network And System (LENS). (n.d.). Retrieved from http://lens.csie.ncku.edu.tw/Joomla_version/index.php/research-projects/past/18-rapid-vanet

Lassous, I. G. (2008). Université Claude Bernard. Lyon: UFR Informatique.

Layouni, M., Weslem, W., Raphael, M., & Tran, A. (2010). *Rapport de Projet Final MASTER 1: Projet VANET.* Rapport de Projet Final MASTER 1.

Lee, J. Y., & Lee, H. S. (2009, JANUARY). A Performance Analysis Model for IEEE 802.11e EDCA Under Saturation Condition. *IEEE TRANSACTIONS ON COMMUNICATIONS , 57*, pp. 56-63.

Lin, L., Jia, W., Han, B., & De, L. Z. (2007). Performance Improvement using Dynamic Contention Window Adjustment for Initial Ranging in IEEE 802.16 P2MP Networks. *IEEE Communications Society subject matter experts for publication in the WCNC 2007 proceedings* .

Local andMetropolitan Area Networks - Speci_c Requirements. Part 11: Wireless LAN Medium Access. The Institute of Electrical and Electronics Engineers IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems .

Lu, N., Ji, Y., Liu, F., & Wang, X. (2010). A dedicated multi-channel MAC protocol design for VANET with adaptive broadcasting. *IEEE Wireless Communications and Networking Conf. (WCNC)* .

Lukyanenko, A., Gurtov, A., & Morozov, E. (2011, Novembe 10). An Adaptive Backoff Protocol With Markovian Contention Window Control.

Maidi M., Temglit T, F., & Achour, N. (2001). *Utilisation des Réseaux de Neurones pour la Construction de Cartes d'Environnements Robotique Mobile.* MEMOIRE DE PROJET DE FIN D'ETUDES, Diplôme d'Ingénieur d'Etat en Electronique, FACULTE DE GENIE ELECTRIQUE INSTITUT D'ELECTRONIQUE DEPARTEMENT INSTRUMENTATION ET AUTOMATIQUE.

Mazen, Y. (2009). *Modélisation, simulation et optimisation des architectures de récepteur pour les techniques d'accès W-CDMA.* l'Université Paul Verla, l'Université Paul Verlaine – Metz . Lorraine: LABORATOIRE INTERFACES CAPTEURS ET MICORELECTRONIQUE, Ecole Doctorale IAEM.

Medepalli, K., & Tobagi, F. (2006, April). Towards Performance Modeling of IEEE 802.11 based Wireless Networks: A Uni_ed Framework and its Applications. *INFOCOM 2006, the 25th IEEE Annual International Conference on Computer Communications* , pp. 1-12.

Mertens, Y., Wellens, M., & Mahonen, P. (2008, May). Simulation-based Performance Evaluation of Enhanced Broadcast Schemes for IEEE 802.11-based Vehicular Networks . *the IEEE 67th Vehicular Technology Conference (VTC Spring 2008)* , pp. 3042-3046.

Mohamed, L. (2009). *Diffusion et couverture basées sur le clustering dans les réseaux de capteurs : application à la domotique.* Thèse de Doctorat, Université A.B Tlemcen, Université A.B Tlemcen & Université de Franche-Comté, U.F.R Sciences et Techniques.

Moustafa, H., & Zhang, Y. (2009). *Vehicular Networks Techniques, Standards, and Applications.* (T. &. Group, Ed.) avril: LLC.

Nardelli, B., Lee, J., Lee, K., Yi, Y., Chong, S., Knightly, E. W., et al. (2011, April 10-15). Experimental Evaluation of Optimal CSMA. *the 30th IEEE Annual International Conference on Computer Communications (INFOCOM 2011)* , pp. 1188-1196.

Nehdi, M. (2005). *Evaluation du protocole EDCA.* TUNISIE: Sup'Com.

Pries, R., Menth, S., Staehle, D., & Tran-Gia, P. (2008). Dynamic Contention Window Adaptation (DCWA) in IEEE 802.11e Wireless Local Area Networks. *IEEE* , pp. 92-97.

Rawat, D. B., Popescu, D. C., Yan, G., & Olariu, S. (2011). Enhancing VANET Performance by Joint Adaptation of Transmission Power and Contention Window Size. *IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS* .

Romdhane, Y. M., & Tabbene, N. M. (2007). *Evaluation des performances des protocoles S-MAC et Directed Diffusion dans les réseaux de capteurs.* Rapport De Projet De Fin d'Etudes, Tunisie.

