



Université
de Toulouse

THÈSE

En vue de l'obtention du

DOCTORAT DE L'UNIVERSITÉ DE TOULOUSE

Délivré par : *l'Université Toulouse 3 Paul Sabatier (UT3 Paul Sabatier)*

Présentée et soutenue le *15/10/2015* par :

Adel BERRADJ

**Contrôle de la diffusion multi-saut pour la dissémination de messages
d'alerte dans les réseaux véhiculaires**

JURY

PASCAL LORENZ	Professeur, Université de Haute-Alsace	Rapporteur
CONGDUC PHAM	Professeur, Université de Pau et des Pays de l'Adour	Rapporteur
FRANCINE KRIEF	Professeur, ENSEIRB-MATMECA, Bordeaux	Examinateur
ANDRÉ-LUC BEYLOT	Professeur, ENSEEIHT-INP, Toulouse	Examinateur
THIERRY GAYRAUD	Professeur, Université Toulouse III	Examinateur
ZOUBIR MAMMERI	Professeur, Université Toulouse III	Directeur de thèse

École doctorale et spécialité :

MITT : Domaine STIC : Réseaux, Télécoms, Systèmes et Architecture

Unité de Recherche :

Institut de Recherche en Informatique de Toulouse (UMR 5505)

Directeur(s) de Thèse :

Zoubir MAMMERI

Rapporteurs :

Pascal LORENZ et Congduc PHAM

**Contrôle de la diffusion multi-saut pour la dissémination de
messages d'alerte dans les réseaux véhiculaires**

Par
Adel BERRADJ

Thèse en vue de l'obtention du titre Docteur de l'Université de Toulouse III

Toulouse, France
15 Octobre 2015

Remerciements

Après ces années de travail laborieux voici le temps de pouvoir remercier les personnes ayant contribué à la réussite de cette thèse.

Tout d'abord, je souhaite exprimer mes sincères remerciements à Monsieur Zoubir MAMMERY, mon directeur de thèse, pour sa confiance et ses encouragements. Son soutien indéfectible et ses conseils avisés m'ont été d'une grande aide tout au long de ma thèse. Je tiens à le remercier tout particulièrement pour l'excellence de son accompagnement ainsi que pour la confiance et l'autonomie qu'il m'a accordées.

Je souhaite également remercier chaleureusement les rapporteurs de ma thèse : Monsieur Congduc Pham, Professeur à l'Université de Pau et des Pays de l'Adour et Monsieur Pascal Lorenz, Professeur à l'Université de Haute Alsace pour m'avoir fait l'honneur d'accepter de rapporter ce travail et d'accorder du temps à une lecture attentive et détaillée de mon manuscrit. Je tiens également à remercier les examinateurs : Madame Francine KRIEF, Professeur à ENSEIRB-MATMECA Bordeaux, Monsieur André-Luc BEYLOT, Professeur à l'ENSEEIH-T-INP Toulouse ainsi que Monsieur Thierry GAYRAUD, Professeur à l'université Toulouse III d'avoir accepté d'examiner mon travail et de participer à mon jury de thèse.

Mes remerciements vont également à tous les membres de notre équipe de recherche T2RS : Cédric Teyssié, Diané Ibrahima, Charaf Eddin Mohammad, Assef Abakar Zakaria Ghada Jaber et Muhammad Imran Khan. Je remercie particulièrement Rahim KACIMI pour ses conseils et pour sa gentillesse. Je le remercie pour les discussions et les échanges instructifs ainsi que son soutien tout au long de cette thèse. Merci au personnel et à l'ensemble des membres de l'IRIT. Je remercie également tous mes collègues doctorants surtout Mohammed El Malki, Hamid Chellal et son épouse. Des remerciements spéciaux vont à mon meilleur ami Mounir Tarai et mes copains Adel Ziani, Abdenour Smaili et son

épouse.

Je remercie profondément mes parents auxquels je dédie ce travail. Ce succès n'aurait pu avoir lieu sans eux. Un grand merci pour mes sœurs et mon frère Amine, sans oublier mes oncles et mes tantes pour leur soutien et leur aide.

Enfin, merci à mon épouse. Que sa patience, sa confiance, ses encouragements et son soutien sans faille malgré mes absences prolongées et répétées soient ici gratifiées.

Résumé

Les applications de sécurité routière sont la principale motivation des réseaux de véhicules, bien que d'autres applications de gestion du trafic routier et de divertissement soient envisagées. La communication par diffusion sur plusieurs sauts est une composante importante de ces applications telles que, la signalisation du danger sur la route où la diffusion sur plusieurs sauts est utilisée pour notifier un accident sur la route, une présence d'animal, un objet qui barre la route, un freinage brusque du véhicule en avant, etc. Comme l'information traitée dans ces applications est très critique et peut avoir un effet sur la vie humaine, la diffusion doit être rapide et fiable.

Cependant, la diffusion de messages sur plusieurs sauts a de nombreux défis à relever tels que le problème de tempête de diffusion (à savoir, des retransmissions redondantes, une haute charge du canal, une grande contention sur le canal de communication et ainsi, un taux de perte de paquets élevé) dans le cas d'un réseau dense, et le problème de déconnexion quand le réseau est clairsemé. En plus, les applications de sécurité routière sont à temps critique et la satisfaction de leurs exigences est très difficile, car il y a un compromis entre la fiabilité de la dissémination et le délai de livraison.

De nombreux travaux ont été menés ces dernières années et une large gamme de mécanismes ont été proposés. Néanmoins, la plupart d'entre eux souffrent toujours de problèmes de collisions quand le réseau est dense et une latence élevée quand la densité du réseau est faible.

Le but de cette thèse est d'étudier les protocoles permettant une livraison fiable et rapide de messages d'alerte, de comprendre leurs limites et de proposer une solution pour la dissémination rapide et fiable de l'information de sécurité dans un réseau de véhicule.

Abstract

Road safety applications are the main motivation of vehicular networks, although other road traffic management and entertainment applications are considered. The multi-hop broadcasting communication is an important component of these applications, such as Road Hazard Signaling application where the multi-hop broadcasting is used to notify an accident on the road, a presence of animal, an object that blocks the road, sudden braking of the vehicle in front, etc. As the information handled in these applications is very critical and can affect the human life the dissemination must be fast and reliable.

However, broadcasting messages over several hops comes with many challenges to overcome such as broadcast storm problem (i.e. redundant retransmissions, high load of the channel, high contention on the communication channel and thus, high packet loss rate) in the case of dense network, and the problem of disconnection when the network is sparse. In addition, road safety applications are time-critical and satisfaction of their demands is very difficult because there is a trade-off between the dissemination reliability and the delivery delay.

Many studies have been conducted in recent years and a variety of mechanisms have been proposed. However, most of them still suffer from problems of collisions when the network is dense and a high latency when the density of the network is low.

The aim of this thesis is to analyze protocols allowing a reliable and fast delivery of alert messages, understand their limitations and propose a solution for fast and reliable dissemination of safety information in vehicular networks.

Table des matières

Chapitre 1	Introduction	1
1.1	Contexte	1
1.2	Contributions.....	3
1.3	Organisation	4
Chapitre 2	Réseaux véhiculaires: Vue d'ensemble.....	7
2.1	Introduction	7
2.2	Définitions.....	8
2.3	Caractéristiques des VANETs.....	9
2.4	Applications	12
2.4.1	Applications de sécurité routière.....	13
2.4.2	Applications de gestion du trafic routier	16
2.4.3	Applications de divertissement et de confort	17
2.5	Standards et architectures protocolaires	22
2.5.1	Architecture IEEE WAVE	24
2.5.2	Architecture ETSI-ITS	25
2.6	Conclusion.....	27
Chapitre 3	Protocoles de dissémination d'alertes dans les VANETs.....	29
3.1	Introduction	29
3.2	Défis et solutions possibles	30
3.2.1	Défis	31
3.2.2	Bases des approches	32
3.3	Classification des mécanismes de dissémination	33
3.3.1	Approche de conception de bas niveau	34

3.3.2	Approche de conception de haut-niveau	36
3.4	Métriques d'évaluation des protocoles de dissémination.....	40
3.5	Discussion	43
3.6	Conclusion.....	49
Chapitre 4	Analyse de performance des mécanismes de dissémination d'alertes	51
4.1	Introduction	51
4.2	Description des mécanismes	52
4.3	Paramètres et scénario de simulation	54
4.3.1	Paramètres de simulation	54
4.3.2	Scénario.....	55
4.4	Métriques d'évaluation de performance.....	56
4.5	Etude de performance.....	58
4.5.1	Analyse du taux de réception de messages	58
4.5.2	Analyse du délai de livraison	59
4.5.3	Analyse du nombre de sauts.....	60
4.5.4	Analyse de la redondance.....	60
4.5.5	Analyse du nombre de rediffusions.....	61
4.6	Etudes de l'impact de la durée du slot sur la performance des mécanismes de dissémination	63
4.6.1	Délai de livraison	64
4.6.2	Nombre de Sauts	66
4.6.3	Nombre de transmissions redondantes	68
4.7	Conclusion.....	72
Chapitre 5	Un protocole adaptatif pour la dissémination d'alertes	73
5.1	Introduction	73
5.2	Motivation	74
5.3	Protocole proposé.....	78
5.3.1	Scénario et hypothèses	78
5.3.2	Description du protocole	79
5.4	Evaluation de performances	86
5.4.1	Plateformes de simulation	86
5.4.2	Paramètres de simulation	87
5.4.3	Métriques d'évaluation.....	90
5.4.4	Analyse des résultats	90
5.5	Conclusion.....	97

Chapitre 6	Conclusions et perspectives.....	99
6.1	Conclusions	99
6.2	Perspectives.....	101
	Références	101
	Liste des publications	109

Table des figures

Figure 2-1 Les composants d'un VANETS.....	9
Figure 2-2 Exemple d'une Autoroute à Houston [70]	10
Figure 2-3 Bande de fréquences réservées aux Etats-Unis	23
Figure 2-4 Allocation de fréquences en Europe.....	24
Figure 2-5 Architecture WAVE.....	25
Figure 2-6 Architecture ETSI-ITS	27
Figure 3-1 Critères de classification de bas niveau [40].	36
Figure 3-2 Critères de classification de haut niveau [40].....	39
Figure 4-1 Exemple d'illustration avec quatre segments.....	53
Figure 4-2 Scénario	56
Figure 4-3 Taux de réception de messages en fonction du nombre de véhicules	58
Figure 4-4 Délai de livraison en fonction du nombre de véhicules.....	59
Figure 4-5 Nombre de sauts en fonction du nombre de véhicules	60
Figure 4-6 Taux de redondance moyen en fonction du nombre de véhicules.....	61
Figure 4-7 Nombre de rediffusions en fonction du nombre de véhicules	62
Figure 4-8 Taux de rediffusion normalisé en fonction du nombre de nœuds	63
Figure 4-9 CBF-Délai de livraison en fonction du nombre de véhicules/voie/km, avec variation de la durée du slot	65
Figure 4-10 RCBF-Délai de livraison en fonction du nombre de véhicules/voie/km, avec variation de la durée du slot.....	65
Figure 4-11 SIP-Délai de livraison en fonction du nombre de véhicules/voie/km, avec variation de la durée du slot.....	66
Figure 4-12 CBF-Nombre de sauts en fonction du nombre de véhicules/voie/km, avec variation de la durée du slot.....	67

Figure 4-13 RCBF-Nombre de sauts en fonction du nombre de véhicules/voie/km, avec variation de la durée du slot.....	67
Figure 4-14 SIP-Nombre de sauts en fonction du nombre de véhicules/voie/km, avec variation de la durée du slot.....	68
Figure 4-15 CBF-Nombre de rediffusions en fonction du nombre de véhicules/voie/km, avec variation de la durée du slot.....	69
Figure 4-16 RCBF-Nombre de rediffusions en fonction du nombre de véhicules/voie/km, avec variation de la durée du slot.....	69
Figure 4-17 SIP-Nombre de rediffusions en fonction du nombre de véhicules/voie/km, avec variation de la durée du slot.....	70
Figure 4-18 CBF- taux de redondance en fonction du nombre de véhicules/voie/km, avec variation de la durée du slot.....	70
Figure 4-19 RCBF- taux de redondance en fonction du nombre de véhicules/voie/km, avec variation de la durée du slot.....	71
Figure 4-20 SIP- taux de redondance en fonction du nombre de véhicules/voie/km, avec variation de la durée du slot.....	71
Figure 5-1 Exemple d'illustration.....	76
Figure 5-2 Scénario	78
Figure 5-3 Exemple avec quatre segments de zone d'attente.....	81
Figure 5-4 Largeur de l'intervalle en fonction de la densité.....	83
Figure 5-5 Valeurs de T_{inf} et T_{sup} en fonction de la distance (Densité = 0.1).....	84
Figure 5-6 Valeurs de T_{inf} et T_{sup} en fonction de la distance (Densité = 0.5).....	85
Figure 5-7 Valeurs de T_{inf} et T_{sup} en fonction de la distance (Densité = 0.9).....	85
Figure 5-8 Délai de livraison de RDS en fonction de la densité et avec variation de la durée du slot	88
Figure 5-9 RDS-Nombre de rediffusion en fonction de la densité et avec variation de la durée du slot.....	89
Figure 5-10 Délai de livraison de notre protocole en fonction de la densité et avec variation de la durée du slot.....	89
Figure 5-11 Notre protocole-Nombre de rediffusion en fonction de la densité et avec variation de la durée du slot.....	90
Figure 5-12 Nombre moyen de rediffusions dans 2 km en fonction du nombre de véhicules/km... 91	91
Figure 5-13 Délai de livraison moyen en fonction du nombre de véhicules/km.....	93
Figure 5-14 Nombre moyen de sauts en fonction du nombre de véhicules/km.	94
Figure 5-15 Taux de Réception en fonction de la Probabilité de connectivité – densité moyenne..	96
Figure 5-16 Taux de Réception en fonction de la Probabilité de connectivité – densité faible.	96

Liste des Tableaux

Table 2-1 Messages d'évitement de collision dans une intersection	19
Table 2-2 Informations provenant de messages des autres véhicules	20
Table 2-3 Messages de sécurité publique.....	21
Table 2-4 Messages d'extension de la signalisation	21
Table 2-5 Messages de diagnostic et de maintenance de véhicule.....	22
Table 3-1 Classification des protocoles de dissémination -Approche de conception de haut-niveau	45
Table 3-2 Classification des protocoles de dissémination -Approche de conception de bas-niveau	46
Table 3-3 Métriques de performance des protocoles de dissémination	47
Table 3-4 Paramètres de simulation	48
Table 4-1 Paramètres de simulation	55
Table 5-1 Paramètres de simulation	88

Table des acronymes

3G : Third Generation
4G : Fourth Generation
BSM : Basic Safety Message
BSS : Basic service Set
C2C-CC : Car-2-Car Communication Consortium
CAMP : Vehicle Safety Communications Consortium
CAMs : Cooperative Awareness Messages
CBF : Contention Based Forwarding
CCH : Control Channel
C-ITS : Cooperative-Intelligent Transport Systems
CW : Contention Window
DENMs : Decentralized Environmental Notifications Messages
DSRC : Dedicated Short Range Communications
DTNs : Réseaux tolérants au délai
ETSI : European Telecommunications Standards Institute
EVAM : Emergency Vehicle Alert Message
FCC : Federal Communications Commission
GPS : Global Positioning System
ICRW : Intersection Collision Risk Warning
IEEE : Institute of Electrical and Electronics Engineers
ITS : Intelligent Transportation Systems
IVC : Inter-Vehicle Communications
LCRW : Longitudinal Collision Risk Warninig
LDM : Local Dynamic Map
LLC : Logical Link Control
MAC : Medium Access Control
MANETs : Mobile Ad hoc NETworks

NS2 : Network Simulator
OBU : Onboard Units
OCB : Outside the Context of BSS
RCBF : Random Contention Based Forwarding
RHS : Road Hazard Signaling
RM : RM
RSU : Road-side Units
RVC : Road-to-Vehicle Communications
S1P : Slotted 1-persistence
SCH : Service Channel
SUMO : Simulation of Urban MObility
TCP : Transmission Control Protocol
UDP : User Datagram Protocol
V2I : Vehicle to Infrastructure
V2V : Vehicle-to-Vehicle communications
VANET : Vehicular Ad Hoc NETwork
VSNs : Vehicular Social Networks
WAVE : Wireless Access in Vehicular Environment
WSA : WAVE Service Advertisement
WSMP : WAVE Short Message Protocole
WSMs : WAVE Short Messages

Chapitre 1

Introduction

1.1 Contexte

La forte augmentation du nombre de véhicules ces dernières années a rendu la conduite plus difficile et dangereuse. Selon la commission européenne des transports, en 2011, plus de 30 000 personnes sont mortes sur les routes de l'Union Européenne, soit l'équivalent d'une ville moyenne. Pour chaque décès il y a environ quatre blessures invalidantes permanentes, telles que des dommages au cerveau ou la moelle épinière, huit blessés graves et cinquante blessés légers [74]. Ce qui nécessite une réflexion sur les moyens permettant d'améliorer la sécurité routière. C'est pourquoi ces dernières années l'amélioration de la sécurité routière et la réduction du nombre d'accidents et leurs conséquences représentent un enjeu de société majeur et qui est d'un grand intérêt pour les autorités publiques et les constructeurs automobiles

Des consortiums ont été créés et des investissements importants ont été faits pour essayer de trouver des solutions permettant d'améliorer la sécurité routière. Leur principale effort a été concentré sur le développement de Systèmes de Transport Intelligents

« Intelligent Transportation Systems (ITS) ». Ces derniers se basent principalement sur des réseaux de communications sans fil, des capteurs intelligents, des équipements installés sur la route et des centrales de service. L'objectif principal de ces systèmes est de fournir des moyens pour améliorer la sécurité sur les routes et ainsi diminuer significativement le nombre d'accidents.

Les ITS couvrent de multiples facettes où les communications sans fil jouent un rôle d'une importance primordiale. Par conséquent, les constructeurs automobiles sont de plus en plus engagés à rendre leurs véhicules capables de communiquer à travers des liaisons sans fil. Comme des vies humaines sont à la pointe de toutes les parties prenantes, les applications de sécurité routière ont deux exigences majeures - la rapidité et la fiabilité - qui doivent être remplies par le réseau de communication sous-jacent.

Les véhicules, échangeant des informations (y compris la congestion du trafic routier, les accidents et les avertissements de sécurité) avec les véhicules voisins, forment ensemble un réseau de véhicule ad hoc « *Vehicular Ad Hoc NETWORK (VANET)* ». Les VANETs peuvent être considérés comme la plus importante application commerciale des réseaux ad hoc mobiles « *Mobile Ad hoc NETWORKS (MANETs)* » avec des applications concrètes. Plus un véhicule échange des informations avec ses voisins, plus est précise sa vision sur son environnement et plus sont efficaces et bien prévues les actions prises par les conducteurs. Cependant, l'échange d'informations est livré avec un coût (exprimé en termes de collisions de paquets) car les véhicules utilisent le même canal de communication. L'un des défis des VANETs est la **dissémination efficace et rapide** de l'information avec une utilisation raisonnable des ressources.

Les applications de sécurité routière sont la principale motivation des réseaux de véhicules, bien que d'autres applications de gestion du trafic routier et de divertissement soient envisagées. La communication par diffusion sur plusieurs sauts est une composante importante de ces applications telles que, la signalisation du danger sur la route « *Road Hazard Signaling* » où la diffusion sur plusieurs sauts est utilisée pour notifier un accident sur la route, une présence d'animal, un objet qui barre la route, un freinage brusque du véhicule en avant, etc. Comme l'information traitée dans ces applications est très critique et peut avoir un effet sur la vie humaine, la diffusion doit être rapide et fiable.

Cependant, la diffusion de messages sur plusieurs sauts a de nombreux défis à relever tels que le problème de tempête de diffusion « *broadcast storm problem* » (à savoir, des

retransmissions redondantes, une haute charge du canal, une grande contention sur le canal de communication et ainsi, un taux de perte de paquets élevé) dans le cas d'un réseau dense, et le problème de déconnexion quand le réseau est clairsemé. En plus, les applications de sécurité routière sont à temps critique et la satisfaction de leurs exigences est très difficile, car il y a un compromis entre la fiabilité de la dissémination et le délai de livraison.

De nombreux travaux ont été menés ces dernières années et une large gamme de mécanismes ont été proposés. Néanmoins, la plupart d'entre eux souffrent toujours de problèmes de collisions quand le réseau est dense et, une longue latence quand la densité du réseau est faible.

Le but de cette thèse est d'étudier les protocoles permettant une livraison fiable et rapide des messages d'alerte, de comprendre leurs limites et de proposer une solution pour la dissémination rapide et fiable de l'information de sécurité dans un réseau de véhicule.

1.2 Contributions

Notre contribution comporte essentiellement deux volets :

- ***Analyse et classification des protocoles de dissémination de l'information dans les réseaux véhiculaires*** : ces dernières années, une large gamme de protocoles ont été présentés dans la littérature afin de considérer les besoins de la dissémination de l'information sur un réseau de véhicules. Nous proposons une extension des classifications existantes dans ce domaine. Notre analyse inclut de nouvelles métriques et critères de classification, pour mieux caractériser les protocoles de diffusion dédiés à la dissémination de l'information de sécurité¹ sur plusieurs sauts dans les VANETs.
- ***Analyse et comparaison de plusieurs solutions pour le contrôle de la rediffusion*** : la distance entre l'émetteur et le récepteur est le paramètre utilisé dans la plupart des mécanismes existants pour réduire le nombre de nœuds relais dans la zone d'intérêt. La fenêtre de contention est un paramètre important et le nombre et la durée du slot de cette fenêtre ont un impact direct sur les performances des protocoles qui se basent sur le délai. Dans le chapitre 4, nous présentons trois

¹ Il convient de remarquer que le terme sécurité correspond ici au sens du terme anglais « safety ».

mécanismes de dissémination et nous évaluons leurs performances sous différentes conditions de trafic routier. Nous discutons l'influence de la fenêtre de contention et la durée du slot sur leurs performances.

- **Proposition d'un protocole de dissémination d'information** : nous proposons un protocole adaptatif constitué d'un mécanisme pour l'estimation de la densité du réseau et un autre mécanisme pour la sélection du prochain nœud relai. Ce dernier se base principalement sur deux fonctions qui calculent l'intervalle de temps à partir duquel chaque nœud tire son temps d'attente avant de décider de rediffuser ou non le message reçu. L'idée principale consiste à combiner un mécanisme de dissémination à base de distance avec un mécanisme **non intrusif** qui se base sur l'estimation de la densité du réseau telle qu'elle est perçue par le nœud en considération (il s'agit d'une densité locale). Lorsque la densité du réseau est élevée, l'intervalle de temps est élargi pour réduire le nombre de transmissions redondantes et éviter ainsi le gaspillage de la bande passante. A l'inverse, quand la densité du réseau est faible (c'est-à-dire quand le réseau est clairsemé) l'intervalle de temps de chaque nœud est réduit pour réduire le délai de livraison de message. Nous avons utilisé deux plateformes de simulation pour évaluer les performances de notre protocole, à savoir, le simulateur NS2 pour les simulations réseau et le simulateur SUMO pour la simulation de la mobilité.

1.3 Organisation

La thèse est organisée comme suit :

- **Chapitre 1 : Introduction générale**
- **Chapitre 2 : Réseaux véhiculaires : vue d'ensemble**

Dans ce chapitre, nous présentons un aperçu des réseaux sans fil ad hoc véhiculaires et leurs principales caractéristiques, puis nous décrivons leurs applications avec une intention toute particulière dédiée aux applications destinées à améliorer la sécurité routière. Par la suite, nous décrivons les différentes architectures protocolaires et les standards qui ont été proposés dans ce domaine, notamment en Europe et aux Etats-Unis.

- **Chapitre 3 : Protocoles de dissémination d'alertes dans les VANETs**

Ce chapitre présente une description des principaux défis liés à la dissémination de

l'information de sécurité dans un réseau de véhicules. Par la suite, nous proposons une classification des différents mécanismes qui ont été présentés dans la littérature, selon deux approches de conception, à savoir, l'approche de conception de haut niveau et l'approche de conception bas niveau. Nous nous concentrons particulièrement sur les mécanismes de sélection du prochain nœud relai et les techniques utilisées. Nous présentons également une classification des métriques utilisées pour évaluer les performances des protocoles de dissémination, et les paramètres de simulation utilisés lors de cette évaluation.

- **Chapitre 4 : Analyse de performance des mécanismes de dissémination alertes**

Ce chapitre est consacré au problème de réduction du nombre de rediffusion (à savoir les transmissions redondantes) lors de la dissémination de message sur une zone d'intérêt. Nous présentons deux protocoles qui utilisent deux approches différentes dans leur mécanisme de sélection du nœud relai. Ces deux mécanismes sont parmi les plus référencés dans la littérature. Nous présentons aussi le scénario que nous avons adopté pour notre évaluation. Nous montrons à travers des scénarios de simulation les limites de ces mécanismes, notamment quand la densité du réseau est élevée.

- **Chapitre 5 : Un protocole adaptatif pour la dissémination de l'information de sécurité dans les VANETS**

Dans ce chapitre, nous présentons notre contribution en termes de protocole pour la dissémination de l'information de sécurité dans les VANETS. Notre protocole propose de combiner la technique de dissémination à base de distance avec la technique à base du trafic routier afin d'améliorer les performances de la dissémination de l'information dans les VANETS en termes de délai et d'efficacité. Nous présentons la conception de notre protocole et nous développons la technique de sélection du prochain nœud relai, les intervalles de temps et leur principe d'adaptation à la densité du réseau ainsi que le fonctionnement général du protocole. Les performances de notre protocole sont évaluées par simulation et comparées à celles d'un protocole avec un principe de fonctionnement similaire.

Chapitre 2

Réseaux véhiculaires: Vue d'ensemble

2.1 Introduction

Les réseaux sans fil véhiculaires sont considérés comme un élément clé des futurs systèmes de transport intelligents « *Intelligent Transportation Systems (ITS)* ». Ils représentent une technologie prometteuse, qui une fois mise en œuvre, offrira la possibilité de déployer une large variété d'applications. Certaines de ces applications visent à améliorer la sécurité routière. D'autres visent à rendre les déplacements des usagers de la route plus confortables. Cette nouvelle technologie représente un des domaines de recherche les plus attractifs de ces dernières années, que ce soit dans le domaine académique ou dans l'industriel.

Dans ce chapitre, nous fixons le contexte de cette thèse en présentant un aperçu des réseaux sans fil véhiculaires. Nous définissons dans un premier temps la notion de réseaux sans fil véhiculaires et nous présentons leurs principales caractéristiques dans les sections 2.2 et 2.3, respectivement. Ensuite, dans la section 2.4, nous présentons une classification

des applications susceptibles d'être déployées dans un environnement véhiculaire. Nous décrivons les caractéristiques et les exigences de chaque catégorie d'application, avec une attention particulière donnée aux applications qui visent à améliorer la sécurité routière. La section 2.5 décrit les standards et les architectures de communication qui ont été proposés en Europe et aux Etats-Unis.

2.2 Définitions

Les réseaux sans fil ad hoc véhiculaires « *Vehicular Ad hoc NETWORKS (VANETs)* » sont considérés comme une classe spécialisée des réseaux ad hoc mobiles « *Mobile Ad hoc NETWORKS (MANETs)* », pour répondre aux exigences et aux caractéristiques des nœuds (véhicules) qui se déplacent sur les routes. Un VANET est composé de deux types d'unités de communication : les « *Onboard Units (OBU)* », embarquées dans des véhicules ; les « *Road-side Units (RSU)* », déployées le long des autoroutes et des trottoirs dans les zones urbaines (cf. figure 2-1). Les RSUs peuvent aussi être embarquées dans des équipements de l'infrastructure routière déjà existante ; par exemple, dans les panneaux de signalisation ou dans les barrières de péage.

Dans un VANET², les véhicules peuvent communiquer directement entre eux. Dans ce cas, les communications sont catégorisées comme des communications véhicule à véhicule « *Vehicle-to-Vehicle communications (V2V)* » ou inter-véhicules « *Inter-Vehicle Communications (IVC)* ». Les véhicules peuvent également communiquer avec l'infrastructure de communication existante, à travers les RSUs. Dans ce cas, les communications sont catégorisées comme des communications véhicule à infrastructure « *Vehicle to Infrastructure communications (V2I)* », appelées aussi « *Road-to-Vehicle Communications (RVC)* » [2].

Plusieurs technologies de communication peuvent être utilisées dans le cas des communications de types V2I, telles que : le WiFi, le réseau mobile (3G/4G) et le WiMax. Le choix entre ces technologies et le type de communication à utiliser (V2V, V2I ou hybride), dépend des exigences des applications considérées. Nous présenterons ces applications et leurs exigences dans la section 2.3.

² Bien que le terme VANETs correspond réellement aux communications dites sans infrastructure ou Ad-hoc. Il est généralement utilisé pour désigner les deux modes de communication V2V et V2I

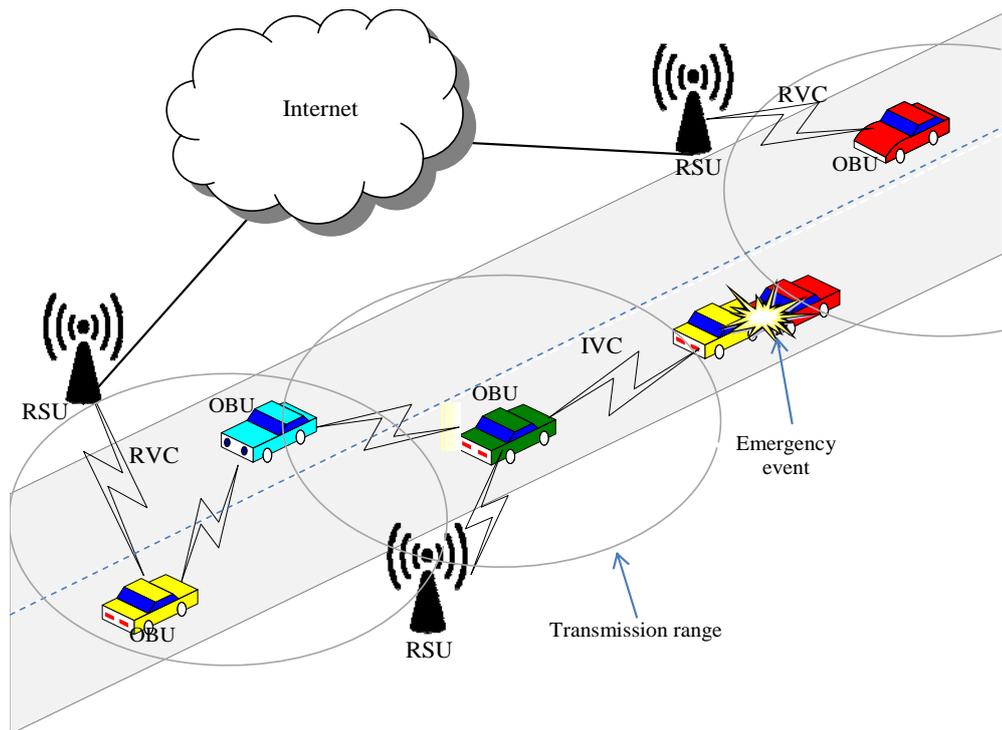


Figure 2-1 Les composants d'un VANETs

2.3 Caractéristiques des VANETs

Bien que les réseaux sans fil véhiculaires représentent une classe particulière des réseaux ad hoc mobiles, ils diffèrent de ces derniers sur de nombreux aspects. Ils sont notamment caractérisés par une topologie très dynamique liée à la vitesse de déplacement des véhicules et à l'infrastructure routière. En effet, contrairement à un réseau sans fil traditionnel (ex : MANET ou Réseau de capteurs sans fil) où les mouvements des nœuds sont aléatoires et la vitesse de déplacement est faible. Les mouvements des nœuds dans un réseau de véhicules ne sont pas aléatoires. Ils sont limités par l'infrastructure routière et le comportement des conducteurs. En plus, la vitesse de déplacement des nœuds peut être élevée et peut aller jusqu'à plus de 130 km/h (c'est la vitesse limite autorisée en France).

