Réseaux ad hoc véhiculaires : vers une dissémination de données efficace, coopérative et fiable

Nadia Haddadou

Université Paris-EST

École Doctorale MSTIC
Mathématiques et Sciences et Technologies de l'Information et de la Communication

Thèse de doctorat

Discipline : Informatique

présentée par

Nadia Haddadou

Réseaux ad hoc véhiculaires : vers une dissémination de données efficace, coopérative et fiable

---

dirigée par Gilles Roussel

Soutenue le 16 juin 2014 devant le jury composé de :

M. André-Luc Beylot	Professeur INP Toulouse	Rapporteur
M. Marcelo Dias De Amorim	DR CNRS	Rapporteur
M. Marco Fiore	Chercheur CNR IEIIT	Examinateur
M. Sidi Mohammed Senouci	Professeur Université de Bourgogne	Examinateur
M. Abderrezak Rachedi	Maître de Conférences UPEM	Co-encadrant de thèse
M. Yacine Ghamri-Doudane	Professeur Université de la Rochelle	Co-encadrant de thèse
M. Gilles Roussel	Professeur UPEM	Directeur de thèse

Remerciements

Je tiens à remercier les membres de mon jury : André-Luc Beylot et Marcelo Dias de Amorim d'avoir accepté de rapporter cette thèse et d'y avoir apporté des remarques et questions, lesquelles ont contribué à son amélioration.

Je remercie tout autant Marco Fiore d'avoir accepté d'être examinateur de cette thèse et Sidi-Mohammed Senouci d'en avoir accepté la présidence.

Je voudrais aussi remercier mes deux encadrants Abderrezak Rachedi et Yacine Ghamri-Doudane pour toute leur aide, leurs conseils, leur patience, ainsi que leurs encouragements. Chacun d'entre eux a su, à sa manière, me guider. Je remercie aussi mon directeur de thèse Gilles Roussel, pour la confiance qu'il m'a accordé.

J'adresse un remerciement à tous ceux qui ont de près ou de loin contribué à la réalisation de ce projet, plus particulièrement à Yesid, Ibtissem et Camila pour leur amitié et leur soutien constant. Aussi je tiens à mentionner mes collègues Patrice, Ismaïl, Sylvain, Safaa, Ali et Philippe pour la bonne ambiance générale au bureau, et pour leur sympathie.

Mes remerciements s'adressent enfin à ma famille, des deux côtés de la méditerranée, qui m'a toujours soutenu et encouragé et sans qui tout cela n'aurait pas pu être possible.

Résumé

Les réseaux ad hoc véhiculaires (VANETs) permettent le partage de différents types de données entre les véhicules, de manière collaborative. Dans cette thèse, nous nous sommes tout particulièrement intéressés aux applications de sûreté et de sécurité routière, dédiées à l'échange des informations sur l'état de l'environnement routier. Les contraintes de ces applications en termes de qualité de services sont des plus rigoureuses, car l'acheminent de leurs données doit être exhaustif et ne souffrir d'aucun retard pour assurer une information utile et en temps opportun au profit de tous les usagers concernés. Cet acheminement doit faire face aux difficultés induites par la dispersion et la forte mobilité des véhicules, l'absence ou l'insuffisance d'infrastructure, la densité variable du réseau, la surcharge en informations à envoyer et l'étendue des zones géographiques à couvrir. En effet, la problématique de diffusion des données dans les VANETs s'avère non-triviale et de nombreux verrous scientifiques doivent être levés pour permettre un support *efficace*, *collaboratif* et *fiable* pour les applications de sûreté et de sécurité routière.

Plus précisément, nous aborderons la problématique de la dissémination collaborative en se posant trois questions : "*comment disséminer les données ? À quel moment le faire ? Mais aussi quoi disséminer et comment inciter à le faire ?* " Nous avons apporté des réponses à travers les trois contributions de cette thèse. La première consiste à proposer une stratégie de dissémination *efficace*, qui soit adaptée à l'importance de l'information échangée et à sa durée de vie, permettant ainsi d'éviter un processus de diffusion intensif. Celui-ci est inapproprié dans ce cas de figure, car il génère de la congestion et beaucoup de redondance. Nous confirmons nos propos et attestons de la validité des performances de notre solution avec une modélisation par une chaîne de Markov à temps discret et à espace d'états discret qui démontre le nombre de retransmissions nécessaires à la réception d'une information par les véhicules concernés. Celle-ci est renforcée par une étude de performances par simulation, laquelle montre une diminution de 90% du taux de messages redondants par rapport au cas de la diffusion par inondation. Afin d'améliorer plus encore les performances du processus de diffusion des messages de sûreté et de sécurité routière, nous proposons, dans un second temps, un ordonnanceur pour l'accès au canal de communication qui a pour objectif de réduire le nombre de collisions dues aux synchronisations afférentes à l'utilisation du multi-canal dans le standard IEEE 802.11p/1609.4 et donc élever le taux de réception des données. Nous basons notre proposition sur la théorie de l'arrêt optimal, qui décide du moment opportun pour l'envoi d'une information en conciliant occupation du canal, efficacité de l'envoi et délai d'ajournement toléré par une information. Dans notre cas, la théorie de l'arrêt optimal est formulée par un processus de décision Markovien (MDP). Nous montrons ainsi par simulation une amélioration substantielle du taux de réception (de 25%) et une diminution importante des pertes (de 47%).

Après s'être intéressé à l'aspect quantitatif des performances du réseau, nous nous intéresserons ensuite à l'amélioration de la *fiabilité* du processus de diffusion. Cette

fiabilité est obtenue grâce à l'incitation des véhicules à la coopération et à l'exclusion des véhicules malicieux de celui-ci. Ceci est réalisé au travers de la proposition d'un modèle de confiance. Ce modèle est inspiré des jeux de signaux, qui sont une classe des jeux bayésiens dynamiques. Il crée une situation d'équilibre, tel que les différentes parties le composant ne soient pas tentées de le contourner, ainsi découle une auto-sélection des véhicules, laquelle est rapide et peu coûteuse. Nous définissons les valeurs des paramètres de notre modèle de confiance via une modélisation par une chaîne de Markov à temps discret et à espace d'états discret. À notre connaissance, notre modèle est le seul à s'attaquer aux effets néfastes des deux types de véhicules, malicieux et égoïstes, en même temps. Comme précédemment, nous évaluons les performances de notre solution au travers d'une modélisation par une chaîne de Markov et divers jeux de simulation. Ceci a permis de montrer que 100% des véhicules malicieux sont exclus, avec le maintien d'un taux de coopération élevé dans le réseau, soit une amélioration de 42%.

Mots-clefs

Réseaux ad hoc véhiculaires, stratégie de dissémination, accès au canal de communication, modèle de confiance, véhicules malicieux et égoïstes.

Vehicular ad hoc networks : towards efficient, collaborative and reliable data dissemination

Abstract

Vehicular Ad Hoc Networks (VANETs) allow sharing different kinds of data between vehicles in a collaborative way. In this thesis, we are particularly interested in road safety applications, designed for the exchange of information on road traffic and conditions. This kind of applications have strict Quality of Service (QoS) requirements, as data must be routed thoroughly and without any delays so for assuring the timely delivery of useful information to the drivers. In this context, data routing must face several issues raised by the high mobility and dispersion of vehicles, inadequate or completely lacking infrastructure, a variable network density, network saturation due to the large of information to deliver, and the size of the geographical areas to cover. Indeed, the problem of data dissemination in VANETs is non-trivial, and several research challenges must be solved in order to provide an *efficient*, *collaborative*, and *reliable* support for road safety applications.

Specifically, we will address the problem of collaborative data dissemination through the following three questions: "*How to perform data dissemination?*", "*When should we do it?*", and "*What must be disseminated?*" We have provided answers to these questions through the three contributions of this thesis. Our first contribution is an *efficient* dissemination strategy, specifically tailored to the importance of the exchanged information as well as its lifespan, which is able to avoid the intensive dissemination process that generates network congestion and data redundancy. We confirm our statements and validate the performance of our solution by modeling it using a discrete-time Markov chain, which demonstrates the number of necessary retransmissions for all concerned vehicles to receive information. Moreover, we performed extensive simulations that show a reduction of up to 90% of redundant messages with respect to message flooding dissemination strategies.

Next, in order to further improve the road safety message dissemination process, we propose a communications channel access scheduler, which aims at reducing the number of collisions caused by IEEE 802.11p/1609.4 multi-channel synchronizations, and thus improving the data reception rate. We base our solution on the optimal stopping theory, which chooses the right moment to send information by balancing the channel occupancy rate, the data delivery efficiency, and the maximum deferment delay tolerated by the information. To this end, we formulate the optimal stopping theory through a Markov decision process (MDP). We show through simulation-based evaluations an improvement of the reception rate of up to 25% and a reduction of up to 47% of message losses.

Finally, after being interested in the quantitative aspect of network performance, we centered our efforts on improving the *reliability* of the dissemination process, which is obtained by motivating vehicles to cooperate and evicting malicious vehicles from the process. To this end, we propose a trust model inspired on signaling games, which are a type of dynamic Bayesian games. Through the use of our model, equilibrium is achieved, thus resulting in a fast and low-cost vehicle self-selection process. We define the parameters of our trust model through a discrete-time Markov chain model. To the best of our knowledge, our solution is the only existing solution that tackles the negative effects introduced by the presence of both malicious and selfish vehicles in a VANET. We evaluated the performance of our solution by modeling it using a Markov chain, and a set of simulations. Our results show that up to 100% of malicious vehicles are evicted while

keeping a high cooperation rate, thus achieving an improvement of 42% when compared to other similar solutions.

keywords

Vehicular Ad Hoc Networks, dissemination strategy, communications channel access, trust model, malicious and selfish nodes.

Table des matières

Chapitre 1

Introduction générale

D'après l'organisation mondiale de la santé, les accidents de la route auront été la cause de $1,2$ millions de morts et de 50 millions de blessés dans le monde, pour la seule année 2004. Ces chiffres, effrayants, iraient en s'aggravant, jusqu'à 65% de plus au cours des vingt prochaines années, si rien n'est fait pour améliorer la prévention et renforcer la sécurité routières [72].

Avec l'augmentation du nombre de véhicules en circulation, il devient impératif de gérer en conséquence, le trafic routier. Grâce aux avancées technologiques, il est possible de nos jours de doter les véhicules d'un équipement GPS et d'une carte réseau afin de former un réseau dynamique nommé réseau ad hoc véhiculaire (VANET). Ces réseaux sont majoritairement composés de véhicules intelligents qui communiquent entre eux et/ou avec des unités de bords de route (RSUs), lorsque celles-ci sont déployées. Tout comme les réseaux ad hoc mobiles (MANETs), les réseaux ad hoc véhiculaires utilisent exclusivement les communications sans fil, mais leurs caractéristiques les rendent plus complexes que les réseaux MANETs. En effet, la forte mobilité des véhicules, l'étendue des zones à couvrir, ainsi que leur densité font que la topologie du réseau est hautement dynamique, ce qui affecte la qualité des connexions entre les véhicules et les rend irrégulières.

Les services qu'ils proposeront auront pour objectif premier de diminuer le nombre d'accidents de la route, d'améliorer le trafic routier et de l'optimiser grâce à leurs applications de sûreté et de gestion du trafic. En plus, ces réseaux pourront fournir des applications ludiques, qui participent à l'amélioration du confort au sein du véhicule. Ces applications nécessitent le partage de données entre utilisateurs, avec une certaine qualité de service. Cependant, les caractéristiques des réseaux VANETs compliquent la dissémination et l'acheminement des données.

1.1 Contributions

Dans cette thèse, nous nous sommes intéressés à la dissémination des données des applications de sûreté et de gestion du trafic. Ces dernières nécessitent un haut taux de délivrance, de courts délais d'acheminement, un faible taux de perte et de la fiabilité pour l'émission des messages. Pour faire face à ces exigences et dans le cadre des trois contributions de cette thèse, nous apportons des réponses aux questions : "*comment disséminer les données ? À quel moment le faire ? Mais aussi quoi disséminer et comment inciter à le faire ?* ".

Notre première contribution consiste à proposer une stratégie de dissémination de données adaptée aux caractéristiques des réseaux ad hoc véhiculaires. Pour répondre à

notre première question de : "*comment disséminer les données ?*" nous définissons les caractéristiques d'une donnée par : son importance géographique et sa durée de validité. Nous considérons que les données n'ont pas à être disséminées de la même façon et avec les mêmes garanties. Car les ressources du canal de communication sont limitées, elles doivent être utilisées à bon escient. Les informations, qui intéressent le plus grand nombre de véhicules et qui sont urgentes, doivent être disséminées le plus largement possible, en leur assurant un faible taux de perte et de courts délais d'acheminement. Tout message ayant dépassé sa zone de dissémination ou son délai d'actualité doit être supprimé du réseau. Nous modélisons cette stratégie de dissémination via une chaîne de Markov à temps discret et à espace d'états discret et nous validons notre étude de performance par des simulations. Dans cette contribution, nous estimons le taux de réception des messages, la vitesse de l'acheminement des données, ainsi que le nombre de messages superflus générés.

Notre deuxième contribution porte, tout comme la première, sur les aspects quantitatifs de la dissémination de données. Elle remédie aux problématiques dues à l'utilisation du multi-canal dans le standard IEEE 802.11p/1609.4. Le multi-canal a été proposé afin d'améliorer la délivrance des messages dans les réseaux ad hoc véhiculaires. En plus de la différentiation de canaux pour les applications, la première moitié de l'intervalle de synchronisation est réservée à l'acheminement des messages de sûreté sur leur canal dédié CCH, alors que la deuxième moitié est allouée au reste des applications, dont les messages sont échangés sur un des six canaux de services (SCH). Néanmoins, ce mécanisme engendre des collisions au début de l'intervalle CCH et un grand déséquilibre de charge sur le canal [37]. Ces deux phénomènes sont dûs à la mise en attente des messages de sécurité routière au cours de la deuxième moitié de l'intervalle de synchronisation. Pour pallier cela, nous proposons un ordonnanceur distribué au niveau de la couche MAC, nommé *DMS*, qui décide de l'instant opportun pour l'envoi d'un message de sécurité routière, lequel permettra de lui assurer un haut taux de réception, quitte à allonger un peu son délai d'acheminement. Notre solution répond à la question : "*À quel moment disséminer ?*" et utilise pour cela *la théorie de l'arrêt optimal* [34]. Cette dernière, définit la stratégie à utiliser si l'on cherche à s'arrêter au bon moment, tout en prenant en considération le délai maximum supporté par le message à envoyer. Nos simulations montrent que lors de l'utilisation de *DMS*, la charge du canal durant l'intervalle CCH converge vers l'équilibre, ce qui augmente fortement le taux de réception des messages et baisse le taux de perte.

Notre troisième contribution s'articule autour des aspects qualitatifs des données à disséminer, pour répondre à la dernière question :"*Quoi disséminer et comment inciter à le faire ?*" Les messages reçus dans les VANETs peuvent contenir de fausses informations ou des informations altérées, à cause de la présence de véhicules malicieux. Cette présence est plausible à cause de l'asymétrie des informations dans un VANET. Les échanges entre véhicules, pris deux à deux, étant rares à cause de leur grand nombre et de leur mobilité. Les véhicules ne peuvent établir des relations de confiance. De plus, lorsqu'un véhicule reçoit un message de sûreté, il n'a pas le temps de vérifier son authenticité.

Ajouté à cela la présence de véhicules égoïstes qui affaiblissent encore plus les performances du réseau diminuant le taux de coopération lors de la retransmission des données. Pour faire face à cela, nous proposons un modèle de confiance, nommé DTM^2, lequel vise à détecter et exclure les véhicules malicieux du réseau, en remédiant aux situations d'informations asymétriques entre les membres d'un réseau. Notre modèle permet aussi d'inciter les véhicules égoïstes à coopérer, en associant à la coopération un intéressement. Ce modèle est construit grâce à une modélisation analytique basée sur les jeux bayésiens dynamiques disposant d'informations incomplètes et est validé aussi bien analytiquement que par des simulations dans deux environnements de mobilité différents.

1.2 Organisation du manuscrit

Cette thèse est composée de six chapitres, organisés selon un cheminement logique et pédagogique de nos contributions pour l'amélioration de la dissémination dans les réseaux ad hoc véhiculaires.

Nous présentons dans le chapitre 2 les réseaux ad hoc véhiculaires et leurs caractéristiques. Nous détaillons leurs applications et leurs contraintes, ainsi que des parties spécifiques du standard IEEE 802.11p, lesquelles sont nécessaires à la complétude du manuscrit. Puis, nous proposons un état de l'art sur la dissémination dans les VANETs, suivi des défis à relever pour les solutions dédiées aux VANETs.

Dans le chapitre 3, nous présentons notre première contribution. Elle porte sur un modèle de classification de données et sur la stratégie de dissémination correspondante. Nous expliquons notre classification de données établie par rapport à l'importance et à la durée de validité d'une donnée, puis, nous détaillons la relation entre celles-ci et la stratégie de dissémination. Nous étudions en détail les impacts de la variation des paramètres réseaux sur notre stratégie de dissémination nommée *ADCD* et analysons ses performances dans chacun des scénarios, de façon analytique et par simulation.

Le chapitre 4 présente les problèmes liés à l'utilisation du multi-canal dans le standard IEEE 802.11p/1609.4. Nous détaillons ses effets indésirables, comme son fort taux de collision. Nous présentons ensuite notre solution nommée *DMS*, qui ordonnance l'envoi des messages avec l'utilisation d'un processus de décision Markovien, en prenant en considération leurs contraintes temporelles ainsi que l'occupation du canal. Nous présentons une analyse de performances et une comparaison de notre solution avec d'autres approches similaires.

Le chapitre 5, aborde les problématiques liées à la présence de véhicules malicieux et égoïstes dans les VANETs. Nous proposons un nouveau type de modèle de confiance, inspiré des jeux bayésiens dynamiques à information incomplète, capable d'exclure les véhicules malicieux du réseau et d'inciter ceux dont le comportement est égoïste à coopérer davantage. Nous proposons une modélisation théorique de ce modèle, pour définir les valeurs des ses paramètres et évaluer ses performances. Nous comparons ensuite ce modèle à d'autres approches traitant les mêmes problématiques.

Nous concluons cette thèse en rappelant les contributions et les résultats de celle-ci, ainsi que quelques perspectives soulevées par nos travaux.

Chapitre 2

Vue d'ensemble des réseaux ad hoc véhiculaires

Sommaire

De nos jours, les véhicules sont considérés autrement que de simples moyens de transport, bien plus. Grâce aux avancées technologiques récentes, une multitude de nouvelles fonctionnalités leurs sont associées, ce qui les dotent d'une source d'intelligence de par leurs interactions avec l'environnement routier. En exploitant leurs récentes capacités de communication, la création d'un réseau dédié permet de rendre plus agréable le temps qu'on passe à bord, tout en améliorant la sécurité routière. Dans ce contexte, les réseaux ad hoc véhiculaires (VANETs) participent en permettant le partage, de manière collaborative, de différents types de données entre les véhicules.

Ce chapitre a pour objectif de donner une vue d'ensemble des VANETs et de délimiter le contexte de cette thèse. Nous présentons dans un premier temps leurs caractéristiques, ainsi que les différents types d'applications qu'ils peuvent proposer. Nous évoquerons, par la suite, les parties de leur standard de communication qui nous intéressent et détaillerons les multiples techniques de dissémination de données existantes, accompagnées de quelques modèles incitatifs et de confiance. Nous conclurons ce chapitre par les défis à relever pour une dissémination de données efficace dans les VANETs, laquelle représente le sujet de cette thèse.

2.1 Réseaux ad hoc véhiculaires

Les VANETs sont considérés comme étant un cas particulier des réseaux mobiles ad hoc (MANETs) [70]. Ils se constituent à partir d'un ensemble d'entités communicantes, composé de véhicules et d'unités de bords de route (RSU). Grâce aux différentes applications que supportent les VANETs, ces réseaux sont considérés comme étant le

moyen le moins cher pour éviter les embouteillages, minimiser la consommation de carburant et réduire le temps passé sur les routes.

La technologie utilisée pour connecter un réseau véhiculaire ad hoc doit être conforme à ses caractéristiques et doit offrir un bon compromis entre les performances, le coût et le taux de pénétration de la technologie. Les technologies de communication utilisables sont :

- **Systèmes de télécommunications :** GSM/GPRS, UMTS.
- **Systèmes de radio diffusion numérique :** RDS/TMC, DAB/DMB, DVB-T/DVB-H.
- **Réseaux informatiques :** le WiMAX, le WiFi, le DSRC.

Les plupart de ces technologies nécessitent le déploiement de stations de base pour permettre la communication avec et entre les véhicules. Ces stations sont utilisées dans les systèmes de télécommunications pour contrôler l'accès au support et gérer le processus d'itinérance, ainsi que dans les systèmes de radio pour diffuser les informations aux véhicules connectées.

Nous nous baserons tout au long de notre étude sur un réseau véhiculaire ne s'appuyant pas sur une infrastructure. Cette hypothèse limite les technologies opérables pour notre réseau à celles du WIFI et du DSRC [9], car seules ces deux technologies supportent aujourd'hui le mode ad hoc sans infrastructure. Utiliser des communications directes entre les véhicules (V2V), sans nécessairement passer par une infrastructure, permet de réduire les délais d'acheminement par rapport à un système centralisé, surtout quand les communications sont locales et courtes, comme il est souvent le cas dans les VANET. Ce mode de communication, V2V, permet aussi de couvrir plus finement les zones concernées par une information, car n'étant plus limité par les caractéristiques réseaux d'une station de base.

La communauté scientifique a choisi d'utiliser le DSRC comme technologie sous-jacente aux VANETs, en réservant notamment des fréquences radios spécifiquement à ces réseaux, ce qui diminue les interférences par rapport à l'utilisation du WIFI. Cette technologie supporte les modes véhicule à véhicule (V2V), ainsi que véhicule à infrastructure (V2I). Aussi le DSRC propose un débit et une portée de communication adéquats pour les applications VANETs.

2.2 Caractéristiques des réseaux ad hoc véhiculaires

Les VANETs possèdent un nombre de caractéristiques spécifiques qui les différencient des autres types de réseaux sans infrastructure. Ces caractéristiques peuvent se traduire par des contraintes ou des points forts ayant un impact sur les communications. Les caractéristiques principales des réseaux ad hoc véhiculaires, lesquelles doivent être prises en compte par toute solution dédiée, sont :

- **Topologie hautement dynamique :** le mouvement des véhicules est caractérisé par des vitesses et des directions susceptibles de varier en fonction des scénarios. Par exemple une voie à grande vitesse (autoroute), une route nationale ou départementale, une localité urbaine (centre ville). Ceci impacte la qualité et la durée de vie des liens radio entre les véhicules et donc, la topologie du réseau. En outre, le comportement des conducteurs influencés par les informations reçues du réseau, peut aussi causer des changements dans la topologie du réseau [56]. Ceci génère :

1. **Une densité variable du réseau :** la densité d'un VANET change en fonction de la densité du trafic routier, allant de densités très fortes, lors d'embouteillage par exemple, à des densités très faibles, comme dans des routes très peu fréquentées [99].

2. **Des déconnexions fréquentes :** en raison de la nature hautement dynamique de la topologie d'un VANET, sa connectivité change fréquemment. En particulier, quand la densité de réseau est très faible, ce qui augmente les risques de déconnexions [23].

– **Fortes contraintes de délai :** certaines applications des VANETs ont de très fortes contraintes de délai. Elles nécessitent en effet que les informations échangées parviennent aux participants du réseau dans les meilleurs délais, afin que leur temps de réaction soit optimal.

– **Réseau à grande échelle :** lors du déploiement des VANETs dans des zones urbaines, des centres-villes ou des autoroutes, qui sont très denses, l'échelle du réseau peut être très importante et un passage à l'échelle de tous leurs protocoles s'impose [110].

– **Mobilité prédictive :** à la différence des autres réseaux mobiles, le mouvement des véhicules est restreint par la topologie et la signalisation routière, ainsi que par les réactions vis-à-vis du mouvement des autres véhicules. De ces faits, la mobilité des véhicules peut être prévue dans une certaine mesure.

– **Absence de contraintes énergétiques et de puissance de calcul :** étant donné que les nœuds composant un VANET sont relativement de grande taille et produisent eux mêmes de l'énergie lors de leurs mouvements. Ceux-ci peuvent être équipés de capteurs, de ressources énergétiques, en nombres et capacités suffisantes.

– **Communications basées sur la localisation géographique :** en plus des types de communications en communs entre les VANETs et les autres réseaux mobiles, comme l'unicast, le multicast et la diffusion, les VANETs supportent aussi les communications basées sur l'acheminement de données vers un groupe de véhicules désigné via sa localisation géographique. Ceci est en effet possible du fait que les véhicules soient équipés le plus souvent de systèmes de localisation plutôt efficaces.

2.3 Domaines d'application

Les réseaux ad hoc véhiculaires (VANETs) offrent plusieurs types d'applications, telles que les applications d'infotainment [99], de gestion du trafic et de sécurité routière. Chacune d'elles requière un niveau de performance et de qualité de service différent. Nous considérons généralement trois types de métriques, le temps d'acheminement de bout en bout, afin de respecter la durée de vie d'une information ; le taux de réception, pour assurer un taux minimal de délivrance des données et enfin le débit, pour assurer un certain taux d'accès au canal.

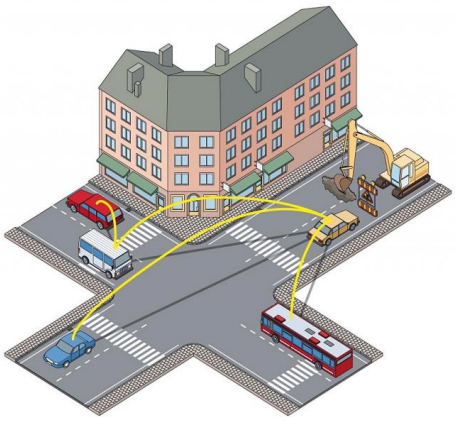


FIGURE 2.1 – Application de gestion du trafic routier [3].

2.3.1 Applications d'information et de divertissement

Les applications d'information et de divertissement, nommées aussi applications d'infotainment, visent à améliorer le confort des conducteurs et des passagers. Elles leur fournissent, d'une part, des informations d'utilité générale, comme des informations météorologiques ou d'autres sur la localisation ou les prix d'une station essence, d'un restaurant ou d'un hôtel ; et d'autre part, elles permettent aux passagers d'accéder à des services basés sur Internet, comme des jeux en ligne ou des messages instantanés [92][57][103][56][108][99].

2.3.2 Applications de gestion du trafic

Les messages échangés au sein des applications de gestion du trafic ont pour but d'améliorer le trafic routier en l'optimisant à travers la sélection de chemins et routes adéquats, en prenant en considération les embouteillages potentiels ou les obstacles afin de les contourner. Ceci permet de répartir le trafic routier, de réduire le temps du voyage des conducteurs et d'économiser sur les consommations de carburant. Un exemple d'application de gestion du trafic routier est illustré dans la figure 2.1.

Même si un véhicule équipé d'un GPS et disposant d'une carte est capable, à lui seul, de calculer le meilleur trajet à suivre, les performances de ces applications sont meilleures lorsque leurs mises à jour sont en temps réel, soit lorsqu'un véhicule reçoit des informations d'actualité concernant le trafic routier, de la part d'une unité de bords de route ou de celle des autres véhicules à proximité. Ces applications ont pour but d'assister le conducteur lors de sa conduite. Leurs critères en terme de qualité de services sont moins restrictives que pour les applications de sûreté, mais tout de même similaires, à savoir, un certain taux de réception doit être garanti [15].

2.3.3 Applications de sûreté et de sécurité routière

Les applications de sûreté et de sécurité routière sont les plus importantes des VANETs. Elles ont pour objectif de réduire les risques d'accidents routiers [54][62] [92], en fournissant aux conducteurs des informations pertinentes en temps opportun. Pour ce faire, des données sont collectées par le biais des capteurs des véhicules afin d'être traitées et disséminées sous la forme de messages de sûreté, destinés aux autres véhicules et aux infrastructures potentiellement disponibles, selon le type d'applications [16] [60]. Il existe

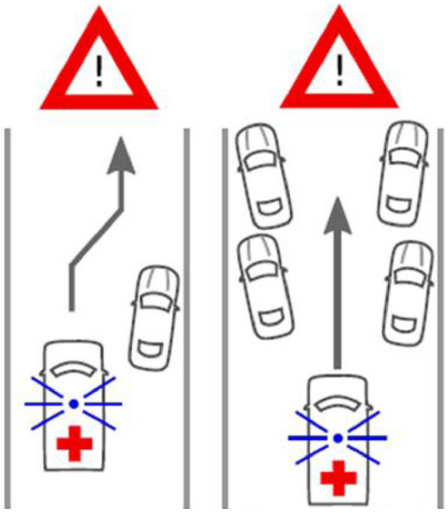


Figure 2.2 – Application d'avertissement pour céder le passage à un véhicule prioritaire [25].

de nombreux types d'applications pour englober les multiples aspects de la sureté et de la sécurité routière, comme la prévention de collisions ainsi que le diagnostic distant pour la maintenance des véhicules [75]. Même si les résultats de cette thèse peuvent s'appliquer à divers type d'applications, c'est les applications de sûreté et de sécurité routière qui ont motivé de nombreux choix dans celle-ci. Ci-dessous, nous présentons donc des exemples de ce type d'applications afin d'en entrevoir les spécificités :

- **Avertissement des risques de collision dans les intersections :** dans ce type de services, les véhicules et infrastructures détectent de possibles collisions entre plusieurs véhicules ne pouvant communiquer entre eux de façon directe. Tout d'abord, le service récupère des informations concernant des véhicules en provenance de différentes directions approchant une intersection, cela à travers des capteurs présents dans l'infrastructure. Ces informations sont analysées et traitées, puis une probabilité d'accident ou de situation dangereuse est calculée, un message d'avertissement est alors disséminé parmi les véhicules se trouvant près de l'intersection, afin de les prévenir du danger.

- **Avertissement d'un véhicule d'urgence à l'approche :** l'objectif de cette application est de fournir une voie libre aux véhicules d'urgence et donc de leur libérer le passage. Dans ce service, des messages d'alerte sont disséminés par le biais de communications unidirectionnelles entre véhicules circulant sur la même voie que le véhicule d'urgence. Les messages contiennent des informations relatives à la vitesse du véhicule d'urgence, à sa direction, à la voie sur laquelle il circule et au chemin suivi. Un exemple est illustré dans la figure 2.2.

- **Services de secours :** le service de secours est utilisé pour alerter en cas de situations potentiellement critiques. Dans le cas d'un accident, par exemple, un signal S.O.S peut être déclenché automatiquement par le service ou par un conducteur. Le signal est ensuite acheminé jusqu'à une infrastructure, en utilisant des communications véhicule à véhicule (V2V) et véhicule à infrastructure (V2I).

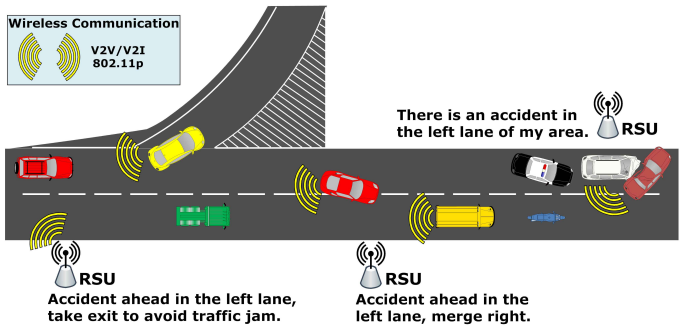


FIGURE 2.3 – Application de sûreté et de sécurité routière [3].

– **Avertissement d'incidents :** cette application vise à prévenir des incidents potentiels suite à une situation dangereuse. Par exemple, s'il y a du brouillard sur la voie, un véhicule en panne, suite à des problèmes mécaniques ou à un accident, envoie des messages d'avertissement aux véhicules à l'approche circulant dans la même direction ou en direction opposée, en utilisant des communications V2V et V2I, afin de les informer de sa situation et de sa localisation. Un exemple de cet application est illustré dans la figure 2.3.

– **Avertissement coopératif pour les incidents :** l'objectif de ce type de services est d'alerter les conducteurs sur les accidents survenus et ceux susceptibles de se produire en raison des conditions du moment. Le service se base sur des communications V2V multi-sauts, afin de partager les messages et d'informer les conducteurs. Ces messages peuvent contenir des données sur la position, la direction, la vitesse et l'accélération des véhicules, afin de les échanger avec les véhicules aux alentours et d'éviter ainsi les risques d'accident.

– **Avertissement sur les conditions de la route :** ce service est chargé de prévenir les véhicules sur les conditions dangereuses de la route, qui sont dues au verglas ou autres présence de substances glissantes sur la chaussée. Les capteurs embarqués dans chaque véhicule récupèrent les informations sur l'état de la chaussée afin d'en avertir le conducteur et d'envoyer des messages aux autres véhicules.

– **Feux de stop d'urgence électronique :** ce service vise à prévenir les autres véhicules d'un éventuel besoin de freinage immédiat, comme dans le cas où la visibilité est faible à cause de la présence d'épais brouillard, les feux de stop n'étant pas suffisamment perceptibles pour alerter les voitures circulant dans le même axe routier. En utilisant les communications V2V, les véhicules peuvent disséminer ces informations entre eux de manière collaborative.

– **Automatisation collaborative des autoroutes :** ce service contrôle la position et la vitesse des véhicules par le biais de communications V2V et V2I, afin de les faire circuler en groupe sur une autoroute. Le service collecte des informations sur les véhicules et les fusionne avec des données cartographiques, afin de contrôler les mouvements des véhicules et améliorer la circulation.

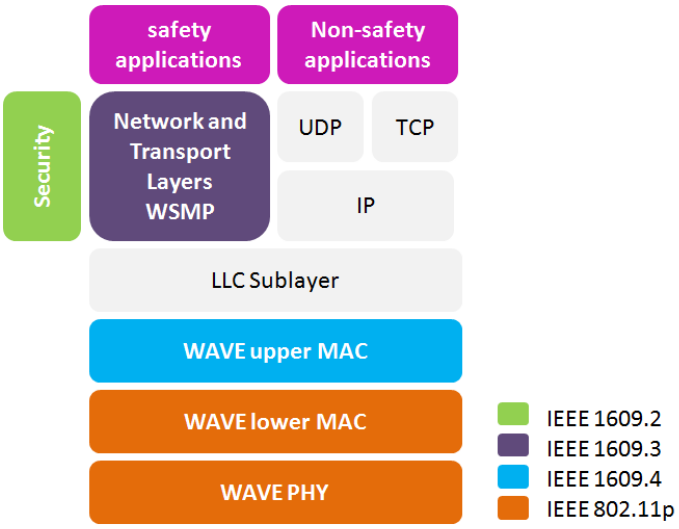


Figure 2.4 – La pile protocolaire WAVE.

Il existe deux types de messages pouvant être disséminés par des applications de sûreté et de sécurité routière [77]. Les *messages périodiques*, ceux-ci contiennent des données importantes, qui ont pour but d'aider les véhicules à décider des actions nécessaires pour prévenir l'apparition de situations dangereuses sur la route. Ces messages nécessitent d'être disséminés fréquemment, ce qui peut engendrer un gaspillage de la bande passante allouée aux communications sans-fil. Le deuxième type de messages disséminés est celui des *messages évènementiels*, ce sont des messages prioritaires, envoyés uniquement lors de détection de conditions dangereuses. Ces messages contiennent la localisation de l'expéditeur, le type d'évènement et une estampille temporelle. Ces messages doivent être délivrés rapidement, soit moins de 100 ms, aux autres véhicules afin de tirer un bénéfice de leur contenu [75]. Comme énoncé précédemment, dans cette thèse nous nous intéresserons tout particulièrement aux applications de sûreté et de sécurité routière collaboratives. Car celles-ci possèdent des contraintes fortes en termes de délai d'acheminement des messages et de qualité de services.

2.4 Normes et standards

Le standard DSRC [9] a été conçu spécifiquement pour les communications au sein des VANETs. Pour cela, des fréquences radios ont été spécifiquement dédiées par la Commission Fédérale des Communications (FCC) aux USA et par l'institut européen des normes de télécommunication (ETSI) [10] et la Conférence Européenne des administrations des Postes et Télécommunications (CEPT) [5] en Europe. Aussi une famille de protocoles IEEE 1609 a été proposée, au sein de la pile protocolaire Wireless Access in Vehicular Environments (WAVE) [102], gérant l'accès sans-fil dans les réseaux véhiculaires. WAVE, représentée dans la figure 2.4, est composée de :

- **IEEE 802.11p** qui décrit les couches physique et MAC, correspondantes aux environnements VANETs.
- **IEEE 1609.1** qui décrit le service de gestion des ressources et définit le format des messages au niveau applicatif.

- **IEEE 1609.2** qui décrit les services de sécurité, comme le format des paquets et les fonctions de chiffrement et d'authentification.
- **IEEE 1609.3** qui décrit les fonctions des couches réseau et transport tel que l'adressage et le routage. Il inclut aussi le protocole Wave Short Messages Protocol (WSMP) pour les communications inter-véhicules, qui est une alternative à l'IPv6.
- **IEEE 1609.4** qui introduit le mode d'accès multi-canal à la couche physique de l'IEEE 802.11p.

Le standard IEEE 802.11-2012 [14], anciennement nommé IEEE 802.11p [11], introduit de nouvelles spécificités à la couche physique, ainsi qu'à la sous-couche MAC, afin d'améliorer la communication dans les VANETs. L'IEEE 802.11p utilise le canal de communication DSRC [9], Dedicated Short Range Communication, qui est spécialement conçu pour les applications à portée moyenne et sensibles au délai, afin de s'adapter à la mobilité des véhicules et de proposer un faible taux d'erreurs, à savoir 10^{-6} lors d'une vitesse de 160 km/h. Le débit proposé varie de 3 Mbit/s à 27Mbit/s, avec une portée de transmission théorique allant jusqu'à 1000 mètres. Par ailleurs, l'utilisation d'accusé de réception (ACK) est ainsi non utilisée pour l'envoi de données par diffusion, afin de réduire la charge du canal de communication. Cependant, le taux de délivrance des messages peut en souffrir, car un véhicule source n'a plus aucune garantie par rapport à la réception de son message.

2.4.1 Couche physique : IEEE 1609.4

L'allocation des canaux est standardisée par la norme ETSI [10] et l'organisation CEPT [5] en Europe. Une largeur de bande de fréquences égale à 30 MHz est attribuée sur le spectre $5.875 - 5.905$ GHz [59], utilisant la technique de transmission OFDM sur DSRC. Tout comme l'ETSI, la commission fédérale de communication (FCC) est responsable de l'allocation des bandes de fréquences aux États-Unis. Cependant, celle-ci a attribué une largeur de bande plus large, égale à 75 MHz sur le spectre $5.850 - 5.925$ GHz.

Les spécifications DSRC de la FCC proposent sept canaux différents de 10 MHZ chacun, comme illustré dans la figure 2.5. Ces sept canaux comprennent un canal de contrôle (CCH) et six canaux de service (SCH). Dans la norme américaine [6], le rôle du canal de contrôle se limite à la transmission des messages de gestion du réseau, comme le basculement entre canaux et les annonces de services. Les canaux de services ont chacun un rôle différent, les canaux 172 et 184 sont dédiés aux applications de sécurité publique. Alors que dans la norme européenne [10], le canal de contrôle est dédié principalement aux messages de sécurité routière et les six canaux de service sont dédiés aux restes des applications. Tout au long de nos travaux, nous considérons le CCH comme étant réservé principalement aux applications de sûreté et de sécurité routière.

Au niveau de la sous-couche supérieure MAC de la pile protocolaire WAVE, un mécanisme de multi-canal est proposé, comme illustré dans la figure 2.6. Il divise un intervalle de synchronisation, d'une durée de 100 ms, en deux temps égaux de 50 ms. Le premier d'entre eux est réservé à l'envoi de messages de sûreté sur le canal CCH, dans le but de maximiser la réception de ces messages prioritaires, ainsi qu'à la transmission des messages de gestion du réseau, pour ordonnancer le basculement entre canaux par exemple. Durant le deuxième intervalle, les véhicules sont libres de choisir leur canal d'écoute. Afin de permettre le changement de canal d'écoute, un intervalle de garde de 4 ms est déclenché. Durant celui-ci, le canal est considéré comme occupé et aucun véhicule ne peu transmettre de message.

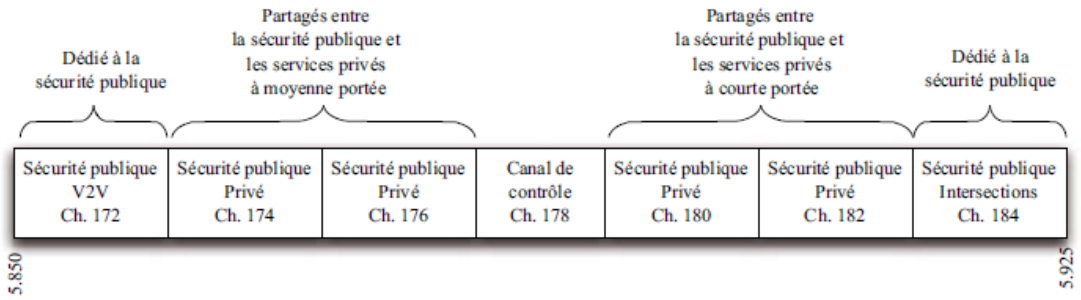


Figure 2.5 – Les sept canaux du standard IEEE 802.11p/WAVE [81].

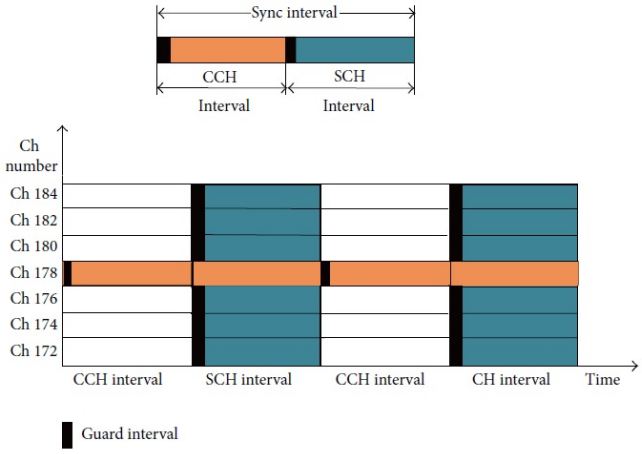


Figure 2.6 – Mécanisme du multi-canal [55].

2.4.2 Couche MAC : EDCA

La sous-couche MAC du standard IEEE 802.11p utilise le mécanisme de contrôle d'accès Enhanced Distributed Channel Access (EDCA) [7], proposé dans le standard IEEE 802.11e [8] pour introduire la différence de service lors de l'accès au canal, via l'utilisation de quatre catégories d'accès (ACs). Chacune de ces ACs : "Voix", "Vidéo", "Best Effort" pour les applications standards et "Background" pour le reste des applications. Cette dernière nécessite le moins de qualité de service. Ces catégories sont aussi nommées AC3 , AC2, AC1 et AC0 dans l'ordre. Chacune d'elles dispose de ses propres valeurs de paramètres pour la taille minimum et maximum de la fenêtre de contention, CW_{min} et CW_{max}, ainsi que le nombre d'espacement temporel entre trames, AIFSN. Ces valeurs sont données dans le tableau 2.1, où CW_{min} est égal à 15 et CW_{max} est égal à 1023 d'après le standard [11]. La valeur du paramètre AIFSN[AC] permet de calculer le temps qu'un message de catégorie AC doit attendre avant de lancer son backoff, soit le temps "Arbitration Inter-Frame Space" (AIFS) calculé avec l'équation (2.1), où la valeur de $SIFS$ est égale à $32us$ et la durée d'un slot time, $SlotTime$, est égale à $13us$. Plus les valeurs de $CW_{min}[AC]$, $CW_{max}[AC]$ et $AIFSN[AC]$ sont petites et plus la catégorie est prioritaire car l'accès au canal est plus rapide.

$$AIFS[AC] = SIFS + AIFSN[AC] \times SlotTime \tag{2.1}$$

Dans le standard IEEE 802.11p, la valeur du paramètre "TXOPLimit" est égale à 0

TABLE 2.1 – Paramètres par défaut d'EDCA dans le standard IEEE 802.11p.

AC	$CW_{min}[AC]$	$CW_{max}[AC]$	$AIFSN[AC]$
$AC0$	CW_{min}	CW_{max}	9
$AC1$	CW_{min}	CW_{max}	6
$AC2$	$(CW_{min}+1)/2-1$	CW_{min}	3
$AC3$	$(CW_{min}+1)/4-1$	$(CW_{min}+1)/2-1$	2

pour toutes les catégories d'accès. Le paramètre TXOPLimit représente un intervalle de temps durant lequel un véhicule a le droit d'émettre en continu les messages d'une même catégorie, sans repasser par un contrôle d'accès au canal. Avec une valeur égale à zéro, les véhicules ne peuvent envoyer qu'un seul message à la fois.

2.5 Techniques de dissémination

Une solution de dissémination efficace pour les VANETs doit absolument prendre en considération les caractéristiques de ces dernières, comme la taille du réseau, la vitesse des véhicules, la connexion intermittente du réseau qui cause son partitionnement en de nombreux ilots, ainsi que les différents besoins des applications en terme de qualité de service. Dans la littérature, plusieurs stratégies ont été proposées. Chacune d'elles, peut nécessiter un ou plusieurs sauts pour l'acheminement de ses données, ainsi que le déploiement ou non d'infrastructure, comme les unités de bords de route (RSUs). Néanmoins, toutes les stratégies se basent sur la coopération des véhicules du réseau pour relayer les messages. C'est pour cette dernière raison qu'une multitude de modèles incitatifs ont été proposés en parallèle aux stratégies de diffusion, comme il est illustré dans la figure 2.7. En plus de la motivation des véhicules à coopérer, il existe un deuxième mécanisme, complémentaire au précédent, dont l'objectif est d'attester de la validité des messages reçus et d'exclure du réseau les véhicules dont le comportement est malicieux. Ci-dessous, nous détaillerons les différentes stratégies de dissémination, les modèles incitatifs, ainsi que les modèles de confiance existants. Ces trois éléments représentent pour nous un ensemble complémentaire de mécanismes qui doivent être mis en place pour l'élaboration d'une solution complète et efficace de dissémination de données dans les VANETs.

2.5.1 Stratégies de dissémination

2.5.1.1 Diffusion

L'une des approches les plus utilisées pour la dissémination de données dans les VANETs est celle utilisant la diffusion. Elle peut être utilisée à un seul saut comme à plusieurs sauts. Un message envoyé par un véhicule émetteur par diffusion est transmis à tous ses voisins directs, puis est retransmis encore une fois par chacun de ses récepteurs, jusqu'à atteindre le (ou les) destinataire(s). Cette approche ne nécessite aucune information préalable sur les voisins du véhicule, ce qui lui permet d'ignorer l'inexistence ou l'inexactitude des informations sur la topologie du réseau. Elle augmente le taux de délivrance et améliore la vitesse d'acheminement des données, car un véhicule destinataire reçoit plusieurs copies du message, arrivant au travers de plusieurs routes. Néanmoins, cette approche augmente aussi la compétition pour l'accès au canal de communication et l'utilisation de la bande passante, ce qui ne lui permet pas le passage à l'échelle au risque de générer une forte congestion du réseau [76].

Les auteurs de l'étude [58] proposent un protocole de diffusion multi-sauts pour les environnements urbains, nommé UMB (Urban multi-hop broadcast protocol), lequel vise

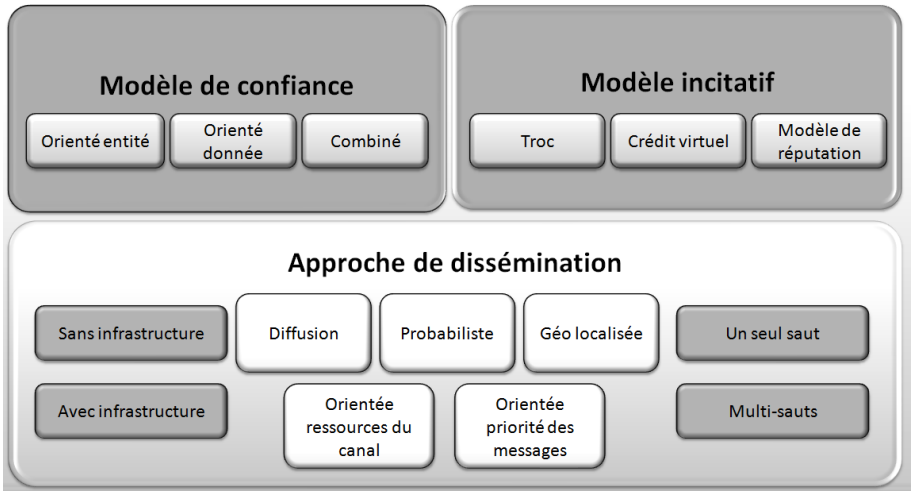


Figure 2.7 – Classification des techniques de dissémination existantes.

à remédier aux problèmes liés à la diffusion massive. Pour l'envoi d'un message, un véhicule émetteur l'envoie par diffusion à ses voisins directs, puis seul le véhicule le plus éloigné le rediffuse. À la rencontre d'une intersection, des véhicules sont sélectionnés comme répéteurs et sont chargés de rediffuser l'information sur les différents segments de l'intersection.

