Université de Montréal

Un protocole de diffusion des messages dans les réseaux véhiculaires

par
Ahizoune Ahmed

Département d'informatique et de recherche opérationnelle
Faculté des arts et des sciences

Mémoire présenté à la Faculté des études supérieures
en vue de l'obtention du grade de
Maîtrise ès sciences (M. Sc.)
en informatique

Avril, 2011

Université de Montréal
Faculté des arts et des sciences

Ce mémoire intitulé :

Un protocole de diffusion des messages dans les réseaux véhiculaires

présenté par :
Ahizoune Ahmed

a été évalué par un jury composé des personnes suivantes :

Marc Feeley, président
Abdelhakim Hafid, directeur de recherche
Ronald Beaubrun, membre du jury

Résumé

De nos jours, la voiture est devenue le mode de transport le plus utilisé, mais malheureusement, il est accompagné d'un certain nombre de problèmes (accidents, pollution, embouteillages, etc.), qui vont aller en s'aggravant avec l'augmentation prévue du nombre de voitures particulières, malgré les efforts très importants mis en œuvre pour tenter de les réduire ; le nombre de morts sur les routes demeure très important.

Les réseaux sans fil de véhicules, appelés VANET, qui consistent de plusieurs véhicules mobiles sans infrastructure préexistante pour communiquer, font actuellement l'objet d'une attention accrue de la part des constructeurs et des chercheurs, afin d'améliorer la sécurité sur les routes ou encore les aides proposées aux conducteurs. Par exemple, ils peuvent avertir d'autres automobilistes que les routes sont glissantes ou qu'un accident vient de se produire.

Dans VANET, les protocoles de diffusion (*broadcast*) jouent un rôle très important par rapport aux messages unicast, car ils sont conçus pour transmettre des messages de sécurité importants à tous les nœuds. Ces protocoles de diffusion ne sont pas fiables et ils souffrent de plusieurs problèmes, à savoir : (1) Tempête de diffusion (*broadcast storm*) ; (2) Nœud caché (*hidden node*) ; (3) Échec de la transmission. Ces problèmes doivent être résolus afin de fournir une diffusion fiable et rapide.

L'objectif de notre recherche est de résoudre certains de ces problèmes, tout en assurant le meilleur compromis entre fiabilité, délai garanti, et débit garanti (Qualité de Service : QdS). Le travail de recherche de ce mémoire a porté sur le développement d'une nouvelle technique qui peut être utilisée pour gérer le droit d'accès aux médias (protocole de gestion des émissions), la gestion de grappe (*cluster*) et la communication. Ce protocole intègre l'approche de gestion centralisée des grappes stables et la transmission des données. Dans cette technique, le temps est divisé en cycles, chaque cycle est partagé entre les canaux de service et de contrôle, et divisé en deux parties. La première partie s'appuie sur

TDMA (Time Division Multiple Access). La deuxième partie s'appuie sur CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance) pour gérer l'accès au medium. En outre, notre protocole ajuste d'une manière adaptative le temps consommé dans la diffusion des messages de sécurité, ce qui permettra une amélioration de la capacité des canaux. Il est implanté dans la couche MAC (Medium Access Control), centralisé dans les têtes de grappes (*CH*, *cluster-head*) qui s'adaptent continuellement à la dynamique des véhicules. Ainsi, l'utilisation de ce protocole centralisé nous assure une consommation efficace d'intervalles de temps pour le nombre exact de véhicules actifs, y compris les nœuds/véhicules cachés; notre protocole assure également un délai limité pour les applications de sécurité, afin d'accéder au canal de communication, et il permet aussi de réduire le surplus (overhead) à l'aide d'une propagation dirigée de diffusion.

Mots-clés : réseau *ad-hoc*, VANET, véhicule, messages de sécurité périodiques, protocoles de diffusion, sans contention.

Abstract

Nowadays, the car has become the most popular mode of transport, but unfortunately its use is accompanied by a number of problems (accidents, pollution, congestion, etc.). These problems will get worse with the increase in the number of passenger cars, despite very significant efforts made to reduce the number of road deaths, which is still very high.

Wireless networks for vehicles called VANET (Vehicle Ad Hoc Networks), were developed when it became possible to connect several mobile vehicles without relying on pre-existing communication infrastructures. These networks have currently become the subject of increased attention from manufacturers and researchers, due to their potential for improving road safety and/or offering assistance to drivers. They can, for example, alert other drivers that roads are slippery or that an accident has just occurred.

In VANETs, broadcast protocols play a very important role compared to unicast protocols, since they are designed to communicate important safety messages to all nodes. Existing broadcast protocols are not reliable and suffer from several problems: (1) broadcast storms, (2) hidden nodes, and (3) transmission failures. These problems must solved if VANETs are to become reliable and able to disseminate messages rapidly.

The aim of our research is to solve some of these problems while ensuring the best compromise among reliability, guaranteed transmission times and bandwidth (Quality of Service: QoS). The research in this thesis focuses on developing a new technique for managing medium access. This protocol incorporates the centralized management approach involving stable clusters. In this technique, time is divided into cycles; with each cycle being shared among the control and service channels, and is divided into two segments. The first is based on TDMA (Time Division Multiple Access) while the second is based on CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) to manage access to the medium. Furthermore, our protocol adaptively adjusts the time consumed in broadcasting

safety messages, thereby improving channel capacity. It is implemented in the MAC (Medium Access Control), and centralized in stable cluster heads that are able to adapt to the dynamics of vehicles. This protocol provides a centralized and efficient use of time intervals for an exact number of active vehicles, including hidden nodes/vehicles. Our protocol also provides time intervals dedicated to security applications for providing access to communication channels, and also reduces overhead via directed diffusion of data.

Keywords: Ad-hoc networks, VANET, Vehicle, Periodic Safety Messages, broadcast protocols, contention-free.

Table des matières

Liste des tableaux

Chapitre 1

Chapitre 2

Chapitre 3

Chapitre 4

Liste des figures

Chapitre 1

Chapitre 2

Chapitre 3

Chapitre 4

Liste des sigles et des abréviations

Acronyme	Description
ACK	Acknowledgement
AFR	Asynchronous Fixed Repetition
AFR-CS	Asynchronous Fixed Repetition with Carrier Sensing
AIFS	A shorter inter-frame space AIFS
AP	Access Point
APR	Asynchronous p-persistent Repetition
APR-CS	Asynchronous p-persistent Repetition with Carrier Sensing
AUs	Applications Units
BG	Back Group
BSS	Basic Service Set
CBR	Constant Bit Rate
CBLR	Cluster-Based Location Routing
CCH	Control Channel
CCP	Cluster Configuration Protocol
CFP	Contention Free Period
CG	Cluster Gateway
CH	Cluster Head
CM	Cluster Member
CP	Contention Period
CSMA/CA	Carrier Sense Multiple Access / Collision Avoidance

CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CTS	Clear To Send
CW	Contention Window
DCF	Distributed Coordination Function)
DDT	Distance Defer Time
DIFS	Distributed Inter Frame Space
DIFS	Distributed Inter Frame Spacing
DISCA	DIrectional Stability-based Clustering Algorithm
DSRC	Dedicated Short Range Communication
DSSS	Direct Sequence Spread Spectrum
EIFS	Extended Inter Frame Spacing
ESS	Extended Service Set
ETSI	European Telecommunications Standards Institute
EYC	Electronic Toll Collection
FB	Fast multi-hop Broadcast
FCC	Federal Communications Commission
FG	Front Group
GPS	Global Positioning System
IBSS	Independant Basic Service Set
IFS	Inter Frame Spac
ITJ	Invite-To-Join
ITS	Intelligent Transportation Systems

IVC	Inter-Vehicle Communication
IVG	Inter-Vehicle Geocast
LLC	Logical Link Control
MAC	Medium Access Control
MANETs	Mobile Ad hoc Networks
MDDV	Mobility-Centric Data Dissemination Algorithm for Vehicular Networks
MHVB	multi-hop vehicular broadcast
NAV	Network Allocation Vector
NS-2	Network Simulator 2
OBU	On'Board Uni
OFDM	Orthogonal Frequency Division Multiplexing
PCF	Point Coordination Function)
PIFS	Priority Inter Frame Spacing
PCH	Primary Cluster Head
SCH	Secondary Cluster Head
QdS	qualité de service
RBM	Role-Based Multicast
RP	Repetition Period
RRAR	Round-Robin Acknowledge and Retransmit
RSUs	Road Side Units
RTJ	Request-To-Join
RTS	Ready To Send

RVC	Roadside-to-Vehicle Communication
SCH	Service Channel
SF	Start Frame
SFR	Synchronous Fixed Repetition
SPR	Synchronous p-persistent Repetition
SBCA	Stability-Based Clustering Algorithm
TDMA	Time Division Multiple Access
TRADE	Rack DEtection
UMB	Urban Multi-Hop Broadcast Protocol
V2I	Véhicule à Infrastructure
V2V	Véhicule à Véhicule
VANET	Vehicule Ad Hoc NETworks
VCS	Virtual Carrier Sense
WAVE	Wireless Ability in Vehicular Environments
WLAN	Wireless Local Area Network

Accord des coauteurs

Dédicace

Je dédie ce mémoire :

À mon père (que Dieu ait son âme)

À ma mère

À mon épouse

À mes enfants

À toute ma famille

À toute ma belle-famille

Remerciements

En préambule à ce mémoire, je souhaitais adresser mes remerciements les plus sincères aux personnes qui m'ont apporté leur aide et qui ont contribué à l'élaboration de ce mémoire ainsi qu'à la réussite de cette formidable année universitaire.

Je tiens à remercier sincèrement Monsieur Abdelhakim Hafid, qui, en tant que directeur de mémoire, s'est toujours montré à l'écoute et très disponible tout au long de la réalisation de ce mémoire, ainsi que pour l'inspiration, l'aide et le temps qu'il a bien voulu me consacrer et sans qui ce mémoire n'aurait jamais vu le jour.

Mes remerciements s'adressent également à Monsieur Racha Ben Ali, pour son aide et son soutien lors de la réalisation de ce projet.

Je n'oublie pas, ma chère Fatima Zahra, pour son soutien quotidien indéfectible et son enthousiasme contagieux à l'égard de mes travaux, comme de la vie en général, ainsi que mes enfants Aya et Ziyad pour leur patience et leur sagesse.

Enfin, j'adresse mes plus sincères remerciements à tous mes proches et amis, qui m'ont toujours soutenu et encouragé au cours de la réalisation de ce mémoire.

Merci à tous et à toutes.

Chapitre 1

Introduction

1.1 Les réseaux sans fil

1.1.1 Qu'est-ce qu'un réseau sans fil

Un réseau sans fil (Wireless network), comme son nom l'indique, est un réseau dans lequel au moins deux terminaux (par exemple, ordinateur portable, PDA, etc.) peuvent communiquer sans liaison filaire.

Le principe des réseaux sans fil est basé sur une liaison utilisant des ondes radioélectriques (radio et infrarouges) au lieu des câbles habituels. Il existe plusieurs technologies qui se distinguent par la fréquence d'émission utilisée ainsi que par le débit et la portée des transmissions.

L'essor des technologies sans fil offre, aujourd'hui, de nouvelles perspectives dans le domaine des télécommunications. L'évolution récente des moyens de la communication sans fil a permis la manipulation de l'information grâce à des unités de calculs portables ayant des caractéristiques particulières (par exemple, une faible capacité de stockage et une source d'énergie autonome) et qui accèdent au réseau à travers une interface de communication sans fil. Le nouvel environnement, dit « environnement mobile », comparativement à l'ancien « environnement statique », permet aux unités de calcul, une libre mobilité sans restriction quant à la localisation des usagers. La mobilité (ou le nomadisme) et le nouveau mode de communication utilisé engendrent de nouvelles caractéristiques propres à l'environnement mobile : une fréquente déconnexion, un débit de communication modeste et des sources d'énergie limitées.

Les réseaux mobiles sans fil peuvent être classés en deux grandes catégories : (1) les réseaux avec infrastructure qui utilisent généralement le modèle de la communication cellulaire dans lequel les clients sans fil sont connectés à un point d'accès (p.ex. répéteur ou commutateur en réseau Ethernet) (Figure 1.1); et (2) les réseaux sans infrastructure ou les réseaux ad hoc dans lesquels les clients sont connectés les uns aux autres sans aucun point d'accès, afin de constituer un réseau point à point (peer to peer) dans lequel chaque machine

joue en même temps le rôle de client et le rôle de point d'accès (p.ex. , l'échange de fichiers entre portables dans un train, dans la rue, au café…) (Figure 1.2). Plusieurs systèmes utilisent déjà le modèle cellulaire et connaissent une très forte expansion à l'heure actuelle (p.ex. les réseaux GSM) mais exigent une importante infrastructure logistique et matérielle fixe

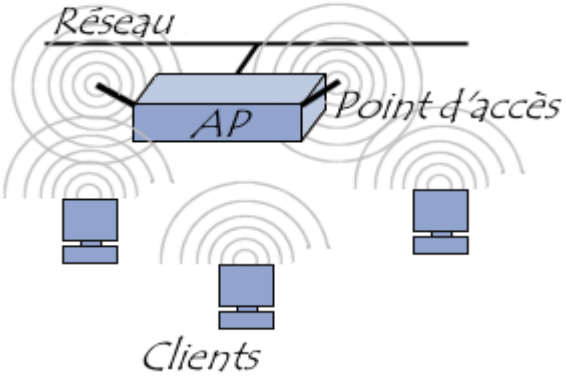


Figure 1.1 - Réseau en mode infrastructure

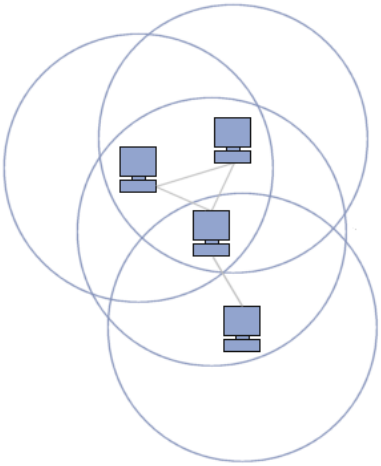


Figure 1.2 - Réseau en mode ad-hoc

1.1.2 Les réseaux avec infrastructure (cellulaires)

En mode avec infrastructure, également appelé le mode BSS (Basic Service Set) certains sites fixes, appelés stations support mobile (Mobile Support Station) ou station de base (SB), sont munis d'une interface de communication sans fil pour la communication directe avec des sites ou des unités mobiles (UM), localisés dans une zone géographique limitée, appelée cellule (voir la figure 1.3).

A chaque station de base correspond une cellule à partir de laquelle des unités mobiles peuvent émettre et recevoir des messages. Alors que les sites fixes sont interconnectés entre eux à travers un réseau de communication filaire, généralement fiable et d'un débit élevé. Les liaisons sans fil ont une bande passante limitée qui réduit sévèrement le volume des informations échangées. Dans ce modèle, une unité mobile ne peut être, à un instant donné, directement connectée qu'à une seule station de base.

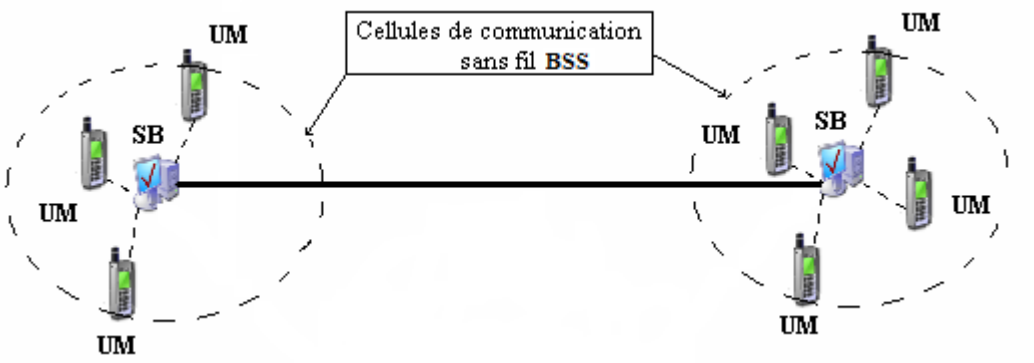


Figure 1.3 - Mode infrastructure avec BSS

Mode de communication de Véhicule à Infrastructure (V2I)

Ce mode de communication permet une meilleure utilisation des ressources partagées et démultiplie les services fournis (par exemple, accès à Internet, échange de données de voiture-à-domicile, communications de voiture-à-garage de réparation pour le diagnostique distant, ...etc.) grâce à des points d'accès RSU (Road Side Units) déployés aux

bords des routes; ce mode est inadéquat pour les applications liées à la sécurité routière car les réseaux à infrastructure ne sont pas performants quant aux délais d'acheminement.

1.1.3 Les réseaux sans infrastructure (AD HOC)

Le réseau mobile sans infrastructure également appelé réseau Ad hoc ou IBSS (Independent Basic Service Set) ne comporte pas l'entité « site fixe », tous les sites du réseau sont mobiles et se communiquent d'une manière directe en utilisant leurs interfaces de communication sans fil (Figure 1.2). L'absence de l'infrastructure ou du réseau filaire composé des stations de base, oblige les unités mobiles à se comporter comme des routeurs qui participent à la découverte et la maintenance des chemins pour les autres hôtes du réseau.

Mode de communication Véhicule à Véhicule (V2V)

Ce mode de communication fonctionne suivant une architecture décentralisée et représente un cas particulier des réseaux ad hoc mobiles. Il est basé sur la simple communication inter-véhicules ne nécessitant pas une infrastructure. En effet, un véhicule peut communiquer directement avec un autre véhicule s'il se situe dans sa zone radio, ou bien par le biais d'un protocole multi-sauts qui se charge de transmettre les messages de bout en bout en utilisant les nœuds voisins qui les séparent comme des relais. Dans ce mode, les supports de communication utilisés sont caractérisés par une petite latence et un grand débit de transmission.

1.2 Les réseaux ad hoc véhiculaires

Les réseaux sans fil de véhicules appelés VANET, pour Vehicule Ad-Hoc NETworks, réalisés par la réunion d'opportunités de plusieurs véhicules mobiles sans infrastructure préexistante pour communiquer, font actuellement l'objet d'une attention accrue de la part des constructeurs et des chercheurs, afin d'améliorer la sécurité sur les routes ou encore les aides proposées aux conducteurs. Par exemple, ils peuvent avertir d'autres automobilistes que les routes sont glissantes ou qu'un accident vient de se

produire. Les réseaux véhiculaires sont une projection des systèmes de transports intelligents (Intelligent Transportation Systems - ITS). Les véhicules communiquent les uns avec les autres par l'intermédiaire de la communication de V2V aussi bien qu'avec les équipements de la route par l'intermédiaire de la communication de V2I. L'objectif est que les réseaux VANETs contribueront à l'élaboration de routes plus sûres et plus efficaces à l'avenir en fournissant des informations opportunes aux conducteurs et aux autorités intéressées. Un exemple de réseau VANET urbain est illustré dans la figure 1.4.

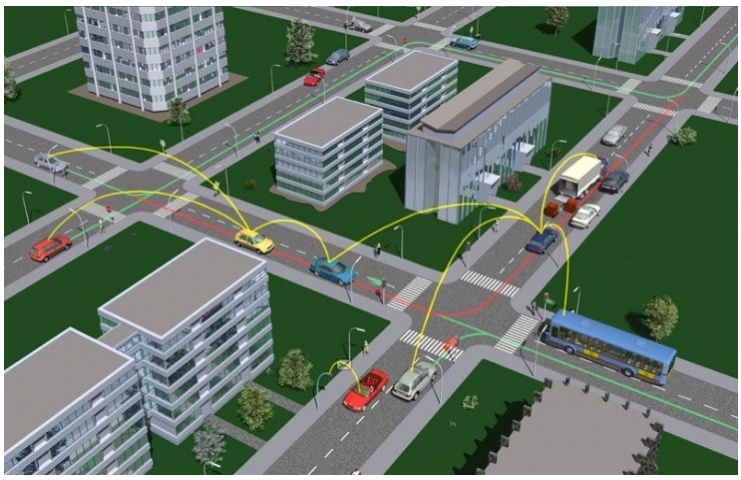


Figure 1.4 - Exemple de réseau VANET (www.car-2-car.org)

1.2.1 Caractéristiques

La réalisation des réseaux VANETs consacrés aux applications embarquées dans les véhicules exigent des techniques et des protocoles qui prennent en compte les incertitudes et les exigences de ces réseaux. Les réseaux VANETs ont des caractéristiques semblables à ceux des réseaux ad-hoc mobiles (MANETs ou Mobile Ad hoc Networks) [18], souvent sous forme de réseaux multi-sauts. Un MANET est un ensemble de nœuds interconnectés par le moyen de communication radio. Ces réseaux sont d'une nature totalement distribuée et totalement dynamique, dans lesquels chaque nœud dois être capable de s'auto-configurer sans la nécessité d'aucune gestion centralisée, ni d'aucune infrastructure préalablement déployée. La figure 1.5 montre un exemple d'un réseau MANET très réduit. Les MANETs

n'ont aucune infrastructure fixe et ils s'appuient plutôt sur les nœuds ordinaires (par exemple, l'ordinateur portable) pour effectuer le routage des messages et des fonctions de gestion de réseau. Cependant, les VANETs peuvent se comporter de façon différente des MANETs classiques, comme le montre le tableau 1. Le comportement des conducteurs, l'absence de contrainte d'énergie (car les équipements sont alimentés à l'énergie des véhicules), la disponibilité d'informations fiables de localisation (par exemple, les cartes routières), des changements fréquents de topologie du réseau en raison de la haute mobilité des véhicules, et la prédictibilité de mobilité des véhicules (par exemple, sur les autoroutes) créent des caractéristiques uniques des réseaux VANETs.

Si nous nous basons sur les caractéristiques indiquées ci-dessus, nous pouvons constater que les liens de communication entre les nœuds dans un réseau VANET sont souvent brisés. Par conséquent, les techniques conçues pour un réseau MANET ne peuvent être directement appliquées dans le contexte de réseau VANET, parce que leurs objectifs de conception ne sont pas valides pour les réseaux à haute mobilité et à un grand nombre de nœuds [19].