Les caractéristiques des VANETs influent sur la conception de leurs protocoles et rendent les protocoles et les mécanismes développés pour les réseaux sans fil traditionnels non applicables directement dans les VANETs [1, 2, 3, 4]. Dans ce qui suit, nous détaillons les caractéristiques des VANETs.

- **Densité du réseau**

Les nœuds sont des véhicules (voitures, bus ...) et leur densité peut varier en fonction de l'environnement (rural, ville, périphérique, autoroute) et du temps (heures de pointe, tard la nuit ou tôt le matin). En effet, le trafic routier peut être très dense comme dans le cas des embouteillages durant les heures de pointe dans les grandes villes. Dans un environnement rural ou tôt le matin dans les villes, le trafic routier est faible et les véhicules sont clairsemés. Dans le premier cas, le nombre de nœuds dans la portée de transmission d'un véhicule peut aller jusqu'à plusieurs centaines (cf. figure 2-2), ce qui pose plusieurs problèmes pour les communications qui se basent sur des liaisons sans fil, tels que les interférences et les collisions de paquets [5]. A l'inverse, quand les véhicules sont clairsemés la connectivité entre les véhicules n'est pas garantie car un véhicule peut ne pas avoir de voisin pendant une longue durée [6, 7]. Les protocoles et les mécanismes développés pour ce nouveau type de réseau sans fil doivent prendre en compte ces variations de la densité du réseau et s'adapter à l'environnement dans lequel ils sont déployés.



Figure 2-2 Exemple d'une Autoroute à Houston [70]

- **Auto-organisation**

Le type de communication (V2V et/ou I2V) à utiliser dans un réseau de véhicules dépend des exigences particulières de l'application à déployer sur ce réseau. Dans la plupart de ces applications³, notamment celles qui visent à améliorer la sécurité routière, les communications sont de type V2V. Dans ce dernier, il n'y a pas d'entité centrale (coordinateur) comme par exemple, dans les réseaux mobiles ou un réseau WiFi avec infrastructure. Un VANET devrait être formé lorsque les véhicules sont présents dans certaines zones et il disparaît lorsque les véhicules quittent la zone.

- **Topologie du réseau très dynamique**

Les nœuds (véhicules) se déplacent dans des rues, des routes, des autoroutes selon des modèles de mobilité différents (vitesse, orientation ...) entraînant des changements dans la topologie du réseau. Les liens entre les nœuds sont intermittents et de très courte durée. Cependant, la trajectoire d'un véhicule peut être planifiée. En effet, comme la carte des routes et la position du véhicule sont facilement accessibles (à l'aide du GPS « *Global Positioning System* » par exemple). Avec ces informations et les informations sur la vitesse et la direction de déplacement du véhicule, on peut prédire sa trajectoire. Cette dernière est très utile notamment pour le routage de paquets [7].

- **Contrainte de délai**

Certaines applications, notamment celles qui visent la sécurité routière, exigent que les paquets soient livrés à temps. Car, contrairement aux autres applications, dans ces applications les paquets transportent des informations de sécurité qui peuvent avoir un impact sur des vies humaines. Une information (ex : freinage brusque) qui arrive en retard est inutile. Les protocoles développés pour ces applications doivent répondre à cette forte contrainte.

- **Pas de contraintes de la batterie**

Puisque les dispositifs de communication sont intégrés dans les véhicules, la consommation d'énergie due à la communication et au traitement, ne représente pas un problème dans la conception de VANET. Ce qui n'est pas le cas pour les

³ Ces applications ainsi que leurs caractéristiques seront détaillées dans la section suivante (2.4).

réseaux ad hoc sans fil traditionnels notamment les réseaux de capteurs sans fil. Dans ces derniers, la contrainte énergétique doit être prise en considération lors de la conception et du développement des protocoles et des applications à déployer sur ces réseaux. Un autre avantage est la possibilité d'installer plusieurs interfaces de communication sans fil (ex : WAVE, WiFi, 3G/4G, Satellite, WiMax) dans l'OBU, et d'avoir une capacité importante de stockage et de calcul.

- **Environnement de communication**

Contrairement aux réseaux sans fil traditionnels où les nœuds communicants se trouvent généralement dans un environnement bien connu et qui ne change pas beaucoup. Dans un réseau VANET, les nœuds se déplacent dans des environnements changeants (tunnels, obstacles, environnement rural ...) et impactant la connectivité et la qualité de réception du signal [9]. Outre, un réseau VANET peut être déployé pour couvrir une grande région ou une grande ville, ce qui pose le problème de passage à l'échelle.

- **Sécurité et confidentialité**

La sécurité représente un grand challenge dans les réseaux véhiculaires où les communications se basent sur des liaisons sans fil (diffusion dans l'air). D'une part, les messages relayés entre les nœuds doivent être sécurisés (pour éviter le déni de service et la propagation de fausses alertes et informations) et d'autre part, l'emplacement et l'itinéraire des utilisateurs devraient être gardés privés [10].

2.4 Applications

Les technologies de communication sans fil offrent des opportunités pour déployer un grand nombre d'applications dans un environnement véhiculaire. Ces applications sont particulièrement dédiées aux usagers de la route. Les applications qui visent à améliorer la sécurité routière sont la principale cible des VANETs. Les autres applications sont dédiées au confort des passagers. Elles viennent notamment pour apporter une valeur ajoutée et

accélérer le taux de pénétration⁴ des VANETs.

Une catégorisation de ces applications a été publiée en 2005 aux Etats-Unis, par le « *Vehicle Safety Communications Consortium (CAMP)* » [11]. En 2009, l'ETSI ITS « a publié un rapport technique qui définit un ensemble d'applications qui peuvent être déployées sur un réseau de véhicule [12]. Ces applications ne sont encore pas complètement standardisées. Les standards de l'ETSI spécifient les exigences minimales de trois groupes d'applications [13] : signalisation du danger sur la route « *Road Hazard Signaling (RHS)* » [14], avertissement sur le risque de collision dans l'intersection « *Intersection Collision Risk Warning (ICRW)* » [15] et l'avertissement sur le risque de collision longitudinale « *Longitudinal Collision Risk Warning (LCRW)* » [16].

Les deux rapports décrivent un ensemble d'applications dont certaines sont communes, mais différent dans la nomination. Néanmoins, en général, trois catégories ont été définies dans les deux rapports: i) applications de sécurité routière, ii) applications de gestion du trafic routier et iii) applications de divertissement et de confort. Chaque application a ses exigences en qualité de service et son mode de communication (messages périodique, message événementielle, broadcast, multicast, unicast, V2V et/ou I2V).

Nous détaillons dans les sections suivantes chacune de ces trois catégories d'applications. Nous nous concentrons plus particulièrement sur les applications destinées à améliorer la sécurité routière. En effet, le contexte de cette thèse est celui des applications dédiées à la sécurité routière.

2.4.1 Applications de sécurité routière

Les applications de cette catégorie visent à améliorer la sécurité sur la route et à réduire les accidents et leurs coûts (humains et matériels). Ces applications se basent sur l'échange de messages de sécurité entre les véhicules d'un VANET, et dans certaines applications avec les RSUs aussi. En effet, par un simple échange de messages, ces applications fournissent au conducteur un ensemble d'informations lui permettant d'étendre son champ de vision. Ce qui va lui permettre d'éviter les situations dangereuses. La portée de diffusion et les contraintes temporelles dépendent du type de message de sécurité échangé. Des études ont montré qu'environ 60% des accidents routiers pourraient être évités si le

⁴ Le taux de véhicules équipés par la technologie VANET

conducteur du véhicule avait été averti au moins une demi-seconde avant la collision [17].

Dans ces applications, deux types de messages sont échangés : les messages périodiques et les messages d'alerte. Les messages périodiques appelés aussi « balises » sont générés et diffusés par chaque véhicule avec une fréquence entre 1Hz et 50 Hz, selon les exigences de l'application. Ces messages sont diffusés sur un seul saut et permettent à chaque véhicule d'avoir une vue locale de son voisinage. Les messages d'alerte sont générés et diffusés par le(s) véhicule(s) qui détecte (ou s'il représente) une situation dangereuse. Contrairement aux balises, les messages d'alerte peuvent être diffusés sur plusieurs sauts pour couvrir une zone particulière (zone de danger).

Aux Etats-Unis, le standard « SAE J2735 » spécifie un ensemble de formats de messages pour supporter toute une gamme d'applications [18]. Le « *Basic Safety Message (BSM)* » est le message le plus important dans le standard SAE J2735. Ce type de message est transmis périodiquement par les véhicules du système. Un BSM transporte des informations sur l'état du véhicule émetteur (position, dynamique du véhicule, etc.). Un autre type de message défini par le standard est le « *Emergency Vehicle Alert Message (EVAM)* ». Ce message est transmis par les véhicules d'urgences/secours comme les ambulances et les voitures de polices.

En Europe, deux types de messages ainsi que leur contenu ont été définis et standardisés par l'ETSI ITS dans [19] pour les messages périodiques et [20] pour les messages d'alerte :

- ***Messages périodiques dits « Cooperative Awareness Messages (CAMs) »***

Chaque message contient plusieurs informations relatives au véhicule telles que: sa position, sa direction, sa vitesse, etc. Ces messages représentent la base des applications de sécurité routière. Ils permettent à chaque véhicule d'être conscient de son environnement. Généralement, ils ne sont diffusés que sur un seul saut.

- ***Messages d'alerte dits « Decentralized Environmental Notifications Messages (DENMs) »***

Chaque DENM contient les informations relatives à l'évènement qui a un impact potentiel sur la sécurité routière. Les conditions de déclenchement de la transmission de ces messages ainsi que leur format ont été aussi définis dans le standard.

Un grand nombre de papiers ont présenté partiellement les applications de sécurité et les services qui peuvent être déployés sur un VANET. Les deux publications les plus complètes sur la catégorisation des applications de sécurité sont le rapport publié par l'ETSI [12] et le CAMP [11]. Ce dernier identifie 34 types d'applications (à savoir échanges de messages) qui sont susceptibles d'être considérées comme des applications de sécurité en fonction de leur capacité à réduire les accidents de la circulation et d'améliorer la sécurité publique générale. La plupart se basent sur des communications de type V2V. Ces applications sont classées en cinq catégories (voir Tables 2-1 à 2-5 pour plus de détails sur les messages de sécurité):

- Evitement de collision dans l'intersection « *Intersection collision avoidance* » ;
- Informations provenant d'autres véhicules « *Information from other vehicles* » ;
- Sécurité publique « *Public safety* » ;
- Applications d'extension de la signalisation « *Sign extention application* » ;
- Diagnostic et entretien du véhicule « *Vehicle diagnostics and maintenance* » ;

Chaque application est caractérisée par six attributs [11] :

❖ **Type de communication**

Il décrit les différentes facettes des communications, y compris la source et la destination de la transmission (à savoir les communications sont de l'infrastructure vers le véhicule, du véhicule vers l'infrastructure ou de véhicule à véhicule), le mode de communication (dialogue entre deux entités ou diffusion), le nombre de destinations prévues (communications point à point ou point-à-multipoint).

❖ **Mode de transmission**

Il décrit si la transmission des événements est périodique ou apériodique.

❖ **Fréquence minimale**

C'est la fréquence à laquelle un message périodique devrait être transmis. Elle va de 1 Hz à 50 Hz. En cas d'un message événementiel (message d'alerte), une fréquence est spécifiée pour indiquer comment le message doit être répété après

l'apparition de l'événement.

❖ **Latence admissible**

C'est la durée maximale de temps admissible entre le moment où l'information est disponible pour être transmise et le moment de sa réception. Elle varie de 20 ms à 5 sec. La latence est une caractéristique cruciale parce que les applications de sécurité routière sont à temps critique.

❖ **Portée de communication maximale requise**

C'est la distance de communication nécessaire entre deux unités pour soutenir efficacement une application particulière. Elle varie de 100 m à plus de 1000 m. Cette caractéristique est utilisée pour déterminer la zone d'intérêt pour la dissémination de chaque type de message.

❖ **Contenu du message**

Il décrit le contenu de la communication (par exemple, la position du véhicule, la vitesse, l'information sur le trafic ...).

2.4.2 Applications de gestion du trafic routier

L'objectif des applications de cette catégorie est de faciliter et d'optimiser les déplacements des usagers de la route. Néanmoins, elles peuvent aussi contribuer à l'amélioration de la sécurité routière. En effet, certaines applications de cette classe visent à réduire les congestions dans les rues et à fluidifier le trafic routier. Ainsi, réduire le nombre d'accidents qu'engendrent ces congestions. Plusieurs cas d'utilisation appartenant à cette catégorie sont proposés.

Le rapport technique de l'ETSI [12] décrit chaque cas d'utilisation, son mode de communication (I2V, V2V, hybride, messages périodiques ou événementiels, broadcast, unicast) et ses exigences (fréquence minimale des messages périodiques et le délai maximum). La plupart de ces cas d'utilisation se basent sur les communications I2V et la diffusion des messages périodiques (CAMs) par les RSUs. Ces messages proviennent d'une entité centrale appelée « *Traffic management entity* ».

Les applications de cette classe sont caractérisées par une flexibilité en termes de délai et la fréquence de diffusion des messages n'est pas élevée comme dans le cas des

applications de sécurité routière (entre 1Hz et 2Hz). Une autre caractéristique importante de cette classe d'applications est la possibilité d'utiliser plusieurs technologies de communication (Satellite, WAVE, WIFI, 3G/4G, WiMax) [21].

Un exemple des applications de cette catégorie est l'application d'informations sur le trafic et la recommandation d'itinéraire « *Traffic information and recommended itinerary* ». Elle informe les véhicules qui s'approchent d'une zone où il y a une situation anormale (embouteillage, travaux, accident) et diffuse des recommandations à travers les RSUs. Les recommandations diffusées sont basées sur les informations collectées à partir de plusieurs sources telles que : les RSUs, les véhicules, les capteurs installés dans les intersections, les caméras, etc. Ces informations sont envoyées à une entité centrale (ex : via les RSUs ou le réseau mobile 3G/4G) qui les traite et envoie les recommandations. Dans l'application limite de vitesse contextuelle « *Regulatory/contextual speed limits* », la RSU diffuse périodiquement la limite de la vitesse recommandée dans la rue. Elle vise à rendre la circulation fluide et réduire la pollution. Ces applications ne sont pas des applications de sécurité routière en tant que telles, mais en revanche, elles peuvent aider à améliorer la sécurité routière.

En plus, les applications de cette catégorie ont des avantages sur le plan économique et écologique. Elles peuvent, par exemple, aider à réduire la consommation du carburant et par conséquent les gaz à effet de serre. Les compagnies de transport public peuvent aussi profiter de ces applications pour optimiser les itinéraires des bus et réduire leurs dépenses.

2.4.3 Applications de divertissement et de confort

Les applications appartenant à cette catégorie n'ont pas d'effet sur la sécurité routière. Elles visent le confort des usagers de la route. Elles ont des objectifs commerciaux, notamment l'accélération du taux de pénétration des VANETs sur le marché. En effet, ces applications peuvent apporter une valeur ajoutée et encourager les utilisateurs à adopter la technologie VANET.

Comme pour les deux premières catégories, l'ETSI dans [12] et le CAMP dans [11] ont défini un ensemble de cas d'utilisation appartenant à cette catégorie tels que : *la notification des points d'intérêt, l'accès à l'internet ou le téléchargement de contenu*.

Les applications de cette classe sont caractérisées par une faible contrainte de délai,

mais le volume de données échangées est élevé. Un exemple de ces applications est la mise à jour de la carte routière dans laquelle plusieurs technologies de communication peuvent être utilisées pour télécharger les éléments de la carte [21]. En effet, les applications de cette classe peuvent s'appuyer sur plusieurs technologies de communication telles que : Satellite, WiFi, 3G/4G, WAVE. Les communications sont généralement I2V/V2I, et les communications V2V sont utilisées en complément dans le cas où la communication avec l'infrastructure de télécommunication est impossible [21].

Un nouveau paradigme de VANET est apparu ces dernières années : les réseaux sociaux véhiculaires « *Vehicular Social Networks (VSNs)* ». Ces réseaux sont formés sur les routes et les rues entre les voyageurs qui ont des relations, des interactions et des intérêts sociaux communs [22]. Les utilisateurs de ces réseaux échangent des informations d'intérêt commun, par exemple, les embouteillages et les dangers sur le chemin. Ils peuvent aussi échanger des fichiers tels que des fichiers multimédias.

Table 2-1 Messages d'évitement de collision dans une intersection

Message	Description	Fréquence (Hz)	Délai (ms)	Portée (m)
Avertissement <i>Violation de la signalisation routière</i>	Il prédit que le conducteur sera en violation et il l'avertit pour qu'il s'arrête à l'endroit prévu par la réglementation.	~10	~100	~250
Avertissement <i>Violation du panneau d'arrêt</i>	Il avertit le conducteur qu'un niveau élevé de freinage est nécessaire pour un arrêt complet.	~10	~100	~250
Assistance <i>Tournement à gauche</i>	Il fournit des informations au conducteur sur le trafic qui arrive dans l'autre sens pour l'aider à tourner à gauche.	~10	~100	~300
Assistance <i>Mouvement après le panneau d'arrêt</i>	Il fournit un avertissement à un véhicule qui est sur le point de traverser une intersection après s'être arrêté à un panneau d'arrêt.	~10	~100	~300
Avertissement <i>Collision dans l'intersection</i>	Il avertit le conducteur dans le cas où une collision à une intersection est probable.	~10	~100	~300
Avertissement <i>Fusion aveugle</i>	Il avertit un véhicule s'il tente de se fusionner à partir d'un endroit où la visibilité est limitée, et un autre véhicule qui s'approche est prédit d'occuper l'espace de la fusion.	~10	~100	~200
Information <i>Passage piéton</i>	Il avertit les conducteurs en cas de danger de collision avec un piéton ou un enfant qui est sur un passage désigné.	~10	~100	~200

Table 2-2 Informations provenant de messages des autres véhicules

Message	Description	Fréquence (Hz)	Délai (ms)	Portée (m)
<i>Pré-détection de collision</i>	Il peut être utilisé pour se préparer aux collisions imminentes et inévitables.	Alerte (~50)	~20	~50
<i>Feux de freinage d'urgence électronique</i>	Lorsque le véhicule freine fort, il envoie un message aux autres véhicules qui le suivent.	Alerte (~10)	~100	~300
Avertissement <i>Changement de voie</i>	Il fournit un avertissement au conducteur si un changement de voie prévu peut causer un accident avec un autre véhicule à proximité.	~10	~100	~150
Avertissement <i>Angle mort</i>	Il avertit le conducteur quand il a l'intention de faire un changement de voie et l'angle mort est occupé par un autre véhicule.	~10	~100	~150
Avertissement <i>Collision dans le croisement autoroute/rail</i>	Il aide à prévenir les collisions entre les véhicules et les trains dans les croisements des voies ferrées.	~1	~1000	~300
<i>Relayage coopératif des avertissements de collision</i>	Il aide le conducteur à éviter ou à atténuer les collisions avec le pare choc arrière du véhicule qui est en avant.	~10	~100	~150
<i>Avertissement coopératif de collision</i>	Il recueille l'emplacement des véhicules et leur dynamique et avertit le conducteur dans le cas où une collision est probable.	~10	~100	~150
<i>Système coopératif d'automatisation des autoroutes</i>	Il fournit à la fois le contrôle de la position et de la vitesse des véhicules dans le but de fonctionner en toute sécurité comme un peloton sur une autoroute.	~50	~20	~100
<i>Contrôle de vitesse adaptatif et coopératif</i>	Il obtient la dynamique du véhicule en tête et améliore la performance du contrôle de vitesse adaptatif courant.	~10	~100	~150
<i>Notification des caractéristiques routières de véhicule à véhicule</i>	Il détecte les caractéristiques routières telles que le degré, le virage, etc. qui dépassent les limites prédéfinies et transmet les informations aux autres véhicules.	Alerte (~2)	~500	~400
<i>Avertissement sur les conditions routières</i>	Il fournit un avertissement aux véhicules à proximité lorsque la surface de la route est gelée.	Alerte (~1)	~1000	~200
<i>Avertissement sur les conditions routières fondées sur les véhicules</i>	Il détecte les conditions routières marginales en utilisant des systèmes et des capteurs embarqués et transmet un avertissement sur les conditions routières.	Alerte (~2)	~500	~400
<i>Assistance à la fusion dans l'autoroute</i>	Il avertit le véhicule se trouvant sur une bretelle d'une autoroute si un autre véhicule est sur son chemin de fusion et peut être dans son angle mort.	~10	~100	~250

2. Réseaux véhiculaires : Vue d'ensemble

<i>Améliorateur de visibilité</i>	Il détecte les situations de mauvaise visibilité (brouillard, fortes pluies, etc.) soit automatiquement ou via la commande de l'utilisateur.	~2	~100	~300
-----------------------------------	--	----	------	------

Table 2-3 Messages de sécurité publique

Message	Description	Fréquence (Hz)	Délai (ms)	Portée (m)
<i>Avertissement Véhicule d'urgence en approche</i>	Il fournit au conducteur un avertissement pour céder le passage à un véhicule d'urgence qui s'approche.	Alerte (~1)	~1000	~1000
<i>Préemption du signal pour véhicule d'urgence</i>	Il permet à un véhicule d'urgence de demander un droit de passage au feu de circulation.	N/A	~1000	~1000
<i>Services SOS</i>	Il envoie des messages SOS après le déclenchement des airbags.	Alerte (~1)	~1000	~400
<i>Avertissement après accident</i>	Il avertit les véhicules qui s'approchent d'un véhicule en panne.	Alerte (~1)	~500	~300

(N/A : Non Applicable)

Table 2-4 Messages d'extension de la signalisation

Message	Description	Fréquence (Hz)	Délai (ms)	Portée (m)
<i>Signalisation à bord du véhicule</i>	Il fournit au conducteur les informations qui sont généralement véhiculées par les panneaux de signalisation.	~1	~1000	~200
<i>Avertissement Vitesse du virage</i>	Il aide le conducteur à entamer les virages à des vitesses appropriées.	~1	~1000	~200
<i>Avertissement Parking à structure basse</i>	Il fournit aux conducteurs des informations concernant la hauteur de dégagement d'un parking.	~1	~1000	~100
<i>Avertissement Mauvais sens de conduite</i>	Il avertit le conducteur que le véhicule roule ou est sur le point de rouler contre le flux du trafic (en contre sens).	~10	~100	~500
<i>Avertissement Pont de niveau bas</i>	Il fournit des messages d'avertissement aux véhicules quand ils s'approchent d'un pont de faible hauteur.	~1	~1000	~300
<i>Avertissement Zone de travail</i>	Il informe que le véhicule est dans un périmètre de la zone de travail active.	~1	~1000	~300

2. Réseaux véhiculaires : Vue d'ensemble

Avertissement <i>Ombre à bord du véhicule</i>	Il envoie des informations d'alerte ombre à l'unité à bord du véhicule.	~1	~1000	~250
---	---	----	-------	------

Table 2-5 Messages de diagnostic et de maintenance de véhicule

Message	Description	Fréquence (Hz)	Délai (ms)	Portée (m)
<i>Notification réparation juste-à-temps</i>	Il communique le diagnostic à bord du véhicule à l'infrastructure et conseille le conducteur sur les services disponibles à proximité.	Alerte (N/A)	~500 0	~400
<i>Avis de rappel de sécurité</i>	Il permet la distribution de données de sécurité envoyées directement à des véhicules via les RSUs, et / ou à des PC à domicile.	Alerte (N/A)	N/A	~400

(N/A : Non Applicable)

2.5 Standards et architectures protocolaires

Le contexte véhiculaire est caractérisé par la diversité des constructeurs automobiles. Ces derniers sont généralement en concurrence entre eux pour gagner des parts de marchés. Cependant, pour le développement et le succès de la technologie VANET, ils doivent travailler ensemble pour assurer l'interopérabilité entre les équipements provenant de différents constructeurs automobile. Par conséquent, un travail de standardisation devient un aspect clé pour le déploiement universel de cette nouvelle technologie.

Plusieurs consortiums ont été créés tels que le consortium des constructeurs automobiles européens « *Car-2-Car Communication Consortium (C2C-CC)* » [23] et le « *Vehicle Safety Communications Consortium (CAMP)* » aux Etats-Unis [11]. Plusieurs projets de recherche ont été lancés ces dernières années en Europe [24] et aux Etats-Unis [25]. Ces travaux de recherche ont abouti à une série de standards.

Aux Etats-Unis, en 1999, la commission fédérale des communications « *Federal Communications Commission (FCC)* » a accordé 75 MHz de spectre dans la bande des 5,9 GHz pour le « *Dedicated Short Range Communications (DSRC)* ». Comme illustré dans la figure 2-3, ce spectre est divisé en 7 canaux de 10 MHz chacun, dont un canal de contrôle (CCH) et 6 canaux de service (SCH). Dans ce standard, le canal 172 est dédié aux applications de sécurité routière. Le canal de contrôle 178 (CCH) est utilisé comme un canal de rendez-vous sur lequel sont diffusés les messages de gestion et les messages

2. Réseaux véhiculaires : Vue d'ensemble

d'annonce de services disponibles sur les autres anneaux. Les règles d'utilisation et d'ordonnement de ces canaux sont définies par le standard IEEE 1609.4.

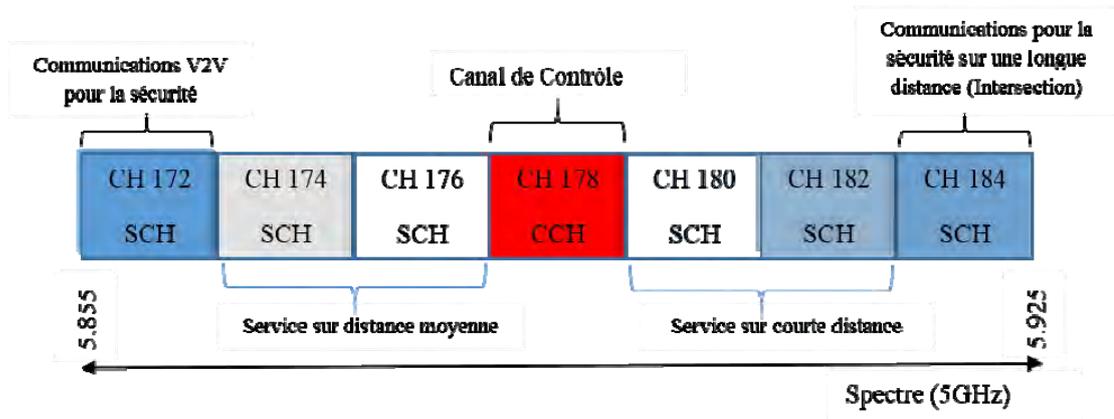


Figure 2-3 Bande de fréquences réservées aux Etats-Unis

En Europe, en 2008, l'ETSI a alloué trois bandes dans la bande 5 GHz pour les ITS. De même que pour le DSRC chaque bande est divisée en canaux de 10 MHz. Comme illustré par la figure 2-4, la première bande dite ITS-G5A, est de 30 MHz. Elle est destinée aux applications de sécurité routière. La deuxième bande de 20 MHz dite ITS-G5B, est destinée aux autres applications. La dernière bande de 20 MHz (ITS-G5D) est réservée pour un usage futur. Dans le standard Européen, le canal 180 (CCH) de la bande ITS-G5A est dédié aux applications de sécurité routière. Les deux autres sont des canaux de services supplémentaires.

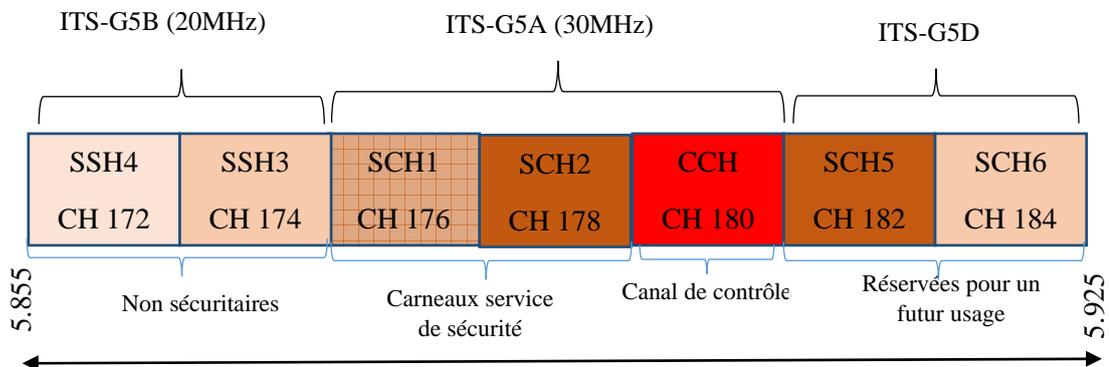


Figure 2-4 Allocation de fréquences en Europe

Les deux sections suivantes présentent les deux architectures protocolaires WAVE et ETSI-ITS, proposées aux Etats-Unis et en Europe, respectivement.

2.5.1 Architecture IEEE WAVE

Cette architecture a été définie par l'IEEE pour l'accès sans fil dans les réseaux de véhicules. Elle est représentée par la famille des standards « *IEEE 1609* ». Cette famille de standards est dite « *Wireless Access in Vehicular Environment (WAVE)* ».

La couche physique et la sous-couche MAC⁵ de cette architecture sont définies par le standard IEEE 802.11p [41]. Ce dernier est une adaptation de la norme IEEE 802.11a pour l'environnement véhiculaire. Par exemple, pour réduire le surcoût des communications et gagner du temps, les procédures de gestion du BSS « *Basic Service Set* » telles que la scrutation du canal, l'authentification et l'association, ont été désactivées. Un nouveau mode de communication appelé « *Outside the Context of BSS (OCB)* », a été défini pour remplacer le BSS. Dans ce mode, les communications sont limitées uniquement aux nœuds qui n'appartiennent pas à un BSS (un nœud ne peut pas participer à une communication OCB s'il appartient à un BSS) [18].

Cependant, cela peut avoir un impact négatif sur le plan sécurité. Le standard 1609.2 [26] offre des services et des mécanismes pour sécuriser les messages de gestion et d'application. Il définit les mécanismes pour l'authentification et le cryptage de messages. Il définit aussi les conditions d'utilisation des échanges de messages sécurisés et comment ces messages doivent être traités à la réception.

Comme illustré dans la figure 2-5, une sous-couche a été introduite dans la pile protocolaire entre la sous-couche MAC et la sous-couche LLC. Cette sous-couche est définie par le standard 1609.4 [27], elle représente une extension de la couche MAC, pour un environnement multicanal. Elle offre des services d'ordonnancement et de coordination de l'utilisation des différents canaux. Elle permet aux nœuds qui utilisent plusieurs canaux radio de se retrouver sur un même canal (le canal CCH) à un intervalle régulier. Dans cet intervalle (ou sur ce canal), les nœuds reçoivent des messages de gestion et des messages

⁵ Medium Access Control

d'annonces de services disponibles sur les autres canaux.

Le standard 1609.3 [28] définit les services de la couche réseau et transport, y compris l'adressage et le routage. Il définit également le protocole « *WAVE Short Message Protocole (WSMP)* ». Ce protocole assure les fonctionnalités des couches réseau et transport. Les paquets envoyés en utilisant ce protocole sont appelés « *WAVE Short Messages (WSMs)* ». Ce standard définit aussi les messages « *WAVE Service Advertisement (WSA)* » qui sont utilisés pour transporter les messages de gestion (ex : débit autorisé) et les messages d'annonces de service. Les *WSA* passent par le plan gestion.