Les auteurs de la solution [98] utilisent la même approche de dissémination. Un message est envoyé par diffusion afin d'atteindre un certain groupe de véhicules. Cependant, à partir de la seconde transmission du message, uniquement les véhicules sur les bords sont sélectionnés comme relayeurs.

Les critères de sélection des relayeurs dans ces deux approches concernent principalement leurs positions géographiques. Ceci n'est pas suffisant pour répondre aux problématiques VANETs, comme par exemple l'adaptation à la densité changeante du réseau, car aucune relation entre le nombre de relayeurs et la densité n'est donnée.

2.5.1.2 Probabiliste

Ce type d'approche, tente de diminuer les messages redondants générés en calculant les probabilités de rencontres entre deux véhicules avant de décider du chemin de dissémination d'une information, sans pour autant nécessiter la connaissance de la topologie du réseau. Un véhicule utilisant cette approche peut se baser sur ses connaissances du réseau, son historique de rencontres avec les autres véhicules, ainsi que sur les informations qu'il a pu collecter sur la mobilité et les localisations des autres véhicules du réseau.

La solution [78] utilise cette approche probabiliste, les décisions concernant les choix des véhicules relayeurs pour la retransmission d'un message se basent sur les probabilités de rencontres du (ou des) véhicule(s) destinataire(s). Alors que dans les solutions [109] et [74], les véhicules récepteurs d'un message calculent eux-mêmes leur probabilité de retransmission, en se basant sur la distance les séparant du véhicule émetteur. Plus cette distance est grande plus leur probabilité de retransmission est importante. Les auteurs de la solution [27] utilisent le critère de la distance entre un véhicule récepteur et un véhicule source pour calculer la probabilité de retransmission et y ajoutent un paramètre concernant la densité locale du réseau, soit le nombre de voisins directes du véhicule récepteur, afin de réduire le nombre de véhicules relayeurs lorsque la

densité est forte.

2.5.1.3 Géographique

Cette approche de dissémination se base sur les informations de localisation des véhicules contenues dans les messages de contrôle, diffusés périodiquement dans le réseau, lorsqu'elle suit une approche pro-active [20], ou alors diffusés à la demande, lors d'une approche réactive [63]. Chaque véhicule tient régulièrement à jour une table contenant l'historique des localisations de ses voisins, afin de pouvoir acheminer ses messages par le chemin le plus court et donc, réduire leur délai d'acheminement. Pour ce fait, lors d'une dissémination, le véhicule le plus proche du (ou des) destinataire(s) est sélectionné lors de chaque saut. Cette approche permet aussi de cibler un groupe de véhicules grâce à leurs coordonnées géographiques, comme font les applications visant à avertir les conducteurs des risques de collision en intersection, par exemple.

2.5.1.4 Orientée ressources du canal

Car les ressources du canal de communication sont limitées, l'accès au canal et l'allocation de ses ressources deviennent un problème d'optimisation. Cependant, ce problème risque d'être NP complet à cause de toutes les variantes qui doivent être prises en considération et du peu d'informations sur le réseau mises à la disposition du véhicule.

Des solutions proposent alors des algorithmes basés sur des heuristiques, tel l'étude [79] qui propose un routage de données accès sur la prise en compte de l'historique des rencontres du véhicule émetteur avec les autres véhicules du réseau. Cela dans le but d'estimer les congestions potentielles ainsi que la densité du réseau, puis de les prendre en considération afin d'améliorer le taux de délivrance et de limiter le nombre de messages doublons. Dans la solution [68], chaque nœud tient une table avec des informations sur le débit et les conditions du canal afin de choisir par quel nœud relayeur il est préférable de transmettre son message. Cependant, ces solutions nécessitent des échanges de messages entre les véhicules pour maintenir un contrôle sur l'utilisation des ressources du canal.

Une autre solution [80], améliore le taux de réception des messages d'urgences en leur allouant une partie de la bande passante disponible. Dans cette solution, chaque nœud envoie en premier un signal sous forme d'impulsion, puis son message d'urgence.

2.5.1.5 Orientée priorité des messages

Pour répondre aux différents besoins en qualité de service des multiples applications des VANETs, des solutions de dissémination proposent une adaptation de la dissémination par rapport à l'importance du contenu des messages échangés. Afin de ne pas supprimer systématiquement tous les nouveaux messages entrants en cas de congestion du réseau. La solution [100] remédie à ce problème en fixant des priorités pour l'accès au canal de communication d'après les catégories d'accès ACs, fixées par EDCA [7], pour chaque message. Une autre solution [42], alloue des jetons aux files d'attente formées par les messages souhaitant l'accès au canal. Elle gère l'accès au canal en pondérant le nombre de jetons offerts par rapport à la densité du canal et à la priorité des messages. Tout comme cette dernière, la solution [86] ordonnance les messages à envoyer sur la base des ressources disponibles du canal et de l'importance du message, en utilisant un système de files d'attentes où une plus grande priorité est donnée aux messages les plus urgents.

2.5.2 Modèles incitatifs à la coopération

La plupart des solutions de dissémination considèrent la coopération des véhicules présents dans le réseau comme acquise, ce qui n'est pas vérifié à cause de la présence potentielle de véhicules égoïstes. Ces derniers préfèrent réserver leurs ressources uniquement pour leurs besoins personnels et refusent donc les demandes de retransmission des messages de leur voisins. Cet attitude baisse l'efficacité des solutions à acheminer les données dans les VANETs. Pour cette raison, il est primordial d'accompagner une solution de dissémination de données par un modèle incitatif à la coopération, afin de s'assurer de la participation de tous les véhicules à la retransmission des données. Trois approches peuvent être utilisées pour motiver les véhicules à coopérer [21] :

2.5.2.1 Le Troc

Dans cette approche, chaque véhicule tient une table retraçant le comportement des autres véhicules à son égard, un véhicule n'accepte de coopérer et de retransmettre le message d'un autre à la condition de réciprocité que ce dernier ait déjà fait de même [17]. Cependant, la forte mobilité des véhicules et les changements fréquents de topologie dans les VANETs ne permettent pas l'établissement de solides relations entre les véhicules, ce qui peut affaiblir les performances de cette approche.

2.5.2.2 Les crédits virtuels

La majorité des modèles incitatifs utilisent des crédits virtuels qui servent à monétiser la coopération des véhicules. Chaque transmission de message fait bénéficier le véhicule relayeur d'une récompense donnée par le véhicule émetteur. Le maintien d'un tel système nécessite le déploiement d'infrastructures ou la disposition dans les véhicules d'équipements spécifiques, afin de gérer le calcul et la distribution des récompenses [28][29]. Les limites de cette approche concernent le calcul des coûts et récompenses, qui souvent peut être basé sur des estimations, ainsi que sur la distribution des crédits, qui peut souffrir de la mobilité des véhicules.

2.5.2.3 Les modèles de réputation

Cette dernière approche mesure la coopération des véhicules à travers des réputations, chaque véhicule relayant un message verra sa réputation mise à jour par le véhicule émetteur. Une réputation de haute valeur ouvre l'accès à des privilèges sur le réseau [24]. Tout comme l'approche basée sur le troc, celle-ci souffre de la mobilité et des changements de topologie dans les VANETs qui ne permettent pas la construction fiable de réputation.

2.5.3 Modèles de confiance

Les solutions proposées aux problématiques de dissémination de données dans les VANETs, se sont souvent intéressées aux aspects quantitatifs pour améliorer le taux de délivrance et réduire les délais, mais sans forcément évaluer la qualité des informations échangées. À cause de la présence de véhicules malicieux dans ces réseaux, des messages

altérés peuvent être disséminés. Les objectifs d'un modèle de confiance consistent à établir des relations de confiance entre les membres d'un réseau, de détecter et d'exclure les véhicules malicieux. Cependant, ces objectifs sont mis à mal à cause du large espace où peut s'étaler un VANET, en plus de sa nature décentralisée, éparpillée, ouverte et très dynamique [111]. Une partie de ces modèles proposent des mécanismes de révocation par l'utilisation de certificats, afin d'exclure les véhicules malicieux, mais pour ce faire nécessite l'existence d'infrastructures [87]. Nous détaillons ci-dessous les trois approches utilisées pour la mise en place d'un modèle de confiance ne nécessitant pas forcément d'infrastructure :

2.5.3.1 Orienté entité

Dans cette approche, la notion de confiance lors de la réception d'une information vise le véhicule émetteur. La solution [43] prône un modèle de confiance sociologique [43], celui-ci consiste à faire confiance ou non à un autre véhicule d'après la situation où ils se trouvent, le niveau d'optimisme du véhicule, ainsi que le système et les garanties que celui-ci propose. Une autre solution [71], s'intéresse aussi à la confiance accordée au véhicule émetteur, mais par l'utilisation de multiples aspects le concernant. Cette solution attribue des rôles et des réputations à tous les véhicules du réseau, afin de pondérer la véracité de leurs dires par ces deux valeurs.

2.5.3.2 Orienté donnée

À l'encontre de la première approche, celle-ci accorde de la confiance à un message par rapport à son contenu, indépendamment de son émetteur. Les auteurs de l'étude [88] proposent un modèle de confiance basé sur cette approche afin de remédier aux problématiques liées aux connexions éphémères dans les VANETs, qui empêchent l'établissement de liens de confiance entre les véhicules. Pour ce faire, un véhicule consulte les rapports émis par les autres concernant une information reçue avant de l'accepter ou de la refuser. Chacun de ces rapports est pondéré par rapport à plusieurs métriques de confiance, comme son lieu et sa date d'émission. Ces rapports et leur poids servent à décider du degré de confiance à accorder à l'information reçue.

2.5.3.3 Combiné

La troisième approche combine les deux premières. Elle utilise les degrés de confiance attribués aux véhicules pour distribuer à son tour des degrés de confiance aux informations reçues. La solution [36] instaure ainsi un nouveau modèle de réputation distribué. Chaque véhicule recevant un message, y insère son avis sur la validité de son contenu avant de le retransmettre. Ces avis permettent aux véhicules récepteurs de choisir le degré de confiance à donner au message et de mettre à jour les réputations des autres véhicules par rapport aux avis donnés.

2.6 Les problématiques dans les VANETs

Les VANETs ont l'avantage de ne pas être conditionnés par les problématique liées à l'espace mémoire, à la capacité de calcul et à l'énergie. Cependant, ils souffrent de l'imposante quantité de données à envoyer et de l'étendue des zones géographiques à couvrir. Celles-ci combinées à la dispersion et la forte mobilité des véhicules, à l'absence ou à l'insuffisance d'infrastructure, ainsi qu'à la densité variable du réseau, créent plusieurs problématiques à la dissémination des données. Ci-dessous nous listons quelques-unes :

- **Problématiques liées à la densité variable et aux connexions sporadiques :** la densité des véhicules dans un VANET est très variable, elle peut être très faible, comme dans le cas d'une route de campagne à faible fréquentation ou très forte dans un réseau urbain fortement encombré. Ceci a un impact sur le taux de délivrance et les délais de l'acheminement des données. En effet, dans les situations de faible densité, les déconnexions sont fréquentes, ce qui peut causer de longs délais de transmission et de faibles taux de livraison de messages. De façon similaire, au cours de situations avec de forte densités, la concurrence pour l'accès au canal de communication est forte, causant des collisions de messages et donc beaucoup de pertes et de faibles taux de délivrance de messages [60][35]. Nous proposons de résoudre les problématiques liées aux densités changeantes lors d'une dissémination de message dans le chapitre 3, par la proposition d'une stratégie de dissémination adaptative.

- **Partage des ressources du canal :** les VANETs ne disposent pas coordinateur pour l'allocation de la bande passante aux véhicules. Il devient alors de la responsabilité de chaque véhicule de gérer, de manière équitable, ces ressources. Ceci peut augmenter les temps d'attentes avant l'accès au canal et donc la latence des messages. Nous avons proposé un ordonnanceur distribué pour l'envoi des messages dans un VANET dans le chapitre 4, pour utiliser équitablement et efficacement les ressources du canal.

- **Établissement de relations de confiance :** la problématique de la modélisation de la confiance pour les membres d'un VANET est délicate et unique en son genre. Dans certains scénarios, les véhicules circulent à des vitesses très élevées, comme sur une autoroute, les réactions des conducteurs devant des situations dangereuses et imminentes doivent être rapides et efficaces, ce qui rend la vérification en temps réel de la fiabilité des informations provenant d'autres véhicules nécessaire mais non triviale. En effet, les VANETs sont des systèmes *décentralisés* et *ouverts*, souvent sans infrastructures dédiées. Les membres peuvent rejoindre ou quitter les ilots composant le réseau voir le réseau lui-même sans passer par une entité centrale. Par conséquent, le mécanisme de confiance à utiliser doit être distribué par essence [111]. Nous proposons un modèle de confiance distribué, ne nécessitant pas le déploiement d'infrastructures, dans le chapitre 5 pour résoudre ce problème.

- **Incitation à la coopération :** la dissémination de données dans les VANETs est effectuée, le plus souvent, de manière collaborative, afin de remédier à la non présence constante d'infrastructure et de supporter la mobilité des véhicules. Pour cela, il est primordial que les véhicules acceptent de coopérer et de transmettre les messages de leurs voisins. Nous apportons de l'incitation à la coopération dans un VANET par

notre modèle de confiance, qui est aussi un modèle incitatif.

– **Le passage à l'échelle :** Le nombre de véhicules croît de manière significative. La quantité d'information collectée et échangée au sein des VANETs fait de même. Cela impose que toute solution proposée pour les VANETs considère dés sa conception la problématiques du passage à l'échelle. Pour cette raison, nous veillons particulièrement à ce que toutes les réponses que nous apportons aux problématiques VANETs supportent le passage à l'échelle.

2.7 Conclusion

Les VANETs ont la capacité de supporter une multitude d'applications, allant de simples applications de confort à d'autres plus importantes comme celles visant la sûreté et la sécurité routières. Ces applications nécessitent des stratégies efficaces pour la gestion des ressources du canal de communication, de la qualité de service et de la sécurité des communications, entre autres. Cependant, même si l'on peut considérer les VANETs comme un sous-ensemble ou un cas spécifique des MANETs, les solutions existantes pour ces dernières ne sont pas applicables comme telle aux VANETs, à cause de leurs caractéristiques particulières. Il existe donc de nombreuses problématiques de recherche dans le domaine des VANETs. Dans cette thèse, nous nous intéresserons à celles liées à la dissémination des données, à l'accès au canal de communication, à l'incitation des véhicules à la coopération et à la confiance envers le contenu des messages.

Chapitre 3

Les messages sont-ils tous égaux face à leur dissémination ?

Sommaire

Tout au long de ce chapitre, nous nous sommes intéressés à la problématique de la dissémination des données dans les réseaux ad hoc véhiculaires (VANETs). Cette problématique vise à permettre la réception des informations envoyées par tous les véhicules concernés, tout en respectant les durées de validité de celles-ci. La condition est de ne pas inonder le réseau de doublons ou d'informations inutiles, comme cela peut être le cas durant une diffusion générale. L'acheminement de données doit faire face aux difficultés induites par la densité variable du réseau, la forte mobilité des véhicules, l'absence ou l'insuffisance d'infrastructure, ainsi que l'étendue des zones géographiques à couvrir.

Nous utilisons le concept de “véhicules concernés" par une information. Nous les considérons comme étant l'ensemble des véhicules pour qui cette information est utile car ils se situent à proximité de la zone de détection de l'évènement, pendant que celle-ci est encore significative dans le temps. Nous adaptons l'étendue de la zone géographique de dissémination, ainsi que la durée de validité d'une information pour chaque type de données. Par ce principe, nous caractérisons une information par une classe et un mode, permettant ainsi d'adapter sa stratégie de dissémination. Un compromis, entre le pourcentage de réception lors d'une dissémination et le nombre de messages superflus générés, est décidé pour chaque type de messages. Cette stratégie est validée par une étude analytique au travers d'une modélisation par une chaîne de Markov à temps discret et à espace d'états discret, ainsi que par simulation.

Ce chapitre débute par une introduction du contexte dans la section 3.1, suivie d'un positionnement bibliographique dans la section 3.2. Nous présentons notre solution *ADCD*, qui est une stratégie de dissémination pour chaque type de données, dans la section 3.3. La section 3.4 présente notre modélisation de la solution par une chaîne de Markov, dans le but

d'étudier l'impact de la variation de ses paramètres. L'étude analytique des performances issues de notre modélisation est présentée dans la section 3.5, tandis que les résultats de l'évaluation obtenus par simulation sont donnés dans la section 3.6. Finalement, la section 3.7 conclut ce chapitre.

3.1 Contexte et motivation

La dissémination de données dans les réseaux ad hoc véhiculaires peut être réalisée en unicast, en multicast et en diffusion, afin de correspondre aux types de données partagées. Le mode de dissémination par diffusion est souvent utilisé pour les données des applications de sûreté et de gestion du trafic routier. Ces informations concernent un nombre important de véhicules, d'où la nécessité de les diffuser à plusieurs sauts. Cependant, une diffusion générale et aveugle a comme effet néfaste l'encombrement du réseau, car elle engendre de nombreux duplicatas, ce qui cause des réceptions multiples. Cette approche peut garantir un taux élevé de réception pour une information. Ceci est cependant atteint aux dépends des performances des autres informations à envoyer et en gaspillant les ressources du canal de communication.

Afin d'éviter la congestion du réseau et la perte de messages, nous introduisons une nouvelle stratégie de dissémination de données, qui s'adapte aux types de données à partager. Notre objectif par cette proposition est d'améliorer le taux de réception, tout en diminuant les redondances. Pour cela, nous ciblons lors d'une dissémination uniquement les véhicules potentiellement intéressés par l'information, dans le but d'éviter une utilisation inutile des ressources du réseau.

Notre solution différencie les données collectées d'après leur importance et leur durée de validité. Ces caractéristiques définissent les limitations spatiales et temporelles du processus de dissémination, permettant d'accentuer le partage des informations les plus importantes. En plus des caractéristiques des informations, notre solution prend en considération la densité du réseau et la distribution des véhicules autour, pour choisir le nombre et les identifiants des véhicules relayeurs lors d'une dissémination.

Une modélisation de notre solution au travers d'une chaîne de Markov à temps discret et à espace d'états discret nous permet également de dimensionner les valeurs des paramètres de notre solution de dissémination et d'en étudier analytiquement les performances. Ainsi, nous calculons le taux moyen de réception pour chaque catégorie de messages, le nombre de messages superflus générés, la probabilité qu'une dissémination soit complète et enfin le nombre minimum de sauts nécessaires à chaque envoi. Puis, nous étayons nos résultats analytiques par des simulations et des comparaisons avec d'autres solutions existantes.

3.2 Travaux existants

Plusieurs solutions sont données dans les études [63] et [32], concernant les architectures et protocoles de communication existants pour les réseaux ad hoc véhiculaires. La première regroupe différentes architectures proposées pour connecter des véhicules et former un réseau. Elle présente quelques méthodes de récolte, de stockage et de dissémination d'informations pour différents contextes. Les auteurs concluent leur étude en démontrant le lien entre les performances d'un réseau VANET et certains facteurs majeurs comme : la méthode d'accès sans fil, la densité et mobilité des véhicules, le nombre et la disposition des infrastructures fixes, ainsi que le type d'informations échangées.

La second étude se focalise davantage sur les protocoles de communication. Ses auteurs détaillent les techniques de transmission par diffusion, telles que celles basées sur une diffusion générale, celles utilisant une diffusion probabiliste, ainsi que d'autres utilisant des accusés de réceptions et de la géo-localisation. Une deuxième partie de leur travail présente quelques stratégies de routage, comme celles utilisant le routage épidémique ou le routage par contrainte de temps [78].

Pour notre part, nous nous intéressons à comment les véhicules récoltent des données et les partagent au sein du réseau. Nous présentons ici quelques solutions existantes et expliquons leurs limites du point de vue des réseaux ad hoc véhiculaires.

3.2.1 Transmission de données basée sur le critère temporel

Une stratégie de partage de données s'accommode aux types d'information à partager et prend en considération les besoins en qualité de service de l'application concernée. Deux choix sont possibles par rapport au critère temporel, le premier consiste en un envoi immédiat de la donnée récoltée, afin de respecter les contraintes temps réel des applications de sûreté, comme ce fut le cas dans les solutions [41][33]. L'inconvénient d'une telle approche réside en la forte redondance de données induites, d'où une congestion potentielle du réseau. La solution [90] fait partie de cette même catégorie, elle utilise comme les deux solutions précédentes la diffusion pour partager des données, mais en utilisant en plus des accusés de réception et en prenant en considération la localisation du véhicule source. Cela permet de cibler les véhicules destinataires, pour diminuer les envois inutiles. Cette solution attache les accusés de réception aux messages HELLO, envoyés de manière périodique dans le réseau, pour ne pas surcharger le réseau. Cependant, ceci introduit un délai supplémentaire à la réception d'un accusé de réception et donc à l'acheminent d'un message.

La seconde catégorie temporise l'envoi des messages, comme dans la solution MobEyes [65][66][64]. Dans celle-ci les véhicules échangent, à des intervalles réguliers, les résumés des données capturées tout au long de leurs déploiements, dans le but de réduire la quantité de données envoyées et de n'envoyer un message que s'il peut intéresser son récepteur. Toutefois, cette solution est incompatible avec les besoins des applications temps réel, à cause de ses délais et du risque qu'une dissémination reste inachevée.

Avec la même approche, la solution [78] propose de choisir le moment opportun à l'envoi d'une information d'après le calcul d'une probabilité de délivrance, tel que la distance séparant le véhicule source et les véhicules destinataires est prise en compte, en plus de la durée de validité de l'information. Le véhicule source choisit d'envoyer le message à un véhicule relais pouvant avoir une plus grande probabilité de délivrance que lui ou alors d'attendre. L'attente s'arrête lorsque le véhicule rencontre le destinataire ou lorsqu'il rencontre un véhicule relais avec une meilleure probabilité de délivrance. Comme beaucoup de solutions, cette dernière suppose l'existence d'unités de bords de route (RSUs), qui déterminent pour chaque information les véhicules récepteurs.

3.2.2 Transmission de données basée sur le type de données

Certaines stratégies de dissémination de données s'adaptent aux types d'informations qu'elles partagent en les classifiant d'après leur importance, leur délai d'acheminement toléré, ainsi que leur débit nécessaire. La première classe est composée de messages d'urgence, comme les notifications d'accidents. Ces messages sont courts, mais nécessitent une grande vitesse de propagation pour assurer un service temps réel [22] [73]. La deuxième classe est constituée de messages d'alerte pour attirer l'attention d'un conducteur, comme

les messages d'aide à la conduite. Ces messages sont moins importants que ceux de la première catégorie, mais requièrent néanmoins un haut débit pour leur envoi. La dernière catégorie comprend les messages concernant la conduite collaborative, qui informent par exemple sur la densité et la vitesse moyenne d'une route. Ces messages sont les moins gourmands en terme de qualité de service. Malgré cette classification pour chaque type de messages, la question sur son utilisation dans une stratégie de diffusion reste vague.

L'étude [19] propose une autre classification des données moins classique. Les auteurs prennent en considération les critères suivants pour chaque donnée à envoyer : l'espace, le temps et l'intérêt du conducteur. Une information est alors caractérisée par rapport à la zone géographique de sa dissémination, la durée dans le temps de sa validité et le type de conducteurs qui seraient intéressés par elle. Les auteurs supposent l'existence d'unités de bords de route qui se chargeraient de l'établissement de ces caractéristiques et de la transmission des données.

Notre solution *ADCD* [49][50] préconise l'envoi immédiat des données récoltées, afin de respecter les contraintes temps réel des applications de sûreté. Un pré-traitement de la donnée est effectué pour éviter la redondance des envois et limiter les diffusions répétitives. Ceci est réalisé en prenant en considération les caractéristiques spatiales et temporelles des données à envoyer, ainsi que leur intérêt auprès des conducteurs. Ainsi, nous proposons une stratégie de dissémination adaptée pour chaque type de données, pour assurer des délais d'acheminement très courts et des taux de réception élevés, mais sans pour autant nécessiter d'infrastructure.

3.3 ADCD : stratégie de dissémination adaptée aux données classifiées

Notre solution *ADCD* a pour objectif de transmettre les bonnes informations aux bons véhicules et particulièrement lorsqu'il s'agit d'informations de sûreté. *ADCD* ne suppose pas l'existence préalable d'unités de bords de route. Nous supposons ici que certains véhicules sont dotés de capteurs, afin de récolter les informations à partager. Aussi, que tous les véhicules acceptent de coopérer en partageant leurs données collectées et en acceptant également d'assurer des retransmissions en cas de demande. Cette stratégie permet une récolte régulière des données et une diffusion adaptée, dans le but d'éviter les risques de congestion et de famine dans les zones éloignées.

Nous considérons que chaque véhicule doit recevoir les informations locales liées à sa route, ainsi que les informations d'urgence récoltées dans un certain périmètre, qui soit plus large que pour les informations locales, tout en respectant une certaine durée de validité pour les données. Ceci, afin qu'un conducteur soit toujours au courant des conditions actuelles du trafic routier.

La stratégie de dissémination d'*ADCD* se base sur trois étapes :

- La récolte et la classification des données.
- L'élection des véhicules relayeurs et l'envoi du message.
- La retransmission itérative du message, d'après les caractéristiques de son contenu.

3.3.1 Récolte et classification des données

Un véhicule peut être équipé de différents capteurs et collecter divers types de données. Nous considérons que chaque information dépend de son lieu de collecte et que sa diffusion n'a de sens qu'aux alentours, cela durant une période de temps limitée afin d'éviter le partage d'informations obsolètes.

Table 3.1 – Caractéristiques des données échangées.

Information	Classe	Mode
Accident	5	3
Embouteillage	4	4
Glissement de terrain	3	5
Risque de dérapage	3	4
Voiture en panne	3	2
Travaux sur la route	3	5
Feux de circulation en panne	2	3
Densité des véhicules dans une route	1	2
Nombre de véhicules voisins	1	1

Nous caractérisons chaque information par deux paramètres : la *classe* et le *mode*. La classe d'une information représente son niveau d'importance, elle définie l'étendue géographique de sa zone de dissémination, alors que son mode définit l'échelle de sa durée de validité dans le temps.

ADCD propose un intervalle $[\sigma_{min}, \sigma_{max}]$ pour les paramètres classe et mode. L'information la plus urgente se voit attribuer la valeur maximale pour sa classe et de même concernant le mode d'une information dont la validité dans le temps est la plus longue. Pour illustrer notre approche, nous proposons dans le tableau 3.1 une caractérisation de quelques informations pouvant être échangées dans des applications de sûreté et de gestion du trafic routier.

Nous considérons qu'un véhicule est concerné par la réception d'une information uniquement s'il se trouve dans sa zone de transmission, laquelle est déterminée par sa classe, durant sa période de validité, qui est déterminée par son mode. Pour pouvoir cibler ces véhicules, nous considérons des zones de dissémination de forme carrée au tour du point de collecte de chaque information à distribuer, de sorte que l'échelle de la taille de chaque coté du carré corresponde à la classe de l'information. Pour l'exemple donné dans le tableau 3.1, nous associons les tailles suivantes pour chacune des cinq classes possibles, dans l'ordre : $200 \times 200m^2$, $300 \times 300m^2$, $400 \times 400m^2$, $600 \times 600m^2$ et $800 \times 800m^2$. À savoir que dans cet exemple nous considérons que des informations concernant la gestion du trafic local, comme la densité locale d'une route, n'ont de sens qu'au sein d'un périmètre de $200 \times 200m^2$. Nous appliquons le même principe pour le mode d'une information.

3.3.2 Dissémination des données

La figure 3.1 illustre le processus à suivre par un véhicule avant le partage d'une donnée. Pour alléger la charge du canal des informations redondantes, les trois conditions suivantes doivent être respectées :

- Le véhicule a récemment collecté des informations, lesquelles sont différentes de ses derniers envois.
- Le véhicule peut retransmettre les mêmes informations une seconde fois si les messages à ce sujet ont atteint leur limite de validité et que l'événement est toujours d'actualité
- Aucun de ses voisins n'a pour l'instant partagé ces mêmes informations.

Une fois ces conditions réunies, un véhicule attend un court instant aléatoire, afin d'éviter les envois simultanés lors de la détection d'un même événement par des véhicules voisins. Si l'information détectée reste différente de celle reçues dernièrement par le

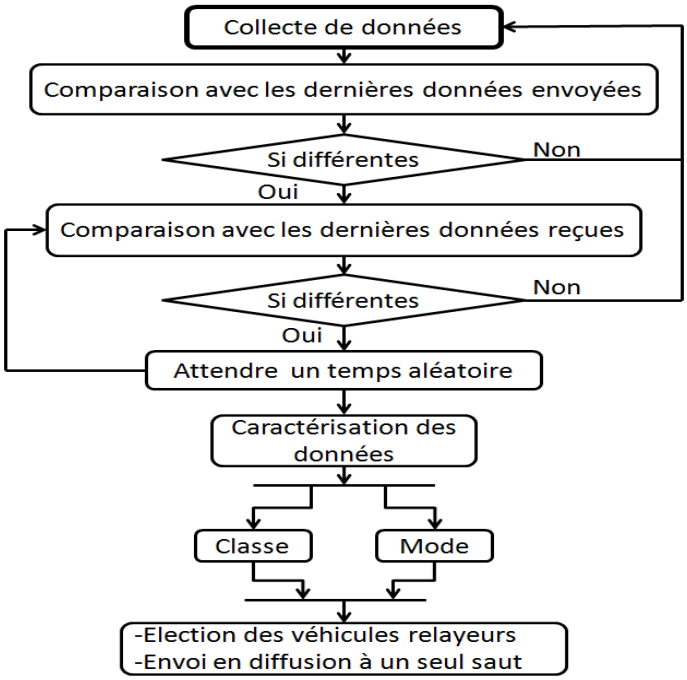


Figure 3.1 – Diagramme de flux pour le partage d'une information.

véhicule, il procède à sa caractérisation en définissant sa classe et son mode, puis incorpore la date et le lieu de collecte de l'information dans le message.

La manière la plus sûre pour que tous les véhicules reçoivent une information est de l'envoyer par diffusion à plusieurs sauts. Cependant, cette méthode cause un phénomène dit de"broadcast storm" [76] et congestionne le réseau. Nous agissons autrement, en effectuant une seule diffusion aveugle à un seul saut, pour que tous les véhicules voisins directs à la source réceptionnent le message. Puis la retransmission de l'information se fait en prenant en considération sa classe et son mode. Le véhicule source est en charge d'élire les relayeurs pour son message parmi ses voisins directs, sachant que chaque véhicule connait tous ses voisins directs avec leurs coordonnées grâce aux messages HELLO échangés périodiquement. Il a aussi connaissance du nombre de voisins de chacun de ses voisins, soit parce que cette information a été ajouté aux messages HELLO ou alors grâce aux messages échangés pour la conduite collaborative.

Une liste de véhicules élus est alors insérée dans le message, afin de limiter son nombre de retransmissions. Le nombre de relayeurs pour un message dépend de l'importance de son contenu, soit la valeur de son paramètre classe. Plus une information est urgente plus sa transmission doit être complète et rapide. Nous choisissons pour l'exemple donné dans le tableau 3.1, une transmission à un seul saut pour les informations de classe 1, soit juste assez pour couvrir la zone de transmission de $200 \times 200m^2$, un nombre de relayeurs élus égal de trois pour chaque saut pour les classes 2 et 3, tant que leurs périmètres respectifs de $300 \times 300m^2$ et de $400 \times 400m^2$ n'ont pas été dépassés. Ces trois véhicules relayeurs sont choisis en prenant en considération le nombre de voisins de chacun d'eux. Ceux qui ont le plus de véhicules à leur portée réseau et donc le plus grand nombre de récepteurs potentiels sont choisis, tout en veillant à bien les répartir autour du véhicule source, avec des positions séparées de 120° pour ce cas de figure. Enfin, nous définissons le nombre de relayeurs élus à quatre pour les classes 4 et 5, nous choisissons ces élus de sorte à couvrir chacune des quatre zones disposées à des angles de 90°.

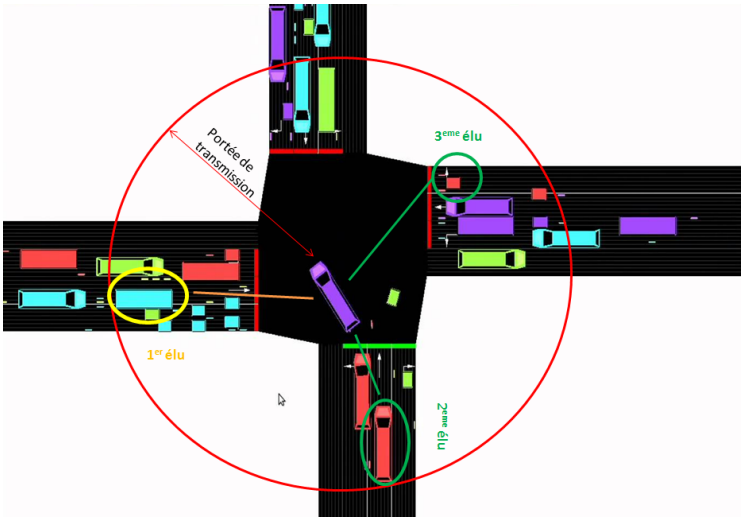


FIGURE 3.2 – Exemple d'élection de trois véhicules pour la retransmission d'un message.

Algorithme 1: Algorithme d'élection.

En entrée : $Nombre\_Elus$
En sortie : $Tableau\_Elus$

$\theta = \frac{360°}{Nombre\_Elus}$
$Y = 1$

$Tableau\_Elus[0]$ = ID du véhicule entouré par la plus forte densité (parmi tous les voisins directs de la source)

while $(Y < Nombre\_Elus)$ **do**
  $Zone[Y]$ = Zone délimitée par (θ, cordonnées du véhicule $Tableau\_Elus[Y-1]$)
  $Tableau\_Elus[Y]$= ID du véhicule entouré par la plus forte densité (dans la zone$[Y]$)
  $Y = Y + 1$
end while

La figure 3.2 illustre un exemple d'élection de véhicules relayeurs pour une information de classe 3. Le premier véhicule relayeur élu est celui avec le plus grand nombre de véhicules à sa portée réseau, nous considérons alors le premier angle à 120° couvert. Pour couvrir les deux angles restants, nous choisissons le véhicule dont le nombre de voisins est le plus important dans chacun d'eux. Ce processus d'élection est représenté par l'algorithme 1, il nécessite en entrée le nombre de relayeurs requis afin de donner en sortie leurs coordonnées.

3.3.3 Retransmission itérative

A la réception d'un message, un véhicule vérifie sa validité par rapport aux caractéristiques spatiales et temporelles de son contenu. Le véhicule compare sa localisation par rapport à la zone de dissémination du message. Celle-ci est calculée par rapport à la classe et aux coordonnées de collecte de l'information. Puis, le véhicule récepteur vérifie si l'information est encore valide dans le temps via son mode et la date de sa collecte. Si le message échoue à une de ces deux vérifications, il se verra éliminé. Sinon le véhicule récepteur prendra en considération l'information et vérifiera s'il est élu pour la retransmission du message. Si oui, il rediffuse le message sans rien changer à ses caractéristiques, mais en actualisant la liste des élus pour la future retransmission. Ceci, à condition que le véhicule élu n'ait pas déjà partagé ces mêmes informations à travers des messages envoyés, qui sont encore valides dans le temps.

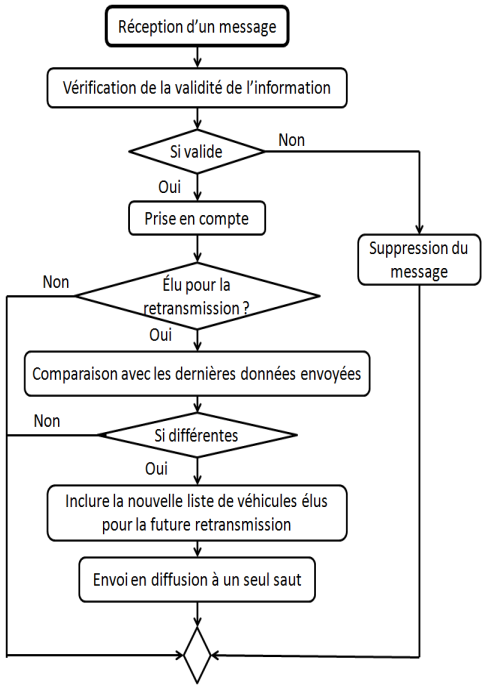


Figure 3.3 – Processus de réception et de retransmission.

ce processus est illustré dans l'organigramme 3.3.

3.4 Modélisation de la stratégie de diffusion par une chaîne de Markov

Nous modélisons le processus de partage de données proposé par *ADCD* par un processus Markovien à temps discret. Il s'agit de modéliser la dissémination d'un message par le véhicule source et sa retransmission par les véhicules élus. Nous modélisons ce processus par une chaîne de Markov à temps discret et à espace d'états discret avec l'utilisation de la loi Binomiale pour définir les probabilités de réception. Nous détaillons chaque partie de notre modélisation ci-dessous.

3.4.1 Description du modèle

Nous considérons un réseau composé de N véhicules mobiles dans un espace clos, où un évènement se produit et est détecté par un véhicule. Celui-ci est alors responsable de son partage avec les autres véhicules du réseau. Nous supposons que tous les véhicules du réseau sont concernés par cette information et souhaiteraient donc la recevoir. Les limites d'une diffusion sont définies par la portée réseau de chaque véhicule, qui détermine si deux véhicules sont voisins ou pas, ainsi que la mobilité qui fait apparaitre et disparaitre fréquemment des liens de connexion réseau entre les véhicules.

Nous modélisons le taux de réception d'une information par tous les véhicules du réseau à travers les états de notre chaîne de Markov. Ces états représentent l'évolution du nombre de véhicules ayant reçu l'information. Les liens de notre chaîne représentent les probabilités de transition d'un état à un autre, soit les probabilités d'évolution du nombre de véhicules informés après chaque étape. Nous considérons une étape comme étant une période (slot) temporelle où un ou plusieurs envois par diffusion sont effectués simultanément.

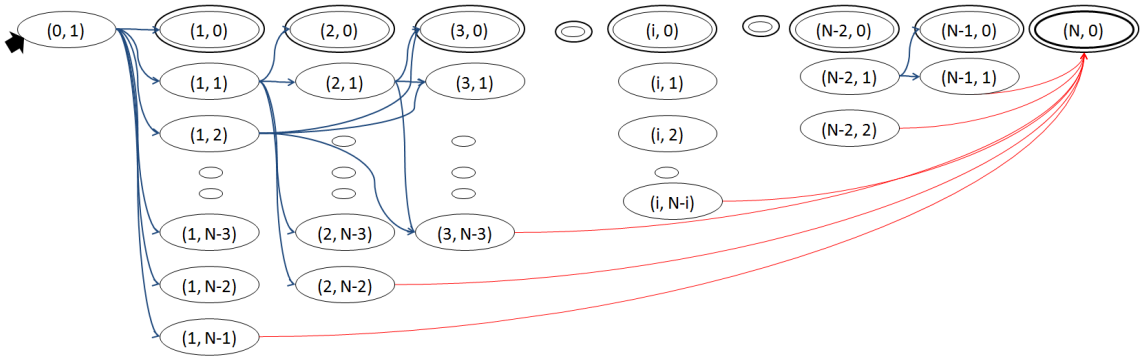


Figure 3.4 – Modélisation du processus de dissémination de données d'*ADCD*, par une chaîne de Markov à temps discret et à espace d'états discret.

3.4.2 Les états

Le protocole *ADCD* ne permet pas la retransmission d'un message plus d'une fois par le même véhicule. Afin de modéliser cette spécificité, nous définissons chaque état de notre modélisation par un couple de valeur (i, j), où $i \in \{0, 1, 2, ..., N\}$, $j \in \{0, 1, 2, ..., N-i\}$ et $i+j \leq N$. La première composante du couple, i, représente le nombre de véhicules ayant déjà reçu l'information et qui l'ont donc retransmise par le passé au maximum une fois (cela dépend de s'ils ont été élus pour la retransmission ou non). La deuxième composante j représente le nombre de véhicules qui viennent tout juste de recevoir l'information, soit durant l'étape elle même. Ce nombre de véhicules j fait parti des véhicules encore non informés, soit $N-i$. Ainsi donc, ils peuvent procéder à la retransmission de l'information à l'étape suivante s'ils sont élus pour.

Le modèle en chaîne de Markov proposé est composée de $1 + \frac{N\times(N+1)}{2}$ états. Ils correspondent à toutes les compositions possibles du couple (i, j) à partir de $i = 1$, soit $\frac{N\times(N+1)}{2}$ états, en plus de l'état initial. Cet état initial est représenté par le couple $(0, 1)$, il représente le cas où le véhicule source vient tout juste d'être informé par l'événement en le collectant par exemple. Dans notre modélisation, il existe plusieurs états finaux et absorbants de la forme $(k, 0)$, où $k \leq N$. Un état final représente le cas où tous les véhicules déjà informés par une information l'ont déjà retransmise s'ils ont été élus pour et qu'il ne reste plus aucun véhicule parmi les élus pour retransmettre l'information. L'état $(N, 0)$ fait partie des états finaux, il représente le cas de figure parfait où tous les véhicules concernés par une information l'ont reçue. La figure 3.4 représente la chaîne de Markov modélisant le processus de partage de données de la solution *ADCD*.

3.4.3 Les transitions possibles entre états

Une transition se produit seulement d'un état (i, j) vers un autre $(i + j, m)$, où $m \in \{0, 1, 2, ..., N - i - j\}$. Elle représente la retransmission potentielle de l'information par les derniers véhicules à l'avoir reçue, dont le nombre est j, ainsi que la réception de l'information pour la première fois par m véhicules.

Pour calculer les probabilités de ce modèle, nous considérons un graphe de connectivité utilisant les probabilités P et Q, comme étant une chaîne de Markov à temps discret avec deux états. Durant le premier état, un véhicule est connecté, alors que durant le deuxième, il ne l'est pas. La probabilité P est celle de passer de l'état déconnecté à celui de connecté, alors que Q représente la probabilité de passer de l'état connecté à celui de déconnecté.

La probabilité stationnaire d'être dans l'état connecté est calculée avec $\pi = \frac{P}{P+Q}$, alors que la probabilité stationnaire d'être dans l'état déconnecté est égale à $\frac{Q}{P+Q}$. La valeur π représente la probabilité de réception pour un véhicule, de la part d'un autre, durant une période (slot) de temps [107]. Elle nous permet aussi de calculer le degré moyen de connexion d'un véhicule avec les autres membres du réseau, soit $\pi \times (N-1)$.

3.4.4 Calcul des probabilités de transition

Le calcul de la probabilité d'une transition de l'état (i,j) vers l'état $(i+j,m)$ est donné dans l'équation (3.1). Nous considérons le processus d'envoi entre deux véhicules comme étant binomial, car un envoi peut amener à un succès ou à un échec. Dans ce processus, nous pouvons avoir jusqu'à j transmissions du message lors de chaque étape temporelle. Le nombre de véhicules m représente les nombre de véhicules ayant reçu l'information pour la première fois. Ce nombre suit une loi binomiale de paramètres n et p, soit $m \sim B(n,p)$, où n est le nombre de véhicules n'ayant pas encore reçu le message, ce qui équivaut à $N-i-j$ dans notre modèle. La probabilité de réception d'un message envoyé par D véhicules, durant la même étape, est calculée avec la fonction de densité de probabilités pour une distribution binomiale Pdf_B. Celle-ci prend en considération la connectivité du réseau π et la probabilité d'envoi avec succès équivalente à $1-(1-\pi)^D$ dans notre cas [107].

$$\begin{aligned} P[(i,j)(i+j,m)] &= Pdf_B(m, 1-(1-\pi)^D, N-i-j) \\ &= \left(\tfrac{(N-i-j)!}{m!\times(N-i-j-m)!}\right) \times (1-(1-\pi)^D)^m \times (1-\pi)^{D(N-i-j-m)} \end{aligned} \tag{3.1}$$

Tel que

$$D = \begin{cases} Nombre\ fixe\ de\ relayeurs\ élus & Si\ D\ >\ j \\ j & Sinon, \end{cases}$$

ADCD utilise une stratégie de diffusion adaptative, qui définit le nombre adéquat de véhicules relayeurs pour chaque type d'information, dans le but de réduire le nombre de messages reçus en double ou inutilement, mais sans pour autant diminuer le taux de réception. Pour étudier les performances d'une telle stratégie, nous incluons dans notre modélisation le paramètre D qui définit le nombre de véhicules relayeurs élus à chaque étape.

Nous représentons les probabilités de transition entre chaque état de notre modélisation dans une matrice M carrée, dont la taille est le nombre d'états possibles dans notre modélisation, soit $1+\frac{N\times(N+1)}{2}$. Chaque case de la matrice, $M[(i,j),(i',j')]$, représente la probabilité d'être dans l'état (i',j'), juste après être passé par l'état (i,j) lors de l'étape précédente.

Un exemple est donné dans la matrice 3.2, pour illustrer les probabilités de transition issues d'une modélisation par une chaîne de Markov d'un partage de données dans un réseau composé de 3 véhicules, avec un nombre de relayeurs fixé à 1, nous avons alors 7 états.

3.5 Étude analytique

Dans le but de sélectionner le nombre adéquat de véhicules relayeurs pour chaque type de messages, catégorisé dans notre modèle par leur classe et leur mode, nous étudions l'évolution du taux de délivrance d'un message dans le temps par rapport à la variation

Table 3.2 – Matrice des probabilités de transition d'une modélisation par une chaîne de Markov, dans un réseau composé de 3 véhicules, avec un nombre de relayeurs fixé à 1.

États	(0,1)	(1,0)	(1,1)	(1,2)	(2,0)	(2,1)	(3,0)
(0,1)	0	$(1-\pi)^2$	$2\pi(1-\pi)$	π^2	0	0	0
(1,0)	0	1	0	0	0	0	0
(1,1)	0	0	0	0	$1-\pi$	π	0
(1,2)	0	0	0	0	0	0	1
(2,0)	0	0	0	0	1	0	0
(2,1)	0	0	0	0	0	0	1
(3,0)	0	0	0	0	0	0	1

du nombre de relayeurs, puis par rapport à la variation de la connectivité π entre les véhicules. Nous approfondissons cette étude en y ajoutant une métrique supplémentaire : la probabilité que l'acheminement soit complet, c.-à-d. que tous les véhicules concernés par le message le reçoivent. Pour finir, nous calculons, pour chaque variation du nombre de relayeurs et de la connectivité, le nombre de messages redondants générés. Nous validerons nos calculs analytiques par une simulation reprenant les mêmes paramètres et métriques.

Les véhicules pouvant être concernés par la réception d'une information dépendent majoritairement de leur localisation à l'instant de collecte de l'information. Dans cette première étude, nous nous concentrons uniquement sur un nombre restreint de véhicules, que nous notons N et qui est égal à 20. Nous considérons que tous ces véhicules sont concernés par ces messages et qu'ils pourront en être les destinataires.

3.5.1 Résultats analytiques

3.5.1.1 Taux de réception

Nous nous intéressons au début de notre étude au taux de délivrance d'une information, qui est une métrique qui concerne tous les types de messages mais avec différents degrés de priorité. Nous calculons le nombre moyen de véhicules, NR, lesquels sont informés par l'information collectée, soit ceux l'ayant reçue plus le véhicule émetteur, cela indépendamment du temps consacré à l'acheminement dans un premier temps. Pour calculer ce nombre, nous commençons par calculer les probabilités de figurer dans chaque état de notre modélisation après τ périodes, sachant qu'une nouvelle émission du message est effectuée par les véhicules ne l'ayant jamais transmis auparavant lors de chaque étape. Ces nouvelles probabilités sont données dans la matrice M à la puissance τ, M^τ. La valeur du paramètre τ est choisie de façon à ce que les probabilités stationnaires du modèle soient atteintes, à savoir que même si on allonge le temps du processus de dissémination, les valeurs de la matrice M^τ ne changent plus. Lors de cette étude analytique, nous attribuons une valeur de 12 au paramètre τ, ceci après plusieurs tests.

En second, nous estimons la moyenne du nombre de véhicules, NR, ayant reçu l'information après τ transmissions par les différents relayeurs. Ce nombre est obtenu à partir de la probabilité de la transition de l'état initial $(1,0)$ à un des états finaux $(k,0)$, après τ périodes. Ces probabilités sont celles de la matrice M^τ. Nous calculons la somme de toutes les probabilités pour k véhicules, parmi les N présents, qui auraient pu recevoir l'information. Puis, nous multiplions, à chaque fois, ces probabilités par le nombre de véhicules k, correspondant. Ce calcul est donné dans l'équation (3.2).