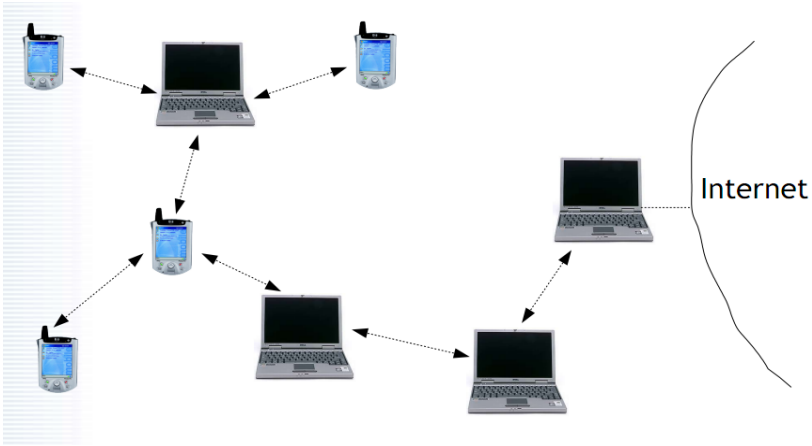


Figure 1.5 - Exemple de réseau MANET

	MANET	VANET
Nombre de nœuds	Habituellement de 100 à 1000	Sans limite, peut être égale à des millions de véhicules
Mobilité	Faible ou moyenne (Vitesse de marche)	Haute (jusqu'à 200km/h)
Trajectoire de nœuds	Aléatoire (p.ex., Waypoint [32])	Déterministe (réseau routier)
Distribution de nœuds	Aléatoire et régulière	Peu dense et irrégulière
Fiabilité	Moyenne	Très élevé
La durée de vie des nœuds (énergie)	Limitée par la vie des batteries dans les nœuds	Illimitée (vie de véhicule)

Tableau 1.1 - Comparaison entre MANET et VANET

1.2.2 Architectures

Les services proposés dans les réseaux VANETs permettent de distinguer plusieurs types de communication (Figure 1.6) [31] : 1) Les communications de V2V, 2) Communications de Véhicule à Infrastructure (V2I) et 3) La combinaison de ces deux types de communications permet d'obtenir une communication hybride.

Un réseau VANET est perçu comme un cas particulier de réseaux MANETs dans lesquels les contraintes d'énergie sont relaxées, et où le modèle de mobilité n'est pas aléatoire, mais prévisible (réseau routier), avec une très forte mobilité. Cette architecture peut être utilisée dans les scénarios de diffusion d'alertes (p.ex., freinage d'urgence, collision, ralentissement, etc.) ou pour la conduite coopérative (p.ex., la priorité au carrefour, la consigne de vitesse au feu, l'indication de raccourcis, l'assistance de changement de voie, le contrôle d'accès, la réservation de places de parking, etc.). En effet, dans le cadre de ces applications pour la sécurité routière, les réseaux à infrastructure montrent leurs limites surtout en termes de délai; aussi le soutien de l'infrastructure n'est pas prévu pour être disponible de façon partout. Il est clair qu'une communication ad-hoc multi-sauts est plus performante qu'une communication passant par un réseau d'opérateurs.

Dans ce mémoire, nous nous concentrons sur les communications V2V, qui jouera un rôle important dans les réseaux VANETs.

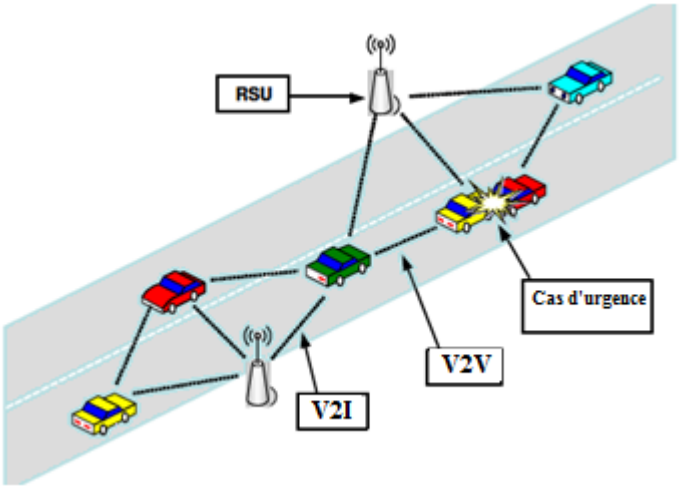


Figure 1.6 - Types de communication dans un réseau de véhicules

1.2.3 Applications

L'intégration des communications et des fonctions informatiques dans les véhicules est faite dans le but de réaliser la communication des véhicules. Le but principal de VANET est de fournir : (1) La prévention et la sécurité routière, les VANETs peuvent améliorer la prévention routière de façon significative, en alertant le conducteur d'une situation dangereuse. Ils permettent également d'élargir le champ de perception du conducteur à celui de l'ensemble des véhicules avec lesquels il peut communiquer, alertes en cas de violations imminentes ou des feux de circulation, notification en cas de freinage urgent; (2) L'optimisation du trafic, le trafic automobile peut être grandement amélioré grâce à la collecte et au partage des données collectées par les véhicules. Une voiture peut, par exemple, être avertie d'un embouteillage, d'un éboulement de rochers ou d'un accident avant qu'elle ne s'en approche, ce qui lui permet de ne pas emprunter la route qui y mène;

(3) Le confort des passagers, les réseaux véhiculaires peuvent aussi améliorer le confort des passagers. En dehors de la sécurité routière et de l'efficacité, les VANETs peuvent également soutenir d'autres applications comme le télépéage, l'accès Internet, le parking, le divertissement instructif (infotainment), les mises à jour du trafic, etc. Pourtant, la sécurité est restée le principal objectif de la recherche VANET. Une littérature abondante est disponible sur le classement des applications VANET [16,17].

Afin de faire communiquer les véhicules, il nous faut un système facile à mettre en place et viable en extérieur. Un dispositif électronique spécial sera placé à l'intérieur de chaque véhicule, qui fournira la connectivité ad-hoc de réseau pour les passagers. Ce réseau tend à fonctionner dans n'importe quelle communication d'infrastructure, de client ou de serveur. Chaque véhicule embarque une plateforme de communication appelée OBU (On Board Unit). Cette plateforme est utilisée par une ou par plusieurs applications appelées AUs (Applications Units). Quant aux points d'accès disposés le long des routes et constituant l'infrastructure fixe, ils sont nommés RSUs (Road-Side Units). Les véhicules équipés des OBU seront des nœuds dans le réseau ad-hoc et ils pourront recevoir et transmettre par relais d'autres messages dans le réseau sans fil. L'OBU est composé de : (1) Émetteur; (2) Antenne omnidirectionnelle; (3) Processeur; (4) Appareil GPS; (5) Cartes numériques; et (6) Capteurs.

1.3 La motivation/problématique

Bien que la recherche dans le domaine des réseaux VANETs soit récente, elle est vaste et diversifiée. En effet, des travaux de recherche conséquents sont actuellement en train d'être effectués par des chercheurs dans le but de normaliser un ou plusieurs protocoles MAC qui peuvent êtres utilisés pour la communication dans les réseaux VANETs; aujourd'hui, il semble que c'est le standard IEEE 802.11p [10] qui sera adopté pour ce type de communication. En outre, de nombreux autres travaux (par exemple, [5], [6], [7] et [8]) portant sur des protocoles de diffusion spécifiques au V2V ont été proposés pour garantir la qualité de service (QdS) pour les applications de diffusion des messages de

sécurité, soutenir la capacité de prioriser et de gérer plusieurs types de messages, etc.. Cependant, le support de la QoS demeure un défi dans les réseaux VANETs.

Les protocoles de diffusion (*broadcast protocols*) joueront un rôle très important par rapport aux messages unicast (point à point) dans les réseaux VANETs, car ils sont conçus pour communiquer des messages de sécurité importants pour tous les nœuds. Ces protocoles de diffusion ne sont pas fiables et ils souffrent de plusieurs problèmes, à savoir : (1) Tempête de diffusion (*broadcast storm*) ; (2) Nœud caché (*hidden node*) : Deux nœuds peuvent entendre l'activité d'un troisième nœud mais ne peuvent pas s'entendre mutuellement pour cause de distance ou de présence d'obstacles qui les empêche de communiquer entre eux ; (3) Échec de la transmission; (4) Congestion, dans des réseaux très denses, causés par le fait que tous les nœuds partagent le même canal. Par conséquent, il y a un besoin pressant de développer de nouveaux protocoles de diffusion dans les réseaux VANET. De plus, de nouvelles approches pour la sécurité de la communication doivent être conçues pour adapter les besoins spécifiques du réseau et garantir des services fiables et dignes de confiance. Ces problèmes doivent être résolus pour fournir une diffusion fiable et rapide.

L'objectif de ce travail de mémoire est de contribuer à la définition de solutions pour le support de la QdS, telles que la fiabilité, le délai, le débit dans VANET ainsi qu'à l'analyse des rendements de cette solution. Le travail se situe plus précisément au niveau de la sous-couche MAC (Medium Access Control) du standard IEEE 802.11p. D'abord, il convient d'adapter le protocole de diffusion le plus approprié aux réseaux VANETs, afin de prendre en considération les paramètres de QdS.

1.4 Les contributions

Dans notre recherche, nous nous sommes concentrés sur les protocoles de diffusion dans le but de fournir une faible latence et un taux élevé de livraison des messages de sécurité et de maximiser le débit pour le trafic non-sécurité sur les communications de V2V. L'idée principale derrière notre approche consiste à intégrer l'algorithme de

clustering (“regroupement”) aux protocoles MAC fondés sur la contention et les protocoles MAC sans contention en vertu de l'architecture DSRC (standard dédié aux communications véhiculaires).

Bien que les protocoles de diffusion (par exemple, [5], [6], [7], [8]) améliorent les performances de VANETs en réduisant le délai et / ou en augmentant le taux de livraison de messages, ils prennent en considération la méthode d'accès au support fondée sur la contention. Celle-ci nécessite des mécanismes complexes (pour résoudre la contention de diffusion pour l'accès au support) qui luttent pour le maintien de bonnes performances en conditions de charge très élevée et surtout pour satisfaire les contraintes en temps réel d'applications de sécurité. En fait, le mécanisme de Détection Virtuelle de la Porteuse (VCS : Virtual Carrier Sense) standard ne peut pas être utilisé pour prévenir les collisions causées par la diffusion des messages de sécurité. En outre, le mécanisme utilisé dans UMB [5] par exemple, ne peut pas garantir une réception sans collision. Dans UMB les requêtes de réservation ajoutent un surcoût considérable et inutile pour la diffusion de messages de sécurité périodique.

Plutôt que de s'appuyer sur un protocole fondé sur la contention MAC, nous proposons, un nouveau protocole de réservation implémenté en particulier et sur mesure pour les applications de diffusion périodique; ce protocole représente notre première contribution et qui a été publiée dans [13]. Cette contribution comprend (1) un nouveau mécanisme VCS [13] dans lequel une seule requête est utilisée durant la période de stabilité, la période pendant laquelle les nœuds restent dans la même grappe et le chef de grappe ne change pas son état (on suppose une structure groupée du réseau de véhicules), pour réserver un intervalle de temps (Time slot) pour une diffusion sans contention des messages de sécurité périodiques; (2) a Time Slot Scheduling Algorithm [13], exécuté par les véhicules chefs de grappe, alloue des intervalles de temps aux véhicules demandant, ce qui permet à la fois d’assurer une faible latence bornée, de réduire la probabilité de collisions entre les nœuds qui ne sont pas en visibilité (problème de nœud caché), et de partager efficacement et équitablement ce canal. Aussi les véhicules chefs de grappe, ajoutent un champ spécifiant l'une des quatre orientations possibles pour le transfert de

diffusion (EST, OUEST, NORD ou du SUD). Cela permettra d'éviter des diffusions inutiles des messages de sécurité qui participent à l'augmentation du niveau de congestion. Les messages d'urgence sont prioritaires par rapport aux messages de sécurité périodiques en utilisant un court espace inter-trame; et (3) a Dynamic CFP Channel Operation Algorithm [13], contrairement au statique utilisé dans IEEE 802.11p; il maximise le débit pour le trafic non-sécurité sur le canal de service tout en garantissant des délais de livraison courts et des taux élevés sur le canal de contrôle.

Dans [13], nous avons développé un protocole dans lequel on a supposé une structure groupée du réseau de véhicules qui intègre l'approche de gestion centralisée des grappes stables. Comme deuxième contribution, soumise à IEEE ICC [36], nous proposons une approche, appelée stability-based clustering algorithm (SBCA), qui permet de construire une structure groupée du réseau. SBCA prend en considération les caractéristiques de mobilité, le nombre de voisins, et la durée de leadership (chef de grappe) en vue de fournir une structure de grappes plus stable et ainsi réduire les frais d'entretien (sur débit) des grappes.

Ce mémoire est présenté sous forme d'articles. Le premier article, *A Contention-Free Broadcast Protocol for Periodic Safety Messages in Vehicular Ad-Hoc Networks* a été publié dans The 35th Annual IEEE Conference on Local Computer Networks (LCN), 2010. Tandis que le second article, *A new stability-based clustering Algorithm (SBCA) for VANETs*, qui a été soumis à IEEE ICC Conference, 2011.

Le reste de ce mémoire est organisé comme suit.

Dans le chapitre 2, nous présentons un aperçu de la documentation sur les techniques utilisées permettant la diffusion des messages sur des réseaux VANETs à fiabilité élevée ainsi que les algorithmes qui les implémentent. Dans le chapitre 3, nous présentons sous forme d'article notre proposition de protocole de diffusion des messages de sécurité sans collision dans les réseaux VANETs. Dans le chapitre 4, nous proposons un nouvel algorithme de clustering basé sur la stabilité pour VANET. Et nous concluons ce travail en établissant quelques perspectives de recherche.

Chapitre 2

Revue de littérature

Presque toutes les applications présentées dans la Sec 1.1.3 dépendent de l'envoi des messages aux véhicules voisins explicitement sans la détermination de leur identité, qui est une diffusion dans sa nature. Notez que, toutes les techniques de signalisation qui sont actuellement déployées dans les véhicules (par exemple, les feux de freinage et de virage à droite/gauche) sont considérées comme une diffusion. Avec la technologie VANET, ces signaux seront échangés directement entre les véhicules eux-mêmes. Cela permettra d'accroître la sensibilisation des conducteurs aux causes et aux conséquences des accidents de la route et ainsi le confort.

Dans ce chapitre, nous passons en revue certains travaux réalisés dans le contexte de la diffusion des messages dans les réseaux VANETs. Nous commençons tout d'abord par une présentation du standard IEEE 802.11 dans le cadre des réseaux VANETs. Ensuite, nous étudions l'utilisation de la norme IEEE 802.11 pour les communications de V2V. Dans une troisième partie, nous présentons les différentes catégories de protocoles de diffusion et les problèmes liés à la diffusion dans les réseaux VANETs. Enfin, dans la dernière partie, nous allons présenter brièvement quelques solutions de diffusion de données dans les réseaux VANETs.

2.1 Généralités sur le IEEE 802.11

2.1.1 Présentation de la norme

La norme IEEE 802.11 [12] est une norme internationale standard décrivant les caractéristiques d'un réseau local sans fil (WLAN). La norme IEEE 802.11 est en réalité la norme initiale offrant des débits de 1 ou de 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 802.11n, appelées normes 802.11 physiques) ou de préciser des éléments, afin d'assurer une meilleure sécurité ou une meilleure interopérabilité.

2.1.2 Topologies du réseau IEEE 802.11

Par rapport au modèle OSI, l'IEEE 802.11 (Figure 2.1) ne concerne qu'une partie de; (1) La couche de liaison de données, constitué de deux sous-couches : le contrôle de la liaison logique (Logical Link Control, ou LLC) et le contrôle d'accès au support (Media Access Control, ou MAC); (2) La couche physique (notée parfois couche PHY), proposant trois types de codages de l'information; (3) reste donc entièrement compatible avec les couches supérieures.

La partie de la norme 802.11 qui nous intéresse est la partie MAC. Pour la partie physique nous utiliserons un codage DSSS (Direct Sequence Spread Spectrum) couplé à une antenne omnidirectionnelle. Il y a trois modes de fonctionnement des réseaux sans fils 802.11: (1) Le mode ad-hoc (ou IBSS, Independant Basic Service Set), pas d'infrastructure fixe, interconnexion directe entre les équipements; (2) Le mode infrastructure basique (BSS, Basic Service Set), présence d'un point d'accès (AP, Access Point) qui peut aussi permettre l'interconnexion à Internet, pas de communication directe entre les équipements; et (3) Le mode infrastructure étendu (ESS, Extended Service Set), présence de plusieurs points d'accès qui peuvent aussi permettre l'interconnexion à Internet, hand-off au niveau MAC entre les différents points d'accès, la mobilité est transparente aux couches supérieures. Nous nous intéresserons seulement au mode ad-hoc car une des particularités des VANET est que chaque nœud est indépendant et qu'aucun ne peut jouer le rôle de point d'accès.

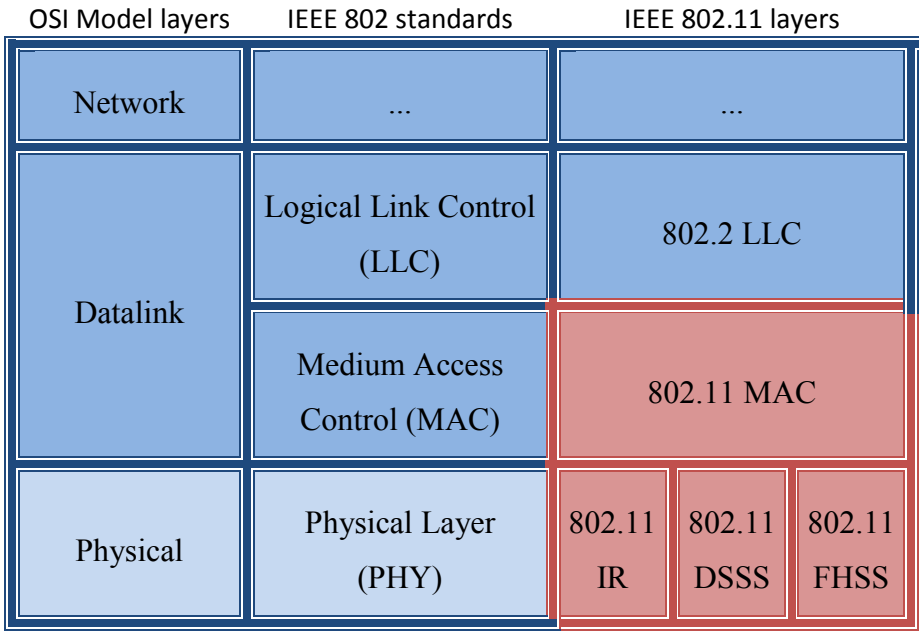


Figure 2.1 - Place du 802.11 dans la pile réseau

2.1.3 Protocoles d'accès dans l'IEEE 802.11

L'architecture MAC de la norme IEEE 802.11 fait coexister deux méthodes d'accès appelées DCF (Distributed Coordination Function) et PCF (Point Coordination Function). La méthode PCF donne un accès sans contention fondé sur des élections alors que la méthode DCF donne un accès avec contention. Le mode PCF peut être utilisé en alternance avec le mode DCF, pendant des périodes alternées qu'on appelle période de contention (CP) et période sans contention (CFP). Nous allons détailler la méthode d'accès DCF, qui concerne le cas d'utilisation le plus courant. Il s'agit d'un même algorithme exécuté par toutes les stations pour qu'elles puissent posséder le canal. La DCF est fondée sur la politique CSMA/CA (Carrier Multiple Acces with Collision Avoidance). Contrairement au réseau local Ethernet classique utilisant le CSMA/CD (Carrier Sense Multiple Access with Collision Detection), le réseau sans fil 802.11 propose la méthode CSMA/CA. La différence provient du fait que pour les premiers réseaux, les machines utilisent le même support physique et peuvent écouter plus efficacement le médium alors que pour les

réseaux sans fil, les stations peuvent ne pas s'entendre. La station qui a des données à transmettre écoute le réseau. Dans le cas où le support est encombré, la transmission est différée. Dans le cas contraire, si le média est libre pendant un temps donné (appelé DIFS pour Distributed Inter Frame Space), alors la station peut émettre. Les autres stations du réseau seront en état de veille durant la durée NAV (Network Allocation Vector). (Figure 2.2)

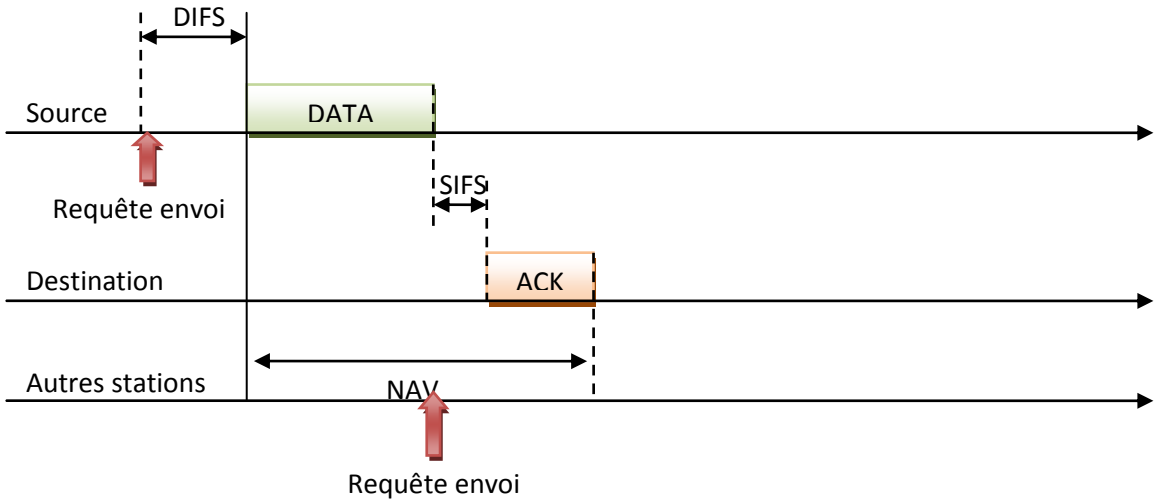


Figure 2.2 - Échange de données pour la méthode d'accès CSMA/CA de base

Au premier temps de la définition du CSMA/CA, la station émet les données lorsque le canal est libre et attend la réception d'un ACK de la station destination. L'ACK reçu, la station émettrice comprendra que la transmission a été faite sans collisions. Dans le cas contraire et à l'expiration d'un temporisateur, l'émetteur retransmet la trame victime de collisions. Le CSMA/CA a pris une nouvelle spécification en introduisant le mécanisme de détection virtuelle. Il s'agit dans ce cas du protocole d'accès à quatre étapes RTS/CTS/DATA/ACK. Ce mécanisme a été introduit pour remédier aux problèmes des stations cachées (Figure 2.3). D'après le cas de la Figure 2.3, les nœuds A et B veulent

émettre un paquet vers le nœud C. Comme ils ne sont pas directement à portée, il se peut qu'ils émettent en même temps et il va en résulter une collision au niveau du récepteur C.