Le standard 1609.1 définit le « *WAVE Resource Manager (RM)* » qui permet aux applications localisées sur des sites distants de communiquer avec les OBU, à travers les RSUs. Il définit aussi le format des messages échangés entre les RSUs et les OBUs [29]. Ce standard n'est pas représenté dans la figure 2-5, mais il peut être positionné au niveau de la couche application.

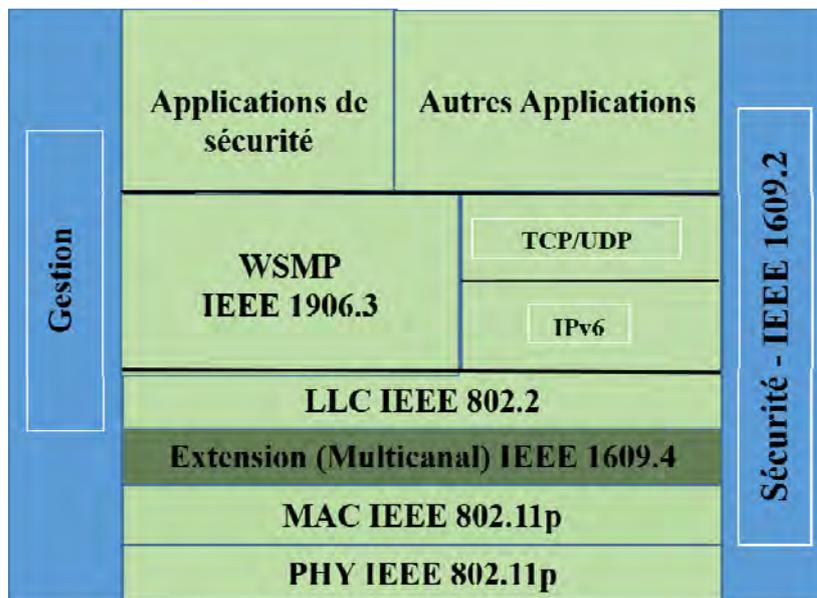


Figure 2-5 Architecture WAVE

2.5.2 Architecture ETSI-ITS

En 2013 le Comité Européen de Normalisation « *CEN* » et l'ETSI ont délivré la

première série de standards pour les systèmes de transport intelligents coopératifs « *Cooperative-Intelligent Transport Systems (C-ITS)* ». Comme illustré dans la figure 2-6, cette architecture est composée de quatre couches, plus les deux plans sécurité et gestion [13].

La technologie d'accès définit en Europe (ITS-G5) est dérivée du standard IEEE 802.11p de l'architecture WAVE et adaptée aux règlements européens [13]. Cependant, contrairement à l'architecture WAVE, l'architecture ETSI-ITS intègre plusieurs technologies de communication (WiFi, ITS-G5, Bluetooth, Réseau Cellulaire, WiMax). Le standard de l'ETSI TS 102 724 [30] représente une extension de la couche MAC de l'ITS-G5 pour un environnement multicanal.

Les couches réseau et transport sont définies dans la série de standards ETSI EN 302 636 [31]. L'utilisation de ces deux couches dépend de l'application. Les protocoles classiques de l'internet IPv6 et TCP/UDP sont utilisés notamment dans les applications de confort qui communiquent avec l'infrastructure de télécommunication. La partie « *Geonetworking & BTP* » est utilisée dans les applications où les communications sont purement ad hoc, notamment dans les applications de sécurité routière.

Cette architecture introduit une nouvelle couche appelée « *Facilities* ». Elle est spécifiée dans le standard [32] et elle fournit trois services :

- *Support d'application* : il fournit des fonctionnalités et des services communs pour l'exécution des applications. Une fonctionnalité importante de ce support est la gestion des CAMs et des DENMs.
- *Support d'information* : il fournit des données communes et des fonctionnalités de gestion de base de données pour l'exécution des applications. Il gère par exemple la carte locale dynamique de l'environnement véhiculaire « *Local Dynamic Map (LDM)* ».
- *Support de communication* : il offre des services pour la communication comme le mode d'adressage et l'interface homme-machine (IHM).

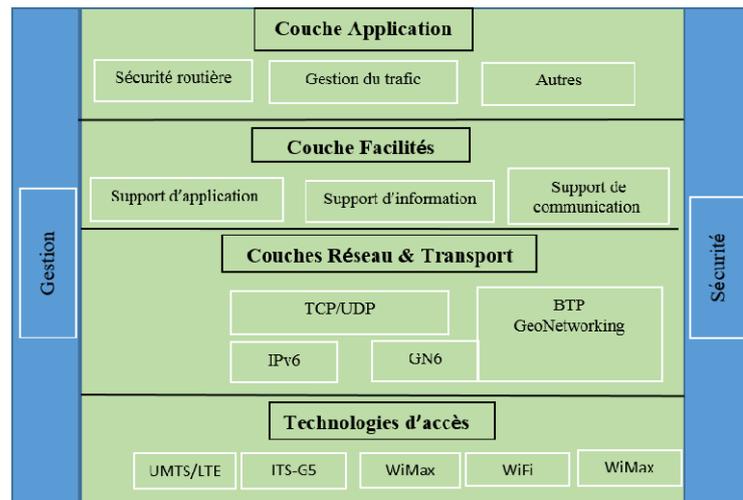


Figure 2-6 Architecture ETSI-ITS

2.6 Conclusion

Notre objectif dans ce chapitre était de présenter le contexte de cette thèse, à savoir les VANETs. Nous avons présenté les différentes caractéristiques de cette nouvelle technologie. Une large gamme d'applications qui peuvent être déployées dans un environnement véhiculaire ont été proposées ces dernières années. Nous avons présenté brièvement de telles applications. Nous avons présenté une classification des applications ainsi que leurs principaux attributs. Comme les applications de sécurité routière sont la principale cible des VANETs, nous nous sommes concentrés beaucoup plus dans ce chapitre sur cette catégorie d'application. Nous nous intéressons plus particulièrement à la dissémination des messages d'alerte dans un environnement autoroutier en l'absence d'infrastructure (des communications de type V2V).

Un grand travail de standardisation a été effectué ces dernières années, en Europe et aux Etats-Unis. Nous avons présenté un résumé des deux principales architectures protocolaires proposées, à savoir l'architecture WAVE aux Etats-Unis et l'architecture ETSI ITS en Europe. Dans cette thèse, nous nous baserons sur le standard IEEE 802.11p de l'architecture WAVE. Ce choix se justifie par l'implémentation de cette architecture dans les plateformes de simulation les plus répandues comme par exemple, le simulateur réseau NS2 [33].

Le format des messages de sécurité a été aussi standardisé. Les messages périodiques sont généralement diffusés par un nœud à destination de ses voisins proches (un seul saut).

Cependant, les messages d'alerte peuvent être destinés à des nœuds qui ne sont pas dans la portée de transmission du nœud source. En plus, contrairement aux autres applications, dans les applications de sécurité routière, les messages d'alerte concernent non seulement un nœud particulier, mais plutôt, plusieurs nœuds localisés dans une zone particulière. Dans ce cas, la diffusion du message sur plusieurs sauts est nécessaire. La diffusion multi-saut représente une thématique importante à laquelle nous consacrons le présent mémoire.

La diffusion de message sur plusieurs sauts, appelée aussi la dissémination de messages, a été largement étudiée dans les réseaux sans fil classiques tels que les MANETs et les réseaux de capteurs sans fil. Une large variété de mécanismes ont été proposés. Comme nous l'avons mentionné dans la section 2.3, les VANETs ont des caractéristiques très particulières, ce qui rend ces mécanismes non applicables directement aux VANETs.

Le chapitre suivant sera consacré à cette thématique, à savoir la dissémination de l'information de sécurité dans les VANETs.

Chapitre 3

Protocoles de dissémination d'alertes dans les VANETs

3.1 Introduction

Les systèmes de transport intelligents qui s'appuient sur les réseaux véhiculaires ont le potentiel de réduire les accidents de la route et de sauver des vies. Plusieurs cas d'utilisation ont été proposés. La plupart d'entre eux, notamment ceux destinés à améliorer la sécurité routière, utilisent des communications par diffusion. Dans le contexte de cette étude, nous nous focalisons sur les applications de sécurité routière. Plus précisément, la dissémination des messages d'alerte.

Comme nous l'avons mentionné dans la section 2.4.1, les deux types de messages qui sont échangés dans ces applications sont les messages périodiques (balises) et les messages d'alerte. La plupart des messages périodiques sont diffusés sur un seul saut, tandis que la plupart des messages d'alerte sont à diffuser loin du nœud source pour couvrir une zone géographique particulière. Dans ce dernier cas, l'application se base sur la diffusion multi-saut pour avertir tous les véhicules présents dans la zone spécifiée « *zone d'intérêt* ».

Cependant, la dissémination de messages sur plusieurs sauts pose de nombreux défis à surmonter, notamment, dans le cas d'un environnement véhiculaire très dynamique (cf. section 2.3). Nous décrivons les propriétés de la dissémination de l'information de sécurité dans la section 3.2.

Plusieurs travaux se sont attaqués au sujet de la dissémination de messages d'alerte dans les VANETs. Une large variété de protocoles ont été proposés. Nous proposerons une classification de ces protocoles dans la section 3.3. Cette classification se base sur un ensemble de critères que nous avons proposé pour mettre en évidence les principes de conception et les performances de ces protocoles (cf. sections 3.3.1 et 3.3.2). Des revues telles que [71, 72, 73] ont proposées différents critères de classification de protocoles de dissémination de l'information dans les VANETs. Dans notre étude, nous avons étendu les critères de classification afin de mieux caractériser les mécanismes de conception des protocoles de dissémination et de permettre leur comparaison du point de vue conceptuel.

Ces protocoles doivent être testés et évalués pour savoir s'ils répondent aux exigences des applications (cf. section 2.4.1) pour lesquelles ils ont été développés. Nous présentons dans la section 3.4 l'ensemble de métriques qui sont utilisées couramment pour comparer les protocoles de dissémination de l'information de sécurité dans les réseaux véhiculaires.

3.2 Défis et solutions possibles

Les informations sur le trafic routier peuvent être échangées périodiquement à travers des messages périodiques, tandis que les messages d'alerte sont diffusés en cas d'urgence ou de changement dans le trafic d'intérêt pour les conducteurs. Les messages périodiques⁶(balises/CAMs) générés par les véhicules sont diffusés pour que les conducteurs soient informés des détails utiles (tels que l'état du trafic routier, la position et vitesse des véhicules), les messages d'alerte (DENMs) sont diffusés pour notifier des changements soudains dans le trafic (freinage brusque, obstacles, accidents, sirène d'alerte de l'ambulance ...). Les messages d'alerte sont à temps critique et devraient avoir une plus grande priorité pour être transmis à temps. Dans ce qui suit nous présentons les défis de la dissémination des messages d'alerte et les solutions proposées dans la littérature.

⁶ Dans le reste de cette thèse nous utiliserons la notation Européenne, à savoir « CAMs », pour les messages périodiques et « DENMs », pour les messages d'alerte.

3.2.1 Défis

Contrairement à l'accès classique à l'internet où les messages sont généralement échangés en unicast, la dissémination de l'information dans les applications de sécurité des VANETs se base sur la diffusion, parce que l'information (en particulier les messages d'alerte) est d'intérêt pour tous les véhicules présents dans la *zone d'intérêt*. En outre, pour atteindre tous les véhicules dans la *zone d'intérêt*, certains d'entre eux étant hors de la portée de transmission de la source du message, la diffusion multi-saut devient nécessaire pour délivrer les messages.

La diffusion multi-saut n'est pas utilisée uniquement dans des applications de sécurité, elle l'est aussi dans d'autres applications telles que les applications de publicité développées pour les restaurants et les stations-service sur les autoroutes. Plusieurs protocoles ont adressé la dissémination des messages dans les VANETs sans accent particulier sur les applications de sécurité. Ces protocoles sont en général basés sur des mécanismes de dissémination semblables à ceux utilisés dans les DTNs (réseaux tolérants au délai) [34].

Contrairement aux autres catégories d'applications, dans les applications de sécurité, l'information traitée est (très) critique, ce qui rend le *Délai* et la *Fiabilité* les deux importantes métriques qui doivent être prises en compte dans le développement et l'évaluation des protocoles développés pour ces applications. En outre, tous les nœuds présents dans la zone concernée par l'événement doivent être informés et devraient recevoir le message diffusé. Un mécanisme de dissémination "parfait" est celui qui permet de livrer les données à tous les nœuds intéressés à temps et avec une utilisation optimale des ressources.

Malheureusement, la communication sans fil est généralement peu fiable et pose de nombreux défis à relever tels que le problème de la station cachée, les collisions de paquets, l'évanouissement du canal et les obstacles. En plus des pertes de paquets, en raison des collisions sur le support, la qualité du signal se dégrade avec la vitesse relative des véhicules [35]. Ainsi, la satisfaction de ces métriques est très difficile et il y a un compromis entre la fiabilité de la diffusion et le délai.

Les protocoles proposés tentent d'approcher le comportement de la dissémination parfaite sous certaines hypothèses et certains critères d'optimisation. Ils essaient de délivrer les messages à un maximum de nœuds accessibles dans la zone cible tout en gardant la

redondance faible.

3.2.2 Bases des approches

D'une part, les technologies DSRC/ITS-G5 sont censées avoir une portée de transmission maximale de 1000 m, et d'autre part les technologies connues actuellement en pratique ont environ 300 m de portée de transmission. De nombreuses applications de sécurité nécessitent jusqu'à plus de 1000 m (cf. tables 2-1 à 2-5) de portée de communication, pour fournir des informations utiles aux conducteurs le plus tôt possible et leur permettre de prendre les bonnes décisions (ralentir, freiner, changer de voie ...).

Afin de satisfaire les exigences des applications de sécurité (atteindre tous les véhicules dans la zone d'intérêt) en termes de portée de communication, il y a trois solutions principales :

- Utiliser des dispositifs à portée de transmission au moins égale à la portée maximale de communication de l'application pour atteindre tous les véhicules dans la *zone d'intérêt* en un seul saut. Même si les VANETs n'ont pas les contraintes de la batterie, l'utilisation d'une grande portée de transmission entraîne une grande perte de paquets et trop de messages retardés à cause des interférences et des collisions, mettant ainsi en péril le fonctionnement de l'application de sécurité. En conséquence, une telle alternative n'est pas recommandée en particulier lorsque la densité du réseau est élevée.
- Utiliser la diffusion avec une faible portée de transmission. Il n'y a pas de coordination dans la diffusion du même événement parce que chaque nœud maintient son propre ensemble d'informations et décide quand diffuser certaines données à ses voisins qui sont sur un seul saut. La diffusion sur un seul saut est un mécanisme non acquitté et, seul, il n'est pas efficace [36]. Notamment, dans les réseaux denses lorsque les nœuds reçoivent et renvoient les mêmes événements/données dans une zone limitée, le nombre de collisions peut être tellement important que la plupart des paquets sont détruits. Ainsi, les nœuds s'empêchent les uns les autres d'envoyer les paquets.
- Utiliser la diffusion sur plusieurs multi-saut avec une faible portée de transmission, et saut par saut tous les véhicules dans la *zone d'intérêt* sont

atteints. Cette solution est la plus utilisée en raison de son efficacité tant que la liaison est établie entre les nœuds pour relayer les messages de manière à ce que la redondance soit réduite. Dans les sections suivantes, nous nous concentrons sur cette solution.

3.3 Classification des mécanismes de dissémination

La façon la plus simple pour gérer la dissémination de l'information est l'inondation «*Flooding*». Cette dernière est une stratégie bien connue dans les réseaux sans fil traditionnels tels que les MANETs ou les réseaux de capteurs. Elle offre une probabilité élevée que tous les nœuds destinataires reçoivent le message dans l'hypothèse où il existe des chemins les reliant à la source.

Malheureusement, l'inondation pure est inefficace en particulier dans les réseaux denses, parce que le nombre de collisions devient de plus en plus élevé avec le nombre de nœuds dans la zone. En effet, dans les réseaux denses, l'inondation peut conduire au problème de tempête de diffusion «*broadcast storm problem*» [37] et ses conséquences négatives, notamment le gaspillage de la bande passante, la perte de paquets et les messages retardés.

Comme chaque nœud rediffuse tous les messages qu'il reçoit, l'inondation en soi conduit à la redondance (plusieurs copies des mêmes messages circulent sur les mêmes liens). L'objectif principal des protocoles de dissémination qui ont été proposés est de réduire la redondance, et par conséquent, améliorer l'utilisation du réseau en sélectionnant de manière distribuée un sous ensemble de nœuds qui rediffusent le message dans la *zone d'intérêt*.

La diffusion multi-saut a été largement étudiée dans les MANETs et les DTNs et de nombreux protocoles qui se basent sur la diffusion multi-saut ont été proposés [3, 38, 39]. Les VANETs étant une classe spécifique des MANETs, les protocoles proposés pour VANETs sont principalement des spécialisations et des adaptations de ceux proposés pour les MANETs. Cependant, les caractéristiques des VANETs, pour supporter les applications de sécurité, rendent les mécanismes proposés pour les MANETs classiques non directement applicables dans les VANETs, et des spécialisations ou une proposition de nouveaux mécanismes devient nécessaire.

Nous proposons une classification à deux niveaux des protocoles de dissémination qui

se basent sur la diffusion multi-saut: une approche de conception de haut niveau et une approche de conception à bas niveau [40]. Au premier niveau c'est l'approche de conception qui distingue un protocole des autres. C'est l'approche de base. L'approche de conception de haut niveau impacte la performance de la diffusion.

3.3.1 Approche de conception de bas niveau

Les protocoles de dissémination à base de diffusion multi-saut peuvent être catégorisés selon quelques mécanismes de base comme notamment (cf. figure 3-1) :

- **Balisage**

Utilisé pour permettre aux nœuds soit de diffuser des données périodiques et/ou d'échanger des informations d'état (nombre de messages reçus, nombre de messages diffusés, position et vitesse du véhicule ...).

- **Acquittement**

C'est un mécanisme de base pour améliorer la fiabilité. L'acquittement peut être explicite (un paquet ACK est utilisé pour accuser réception) ou implicite (après l'envoi d'un message, un nœud i écoute le canal et quand son voisin j rediffuse le message, le nœud i conclut que le message a été reçu par le nœud j). On notera que l'acquittement explicite engendre une augmentation dans le surcoût, essentiellement en termes de délai.

- **Adaptation de la portée de transmission**

Certains protocoles adaptent dynamiquement la portée de transmission selon la densité du réseau observée/estimée (c'est-à-dire transmettre avec une faible portée lorsque le réseau est dense et une portée élevée lorsque le réseau n'est pas dense).

- **Diffusion multi-canal**

Certains protocoles profitent des canaux disponibles pour diffuser les données sur plusieurs canaux. Il convient de noter que d'une part le nombre de canaux est très limité sous le DSRC (7 canaux aux Etats-Unis et 5 en Europe) et d'une autre part la gestion du multi-canal a un coût. En outre, les principaux acteurs de la

3. Protocoles de dissémination d'alertes dans les VANETs

sécurité dans le monde (principalement les États-Unis et l'Europe) ont fixé le nombre de canaux de distribution dédiés aux applications de sécurité. Par exemple, les canaux 172 aux États-Unis et 180 en Europe, sont exclusivement affectés à des applications de sécurité.

- **Utilisation d'infrastructure**

Certains protocoles s'appuient partiellement sur l'infrastructure fixe (ex : les RSUs) pour diffuser les données de sécurité tandis que d'autres sont entièrement sans infrastructure.

- **Zone de dissémination**

La zone de dissémination (à savoir *zone d'intérêt*) peut être explicite ou implicite. Différents paramètres (tels que la direction et la portée de communication) peuvent être utilisés pour spécifier cette zone. Lorsqu'elle n'est pas spécifiée, la dissémination peut être très coûteuse. Par conséquent, les protocoles existants qui ne spécifient pas la zone de dissémination devraient être adaptés avant leur déploiement.

- **Scénario du trafic**

Certains protocoles sont polyvalents (ils ciblent de multiples formes de trafic) tandis que d'autres sont spécifiques au contexte (par exemple la dissémination dans les zones urbaines ou sur des autoroutes).

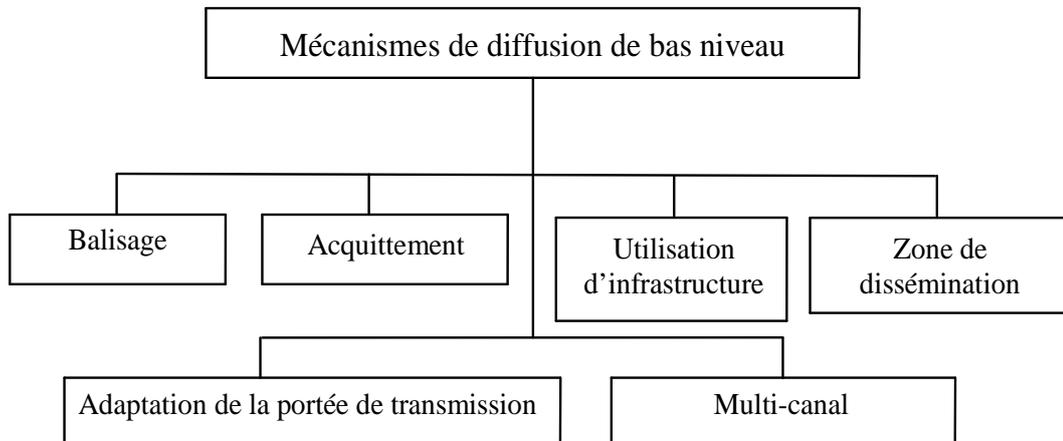


Figure 3-1 Critères de classification de bas niveau [40].

3.3.2 Approche de conception de haut-niveau

Nous avons identifié neuf classes de disséminations basées sur les mécanismes utilisés pour guider la rediffusion des messages reçus (cf. figure 3-2).

- **Dissémination à base de compteur**

Chaque nœud compte le nombre de fois qu'un paquet est reçu pendant une période déterminée, puis il compare ce nombre avec un seuil prédéterminé pour décider s'il rediffuse le paquet ou le détruit. L'avantage de cette approche est que les nœuds n'ont pas besoins d'échanger les états des voisins pour construire collectivement une décision sur la rediffusion.

- **Dissémination à base de délai**

Chaque nœud recevant un message à rediffuser, le garde pour un certain temps d'attente avant de décider de le rediffuser. Les temps de maintien sont choisis au hasard par les nœuds. Le nœud ayant le temps de maintien le plus court a la priorité la plus élevée pour rediffuser le message. Un nœud qui a un message à rediffuser ne le rediffuse pas s'il sait que le message a été rediffusé par un autre nœud voisin.

- **Dissémination à base de distance**

Les messages sont rediffusés en considérant la distance entre l'émetteur et les récepteurs. Lorsqu'un nœud reçoit un message, il ne le rediffuse pas si la distance entre lui et son voisin le plus proche qui a déjà rediffusé le même message est inférieure à un seuil prédéfini. La raison est que si un nœud a reçu un message d'un autre nœud très proche de lui, il y a peu d'avantages dans la couverture supplémentaire obtenue par la rediffusion du message reçu. Par conséquent, les nœuds devraient favoriser la rediffusion lorsque la distance au dernier relai est grande.

- **Dissémination à base de localisation**

Les messages sont diffusés aux nœuds sur la base des positions géographiques de la source et de la destination. Ce mécanisme suppose qu'un service de localisation est disponible pour permettre de localiser les nœuds. Le principe de cette approche est de réduire le nombre de nœuds relais en sélectionnant les nœuds permettant un maximum de progrès dans la direction de dissémination. Tous les récepteurs sont des relayeurs potentiels du message, et ils sont en concurrence entre eux pour rediffuser le message reçu, la période de contention est le temps qu'attendent les nœuds avant de rediffuser le message. Dans l'approche à base de localisation, cette période dépend essentiellement de la distance parcourue dans la direction de la dissémination.

- **Dissémination à base de trafic**

Des informations reflétant le trafic (densité, la vitesse du véhicule ...) sont utilisées pour guider les opérations de rediffusion. Il faut remarquer que la densité est le seul paramètre utilisé réellement dans les protocoles à base de trafic existants. L'utilisation d'autres paramètres peut entraîner un coût élevé pour recueillir les données d'état.

- **Dissémination à base de clusters**

Les messages sont diffusés à un groupe de véhicules (par exemple les taxis, les ambulances, peloton de véhicules sur une autoroute) se déplaçant sur un chemin commun. Le groupe peut être structuré en un niveau ou en une hiérarchie. Seulement, les nœuds têtes de clusters « Clusters Heads » rediffusent les

messages à l'intérieur de leur cluster.

- **Dissémination probabiliste**

Quand un nœud reçoit un message, il le rediffuse selon une valeur de probabilité. Plus est faible la probabilité de rediffusion, plus est faible le coût (la consommation de la bande passante) de la dissémination des données, et plus est faible la probabilité de livraison des messages à tous les destinataires. Plus est élevée la probabilité de rediffusion, plus est élevé le coût de la dissémination et plus est élevée la probabilité de livraison du message. Par conséquent, il existe un compromis entre le coût de la dissémination et la probabilité de livraison. Dans le cas d'une distribution uniforme de n nœuds dans une *zone d'intérêt*, en utilisant la même probabilité de diffusion P , le nombre moyen de nœuds qui rediffusent le message est $n * P$.

Les protocoles de dissémination existants ont proposé différentes façons pour dériver la probabilité de rediffusion : une valeur fixe pendant toute la durée de vie du réseau, une valeur fixe pendant une certaine période de temps, une valeur qui est fonction du nombre de messages reçus dans un intervalle de temps, une valeur qui est fonction du nombre de voisins à un saut, la distance entre l'émetteur et le récepteur du message, etc. Chaque modèle de calcul de la probabilité de rediffusion a ses avantages (simplicité et flexibilité) et ses inconvénients (surcharge due à la collecte des données utilisées dans le calcul de probabilité). Dans les protocoles existants, le mécanisme basé sur la probabilité est combiné avec d'autres mécanismes (par exemple, la distance ou la densité) pour améliorer la performance de la dissémination.

- **Dissémination à base de codage réseau**

Depuis quelques années, le codage réseau [42] est devenu très populaire. Il offre un mécanisme efficace pour réduire la consommation de bande passante dans les réseaux tout en augmentant le taux de livraison des messages. L'idée de base du codage réseau est la suivante: au lieu de simplement rediffuser les paquets qu'ils reçoivent, les nœuds prennent plusieurs paquets et les combinent dans un seul paquet pour la transmission. La combinaison des paquets est basée sur des opérations (linéaires) appliquées à n paquets pour obtenir un paquet. Actuellement, très peu de protocoles sont basés sur le codage réseau. Il a été

3. Protocoles de dissémination d'alertes dans les VANETs

démontré que le codage réseau peut améliorer la diffusion multi-saut dans les VANETs sans augmenter la complexité de conception des protocoles.

- Dissémination hybrides (basée sur plusieurs critères)

De nombreux protocoles proposés ne sont pas basés sur un seul critère, mais plutôt combinant différents critères pour prendre de meilleures décisions de rediffusion. Par exemple, les méthodes à base de probabilité utilisent la distance ou la densité pour dériver la probabilité de rediffusion, et les méthodes à base de délai utilisent la distance et la localisation pour calculer la valeur de délai d'attente avant de tenter de rediffuser.

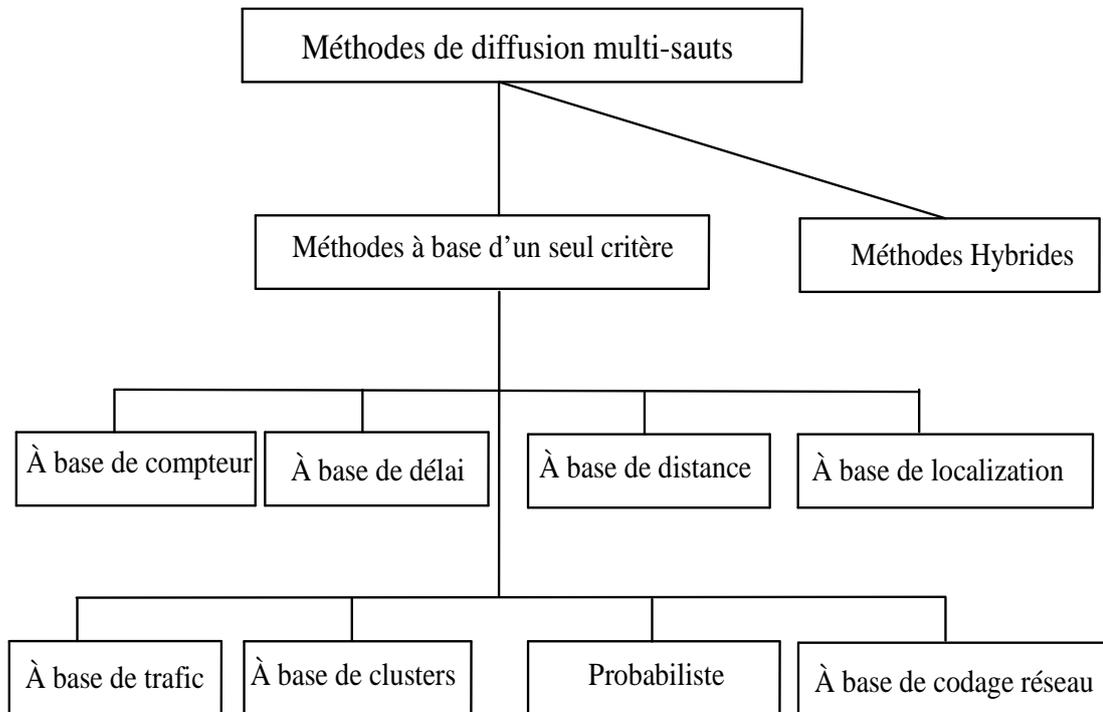


Figure 3-2 Critères de classification de haut niveau [40]

3.4 Métriques d'évaluation des protocoles de dissémination

Pour évaluer comment un protocole donné fonctionne par rapport à d'autres protocoles ou à la dissémination parfaite, des métriques ont été utilisées. Certaines métriques sont primitives tandis que d'autres peuvent être obtenues à partir d'autres métriques. Il est à noter que la définition de la même métrique peut varier selon les auteurs. En outre, certaines métriques sont plus pertinentes pour évaluer un protocole spécifique que, pour comparer différents protocoles.

Il convient également de remarquer que la performance observée (fournie par la simulation ou l'observation réelle des véhicules) dépend de nombreux facteurs, notamment de la densité du trafic et de la portée de transmission.

Il existe trois modèles de trafic, appelés régimes de trafic [7], qui impactent significativement les performances des protocoles de dissémination et nécessitent une adaptation de la diffusion : trafic dense, trafic clairsemé et trafic régulier.

- *Régime de trafic dense* : c'est lorsque le trafic est supérieur à une certaine valeur. Dans ce cas -également connu comme *problème de tempête de diffusion* « *Broadcast Storm problem* » [NTCS99]-, la probabilité de collision entre les nœuds en contention est très élevée, ce qui entraîne la perte ou le retard de paquets.
- *Régime de trafic clairsemé* : il est observé dans certaines heures de la journée/semaine lorsque la densité de la circulation peut être si faible que la connectivité entre les nœuds devient indisponible et les messages ne peuvent pas atteindre à temps leur destination en raison d'insuffisance de nœuds relayeurs.
- *Régime de trafic régulier* : c'est le régime dominant lorsque le trafic des véhicules est observé. Il se caractérise par un trafic non-homogène (quelques nœuds peuvent avoir quelques voisins, tandis que d'autres en ont beaucoup).