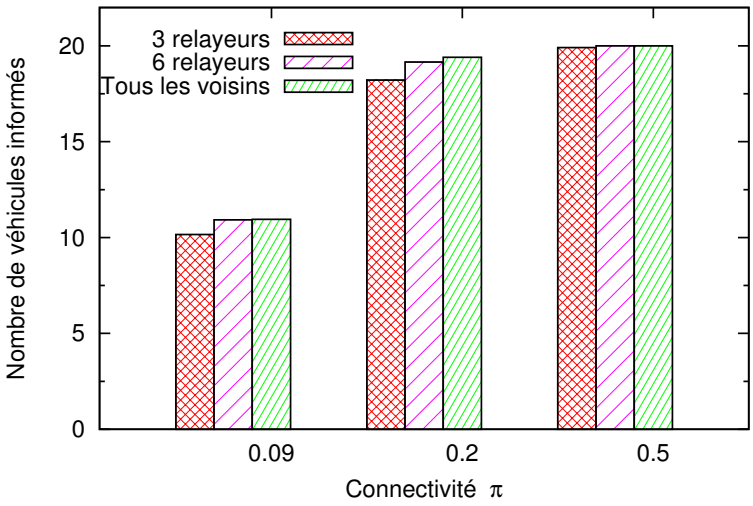


Figure 3.5 – Nombre de véhicules concernés par une information et l'ayant reçue, par rapport à différent nombre de relayeurs et à différente connectivité dans le réseau.

$$NR = \sum_{k=1}^{N} M^{\tau}[(1,0),(k,0)] \times k \tag{3.2}$$

La figure 3.5 illustre les valeurs du nombre de véhicules concernés par une information et l'ayant reçue. Ceci est obtenu dans un premier temps par rapport à la variation du nombre de relayeurs élus D, sa valeur varie entre 3, 6 et tous les voisins. Pour tous les voisins on entend que chaque véhicule venant de recevoir pour la première fois l'information est dans l'obligation de la retransmettre. La variation du nombre de véhicules informés est également calculée par rapport au changement de la connectivité π entre les véhicules. Cette valeur prend les valeurs suivantes : 0.09, 0.2 et 0.5 qui représentent une faible, une moyenne et une forte connectivité dans le réseau.

Nous remarquons que lorsque la connectivité est faible, il est préférable de demander la retransmission du message à tous les véhicules voisins, afin de maximiser la proportion des véhicules recevant l'information. En effet, dans ce cas même si tous les véhicules sont relayeurs, la proportion ne dépasse pas les 55%. Alors que lorsque la densité est moyenne ou forte, avec π égal à 0.2 ou 0.5, le nombre de relayeurs élus peut être restreint à 3 ou à 6, car le taux de délivrance peut atteindre dans ces cas 90% et les différences de taux de réception entre les cas de figure sont minimes.

3.5.1.2 Vitesse de dissémination

Ici, nous nous intéressons au temps nécessaire pour atteindre les taux de réception présentés dans la métrique précédente. Pour cela, nous calculons le nombre de sauts réalisés avant d'atteindre les états finaux et absorbants. Chaque saut représente la retransmission d'une information par les derniers véhicules à l'avoir reçue s'ils sont élus.

Ce nombre de saut est obtenu après le calcul du plus court chemin entre l'état initial $(0,1)$ et l'état final $(k,0)$, état final dont dont la probabilité est la plus importante. Ce calcul utilise l'algorithme de Dijkstra avec comme métrique de plus court chemin les probabilités de transition entre les états.

Les résultats obtenus sont donnés dans le tableau 3.3. Nous remarquons que plus il y a d'élus pour la retransmission et moins de sauts sont nécessaires pour l'accomplissement de

Table 3.3 – Nombre de sauts requis avant l'arrêt du processus de dissémination.

Élus D / Connectivité	3	6	Tous les voisins
π=0.09	6	5	4
π=0.2	4	3	3
π=0.5	3	2	2

la dissémination. Le nombre de sauts nécessaires lorsque la connectivité est faible est de 6 lorsque le nombre de relayeurs est fixé à 3, mais il diminue à 4 lorsque tous les véhicules voisins sont élus. Cette différence est moins importante lorsque la connectivité est forte, soit $\pi = 0.5$. Dans ce cas, le nombre de sauts passe de 3, lorsque $D = 3$, à 2 lorsque $D = 6$ ou même lorsque tous les véhicules sont relayeurs.

Nous en déduisons que lorsque l'application a des contraintes temps réel, il est préférable de maximiser le nombre de relayeurs, surtout pour les situations de faible connectivité dans le réseau.

3.5.1.3 Probabilité d'un acheminement complet

Un acheminent complet est réalisé lorsque tous les véhicules concernés par une information la reçoivent, sa probabilité est celle d'atteindre l'état final $(N, 0)$. Cette métrique est très importante pour les applications de sûreté et de sécurité routière, dont les informations peuvent être vitales pour les usagés. Nous calculons alors la probabilité d'un acheminent complet $P_{ac}(t)$ par rapport au nombre de sauts t réalisés dans le processus de dissémination, au travers de l'équation (3.3), où nous récupérons la probabilité d'être dans l'état $(N, 0)$ à partir de l'état initial $(0, 1)$ après t sauts.

$$P_{ac}(t) = M^t[(1, 0), (N, 0)] \tag{3.3}$$

Ces probabilités sont illustrées dans les figures 3.6, 3.7 et 3.8 durant 11 sauts, pour une connectivité π égale à 0.09, 0.2 et 0.5, respectivement. Comme pour les métriques précédentes, nous varions le nombre de véhicules élus pour la retransmission d'un message. Lorsque la connectivité est faible, avec $\pi = 0.09$, la probabilité d'un acheminement complet est égale à 0.25 lorsque tous les véhicules sont élus pour relayer l'information. Cette valeur diminue jusqu'à 0.021 lorsque les relayeurs sont 6 au maximum et diminue même jusqu'à 0.006 lorsque le nombre de relayeurs est fixé à 3. Lorsque la connectivité est moyenne, $\pi = 0.2$, les probabilités $P_{ac}(t)$ diffèrent beaucoup à cause du nombre de relayeurs élus. Lorsque celui-ci est important, soit tous les voisins ayant reçu le message le retransmettent une fois, la probabilité P_{ac} croît très rapidement dés le deuxième saut, elle atteint la valeur de 0.75 et se stabilise à partir du sixième saut. Alors que cette probabilité ne dépasse pas la valeur 0.6 avec $D = 6$ et 0.3 avec $D = 3$, ce qui est très faible comme probabilité.

Lorsque la connectivité du réseau est forte, avec $\pi = 0.5$, la différence entre les probabilités P_{ac} est moins importante. Nous remarquons que les trois probabilités sont supérieures à la valeur 0.9. Il existe même un chevauchement entre les probabilités des deux cas où tous les véhicules sont relayeurs et celui fixant D à 6. Nous remarquons aussi la rapide croissance de ces trois probabilités. Elles atteignent leur valeur maximum dés le quatrième saut, ce qui est un critère très important pour les applications de sûreté à cause de leurs contraintes temps réel.

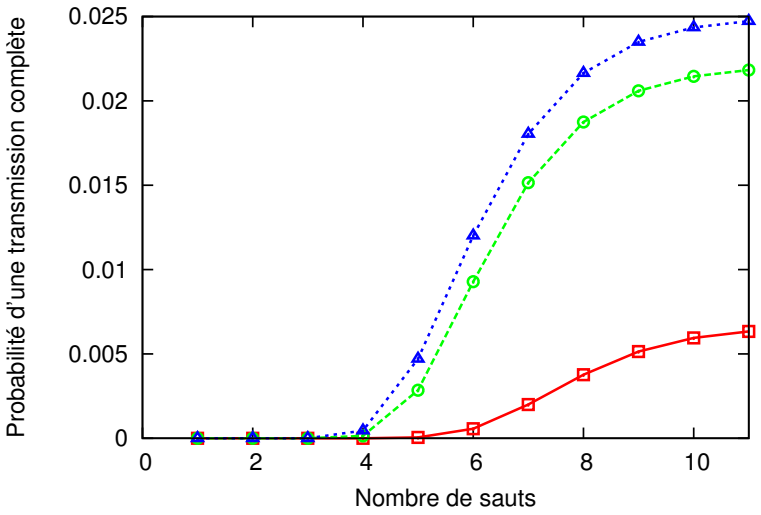


Figure 3.6 – Probabilité d'un acheminement complet avec $\pi = 0.09$.

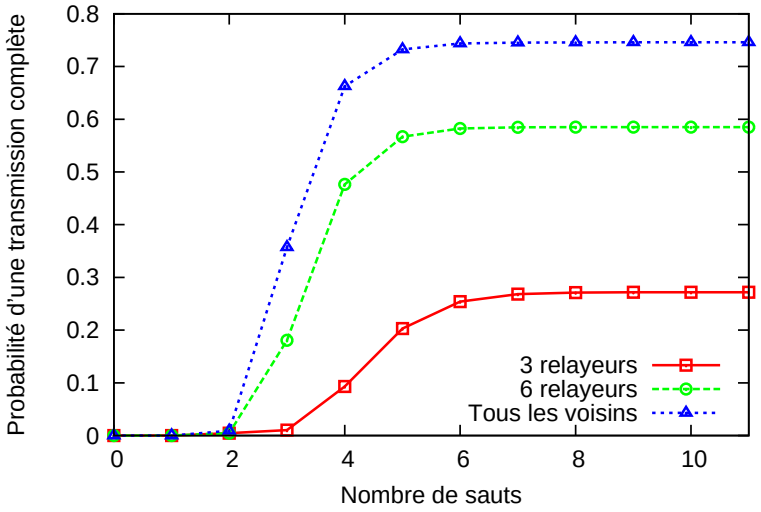


Figure 3.7 – Probabilité d'un acheminement complet avec $\pi = 0.2$.

3.5.1.4 Redondance

La stratégie de dissémination *ADCD* a pour but de maximiser le taux de réception des véhicules concernés par une information, mais sans inonder le réseau avec des messages redondants. Nous calculons alors, via notre modélisation par une chaine de Markov, le nombre moyen de messages superflus reçus par les véhicules lors d'un processus de dissémination, en variant la connectivité du réseau ainsi que le nombre de relayeurs élus. Nous considérons, lors de notre modélisation, qu'un message est superflu dés lors qu'il est reçu plus d'une fois par un véhicule.

Pour calculer le nombre moyen total des messages superflus, TMS, générés depuis l'état initial $(0, 1)$ jusqu'à l'état final $(k, 0)$, nous débutons par estimer le nombre de messages superflus, $MS[(i, j), (i + j, m)]$, générés entre chaque transition d'un état (i, j) vers un autre état $(i + j, m)$ au travers de l'équation (3.4). Dans cette équation, nous incluons la probabilité de réception d'un message en double par y véhicules, appartenant aux $(i + j)$ véhicules l'ayant déjà reçu, en soustrayant le véhicule émetteur à cet instant là, soit $(i +$

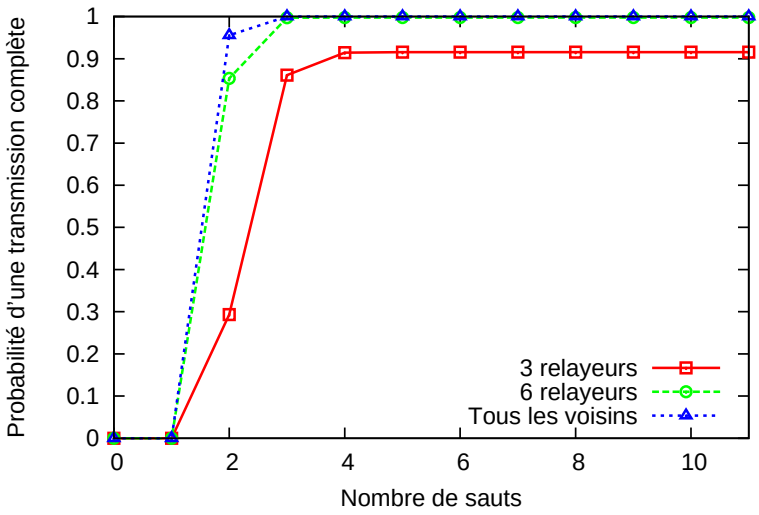


Figure 3.8 – Probabilité d'un acheminement complet avec $\pi = 0.5$.

$j-1$). Le nombre de messages redondants générés lors d'une transition dépend du nombre de véhicules $(i+j)$, qui ont déjà reçu le message et qui sont donc susceptibles de recevoir un message doublon, ainsi que du nombre de relayeurs choisis D et de la probabilité de transition entre les états (i,j) et $(i+j,m)$.

$$MS[(i,j),(i{+}j,m)] = \sum_{y=1}^{i+j-1} Pdf_B(y,\pi,i{+}j{-}1){\times}D{\times}(i{+}j){\times}Pdf_B(m,1{-}(1{-}\pi)^D,N{-}i{-}j) \tag{3.4}$$

Une fois le nombre de messages superflus calculé pour chaque transition, nous le pondérons par la probabilité d'occurrence de chaque transition, lorsque l'état initial est $(0,1)$ et l'état final $(k,0)$, comme décrit dans l'équation (3.5).

$$TMS = \frac{\sum_{i=0}^{N}\sum_{j=0}^{N-i} MS[(i,j),(i+j,m)] \times M[(i,j),(i+j,m)]}{\sum_{i=0}^{N}\sum_{j=0}^{N-i} MS[(i,j),(i+j,m)]} \tag{3.5}$$

Le nombre moyen de messages superflus générés durant un processus de dissémination est donné dans la figure 3.9. Nous calculons ce nombre pour différents nombres de relayeurs élus et différentes connectivités dans le réseau. Nous remarquons que le taux de croissance de ces valeurs augmente énormément, lorsque la connectivité est moyenne ou importante, ou que le nombre des relayeurs n'est pas limité. D'après ces résultats, nous en concluons que lorsque la connectivité est faible, le processus de dissémination peut demander la retransmission de l'information au moins une fois à tous les véhicules, car la différence engendrée en terme de messages superflus n'est pas conséquente par rapport à une dissémination avec un nombre maximum fixe de relayeurs. Cependant, lorsque la connectivité n'est pas faible, le choix des relayeurs doit absolument être limité pour ne pas congestionner le réseau.

3.5.2 Validation des résultats par simulation

Pour valider notre modélisation analytique, nous avons simulé les mêmes scénarios de l'étude analytique, en utilisant les mêmes paramètres, soit 20 véhicules avec une connectivité variable. Nous avons utilisé le simulateur NS2 [1] et le générateur de scénario

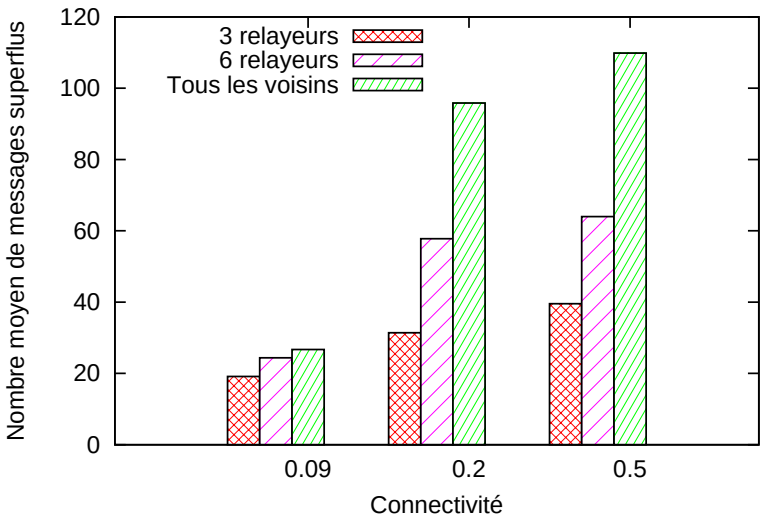


Figure 3.9 – Nombre de messages superflus générés lors du processus de dissémination.

de mobilité véhiculaire urbaine SUMO [4]. Nous varions la connectivité π entre les véhicules, qui influence le nombre de voisins $\pi \times (N-1)$ de chaque véhicule, en espaçant et réduisant l'étendue géographique du réseau. Ainsi, nous obtenons une connectivité de $\pi = 0.09$ pour une taille de réseau de $1000 \times 1000m^2$, une connectivité de $\pi = 0.2$ pour une taille de $800 \times 800m^2$ et une connectivité de $\pi = 0.5$ pour une taille de $500 \times 500m^2$.

La figure 3.10 illustre le nombre de véhicules ayant reçu une information envoyée par l'un d'entre eux et les concernant. Ces résultats sont similaires aux résultats analytiques présentés dans la figure 3.5. Le choix du nombre de relayeurs ne change pas le taux de réception lorsque la connectivité est forte, cependant, lorsque celle-ci est faible ou moyenne, avec une taille de réseau égale à $1000 \times 1000m^2$ ou $800 \times 800m^2$, le choix de 6 relayeurs au maximum donne les mêmes résultats que celui où le nombre de relayeurs n'est pas limité, alors que lorsque D est égal à 3, ce taux diminue.

La figure 3.11 présente le nombre de messages superflus générés par chaque choix de dissémination, d'après le nombre de relayeurs choisis, tout en variant la connectivité du réseau. Ces résultats restent identiques à ceux obtenus lors de notre modélisation du même scénario et qui sont illustrés dans la figure 3.9. Le nombre de messages redondants est stable, lorsque la connectivité du réseau est faible à cause de la grande étendue géographique du réseau qui dilue les connexions entres les véhicules, malgré les différents choix de nombre de relayeurs. Toutefois, le nombre de messages redondants diffère énormément lorsque la connectivité est forte, ainsi la non limitation du nombre de relayeurs augmente de 120% ce nombre par rapport à un choix de relayeurs limité à 3.

3.5.3 Vue d'ensemble des métriques

Il est nécessaire de prendre en considération les résultats de l'ensemble des métriques en même temps, afin de pouvoir choisir le nombre adéquat de relayeurs à élire dans chaque situation, pour respecter les contraintes de qualité de service de chaque classe de message. Nous regroupons ces résultats dans la figure 3.12, où nous les comparons les uns aux autres en utilisant des pourcentages, où un pourcentage de 100% est attribué au choix offrant la meilleure performance pour une métrique. Nous varions aussi la connectivité du réseau pour y adapter notre choix sur le nombre de relayeurs.

Lorsque la connectivité du réseau est faible, $\pi = 0.09$, le choix d'élire tous les

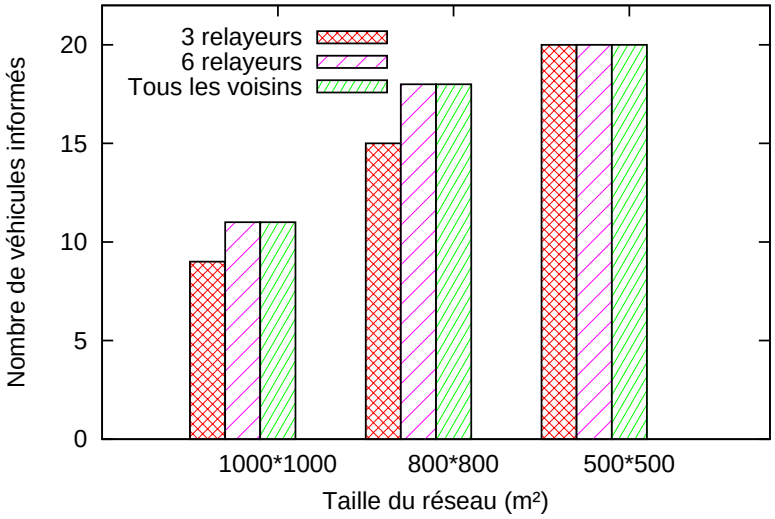


Figure 3.10 – Nombre de véhicules informés.

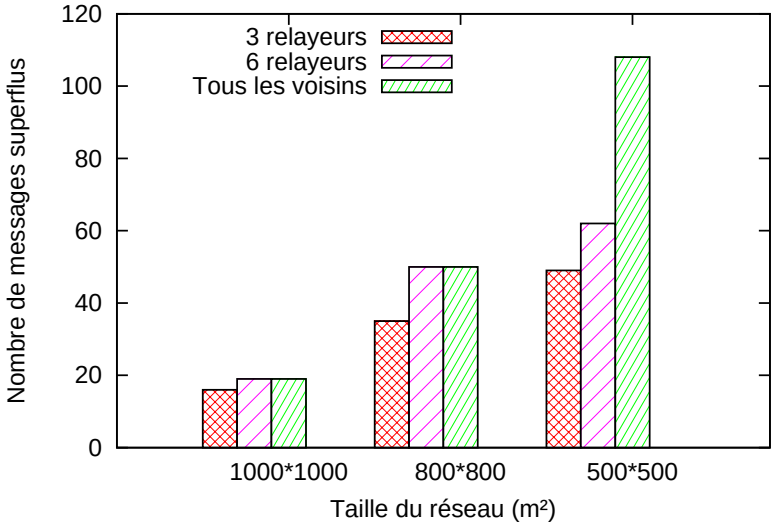
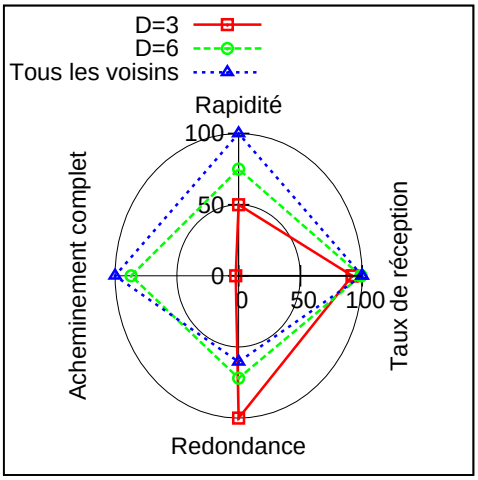


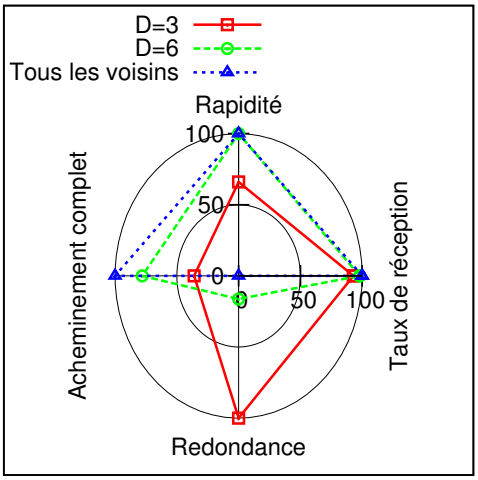
Figure 3.11 – Nombre de messages superflus.

voisins comme relayeurs a les meilleurs performances concernant les métriques du taux de réception, de la rapidité de la dissémination et de la probabilité d'un acheminement complet. Il n'est surpassé par les autres choix que pour la métrique concernant le nombre de messages redondants reçus. Les performances de ce choix sont talonnées de prêt par celles issues du choix avec un nombre limité de relayeurs fixé à 6, car la dissémination avec ce nombre de relayeurs est un peu moins rapide, mais génère moins de redondance. L'utilisation de 3 relayeurs au maximum lors d'une connectivité de réseau faible n'est pas un bon compromis, car l'écart entre ces performances et celles des autres choix est trop important.

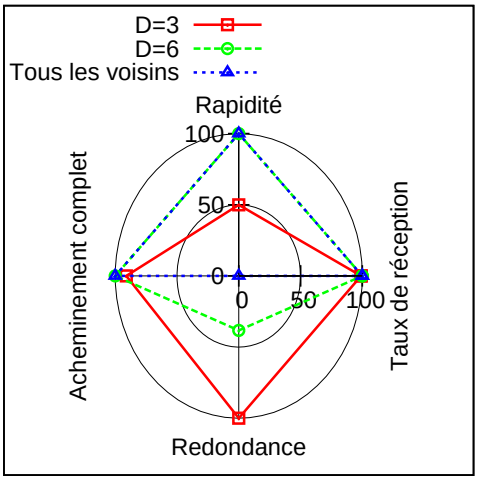
Lorsque la connectivité est moyenne, avec $\pi = 0.2$, le compromis qu'offre le choix de 6 relayeurs est meilleur que celui où le nombre de relayeurs est au maximum. Le choix entre une valeur de D égale à 3 ou 6 dépend de la classe du message, si c'est un message important, il est nécessaire que son acheminent soit complet et rapide, ce qui désigne le choix de 6 pour les relayeurs. Alors que si l'information est moins importante, la condition



(a) π=0.09



(b) π=0.2



(c) π=0.5

Figure 3.12 – Vue d'ensemble des différentes métriques, avec différentes connectivités dans le réseau.

d'un acheminement complet n'est pas requise, on peut choisir un nombre de relayeurs égal à 3, cela garantie tout de même un bon taux de réception et diminue le nombre de messages redondants.

Enfin lorsque la connectivité du réseau est forte, soit $\pi = 0.5$, le choix d'un nombre de relayeurs non limité est loin d'être le meilleur, il est surpassé par les deux autres choix avec $D = 6$ et $D = 3$. Le choix entre un nombre de relayeurs égal à 6 ou à 3 dépend, comme précédemment, de la classe du message. Cependant, le choix avec $D = 3$ est meilleur car il offre les mêmes performances pour les métriques du taux de réception et de la probabilité d'un acheminement complet. Même s'il est surpassé de 50% pour la métrique de la rapidité, il surpasse à son tour de 62% le choix avec $D = 6$ en ce qui concerne la métrique de la redondance.

Dans le reste de notre étude, nous choisirons un nombre faible de relayeurs, soit $D = 3$, pour les messages les moins importants, soit ceux dont la classe est de 1, 2 ou 3. Car leur contraintes de qualité de service ne sont pas si contraignantes, nous préférons choisir un compromis entre la probabilité d'un acheminement complet et le nombre de messages superflus générés, surtout que ces messages sont les plus fréquemment diffusés dans le réseau. Avec le choix de $D = 3$ nous diminuons fortement le gaspillage des ressources du canal de communication. Nous choisissons un nombre de relayeurs plus élevé pour les applications les plus importantes, dont les classes sont 4 et 5, avec un nombre de relayeurs D supérieur égal à 4. Ce nombre est compris entre 3 et 6, afin de garantir un acheminent rapide et complet de ces données, ainsi que pour baisser le nombre de messages superflus potentiellement générés.

3.6 Évaluation de performance

Après l'étude du nombre de véhicules relayeurs nécessaires pour chaque classe de message, nous procédons à une étude de performance plus générale. Comme précédemment, nous utilisons le simulateur NS2 [1] et le générateur de mobilité SUMO [4]. Au cours de cette simulation, nous varions le nombre de véhicules afin d'étudier l'impact de la densité sur les performances de la solution.

Nous générons des événements, dont la classe et le mode sont compris dans l'intervalle $[1, 5]$, détectés par un ou plusieurs véhicules, chaque 5 secondes durant notre simulation. Nous établissons des probabilités à l'occurrence des ces événements d'après leur classe d'importance, celles-ci sont égales à 0.60, 0.20, 0.10, 0.05 et 0.05 pour les classes 1, 2, 3, 4 et 5, respectivement. Le reste des paramètres utilisés lors de notre simulation sont donnés dans la tableau 3.4.

Nous comparons notre solution *ADCD* à deux autres approches. La première est celle d'une diffusion classique à plusieurs sauts, où chaque véhicule qui reçoit une information la rediffuse une seule fois. Cette solution propose un taux de réception élevé, mais génère beaucoup de messages redondants. En second, nous nous comparons à une version adaptée de la solution MobEyes [66]. Un véhicule utilisant cette approche envoie toutes les 12 secondes un message contenant les dernières informations collectées ou reçues en version résumée, le nombre d'informations maximum par message est fixé à 5. Pour améliorer l'efficacité de cette approche, nous établissons à 3 le nombre de sauts lors d'une dissémination d'un message.

Nous comparons ces approches par rapport aux métriques suivantes :

- le pourcentage de réception général, ainsi que celui par classe.
- La vitesse d'acheminement de l'information.

Table 3.4 – Valeur des paramètres de simulation.

Nombre de véhicules	100, 200, 300
Débit	$11Mbps$
Modèle de propagation	Two-ray ground reflection
Portée de transmission	$250m$
Environnement de mobilité	Urbain
Étendue géographique du réseau	$9000 \times 9000m^2$
Vitesse moyenne	$13.9m/s$
Durée de simulation	$300s$

Table 3.5 – Pourcentages de réception auprès des véhicules concernés.

Classes	ADCD	Diffusion	MobEyes adapté
Classe 1	100%	77%	58%
Classe 2	100%	76%	74%
Classe 3	100%	75%	61%
Classe 4	65%	52%	60%
Classe 5	50%	35%	35%

– Le nombre de messages superflus reçus, en considérant tous les messages redondants ainsi que ceux dépassant leur zone et intervalle de dissémination.
– L'impact de la densité sur le taux de réception.
– L'impact de la densité sur le nombre de messages superflus reçus.

3.6.1 Pourcentage de réception

Lors de cette simulation, nous mettons à jour de manière continue le nombre et les identifiants des véhicules concernés par une information, d'après leur traversée ou sortie de la zone de dissémination cible de la donnée, afin de calculer la proportion exacte des véhicules concernés l'ayant reçu. Les pourcentages moyens de réception des informations envoyées, lors de notre simulation avec 300 véhicules, sont données dans le tableau 3.5. Ce tableau présente les pourcentages moyens en détail pour chacune des cinq classes, lors du déploiement des trois approches : *ADCD*, *Diffusion* et *MobEyes adaptée*.

Nous rappelons que les classes 4 et 5 sont prioritaires, leur étendue géographique est la plus grande, $600 \times 600m^2$ et $1000 \times 1000m^2$, respectivement, ce qui augmente le nombre de véhicules concernés par la réception de leur messages. D'ailleurs, leur pourcentage de réception est le plus élevé lors de l'utilisation d'*ADCD*, il est égal à 65% pour la classe 4 et 50% pour la classe 5 avec l'élection de quatre relayeurs au maximum à chaque dissémination. Ce pourcentage est plus bas lors du déploiement des deux autres approches, il est compris dans l'intervalle $[35\%, 60\%]$. En effet, à cause des multiples envois effectués par la solution *diffusion*, un fort taux de collisions peut faire baisser le taux de réception, alors que l'approche *MobEyes* est moins précise lors de sa dissémination des messages, à cause du fait de stocker les messages avant de les envoyer, ce qui peut les éloigner de leur zone cible.

ADCD atteint un pourcentage de 100% pour les trois premières classes, alors que le pourcentage des solutions concurrentes varie entre 58% et 77%. Le pourcentage moyen de réception pour toutes les classes de messages est égal à 95.75% pour l'approche *ADCD*, à 73.25% pour l'approche *Diffusion* et à 60.45% pour l'approche *MobEyes*, ceci d'après les probabilités d'occurrences des classes choisies pour notre scénario. Une amélioration de

30% est réalisée par *ADCD* par rapport au pourcentage de réception obtenu par l'approche *Diffusion* et de 58% par rapport à celui de l'approche *MobEyes*. Dans la sous-section suivante, nous détaillerons l'évolution de ces pourcentages de réception en fonction du temps.

3.6.2 Vitesse d'acheminement

L'acheminement des messages de sûreté est conditionné par le taux de réception ainsi que par la vitesse de l'acheminement des données. Pour valider les résultats de la métrique précédente, il est important de l'accompagner du critère temps. La figure 3.13 illustre le pourcentage moyen de réception d'une information auprès des véhicules concernés. Les pourcentages de réception au cours du déploiement d'*ADCD* sont donnés pour chaque classe de messages séparément, alors qu'un pourcentage moyen général est donné pour les deux autres approches. Car ces dernières ne comportent pas de différentiation par classe dans leur approche. Ces pourcentages sont illustrés tout au long d'un intervalle de 7 secondes.

La hausse du pourcentage de réception la plus rapide est celle d'*ADCD* pour la classe 1, suivie de prêt par celle de l'approche *Diffusion*, puis dans l'ordre les quatre autres classes d'*ADCD* et enfin celle de l'approche *MobEyes*. Pour cette dernière, cela s'explique par le temps de stockage des informations par les véhicules avant leur émission. L'approche *Diffusion* a de bons résultats pour cette métrique, car elle accélère l'évolution du taux de réception de ses messages en rediffusant un message par tous ses véhicules récepteurs.

Nous nous intéresserons par la suite à l'instant de stabilisation de ces pourcentages, les messages dont la classe est 1, 2 ou 3 sont reçus par environ 100% des véhicules concernés dans un délai maximum de 0.5 seconde, ce qui est plus performant que lors de l'utilisation de l'approche *Diffusion*. Le délai nécessaire à l'acheminement des messages des classes 4 et 5 est tout aussi rapide que pour les autres, même si leur taux de réception est moins élevé, car les véhicules souhaitant leur réception sont plus nombreux et souvent plus difficiles à atteindre. Notre dernière remarque concerne le taux d'acheminement très long nécessaire à la solution *MobEyes*, soit au moins 7 secondes pour atteindre un pourcentage de réception de 61%. Car un véhicule, utilisant cette approche, envoie un message contenant plusieurs résumés uniquement chaque 12 secondes, ce qui ralentit fortement la vitesse d'acheminement des données.

3.6.3 Nombre de messages superflus

Une fois le taux de réception étudié, nous nous intéresserons au nombre de messages superflus reçus lors de la dissémination. Ces nombres sont présentés dans la figure 3.14 pour chacune des trois approches implémentées, lors du déploiement de 300 véhicules. Nous comptabilisons comme message superflu :

- Tout message dont le contenu a été reçu en double.
- Tout message reçu par un véhicule dont le contenu le concerne pas, c.-à-d un véhicule n'étant pas dans la zone de dissémination cible de l'information.
- Tout message sorti de sa zone de dissémination cible.

D'après les résultats obtenus, la solution *ADCD* génère un nombre très faible de messages superflus lors de son utilisation, car elle cible uniquement les véhicules concernés par une information et n'importune pas les autres véhicules, ni n'occupe le réseau avec l'envoi de messages non significatifs. Cependant, les deux autres solutions ne font pas cas de cette métrique. Le nombre de messages superflus reçus lors de l'utilisation de l'approche *Diffusion* est $9,44$ plus élevé que lors de l'utilisation d'*ADCD*, autrement

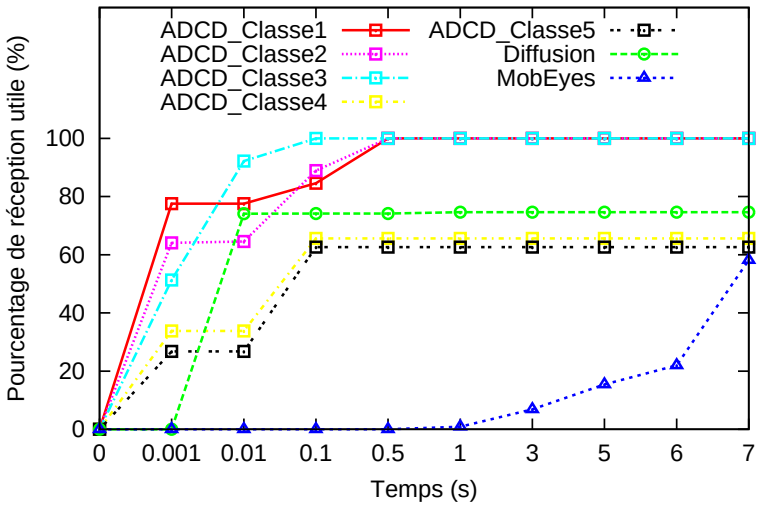


Figure 3.13 – Pourcentage de réception en fonction du temps.

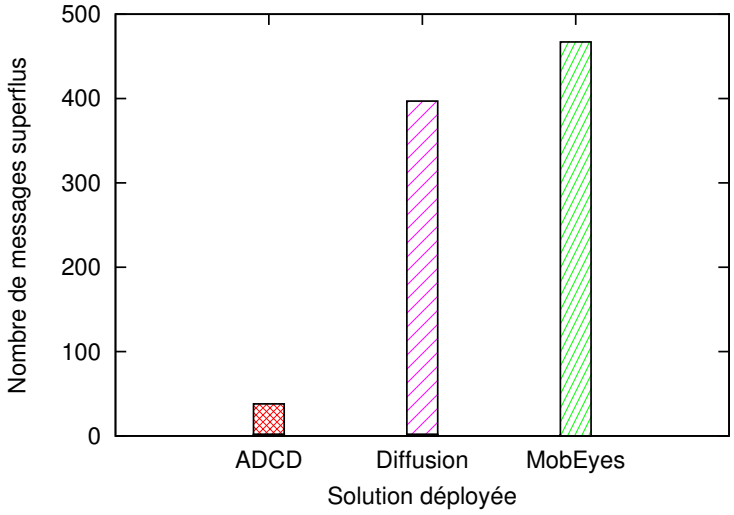


Figure 3.14 – Nombre de messages superflus générés.

dit nous obtenons une diminution de 90.4% avec l'utilisation d'*ADCD*. Cette différence s'élève même jusqu'à 11, 28 lors de la comparaison des performances de *MobEyes* et celles d'*ADCD*, soit une diminution de 91, 86% proposée par *ADCD* par rapport à *MobEyes*. Ce nombre important pour *MobEyes* s'explique, en premier, par le fait que chaque message contient 5 informations, ce qui augmente les risques de réceptions multiples d'une même information. Aussi, le temps de stockage de chaque donnée combiné à la mobilité des véhicules peuvent causer une dissémination auprès des véhicules non concernés. De plus, le fait qu'aucune restriction n'est imposée sur l'envoi répétitif des résumés par le même véhicule accentue encore plus cet effet. Par contre, *ADCD* arrive à baisser ce nombre en utilisant les paramètres classe et mode lors de la dissémination d'une information, de sorte qu'aucun message n'est retransmis si son mode ou classe ne l'autorisent pas, en plus de sa limitation du nombre de relayeurs.

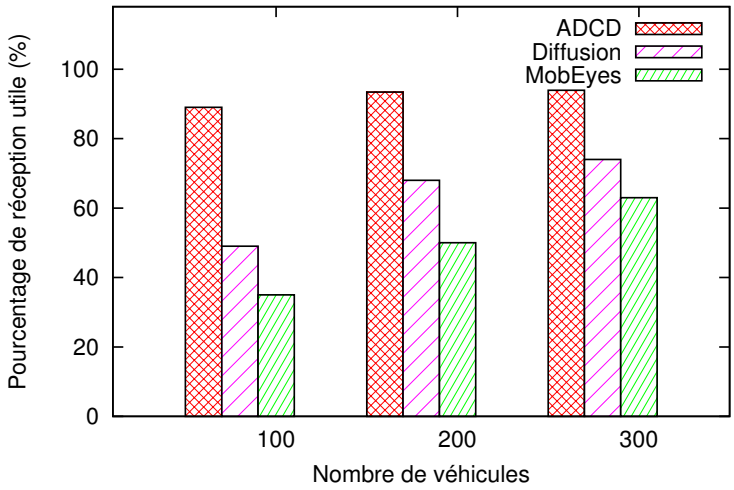


Figure 3.15 – Pourcentages de réception, avec 100, 200 et 300 véhicules.

3.6.4 Impact de la densité sur le taux de réception

Dans le but d'évaluer l'impact de la densité des véhicules dans un réseau, nous varions ce paramètre et calculons le pourcentage moyen de réception lors du déploiement des trois approches implémentées. Nous utilisons en premier un nombre de véhicules de 100, sans pour autant changer l'étendue géographique, ce qui baisse la connectivité dans le réseau. Puis nous utilisons un nombre de véhicules égal à 200 et enfin à 300. Ces résultats sont donnés dans la figure 3.15.

Les pourcentages issus de la solution *ADCD* ne diffèrent pas beaucoup avec le changement de la densité dans le réseau. Ils sont toujours supérieurs à 90%, ce qui les amènent à être meilleurs que ceux des deux autres approches. Les pourcentages de l'approche *Diffusion* s'améliorent avec l'augmentation du nombre de véhicules présents. Le pourcentage moyen débute à 49% lorsqu'il existe 100 véhicules dans le réseau, puis passe à 68% pour 200 véhicules et enfin à 74% avec 300 véhicules. Cette remarque est aussi valable pour l'approche *MobEyes*, qui dépend aussi de la densité du réseau pour offrir un haut taux de réception aux véhicules. Celle-ci reste cependant limitée par rapport à *ADCD*, pour les mêmes raisons évoquées précédemment.

Ces résultats confirment la supériorité d'*ADCD* pour la dissémination de données, même lorsque la densité du réseau est faible, car cette dernière, limite les possibilités de transmission de l'information dans le réseau.

3.6.5 Impact de la densité sur le nombre de messages superflus reçus

Si l'impact d'une faible densité est négatif sur le pourcentage moyen de réception, il est néanmoins positif sur le nombre de messages superflus reçus par les véhicules. La figure 3.16 illustre l'évolution de ce nombre pour chacune des trois solutions : *ADCD*, *Diffusion* et *MobEyes*, avec un nombre de véhicules de 100, puis de 200 et enfin de 300. Nous observons une croissance linéaire à courbure faible pour le nombre de messages superflus reçus lors du déploiement d'*ADCD* par rapport à celle des deux autres solutions, dont la courbure est beaucoup plus importante. Ainsi, le nombre de messages superflus reçus lors du déploiement de l'approche *Diffusion* est 6 à 9 plus important que celui d'*ADCD*, cette différence est encore plus importante s'agissant de la différence entre *MobEyes* et *ADCD*, qui se situe dans une tranche de 11 à 13.

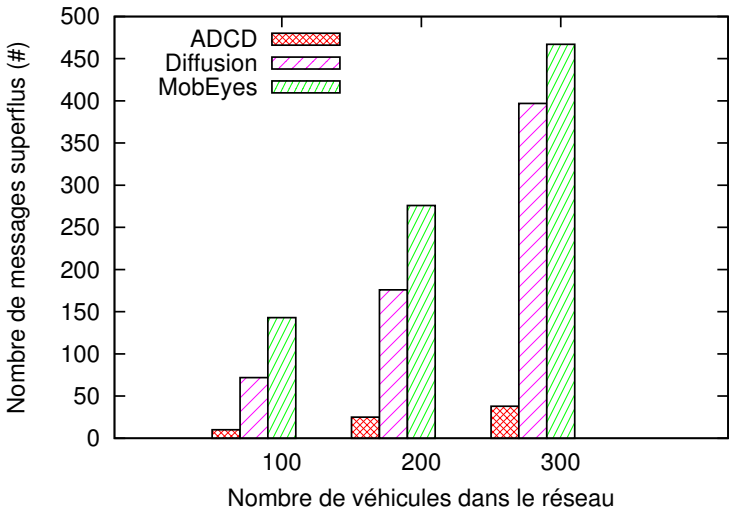


Figure 3.16 – Nombre de messages superflus reçus, avec 100, 200 et 300 véhicules.

Nous rappelons que l'envoi d'un nombre important de messages redondants ou inintéressants pour les véhicules occupe le canal de communication et peut empêcher la dissémination d'autres messages qui seraient plus pertinents. Leurs conséquences peuvent être néfastes pour les performances des applications de sûreté.

3.7 Conclusion

Les informations issues des applications de sûreté et de sécurité routière requièrent une dissémination rapide et complète pour tous les véhicules se situant dans la zone cible de dissémination, pendant tout le temps de validité de chaque donnée. Nous traduisons ces contraintes par les notions de classes et modes qu'on associe aux différents types de messages, de sorte qu'une classe corresponde à la couverture géographique de la zone de dissémination et qu'un mode à la validité dans le temps de l'information. En se basant sur cela, nous proposons ensuite une stratégie de dissémination adaptée pour chaque type (classe, mode) de messages, nommée *ADCD*. Cette approche propose un compromis entre le taux de réception, la vitesse de dissémination des messages et le nombre de messages superflus qu'elle peut générer. *ADCD* adapte sa stratégie de dissémination en choisissant le nombre de relayeurs adéquat pour chaque type de message, afin de respecter ses contraintes. Ce compromis a été étudié analytiquement au travers d'une modélisation par une chaîne de Markov.

Ainsi, nous avons validé les performances d'*ADCD*, en premier, de façon analytique. Nous avons étudié l'évolution du pourcentage de réception, sa rapidité, la probabilité qu'un acheminement soit complet et enfin le nombre de messages superflus que cela peut engendrer, tout en variant le nombre de relayeurs et la connectivité du réseau. Ensuite, nous avons validé ses performances par simulation, en réitérant les mêmes métriques. *ADCD* maintient un haut taux de réception, tout en diminuant le nombre de messages non significatifs, à savoir 90%.

Après avoir étudié dans ce chapitre la dissémination au niveau de la couche réseau laquelle a été adaptée à l'importance et aux types de messages, nous nous intéresserons dans le prochain chapitre aux problématiques de dissémination liées à la couche MAC. En effet, le principe du multi-canal, inhérent au standard IEEE 802.11p/1609.4 [11][12],

conditionne fortement les performances de la dissémination des applications de sûreté par rapport à l'accès au canal.

Chapitre 4

Retarder pour mieux transmettre avec le standard IEEE 802.11p/1609.4

Sommaire

Précédent, nous nous étions intéressés à améliorer le taux de réception des messages dans les réseaux ad hoc véhiculaires (VANETs) et à réduire de leur temps d'acheminement. Pour cela, nous avions proposé une nouvelle stratégie de dissémination *ADCD* au niveau de la couche réseau. Cependant, cette solution n'est plus suffisante depuis l'entrée en vigueur du multi-canal dans le standard de la couche MAC véhiculaire, soit le IEEE 802.11p/1609.4 [11][12], car son utilisation mène à une surcharge et à une sous-utilisation du canal de façon répétitive. En effet, l'utilisation du multi-canal dans les VANETs cause de multiples collisions suite à la synchronisation des envois ([37],[30]).

Nous détaillons dans ce chapitre notre solution pour la répartition équilibrée des ressources dans le temps lors de l'utilisation du multi-canal. Elle consiste en un ordonnanceur distribué, basé sur la théorie de l'arrêt optimal [34]. Cette dernière définit la stratégie à suivre pour maximiser un gain futur qui représente le taux de réception d'un message dans notre cas. Notre ordonnanceur *DMS* [52] permet de définir le moment opportun à l'envoi d'un message, tout en respectant la durée de validité de son contenu. Par ceci une répartition de charge sur le canal se crée de manière distribuée. Notre solution se base sur une modélisation en processus de décision markovien [82], qui attribue des récompenses aux chances de succès d'un envoi et inflige des coûts au risque d'échec, ainsi qu'au retard imposé.

La suite de ce chapitre est organisée comme suit : La section 4.1 motive ce travail et définit son contexte. Elle est suivie par une présentation des différentes approches existantes pour la résolution de notre problème dans la section 4.2. Puis nous présentons notre solution *DMS* dans la section 4.3, où nous y détaillons son fonctionnement et la définition de ses paramètres. Nous décrivons ensuite dans la section 4.4 l'étude de

performances sur deux scénarios différents et analysons sa capacité à équilibrer la charge du canal. Enfin, la section 4.5 conclut le chapitre.

4.1 Motivation et contexte

L'acheminement des messages de sûreté se fait par la diffusion, ce qui rend incertain leur réception dans l'IEEE 802.11p [11] à cause de l'absence d'accusé de réception pour. Un véhicule source est alors incapable de s'assurer de la bonne réception de ses messages envoyés. Cela est critique lorsqu'il s'agit de messages urgents dont la réception est vitale, ce qui rend leur acheminement sensible aux congestions, aux pertes et aux longs délais de bout en bout.

Afin de pallier ces limites, le standard IEEE 802.11p [11] coexiste entre les applications de sûreté et les autres en utilisant une approche multi-canal, soit l'IEEE 1609.4 [12]. Celle-ci a pour but d'avantager la transmission des messages de sûreté, néanmoins elle crée de nouvelles problématiques en mettant en attente ces mêmes messages durant les intervalles de *SCH* et de *garde*, soit 54 ms chaque 100 ms. Ces messages ne sont transmis que durant la première moitié de l'intervalle de synchronisation et cela sur le canal de contrôle (d'après la norme européenne) pour pouvoir être reçus par tous les véhicules aux alentours.

Cette mise en attente augmente fortement la compétition pour l'accès au canal au début de l'intervalle *CCH*, ce qui génère des collisions synchronisées et des pertes en rafale comme par le passé démontrées dans les études [37] et [30]. La forte compétition pour l'accès au canal au début de l'intervalle *CCH* crée un déséquilibre dans la répartition de charge tout au long des 46 ms qui constituent l'intervalle *CCH*. La figure 4.1 représente ce déséquilibre en illustrant le pourcentage d'occupation du canal durant un intervalle *CCH*. La charge de ce canal est générée par 20 véhicules, qui partagent la même couverture réseau et qui envoient dans un premier temps un message de sûreté par intervalle de synchronisation de 100 ms, puis dans un deuxième scénario deux messages durant le même intervalle. Nous remarquons que la charge du canal est mal partitionnée, la majorité des véhicules sont en compétition au début de l'intervalle *CCH*, car les véhicules veulent diminuer le délai d'acheminement de leurs messages après leur mise en attente durant les intervalles de *SCH* et de *garde*. Ceci sature le canal et crée d'importantes pertes, alors qu'une bonne répartition de charge tout au long de l'intervalle assure un meilleur taux de réception pour les messages envoyés.

Pour équilibrer la charge tout au long des intervalles *CCH* et éviter les collisions synchronisées des débuts d'intervalles, nous proposons un ordonnanceur distribué au niveau de la couche MAC nommé *DMS*, qui retarde l'envoi de quelques messages pour maximiser leur futur taux de réception. La solution est distribuée, chaque véhicule prend sa décision indépendamment des autres, ce qui évite le déploiement d'infrastructures supplémentaires, ainsi que les échanges à but coordinateur entre les véhicules. Un véhicule décide de retarder ou non l'envoi de son message par rapport aux taux d'occupation du canal dans les différentes périodes qui composent un intervalle *CCH*. Deuxièmement, par rapport à l'efficacité de chacune de ces périodes de temps. Nous estimons l'efficacité d'une période de temps dans un intervalle *CCH* la différence entre le nombre de messages réellement reçus et leur nombre potentiel d'après l'occupation du canal. Notre solution *DMS* considère la catégorie d'accès (AC), qui est la priorité définie par EDCA [7] pour le message à envoyer, comme un troisième critère, afin de limiter le temps de retardement avant l'envoi, pour que les messages les plus importants soient le moins possible retardés, ceci favorise leur envoi sur les autres priorités de messages dans les cas de saturation de canal.

