THESE

En vue de l'obtention du

DOCTORAT DE L'UNIVERSITÉ DE TOULOUSE

Délivré par l'*Université Toulouse III - Paul Sabatier*
Discipline ou spécialité : *Informatique*

Présentée et soutenue par *Jonathan Petit*
Le *13 Juillet 2011*

Titre : *Surcoût de l'authentification et du consensus dans la sécurité des réseaux sans fil véhiculaires*

JURY

Président du jury	Guy Juanole	Professeur émérite, Université Paul Sabatier, Toulouse
Rapporteur	Francine Krief	Professeur, ENSEIRB, Bordeaux
Rapporteur	Maryline Laurent	Professeur, Télécom SudParis, Evry
Examinateur	Pascal Lorenz	Professeur, Université de Haute Alsace, Colmar
Examinateur	Zoubir Mammeri	Professeur, Université Paul Sabatier, Toulouse
Examinateur	Patrick Sénac	Professeur, ISAE, Toulouse

Ecole doctorale : *Mathématiques, Informatique Télécommunications de Toulouse*
Unité de recherche : *Institut de Recherche en Informatique de Toulouse – UMR5505*
Directeur(s) de Thèse : *Zoubir Mammeri*

À mon épouse,

Remerciements

Faire un doctorat c'est apprendre à devenir chercheur. Mais avant d'être une recherche scientifique, c'est avant tout une recherche de soi. On se découvre des forces et des faiblesses. C'est un chemin long et semé d'embuches qui ne peut se réaliser sans un soutien important.

C'est pourquoi je voudrais remercier mon directeur de thèse Zoubir Mammeri pour son encadrement, les réunions de travail et les discussions tant scientifiques que personnelles que nous avons pu avoir. Sans lui, je n'aurai pas choisi la voie du doctorat, je lui adresse donc un grand merci.

Les collègues sont le deuxième pilier : Cédric Téyssié, David Espès, Mahboub Bali, Galem Boudour, Rahim Kacimi, Mehdi Zaier. Merci Cédric pour m'avoir appris à être un enseignant, ainsi que pour les discussions et les bons moments. Merci David pour ton soutien, ton rire et ton ouverture d'esprit. Merci Mahboub pour les nombreuses discussions sur tout, merci de m'avoir montrer la Voie. Merci Mehdi pour m'avoir imprimer la thèse lorsque j'étais en Finlande. Merci Rahim pour tes conseils postdoctoraux notamment. Merci Ghalem pour ta bonne humeur.

Les amis sont le troisième pilier. Tout d'abord les amis de la fac : Greg (merci pour les parties endiablées), AProDoc (spéciale dédicasse aux 2S), DocToMe. Puis les amis « extérieurs » : Jean-Léon Bouraoui, Briac et Luc ; Julien, Arnaud, JD (du Jeet Kune Do) ; Alexey et Sergey (de Tampere University of Technology) ; Gwen et Maloh.

Le quatrième pilier est ma famille : même si une thèse n'est pas une chose facile à comprendre pour « le commun des mortels », je sais qu'ils m'ont soutenu dans cette quête.

Pour finir (on garde le meilleur pour la fin), le cinquième pilier de ma thèse : mon épouse. Quel courage faut-il avoir pour pouvoir supporter les humeurs d'un doctorant : stress, angoisse, découragement, tout y passe. Elle a su faire preuve d'empathie, de comprehension, de patience et d'amour. Elle a su trouver les mots qu'il faut pour m'aider. Cette thèse lui est dédicassée.

Merci à tous ! Vous avez aidé à construire l'homme que je suis aujourd'hui.

Résumé

Les réseaux ad hoc sans fil véhiculaires (VANET) permettent les communications entre véhicules afin d'augmenter la sécurité routière et d'agrémenter l'expérience de conduite. Une catégorie d'applications ayant suscité un fort intérêt est celle liée à la sécurité du trafic routier. Un exemple prometteur est l'alerte de danger local qui permet d'accroitre la « ligne de vue » du conducteur en lui proposant un ensemble d'alertes afin d'anticiper des situations potentiellement dangereuses. En raison de leurs contraintes temporelles fortes et les conséquences critiques d'une mauvaise utilisation, il est primordial d'assurer des communications sécurisées. Mais l'ajout de services de sécurité entraîne un surcoût de calcul et réseau. C'est pourquoi l'objectif de notre travail est d'établir un cadre général (de manière analytique) du surcoût de la sécurité sur le délai de transfert d'une alerte.

Parmi les mécanismes de sécurité conventionnels, le service d'authentification apparaît comme la pierre angulaire de la sécurité des VANETs. De plus, l'authentification est utilisée pour chaque message émis ou reçu. Il est donc potentiellement le service le plus consommateur. C'est pourquoi, nous nous focalisons sur ce service. Nous nous posons ainsi les questions suivantes : quel est le coût de l'authentification ? Quel est son impact sur l'application d'alerte de danger local ? La première contribution de cette thèse est l'élaboration d'une formule permettant le calcul du surcoût de la signature numérique.

Mais l'authentification ne sera pas le seul mécanisme de sécurité déployé. Le consensus est notamment un des mécanismes fréquemment employés afin d'instaurer une confiance entre les véhicules. En effet, grâce à une méthode de décision et à partir d'un ensemble de messages, le consensus vise à obtenir un commun accord sur une valeur ou une action entre les véhicules. Ainsi, nous devons comprendre comment définir les paramètres de consensus afin de réduire l'impact de ce mécanisme sur le délai et la distance de freinage ? Comment s'intègre le consensus dans la formule globale de surcoût de l'authentification ? C'est notamment à ces questions que cette thèse répond. Notre deuxième contribution est une méthode de décision dynamique qui analyse l'environnement réseau courant (nombre de voisins à portée de communication), et explore le contenu des alertes. Il en résulte une réduction du nombre de paquets à examiner et donc une réaction plus rapide et plus adaptée à l'alerte.

Mot clés : Authentification, Consensus, Sécurité, Réseaux sans fil véhiculaires, Surcoût, DSRC.

Abstract

Vehicular Ad Hoc Networks (VANET) provide vehicle-to-vehicle communications to increase the road safety. The safety-related applications have gained a lot of attention. A promising example is the Local Danger Warning application that increase the line-of-sight of the driver by providing warnings about potential dangerous situations ahead. Because of their real-time constraints and life-threatening consequences of misbehavior, communications have to be secured. But, security mechanisms come with processing and network overheads. The main goal of this PhD thesis is to propose a general (and analytical) framework on the impact of the security overhead on the transfer delay of a warning.

Among the conventional security mechanisms, the authentication mechanism appears as the cornerstone of VANET security. Moreover, the authentication is used for every message sent or received. So it may be the most consuming mechanism. This is the reason why we first focus on the authentication overhead and propose a global formula to assess it.

But the authentication won't be the only security mechanism to be deployed in VANET. The consensus is often used to provide trust between vehicles. Indeed, with a decision method and from a set of messages, the consensus aims at a common agreement on a value or an action between vehicles. We analyze how to define the consensus parameters in order to respect the real-time constraints. The second contribution of this thesis is a dynamic decision method that uses the network environment and the content of the warning to decrease the number of messages to verify and so provide an adapted reaction.

Keywords: Authentication, Consensus, Security, Vehicular networks, Overhead, DSRC.

Table des Matières

Table des Figures

Liste des Tables

Introduction

Depuis de nombreuses années, les gouvernements, constructeurs automobiles et consortium d'industriels, ont fixé la réduction des accidents de la route comme une priorité majeure. Afin de réussir ce challenge, une idée novatrice a été de rendre les véhicules et les routes plus intelligents par le biais des communications sans fil. En effet, les véhicules actuels génèrent et analysent déjà une quantité de données importante, mais ne diffusent rien. Avec des communications sans fil, l'environnement du véhicule et le « champ de vision » du conducteur sont accrus. Ainsi, grâce à des véhicules à l'écoute de leur environnement, plus de 75 applications potentielles ont été identifiées, dont 34 à vocation de sécurité (les 41 restantes étant pour l'optimisation du trafic routier et le confort des usagers).

Avec l'avènement des technologies sans fil telles que la 3G, le Wifi, ou le Bluetooth, les communications sans fil sont devenues omniprésentes et peu onéreuses. C'est pourquoi, afin de déployer ces applications, un type de réseau a émergé : le réseau sans fil véhiculaire. Une des principales composantes d'un tel réseau est la communication inter-véhicules. En effet, elle permet d'assurer une disponibilité des services en cas d'infrastructure inexistante. Le réseau est alors appelé réseau sans fil ad hoc véhiculaire (VANET, *Vehicular Ad hoc NETwork)*.

La conception et la mise en œuvre des protocoles et des applications dans les réseaux sans fil véhiculaires imposent que soient relevés de nombreux défis traditionnellement connus des communications sans fil (mobilité, connectivité, sécurité, etc.). De plus, les applications exigent dans la plupart des cas une fiabilité des communications, une qualité de service minimale et parfois même des communications temps réel. Or, cela vient en opposition avec la nature fortement dynamique des réseaux véhiculaires (changement de topologie, distance variable entre véhicules, perte fréquente de connectivité, non-fiabilité des communications, délai, etc.).

Dans les applications de sécurité du trafic routier, telles que l'alerte de danger local (LDW, *Local Danger Warning*), les véhicules émettent des messages d'alerte pour informer les autres usagers de situations potentiellement dangereuses (conditions de route dégradées, freinage d'urgence d'un autre

véhicule, obstacle, etc.). Si ces alertes sont envoyées à tort, ou à outrance, alors l'utilisateur n'y prêtera plus d'attention. L'alerte elle-même peut devenir une menace, et provoquer des accidents à cause des réactions inappropriées des utilisateurs. Ainsi, un attaquant pouvant injecter des messages falsifiés dans le VANET pourra causer la « désensibilisation » de l'utilisateur ou des accidents, contrairement à l'objectif d'amélioration du trafic routier. Afin de décourager les attaquants, et de se prémunir de telles situations, il est nécessaire de déployer des services de sécurité tels que l'authentification, l'intégrité ou la non-répudiation par exemple.

Au-delà des problèmes de sécurité, les VANETs soulèvent aussi des contraintes temporelles. Par exemple, avec un environnement fortement dynamique, caractérisé par une topologie très changeante, et des connexions de courte durée, le déploiement d'une solution de sécurité doit faire face à des contraintes de temps et des configurations spécifiques. L'objectif de cette thèse est de modéliser et d'évaluer l'impact des mécanismes de sécurité sur la prédictibilité des systèmes embarqués temps réel que sont les équipements de communication sans fil véhiculaire.

En effet, les mécanismes de sécurité doivent être choisis avec précaution afin de garantir un coût minimal en matière de temps de calcul et de communication. De plus, les applications peuvent avoir des exigences temporelles. Les mécanismes de sécurité doivent alors respecter les contraintes applicatives.

Dans le contexte critique d'applications telles que l'alerte de danger local, le temps de calcul et de transfert de l'alerte a un impact sur la réaction du conducteur. Si l'on considère que le conducteur doit freiner, l'ajout de mécanismes de sécurité peut alors avoir un impact sur la distance de freinage. En effet, sans mécanisme de sécurité, le véhicule ayant une vitesse de 130 km/h s'arrêtera en 96 mètres. Grâce à l'application LDW, le conducteur pourra anticiper un danger et ainsi réagir plus tôt que s'il n'avait pas eu d'équipement DSRC. Mais en ajoutant un temps de traitement (à l'émission et à la réception), ce gain (en terme de temps et donc de distance entre le véhicule et l'obstacle) peut être réduit. En effet, l'ajout de mécanismes de sécurité impose un surcoût :

- Temporel : Temps de calcul (signature numérique, certificat, vérification de certificat, hachage, etc.).

- Charge du réseau : Les mécanismes de sécurité entraînent des échanges de messages supplémentaires (de vérification de certificat, de récupération de listes de révocation (CRL), d'envoi de la clé privée, etc.). Les messages signés ou chiffrés ont aussi une taille supérieure à celle des messages non sécurisés.

- Financier : Les équipements dédiés à la sécurité ajoutent un coût financier à la production de chaque unité DSRC. De plus, la gestion de systèmes de sécurité peut être chère (mise en place de serveurs de stockage de CRL, etc.).

L'objectif de notre travail est d'établir, de manière analytique, un cadre général du surcoût de la sécurité sur le délai de transfert d'une alerte.