Nous présentons l'ensemble des métriques qui sont utilisées couramment pour comparer les protocoles de dissémination qui se basent sur la diffusion multi-saut. En général, la valeur moyenne de la métrique est considérée pour l'évaluation/comparaison des performances. Nous avons identifié douze métriques qui peuvent être catégorisées comme suit:

❖ Métriques temporelles et spatiales

- *Délai de bout en bout* : c'est le temps écoulé entre la première diffusion du message et sa réception par le dernier récepteur dans la zone d'intérêt. La valeur requise de la métrique dépend de l'application de sécurité considérée (cf. tables 2-1 à 2-5).
- *Distance de propagation* : elle mesure à quelle distance de la source le message est diffusé dans la zone d'intérêt. Une distance proche de (ou supérieure) à la portée de communication requise par l'application est attendue (cf. tables 2-1 à 2-5).
- *Vitesse de propagation (ou vitesse de dissémination)* : elle mesure la vitesse à laquelle le message se propage dans le réseau. Elle s'exprime par la distance parcourue par unité de temps, ou la portion de nœuds qui reçoivent le message par unité de temps.

❖ Fiabilité

- *Le taux (ou ratio) de livraison* : il mesure la proportion de véhicules dans la zone d'intérêt qui reçoivent le message. Une valeur proche de 100% est fortement préférable pour rendre réellement les VANETs très efficaces pour le support des applications de sécurité. Le taux de livraison est aussi appelé *Taux (ou ratio) de réception* (ou probabilité de réception).
- *Débit de réception* : c'est le nombre de messages (ou bits) reçus par un nœud dans une période de temps (par exemple en secondes). Cette mesure est particulièrement utile lorsque des données périodiques sont diffusées. Etant donné la période et la taille d'un message (cf. tables 2-1 à 2-5), cette mesure permet d'évaluer comment le débit de réception des nœuds est proche du débit optimal requis par l'application.
- *Taux de perte de paquets* : à cause des collisions, certains messages n'atteignent jamais certaines (ou toutes) destinations. Cette métrique, qui s'applique aux messages périodiques et aux messages d'alerte, est utile pour évaluer la fiabilité du réseau.

❖ Mesures d'efficacité

3. Protocoles de dissémination d'alertes dans les VANETs

- *Taux de Collisions* : comme les nœuds partagent le même canal sans fil, les collisions peuvent se produire lorsque les nœuds rediffusent les messages. Cette métrique donne une indication sur la façon dont les opérations de la rediffusion impactent les performances du réseau.
- *Taux de redondance* : il mesure le nombre de paquets dupliqués par un paquet source. En d'autres termes, la redondance indique combien de fois un paquet est rediffusé pour atteindre les véhicules dans la zone d'intérêt. C'est un indicateur de surcoût. La limite supérieure du taux de redondance est donnée par l'inondation pure. La redondance est un indicateur clé de performance d'un protocole de dissémination. Un bon protocole devrait être en mesure de disséminer l'information à travers toute la *zone d'intérêt* avec le moins de redondance ou de surcoût.
- *Surcoût de la diffusion du nœud* : au lieu du taux de redondance, certains auteurs utilisent le surcoût de la rediffusion, qui est le nombre de messages rediffusés collectivement dans la zone d'intérêt.
- *Taux de nœuds diffuseurs* : il mesure la proportion de nœuds qui rediffusent un message. C'est un indicateur de l'implication des nœuds dans la rediffusion. La limite supérieure est de 100% (d'inondation pure) ce qui signifie que tous les nœuds rediffusent le message.
- *Taux de rediffusion du nœud* : il mesure le nombre de fois que le nœud rediffuse les messages dans un intervalle de temps donné. Il mesure l'équité dans la rediffusion. Cette mesure peut être utilisée pour détecter les nœuds avec une forte participation dans la rediffusion (par exemple des nœuds avec le rayon de communication plus élevé ou des nœuds qui attaquent le réseau pour diffuser de fausses alertes ...).
- *Utilisation du canal* : elle mesure comment la charge globale de la rediffusion occupe le canal. Dans les applications de sécurité, l'utilisation du canal doit rester faible ce qui signifie que le canal doit être libre de temps en temps pour permettre la diffusion de messages d'alerte.

3.5 Discussion

Un grand nombre de protocoles de dissémination ont été proposés dans la littérature ces dernières années. Nous fournissons quatre tables (Tables 3-1, 3-2, 3-3 et 3-4) comparatives de 27 protocoles de dissémination. Cette classification est basée sur les critères que nous avons présentés dans la section 3.3. Les Tables 3-3 et 3-4 sont une synthèse de l'analyse des performances qualitatives des protocoles de dissémination. Elles montrent les métriques évaluées par les auteurs et les paramètres de simulation utilisés.

Presque tous les protocoles sont basés sur plusieurs critères où la *localisation*, la *distance* et le *trafic* sont considérés ensemble (parfois avec d'autres critères) pour guider les décisions de rediffusion. Aussi, presque tous les protocoles sont basés sur le délai, ce qui signifie que les nœuds attendent pour une période (aléatoire) de temps avant de tenter de rediffuser. C'est un mécanisme simple et puissant pour réduire la redondance de messages.

Les RSUs ne sont pas susceptibles d'être déployées dans le moyen terme en raison de leur coût financier. Par conséquent, presque tous les protocoles ne sont pas basés sur une infrastructure fixe. Les protocoles de dissémination existants sont de nature ad hoc. Une autre constatation est que l'adaptation de la portée de transmission et le multi-canal sont considérés dans très peu de protocoles, car ils nécessitent du matériel spécial supplémentaire sans surpasser nettement les autres protocoles.

S'il est possible de discuter de la performance des protocoles de dissémination du point de vue qualitatif, il est très difficile de comparer quantitativement leurs performances sur la base des résultats rapportés par les auteurs dans leurs papiers, compte tenu des hypothèses et les scénarios envisagés par les auteurs des protocoles.

Pour donner des résultats de performance, la *densité* est le principal paramètre de simulation qui est utilisé dans tous les articles que nous avons examinés. La *distance* de diffusion est utilisée à peu près dans la moitié des protocoles. La *vitesse* du véhicule est considérée de trois façons: une valeur constante pour tous les véhicules, une valeur aléatoire choisie dans un intervalle ou une valeur aléatoire ne dépassant pas un maximum

Comme on peut le remarquer sur les tables 3-3 et 3-4, très peu d'articles ont fourni une simulation intensive et "complète". Certains papiers ciblant les applications de sécurité ont présenté des résultats de simulation non pertinente (sans importance) à ces applications,

3. Protocoles de dissémination d'alertes dans les VANETs

parce que certains auteurs ont mal compris les exigences des applications de sécurité (par exemple en fournissant des résultats avec une distance de dissémination de plus de 10 km, ce qui est beaucoup plus élevé que ce qui est requis par les applications de sécurité, cf. tables 2-1 à 2-5).

Les modèles de mobilité utilisés dans de nombreuses simulations sont trop simplistes. Par conséquent, presque tous les protocoles proposés ont besoin de plus d'analyse de performance afin de mieux déterminer les conditions dans lesquelles leurs mesures de performance sont acceptables ou non.

Comme indiqué précédemment, les principales exigences des applications de sécurité sont la rapidité et la fiabilité. La table 3-3 montre que presque tous les protocoles des auteurs ont rapporté des résultats sur le *délai de bout en bout* et le *ratio de livraison*. Aussi, presque tous les auteurs de protocoles fournissent quelques résultats sur le *taux de redondance* (qui est une métrique de surcoût).

3. Protocoles de dissémination d'alertes dans les VANETs

Table 3-1 Classification des protocoles de dissémination -Approche de conception de haut-niveau

Critères Protocoles	Compteur	Localisation	Distance	Cluster	Trafic	Délai	Probabilité	Codage réseau
AMB [52]		√	√			√		
BZB [47]		√	√		√	√		
CBD [53]		√	√			√		
CTR [54]		√	√			√		
DBA-MAC [55]		√	√	√	√	√		
DBBP [56]		√	√			√		
FB [48]		√	√			√		
FR-EDM [49]		√	√		√	√		
LBF [57]	√	√	√		√	√	√	
LDNC [58]		√			√			√
MHVB [59]	√	√	√		√	√		
NTPP [60]			√		√	√	√	
OAPB [61]	√				√	√	√	
ODAM [44]		√	√			√		
OPbG [62]	√	√	√		√		√	
PAB [63]		√	√		√	√		
PbG [64]		√			√		√	
p-IVG [50]		√	√		√	√	√	
REACT [65]		√			√			
REAR [66]		√			√	√	√	
SB [46]		√	√		√	√		
SPP [5]		√	√			√	√	
StaB [67]			√		√			
StocB [68]					√		√	
S1P [5]		√	√			√		
UMB [69]		√	√			√		
WPP [5]		√	√			√	√	

3. Protocoles de dissémination d'alertes dans les VANETs

Table 3-2 Classification des protocoles de dissémination -Approche de conception de bas-niveau

Critères Protocoles	Balilage	Acquittement	Adaptation de la portée de transmission	Multicanal	Zone de Dissémination	Utilisation de l'infrastructure	Scénario de trafic
AMB [52]		E			D		AT/U
BZB [47]	√				D; A	√	AT/U
CBD [53]	√		√		D; A		AT
CTR [54]				√	D; A; T		AT
DBA-MAC [55]	√	E			D; A; T		AT
DBBP [56]	√				D; A		AT
FB [48]	√				A		AT
FR-EDM [49]	√	I			D; A	√	AT
LBF [57]					-		AT
LDNC [58]	√				-		AT
MHVB [59]	√				A		AT
NTPP [60]	√		√		-		AT
OAPB [61]	√				A	√	AT/U
ODAM [44]		I			A		AT/U
OPbG [62]	√				D		AT/U
PAB [63]					D		AT
PbG [64]	√				D		AT
p-IVG [50]	√				-		AT
REACT [65]	√	I			D; A; T		AT
REAR [66]	√				D		AT
SB [46]		I			D		AT
SPP [5]					-		AT
StaB [67]					-		-
StocB [68]					-		-
S1P [5]					-		AT
UMB [69]		E			D	√	AT/U
WPP [5]					-		AT

- : Non spécifiée ; D : Direction ; A : Aléatoire ; T : TTL (Time to live) ; E : ACK explicite ; I : ACK implicite ; AT : Autoroute ;

U :

Urbain

3. Protocoles de dissémination d'alertes dans les VANETs

Table 3-3 Métriques de performance des protocoles de dissémination

	Temporelles et spatiales			Fiabilité			Efficacité			
	Délai de bout en bout	Vitesse de Propagation	Distance de Propagation	Débit de réception	Taux de réception	Taux de perte de paquets	Taux de redondance	Surcoût du nœud	Taux de nœuds diffuseurs	Utilisation du canal
AMB		√			√		√			
BZB	√						√			
CBD	√				√		√			√
CTR	√				√				√	
DBA-MAC	√					√	√			
DBBP	√				√				√	
FB						√				
FR-EDM	√				√					
LBF					√		√			
LDNC				√						
MHVB					√	√				
NTPP	√							√		
OAPB	√				√		√			
ODAM					√					
OPbG					√		√			
PAB	√								√	
PbG					√		√			
p-IVG	√				√					√
REACT	√					√				
REAR	√				√		√			
SB		√								
SPP	√	√				√				√
StaB					√			√		
StocB					√			√		
SIP	√	√				√				√
UMB		√			√		√			
WPP	√	√				√				√

√: analysée par les auteurs du protocole; -: non spécifiée

3. Protocoles de dissémination d'alertes dans les VANETs

Table 3-4 Paramètres de simulation

Protocoles	Vitesse des véhicules (km/h)	Distance	Densité des nœuds	Erreur du canal	Portée de transmission	Moyenne de génération de paquets	Taille du paquet
AMB	40 ± 5		√			√	√
BZB	-	√	√				√
CBD	120	√					
CTR	[72,97]	√			√		√
DBA-MAC	[72,108]	√	√			√	
DBBP	≤ 151	√	√				
FB	[72,144]		√		√		
FR-EDM	100	√	√	√			
LBF	-	√	√				
LDNC	-		√			√	
MHVB	≤ 80	√	√				
NTPP	[70,120]				√	√	
OAPB	72 ± 14		√				
ODAM	90 ± 18		√		√		
OPbG	0; 72		√				
PAB	[70,110]	√	√				
PbG	0; 30; 60; 140		√				
p-IVG	≤108	√	√				
REACT	[72,108]	√	√				
REAR	[72,108]		√				
SB	-		√				
SPP	-		√				
StaB	-		√	√			
StocB	-		√				
SIP	-		√				
UMB	40 ± 5		√			√	√
WPP			√				

3.6 Conclusion

La diffusion multi-saut est une composante essentielle des protocoles de dissémination pour supporter les applications de sécurité routière. Dans ce chapitre, nous avons présenté une étude des protocoles de dissémination qui se basent sur la diffusion multi-saut les plus connus et les plus cités. Ces protocoles ont été conçus pour satisfaire les exigences des applications de la sécurité routière (principalement la contrainte de délai et de fiabilité) tout en gardant un surcoût protocolaire acceptable.

Chaque protocole a ses propres avantages et ses limites, et un compromis entre eux doit être accepté. Il n'existe pas de protocole parfait, et, approcher d'un tel protocole soulève de nombreux défis pour la recherche future. Certains protocoles sont efficaces pour délivrer des messages périodiques (balises) tandis que d'autres sont efficaces pour délivrer les messages d'alerte. Certains protocoles se comportent bien uniquement sous une densité faible, tandis que d'autres ont un rendement acceptable dans des réseaux denses.

Nous avons présenté des métriques pour évaluer les protocoles de dissémination. Notre étude s'est limitée à une évaluation de la performance qualitative, basée sur les résultats de simulation présentés dans les papiers originaux. Il convient de noter que la comparaison quantitative des protocoles existants nécessite beaucoup de travail pour examiner les protocoles dans les mêmes hypothèses (mobilité et scénario de simulation).

La sécurité et la vie privée, sont des problèmes bien connus en raison d'attaques dont les VANETs tels que le déni de service, la diffusion d'informations et alertes fausses, et la collecte de données privées (telles que les emplacements et les itinéraires). La conception des protocoles qui se basent sur la diffusion multi-saut et qui répondent aux exigences de rapidité, de fiabilité et de sécurité tout en optimisant l'utilisation des ressources, est très difficile.

Comme nous l'avons mentionné dans la section 3.5, la plupart de ces protocoles se base sur la distance et le délai dans leur mécanisme de sélection du prochain nœud relai. En effet, la distance est utilisée notamment pour définir une fenêtre de contention⁷ à partir de laquelle les nœuds choisissent leurs temps d'attente. Les performances de ces protocoles dépendent essentiellement de cette fenêtre. Cependant, plusieurs paramètres doivent être considérés dans la définition de cette dernière, notamment la densité du réseau.

⁷ Il convient de noter que c'est une fenêtre au niveau de la couche réseau et à ne pas confondre avec la fenêtre de contention au niveau de la couche MAC.

Chapitre 4

Analyse de performance des mécanismes de dissémination d'alertes

4.1 Introduction

Ce chapitre fournit une étude de la dissémination de messages dans les réseaux véhiculaires. Nous évaluons et nous comparons les performances de l'approche à base de distance. Notre choix se justifie par le fait que ce mécanisme est à la base de la plus part des protocoles de dissémination qui ont été présentés dans la littérature. Notons en outre qu'il est le mécanisme adopté par l'ETSI ITS dans le protocole Geonetworking [75].

Dans cette étude, nous avons choisi trois variantes du mécanisme à base de distance, à savoir : *Contention Based Forwarding* [75, 53], *Slotted 1-persistence* [5] et *Random Contention Based Forwarding* [47]. Dans chacun de ces trois mécanismes, la distance est

utilisée de différentes façons comme une variable discriminatoire pour favoriser certains nœuds pour rediffuser le message dans la zone d'intérêt. En plus de ces mécanismes, nous avons implémenté le mécanisme d'inondation « *Flooding* » qui sera utilisé comme un mécanisme de référence. Nous décrivons en détail ces mécanismes dans la section suivante.

Dans cette analyse, nous utilisons le simulateur de réseaux NS2 [33] et le simulateur de mobilité SUMO [51]. La section 4.3 définit les paramètres et le scénario de simulation, respectivement. Dans la section 4.4, nous définissons les métriques d'évaluation. Ensuite, nous étudions les performances de ces mécanismes et nous analysons les résultats obtenus, dans la section 4.5. Finalement, dans la section 4.6, nous étudions l'impact de la durée du slot sur les performances des trois mécanismes présentés.

4.2 Description des mécanismes

- *Contention Based Forwarding* « *CBF* » [75, 35]

C'est un mécanisme simple dans lequel chaque nœud qui reçoit un nouveau message, attend un délai qui est inversement proportionnel de sa distance par rapport au dernier relai, avant de décider de rediffuser ou non le message. Durant ce temps d'attente, si le nœud reçoit le même message, rediffusé par un autre nœud, il détruit le message et abandonne la procédure. Sinon, il le rediffuse dès que son temps d'attente expire. Ce dernier est calculé comme suit :

$$T = T_{max} \times \left(1 - \frac{D}{R}\right) \quad (4.1)$$

où T est le temps d'attente, T_{max} le temps d'attente maximum, D est la distance entre l'émetteur et le récepteur et R est le rayon de transmission.

- *Slotted 1-persistence* « *SIP* » [5]

Dans *slotted 1-persistence*, la portée de transmission de l'émetteur est divisée en plusieurs segments de taille fixe. Chaque nœud est affecté à un segment, selon sa distance par rapport au nœud émetteur/dernier relai. Les nœuds appartenant au segment le plus éloigné du dernier relai ont le plus court temps d'attente. Ce dernier est calculé comme suit :

$$T_{S_{ij}} = S_{ij} \times \tau \quad (4.2)$$

$$S_{ij} = N_s \left(1 - \left[\frac{\min(D_{ij}, R)}{R} \right] \right) \quad (4.3)$$

où D_{ij} est la distance entre les nœuds i et j , R est le rayon de transmission, N_s est le nombre de slots, τ est le délai estimé d’un saut (délai d’accès au canal et le délai de propagation).

Chaque nœud rediffuse le message dans son slot de temps s’il n’entend pas le message rediffusé par un autre nœud voisin. La figure 4.1 illustre un exemple avec quatre segments de longueur fixe.

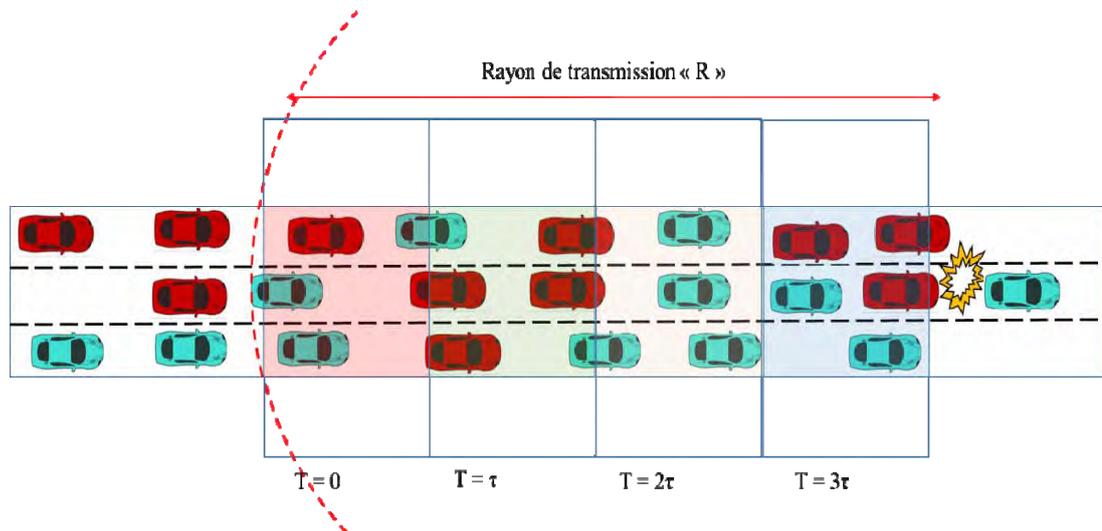


Figure 4-1 Exemple d’illustration avec quatre segments

- **Random Contention Based Forwarding « RCBF »**

Dans ce mécanisme, chaque nœud qui reçoit le message tire une valeur de temps d’attente dans une fenêtre de contention $[C_{\min}, C_{\max}]$. Les bornes de cette fenêtre dépendent de la distance du nœud par rapport au dernier nœud relai. Ce dernier a été inspiré des mécanismes présentés dans [47] et [48]. Comme il est indiqué dans les équations (4.4) et (4.5) les nœuds les plus éloigné auront la plus courte fenêtre de contention.

$$C_{min} = T_{min} \quad (4.4)$$

$$C_{max} = T_{max} \times \left(1 - \frac{D}{R}\right) \quad (4.5)$$

Où T_{min} est le temps d'attente minimum, T_{max} le temps d'attente maximum, D est la distance entre l'émetteur et le récepteur et R est le rayon de transmission. De même que les deux autres mécanismes, le nœud rediffuse le message après expiration de son timer, s'il n'entend pas le message rediffusé par un autre nœud.

- ***Flooding*** [37, 75]

C'est le mécanisme d'inondation où chaque nœud à l'intérieur de la zone d'intérêt rediffuse immédiatement, sans attendre, le message qu'il reçoit pour la première fois. Chaque nœud rediffuse le message une seule fois.

4.3 Paramètres et scénario de simulation

4.3.1 Paramètres de simulation

Nous avons implanté les quatre mécanismes de dissémination dans le simulateur NS2 [33]. La couche physique du standard IEEE 802.11p (nous nous fondons sur le modèle étendu 802.11Ext du simulateur NS2) est utilisée avec un débit de 12Mbit/s.

Pour *slotted 1-persistence*, nous avons fixé le nombre de slots à 5 « $N_s = 5$ », ce qui correspond à cinq segments d'une longueur de 60m (avec un rayon de transmission de 300 m). Nous fixons la durée de slot à 0.52 ms ce qui correspond à 40 fois le slot MAC du standard 802.11p (durée du slot = 40 × 0,013 ms). L'impact de la variation de la durée du slot sera étudié plus en détail dans la section 4.6.

Les modèles de mobilité sont générés en utilisant le simulateur du trafic routier SUMO [51]. Le nombre de véhicules varie de 10 véhicules/voie/km à 60 véhicules/voie/km, ce qui correspond à un nombre total de véhicules variant entre 360 et 2160. La vitesse maximale est fixée à 130 km/h (vitesse maximale sur les routes en France).

4. Analyse de performance des mécanismes de dissémination d'alertes

Nous supposons que chaque véhicule est équipé d'une OBU implémentant le standard WAVE/DSRC et un moyen de localisation tel que le GPS. Les paramètres de simulation utilisés sont résumés dans la table 4.1.

Table 4-1 Paramètres de simulation

Paramètre	Valeur
Longueur de la zone de simulation	6 km*3voies/ Deux Directions
Zone d'intérêt	3 km
Rayon de transmission	300m
Taille des DENMs	50 octets
Taille des CAMs	40 octets
Durée du slot de temps	0.52ms
Modèle de propagation	Nakagami
Temps de simulation	60s
Débit	12Mbps
Fréquence des DENMs	1Hz
Fréquence des CAMs	10 Hz
T_{\max}	100 ms
T_{\min}	0

4.3.2 Scénario

Nous considérons un scénario d'un segment de 6 km d'une autoroute sans intersection, avec trois voies dans chaque direction. Les véhicules communiquent directement entre eux. Chaque véhicule envoie des CAMs à une fréquence de 10 Hz.

Il convient de noter que dans [5], les auteurs de *slotted 1-persistence* ne considèrent pas la présence des CAMs. Comme la plus part des applications de sécurité routière se basent sur les CAMs, dans notre étude ils seront considérés comme un trafic de fond. En plus, dans notre étude nous considérons la dissémination de messages dans les deux directions de circulation.

Dans notre étude de performance, nous avons mis une source de DENMs qui génère des

4. Analyse de performance des mécanismes de dissémination d'alertes

DENMs à une fréquence de 1 Hz. Cette source peut être considérée aussi comme une RSU qui diffuse périodiquement des informations sur le trafic routier (cf. figure 4.2). Ces messages doivent être relayés pour couvrir tous les nœuds présents dans une *zone d'intérêt* sur 3 km.

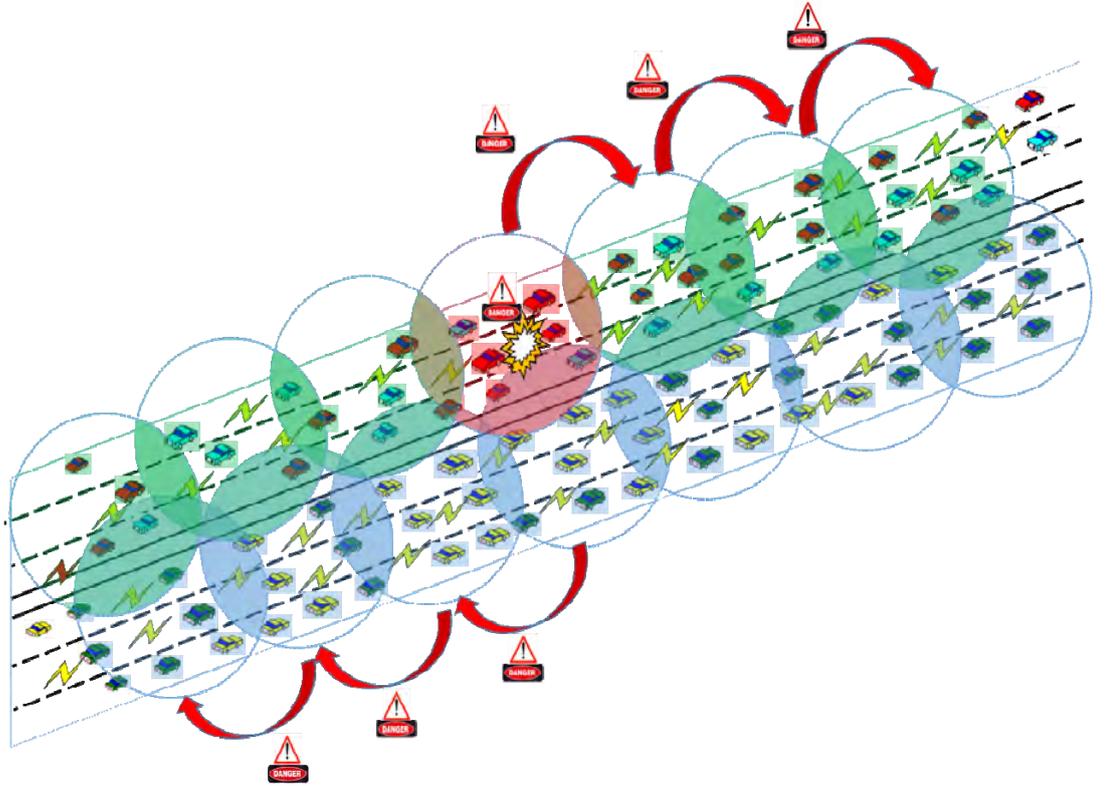


Figure 4-2 Scénario

4.4 Métriques d'évaluation de performance

Afin d'étudier les performances de ces mécanismes, nous définissons les métriques suivantes :

- **Taux de réception de messages :** c'est une métrique importante dans les applications de sécurité routière car il est important que tous les véhicules présents dans la zone de danger reçoivent correctement les messages d'alerte diffusés par des véhicules en situation anormale ou par une RSU. Il représente la moyenne du nombre de messages reçus par chaque nœud divisé par le nombre total de messages générés :

4. Analyse de performance des mécanismes de dissémination d'alertes

$$T_{\text{recp}} = \frac{\text{moyenne du no. msg Rx}}{\text{no. msg générés}} \quad (4.6)$$

- **Délai de livraison** : le délai de livraison est aussi une métrique importante dans les applications de sécurité routière comme par exemple l'application « Avertissement *Collision dans l'intersection* » (cf. Table 2.1). Il représente le délai entre la transmission du message et sa réception par la destination :

$$D = t_{R_r} - t_{T_r} \quad (4.7)$$

- **Nombre de sauts parcourus** : il est défini comme étant le nombre moyen de sauts parcourus par un message pour atteindre le nœud le plus éloigné dans la zone d'intérêt.
- **Taux de redondance** : les retransmissions redondantes de message engendrent une augmentation de la contention sur le canal et par conséquent, une augmentation du nombre de collisions. C'est pour cette raison que les mécanismes de dissémination tentent de réduire au minimum le nombre de transmissions redondantes. Nous définissons le taux de redondance comme étant la moyenne du nombre de messages dupliqués reçus par les nœuds, divisé par le nombre de paquets générés. Cette métrique permet de mesurer le nombre de messages dupliqués par un message source :

$$TRD = \frac{\text{no. msg. dupliqués}}{\text{no. msg. générés}} \quad (4.8)$$

- **Nombre moyen de rediffusions** : il représente le nombre moyen de fois que le message a été rediffusé dans la zone d'intérêt. Cette métrique intègre les rediffusions dans les deux directions de circulation.

4.5 Etude de performance

4.5.1 Analyse du taux de réception de messages

Dans la figure 4-3, nous présentons le taux de réception en fonction de la densité du réseau des différents mécanismes. Il convient de noter que dans cette étude nous considérons que le réseau est bien connecté et il n'y a pas de déconnexion ou de nœuds isolés. Par conséquent, si un message n'est pas reçu par un nœud, cela est dû à la perte à cause de collisions.

Comme le montre la figure 4-3, le taux de réception de CBF et RCBF est supérieur à 98 %. A 10 véhicules/voie/km, le taux de réception de S1P et Flooding est à 31 % et 91 %, respectivement. En effet, ces deux mécanismes génèrent plus de transmissions redondantes par rapport à CBF et RCBF (cf. figure 4-7) ce qui augmente le risque de collisions. Dans S1P, plusieurs nœuds peuvent être présents dans le même segment. Dans ce cas, ces nœuds vont avoir le même slot de temps et vont rediffuser en même temps. En analysant les fichiers traces générés de Flooding et S1P, nous avons remarqué que, à cause de collisions, certains messages meurent avant de couvrir toute la zone d'intérêt (3km).

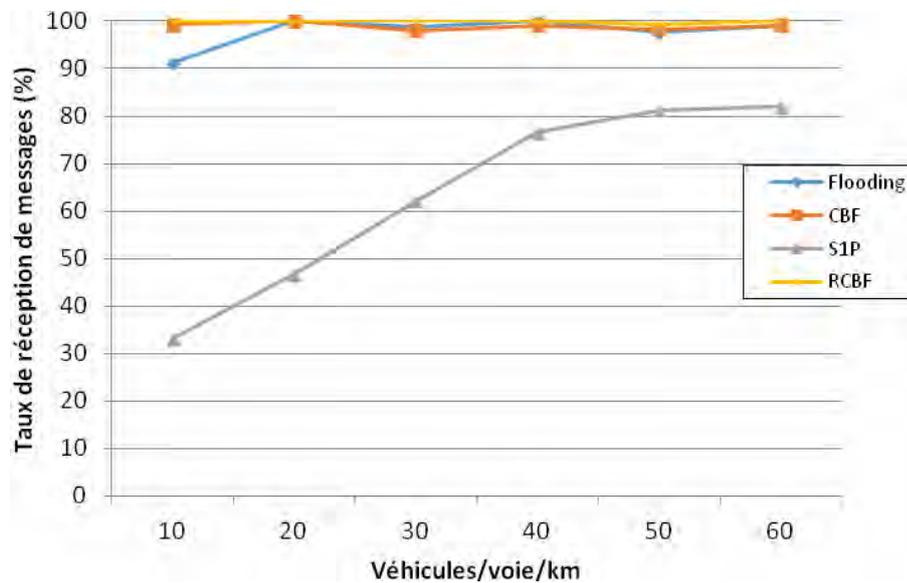


Figure 4-3 Taux de réception de messages en fonction du nombre de véhicules

4. Analyse de performance des mécanismes de dissémination d'alertes

Comme illustré dans la figure 4-3, le taux de réception de CBF et RCBF ne diminue pas car ces mécanismes réduisent considérablement le nombre de rediffusions dans la zone d'intérêt (cf. figure 4-7).