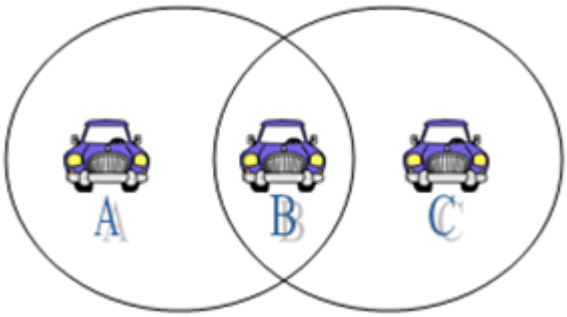


Figure 2.3 - Problème de noeud caché

C'est ainsi que se présentent les problèmes du CSMA/CA original auquel il a fallu ajouter un mécanisme adéquat permettant, d'un côté de diminuer les collisions et d'un autre augmenter le débit et optimiser l'utilisation du canal. À ce fait, le mécanisme du RTS/CTS/DATA/ACK a été introduit. (Figure 2.4)

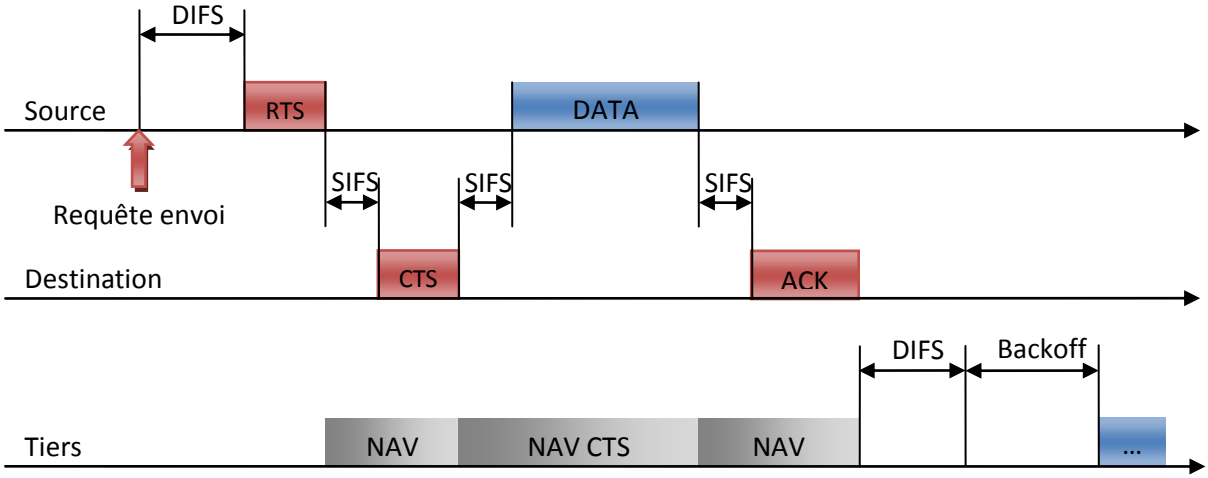


Figure 2.4 - Échange de données pour la méthode d'accès CSMA/CA avec le mécanisme de détection virtuelle

La première étape du mécanisme consiste dans le fait que la station qui veut émettre écoute le canal et s'il est libre elle transmet un message appelé Ready To Send (signifiant prêt à émettre) contenant des informations sur le volume des données qu'elle souhaite émettre et sa vitesse de transmission (l'information NAV (RTS)). La temporisation d'émission, appelé NAV (Network Allocation Vector) permet d'éviter les collisions en retardant les émissions de toutes les stations qui détectent que le support est occupé. Le récepteur répond par un Clear To Send (CTS, signifiant que le champ est libre pour émettre et donc signalant la durée NAV (CTS)), puis la station source commence l'émission des données (l'information NAV (DATA)). À la réception de toutes les données émises par la station, le récepteur envoie un accusé de réception (ACK). Toutes les stations avoisinantes patientent, alors, pendant un temps qu'elles considèrent être celui nécessaire à la transmission du volume d'information à émettre à la vitesse annoncée. Pour 802.11 utilisant le mécanisme de détection virtuelle, les collisions se produisent au niveau du RTS. Lorsque le RTS n'est pas reçu. Le RTS sera retransmis comme cause de collisions ou de pertes. Dans la norme 802.11 il existe trois espaces inter-trame IFS (Inter Frame Spacing), qui sont déterminés par trois intervalles de temps entre l'émission de deux trames : (1) SIFS (Short Inter Frame Spacing) est le plus court espace inter-trames. Il sépare les transmissions d'un unique dialogue, par exemple entre une trame émise et son ACK; (2) PIFS (Priority Inter Frame Spacing) est l'espace inter-trames utilisé par l'AP pour qu'il possède une priorité d'accès au canal. PIFS = SIFS + 1 Time slot; (3) DIFS (Distributed Inter Frame Spacing) est l'espace inter-trames utilisé par les stations pour accéder au support. DIFS = PIFS + 1 Time slot; (4) EIFS (Extended Inter Frame Spacing) est l'espace inter-trames le plus long utilisé si la station reçoit une trame erronée. Lors de la transmission, les autres stations en écoute constatent une émission et déclencheront pour une durée fixée leur indicateur NAV (Network Allocation Vector) et utiliseront cette information pour retarder toute transmission prévue. Dans le cas où le médium est occupé, la station reporte sa transmission jusqu'à ce que le médium redevienne libre. Une fois que le médium est redevenu libre, chaque station attend une durée fixe DIFS suivie d'une durée aléatoire

appelée backoff time, avant de commencer à émettre, si le canal est toujours libre. (Figure 2.5)

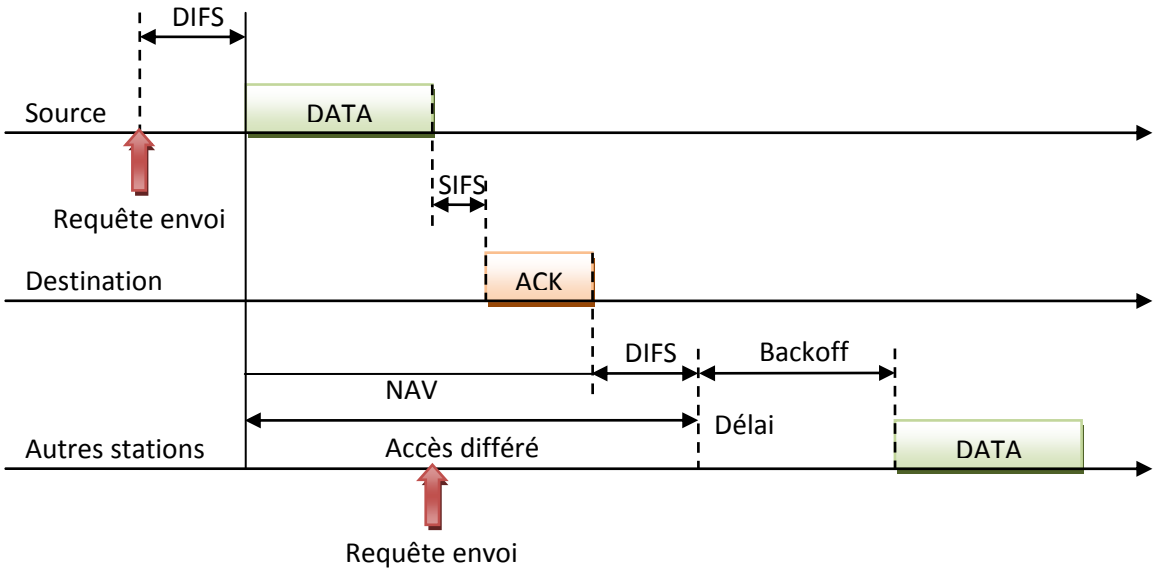


Figure 2.5 - Illustration de l'algorithme de Backoff

L'algorithme de Backoff utilise la notion de fenêtre de contention CW. Le CW correspond au nombre maximum pour la sélection aléatoire. CW prend ses valeurs entre CWmin et CWmax. Le 802.11 affecte une valeur de CWmax égale à 1023 et à CWmin une valeur de 15 et ceci dans le cas du 802.11a et g. La procédure de Backoff peut être déclenchée pour une première transmission. Cela veut dire que la station voulant émettre trouve le canal occupé pour une période d'écoute DIFS. Dans ce cas, la procédure suivante est exécutée : (1) Initialisation de CW avec CWmin ; (2) Si le canal devient libre, après un DIFS la station commence à décrémenter son temporisateur Time Slot par Time Slot ; (3) Si le Backoff_Timer est égal à 0, la station émet. Si au cours de la décrémentation, une autre station émet, la station en question bloque son Backoff_Timer et ne pourra le décrémenter que si la station finit d'émettre (canal libre avec une attente de la durée DIFS). Lorsqu'il se produit une collision ou une perte d'acquittement de niveau liaison, l'algorithme de Backoff consiste à augmenter exponentiellement CW.

2.2 IEEE 802.11 et les communications inter-véhicules

2.2.1 Les préliminaires de VANETs

Penchons-nous d'abord sur l'histoire du développement et de la mise en place de VANET. En octobre 1999, la Commission Fédérale des Communications (*Federal Communications Commission* FCC)) américaine a alloué une bande de fréquence dans les 5.9 GHz pour les applications liées au domaine des systèmes de transport intelligents. Le standard DSRC (Dedicated Short Range Communications) utilise cette bande fréquence, il est basé sur la couche physique de la norme IEEE 802.11a ainsi que sur la couche MAC de la norme IEEE 802.11e [22]. La portée théorique de communication est de 1000 mètres, mais en pratique, elle se situe plutôt aux alentours de 200 mètres [23]. Le principal avantage du DSRC est le temps de latence très bas, sous les 100 millisecondes, ce qui est idéal pour les applications de sécurité qui demandent un délai dans cette plage.

2.2.2 Objectifs de diffusion

Tout protocole de diffusion devrait satisfaire à tous les objectifs suivants: (1) Haute fiabilité, l'émetteur doit être reconnu de la diffusion du message sur le véhicule(s) destiné; (2) Faible temps de latence, la durée de la première tentative de transmission à la fin de la phase de diffusion, doit être aussi faible que possible; (3) Faible probabilité de collision, le protocole devrait souffrir de la collision au minimum possible, par conséquent, une plus grande fiabilité et une latence plus faible; (4) Problème de nœud caché, les collisions à la réception causées par le nœud caché doivent être évitées.

2.2.3 DSRC et IEEE 802.11p

Pour communiquer de véhicule à véhicule au sein d'un peloton, l'ASTM (American Society for Testing and Materials) a adopté en 2002 une norme sans-fil appelée DSRC (Dedicated Short Range Communication) [26]. En 2003, le groupe de travail IEEE a repris ces travaux pour définir un nouveau standard dédié aux communications inter-vehicules, nommé WAVE (Wireless Ability in Vehicular Environments) et aussi connu sous le nom

de IEEE 802.11p [25]. Cette norme utilise le concept de multi-canaux afin d'assurer les communications pour les applications de sécurité et les autres services du Transport Intelligent.

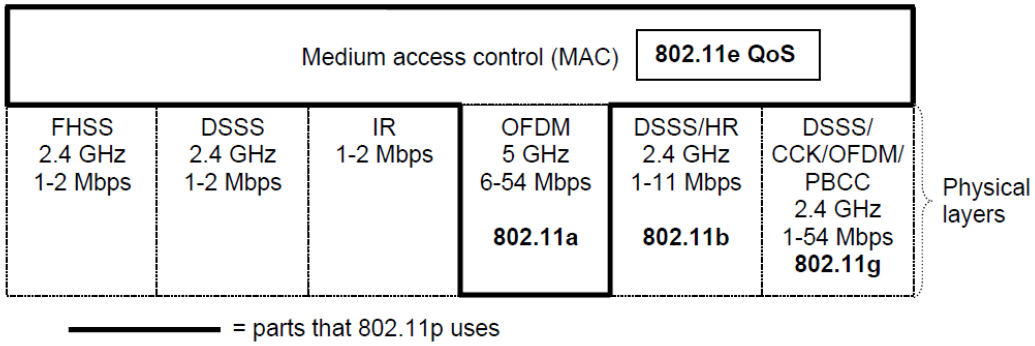


Figure 2.6 - Un aperçu de la partie de la norme IEEE 802.11 utilisé par 802.11p

IEEE 802.11p est généralement une variante personnalisée de l'IEEE 802.11a couche PHY (Figure 2.6) spécialement adaptée pour permettre un fonctionnement à faible charge dans le spectre DSRC. Il combine les parties de la norme d'origine avec l'amendement 802.11e MAC pour le support de QoS (Figure 2.6). Pour plus de détails, les auteurs de [15] présentent les concepts, les applications et les caractéristiques de performance derrière ces technologies utilisées pour les communications V2V.

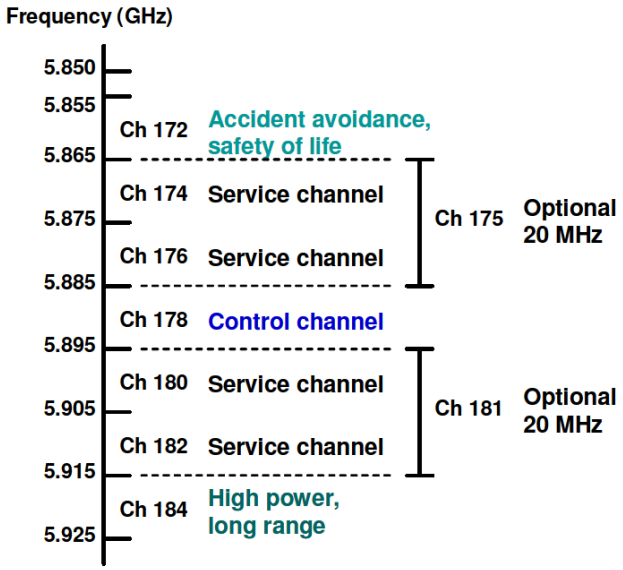


Figure 2.7 - Attribution des canaux DSRC en Amérique du Nord

DSRC œuvre dans la bande de fréquence des 5.9 GHz (Europe et États-Unis) ou 5.8 GHz (Japon). Cette bande de fréquence est définie en Europe et aux États-Unis respectivement par l'ETSI (European Telecommunications Standards Institute) et le FCC (Federal Communication Commission). Elle est généralement segmentée en 7 canaux de 10 MHz chacun, l'ensemble des canaux se répartissant fonctionnellement en 1 canal de contrôle et 6 canaux de service (Figure 2.7). Le canal de contrôle est réservé à la transmission des messages de gestion du réseau et des messages de très haute priorité a l'instar des certains messages critiques lies à la sécurité routière. Les 6 autres canaux sont quant à eux dédiés a la transmission des données des différents services annoncés sur le canal de contrôle. Plus largement, DSRC regroupe une série de standards et de protocoles dédiés aux communications véhiculaires. Certains de ces standards et protocoles sont en cours de définition aux États-Unis, notamment au sein de l'IEEE. Ainsi, DSRC se fonde sur une couche physique et une couche MAC définies dans le standard IEEE 802.11p (WAVE). Cette couche physique est dérivée de l'IEEE 802.11a. Elle est capable d'offrir un débit entre 6 et 27 Mbps (pour des distances jusqu'a 1000 mètres) avec une modulation de type OFDM (Orthogonal Frequency Division Multiplexing) (Figure 2.8). De même, la

couche MAC du 802.11p reprend le principe du CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) développé dans le protocole MAC de l'IEEE 802.11, avec un complément apportant la gestion de la qualité de service et le support du protocole de marquage de priorité. En effet, la couche MAC du WAVE est gérée en utilisant des priorités d'accès comme la norme IEEE 802.11e. Ainsi, la fenêtre de contention est calculée selon les quatre priorités disponibles.

Modulation	Coded bits per periodic wave form	Coded bits per OFDM symbol	Coding rate	Data bits per OFDM symbol	Data rate for a 10 MHz wide channel (Mbps)	SINR threshold for frame reception (dB)
BPSK	1	48	1/2	24	3	5
BPSK	1	48	3/4	36	4.5	6
QPSK	2	96	1/2	48	6	8
QPSK	2	96	3/4	72	9	11
16-QAM	4	192	1/2	96	12	15
16-QAM	4	192	3/4	144	18	20
64-QAM	6	288	2/3	192	24	25
64-QAM	6	288	3/4	216	27	N/A

Figure 2.8 - Débit de données pris en charge dans IEEE 802.11p

Le reste de la pile protocolaire de DSRC se situant entre la couche liaison et la couche application est en cours de standardisation par le groupe de travail IEEE 1609 [14]. Par conséquent, IEEE 1609 est un standard pour les couches hautes sur lequel IEEE 802.11p se fonde. La famille des standards IEEE 1609 pour WAVE, se décompose en quatre standards (Figure 2.9): pour la gestion des ressources (IEEE 1609.1 - WAVE Resource Manager), pour la sécurisation des messages (IEEE 1609.2 – WAVE Security Services for Applications and Management Messages), pour les services de niveau réseau et transport incluant l’adressage, le routage (IEEE 1609.3 – WAVE Networking Services),

et pour la coordination et la gestion des sept canaux DSRC (IEEE 1609.4 - WAVE Multi-Channel Operation).

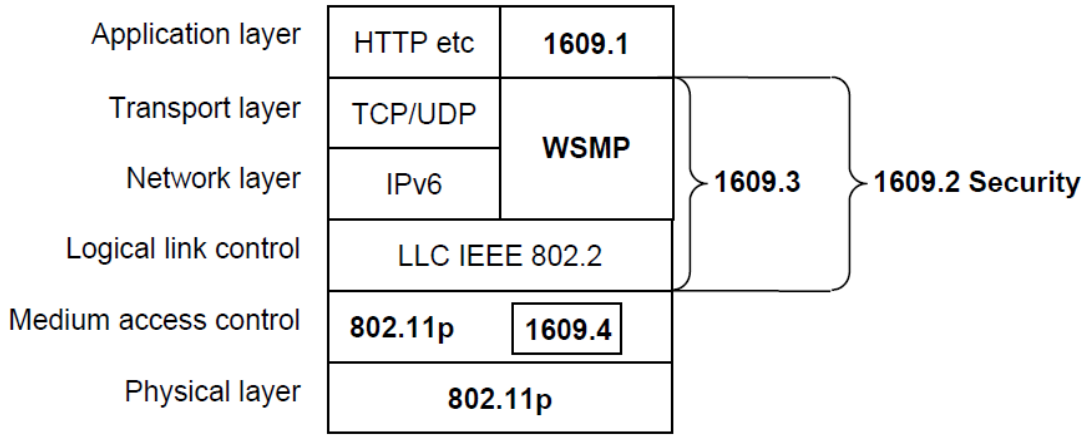


Figure 2.9 - Présentation de pile de protocole WAVE

2.2.4 Conclusion

Les protocoles de diffusion (*broadcast protocols*) joueront un rôle très important par rapport aux messages unicast (point à point) dans les réseaux VANETs, car ils sont conçus pour communiquer des messages de sécurité importants pour tous les nœuds (par exemple, [5], [6], [7] et [8]). Si nous nous fondons sur la norme IEEE 802.11 indiquées ci-dessus, nous pouvons constater que ces protocoles de diffusion ne sont pas fiables et ils souffrent de plusieurs problèmes, à savoir : (1) Aucune retransmission n'est possible pour une transmission par diffusion échouée, à cause du manque de confirmation explicite pour les trames de diffusion. Pour pouvoir détecter les transmissions unicast échouées, la couche MAC 802.11 utilise des acquittements qui confirment la bonne réception d'une trame. La non-réception de l'acquittement (ACK) permet à l'émetteur d'en déduire la perte du paquet expédié qui sera alors réémis. Si les acquittements avaient été utilisés pour les diffusions, un problème connu comme le « ACK problème d'explosion » existerait. Chaque nœud de réception renvoie un ACK à l'émetteur. Le « ACK problème d'explosion » aboutit à une

plus grande probabilité d'apparitions de collisions; (2) Suite à la non-utilisation de l'échange de RTS/CTS, le réseau explose à cause du problème de la station caché; (3) La taille de la fenêtre de contention, CW, ne peut changer, parce qu'il n'y a pas de reprise au niveau MAC pour les trames de diffusion. Puisqu'il n'y a aucune détection de transmissions de diffusion échouées, la taille du CW échoue à changer le trafic de diffusion comme il le fait pour le trafic unicast. Les nœuds transmettront toujours avec CWmin pour la fenêtre de backoff.

L'utilisation de logiciel de simulation NS2 (Network Simulator 2) nous a permis d'effectuer des tests mettant en place des réseaux allant de deux à cent véhicules. Ces expériences nous ont permis d'évaluer les performances de la norme ainsi que de comprendre les problèmes qui surviennent lors de la communication inter véhicules. Par conséquent, les techniques conçues pour une communication unicast dans le réseau ad-hoc classique ne peuvent être directement appliquées dans le contexte de communications de diffusion dans les réseaux de véhicules à haute mobilité et à un grand nombre de nœuds [19]. Il est important de soulever ces problèmes pour fournir une diffusion extrêmement fiable et rapide.

2.3 Présentation des protocoles de diffusion déjà existants

Dans les réseaux ad-hoc, une diffusion est dite fiable (reliable) lorsqu'elle permet de transmettre l'information à l'ensemble des nœuds joignables. D'un point de vue local, chaque nœud doit alors garantir que l'ensemble de son voisinage est contacté par le message de diffusion. À l'opposé, un protocole de diffusion est dit non fiable (unreliable) lorsque l'algorithme ne garantit pas la diffusion de l'information à l'ensemble des nœuds joignables.

Toutes les contributions proposées (par exemple, [29], [24], [30], [11], [20] et [5]) essaient de résoudre juste deux questions; la première question est « Comment livrer le message de diffusion aux nœuds voisins, dans la portée de communication, avec la plus grande fiabilité possible? ». La deuxième question est « Comment livrer le message de

diffusion avec la plus grande fiabilité possible au réseau entier? ». Différentes catégories de protocoles de diffusion sont désignées pour répondre à ces deux questions. Pour la première question, les catégories des protocoles désignés sont: (1) «Rediffusion» [29] où le nœud émetteur retransmet le même message plusieurs fois; (2) «Acquittement Sélectif» [30] où l'émetteur exige Acquittement (ACK) à partir d'un petit ensemble de ses voisins; et (3) «Modification des paramètres» [11] où l'émetteur change de paramètres de transmission selon l'état attendu du réseau. Pour la deuxième question, les catégories des protocoles désignés sont : (1) «Les inondations» [20] où chaque nœud est responsable de déterminer s'il va retransmettre le message ou non, et (2) «le relais unique» [5] où l'émetteur est responsable de déterminer le nœud du saut suivant. Bien que les deux questions se ressemblent les unes les autres, la première est utilisée avec des applications liées à des voisins directs (par exemple, l'évitement des collisions) et la deuxième est utilisée avec des applications liées à l'ensemble du réseau (gestion du trafic, par exemple).

La figue 2.10 montre les différentes catégories de protocoles de diffusion.