Parmi les mécanismes de sécurité conventionnels, le service d'authentification apparaît comme la pierre angulaire de la sécurité des VANETs. De plus, l'authentification est utilisée pour chaque message émis ou reçu. Il est donc potentiellement le service le plus consommateur. C'est pourquoi, nous nous focalisons sur ce service. Nous nous posons ainsi les questions suivantes : quel est le coût de l'authentification ? Quel est son impact sur l'application d'alerte de danger local ?

Mais l'authentification ne sera pas le seul mécanisme de sécurité déployé. En effet, le problème de confiance est récurrent dans les réseaux de type « ad hoc », et les VANETs n'échappent pas à ce problème. Ainsi, lorsque l'on se place dans le cadre d'applications de sécurité du trafic routier qui ont un impact direct sur la sécurité routière et la vie des usagers, ce besoin de confiance est exacerbé. Le consensus est un des mécanismes fréquemment employés afin d'instaurer une confiance entre les véhicules. En effet, grâce à une méthode de décision et à partir d'un ensemble de messages, le consensus vise à obtenir un commun accord sur une valeur ou une action entre les véhicules. Ainsi, nous devons comprendre comment définir les paramètres de consensus afin de réduire l'impact de ce mécanisme sur le délai et la distance de freinage ? Comment s'intègre le consensus dans la formule globale de surcoût de l'authentification ? C'est notamment à ces questions que cette thèse répondra.

Notre première contribution consiste à analyser l'impact du protocole d'authentification *Elliptic Curve Digital Signature Algorithm* (ECDSA) sur les performances des VANETs. En effet, l'utilisation d'ECDSA entraine l'augmentation du temps de traitement au niveau de chaque véhicule et une taille de paquet transporté sur le réseau plus importante. D'après la criticité des applications de sécurité du trafic routier, il est primordial que les conséquences d'un ajout de mécanisme de sécurité tel que l'authentification ne viennent pas en opposition avec l'objectif des VANETs. Nous nous intéressons principalement au délai de transfert d'un message. Étant donnée la propriété forte de mobilité du contexte véhiculaire, le temps correspond à une distance parcourue. Ainsi, nous analysons aussi l'impact de l'authentification sur la distance de freinage. Le résultat de cette contribution est l'élaboration d'une formule permettant le calcul du surcoût de la signature numérique. Ce modèle analytique est validé par le biais d'expérimentation et de simulation.

La deuxième contribution de cette thèse se focalise sur l'optimisation du mécanisme de consensus. Nous proposons une méthode de décision dynamique qui est une extension du modèle « *Majority of Freshest X with Threshold* » d'Ostermaier *et al*. [OST 07]. La particularité de notre méthode de décision par rapport aux solutions existantes est qu'elle est adaptative. En effet, notre méthode de décision analyse l'environnement réseau courant (nombre de voisins à portée de communication), explore le contenu des alertes. Grâce à l'ajout de modules de filtrage et de marquage, il en résulte une réduction du nombre de paquets à examiner et donc une réaction plus rapide et plus adaptée à l'alerte. Nous proposons une modélisation des méthodes de décision et explicitons la méthodologie pour définir les paramètres du consensus. Pour conclure, nous intégrons le consensus dans la formule globale du surcoût de la sécurité.

Cette thèse est organisée en quatre chapitres. Nous présentons dans le premier chapitre les réseaux sans fil véhiculaires. Plus précisément, nous détaillons les applications potentielles, les entités communicantes, les architectures de communication possibles et les caractéristiques d'un réseau sans

fil véhiculaire. Nous introduisons aussi le standard IEEE 1609 qui régit les communications sans fil véhiculaires.

Dans le chapitre 2, nous nous focalisons sur la sécurité des réseaux sans fil véhiculaires. À partir de la définition des attaquants et des attaques possibles, nous présentons les services de sécurité et les mécanismes associés pour les contrer. Nous analysons plus particulièrement la sécurité de l'application d'alerte de danger local. Nous détaillons les procédures d'authentification et de chiffrement définies par le standard IEEE 1609.2.

Le chapitre 3 présente notre première contribution qui est l'analyse de l'impact des mécanismes d'authentification sur les performances des réseaux sans fil ad hoc véhiculaires. Nous présentons le protocole d'authentification ECDSA, et analysons sa complexité. Ensuite, par le biais d'expérimentations et de simulations, nous analysons l'impact de l'authentification sur le temps de calcul, le délai de transfert et la distance de freinage.

Le chapitre 4 présente le problème de consensus dans les VANETs. Après avoir détaillé le fonctionnement et l'utilité d'un mécanisme de consensus, nous analysons les méthodes de décision. Nous proposons une méthode de décision dynamique afin d'assurer des propriétés de flexibilité, d'adaptation au contexte et donc de réduction de coût. Nous proposons aussi une modélisation de méthode de décision afin d'en déduire le délai de calcul et de communication.

Nous conclurons cette thèse en présentant les conclusions et quelques perspectives.

1 Réseaux véhiculaires : Architectures, Protocoles et Applications

En 2007, les accidents de la route ont causé la mort de 110 personnes par jour et fait plus de 4600 blessés, pour un coût de plus de 438 millions d'euros quotidiennement dans l'Union Européenne [CAR 07]. Le constat est similaire aux États-Unis où il y a eu 102 morts, 7900 blessés, pour un coût de plus de 630 millions de dollars par jour [NHT 08]. Ainsi, à cause du grand nombre de morts et de l'impact économique, de nombreux gouvernements, constructeurs automobiles et consortium d'industriels, ont fixé la réduction des accidents de la route comme une priorité majeure [BLI 02]. Afin de réussir ce challenge, l'idée première a été de rendre les véhicules et les routes plus intelligents par le biais des communications sans fil. Grâce à des véhicules à l'écoute de leur environnement, plus de 75 applications potentielles ont été identifiées [VSC 05]. Une application du concept d'intelligence ambiante consiste à munir véhicules et routes de capacités permettant de rendre la conduite plus sûre (informations trafic, accidents, dangers, déviations possibles, informations météorologiques, etc.) et de rendre le temps passé sur les routes plus convivial (accès Internet, jeux en réseau, suivi de véhicules, groupe de discussion dans un embouteillage, etc.). Ces applications sont des exemples types de ce qu'on appelle les systèmes de transport intelligents (ITS, *Intelligent Transportation System*). Le but des ITS est l'amélioration de la sécurité, l'efficacité et la convivialité dans les transports routiers au travers de l'utilisation des nouvelles technologies d'information et de communication (NTIC). En effet, les ordinateurs, l'électronique embarquée, les satellites, jouent un rôle de plus en plus important dans les systèmes de transport (ferroviaire, routier, aérien, fluvial). Les applications et les services ITS sont basés sur la collecte, le traitement et l'échange d'une grande variété de données, tant de sources

publiques et privées, y compris des informations sur le trafic et les accidents, mais également des données à caractère personnel, telles que les habitudes de conduite et les modes de déplacement des usagers.

Ce chapitre a pour objectif d'appréhender la notion de réseau sans fil véhiculaire et de définir le contexte de cette thèse. Nous présentons dans un premier temps les applications potentielles. Ensuite, nous décrivons les entités communicantes, les architectures de communication et les caractéristiques des réseaux sans fil véhiculaires. Nous analysons les technologies d'accès utilisables afin de déployer ces applications, avant de présenter les standards de communication véhiculaire.

1.1 Applications

Après avoir présenté l'utilité des réseaux sans fil véhiculaires, nous détaillons les applications qui peuvent être déployées sur ce type de réseau. Un consortium d'industriels (General Motors, Daimler Chrysler, Toyota, Nissan, Volkswagen, Ford, BMW) a établi un rapport [VSC 05] qui fait actuellement autorité, et qui liste 75 applications. Nous pouvons distinguer trois classes d'applications : la gestion du trafic, le confort, et la sécurité du trafic routier.

1.1.1 Applications de gestion du trafic routier

Les applications de gestion du trafic routier visent à optimiser le trafic routier et à prévenir la congestion. Grâce à la communication entre véhicules, ces derniers deviennent alors des capteurs de trafic. La granularité de l'information devient donc plus fine qu'avec la simple utilisation de bornes de comptage (présentes tous les 500 mètres sur la rocade toulousaine par exemple). Deux projets de recherche REACT [REA 06] et Com2REACT [COM 10] illustrent l'utilité et les bénéfices de ce type d'applications (notamment en volumes de carburant économisés). Des exemples d'applications sont la coopération entre les véhicules afin de faciliter le passage des véhicules d'urgence, ou les itinéraires alternatifs. Ce dernier exemple est de plus en plus proposé par les systèmes de navigation actuels en cas d'embouteillage.

1.1.2 Applications de confort

Cette catégorie comporte toutes les applications qui participent au confort du conducteur et qui ne relèvent pas de la gestion du trafic ni de la sécurité routière. Ces applications se présentent donc en tant que services fournis au conducteur. Parmi ces applications, citons les panneaux d'annonces locales : d'ordre commercial comme les offres de restaurants, la présence de stations-service à proximité, ou culturel comme des informations touristiques relatives à la localisation du véhicule. Il y a aussi des services télématiques comme le péage à distance sur autoroute, le paiement automatique dans les stations-service (ce qui peut faciliter la vie des handicapés). Un autre type d'application de confort est la communication à vocation de divertissement. Une offre de connexion internet à bord avec vidéo à la demande en est un parfait exemple. À toutes ces applications s'ajoutent aussi les communications point à point entre deux conducteurs qui voyagent ensemble. Ils peuvent ainsi

s’échanger des messages ou partager des données (vidéo, musique, itinéraire, jeux en réseau). La vie des usagers pourra aussi être facilitée par le contrôle à distance de véhicule de manière électronique (vérification du permis de conduire, contrôle technique, plaque d’immatriculation) pour les services compétents (police, douane, gendarmerie).

1.1.3 Applications de sécurité du trafic routier

La diminution du nombre de personnes blessées ou tuées sur les routes est une des principales motivations du développement et de l’étude des communications véhiculaires. Cette catégorie contient tous les services qui visent à améliorer la sécurité routière. Il s’agit d’améliorer le champ de vision du conducteur en lui proposant une aide à la conduite. Le conducteur pourra ainsi anticiper et agir pour rendre la conduite plus sûre. Le conducteur pourra être informé qu’un véhicule vient de passer un feu rouge ou qu’un piéton est en train de traverser la route. Une application, qui est déjà déployée dans les véhicules haut de gamme, est le service SOS. En cas d’accident, lors du déclenchement de l’airbag (c’est-à-dire dans les dix millisecondes qui suivent la collision), un message est émis afin de prévenir le centre de secours le plus proche. Ce service permet d’économiser de précieuses minutes dans le processus d’arrivée des secours.

Dans cette catégorie, on retrouve les applications qui utilisent les informations des autres véhicules : l’alerte d’état de la route (verglas, obstacle), l’aide au dépassement (calcul des distances, vérification de l’angle mort), l’alerte de freinage ou de collision en amont du trajet. On remarque donc que les applications de sécurité du trafic routier ont un rôle majeur dans la réduction du nombre d’accidents. On remarque aussi que cette catégorie d’applications a des contraintes temporelles fortes. En effet, si l’alerte de danger arrive trop tard, alors le conducteur ne pourra pas anticiper. Nous perdons ainsi les bénéfices de telles applications.

Le travail effectué durant cette thèse se focalise sur cette catégorie d’applications. Nous nous intéressons plus précisément au service coopératif d’alerte de danger local. Le service d’alerte de danger local permet à chaque véhicule de diffuser un message d’alerte afin de prévenir les véhicules arrivant dans la zone de danger. Cette application a donc de fortes contraintes temporelles, car recevoir un message d’alerte en retard met à mal le bien-fondé de cette application et peut engendrer de graves conséquences comme le suraccident. Nous distinguons deux types d’alerte en fonction de la gravité de l’alerte :

- Dans le cas d'un accident : ce service avertit les véhicules se dirigeant vers le lieu de l'accident que les conditions de circulation sont modifiées et qu'il est nécessaire de redoubler de vigilance. Il est nécessaire, également, en cas de densité réduite de véhicule de pouvoir conserver l'information pour pouvoir la retransmettre si un véhicule entre dans la zone de retransmission.

- Dans le cas de ralentissement anormal (embouteillage, travaux, intempéries, etc.) : ce service permet d’avertir les automobilistes de situations de circulation particulières. L'information, quelle que soit la nature des difficultés de circulation, renseigne l'automobiliste de la menace et qu'il est nécessaire de ralentir. Le message d'alerte est émis par un véhicule détectant les difficultés de

circulation (freinage important, déclenchement des feux de détresse, pluie par exemple). Un véhicule banalisé effectuant des travaux peut également être à l'origine du message d'alerte. Comme pour le message d'alerte informant d'un accident, le message d'alerte informant d'un ralentissement doit être transmis aux autres véhicules de façon efficace et rapide.