4.5.2 Analyse du délai de livraison

La figure 4-4 illustre le délai moyen de livraison à 3km des messages pour les quatre mécanismes. Comme attendu, le délai de livraison des différents mécanismes augmente avec l'augmentation de la densité du réseau. Dans Flooding, les nœuds n'attendent pas et rediffusent le message dès qu'il est reçu, ce qui justifie le faible délai de livraison.

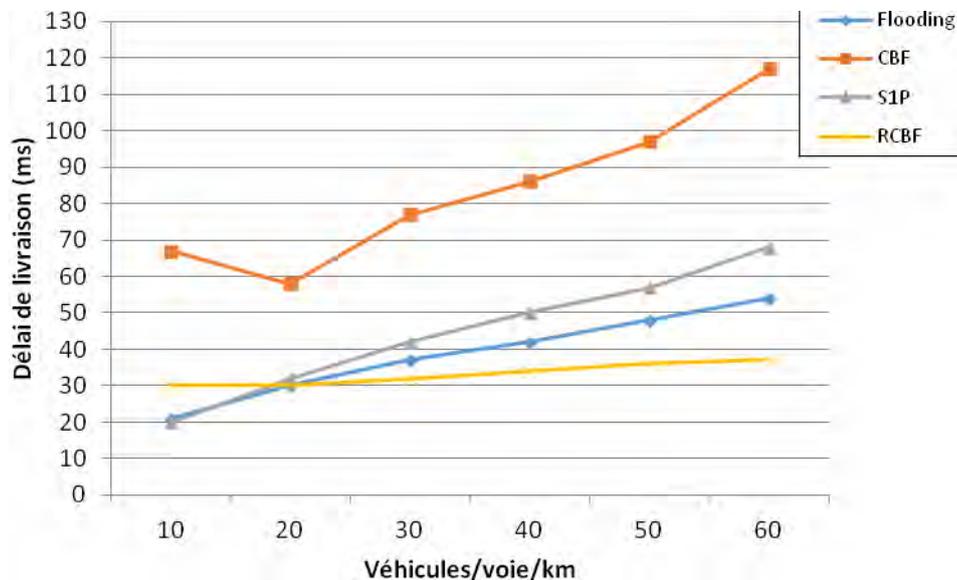


Figure 4-4 Délai de livraison en fonction du nombre de véhicules

Pour CBF, le délai est élevé car chaque nœud doit attendre un délai avant de rediffuser, ce qui augmente le délai de livraison du message, particulièrement quand la densité du réseau est faible. Dans ce dernier cas, il se peut qu'aucun relai potentiel n'existe à la limite de rayon de transmission (nœud avec un timer égal ou proche de zéro), donc il faut attendre qu'un des nœuds proches de l'émetteur (avec un timer plus grand) décrémente son timer, ce qui augmente le délai. Avec RCBF, le délai est réduit car les nœuds tirent leur valeur dans un intervalle et la valeur tirée n'est pas forcément proportionnelle de sa distance par rapport au dernier relai, comme dans le cas de CBF où elle peut être

inférieure.

4.5.3 Analyse du nombre de sauts

La figure 4-5 représente le nombre de sauts moyen parcourus par un message pour atteindre le dernier nœud dans la zone d'intérêt (à une distance de 3km). Comme illustré dans cette figure, CBF a le petit nombre de sauts. Le nombre de sauts de RCBF est élevé par rapport à CBF car comme nous l'avons expliqué dans la section précédente, les nœuds tirent leur valeur du timer dans un intervalle et le nœud sélectionné (avec la plus courte valeur du timer) n'est pas forcément le nœud le plus éloigné. Le nombre de sauts de S1P est élevé, car avec la redondance dans les transmissions (cf. figure 4-7) le nombre de collisions augmente et par conséquent les nœuds dans les segments proches de l'émetteur rediffusent, ce qui augmente le nombre de sauts.

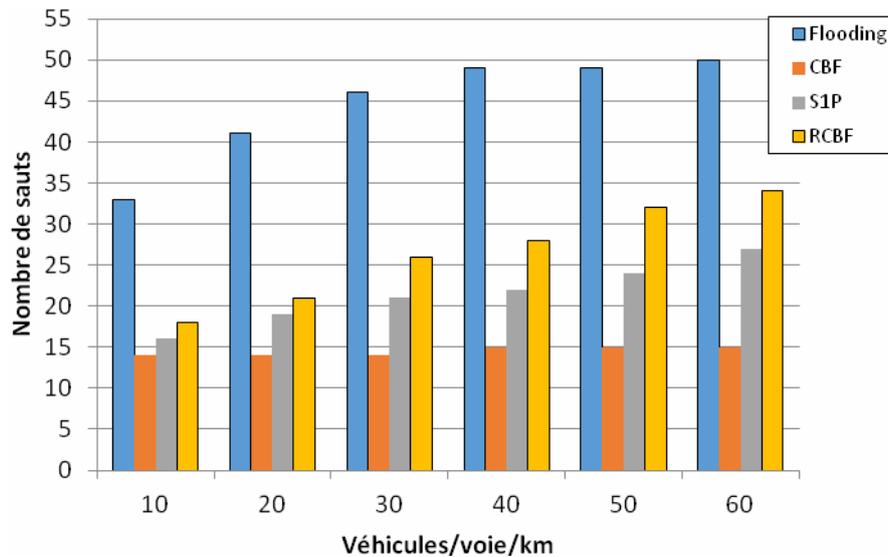


Figure 4-5 Nombre de sauts en fonction du nombre de véhicules

4.5.4 Analyse de la redondance

La figure 4-6 représente le taux de redondance en fonction de la densité de véhicules pour les quatre mécanismes. Comme illustré dans la figure 4-6 S1P n'offre pas une grande amélioration par rapport au Flooding, en termes de réduction du nombre de messages redondants, notamment quand la densité du réseau est élevée. La différence entre les deux

4. Analyse de performance des mécanismes de dissémination d'alertes

est légère, par exemple à 60 véhicules/voie/km le nombre de messages redondants pour SIP et Flooding est 9,3 et 9,86, respectivement. En effet, dans ce mécanisme la probabilité d'avoir plusieurs véhicules dans le même segment augmente avec l'augmentation dans la densité du réseau. Dans ce cas, plusieurs nœuds vont diffuser en même temps, ce qui augmente le nombre de messages redondants. En revanche, CBF et RCBF réduisent significativement le nombre de messages redondant, notamment CBF.

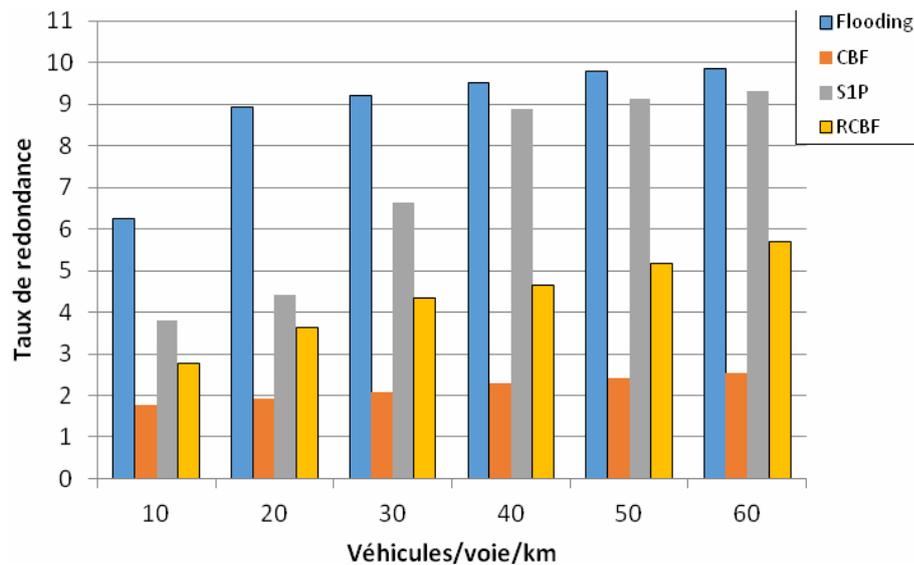


Figure 4-6 Taux de redondance moyen en fonction du nombre de véhicules

4.5.5 Analyse du nombre de rediffusions

La figure 4-7 illustre le résultat du nombre moyen de rediffusions des quatre mécanismes dans la zone d'intérêt (3 km). Le nombre de rediffusions augmente avec l'augmentation de la densité du réseau. Cependant, dans CBF et RCBF le nombre de rediffusions augmente légèrement. En effet, lorsque la densité du réseau augmente, la distance entre les nœuds diminue et plusieurs nœuds sont proches les uns des autres ; ce qui augmente la probabilité que deux ou plusieurs nœuds aient la même valeur du timer, dans le cas de CBF. Comme nous pouvons le voir sur la figure 4-7, le nombre de rediffusions de RCBF est légèrement supérieur à CBF. En effet, dans RCBF, comme la valeur du timer est aléatoire, il se peut que deux ou plusieurs nœuds tirent la même valeur, notamment quand le réseau est dense. Par conséquent le nœud sélectionné peut ne pas être le nœud le plus éloigné du dernier relai, ce qui augmente le nombre de sauts et par

4. Analyse de performance des mécanismes de dissémination d'alertes

conséquent le nombre de rediffusions. Par contre, le délai de livraison dans RCBF est meilleur (cf. figure 4-4).

Pour bien illustrer la réduction du nombre de rediffusions réalisées par S1P, CBF et RCBF par rapport au Flooding, nous présentons dans la figure 4-8 le taux de rediffusion de S1P, CBF et RCBF normalisé par rapport au nombre de rediffusions de Flooding.

Comme illustré dans la figure 4-8, S1P n'apporte pas une grande amélioration par rapport au Flooding, notamment à 50 et 60 véhicules/voie/km où le taux de rediffusions est de 62% et donc il est de 38% moins que le Flooding.

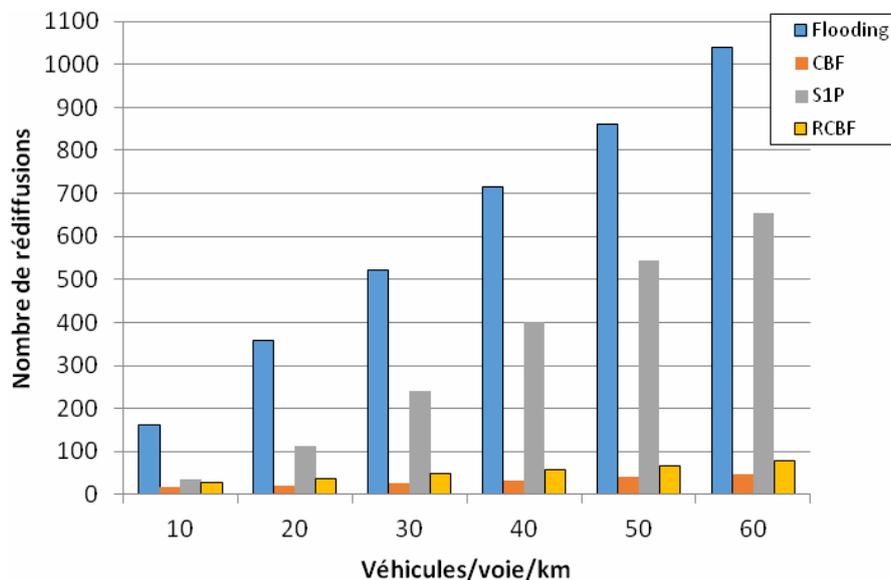


Figure 4-7 Nombre de rediffusions en fonction du nombre de véhicules

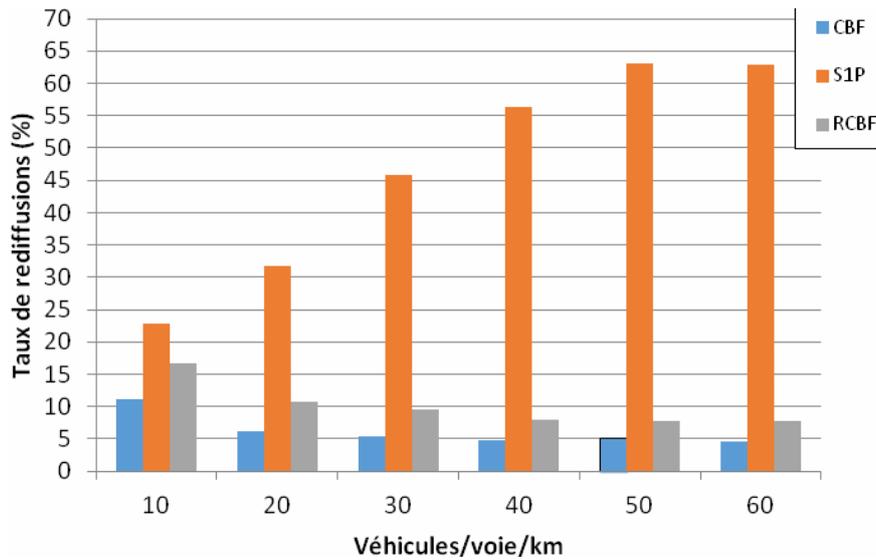


Figure 4-8 Taux de rediffusion normalisé en fonction du nombre de nœuds

4.6 Etudes de l'impact de la durée du slot sur la performance des mécanismes de dissémination

Les trois mécanismes que nous avons présentés dans ce chapitre, à savoir S1P, CBF et RCBF, utilisent, au niveau de la couche Réseau, une valeur de slots de temps pour déterminer les temps d'attente. En effet, chaque nœud tire un certain nombre de slots et attend avant de décider de rediffuser ou non le message. Durant ce temps si le nœud entend le message rediffusé par un de ses voisins, il annule la transmission. Comme ces mécanismes opèrent au niveau de la couche réseau, une fois le message passé à la couche MAC, il n'est plus possible d'annuler sa transmission, dans le cas où le nœud reçoit le même message rediffusé par un de ses voisins. Par conséquent, chacun des nœuds en contention doit s'assurer de l'arrivée de toutes les transmissions en cours avant de décider de rediffuser.

Par exemple, si on suppose que deux nœuds $n1$ et $n2$ tirent un slot et deux slots, respectivement. Après avoir attendu la durée d'un slot, le nœud $n1$ rediffuse le message (passe le message à la couche MAC), s'il n'entend pas le message rediffusé par un de ses voisins. Cependant, au niveau MAC, le message peut être retardé encore un certain temps surtout quand le réseau est dense. Si la durée d'un slot est inférieure à ce délai (délai MAC), le nœud $n2$ transmet son message après avoir attendu la durée de son deuxième slot

4. Analyse de performance des mécanismes de dissémination d'alertes

qui est inférieure au délai de transmission à un seul saut (délai MAC + délai de transmission + délai de propagation). On a donc une transmission redondante, ce qui augmente le nombre global de transmissions dans la zone d'intérêt et par conséquent le nombre de collisions.

La durée du slot de temps est un paramètre important qui peut avoir un impact sur la performance de ces mécanismes. Elle doit être supérieure au délai de transmission sur un seul saut qui est égale au délai MAC plus le temps de transmission et le délai de propagation. Ces deux derniers peuvent être négligés si on considère que l'on transmet des messages d'alerte (donc de petite taille) sur une courte distance (qui correspond au rayon de transmission).

Dans ce qui suit nous présentons les résultats qui montrent l'impact de la durée du slot sur la performance de S1P, CBF et RCBF. Nous utilisons le scénario précédent avec cinq valeurs du slot de temps : 0,013 ms (qui correspond au la durée du slot MAC du standard 802.11p), 0,13 ms ; 0,26 ms, 0,39 ms et 0,52 ms (des pas de dix slot MAC). Nous étudions l'effet de la variation de la durée du slot sur le délai de livraison, le nombre de sauts et le nombre de transmissions redondantes dans la zone d'intérêt.

4.6.1 Délai de livraison

Les figures 4-9, 4-10 et 4-11 illustrent l'impact de la durée du slot sur le délai de livraison des trois mécanismes CBF, RCBF et S1P, respectivement. Comme attendu, les trois mécanismes sont impactés par la durée du slot. Il est évident que le délai de livraison augmente avec l'augmentation de la durée du slot. Cependant, RCBF quand la durée du slot est égale à 0,013 ms le délai de livraison est légèrement élevé par rapport au cas 0,13 ms. En effet, avec un slot de petite durée le nœud rediffuse avant l'arrivée des transmissions en cours, ce qui augmente le nombre de transmissions (cf. figures 4-15, 4-16 et 4-17, section 4.6.3) et de collisions et par conséquent le nombre de sauts et le délai de livraison. Avec les autres valeurs de slot le nombre de sauts est réduit (cf. figures 4-12, 4-13 et 4-14, section suivante).

En plus, dans le cas de CBF et RCBF, quand la densité du réseau est faible (10 véhicules/voie/km) les valeurs du délai de livraison sont divergente et elles ont tendance à converger avec l'augmentation de la densité du réseau. A l'inverse, dans RCBF, les valeurs du délai divergent quand la densité du réseau augmente.

4. Analyse de performance des mécanismes de dissémination d'alertes

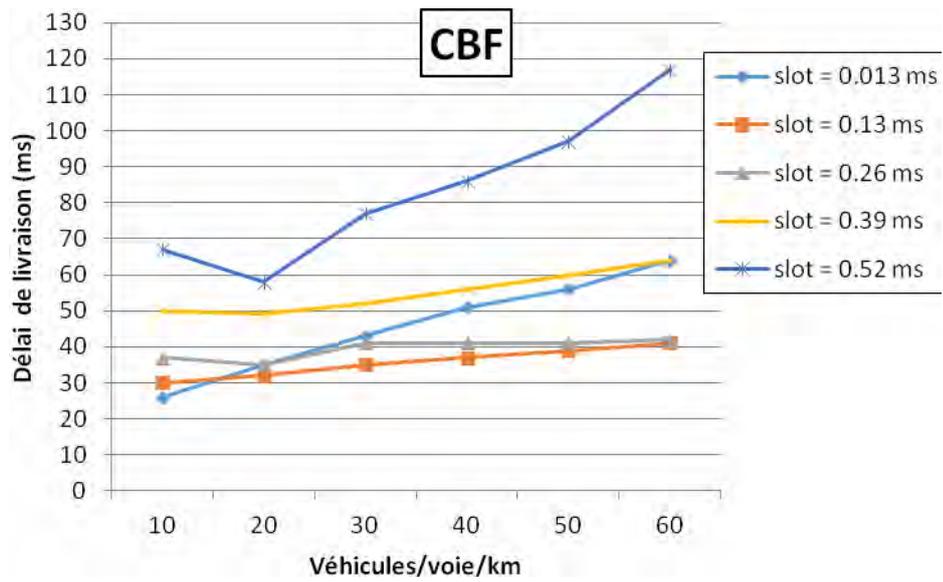


Figure 4-9 CBF-Délai de livraison en fonction du nombre de véhicules/voie/km, avec variation de la durée du slot

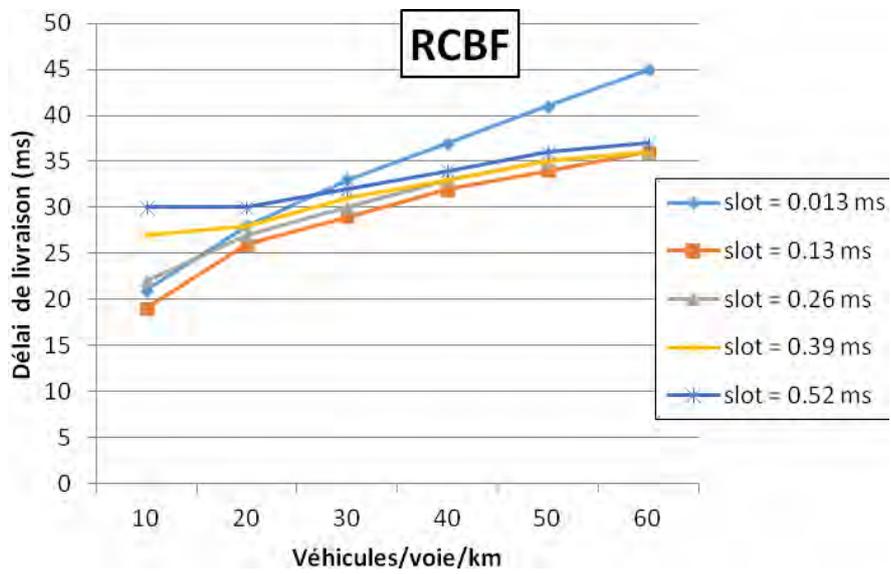


Figure 4-10 RCBF-Délai de livraison en fonction du nombre de véhicules/voie/km, avec variation de la durée du slot

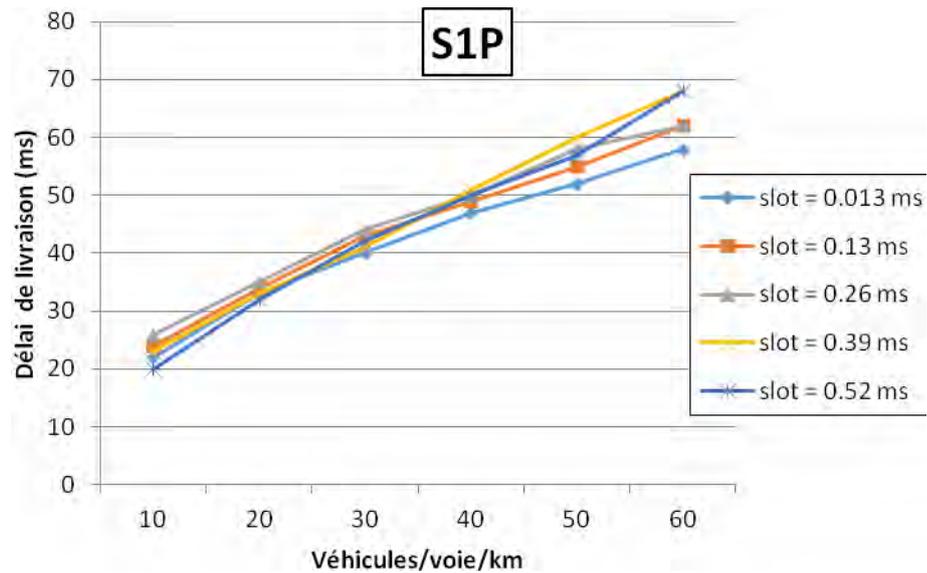


Figure 4-11 S1P-Délai de livraison en fonction du nombre de véhicules/voie/km, avec variation de la durée du slot

4.6.2 Nombre de Sauts

Comme le montre les figures 4-12, 4-13 et 4-14, le nombre de sauts des trois mécanismes augmente quand la durée du slot est très petite. Avec un slot de courte durée les nœuds en contention diffusent leurs messages avant de permettre aux transmissions qui sont en cours de se terminer, ce qui augmente le nombre de transmissions redondantes et par conséquent le nombre de collisions, et donc le message va parcourir plus de sauts pour couvrir toute la zone d'intérêt.

4. Analyse de performance des mécanismes de dissémination d'alertes

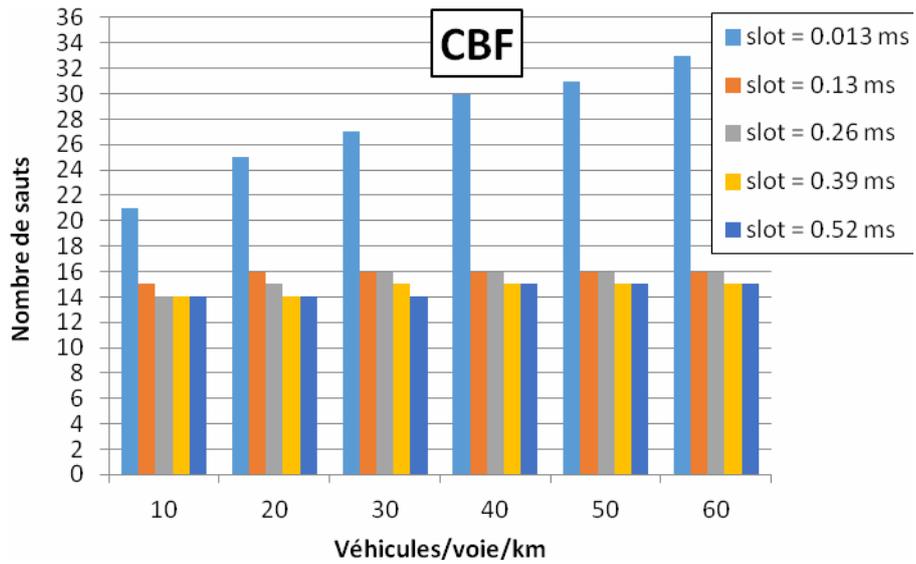


Figure 4-12 CBF-Nombre de sauts en fonction du nombre de véhicules/voie/km, avec variation de la durée du slot

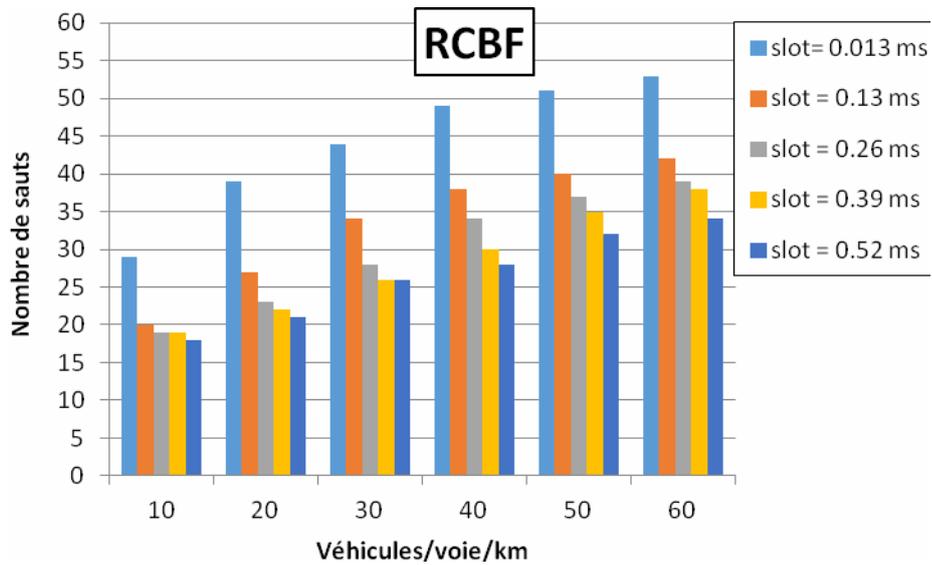


Figure 4-13 RCBF-Nombre de sauts en fonction du nombre de véhicules/voie/km, avec variation de la durée du slot

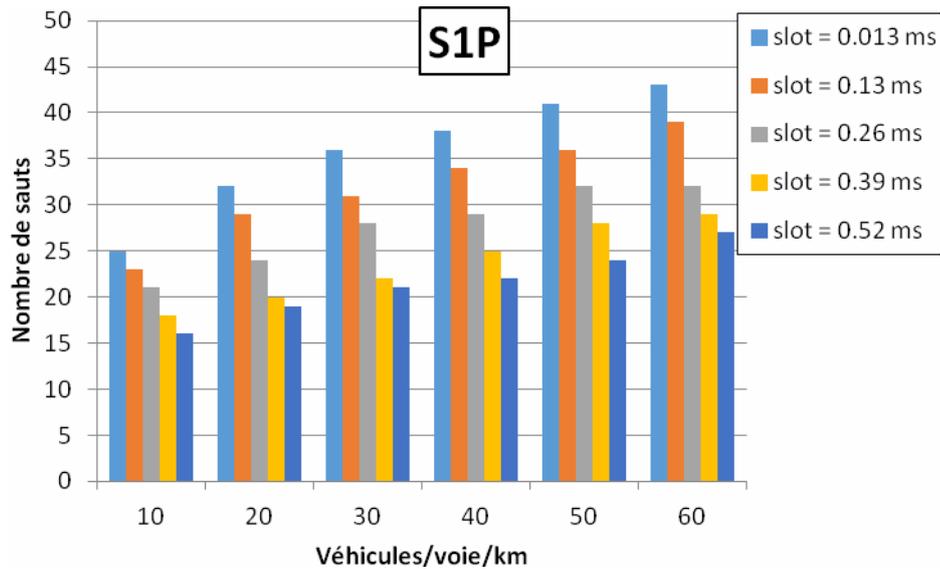


Figure 4-14 S1P-Nombre de sauts en fonction du nombre de véhicules/voie/km, avec variation de la durée du slot

4.6.3 Nombre de transmissions redondantes

Les figures 4-15, 4-16 et 4-17 illustrent le nombre de transmissions redondantes en fonction de la densité du réseau pour les trois mécanismes, en faisant varier la durée du slot. Comme attendu, le nombre de transmissions, dans les trois mécanismes, augmente quand la durée du slot est petite. En effet, comme nous l'avons expliqué au début de la section 4.6, si la durée du slot est trop petite, les nœuds vont transmettre avant la fin des transmissions en cours. Il est évident que lorsque le nombre de transmissions augmente le taux de redondance augmente (le nombre de messages dupliqués par un message source). Les figures 4-18, 4-19 et 4-20 illustrent le taux de redondance des trois mécanismes.