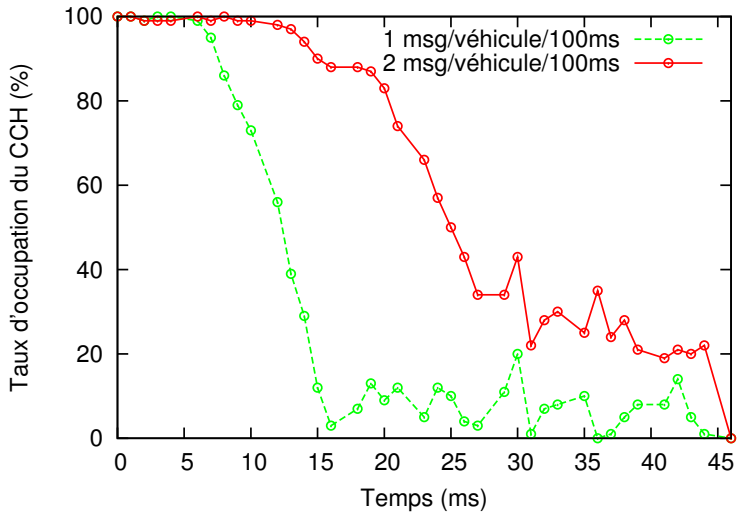


Figure 4.1 – Pourcentage d'occupation du canal lors des intervalles de *CCH*.

Notre solution se base sur *la théorie de l'arrêt optimal* [34][13], dont la problématique est de trouver le moment opportun pour agir et ne plus attendre. *DMS* s'en inspire pour trouver un compromis entre le retard ajouté avant l'envoi d'un message et les chances de succès de son envoi. Ce compromis, choisi de manière distribuée par chacun des véhicules composant le réseau, permet d'augmenter le taux de réception des messages tout en respectant la durée de validité des informations échangées. En plus, il permet de façon indirecte de rééquilibrer la charge du canal tout au long de l'intervalle *CCH*. La modélisation et résolution de la théorie de l'arrêt optimal se font à travers un processus de décision markovien (MDP) [82].

Nos contributions dans ce chapitre sont :

– Un ordonnanceur distribué au niveau de la couche MAC pour l'envoi de messages, qui induit à une répartition équitable de la charge au long de l'intervalle de contrôle.

– L'obtention d'un compromis entre la maximisation du taux de réception d'un message et la minimisation de son temps d'acheminement, via un processus de décision markovien (MDP).

4.2 État de l'art

Plusieurs approches ont été proposées par le passé pour remédier aux effets négatifs induits par l'accumulation des messages de sécurité routière dans la file d'attente durant les intervalles de *SCH* et de *garde*. Un de ces effets est la forte compétition pour l'accès au canal au commencement de l'intervalle *CCH*, ce qui engendre des collisions synchronisées. Le standard IEEE 802.11p [11] propose de solutionner le problème de l'accès au canal par le mécanisme du *back-off*, ainsi que par celui de *l'espacement inter-frame arbitraire (AIFS)*, en prenant en considération la priorité de l'information d'après les catégories d'accès au canal (ACs) définies dans EDCA [7]. Plus précisément, EDCA définie des tailles de fenêtre de contention (CW) et des valeurs pour *le nombre d'espacement Inter-Frame arbitraire (AIFSN)* adaptées à chacune des quatre catégories ACs (AC3, AC2, AC1, AC0). Ces dernières différencient entre les types de messages d'après leurs critères en qualités de service, en assignant généralement la classe AC3 aux messages les plus urgents. Les études

menées dans [37] et [30] démontrent l'inefficacité et l'insuffisance de ces mécanismes à garantir les performances requises aux applications de sécurité routière.

Les solutions déjà existantes peuvent être classifiées en quatre catégories : des approches basées sur le changement de taille de la fenêtre de contention CW [105][38], d'autres basées sur le changement de la valeur de l'AIFSN [91], d'autres sur le changement de la taille des intervalles *CCH* et *SCH* [104]. Finalement, la quatrième catégorie, qui tout comme notre approche, DMS, retarde l'envoi des messages pour augmenter leurs chances de réception [39]. Le retard dépend généralement du taux d'occupation du canal durant l'intervalle *CCH*. Nous détaillons chacune de ces approches ci-dessous.

4.2.1 Approches basées sur le changement de la taille de la fenêtre CW

Multiples sont les travaux qui proposent de modifier la taille de la fenêtre de contention, de façon statique ou dynamique, dans le but d'améliorer le mécanisme de contention de la couche MAC. Les auteurs de l'étude [105] proposent un compromis entre le débit et la fiabilité de l'envoi des messages en ajustant la valeur de la fenêtre CW. Ils réalisent une étude analytique pour le calcul de la probabilité de l'envoi avec succès d'un message par rapport au débit de l'envoi. Puis, ils analysent l'évolution de ces deux valeurs en considérant le nombre de nœuds dans le réseau, la taille des messages échangés, ainsi que la taille de la fenêtre CW. Finalement, à l'aide d'un optimum de Pareto issu de leurs résultats, un intervalle pour la fenêtre de contention est défini d'après les critères applicatifs décrits par l'application, en terme de débit et de fiabilité. À la différence de notre solution, DMS, cette étude ne prend pas directement en considération l'évolution et le changement du taux d'occupation du canal.

Un deuxième travail [38] améliore aussi le débit des messages et diminue la probabilité de collision, en estimant la valeur optimale de la taille de la fenêtre CW. Contrairement à l'approche [105], celle-ci optimise en plus l'utilisation des ressources du spectre DSRC en utilisant la radio cognitive. La solution requiert le déploiement d'infrastructures aux bords des routes (RSUs), pour écouter le canal de contrôle et calculer le taux de réception nécessaire aux messages à envoyer. Ceci dans le but de diffuser au fur et à mesure de nouvelles valeurs optimales pour la configuration de la couche MAC, à savoir la taille de la fenêtre CW et la valeur de la bande passante du canal de contrôle. En revanche, *DMS* améliore les performances des applications de sûreté en ordonnançant de manière distribuée la charge du canal sans nécessiter aucune infrastructure additionnelle, ni échange de messages dans le but de synchroniser les configurations de la couche MAC auprès des véhicules.

4.2.2 Approches basées sur le changement de la valeur AIFSN

La seconde alternative proposée pour remédier au problème des collisions synchronisées est d'ajuster la valeur de l'AIFSN, comme proposé dans [91]. Les auteurs nomment leur approche comme étant l'isolation des catégories de messages, elle consiste à incrémenter la valeur AIFSN pour les messages des catégories les moins importantes, pour éviter un potentiel chevauchement dans le temps lors de la compétition pour l'accès au canal avec les messages les plus importants. Cette approche est statique comparée à notre solution, qui s'adapte à l'évolution de la charge du trafic sur le canal.

4.2.3 Approches basées sur le changement de la taille des intervalles *CCH* et *SCH*

Les auteurs de l'étude [104] proposent une autre méthode pour améliorer le débit et réduire les délais de transmission dans l'IEEE 802.11p/1609.4. Elle consiste à dynamiquement ajuster les tailles des intervalles *CCH* et *SCH*, d'après les estimations des unités de bords de route (RSUs). Ces estimations portent sur les performances des transmissions actuelles sur le canal, ainsi que sur le nombre de véhicules partageant la même zone de couverture réseau. Les nouvelles tailles des intervalles *CCH* et *SCH* sont alors annoncées par les RSUs aux véhicules via des messages de diffusion. Cependant, la forte mobilité dans les VANETs et leurs changements fréquents de topologie rendent cette solution inappropriée et imprécise, étant donné qu'un accord doit être établi et respecté par tous les véhicules voisins sur la taille des intervalles *CCH* et *SCH*.

4.2.4 Approches basées sur le retardement d'envoi des messages

Cette quatrième approche, similaire à la notre, a été choisie dans l'étude [39]. La solution proposée pallie les mauvaises performances des applications de sûreté causées par les mises en attente des messages et le changement de canaux durant l'intervalle de synchronisation, en adaptant dynamiquement le temps d'attente avant l'envoi d'un message. Un véhicule utilisant cette solution écoute et stocke ses informations locales sur la charge du canal *CCH*, puis les échange avec ses voisins directs via les messages HELLO. Un véhicule calcule alors une moyenne du taux d'occupation du canal grâce aux retours de ses voisins. Pour chaque message à envoyer, une priorité d'envoi est calculée sur la base du taux d'occupation du canal et du nombre de fois que le message a été retardé. Un message peut être retardé car le canal *CCH* a expiré ou par décision de la solution. Lorsque la décision de retarder est choisie, la procédure du *back-off* avant l'envoi d'un message est réinitialisée avec une fenêtre de contention deux fois plus grande, ceci jusqu'à ce que la priorité de l'envoi induise à la décision de l'envoi immédiat.

L'inconvénient de cette solution est qu'il n'est pas possible de déterminer avec certitude le délai de retardement d'un message et que ce délai peut s'allonger de beaucoup. Ceci est causé par le fait que le retard est induit par la réitération du mécanisme du back-off, qui se met souvent en pause lorsque le canal est occupé, en risquant de faire de longues boucles jusqu'à ce que la décision de l'envoi immédiat soit prise.

4.2.5 Discussion

Notre solution, DMS, diffère de la solution précédente [39] dans la façon dont sont décidés l'envoi immédiat et le retardement d'un message, ainsi que dans le calcul de la période de retardement. Dans DMS, en plus de l'estimation de l'occupation du canal durant l'intervalle *CCH*, chaque véhicule évalue l'efficacité de l'envoi tout au long de l'intervalle *CCH*. Cette efficacité concerne le nombre de messages reçus et le nombre estimé d'après le taux d'occupation du canal dans chaque période de temps. Disposant de l'historique de l'occupation du canal et de l'efficacité de chacune de ses périodes, un véhicule se base sur la théorie de l'arrêt optimal afin de trouver le moment opportun pour envoyer son message, tout en respectant les contraintes de temps de son message, liées à sa catégorie d'accès sur EDCA. Dans DMS, un compromis est trouvé entre la probabilité d'envoi d'un message avec succès et le délai additionnel avant son envoi.

4.3 DMS : un ordonnanceur distribué inspiré de la théorie de l'arrêt optimal

Pour remédier aux problèmes des collisions synchronisées et au déséquilibre de charge sur le canal *CCH*, nous proposons une solution nommée DMS inspirée de la théorie mathématique de l'arrêt optimal [34]. Cette théorie répond à la question : *"Est-il plus opportun d'envoyer mon message maintenant ou de retarder son envoi ? Et de combien je le retarde si c'est le cas ?"* .

4.3.1 Ordonnancement des messages via la théorie de l'arrêt optimal

La théorie mathématique de l'arrêt optimal [34] est généralement utilisée en statistique, en mathématiques financières et en économie. Elle permet de prendre une décision quand les critères qui maximisent un gain final sont difficiles à joindre ensemble. Cette théorie est souvent illustrée avec l'exemple de la vente d'une maison par un particulier. Il s'agit pour un particulier d'accepter la meilleure offre de prix pour la vente de sa maison, sachant que quand il refuse une offre elle est à jamais perdue et que temporiser la vente lui coûte de l'argent, ces coûts peuvent être liés à des taxes ou à des bénéfices de la banque sur un prêt par exemple. Le particulier doit prendre une décision pour chaque offre qu'il reçoit. Il doit savoir arrêter d'attendre et choisir une offre malgré le peu d'informations qu'il a sur ce qui va advenir, cela dans le but de maximiser son gain final qui est le prix de vente et minimiser ses coûts. La théorie de l'arrêt optimal prend la décision d'attendre encore ou d'accepter une offre en se basant uniquement sur les observations du passé.

Nous calquons notre problématique concernant l'instant propice à l'envoi d'un message par un véhicule sur celle de la vente d'une maison par un particulier. Sachant que comme le retard pris par une vente, le retard ajouté avant l'envoi d'un message n'est pas recommandé et peut être coûteux. Aussi l'objectif d'un véhicule est de maximiser le pourcentage de réception de son message, ceci représente sa récompense, tout comme le prix de vente de la maison. Le gain final dans les deux exemples est obtenu par la soustraction des coûts à la récompense. Un véhicule maximise le pourcentage de réception de son message en l'envoyant pendant que le canal est libre ou peu occupé. Un envoi durant un canal libre maximise certes les chances de réception du message, mais peut aussi allonger énormément son délai d'acheminement si la charge du canal met longtemps à s'alléger et par conséquent faire expirer sa durée de validité VT.

Un compromis doit être trouvé entre le taux de réception d'un message et le délai additionnel induit par son retardement, afin de ne pas surcharger le canal avec des informations qui sont passées d'actualité.

4.3.2 Formulation du problème

La décision choisie représente un compromis entre le gain final qui est le taux de réception et le coût lié au retard potentiel. La résolution de cette problématique est obtenue via une modélisation en Processus de Décision Markovien (MDP) [82]. La durée de validité, VT, d'une information étant limitée, le retard toléré pour son envoi l'est aussi. Alors, nous proposons un ensemble T de N périodes dans le temps comprises uniquement dans les intervalles *CCH*, de durée t chacune, durant lesquelles un véhicule peut envoyer son message, ou décider de le retarder jusqu'à la période de temps suivante.

Table 4.1 – Notations utilisées pour la modélisation.

VT	Durée de validité d'une information
N	Nombre de période dans le temps
T_i	Période numéro i comprise dans VT
t	Durée d'une période T_i
T_{SCH}	Durée de l'intervalle *SCH*
T_{garde}	Durée de l'intervalle de *garde*
s^{T_i}	État s de la chaîne de Markov à la période de temps T_i
F^S	État absorbant de la chaîne de Markov, atteint lors d'un envoi avec succès
F^E	État absorbant de la chaîne de Markov, atteint lors d'un envoi avec échec
$A_s^{T_i}$	Action choisie pour l'état s^{T_i}
A_w	Action pour retarder
A_m	Action pour envoyer immédiatement
$R(s'^{T_{(i+1)}}, s^{T_i})$	Récompense pour la transition entre les états $s^{T_{(i)}}$ et $s'^{T_{(i+1)}}$
R_s	Récompense attribuée pour l'envoi avec succès d'un message
R_f	Coût à déduire après l'envoi avec échec d'un message
R_w	Coût à déduire après l'ajournement de l'envoi d'un message
$P(s'^{T_{(i+1)}}\|a, s^{T_i})$	probabilité de transition entre deux états, avec le choix de l'action a
δ	Espacement de l'intervalle d'un état concernant l'occupation du canal
E^{T_i}	Efficacité de l'envoi sur le canal lors d'une période de temps T_i
NM^{T_i}	Nombre de message reçu avec succès durant une période de temps T_i
$\pi^\star$	Politique contenant la meilleure décision pour chaque situation
$V^\pi(T_i, s)$	Matrice des gains pour une politique π

L'ensemble des périodes de temps pour l'envoi d'un messages sont : $T = \{T_1, ..., T_N\}$ avec $N = \frac{VT}{t}$, tel que :

$$T_{i+1} - T_i = t + \eta \times T_{SCH} + \upsilon \times T_{garde} \qquad \text{lorsque } i < N$$

Où

$$\eta = \begin{cases} 1 & \textit{Lors de la rencontre de l'intervalle SCH} \\ 0 & \textit{Sinon} \end{cases}$$

$$\upsilon = \begin{cases} 1 & \textit{Lors de la rencontre de l'intervalle de garde} \\ 0 & \textit{Sinon} \end{cases}$$

Notre modélisation en MDP est composée d'un ensemble S d'états possibles pour le système, des actions $A_s^{T_i}$, des récompenses et des coûts $R(s'^{T_{(i+1)}}, s^{T_i})$ qui dépendent des deux états en paramètre et enfin des probabilités de transition $P(s'^{T_{(i+1)}}|a, s^{T_i})$ entre les deux états $s'^{T_{(i+1)}}$ et s^{T_i}, qui sont séparés dans le temps de $(T_{(i+1)} - T_i)$, lorsque l'action choisie est a. Les notations utilisées dans notre modélisation sont données dans le tableau 4.1.

4.3.2.1 Les états

L'ensemble S des états du processus comprend deux parties, les états C qui concernent le pourcentage d'occupation du canal allant de 0% à 100% pour chacune des périodes T_i de la durée de validité d'une information. S'ajoute à cela les deux états absorbants F qui représentent l'état d'envoi d'un message avec succès et celui avec échec. Ces états sont atteints dés lors qu'un véhicule envoie son message. Cet ensemble d'états est illustré dans

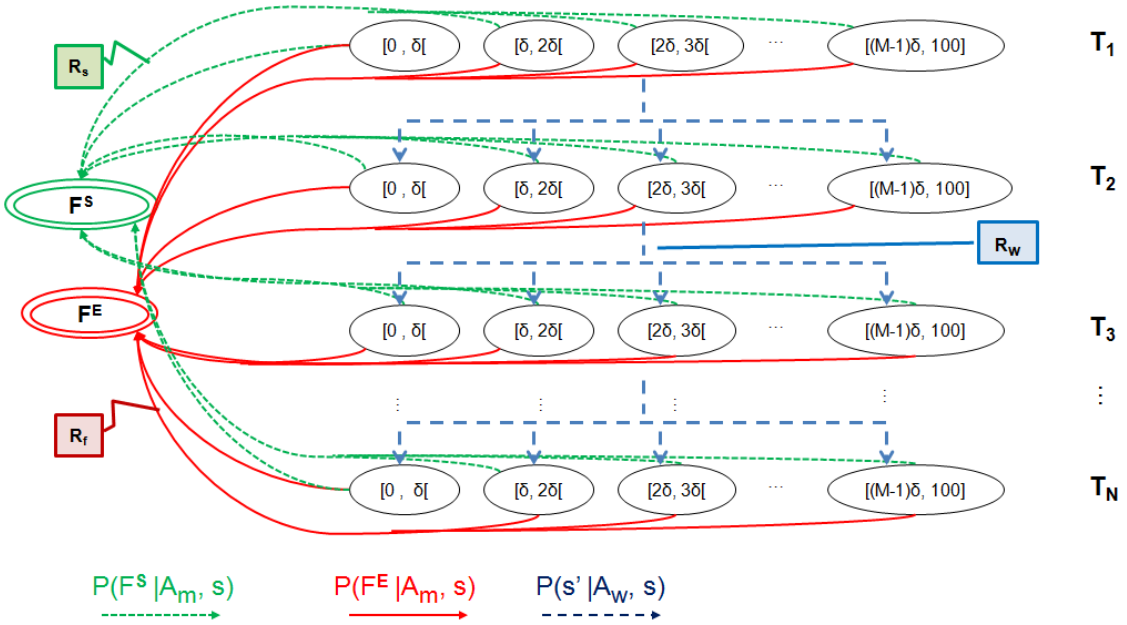


FIGURE 4.2 – Modélisation de la solution *DMS* en un processus de décision markovien.

la figure 4.2. Tous ces états sont reliés entre eux par des probabilités de transition, dont découlent des coûts R_f et R_w ou des récompenses R_s.

$C = \{S_0^{T_i}, S_1^{T_i}, ...S_j^{T_i}, ...S_{M-1}^{T_i}\} \qquad 0 < i \leq N$

Où $M = 100/\delta$ et $S_j^{T_i} = [j\delta\%, (j+1)\delta\%]$, δ est la précision choisie pour les intervalles des états C et $0 \leq j < N$

$F = \{F^S, F^E\}$

4.3.2.2 Les actions

Deux actions $A_s^{T_i}$, présentées dans le système (4.1), peuvent être choisies durant une période de temps T_i et pour un état $s \in C$. La première action A_m consiste à envoyer immédiatement le message ; la deuxième action A_w retarde son envoi d'une période de temps. Un message est retardé jusqu'à ce qu'il rencontre une décision d'envoi immédiat ou que sa durée de validité expire.

$$A_s^{T_i} = \begin{cases} \{A_w, A_m\} & Si \quad s^{T_i} \in C \quad et \quad i < N \\ A_m & Si \quad s^{T_i} \in C \quad et \quad i = N \end{cases} \tag{4.1}$$

4.3.2.3 Les récompenses et coûts

Chaque décision est prise afin de maximiser un gain final, celui-ci représente le taux de réception pour un message envoyé. Son calcul dépend des $R(s'^{T_{(i+1)}}, s^{T_i})$ obtenus lors des transitions entre états. Ils peuvent représentés des récompenses attribuées ou des coûts à déduire. Une récompense R_s est attribuée lorsque un message est envoyé avec succès, alors qu'un coût R_f est infligé lorsque l'envoi échoue. Le coût induit par l'ajournement d'un message d'une période de temps, R_w, est le troisième paramètre pris en considération lors de la prise de décision. Cette définition est résumée dans le système (4.2).

La récompense R_s est toujours positive, pour motiver les véhicules à envoyer leur message. Alors que les coûts liés à l'échec de l'envoi et au délai additionnel du retard sont soit négatifs ou égaux à zéro. La valeur de chacun de ses paramètres peut être pondérée à la catégorie d'accès (AC) du message à envoyer.

$$R(s'^{T_{(i+1)}}, s^{T_i}) = \begin{cases} R_s & Si\ s'^{T_{(i+1)}} = F^S,\ s^{T_i} \in C,\ a = A_m \\ R_f & Si\ s'^{T_{(i+1)}} = F^E,\ s^{T_i} \in C,\ a = A_m \\ R_w & Si\ s'^{T_{(i+1)}},\ s^{T_i} \in C,\ a = A_w,\ i < N \end{cases} \tag{4.2}$$

4.3.2.4 Les probabilités de transition

Enfin, une modélisation en MDP comporte des probabilités de transition $P(s'^{T_{(i+1)}}|a, s^{T_i})$ pour chaque action a choisie entre deux états du processus. Les probabilités de transition, quand l'action choisie est celle de retarder le message A_w, sont les mêmes que les probabilités d'être à l'état $s'^{T_{(i+1)}}$ d'occupation du canal à la période de temps $T_{(i+1)}$. Pour avoir des probabilités représentatives, chaque véhicule enregistre son historique local du taux d'occupation du canal durant α intervalles *CCH*. Alors il calcule le pourcentage moyen d'occupation dans le temps pour chaque période de l'intervalle *CCH*.

Quand l'action choisie est celle de l'envoi, A_m, deux probabilités sont possibles, celle de l'envoi avec succès et celle avec échec. L'une est complémentaire à l'autre, elles sont calculées sur la base du pourcentage de l'occupation du canal au moment de l'envoi, soit l'état s, ainsi que l'efficacité de réception à cette même période de temps E^{T_i}. L'efficacité est le ratio entre le temps d'occupation qui a servi à la réception avec succès d'un nombre de messages NM^{T_i}, avec une taille moyenne de $Size$ et un débit de D et le temps total d'occupation du canal à cette même période T_i, son calcul est donné dans l'équation (4.3). Ces deux paramètres d'occupation et d'efficacité du canal sont pondérés dans les probabilités d'envoi avec succès ou échec par la variable $\rho \in [0, 1]$. Ce dernier est un paramètre d'entrée, sa valeur doit privilégier le paramètre efficacité lorsque le canal est souvent surchargé, car le paramètre occupation du canal perdrait de sa valeur à ce moment là (car tout le temps élevé). Le système (4.4) résume les valeurs possibles pour les probabilités de transition.

$$E^{T_i} = \frac{NM^{T_i} \times \frac{Size}{D}}{\frac{\delta \times s}{100} \times t} \tag{4.3}$$

$$P(s'^{T_{(i+1)}}|a, s^{T_i}) = \begin{cases} P(s'^{T_{(i+1)}}) & Si\ s^{T_i},\ s'^{T_{(i+1)}} \in C,\ a = A_w \\ P(s'|a, s^{T_i}) & Si\ s^{T_i} \in C,\ s' \in F,\ a = A_m \\ 0 & Sinon \end{cases} \tag{4.4}$$

Où

$$P(s'|a, s^{T_i}) = \begin{cases} P(F^S|A_m, s^{T_i}) = \rho\frac{\delta \times s}{100} + (1 - \rho) \times E^{T_i} \\ P(F^E|A_m, s^{T_i}) = 1 - P(F^S|A_m, s^{T_i}) \end{cases}$$

4.3.3 Solution au problème

La solution à ce problème est une politique optimale $\pi^\star$ d'actions pour chaque état d'occupation du canal s et période de temps T_i. Une politique π est associée à une matrice $V^\pi(T_i, s)$, pour enregistrer le gain futur maximum pour toutes les combinaisons possibles entre la période de temps T_i et l'état d'occupation du canal s pour un véhicule.

Algorithme 2: Programmation dynamique pour la résolution du MDP.

Données : $i \in \{1..N\}, \quad s \in C$

Phase 0 :

$\pi(T_i) = \{A_m\}$;
$V^{\pi}(T_i, s) = \{0\}$;
$V'^{\pi}(T_i, s) = \{0\}$;

Phase 1 :

repeat
  $V'^{\pi}(T_i, s) = V^{\pi}(T_i, s)$;
  while $(i < N)$ **do**
    while $(s \in C)$ **do**
      Phase 1.a :
      $V_m =$
      $P(F^S|A_m, s^{T_i}) \times (R_s + V^{\pi}[T_i, F^S]) + P(F^E|A_m, s^{T_i}) \times (R_f + V^{\pi}[T_i, F^E])$;
      $V_w = \sum_{s'}^{C} P(s'^{T_{i+1}}|A_w, s^{T_i}) \times (R_w + V^{\pi}[T_i, s'])$;
      Phase 1.b :
      if $(V_w < V_m)$ **then**
        $\pi[T_i] = A_m$;
        $V^{\pi}[T_i, s] = V_m$;
      else
        $\pi[T_i] = A_w$;
        $V^{\pi}[T_i, s] = V_w$;

until $(V'^{\pi}(T_i, s) - V^{\pi}(T_i, s) < \epsilon)$;

Phase 2 :

$\pi(T_i)^{\star} = \pi(T_i)$;

Afin de déterminer $\pi^{\star}$, nous utilisons *la programmation dynamique* [83], qui consiste à faire autant d'itérations que nécessaire pour obtenir la convergence des résultats, soit que les décisions prises pour chaque combinaison soient fixes, ainsi que leur gain final correspondant ne puissent changer que d'un pas minime ϵ. Nous considérons comme négligeable le temps de convergence des données, car le nombre de combinaisons possibles est un nombre fini, de même, nous considérons comme importantes les capacités du processeur d'un véhicule.

4.3.4 Algorithme de résolution

Ces étapes sont décrites dans l'algorithme 2. Nous initialisons, durant la *Phase 0*, toutes les décisions de notre politique $\pi(T_i)$ à celles de l'envoi A_m, tous les gains finaux $V^{\pi}(T_i, s)$ à 0 et nous ajoutons une matrice prime $V^{'\pi}(T_i, s)$ à laquelle nous nous comparerons pour vérifier la convergence des résultats. Durant la *Phase 1*, nous commençons par enregistrer les anciennes valeurs de la matrice des gains finaux dans la matrice prime, afin de réaliser une comparaison à la fin de l'itération. Puis, lors de la *Phase 1.a*, nous calculons les gains V_m et V_w pour chaque combinaison alliant le paramètre temps T_i et l'état du canal s. Les deux valeurs, V_m et V_w, correspondent aux gains de l'action de l'envoi immédiat A_m et à celui de l'action de l'ajournement A_w, respectivement. V_m est la somme des deux probabilités du succès et de l'échec pour un envoi de message, chacune de ces probabilités est multipliée par : la récompense ou le coût correspondant, ainsi que la dernière valeur du gain obtenu pour la même combinaison. Le gain V_w est calculé à partir de la somme des probabilités de transitions, à la période de temps suivante, vers tous les états d'occupation du canal possibles, représentés par s', cette transition a lieu lorsque le véhicule décide de retarder l'envoi de son message. La somme de toutes ces probabilités est multipliée par le coût infligé par notre modèle pour chaque période d'ajournement, ainsi qu'à la valeur du gain précédent pour cette même combinaison.

Nous comparons dans la *Phase 1.b* le gain généré par les deux actions, soit V_m et V_w. Nous enregistrons pour chaque combinaison le gain maximum dans la matrice $V^{\pi}(T_i, s)$, ainsi que la décision correspondante dans la politique $\pi(T_i)$. Lorsque la différence des gains entre deux itérations successives est minime, à savoir inférieure à ϵ, nous stoppons les itérations et enregistrons la dernière version de la politique d'actions, cette dernière est considérée comme étant la politique optimale et marque la fin de la *Phase 2*.

Un message n'est envoyé que lorsque le véhicule atteint une combinaison de temps et d'état d'occupation du canal qui a comme décision optimale l'action d'envoyer A_m. Sinon, le véhicule retarde d'une, de deux, ou de (N-1) périodes de temps l'envoi de son message, afin de maximiser ses chances d'envoi avec succès, cela à condition de ne pas dépasser la durée de validité de l'information.

4.4 Évaluation de performance

Nous évaluons les performances de notre solution, DMS, en étudiant sa capacité à équilibrer la charge du trafic sur un intervalle *CCH* et celle d'éviter les collisions synchronisées à son début. Pour cela, nous mesurons le taux d'occupation du canal lors du déploiement de quatre différentes solutions. La première solution déployée est la configuration standard de la couche MAC de l'IEEE 802.11p/1609.4 que nous nommons *Standard IEEE 1609.4*. En second, nous déployons une solution que nous nommons *Ajournement aléatoire*, dont le principe est de différer l'envoi d'un message avec un retard aléatoire compris entre 0 et 100 ms. La solution *WAB* proposée dans [39], est la troisième

approche déployée dans notre étude de performances, elle calcule la priorité d'envoi d'un message d'après le taux d'occupation du canal et le nombre de fois qu'un message a été retardé, soit par décision de retard ou à cause de l'expiration de l'intervalle *CCH*. Un message est retardé dans *WAB* en rejouant à nouveau son *back-off* avec une fenêtre de contention doublement plus grande. Notre solution *DMS* est déployée en quatrième approche.

Pour notre évaluation de performances, nous avons choisi quatre métriques :

- Le pourcentage moyen d'occupation du canal durant les intervalles *CCH*.
- Le pourcentage de messages perdus, qui est directement lié à l'envergure des collisions synchronisées au début des intervalles *CCH*.
- Le pourcentage de réception des messages envoyés avec succès durant les intervalles *CCH*. Cette troisième métrique nous retourne uniquement la moyenne du pourcentage de réception des messages, qui ont été reçus au moins une fois par un véhicule voisin. Ceci afin d'étudier les effets des collisions indirectes et ceux de la mobilité des véhicules, indépendamment de ceux des collisions directes étudiées dans la deuxième métrique.
- La quatrième métrique concerne le délai de bout en bout des messages envoyés, afin de vérifier leur validité dans le temps à leur réception.

Nos simulations ont été conduites sur NS2 [1], muni de l'extension [44] pour modéliser la partie IEEE 1609.4 qui gère le multi-canal. Alors, tous les véhicules écoutent le canal de contrôle durant la première moitié de l'intervalle de synchronisation, alors qu'ils restent libres de rester sur ce canal ou de changer pour un des six canaux de service durant la deuxième moitié.

La charge de trafic dans nos simulations est constituée par l'envoi de 10 messages de sécurité routière chaque seconde, par chaque véhicule, d'après une distribution de Poisson. Chacun de ces messages appartient à une catégorie d'accès (AC) allant de 0 à 3 d'après une distribution uniforme.

Afin d'évaluer les performances de notre solution nous varions la charge du trafic sur le canal, pour cela nous modifions le nombre de véhicules partageant la même portée réseau et introduisons de la mobilité. Car tous les messages échangés sont envoyés par diffusion une seule fois par le véhicule source, sans être retransmis par aucun véhicule à sa réception, nous supposons dans un premier temps un scénario où les véhicules restent statiques. En effet, si nous nous intéressons durant notre étude qu'aux performances du canal durant les intervalles *CCH* et qu'aux véhicules partageant la même portée réseau, nous pouvons considérer la mobilité des véhicules durant les 46 ms, que représente un intervalle *CCH* dont est déduit son intervalle de *garde*, comme minimale. Notre supposition sur la non mobilité des véhicules a aussi été considérée dans les études [38], [105], [30], [104] et [31]. En choisissant des véhicules côtes à côtes et partageant la même portée réseau, ce premier scénario ignore les pertes de messages dues aux interférences des fréquences radios et les collisions dues aux stations cachées, ce qui purifie les résultats de notre simulation des bruits indésirables.

Pour notre premier scénario :

- Nous avons choisi de déployer 40 véhicules statiques, afin d'occuper entièrement le canal durant l'intervalle *CCH* lorsque tous les véhicules enverront de façon ordonnancée un message lors de chaque intervalle de synchronisation. La taille et le débit utilisés pour l'envoi sont ceux spécifiés dans les paramètres de simulation dans le tableau 4.2.
- Ces véhicules échangent des messages durant une durée de simulation de 10 secondes,

Table 4.2 – Paramètres de simulation.

Nombre de véhicules	40, 100
Taille des paquets	400 octets
Portée de transmission	250 m
Débit	3 Mbps
Vitesse moyenne	120 km/h
Longueur de l'autoroute	10 Km
Générateur de mobilité	VanetMobiSim [40]
Taille de la fenêtre de contention CW	15
Durée de l'intervalle de *garde*	4 ms
Durée de l'intervalle de synchronisation	100 ms
Durée des intervalles *CCH* et *SCH*	50 ms
Délai maximum de retard pour AC3	60 ms
Délai maximum de retard pour AC2	80 ms
Délai maximum de retard pour AC1	100 ms
Délai maximum de retard pour AC0 :	100 ms
t = taille du paquet/débit	δ=5
$\rho = 0.5$	α =5
$R_s = 0$	$R_f = -5$
R_w = -10 dés que le délai additionnel > délai maximum de retard pour l'AC	

ce qui équivaut à 100 intervalles *CCH*.

Pour notre deuxième scénario :

– Nous simulons 100 véhicules mobiles sur une autoroute.

– Avec une vitesse moyenne de 120 km/h.

– Durant 100 secondes, ce qui équivaut à 1000 intervalles *CCH*.

Ce deuxième scénario inclut les effets de la mobilité et des collisions indirectes dans l'étude de performances. Plus de paramètres de simulation sont donnés dans le tableau 4.2.

4.4.1 Taux d'occupation du canal

La mauvaise gestion des ressources du canal lors de l'utilisation de l'IEEE 1609.4 affaiblit les performances des applications de sûreté. Nous débuterons notre étude de performances par la métrique concernant l'évolution de l'occupation du canal tout au long des intervalles *CCH*, afin de déterminer la bonne ou mauvaise gestion de ses ressources. Pour calculer le taux d'occupation du canal au long de l'intervalle *CCH*, nous utilisons les informations collectées à partir de la couche physique de chaque véhicule. Celles-ci donnent les intervalles de temps pendant lesquelles le canal était considéré comme occupé ou comme libre par le véhicule. Nous divisons l'intervalle *CCH* en période de temps de longueur t et nous calculons pour chacune d'elles le pourcentage d'occupation par rapport aux données de la couche physique.

Les figures 4.3 et 4.4 illustrent le pourcentage moyen pour tous les véhicules présents durant la simulation à propos de l'occupation du canal, durant un intervalle *CCH*, lors de chacun de nos deux scénarios. Comme on peut le remarquer l'occupation du canal est déséquilibrée lors du déploiement des solutions *"Standard IEEE 1609.4"* et *"Ajournement*

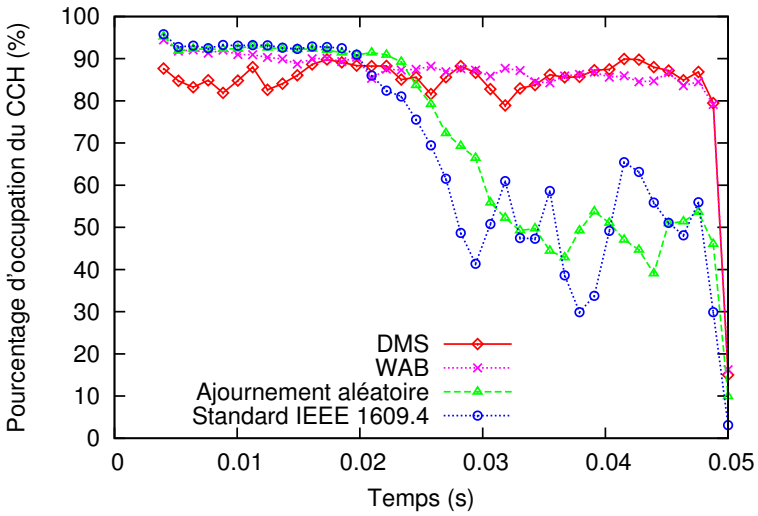


FIGURE 4.3 – Pourcentage moyen d'occupation du canal durant un intervalle *CCH* avec 40 véhicules statiques.

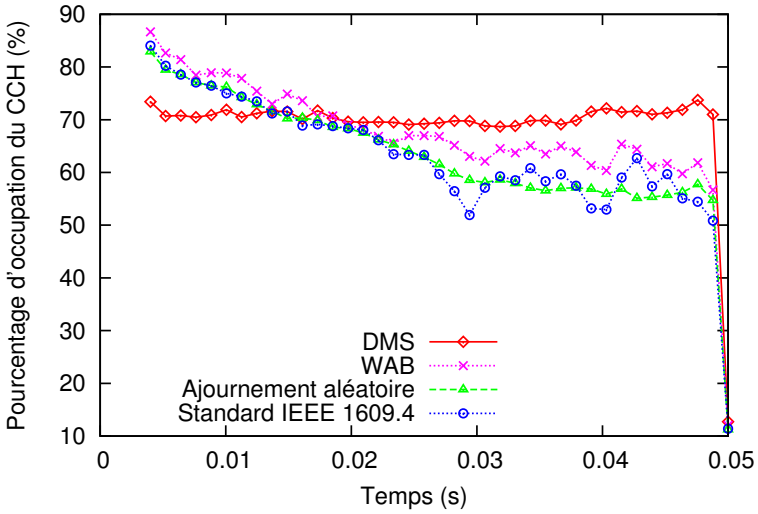


FIGURE 4.4 – Pourcentage moyen d'occupation du canal durant un intervalle *CCH* avec 100 véhicules mobiles.

aléatoire". Ce déséquilibre est occasionné par les messages de sûreté générés durant la deuxième moitié de l'intervalle de synchronisation, soit durant l'intervalle *SCH* et qui sont stockés jusqu'au début de l'intervalle *CCH* suivant. Leur mise en attente induit à ce qu'ils soient envoyés dés le début de l'intervalle *CCH*, ce qui crée un envoi simultané dans le réseau, cela a pour conséquence un taux d'occupation très important au début de l'intervalle *CCH*.

Le pourcentage d'occupation du canal lors du premier scénario est donné dans la figure 4.3. Durant ce scénario, la charge du trafic est importante car 40 véhicules se trouvent à portée l'un de l'autre et partagent donc les mêmes ressources du canal. Le pourcentage d'occupation du canal atteint les 90% au tout début de l'intervalle *CCH* pour chacune des trois solutions suivantes : *Standard IEEE 1609.4*, *Ajournement aléatoire* et *WAB*. Ce pourcentage reste important durant la première moitié de l'intervalle, mais décroit suffisamment pour atteindre une moyenne de 50% lors de la deuxième moitié de

l'intervalle, ce qui démontre le déséquilibre de la charge du trafic et l'absence de gestion des ressources. Contrairement à ces trois solutions, lors de l'utilisation de *DMS*, le pourcentage d'occupation du canal reste stable avec une moyenne d'occupation de 85% tout au long de l'intervalle *CCH*. Ce résultat est atteint grâce aux retards proportionnels à chaque type de messages, ajoutés par la solution, afin de répartir la charge du trafic tout au long de l'intervalle *CCH*.

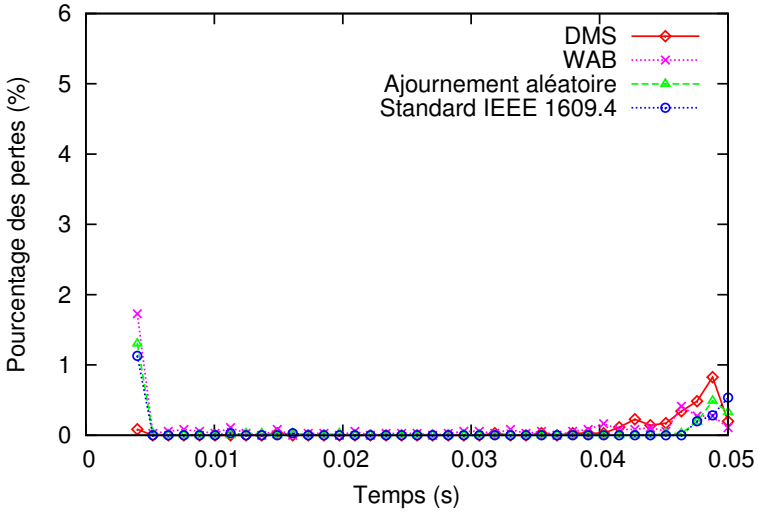
Les résultats concernant le deuxième scénario sont représentés dans la figure 4.4. Les véhicules y sont mobiles, en conséquence leur topologie change fréquemment, ainsi que la densité en véhicules de leur portée de transmission. Le pourcentage d'occupation du canal et son déséquilibre dans ce scénario sont moins importants que dans le premier, ce qui permet même à notre solution *DMS* d'atteindre une répartition de charge presque parfaite sur le canal. Contrairement à *DMS*, la solution *WAB* échoue dans le rééquilibrage de la charge du trafic au long de l'intervalle *CCH*, car son choix d'envoyer immédiatement ou de retarder un message ne se base que sur deux paramètres. Le premier est la priorité calculée à partir du taux d'occupation du canal, le deuxième est le nombre de fois que le message a été retardé par le passé, en considérant toutes les fois où il a été retardé par décision de la solution ainsi que celles dues à l'expiration de l'intervalle *CCH*. Alors que *DMS* prend aussi en considération l'efficacité de l'envoi durant les périodes de temps composant un intervalle *CCH*. Cette efficacité est jugée par rapport au nombre de messages qu'un véhicule a reçu durant une période de temps comparé au pourcentage d'occupation total du canal à cette même période. Ce paramètre d'efficacité met en évidence le temps où le canal est occupé à cause des collisions.

4.4.2 Perte de messages

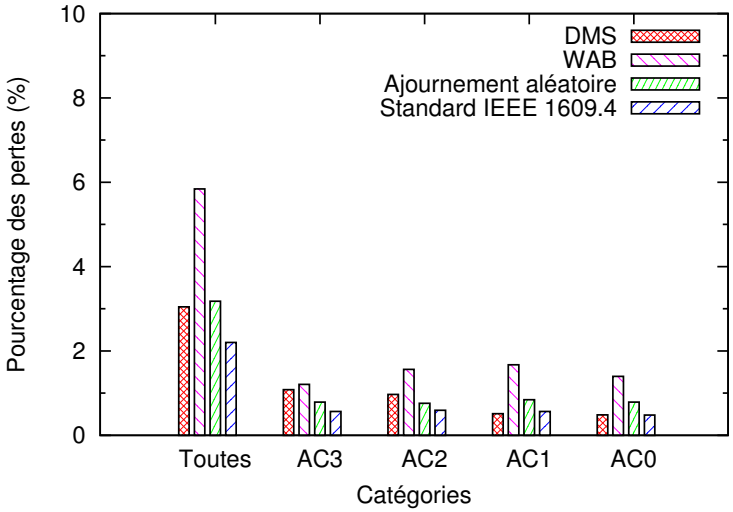
Pour évaluer l'étendue des collisions synchronisées dans nos deux scénarios, nous analysons à travers les figures 4.5 et 4.6 le pourcentage des messages perdus suite à des collisions ou à des erreurs lors d'un acheminement à un seul saut. Pour cela nous étudions le pourcentage de pertes au cours d'un intervalle *CCH* dans les figures 4.5(a) et 4.6(a), puis la moyenne des pertes par catégorie d'accès (AC) dans les figures 4.5(b) et 4.6(b).

Nous remarquons dans les figures 4.5(a) et 4.6(a) que le pourcentage de pertes au début de l'intervalle *CCH* est très élevé pour les trois approches concurrentes à *DMS* au cours des deux scénarios choisis. Cela se traduit par l'ampleur des envois synchronisées dus à la mise en attente des messages. Ce pourcentage de pertes est au alentour de 1.5% durant le premier scénario, mais accroit énormément lors du second scénario à cause du nombre plus élevé de véhicules. Il atteint 9% de l'ensemble des messages envoyés durant la simulation pour l'approche *Standard IEEE 1609.4*, 8% pour celle de l'*Ajournement aléatoire* et 6% pour *WAB*. Alors que ce même pourcentage de pertes au début de l'intervalle *CCH* est égal à 0.08% lors du premier scénario et à 0.6% lors du second, avec l'utilisation de *DMS*. Ces pourcentages démontrent la capacité ou pas d'une solution à sélectionner les messages à envoyer et ceux à retarder lorsque la concurrence est rude pour l'accès au canal. Ils sont bas lors de l'utilisation de *DMS* car des retards sont introduits à l'envoi de chaque message d'après l'historique de l'occupation du canal ainsi que la durée de validité lui restant, afin de désynchroniser de manière distribuée l'envoi des messages au début des intervalles *CCH*.

Sur ces mêmes figures, nous remarquons aussi une légère perte de message à la fin de l'intervalle *CCH*, soit juste avant le passage à l'intervalle de *garde*. Cette perte est plus importante pour notre solution, *DMS*, mais reste inférieur à 1% des messages envoyés pour les deux scénarios. Elle est due à la contrainte de temps imposée par *DMS* pour l'envoi du message, à savoir qu'aucun message ne doit dépasser le délai maximum de retardement fixé



(a) Pourcentage moyen de pertes au cours d'un intervalle *CCH*

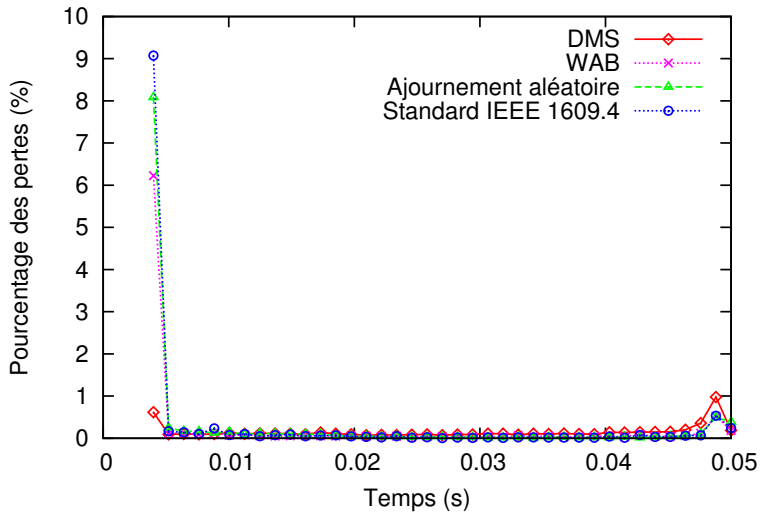


(b) Pourcentage moyen de pertes pour les différentes catégories d'accès

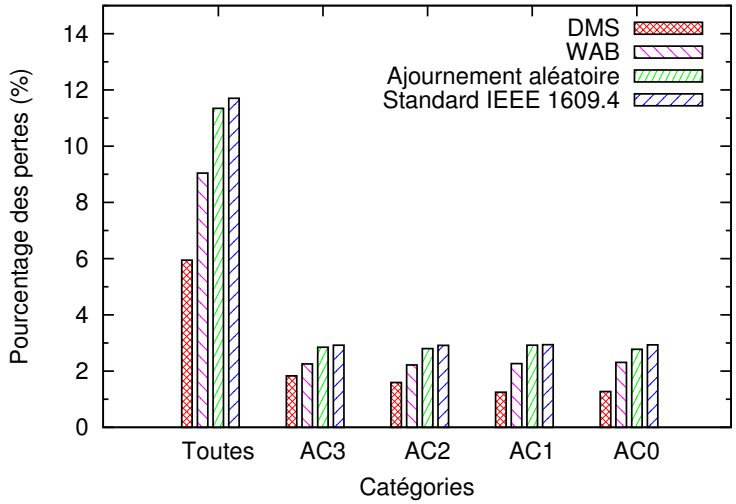
FIGURE 4.5 – Pourcentage moyen de pertes, avec 40 véhicules statiques.

pour sa catégorie d'accès. Alors, beaucoup des véhicules qui n'ont pas encore eu l'occasion d'envoyer leur message durant l'intervalle *CCH* et ceux dont le message a été généré à la fin de l'intervalle *CCH* sont dans l'obligation d'envoyer leur message avant la fin de l'intervalle, même si celui-ci est occupé. Car l'attente de l'intervalle suivant rajouterai 54 ms au délai de transmission à cause des intervalles de *SCH* et de *garde* et risquerai donc de faire expirer la durée de validité de l'information.