Le Tableau 1-1 liste de manière non exhaustive les applications et leurs contraintes. Par exemple, on remarque que chaque application fonctionne avec un type de communication particulier, un type de message, une fréquence d'émission, une latence maximale et une portée minimale.

Le but est donc de mettre en place des réseaux sans fil véhiculaires composés d'équipements intelligents permettant le déploiement des applications listées. Dans les sections suivantes, nous décrivons les réseaux sans fil véhiculaires et analysons comment déployer les applications et sur quelles technologies d'accès.

Application		Information sur l'application				
		Communication	**Type de message**	**Fréquence d'émission (ms)**	**Latence (ms)**	**Autres prérequis**
1	Feux de freinage d'urgence électronique	Ad hoc V2V	Événementiel, diffusion limitée dans le temps	100	100	Portée : 300 m Priorité haute
2	Alerte de véhicule lent	Ad hoc V2V	Diffusion périodique permanente	500	100	Priorité haute
3	Alerte de collision (intersection)	Ad hoc, infrastructure V2I, V2V	Diffusion périodique permanente	100	100	Positionnement précis Priorité haute
4	Alerte de zone dangereuse	Ad hoc, infrastructure I2V, V2V	Événementiel, diffusion localisée limitée dans le temps	100	100	Priorité haute
5	Alerte de violation de feux tricolores	Ad hoc, infrastructure I2V	Événementiel, diffusion limitée dans le temps	100	100	Portée : 250 m Priorité haute
6	Détection pré-accident	Ad hoc V2V	Diffusion périodique, unicast	100	50	Portée : 50 m Priorité haute/moyenne
7	Alerte de changement de voie	Ad hoc V2V	Diffusion périodique	100	100	Précision de positionnement < 2 m Portée : 150 m
8	Alerte coopérative de collision	Ad hoc V2V	Périodique, diffusion événementielle, unicast	100	100	Précision de positionnement < 1 m Portée : 150 m
9	Gestion d'intersection	Ad hoc, infrastructure V2I, V2V	Diffusion périodique, unicast	1000	500	Précision de positionnement < 5 m
10	Alerte d'accès limité et de déviation	Infrastructure I2V, autre réseau de diffusion	Diffusion périodique	100	500	Priorité moyenne/basse
11	Contrôle de la vitesse de croisière	Ad hoc V2V	Diffusion unicast	500	100	Priorité moyenne
12	Télépéage	Ad hoc, infrastructure V2I, cellulaire	Diffusion périodique, unicast	1000	200	DSRC
13	Diagnostic distant	Ad hoc, infrastructure V2I, V2V, cellulaire	Unicast, diffusion, événementiel	N/A	500	Accès Internet Service disponible
14	Téléchargement de média	Infrastructure cellulaire, autre réseau de diffusion	Unicast, diffusion, à la demande	N/A	500	Accès Internet Gestion des droits numériques
15	Téléchargement de cartes routières	Ad hoc, infrastructure cellulaire, autre réseau de diffusion, V2I, V2V	Unicast, diffusion, à la demande	1000	500	Accès Internet Gestion des droits numériques Service disponible
16	Assistance de conduite économique	Ad hoc, infrastructure V2I, V2V, cellulaire	Unicast, diffusion, à la demande	1000	500	Accès Internet Service disponible

Tableau 1-1. Exemple d'applications et leurs contraintes [PAP 09]

1.2 Messagerie et architectures des réseaux sans fil véhiculaires

Un réseau sans fil véhiculaire est un ensemble d'entités communicantes organisées selon une architecture de communication. Ces entités embarquées peuvent rencontrer différents environnements (urbain, péri-urbain, autoroutier), ayant leurs contraintes propres.

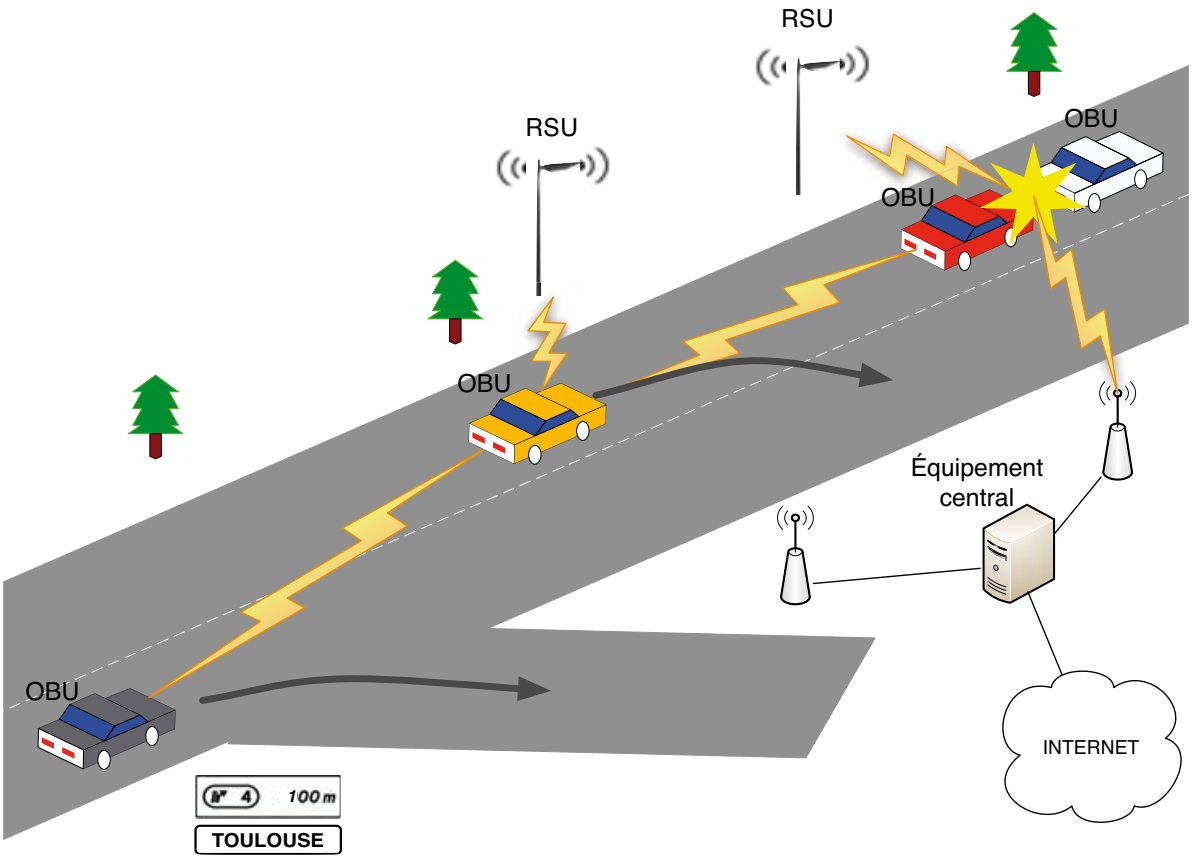

Figure 1-1. Exemple de réseau véhiculaire [LIN 08]

1.2.1 Entités communicantes

Dans un réseau sans fil véhiculaire, il existe quatre entités communicantes : l'équipement personnel, le véhicule, l'équipement de bord de route et l'équipement central. La Figure 1-1 illustre un exemple de réseau véhiculaire faisant intervenir les différentes entités lors d'un accident de la route.

- Les équipements personnels sont les équipements qui peuvent être apportés par l'utilisateur à l'intérieur de son véhicule. Cela peut être un téléphone portable, un ordinateur portable ou encore un GPS autonome. Ces équipements peuvent interagir avec le véhicule. De nos jours, en activant l'interface Bluetooth du téléphone portable, on peut utiliser son téléphone portable par commande vocale (en utilisant les microphones intégrés au véhicule) ou par le biais de l'interface Homme-Machine (IHM) du véhicule.

- Les véhicules modernes sont équipés d'un ensemble de processeurs connectés à une plateforme centrale de calcul qui dispose d'interfaces filaires et sans fil. Les véhicules intelligents sont des véhicules équipés d'une unité nommée *On-Board Unit* (OBU). Cette unité peut enregistrer, calculer, localiser et envoyer des messages sur une interface réseau. La Figure 1-2 illustre un exemple de véhicule intelligent et les équipements le constituant. Ces équipements forment un système nommé DSRC (*Dedicated Short Range Communication*).

- Les entités de bord de route sont appelées *Road-Side Unit* (RSU). Ces unités peuvent informer les véhicules à proximité en diffusant les conditions de trafic, météorologiques ou spécifiques à la route (vitesse maximale, autorisation de dépassement, etc.). Les RSU peuvent aussi jouer le rôle de station de base en relayant l'information envoyée par un véhicule.

- L'équipement central se situe du côté « serveur ». Il est transparent pour l'utilisateur. Cet équipement central pourra être un serveur de stockage, un point d'entrée à un réseau filaire (Internet) ou un serveur de transaction (télépéage par exemple).

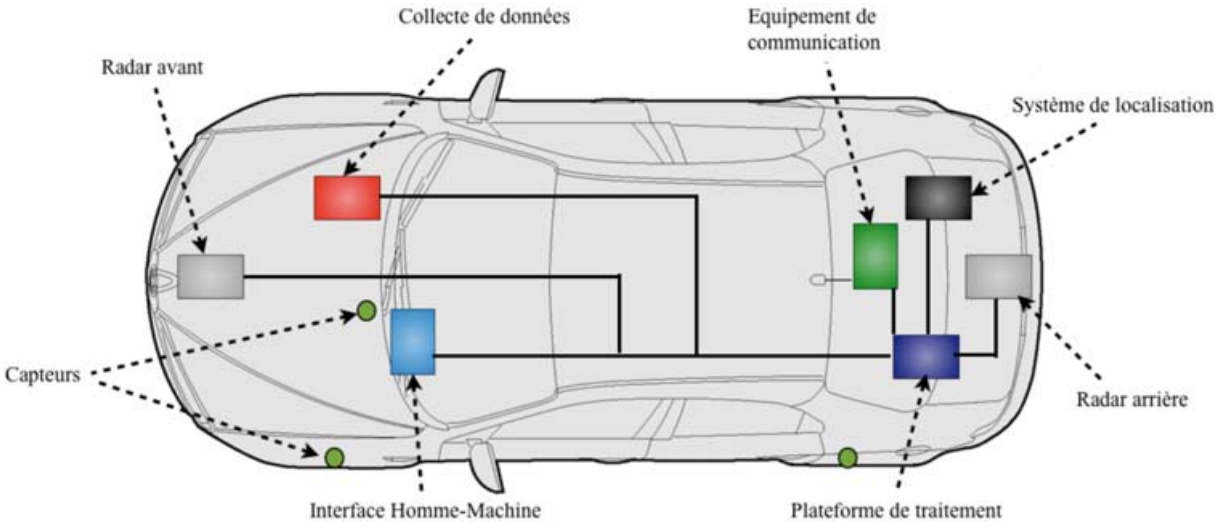

Figure 1-2. Exemple de véhicule intélligent [HUB 05]

1.2.2 Types de message

Les entités formant un réseau sans fil véhiculaire vont générer et s'échanger des messages. En fonction de l'application et du contexte environnemental, un véhicule peut envoyer (ou recevoir) un message de contrôle, d'alerte ou « autre ».

1.2.2.1 Message de contrôle

Le message de contrôle est généré à intervalle régulier. Conventionnellement, chaque véhicule émet un message de contrôle toutes les 100 ms. Ce message, appelé aussi « beacon », contient la position, la vitesse, la direction et l'itinéraire du véhicule émetteur. Grâce aux messages de contrôle, chaque véhicule se crée une vue locale de son voisinage. Le véhicule peut aussi prédire et anticiper des

situations accidentogènes ou de congestion. Le message de contrôle est l'équivalent du message HELLO des protocoles de routage. Chaque véhicule se fait donc connaître de son voisinage direct. Bien entendu, les messages de contrôle ne sont pas transférés et utilisent une diffusion à un saut.

1.2.2.2 Message d'alerte

Le message d'alerte est généré lorsqu'un événement est détecté. Cela peut être la détection d'un accident, d'un obstacle ou la réception d'un autre message d'alerte. Le message d'alerte doit être émis à intervalle régulier afin d'assurer la pérennité de l'alerte. Ainsi le ou les véhicules désignés pour la retransmission des messages émettront des alertes à instants réguliers. Les messages d'alerte doivent donc être de taille réduite pour être transmis le plus rapidement possible. Les messages contiennent en particulier les coordonnées du lieu de l'accident et les paramètres de la zone de retransmission.