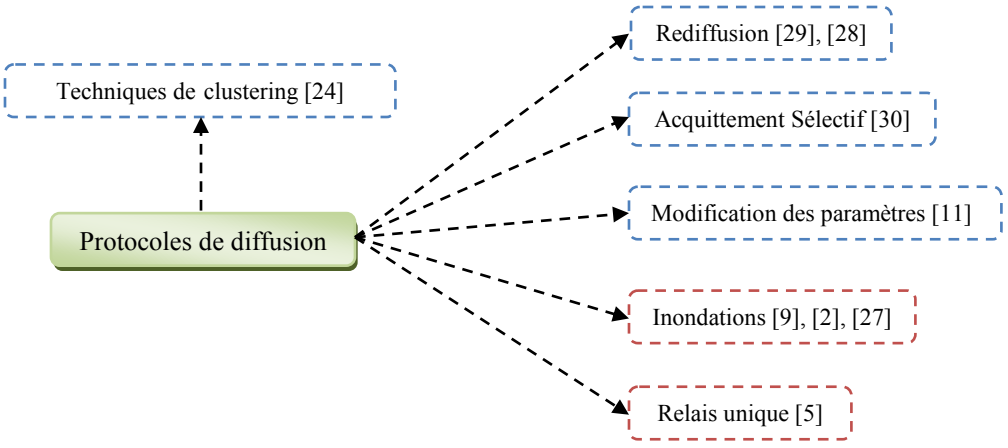


Figure 2.10 - Différentes catégories de protocoles de diffusion

L'apparition de VANETs a ouvert un défi pour la recherche de nouveaux protocoles de diffusion fiables avec des contraintes de temps réel, destinés à désservir plusieurs applications liées à la sécurité publique. Le but est de concevoir un protocole qui peut diffuser un message provenant d'une source unique pour chaque nœud dans sa portée de transmission avec la plus grande fiabilité possible et une latence minimale. Les indicateurs de performance clés pour les protocoles fiables sont les suivants: (1) Taux de réussite: le nombre de nœuds qui ont reçu avec succès la diffusion, divisé par le nombre de nœuds dans la portée de communication de l'émetteur; et (2) Temps de latence: le temps total nécessaire dans une phase de diffusion unique. Les chercheurs ont utilisé trois méthodes pour augmenter la fiabilité de diffusion: «Rediffusion», «Accusé de réception sélectif» et «Modification des paramètres». Les chercheurs ont aussi utilisé deux méthodes pour augmenter la fiabilité de dissémination: «Inondations» et «Relais unique».

2.3.1 Protocoles MAC de diffusion sans contention (reposant sur TDMA)

Dans les protocoles de diffusion fondés sur la méthode Accès Multiple par Répartition dans le Temps (AMRT ou TDMA Time Division Multiple Access) [24, 34, et 35] le temps est divisé en trames (périodiques) et chaque trame se compose d'un certain nombre de slots de temps. À chaque nœud est attribué un ou plusieurs slots par trame selon un certain algorithme d'ordonnancement. Un nœud ne peut pas accéder au canal pendant l'intervalle de temps réservé à un autre. Il utilise ces slots pour l'émission/réception de paquets de/vers d'autres nœuds. De ce fait, il n'y a jamais de collision dans ce type de protocole MAC. Le mécanisme TDMA est une méthode sans contention qui permet d'assurer des communications de fiabilité élevée, d'éviter le problème du nœud caché, et d'assurer, avec une forte probabilité, la QoS dans les réseaux pour le support d'applications en temps réel. Pour que TDMA puisse bien fonctionner, il faut un bon niveau de synchronisation entre les nœuds (dans le cas de réseau de véhicule on utilise GPS). La technique TDMA peut garantir une limite supérieure sur le délai de diffusion des messages, le délai est déterministe (le délai d'accès des messages est borné), même dans des environnements saturés. Cependant, cette technique a besoin d'une procédure de

synchronisation complexes (par exemple, point central de distribuer équitablement les ressources entre les nœuds). Dans de nombreux cas, les nœuds sont regroupés pour former des grappes avec un tête de grappe qui est chargé d'attribuer les slots de temps pour les nœuds de sa grappe (par exemple, Clustering-Based Multichannel MAC [24]). Certaines des méthodes utilisent TDMA distribué pour l'accès au support (par exemple, Vehicular Self-Organizing MAC (VeSOMAC) [35]), alors que la plupart des autres utilisent la structure centralisée comme les techniques de clustering, les nœuds sont regroupés pour former des grappes avec un tête de grappe qui est chargé d'attribuer les slots de temps pour les nœuds de sa grappe (par exemple, Clustering-Based Multichannel MAC [24] et hybrid media access technique for cluster-based [34]).

Dans [35] les auteurs ont proposé une approche itérative, en utilisant les accusés de réception par les bitmaps, pour résoudre le problème de collision. Cependant, cette approche est inefficace lorsque le nombre de véhicules dépasse le nombre d'intervalles de temps dans un certain endroit.

Dans [24] les auteurs tentent de faire le meilleur usage des canaux DSRC en proposant un cluster-based multi-channel communication scheme. Le protocole proposé intègre le clustering avec les protocoles MAC à contention et / ou sans contention. Les auteurs ont supposé que chaque véhicule est équipé de deux émetteurs-récepteurs DSRC qui peuvent travailler simultanément sur deux canaux différents. Les auteurs ont également redéfini la fonctionnalité de tous les canaux DSRC de telle sorte que chaque canal est utilisé pour une tâche spécifique.

Un réseau ad-hoc de véhicules a pour particularité la grande mobilité de ses nœuds. Les changements fréquents de topologie impliquent des changements dans les intervalles de temps attribués pour les nœuds. À première vue, on peut dire que TDMA est bien adapté aux réseaux de véhicules en ce qui concerne la fiabilité requise pour les applications de sécurité routières car il n'y a pas de collisions. Cependant, l'attribution des intervalles de temps de TDMA est effectuée d'une manière statique : (1) 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; (2) si un intervalle de temps déjà défini mais n'a pas été réservé par aucun nœud, cela occasionne un gaspillage de bande passante.

2.3.2 Protocoles MAC de diffusion avec contention

Les protocoles avec contention sont les plus populaires et représentent la majorité des protocoles de diffusion proposés pour les réseaux de véhicules. Dans ce qui suit, nous allons présenter brièvement quelques solutions de diffusion de données dans les réseaux de véhicules. En effet, étant donné la nature et les services des applications de sécurité routière, les architectures de communication des réseaux de véhicules doivent intégrer des mécanismes de diffusion des données efficaces et adaptés.

A. Modification des paramètres

Dans [11] les auteurs ont proposé un protocole qui minimise le taux de collision et donc augmente la fiabilité de diffusion, un nœud dans VANET est capable de détecter les collisions et la congestion par simple analyse des numéros de séquence des paquets qu'il a récemment reçus. Chaque nœud diffuse (par inondation) périodiquement à ses voisins son statut, par exemple, les renseignements pertinents sur sa position, sa vitesse et son accélération. Alors qu'un nœud ne sait pas si les paquets qu'il a envoyés sont livrés correctement, il connaît le pourcentage exact de paquets envoyés et si ses voisins les ont reçus avec succès lorsqu'un mécanisme de feedback est mis en œuvre. En se fondant sur ce mécanisme, un nœud est capable d'ajuster dynamiquement les paramètres qu'il utilise, comme la taille de la fenêtre de contention (*contention window CW*), le taux de transmission, et d'améliorer le taux de livraison des messages diffusés. La probabilité de collisions des transmissions peut être réduite, et le taux de livraison des paquets peut être amélioré si la taille de la CW utilisée pour diffuser des messages est capable de s'adapter en fonction des conditions de réseau. Bien que le protocole minimise la probabilité de collision, il ne tient pas en compte le problème de nœud caché et l'évanouissement du canal.

Plutôt que de s'appuyer sur des messages de feedback pour chaque message de diffusion envoyé par la source, ce qui a pour effet d'augmenter la probabilité de collisions et d'interférences sur le support sans fil partagé, nous ne proposons la transmission de message de feedback que dans deux cas : (a) apparition de la congestion ; (b) lorsque d'autres problèmes de livraison de messages (p. ex., problème de nœud caché) surviennent.

B. Acquittement sélectif

Dans The Round-Robin Acknowledge and Retransmit (RRAR) [30], les auteurs proposent un protocole de diffusion où chaque message diffusé doit contenir une demande d'accusé de réception à un seul de ses voisins. Pour chaque nouveau paquet qui sera diffusé, l'émetteur choisit un autre nœud dans un style round-robin. Le RRAR utilise un simple et efficace mécanisme DATA/BrACK. Quand une trame est prête pour la transmission, après avoir terminé la phase d'évitement de collision, l'émetteur exige, dans l'en-tête de la trame de diffusion des données DATA, à un seul de ses voisins de renvoyer un accusé de réception, appelé BrACK (Broadcast Acknowledgment). Ce scénario DATA/BrACK est réalisé dans un style round-robin (Figure 2.11) pour tous les voisins. Alors, en vérifiant le bitmap dans BrACKs reçu, l'émetteur des données calcule et enregistre les trames perdues et les retransmet si elles sont encore stockées. Le fonctionnement de ce protocole suppose que chaque nœud a une liste actualisée de ses nœuds voisins, ce qui est impossible dans des environnements VANET.

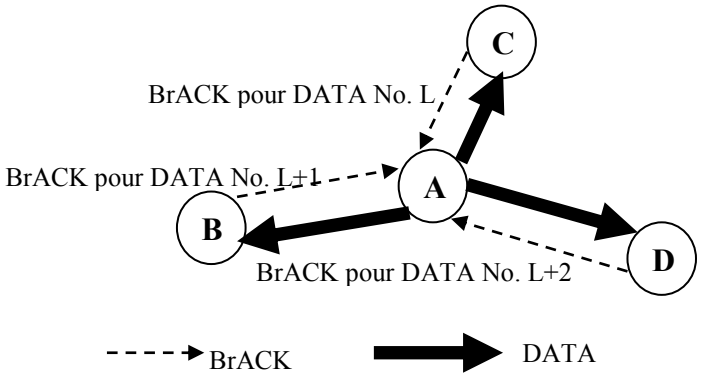


Figure 2.11 - Round-Robin Acknowledgement Retransmission

C. Rediffusion

Dans [29], les auteurs ont exploré les effets de la retransmission en augmentation de la fiabilité et ont développé six MAC protocoles: (1) Répétition Fixée Asynchrone (AFR, Asynchronous Fixed Repetition) : où le message est répété dans chaque intervalle de temps pour un nombre fixé de temps; (2) La Répétition p-persistent Asynchrone (APR, Asynchronous p-persistent Repetition) : où le nœud émetteur transmet le message dans chaque intervalle de temps avec une probabilité P, où P est un paramètre configurable; (3) Répétition Fixée Synchrone (SFR, Synchronous Fixed Repetition) : est le même que AFR, sauf que tous les nœuds du réseau sont synchronisés sur une horloge globale; (4) La Répétition p-persistent Synchrone (SPR, Synchronous p-persistent Repetition) : est le même que APR, sauf que tous les nœuds du réseau sont synchronisés sur une horloge globale; (5) La Répétition Fixée Asynchrone avec détection de porteuse (AFR-CS, Asynchronous Fixed Repetition with Carrier Sensing) : est le même que AFR sauf la détection de canal avant transmission; et (6) La Répétition p-persistent Asynchrone avec détection de porteuse (APR-CS, Asynchronous p-persistent Repetition with Carrier Sensing) : est le même que APR sauf la détection de canal avant transmission. Bien que les deux protocoles et SFR et AFR-CS aient donné le meilleur taux de réussite, l'auteur suggère d'utiliser le CS-AFR car il ne nécessite pas de synchronisation globale. Ce protocole ne permet pas de résoudre le problème de la station cachée, et le protocole AFR-CS exige le même nombre de répétitions négligeant l'effet de l'état du réseau et le volume du trafic.

D. Inondations

Dans les réseaux *ad-hoc* sans fil, les portées de communication des nœuds étant limitées, on considère généralement qu'il est impossible pour l'hôte source de pouvoir contacter directement l'ensemble du réseau. Donc, pour diffuser des informations sur une zone supérieure à celle couverte par la portée de transmission d'un nœud, il est nécessaire d'utiliser un mécanisme de transmission par relais multi-sauts. Le moyen le plus simple d'effectuer le relais multi-sauts est par les inondations (*flooding*) d'un paquet, ce qui garantit que le message finira par atteindre tous les nœuds du réseau. Son principe est le

suivant : chaque hôte recevant pour la première fois le message à diffuser le réémet à destination de ses voisins. Malheureusement, cet algorithme très simple n'est pas efficace, car il requiert la participation de tous les hôtes, alors que cela n'est pas toujours nécessaire. Par conséquent, il conduit à une grande quantité de messages redondants, ce qui aura plusieurs conséquences, à savoir des problèmes de collisions, des tempêtes de diffusion, des nœuds cachés, une fiabilité plus faible et une consommation plus élevée de la bande passante. Par exemple, un message envoyé aux n nœuds aboutit à un message rediffusé n fois. Le problème est caractérisé par la diffusion redondante, par les contentions et les collisions. La création d'une diffusion de multi-sauts efficace est un problème ouvert.

Ni, *et al.* (1999) [20] a été le premier à utiliser les techniques des inondations dans les réseaux mobiles ad-hoc, et a introduit le terme « broadcast storm » problème de tempête de diffusion. Ce problème se produit lorsque vous tentez d'envoyer le message destiné à tous les nœuds en forçant chaque nœud de retransmettre le message (les inondations simples). « Simples inondations » se traduira par : (1) Redondances graves (tous les voisins ont déjà reçu le message), (2) Contention; (3) et la collision (transmissions simultanées et l'absence de RTS / CTS). Il a présenté différentes stratégies pour réduire la redondance en inhibant certains nœuds de rediffuser. Ces stratégies sont: (1) Réseaux véhiculaire basés sur la probabilité : la première fois qu'un message est reçu il est diffusé avec une probabilité $0 \leq p \leq 1$, en considérant qu'une absence de diffusion peut être compensée par les voisins, si la valeur de p est bien adaptée. Notez que lorsque $p = 1$, ce schéma sera identique à l'inondation simple (Figure 2.12); (2) Réseaux véhiculaires basés sur le comptage: ne pas diffuser un paquet s'il a déjà été diffusé.

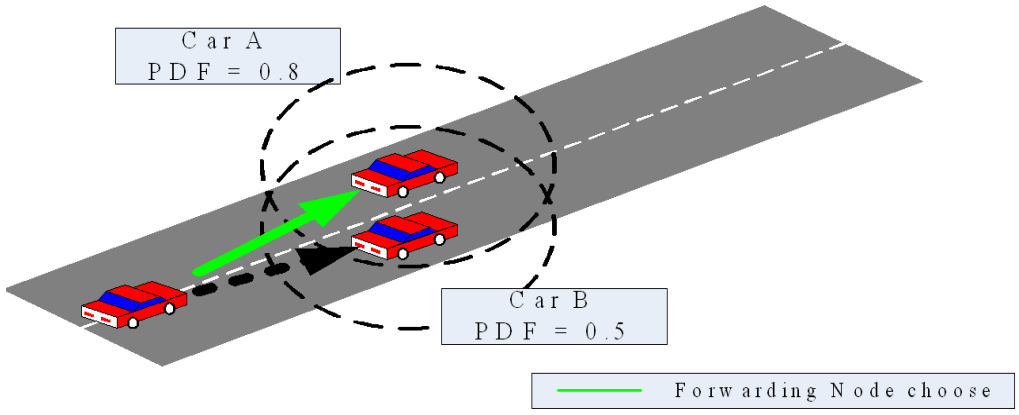


Figure 2.12 - Réseaux véhiculaires basés sur la probabilité

Cette solution est simple et évite les redondances mais elle n'est pas toujours efficace; (3) ou encore des réseaux véhiculaires basés sur la distance: ne pas diffuser un paquet, s'il vient d'une station proche d'une distance d > D, où D est une constante, puisque une diffusion aura environ la même portée (Figure 2.13); (4) Réseaux véhiculaires basés sur la localisation: chaque nœud compare sa position avec l'emplacement de l'émetteur et calcule la couverture supplémentaire qui peut être fournie en supposant que tous les nœuds ont une couverture omnidirectionnelle.

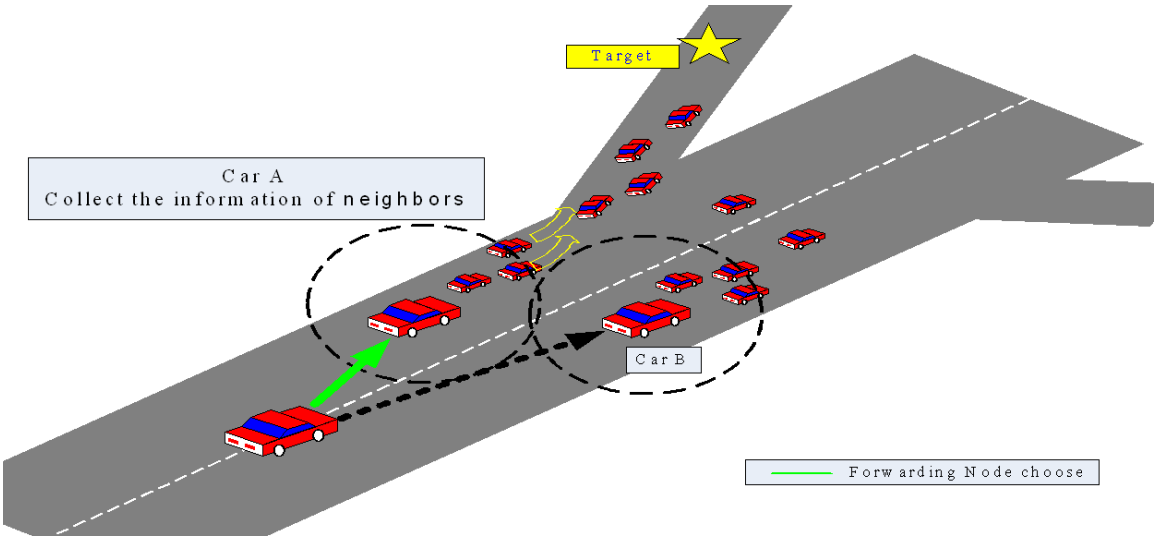


Figure 2.13 - Réseaux véhiculaires basés sur la distance

Un noeud retransmet le message que si la couverture additionnelle > A, où A est une constante (Figure 2.14); (5) Réseaux véhiculaire basés sur les grappes: dans ce schéma, l'auteur suggère de diviser le réseau en grappe circulaire, chaque grappe a un petit ensemble de nœuds agissant comme une passerelle vers les grappes voisins. Ici, les nœuds passerelle seuls ont le droit de retransmettre le message (Figure 2.15).

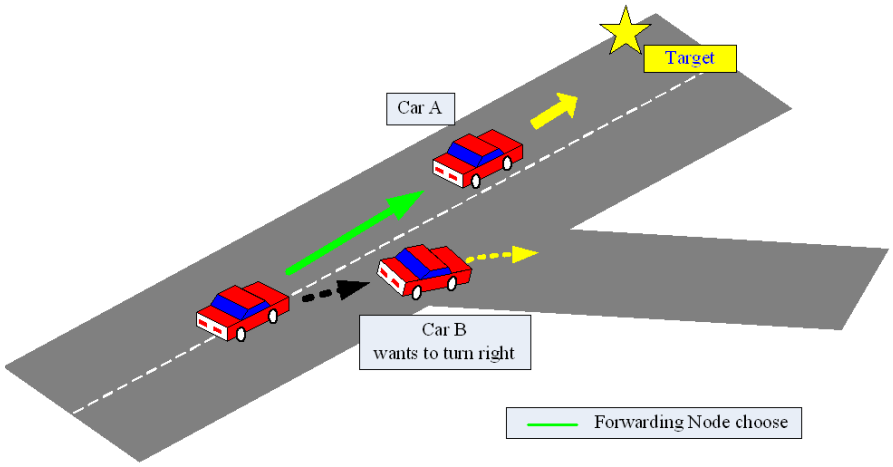


Figure 2.14 - Réseaux véhiculaires basés sur la localisation

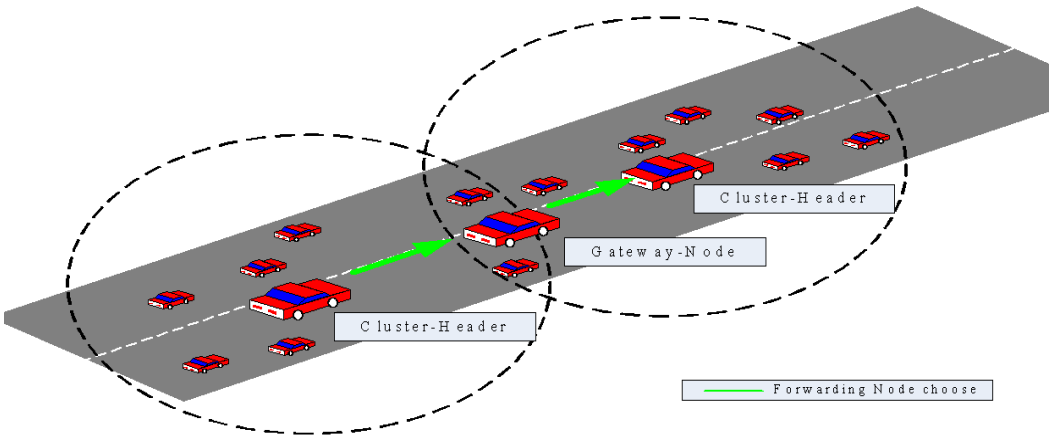


Figure 2.15 - Réseaux véhiculaire basés sur les grappes

Enfin, l'auteur conclut que le régime de localisation a abouti au minimum redondant. Bien qu'il ait été, la première fois, incapable de clarifier les problèmes liés à la diffusion à multi-sauts dans les réseaux ad-hoc, l'auteur a présenté une bonne analyse et des solutions élégantes. L'algorithme n'est pas efficace pour gérer des surcharges des paquets élevées et il souffre de problème de nœud caché.

MDDV (Mobility-Centric Data Dissemination Algorithm for Vehicular Networks) [9] est un algorithme de diffusion qui, contrairement aux autres algorithmes géographiques, considère que les véhicules ne disposent pas des positions des véhicules voisins. Le réseau routier est modélisé comme un graphe orienté où les nœuds représentent les intersections, et les liens les segments routiers. Un poids est associé à chaque lien pour refléter la distance et la densité de trafic correspondante. MDDV utilise une trajectoire de relai spécifiée comme le chemin ayant la plus petite somme de poids d'une source vers la 'région destination' dans le graphe orienté.

Ces protocoles permettent de réduire la redondance de manière efficace, mais aucune amélioration pour la probabilité pour qu'une collision se produise (par exemple, station caché). En outre, l'absence de l'acquittement explicite la fiabilité globale.