Les figures 4.5(b) et 4.6(b) illustrent le pourcentage moyen de pertes au cours d'un intervalle *CCH* pour toutes les catégories de messages, puis pour chacune d'elles séparément, afin de vérifier si les différents délais maximums fixés par notre solution *DMS* influencent sur ce taux. Dans le premier scénario, le pourcentage moyen de pertes est le plus élevé pour la solution *WAB*, il atteint 5.8%. Ce résultat est conforme à ce que nous avions remarqué dans la figure 4.5(a), à savoir que cette solution gère le moins bien les collisions synchronisées du début de l'intervalle *CCH*. Les deux autres solutions concurrentes, *Standard IEEE 1609.4* et *Ajournement aléatoire* ont chacune un pourcentage



(a) Pourcentage moyen de pertes au cours d'un intervalle *CCH*

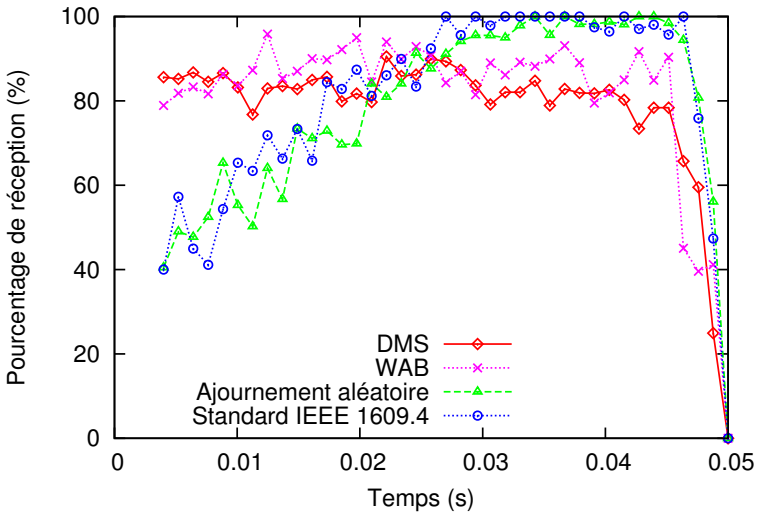


(b) Pourcentage moyen de pertes pour les différentes catégories d'accès

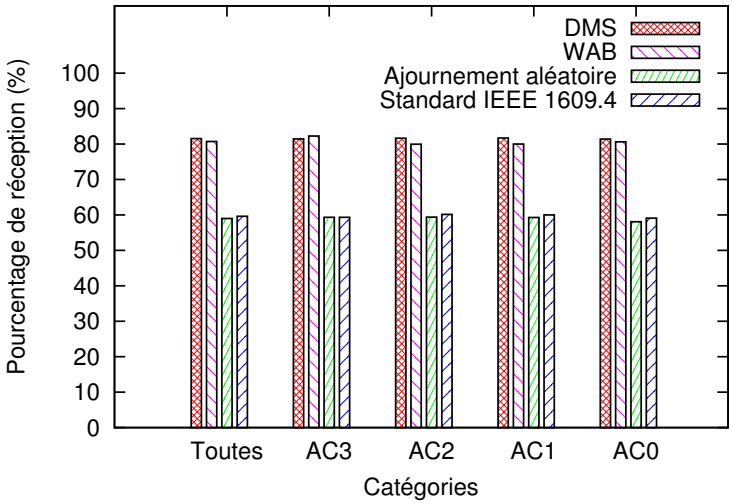
Figure 4.6 – Pourcentage moyen de pertes, avec 100 véhicules mobiles.

moyen de pertes de 2.2% et de 3.1%, respectivement. *DMS* a un taux moyen de pertes de 3%. Contrairement aux résultats dans le premier scénario, ces derniers sont plus importants dans le deuxième. Le taux moyen de pertes atteint 11.7% pour la solution *Standard IEEE 1609.4*, 11.3% pour la solution *Ajournement aléatoire*, 9% pour celle de *WAB* et enfin 5.9% pour notre solution *DMS*, ce qui marque une nette réduction du taux de pertes par rapport aux trois autres solutions.

Car *DMS* est la seule solution à imposer des délais de transmission maximums et différents pour chaque catégorie d'accès, soit 60 ms pour AC3, 80 ms pour AC2 et 100 ms pour AC1 et AC0, le pourcentage moyen de pertes entre ces catégories d'accès diffère seulement lorsque leurs délais maximums diffèrent. Cette différence existe seulement pour *DMS* et est légère, elle est au plus égale à 0.6% dans nos deux scénarios. Cette différence privilégie les catégories d'accès avec le plus de délais de transmission, soit AC1 et AC0 dans notre cas, car l'envoi est moins contraignant dans le temps et il existe donc plus de choix pour la période d'envoi.



(a) Pourcentage moyen de réception d'un message au cours d'un intervalle *CCH*



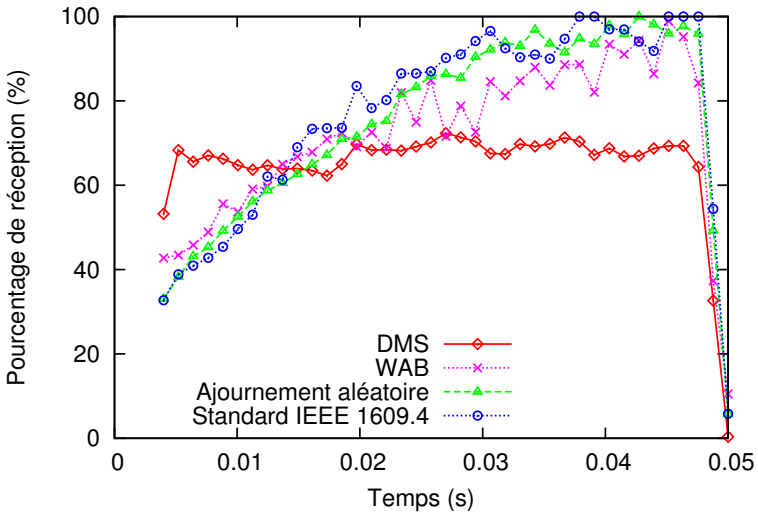
(b) Pourcentage moyen de réception d'un message pour les différentes catégories d'accès

FIGURE 4.7 – Pourcentage moyen de réception, avec 40 véhicules statiques.

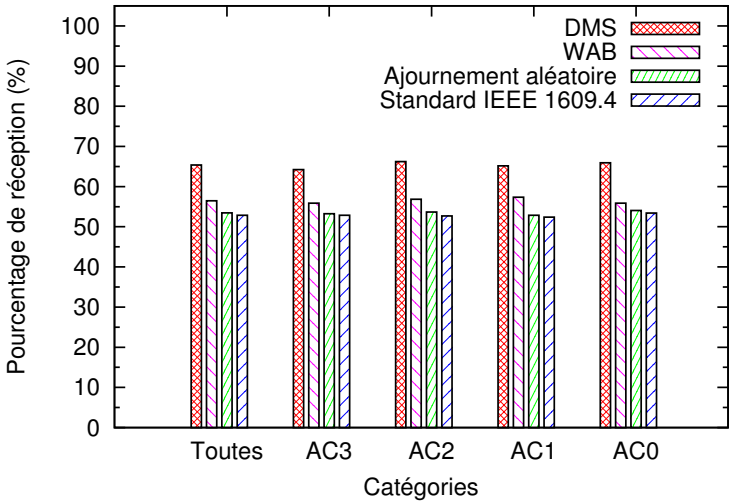
4.4.3 Taux de réception des messages

Afin d'étudier le taux de réception des messages envoyés avec succès auprès des véhicules concernés par, nous considérons uniquement les messages reçus au moins une fois. Nous mesurons et illustrons dans les figures 4.7 et 4.8 leur pourcentage de réception auprès des voisins directs de la source, à savoir tous les véhicules qui sont à la portée réseau de la source. Cette métrique est différente de la précédente, car elle ne s'intéresse qu'aux messages au moins une fois reçus, ce qui exclut les messages perdus. Par conséquent, elle ne s'intéresse qu'aux effets des collisions indirectes et des stations cachées sur le pourcentage de réception des messages, ainsi que ceux de la mobilité au cours du second scénario.

Dans les figures 4.7(a) et 4.8(a), le pourcentage de réception est illustré au cours d'un intervalle *CCH* pour nos deux scénarios. Les courbes de pourcentage sont à l'inverse de celles de l'occupation du canal dans les figures 4.3 et 4.4, car plus le canal est libre et



(a) Pourcentage moyen de réception d'un message au cours d'un intervalle *CCH*



(b) Pourcentage moyen de réception d'un message pour les différentes catégories d'accès

Figure 4.8 – Pourcentage moyen de réception, avec 100 véhicules mobiles.

plus le pourcentage de réception d'un message est élevé. Dans le premier scénario, les deux solutions *Standard IEEE 1609.4* et *Ajournement aléatoire* ont un pourcentage de réception assez bas au début de l'intervalle *CCH*. Il est égal à 40%, puis il varie et accroît jusqu'à atteindre une moyenne de 95%, cette évolution est due à celle de l'occupation du canal. Au début de l'intervalle, la charge du canal est très importante et les quelques messages envoyés qui ne rencontrent pas de collisions directes rencontrent tout de même des collisions indirectes par la suite, ce qui diminue de leur taux de réception auprès des véhicules voisins. Le reste de l'intervalle *CCH* est peu occupé à cause de la mauvaise gestion des ressources du canal, ce qui laisse le champ libre au peu de messages qui restent à envoyer. C'est pour cette raison que le taux de réception augmente énormément vers la deuxième moitié de l'intervalle. Durant ce premier scénario, les deux autres solutions *WAB* et *DMS* arrivent à équilibrer la charge du canal, ce qui leur vaut un pourcentage de réception stable pour les messages envoyés, équivalent à 80%.

Durant le deuxième scénario, la mobilité se rajoute comme contrainte et les performances changent par rapport au premier scénario. Les trois solutions *Standard IEEE 1609.4*, *Ajournement aléatoire* et *WAB* voient leur pourcentage de réception se déséquilibrer davantage, avec un taux inférieur à 35% au début de l'intervalle *CCH* pour les deux premières solutions et égale à 42% pour la troisième. Alors que la solution *DMS* obtient un semblant d'équilibre pour son taux de réception autour de 65%.

Les figures 4.7(b) et 4.8(b) illustrent le pourcentage moyen de réception au cours d'un intervalle *CCH* pour toutes les catégories de messages réunies, puis pour chacune d'elles séparément, lors de nos deux scénarios. Comme déjà constaté, le pourcentage moyen de réception est le plus bas pour les solutions *Standard IEEE 1609.4* et *Ajournement aléatoire* durant le premier scénario, il est égal à 59%. Alors que pour les deux autres solutions restantes, il est égal à 80% pour *WAB* et à 81% pour *DMS*. Durant le deuxième scénario, les performances des trois solutions concurrentes s'affaiblissent davantage, le pourcentage moyen de réception est égal à 52% pour *Standard IEEE 1609.4*, à 53% pour *Ajournement aléatoire* et à 56% pour *WAB*, alors qu'il est égal à 65% pour notre solution *DMS*. Ceci prouve sa capacité à bien appréhender la charge d'occupation du canal pour choisir les moments opportuns à l'envoi des messages, afin d'éviter les collisions directes et indirectes. Ce pourcentage de réception reste inchangé pour les différentes catégories d'accès malgré les contraintes de temps que *DMS* impose, ce qui démontre la stabilité de notre solution.

4.4.4 Délai de transmission

Notre quatrième métrique s'intéresse au temps de retard induit par chacune des quatre solutions implémentées, afin de vérifier, grâce au délai d'acheminement, si l'information est toujours valide dans le temps une fois reçue et éviter de surcharger le canal avec des informations plus d'actualité. Notre solution, *DMS*, fixe dés le départ un délai maximum pour l'ajournement possible de chacune des catégories d'accès, ceci à travers les coûts liés au retard, R_w, afin de rendre inintéressant l'envoi d'un message après un certain temps de retard.

La figure 4.9 illustre ce délai de bout en bout lors de l'envoi de messages durant le premier scénario. Car la solution *Standard IEEE 1609.4* n'ajoute délibérément aucun retard avant l'envoi d'un message, son délai de bout en bout est le plus court, il est égal à 21 ms. La deuxième solution, *Ajournement aléatoire*, induit un retard aléatoire compris entre 0 et 100 ms, son délai de bout en bout moyen est de 71 ms. La solution *WAB* a les délais les plus critiques, son délai moyen de bout en bout est égal à 178 ms. Ce dernier est le plus long car la solution n'impose aucune limite au temps de retard induit. Elle base son ajournement sur la réitération du mécanisme du *back-off* d'un message en doublant au fur et à mesure la taille de sa fenêtre de contention. Cet ajournement est allongé dans le temps à chaque fois que le mécanisme du *back-off* est mis en pause à cause de l'occupation du canal. En plus de cela, le nombre maximum de réitérations n'est pas fixé, un envoi n'est effectué que lorsque sa priorité, avec en paramètre le nombre de fois dont il a été retardé par le passé, dépasse une valeur générée aléatoirement et comprise entre 0 et 1.

Notre solution *DMS* a un délai moyen de bout en bout égal à 48 ms dans le premier scénario et à 49 ms dans le deuxième, dont les résultats sont illustrés dans la figure 4.10. Cela démontre que malgré la mobilité et la densité changeante des véhicules, la solution respecte ces contraintes en temps, ce qui n'est pas toujours le cas des autres solutions. Les délais de bout en bout des solutions *Standard IEEE 1609.4* et *Ajournement aléatoire* ne varient pas dans le deuxième scénario à la différence de ceux de la solution *WAB*, à savoir que son délai moyen de bout en bout est égal à 103 ms dans le deuxième scénario, ce changement important nous interpelle sur le passage à l'échelle d'une telle solution.

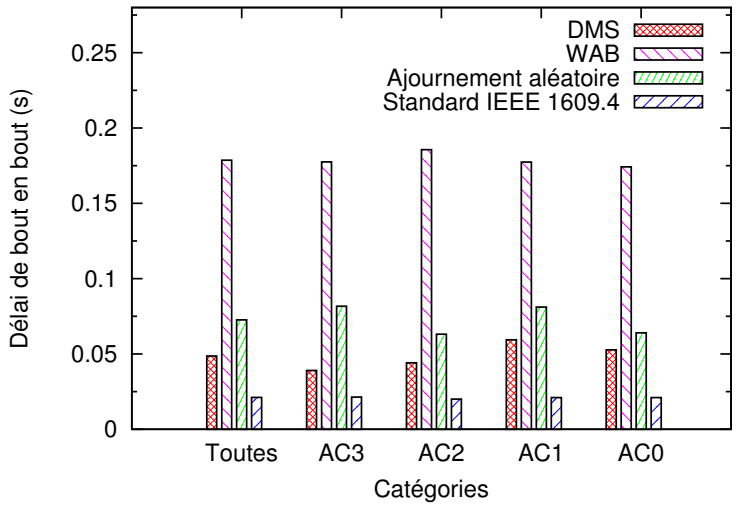


Figure 4.9 – Délai moyen de bout en bout pour les différentes catégories d'accès, avec 40 véhicules statiques.

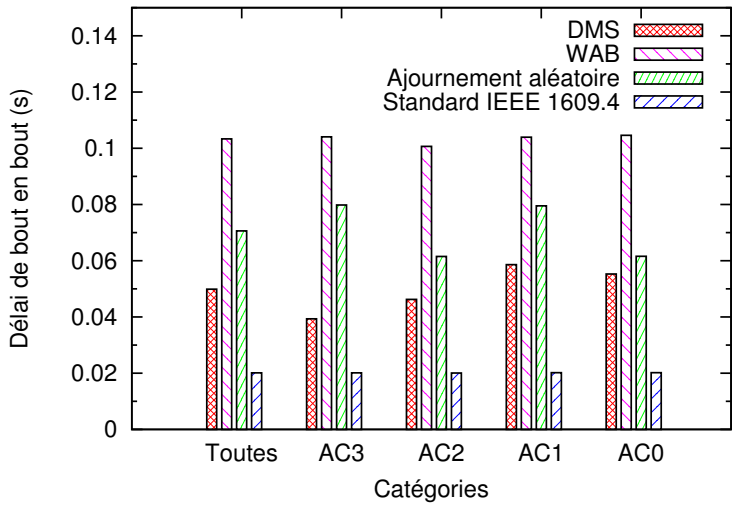


Figure 4.10 – Délai moyen de bout en bout pour les différentes catégories d'accès, avec 100 véhicules mobiles.

DMS respecte aussi les contraintes en temps de chacune des catégories d'accès, tel que le délai de bout en bout moyen des messages AC3, dont le délai de retard maximum est de 60 ms, est égal à 39 ms dans les deux scénarios. Ce délai est égal à 45 ms pour AC2 dont le maximum toléré est de 80 ms et enfin égal à 55 ms pour AC1 et AC0, dont le maximum est de 100 ms. Ces résultats démontrent l'aptitude de *DMS* à répartir la charge du canal équitablement tout au long d'un intervalle *CCH*, tout en respectant les contraintes de temps de chaque catégorie de messages.

Une application peut modifier les délais maximums tolérés pour chacune des catégories d'accès de message et adapter à son gré les valeurs des coûts et récompenses, afin de satisfaire ses propres critères de qualité de service.

4.5 Conclusion

Durant ce chapitre, nous avons traité la problématique de la mal-répartition dans le temps de la charge du canal de contrôle pour les réseaux véhiculaires. Cette problématique est due à l'utilisation du multi-canal dans le standard IEEE 802.11p/1609.4, qui alloue la première moitié de l'intervalle de synchronisation exclusivement à la diffusion des messages de sécurité routière sur le canal de contrôle et la deuxième moitié aux restes des applications. La mise en attente des messages de sûreté durant la seconde moitié génère une importante compétition entre les véhicules pour l'accès au canal dés le commencement de l'intervalle *CCH*, ce qui crée une surcharge du canal à ce moment là et d'importantes collisions synchronisées.

Nous avons proposé DMS, un ordonnanceur distribué au niveau de la couche MAC, pour améliorer la répartition de la charge sur le canal durant les intervalles *CCH*, limiter les pertes de messages à cause des collisions synchronisées et améliorer le taux de réception des messages envoyés. DMS est inspiré de *la théorie de l'arrêt optimal* pour choisir l'instant propice à l'envoi d'un message qui maximisera son taux de réception, tout en prenant en considération le retard maximum que son contenu peut tolérer. Ces choix sont basés sur l'historique que détient un véhicule à propos de l'occupation du canal et de l'efficacité de l'envoi de chacune des périodes composant un intervalle *CCH*. DMS est modélisé via un processus de décision Markovien, en instaurant une récompense pondérée par les chances de succès de l'envoi d'un message à un moment donné et des coûts aux risques d'échec de l'envoi et au retard ajouté avant l'envoi.

Notre étude de performances montre la qualité de DMS par rapport aux autres solutions auxquelles nous nous sommes comparés. DMS réussi à atteindre un semblant d'équilibre dans la répartition de la charge du canal tout au long de l'intervalle *CCH*, cela dans les deux cas de véhicules mobiles et statiques. Cette capacité lui permet de réduire de 80% le pourcentage de pertes de messages au début des intervalles *CCH*, soit les pertes à cause des collisions synchronisées. Notre étude a démontré qu'en plus d'éviter les pertes à cause des collisions directes, DMS augmentait le pourcentage de réception des messages envoyés avec succès de 25%, soit que DMS diminuait de l'effet des collisions indirectes souvent liées aux stations cachées. Ces résultats sont obtenus alors que DMS est restreint par les délais de retard maximums fixés pour chaque type d'informations.

Ces travaux ont été conduits dans le but d'améliorer les performances des applications de sûreté et d'équilibrer la charge du réseau en évitant de le surcharger avec des informations passées d'actualité. Une autre problématique nous vient à l'esprit : *Est-ce que tout ces messages sont assez fiables pour être relayés ? Sommes nous sûres de la validité des informations que nous recevons en tant qu'utilisateur ? Ne serait-ce pas mieux de faire le tri avant d'envoyer tout ces messages ? Est-ce que tous les utilisateurs sont prêts à coopérer pour envoyer des alertes ou font ils que consommer ?* . Nous nous sommes posés toutes ces questions et nous tentons d'y répondre dans le chapitre suivant.

Chapitre 5

Véhicules malicieux et égoïstes, comment leur faire entendre raison ?

Sommaire

DANS les deux chapitres précédents, nous nous sommes intéressés à améliorer le taux de réception des messages des applications de sécurité routière, ainsi qu'à raccourcir leur délai d'acheminement et à diminuer leur taux de perte, en proposant *ADCD* et *DMS*, des solutions pour la couche réseau et la couche MAC, respectivement. Dans ce chapitre nous abordons deux problématiques liées l'une à l'autre, la première concerne la robustesse en terme de cohérence des informations échangées. En effet des messages falsifiés peuvent être envoyés par des véhicules au comportement malicieux et induire en erreur les autres véhicules, au point même de mettre en danger la vie des passagers. La deuxième problématique de ce chapitre concerne la robustesse de la dissémination collaborative, car l'hypothèse concernant la collaboration des véhicules lors d'une dissémination de messages est souvent émise et considérée comme vraie sans justification.

Dans ce chapitre, nous proposons un modèle de confiance afin de contrer le comportement des véhicules malicieux et les exclure du réseau, tout en incitant les véhicules égoïstes à la coopération au sein du réseau et par cela justifiée l'hypothèse souvent considérée. La difficulté d'une telle proposition réside dans son passage à l'échelle et sa résistance aux contraintes liées aux réseaux ad hoc véhiculaires. En effet, la forte mobilité des véhicules et l'étendue géographique d'un réseau VANET affaiblissent les performances d'un modèle de confiance basé sur la réputation, particulièrement quand celui-ci utilise des listes de révocation pour exclure les véhicules malicieux. Notre modèle de confiance est

conçu pour s'accommoder à ces contraintes et à supporter les comportements malicieux et égoïstes. Pour cela, nous nous basons sur les jeux de signaux [93] et spécifiquement sur le modèle du marché de l'emploi, aussi nommé le modèle de Spence [94].

Ce chapitre est structuré comme suit : La section 5.1 présente notre problématique et définit le contexte et la motivation de notre travail. Dans la section 5.2 nous présentons les différents modèles de confiance existants dans les réseaux véhiculaires. Puis, nous définissons et justifions nos hypothèses dans la section 5.3. Elle est suivie par la section 5.4 où nous présentons le modèle du marché de l'emploi, dont nous prenons exemple. La section 5.5 présente notre solution DTM^2, dont la modélisation par une chaîne de Markov à temps discret et à espace d'états discret est donnée dans le section 5.6, afin de choisir les valeurs de ses paramètres. Dans la section 5.7 nous évaluons les performances de notre modèle de confiance, elle comprend une partie analytique et une autre sur les résultats de simulation. Puis, une analyse de sécurité est détaillée dans la section 5.8. Finalement, la section 5.9 conclut ce chapitre.

5.1 Problématique et contexte

Le bon fonctionnement des applications de sûreté nécessite l'intégrité des données échangées, l'authentification des véhicules sources, l'acheminement des messages en un temps très court et un taux de réception élevé pour les véhicules concernés par une information. Car les informations échangées relèvent de la sécurité des utilisateurs, un usager ne devrait jamais prendre en considération une information reçue sans la garantie de son authenticité. Chaque altération d'un message de sûreté peut causer des accidents, comme par exemple dans le cas où un utilisateur malicieux dissémine une fausse information pour faire dévier de leur route quelques véhicules, alors que la route proposée comprend des dangers tel qu'un glissement de terrain. Cependant, un véhicule n'a pas toujours le temps ou l'occasion de vérifier l'authenticité d'une information en amont, à cause du court de délai de réflexion lié aux informations de sécurité routière. Cette vérification se complique davantage quand aucune infrastructure n'est déployée ou quand elles sont peu nombreuses.

Dans les réseaux collaboratifs ad hoc mobiles tels que les réseaux véhiculaires, les informations concernant le comportement de chaque membre du réseau sont asymétriques à cause de leur nombre important. En plus de cela, la forte mobilité des véhicules et l'étendue géographique importante des réseaux véhiculaires génèrent des connexions sporadiques entre les véhicules et donc des intervalles de rencontre irréguliers [18]. Car établir et maintenir des connexions à un saut avec les autres véhicules est difficile, des membres malicieux et égoïstes sont apparus dans les réseaux véhiculaires. Les véhicules malicieux introduisent de fausses informations ou falsifient les informations reçues avant de les retransmettre. Quelques-uns d'entre eux agissent tout le temps de la sorte, d'autres alternent entre un comportement malicieux et un autre correct, à leur gré. Alors que les véhicules égoïstes ont pour but de servir leurs propres intérêts, mais sans pour autant vouloir porter préjudice aux autres. Ces membres préfèrent utiliser leurs ressources que pour leurs propres besoins, ce qui réduit leur coopération au sein du réseau. À la différence des véhicules malicieux, les véhicules égoïstes sont rationnels, ce qui leur permet de coopérer, par exemple, quand cela leur est profitable.

Les modèles de réputation [71][17] sont souvent utilisés pour remédier à ce genre de problèmes, mais leur efficacité est limitée dans les réseaux véhiculaires à cause des connexions irrégulières entre les membres du réseau, qui ne permettent pas d'établir des réputations fiables. Aussi, la radiation d'un véhicule malicieux peut prendre beaucoup de

temps lors de l'utilisation d'un modèle de réputation, car la convergence des réputations au sein des multiples véhicules est un long processus, ce qui n'est pas permis pour des applications de sûreté.

Nous proposons une solution, parant ce genre de comportements, sans aucune hypothèse sur le déploiement préalable d'infrastructures, comme ce fut déjà le cas dans les deux chapitres précédents. Afin de pallier aux problèmes liés à la dispersion des véhicules dans l'importante étendue géographique des réseaux véhiculaires, nous proposons de munir chaque véhicule d'un compte à crédits [28], dont le montant de crédit croît ou décroît en rapport avec le comportement du véhicule. Ce crédit permet d'obtenir des avantages au sein d'un réseau, tel que la possibilité d'envoyer et de recevoir des messages. Un véhicule qui épuise tous ses crédits est radié du réseau, car il est dans l'incapacité d'envoyer ou de recevoir des messages. Pour gérer les crédits des véhicules, nous proposons une solution basée sur un modèle économique nommé le "marché de l'emploi" [94], appartenant à la famille des jeux des signaux [93]. Ces modèles sont souvent utilisés quand les informations sont asymétriques au sein des membres d'un même réseau [97]. L'utilisation de tels modèles dans les réseaux véhiculaires permettrait d'avoir une vue plus large du comportement des véhicules dans un réseau véhiculaire.

Nos contributions dans ce chapitre sont :

- Un nouveau modèle de confiance distribué, nommé DTM^2 [48] (Distributed Trust Model inspired from job-Market), pour les VANETs, inspiré du modèle du marché de l'emploi.
- Un mécanisme préventif qui décourage les comportements malicieux, détecte et évince les véhicules malicieux du réseau, en épuisant leurs crédits.
- Un mécanisme incitatif qui accroît la coopération des véhicules égoïstes, en créant un besoin constant de détenir du crédit.
- Une modélisation de la solution [51] en chaine de Markov à temps discret et à espace d'états discret afin de choisir les valeurs les plus adaptées à ses paramètres.
- Une étude de performance analytique et une autre par simulation dans divers scénarios.

5.2 Positionnement bibliographique

Plusieurs modèles de confiance ont été proposés dans le cadre des réseaux véhiculaires, les auteurs Govindan et Mohapatra proposent un état de l'art poussé sur ce sujet [45]. Ces solutions remédient généralement aux comportements malicieux ou aux comportements égoïstes, mais rarement aux deux en même temps. Elles peuvent être classifiées en trois catégories : les approches incitatives utilisant des modules TPM, comme c'est le cas dans notre solution DTM^2 ; la deuxième catégorie concerne les approches incitatives nécessitant le déploiement d'infrastructures ; les modèles de réputation sont représentés dans la troisième catégorie.

5.2.1 Les approches incitatives nécessitant l'utilisation de modules TPM

Dans le but d'améliorer la coopération au sein d'un réseau, multiples sont les solutions qui proposent une récompense en retour de chaque participation d'un de ses membres. Les modèles incitatifs sont basés sur un système de coûts et de récompenses, comme c'est le cas dans les études [28] et [29]. Ces solutions utilisent des *nuglets* comme moyen de paiement afin d'inciter les véhicules à coopérer. Ces solutions supposent que chaque véhicule est équipé d'un dispositif résistant aux attaques pour gérer ses nuglets.

Buttyàn et al. proposent dans l'étude [28] deux manières différentes d'estimer la récompense d'un véhicule pour la retransmission d'un message. La première se base sur le principe d'un porte-monnaie, la deuxième sur celui d'un commerce. Dans la première approche, la récompense est estimée d'après le nombre de véhicules intermédiaires entre la source et la destination, la récompense totale en nuglets est embarquée dans le message et à chacune de ses retransmissions par un véhicule, celui ci se récompense à travers ces nuglets. Cependant, cette approche est inefficace à cause de la vitesse de propagation des informations dans les VANETs [113], la forte mobilité des véhicules rend les estimations sur la récompense totale inappropriée et souvent sous-estimée ou surestimée. Dans la deuxième approche, c'est le destinataire qui récompense le dernier véhicule intermédiaire pour la retransmission du message, néanmoins ce coût peut vite augmenter si les intermédiaires sont nombreux, car chaque véhicule intermédiaire a dû récompenser le précédant tout au long de la transmission du message, ce qu'on peut associer à un mécanisme de vente et de revente. Toutefois ces deux approches ne s'intéressent qu'aux comportements égoïstes.

Dans l'étude [29], les mêmes auteurs que précédemment proposent des comportements à suivre par les véhicules d'après différents niveaux de coopération proposés. Ces niveaux prennent en considération leurs besoins en crédits et leurs volontés de coopération. Néanmoins, ces niveaux risquent de mener à une participation quantitative des véhicules pour remédier à leur besoin en crédits, mais pas forcément de manière constante dans le temps, car rien dans le modèle ne les y obligent, ce qui peut mener au déclin de la connectivité dans le réseau.

5.2.2 Les approches incitatives nécessitant le déploiement d'infrastructures

La théorie des jeux est souvent utilisée pour concevoir des modèles incitatifs, comme ce fut le cas dans l'étude [85], ses auteurs l'ont utilisée pour améliorer la sécurité dans un réseau ad hoc mobile. Ils s'en ont servi pour motiver les nœuds d'un réseau à coopérer davantage en augmentant leur réputation auprès de l'autorité du réseau pour qu'elle leur octroie des privilèges.

D'autres solutions, notamment celles proposées dans [67], [101] et [114], génèrent de l'incitation en proposant des récompenses aux nœuds qui acceptent de relayer des messages jusqu'à leur destinataire. Ces trois solutions se basent toutes sur l'existence d'infrastructures comme des unités de bords de route. Les auteurs de l'étude [67] proposent deux sortes de récompenses, la première dépend uniquement de l'action réalisée par un nœud, alors que la deuxième tient plutôt d'un système de loterie où une récompense est donnée à un seul nœud parmi les participants, celui ci est choisi au hasard. Cette solution permet de limiter les dépenses en récompenses pour un nœud source, particulièrement quand le nombre de nœuds intermédiaires est important. Car un nœud source n'aura pas à proposer d'importantes récompenses aux nœuds relayeurs égoïstes, puisque la chance d'être tiré au sort pour recevoir la deuxième récompense les motive aussi. Cependant, cette solution nécessite l'existence d'infrastructures, car un nœud source a besoin de l'autorisation d'une autorité pour envoyer son message et aussi pour lui remettre le montant des récompenses des nœuds relayeurs afin qu'elle le leur redistribue. Aussi, ce modèle n'apporte de solution que pour les nœuds égoïstes et ne traite pas le cas des nœuds malicieux.

Une autre solution utilisant l'incitation est proposée dans [101], celle ci encourage les nœuds égoïstes à coopérer en échange de récompenses à travers un système sécurisé utilisant le code de Reed-Solomon [89]. Ceci afin d'éviter de potentielles fraudes qui peuvent avoir lieu quand un nœud source refuse de récompenser les nœuds intermédiaires, ou quand

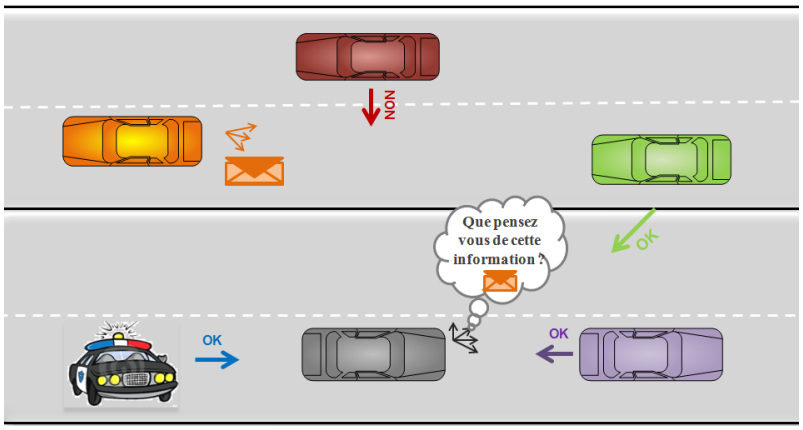


Figure 5.1 – Exemple d'un échange de message avec la solution MEB_Trust.

un nœud intermédiaire demande une plus grande récompense que prévu. La solution [114] s'intéresse aussi à la sécurité de ces modèles incitatifs. Elle propose de vérifier tous les reçus émis, qui constituent des preuves pour leurs actions, lors de l'exécution de chaque action par un nœud intermédiaire. Ceci au travers d'un service sécurisé dédié à la gestion des crédits, afin d'attribuer les récompenses correspondantes aux nœuds coopératifs. L'utilisation de cette méthode peut faire augmenter les délais dans un réseau et donc négativement impacter ses performances.

5.2.3 Les approches basées sur l'utilisation de la réputation

La troisième catégorie des modèles de confiance utilise la réputation des véhicules. Une solution se basant sur cette approche est proposée par Minhas et al. [71]. Nous la nommons MEB_Trust dans ce chapitre. Cette solution prend en considération la catégorie ou le rôle du conducteur dans le but de différencier entre un agent de la loi et un conducteur ordinaire. Lors de la réception d'un message par un véhicule, la solution préconise que le conducteur demande l'avis de ses voisins directs sur l'authenticité de l'information reçue. Une fois que le nombre minimum de réponses exigé par la solution est atteint, le conducteur calcule une moyenne d'après les avis de ses voisins en les pondérant d'après la catégorie de chacun, tel que l'avis d'un policier est plus important que celui d'un citoyen ordinaire. La pondération entre les citoyens ordinaires dépend de la réputation de chacun d'eux auprès du conducteur. Ce mécanisme est illustré dans la figure 5.1. Cependant, cette solution génère beaucoup de messages additionnels et peut faire augmenter le temps de décision à propos de la prise en considération ou non d'une information.

Une deuxième solution proposée dans [17] utilise la réciprocité comme critère de coopération. À chaque fois qu'un véhicule coopère avec un autre, ce dernier augmente sa réputation. Ces valeurs de réputation sont alors consultées pour décider si oui ou non un véhicule coopérera avec un autre dans le futur. Cette solution induit à des coûts importants, car une surveillance de rigueur doit être maintenue dans le temps pour établir ces réputations, comme cela a été démontré dans l'étude [84].

Notre solution DTM^2 est capable de gérer en même temps les véhicules dont le comportement est malicieux, ainsi que ceux dont le comportement est égoïste, sans nécessiter le déploiement d'aucune infrastructure additionnelle. DTM^2 supporte la forte mobilité des véhicules et gère l'asymétrie de l'information au sein d'un réseau ad hoc véhiculaire, car les récompenses et les coûts qu'il propose ne se basent pas sur des estimations. Celles-ci pourraient être faussées à cause des caractéristiques des VANETs

comme les nombreux changements de topologie du réseau. DTM^2 amène à une auto-sélection au sein du réseau via l'utilisation des signaux. Ceux ci aident à l'évincement des véhicules malicieux et à la coopération des véhicules égoïstes.

5.3 Système utilisé

5.3.1 Définitions et hypothèses

Nous considérons un réseau composé de véhicules dont le comportement est différent. Celui-ci peut être bon, malicieux [111] ou égoïste [29].

- **Les véhicules malicieux** ont le comportement le plus dévastateur pour les performances d'un réseau. Ils peuvent, dans leur intérêt ou juste pour porter atteinte aux autres membres du réseau, modifier le contenu d'un message avant de le relayer ou générer pour envoyer de fausses informations. Lors de l'utilisation de notre solution DMS^2 (Distributed Trust Model inspired from job-Market), nous supposons aussi que les véhicules malicieux trichent sur les signaux envoyés. Ces véhicules malicieux peuvent alterner entre un comportement correct et un autre malicieux pour éviter d'être détectés.

- **Les véhicules égoïstes**, contrairement aux malicieux, altèrent les performances du réseau de façon passive. Un véhicule égoïste peut refuser de relayer un message par exemple, pas pour alléger la charge du réseau mais parce que cette action diminue de ses ressources personnelles, comme par exemple son temps d'accès au canal. Il refuse alors, car la tâche ne lui apporte aucun bénéfice. Les véhicules égoïstes restent néanmoins rationnels et en aucun cas ils n'altèrent le contenu des messages à relayer.

Notre solution se base sur les jeux de signaux, dont l'idée principale consiste en l'échange de signaux entre les membres d'un réseau.

- **Un signal** informe le récepteur sur la nature du comportement de la source et indirectement sur l'authenticité du message reçu. Un signal doit induire un coût à son utilisateur. Ce coût doit correspondre à la nature réelle du véhicule, tel que plus son comportement est malicieux ou égoïste, plus son coût de signal est élevé. Ceci afin que ce signal agisse comme une garantie pour les véhicules récepteurs d'un message. Un signal est choisi de façon libre par un véhicule et est observé par tous les véhicules voisins à l'émetteur, car il est échangé avec le message à envoyer par diffusion. La valeur d'un signal permet aux autres véhicules de prendre une décision par rapport à l'authenticité ou pas de l'information échangée.

Un exemple sur l'échange de signaux est donné la figure 5.2, où trois véhicules envoient des messages, avec différents signaux et différents coûts relatifs. Un signal ne peut être envoyé que si son véhicule émetteur a assez de crédits pour payer son coût.

Afin de permettre le bon fonctionnement de notre solution, chaque véhicule est équipé d'un module **TPM** (Trusted Platform Module) [2] résistant aux attaques, afin de gérer ses crédits. Ceci consiste en le calcul du coût d'un signal choisi et la déduction de ce montant des crédits du véhicule, afin de rendre impossible la falsification du nombre de crédit détenu par un véhicule malicieux ou l'envoi et la réception de messages par un véhicule ne

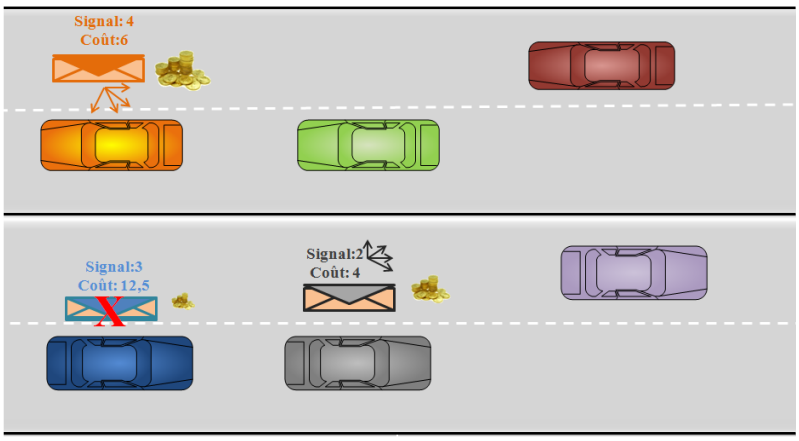


Figure 5.2 – Échange de signaux entre véhicules.

disposant plus de crédits. Dans notre système, nous considérons qu'un véhicule est détecté comme malicieux et est donc exclu du réseau dès qu'il épuise ses crédits.

5.3.2 Description du module TPM

Le module TPM, de nom courant "Trusted Platform Module" est une puce matérielle proposée par le groupe Trusted Computing Group Association [2]. Ce module est déjà utilisé dans plusieurs travaux [47], [46] et [106]. Le module TPM possède un générateur de nombres aléatoires, un moteur SHA-1, des capacités cryptographiques asymétriques et symétriques utilisant le RSA ou les courbes elliptiques. Aussi, il est résistant aux attaques. La composition d'un module TPM est donnée dans la figure 5.3.

Le module TPM gère les crédits d'un véhicule, il stocke ces crédits dans un emplacement sécurisé et inaccessible de l'extérieur, il calcule et déduit de ces crédits le coût du signal choisi par le véhicule lors de l'envoi d'un message, ainsi que le coût lié à l'accès au contenu d'un message reçu. Également, le module TPM est responsable de l'ajout du crédit pour un véhicule qui reçoit une récompense. Le module TPM stocke une empreinte digitale des applications dont il est responsable, ce qui lui permet de détecter tout changement induit par un attaquant [46]. Les études [112] et [69] ont démontré que les capacités cryptographiques du module TPM respectent les délais très courts des applications de sûreté dans les VANETs.

5.3.3 Les clés dont dispose un module TPM

Chaque module TPM possède et stocke de manière sécurisée une unique clé d'endossement (EK) générée par le fabriquant. Cette clé est uniquement utilisée pour les fonctions internes du module TPM. Chaque module TPM possède aussi une clé d'attestation identitaire (AIK) et le certificat correspondant. Cette clé est un alias de la clé d'endossement utilisée pour attester de son identité lors des échanges de messages ; tout comme la clé EK, elle est générée par le fabricant. Le plus souvent, la clé AIK est une paire de clés RSA de 2048 bits composée d'une clé privée et d'une autre publique. Pour des raisons d'anonymat, un module TPM peut générer plusieurs paires de clé AIK, tant qu'une autorité de certification CA les certifie [47]. Durant notre étude, nous supposons que ces clés sont déjà embarquées dans les véhicules par le fabriquant ; aussi nous ne n'utiliserons aucun mécanisme de révocation de clés, même dans le cas de détection d'un véhicule malicieux, car notre exclusion est liée à la possession de crédits.

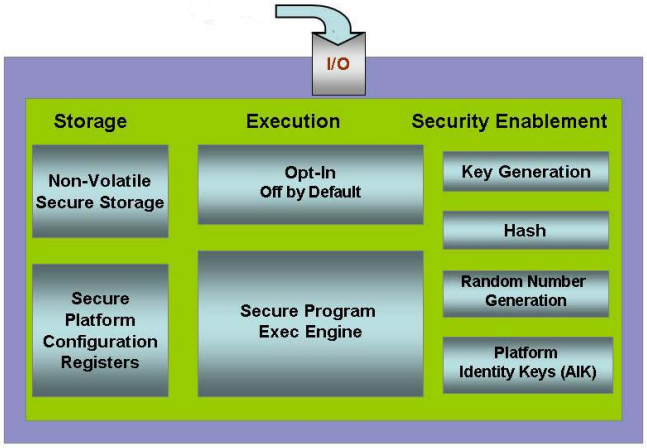


Figure 5.3 – Composition d'un module TPM.

5.3.3.1 Signature d'un message par le module TPM

Pour ne pas affaiblir la sécurité fournie par la clé AIK lors d'une utilisation répétitive, les auteurs de l'étude [61] proposent de générer une clé de signature (SK) qui soit renouvelable par le module TPM. Afin de sécuriser les échanges, un véhicule demande à son module TPM de signer le message qu'il veut envoyer. Le module TPM lui retourne alors une version du message signé par sa clé SK, ainsi que le certificat de la clé SK afin que les véhicules récepteurs puissent vérifier la signature. Ce certificat contient la version signée de la clé SK par la clé AIK, en plus du certificat délivré par une autorité de certification CA à propos de la clé AIK, comme présenté dans l'étude [47]. Le suivi de ce processus pour la signature d'un message permet à un véhicule récepteur d'identifier le véhicule source via la clé AIK de son module TPM, en détenant juste la clé publique de l'autorité de certification CA, mais aucune autre concernant la source grâce à la certification du CA.

5.3.3.2 Chiffrement d'un message par le module TPM

DTM^2 utilise aussi le module TPM dans le but de garantir la confidentialité des informations échangées en les chiffrant avec une même clé secrète (SyK) embarquée par le fabriquant, soit en utilisant de la cryptographie symétrique. Ceci permet de faire passer absolument tous les véhicules par leur module TPM pour pouvoir accéder à la version déchiffrée d'un message reçu. DTM^2 peut alors faire payer aux véhicules l'accès aux informations reçues dans le but de créer un besoin de crédit auprès des véhicules égoïstes.

5.4 Informations asymétriques et jeux de signaux

Les jeux de signaux [93] font partie des jeux bayésiens dynamiques disposant d'informations incomplètes, souvent utilisés pour solutionner des problématiques en économie. Elles sont liées au manque d'informations dont dispose un acheteur sur la qualité des marchandises proposées par un vendeur. Les jeux de signaux se réfèrent à un modèle stratégique où deux agents interagissent entre eux alors que seulement l'un d'entre eux dispose de toutes les informations. Alors pour informer le deuxième agent, le premier utilise des signaux. Un signal est une caractéristique observable par un individu, il est utilisé afin de différencier son auteur des autres. Il est utilisé par un vendeur dans un marché, par

exemple, pour vanter la qualité de ses produits dans le but de se faire remarquer. Un signal doit représenter un investissement pour son utilisateur et un coût pour décourager les autres de l'imiter.

L'asymétrie dans les informations concernant les produits proposés dans un marché peut être levée grâce aux garanties que peut offrir un vendeur. Celles-ci témoigneraient de la confiance que porte un vendeur sur la qualité de ses produits auprès des acheteurs. Un des signaux les plus utilisés de nos jours est la publicité, quand une entreprise est sûre de la qualité de ses produits, elle lance une compagne publicitaire. Cette publicité est considérée comme un signal auprès des potentiels acheteurs et elle est un investissement pour la compagnie. Malgré son coût, un signal peut générer des profits s'il est bien perçu par les clients. Nous nous sommes intéressés à reproduire le même principe dans un modèle de confiance pour les VANETs, afin de lever le manque d'information sur la vraie nature du comportement des véhicules. Pour cela, nous adaptons le modèle de signal du marché de l'emploi, établi par M. Spence, à notre cas d'étude pour construire un modèle de confiance pour les VANETs, qui saurait aussi inciter à la coopération.

5.4.1 Le modèle du marché de l'emploi

Le modèle de signal du marché de l'emploi [96] est couramment illustré par la résolution du problème de l'embauche de futurs employés. Dans cet exemple, les informations concernant la productivité et les réelles compétences des candidats sont asymétriques entre le recruteur et les candidats. Un employeur n'est alors jamais sûr de la future productivité d'un candidat lors d'une embauche et n'a pas de réelle garantie pour le salaire offert. Dans le marché du travail, une partie détient toutes les informations, au contraire de la deuxième, malgré cela, ces deux parties doivent interagir entre elles.

Pour convaincre un recruteur de l'embaucher, un candidat fait référence à ses compétences en lui envoyant des informations perçues comme un signal. Le signal dans cet exemple est le degré d'éducation d'un candidat. On suppose alors que le niveau d'éducation d'un candidat ne constitue pas sa productivité, mais est directement et positivement corrélé avec. Alors, plus le niveau d'éducation d'un candidat est élevé, plus il est considéré comme compétent et productif.

Afin de rendre le signal inimitable, il doit avoir un prix. Ce coût doit être négativement corrélé à la productivité, soit qu'un diplôme coûte moins pour un individu ayant des aptitudes élevées que pour un autre avec des aptitudes plus faibles. Il est alors représenté par le nombre d'années d'études pour l'obtention d'un diplôme. Cependant, un employeur n'est au courant que des diplômes obtenus par un candidat et non du nombre d'années passées pour, soit qu'il est juste au courant du signal envoyé par un candidat et non du coût lié à celui ci. Un employeur ne calcule le salaire proposé à un employé que sur ses diplômes obtenus, qui sont sensés refléter la productivité du candidat. De ce fait, un candidat qui est au courant de ses réelles compétences choisit délibérément le degré d'étude qui lui convient par rapport au nombre d'années nécessaires et des salaires proposés dans le marché de l'emploi.

Deux types de résolutions pour les candidats existent, l'équilibre mélangeant et l'équilibre séparateur. Nous considérons être "un équilibre" toute situation où aucun membre n'est tenté de dévier de son choix.

5.4.1.1 Équilibre mélangeant

Dans cet équilibre, tous les candidats à l'embauche décident d'utiliser le même signal en obtenant les mêmes diplômes, afin de ne pas se différencier et de minimiser leurs coûts

d'éducation. Dans ce cas, un employeur ne détient aucune information pour départager les candidats et leur propose à tous le même salaire. Le montant du salaire représente l'estimation du recruteur de la productivité moyenne de l'ensemble des candidats. Un tel équilibre est plus intéressant pour les individus avec les plus faibles compétences, car ça leur assure un salaire plus important comparé à leur réelle productivité.

Les candidats avec de fortes compétences peuvent aussi apprécier cet équilibre à condition qu'ils soient plus nombreux que le reste des candidats, afin d'augmenter l'estimation de l'employeur sur la productivité moyenne de l'ensemble et par la suite hausser le salaire proposé. Cet équilibre permet à ces candidats d'économiser les frais d'éducation qui auraient permis de les différencier.