1.2.2.3 Autres messages

Ce type de message contient tous les messages qui ne sont pas des messages d'alerte ou de contrôle. Ces messages ne sont généralement pas répétés à intervalle régulier. En effet, cela peut être par exemple un message de transaction financière ou l'envoi de courrier électronique.

Tous les messages reçus seront stockés dans un « cache des messages récemment reçus ». Chaque message se verra associer une durée de vie dans le cache.

1.2.3 Architectures de communication

Les systèmes de gestion de trafic « conventionnels » sont basés sur des infrastructures centralisées où des caméras et des capteurs implantés sur la route collectent des informations sur la densité et l'état du trafic. Ces informations sont transmises à une unité centrale pour les traiter et prendre les décisions adéquates. De tels systèmes exhibent un coût de déploiement assez important et se caractérisent par un temps de réaction de l'ordre de la minute pour le traitement et le transfert des informations. Dans un contexte où le délai de transmission de l'information est vital et revêt une importance majeure dans ce type de systèmes, ce délai est un véritable frein. De plus, les équipements mis en place sur les routes nécessitent une maintenance périodique et chère. Par conséquent, pour déployer un tel système à large échelle, un important investissement dans l'infrastructure de communication et de capteurs est nécessaire. Cependant, avec le développement rapide des technologies de communication sans fil, des systèmes de localisation et de collecte d'information par capteurs, une nouvelle architecture décentralisée (ou semi-centralisée) basée sur des communications véhicule-à-véhicule (V2V, *Vehicle to Vehicle*) suscite ces dernières années un réel intérêt auprès de la communauté scientifique, des constructeurs automobiles et des opérateurs Télécoms. Ce type d'architecture s'appuie sur un système distribué, autonome, et est formé par les véhicules eux-mêmes sans l'aide d'une infrastructure fixe pour le relayage des données et des messages. On parle dans ce cas d'un réseau ad hoc de véhicules (VANET, *Vehicular Ad hoc NETwork*). Le VANET n'est autre qu'une application dédiée et spécifique

des réseaux ad hoc mobiles conventionnels (MANET, *Mobile Ad hoc NETwork*)[1]. La figure 1-3 donne un exemple d'architecture réseau de DSRC. On y retrouve les entités communicantes détaillées en section 1.2.1. On remarque aussi la présence de deux types de communications nommées V2V et V2I.

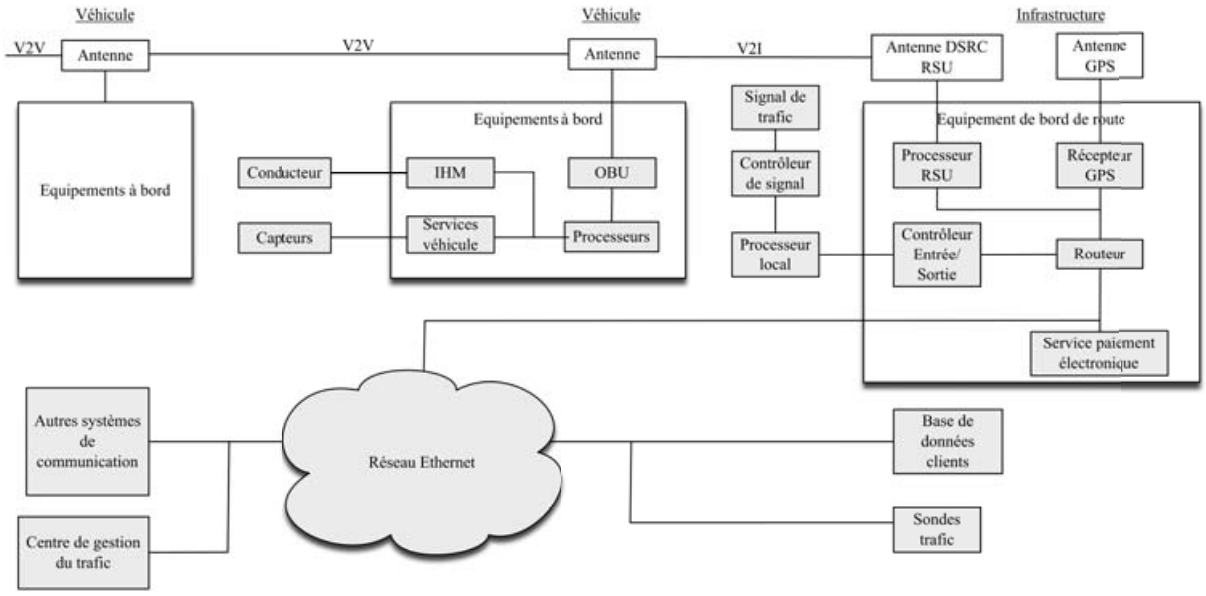

Figure 1-3. Architecture réseau de DSRC dans le projet VII [ZEN 09]

1.2.3.1 Communication Véhicule-Infrastructure

L'architecture Véhicule-vers-Infrastructure (V2I) est composée de RSU, auxquels les véhicules accèdent pour les applications de sécurité, de gestion et de confort. Les RSU sont administrés par un ou plusieurs organismes publics ou bien par des opérateurs autoroutiers. Un véhicule qui informe le service de voirie au sujet d'un obstacle est un exemple de communication V2I. Dans cet exemple, la communication est unidirectionnelle, du OBU vers le RSU.

Nous parlons de I2V dans le cas de communication Infrastructure-vers-Véhicule. Un panneau de signalisation équipé d'un RSU qui envoie une information aux véhicules passant à proximité est un exemple de communication I2V. Dans la suite, par V2I, nous englobons toutes les communications Véhicule-Infrastructure, quelle que soit la direction du trafic de données.

1.2.3.2 Communication Véhicule-à-Véhicule

L'architecture de communication inter-véhicules (V2V ou IVC pour *Inter Vehicle Communication*) est composée uniquement d'OBU (véhicules légers, poids lourds, véhicules de secours, etc.). Ils forment alors un réseau mobile sans avoir besoin d'un élément de coordination centralisé. Cette situation est plausible (et essentielle) si certains équipements RSU deviennent indisponibles (en panne ou hors de

[1] Un réseau mobile ad hoc (MANET) est un système autonome composé de stations mobiles interconnectées par des liens sans fil sans infrastructure centralisée. Les stations (ou nœuds) mobiles peuvent jouer le rôle de routeur ou d'hôte.

portée). Dans ce cas, le réseau doit continuer de fonctionner. Les véhicules doivent alors collaborer pour assurer la disponibilité du service. Ce mode de fonctionnement est communément appelé « ad hoc » et est utilisé par les VANETs. L'architecture V2V en mode ad hoc peut aussi être utilisée dans les scénarios de diffusion d'alerte (freinage d'urgence, collision, ralentissement, etc.) ou pour la conduite coopérative. En effet, dans le cadre d'applications de sécurité routière, les réseaux à infrastructure montrent leurs limites, surtout en terme de délai. Prenons l'exemple d'un véhicule en difficulté sur la chaussée qui diffuse un message d'alerte. Il semble plus rapide d'envoyer l'information directement aux autres véhicules plutôt que de la faire transiter par une station de base.

Une autre raison de l'existence de ce type d'architecture de communication vient du fait de la densité des réseaux routiers français. En effet, le million de kilomètres de routes françaises nécessitent, par exemple, un nombre important de RSU, ce qui entraîne un coût financier non négligeable [RES 08]. Même si les RSU sont déployés plus densément que prévu, ils ne seront pas tous opérationnels durant la phase de déploiement incrémental. Les communications V2V seront donc aussi utiles durant cette période d'installation.

Nous comprenons ainsi que le V2V joue un rôle primordial afin d'assurer une disponibilité du service. L'architecture V2V permet les communications critiques (alerte de danger local entre plusieurs véhicules proches, alerte d'un véhicule de secours se rapprochant, alerte de violation de feux tricolores). C'est pourquoi nous nous intéressons à ce type d'architecture dans la suite de cette thèse.

1.2.3.3 Hybride

La combinaison de ces deux types d'architecture de communication permet d'obtenir une architecture hybride intéressante. En effet, les portées des infrastructures étant limitées, l'utilisation de véhicules comme relais permet d'étendre cette distance. Dans un but économique et en évitant de multiplier les bornes à chaque coin de rue, l'utilisation de sauts par véhicules intermédiaires prend toute son importance. Néanmoins, les communications inter-véhiculaires souffrent de problèmes de routage lors de transmission longue distance. Dans de telles situations, l'accès à une infrastructure peut améliorer les performances réseau. Nous comprenons donc la complémentarité des deux types de communication et l'intérêt d'une architecture hybride.

Un cas particulier de l'architecture hybride est le réseau VSN (*Vehicular Sensor Network*). En effet, ce type de réseau émerge en tant que nouvelle architecture de réseaux de véhicules. Le VSN a pour objectif la collecte et la diffusion proactive en temps réel des données relatives à l'environnement dans lequel évoluent les véhicules, et ce, plus particulièrement en zone urbaine. En effet, les voitures sont munies de plus en plus de capteurs de toutes catégories (caméras, capteurs de pollution, capteurs de pluie, capteurs d'état des pneumatiques, ESP, ABS, géolocalisation satellite, etc.). Les informations délivrées par ces équipements peuvent être utiles pour l'obtention d'états sur le trafic routier (embouteillages, ralentissements, vitesse moyenne du trafic, etc.), sur les places de parking disponibles, pour des informations plus générales telles que la consommation moyenne de carburant et le taux de pollution, ou encore pour des applications de surveillance (grâce aux caméras embarquées sur des véhicules).

1.2.4 Environnements de déploiement

Le réseau routier est diversifié et propose plusieurs milieux de déplacement. Ces milieux se différencient par leur localisation (urbain, périurbain, rural, montagneux) et par leurs moyens (autoroute, route départementale, route nationale, chemins communaux, etc.). En raison de leurs spécificités (vitesse, densité du trafic routier), nous nous intéressons au milieu urbain et au milieu autoroutier.

1.2.4.1 Milieu urbain

Nous définissons le milieu urbain comme un réseau routier formé d'intersections et de points d'arrêt (feux tricolores, stop, cédez le passage, etc.). Il s'agit d'un environnement où les ondes sont fortement perturbées à cause de la forte présence de bâtiments notamment. Le milieu urbain se caractérise par un modèle de mobilité complexe, une densité de véhicules importante et une vitesse réduite (inférieure à 60 km/h). De plus, il y a déjà une infrastructure importante (panneaux, etc.). Il semble donc facile d'ajouter un équipement sur cette infrastructure afin de déployer les réseaux sans fil véhiculaires (V2I). Dans ce milieu, les réseaux V2V sont aussi réalisables et présentent l'avantage d'éviter le déploiement de RSU.

1.2.4.2 Milieu autoroutier

Le milieu autoroutier est caractérisé par une vitesse des véhicules importante (limitée à 130 km/h en France), une forte densité et une impossibilité (financière et de maintenance) de couvrir toutes les autoroutes avec des RSU. On y retrouve aussi une forte diversité de véhicule (poids lourd, voitures). En raison de l'absence d'obstacles tels que des immeubles, cet environnement semble moins perturbant pour les ondes radio. Néanmoins, il rencontre des problèmes d'étalement Doppler à cause de la vitesse élevée. De plus, certaines solutions actuelles, comme l'analyse par caméra numérique, sont perturbées par les poids lourds. En effet, ils gênent la vision des caméras, mais sont aussi des obstacles perturbants pour les communications.

Sur une autoroute, un « simple » accident peut vite dégénérer à cause, en partie, de la vitesse. La vitesse élevée peut engendrer des accidents plus graves, et soulève des contraintes de temps réel, de tolérance aux fautes et de fiabilité. Les applications de sécurité du trafic routier y seront donc très utiles. C'est pourquoi dans cette thèse nous nous focalisons sur cet environnement.

1.3 Caractéristiques des réseaux sans fil véhiculaires

Les VANETs sont une catégorie des MANETs permetttant la communication entre les véhicules. En plus des caractéristiques des réseaux ad hoc mobiles classiques, les VANETs ont la particularité d'avoir une très grande mobilité (les nœuds mobiles circulent à très grande vitesse). La topologie dynamique provoque de nombreuses reconfigurations (mise à jour des tables de routage, etc.), et soulève par conséquent des problèmes de performances. Après cet aperçu, nous détaillons, dans cette section, les caractéristiques des VANETs.