4. Analyse de performance des mécanismes de dissémination d'alertes

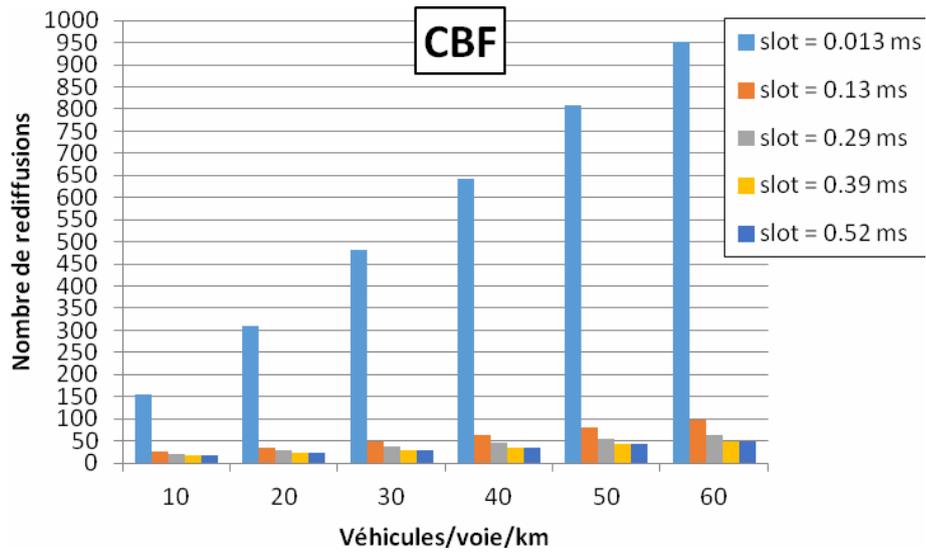


Figure 4-15 CBF-Nombre de rediffusions en fonction du nombre de véhicules/voie/km, avec variation de la durée du slot

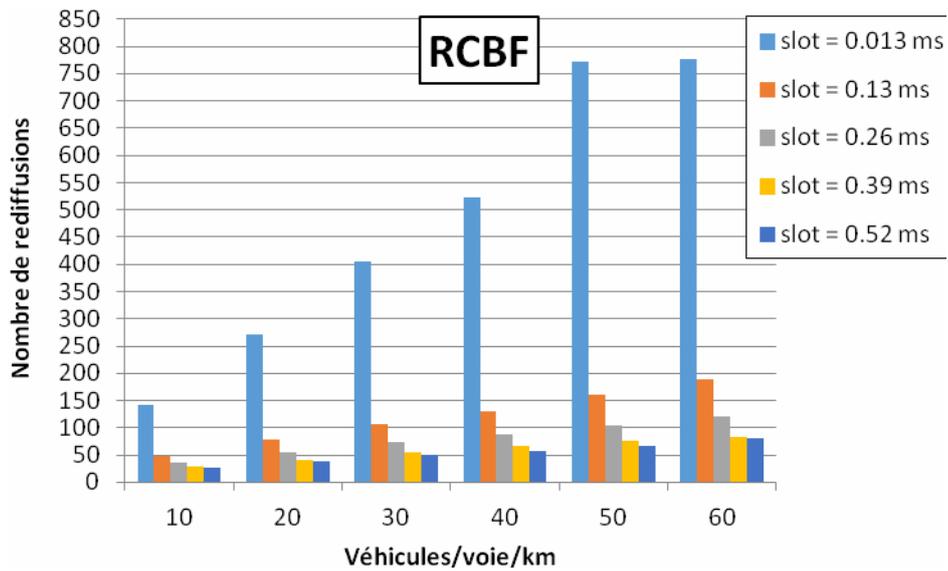


Figure 4-16 RCBF-Nombre de rediffusions en fonction du nombre de véhicules/voie/km, avec variation de la durée du slot

4. Analyse de performance des mécanismes de dissémination d'alertes

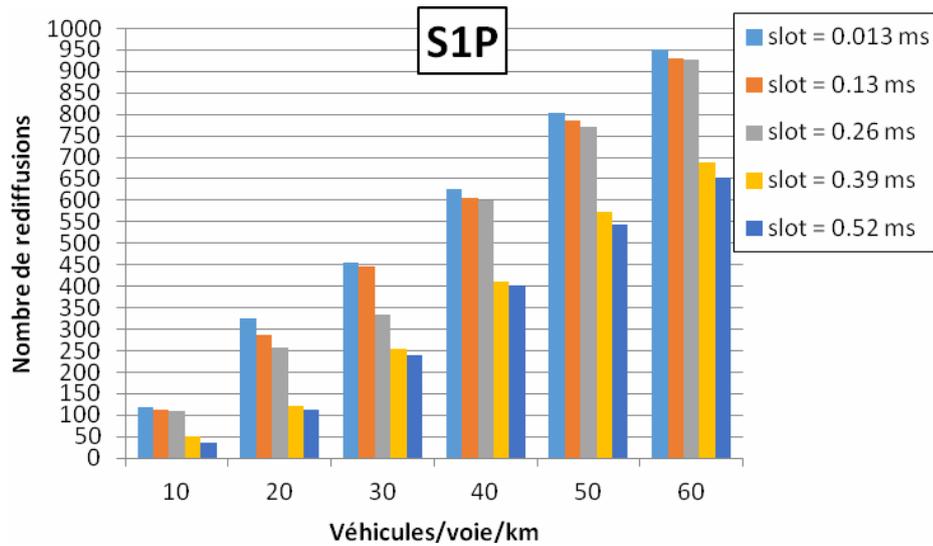


Figure 4-17 S1P-Nombre de rediffusions en fonction du nombre de véhicules/voie/km, avec variation de la durée du slot

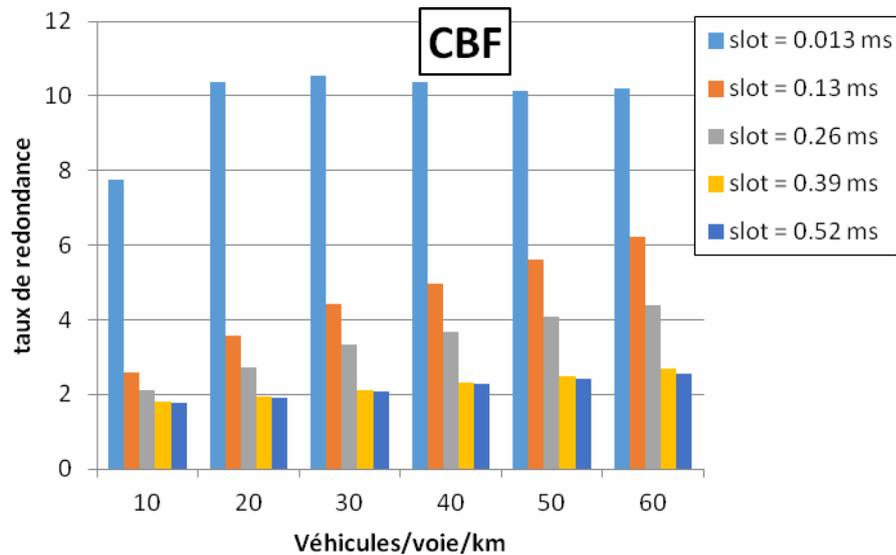


Figure 4-18 CBF- taux de redondance en fonction du nombre de véhicules/voie/km, avec variation de la durée du slot

4. Analyse de performance des mécanismes de dissémination d'alertes

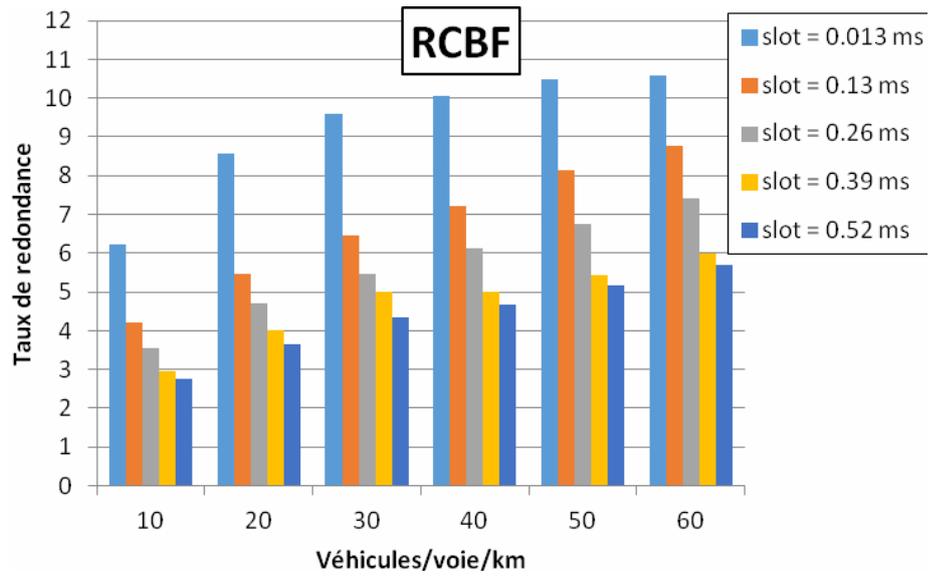


Figure 4-19 RCBF- taux de redondance en fonction du nombre de véhicules/voie/km, avec variation de la durée du slot

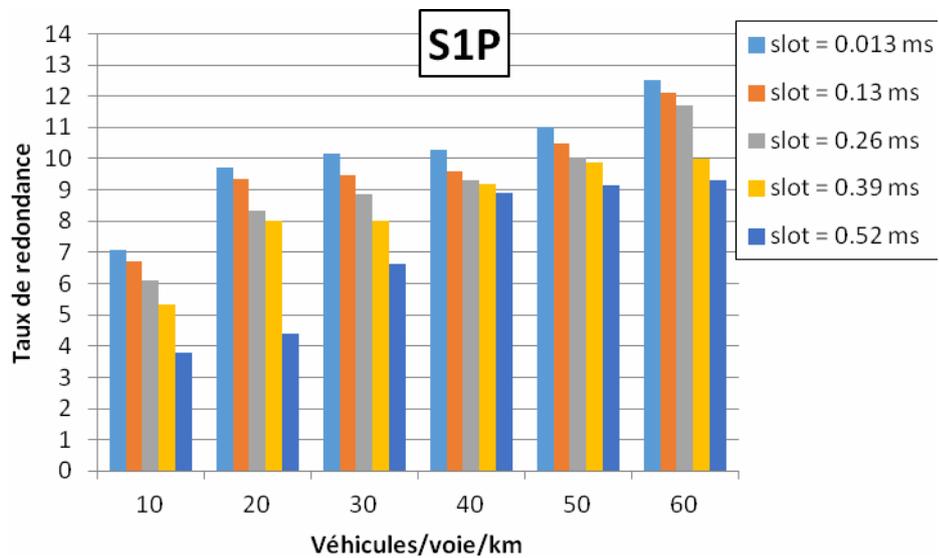


Figure 4-20 S1P- taux de redondance en fonction du nombre de véhicules/voie/km, avec variation de la durée du slot

4.7 Conclusion

Dans ce chapitre nous avons étudié les performances de trois mécanismes de dissémination (en plus du Flooding). Les résultats de cette étude montrent que les mécanismes à base de contention (CBF et RCBF) offrent de meilleures performances par rapport au mécanisme S1P. Le délai de livraison du mécanisme CBF est élevé par rapport à celui du mécanisme RCBF. Ce dernier offre un délai de livraison faible mais avec un peu plus de redondance et un nombre de sauts un peu plus élevé. Cependant, le délai de livraison de CBF reste acceptable pour la plus part des applications de sécurité routière (117 ms à 60 véhicules/voie/km avec un slot de 0.52 ms).

Notre étude dans le chapitre précédent et ce chapitre, nous a sensibilisés sur l'importance de l'intégration de la densité dans les mécanismes de dissémination. Nous pensons, que les performances du RCBF peuvent être améliorées s'il intègre un mécanisme lui permettant de s'adapter à la densité du réseau.

Le chapitre suivant présente notre contribution en termes de protocole de dissémination de l'information de sécurité.

Chapitre 5

Un protocole adaptatif pour la dissémination d'alertes

5.1 Introduction

Dans ce chapitre, nous présentons notre proposition d'un protocole de dissémination de l'information de sécurité dans un réseau de véhicules. L'application considérée dans ce chapitre est : *l'application de signalisation du danger sur la route* « *Road Hazard Signaling (RHS)* ». Comme nous l'avons évoqué dans le chapitre 2, cette application s'appuie principalement sur la diffusion multi-saut pour délivrer les messages d'alerte à tous les nœuds présents dans la *zone d'intérêt*. Notre objectif est de répondre aux limites et aux problèmes que nous avons identifiés lors de notre étude des principaux protocoles de dissémination d'information dans les réseaux véhiculaires. Ces limites seront détaillées dans la section suivante (section 5.2).

Notre protocole permet d'éviter le problème de tempête de diffusion en réduisant significativement le nombre de nœuds relais dans la *zone d'intérêt*. Le délai de

dissémination de message d'alerte est aussi réduit notamment, quand la densité du réseau est faible. La section 5.3 décrit en détail notre protocole. Dans la section 5.4, nous décrivons l'environnement de simulation que nous avons utilisé pour évaluer les performances de notre protocole, puis nous présentons les résultats de cette évaluation dans la section 5.4.4.

5.2 Motivation

Pour réduire le délai de livraison de message, la plupart des protocoles proposés utilisent la distance entre l'émetteur/dernier relai et le récepteur pour sélectionner le nœud permettant de progresser au maximum dans la direction de dissémination. Généralement, cette distance est utilisée par le nœud, pour définir son temps d'attente avant de décider de rediffuser ou non le message ou pour définir sa probabilité de rediffusion.

Dans les premiers protocoles qui se basent sur cette approche [43, 44, 45], chaque nœud qui reçoit le message diffusé, attend un délai qui est inversement proportionnel de sa distance par rapport à l'émetteur avant de décider de rediffuser ou non le message. Durant ce temps d'attente, si le nœud reçoit le même message rediffusé par un autre nœud, il abandonne. Sinon, il rediffuse le message dès que son temps d'attente expire.

Dans les protocoles que nous venons de décrire, si deux ou plusieurs nœuds se trouvent à la même distance du dernier, ces nœuds vont rediffuser en même temps (avoir le même temps d'attente ou avoir la même probabilité de rediffusion), ce qui augmente la redondance et les collisions de messages notamment quand le réseau est dense.

Une nouvelle approche consiste à définir un intervalle de temps⁸ (à savoir une fenêtre de contention) à partir duquel les nœuds tirent leur temps d'attente (timer) avant de décider de rediffuser ou non le message reçu. La borne inférieure et la borne supérieure de cet intervalle de temps dépendent de la distance entre le dernier relai et le récepteur. Plusieurs paramètres (densité, état du canal radio, etc.) peuvent être considérés lors du calcul de cet intervalle.

Dans *Smart Broadcast* [46] par exemple, la portée de transmission dans la direction de dissémination est divisée en plusieurs secteurs de taille fixe. Un intervalle de temps est affecté à chaque secteur. Les intervalles sont dimensionnés de telle sorte que les nœuds

⁸ Nous utilisons « intervalle de temps » au lieu de fenêtre de contention, mais à ne pas confondre avec la fenêtre de contention de la couche MAC

5. Un protocole adaptatif pour la dissémination d'alertes

appartenant au secteur le plus éloigné du dernier relai tirent la plus petite valeur du timer.

Bien que ces protocoles réduisent significativement le nombre de nœuds relais dans la zone de dissémination, ils entraînent un délai important quand la densité du réseau est faible. En plus, si plusieurs nœuds sont présents dans le même secteur, comme dans le cas de *slotted 1-persistence*, ces nœuds vont tous avoir le même temps d'attente et ils vont rediffuser le message en même temps. Dans le cas de *Smart Broadcast*, ces nœuds vont avoir le même intervalle de temps et la probabilité de tirer la même valeur augmente avec l'augmentation de la densité du réseau.

Les mécanismes que nous venons de présenter souffrent toujours de problèmes de collisions quand le réseau est dense et une latence élevée quand la densité du réseau est faible (cf. résultats de simulations chapitre 4). Leur limitation c'est qu'ils ne considèrent pas la densité du réseau dans le calcul de l'intervalle à partir duquel ils tirent leur temps d'attente. L'étude que nous avons menée dans le chapitre précédent nous a sensibilisé sur l'importance de la considération de la densité dans le mécanisme de sélection du prochain nœud relai, particulièrement dans le calcul de temps d'attente.

Par exemple, dans *Bi-Zone* [47], chaque nœud tire un timer dans un intervalle $[T_{lower}, T_{upper}]$ avant de décider de rediffuser ou non le message reçu. La valeur de T_{lower} des nœuds dont la distance est supérieure à un seuil prédéfini est fixée à zéro et la valeur de leur T_{upper} est calculée comme suit :

$$T_{upper} = T_{max} \times \left(1 - \frac{Dist}{R}\right) \quad (5.1)$$

où R est le rayon de transmission, T_{max} est le temps d'attente maximum et $Dist$ est la distance par rapport au dernier relai.

Pour les nœuds qui sont proches de l'émetteur (leur distance par rapport au dernier relai est inférieure au seuil prédéfini), la valeur de T_{upper} est fixée au temps d'attente maximum T_{max} et la valeur de leur T_{lower} est calculée comme suit :

$$T_{lower} = T_{max} \times \left(1 - \frac{Threshold}{R}\right) \quad (5.2)$$

Prenons le cas où plusieurs nœuds sont situés à la limite de la portée de transmission

5. Un protocole adaptatif pour la dissémination d'alertes

comme illustré dans la figure 5-1. Dans ce cas : $Dist/R = 1$, puis $T_{upper} = 0$. Par conséquent, tous ces nœuds auront la même valeur de T_{upper} , qui est 0.

Dans ce cas, ces nœuds rediffusent le message en même temps sans attendre. Cela conduit à une redondance élevée des messages, une charge élevée du canal, une grande contention et donc un gaspillage de la bande passante. Ce qui est particulièrement dommageable quand la densité du réseau est élevée.

Avec la formule (5.1), même si certains nœuds ne sont pas exactement à la même distance du dernier relai, leurs intervalles de temps sont presque identiques. Dans ce cas, l'intervalle de temps de chaque nœud chevauche largement avec ceux de ses voisins. Cela augmente la probabilité que deux ou plusieurs nœuds tirent la même valeur du timer, ce qui encore est très probable quand le réseau est dense.

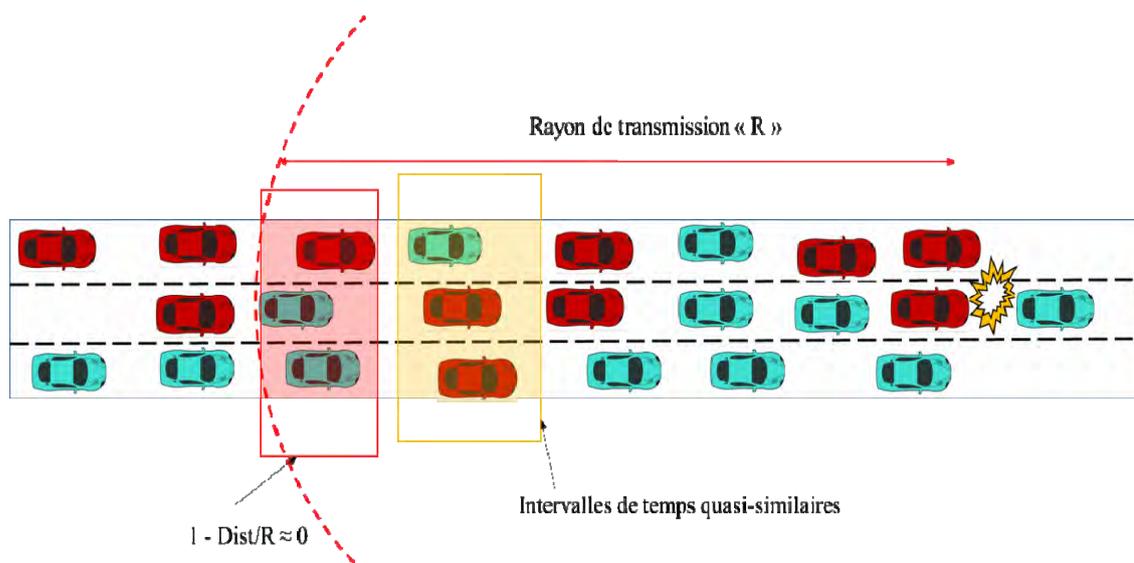


Figure 5-1 Exemple d'illustration

Bien que dans [48] les auteurs définissent un nouveau mécanisme de sélection du prochain nœud relai avec une fonction différente pour le calcul de l'intervalle de temps, le même problème peut se produire. En fait, dans [48] le temps d'attente est calculé sur la base d'une fenêtre de contention (CW) qui varie entre un minimum (CW_{min}) et un maximum (CW_{max}), en fonction de la distance par rapport au dernier relai et la portée de transmission estimée, comme indiqué dans l'équation (5.3) :

$$CW = \left[\left(\frac{EstTrans - Dist}{EstTrans} \times (CW_{max} - CW_{min}) \right) + CW_{min} \right] \quad (5.3)$$

où *EstTrans* est le rayon de transmission estimée (un mécanisme permettant l'estimation de la portée de transmission de chaque nœud a été aussi proposé par les auteurs) et *Dist* est la distance par rapport au dernier relai.

En plus, ces mécanismes favorisent les nœuds qui sont à la limite de la portée de transmission. Il est bien connu que la probabilité de réception est faible dans cette zone [35]. Si le nœud sélectionné ne reçoit pas correctement le message diffusé (à cause de l'évanouissement du signal ou de l'ombrage) ou s'il n'existe pas, comme dans le cas d'un réseau clairsemé, les nœuds qui sont proches du nœud relai sont pénalisés et attendent inutilement.

Un exemple d'un mécanisme qui intègre la densité dans le calcul de l'intervalle de temps est FR-EDM [49]. En fait, comme *slotted 1-persistence* et *Smart Broadcast*, ce protocole se base aussi sur la division de la portée de transmission dans la direction de dissémination en plusieurs secteurs. Cependant, contrairement aux autres protocoles, dans FR-EDM, la taille du secteur n'est pas fixe ; elle dépend de la densité du réseau. Quand le réseau est dense la taille du secteur est réduite pour éviter d'avoir plusieurs véhicules dans le même secteur et qui peuvent rediffuser en même temps. A l'inverse, quand le réseau n'est pas dense, le secteur est élargi pour réduire le délai d'attente des nœuds relai potentiels. Cependant, ce mécanisme suppose l'existence d'un système centralisé qui diffuse l'état du trafic routier (à savoir la densité du réseau) à travers les RSU, ce qui est coûteux et difficile à avoir, notamment dans les premières phases de déploiement des VANETs et les environnements ruraux. Dans notre protocole, c'est la taille de l'intervalle de temps qui dépend de la densité du réseau.

Dans P-IVG [50], chaque nœud qui reçoit un nouveau message tire une valeur dans l'intervalle [0, 1] avant de déclencher son timer. Ce dernier est inversement proportionnel à sa distance par rapport au dernier relai. Si la valeur tirée est inférieure à l'inverse de la densité, le nœud déclenche son timer et rediffuse le message dès que ce dernier expire.

5. Un protocole adaptatif pour la dissémination d'alertes

Sinon, il annule le processus et ne rediffuse pas le message. Cela signifie que le nombre de nœuds autorisés à démarrer leur timer dépend de la densité du réseau. Plus le réseau est dense, plus faible est le nombre de nœuds autorisés à rediffuser le message. Bien que ce protocole traite le problème de tempête de diffusion, il ne traite pas le problème de latence élevée quand la densité du réseau est faible.

5.3 Protocole proposé

5.3.1 Scénario et hypothèses

Dans notre étude, nous allons nous concentrer sur le contexte autoroutier. Comme illustré dans la figure 5-2, nous représentons un tronçon d'une autoroute avec trois voies dans la même direction. Nous supposons que tous les véhicules sont équipés d'un récepteur GPS, par conséquent, chaque véhicule est en mesure d'obtenir sa propre position. Tous les véhicules sont équipés de dispositif WAVE/DSRC leur permettant de communiquer, directement ou à travers des communications multi-saut.

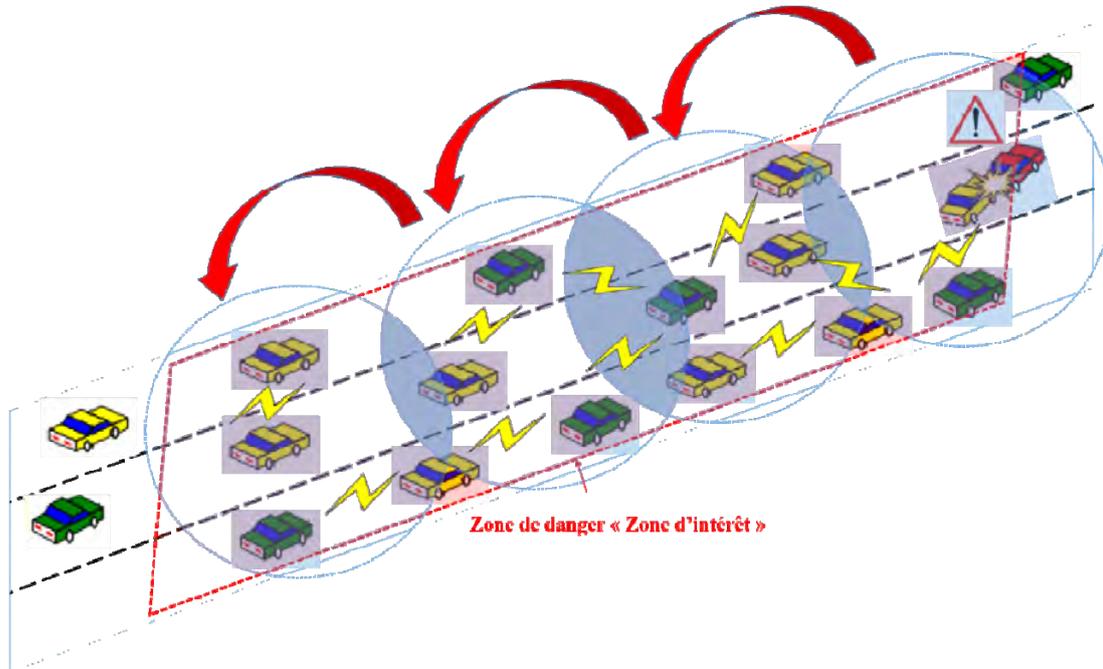


Figure 5-2 Scénario

5. Un protocole adaptatif pour la dissémination d'alertes

Nous considérons un réseau de véhicules sans infrastructure (des communications de type V2V). À un instant donné, un message d'alerte est généré par un véhicule en tête du peloton. Ce message doit être relayé pour couvrir une zone particulière derrière le véhicule source du message, c'est la « *zone d'intérêt* ».

Nous définissons la densité locale d'un nœud par :

$$\text{Densité} = N / N_{max} \quad (5.4)$$

où N est le nombre de voisins sur un seul saut et N_{max} est le maximum de voisins à un saut dans un scénario de trafic très dense (dans un embouteillage par exemple).

5.3.2 Description du protocole

5.3.2.1 Description du comportement des nœuds

- **Messages périodiques**

Chaque nœud diffuse périodiquement un « *Cooperative Awareness Message (CAM)* » qui contient sa position, sa direction, sa vitesse, etc. Les CAMs sont utilisés par la plupart des applications de sécurité et ils sont considérés comme un trafic de fond. Dans notre cas, les CAMs ne sont pas nécessairement échangés à une fréquence élevée, ils sont utilisés par les nœuds pour avoir une estimation instantanée du nombre de leurs voisins.

Chaque nœud maintient une table dans laquelle il stocke des informations sur les nœuds qui sont dans sa portée de transmission.

- **Message d'alerte**

Quand un accident se produit ou une situation dangereuse est détectée, un « *Decentralized Environment Notification Message (DENM)* » est généré par le véhicule concerné. Le DENM doit être relayé jusqu'à ce qu'il atteigne tous les véhicules présents dans la *zone d'intérêt*. Ce message comprend l'emplacement de l'événement, la direction de diffusion, la taille de la *zone d'intérêt*, etc.

Chaque récepteur du DENM vérifie s'il s'agit d'un nouveau message et s'il est dans la direction de dissémination du message. Ceci est basé sur les informations

5. Un protocole adaptatif pour la dissémination d'alertes

contenues dans le DENM. Si les deux conditions sont remplies, le récepteur déclenche son timer. Ce dernier est tiré dans un intervalle de temps calculé par notre mécanisme adaptatif (voir section suivante).

Lorsque le timer expire, le nœud ajoute ses coordonnées dans le message et le rediffuse. Si un nœud reçoit le même message au cours de sa période d'attente, il sort de la phase de contention et supprime le message.

Il est à noter que le récepteur du message d'alerte utilise ses coordonnées GPS courantes et les coordonnées du nœud source (à savoir l'initiateur du DENM) incluses dans le DENM pour déterminer s'il se trouve dans la zone d'intérêt ou non.

5.3.2.2 Description du mécanisme de calcul de l'intervalle de temps

Pour réduire le nombre de nœuds relais et le délai de livraison, notre mécanisme considère à la fois la distance et la densité du réseau dans le calcul du temps qu'attend chaque nœud avant de décider de rediffuser le message reçu. Par conséquent, notre protocole repose sur deux fonctions qui calculent les valeurs des limites de l'intervalle de temps $[T_{inf}, T_{sup}]$ à partir duquel ce temps est tiré.

Notre mécanisme repose sur le critère de distance pour réduire le nombre de sauts et ainsi, le délai de dissémination du message dans la *zone d'intérêt*. Il essaie de sélectionner le nœud permettant d'avancer au maximum dans la direction de dissémination. Comme illustré dans la Fig.5-3, la portée de transmission de l'émetteur/dernier relai dans la direction de dissémination est divisée en plusieurs segments d'une largeur fixe.

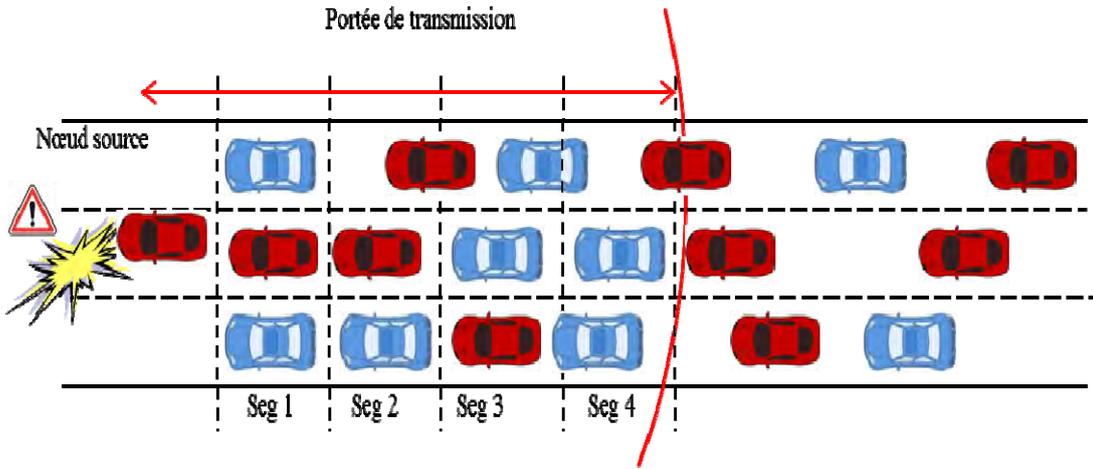


Figure 5-3 Exemple avec quatre segments de zone d'attente

À chaque segment est assigné un intervalle de temps à partir duquel les nœuds situés dans ce segment tirent leur temps d'attente avant de décider de rediffuser ou non le message. Les limites T_{sup} et T_{inf} de l'intervalle de temps sont données dans (5.5) et (5.6), respectivement. La description détaillée de ces fonctions sera discutée dans la section suivante.

$$T_{sup} = \max\{T_{max} \times (1 - \Delta_{dist}) \times Densité, T_{min} + CW_{long}\} \quad (5.5)$$

$$T_{inf} = T_{sup} - CW_{long} \quad (5.6)$$

où T_{min} et T_{max} sont le minimum et le maximum temps d'attente, respectivement ; $Dist$ est la distance par rapport au dernier relai, $Densité$ est la densité locale perçue par le nœud considéré, R est le rayon de transmission, $LongSeg$ est la longueur du segment, $NbrSeg$ est le nombre de segments; CW_{long} et Δ_{dist} sont donnés dans (5.7) et (5.9) respectivement.

$$CW_{long} = (T_{max} - T_{min}) \times \frac{Densité}{NbrSeg} \quad (5.7)$$

$$NbrSeg = \frac{R}{LongSeg} \quad (5.8)$$

$$\Delta_{dist} = \left\lfloor \frac{Dist}{LongSeg} \right\rfloor \times \frac{1}{NbrSeg} \quad (5.9)$$

5.3.2.3 Description des fonctions

L'idée de base est d'avoir des intervalles de temps dont les deux bornes coulisent en fonction de la distance du nœud par rapport au dernier relai et de la densité du réseau. En effet, nous visons à étendre la largeur de l'intervalle de temps quand la densité du réseau est élevée pour réduire la probabilité que deux ou plusieurs nœuds tirent la même valeur du timer. Nous essayons de trouver un compromis entre le délai de livraison et la redondance des messages. Contrairement à FR-EDM [49] où la taille des segments (secteurs) est ajustée en fonction de la densité du réseau, dans notre protocole c'est l'intervalle de temps qui est ajusté en fonction de la densité du réseau.

- **La fonction T_{inf}**

Contrairement aux autres mécanismes où la valeur de T_{inf} est fixe, dans notre mécanisme de la valeur de T_{inf} dépend de la distance du nœud par rapport au dernier relai et aussi de la densité du réseau. Lorsque la densité du réseau est élevée, les nœuds proches du dernier relai sont pénalisés parce que leur T_{inf} ne démarre pas de zéro, ce qui les empêche de commencer la rediffusion et donne plus de chance aux nœuds qui sont loin du dernier relai pour commencer la rediffusion. Cela réduit le chevauchement des intervalles de temps des nœuds intérieurs (les nœuds proches du dernier relai) avec ceux situés à la limite de la portée de transmission.