E. Relais unique

UMB (Urban Multi-Hop Broadcast) Protocol [5] est un algorithme de diffusion qui modifie la couche d'accès 802.11 pour l'adapter au contexte des IVC dans le but de réduire les collisions et d'utiliser efficacement la bande passante. Il comprend deux phases : la première appelée diffusion directionnelle où la source sélectionne un nœud dans la direction de diffusion pour effectuer le relai des données sans aucune information sur la topologie, et la deuxième diffusion aux intersections, pour disséminer les paquets dans toutes les directions, en installant des répéteurs vers tous les segments de route. La sélection du nœud le plus éloigné est fondée sur la transmission du plus long signal. Cela implique une latence élevée et limite son usage dans les cas d'urgence; de plus, UMB protocole n'est pas un candidat de la version actuelle de la norme 802.11.

Dans RBM (Role-Based Multicast) [28], les auteurs proposent un protocole de multicast où chaque nœud maintient deux listes : une liste de voisins et une liste des nœuds émetteurs. En fonction des contenus de ces deux listes, un nœud décide ou pas de rediffuser le message après un certain temps. Dans cette approche, le protocole suppose l'existence d'une couche liaison qui maintient la liste des nœuds voisins.

Dans [2], les protocoles de diffusion appelés TRADE (TRack DEtection) et DDT (Distance Defer Time) ont été proposés. Pour TRADE l'objectif est de garantir une meilleure fiabilité avec un nombre de rediffusions limité. Un véhicule doit alors désigner parmi ses voisins, en fonction de leurs déplacements, ceux qui assurent la retransmission des messages. DDT quant à lui, utilise un temps d'attente (defer time) avant la rediffusion d'un message reçu, et si pendant ce temps il reçoit le même message provenant d'un autre véhicule il ne le rediffuse plus.

IVG (Inter-Vehicle Geocast) [27] est une nouvelle méthode de diffusion qui généralise les méthodes précédentes (TRADE et DDT) et permet de surmonter les problèmes de fragmentation du réseau, de fiabilité et de calcul de voisins. Des relais dynamiques sont introduits pour rediffuser périodiquement les messages d'alerte. Ces relais sont désignés en fonction de la distance relative au véhicule source. Une comparaison avec

les méthodes TRADE et DDT a été réalisée en utilisant un modèle analytique et des simulations, et a montré les améliorations apportées, et ce indépendamment de l'environnement (rural ou urbain).

Ces protocoles optimisent la dissémination d'information en sélectionnant seulement quelques nœuds pour la retransmission des messages. Ils tentent d'assurer à la fois un délai d'acheminement réduit et une meilleure utilisation des ressources.

2.4 Conclusion

Nous avons parcouru dans ce chapitre les techniques utilisées pour garantir la QdS pour les applications de diffusion, soutenir la capacité de prioriser et de gérer plusieurs types de messages, etc. Ces travaux demeurent un défi dans les réseaux VANETs.

Dans la documentation, plusieurs protocoles de diffusion ont été proposés. Parmi ces protocoles, il existe une catégorie (par exemple, [11], [2], [30] et [29]) qui permet de réduire la charge de la diffusion et d'améliorer les performances en termes de taux de livraison de paquets. En raison du problème bien connu de tempête de diffusion [20], les protocoles de diffusion de VANET doivent inclure un protocole efficace des inondations. D'autres catégories de protocoles (par exemple, [24] et [5]) s'attaquent au problème de la station cachée qui est plus accentuée dans le mode de diffusion par rapport au mode unicast et utiliser l'information de position du véhicule afin de limiter le nombre de nœuds à relayer les messages diffusés. Le tableau 1 donne un aperçu des propriétés de quelques protocoles (section 2.4 du chapitre 2). Nous remarquons qu'un grand nombre d'entre eux réduisent la latence et aussi le problème du nœud caché; cependant, les protocoles à contention ne garantissent pas une borne supérieure pour la latence. En outre, l'absence de l'acquittement explicite la fiabilité globale. Bien que la plupart de ces protocoles de diffusion permettent d'améliorer les performances de VANETs tout en réduisant le délai et/ou le taux de succès de livraison des messages, ils assument que l'accès au médium est fondée sur la contention. Cela nécessite des mécanismes plus complexes, qui permettent le maintien de bonnes performances en conditions de charge très élevée et surtout pour satisfaire les contraintes en

temps réel d'applications de sécurité. En fait, le mécanisme VCS standard fondé sur l'envoi de RTS/CTS (Request to broadcast/ Clear to Broadcast), ne peut pas être utilisé pour prévenir les collisions (causées par les nœuds cachées) lors de diffusion de messages de sécurité. En outre, les mécanismes utilisés dans RTB/CTB, comme dans UMB [5] par exemple, ne peuvent pas garantir une réception sans collision de la CTB. En outre, la réservation RTB/CTB pour chaque transmission de diffusion ajoute un surcoût considérable et inutile pour la diffusion de messages de sécurité périodiques. Plutôt que de s'appuyer sur un protocole fondé sur la contention MAC, nous proposons un nouveau protocole de réservation adéquat en particulier pour les applications de diffusion périodique. Notre VCS est fondé sur l'envoi de trames RTB/CTB dans lequel un seul RTB est utilisé pour réserver un intervalle de temps périodique prédéterminé (Time slot) pour une diffusion sans contention durant une période de stabilité. Les confirmations RTB et CTB sont envoyées durant la période de contention (CP, Contention Period) pour chaque période de service. Durant la période sans contention (CFP, Contention Free Period) les messages d'urgence sont prioritaires par rapport aux messages de sécurité périodiques en utilisant un court espace inter-trame (AIFS1). A Time Slot Scheduling Algorithm [13], exécuté par les véhicules chefs de grappe (on suppose une structure groupée du réseau de véhicules), ce qui alloue des intervalles de temps de diffusion périodiques aux véhicules demandant afin de minimiser les effets du problème des stations cachées. Aussi, nous ajoutons un champ dans RTB spécifiant l'une des quatre orientations possibles pour le transfert de diffusion (EST, OUEST, NORD ou du SUD). Cela permettra d'éviter des diffusions inutiles des messages de sécurité qui participent à l'augmentation du niveau de congestion. A Dynamic CFP Channel Operation Algorithm [13], contrairement au statique utilisé dans IEEE 802.11p; il maximise le débit sur le canal de service tout en garantissant des délais de livraison courts et des taux élevés sur le canal de contrôle. Par ce protocole, nous visons à: (1) Améliorer considérablement le taux de livraison des messages de sécurité périodiques tout en offrant une borne supérieure au délai de réservation/accès au canal; (2) Réduire la probabilité de collisions entre les nœuds qui ne sont pas en visibilité (problème de nœud caché); (3) Réduire le surdébit par l'utilisation d'une demande de réservation

unique pour l'accès périodique au support pendant la session de grappe d'un véhicule et par la prévention des diffusions inutiles des messages; (4) Maximiser le débit pour d'autres applications par un ajustement d'adaptation d'une période sans contention (CFP) et une période de contention (CP).

	Fiabilité	Faible latence	Probabilité de collision	Problème nœud caché	Débit	Sur-débit (Tempête de diffusion)	Mécanisme de réservation/accès de canal
Feedback [11]	Amélioré	Non	Réduite	Non	Amélioré	Réduit	Accès avec contention
RRAR [30]	Oui	Non	Réduite	Non	Amélioré	Réduit	Accès avec contention
PRF [29]	Oui	Pour 1-Saut	Réduite	Non	Amélioré	Réduit	Accès avec contention
Cluster based multi-channel MAC[24]	Oui	Oui	Réduite	Oui	Maximisé pour les messages de sécurité et non-sécurité (deux antenne)	Réduit	Accès avec et/ sans contention
Broadcast storm [20]	Amélioré	Non	Réduite	Non	Amélioré	Réduit	Accès avec contention
TRADE et DDT [2], IVG [27] et UMBR [5]	Oui	Oui	Réduite	Non sauf [5]	Amélioré	Réduit	Accès avec contention
Notre protocole [13]	Amélioré	Oui avec borne supérieure (Un time slot prédéterminé à chaque nœud)	Résolu (réseau peu dense) et réduite (réseaux très denses)	Résolu	Maximisé pour les messages de sécurité et non-sécurité (dynamique CFP avec un seul antenne)	Très réduit - Unique RTB/CTB pendant la session de group d'un véhicule. - Évite les retransmissions inutiles.	Mécanisme de réservation RTB/CTB dans la CP pour un accès sans contention dans la CFP

Tableau 2.1 - Aperçu des propriétés d'un ensemble de protocoles de diffusion

Chapitre 3

Ce chapitre correspond à notre premier article «A Contention-Free Broadcast Protocol for Periodic Safety Messages in Vehicular Ad-Hoc Networks», qui a été publié dans les actes de The 35th Annual IEEE Conference on Local Computer Networks (LCN), 2010.

Ma contribution, dans cet article a été la suivante : (1) Développement d'un nouveau protocole de réservation, implémenté sur mesure pour les applications de diffusion périodique, qui peut être utilisé pour gérer le droit d'accès aux médias (protocole de gestion des émissions) dans les réseaux véhiculaires (voir Chapitre 3, page 45); et (2) Implémentation de ce protocole puis comparaison et analyse des résultats avec d'autres protocoles de gestion des émissions.

Résumé en Français

Les protocoles Ad-hoc de diffusion multi-sauts sont généralement utilisés dans les réseaux véhiculaires pour fournir des services de sécurité. Ces protocoles de diffusion ne sont pas fiables et ils souffrent de plusieurs problèmes, à savoir : (1) Tempête de diffusion (*broadcast storm*) ; (2) Nœud caché (*hidden node*); (3) Échec de la transmission. Ces problèmes empêchent les applications de sécurité de garantir un meilleur taux de livraison des messages et entraînent des délais d'accès limité. Dans cet article, nous abordons ces problèmes en utilisant un nouveau protocole de diffusion sans contention basé sur des grappes. En particulier, nous proposons un nouveau protocole de réservation des intervalles de temps, centralisé dans les têtes de grappes qui s'adaptent continuellement à la dynamique des véhicules. Ainsi, l'utilisation de ce protocole centralisé nous assure une consommation efficace d'intervalles de temps pour le nombre exact de véhicules actifs, y compris les nœuds/véhicules cachés; notre protocole assure également un délai limité pour les applications de sécurité, afin d'accéder au canal de communication et il permet également de réduire le surplus (*overhead*) à l'aide d'une propagation dirigée de diffusion et une seule requête de réservation pour l'accès périodique au support est utilisée durant la période de stabilité, période pendant laquelle les nœuds restent dans la même grappe et que le chef de grappe ne change pas son état. Notre protocole maximise le débit dans d'autres applications par un ajustement d'adaptation d'une période sans contention et une période de

contention. Nous avons démontré, à l'aide de simulations, que le protocole proposé peut améliorer considérablement le taux de livraison des messages de sécurité périodiques, tout en offrant un délai d'accès limité.

A Contention-Free Broadcast Protocol for Periodic Safety Messages in Vehicular Ad-Hoc Networks

Ahmed Ahizoune, Abdelhakim Hafid, Racha Ben Ali
Network Research Lab, University of Montreal, Canada

Abstract

Ad-hoc multi-hop broadcast protocols are usually used in vehicular networks to provide safety services. However, these protocols face several issues, namely broadcast storms, hidden nodes, and message delivery failures, that prevent safety applications from guaranteeing their required high message delivery ratio and low delays. In this paper, we tackle these issues using a novel cluster-based contention-free broadcast protocol. Particularly, we propose an efficient time slot reservation protocol, centralized in stable cluster heads that continuously adapts to vehicles dynamics. Thus, using a centralized protocol, we ensure an efficient utilization of the time slots for the exact number of active vehicles including hidden nodes; our protocol also ensures a bounded delay for safety applications to access communication channel. We reduce the overhead of our reservation protocol using a directed broadcast propagation and a single reservation request for a periodic medium access during a vehicle's cluster session. During the recurrent service interval, a contention-based period follows the efficiently-used contention free period; it is dynamically adjusted to improve throughput-sensitive non-safety applications. Extensive simulation results show that the proposed scheme can significantly improve the periodic safety application performance in terms of safety message delivery ratio and delay.

Keywords- *VANET, Periodic Safety Messages, broadcast protocols, contention-free.*

Status: This paper is published in the 35th Annual IEEE Conference on Local Computer Networks (LCN) [13].

I. INTRODUCTION

New wireless technologies have the potential to enable inter-vehicle communications with the purpose of crash avoidance and transportation system efficiency improvement. Consequently, the Federal Communications Commission (FCC) of the U.S. approved the 75MHz bandwidth at 5.850-5.925GHz band, in year 1999, for Intelligent Transportation System (ITS). This wireless spectrum is commonly known as the Dedicated Short-Range Communication (DSRC) allocated by the regulator to be used exclusively for vehicle to vehicle (V2V) and vehicle to roadside (V2R) communications [11]. The DSRC spectrum is divided into seven channels: one control channel generally restricted to safety communications; two channels reserved for future accident avoidance applications and high-powered public safety usages; and four service channels available for both safety and non-safety usage. An IEEE 802.11p Task Group was created to standardize DSRC. It is commonly called WAVE (Wireless Access for Vehicular Environments). This IEEE 802.11p is typically a customized variant of IEEE 802.11a PHY layer specially adapted to provide low-overhead operation in the DSRC spectrum. It combines parts from the original standard together with the MAC amendment 802.11e for QoS support. For more details, authors in [1] introduces the concepts, applications and performance characteristics behind these technologies used for V2V communications. DSRC will support safety critical communications, such as collision warnings, as well as other valuable Intelligent Transportation System applications, such as Electronic Toll Collection (ETC) and real-time traffic advisories, digital map update. The versatility of DSRC greatly enhances the likelihood of its deployment by various industries and adoption by consumers. Broadcast protocols will play a major role in the success of Vehicular Ad Hoc Networks (VANETs) since they will support a large variety of new safety applications. Some of the uses of broadcast protocols are: sending emergency warning messages, transmitting state

information to other vehicles, broadcasting aggregate data, address resolution, and determining routes.

However, existing broadcast protocols suffer from several issues not totally resolved in the literature. In fact, due to the specific characteristics of the vehicular network in establishing multi-hop communications over a limited number of channels and commonly using a single radio interface per vehicle, interference related problems occur. Broadcast storms, hidden nodes and reliable delivery of critical messages are the main issues specific to broadcast safety services; these issues that cannot be resolved by the existing IEEE 802.11p broadcast protocol derived from IEEE 802.11.

Our contributions in this paper can be summarized as follows: (1) An improved virtual carrier sense (VCS) mechanism for periodic broadcast messages in which a single Request-To-Broadcast (RTB) is used to reserve periodic time slots for a contention free broadcast during a stability period. RTB and Clear-To-Broadcast (CTB) confirmations are sent during a contention period for each service period. During contention free, emergency messages are prioritized over periodic Safety messages by using a shorter inter-frame space (AIFS1); (2) A time slot scheduling algorithm, implemented by cluster-head vehicles (we assume a clustered structure of the vehicular network), that allocates periodic broadcast time slots to requesting vehicles which minimizes the effects of the hidden station problem; and (3) A dynamic CFP channel operation algorithm, in opposition to the static one used in IEEE 802.11p; it maximizes the throughput on the service channel while guaranteeing low delays and high delivery rates on the control channel.

The remainder of this paper is organized as follows. In Section II, we present related work. Section III presents definitions and assumptions. In section IV, we describe the protocol architecture. In section V, we present the protocol operation analysis. Section VI presents simulation and performance analysis. Section VII concludes the paper.

II. RELATED WORK

Broadcast protocols will play a larger role than unicast messages in vehicular networks since they are designed to communicate important safety messages to all surrounding vehicles in the area.

Because of the broadcast and multi-hop inherent characteristics of VANETs, flooding is generally used in VANETs to disseminate messages to all vehicles several hops away from the source. Broadcasting in VANETs using local information has been widely studied in the literature. Most of these contributions [1,2 and 3] reduce broadcasting load and improve performance in terms of packet delivery ratio.

Due to the well known broadcast storm problem, broadcasting protocols in VANETs usually include an efficient flooding protocol. Most of these protocols use the vehicles positions information to limit the number of nodes relaying the broadcast messages. Multi-hop Broadcast protocol (UMB) [4] introduces a new RTB and CTB handshake for IEEE 802.11. UMB tackles the problem of hidden node problem which is more accentuated in broadcast mode compared to the unicast mode. It selects the farthest vehicle from a transmitter to retransmit the message. UMB uses repeaters at street intersections to rebroadcast packets in all directions. Authors show that UMB improves the delivery ratio and the bandwidth utilization compared to the standard IEEE 802.11. However, packet dissemination speed is slower for small packets and is relatively worse at higher transmission rates.

The multi-hop vehicular broadcast (MHVB) [5] efficiently broadcasts local information for safety services, such positions and velocities, in VANETs. It includes a congestion detection algorithm that avoids unnecessary broadcasts in congestion situations and a backfire algorithm that selects the broadcast relaying nodes based on the distance. Authors show that MHVB improves the performance of broadcast services in VANETs. The same authors improve this protocol in [6] by altering the backfire area from a circular shape to a sectoral shape. Furthermore, they introduce a dynamic priority scheduling algorithm based on the "processing" of the received messages. Particularly, this improved

MHVB make vehicles that are at a distance farther than 200m re-transmitting the received information earlier than all the other nodes in the network. Thus, emergency information is forwarded more quickly over longer distances.

The mobility-centric approach for data dissemination (MDDV) in VANETs [7] is designed to exploit mobility for message broadcasting. It combines opportunistic forwarding, trajectory based forwarding and geographical forwarding. MDDV determines a forwarding path to a destination region, and its closest vehicles within the path to participate in group forwarding.

Palazzi et al. [9] propose a Fast multi-hop Broadcast protocol (FB) to quickly propagate broadcast messages by adapting to transmission range variations when minimizing the number of relaying hops. Particularly, FB allows each vehicle to estimate its current transmission range and transmit it to other vehicles. Receiving vehicles use these estimations to determine their relative positions and assign to themselves priorities in becoming next forwarders of broadcasted messages.

Although these broadcast protocols improve the performance of VANETs by reducing the message delivery delay and/or the message delivery success rate, they assume a contention based medium access. This latter requires complex mechanisms, (to resolve broadcast contentions) that struggle to maintain good performance in very high load conditions and especially to satisfy real-time constraints of safety applications. In fact, since standard VCS mechanism, i.e. RTS/CTS, cannot be used to prevent hidden nodes collisions when broadcasting safety messages, frequent collisions in larger hidden node areas are experienced in this broadcast environment compared to a unicast one. Moreover, the mechanisms used in RTB/CTB schemes, such as in UMB [4] for instance, cannot guarantee a collision free reception of the CTB. Furthermore, the reservation RTB/CTB for each broadcast transmission adds a considerable and unnecessary overhead for periodic safety message broadcast. Rather than relying on a contention-based MAC protocol, we propose a novel reservation based protocol especially customized for periodic broadcast applications. By this protocol, we aim to: (1) efficiently reduce the reservation signalling

overhead using a stable-cluster-based centralized (at the cluster head) reservation protocol that manages an efficient schedule of contention free periods with less signalling overhead; (2) guarantee a deterministic access for the delay-sensitive applications with a high delivery ratio; and (3) maximize the throughput for other applications by an adaptive adjustment of contention free period (CFP) and contention period (CP).

III. DEFINITIONS AND ASSUMPTIONS

In this section we present the definitions of key terms and assumptions used in this paper.

As shown in Figure 3.1 we identify three basic states/roles of a node:

Cluster Head (CH): A cluster head serves as a local coordinator for its cluster, performing inter-cluster routing, data forwarding and so on. In our protocol, each CH maintains two groups of vehicles: the Back Group (BG) and the Front Group (FG).

Back Group (BG): Contains every cluster member whose position X_i is smaller than X where X is the position determined by CH in order to avoid interferences (see Section V). In this paper, we assume that the coordinates of a node correspond to its projection on a reference axis (x-axis) for which an origin is defined, according to a given direction. Only one coordinate, X, is thus sufficient to define the position of a car.

Front Group (FG): Contains every cluster member whose position X_i is bigger than X where X is the position determined by CH in order to avoid interferences.

Cluster Gateway (CG): A cluster gateway is not a CH with inter-cluster links; thus, it can access directly (1-hop communication) neighboring clusters and forward information between clusters. In our proposed scheme, the election of CG is based on the distance D between two neighbouring CHs. If D is 2-hops (Figure 3.1-(b)), then the node part of the shortest path between the two CHs is elected as CG. If D is bigger than 2-hops then, as shown in Figure 3.1-(a), CH_n and CH_m elect CG_n and CG_m according to the following rule: CG_m belongs to BG of U_m (Um_BG) and is the farthest from CH_m and

CG_n belongs to FG of U_n (Un_BG) and is the farthest from CH_n. The cluster-head keeps updating these lists according to topology changes.

Cluster Member (*CM):* A cluster member is a node that is neither a CH nor a CG.

Sometimes, an additional state called Undecided State (US) is used for the initial state of a node.

We call forward CG the selected forwarder in the forward direction of cluster vehicles movement. Similarly, we call backward CG the selected forwarder in the backward direction of cluster vehicles movement.

In this paper, we assume that vehicles positions and timing information are provided using GPS (Global Positioning System) timing information. All vehicles have the same transmission power and thus the same transmission range r and the same interference range R ($R = 1.78 * r$ [14]).

Also, we assume that time is partitioned into periodic, regulated intervals, called the Repetition Period (RP). RP is of length T. Each RP is shared between service and control channels and divided into two periods, CFP and CP.

IV. PROPOSED PROTOCOL

IEEE 802.11 broadcast transmission is not reliable. Vehicle safety applications need to be designed to tolerate some broadcast message delivery failures. Nevertheless, it is important, when designing a safety application protocol for VANETs, to consider reducing the number of broadcasts that generate bad receptions. A node in a VANET is able to detect collisions and congestion by simply analyzing the sequence numbers of packets it has recently received [15]. Each node will periodically broadcast its status, e.g., relevant information about its location, speed, and acceleration to its neighbours. While a node does not know whether the packets it sent are correctly delivered, it knows the exact percentage of packets sent to it, from its neighbours that are successfully received if a feedback mechanism is implemented. Based on this feedback, a node is able to dynamically adjust the parameters it uses, such as contention window (CW) size, transmission rate, and

transmission power, to improve the delivery rate of broadcast messages. The probability of transmission collisions can be reduced and the packet delivery rate can be improved if the size of the CW used to send broadcast messages is able to adapt based on the network conditions.

Rather than relying on feedback messages, for each broadcast message sent by the source, that increase interferences and collision probability on the shared wireless medium, we propose to allow the transmission of feedback messages only in two situations (a) occurrence of congestion and (b) or other message delivery problems (e.g. hidden node problem).

In fact, due to the specific periodicity of safety messages, we do not need, as in the standard 802.11 protocol, to exchange a RTB/CTB each time a message needs to be broadcasted. Therefore, we propose to synchronize the nodes using GPS timing information and include 802.11 transmission opportunity periodicities in the RTB message. Consequently, each node will establish periodic Network Allocation Vector (NAV) periods during which it is not allowed to transmit since these periods are reserved for transmissions of other nodes; this will considerably reduce interferences and collisions. Furthermore, by adding a congestion notification field in CTB messages, the local node, upon receipt of these messages, can be aware of its participation to a remote congestion along the broadcast forwarding path. Thus, it can adjust its broadcast rate f based on the level of measured congestion. We assume that the periodic safety application adjusts its message broadcast rate f based on lower layer congestion.