1.3.1 Énergie

À la différence des réseaux sans fil traditionnels où la contrainte d'énergie représente un facteur limitant important, les entités des réseaux véhiculaires disposent de capacités énergétiques suffisantes qu'elles tirent du système d'alimentation des véhicules. Même en cas d'arrêt du moteur et donc d'arrêt du système d'alimentation, il est possible pour une plateforme embarquée de recourir au dispositif de batteries dont seul un véhicule, du fait de sa taille, peut disposer. Les plateformes embarquées dans les véhicules étant pleinement alimentées, elles peuvent bénéficier de capacités de calcul plus massives et de multiples interfaces de communication.

1.3.2 Environnement de communication

Si les environnements de communication des réseaux sans fil traditionnels se résument généralement à des espaces complètement ouverts et sans obstacle ou à des espaces clos en intérieur, les réseaux véhiculaires imposent la prise en compte d'une plus grande diversité environnementale. Du fait de la mobilité des véhicules, il est en effet possible de passer d'un environnement urbain à un environnement autoroutier présentant des caractéristiques radicalement différentes. Il est également nécessaire de prévoir une volatilité des conditions climatiques et des contraintes topologiques. Cet environnement de communication conduit à des modèles de propagation d'ondes complexes.

1.3.3 Mobilité

Les réseaux véhiculaires se distinguent également des réseaux sans fil « classiques » (réseaux sans fil domestiques) par un modèle de mobilité dont une des traductions les plus évidentes est l'importante vitesse des nœuds. Cette contrainte de mobilité réduit considérablement les durées pendant lesquelles les nœuds peuvent communiquer. Ces conditions sont de nature à poser d'importants problèmes de connectivité couplés à une aggravation de l'instabilité de la propagation radio (par exemple évanouissement multi-trajet, effet de masque, atténuation de parcours, etc.). Ainsi la durée de vie des liens sur autoroute est de 50 secondes pour des véhicules allant dans la même direction, et inférieure à cinq secondes pour les véhicules allant en sens opposé [BLU 04]. Néanmoins, les déplacements des véhicules sont délimités et prédéfinis par les infrastructures routières et le comportement des conducteurs. Les informations sur les infrastructures routières sont souvent disponibles par le biais d'équipements de positionnement comme le GPS. À partir de la vitesse courante, de la vitesse moyenne et de la trajectoire de la route, la prochaine position du véhicule peut être prédite. Cette prédiction peut être affinée par la prise en compte de modèles de déplacement des usagers de la route. En effet, les véhicules sont la plupart du temps dans la même zone géographique, c'est-à-dire à 50 km de la maison du propriétaire. On retrouve aussi les modèles de déplacement réguliers comme le trajet maison-travail.

1.3.4 Géolocalisation

Un service de positionnement géospatial autonome et précis est nécessaire au bon fonctionnement de la plupart des applications déployées sur les réseaux VANETs. Avec un coût faible des récepteurs sol et une couverture importante, le système de positionnement par satellites (GNSS) est plus attractif que les systèmes de localisation basés sur les radars, lidars, capteurs ultrasons, ou caméras. De plus, les satellites GNSS proposent une horloge commune globale et un système de coordonnées terrestres commun pour les applications distribuées sur de nombreux véhicules. Ces avantages font que GNSS est une technologie de positionnement précise et adaptée pour les systèmes DSRC. Un exemple bien connu du système GNSS est le GPS (*Global Positioning System*). La précision actuelle des récepteurs GPS intégrés dans les véhicules est de l'ordre de 10-15 mètres. Cette précision n'est acceptable que pour le guidage. Pour les applications de sécurité routière, cette précision doit être améliorée. C'est un domaine de recherche actif, où de nombreux travaux sont conjointement développés par le milieu académique et industriel [DRA 07].

Afin d'améliorer la précision, une approche de cette technologie est le GPS différentiel (DGPS). Le DGPS utilise un réseau de stations de référence fixes qui transmet l'écart entre les positions indiquées par les satellites et leurs positions réelles connues. Le récepteur reçoit donc la différence entre les distances mesurées par les satellites et les véritables distances et peut alors corriger ses mesures de position. Ainsi la meilleure précision obtenue est de l'ordre d'un mètre. Néanmoins, cela n'est pas encore suffisant pour certaines applications coopératives de sécurité routière. Un autre domaine de recherche pour l'amélioration de la précision de positionnement est la cinématique temps réel (RTK). Cette technique promet une précision de l'ordre du centimètre grâce à l'utilisation de mesures de phase des ondes porteuses des signaux émis par les systèmes GPS ou Galiléo.

Mais l'inconvénient des techniques de positionnement par satellites est la perte de signal satellite. Cette situation arrive fréquemment quand les véhicules traversent des tunnels, ou des forêts denses par exemple. Afin de réduire ce temps de perte de signal, une solution consiste à fusionner GNSS et les capteurs inertiels du véhicule. Par exemple, à l'heure actuelle, la société Gladiator Technogies propose le LandMark 20, qui offre une précision de 2,5 m lorsqu'un signal GPS est disponible, et une perte de signal inférieure à une seconde. En compensant ainsi la perte de signal, la précision des positionnements entre véhicules augmente et les applications coopératives de sécurité routière pourront être déployées.

1.3.5 Modèle de communication

L'une des applications clés des réseaux de véhicules étant la prévention et la sécurité routière, les types de communication s'axent sur la diffusion de messages d'une source vers plusieurs destinataires. Bien entendu, les véhicules peuvent aussi communiquer en point à point. Dans le cas de diffusion, les véhicules sont plus ou moins concernés en fonction de leur position géographique et leur degré d'implication dans l'événement routier. Par exemple, un véhicule sur une route parallèle à une autoroute ne sera pas concerné par l'information d'un accident sur l'autoroute.

Nous retrouvons ainsi deux modèles de communication dominants : la diffusion totale (*broadcast*) et la diffusion multipoint vers une zone géographique définie (*geocast*). Un exemple d'application utilisant la diffusion est le « peloton » ou « train de véhicules ». Dans cette application, les véhicules sont organisés en convoi afin d'accroitre la capacité des routes. Au sein d'un peloton, un véhicule est élu « chef de convoi ». Le chef diffuse des informations, telles que le changement de vitesse, et les véhicules le suivant agissent en conséquence. L'avantage de la diffusion est qu'avec un taux de pénétration du marché entre 2 % et 10 %, un message peut atteindre six kilomètres (avec un rayon de communication de 1000 mètres) [WIS 05]. C'est pourquoi nous nous intéressons par la suite au modèle de communication par diffusion.

1.3.6 Topologie du réseau et connectivité

Un véhicule peut rapidement rejoindre ou quitter le réseau en un temps très court, ce qui rend les changements de topologie très fréquents. De plus, des problèmes tels que le partitionnement du réseau peuvent fréquemment apparaître, essentiellement quand le système DSRC n'est pas largement répandu et équipé dans la majorité des véhicules. Une seconde raison du partitionnement du réseau intervéhiculaire est que la probabilité de formation d'une chaine ininterrompue de véhicules à portée radio décroit exponentiellement [LOC 07]. Les solutions proposées doivent alors prendre en considération cette contrainte spatiotemporelle où la connectivité est un des paramètres clés, avec un diamètre de réseau limité. L'hétérogénéité des nœuds en terme de vitesse (les bus ont par exemple une vitesse régulière et inférieure aux véhicules particuliers) offre des informations supplémentaires à prendre en compte dans l'élaboration des solutions et des architectures pour les réseaux de véhicules. Par ailleurs, les propriétés inhérentes aux réseaux VANETs, notamment en terme de taille, ouvrent des problématiques de passage à l'échelle.

1.3.7 Discussion

Les réseaux sans fil véhiculaires soulèvent de nombreux challenges. En terme d'énergie, malgré la capacité énergétique importante d'un véhicule, celui-ci doit y faire attention. En effet, avec l'ajout de nouveaux capteurs, d'interfaces réseau, d'applications, la gestion énergétique du véhicule se complexifie. De nos jours, le véhicule doit être de plus en plus écologique et engagé dans le développement durable. Il faut donc développer les VANETs avec ce souci d'économie d'énergie.

D'un point de vue « économique », les VANETs sont particulièrement sensibles à la pénétration du marché. Par pénétration du marché, nous définissons le pourcentage de véhicules équipés du système permettant les communications sans fil véhiculaires DSRC. Plus il est important, meilleur est le service pour le client, car les applications fonctionneront mieux. S'il est faible, alors le réseau formera une multitude de graphes non connexes. Ainsi, les VANETs doivent être utilisables avec une densité très basse, mais doivent aussi supporter le passage à l'échelle. En 2005, une étude menée par Matheus *et al.* [MAT 05] prévoit que même si les véhicules de gamme intermédiaire (et au-dessus) sont équipés avec la technologie VANET, cela prendra trois années pour atteindre un pourcentage de pénétration du

marché de 10 %, et 16 ans pour 45 %. Nous comprenons ainsi que le réseau sera formé par de nombreux clusters non connexes.

1.4 Technologies d'accès

Afin de déployer les applications, nous faisons un tour d'horizon des technologies de communication sans fil existantes. Ce tour d'horizon permet de présenter les caractéristiques des technologies envisagées pour les VANETs. Il existe deux types de système possible :

- Les systèmes intra-véhiculaires composés de capteurs internes au véhicule et ne visant pas à diffuser de l'information vers l'extérieur du véhicule.

- Les systèmes extra-véhiculaires visant à l'échange d'informations entre une entité et son environnement.

Les systèmes extra-véhiculaires sont divisés en trois sous-systèmes selon leur utilisation :

- Les systèmes de télécommunications, qui sont dominants dans le domaine des communications mobiles, mais qui nécessitent une infrastructure. Ils sont particulièrement utilisés pour les applications de confort de l'usager (Internet à bord, vidéoconférence, autres services payants).

- Les systèmes de radio diffusion (éventuellement numériques), qui proposent de l'information de manière unidirectionnelle. Ils sont particulièrement utilisés pour les applications de gestion du trafic routier.

- Les réseaux informatiques extra-véhiculaires, qui proposent des échanges directs d'informations entre les entités. Ils sont particulièrement utilisés pour les communications V2V et les applications de sécurité routière.

Nous allons détailler chacun de ces systèmes.

1.4.1 Systèmes de communication intra-véhiculaires

Nous définissons les systèmes intra-véhiculaires comme des systèmes ne visant pas à la diffusion d'information à l'extérieur du véhicule. Les systèmes intra-véhiculaires sont composés de capteurs, d'une plateforme de calcul et de réseaux filaires (CAN) ou sans fil (Bluetooth, WiFi). Ces systèmes ont été les premiers développés par les industriels. Chaque constructeur pouvait définir son propre système sans devoir assurer l'interopérabilité avec les véhicules de marque concurrente. Ces systèmes sont connus sous le nom de « systèmes avancés d'aide à la conduite » (ADAS).

Dans la première phase d'acquisition de connaissance sur l'environnement de conduite, les systèmes actuels d'aide à la conduite utilisent deux sortes de capteur ou source d'informations :

1. Les capteurs proprioceptifs : Ce genre de capteurs fournit des informations internes au véhicule. Ces capteurs se limitent donc à renvoyer des informations sur le comportement et sur les paramètres du véhicule lui-même sans se préoccuper directement de l'environnement de conduite. Toutefois, ces capteurs fournissent des informations précieuses en termes de définition et de détermination du risque. Citons à titre d'exemple les informations sur la vitesse du véhicule acquises grâce à l'odométrie, sur les accélérations (par gyromètre), sur l'état du moteur du véhicule, sur l'état des freins, sur l'adhérence à la route, etc. Ces informations forment une source d'informations indispensable pour connaître, dans un premier temps, l'état et les capacités du véhicule lui-même pour mieux définir le risque encouru et pouvoir proposer, dans un second temps, des solutions pour réduire ce risque. Ces informations sont d'ailleurs utilisées par le système d'antiblocage des roues (ABS) ou le système d'antipatinage (ASR).

2. Les capteurs extéroceptifs : contrairement à la première catégorie, ces capteurs embarqués sur le véhicule auront pour mission de percevoir l'environnement de navigation du véhicule. Ils fournissent des informations sur le véhicule lui-même et sur les objets qui l'entourent à partir de leur perception de l'environnement. Citons à titre d'exemple la vision monoculaire ou stéréoscopique, la télémétrie laser ou radar, les ultrasons, etc. Plus communément, il existe le régulateur de vitesse adaptatif ou le parcage automatique. Ces capteurs acquièrent des informations sur les objets dans l'environnement de conduite. Ce genre de capteurs est plutôt utilisé dans la classe des ADAS autonomes puisqu'ils n'exigent aucune interaction physique avec l'environnement et se contentent de percevoir passivement.