5.4.1.2 Équilibre séparateur

Dans cet équilibre, chaque candidat signale son degré d'éducation afin de maximiser son salaire. Les candidats avec de solides compétences poussent au plus loin leurs études dans le but de se faire catégoriser comme étant des candidats à fort potentiel productif, car cela leur coûte moins en termes d'années scolaires que le reste des candidats. Contrairement à eux, le reste des candidats décident de leur degré d'étude d'après le coût de celles-ci en terme d'années et d'après le salaire promis par les recruteurs pour chaque diplôme. Ils choisissent alors entre écourter leurs études pour minimiser les coûts au dépend d'un salaire faible dans le futur, ou inversement. Les paramètres utilisés pour le calcul des coûts et des salaires font que les candidats avec de faibles compétences choisissent de minimiser leur coût d'étude et ceux avec de meilleures compétences de maximiser leur salaire, ceci crée une séparation automatique d'après les réelles compétences des candidats.

5.4.2 Exemple de l'embauche d'après le modèle du marché de l'emploi

Nous nous sommes intéressés à reproduire un équilibre séparateur parmi les véhicules, d'après la vraie nature de leur comportement, le même que celui obtenu parmi les candidats à l'embauche d'après leurs compétences. Nous expliquons ci dessous l'obtention de cet équilibre d'après le même exemple de l'embauche [95], puis nous l'adaptons à notre problématique.

Nous supposons l'existence de deux catégories d'employés d'après leur productivité, soit $Z = \{H, L\}$. La première catégorie H a une productivité et des compétences élevées, alors que celles de la seconde catégorie L le sont moins. Nous nous référons au signal choisi par un candidat par la variable Y. Dans cet exemple, le coût d'un signal pour la catégorie L est égal à la même valeur du signal, alors qu'il est deux fois plus petit pour la catégorie H. Un employeur offre un salaire de $W(Y)$ à ses employés, ce salaire dépend uniquement du signal donné par eux, vu que leur réelle productivité n'est pas visible à l'employeur lors de l'embauche. L'hypothèse la plus importante de cet exemple est que le coût d'un même signal est plus élevé pour la catégorie L que pour la catégorie H, ceci incite les candidats les plus prometteurs à obtenir plus de diplômes dans le but de se démarquer lors d'une embauche.

La figure 5.4 illustre l'évolution des coûts pour chacune des deux catégories de candidats d'après le signal choisi. La courbe tracée en pointillés courts représente le coût du signal pour la catégorie L et celle en pointillés longs le coût pour la catégorie H. Les deux différents salaires choisis par l'employeur sont illustrés par la courbe tracée avec un trait plein. Le salaire est choisi via l'estimation de l'employeur de la productivité d'un candidat à travers son signal envoyé. D'après les deux courbes représentant le coût du signal, nous observons qu'un candidat de la catégorie L a un net bénéfice de 1 lorsque sa valeur de

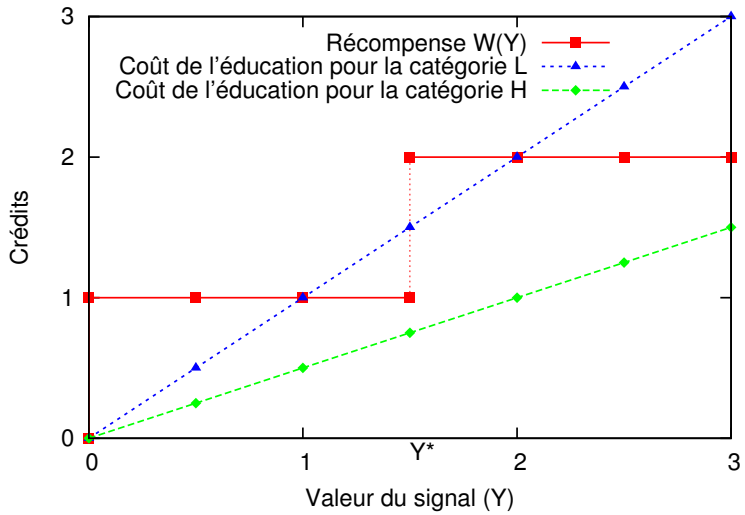


Figure 5.4 – Les coûts et salaires dans le modèle du marché de l'emploi. Dans cet exemple, la catégorie H signale sa productivité avec un signal de $Y^\star$, dont le coût est de $\frac{Y^\star}{2}$; alors que la catégorie L utilise un signal de 0 qui ne lui coûte rien, soit 0.

signal équivaut à 0, soit la différence entre le salaire perçu et le coût du signal. Alors que ce bénéfice est de $2 - Y^\star$ lorsque le signal choisi est $Y^\star$ et à 0 lorsque son signal est de 1 ou de 2. Rationnellement, un candidat de cette catégorie choisira toujours un signal de $Y = 0$. Contrairement à lui, un candidat de la catégorie H a un bénéfice net maximum égal à $2 - \frac{Y^\star}{2}$ lorsque son signal choisi est de $Y^\star$. Cette valeur de signal de $Y^\star$ définit notre équilibre séparateur, car elle sépare les deux catégories de candidats.

Pour définir la valeur du signal qui crée un équilibre séparateur, soit $Y^\star$, deux conditions (5.1) doivent être respectées. La première condition est que les membres de la catégorie H maximisent leurs bénéfices nets en choisissant cette valeur de signal, soit que le soustraction du coût du signal : $\frac{Y^\star}{2}$ du salaire donné 2 pour la valeur du signal $Y^\star$ soit plus intéressante que la soustraction du coût de 0 du salaire reçu de 1 pour un signal choisi de valeur 0. La seconde condition est que les membres de la catégorie L utilisent une valeur de signal inférieure à $Y^\star$ car le bénéfice net obtenu par l'utilisation de celle ci n'est pas intéressant, soit que la soustraction du coût : $Y^\star$ du salaire de 2 soit inférieure à la soustraction du coût de 0 du salaire reçu de 1 lors du choix d'un signal égal à 0, car le coût du signal $Y^\star$ n'est pas le même pour les deux catégories.

Dans cet exemple, l'équilibre séparateur est atteint en définissant la valeur de $Y^\star$ dans l'intervalle $]1, 2[$ après résolution du système (5.1), une infinité d'équilibres séparateurs est possible alors. Par cet équilibre, nous obtenons une différenciation automatique des membres d'après leur productivité, alors que chacun d'eux a juste pour but de maximiser son propre bénéfice net.

$$\begin{cases} 2 - \frac{Y^\star}{2} > 1 - 0 \\ 1 - 0 > 2 - Y^\star \end{cases} \tag{5.1}$$

Alors, le résultat est : $1 < Y^\star < 2$

5.4.3 Du marché de l'emploi aux VANETs

Le Modèle du marché de l'emploi différencie entre les candidats lors d'une embauche selon leurs productivités alors que les informations sont asymétriques entre les candidats et

le recruteur. Nous nous sommes intéressés à adapter ce concept à notre cas d'étude, afin de différencier les véhicules suivant leur comportement alors que les informatiques sont aussi asymétriques entre eux. Ceci dans le but de réaliser une auto-sélection parmi les véhicules, qui supporterait leur forte mobilité et qui soit peu onéreuse en infrastructures.

Les fréquents changements de topologie des VANETs ainsi que leur étendue géographique amplifient le phénomène d'asymétrie d'informations. Car ils créent plus de dispersions parmi les membres du réseau et de courts et irréguliers intervalles de rencontre entre les véhicules. Tout comme dans l'exemple du marché de l'emploi, il est difficile d'établir de solides liens entre les membres, ce qui rend d'ailleurs inefficace les modèles de réputation utilisés seuls comme solution aux problématiques de confiance dans les VANETs. Pour contourner ces contraintes, les véhicules échangent des signaux lors de leurs émissions de messages dans notre solution. Ces signaux sont observables par tous les autres et induisent un coût correspondant à leurs auteurs.

Tout comme l'exemple de l'embauche qui utilise l'incitation à travers des montants de salaire équitables et proportionnels aux compétences des candidats dans le but d'attirer les plus prometteurs d'entre eux, notre solution suit le même principe pour les VANETs. Elle utilise l'incitation au travers des récompenses aux véhicules les plus coopératifs, tel que plus un véhicule participe à la diffusion d'information en collectant des informations authentiques et en relayant celles de ses voisins au besoin, plus sont élevées ses récompenses.

En plus de notre adaptation du modèle du marché de l'emploi pour les VANETs, nous avons rajouté à notre solution un mécanisme concernant l'expulsion des véhicules malicieux. Il est impératif de s'assurer que les messages échangés dans le cadre des applications de sûreté soient authentiques et en aucun cas falsifiés, surtout quand on ne peut se référer à une entité centralisée par manque d'infrastructures ou par manque de temps. Pour cette raison, il est impératif pour les véhicules de posséder du crédit. Celui-ci est directement lié à leur comportement et permet au véhicule de participer au sein du réseau. Lors de l'épuisement du crédit d'un véhicule, ce véhicule est considéré comme exclu du réseau.

Dans un modèle de signal, les principes suivants sont respectés :

- Les convictions d'un agent à propos d'un autre dépendent de la stratégie utilisée par ce dernier. Dans notre contexte, ceci se réfère à ce que l'opinion que se fait un véhicule sur sur un autre dépende du comportement de ce dernier et des signaux qu'il utilise. Ceux-ci sont directement liés à l'authenticité de ses messages envoyés ainsi qu'à sa coopération au sein du réseau.
- La réponse d'un agent à l'action d'un autre dépend de ses convictions à son propos tout en restant optimale et rationnelle. Par ceci, un véhicule accepte à ce que un véhicule source soit récompensé si son message est valide.
- Les actions choisies par un agent doivent être bénéfiques pour lui par rapport aux potentielles réactions des autres. Ce qui équivaut à ce qu'un véhicule prenne en considération sa potentielle future récompense pour l'envoi d'un message avant de décider du signal qu'il veut utiliser lors de son envoi. Ceci réfère à maximiser son bénéfice net, en prenant en considération sa récompense et son coût d'envoi.

5.5 DTM^2 : un modèle de confiance distribué et inspiré du marché de l'emploi

Le modèle du marché de l'emploi apporte une solution à l'asymétrie des informations dans un réseau et dévoile de façon indirecte la vraie nature de ses membres, en

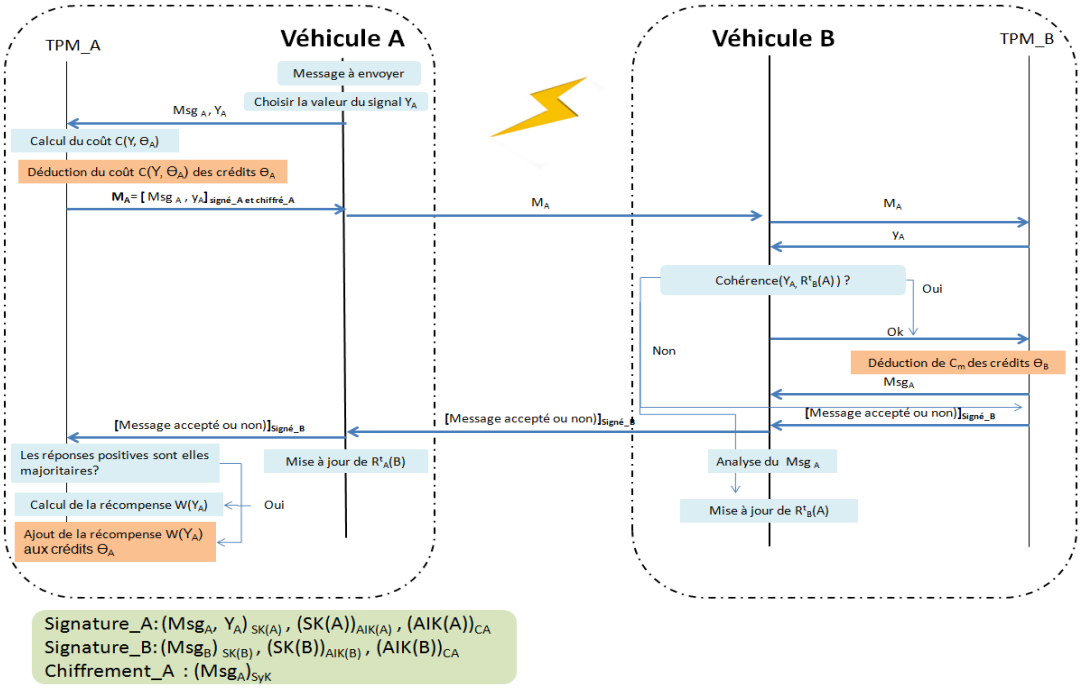


FIGURE 5.5 – Processus d'envoi et de réception d'un message dans DTM^2.

encourageant chacun d'eux à choisir simplement l'action qui lui est la plus bénéfique. Par ce biais, les membres du réseau sont gagnants et le réseau est plus performant, sans avoir à déployer de coûteuses infrastructures. En plus d'exclure les véhicules malicieux du réseau une fois leurs crédits épuisés, notre solution fait croître la coopération parmi les véhicules, en incitant les véhicules égoïstes à participer dans le réseau grâce aux récompenses allouées.

Notre solution remplace le niveau d'éducation utilisé comme signal dans l'exemple de l'embauche par une valeur que les véhicules sont libres de choisir, à condition qu'ils puissent payer le coût correspondant. Ce signal est attaché alors au message à envoyer et est observé par tous les véhicules voisins. Il est perçu comme une garantie sur l'authenticité du message émis par le véhicule source aux véhicules récepteurs, à cause du coût qu'il lui a induit. Tous les véhicules reçoivent le même montant de crédit lors de leur première connexion au réseau, ils doivent bien le gérer afin de pouvoir toujours accéder au réseau. En effet, les véhicules ont besoin de crédit pour payer le coût de leur signal lors de l'envoi d'un message. Aussi, pour payer le coût de réception pour pouvoir accéder à leurs messages reçus. Car ces derniers sont chiffrés et seul les modules TPM détiennent les clés de chiffrement. Les véhicules gagnent du crédit lorsqu'ils participent au bon fonctionnement du réseau.

Dans le reste de cette section, nous définissons la façon dont notre solution DTM^2 sécurise l'attribution et la déduction de crédits, puis le calcul du coût d'un signal, le calcul du montant d'une récompense et le calcul des valeurs de signal optimales à chaque véhicule. À cela s'ajoute, le processus de décision sur l'acceptation ou non d'un message reçu et le coût de lecture des messages reçus. Finalement, nous détaillons une technique de sauvegarde de crédit pour les véhicules afin d'éviter les faux positifs.

5.5.1 Scénario basic de fonctionnement

La figure 5.5 illustre le processus d'échange d'un message dans la solution DTM^2. Dans cet exemple, le véhicule A diffuse un message et le véhicule B le reçoit. Avant l'envoi, le

Table 5.1 – Notations utilisées dans DTM^2.

θ_A	Montant du crédit du véhicule A
C_m	Coût de l'accès au contenu d'un message reçu
Y_A	Valeur du signal choisi par le véhicule A
$Y^\star(i)$	Valeur optimale du signal pour un véhicule détenant i crédits
$W(Y)$	Valeur de la récompense pour un véhicule ayant utilisé une valeur de signal Y
$C(Y,i)$	Coût d'un signal Y pour un véhicule détenant i crédits
$R_B^t(A)$	Réputation du véhicule A auprès du véhicule B

véhicule A choisit sa valeur de signal à utiliser, soit Y_A. Cette valeur est attachée au message à envoyer Msg_A. Puis, elle est remise avec le message au module TPM du véhicule, soit TPM_A. Le module TPM se base alors sur la valeur du signal choisie par le véhicule et le montant du crédit dont il dispose, soit θ_A, pour calculer le coût du signal $C(Y,\theta_A)$. Le module TPM le soustrait alors du compte à crédits du véhicule. Pour garantir l'intégrité du message M_A, ainsi que celle du signal utilisé par le véhicule, les deux sont signés par le module TPM via sa clé de signature $SK(A)$, qui est accompagnée de son certificat $(SK(A)_{AIK(A)}AIK(A)_{CA})$. Aussi, le message M_A est chiffré par le module TPM via la clé secrète symétrique SyK. Ceci, pour pouvoir contrôler l'accès aux informations reçues et ne l'autoriser qu'après paiement du coût de réception. Le message attaché avec la valeur du signal est retourné au véhicule afin qu'il procède à son envoi. La table 5.1 rappelle les notations les plus utilisées dans notre modèle.

Lors de la réception du message par le véhicule B, celui ci demande à son module TPM de vérifier la signature du message, afin d'identifier le véhicule source et demande aussi à ce qu'il lui soit communiqué la valeur du signal utilisé. Le véhicule B peut alors évaluer la cohérence de la valeur du signal utilisé par le véhicule A avec la réputation qu'il détient à son propos, $R_B^t(A)$. Cette dernière peut aussi signifier la non connaissance du véhicule source, elle sera alors ignorée dans ce cas là.

Si la réputation est cohérente avec le signal utilisé, soit plus la réputation est douteuse plus le signal donné par le véhicule source doit être élevé, comme au fonctionnement d'une assurance, alors le véhicule B accepte le message et demande à son module TPM de le lui déchiffrer afin d'accéder à son contenu. Le module TPM_B déduit du crédit du véhicule B le coût de réception d'un message, C_m. La valeur de ce coût est fixée d'avance par l'application. Le module TPM_B délivre le contenu du message reçu, puis envoie au module TPM du véhicule source un message signé accusant l'acceptation du message envoyé. Dans le cas où le message est refusé par le véhicule B, une notification de refus est envoyée par le module TPM_B au module TPM_A.

Dans les deux cas, de refus ou d'acceptation, les deux véhicules A et B mettent à jour leur réputation respective, par rapport au message envoyé par A et l'acceptation ou le refus du véhicule B de ce message. Ces réputations sont locales et ne sont pas échangées dans le réseau pour ne pas faire augmenter la charge du canal de communication. Finalement, si le véhicule A reçoit une majorité d'accusés de réception positifs par rapport à l'authenticité de son message envoyé, son module TPM incrémente son crédits d'une valeur $W(Y_A)$, représentant sa récompense. Cette récompense dépend du signal utilisé lors de l'envoi, soit Y_A.

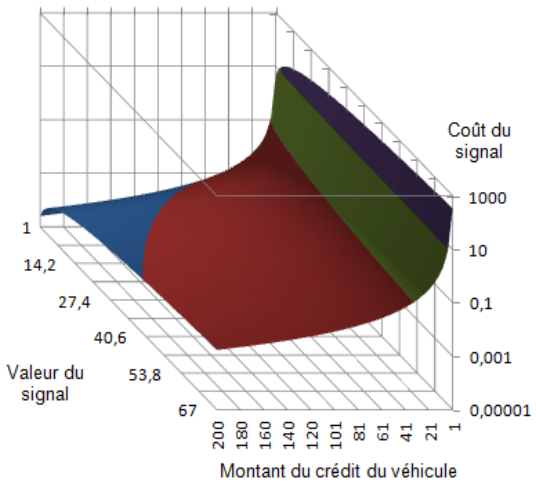


FIGURE 5.6 – Variation du coût d'un signal d'après sa valeur et le montant de crédit détenu par un véhicule.

5.5.2 Calcul du coût d'un signal

Le coût d'un signal est positivement corrélé à la valeur du signal utilisé Y et est négativement corrélé au montant de crédit θ détenu par un véhicule, d'après les deux conditions du modèle du marché de l'emploi. Elles sont présentées dans l'ensemble d'équations (5.2).

$$\begin{cases} C(Y_1,\theta) > C(Y_2,\theta) & Pour \quad Y_1 > Y_2, \\ C(Y,\theta_1) < C(Y,\theta_2) & Pour \quad \theta_1 > \theta_2, \end{cases} \tag{5.2}$$

Le calcul du coût d'un signal est présenté dans l'équation (5.3). Il nécessite deux coefficients positifs β et α. Le premier, β, sert à normaliser la valeur du signal par rapport au montant de crédit que possède un véhicule. Le deuxième coefficient, α, est utilisé pour définir le poids à donner au montant de crédit dans le calcul du coût d'un signal. Plus celui-ci est élevé et plus le montant de crédit détenu par un véhicule impacte le coût du signal. Ceci, afin de creuser davantage la séparation entre les véhicules ayant différents comportements et donc accélérer la détection et l'exclusion des véhicules malicieux.

$$C(Y,\theta) = \frac{\beta \times Y}{\theta^{\alpha}} \tag{5.3}$$

Où β, α, θ >0

Les valeurs des coefficients β et α sont établies par avance par l'application, en rapport à ses attentes de performances réseaux. La figure 5.6 illustre l'évolution du coût d'un signal par rapport à différentes valeurs de signal et différents montants de crédits. Lors de ces calculs, nous avons choisi une valeur de 5 pour le paramètre β et de 2.3 pour le paramètre α. Nous remarquons clairement que les variations du coût d'un signal dépendent plus du montant de crédit détenu par le véhicule que par la valeur du signal.

Le modèle du marché de l'emploi exige une corrélation négative entre le coût du signal et les crédits détenus par un véhicule. Cette première condition est vérifiée lorsque $\frac{\partial C(Y,\theta)}{\partial Y} > 0$. La deuxième condition du modèle concerne la corrélation positive entre le coût du signal et sa valeur, elle est vérifiée lorsque $\frac{\partial C(Y,\theta)}{\partial \theta} < 0$ et $\frac{\partial^2 C(Y,\theta)}{\partial Y \partial \theta} < 0$. Cette dernière concerne la dérivée du coût du signal par rapport aux crédits détenus par un véhicule et à la valeur du signal choisi, ainsi que la deuxième dérivée de ce même coût. Le système les

concernant est donné dans (5.4).

$$\begin{cases} \frac{\partial C(Y,\theta)}{\partial Y} & = \frac{\beta}{\theta^{\alpha}} > 0 \\ \frac{\partial C(Y,\theta)}{\partial \theta} & = \frac{-\alpha \times \beta \times Y}{\theta^{\alpha+1}} < 0 \text{ et } \frac{\partial^2 C(Y,\theta)}{\partial Y \partial \theta} = \frac{-\alpha \times \beta}{\theta^{\alpha+1}} < 0 \end{cases} \tag{5.4}$$

Afin d'assurer le bon fonctionnement de notre solution et d'éviter de potentielles tricheries, un véhicule ne fait que choisir sa valeur de signal. Son module TPM, qui est résistant aux attaques d'après notre hypothèse, se charge de calculer le coût correspondant au signal choisi et de le déduire des crédits dont dispose le véhicule. Le module TPM retourne alors au véhicule un message, avec la valeur du signal choisi, signé et chiffré afin que le véhicule l'envoie.

Car le montant de crédit détenus par un véhicule n'est pas affecté par l'impact de la mobilité, celui-ci fait référence au vrai comportement du véhicule. Car plus le comportement d'un véhicule est en concordance avec les besoins du réseau et plus son montant de crédit est élevé. Même si le module TPM d'un véhicule ne peut détecter un comportement malicieux ou un refus de coopération, il détient néanmoins la valeur du montant de crédit que possède un véhicule, il se base sur celle-ci pour calculer son coût de signal.

5.5.3 Calcul de la récompense

Pour inciter les véhicules à coopérer, DTM^2 propose de récompenser les véhicules dont le comportement profite aux performances du réseau à travers leur coopération et leur envoi d'informations authentiques. Le calcul du montant d'une récompense pour l'envoi d'un message, validé par ses récepteurs, dépend de la valeur du signal utilisé par le véhicule source. Cette récompense a pour but de créer un équilibre séparateur entre les véhicules en les incitant à maximiser leur bénéfice net. Pour maximiser ce bénéfice net, soit la différence entre la récompense et le coût d'un envoi pour un véhicule, le véhicule doit choisir la valeur de signal correspondante au montant de crédit dont il dispose, car les calculs du coût d'un signal et de la récompense pour un envoi en dépendent. En incitant les véhicules à ne pas tricher sur la valeur de signal qu'ils choisissent, ils révèlent indirectement la nature de leur comportement. L'avantage de cet équilibre séparateur est qu'il n'est pas altéré par les fréquents changements de topologies des VANETs.

Dans ce modèle, une récompense $W(Y)$ est toujours plus importante que le coût payé par un véhicule, tant que celui-ci choisit le signal lui correspondant. Deux conditions concernant le calcul de la récompense sont données dans le système (5.5).

$$\begin{cases} \frac{dW(Y)}{dY} & = \frac{\partial C(Y,\theta)}{\partial Y} \\ W(Y) & = \frac{\theta}{\sigma} \end{cases} \tag{5.5}$$

Où σ>0

La première évoque le raisonnement rationnel d'un véhicule en choisissant une valeur de signal Y qui maximise son bénéfice net. Cette condition est réalisée lorsque la dérivée de la récompense égale celle du coût, par rapport à la valeur de signal choisie. La deuxième condition définie une base pour le calcul de la récompense, elle doit être connue par avance par tous les véhicules. Cette base dépend du crédit restant pour un véhicule, car ce montant est directement lié à son comportement. La base est définie comme étant le ratio entre le montant de crédit d'un véhicule et un coefficient σ que l'application défini, tel que plus ce coefficient est élevé plus stricte est l'application par rapport aux récompenses données.

En replaçant $\frac{\partial C(Y,\theta)}{\partial Y}$ par sa valeur : $\frac{\beta}{\theta^{\alpha}}$ et en mettant en avant θ, nous obtenons le système (5.6).

$$\begin{cases} \frac{dW(Y)}{dY} & = \frac{\beta}{\theta^\alpha} \\ \theta & = W(Y) \times \sigma \end{cases} \tag{5.6}$$

Nous remplaçons la valeur de θ par $(W(Y) \times \sigma)$ dans le calcul de $\frac{dW(Y)}{dY}$ dans l'équation (5.7), puis nous mettons en avant les valeurs liées à $W(Y)$ dans l'équation (5.8).

$$\frac{dW(Y)}{dY} = \frac{\beta}{(W(Y) \times \sigma)^\alpha} \tag{5.7}$$

$$W(Y)^\alpha \times \frac{dW(Y)}{dY} = \frac{\beta}{\sigma^\alpha} \tag{5.8}$$

L'équation (5.8) est résolue par l'utilisation de l'intégration par partie par rapport à Y dans l'intervalle $]0, \infty[$ comme décrit dans l'équation (5.9) et résolue dans l'équation (5.10), où C est une constante réelle.

$$\int W(Y)^\alpha \times \frac{dW(Y)}{\partial Y}\, dY = \int \frac{\beta}{\sigma^\alpha}\, dY \tag{5.9}$$

$$\frac{[W(Y)^{\alpha+1}]}{\alpha+1} = \frac{\beta}{\sigma^\alpha} \times [Y] + C \tag{5.10}$$

L'équation finale du calcul de la récompense d'un véhicule par rapport au signal utilisé Y est donnée dans (5.11). Nous considérons alors la constante C égale à 0 pour limiter le nombre de solutions possibles.

$$W(Y) = \left(\frac{\beta \times (\alpha+1) \times Y}{\sigma^\alpha}\right)^{\frac{1}{\alpha+1}} \tag{5.11}$$

Une récompense pour l'envoi d'un message est attribuée à un véhicule par son module TPM si la majorité des notifications envoyées par ses voisins au sujet du message reçu sont positives, soit que les notifications positives sont plus nombreuses que les négatives. Ces notifications sont générées par les modules TPM des véhicules qui ont reçu le message envoyé. Lorsque un véhicule demande à accéder à la version déchiffrée du message, cela équivaut à une acceptation de l'information et donc à l'envoi d'une notification positive. Ces messages de notification sont à leur tour signés pour éviter toute tentative de tricherie.

5.5.4 Valeur optimale pour un signal

Afin d'inciter les véhicules à dévoiler la vraie nature de leur comportement, le modèle maximise leurs bénéfices nets lorsque la valeur de signal utilisée pour leur envoi est celle correspondante au montant de leurs crédits restants θ. Ceci, car le montant de crédit restant est directement lié au comportement d'un véhicule. La valeur de signal $Y^\star(\theta)$ est définie comme la valeur optimale de signal pour un véhicule possédant θ crédits. DTM^2 incite les véhicules à choisir cette valeur de signal afin que les véhicules récepteurs d'un message sachent la nature du comportement du véhicule source à travers le montant de crédit dont il dispose. Ainsi, ils décident en toute connaissance de cause de prendre ou pas en considération l'information reçue.

En remplaçant $W(Y)$ par $\frac{\theta}{\sigma}$, nous obtenons la valeur optimale pour un signal dans l'équation (5.12).

$$Y^\star = \frac{\theta^{\alpha+1}}{\sigma \times \beta \times (\alpha+1)} \tag{5.12}$$

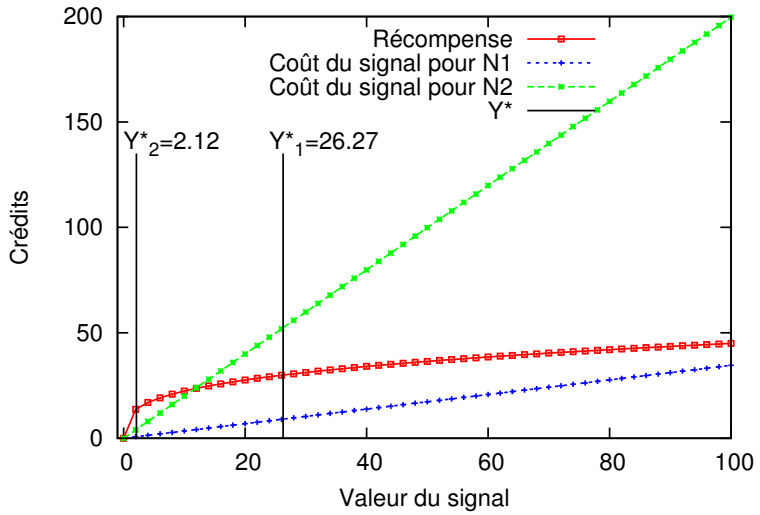


Figure 5.7 – Exemple des valeurs des coûts et des récompenses, lors de l'utilisation de différents signaux, pour chacune des sources N1 et N2.

La non utilisation par un véhicule de sa valeur de signal optimale $Y^\star$ lui cause un déficit ou une perte de crédits, comme illustré dans la figure 5.7. Cette figure comporte deux courbes représentant les coûts des signaux utilisés par deux véhicules sources N1 et N2, ainsi que la courbe des récompenses reçues pour leurs messages envoyés avec l'hypothèse que ces messages soient acceptés. Le premier véhicule source N1 dispose de 150 crédits, ce qui équivaut à un bon comportement dans cet exemple, le deuxième véhicule source N2 possède seulement 40 crédits, ce qui fait référence à un comportement malicieux où égoïste. Nous fixons le crédit initial, θ_0, dont sont dotés les véhicules à 100 crédits. Les deux courbes tracées en pointillés montrent l'évolution des coûts pour des valeur de signal allant de 0 à 100. Ceci, avec les valeurs de paramètres suivantes : $\beta = 3.5 \cdot 10^4$, α=2.3 et σ=5. Les récompenses attribuées aux véhicules, tracées avec un trait plein dans la figure, dépendent uniquement de la valeur de signal utilisée. Dans notre exemple les bénéfices nets du premier véhicule source sont plus avantageux. Cependant, dans le cas où un de ces deux véhicules ne respectent pas sa valeur optimale de signal, définie par $Y_1^\star$ pour N1 et $Y_2^\star$ pour N2, leurs bénéfices nets NB sont moins intéressants, comme illustré dans la figure 5.8. Les bénéfices nets pour le véhicule N2, qui est considéré comme moins fiable d'après ses crédits, décroissent plus rapidement que ceux du premier véhicule lors de la non utilisation de son signal optimal. Ceci est conçu dans le but d'accélérer l'épuisement du crédit des véhicules malicieux et donc leur exclusion. L'équation (5.13) du bénéfice net est donnée ci-dessous.

$$\begin{aligned} NB &= W(Y) - C(Y,\theta) \\ NB &= [\tfrac{\beta\times(\alpha+1)\times Y}{\sigma^\alpha}]^{\frac{1}{\alpha+1}} - \tfrac{\beta\times Y}{\theta^\alpha} \end{aligned} \tag{5.13}$$

5.5.5 Acceptation d'un message reçu

Le second moyen utilisé par notre solution pour encourager les véhicules à coopérer passe par la création du besoin de posséder et de gagner du crédit. Dans ce but, l'accès à la version en clair d'un message reçu est payante dans notre solution afin de pousser les véhicules et particulièrement ceux dont le comportement est égoïste à utiliser leurs crédits. Les véhicules qui ne coopèrent pas assez pour gagner du crédit verront leur stock de crédit

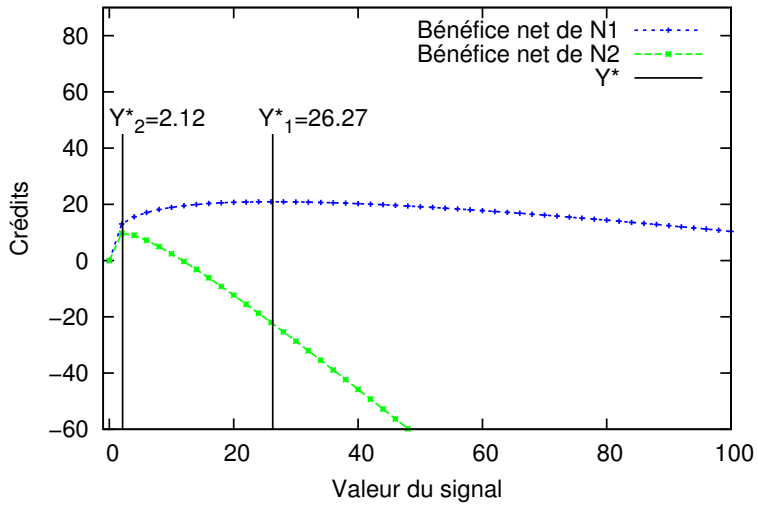


FIGURE 5.8 – Exemple du bénéfice net d'après la valeur de signal utilisée pour chacune des sources N1 et N2.

s'amincir et ne pourront plus lire les messages reçus après un certain moment.

Le coût d'accès à un message reçu C_m est fixé par l'application. Sa valeur est calculée d'après le coût d'envoi d'un message pour un véhicule possédant le montant initial du crédit donné, soit θ_0. Aussi la valeur de ce coût dépend du coefficient μ décidé par l'application. Le coût de réception est calculé par l'équation (5.14), tel que plus le coefficient μ est élevé moins un véhicule paie pour l'accès aux données chiffrées. Ce coût est soustrait du compte du véhicule récepteur par son module TPM dès sa demande d'accès au message. La décision d'acceptation ou non d'un message dépend de :

- La réputation du véhicule source auprès du véhicule récepteur.
- La valeur de signal, qui acte comme une garantie, utilisée par le véhicule source lors de son envoi.

$$C_m = C(Y^\star, \theta_0)/\mu \tag{5.14}$$

Une réputation $R_r^t(s)$ d'un véhicule source s auprès d'un véhicule récepteur r au temps t est dans l'intervalle [0, 1]. Cette réputation est locale, soit une réputation de première main, elle est basée uniquement sur les observations directes du véhicule r. Elle dépend de si le véhicule a pu par la suite vérifier l'information reçue, par lui même ou en recevant la même information plusieurs fois par ses voisins. Lorsque celle-ci est trop mauvaise, soit en dessous d'un seuil de valeur ρ choisi par l'application, la réputation est considérée comme étant un critère éliminatoire à l'acceptation d'un message reçu. Ce critère est important au début de l'application lorsque tous les véhicules ont encore tous leurs crédits initiaux, car ce n'est qu'avec la réputation, si existante, qu'on peut différencier entre deux véhicules à ce stade là. Le calcul de cette réputation est donnée dans l'équation (5.15), où $\psi_r(s)$ est la valeur de la dernière observation du véhicule r concernant le véhicule s, ω est le facteur d'atténuation dans le temps des différentes observations, sa valeur est comprise dans l'intervalle $[0, 1]$.

$$R_r^t(s) = \omega \times R_r^{t-1}(s) + (1 - \omega) \times \psi_r(s) \tag{5.15}$$

Une fois la réputation du véhicule source vérifiée, le véhicule récepteur vérifie la valeur de signal utilisée par le véhicule source. Un seuil minimum est aussi défini pour la valeur

de signal utilisée. Nous le fixons à la valeur de $Y^{\star}(\gamma \times \theta_0)$, ce qui équivaut à la valeur de signal optimale pour un véhicule possédant seulement $\gamma \times \theta_0$ crédits.

5.5.6 Consigne pour la sauvegarde de crédits

Afin d'éviter que les véhicules dont le comportement est bon épuisent tous leurs crédits et soient, par erreur détectés comme véhicules malicieux par l'application, ceci serait considéré comme état un cas de faux positif, nous introduisons une consigne pour la sauvegarde de crédit à suivre quand les montants de crédit des véhicules sont faibles. À cause des caractéristiques des VANETs, des véhicules peuvent avoir moins de messages à envoyer ou à retransmettre. Ceci peut arriver lors du déploiement de stratégies de diffusion avec élection de véhicules relayeurs, comme la solution ADCD présentée dans le chapitre 3, dans le but d'éviter les problèmes liés à la diffusion massive [76]. En effet, ces stratégies peuvent faire baisser le taux de coopération de quelques véhicules indépendamment de leur vouloir, en ne les élisant pas pour les retransmissions, et donc créer un déséquilibre entre le nombre de messages envoyés et le nombre de messages reçus. Ce déséquilibre épuise les crédits des véhicules. À l'inverse des modèles théoriques où les probabilités de réception et d'envoi sont égales pour tous les véhicules, un déploiement réel peut faire survenir des déséquilibres.

Pour y remédier, DTM^2 propose aux véhicules dont le crédit est faible de ne plus accepter les messages reçus pour ne plus avoir à payer de coûts de réception jusqu'à ce que leur montant de crédit s'élève. Le seuil choisi pour l'arrêt d'acceptation de message est fixé à : $\theta \leq \theta_0 \times \eta$, où le facteur η est compris entre $]0, 1[$. Il a pour but de pallier les problèmes d'inégalité dans les opportunités de coopération. Une fois que le montant de crédit du véhicule concerné s'élève à plus du seuil, soit en coopérant davantage ou en changeant de voie par exemple, il peut alors accepter tous les messages qui lui semblent valides.

5.6 Modèle de performance des paramètres

Pour ajuster les valeurs des paramètres de DTM^2 et étudier leur impact sur les performances, nous modélisons en chaîne de Markov à temps discret et à espace d'états discret l'évolution du montant du crédit d'un véhicule utilisant DTM^2. Notre modélisation prend en considération les caractéristiques du réseau, telles que la probabilité de collision d'un message, la portée de transmission d'un véhicule, la fréquence de détection d'événements à partager au sein du réseau et la connectivité entre les véhicules, dans le but d'atteindre un certain degré de réalisme. Ce modèle nous permet d'obtenir de façon analytique les pourcentages de détection et d'exclusion des véhicules malicieux au fil du temps, ainsi que le pourcentage de faux positifs, relatif à l'exclusion par erreur de véhicules dont le comportement est bon ou égoïste.

5.6.1 Définition du modèle

Nous modélisons au travers d'une chaîne de Markov l'évolution du montant de crédit d'un véhicule par rapport à son comportement dans le réseau. Notre chaîne comporte $(\theta_{max} + 1)$ états. Chacun d'entre eux représente le montant de crédit θ d'un véhicule. Ce montant est compris dans l'intervalle $[0, \theta_{max}]$. Les probabilités de transition entre deux états dépendent des actions influant sur un montant de crédits, tel que l'envoi d'un message, l'acceptation d'un message reçu et la réception d'une récompense.

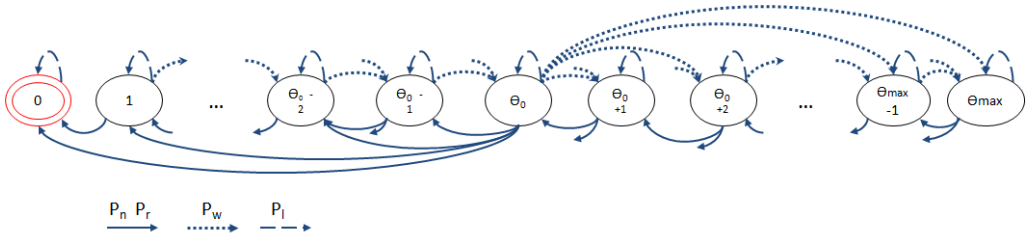


Figure 5.9 – Modélisation en chaîne de Markov pour l'optimisation des paramètres de DTM^2.

Table 5.2 – Notations utilisées lors de la modélisation de DTM^2.

P_t	Probabilité de réception d'un message à retransmettre
P_c	Probabilité de collision
θ_i	Montant du crédit à l'état i
P_m	Probabilité d'un comportement malicieux
P_g	Probabilité d'un comportement bon
P_s	Probabilité d'un comportement égoïste
λ	Intensité du processus de Poisson pour l'arrivée des événements détectés
$P[\theta_i][\theta_j]$	Probabilité de transition entre l'état θ_i et l'état θ_j
P_f	Probabilité qu'un message envoyé soit refusé à sa réception
P_v	Probabilité qu'un message envoyé soit accepté à sa réception
Pdf_B	Densité de probabilité pour une distribution binomiale
π	Probabilité stationnaire concernant la connectivité des véhicules entre eux
$P(x = k)$	Probabilité de détecter k événements d'après un processus de Poisson
P_n	Probabilité de non réception de récompense après l'envoi d'un message
P_r	Probabilité de réception d'un message
P_w	Probabilité de hausse du crédit après la réception d'une récompense
P_l	Probabilité de stagnation du crédit d'un véhicule

Nous modélisons la détection d'événements par les véhicules comme étant un processus de Poisson $P(x = k)$ d'intensité $\frac{\lambda}{N}$ pour chaque véhicule. Au départ de notre modélisation, un véhicule détient un montant de crédit égal au montant initial θ_0 défini par l'application. Il atteint l'état final et absorbant de notre modélisation lorsque son crédit est égal à zero. Le véhicule est alors exclu du réseau. Nous illustrons ces différents états dans la figure 5.9, nous donnons et expliquons les abréviations utilisées pour la modélisation dans le tableau 5.2.

Notre objectif est d'établir les probabilités stationnaires de notre modèle afin de déterminer le seuil maximum d'erreur sur les détections des véhicules dont le comportement n'est pas malicieux, à savoir le pourcentage de faux positifs. Pour cela, nous calculons la probabilité de détection d'un véhicule d'après le comportement qui lui a été assigné par le modèle. Un comportement assigné est un mélange de ces trois types de comportement : bon, égoïste et malicieux, avec différents pourcentages dont la somme est égale à un.

Un véhicule envoie un message dans deux cas, premièrement lorsqu'il détecte un événement. Cela se produit avec une probabilité de $1 - P(x = 0)$ suivant le processus de Poisson. Le second cas, dont la probabilité est de P_t, survient lorsqu'un véhicule reçoit un message qu'il doit retransmettre.

Dans notre modèle, le crédit d'un véhicule baisse dans trois cas :

1. La perte d'un message envoyé à cause d'une collision.
2. Le refus de réception d'un message envoyé pour manque de confiance en son authenticité.
3. Le paiement du coût de réception d'un message pour l'accès à son contenu.

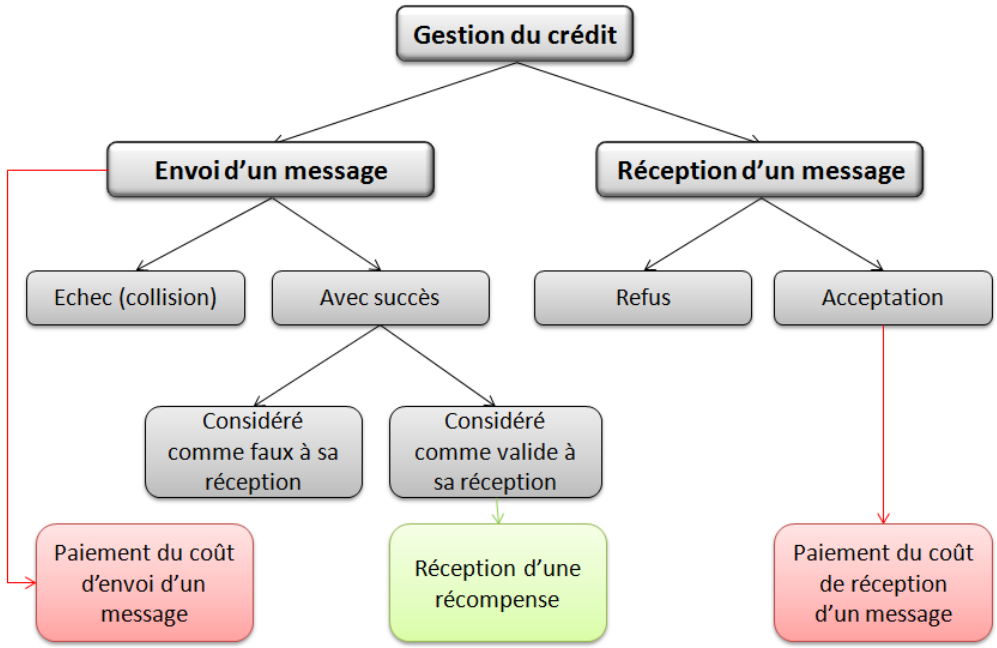


FIGURE 5.10 – Cas d'utilisation du crédit.

Le montant de crédit d'un véhicule croît uniquement après la réception d'une récompense. Ces cas d'utilisation sont illustrés dans la figure 5.10. Dans la suite, nous discuterons chaque possible changement d'état dans notre chaîne de Markov.

5.6.2 Perte d'un message envoyé ou refus de sa réception

Lorsqu'un véhicule détecte un événement à partager ou reçoit un message à retransmettre, il choisit un signal pour l'envoyer et paie le coût correspondant. Cependant, un message peut être perdu à cause d'une collision avec une probabilité P_c [53], ou alors malgré sa bonne réception, il est refusé par la majorité de ses véhicules récepteurs car perçu comme non authentique. Nous définissons cette probabilité par P_f. Lors de ces deux cas, le véhicule source ne reçoit pas de récompense malgré le coût payé pour son envoi, nous définissons ceci par la probabilité P_n.

$P_n[\theta_i][\theta_j]$ est la probabilité de transition d'un état avec θ_i crédits à celui avec θ_j crédits après le paiement du coût d'envoi pour un message. Son calcul est donné dans l'équation (5.16). Ce changement d'état fait référence au paiement d'un coût d'envoi de $C(Y^\star(\theta_i), \theta_i)$. Celui-ci est obtenu par l'équation (5.3) du calcul d'un coût d'envoi pour un véhicule possédant θ_i crédits et utilisant sa valeur optimale de signal. Le paramètre P_c de cette équation est la probabilité de collision d'un message par rapport à la densité des véhicules dans le réseau, comme détaillée dans l'étude [53]. Le paramètre Υ est défini, plus bas, dans le système d'équation (5.18).

$$P_n[\theta_i][\theta_j] = ((1 - P(x = 0)) + P_t) \times \Upsilon \times (P_c + (1 - P_c)P_f), \tag{5.16}$$

Où $\theta_j = \theta_i - C(Y^\star(\theta_i), \theta_i)$ et $\theta_j \geq 0$

L'envoi d'un message dépend de la nature du comportement de son émetteur. Nous définissons un comportement via une probabilité d'égoïsme P_s, de malice P_m et de conformité P_g, tel que la condition décrite dans l'équation (5.17) est respectée.

$$P_s + P_m + P_g = 1 \tag{5.17}$$

Lorsqu'un véhicule a un comportement conforme aux attentes du réseau, il procède à l'envoi d'un message avec l'utilisation de son signal optimal avec une probabilité de 1. À l'inverse, un véhicule égoïste procède à l'envoi d'un message uniquement lorsqu'il souhaite hausser son montant de crédits. Alors qu'un véhicule malicieux procède à l'envoi en altérant le contenu du message et en trichant sur la valeur de signal choisie, il utilise toujours une valeur de signal supérieure ou égale à $Y^\star(\theta_0)$ tant qu'il peut payer le coût correspondant. Ceci, afin de toujours apparaitre comme étant un véhicule dont le crédit est supérieur ou égal à θ_0, dans le but de gagner la confiance des véhicules ne le connaissant pas.