Dans le cas d'une faible densité du réseau, la valeur de T_{inf} diminue. Cela réduit le temps d'attente du nœud parce qu'en même temps la valeur de T_{sup} et la largeur d'intervalle sont réduites. En d'autres termes, lorsque la densité du réseau est faible, notre protocole évite de bloquer inutilement les nœuds à proximité du dernier relai en attendant un nœud hypothétiques plus éloignés pour rediffuser.

- **La fonction T_{sup}**

La valeur de T_{sup} dépend de la distance du nœud par rapport au dernier relai et de la densité du réseau. La fonction de T_{sup} permet d'étendre l'intervalle en fonction de la densité du réseau. Lorsque la densité du réseau est élevée, contrairement aux mécanismes existants, dans notre mécanisme, les nœuds situés à la limite de

la portée de transmission n'ont pas T_{sup} égale/proche de zéro. Dans ce cas, l'intervalle de temps de notre protocole est plus large, ce qui réduit la probabilité que deux ou plusieurs nœuds situés à la même distance du dernier relai tirent la même valeur du timer. Par conséquent, le nombre de nœuds relais et les messages redondants sont réduits, en particulier quand la densité du réseau est élevée. La figure 5-4 présente un exemple d'évolution de la largeur de l'intervalle en fonction de la densité avec un $T_{max} = 1024$ slots. Dans (5.9), nous prenons la partie entière de la division de la distance par le nombre de segments ($Dist/LongSeg$) pour regrouper les nœuds très proches les uns des autres dans le même segment. Le $LongSeg$ peut être ajustée pour répondre aux besoins des exigences spécifiques de l'application. Une distance correspond à la longueur d'un véhicule peut être préconisée.

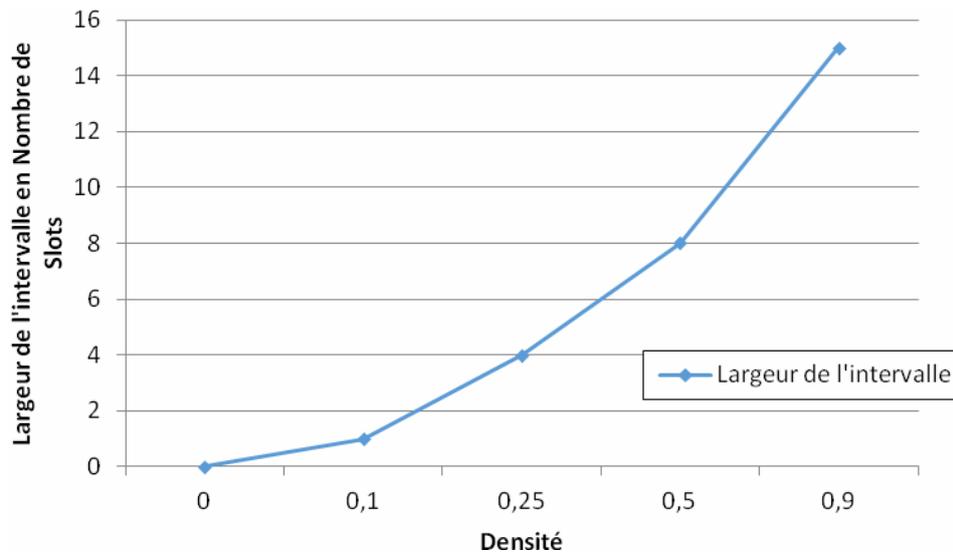


Figure 5-4 Largeur de l'intervalle en fonction de la densité

- Le paramètre CW_{long}

CW_{long} représente la largeur de l'intervalle duquel est tiré aléatoirement le temps d'attente. Ce paramètre dépend à la fois de la densité du réseau et du nombre de segments créés. Lorsque le réseau est clairsemé, CW_{long} diminue pour resserrer l'intervalle. Par conséquent, le temps d'attente des nœuds relais potentiels est

5. Un protocole adaptatif pour la dissémination d'alertes

réduit. Lorsque la densité du réseau est élevée, CW_{long} est augmenté et l'intervalle est élargi afin de réduire la probabilité que deux ou plusieurs nœuds choisissent la même valeur du timer. Il convient de noter que les équations (5.5) et (5.6) conduisent à un intervalle de temps d'une largeur fixe pour une densité donnée du réseau.

- Les valeurs de T_{min} et T_{max}

Les valeurs de T_{min} et T_{max} sont fixées selon les exigences de l'application considérée. La valeur de T_{min} peut être fixée à une valeur choisie en fonction des besoins spécifiques dans l'intervalle $[0, T_{max}]$.

Dans les figures 5-5, 5-6 et 5-7, nous présentons trois exemples de l'évolution de l'intervalle de temps en fonction de la densité (0.1, 0.5 et 0.9).

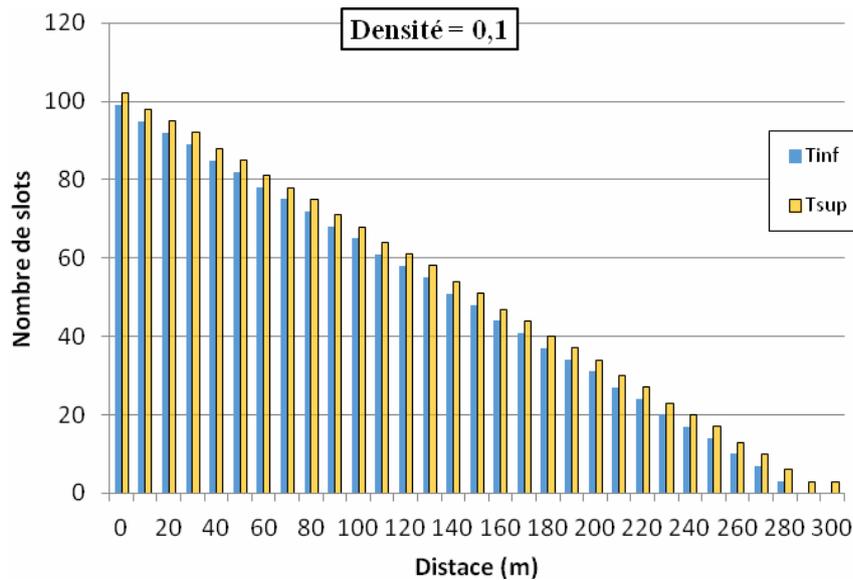


Figure 5-5 Valeurs de T_{inf} et T_{sup} en fonction de la distance (Densité = 0.1)

5. Un protocole adaptatif pour la dissémination d'alertes

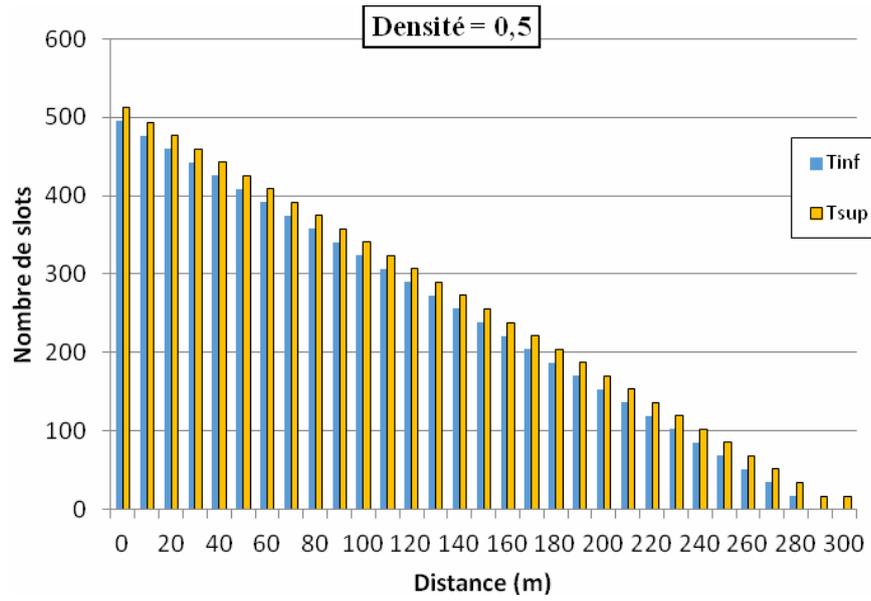


Figure 5-6 Valeurs de T_{inf} et T_{sup} en fonction de la distance (Densité = 0.5)

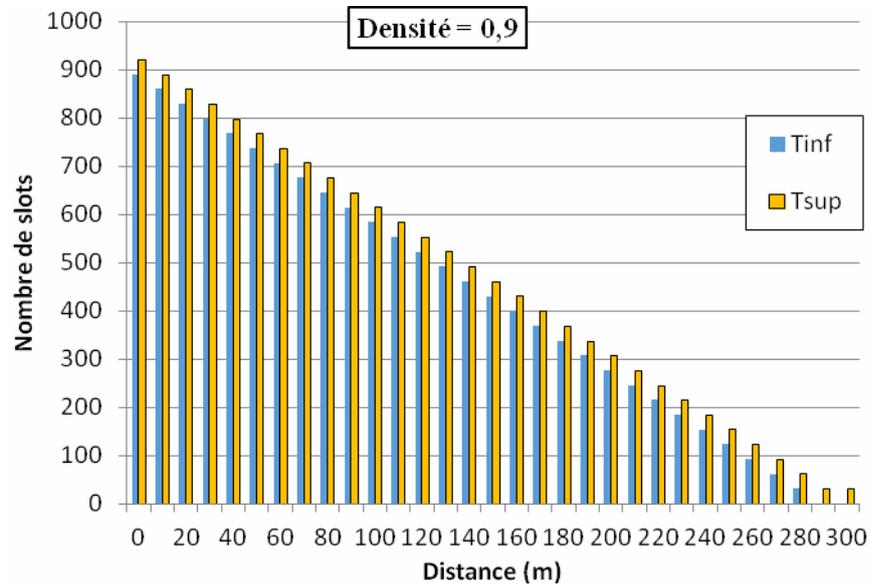


Figure 5-7 Valeurs de T_{inf} et T_{sup} en fonction de la distance (Densité = 0.9)

5.4 Evaluation de performances

Dans cette section, nous évaluons les performances de notre protocole. Nous comparons ses performances avec celles d'un protocole similaire qui utilise le mécanisme de dissémination à base de distance. Cependant, ce protocole n'intègre pas la densité du réseau dans le calcul de l'intervalle de temps. Nous appelons ce protocole « *Random Distance-Based Scheme (RDS)* ». Ce dernier a été inspiré des mécanismes présentés dans [47] et [48]. La fonction qui calcule la valeur de T_{sup} de RDS est donnée dans (5.10) et la valeur de T_{inf} est fixée à zéro.

$$T = T_{max} \times \frac{D}{R} \quad (5.10)$$

5.4.1 Plateformes de simulation

- *Simulateur Réseau*

Dans notre évaluation, nous nous basons sur le simulateur réseau NS2.34 [33] dans lequel nous avons implémenté notre protocole. Notre choix se justifie par la large diffusion de ce simulateur dans la communauté scientifique et par la possibilité de simuler des communications qui se basent sur le standard IEEE 802.11p de l'architecture WAVE. En effet, dans notre simulation, nous avons modifié les paramètres des couches MAC et physique implémentés dans NS-2 (le module 802.11 Ext de ns2.34) pour les rendre similaire aux paramètres du standards IEEE 802.11p. Nous avons aussi désactivé les mécanismes ACK/RTS/CTS.

- *Simulateur de mobilité*

Nous utilisons le simulateur « *Simulation of Urban Mobility (SUMO)* » [51] pour générer les modèles de mobilité (fichiers trace) qui seront par la suite utilisés par le simulateur NS2. SUMO est un simulateur open source développé par le « *German Aerospace Center(DLR)* ». Il permet la modélisation du trafic routier tel que les véhicules, le transport public et même les piétons. SUMO permet de simuler la mobilité des véhicules au niveau microscopique. Ce dernier représente à la fois les entités et les interactions entre elles avec un haut niveau de détails. Le comportement d'un véhicule dépend de l'état de ces voisins et même des caractéristiques du

conducteur.

5.4.2 Paramètres de simulation

Nous simulons une section de 4 km d'une autoroute avec trois voies dans la même direction. La longueur de la zone d'intérêt est de 2 km et la densité des véhicules varie de 20 véhicules/km à 120 véhicules/km. Nous utilisons six traces de mobilité en faisant varier le nombre de véhicules et la vitesse maximale des véhicules pour couvrir trois scénarios de vitesse sur les routes :

- **Scénario vitesse élevée** : représenté par les deux scénarios de densité : 20 véhicules/km et 40 véhicules/km. Les véhicules de ce scénario ont une vitesse comprise dans l'intervalle [100 km/h, 120 km/h].
- **Scénario vitesse moyenne** : représenté par les deux scénarios de densité : 60 véhicules/km et 80 véhicules/km. Les véhicules de ce scénario ont une vitesse comprise dans l'intervalle [80 km/h, 100 km/h]
- **Scénario vitesse faible** : représenté par les deux scénarios de densité : 100 véhicules/km et 120 véhicules/km. Les véhicules de ce scénario ont une vitesse comprise dans l'intervalle [20 km/h, 40 km/h].

Les CAMs sont envoyées avec une fréquence de 10 Hz. Pour la valeur de T_{sup} , comme dans [48], nous nous sommes inspirés par la norme IEEE 802.11 et nous l'avons fixée à 1024 slots de temps. Le tableau I résume les paramètres de simulation.

Il est clair que la durée et le nombre de slots impactent la performance du protocole notamment, le délai de livraison qui augmente avec l'augmentation de la durée et du nombre de slots. Cependant, si la valeur du slot de temps est très petite, le nombre de collisions de messages augmente et par conséquent, le nombre de rediffusions augmente aussi.

Nous avons testé plusieurs valeurs de slots (0,2 ms, 0,5 ms, et 0,8 ms) et les résultats que nous avons obtenus montrent que la valeur de 0,5 ms fournit une meilleure performance en termes de délai de livraison et de redondance des messages (cf. figures 5-8 à 5-11).

5. Un protocole adaptatif pour la dissémination d'alertes

Table 5-1 Paramètres de simulation

Paramètre	Valeur
Zone de simulation	4 km*3voies
Zone d'intérêt	2 km
Rayon de transmission	300m
Taille des DENMs	256 octets
Taille des CAMs	100 octets
T_{min}	0
T_{max}	1024
Durée du slot	0.5ms
Modèle de propagation	Nakagami
Temps de simulation	200s
Débit	12Mbps

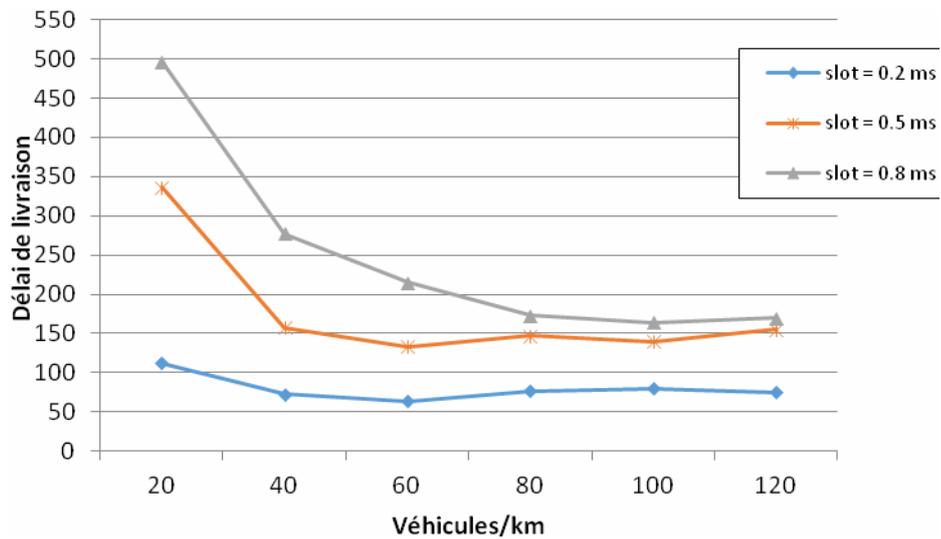


Figure 5-8 Délai de livraison de RDS en fonction de la densité et avec variation de la durée du slot

5. Un protocole adaptatif pour la dissémination d'alertes

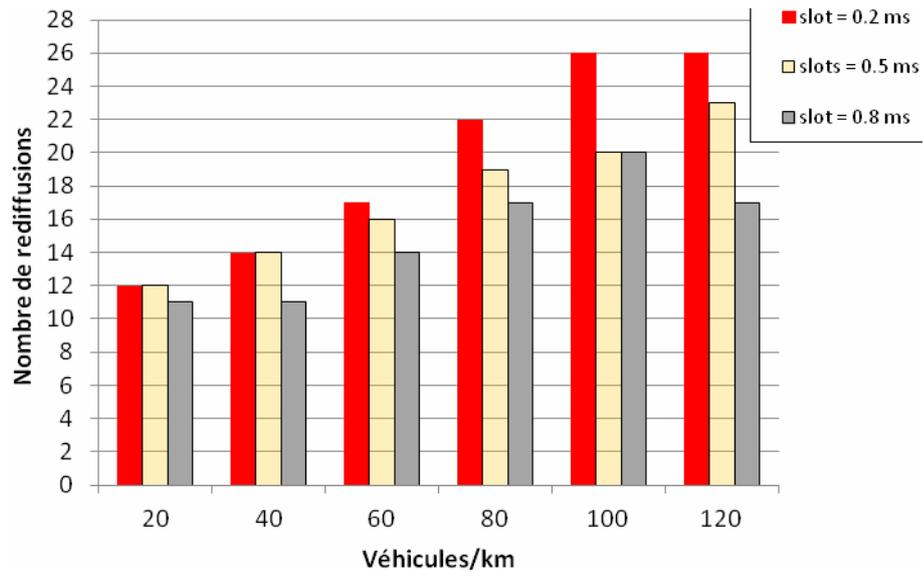


Figure 5-9 RDS-Nombre de rediffusion en fonction de la densité et avec variation de la durée du slot

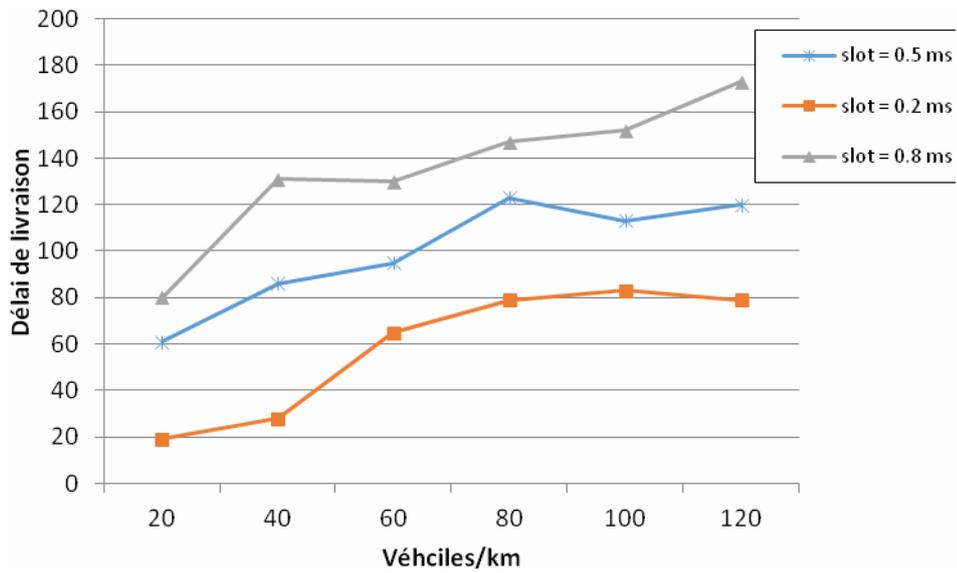


Figure 5-10 Délai de livraison de notre protocole en fonction de la densité et avec variation de la durée du slot

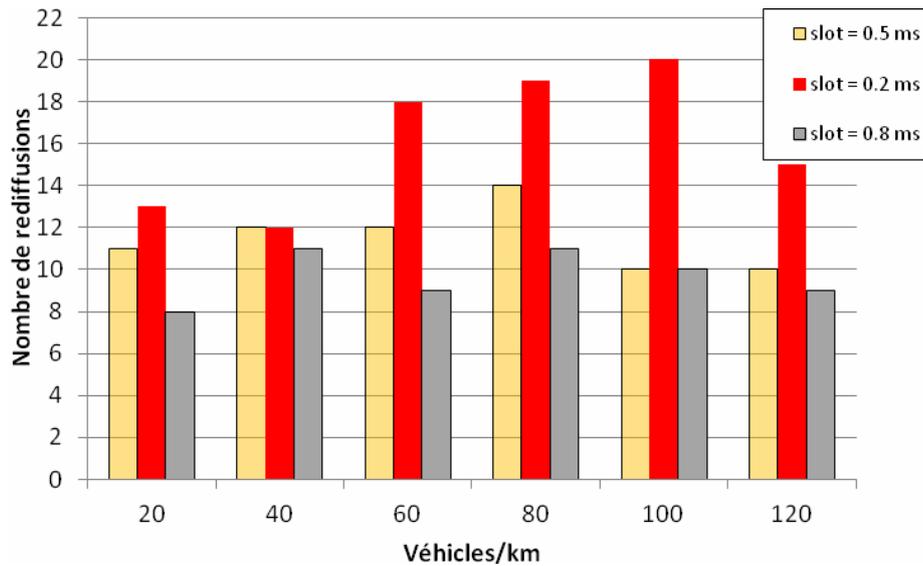


Figure 5-11 Notre protocole-Nombre de rediffusion en fonction de la densité et avec variation de la durée du slot

5.4.3 Métriques d'évaluation

Les critères de performance que nous avons retenus pour évaluer la performance de notre protocole sont les suivants :

- **Nombre moyen de rediffusions** : il représente le nombre moyen de fois que le message a été rediffusé dans la *zone d'intérêt*.
- **Délai de dissémination/livraison**: il est défini comme le délai moyen que prend un message pour atteindre les nœuds les plus éloignés dans la *zone d'intérêt* (2 km).
- **Fiabilité de la dissémination** : avec ce critère nous mesurons la proportion des véhicules dans la *zone d'intérêt* qui reçoivent les messages.

5.4.4 Analyse des résultats

5.4.4.1 Analyse du nombre moyen de rediffusions

La figure 5-12 illustre le résultat du nombre moyen de rediffusions dans la *zone d'intérêt* (2km). Comme attendu, le nombre de rediffusions dans les cas de RDS augmente avec l'augmentation de la densité du réseau. En effet, lorsque la densité du réseau

5. Un protocole adaptatif pour la dissémination d'alertes

augmente la distance entre les nœuds diminue et plusieurs nœuds sont proches les uns des autres. Comme nous l'avons expliqué dans la section 5.3, dans ce cas, il est plus probable que deux ou plusieurs nœuds avec la même valeur du timer rediffusent en même temps ; ce qui engendre une augmentation du nombre de collisions de messages et donc une augmentation dans les rediffusions.

Comme nous pouvons le voir sur la figure 5-12, la performance de notre protocole est meilleure que celle de RDS. Le nombre moyen de rediffusions est considérablement réduit en particulier dans le cas de 100 véhicules/km et 120 véhicules/km où le nombre de rediffusions est réduit de 50% et 57%, respectivement.

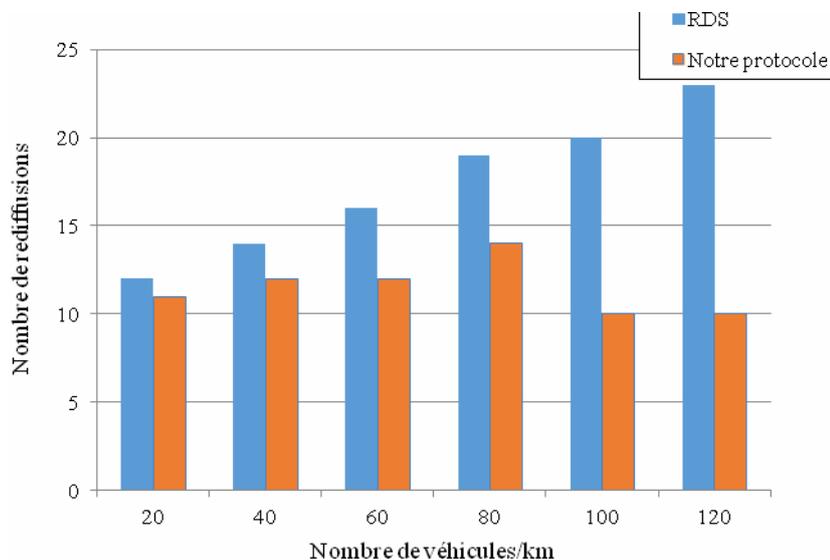


Figure 5-12 Nombre moyen de rediffusions dans 2 km en fonction du nombre de véhicules/km.

5.4.4.2 Analyse du délai moyen de livraison

Comme le montre la figure 5-13, le délai moyen de RDS commence avec une valeur élevée (336 ms à 20 véhicules/km) et il diminue jusqu'à 133 ms à 60 véhicules/km. En effet, lorsque le réseau est clairsemé la probabilité de trouver un nœud relai à la limite de la portée de transmission (avec une valeur de temps d'attente égale ou proche de zéro) est faible. Ainsi, les nœuds internes proches du dernier nœud relai ont plus de chance de décompter à zéro et de rediffuser le message, ce qui augmente le délai de livraison du message. La diminution du délai de livraison est due au fait que le réseau devient plus connecté, ce qui augmente la probabilité de trouver un nœud relai à la limite de la portée de communication.

La figure 5-14 illustre le nombre moyen de sauts qu'a pris le message pour atteindre les derniers nœuds dans la *zone d'intérêt* (à 2 km). Notre protocole nécessite moins de sauts pour que le message soit propagé sur toute la zone d'intérêt. RDS nécessite beaucoup plus de sauts en particulier à 100 véhicules/km et 120 véhicules/km. En effet, dans RDS, comme le tirage du timer est entièrement aléatoire, le nœud sélectionné n'est pas forcément le plus éloigné. En outre, lorsque plusieurs nœuds situés à la limite de la portée de transmission ne parviennent pas à transmettre (en raison des collisions de messages), il est plus probable qu'un autre nœud interne décompte à zéro et rediffuse le message, ce qui augmente le nombre de sauts.

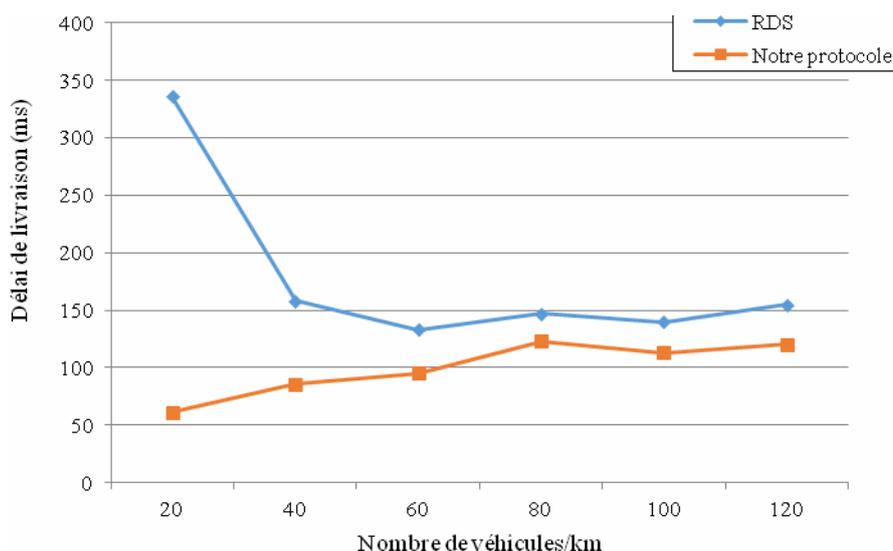


Figure 5-13 Délai de livraison moyen en fonction du nombre de véhicules/km.

En revanche, dans notre protocole le nombre de sauts n'augmente pas lorsque la densité du réseau augmente et se maintient à sept sauts. En fait, avec une portée de transmission de 300 m et une zone de pertinence de 2 km, le plus petit nombre de sauts est de sept, ce qui correspond à nos résultats (cf. Fig. 5-14). Le nombre de sauts augmente légèrement (huit sauts) dans les cas de 20 véhicules/km et 40 véhicules/km. Cela est dû au fait que la densité du réseau est faible et le relai sélectionné à chaque saut lors de la dissémination du message peut ne pas être à la limite de la portée de communication.

La figure 5-13 montre aussi que notre protocole permet d'obtenir un meilleur délai de dissémination dans différentes valeurs de densité de véhicules. En effet, contrairement à RDS, dans notre protocole T_{sup} est réduite lorsque la densité du réseau est faible, pour réduire le délai de dissémination lorsque le réseau est clairsemé. Comme nous l'avons expliqué dans la section 5.2.3.3, plus la densité du réseau est élevée, plus la fonction (5.5) étend l'intervalle de temps du côté de T_{sup} pour réduire la probabilité que deux ou plusieurs nœuds tirent la même valeur du timer.

En outre, quand le nombre de véhicules dans le réseau est de 120 véhicules/km, le délai moyen de livraison de notre protocole ne dépasse pas les 120 ms, ce qui est acceptable par les applications de sécurité routière telle que l'application RHS que nous avons présentée dans la section 5.1.

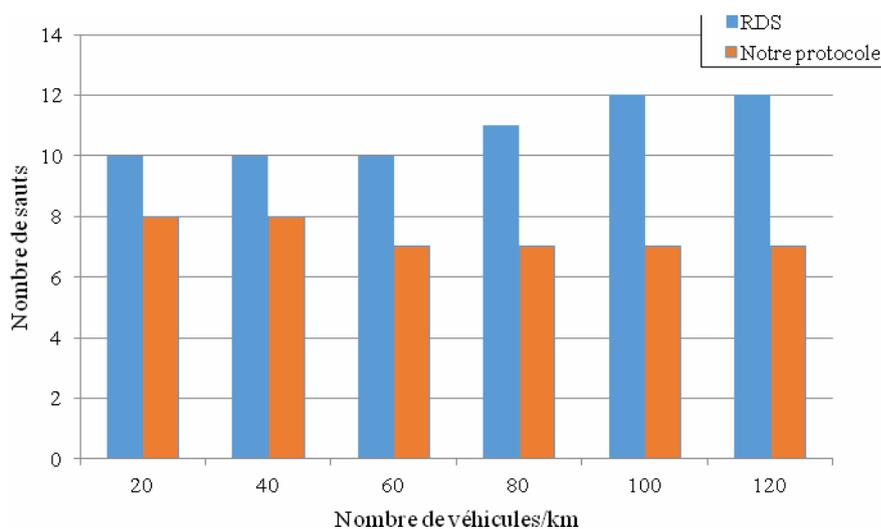


Figure 5-14 Nombre moyen de sauts en fonction du nombre de véhicules/km.

5.4.4.3 Analyse de la fiabilité de la dissémination

Dans les scénarios précédents, le taux de livraison, qui mesure la proportion de véhicules dans la *zone d'intérêt* qui ont reçu le message, est de 100% pour les deux protocoles sauf quand le nombre de nœuds dans le réseau est de 20 véhicules/km. Dans ce dernier cas, le taux de livraison est de 97%. En fait, dans ce cas, le réseau est clairsemé et des trous⁹ peuvent exister dans la topologie. Comme la distribution des nœuds n'est pas uniforme, lorsque le message est diffusé, il se peut qu'aucun nœud n'existe pour le rediffuser. Par conséquent, le message meurt avant de couvrir toute la distance de dissémination.