Nous remarquons que les systèmes intra-véhiculaires sont une source importante d'informations précises sur le véhicule. Malheureusement, elles sont limitées au véhicule courant. De plus, ce système n'apporte qu'une connaissance locale et à courte portée de l'environnement du véhicule. Il est donc intéressant de coupler ce système à un système de communication sans fil extra-véhiculaire.

1.4.2 Systèmes de communication extra-véhiculaires

1.4.2.1 Systèmes de télécommunications

Les systèmes de télécommunications sont également connus sous le nom de réseaux cellulaires mobiles. Cette section traite des standards de télécommunications dominants en Europe : GSM et son extension GPRS, et UMTS (3G). L'architecture réseau d'un système de télécommunications contient une station de base qui contrôle l'accès au support et gère le processus d'itinérance (handover).

1.4.2.1.1 GSM/GPRS

Le *Global System for Mobile communication* (GSM) est la deuxième génération de téléphonie mobile orientée vers la communication de la voix. Avec l'avènement de l'Internet mobile, le *General Packet Radio Service* (GPRS) a été développé pour permettre la communication des paquets de données. Le GPRS est la génération 2,5 de téléphonie mobile basée sur la commutation de paquets et son débit théorique maximal est de 171,2 kbit/s. Néanmoins, la voix conserve une priorité supérieure dans la plupart des réseaux basés sur GSM. Le GSM/GPRS est un système radio à délai modéré, à faible débit, entre une station de base et un véhicule. Le trafic de données, plus particulièrement quand il transporte des informations de sécurité routière, a des besoins différents. En effet, il exige une communication en

temps réel ayant un faible délai, et une fiabilité de données élevée. Cette technologie n'est donc pas adaptée au transport de paquets pour les applications de sécurité du trafic routier. Par contre, le GSM/GPRS fournit une connexion internet (minimale en terme de débit) utilisée par le service SOS de certains constructeurs automobiles par exemple. Toutefois, cette technologie tend à être remplacée par l'UMTS qui propose notamment des débits supérieurs.

1.4.2.1.2 UMTS

L'*Universal Mobile Telecommunication System* (UMTS) est la norme de la troisième génération de téléphonie mobile. La transmission de données peut atteindre théoriquement des débits de transfert de 1,92 Mbit/s, et de 128 kbit/s pour les équipements mobiles à grande vitesse. Comme chaque utilisateur est lié à un opérateur téléphonique qui gère la facturation, l'UMTS est employé pour l'accès aux services payants tels que l'Internet à bord, la vidéo à la demande ou les jeux en réseau.

Grâce à ses caractéristiques techniques, l'UMTS est plus adapté aux applications de sécurité du trafic routier que le GSM/GPRS. En effet, le débit est constamment augmenté, et comme les applications de sécurité du trafic routier génèrent un volume important de données, l'UMTS répond à ce besoin. Mais des manques perdurent notamment en terme de garantie de délai.

Les systèmes de télécommunications sont une solution peu onéreuse et déjà existante. Mais dans notre contexte de communication véhiculaire sur autoroute ces systèmes n'assurent aucune garantie de délai. De plus, rien ne dit que les véhicules utiliseront le même opérateur. Il y aura donc un délai supplémentaire afin d'atteindre le(s) réseau(x) opérateur(s) des autres véhicules. Cela explique donc pourquoi les systèmes de télécommunications sont principalement utilisés pour les applications de confort de l'usager.

1.4.2.2 Systèmes de radio diffusion numérique

Les systèmes de radio diffusion numérique proposent de diffuser l'information depuis la station de base jusqu'aux utilisateurs. C'est donc un système unidirectionnel. Leur avantage est que les véhicules reçoivent la même information « au même moment ». Cette section présente trois standards pour la diffusion mobile : RDS/TMC, DAB/DMB, et DVB-T/DVB-H.

1.4.2.2.1 RDS/TMC

Les systèmes de navigation dotés d'un récepteur RDS/TMC (*Radio Data System/Traffic Message Channel*) leur permettent de calculer les itinéraires en tenant compte des informations délivrées par les opérateurs de service. Le RDS est un système de diffusion de données par la radio permettant d'envoyer des informations, transportées en plus du signal audio normal en modulation de fréquence, grâce à une sous-porteuse de la FM. Le débit de données RDS est de 1,2 kbit/s. Le TMC désigne une norme européenne de diffusion de données numérique sur les systèmes de navigation [ISO 03]. Les données transitent ainsi jusqu'à l'utilisateur sur le canal RDS de la radio FM.

1.4.2.2.2 DAB/DMB

Le DMB (*Digital Multimedia Broadcasting*) est une évolution du DAB (*Digital Audio Broadcasting*), développé et normalisé par l'European Telecommunication Standards Institute (ETSI) en 2005. Le DMB utilise un nouveau mode de compression en MPEG-4 qui permet de diffuser de la radio numérique avec des contenus multimédias, mais aussi de la télévision mobile, sur des appareils de petite dimension tels que des téléphones mobiles. Le DMB a été développé afin d'être le remplaçant de la radio FM. Malheureusement, avec un débit de 2,4 Mbit/s, une latence de 100 ms, un délai non borné et une communication unidirectionnelle, ces technologies ne peuvent supporter que les applications d'information de trafic routier.

1.4.2.2.3 DVB-T/DVB-H

Le *Digital Video Broadcasting* (DVB) est une technologie de diffusion pour la télévision numérique concurrente du DAB/DMB. Le *Digital Video Broadcasting-Terrestrial* (DVB-T) est un système qui transmet la voix et la vidéo via un flux compressé MPEG. Le DVB-H (*Digital Video Broadcasting-Handheld*) est une version optimisée de DVB-T, lequel n'avait pas été conçu à l'origine pour un usage nomade. Le DVB-H ajoute au DVB-T une redondance temporelle et une forte protection des flux transmis. Le DVB-H est ainsi adapté pour la réception mobile. Les différences par rapport au DAB/DMB sont un débit supérieur et une portée réduite. Bien que ces deux technologies soient adaptées pour le transport de vidéo, elles ne répondent pas aux contraintes pour les applications de sécurité du trafic routier. En effet, le DVB-T/DVB-H a une latence de six secondes, ce qui est trop important dans le contexte critique de ces applications. Toutefois, le DVB-T/DVB-H est utilisé pour les applications de confort utilisant les communications I2V uniquement. Par exemple, la diffusion vidéo dans un véhicule roulant à plus de 80 km/h utilise le DVB-H.

Les systèmes de radio diffusion numérique sont utilisés pour la diffusion d'informations à large échelle. Le TMC est de nos jours utilisé par certaines stations radio afin d'alerter les usagers des périphériques et des autoroutes de France. Comme il n'y a pas de canal montant, on parle donc d'information et non de communication. Ces systèmes ne sont donc pas applicables dans notre contexte de communication intervéhiculaire pour des applications à fortes contraintes temporelles. Néanmoins, nous retiendrons que le principe de fonctionnement peut être adapté aux communications infrastructure vers véhicules (I2V). Pour preuve, la société Médiamobile est un fournisseur d'information trafic qui utilise DMB comme technologie de diffusion.

1.4.2.3 Réseaux informatiques extra-véhiculaires

Dans cette section, nous étudions les réseaux informatiques sans fil extra-véhiculaires. Nous détaillons quatre technologies : l'infrarouge, le WiMAX, le WiFi, et le DSRC.

1.4.2.3.1 Infrarouge

L'infrarouge (IR) est un réseau à visibilité directe. Les émetteurs et récepteurs doivent être proches les uns des autres. Il est adapté pour des communications intervéhiculaires à très courte portée en point à point. Des exemples d'application de l'IR pour les communications V2V sont les projets CarTALK [REI 02] et PATH [HED 97]. Ils utilisent l'infrarouge par le biais de capteurs afin de calculer la

distance entre deux véhicules consécutifs. Grâce à l'IR, les véhicules conservent leur distance de sécurité.

Dans les travaux de Tajima [TAJ 03], un véhicule a été équipé d'un système de communication par IR pour l'analyse et la gestion du trafic. Les résultats ont montré que la communication avec le véhicule est possible jusqu'à 70 km/h.

Malgré une vitesse de transmission faible (1024 kbit/s sur la liaison descendante et 64 kbit/s pour la liaison montante), un ensemble d'applications de communication V2V, V2I, permettant l'identification du véhicule ou de son propriétaire, a été développé à partir de cette technologie. Par exemple, le paiement automatique de parking [STA 03].

Néanmoins, cette technologie souffre de plusieurs limitations. En plus d'être uniquement en point à point, l'IR est une technologie de « ligne de visée » qui ne peut traverser les murs, et requiert donc que la voie entre les périphériques soit dégagée. Cette technologie souffre aussi des perturbations dues aux interférences lumineuses.

1.4.2.3.2 WiMAX

Le réseau sans fil métropolitain, WiMAX, basé sur la norme IEEE 802.16, permet d'atteindre des débits de 70 Mbit/s sur un rayon de 50 kilomètres. Avec un débit élevé et un délai modéré, le WiMAX est adapté pour l'accès à Internet. Sa version mobile, Mobile WiMAX (basé sur le standard IEEE 802.16e), offre aussi une connectivité à moyenne et longue portée, mais adaptée pour des véhicules à vitesse modérée. Les travaux de Aguado *et al.* [AGU 08] démontrent que le WiMAX répond aux besoins des applications temps réel comme la voix sur IP (VoIP) et la vidéo à la demande. Cela positionne Mobile WiMAX comme une solution compétitive dans le contexte des communications véhicule-à-infrastructure. Mais le déploiement de cette technologie soulève tout de même un problème d'installation. Contrairement à la 3G qui est déjà présente sur le territoire français, le WiMAX nécessite l'installation de stations de base. Cela aura donc un coût financier important. De plus, à cause de ce besoin constant d'être à portée d'une station de base, le WiMAX propose un délai trop élevé pour les communications V2V.

1.4.2.3.3 WiFi

Aujourd'hui, la technologie *Wireless Fidelity* (WiFi) est devenue omniprésente dans les ordinateurs portables, les téléphones portables ou les consoles de jeux. Grâce à cette démocratisation et le faible coût de production, la technologie WiFi est une technologie abordable pour le déploiement de réseaux sans fil véhiculaires. Depuis la fin des années 1990, date d'apparition des premiers équipements utilisant la technologie WiFi sur le marché, trois spécifications de la couche physique pour le standard IEEE 802.11 furent ajoutées afin d'accroitre la vitesse de transmission. La dernière spécification en date est le 802.11n qui propose des débits théoriques de 300 Mbit/s. Malheureusement, en pratique le surcoût du protocole réduit de moitié les débits potentiels de la couche application. Cette dégradation de débit peut être pénalisante, surtout dans les réseaux véhiculaires. À première vue, la couverture radio omnidirectionnelle de 400 mètres semble suffisante pour maintenir une connectivité multisaut dans le milieu autoroutier ou urbain. Mais de nombreux travaux de recherche ont démontrés qu'à

cause des caractéristiques uniques des VANETs, cette technologie ne peut pas être appliquée telle quelle. À plus forte raison dans le contexte d'application de sécurité du trafic routier où le IEEE 802.11(g) affiche un taux de perte de paquets élevé à vitesse élevée.

1.4.2.3.4 DSRC

Dedicated Short Range Communication (DSRC) regroupe un ensemble de technologies dédiées aux communications véhiculaires. À l'origine, la technologie DSRC a été conçue pour répondre au besoin de transactions financières électroniques (télépéage). C'était un modèle de communication à courte portée (4 à 10 mètres) avec des débits inférieurs à 1 Mbit/s. Ensuite, le standard DSRC a évolué à partir du IEEE 802.11a [IEE 99] vers la norme IEEE 802.11p ou WAVE (*Wireless Access for Vehicular Environments*) [IEE 10] afin de répondre aux caractéristiques des VANETs. Le DSRC propose un canal de communication spécialement conçu pour transmettre des messages de très haute priorité à l'instar de certains messages critiques liés à la sécurité routière. Le WAVE présente aussi des caractéristiques beaucoup plus adaptées à la mobilité (comme des temps d'établissement de connexion plus courts) qui permettent l'envoi à la volée d'informations à des véhicules roulants à grande vitesse. Il présente une bonne fiabilité avec un taux d'erreur de 10^{-6} à 160 km/h. La technologie IEEE 802.11p est particulièrement adaptée pour les applications à portée moyenne et sensibles au délai.