Dans le système (5.18) est donné Υ qui représente la probabilité qu'un véhicule procède à l'envoi d'un message en utilisant sa valeur de signal optimale, d'après son type de comportement et le montant de crédit qu'il possède. Lorsque le crédit d'un véhicule est inférieur à θ_0, Υ est égale à la somme des pourcentages d'un comportement bon et d'un comportement égoïste. Nous n'incluons pas à Υ le pourcentage d'un comportement malicieux car un véhicule de ce type n'utilise pas son signal optimal lorsque son crédit est faible, nous traiterons ce cas plus loin dans cette section. Quand le montant de crédit détenu par un véhicule est supérieur, Υ est égale à la somme des probabilités d'un comportement bon et d'un comportement malicieux. Nous ne considérons pas ici le comportement égoïste, car un véhicule égoïste ne coopère pas lorsque son montant de crédit est élevé.

$$\Upsilon = \begin{cases} P_g + P_s & Si\ \theta_i < \theta_0, \\ P_g + P_m & Sinon, \end{cases} \tag{5.18}$$

Nous définissons la probabilité de refus d'un message envoyé par ses récepteurs avec P_f. Son calcul dépend du signal Y utilisé lors de l'envoi, ainsi que du seuil de tolérance des véhicules récepteurs pour celui-ci. Nous définissons ce seuil à $Y^\star(\theta_0 \times \tau\%)$, soit un véhicule détenant seulement un pourcentage de $\tau\%$ du montant de crédit initialement donné n'inspire pas suffisamment confiance pour que les véhicules récepteurs de son message le valident. Son calcul est donné dans l'équation (5.19). Sa valeur est égale à 1 lorsque le signal est inférieur au seuil, à savoir que le message est refusé d'office. Dans le cas inverse, la valeur de P_f dépend du pourcentage de malice P_m dans le comportement d'un véhicule. Car il nous est impossible d'incorporer à notre modélisation de vraies réputations comme dans DTM^2 pour décider de l'acceptation ou non d'un message reçu, nous nous basons sur le pourcentage du comportement malicieux P_m du véhicule source pour remplacer sa valeur de réputation et donc définir la probabilité de refus de ses messages envoyés par ses voisins.

$$P_f = \begin{cases} 1 & Si\ Y < Y^\star(\theta_0 \times \tau\%), \\ P_m & Sinon, \end{cases} \tag{5.19}$$

Lorsque le crédit d'un véhicule malicieux est en dessous du montant θ_0, il triche sur les valeurs de signal qu'il utilise pour l'envoi de ses messages en utilisant le signal $Y^\star(\theta_0)$. Ceci, afin de donner une meilleur impression aux véhicules récepteurs et éviter de se faire refuser ses messages. Dans ce cas, la probabilité de transition de l'état θ_i, tel que $\theta_i < \theta_0$, à celui de θ_j à cause d'une perte de message après une collision ou d'un refus d'acceptation d'un message envoyé est donnée dans l'équation (5.20).

$$P_n[\theta_i][\theta_j] = ((1 - P(x = 0)) + P_t) \times P_m \times (P_c + (1 - P_c)P_f), \tag{5.20}$$

Où

$$\theta_j = \theta_i - C(Y^\star(\theta_0), \theta_i), \quad Avec\ \theta_j \geq 0$$
$$P_f = P_m$$

5.6.3 Paiement pour la réception d'un message

$P_r[\theta_i][\theta_j]$ est la probabilité de transition entre un état θ_i et un autre θ_j après le paiement du coût C_m pour l'accès à la version déchiffrée d'un message reçu. Son calcul est donné dans l'équation (5.21). Sa valeur dépend de la probabilité de recevoir un message. Cette dernière dépend à son tour de la probabilité qu'un des véhicules voisins détecte un événement et l'envoie sans rencontre de collision.

$$P_r[\theta_i][\theta_j] = N \times (1 - P(x = 0))\Phi(1 - P_c), \tag{5.21}$$

Où

$$\theta_j = \theta_i - C_m, \quad Avec\ \theta_j \geq 0$$
$$\Phi = \sum_{m=1}^{N-1} Pdf_B(m, \pi, N-1)\frac{m}{N-1}$$
$$Pdf_B(m, \pi, N-1) = \frac{(N-1)!\ \pi^m\ (1-\pi)^{N-1-m}}{(m!\ (N-1-m)!}$$

Φ représente la probabilité de réception d'un message par m véhicules parmi les véhicules du réseau hormis le véhicule source, soit $(N-1)$ véhicules. Avec une probabilité stationnaire de π concernant la connectivité du réseau. Son calcul dépend de la fonction de densité de probabilité pour une distribution binomiale $Pdf_B(m, \pi, N-1)$, définie dans [107], ainsi que la probabilité qu'un véhicule appartienne aux m véhicules qui ont reçu l'information, soit la probabilité $\frac{m}{N-1}$. Nous prenons en considération toutes les valeurs de m allant de 1 jusqu'à $(N-1)$.

Tout au long de notre modélisation, nous supposons pour plus de simplicité, que la probabilité d'avoir un message à retransmettre P_t est égale à celle de recevoir un message, avec l'hypothèse que tout message reçu est retransmis. P_t est donnée dans l'équation (5.22).

$$P_t = N \times (1 - P(x = 0))\ \Phi\ (1 - P_c) \tag{5.22}$$

5.6.4 Réception d'une récompense

Une récompense $W(Y)$ est attribuée à un véhicule lorsque son message envoyé est validé et considéré comme authentique par ses récepteurs. Dans notre modélisation un message reçu est validé si le pourcentage du comportement malicieux du véhicule source est en dessous d'un certain seuil, soit $P_m < \rho$; ainsi que si son signal utilisé est supérieur au seuil minimum fixé, soit $Y > Y^\star(\gamma \cdot \theta_0)$. La probabilité $P_w[\theta_i][\theta_j]$ de transition d'un état θ_i à un autre θ_j lors de la réception d'une récompense est calculée dans l'équation (5.23).

$$P_w[\theta_i][\theta_j] = ((1 - P(x = 0)) + P_t)\ \Upsilon\ P_v, \tag{5.23}$$

Où

$$\theta_j = \theta_i - C(Y^\star(\theta_i), \theta_i) + W(Y^\star(\theta_i))$$
$$Avec\ 0 \leq \theta_j \leq \theta_{max}$$
$$\Upsilon = \begin{cases} P_g + P_s & Si\ \theta_i < \theta_0 \\ P_g + P_m & Sinon \end{cases}$$
$$P_v = \begin{cases} 0 & Si\ (Y \leq Y^\star(\gamma \cdot \theta_0))\ ou\ (P_m \geq \rho) \\ 1 - P_m - P_c & Sinon \end{cases}$$

Tel que $P_v \geq 0$

La probabilité de réception d'une récompense dépend de la probabilité d'avoir un message à envoyer, soit de $((1 - P(x = 0)) + P_t)$, de la probabilité d'envoyer un message avec le signal correspondant au véhicule source avec Υ et enfin la probabilité de se voir accepter son message envoyé par ses récepteurs avec la probabilité P_v.

Un véhicule dont le comportement est bon ou égoïste utilise lors de son envoi un signal correspondant à son montant de crédit $Y^\star(\theta_i)$ et recevra une récompense de $W(Y^\star(\theta_i))$ d'après la probabilité P_w donnée dans l'équation (5.23). Alors qu'un véhicule malicieux, avec un crédit inférieur à θ_0 utilise un signal de $Y^\star(\theta_0)$, sa probabilité P_w diffère à cause de cela. Elle est donnée dans l'équation (5.24).

$$P_w[\theta_i][\theta_j] = ((1 - P(x = 0)) + P_t)\ P_m\ P_v, \tag{5.24}$$

Où

$$\theta_j = \theta_i - C(Y^\star(\theta_0), \theta_i) + W(Y^\star(\theta_0))$$

5.6.5 Stagnation du crédit

Le crédit d'un véhicule reste inchangé lorsqu'aucun envoi et aucune réception n'ont eu lieu. Cette probabilité de stagnation du crédit, P_l, est décrite dans l'équation (5.25).

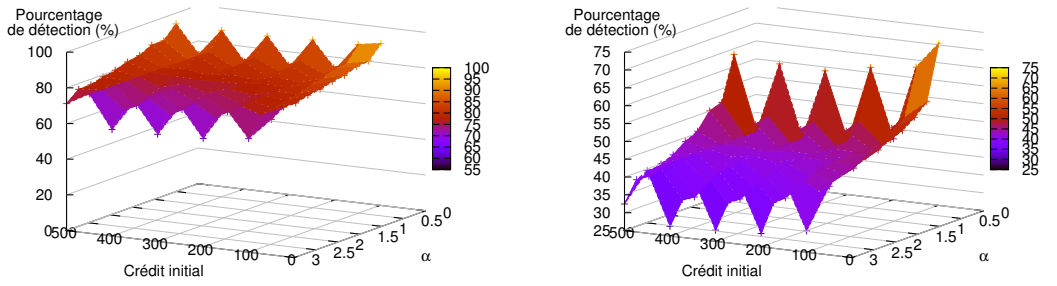
$$P_l[\theta_i][\theta_i] = 1 - \sum_{\theta_j=0}^{\theta_{max}} P[\theta_i][\theta_j] \tag{5.25}$$

L'état final et absorbant de notre chaine est atteint lorsqu'un véhicule épuise son crédit et qu'il ne peut plus participer dans le réseau. Les propriétés de cet état final sont décrites dans l'ensemble (5.26).

$$\begin{aligned} &P[0][0] = 1 \\ &P[0][\theta_j] = 0 \quad Avec\ \theta_j > 0 \end{aligned} \tag{5.26}$$

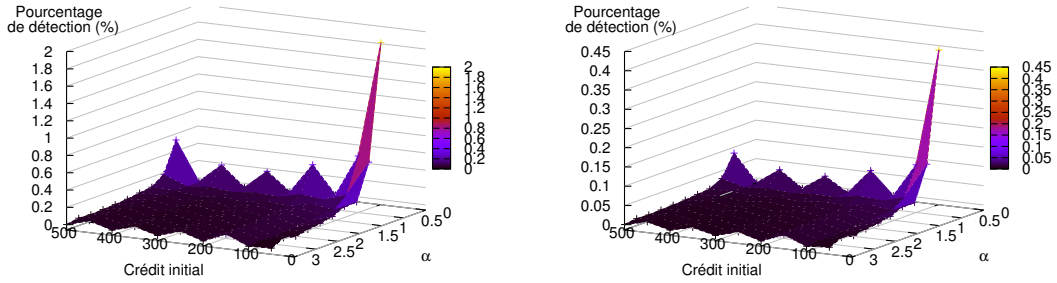
5.6.6 Discussion et analyse

Pour améliorer les performances de notre solution DTM^2 et ajuster ses résultats par rapport aux exigences des applications de sûreté, nous étudions l'impact de ses différents paramètres sur le pourcentage et la vitesse de détection des véhicules malicieux, ainsi que sur le pourcentage de faux positifs. Nous commençons par étudier l'impact du montant de crédit initialement donné à chaque véhicule lors de sa première connexion, θ_0, combiné à celui du paramètre α, soit le poids du crédit dans le calcul du coût d'un signal. En deuxième, nous étudions l'impact du changement de valeur pour le calcul de la base de récompense avec le coefficient σ. Pour finir, nous évaluerons l'impact du coefficient μ, qui est lié au coût de réception d'un message.



(a) $\lambda = 1$ (b) $\lambda = 0.2$

Figure 5.11 – Pourcentage de détection des véhicules malicieux par rapport à différentes valeurs de θ_0 et de α.



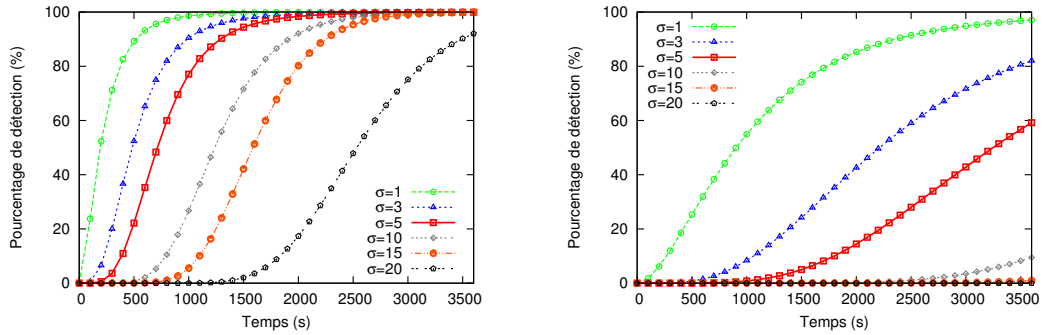
(a) $\lambda = 1$ (b) $\lambda = 0.2$

Figure 5.12 – Pourcentage de faux positifs par rapport à différentes valeurs de θ_0 et de α.

5.6.6.1 L'impact des paramètres θ_0 et α

Un montant de crédit important donné à chaque véhicule lors de sa première connexion au réseau lui donne l'opportunité de participer à sa guise au début. Car il peut accepter autant de messages qu'il le souhaite et en envoyer aussi, même si ses messages envoyés ne sont pas toujours validés. La participation d'un véhicule au réseau lui permet, ainsi qu'aux autres, de se connaitre et d'établir des réputations. Cependant, cette liberté donnée au début permet aussi aux véhicules malicieux d'envoyer beaucoup de faux messages et d'allonger leur durée de vie dans le réseau en payant les coûts d'envoi avec leur crédit initial.

Car les deux paramètres θ_0 et α influencent le calcul du coût d'envoi d'un message, comme décrit dans l'équation (5.3), nous étudions leurs impacts simultanés sur les performances de DTM^2 en termes de détection. Une faible valeur pour le paramètre α induit un coût de signalisation élevé et raccourcit la durée d'existence d'un véhicule malicieux dans le réseau en épuisant rapidement ses crédits. Cependant et comme ce fut le cas pour le montant de crédit initialement donné, des valeurs de paramètres extrêmes peuvent accélérer les détections de véhicules malicieux mais aussi engendrer beaucoup de faux positifs. La figure 5.11 illustre le pourcentage de détection des véhicules malicieux pour des valeurs de θ_0 allant de 50 jusqu'à 500 et des valeurs de α comprises dans l'ensemble $\{0.5, 1, 1.5, 2, 2.3, 2.5, 3\}$. Nous calculons les pourcentages de détection avec deux intensités d'arrivées d'évènements λ, car plus il y a d'échanges dans le réseau plus il y a d'interactions



(a) $\lambda = 1$ (b) $\lambda = 0.2$

Figure 5.13 – Pourcentage de détection des véhicules malicieux par rapport à la variation de σ, qui impacte les récompenses données.

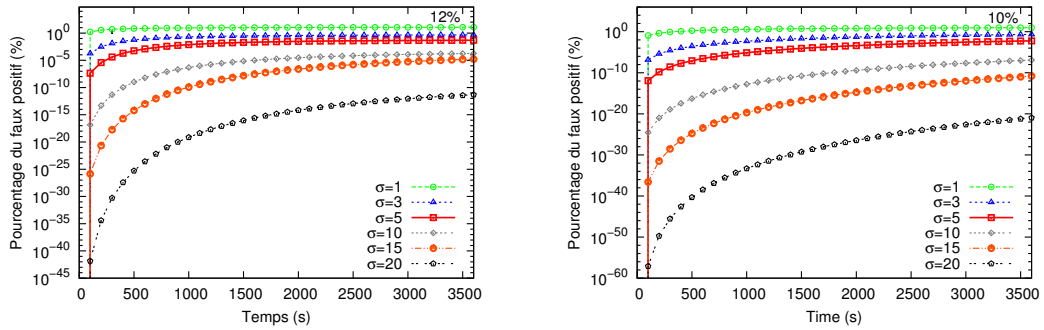
entre les véhicules et plus de crédits sont dépensés. Avec une valeur de λ égale à 1 les messages échangés sont nombreux entre les véhicules. Le pourcentage de détection d'un véhicule après 1000 secondes au sein d'un réseau de 500 véhicules est déjà important, il est illustré dans la figure 5.11(a). Le pourcentage du scénario avec $\lambda = 0.2$ est donné dans la figure 5.11(b) après 3000 secondes. Dans ce dernier, les résultats sont illustrés à un instant plus tardif que dans le premier cas à cause du faible taux d'évènements à envoyer. En effet, cela ralentit l'utilisation du crédit par les véhicules et donc ralentit aussi la détection. Nous remarquons un léger pic de détection avec $\lambda = 1$ et un autre plus important avec $\lambda = 0.2$ lorsque la paire (θ_0, α) est égale à $(50, 0.5)$. Pour le reste des combinaisons du couple (θ_0, α), le pourcentage de détection change plus rapidement avec les variations de valeurs du paramètre α. Cela se justifie par la relation exponentielle entre α et le coût d'un signal.

Dans la figure 5.12 sont donnés les pourcentages d'erreur dans les détections, soit le pourcentage de faux positifs. L'évolution de ce pourcentage suit celui des détections de véhicules malicieux, à savoir que deux pics sont aussi obtenus avec la paire $(50, 0.5)$. Le pourcentage de faux positifs avec l'utilisation de la paire $(50, 0.5)$ est égal à 1.9% avec $\lambda = 1$ et à 0.4% avec $\lambda = 0.2$. Alors qu'il est à 0.0074% et à 0.0028% avec $\lambda = 1$ et 0.2, respectivement, lorsque la paire $(100, 2.3)$ est choisie. Nous déduisons que plus la valeur de θ_0^α est petite, plus le pourcentage de faux positifs est important. Dans le reste de notre étude, nous choisissons des valeurs intermédiaires pour le couple (θ_0, α), soit $(100, 2.3)$, afin d'avoir un juste milieu entre les détections exactes et celles erronées.

5.6.6.2 L'impact de variation des récompenses à travers σ

Nous nous intéressons en second à l'impact qu'à la valeur des récompenses attribuées par le modèle, dont le calcul est effectué dans l'équation (5.5). Ce calcul utilise le paramètre σ pour définir une base pour les récompenses par la formule : $\frac{\theta}{\sigma}$. La figure 5.13 représente les performances de DTM^2 en termes de détection par rapport à différentes valeurs de σ allant de 1 jusqu'à 20.

La figure 5.13(a) illustre le pourcentage de détection des véhicules malicieux avec une valeur de $\lambda = 1$. Dans celle-ci, la détection débute à partir de 100 secondes lorsque $\sigma = 1$ et à partir de 1500 secondes lorsque $\sigma = 20$. Il existe alors une corrélation positive entre la valeur de σ et la vitesse de détection, car plus la valeur de σ est grande, plus la base d'une récompense est importante et moins vite diminue le crédit d'un véhicule malicieux. Cette corrélation reste la même avec l'utilisation de $\lambda = 0.2$, comme illustrée dans la figure 5.13(b). La détection avec une valeur de $\sigma = 1$ débute à partir de 150 secondes,



(a) $\lambda = 1$ (b) $\lambda = 0.2$

Figure 5.14 – Pourcentage de faux positifs par rapport à la variation de σ, qui impacte les récompenses données.

alors qu'elle ne débute qu'à partir de 3600 secondes avec une valeur de $\sigma = 15$ ou de 20. Nous en concluons que lorsque la base de référence d'une récompense est élevée, les performances de notre solution en sont réduites.

Tout comme notre observation précédente, dès que le pourcentage de détection des véhicules malicieux est élevé et la détection est rapide, il est de même pour le pourcentage de faux positifs, comme illustré dans la figure 5.14 pour λ égale à 1 et à 0.2. Même si ce pourcentage de faux positifs est faible généralement, il atteint quand même la valeur de 12% quand $\sigma = 1$ et $\lambda = 1$, car les récompenses attribuées avec ces valeurs de paramètres sont minces et insuffisantes pour couvrir les dépenses liées à l'envoi de messages et à l'accès aux messages reçus.

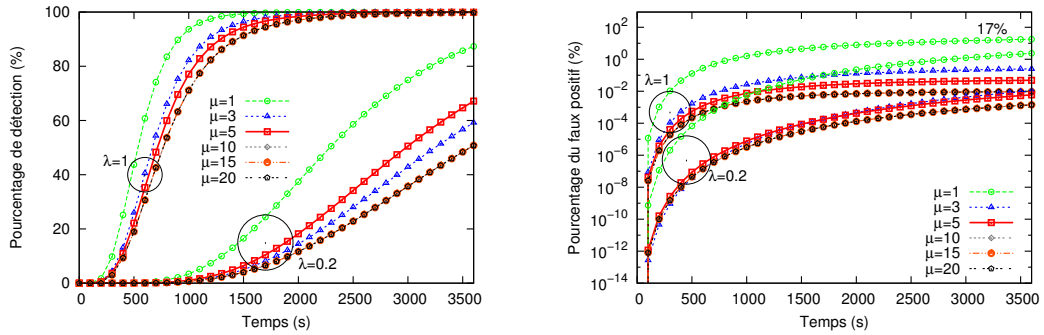
Dans le reste de notre étude nous choisirons une valeur de $\sigma = 5$, pour respecter un compromis entre le pourcentage de détection des véhicules malicieux et celui de la détection erronée.

5.6.6.3 L'impact de variation du coût de réception à travers μ

Le troisième paramètre étudié est μ. Ce dernier influe sur le calcul du coût de réception d'un message. Nous étudions l'impact de variation de la valeur de ce paramètre sur la détection des véhicules malicieux, ainsi que sur la coopération des véhicules égoïstes. En plus de contrôler l'évolution du crédit des véhicules, ce paramètre conditionne aussi la création du besoin en crédit auprès des véhicules égoïstes.

Dans la figure 5.15(a), le pourcentage de détection des véhicules malicieux est donné pour λ égale à 1 et à 0.2. Lorsque la valeur de μ est égale à 1, le coût de réception d'un message est égal à celui de la signalisation pour l'envoi d'un message pour un véhicule possédant θ_0 crédits d'après l'équation (5.14). Cela représente un coût de réception trop élevé pour un véhicule, car il reçoit beaucoup plus de messages qu'il n'en envoie.

Dans cette figure, la détection est rapide lorsque la valeur μ est petite. Le pourcentage est égal à 93% pour $\mu = 1$ et $\lambda = 1$, à 77% pour $\mu = 5$ et à 71% pour $\mu = 20$. Les résultats pour l'utilisation de $\lambda = 0.2$ sont semblables, le pourcentage est égal à 74%, 42% et 35% pour μ égal à 1, 5 et 20, respectivement. Le pourcentage de faux positifs évolue de façon similaire, comme illustré dans la figure 5.15(b). Ce pourcentage est égal à 17% avec $\mu = 1$ et $\lambda = 1$ et à 2% dans le deuxième scénario avec $\lambda = 0.2$. Ces valeurs sont disproportionnées par rapport au reste des valeurs obtenues avec une valeur plus grande de μ telle que 5, où les pourcentages sont de 0.048% et de 0.000059% dans les deux scénarios. Nous en concluons que plus le coût de réception est élevé plus important est le pourcentage



(a) Pourcentage de détection des véhicules malicieux

(b) Pourcentage de faux positifs

Figure 5.15 – Pourcentage de détection par rapport à différentes valeurs de μ, influant sur le coût de réception d'un message.

de détection des véhicules malicieux et de même pour le pourcentage de faux positifs. Nous fixons à 5 la valeur de μ dans le reste de notre étude, afin d'atteindre un haut pourcentage de détection de véhicules malicieux, tout en minimisant le pourcentage de faux positifs.

5.7 Évaluation de performance

5.7.1 Paramètres de l'étude de performance

Nous évaluons les performances de notre modèle de confiance par rapport à sa capacité à détecter et à exclure les véhicules malicieux et à celle d'inciter les véhicules égoïstes à coopérer. Dans notre étude de performances, un véhicule malicieux envoie de fausses informations et utilise, même s'il faut tricher, un signal toujours supérieur ou égal à $Y^{\star}(\theta_0)$. Alors qu'un véhicule égoïste ne coopère que lorsqu'il a besoin de gagner du crédit. Nous fixons ce seuil de besoin en crédit pour un véhicule égoïste à θ_0.

Les métriques choisies pour notre étude de performances sont :

- Le pourcentage de détection des véhicules malicieux, ainsi que le pourcentage de faux positifs. Ceci via notre modélisation, ainsi que nos deux scénarios de simulations, afin d'étudier les performances de notre modèle vis-à-vis des véhicules malicieux.
- Le nombre de faux messages considérés comme valides par les véhicules récepteurs, lors de différentes compositions du réseau par rapport au nombre de véhicules malicieux présents, afin d'étudier l'impact des faux messages sur le réseau avant l'exclusion des véhicules malicieux.
- Le taux de coopération dans un réseau comportant différents pourcentages de véhicules égoïstes, afin d'évaluer l'efficacité de la partie incitative de DTM^2.

Nous évaluons chacune de ces métriques avec une intensité d'arrivée λ différente pour les événements à détecter et à envoyer dans le réseau. Nous choisissons une fréquence élevée avec $\lambda = 1$, soit un événement est détecté et envoyé par un véhicule chaque 1 seconde. Ainsi qu'une fréquence moins élevée avec $\lambda = 0.2$, soit un événement envoyé en moyenne chaque 5 secondes. Nous détaillons et justifions les résultats analytiques obtenus via notre modèle analytique et ceux obtenus par simulation pour chacune de nos métriques.

Nous effectuons nos simulations sur NS2-34 [1] en incluant l'extension requise pour le protocole de la couche MAC 802.11p [11]. Nous utilisons deux générateurs de mobilité, VanetMobisim [40] pour le scénario autoroute et SUMO [4] pour l'urbain, afin de bénéficier de la précision de chacun d'eux dans son domaine d'expertise [26]. Le premier scénario

Table 5.3 – Paramètres de simulation.

Nombre de véhicules : 500	Protocole de la couche Mac : IEEE 802.11p
Portée de transmission : 250m	Durée de la simulation : 3600s et 10800s
Taille de la zone urbaine : 6×6 Km^2	Longueur de l'autoroute : 35 Km
Vitesse dans la zone urbaine : 20-50 km/h	Vitesse dans l'autoroute : 90-160 km/h
Intensité d'arrivée des événements λ=1 et 0.2	Débit : 6 Mbps
Stratégie de dissémination des données : ADCD [50]	τ=20
β=5	α=2.3
σ=5	θ_0=100
π=0.01	P_c=0.02
ρ=0.5	γ=20%
η=10%	μ=5

se passe sur une autoroute de 35 Kilomètres, avec une vitesse allant de 90 km/h jusqu'à 160 km/h pour les véhicules simulés. Le deuxième scénario se passe quand à lui dans un environnement urbain d'une taille de 36 km^2, avec une vitesse comprise dans l'intervalle $[20, 50]$ km/h. Nos deux scénarios comportent 500 véhicules chacun, par contre nous varions la durée de simulation d'après la valeur de λ utilisée. Avec une fréquence d'envoi de messages importante, une durée de simulation de 3600s est suffisante pour nos mesures, alors que quand la fréquence est basse, nous rallongeons notre simulation jusqu'à 10800s. Les valeurs des autres paramètres utilisés dans notre étude de performances sont données dans le tableau 5.3. Afin d'avoir des véhicules avec différents comportements, nous instaurons un pourcentage de comportement malicieux et un autre pour le comportement égoïste dans chaque véhicule, tel que :

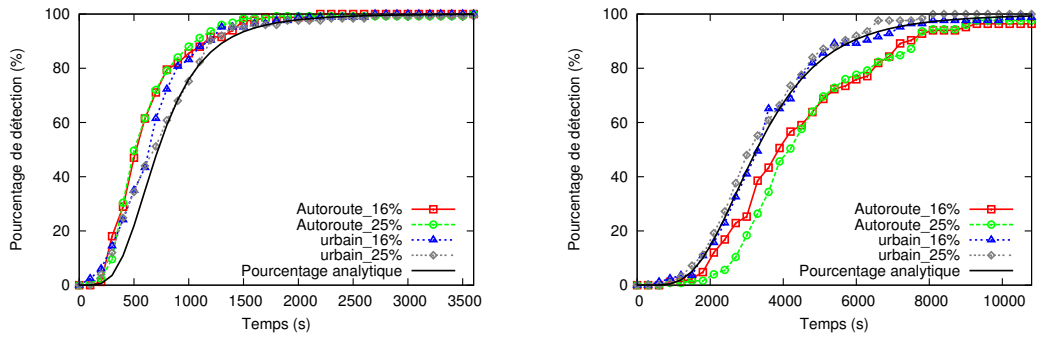
- Les véhicules que nous nommerons malicieux sont ceux avec le pourcentage de comportement malicieux le plus élevé. Nous le définissons à 80%. Ces véhicules sont aussi bons à 20% et 0% égoïstes.
- Les véhicules égoïstes ont un pourcentage de comportement égoïste égal à 80%. Ils sont aussi bons à 20% et 0% malicieux.

Chacun de ces véhicules, indifféremment de sa nature, se voit doter d'un crédit initial égal à 100 crédits lors de sa première connexion au réseau.

5.7.2 Pourcentages et délais de détection

Les figures 5.16(a) et 5.16(b) présentent l'évolution du pourcentage de détection des véhicules malicieux tout au long de la durée de simulation dans les deux scénarios avec λ égale à 1 puis à 0.2. Nous comparons, à chaque fois, les résultats de simulations dans les deux environnements autoroute et urbain, ainsi qu'avec les résultats analytiques. Nous remarquons à chaque fois la concordance entre les résultats issus de la simulation avec ceux de l'étude analytique. En plus de varier les environnements, nous changeons aussi la composition du réseau par rapport au pourcentage de véhicules malicieux présents, nous choisissons les valeurs de 16% et de 25%.

Dans le premier scénario, où les fréquences d'envoi de messages sont élevées avec $\lambda = 1$, le pourcentage de détection atteint 50% aux alentours de l'intervalle $[500, 700]$ secondes pour les différents environnements et compositions du réseau. Après 2000s de simulation, le pourcentage de détection dépasse les 98% et est égal à 100% après 3000s. Comparés aux résultats donnés dans la figure 5.16(a), ceux de la figure 5.16(b) atteignent les 100% de pourcentage de détection bien plus tard dans la simulation. Ceci est dû à la basse fréquence d'envoi de messages, car moins d'échanges il y a, moins de coûts d'envoi et de réceptions sont payés, ce qui ralentit l'épuisement du crédit des véhicules malicieux. Avec $\lambda = 0.2$, le



(a) $\lambda = 1$ (b) $\lambda = 0.2$

Figure 5.16 – Pourcentage de détection des véhicules malicieux.

pourcentage de détection de 50% est atteint après 3300s dans l'environnement urbain et après 4100s quand il s'agit du scénario autoroute. De même pour le pourcentage 75% qui est atteint après 4400s et 5900s, respectivement. Enfin le pourcentage de détection est à 96% après 7000s et 9000s dans les deux environnements de mobilité.

Dans la figure 5.16(a), l'importante fréquence d'envoi accélère l'établissement des réputations locales entre les véhicules et par cela affine les décisions des véhicules sur l'acceptation ou non des messages reçus. Grâce à cette précision, les crédits des véhicules malicieux diminuent rapidement et s'épuisent. Cependant, nous remarquons que la composition du réseau en nombre de véhicules malicieux, soit en 16% et en 25%, n'a pas d'impact significatif sur la vitesse et le taux de détection.

Notre deuxième remarque concerne la légère hausse des courbes du pourcentage de détection dans l'environnement autoroute par rapport à l'urbain avec $\lambda = 1$, puis l'inversion qui a lieu dans le scénario utilisant $\lambda = 0.2$. Nous justifions cela par les différents degrés de connectivité qu'ont les véhicules dans ces environnements. En effet, dans un environnement urbain la topologie du réseau est plus changeante que dans un environnement autoroute, ceci ne permet donc pas d'avoir des réputations très précises et ralentit un peu la détection des véhicules malicieux dans le premier scénario. Par contre, ce changement fréquent permet de rencontrer plus de véhicules que dans un environnement autoroute et d'avoir une vue plus globale même si elle n'est pas très précise. Ceci dynamise l'envoi des messages et augmente leur taux de retransmission. Alors que l'envoi des messages est limité par les trajectoires qui sont constantes dans un environnement autoroute. Comme déjà remarqué dans cette étude, plus d'échanges il y a et plus vite sont détectés les véhicules malicieux.

5.7.3 Pourcentages des faux positifs

Les pourcentages des détections et d'exclusions erronées sont donnés dans la figure 5.17, où quatre courbes illustrent les résultats issues de l'étude analytique. Nous varions la valeur de λ et le type de véhicules exclus par erreur, afin d'obtenir le pourcentage de faux positifs pour chacun des véhicules dont le comportement est bon ou égoïste séparément. Nous ne représentons pas le pourcentage de faux positifs issu de notre simulation car il est égal à 0, nous n'avons eu aucune détection erronée durant nos différents scénarios de simulation. Nos résultats analytiques nous réconfortent sur ce point, le risque le plus élevé de détecter par erreur est de 0.236583% pour un véhicule égoïste après 70000s avec une intensité d'envoi de messages de $\lambda = 0.2$, ce risque est très faible. Dans nos autres scénarios, ce pourcentage de faux positifs se stabilise dans le temps, ce qui nous fait penser que des probabilités

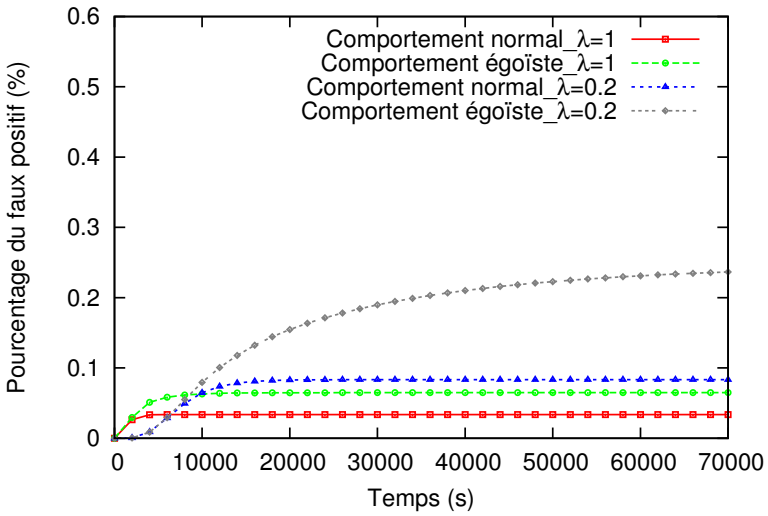


Figure 5.17 – Pourcentage analytique de faux positifs.

stationnaires ont été atteintes et que même si l'étude s'allonge davantage dans le temps elles ne changerons pas. Ce pourcentage est égal et se stabilise à 0.0336701% après une durée de 8300s avec $\lambda = 1$ pour un véhicule dont le comportement est bon et à 0.0833375% après un temps de 42500s avec $\lambda = 0.2$. Ce pourcentage augmente un peu lorsqu'il s'agit de la détection erronée d'un véhicule égoïste, il se stabilise à 0.0648695% après un temps de 43100s avec $\lambda = 1$ et à 0.236583% après 70000s avec $\lambda = 0.2$.

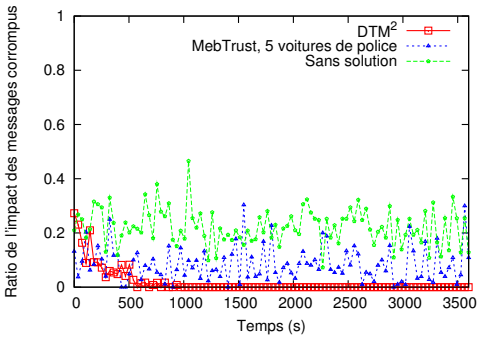
Les performances de notre solution dépendent du nombre d'échanges de messages entre les véhicules. Lorsque celui-ci est très faible avec $\lambda = 0.2$, une légère hausse du pourcentage de faux positifs a lieu. Elle concerne davantage les véhicules égoïstes que les véhicules bons. Car les véhicules égoïstes, après avoir refusé de coopérer, peuvent ne plus avoir l'occasion de le faire quand l'intensité d'arrivée des évènements est faible, ce qui finit par épuiser leurs crédits sans qu'ils aient eu le temps de se rattraper. Nous minimisons ces pourcentages de faux positifs grâce à la technique de sauvegarde de crédit de DTM^2, tel qu'il est conseillé à un véhicule dont le montant de crédit est trop faible, soit inférieur à "$\theta_0 \times \eta$" de suspendre l'acceptation de message le temps nécessaire pour retrouver un niveau de crédit suffisant.

5.7.4 L'impact des faux messages

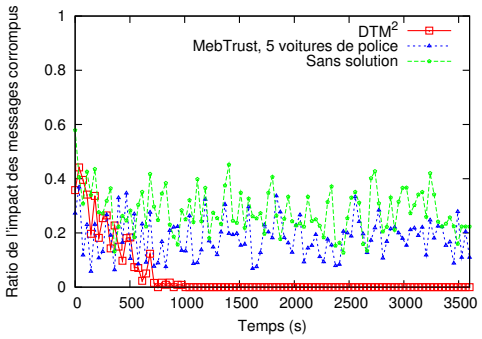
Les objectifs du modèle de confiance DTM^2 ne se limitent pas à exclure les véhicules malicieux du réseau mais aussi à contrer la diffusion des fausses informations générées par eux et acceptées puis retransmises par erreur par des véhicules non malicieux. Pour étudier l'efficacité de DTM^2, nous calculons le pourcentage de faux messages acceptés et considérés comme vrais par les véhicules récepteurs. Nous comparons ce pourcentage dans un réseau utilisant le modèle confiance DTM^2, avec un deuxième utilisant la solution MEB_Trust [71] et un troisième n'utilisant aucune solution.

Un véhicule utilisant la solution MEB_Trust demande à ses voisins directs leur avis pour chaque information qu'il reçoit afin de l'accepter ou de la refuser. Une fois un nombre minimum de réponses reçues, ce véhicule calcule la moyenne des avis en les pondérant par rapport à la réputation qu'il détient sur chacun de leur auteur. Les auteurs de cette solution, incluent aussi le critère du rôle ou de la catégorie du conducteur qui a émis l'avis, plus de poids est donné alors à un véhicule de police qu'à un véhicule ordinaire.

Nous comparons notre solution avec MEB_Trust par rapport à la métrique

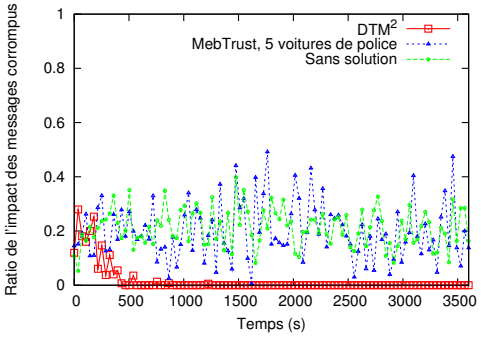


(a) *Pourcentage de véhicules malicieux* = 16%

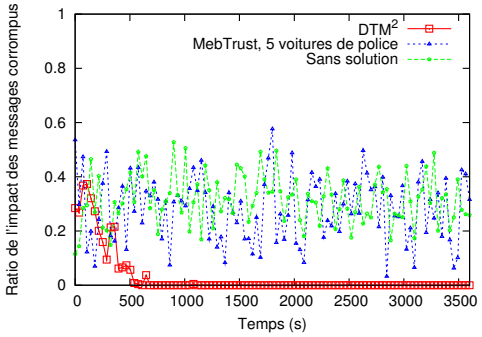


(b) *Pourcentage de véhicules malicieux* = 25%

FIGURE 5.18 – Taux moyen de messages corrompus acceptés dans le scénario urbain, avec $\lambda = 1$.



(a) *Pourcentage de véhicules malicieux* = 16%



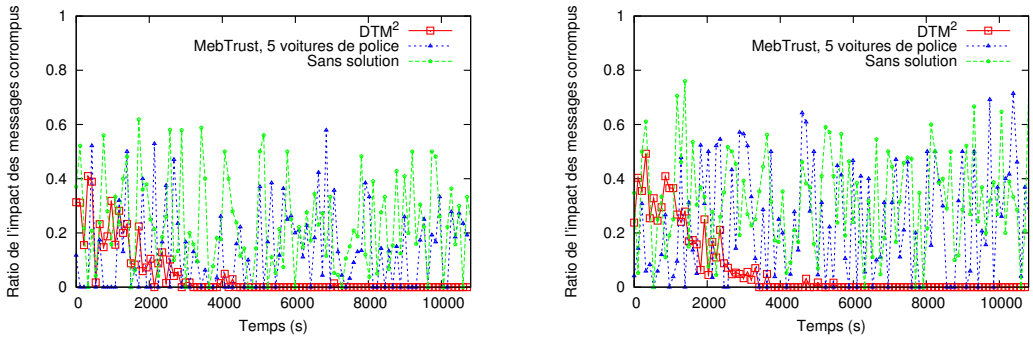
(b) *Pourcentage de véhicules malicieux* = 25%

FIGURE 5.19 – Taux moyen de messages corrompus acceptés dans le scénario autoroute, avec $\lambda = 1$.

concernant l'étendue des faux message dans un réseau. Car même si cette solution n'exclut pas les véhicules malicieux elle freine néanmoins l'acceptation de leurs faux messages auprès des véhicules récepteurs. Les performances de MEB_Trust dépendent du nombre de véhicules de police déployés dans le réseau. Ces derniers savent toujours si une information est correcte ou pas et peuvent répondre correctement aux véhicules qui les contactent. Durant nos simulations nous avons utilisé cinq voitures de police dans notre réseau de 500 véhicules, soit 1% des membres du réseau sont des policiers, ce qui est la même proportion utilisée dans les simulations de ses auteurs [71].

Les figures 5.18 et 5.19 illustrent le pourcentage moyen de faux messages reçus et acceptés par les véhicules pour chacun de nos deux environnements de mobilité, avec deux fréquences d'envoi de messages différentes et deux compositions de réseau par rapport au pourcentage de présence des véhicules malicieux.

La première figure présente les résultats pour le scénario de mobilité urbain avec $\lambda = 1$. Nous y remarquons que le pourcentage de faux messages acceptés par les véhicules utilisant la solution DTM^2 décroit rapidement et atteint les 0% avant les 1000s de temps de simulation dans les deux cas où le réseau contient 16% et 25% de véhicules malicieux. Nous rappelons que le pourcentage d'exclusion des véhicules malicieux a atteint les 100% dans ce même scénario qu'à partir de 3000s, soit bien après que le pourcentage d'acceptation de faux messages atteigne les 0%. Cela est dû au mécanisme d'acceptation de messages reçus proposé par DTM^2, où un véhicule se base sur la réputation locale qu'il détient sur



(a) *Pourcentage de véhicules malicieux* = 16% (b) *Pourcentage de véhicules malicieux* = 25%

Figure 5.20 – Taux moyen de messages corrompus acceptés dans le scénario urbain, avec $\lambda = 0.2$.

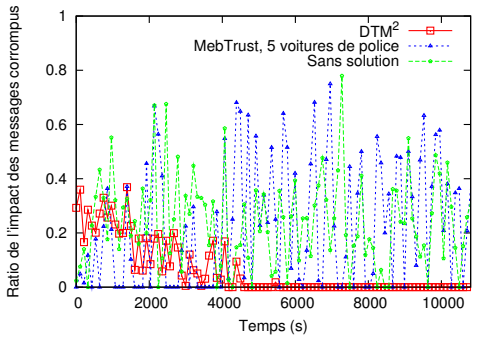
l'auteur d'un message ainsi que sur son signal utilisé pour accepter ou non un message, ainsi il arrive à reconnaitre les véhicules malicieux et à refuser leurs messages avant leur exclusion du réseau.

Meb_Trust apporte une légère amélioration par rapport au scénario où aucune solution n'est déployée, mais son pourcentage d'acceptation de faux messages n'atteint jamais les 0%, car la solution n'exclut pas les véhicules malicieux du réseau. Aussi, cette solution ne passe à l'échelle car elle est moins performante lorsque 25% des véhicules du réseau sont malicieux par rapport au cas avec 16%.

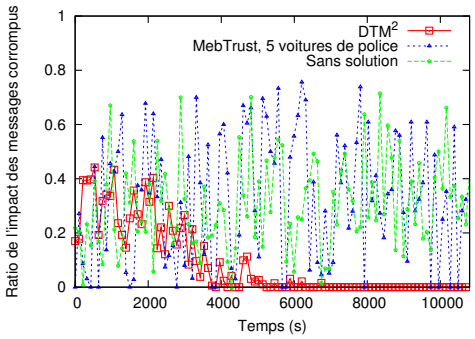
Les résultats issus du scénario autoroute avec $\lambda = 1$ sont donnés dans les figures 5.19(a) et 5.19(b). Ils sont similaires à ceux du scénario urbain et même un peu mieux concernant les performances de DTM^2. Le pourcentage 0% est atteint aux alentours de 500s, soit un peu plus tôt que pour le scénario urbain, car les réputations s'établissent plus rapidement et sont plus précises dans un environnement autoroute où les changements de topologie sont moins importants.

En diminuant la fréquence d'envoi des messages lors de l'utilisation de $\lambda = 0.2$, les résultats différent des scénarios précédents avec $\lambda = 1$. Ils sont illustrés dans les figures 5.20 et 5.21 pour les deux scénarios dont l'environnement est urbain ou en autoroute. Le pourcentage de réception de faux messages oscille énormément pour le scénario utilisant la solution *Meb_Trust*, ainsi que pour le scénario qui n'utilise pas de solution. Les performances de *Meb_Trust* dépendent énormément de la présence de véhicules de police pour répondre aux interrogations des conducteurs sur la validité des informations reçues, ainsi que l'établissement et la précision des réputations entre les véhicules. Ce dernier point a plus de difficultés à converger lorsque la fréquence d'échanges de messages est faible ou que les véhicules malicieux sont trop nombreux. Cette solution est alors insuffisante et inefficace lorsqu'il s'agit de grand réseau avec une mobilité forte tel que les VANETs.

Lors de l'utilisation de DTM^2, ce pourcentage a atteint 0% après 4400s avec une présence de véhicules malicieux égale à 16% et après 5500s lorsque la proportion des véhicules malicieux était à 25%. Ce pourcentage est à 0% avant même l'exclusion totale des véhicules malicieux du réseau dans les ceux cas. Comme pour *Meb_Trust*, les échanges peu fréquents diminuent des performances de DTM^2, mais à moins grande échelle.



(a) *Pourcentage de véhicules malicieux* = 16%



(b) *Pourcentage de véhicules malicieux* = 25%

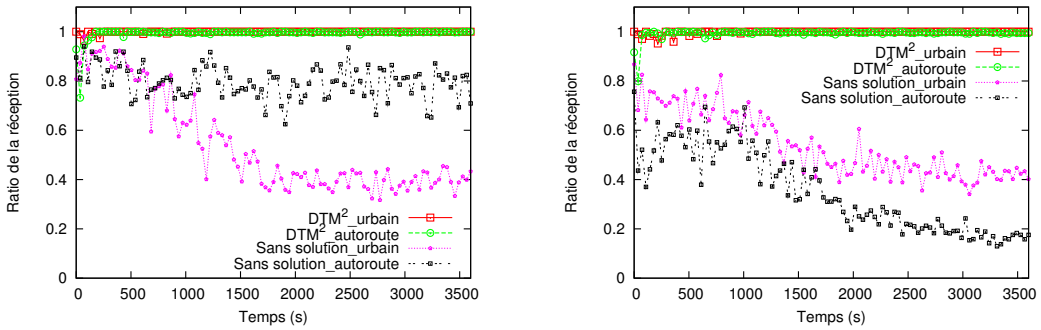
FIGURE 5.21 – Taux moyen de messages corrompus acceptés dans le scénario autoroute, avec $\lambda = 0.2$.

5.7.5 La coopération dans un réseau comportant des véhicules égoïstes

Car la non réception d'information de sûreté peut mettre en danger les conducteurs, nous étudions l'efficacité de notre solution par rapport à la présence de véhicules égoïstes dans le réseau. Pour cela, nous calculons le taux de réception des événements détectés auprès des véhicules aux alentours. Ce taux est directement lié à la coopération et participation des véhicules avec l'envoi des événements détectés et la retransmission des messages reçus quand le véhicule est désigné pour. Dans notre scénario, un véhicule égoïste est rationnel, ce qui le fait coopérer quand ses crédits sont peu nombreux, soit inférieur à θ_0 dans cette simulation.

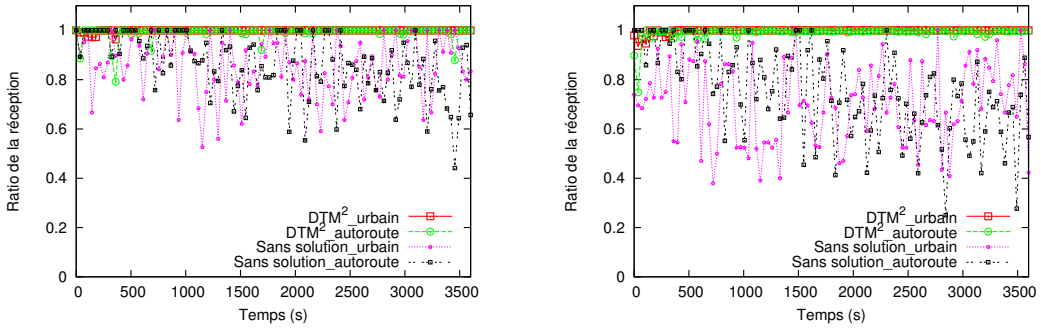
Nous comparons les performances d'un réseau utilisant la solution DTM^2 à un autre qui n'utilise aucune solution, dans différents scénarios. Les figures 5.22(a) et 5.22(b) illustrent le ratio moyen de réception pour nos deux scénarios de mobilité avec $\lambda = 1$ et une présence de 25% puis de 50% de véhicules égoïstes. Ce ratio se stabilise rapidement à 1 avec l'utilisation de DTM^2 pour les deux scénarios de mobilité, ainsi que pour les deux compositions de réseau en véhicules égoïstes. Car DTM^2 arrive rapidement à créer un besoin constant en crédit auprès de ces véhicules égoïstes grâce au paiement pour l'accès aux messages reçus. Ceci se reflète par leur coopération constante dans le temps. Alors que ce ratio se dégrade énormément dans le temps s'agissant du réseau n'utilisant pas de solution. On remarque nettement alors les effets négatifs qu'ont les véhicules égoïstes sur les performances d'un réseau.