Sawaya, J. N., & Ghaddar, B. (2005). A Fuzzy Logic Approach for Adjusting The Contention Window Size in IEEE 802.11e Wireless Ad Hoc Networks. Ontario, University of Waterloo, Canada.

Shirani, R., & Hendessi, F. (2009, September). Store-Carry-Forward Message Dissemination in Vehicular Ad-Hoc Networks with Local Density Estimation . *70th IEEE Vehicular Technology Conference (VTC Fall 2009)* , pp. 1-6.

Siad, L. (2007). *ANALYSE ET SIMULATION DES COLLISIONS DANS UN RÉSEAU IEEE 802.11.* thèse de MAGISTER EN INFORMATIQUE, Institut National de formation en Informatique I.N.I, Alger.

Sjöberg, K. (2013). *Medium Access Control for Vehicular Ad Hoc Networks.* Thesis for the degree of Doctor of Philosophy, CHALMERS UNIVERSITY OF TECHNOLOGY, Göteborg, Sweden.

Stanica, R. (2011). Congestion Control in Vehicular Ad-Hoc Networks. In R. STANICA, *thèse de doctorat.* TOULOUSE, Institut National Polytechnique de Toulouse (INP Toulouse).

Stricker, M. (2000). Thèse de Doctorat , l'Université Pierre et Marie Curie - Paris VI .

SUMO - Simulation of Urban Mobility. (n.d.). Retrieved from http://www.safespot-eu.org/

Tchepnda, C. (2008). *Authentification dans les Réseaux Véhiculaires Opérés.* Thèse de Doctorat, L'Ecole Nationale Supérieure des Télécommunications PARIS.

TCHEPNDA, C. (2008). *Authentification dans les Réseaux Véhiculaires Opérés.* L'Ecole Nationale Supérieure des Télécommunications PARIS.

Terre, M. (2007). WiFi Le Standard 802.11 Couche physique et couche. In u. Paris, *Cours du Conservatoire National des Arts et Métiers.* université Paris.

The Network Simulator - ns-2. (n.d.). Retrieved from http://www.isi.edu/nsnam/ns/

Tibi, N., & Tabbana, F. (2005). *Etude des mécanismes de différentiation de service niveau IP et MAC.* TUNISIE: SUP'COM.

Touzet, C. (1992). *LES RESEAUX DE NEURONES ARTIFICIELS INTRODUCTION AU CONNEXIONNISME COURS, EXERCICES ET TRAVAUX PRATIQUES.*

Urmeneta, P. (2010). *Simulation and Improvement of the Handover process in IEEE 802.11p based VANETs (Vehicle Ad-hoc NETworks).* College of Electronics and Information Engineering, Tongji University Escola.

Vales-Alonso, J., Vicente-Carrasco, F., & Alca, J. J. (2011). Optimal configuration of roadside beacons in V2I communications. *Computer Networks , 55*, 3142–3153.

Vinel, A., Campolo, C., Petit, J., & Koucheryavy, Y. (2011). Trustworthy Broadcasting in IEEE 802.11p/WAVE Vehicular Networks: Delay Analysis. *IEEE COMMUNICATIONS LETTERS , 15* (9), pp. 1010-1012.

Vittorio, S., Toscano, E., & Bel, L. L. (2008). CWFC: A ContentionWindow Fuzzy Controller for QoS support on IEEE 802.11e EDCA. *IEEE* (1-4244-1506-3), pp. 1193-1196.

Wang, C., Li, B., & Li, L. (2004, July). A New Collision Resolution Mechanism to Enhance the Performance of IEEE 802.11 DCF. *IEEE Transactions on Vehicular Technology , 53* (4), pp. 1235-1246.

Wang, Q., Leng, S., Fu, H., & Zhan, Y. (2010). An Enhanced Multi-channel MAC for the IEEE 1609.4 based Vehicular Ad Hoc Networks. *IEEE INFOCOM* , p. IEEE Communications Society subject matter experts for publication in.

Wang, Y., Ahmed, A., Krishnamachari, B., & Psounis, K. (2008, September 22-24). IEEE 802.11p Performance Evaluation and Protocol Enhancement. *Proceedings of the 4th IEEE International Conference on Vehicular Electronics and and Safety (ICVES 2008)* , pp. 317-322.

Yu, F., & Biswas, S. (2007). Self-Configuring TDMA Protocols for Enhancing Vehicle Safety With DSRC Based Vehicle-to-Vehicle Communications . *IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS , 25* (8).

Zerrouki, H., Moussaoui, S., & Doukha, Z. (2013, Avril 28 - 29). An adaptative Backoff mechanism for VANETs. *Workshop International: Evaluation de Performance et Qualité de Service EPQoS* .