1.4.3 Discussion

Dans le Tableau 1-2, les systèmes radio sont examinés selon plusieurs critères considérés comme représentatifs pour un système véhiculaire coopératif.

- Débit : DL représente le débit descendant et UL le débit montant en kbit/s.

- Portée radio maximale : rayon de communication maximal pour une communication à un saut de l'émetteur.

- Aptitude à la mobilité : indique la vitesse maximale autorisée pour un nœud par rapport à un point fixe. En fonction de cette vitesse, nous indiquons si la technologie est apte à la mobilité.

- Support trafic temps réel : indique si la technologie peut supporter un trafic de données temps réel en proposant des mécanismes de garantie temporelle. Lorsque la mention « selon la distance à la BS » est indiquée, cela signifie que cela dépend de la distance entre l'utilisateur et la station de base à laquelle il est connecté.

- Latence : indique le délai moyen entre l'émission d'un message et sa correcte réception.

- Modèle de communication supporté : V2V pour les communications intervéhiculaires, V2I pour les communications véhicule-infrastructure (quel que soit le sens).

	GSM GPRS	UMTS	RDS/TMC	DAB DMB	Infrarouge	WiMAX	WiFi	DSRC
Débit (kb/s)	DL : 60-80 UL : 20-40	DL : 384 UL : 384	RDS : 0,730 UL : n/a	DL : 2400 UL : n/a	DL/UL : 6000	DL/UL : 4500-22000	DL/UL : 54000	DL/UL : 3000-27000
Portée maximale	35 km	20 km (selon la cellule)	20 km	n/a	1-100 m	50 km	400 m	1000 m
Aptitude à la mobilité	Élevée 300 km/h	Élevée 500 km/h	Élevée 300 km/h	Élevée 150 km/h	Moyenne 70 km/h	Moyenne 70 km/h	Élevée 250 km/h	Élevée 300 km/h
Support trafic temps réel	Non	Oui (selon la distance à BS)	Non	Non	Oui (8 niveaux de priorité)	Oui (selon la distance à BS)	Oui (EDCA)	Oui
Latence (ms)	500-700	200-300	10 min	< 100	10	50	Selon implémentation	< 5
Mode de transmission	V2I	V2I	V2I	V2I	V2V, V2I	V2I	V2V, V2I	V2V, V2I

Tableau 1-2. Caractéristiques des technologies [COM 09][PAP 09]

Les communications directes entre véhicules (VANET utilisant DSRC) font face à une forte concurrence des communications cellulaires actuelles et futures (3G, 4G). Par exemple, les systèmes 3G offrent déjà un accès Internet mobile étendu, et ce, à prix compétitif. Nous pouvons raisonnablement affirmer que l'accès Internet par communication cellulaire à bas prix est devenu chose courante. Pour les VANETs, il va falloir attendre quelques années avant que cela ne soit une réalité. Le principal avantage des communications cellulaires est d'avoir accès à un réseau d'interconnexion « en un seul saut sans fil ». Une fois que la donnée a atteint la station de base du réseau cellulaire, les problèmes de connectivité sans fil disparaissent. C'est particulièrement important lorsque la donnée doit parcourir une longue distance géographique. Un autre avantage des réseaux cellulaires est qu'ils sont déjà disponibles. Par conséquent, un grand nombre d'applications nécessitant une communication entre un véhicule et Internet (ou entre deux véhicules) auront tendance à utiliser les réseaux cellulaires.
D'un autre côté, les VANETs sont adaptés pour les échanges locaux rapides de grands volumes de données. Il est « plus rapide » et plus efficace d'échanger des données directement entre véhicules plutôt que de les faire transiter par un réseau cellulaire. Comme nous l'avons mentionné plus haut, il existe des applications, comme l'information trafic, où la donnée est intéressante pour tous les véhicules à proximité du véhicule émetteur. Là encore, les communications directes entre véhicules ont un avantage par rapport aux communications cellulaires. En effet, dans ce scénario, le mécanisme de diffusion (broadcast) pourra être utilisé. Enfin, les communications VANET sont gratuites. Ce qui les rend très attractives pour beaucoup d'applications, à condition de se satisfaire d'une capacité restreinte et d'une connectivité limitée. Comme les véhicules communiquent entre eux directement, sans station de base intermédiaire, le délai de communication est intrinsèquement plus faible comparativement aux systèmes centralisés. Les communications sont établies par les véhicules eux-mêmes. Il n'y a donc pas de problème de couverture (donc de disponibilité) dans les zones blanches (campagne) contrairement aux systèmes cellulaires.

Afin d'expliquer le choix fait par la communauté scientifique, nous comparons les technologies les plus représentatives de chaque catégorie : UMTS, RDS/TMC, WiFi, WiMAX et DSRC. Les technologies restantes sont indiquées à titre d'information.

- Débit : Les réseaux informatiques offrent un débit nettement supérieur aux systèmes de télécommunication ou de radio diffusion. Dans notre contexte d'application de sécurité routière, plus le débit est élevé, plus tôt le conducteur sera prévenu.

- Portée maximale : Les trois catégories proposent une portée maximale homogène. La portée peut aller jusqu'à 20 km en moyenne. Mais est-ce bien utile dans notre contexte ? L'alerte d'un accident n'a pas besoin d'être émise à 20 km par exemple. Dans le cadre d'application utilisant un modèle de communication à diffusion et un protocole de routage multisaut, une portée minimale de 300 m est suffisante pour atteindre une distance de plusieurs kilomètres. N'oublions pas non plus qu'une portée de communication grande entrainera un temps d'accès au support plus long (notamment avec une couche MAC utilisant CSMA/CA).

- Support du trafic temps réel : Nous nous intéressons à des applications de sécurité du trafic routier qui nécessitent une garantie de délai. Une tendance se dégage : les réseaux informatiques et la 3G peuvent assurer un trafic temps réel.

- Latence : En relation avec le support du trafic temps réel, il est intéressant d'estimer le délai moyen de réception d'un message émis. Une application de sécurité routière requiert une latence inférieure à 100 ms. Dans ce cas, les solutions envisageables sont le WiMAX, l'IR, le DAB/DMB et le DSRC.

- Mode de transmission supporté : Les applications de sécurité considérées dans notre contexte nécessitent une communication V2V. En effet, en permettant la communication directe entre deux véhicules (ou plusieurs), nous pouvons espérer un délai plus faible qu'en passant par une station de base pour chaque transmission.

À l'issue de cette comparaison, la communauté scientifique a choisi la technologie DSRC car elle répond à tous les critères considérés comme représentatifs pour le fonctionnement d'application de sécurité du trafic routier. En effet, DSRC propose un débit suffisant pour le volume de données transporté, une portée de communication à un saut suffisante pour améliorer le champ de vision et permettre une anticipation. Cette technologie supporte une forte mobilité ainsi que le trafic de données temps réel avec une latence faible. DSRC propose aussi tous les types de communication véhiculaires.

Mais on remarque que chaque système radio est développé dans un but bien défini. Ainsi, il peut être intéressant de combiner certaines technologies afin de mettre en place un environnement d'interconnexion hétérogène le plus efficace possible. Le concept de l'architecture CALM (*Communication Architecture for Land Mobile environment*) permet le développement d'applications, indépendamment du média de communication utilisé [CAL 06]. Dans CALM, le CME (*CALM Management Entity*) est chargé de choisir la meilleure technologie de communication en fonction de leur disponibilité et des besoins des utilisateurs. Cette architecture permet des communications V2V et V2I, et un accès internet continu à travers différentes technologies potentiellement utilisées de manière simultanée. CALM inclut d'ores et déjà les technologies étudiées. Cependant, dans le contexte des réseaux véhiculaires, un consensus technologique semble se dégager autour du standard DSRC/IEEE 802.11p pour les déploiements à venir [TCH 08].

1.5 Standards de communication sans fil véhiculaire

L'IEEE a étendu sa famille de protocoles 802.11 en ajoutant le 802.11p [IEE 10], s'inspirant pour cela du standard ASTM E2213-03 [AST 07], lui-même basé sur le 802.11a [IEE 99]. Ce protocole modifie la couche physique et la couche MAC pour s'adapter aux réseaux de véhicules, en conformité avec la bande DSRC[2]. En complément, l'IEEE a défini la famille de protocoles 1609, dite WAVE, pour l'accès sans fil dans les réseaux de véhicules [IEE 10]. Ce standard, structuré en quatre composantes

[2] Actuellement, la « bande DSRC » ne désigne pas les mêmes gammes de fréquences d'un continent à l'autre.

(1609.1 à 1609.4), définit l'architecture, le modèle de communication, la structure de gestion, la sûreté et l'accès physique. Comme l'illustre la figure 1-4, 802.11p et WAVE spécifient une pile protocolaire complète. Le modèle DSRC/WAVE utilise deux piles. Une pile pour les applications de sécurité routière et une plus « classique » pour les deux autres catégories d'applications.

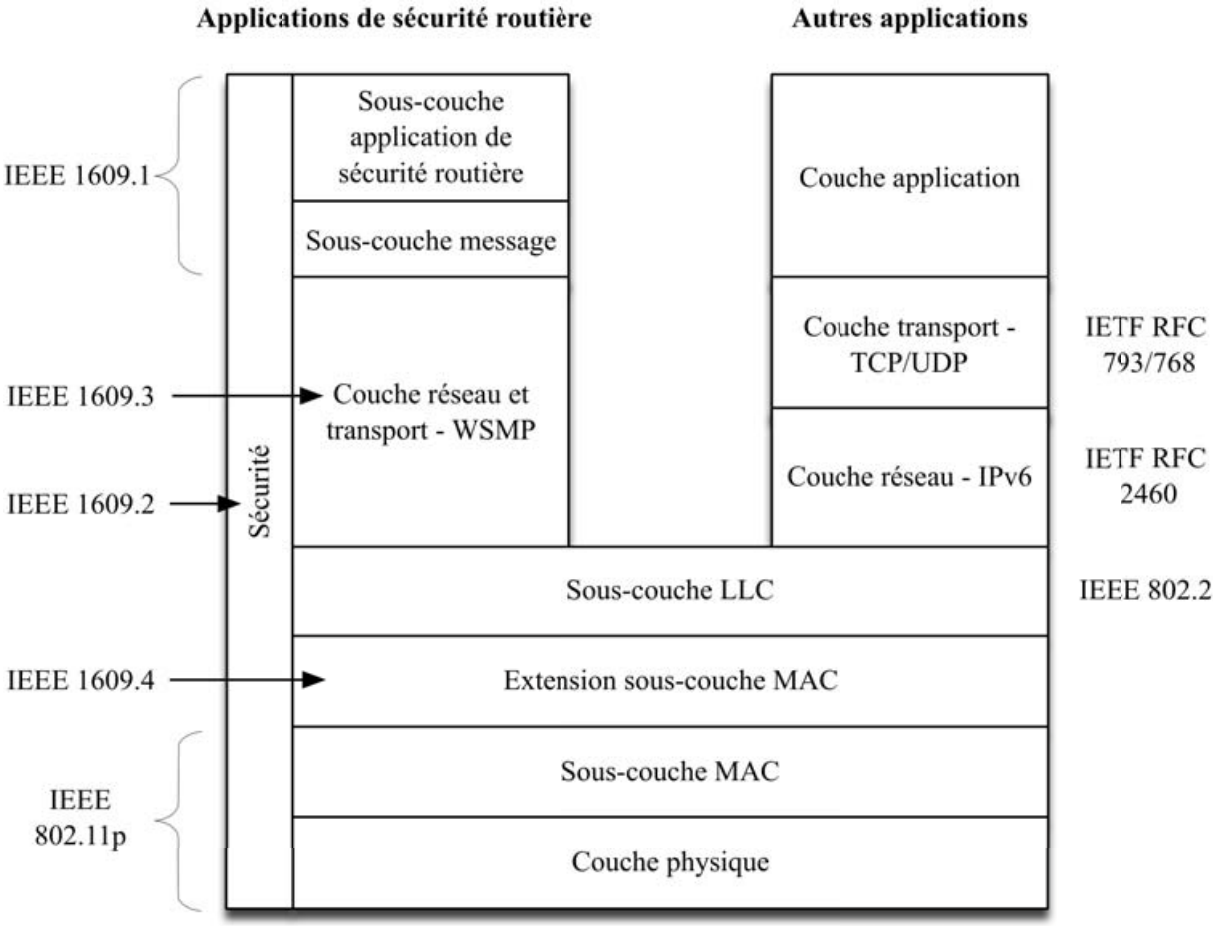

Figure 1-4. Le modèle DSRC/WAVE : IEEE 1609

1.5.1 IEEE 1609.1

Le standard IEEE 1609.1 se positionne au niveau de la couche application et définit les formats de messages et le mode de stockage des données utilisées par la couche application. Ce standard définit un gestionnaire de ressources qui autorise des applications de l'équipement de bord de route (RSU) à communiquer avec les *On-Board Units* (OBU) des véhicules à proximité. Il décrit trois composants de la couche application qui seront inclus dans un OBU :

- *Resource Manager Applications* (RMA) : Entité distante qui utilise le RM pour communiquer avec le RCP.