Broadcast forwarders (multi-point relaying) selection: In most cases, safety messages do not need to be flooded over all directions. Indeed, several nodes, such as vehicles upward a sudden traffic jam may not be interested in the information it encapsulates. Therefore, in our proposed protocol we add a field in the RTB message specifying one of the four possible broadcast forwarding directions (eastbound, westbound, northbound or southbound). This will prevent unnecessary safety message broadcasts to participate in increasing the congestion level. The forwarder is selected among the n nodes

in the broadcast range quadrant of the specified direction that reports the n lowest signal strengths. These nodes correspond to the n farthest vehicles from the CH within the broadcast range quadrant. This simple forwarder selection process will ensure that a minimal number of hops will be used to forward the broadcast message; other more dynamic forwarder selection mechanisms, such as the mechanism reported in [8], may also be used.

In opposition to the RTB/CTB message exchanges used in [4] (where these exchanges are repeated for each packet broadcast), in our proposed protocol it is performed only once during a cluster join session. This being said, the verification of the availability of the forwarder is performed for each packet transmission using timeout ACK.

SCH/CCH channel switching algorithm: In the DSRC standard, the radio interface of the vehicle has to switch between the control channel (CCH) on which safety messages are broadcasted and the service channels (SCH) on which other unicast data communications are transmitted. Since safety and non-safety applications can not transmit on different channels at the same time using a single radio, CCH/SCH switching has to be performed where a pre-emptive priority is given to transmit the emergency safety messages. Indeed, if a safety application generates an emergency message while a non-safety application is transmitting on the SCH, this latter has to be pre-empted, i.e. temporarily suspended. This is done in order to allow the safety application to switch the single radio interface to CCH on which the urgent message will be transmitted. However, due to the overhead latency of the channel switching process, broadcast safety messages could be lost while the radio is busy switching channels, and therefore, retransmissions are usually needed to ensure reliable delivery. In addition to this pre-emptive switching used for instance in the PeerCast protocol [1], a periodic switching is performed to balance between periodic safety message transmission over the CCH and applications over the SCH.

The DSRC standard uses static time intervals during which the radio is assigned to CCH and SCH channels. In our protocol, we propose to dynamically maximize the time

interval for throughput-sensitive applications over SCH channel while guaranteeing a deterministic collision-free access for delay-sensitive safety applications over SCH/CCH channel. The minimal time interval duration for CCH can be computed by cumulating periodicity information in the RTB messages and taking into account different congestion and wireless medium factors (e.g. AIFS, CW, beacons, etc.).

In this paper, the design of our protocol is motivated by the fact that DSRC spectrum at 5.9-GHz band is divided into seven channels, including Ch172, Ch174, Ch176, Ch178, Ch180, Ch182, and Ch184, each spanning 10 MHz. One of these seven channels is identified as a control channel Ch178; it can be used for Inter-cluster management, delivering safety messages and announcements between CMs and their CH, and between neighboring CHs via CGs. The remaining six channels are called service channels; they are used for Intra-cluster management and safety message delivery within the cluster. In addition, CMs can use service channels to exchange non-safety data with one another and with members of neighboring clusters.

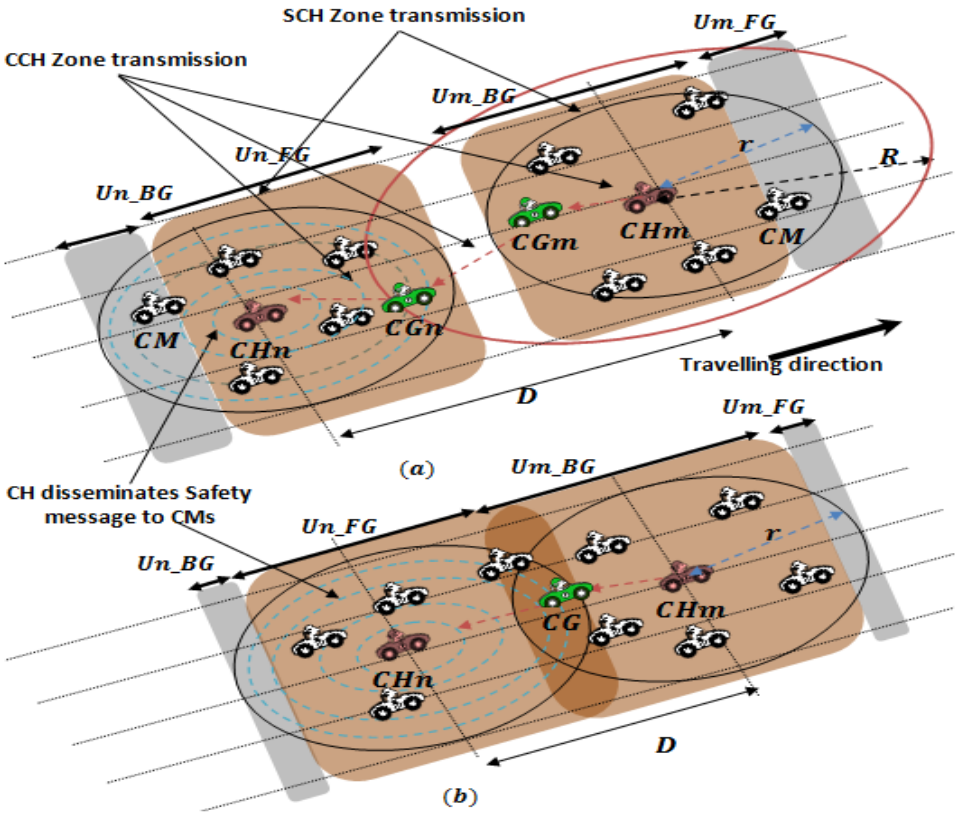


Figure 3.1 - Highway scenario

Our proposed scheme aims to provide low latency and high message delivery ratio of real-time data safety messages and increasing the throughput for the non-safety traffic over the V2V-based VANETs. The key idea behind our proposed scheme is to integrate the clustering algorithm with both the contention-free and contention-based MAC protocols under the DSRC architecture.

TDMA-based (Time Division Multiple Access) MAC protocols are usually used to achieve collision-free transmission of data over the shared wireless medium. In these protocols, a central node such as the access point, assigns the different time slots to data sources. However, since VANETs do not rely on a centralized node in a fixed infrastructure, we need to elect a vehicle that will act as a central node for time slot

scheduling and management. Therefore, our proposed protocol uses a CH election algorithm to select the central node.

A. Cluster Formation algorithm

In VANET, vehicles moving in platoons share similar traffic patterns like the average speed, the average acceleration, and the direction of motion. This group of vehicles can be united together to form a new entity called a cluster. Clustering schemes [9-11] can be used to reduce data congestion and increase the probability of safety and non-safety data delivery. There are many techniques for cluster formation (e.g. [11, 12, 13 and 16]). In this paper, we adopt a mobility-based clustering scheme for Vehicle Ad hoc Networks, [16], that uses the Affinity Propagation algorithm in a distributed manner. This algorithm determines clusters that minimize both relative mobility and distance from each CH to its CMs. The resulting clusters are stable and exhibit long average CM duration, long average CH duration, and low average rate of CH changes.

B. Repetition period

The CFP is divided into time slots. Each time slot can be owned by only one CM on service channel. The time slots are grouped into virtual frames VF=F1 + F2. F1 contains time slots of vehicles in the range of the forward CG node whereas time slots in F2 are allocated for vehicles in the range of the backward gateway node. During its assigned time slot, a vehicle can transmit its safety messages while all others must remain silent but they can receive or overhear others' transmissions. The time slot size is related to the transmission latency of the longest safety message packet. The time slot duration of a packet with a maximum size S is denoted by $T_{Slot} = \frac{S}{R}$ where, R is the channel data rate.

CP follows CFP in the RP, T, as illustrated in Figure 3.2. CH responds to requests from vehicles joining the cluster, updates the list of CMs and elects the backward and the forward CGs. A CM keeps listening to the service channel until the end of CP, or switches to the control channel if it loses contact with its CH.

C. Slot management

Vehicles act as mobile nodes with different speeds in VANETs. A vehicle knows that it is in the range of a given CH when it receives an advertisement message from it. Each vehicle broadcasts, during CP, a Hello message that includes information about its speed and position. If it needs to send a safety message, the vehicle will send a slot request RTB during CP. Due to the specific periodicity of safety messages, each CM does not need, as in IEEE 802.11, to exchange RTB each time a safety message needs to be broadcasted; it requests to reserve a periodic time slot for CFP allocation by a single RTB during a stability period. In this paper, we define a stability period as the period during which CMs remain in the same cluster and the CH does not change its state. When a CH gets a RTB for CFP allocation, it checks the current state of CFP allocation and the list of vehicles in the cluster. Then, CH adds the CM identifier to BG or FG and assigns the corresponding CFP time slots to the CM by replying with CTB containing the slot identifier. The CH, maintains a slot schedule as illustrated in Figure 3.2-(b). In the same way de-allocating CFP slots are performed by the CH after a CM resigns (i.e., requests leaving the cluster) or a CM's dead time interval expires elapses (i.e., a hello reception timeout). In other words, if the CH does not receive any message from a given CM after a specific time period, it declares the vehicle in an out of transmission range and therefore, the vehicle is no longer a member of the cluster.

V. PROTOCOL OPERATION ANALYSIS

A. Intra-cluster communication

According to our protocol, access to the wireless medium for intra-cluster and inter-cluster communication is divided into CFP and CP. The periodicity of Safety message within a cluster is defined within CFP. Thus, time slots in CFP are assigned to vehicles in order that each vehicle can broadcast its Safety message in a dedicated and predictable duration.

Time slot scheduling protocol: In order to avoid interference among CMs and, thus, avoid the hidden-terminal problem, we propose a novel time slot scheduling protocol to be

executed by CHs; the protocol allocates periodic broadcast time slots to a requesting vehicle based on the position of its neighbouring CHs and the number CMs (per neighbouring CH).

Let us consider clusters U_n and U_m of N, M vehicles (see Figure 3.1):

$$U_n = \{V_1, \dots, V_n\} \text{ and } U_m = \{V_1, \dots, V_m\};$$

$\overrightarrow{PQ} = (X_m - X_n,\ Y_m - Y_n)$ is the velocity vector where $P(X_n, Y_n)$, $Q(X_m, Y_m)$ are the positions of the CHs (CH_n and CH_m) of U_n and U_m respectively.

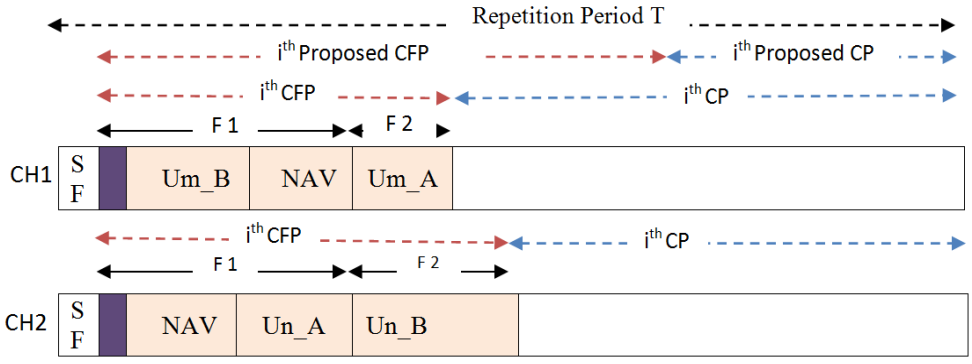
As shown in figure 3.1, Um_BG contains every cluster member CM_i whose position X_i is smaller than $(r + R + X_M = 2.78 * r + X_M)$ and Um_FG contains every cluster member CM_i whose position is bigger than $(2.78 * r + X_M)$. Un_BG contains every cluster member CM_i whose position X_i is smaller than $(X_M - r - R = X_M - 2.78 * r)$ and Un_FG contains every cluster member CM_i whose position is bigger than $(X_M - 2.78 * r)$.

In order to know which slot is assigned to which vehicle, CH_m and CH_n transmit a Start Frame SF to their CMs that contains a map with the time slots allocation of the virtual frame VF =F1+F2. As shown in Figure 3.2-(a), Um_B, Um_A in F1, F2 contain the Time slot of vehicles in BG, FG groups respectively. Newly arriving mobile vehicles in a cluster negotiate the allocation of CFP slots in the CP period on control channel.

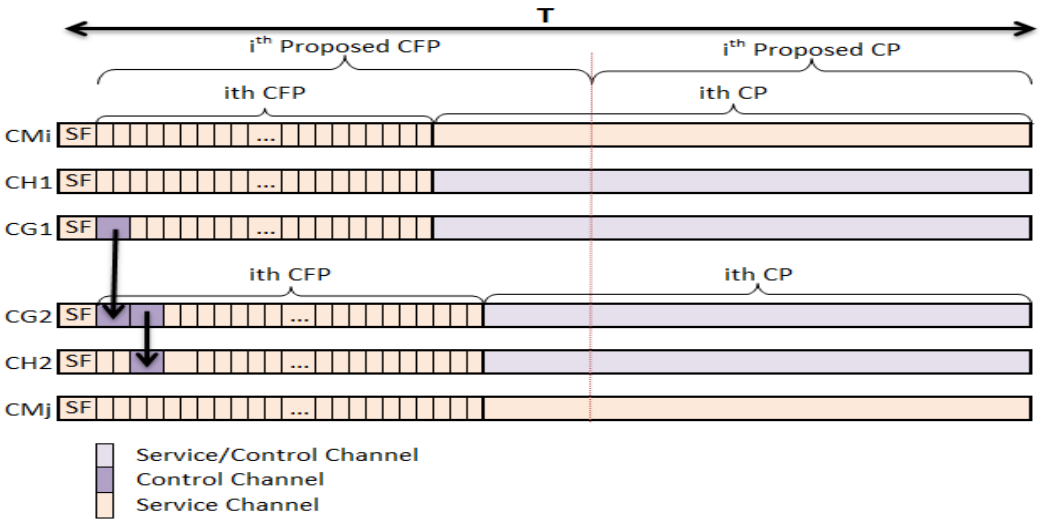
B. Inter-cluster communication

After receiving safety messages, CHs use data fusion techniques (e.g. [11]) to consolidate the safety information and send it to elected CGs on CCH. The CG uses its time slot during CFP period on CCH to forward backward the safety information, to the neighboring CH (see Figure 3.2-(b), or neighboring forward CG in case the current CG is out of neighboring CH range. The CH keeps receiving safety messages from neighboring clusters via CG. Note that, during CP, CMs can exchange data with one another and also with neighboring clusters via service channels. The CH transmits a Start Frame (SF), which

is very similar to a beacon frame. This SF contains the mapping information between CMs and VF time slots. It is broadcasted at the beginning of the service interval to all CMs.



(a)



(b)

Figure 3.2 - The frame structure used for our concept

C. Dynamic CFP channel operation algorithm

If node=CM:

1. Listen on CCH channel and wait for SF.
2. Extract its reserved time slot information from SF and switch listening to SCH.
3. Activate the NAV until its reserved time slot occurrence.
4. Transmit its broadcast periodic safety message after waiting an arbitrary AIFS2 which is longer than AIFS1 used to broadcast emergency safety messages.

5. Wait for the end of dynamic CFP.
6. Transmit its unicast non-safety messages on SCH or switch to CCH if emergency safety messages need to be transmitted and switch back to SCH.
7. Go to 1.

If node=CG:

1. Listen on CCH channel and wait for SF.
2. Extract its reserved time slots information from SF.
3. Activate the NAV until its reserved time slot occurrence.
4. Listen for safety messages from neighbors cluster's CH and forward it to its own CH during its first reserved time slot.
5. Switch to SCH and Transmit its broadcast periodic safety message during its second reserved time slot.
6. Wait for the end of dynamic CFP.
7. Transmit its unicast non-safety messages on SCH or switch to CCH if emergency safety messages need to be transmitted and switch back to SCH.
8. Go to 1.

If node=CH:

1. Compute its own reserved set of time slots (based on the number of CMs) in addition to its CMs reserved time slots and transmit this information in SF on CCH channel.
2. Forward safety messages to neighboring CHs via CGs during its reserved time slots.
3. Switch to SCH and transmit its broadcast periodic safety message.

4. Wait for the end of dynamic CFP.
5. Transmit its unicast non-safety messages on SCH or switch to CCH if emergency safety messages need to be transmitted and switch back to SCH.
6. Go to 1.

VI. SIMULATION RESULTS

In this section, we present our simulation and analysis to evaluate the proposed protocol.

A. Simulator Setup

All simulations are run using NS-2 version 2.33. Table 1 lists the various IEEE 802.11p parameters settings configured in the simulator.

TABLE 3.1. VARIOUS PARAMETER VALUES USED IN THE SIMULATOR

Parameter	Value
Power	6 dBm
Frequency	5.9 GHz
Data Rate	6Mbps
RxTh	-87.88 dBm
CSTh	-91 dBm
CpTh	4 dB
Slot Time	9 µs
SIFS Time	16 µs
Preamble Length	60 bit

Based on a transmission rate of R=6 Mbps, and a packet size of S=200 bytes, including 25 bytes of header, the lowest theoretical transmission delay is $T_{Slot} = 0.3\text{ms}$. Considering that collision warning messages should have a maximum delay of 100 ms to be able to provide a reliable service. Therefore, we set RP (T) to 100 ms, and the max length of a TDMA frame $T_{cfb} = 70\text{ms}$.

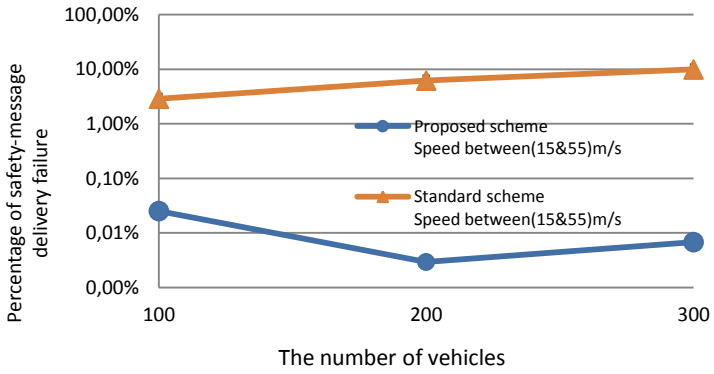


Figure 3.3 - The probability of safety-message delivery failure vs. the density of vehicles

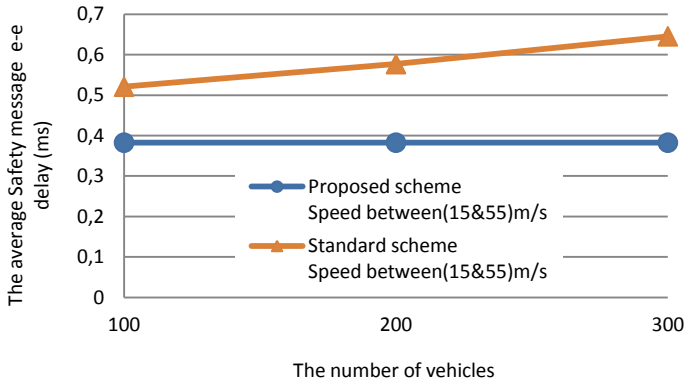


Figure 3.4 - The average Safety message Link delay vs.the densities of vehicles

B. Scenario description

The mobility model used in the simulations is the freeway mobility model with four highway lanes, all in the same direction. When vehicles arrive at the end of the highway, they wrap around from the beginning position of the same lane of the highway. The scenario setup is shown in Figure 3.1. Each node in the simulation is restricted to only travel within its lane. The velocity of each node is temporally restricted based on the nodes previous velocity. A safety distance is maintained so that a node cannot exceed the velocity of the node in front of it if they are within the safety distance.

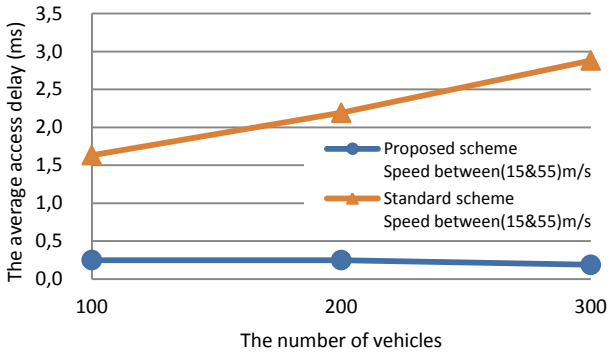


Figure 3.5 - The average access delay vs. the densities of vehicles

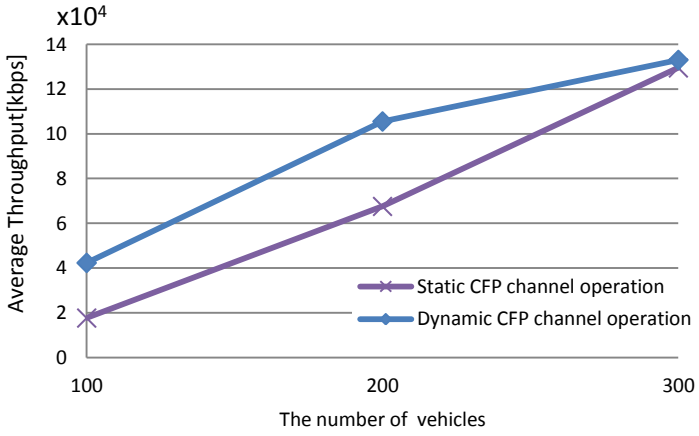


Figure 3.6 - Throughput: dynamic CFP vs. Static CFP

We consider the following metrics to evaluate our proposed scheme (1) Average safety message delivery delay: $\overline{D} = \frac{1}{n}\sum_{i=1}^{n} d_i$ where n is the total number of vehicles, d_i is the time taken to send and receive a data packet ; (2) Probability of safety message delivery failure: $\overline{P} = \frac{1}{n}\sum_{i=1}^{n} P(S_i)$; $P(S) = \frac{1}{x}(\frac{1}{m}\sum_{i=1}^{m} y_i)$ where n is the total number of vehicles in our simulation, x is the packet generation rate, m is number of neighbors of node S, y_i is the number of packets unsuccessfully received from sender S and (3) The non-safety message

throughput: the average rate of successful message delivery over the whole target region in the network.