Une différence est visible pour les performances de ce réseau dans les deux scénarios de mobilité. Les performances sont moins affectées dans le scénario autoroute lorsque la présence des véhicules égoïstes est faible, alors qu'elles le sont beaucoup plus que dans le scénario urbain lorsque la présence des véhicules égoïstes est à 50%. Ceci s'explique par le type d'interactions entre les véhicules de chaque scénario. Le scénario autoroute supporte bien la présence de 25% de véhicules égoïstes, car les véhicules sont disposés en forme de petits groupes par rapport à leur portée de communication. Un événement détecté ne concerne alors qu'un seul petit groupe à la fois, ce qui rend plus facile la transmission d'un message même lorsque 1 véhicule sur 4 refuse de le relayer. Alors que lorsque ce refus passe à un taux de 1 sur 2, la transmission devient beaucoup plus difficile surtout quand c'est le véhicule égoïste lui même qui détecte l'information et refuse de l'envoyer. Car les véhicules ne forment pas de petits groupes dans un scénario urbain, les véhicules concernés par un événement sont beaucoup plus difficiles à atteindre et le fait qu'une partie des potentiels relayeurs, avec un pourcentage de 25% ou de 50%, refusent de coopérer cela rend la tâche



(a) 25% de véhicules égoïstes (b) 50% de véhicules égoïstes

Figure 5.22 – Pourcentage moyen de réception dans un réseau comportant des véhicules égoïstes, avec $\lambda = 1$.



(a) 25% de véhicules égoïstes (b) 50% de véhicules égoïstes

Figure 5.23 – Pourcentage moyen de réception dans un réseau comportant des véhicules égoïstes, avec $\lambda = 0.2$.

encore plus difficile.

Les figures 5.23(a) et 5.23(b) présentent les résultats lors de l'utilisation d'une valeur de λ égale à 0.2. Les taux de réception sont meilleurs car moins de messages sont envoyés, soit les véhicules ratent moins de messages à cause du refus de coopération des véhicules égoïstes. Le taux de réception lors de l'utilisation de DTM^2 est comme auparavant égal à 1 dans tous les scénarios, alors que le taux lorsqu'aucune solution n'est déployée oscille entre 1 et 0.4, soit une amélioration de 42%.

Cette étude de performances nous a permis d'étudier l'efficacité de la détection et de l'exclusion des véhicules malicieux du réseau par notre modèle de confiance DTM^2. Tous les véhicules malicieux ont été exclus du réseau, soit un pourcentage de détection égal à 100%, avec des pourcentages de faux positifs inférieurs à 0.24%. Nous avons aussi vérifié que l'impact des véhicules malicieux dans le réseau s'affaiblissait avec le temps, même avant leur exclusion totale. Enfin, nous avons étudié l'efficacité du mécanisme incitatif de DTM^2 par rapport aux véhicules égoïstes et à leur coopération au sein du réseau. Nous avons démontré une amélioration de 42% dans le taux de réception des messages.

5.8 Analyse de sécurité

Un véhicule malicieux est libre de choisir la valeur du signal à utiliser lors de ses envois de messages. Il peut alors manipuler cette valeur de façon malicieuse, dans le but

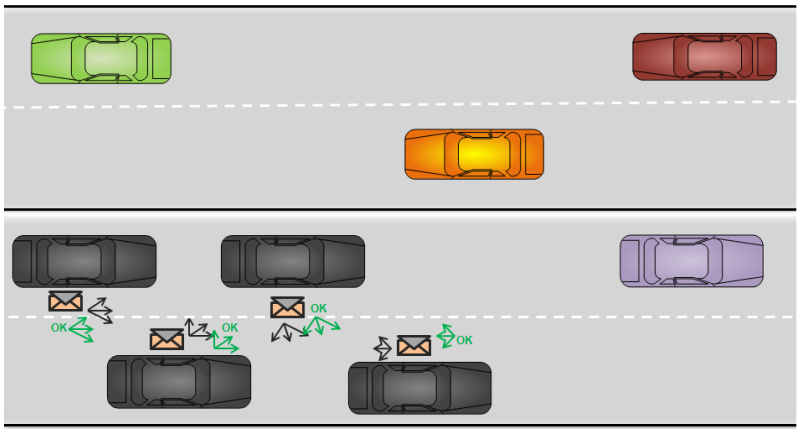


Figure 5.24 – Exemple d'une attaque coopérative entre véhicules malicieux. Ces véhicules s'entraident en s'envoyant des notifications positives.

de tromper les autres véhicules. Il peut aussi organiser des attaques coopératives avec les autres véhicules malicieux pour gagner plus de crédits, ou même alterner entre un comportement malicieux et un autre bon pour retarder sa détection et exclusion du réseau. Nous présentons ci-dessous ces trois cas de figure et nous détaillons comment notre modèle de confiance y fait face.

5.8.1 Manipulation malicieuse du signal

Un véhicule peut tricher de deux façons différentes à propos du choix de son signal lors de ses envois. Un véhicule malicieux peut décider de coopérer et de bien agir durant une certaine période de temps dans le but de hausser son montant de crédits. Pour cela, il utilise des valeurs de signal importantes dans le but de gagner la confiance des véhicules récepteurs de ses messages et ainsi recevoir des récompenses importantes, étant donné que ces dernières sont proportionnelles aux valeurs de signal utilisées. Cependant, l'utilisation de valeur de signal non correspondante à son réel montant de crédit coûte cher, car même avec d'importantes récompenses reçues dans le cas où les messages envoyés sont acceptés, le bénéfice net d'un véhicule qui a triché sur son signal est minime et souvent négatif. Plus un véhicule triche sur ses signaux plus son crédit baisse et plus ces mêmes signaux lui coûtent cher dans le futur.

Tout comme hausser ses valeurs de signal, un véhicule peut les baisser dans le but de minimiser ses frais d'envoi de messages. L'utilisation de faibles valeurs de signal introduit de la méfiance auprès des véhicules récepteurs et fait croître leur taux de refus pour les messages reçus. Sans une majorité de véhicules récepteurs qui acceptent un message reçu, un véhicule source n'est pas récompensé, ce qui ne lui permet pas de couvrir ses frais d'envoi. Il finit donc par épuiser son crédit.

DTM^2 incite les véhicules à choisir le signal leur correspondant en maximisant les gains des véhicules lors de l'utilisation de $Y^\star$. Ceci dans le but de donner une indication sur leurs comportements aux autres véhicules présents et à remédier à l'asymétrie de l'information dans les VANETs.

5.8.2 Attaques coopératives des véhicules malicieux

DTM^2 attribue des récompenses lorsque la majorité des notifications reçues à propos d'un message envoyé sont positives. Des véhicules malicieux peuvent alors s'entraider en

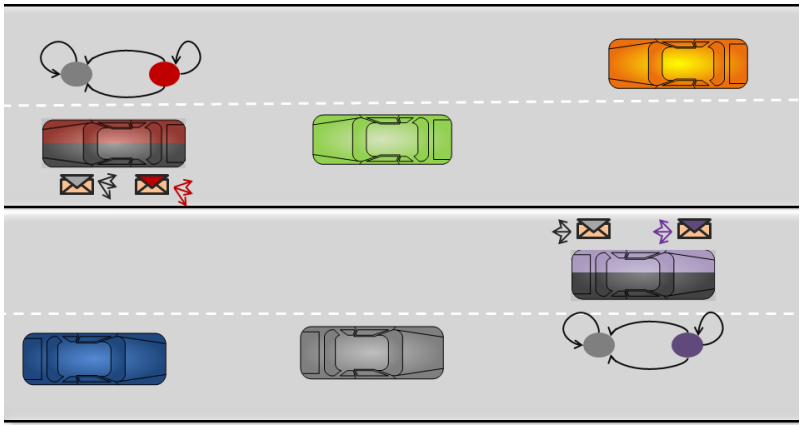


Figure 5.25 – Exemple de véhicules alternant entre comportements malicieux et bon. Les véhiculés en haut à gauche et en bas à droite de la figure alternent entre bon et mauvais comportement. Ceci est illustré par un changement de couleur au sein de ces véhicules.

s'envoyant des notifications positives pour leurs envois de messages respectifs, comme illustré dans la figure 5.24. Notre modèle de confiance empêche cela en imposant un paiement pour l'accès aux messages reçus. Une notification d'acceptation n'est envoyée au véhicule source qu'après ce paiement. Dans le cas où un véhicule doit accepter tous les messages envoyés par ses semblables, ses frais en coût de réception explosent par rapport à la récompense qu'il reçoit pour son message envoyé et validé en retour.

DTM^2 contrôle cela en décidant du rapport entre le coût de réception et le coût d'envoi pour un message via le paramètre μ, soit jusqu'à quel point il est intéressant pour un véhicule de valider les messages des autres pour qu'on lui valide le sien en retour. Aussi une seconde condition peut être établie par rapport à ce genre de complot, comme fixer le nombre minimum de notifications à recevoir avant de prendre une décision sur l'attribution ou non de récompense, afin d'éviter que de petits groupes de véhicules malicieux s'isolent du reste des véhicules pour comploter entre eux.

5.8.3 Alternance entre bon et mauvais comportement

Le changement de comportement pour un véhicule malicieux est un classique. Un modèle de confiance doit être en mesure de différencier entre un véhicule malicieux qui change à sa guise de comportement et un véhicule dont le comportement est toujours bon. Un exemple de ce cas est illustré dans la figure 5.25.

Ce cas de figure est directement lié à l'asymétrie de l'information dans les VANETs. DTM^2 y remédie en imposant l'utilisation de signal pour l'envoi de messages. Un signal dont le coût est lié aux crédits détenus par un véhicule incite à l'utilisation du signal optimal proposé par DTM^2 car il maximise le bénéfice net d'un véhicule. Cet échange de signal réinstalle de la symétrie dans les informations détenues par les véhicules sans avoir recours à un modèle de réputation où l'échange de réputations est coûteux en termes de messages additionnels générés. Deux véhicules qui n'ont jamais été en contact auparavant, peuvent avec les signaux utilisés par chacun d'eux se faire une idée sur la nature de leur comportement.

Un véhicule malicieux peut décider de bien agir durant une période de temps dans le but d'augmenter son montant de crédit et de pouvoir rester plus longtemps dans un réseau. La difficulté de ce changement de comportement réside en sa fréquence. Dans la figure 5.26,

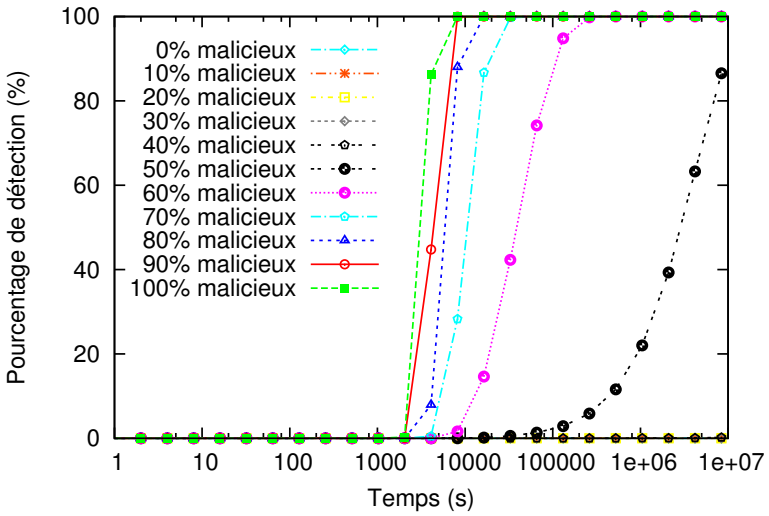


Figure 5.26 – Pourcentage de détection pour différents types de véhicules malicieux.

nous illustrons le pourcentage de détection de véhicules qui changent et alternent leur comportement, entre bon et malicieux, en variant le pourcentage de temps pendant lequel ils sont malicieux. Ces résultats proviennent de notre modélisation en chaîne de Markov. Nous faisons varier la proportion d'agissements en tant que véhicule malicieux entre 0% et 100%. Nous remarquons que tous les véhicules qui sont 50% du temps ou plus malicieux sont détectés et exclus du réseau. Cette détection est plus rapide pour les véhicules dont le comportement est majoritairement malicieux. Ces résultats sont liés aux valeurs choisies pour les paramètres de DTM^2, d'autres choix de paramètres peuvent rendre la détection plus ou moins stricte.

5.9 Conclusion

Tout au long de ce chapitre, nous avons abordé les problématiques liées à la présence de véhicules malicieux et égoïstes au sein d'un réseau VANET. La dissémination de fausses informations de la part des malicieux et le refus de coopérer pour les égoïstes diminuent des performances d'un réseau. Nous avons expliqué les limites des modèles de réputation classiques et celle des modèles incitatifs existants. Nous avons proposé DTM^2, un modèle de confiance distribué et inspiré du modèle du marché de l'emploi. Il résout les problématiques liées à l'asymétrie de l'information en introduisant l'utilisation de signaux pour l'envoi de messages, accompagné d'un système de coûts et de récompenses. Avec ceci, DTM^2 arrive à détecter et à exclure rapidement et efficacement les véhicules malicieux dans un réseau, ainsi qu'à motiver les véhicules égoïstes à coopérer, sans le déploiement d'infrastructures additionnelles. Nous avons modélisé notre solution au travers d'une chaîne de Markov et étudié ses performances de façon analytique et par simulations, en variant les scénarios. Nous avons démontré les performances de DTM^2 en termes de rapidité et pourcentage de détection pour les véhicules malicieux, dans des réseaux comportant 16% puis 25% de malicieux, ainsi que par rapport aux détections erronées et à l'impact des faux messages envoyés auprès des autres véhicules. Finalement nous avons étudié le taux de coopération dans un réseau incluant des véhicules égoïstes avec des pourcentages de 25% et 50%. DTM^2 améliore ce taux de 47% par rapport à un réseau ne disposant pas de modèle incitatif.

Chapitre 6

Conclusions et perspectives

Cette thèse a eu pour but d'apporter des solutions adaptées aux réseaux ad hoc véhiculaires, en proposant une dissémination efficace des données des applications de sûreté et de gestion du trafic routier. Par efficace, nous entendons, une dissémination complète, rapide, collaborative et fiable. Pour ce faire, nous avons structuré notre étude en trois sous problématiques. En premier nous nous sommes intéressés aux stratégies de dissémination de données. Nous avons pris en considération le contenu des messages échangés et nous avons disposé les stratégies de dissémination de ces messages selon leur importance et leur durée de vie. Grâce à cela, nous avons réussi à augmenter le taux de réception des messages de plus de 30% par rapport aux solutions concurrentes. Ainsi, qu'à réduire leur temps d'acheminement, car nous avons diminué le nombre de messages superflus de 90% dans le réseau et réduit les déperditions de ressources du canal. L'étude de performance de notre solution a été réalisée de manière analytique, au travers d'une modélisation en chaîne de Markov, ainsi que par simulation.

Une fois la stratégie de dissémination adaptée au type de message, nous nous sommes intéressés à la couche MAC et au standard IEEE 802.11p/1609.4 [12]. Ce dernier introduit l'utilisation du multi-canal pour dédier une période de temps et un canal à l'envoi des messages de sûreté. Cependant, cela implique la mise en attente de ces mêmes messages durant l'intervalle de temps affecté aux autres applications, ce qui engendre d'importantes collisions à cause de la forte compétition pour l'accès au canal une fois l'intervalle dédié débute à nouveau. Nous remédions à ce problème par l'utilisation d'un ordonnanceur, qui décide du meilleur moment pour envoyer un message, afin de maximiser ses chances de réception. Pour cela, il prend en considération le taux d'occupation du canal, l'efficacité des envois durant ce même intervalle et le temps de retard toléré par l'information. Puis, il utilise la *théorie de l'arrêt optimal*, formulée sous forme de processus de décision Markovien, pour décider du moment d'envoi adéquat. Par nos simulations, nous avons démontré l'amélioration du taux de délivrance par 25%, la réduction des risques de collision par 80% ainsi qu'un meilleur équilibrage de la charge du canal.

Notre troisième contribution vise deux objectifs par la proposition d'un modèle de confiance. Celui-ci garantit la fiabilité des données échangées et assure aussi la coopération dans le réseau. Pour cela, nous nous sommes basés sur les jeux de signaux, qui remédient aux situations d'asymétrie d'information. Une asymétrie d'information cause un déséquilibre dans l'établissement des relations de confiance entre les véhicules, elle est d'ailleurs une des raisons de l'échec des solutions basées sur le calcul de réputations dans les VANETs. Cette asymétrie est due aux caractéristiques des VANETs, notamment le nombre élevé de véhicules dans le réseau et les fréquents changements de topologie. Nous contournons ces contraintes par l'utilisation de crédits dans notre modèle de confiance, car

un montant de crédit est insensible à la mobilité des véhicules et à leurs changements de voisinage, contrairement à des valeurs de réputation. Dans notre modèle, nous exigeons des véhicules un paiement en crédits pour chaque envoi et lecture d'un message reçu, tout en les rémunérant pour chaque message envoyé ou transféré, lequel est préalablement considéré comme fiable. Ce mécanisme décrémente les crédits des véhicules malicieux et finit par les exclure du réseau après l'épuisement de leurs crédits. Il permet aussi d'inciter les véhicules égoïstes à coopérer dans le réseau, pour augmenter leur montant de crédit et ainsi pouvoir payer pour la lecture des messages reçus (c.-à-d, bénéficier du système). L'étude de performance de notre modèle, réalisée au travers d'une modélisation par une chaîne de Markov à espace d'états discret et par simulation, a démontré sa capacité à détecter les véhicules malicieux présents dans un réseau avec un pourcentage qui avoisine les 100%, à réduire leur impact avant même leur exclusion et à inciter les véhicules égoïstes à coopérer de manière continue, jusqu'à faire disparaitre leur effets sur le taux de coopération globale du réseau.

Par ces trois contributions, nous avons pu répondre aux questions initialement posées, pour proposer une solution d'acheminement de données, pour les applications de sûreté et de gestion du trafic routier, adaptée aux VANETs. Nous avons abordé la problématique, en premier, du point de vue quantitatif. Nous avons alors proposé une solution au niveau de couche réseau, puis une autre au niveau la couche MAC. Puis, nous nous sommes intéressés à valider notre hypothèse concernant la coopération des véhicules, en proposant un modèle de confiance incitatif. Celui-ci garantie aussi la fiabilité des données dans le réseau, en excluant tout véhicule malicieux.

Perspectives de la thèse

Cette thèse nous a permis de répondre à quelques questions, sans épuiser le sujet, loin de là et au contraire, elle a ouvert le champ à différentes réflexions.

Dans nos deux premières contributions, nous nous étions intéressés aux aspects quantitatifs des performances de la dissémination dans les VANETs. Ceci s'est matérialisé par la proposition d'une stratégie de dissémination de données au niveau de la couche réseau, ainsi que d'un ordonnanceur de messages au niveau de la couche MAC. Cependant, les performances de ces solutions restent limitées par la bande passante disponible et par la connectivité intermittente du réseau. En effet, lors de situations de saturation du canal ou de connexions très courtes et sporadiques entre les véhicules, le taux de réception des messages, notamment les messages de sûreté, est faible. Pour remédier à cette situation, nous pensons à fiabiliser la communication par la mise en place d'accusés de réception intelligents et légers. Notre accusé de réception aura la forme d'un signal par impulsion envoyé par chaque véhicule lors de la réception d'un message de sûreté. Chacun de ces signaux sera doté d'un code unique faisant référence au message et à l'identifiant ou à la localisation du véhicule, en utilisant par exemple des codes pseudo-aléatoires. Ces codes permettront d'identifier les véhicules ayant reçu ou non un message urgent disséminé, cela même dans les cas de superposition avec les signaux des autres véhicules lors d'un envoi simultané de signaux, après la réception d'un même message par exemple. Cette superposition permettrait même de réduire le temps d'occupation du canal par ces nouveaux types d'accusé de réception. Cela pourra être effectué après quelques études et améliorations au niveau de la couche physique, afin de remédier, par exemple, au défaut de synchronisation entre les véhicules.

Notre deuxième perspective, qui concerne également l'amélioration de la dissémination dans les VANETs, porte sur l'utilisation de techniques d'agrégation pour les messages

disséminés. Cette technique permettra de combiner plusieurs résumés d'informations dans un seul message. Ce moyen pourra être utilisé comme complément à nos solutions de dissémination, dans les cas où le taux de perte est important à cause d'un canal de communication saturé ou lorsque la connectivité du réseau est faible. La dissémination des agrégats pour les informations urgentes augmentera ainsi leurs probabilités de réception auprès des véhicules. Un compris entre le taux de réception et le délai sera alors à trouver.

Notre troisième perspective à ce sujet consiste en l'interconnexion des réseaux VANETs avec les réseaux de télécommunication LTE ou LTE-Advanced, afin de répartir la charge d'un de ces deux types de réseau au besoin vers le second type. Le réseau VANET pourra se servir du réseau LTE-A pour étendre sa couverture réseau et atteindre les véhicules isolés, alors que le réseau LTE-A pourra utiliser le réseau VANET pour diminuer sa charge de trafic et réduire les délais de ces acheminements de messages. Dans ce contexte, on pense que notre solution pour l'accès au canal par l'utilisation de la théorie de l'arrêt optimal peut être adaptée à ce cas de figure, au travers de l'ajout du choix de passer ou non par un second type de réseau. Ceci reviendra alors à choisir lors de l'utilisation de la solution *DMS* entre l'option d'ajournement du message pour l'accès au canal et l'option du réseau à utiliser : VANET ou LTE. Nous pouvons aussi ajouter à cela l'option de la suppression d'un message ou du maintien d'un message plus longtemps dans les files d'attentes pour l'accès au canal et ce malgré l'expiration de sa durée de validité entre deux intervalles CCH successifs.

La troisième contribution de cette thèse a été la proposition d'un modèle de confiance, gérant les comportements malicieux et égoïstes des véhicules. Pour cela, nous avions introduit l'utilisation des jeux de signaux par les VANETs. Cette adaptation a donné des résultats assez prometteurs, ce qui nous laisse penser que son champ d'utilisation peut être élargi à d'autres types de réseau, comme les DTNs. Ces derniers souffrent encore plus de l'asymétrie de l'information entre leurs membres par rapport aux VANETs, même si leurs délais d'acheminement sont beaucoup moins contraignant que dans les VANETs. Dans ce cadre, notre modèle devra être adapté aux caractéristiques des DTNs. En effet, les connexions non continues des DTNs peuvent retarder de beaucoup l'envoi des notifications d'acceptation ou de refus des messages envoyés. Le mécanisme de récompense de notre modèle de confiance devra prendre ceci en considération, afin de ne pas pénaliser un nœud dont les notifications n'ont pas encore été reçues. Une deuxième adaptation de notre modèle peut concerner l'ajout de l'action de stockage des données comme un action de coopération, dans le but de les transmettre lorsque l'occasion se présente, soit avec le mécanisme "store-and-forward". Le modèle devra alors inciter les nœuds à coopérer par la retransmission des données, ainsi que pas leur stockage.

Enfin, dans cette thèse, nous nous sommes essentiellement intéressés à améliorer les performances des applications de sûreté et de gestion du trafic routier des points de vue quantitatifs et qualitatifs. Néanmoins, un troisième point de vue reste à étudier. Celui-ci consiste en la prise en compte de l'expérience utilisateur, à savoir son ressenti, dans la conception et l'évaluation de nos solutions. Cette expérience utilisateur, laquelle concerne sa satisfaction, est liée à la psychologie de l'être humain. Ses valeurs peuvent être utilisées pour rendre plus efficaces et plus fonctionnelles les solutions proposées. Elles permettraient aussi de cibler davantage les besoins des utilisateurs et surtout permettraient de leur donner des priorités. La première question concernant cette expérience utilisateur consiste en comment la calculer. L'observation du comportement des utilisateurs vis-à-vis de nos solutions peut être une des pistes à explorer. La deuxième question consiste en comment prendre ces résultats en considération pour améliorer encore les solutions.

Liste des travaux et articles

Revues internationales

N. Haddadou, A. Rachedi, et Y. Ghamri-Doudane, "A Job Market Signaling Scheme for Incentive and Trust Management in Vehicular Ad Hoc Networks," accepté pour une publication à l'IEEE Transactions on Vehicular Technology, en septembre 2014.

N. Haddadou, A. Rachedi, et Y. Ghamri-Doudane, "Modeling and Performance Evaluation of Advanced Diffusion with Classified Data in Vehicular Sensor Networks," Wireless Communications and Mobile Computing, vol. 11, no. 12, pp. 1689-1701, Oct. 2011.

Soumis à des revues

N. Haddadou, A. Rachedi, et Y. Ghamri-Doudane, "To Send or To Defer ? Improving the IEEE 802.11p/1609.4 Transmission Scheme," soumis en Mars 2014.

Conférences internationales avec actes et comité de lecture

N. Haddadou, et A. Rachedi, "Dtm^2 : Adapting Job Market Signaling for Distributed Trust Management in Vehicular Ad hoc Networks," IEEE International Conference on Communications, ICC'13, Budapest, Hungary, June 2013.

N. Haddadou, A. Rachedi, et Y. Ghamri-Doudane, "Trust and Exclusion in Vehicular Ad hoc Networks : an Economic Incentive Model Based Approach," Computers, Communications and IT Applications Conference, ComComAp'13, Hong Kong, China, April 2013.

N. Haddadou, A. Rachedi et Y. Ghamri-Doudane, "Advanced Diffusion of Classified Data in Vehicular Sensor Networks," International Conference on Wireless Communications and Mobile Computing, IWCMC'11, Istanbul, Turkey, July 2011.

Conférences nationales

N. Haddadou, A. Rachedi, et Y. Ghamri-Doudane, "L'instant propice à l'envoi d'un message sur la couche IEEE 802.11p/1609.4," 10èmes journées francophones Mobilité et Ubiquité, Ubimob'14, Sophia Antipolis, France, Juin 2014.

Posters

N. Haddadou, A. Rachedi, et Y. Ghamri-Doudane, "DTM^2 : Adapting Job Market Signaling for Distributed Trust Management in Vehicular Ad Hoc Networks," Journée thématique « Geocast, Geonetworking, VANET, réseaux en overlay», DGA/INRIA, Paris, France, Novembre 2013.

N. Haddadou, A. Rachedi, et Y. Ghamri-Doudane, "Modèle de confiance pour la dissémination de données dans les réseaux ad hoc véhiculaires (VANETs) : comment éviter les nœuds malicieux et faire coopérer les nœuds égoïstes ? " Les Journées Nationales des Communications dans les Transports, JNCT'13, Nevers, France, Mai 2013.

N. Haddadou, A. Rachedi, et Y. Ghamri-Doudane, "Advanced Diffusion and Security for Vehicular Sensor Networks," École d'été du pôle Rescom, la Palmyre, France, Juin 2011.

Bibliographie

[1] Le site de NS-2. http://www.isi.edu/nsnam/ns/.

[2] Le site du trusted platform module (tpm). https://www.trustedcomputinggroup.org/groups/tpm/.

[3] Openvanet. https://sites.google.com/a/ochin.mygbiz.com/my-scientific-work/my-academic-work/openvanet.

[4] Sumo project. http://sourceforge.net/projects/sumo/.

[5] CEPT. http://www.anfr.fr/fr/l-anfr/organisation/le-cadre-europeen/cept-ecc.html.

[6] Us federal communications commission, amendment of the commission's rules regard- ing dedicated short-range communications services in the 5.850-5.925 ghz (5.9 ghz band).

[7] Standards Committee, Wireless Lan Medium Access Control (MAC) and Physical layer (PHY) specifications : Amendment 8 : Medium Access Control (MAC) Quality of Service Enhancements, Jan 2005.

[8] Wireless lan medium access control (mac) and physical layer (phy) specifications amendment 8 : Medium access control (mac) quality of service enhancements, ieee std. 802.11e, Nov 2005.

[9] ASTM International, Standard Specification for Telecommunications and Information Exchange Between Roadside and Vehicle Systems - 5 GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications, April 2009.

[10] Etsi, intelligent transport systems (its) ; european profile standard for the physical and medium access control layer of intelligent transport systems operating in the 5 ghz frequency band, etsi std, 2010.

[11] IEEE 802.11p, Amendment 6 : Wireless Access in Vehicular Environments, July 2010.

[12] IEEE 1609.4-2010, IEEE Standard for Wireless Access in Vehicular Environments (WAVE)-Multi-channel Operation, February 2011.

[13] Markov decision processes : Lecture notes for stp 425, Nov 2012.

[14] IEEE 802.11-2012, IEEE Standard for Iinformation 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, 2012.

[15] ETSI TR 102 638. Intelligent transport system (its) ; vehicular communications ; basic set of applications ; definition. Technical report, 2009.

[16] S. Al-Sultan, M.M. Al-Doori, and H. Zedan A.H. Al-Bayatti. A comprehensive survey on vehicular ad hoc network. *Journal of Network and Computer Applications*, 37 :380–392, 2014.

[17] M.Z. Ashtiani and Q. Dongyu. Achieving fair cooperation for multi-hop ad hoc networks. In *QBSC*, Queen's University Kingston, Canada, May 2010.

[18] E. Baccelli, P. Jacquet, B. Mans, , and G. Rodolakis. Information propagation speed in bidirectional vehicular delay tolerant networks. In *IEEE INFOCOM*, Shanghai, China, April 2011.

[19] F. Bai and B. Krishnamachari. Exploiting the wisdom of the crowd : localized, distributed information-centric vanets. *IEEE Communications Magazine*, 48(5) :138–146, May 2010.

[20] M. Bakhouya, J. Gabet, and M. Wack. Performance evaluation of dream protocol for inter-vehicle communication. In *Wireless Communication, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology*, Aalburg, Netherlands, May 2009.

[21] N. Benamara, D. Kamal, M. Benamara, D. El Ouadghiria, and J.M. Bonninb. Routing protocols in vehicular delay tolerant networks : A comprehensive survey. *Computer Communications*, 2014.

[22] A. Benslimane. Optimized dissemination of alarm messages in vehicular ad-hoc networks (vanet). *High Speed Networks and Multimedia Communication*, 3079 :655–666, July 2004.

[23] J. Blum, A. Eskandarian, and L. Hoffman. Challenges of intervehicle ad hoc networks. *IEEE Transactions on Intelligent Transportation Systems*, 5(4) :347–351, 2004.

[24] S. Buchegger and J.Y.L. Boudec. Performance analysis of the confidant protocol : Cooperation of nodes - fairness in dynamic ad-hoc networks. In *The Third ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc' 02)*, Lausanne, Switzerland, 2002.

[25] A. Buchenscheit, F. Schaub, F. Kargl, and M. Weber. A vanet-based emergency vehicle warning system. In *Vehicular networking conference (VNC' 09)*, Tokyo, Japan, October 2009.

[26] S. Busanelli, G. Ferrari, and V. A. Giorgio. I2v highway and urban vehicular networks : A comparative analysis of the impact of mobility on broadcast data dissemination. *Journal of Communications*, 6(1) :87–100, 2011.

[27] S. Busanelli, G. Ferrari, and S. Panichpapiboon. Efficient broadcasting in ieee 802.11 networks through irresponsible forwarding. In *IEEE Global Telecommunication Conference (GLOBECOM' 09)*, Honolulu, Hawai, USA, 2009.

[28] L. Buttyán and J.P. Hubaux. Enforcing service availability in mobile ad-hoc wans. In *ACM MobiHoc*, Boston, USA, Aug 2000.

[29] L. Buttyán and J.P. Hubaux. Stimulating cooperation in self-organizing mobile ad hoc networks. *ACM/Springer MONET*, 8 :579–592, 2003.

[30] C. Campolo, A. Molinaro, and A. Vinel. Understanding the performance of short-lived control broadcast packets in 802.11p/wave vehicular networks. In *IEEE Vehicular Networking Conference (VNC'11)*, Amsterdam, Netherlands, November 2011.

[31] C. Campolo, A. Molinaro, A. Vinel, and Y. Zhang. Modeling prioritized broadcasting in multichannel vehicular networks. *IEEE Transactions on Vehicular Technology*, 61(2) :687–701, February 2012.

[32] A. Casteigts, A. Nayak, and I. Stojmenovic. Communication protocols for vehicular ad hoc networks. *Wireless Communications and Mobile Computing, Special Issue : Wireless Mesh and Other Emerging Wireless Network Technologies*, 11(5) :567–582, May 2011.

[33] C. F. Chiasseriniy, E. Fasoloz, R. Furiatoz, R. Gaetax, M. Garettoy, M. Gribaudox, M. Serenox, and A. Zanellaz. mart broadcast of warning messages in vehicular ad hoc networks. In *Workshop Interno Progetto NEWCOM (NOE' 05)*, Turin, Italy, November 2005.

[34] Y.S. Chow, H. Robbins, and D. Siegmund. *Great expectations : the theory of optimal stopping*. Boston [etc.] : Houghton Mifflin, 1971.

[35] F. Domingos Da Cunha, L. Aparecido Vilas, A. Carneiro Viana, and A.A.F. Loureiro. Data Communication in VANETs : A Survey, Challenges and Applications. Technical report, January 2014.

[36] F. Dotzer, L. Fischer, and P. Magiera. Vars : A vehicle ad-hoc network reputation system. In *Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks (WoWMoM' 05)*, Giardini Naxos, Italy, 2005.

[37] S. Eichler. Performance evaluation of the ieee 802.11p wave communication standard. In *IEEE 66th Vehicular Technology Conference (VTC Fall'07)*, Baltimore, MD, USA, November 2012.

[38] M. Di Felice, L. Bedogni, and L. Bononi. Dysco : a dynamic spectrum and contention controlframework for enhanced broadcast communication invehicular networks. In *the 10th ACM international symposium on Mobility management and wireless access (MobiWac'12)*, New York, NY, USA, 2012.

[39] M. Di Felice, A.J. Ghandour, H. Artail, and L. Bononi. On the impact of multi-channel technology on safety-message delivery in ieee 802.11p/1609.4 vehicular networks. In *21st International Conference on Computer Communications and Networks (ICCCN'12)*, Munich, Germany, August 2012.

[40] M. Fiore, J. Härri, F. Fethi, and C. Bonnet. Vehicular mobility simulation for vanets. In *IEEE ANSS*, Norfolk, USA, March 2007.

[41] T. Fukuhara, T. Warabino, T. Ohseki, K. Saito, K. Sugiyama, T. Nishida, and K. Eguchi. Broadcast methods for inter-vehicle communications system. *Proceedings of IEEE Wireless Communications and Networking Conference*, 4 :2252–2257, 2005.

[42] M. Gerharz, C. de Waal, and M. Frank. A practical view on qualityof-service support in wireless ad hoc networks. In *The 3rd IEEE Workshop on Applications and Services in Wireless Networks (ASWN' 03)*, 2003.

[43] M. Gerlach and F. Fokus. Trust for vehicular applications. In *IEEE Eighth International Symposium on Autonomous Decentralized Systems (ISADS'07)*, Sedona, AZ, USA, 2007.

[44] A.J. Ghandour, M. Di Felice, L. Bononi, and H. Artail. Modeling and simulation of wave 1609.4-based multi-channel vehicular ad hoc networks. In *Proceedings of the 5th International ICST Conference on Simulation Tools and Techniques (SIMUTOOLS'12)*, Desenzano, Italy, 2012.

[45] K. Govindan and P. Mohapatra. Trust computations and trust dynamics in mobile ad hoc networks : A survey. *IEEE Communications Surveys and Tutorials*, 14(2) :279–298, 2012.

[46] G. Guette and C. Brce. Using tpms to secure vehicular ad-hoc networks (vanets). In *WISTP*, Sevilla, Spain, May 2008.

[47] G. Guette and O. Heen. A tpm-based architecture for improved security and anonymity in vehicular ad hoc networks. In *VNC*, Tokyo, Japan, October 2009.

[48] N. Haddadou and A. Rachedi. Dtm^2 : Adapting job market signaling for distributed trust management in vehicular ad hoc networks. In *IEEE ICC*, Budapest, Hungary, June 2013.

[49] N. Haddadou, A. Rachedi, and Y. Ghamri-Doudane. Advanced diffusion of classified data in vehicular sensor networks. In *Wireless Communications and Mobile Computing Conference (IWCMC'11)*, Istanbul, Turkey, July 2011.

[50] N. Haddadou, A. Rachedi, and Y. Ghamri-Doudane. Modeling and performance evaluation of advanced diffusion with classified data in vehicular sensor networks. *Wireless Communications and Mobile Computing*, 11(12) :1689–1701, October 2011.

[51] N. Haddadou, A. Rachedi, and Y. Ghamri-Doudane. A job market signaling scheme for incentive and trust management in vehicular ad hoc networks. *Accepted with minor revisions in IEEE Transactions on Vehicular Technology*, 2014.

[52] N. Haddadou, A. Rachedi, and Y. Ghamri-Doudane. To send or to defer ? improving the ieee 802.11p/1609.4 transmission scheme. *Submitted to IEEE Transactions on Parallel and Distributed Systems*, 2014.

[53] M.I. Hassan, H.L. Vu, and T.Sakurai. Performance analysis of the ieee 802.11 mac protocol for dsrc safety applications. *IEEE Transactions on Vehicular Technology*, 60(8) :3882–3896, 2011.

[54] J. K. Hedrick, M. Tomizuka, and P. Varaiya. Control issues in automated highway systems. *IEEE Control Systems Magazine*, 14(6) :21–32, 1994.

[55] Y. Hongseok and K. Dongkyun. Dynamic channel coordination schemes for ieee 802.11p/1609 vehicular networks : A survey. *International Journal of Distributed Sensor Networks*, 2013(827317), 2013.

[56] J. Jakubiak and Y. Koucheryavy. State of the art and research challenges for vanets. In *Consumer communications and networking conference (CCNC' 08)*, Las Vegas, Nevada, USA, 2008.

[57] ITS JPO. Vehicle safety applications. us dot intellidrive(sm) project - its joint program office. Technical report, 2008.

[58] G. Korkmaz, E. Ekici, F. Ozguner, and U. Ozguner. Urban multi-hop broadcast protocol for inter-vehicle communication systems. In *ACM International Workshop on Vehicular Ad Hoc Networks*, New York, NY, USA, 2004.

[59] T. Kosch, I. Kulp, M. Bechler, M. Strassberger, B. Weyl, and R. Lasowski. Communication architecture for cooperative systems in europe. *IEEE Communications Magazine*, 47(5) :116–125, May 2009.

[60] R. Kumar and M. Dave. A review of various vanet data dissemination protocols. *International Journal of U- and E-Service, Science and Technology*, 5(3) :27–44, 2012.

[61] N. Kuntze and A.U. Schmidt. Trusted ticket systems and applications. *Trusted Computing - Challenges and Applications. Lecture Notes in Computer Science*, 232 :49–60, 2007.

[62] J. Lebrun, J. Anda, C.N. Chuah, M. Zhang, and D. Ghosal. Vgrid : Vehicular ad hoc networking and computing grid for intelligent traffic control. In *IEEE Vehicular Technology Conferenc (VTC' 05)*, Dallas, TX, USA, 2005.

[63] U. Lee and M. Gerla. A survey of urban vehicular sensing platforms. *Elsevier Computer Networks Journal*, 54(4) :527–544, March 2010.

[64] U. Lee, E. Magistretti, M. Gerla, P. Bellavista, and A. Corradi. Dissemination and harvesting of urban data using vehicular sensing platforms. *IEEE Transactions on Vehicular Technology*, 58(2) :882–901, 2009.

[65] U. Lee, E. Magistretti, B. Zhou, M. Gerla, P. Bellavista, and A. Corradi. Efficient data harvesting in mobile sensor platforms. In *IEEE International Conference on Pervasive Computing and Communications (PERCOM'06)*, Pisa, Italy, March 2006.

[66] U. Lee, E. Magistretti, B. Zhou, M. Gerla, P. Bellavista, and A. Corradi. Mobeyes : smart mobs for urban monitoring with a vehicular sensor network. *IEEE Wireless Communications*, 13(5) :52–57, November 2006.

[67] F. Li and J. Wu. Frame : an innovative incentive scheme in vehicular networks. In *IEEE ICC*, Dresden, Germany, June 2009.

[68] P. Liu, Z. Tao, S. Narayanan, T. Korakis, and S.S. Panwar. Coopmac : A cooperative mac for wireless lans. *IEEE Journal on Selected Areas in Communications*, 25(2) :340–354, Feb 2007.

[69] T. K. Mak, K. P. Laberteaux, and R. Sengupta. Implementation of ecc-based trusted platform module. In *Machine Learning and Cybernetics, 2007 International Conference on*, Hong Kong, 2007.

[70] G.F. Marias, P. Georgiadis, D. Flitzanis, and K. Mandalas. Cooperation enforcement schemes for manets : A survey. *Wireless Communications and Mobile Computing*, 6(3) :319–332, May 2006.

[71] U. F. Minhas, J. Zhang, T. Tran, and R. Cohen. Towards expended trust management for agents in vehicular ad-hoc networks. *International Journal of Computational Intelligence : Theory and Practice(IJCITP)*, 5(1) :03–15, June 2010.

[72] Organisation mondiale de la Santé. Vehicle safety communications project task 3 final report, identify intelligent vehicle safety applications enabled by dsrc, 2004.

[73] M. Torrent Moreno, D. Jiang, and H. Hartenstein. Broadcast reception rates and effects of priority access in 802.11based vehicular ad hoc networks. In *ACM International Workshop on Vehicular Ad hoc Networks (VANET' 04)*, Philadelphia, USA, October 2004.

[74] M.Slavik and I. Mahgoub. Stochastic broadcast for vanet. In *IEEE Consumer Communication and Networking Conference (CCNC' 10)*, Las Vegas, Nevada, USA, 2010.

[75] N.H.T.S.A. Rapport mondial sur la prévention des traumatismes dus aux accidents de la circulation, March 2005.

[76] S. Ni, Y. Tseng, Y. Chen, and J. Sheu. The broadcast storm problem in a mobile ad hoc network. In *Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking (MobiCom' 99)*, New York, USA, 1999.

[77] S. Olariu and M.C. Weigle. *Vehicular networks : from theory to practice*. Chapman and Hall/CRC, 2009.

[78] C. Palazzi, F. Pezzoni, and P. Ruiz. Delay-bounded data gathering in urban vehicular sensor networks. *Elsevier Journal of Pervasive and Mobile Computing, Special Issue on Vehicular Sensor Networks and Mobile Sensing over Wide-Scale Deployment Environments*, 8(2) :180–193, 2011.

[79] A. Palma, P.P. Pereira, and A. Casaca. Multicast routing protocol for vehicular delay-tolerant networks. In *IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob' 12)*, Barcelona, Spain, October 2012.

[80] J. Peng and L. Cheng. A distributed mac scheme for emergency message dissemination in vehicular ad hoc networks. *IEEE Transactions on Vehicular Technology*, 56(6) :3300–3308, Nov 2007.

[81] J. Petit. *Surcoût de l'authentification et du consensus dans la sécurité des réseaux sans fil véhiculaires*. PhD thesis, l'Université Toulouse III Paul Sabatier, 2011.

[82] M. L. Puterman. Chapter 8 markov decision processes. *Handbooks in Operations Research and Management Science*, 2 :331 – 434, 1990.

[83] M. L. Puterman. *Markov Decision Processes : Discrete Stochastic Dynamic Programming*. John Wiley & Sons, 2009.

[84] A. Rachedi and A. Benslimane. Toward a cross-layer monitoring process for mobile ad hoc networks. *Security and Communication Networks, John Wiley InterScience*, 2(4) :351–368, 2009.

[85] A. Rachedi, A. Benslimane, H. Otrok, N. Mohammed, and M. Debbabi. A secure mechanism design-based and game theoretical model for manets. *Mobile Networks and Applications*, 15(2) :191–207, 2010.

[86] A. Rahim, M. Yasin, I. Ahmad, Z.S. Khan, and M. Sher. Relevance based approach with virtual queue for vehicular adhoc networks. In *International Conference on Computer, Control and Communication (IC4' 09)*, Karachi, Pakistan, 2009.

[87] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux. Eviction of misbehaving and faulty nodes in vehicular networks. *IEEE Journal on Selected Areas in Communications*, 25(8) :1557 – 1568, October 2007.

[88] M. Raya, P. Papadimitratos, V.D. Gligory, and J.P. Hubaux. On data-centric trust establishment in ephemeral ad hoc networks. In *IEEE Conference on Computer Communications (INFOCOM' 08)*, Phoenix, AZ, USA, 2008.

[89] I. S. Reed and G. Solomon. Polynomial codes over certainfinite fields. *Journal of the Society for Industrial and AppliedMathematics*, 8(2) :300–304, 1960.

[90] F. Ros, M. Ruiz, and I. Stojmenovic. Reliable and efficient broadcasting in vehicular ad hoc networks. In *IEEE Vehicular Technology Conference (VTC' 2009 Spring)*, Barcelona, Spain, April 2009.

[91] S. Sharafkandi, G. Bansal, J.B. Kenney, and D.H.C. Du. Using edca to improve vehicle safety messaging. In *IEEE Vehicular Networking Conference (VNC'12)*, Seoul, Republic of Korea, October 2007.

[92] M. L. Sichitiu and M. Kihl. Inter-vehicle communication systems : A survey. *IEEE Communications Surveys and Tutorials*, 10(2) :88–105, 2008.

[93] J. Sobel. Signaling games. *Computational Complexity Theory, Techniques, and Applications*, pages 2830–2844, 2012.

[94] M. Spence. Job market signaling. *The Quarterly Journal of Economics*, 87(3) :355–374, 1973.

[95] M. Spence. Job market signaling. *The Quarterly Journal of Economics, MIT Press*, 87(3) :355–374, 1973.

[96] M. Spence. *Market Signaling : Informational Transfer in Hiring and Related Screening Processes*. Harvard economic studies, 1974.

[97] M. Spence. Signaling in retrospect and the informational structure of markets. *The American Economic Review*, 92(3) :434–459, 2002.

[98] M. Sun, W. Feng, T.H. Lai, K. Yamada, H. Okada, and K. Fujimura. Gps-based message broadcasting for inter-vehicle communication. In *International Conference on Parallel Processing (ICPP' 00)*, Toronto, Canada, 2000.

[99] Y. Toor, P. Muhlethaler, and A. Laouiti. Vehicle ad hoc networks : applications and related technical issues. *IEEE Communications Surveys Tutorials*, 10(3) :74–88, 2008.

[100] M. Torrent-Moreno, D. Jiang, and H. Hartenstein. Broadcast reception rates and effects of priority access in 802.11-based vehicular ad-hoc networks. In *The first ACM Workshop on Vehicular Ad Hoc Networks (VANET' 04)*, Philadelphia, Pennsylvania, USA, October 2004.

[101] F.K. Tseng, Y.H. Liu, J.S. Hwu, and R.J. Chen. A secure reed-solomon code incentive scheme for commercial ad dissemination over vanets. *IEEE Transactions on Vehicular Technology*, 60(9) :4673–4731, November 2011.

[102] R. UzcÃ¡tegui and G. Acosta-Marum. Wave : A tutorial. *IEEE Communications Magazine*, 47(5) :126–133, May 2009.

[103] VSC-A. Us dot, vehicle safety communications applications (vsc-a) project dot hs 810 073. Technical report, 2009.

[104] Q. Wang, S. Leng, H. Fu, and Y. Zhang. An ieee 802.11p-based multichannel mac scheme with channel coordination for vehicular ad hoc networks. *IEEE Transactions on Intelligent Transportation Systems*, 13(2) :449 – 458, 2012.

[105] Z. Wang and M. Hassan. The throughput-reliability tradeoff in 802.11-based vehicular safety communications. In *6th IEEE Consumer Communications and Networking Conference (CCNC'09)*, Las Vegas, NV , USA, January 2009.

[106] J. Wanga, Y. Liu, and Y. Jiao. Building a trusted route in a mobile ad hoc network considering communication reliability and path length. *Journal of Network and Computer Applications*, 34(4) :1138–1149, 2011.

[107] J. Whitbeck, V. Conan, and M. Dias de Amorim. Performance of opportunistic epidemic routing on edge-markovian dynamic graphs. *IEEE Transactions on Communications*, 59(5) :1259–1263, May 2011.

[108] L. Wischhof, A. Ebner, and H. Rohling. Information dissemination in self-organizing intervehicle networks. *IEEE Transactions on Intelligent Transportation Systems*, 6(1) :90–101, 2005.

[109] N. Wisitpongphan, O.K. Tonguz, J.S. Parikh, P. Mudalige, F. Bai, and V. Sadekar. Broadcast storm mitigation techniques in vehicular ad hoc networks. *IEEE Wireless Communications*, 14(6) :84–94, 2007.

[110] S. Yousefi, M.S. Mousavi, and M. Fathy. Vehicular ad hoc networks (vanets) : challenges and perspectives. In *Proceedings of the 6th International Conference on ITS telecommunications*, Chengdu, China, 2006.

[111] J. Zhang. A survey on trust management for vanets. In *IEEE International Conference on Advanced Information Networking and Applications (AINA' 12)*, Biopolis, Singapore, 2011.

[112] X. Zhang, M. Zhou, J. Zhuang, and J. Li. A multi-channel vanet providing concurrent safety and commercial services. In *Proceedings of the 2Nd ACM International Workshop on Vehicular Ad Hoc Networks*, VANET '05, New York, NY, USA, 2005.

[113] Z. Zhang, G. Mao, and B. D. O. Anderson. On the information propagation process in multi-lane vehicular ad-hoc networks. In *IEEE ICC*, Ottawa, Canada, June 2012.

[114] S. Zhong, J. Chen, and Y.R. Yang. Sprite : A simple, cheat-proof, credit-based system for mobile ad-hoc networks. In *IEEE INFOCOM*, San Francisco, USA, April 2003.