Pour explorer cette question et pour forcer la simulation à générer les cas où les messages ne sont pas rediffusés, par conséquent perdus, nous incluons un aspect aléatoire dans la décision du nœud relai sélectionné.

Pour forcer l'apparition de trous, c'est-à-dire pas de connectivité, nous simulons les mêmes scénarios sous une contrainte. En effet, dans cette étape d'évaluation de notre protocole, le nœud relai sélectionné rediffuse le message avec une probabilité de rediffusion P .

Si un nœud sélectionné comme relai décide de ne pas rediffuser, nous considérons que

⁹ Zone sans couverture/connectivité

5. Un protocole adaptatif pour la dissémination d'alertes

cela signifie que le nœud est déconnecté et le message rediffusé n'est reçu par aucun nœud dans la direction de la dissémination (par exemple, cas où le nœud sélectionné comme prochain relai est un nœud isolé). Nous varions cette probabilité de rediffusion pour mesurer son effet sur le taux de réception de notre protocole et aussi RDS. Nous utilisons quatre scénarios de mobilité : 20 véhicules/km et 40 véhicules/km pour représenter le cas d'une densité faible ; 60 véhicules/km et 80 véhicules/km pour représenter le cas d'une densité moyenne.

Les figures 5-15 et 5-16 montrent le taux de livraison des deux protocoles en variant la probabilité et la densité du réseau. Comme prévu, les deux protocoles sont négativement affectés par la faible probabilité de connectivité. Cependant, RDS est légèrement mieux que notre protocole lorsque la connectivité du réseau est très faible (0,2). En effet, comme dans le scénario avec 20 véhicules/km la redondance générée par RDS est faible (cf. figure 5-12), la différence entre le taux de réception des deux protocoles n'est pas significative.

Cependant, dans les autres scénarios, RDS génère plus de redondance que notre protocole, ce qui lui permet d'offrir un taux de réception meilleur de celui de notre protocole. Cela se justifie par le fait que dans notre protocole le relai ne rediffuse le message qu'une seule fois et dans le cas de déconnexion du réseau, le message meurt avant de couvrir toute la distance dissémination.

Certaines solutions ont été proposées dans la littérature pour traiter ce problème [40]. Par exemple, l'accusé de réception implicite peut être inclus dans notre protocole. Dans ce mécanisme, le nœud rediffuse périodiquement le message jusqu'à ce qu'il entende le même message rediffusé par un autre relai sélectionné.

5. Un protocole adaptatif pour la dissémination d'alertes

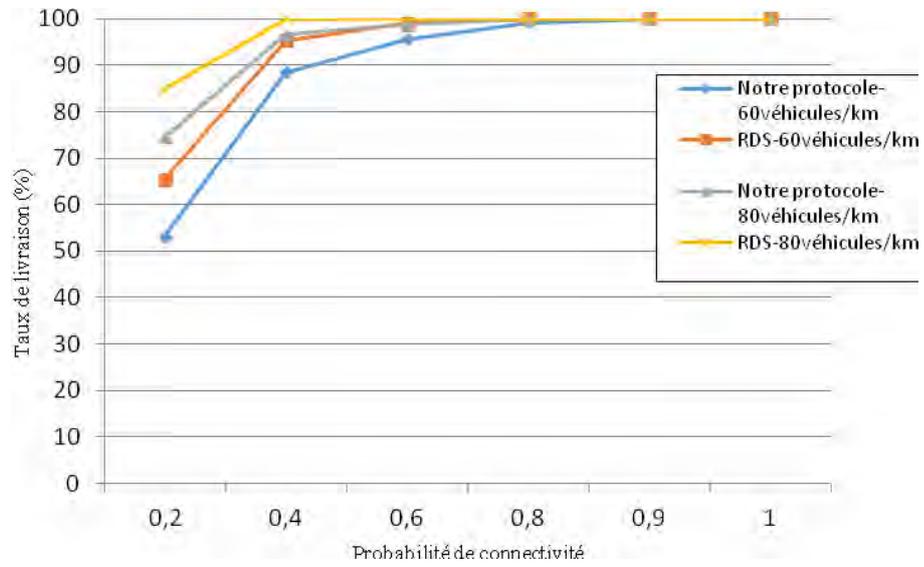


Figure 5-15 Taux de livraison en fonction de la Probabilité de connectivité – densité moyenne.

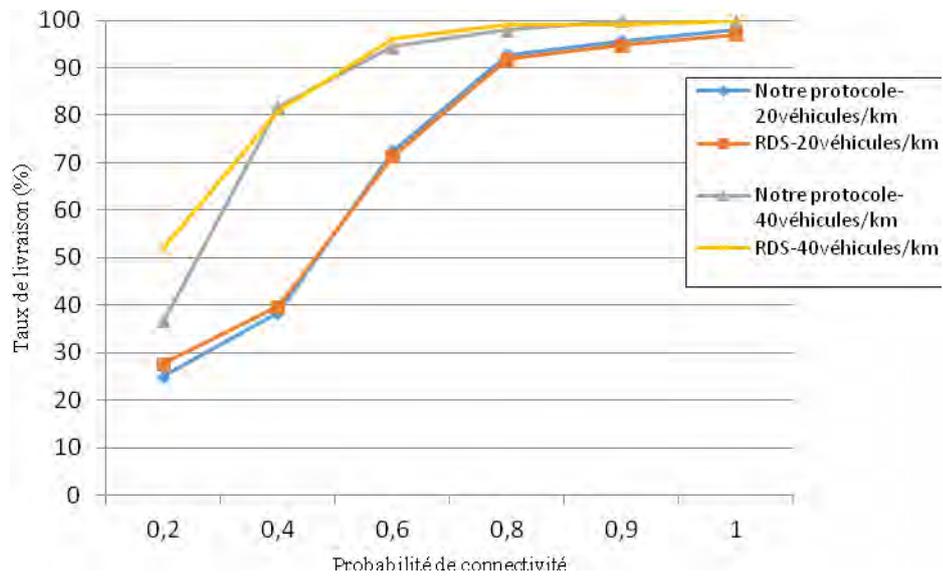


Figure 5-16 Taux de livraison en fonction de la Probabilité de connectivité – densité faible.

5.5 Conclusion

Dans ce chapitre, nous avons introduit notre protocole de dissémination de messages d'alerte dans un contexte autoroutier. A l'inverse des protocoles de dissémination proposée récemment qui ont une limitation à l'égard du délai de livraison du message, quand le réseau est clairsemé, et la redondance des rediffusions, quand le réseau est dense. Notre protocole de dissémination de messages d'alerte tente de résoudre ces problèmes en tenant compte de la densité du réseau lors du calcul du temps d'attente de chaque nœud, avant que ce dernier ne décide de rediffuser.

Notre protocole adopte une approche à base de contention dont la distance est utilisée comme variable discriminante pour favoriser certains nœuds sur d'autres à rediffuser le message dans la *zone d'intérêt*. Notre protocole prend en compte aussi bien la densité du réseau et ses changements au cours du temps. Ainsi, notre protocole est capable de s'adapter à l'environnement dans lequel il évolue pour réduire : (i) le délai de livraison de messages, (ii) le nombre de transmissions redondantes dans la zone d'intérêt et ainsi, (iii) éviter le gaspillage de la bande passante.

Notre analyse des résultats de simulation a montré que notre protocole offre une amélioration qui peut aller jusqu'à 57% de réduction dans les rediffusions quand la densité du réseau est élevée, et une réduction de 82% dans le délai de livraison du message quand le réseau est clairsemé.

Chapitre 6

Conclusions et perspectives

6.1 Conclusions

La nécessité d'avoir des routes plus sûres et plus sécurisées a encouragé le développement et la promotion des systèmes de transport intelligents. Ces derniers s'appuient principalement sur les réseaux véhiculaires pour permettre aux véhicules d'être à l'écoute de leur environnement et de partager des informations. Cette nouvelle catégorie de réseaux ad hoc sans fil a donné naissance à une large gamme d'applications allant des applications de sécurité routière et de gestion du trafic routier aux applications de divertissement et de confort des passagers.

La plupart des applications de sécurité routière se basent sur la diffusion pour disséminer les messages d'alerte sur une zone géographique spécifiée. Nous nous sommes intéressés dans cette thèse à ces mécanismes de dissémination de messages d'alerte sur un réseau de véhicules. Plus précisément la dissémination de messages d'alerte dans un contexte autoroutier. Cette application va se caractériser par des messages d'alerte à diffuser rapidement et efficacement dans une zone géographique spécifiée « *zone d'intérêt* ».

6. Conclusions et perspectives

Nous avons étudié et examiné ces mécanismes et nous avons proposé une classification de ces mécanismes basée sur un ensemble de critères que nous avons proposé. Ainsi, nous avons complété les critères déjà existants dans la littérature.

Aussi, nous avons présenté un ensemble de paramètres de simulation et les métriques évaluées par les auteurs. Comme l'étude quantitative des protocoles existants nécessite que ces derniers soient évalués dans les mêmes conditions, nous avons présenté dans un premier temps une étude de performance qualitative.

Ensuite, nous avons présenté une étude quantitative des mécanismes de dissémination les plus représentatifs, car ils intègrent le mécanisme à base de distance, le mécanisme à base de délai et le mécanisme probabiliste. En effet, dans les mécanismes que nous avons choisis, la distance est utilisée pour calculer le temps d'attente. Ce temps peut être fixé en fonction de la distance ou aléatoire tiré dans un intervalle dont les bornes dépendent de la distance. Les résultats obtenus montrent que les mécanismes CBF et RCBF offrent un délai de livraison acceptable par les applications de sécurité routière avec un taux réception de messages supérieur à 90 %. Les résultats montrent aussi que le nombre de transmissions redondantes est réduit, ce qui permet de conserver la bande passante. Cependant, la performance de ces protocoles reste toujours sensible à la densité du réseau, ce qui est un paramètre important qui n'est pas considéré par ces mécanismes.

Notre étude de l'état de l'art nous a sensibilisés sur l'importance de l'intégration de la densité dans les mécanismes de dissémination pour améliorer la performance du processus de dissémination, ce qui représente l'objet de la dernière partie de notre travail de thèse.

Dans la dernière partie de notre travail de thèse, nous avons présenté notre protocole pour la dissémination de messages d'alerte dans les réseaux véhiculaires. Notre protocole est principalement basé sur le mécanisme à base de distance pour sélectionner le prochain nœud relai. Cette distance est utilisée pour calculer l'intervalle du temps à partir duquel les nœuds tirent la valeur de leur temps d'attente. Cependant, contrairement aux autres mécanismes, notre mécanisme intègre la densité du réseau dans le calcul de l'intervalle de temps. Les résultats obtenus montrent que cette intégration permet de réduire considérablement le délai de livraison quand la densité du réseau est faible. De plus, notre protocole permet de réduire le nombre de transmissions redondantes dans la zone d'intérêt.

6.2 Perspectives

Dans ce rapport de thèse nous avons présenté notre travail qui peut être poursuivi à court et moyen termes, notamment en ce qui concerne les points suivants :

- ***Intégration d'un mécanisme de fiabilité permettant de prendre en considération la déconnexion du réseau et la présence de nœuds isolés*** : dans la littérature, deux mécanismes de fiabilité ont été présentés, à savoir le mécanisme d'acquiescement explicite et le mécanisme d'acquiescement implicite. Dans le premier, les nœuds accusent explicitement la réception de message, ce qui peut causer le problème de tempête de diffusion car les nœuds communiquent par diffusion et si chaque nœud doit accuser le message diffusé, la contention sur le canal augmente et par conséquent les collisions. L'acquiescement implicite semble plus adapté. En effet, dans ce mécanisme chaque nœud relai rediffuse périodiquement le message jusqu'à ce qu'il entende le message rediffusé par un de ses voisins.
- ***Sélection de nœud relai par l'émetteur*** : notre mécanisme est orienté récepteur c'est-à-dire la sélection du prochain nœud relai ne se fait pas au niveau de l'émetteur et ce sont les récepteurs qui rentrent en contention entre eux pour sélectionner un relai d'une manière distribuées. Nous allons travailler sur le renforcement de notre mécanisme de sélection du nœud relai par un autre mécanisme qui sera installé au niveau du nœud émetteur/relai. En effet, l'émetteur sélectionne un de ses voisins (le plus éloigné) et rajoute son identifiant dans l'entête du message avant de le rediffuser. Sur réception de message le nœud qui trouve son identifiant dans l'entête du message le rediffuse immédiatement, les autres nœuds entrent dans la procédure de contention. Nous remarquons que le mécanisme orienté émetteur a été proposé pour les MANETs et certains protocoles de communication point à point proposés pour les VANETs l'utilisent.
- ***Amélioration des fonctions de calcul d'intervalle d'attente*** : nos fonctions de calcul des bornes de l'intervalle d'attente avant de diffuser un message reçu peuvent être améliorées en proposant d'autres fonctions basées sur une meilleure pondération des paramètres Distance, Densité et Rayon de transmission.
- ***Etude de la valeur du slot*** : les temps d'attente sont des multiples de la valeur du slot de base. Nous souhaitons investiguer l'impact de la valeur du slot sur les

performances des mécanismes de dissémination. En d'autres termes, quelle serait la valeur minimale du slot permettant d'avoir les meilleures performances et à partir de quelle valeur les performances commenceraient à se dégrader en fonction du contexte (en particulier en fonction de la densité du réseau) ?

- **Conception orientée cross-layer** : la sous-couche MAC des nœuds véhiculaires fonctionne à l'aide de paramètres, particulièrement les valeurs de *backoff* et le rayon de transmission. Une adaptation de ces paramètres en fonction de la densité permet d'améliorer certainement les performances des protocoles de dissémination. Il s'agit là d'une piste intéressante à investiguer.
- **Expérimentation du protocole proposé** : de nos jours, les plates-formes à base de mini-ordinateurs (tels que les Raspberry Pi) se développent de plus en plus et permettent, à moindre coût, de faire des expérimentations de protocoles de réseau. Nous envisageons d'implanter notre protocole sur un réseau de nœuds à base de Raspberry Pi.

Références

- [1] J. J. Blum, A. Eskandarian, and L. J. Hoffman, *Challenges of Intervehicle Ad Hoc Networks*, IEEE Transactions on Intelligent Transportation Systems, vol. 5, no. 4, pp. 347-351, 2004.
- [2] M. Sichitiu and M. Kihl, *Inter-Vehicle Communication Systems: A survey*, IEEE Communications Surveys & Tutorials, vol. 10, no. 2, pp. 88-105, 2008.
- [3] W. Kiess, J. Rybicki, and M. Mauve, *On the Nature of Inter-vehicle Communication*, Proceedings of the 4th Workshop Mobile Ad Hoc Networks (WMAN 07), pp. 493–502, 2007.
- [4] E. Spaho, M. Ikeda, L. Barolli, and F. Xhafa, *Performance Evaluation of OLSR and AODV Protocols in a VANET Crossroad Scenario*, Proceedings of the IEEE International Conference on Advanced Information Networking and Applications (AINA), pp. 577-582, 2013.
- [5] N. Wisitpongphan, O. Tonguz, J. S. Parikh, P. Mudalige, F. Bai, and V. Sadehar, *Broadcast Storm Mitigation Techniques in Vehicular Ad Hoc Networks*, IEEE Wireless Communications, vol. 14, no. 6, pp. 84-94, 2007.
- [6] W. Viriyasitavat, O. K. Tonguz, and F. Bai, *Network Connectivity of VANETs in Urban Areas*, 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON'09), pp. 1–9, Jun. 2009.
- [7] O. Tonguz, N. Wisitpongphan, and F. Bai, *DV-CAST: A Distributed Vehicular Broadcast Protocol for Vehicular Ad Hoc Networks*, IEEE Wireless Communications, vol. 17, no. 2, pp. 47-56, 2010.
- [8] J. Haerri, C. Bonnet, and F. Filali, *Kinetic mobility management applied to vehicular ad hoc network protocols*, Elsevier Computer Communications (COMCOM) "Special Issue on Mobility Protocols for ITS VANET", vol. 31, no. 12, July 2008.
- [9] M. Torrent-Moreno, M. Killat, and H. Hartenstein, *The challenges of robust inter-vehicle communications*, Proceedings of the 26th IEEE Vehicular Technology Conference (VTC-2005-Fall), pp. 319–323, September, 2005.
- [10] H. Moustafa and G. Bourdon, *Vehicular Networks Deployment View: Applications, Deployment Architectures and Security Means*, Ubiquitous Computing and Communication Journal - Special Issue of UbiRoads, 2008.
- [11] CAMP consortium, *Vehicle Safety Communications Project Task 3 Final Report - Identify Intelligent Vehicle Safety Applications Enabled by DSRC*, CAMP Vehicle Safety Communications Consortium, US, DOT HS 809 859, 2005.

Références

- [12] The European Telecommunications Standards Institute, *Intelligent Transport Systems (ITS); Vehicular Communications; Basic set of Applications; Definitions*, Technical Report ETSI TR 102 638 V1.1.1 (2009-06).
- [13] A. Festag, *Cooperative Intelligent Transport Systems in Europe*, IEEE Communication Magazine, vol. 52, no. 12, pp. 166-172, 2014.
- [14] The European Telecommunications Standards Institute, *Intelligent Transport Systems (ITS); V2X Applications; Part 1: Road Hazard Signaling (RHS) application requirements specification*, Technical Specification ETSI TS 101 539-1 V1.1.1 (2013-08).
- [15] The European Telecommunications Standards Institute, *Intelligent Transport Systems (ITS); V2X Applications; Part 1: Intersection Collision Risk Warning (ICRW) application requirements specification*, Technical Specification ETSI TS 101 539-2 V. 1.1.1 (2013-11).
- [16] The European Telecommunications Standards Institute, *Intelligent Transport Systems (ITS); V2X Applications; Part 3: Longitudinal Collision Risk Warning (LCRW) application requirements specification*, Technical Specification ETSI TS 101 539-3 V. 1.1.1 (2013-11).
- [17] C. D. Wang and J. P. Thompson, *Apparatus and method for motion detection and tracking of objects in a region for collision avoidance utilizing a real-time adaptive probabilistic neural network*, U.S. Patent, No. 5, 613, 039, Mar. 1997.
- [18] J. B. Kenney, *Dedicated Short-Range Communications (DSRC) Standards in the United States*, *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1162-1182, 2011.
- [19] The European Telecommunications Standards Institute, *Intelligent Transport Systems (ITS); Vehicular Communications; Basic set of Applications; Part 2: Specification of Cooperative Awareness Basic service*, ETSI TS EN 302 637-2, V. 1.3.0, 2013.
- [20] The European Telecommunications Standards Institute, *Intelligent Transport Systems (ITS); Vehicular Communications; Basic set of Applications; Part 3: Specification of Decentralized Environmental Notification Basic Service*, ETSI TS EN 302 637-3, V. 1.2.0, 2013.
- [21] D. F. Astudillo-Salinas, *Téléchargement de Contenus dans les réseaux véhiculaires*, Thèse doctorat, Institut National Polytechnique de Toulouse (INP Toulouse), 2013.
- [22] F. Mezghani, R. Dhaou, M. Nogueira, and A. L. Beylot Content, *Dissemination in Vehicular Social Networks: Taxonomy and User Satisfaction*, IEEE Communication Magazine, vol. 52, no. 12, pp. 34 – 40, 2014.
- [23] CAR 2 CAR Communication Consortium, URL : <https://www.car-2-car.org>.
- [24] C. WEIß, *V2X communication in Europe—From research projects towards standardization and field testing of vehicle communication technology*, Computer Networks, vol. 55, no 14, p.

- 3103-3119, 2011.
- [25] J. A. Misener, S. Biswas, and G. Larson, *Development of V-to-X systems in North America: The promise, the pitfalls and the prognosis*, Computer Networks, vol. 55, no. 14, pp. 3120-3133, 2011.
- [26] The Institute of Electrical and Electronics Engineers, *IEEE Standard for Wire-less Access in Vehicular Environments - Security Services for Applications and Management Messages*, April 2013.
- [27] The Institute of Electrical and Electronics Engineers, *IEEE Standard for Wire-less Access in Vehicular Environments (WAVE) - Multi-channel Operation*, February 2011.
- [28] The Institute of Electrical and Electronics Engineers, *IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services*, 2010.
- [29] The Institute of Electrical and Electronics Engineers, *IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE)-Resource Manager*, October 2006.
- [30] The European Telecommunications Standards Institute, *Intelligent Transport Systems (ITS); Harmonized Channel Specifications for Intelligent Transport Systems operating in the 5 GHz frequency band*, ETSI TS V1.1. 2012.
- [31] The European Telecommunications Standards Institute, *Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality*, ETSI Std V1.2.0, 2013.
- [32] The European Telecommunications Standards Institute, *Intelligent Transport Systems (ITS); Users and Applications Requirements; Part 1 : Facility Layer Structure, Functional Requirements and Specifications*, ETSI TS 102 894-1, V 1.1.1, August 2013.
- [33] Network simulator—ns (version 2). [Online]. Available: <http://isi.edu/nsnam/ns/>.
- [34] S. Jain, K. Fall, and R. Patra, *Routing in a Delay Tolerant Network*. In ACM Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, pp. 145-157), Portland, Oregon, USA, 2004.
- [35] F. Schmidt-Eisenlohr, M. Torrent-Moreno, J. Mittag, and H. Hartenstein, *Simulation platform for inter-vehicle communications and analysis of periodic information exchange*, Proceedings of the Fourth Annual conference on Wireless on Demand Network Systems and Services, Obergurgl, Tyrol, Austria, pp. 50–58, Jan. 2007.
- [36] S. Schnauffer, H. Fubler, M. Transier, and W. Effelsberg, *Vehicular Ad-Hoc Networks: Single-Hop Broadcast is not Enough*, Proceedings of the 3rd International Workshop on Intelligent

- Transportation, pp. 49-54, Hamburg, Germany, 2006.
- [37] S. Ni, Y. Tseng, Y. Chen, and J. Sheu, *The Broadcast Storm Problem in a Mobile Ad Hoc Network*, Proceedings of the ACM/IEEE international conference on Mobile computing and networking, pp. 151-162, Seattle, USA, 1999.
- [38] E. Royer and C. Toh, *A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks*, IEEE Personal Communications, vol. 6, no. 2, pp. 46-55, 1999.
- [39] Y. Tseng, S. Ni, and E. Shih, *Adaptive Approaches to Relieving Broadcast Storms in a Wireless Multihop Mobile Ad Hoc Network*, IEEE Transactions on Computers, vol. 52, no.5, pp. 545-557, 2003.
- [40] A. Berradj and Z. Mammeri, *Multi-hop broadcasting in VANETs for safety applications: Review and classification of protocols*, International Journal of Business Data Communications and Networking, vol. 9, no. 4, pp. 86-104, Oct. 2013.
- [41] IEEE Standard for Information technology –Telecommunications and information exchange between systems–Local and metropolitan area networks–Specific requirements Part 11 : *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6 : Wireless Access in Vehicular Environments*, IEEE Std., 2010.
- [42] R. Ahlswede, N. Cai, N. Y. Li, and R. W. Yeung, *Network Information Flow*, IEEE Transactions on Information Theory, vol. 46, no. 4, pp. 1204-1216, 2000.
- [43] H. Füßler, H. Hartenstein, J. Widmer, and M. Mauve, *Contention based forwarding for street scenarios*, Proceedings of the 1st International Workshop in Intelligent Transportation (WIT 2004), pages 155–160, Hamburg, Germany, March 2004.
- [44] A. Benslimane, *Optimized Dissemination of alarm Messages in Vehicular Ad-hoc Networks (VANET)*, Proceedings of the IEEE International Conference on High Speed Networks and Multimedia Communications (HSNMC'04), 2004.
- [45] M. Sun, W. Feng, T. Lai, K. Yamada, H. Okada, and K. Fujimura, *GPS based message broadcast for adaptive inter-vehicle communications*, Proceedings of the 52nd IEEE Vehicular Technology Conference (VTC-Fall-2000), May 2000.
- [46] E. Fasolo, A. Zanella, and M. Zorzi, *An Effective Broadcast Scheme for Alert Message Propagation in Vehicular Ad hoc Networks*, Proceedings of the IEEE International Conference on Communications (ICC'06), pp. 3960-3965, 2006.
- [47] F. Hrizi, Christian Bonnet, Jérôme Härri, Fethi Filali, *Adapting Contention-based Forwarding to Urban Vehicular Topologies for Traffic Safety Applications*, Annals of Telecommunications, Springer, vol. 68, no. 5-6, pp. 267–285, 2012.

- [48] C. E. Palazzi, M. Roccetti, and S. Ferretti, *An intervehicular communication architecture for safety and entertainment*, IEEE Transaction on Intelligent Transportation Systems., vol. 11, no. 1, pp. 90–99, Mar. 2010.
- [49] J. F. Lee, C. S. Wang, and M. C. Chuang, *Fast and reliable emergency message dissemination mechanism in vehicular ad hoc networks*, Proceedings of the IEEE Wireless Communications and Networking Conference, Sydney, Australia, pp. 1-6, 2010.
- [50] K. Ibrahim and C. Michele, *p-IVG: Probabilistic Inter-Vehicle Geocast for Dense Vehicular Networks*, Proceedings of the 69th IEEE Vehicular Technology Conference (VTC-2009-Spring), 5 pages, Barcelona, Spain, 2009.
- [51] Sumo project. [Online]. Available: <http://sourceforge.net/projects/sumo>.
- [52] G. Korkmaz, L. Ekici, and F. Ozguner, *An Efficient Fully Ad-Hoc Multi Hop Broadcast Protocol for Inter-Vehicular Communication Systems*, Proceedings of the IEEE International Conference on Communications, pp. 423-428, Istanbul, Turkey, 2006.
- [53] M. Torrent-Moreno, *Inter-Vehicle Communications: Assessing Information Dissemination under Safety Constraint*, Proceedings of the Annual Conference on Wireless on Demand Network Systems and Services, pp. 59-64, Tyrol, Austria, 2007.
- [54] P. Akkhara, Y. Sekiya, and Y. Wakahara, *Efficient Alarm Messaging by Multi-Channel Cut-Through Rebroadcasting based Inter-Vehicle communication*, Proceedings of the International Journal of Computer Science, vol. 36, no. 2, pp. 157-166, 2009.
- [55] L. Bononi and M. Di Felice, *A Cross Layered MAC and Clustering Scheme for Efficient Broadcast in VANETS*, Proceedings of the IEEE International Conference on Mobile Ad Hoc and Sensor Systems, 8 pages, Pisa, Italy, 2007.
- [56] F. Hrizi and F. Filali, *Achieving Broadcasting Efficiency in V2X Networks with a Distance-based Protocol*, Proceedings of the International Conference on Communications and Networking, 8 pages, Hammamet, Tunisia, 2009.
- [57] S. Oh, J. Kang, and M. Gruteser, *Location-Based Flooding Techniques for Vehicular Emergency Messaging*, Proceedings of the 3rd IEEE Annual International Conference on Mobile and Ubiquitous Systems, 9 pages, San Jose, USA, 2006.
- [58] H. Luo, D. Zhang, and C. YE, *Local-directed Network Coding in Vehicular Ad-Hoc Networks*, Proceedings of the International Symposium on Intelligent Signal Processing and Communication Systems, pp. 1-4, Chengdu, China, 2010.
- [59] T. Osafune, L. Lin, and M. Lenardi, *Multi-Hop Vehicular Broadcast (MHVB)*, Proceedings of the 6th International Conference on ITS Telecommunications, pp. 757-760, Chengdu, China,

- 2006.
- [60] K. Hafeez, L. Zhao, and Z. Liao, *A New Broadcast Protocol for Vehicular Ad Hoc Networks Safety Applications*, Proceedings of the IEEE Global Telecommunications Conference, 5 pages, Miami, FL, USA, 2010.
- [61] H. Alshaer and E. Horlait, *An Optimized Adaptive Broadcast Scheme for Inter-vehicle Communication*, Proceedings of the 61st IEEE Vehicular Technology Conference (VTC-Spring-2005), vol. 5, pp. 2840-2844, Stockholm, Sweden, May 2005.
- [62] B. Bako, E. Schoch, F. Karl, and M. Weber, *Optimized Position Based Gossiping In VANETs*, Proceedings of the 68th IEEE Vehicular Technology Conference(VTC-Fall-2008),5 pages. Calgary, Canada, September 2008.
- [63] Y. T. Yang, and L. D. Chou, *Position-Based Adaptive Broadcast for Inter-Vehicle Communications*, Proceedings of the IEEE International Conference on Communications Workshop, pp. 410-414, Beijing, China, 2008.
- [64] B. Bako, I. Rikanovic, F. Kargl, and E. Schoch, *Adaptive Topology Based Gossiping in VANETs Using Position Information*, Proceedings of the International conference on Mobile ad-hoc and sensor networks, 13 pages, Beijing, China, 2007.
- [65] E. Van de Velde, and C. Blondia, *Adaptive REACT Protocol for Emergency Applications in Vehicular Networks*, Proceedings of the 32nd IEEE Conference on Local Computer Networks, pp. 613-619, Dublin, Ireland, 2007.
- [66] S. Jain, K. Fall, and R. Patra, *Routing in a Delay Tolerant Network*, Proceedings of the ACM Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, pp. 145-157, Portland, Oregon, USA, 2004.
- [67] M. Slavik and I. Mahgoub, *Stochastic Broadcast for VANET*, Proceedings of the 7th IEEE Consumer Communications and Networking Conference (CCNC), pp. 1-5, Las Vegas, USA, 2010.
- [68] M. Slavik and I. Mahgoub, *Statistical Broadcast Protocol Design for Unreliable Channels in Wireless Ad-hoc Networks*, Proceeding of the IEEE Global Telecommunications Conference (GLOBECOM 2010), 5 pages, Miami, FL, USA, December 2010.
- [69] G. Korkmaz, E. Ekici, F. Ozguner, and U. Ozguner, *Urban Multi-hop Broadcast Protocol for Inter-vehicle Communication Systems*, Proceedings of the 1st ACM workshop on Vehicular Ad Hoc Networks, pp. 76-85, Philadelphia, PA, USA, 2004.
- [70] U. S. Department of Transportation, Federal Highway administration, URL:
http://ops.fhwa.dot.gov/eto_tim_pse/reports/2010_cong_evac_study/houston_tx.htm

Références

- [71] R. Chen, W. L. Jin, and A. Regan, *Broadcasting Safety Information in Vehicular Networks: Issues and Approaches*, IEEE Network, vol. 24, no. 1, pp. 20-25, 2010.
- [72] R. Kumar and M. Dave, *A Review of Various VANET Data Dissemination Protocols*, International Journal of u- and e- Service, Science and Technology, vol. 5, no. 3, pp. 27-44, 2012.
- [73] S. Panichpapiboon and W. Pattara-Aticom, *A review of Information Dissemination Protocols for Vehicular Ad Hoc Networks*, IEEE Communications Surveys & Tutorials, vol. 14, no. 3, pp. 784-798, 2012.
- [74] European Commission, Road Safety, URL: http://ec.europa.eu/transport/road_safety/specialist/statistics/index_en.htm.
- [75] The European Telecommunications Standards Institute, *Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical Addressing and Forwarding for Point-to-Point and point-to-Multipoint communications; sub-part 1: Media-Independent Functionality*, ETSI EN 302 636-4-1 V1.2.1, Jul. 2014.

Liste des publications

- A. Berradj, Z. Mammeri, Adaptive Contention Window Scheme to Improve Multihop Broadcast in VANETs, IEEE 81st Vehicular Technology Conference: VTC2015-Spring, 11–14 May 2015, Glasgow, Scotland, 6 pages.

- A. Berradj, Z. Mammeri, Multi-Hop Broadcasting in VANET for Safety Applications: Review and Classification of Protocols, International Journal of Business Data Communications and Networking, October-December 2013, Vol. 9, No. 4, pp. 86-104.