A velocity range is specified for the nodes; the acceleration of the vehicles is set to 10% of the maximum velocity. To determine the effectiveness of our proposed broadcast algorithm, described in Section IV, a number of simulations were carried out. In these simulations, we compare the performance of the standard 802.11p protocol against our proposed adaptive and reservation based protocol. We consider the results for three different cases in terms of densities of vehicles, including low density, medium density, and high density. The vehicle density cases that were considered are on average 100 (low density), 200 (medium density) and 300 (high density) vehicles/km/4 lanes. For each traffic density, the average preferred speed of vehicles varies uniformly between 15 and 55 m/s. We use Constant Bit Rate (CBR) traffic of 10 packets per seconds to simulate the safety message application packet generator in each vehicle.

Figure 3.3 presents the probability of safety-message delivery failure when we increase the number of vehicles and the average speed. Figure 3.4 shows the safety message delivery delay for different densities of vehicles and average preferred speeds. Using our proposed scheme, we observe that, the probability of safety-message delivery failure does not increase with the increase of the number of vehicles and does not exceed 0.05% in the worst case versus 9.5% for the standard scheme. We also observe that our proposed scheme, compared to the standard one, can achieve a low and stable safety-message delivery failure probability as well as a low average safety message delay under different traffic scenarios (Figure 3.4). This is due to the proposed time slot scheduling protocol implemented with the clustering techniques (CMs of a cluster exchange safety messages without contention, leading to the timely safety-message delivery), which can significantly decrease the packet collisions and increase the successful broadcast rate. Figure 3.5 also shows that unlike the standard scheme, all nodes are not trying to simultaneously access the channel, and therefore the access delay remains short. Furthermore, since the packets are transmitted during their reserved time slot in the service

interval no later than 100 ms on each hop, our protocol provides a bounded constant delay in average.

Figure 3.6 shows the gains in non-safety message throughput for a dynamic and a static CFP channel operation algorithm when static CFP period is 70ms against the densities of vehicles.

We can observe that for low and medium densities of vehicles (100 and 200), the proposed dynamic CFP channel operation algorithm can provide higher throughput on the SCH compared to the static CFP channel operation algorithm while guaranteeing low delays and high delivery rates on CCH. However, when the vehicle density is high (300), the dynamic and static CFP channel operation algorithms provide the same throughput. This is due to the saturation of the total number of time slots that can be used in dynamic CFP.

VII. CONCLUSION

In this paper, we proposed a new contention-free broadcast protocol for periodic safety messages in vehicular networks. It is based on a dynamic time slot reservation schedule managed by stable CHs that continually adjust to vehicle dynamics. It provides an efficient utilization of the time slots for the exact number of active vehicles including hidden nodes. Moreover, the overhead is reduced using single reservation request for a periodic medium access during a vehicle's cluster session. The simulation results show that the proposed protocol can significantly improve the delivery ratio of periodic safety messages while providing a bounded access delay. We also show that a dynamic CFP used in combination with our protocol provides a higher throughput compared to a static CFP. As a future work, a comparison with other existing broadcast protocols other than the standard 802.11p will be performed. Furthermore, an anticipation of time slot reservations for vehicles joining/leaving a cluster can be investigated, since vehicles movements in a highway are predictable to some extent. For instance, the Efficient Neighborhood Prediction Protocol [10] is one of the good examples of prediction protocols that can be used for that purpose.

References

[1] D. Jiang, V. Taliwal, A. Meier, W. Holfelder, and R. Herrtwich, "Design of 5.9 GHz DSRC-based vehicular safety communication," IEEE Wireless Communications, vol. 13, pp. 36-43, 2006.

[2] V. Naumov, R. Baumann, and T. Gross, “An evaluation of inter-vehicle ad hoc networks based on realistic vehicular traces,” in MobiHoc : Proceedings of the seventh ACM international symposium on Mobile ad hoc networking and computing, pp. 108–119, 2006.

[3] M.-T. Sun, W. Feng, T. Lai, K. Yamada, H. Okada, and K. Fujimura, “GPS-based message broadcast for adaptive intervehicle communications,” in Proceedings of the IEEE Vehicular Technology Conference (VTC), vol. 6, pp. 2685–2692, 2000.

[4] G. Korkma z, and E. Ekici, “Urban Multi-Hop Broadcast Protocol for Inter-Vehicle Communication Systems,” Proceedings of the 1st ACM international workshop on VANETs, pp.76-85, 2004.

[5] T. Osa fune, L. Lin, and M. Lenardi, “Multi-Hop Vehicular Broadcast (MHVB),” Proceedings of the 6th IEEE ITS Telecom., pp.757-760, 2006.

[6] M.N. Mariyasagayam, T. Osafune, M. Lenardi, Enhanced Multi-Hop Vehicular Broadcast (MHVB) for Active Safety Applications, 7th International Conference on ITS Telecommunications, pp. 223-228, 2007.

[7] H. Wu, R. Fujimoto, R. Guensler, and M. Hunter, “MDDV: A mobilitycentric data dissemination algorithm for vehicular networks,” in Proc. 1st ACM VANET, pp. 47–56, 2004.

[8] J. Härri, C. Bonnet, and F. Filali, "Kinetic mobility management applied to vehicular ad hoc network protocols," Computer Communications, vol. 31, pp. 2907-2924, 2008.

[9] C. Palazzi, S. Ferretti, and M. Roccetti, "Fast Multi-Hop Broadcast over Vehicular Networks: A Real Testbed Evaluation," Consumer Communications and Networking Conference, (CCNC). 6th IEEE, pp. 1-5, 2009.

[10] C. Rezende, R. Pazzi, and A. Boukerche, "An efficient neighborhood prediction protocol to estimate link availability in VANETs," In Proceedings of MOBIWAC, pp. 83-90, 2009.

[11] H. Su and X. Zhang, "Clustering-Based Multichannel MAC Protocols for QoS Provisionings Over Vehicular Ad Hoc Networks," IEEE Transactions on Vehicular Technology, vol. 56, pp. 3309-3323, 2007.

[12] Z. Rawashdeh and S. Mahmud, "Media access technique for cluster-based vehicular ad hoc networks," Vehicular Technology Conference, VTC 2008-Fall. IEEE 68th, pp. 1–5, 2008.

[13] R. T. Goonewardene, F. H. Ali, and E. Stipidis, "Robust Mobility Adaptive Clustering Scheme with Support for Geographic Routing for Vehicular Ad Hoc Networks," IEEE Journals on Intelligent Transport Systems, vol. 3, no. 2, pp. 148-158, 2009.

[14] K. Xu, M. Gerla, and S. Bae. "Effectiveness of RTS/CTS handshake in IEEE 802.11 based ad hoc networks. Journal of Ad Hoc Networks," Ad Hoc Networks J., vol. 1, pp. 107-123, 2003.

[15] N. Balan and J. Guo, "Increasing broadcast reliability in vehicular ad hoc Networks," in Proc. the 3rd ACM International Workshop on Vehicular Ad Hoc Networks (VANET), 2006.

[16] Shea, Christine; Hassanabadi, Behnam; Valaee, Shahrokh "Mobility Based Clustering in VANETs Using Affinity Propagation," in IEEE GlobeCom, P. 1-6, 2009.

Chapitre 4

Ce chapitre correspond à notre deuxième article «A new stability-based clustering Algorithm (SBCA) for VANETs », qui a été soumis à IEEE ICC conférence, 2011.

Ma contribution, dans cet article a été la suivante : (1) Développement d'un nouveau algorithme de regroupement ("clustering") basé sur la stabilité pour les réseaux véhiculaires (voir Chapitre 4, page 71/72); et (2) Implémentation de cet algorithme puis comparaison et analyse des résultats avec d'autres algorithmes de regroupement.

Résumé en Français

Dernièrement, des efforts de recherches approfondies ont été déployés pour améliorer les algorithmes de *clustering* afin d'organiser les nœuds dans les réseaux ad hoc véhiculaires (VANETs, Vehicular Ad Hoc Networks) en groupes de nœuds ou grappes. Pourtant, en raison de la nature dynamique de VANETS, dans lequel les nœuds sont mobiles et peuvent se joindre ou quitter la grappe à tout moment, la stabilité du réseau est fortement perturbée. L'impact de ces perturbations est encore plus fort en ce qui concerne les performances du réseau si ces nœuds sont des têtes de grappes. Par conséquent, la stabilité de la grappe constitue un grand défi à relever pour obtenir une performance. Dans cet article, nous proposons une approche, appelée *stability-based clustering algorithm* (SBCA), qui permet de construire une structure groupée du réseau. SBCA prend en considération les caractéristiques de mobilité, le nombre de voisins et la durée de leadership en vue de fournir une structure de grappes plus stable et ainsi réduire les frais d'entretien (sur débit) des grappes. Des simulations approfondies montrent que l'algorithme proposé peut améliorer considérablement la stabilité du réseau en rendant la durée de vie de chef de grappe plus longue par rapport aux autres algorithmes existants.

A new stability-based clustering Algorithm (SBCA) for VANETs

Ahmed Ahizoune, Abdelhakim Hafid
Network Research Lab, University of Montreal, Canada

Abstract

Lately, extensive research efforts have been dedicated to the design of clustering algorithms to organize nodes in Vehicular Ad Hoc Networks (VANETs) into sets of clusters. However, due to the dynamic nature of VANETS, nodes frequently joining or leaving clusters jeopardize the stability of the network. The impact of these perturbations becomes worse on network performance if these nodes are cluster heads. Therefore, cluster stability is the key to maintain a predictable performance and has to consider reducing the clustering overhead, the routing overhead and the data losses. In this paper, we propose a new stability-based clustering algorithm (SBCA), specifically designed for VANETs, which takes mobility, number of neighbors, and leadership (i.e., cluster head) duration into consideration in order to provide a more stable architecture. Extensive simulations show that the proposed scheme can significantly improve the stability of the network by extending the cluster head lifetime longer than other previous popular clustering algorithms do.

Keywords- *Vehicular Ad Hoc Network, Clustering Stability, Communications Overhead, Cluster Residence Time.*

Status: This paper is submitted to IEEE ICC Conference, 2011 [36].

I. INTRODUCTION

New wireless technologies have the potential to enable inter-vehicle communications with the purpose of crash avoidance and transportation system efficiency improvement. Consequently, the Federal Communications Commission (FCC) of the U.S. approved the 75MHz bandwidth at 5.850-5.925GHz band, in year 1999, for Intelligent Transportation System (ITS). This wireless spectrum is commonly known as the Dedicated Short-Range Communication (DSRC) allocated by the regulator to be used exclusively for vehicle to vehicle (V2V) and vehicle to roadside (V2R) communications. Due to the high infrastructure cost associated with V2R communications V2V is considered to be a more economical and practical approach for safety and non-safety information delivery.

One of the many challenges in VANETs is the dynamic and dense network topology. The dynamic topology causes significant re-routing difficulties and thus congestion, while the dense network leads to the hidden terminal problem. A clustered structure can make the network appear smaller and more stable in the view of each node. By clustering the vehicles into groups of similar mobility, the relative mobility between communicating neighbouring nodes will be reduced, leading to intra-cluster stability; in addition, the hidden terminal problem can be diminished by clustering [9].

Recent ad hoc network research [1, 9, 10] discussing cluster-based MACs and routing schemes, motivates the need for a stable VANET clustering scheme. In this paper, we propose a new stability-based clustering algorithm (SBCA) for VANETs; SBCA aims to increase significantly the stability and reliability in VANETs.

The remainder of this paper is organized as follows. In Section II, we present related work. Section III describes SBCA. Section IV presents simulation and performance analysis. Section V concludes the paper.

II. RELATED WORK

Figure 4.1 shows a cluster that is composed of 2 Cluster Heads (CH), one Cluster Gateway (CG), and 6 Cluster Members (CM). All the mobile nodes within the radio range

of CH are selected CMs of the cluster. A CG is CM that belongs to more than one cluster; it acts as the communication gateway between CHs. Sometimes, an additional state called Undecided State (US) is used for the initial state of a node.

Fan et al. [3] propose a utility-based clustering scheme; a vehicle chooses its CH based on the values produced by the utility function after receiving status information from neighbouring nodes. The node with the highest utility value is selected. This approach attempts to improve the performance of classical clustering algorithms by making them aware of the vehicle's movement; however, all nodes attempt to re-evaluate their conditions (computing utility values) at the same time which may cause traffic increase and therefore consume more bandwidth.

Node mobility should play an integral part in cluster creation in order to achieve stability. In [2], mobility is addressed during clusters' collisions; when two CHs come within range, the winning CH will be the one with both lower relative mobility and closer proximity to its members. The algorithm used for cluster formation is based on CBLR [6]. Alternatively, Kayis et al. [1411] address mobility by classifying nodes into speed groups, such that nodes will only join a CH of similar velocity.

Kwon and Gerla [3] proposed a Passive Clustering algorithm (PC) for on demand creation and maintenance of the clustering structure which can avoid potential long setup time and reduce re-forwarding significantly. PC performs well in a high mobility network where cluster topology changes frequently. PC is immune from increased control overhead due to frequent changes in network topology; it is, however, dependent on traffic to function.

Similarly, several other existing clustering algorithms in the literature have been proposed for VANETs considering cluster stability as the design objective. De souza et al. [11] present a beacon-based clustering algorithm aimed at extending the cluster lifetime in VANETs; it uses a new aggregate local mobility criterion to decide cluster reorganization. The scheme incorporates a contention method to avoid triggering frequent reorganizations when two CHs encounter each other for a short period of time. Shea et al. [12] use the

Affinity Propagation algorithm in a distributed manner; this algorithm determines clusters that minimize both relative mobility and distance from each CH to its CMs; the resulting clusters are stable. Fan et al. [13] present a theoretical analysis of a directional stability based clustering algorithm. Rawashdeh et al. [10] propose establishing clusters to maximize the advance of the relayed information and to avoid interferences; however, they assume that a CH must know the exact positions of nodes in the cluster which is difficult to achieve in real life situations.

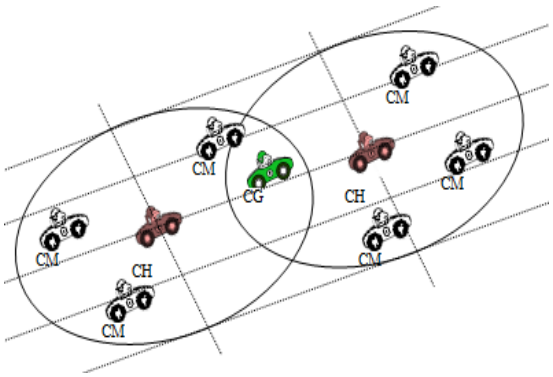


Figure 4.1 - A configuration of clusters

Most implementations of these existing algorithms focus mainly on how CHs are elected. The communication overhead for the formation and maintenance of clusters have not been taken fully into account. There has been few contributions that assess analytically the communication overhead incurred in hierarchical routing. In particular, Fan et al. [13] show that the overhead incurred by DISCA [13] is bound by a constant per node per time step, avoiding expensive re-clustering chain reactions; hence, this overhead increases with the number of nodes.

Since a CH acts as a coordinator in a cluster, if it is absent for any reason, the clustering architecture has to be reconfigured; this will significantly increase the message overhead. However, in our research, we believe that a more efficient way to form a stable clustering architecture, with reduced overhead, is that a mobile node should be associated

to a cluster and not to a CH. Indeed, replacing CH is considered only as an incremental update and does not require a whole reconfiguration of the cluster structure; this will definitively increase the lifetime of the clustering architecture. The resulting clusters are stable and exhibit long average CM duration, long average CH duration, and low average rate of CH changes. In this paper, we propose a new stability-based clustering algorithm protocol (SBCA) aiming to reduce the communication overhead that is caused by the cluster formation and maintenance, as well as to increase the lifetime of the cluster. SBCA makes use of (1) The cluster configuration protocol that is based on the velocities' differences among neighboring vehicles to select a primary CH (PCH) for each cluster; and (2) The election of a secondary CH (SCH) for each cluster; similarly to the clustering scheme proposed in [5], SCH works as a backup for PCH.

III. THE SBCA PROTOCOL DESCRIPTION

In this section, we describe how SBCA forms and maintains stable clustering architecture able to achieve stability and thus low communication overhead. SBCA involves two phases: setup and maintenance. In the cluster setup phase, nodes in close proximity to each other are organized into clusters with CHs selected. In the cluster maintenance step, a secondary CH (SCH) is selected for each cluster; CHs selected in the setup phase become primary CHs (PCH). The nodes remain associated with a given cluster (and not CH as in existing approaches); indeed, when a PCH is no longer in the cluster, SCH takes over; the cluster structure does not change but only the node playing the role of CH. This allows for stable cluster architecture, with low overhead, and thus better performance.

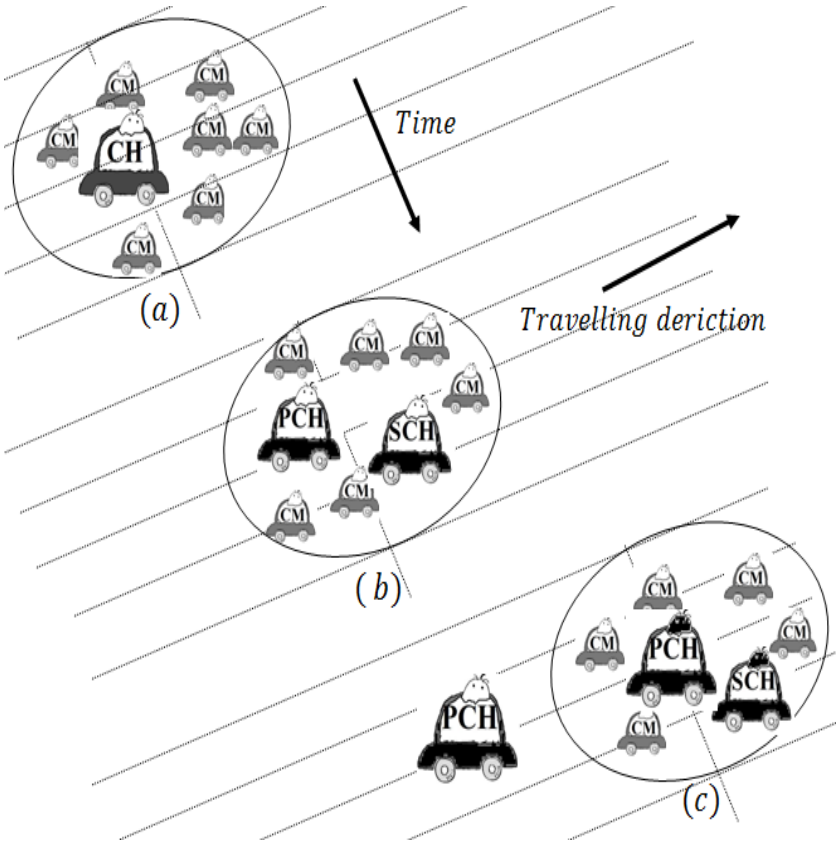


Figure 4.2- Illustrated example. (a) Setup phase; (b) Maintenance phase: SCH selection; and (c) Maintenance phase: SCH becoming PCH

Before discussing the details of SBCA, let us consider an example that shows how SBCA provides cluster stability and thus less overhead. Figure 4.2 (a) shows a cluster with CH and a number of CMs; this structure can be created, for example, using CCP [1]. Figure 4.2 (b) shows a cluster with two CHs: primary cluster head (PCH) and secondary cluster head (SCH); PCH corresponds to CH in Figure 4.2 (a) and SCH is elected using SBCA. Figure 4.2 (c) shows that when PCH is out of the cluster (e.g., slows down to take an exit), SCH takes the role of PCH and a new SCH is elected. Thus, the original cluster (Figure 4.2 (a)) still exists; the only change concerns a new CH (PCH). This means that CMs do not have to look for a new cluster (as in the case of existing protocols, such as CCP [1]) and

thus do not need to generate extra packets (overhead) to perform this action. The only overhead generated by SBCA, in this case, is the maintenance and selection of SCH.

A. Setup Phase

In the SBCA setup phase, the main activities consist of the cluster structure creation and the election of CHs. The operation of SBCA in this phase represents an adapted version of CCP [1].

Initially, every network node is in Undecided State (US). If a node receives an invite-to-join (ITJ) message (in this case a neighboring CH exists; CH sends invite-to-join (ITJ) messages every tj time units), it will check the received signal strength denoted Pr; in the case where Pr is bigger than some predefined threshold Pth, the node sends a request-to-join (RTJ) message, to the neighboring CH, including the node's ID and the network address to the advertising CH; upon receipt of the corresponding ACK, the node becomes CM of this cluster. If a node stays in US more than tj time units (i.e., does not receive ITJ message during [t,t+tj]), then the node becomes CH.

A node remains CM (of a cluster) as long as it receives ITJ message from its CH every tj time units. If it does not receive ITJ message during [t, t+2tj], it considers its association, with its CH, is lost and switches to US. If a CM receives an ITJ message (with Pr bigger than Pth) from another neighboring CH, then it switches to CG after sending RTJ and receiving the corresponding ACK.

A CH broadcasts ITJ messages every tj time units; upon receipt of a RTJ message, it sends an ACK and adds the requesting node to its cluster-member list. If CH does not hear from one of its CMs during [t, t+3tj], it removes this CM from its cluster-member list. A CH switches to US, if its cluster-member list becomes empty. If a CH is in the transmission range of another CH (i.e., both will receive ITJ messages from each other), only one of them will keep its CH role while the other(s) will become CM; the CMs of the cluster (whose CH has just become CM) will switch to US; they will change their role according to the procedure explained earlier (e.g., they will all become CMs of the new CH if they are in the transmission rage of this CH). The decision of CH to give up or not its role

is based on a weighted factor CH* (see Equation 1); this factor represents the minimum of the difference between the sum of velocity differences between the CH and its neighboring nodes and the number of neighboring nodes of this CH. The CH that will keep its role corresponds to CH that produces the minimum value of this difference.

$$CH^{*} = \arg_{CH}\min\left[\alpha * \sum_{i \in Cluster(CH)} |V_{CH} - V_i| - \beta * N_{neighbors}\right]; \quad (1)$$

where $\alpha + \beta = 1$, i is a CM of the cluster headed by CH, V_{CH} is the speed of CH, V_i is the speed of i, and $N_{neighbors}$ is the number of neighboring nodes of CH.

B. Maintenance phase

The objective of the maintenance phase is to achieve stability and reliability (less packet losses and thus better packet delivery) of the cluster structure produced in the setup phase. The basic idea is to use two CHs: (a) primary CH (PCH): it is elected in the setup phase; and (b) secondary CH (SCH): it is elected in the maintenance phase.

Once a PCH is elected during the setup phase, it generates a unique identifier, Cluster_ID, for the cluster. Cluster_ID is computed using the following hash function:

$$Cluster\_ID = Hash(t \oplus PCH\_ID) \quad (2)$$

where t is the current time and PCH_ID is the unique identifier of the primary cluster head.

PCH periodically selects SCH among its CMs; the node that produces the minimum sum, of velocity difference between PCH and CM and distance between PCH and CM (see Equation 3), is selected SCH.

$$SCH^{*} = arg_i min\left[\alpha * \left|V_{PCH} - V_i\right| + \beta * D_i\right]; \quad (3)$$

where $\alpha + \beta = 1$, i is a CM of the cluster headed by PCH, V_{PCH} is the speed of PCH, V_i is the speed of i, and D_i is the distance between PCH and i.

If PCH can no longer be a CH (e.g., leaving the cluster by taking a highway exit), it will order SCH to switch to PCH and change its own state to CM; it will eventually change to undecided state when it no longer receives ITJ messages. The new PCH will keep the same identifier (Cluster_ID) as the previous PCH; thus, the cluster structure will remain intact (CMs of the cluster do not have to reorganize in new cluster(s) as the case of existing protocols); indeed, no re-clustering is needed and thus no re-clustering overhead is generated. The new PCH will also select a new SCH.

In VANETS, nodes are highly mobile; thus, the determination of when PCH needs to order SCH to take the role of PCH is a challenge. We propose to use mobility prediction techniques to allow PCH to predict, ahead of time, when it will move out of the cluster; thus, it will have enough time to communicate with SCH. Mobility prediction is not trivial in MANET [5]; the random way point mobility models [7] are widely applied. Fortunately, with the roadway topology constraints in VANET, we can use the existing driver behaviour model [8] to make a better mobility prediction; this will increase the probability of a better communication between PCH and SCH during the switching process and thus better reliability (in terms of packet losses and packet delivery). However, in the case where PCH moves out of the cluster without notifying SCH (e.g., bad mobility prediction), SCH will elect itself PCH after T time units without receiving ITJ messages from its PCH; we believe that such cases will be rare.

IV. SIMULATION RESULTS

In this section, we present our simulation and analysis evaluation of our proposed protocol.

A. Simulator Setup

All simulations are run using NS-2 version 2.33. Table I lists the various IEEE 802.11p parameters settings configured in the simulator.

TABLE 4.1. PARAMETERS' VALUES USED IN THE SIMULATION

Parameter	Value
Power	6 dBm
Frequency	5.9 GHz
Data Rate	6Mbps
RxTh	-87.88 dBm
CSTh	-91 dBm
CpTh	4 dB
Slot Time	9 µs
SIFS Time	16 µs
Preamble Length	60 bit

B. Scenario description

The mobility model used in the simulations is the freeway mobility model with four highway lanes, all in the same direction. When vehicles arrive at the end of the highway, they wrap around from the beginning position of the same lane of the highway. The scenario setup is shown in Figure 4.1. Each node in the simulation is restricted to only travel within its lane. The velocity of each node is temporally restricted based on the node's previous velocity. A safety distance is maintained so that a node cannot exceed the velocity of the node in front of it if they are within the safety distance.

A velocity range is specified for the nodes and the vehicle acceleration is set to 10% of the maximum velocity. In these simulations, we compare the performance of the cluster

configuration protocol (CCP) proposed in [1] against our proposed SBCA protocol; CCP has been chosen because it provides better CH stability, better cluster structure stability and low communication overhead compared to existing protocols. We consider the results for three different cases in terms of vehicle densities, including low, medium and high; these values are on average 50 (low density), 100 (medium density) and 150 (high density) vehicles/km/4 lanes. For each traffic density, the average preferred vehicle speed varies uniformly between 25 and 35 m/s. In each scenario (with a distinct traffic density), we ran the simulations ten times to obtain the mean value of the final performance metric.

C. Simulation Results

To evaluate our proposed scheme we considered the following metrics: (1) Average cluster lifetime: the time a node remains associated with a given cluster; (2) Clustering overhead: the total clustering related messages (i.e., RTJ, ITJ and corresponding ACK) divided by the total messages that are transmitted; this is an important metric because it shows how efficient the scheme is in reducing clustering communication overhead; and (3) Packet delivery ratio, the number of packets successfully delivered divided by the total number of packets generated.

Figure 4.3 shows that the average cluster lifetime, when using SBCA, is considerably bigger than the average cluster lifetime when using CCP. Therefore, we can conclude that, when using SCBA, the cluster topology is more stable, since CMs are associated with the cluster and not CH; in the case of CCP, if the CH is absent for any reason, the cluster will collapse and a new cluster will be formed. However, with SCBA, when PCH can no longer be a CH, SCH takes over the CH responsibility and thus the cluster leadership will be changed from PCH to SCH; the CMs being heard by their SCH would continue their cluster residency within SCH when it has become a PCH. Hence, the cluster will still survive and its cluster membership lifetime will be extended. Figure 4.3 also shows that when increasing the number of nodes from 50 to 150, the cluster lifetime is gradually improved by three to four times respectively. Therefore, the larger the network is, the more stability our protocol provides compared to the cluster configuration protocol.

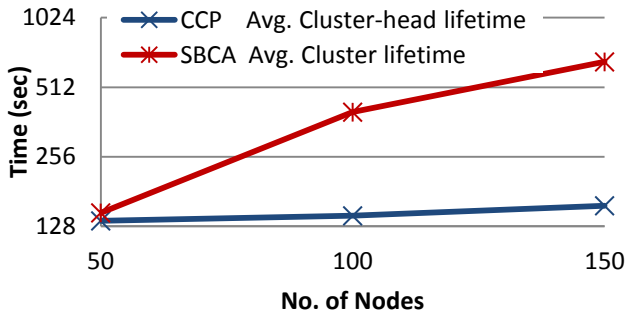


Figure 4.3- Average cluster lifetime vs. density (number of nodes)

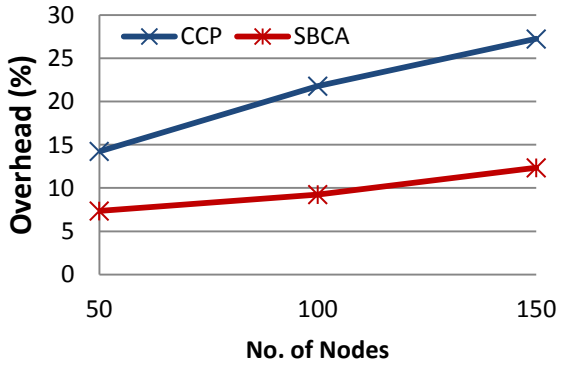


Figure 4.4- Overhead vs. density (number of nodes)

Figure 4.4 shows that the average clustering overhead increases with the number of nodes. This is expected because increasing the number of nodes increases the number of clusters created and generally decreases CH duration. Therefore, a node will join more clusters during its lifetime generating more clustering related messages. Obviously, the overhead generated by SBCA is far less than the overhead generated by CCP; this is expected, since a CH leaving a cluster does not cause necessarily re-clustering, when using SBCA; in this case, SCH takes over the role of cluster head of the cluster; therefore, a node does not need to change clusters and thus does not need to exchange more clustering related messages. We observe, from Figure 4.4, that CCP generates more than twice the overhead generated by SBCA.

Figure 4.5 shows that SBCA performs far better than CCP in terms of communication efficiency. Although the performance generally decreases when the number of nodes in the network increases, SBCA outperforms handily CCP. This can be explained by the fact that SBCA has more stable clusters, thus resulting in fewer route interruptions and thus few packet losses and subsequent packet retransmissions.

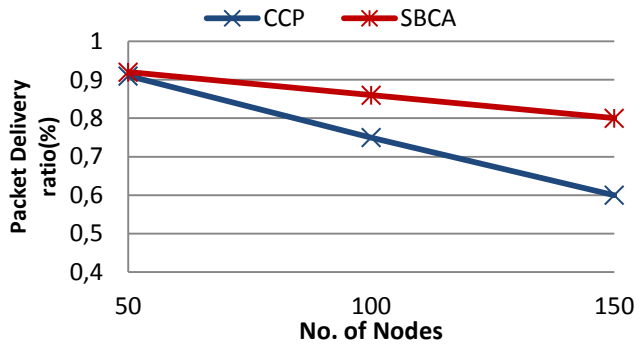


Figure 4.5- Packet Delivery ratio vs. density (number of nodes)

V. CONCLUSION

In this paper we proposed a new clustering algorithm protocol (SBCA) based on stability, for use in VANETs. The SBCA protocol involves two phases, setup and maintenance. In the cluster setup phase, nodes in close vicinity with each other are organized into clusters. In the cluster maintenance step, all nodes remain associated with these clusters, maintaining the hierarchical structure formed within the dynamic environment, thus providing stable cluster architecture and minimizing cluster maintenance costs. The basic idea of SBCA protocol is the election of a secondary cluster head (SCH) for each cluster. SCH works as a backup for PCH, which was selected in setup phase and the future leader of the cluster. The aim of SCH is to provide clustering stability as well as routing reliability. In SBCA, SCH reforms the cluster very quickly, thus reducing the overhead needed to select new cluster heads. The simulation results show that the proposed protocol can significantly improve the cluster residence time, for each node, reducing the overhead and thus improving the performance/reliability (in terms of packet delivery).

References

[1] H. Su and X. Zhang, "Clustering-Based Multichannel MAC Protocols for QoS Provisionings Over Vehicular Ad Hoc Networks," IEEE Transactions on Vehicular Technology, vol.56, pp. 3309-3323, 2007.

[2] Y. Gunter, B. Wiegel, and H. P. Grossmann, “Cluster-based medium access scheme for vanets,” Intelligent Transportation Systems Conference, IEEE, pp. 343–348, 2007.

[3] P. Fan, J. G. Haran, J. Dillenburg, and P. C. Nelson, “Cluster-based framework in vehicular ad-hoc networks,” Lecture Notes in Computer Science, vol. 3738, pp. 32–42, 2005.

[4] T. J. Kwon, M. Gerla, V. K. Varma, M. Barton, and T. R. Hsing, “Efficient flooding with passive clustering-an overhead-free selective forward mechanism for ad hoc/sensor networks ,” in Proc. of the IEEE, Vol. 91, Issue 8, pp.1210 - 1220, 2003.

[5] Mohammed S. Al-kahtani, Hussein T. Mouftah. SERC/LC3R: A new paradigm for cluster-based routing in MANETs. In Proceedings of BROADNETS, pp. 469-478, 2005.

[6] R.A. Santos, R.M. Edwards, A. Edwards, ”Cluster-based location routing algorithm for vehicle to vehicle communication”, Radio and Wireless Conference, pp. 39-42, 2004.

[7] W. Su, S.J. Lee and M. Gerla, ”Mobility prediction and routing in adhoc wireless networks,” International Journal of Network Management, Volume 11, No. 1, pp. 3-30, 2001.

[8] K. Nagel, M. Schrekenberg, "A cellular automaton model for freeway traffic", J. Phys. I 2, pp. 2221-2229, 1992.

[9] A. Ahizoune, A. Hafid, R. Ben Ali, “A Contention Free Broadcast Protocol for Periodic Safety Messages in Vehicular Ad-Hoc Networks,” 35th Annual IEEE Conference on Local Computer Networks and Workshops, (LCN), pp. 48-55, 2010.

[10] Z. Rawashdeh and S. Mahmud, “Media access technique for cluster-based vehicular ad hoc networks,” Vehicular Technology Conference,(VTC), IEEE 68th, pp. 1–5, 2008.

[11] E. de Souza, I. Nikolaidis, and P. Gburzynski, "A New Aggregate Local Mobility (ALM) Clustering Algorithm for VANETs." Proceedings of ICC, Cape Town, South Africa, 2010.

[12] C. Shea, B. Hassanabadi, and S. Valaee, “Mobility-based clustering in VANETs using affinity propagation,” in IEEE Globecom, 2009.

[13] P. Fan, P. Sistla, and P. C. Nelson, Theoretical analysis of a directional stability-based clustering algorithm for vanets. Vehicular Ad Hoc Networks, 2008.

[14] S. Kuklinski and G. Wolny, “Density based clustering algorithm for VANETs,” 5th International Conference on Testbeds and Research Infrastructures for the Development of Networks & Communities and Workshops, pp. 1-6, 2009.

[15] O. Kayis and T. Acarman, “Clustering formation for inter-vehicle communication,” Intelligent Transportation Systems Conference, IEEE, pp. 636–641, 2007.

Chapitre 5

Conclusion et perspectives

5.1. Conclusion

Dans ce mémoire, nous nous sommes intéressé aux problèmes majeurs de la diffusion dans les réseaux VANETs : amélioration du taux de livraison des messages de sécurité périodiques, tout en offrant un délai d'accès limité. Nous avons proposé à ce sujet un nouveau protocole de diffusion sans contention pour les messages de sécurité périodiques dans les réseaux VANETs. Il est basé sur un calendrier de réservation dynamique du *time slot* géré par un chef de group stable qui s'adapte continuellement à la dynamique des véhicules. Il prévoit une utilisation efficace des intervalles de temps pour le nombre exact de véhicules actifs, y compris les nœuds cachés. En outre, le surdébit est réduit par l'utilisation d'une demande de réservation unique pour l'accès périodique au support pendant la session de groupe d'un véhicule.

Ce protocole intègre l'approche de gestion centralisée des grappes et la transmission des données dans VANET. Dans cette technique, le temps est divisé en cycles, chaque cycle étant partagé entre les canaux de service et de contrôle, et divisé en deux parties. Au cours de la première partie, nous nous sommes appuyés sur AMRT (Accès multiple par répartition dans le temps) et TDMA (*Time Division Multiple Access*). Dans la deuxième partie, nous nous sommes appuyés sur l'accès multiple avec écoute de porteuse et évitement de collision ou CSMA/CA (*Carrier Sense Multiple Access / Collision Avoidance*s) pour gérer l'accès au médium. En outre, notre protocole ajuste d'une manière adaptative le temps consommé dans la diffusion des messages de sécurité, ce qui permettra une amélioration de la capacité des canaux.

Nous avons démontré, à l'aide de simulations, que le protocole proposé peut améliorer considérablement le taux de livraison des messages de sécurité périodiques tout en offrant un délai d'accès limité. Nous montrons aussi que la dynamique de la CFP utilisé en

combinaison avec notre protocole fournit un débit plus élevé par rapport à un ensemble statique de la CFP.

5.2. Perspectives

Dans la continuité du travail présenté, nous pourrions approfondir notre étude afin d'améliorer les résultats obtenus. Dans le premier volet de ce mémoire, nous avons proposé un nouveau mécanisme de réservation adéquat en particulier pour les applications de diffusion périodique. Dans le deuxième volet, nous avons proposé un nouveau stability-based clustering algorithm (SBCA) conçu pour VANET, qui prend en considération les caractéristiques de mobilité, le nombre de voisins, et la durée de leadership en vue de remédier aux frais d'entretien de cluster et de fournir une architecture plus stable.

Parmi les développements futurs de ce projet, une comparaison avec d'autres protocoles de diffusion existants autres que les 802.11p standard sera effectuée. En outre, une anticipation des réservations de cycles de temps pour les véhicules qui vont joindre/quitter un groupe peut être étudiée; en effet, les mouvements de véhicules sur une route sont prévisibles, dans une certaine mesure. Par exemple, Efficient Neighborhood Prediction Protocol (NPP) [33] est l'un des bons exemples de protocoles de prédiction qui peut être utilisé à cette fin. NPP tente d'anticiper la disponibilité des liens futurs entre les véhicules grâce à un modèle de prédiction de la mobilité. Par conséquent, les changements de topologie peuvent être détectés plus tôt et traités correctement avant de dégrader les performances du réseau.

Bibliographie

[1] D. Jiang, V. Taliwal, A. Meier, W. Holfelder, and R. Herrtwich, "Design of 5.9 GHz DSRC-based vehicular safety communication," IEEE Wireless Communications, vol. 13, p. 36-43, 2006.

[2] M. Sun, W. Feng, T. Lai, K. Yamada, H. Okada, and K. Fujimura, "GPS-based message broadcast for adaptive inter-vehicle communications," in Proc. of International Conference on Parallel Processing (ICPP), pp. 2685-2692, 2000.

[3] V. Naumov, R. Baumann, and T. Gross, "An evaluation of inter-vehicle ad hoc networks based on realistic vehicular traces," in MobiHoc : Proceedings of the seventh ACM international symposium on Mobile ad hoc networking and computing, pp. 108-119, 2006.

[4] L. Wischhof, A. Ebner, H. Rohling, M. Lott, and R. Halfmann, "Adaptive broadcast for travel and traffic information distribution based on inter-vehicle communication," Proc. of IEEE Intelligent Vehicles Symposium, Columbus, 2003.

[5] G. Korkma z, and E. Ekici, "Urban Multi-Hop Broadcast Protocol for Inter-Vehicle Communication Systems," Proceedings of the 1st ACM international workshop on VANETs, Philadelphia, pp.76-85, 2004.

[6] G. Korkmaz, E. Ekici, and F. Özgüner, "An Efficient Fully Ad-Hoc Multi-Hop Broadcast Protocol for Inter-Vehicular Communication Systems," IEEE ICC, vol. 1, 2006.

[7] T. Osa fune, L. Lin, and M. Lenardi, "Multi-Hop Vehicular Broadcast (MHVB)," Proceedings of the 6th IEEE ITS Telecom, pp. 757-760, 2006.

[8] M. Mariyasagayam, T. Osafune and M. Lenardi, "Enhanced Multi-Hop Vehicular Broadcast (MHVB) for Active Safety Applications", in Proceedings of the 7th International Conference on ITS Telecommunications (ITST), pp. 1-6, 2007.

[9] H. Wu, R. Fujimoto, R. Guensler, and M. Hunter, “MDDV: A mobilitycentric data dissemination algorithm for vehicular networks,” in Proc. 1st ACM VANET, pp. 47-56, 2004.

[10] Jiang Daniel and Delgrossi Luca, “IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments,” IEEE VTC, pp. 2036-2040, 2008.

[11] N. Balan and J. Guo, “Increasing broadcast reliability in vehicular ad-hoc Networks,” in Proc. the 3rd ACM International Workshop on Vehicular Ad-Hoc Networks (VANET), 2006.

[12] P 802.11 Draft Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, 1997.

[13] A. Ahizoune, A. Hafid, R. Ben Ali, “A Contention Free Broadcast Protocol for Periodic Safety Messages in Vehicular Ad-Hoc Networks,” 35th Annual IEEE Conference on Local Computer Networks and Workshops, (LCN), pp.48-55, 2010.

[14] IEEE 1609 Family of Standards for Wireless Access in Vehicular Environments; available from IEEE Standards.

[15] W. Kiess, J. Rybicki, M. Mauve. "On the nature of Inter-Vehicle Communication", WMAN 2007: Proceedings of the 4th Workshop on Mobile Ad-Hoc Networks, pp. 493-502, 2007.

[16] CAR 2 CAR Communication Consortium Manifesto version 1.1. Technical report,CAR 2 CAR Communication Consortium (C2C-CC), Aug 2007. Available through http://www.car-to-car.org/. Last accessed: 2009.

[17] Vehicle Safety Communications Project Task 3 Final Report. Technical report, The CAMP Vehicle Safety Communications Consortium. Sponsored by U. S. Department of Transportation (USDOT). Available through National Technical Information Service, Springfield, Virginia 22161, 2005.

[18] Moez Jerbi, Rabah Meraihi, Sidi-Mohammed Senouci, and Yacine Ghamri-Doudane. An Improved Vehicular Ad-Hoc Routing Protocol for City

Environments. IEEE International Conference on Communications (ICC), pp. 3972-3979, 2007.

[19] H. HO Yao, H. HO Ai, A. HUA Kien. "Routing protocols for inter-vehicular networks: A comparative study in high-mobility and large obstacles environments," Computer Communications Journal (ComCom), 2008.

[20] Sze-Yao Ni, Yu-Chee Tseng, Yuh-Shyan Chen, Jang-Ping Sheu, The broadcast storm problem in a mobile ad hoc network, Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking, pp.151-162, 1999.

[21] O. Tonguz, N. Wisitpongphan, F. Bai, P. Mudalige, V. Sadekar, " Broadcastin in VANET" Mobile Networking for Vehicular Environments, pp. 7-12, 2007.

[22] Yin, J., ElBatt, T., Yeung, G., Ryu, B., Habermas, S., Krishnan, H. et Talty, T. "Performance evaluation of safety applications over dsrc vehicular ad-hoc networks," In Proceedings of the 1st ACM international workshop on Vehicular ad-hoc networks (VANET), 2004.

[23] Bishop, R. (2005). Intelligent Vehicle Technology and Trends. Artech House. Borgonovo, F., Campelli, L., Cesana, M., Coletti, L. et di Milano, P. Mac for ad-hoc inter-vehicle network: services and performance. In Proceedings of the Vehicular Technology Conference (VTC), pp. 2789-2793, 2003.

[24] H. Su and X. Zhang, "Clustering-Based Multichannel MAC Protocols for QoS Provisionings Over Vehicular Ad Hoc Networks," IEEE Transactions on Vehicular Technology, vol. 56, pp. 3309-3323, 2007.

[25] IEEE 802.11p Amendment, "Wireless Access in Vehicular Environments," v. D3.0, work in progress, 2007.

[26] DSRC (Dedicated Short Range Communication), http://www.leearmstrong.com/DSRC/DSRCHomeset.htm

[27] A. Benslimane, et A. Bachir, "Réseaux Ad Hoc Mobiles : Géodiffusion InterVéhicules", Chapitre de livre traité IC2 : L'internet ambiant, HERMES Science Publisher, pp. 215-236, 2004.

[28] L. Briesemeister , and G. Hommel,"Role-based multicast in highly mobile but sparsely connected ad hoc networks", First annul workshop on Mobile and Ad Hoc Networking and Computing (MobiHOC), pp. 45-50, 2000.

[29] Q. Xu, T. Mak, J. Ko, and R. Sengupta, "Vehicle-to-vehicle safety messaging in DSRC," In Proc. of the 1st ACM Int. Workshop on Vehicular Ad Hoc Networks (VANET), pp.19-28, 2004.

[30] J. Xie, A. Das, S. Nandi, and A.K. Gupta, "Improving the reliability of IEEE 802.11 broadcast scheme for multicasting in mobile ad hoc networks," In Proc. of the IEEE Wireless Communications and Networking Conf., vol.1, pp.126-131, 2005

[31] Moez JERBI: « Protocoles pour les communications dans les réseaux de véhicules en environnement urbain: Routage et GeoCast basés sur les intersections », Université d'Evry Val d'Essonne, Thèse de Doctorat soutenue en Novembre 2008.

[32] D. B. Johnson and D. A. Maltz, 'Dynamic source routing in ad hoc wireless networks', volume 353, Kluwer Academic Publishers, 1996.

[33] C. Rezende, R. Pazzi, and A. Boukerche, "An efficient neighborhood prediction protocol to estimate link availability in VANETs," pp. 83-90, 2009.

[34] Z. Rawashdeh and S. Mahmud, "Media Access Technique for Cluster-Based Vehicular Ad Hoc Networks," pp. 1-5, 2008.

[35] Yu, Fan F. and Biswas, S. A Self-Organizing MAC Protocol for DSRC based Vehicular Ad Hoc Networks, ICDCS Workshops 2007.

[36] A. Ahizoune, A. Hafid, "A new stability-based clustering Algorithm (SBCA) for VANETs," submitted to IEEE ICC Conference, 2011.