- *Resource Manager* (RM) : Le gestionnaire des ressources relaie le message du RMA vers le RCP. Le RM assure les services qui permettent au RMA de contrôler les interfaces présentes dans l'OBU.

- *Resource Command Processor* (RCP) : Il exécute les commandes données par le RMA et fournit une réponse au RMA via le RM.

Lorsqu'une application (présente sur un OBU ou un RSU) veut envoyer une commande à un OBU, le composant RMA envoie un message au RM. Le RM envoie la commande au RCP qui va commander les OBU connectés. Le RCP enverra un message de réponse au RM afin de délivrer le résultat. Le RM est donc le lien entre les applications d'un RSU (ou OBU) et les OBU d'autres véhicules. La figure 1-5 représente les modules du standard IEEE 1609.1.

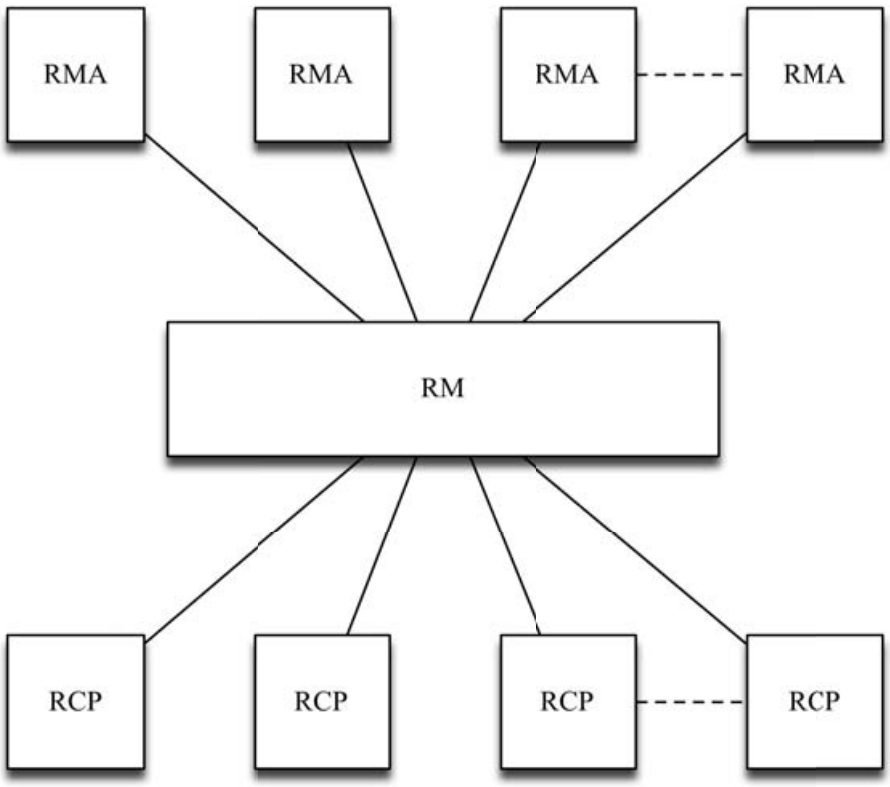

Figure 1-5. Modules du standard IEEE 1609.1 [RAO 09]

1.5.2 IEEE 1609.2

Le but de ce standard est de définir le format des messages sécurisés pour le système DSRC/WAVE. Le standard spécifie les méthodes pour sécuriser les messages de gestion et d'application. Il décrit aussi les procédures que doit accomplir le véhicule afin d'assurer les services de sécurité tels que l'authenticité, la confidentialité, l'intégrité, ou la non-répudiation. Bien que chaque application ne requiert pas forcément tous les services de sécurité, certains sont obligatoires. Par exemple, les applications de sécurité routière n'ont pas besoin de confidentialité contrairement aux applications de

transactions financières. Pourtant ces deux types d'applications nécessitent l'authenticité du véhicule et du message.

Selon les services de sécurité déployés, le format de message est différent. Par exemple, un message de transaction est signé et chiffré tandis que le message d'alerte est seulement signé. Le IEEE 1609.2 protège ainsi les messages et les véhicules d'attaques comme l'écoute clandestine, l'usurpation d'identité, l'altération, ou le rejeu de message. Nous détaillerons ce standard dans le chapitre suivant consacré à la sécurité dans les VANETs.

1.5.3 IEEE 1609.3

Le standard 1609.3 définit le *WAVE Short Message* (WSM) et le protocole d'échange associé *WAVE Short Message Protocol* (WSMP) afin d'assurer les fonctionnalités des couches réseau et transport pour les applications de sécurité routière. Le 1609.3 définit aussi le message *WAVE Service Advertisement* (WSA), qui est utilisé pour annoncer la disponibilité de services DSRC à une localisation donnée. Un WSA peut par exemple être envoyé pour annoncer la présence d'un service d'information trafic offert par un RSU.

D'après la Figure 1-4, la couche réseau utilise le protocole IPv6 pour ses caractéristiques de mobilité, de qualité de service et son espace d'adressage important. En effet, cette dernière caractéristique est primordiale dans un système avec plus de 500 millions de véhicules dans le monde. Le protocole IPv6 est utilisé pour les applications financières par exemple. D'un autre côté, le protocole WSMP est présenté comme une alternative à IPv6 [RIT 09]. Dans WSMP, les messages sont routés avec un identifiant de classe d'application (*Application Class IDentifier*, ACID) et une marque de contexte applicatif (*Application Context Mark*, ACM) en lieu et place de l'adresse IP et de l'identificateur de flux (*flow label*) [IEE 07]. Le WSMP permet aussi le contrôle de la puissance de transmission, du canal et du débit. Les applications de sécurité routière comme l'alerte de danger local (LDW) utilisent le WSMP car elles nécessitent une latence faible.

Ce standard définit deux plans, le plan gestion et le plan de données. Dans le plan de données, les données sont transmises en utilisant le protocole WSMP ou IPv6. Dans le plan de gestion, on y trouve plusieurs services comme l'enregistrement de service DSRC (un RSU déclare assurer un service de diffusion de vitesse maximale par exemple), ou la surveillance des canaux radio (afin de choisir le canal le moins chargé).

1.5.4 IEEE 1609.4 et IEEE 802.11p

Le standard IEEE 802.11p définit la couche physique du système DSRC. La technologie DSRC est définie dans la bande de fréquence des 5.9 GHz sur une largeur de bande totale de 75 MHz (5.850 GHz – 5.925 GHz). Comme illustrée par la figure 1-6, cette largeur de bande est segmentée en 7 canaux de 10 MHz chacun. Ces canaux se répartissant fonctionnellement en 1 canal de contrôle (CCH) et 6 canaux de service (SCH), chacun pouvant offrir des débits allant de 6 à 27 Mbit/s. Optionnellement, des canaux peuvent être configurés sur une largeur de bande de 20 MHz, ce qui

permet d'obtenir des débits pouvant aller jusqu'à 54 Mbit/s. La portée de transmission d'un système DSRC peut atteindre les 1000 mètres.

Le standard IEEE 1609.4 définit l'organisation, l'ordonnancement et l'utilisation de ces différents canaux. Le but de l'IEEE 1609.4 est de définir un mécanisme permettant à plusieurs équipements (multi-canaux) de se trouver, c'est-à-dire s'accorder sur le même canal au même moment afin de pouvoir communiquer. Deux concepts sont utilisés : le rendez-vous et la répartition dans le temps.

- Le canal de rendez-vous est un canal que chaque équipement doit consulter à intervalle régulier. Le canal de contrôle (CCH) est le canal de rendez-vous du standard IEEE 1609.4. Les autres canaux sont des canaux de services (SCH). Le canal de contrôle est notamment réservé à la transmission des messages de gestion du réseau (basculement entre canaux, annonces de services, etc.).

- Le concept de répartition dans le temps suppose que tous les équipements ont accès à une source commune de temps afin d'être synchronisés. Cette source de temps est disponible dans des systèmes globaux de positionnement comme le GPS (cf. §1.3.4). En l'absence de récepteur GPS, un équipement peut être synchronisé en recevant des signaux de temps depuis un autre équipement. Une fois les OBU synchronisés, l'IEEE 1609.4 impose un ordonnancement entre le CCH et les SCH afin d'assurer un service garanti aux applications de sécurité routière et un service minimum aux autres types d'applications.

Le standard IEEE 1609.4 a une forte relation avec le mécanisme EDCA de la sous-couche MAC. EDCA (*Enhanced Distributed Channel Access*) est basé sur CSMA/CA et est utilisé dans les réseaux WiFi supportant le standard IEEE 802.11e. EDCA assure un accès au support distribué et différencié en utilisant huit niveaux de priorité utilisateurs pour quatre catégories d'accès (Voix, Video, *Best Effort*, *Background*). Ce mécanisme permet ainsi d'attribuer une priorité à chaque message. Par exemple, un message d'application de sécurité du trafic routier aura une priorité supérieure à celle d'un message d'application de confort.

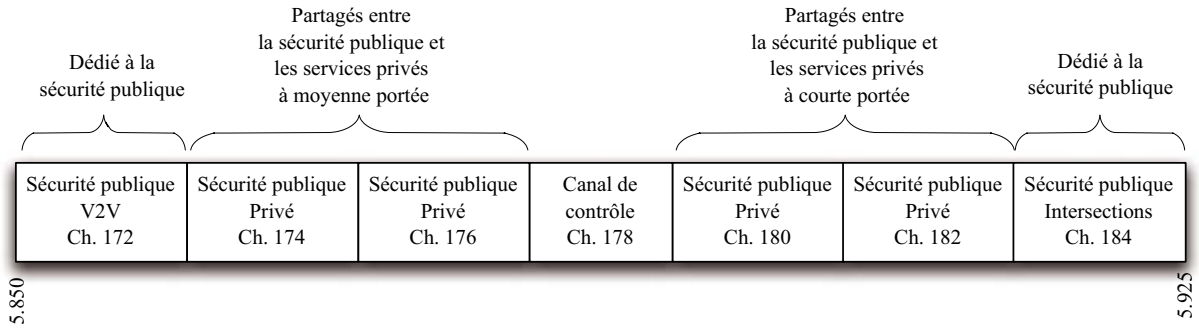

Figure 1-6. Canaux du standard IEEE 802.11p

1.6 Conclusion

Depuis quelques années, le développement des nouvelles technologies a favorisé une évolution du système de transport. Cette évolution vise à rendre le transport plus sûr, plus efficace, plus fiable et plus écologique, sans avoir nécessairement à modifier matériellement l'infrastructure existante. La gamme des technologies en jeu comprend l'informatique, les technologies de capteurs, les systèmes de contrôle et les télécommunications. Les principaux objectifs d'un système de transport intelligent concernent :

(i) l'amélioration de la sécurité des déplacements ;

(ii) l'amélioration de l'efficacité globale du système de transports en réduisant les temps de parcours et les congestions ;

(iii) l'intégration des transports dans une politique de développement durable, notamment en réduisant les émissions de gaz pour les véhicules légers et les poids lourds et en optimisant la maintenance de l'infrastructure ;

(iv) l'amélioration du confort de l'usager en lui fournissant une multitude de services d'information, d'aide à la décision, de guidage, et d'accès à Internet.

Dans ce chapitre, nous avons tout d'abord identifié les applications déployables dans un réseau sans fil véhiculaire, et les avons classés en trois catégories : confort, gestion du trafic routier et sécurité du trafic routier. En raison de la criticité des messages envoyés par les applications de sécurité routière, nous nous intéressons à cette catégorie. En effet, ces applications ont des contraintes temporelles fortes et un impact direct sur la vie des usagers. Nous nous focalisons plus particulièrement sur l'application d'alerte de danger local qui diffuse des messages d'alerte.

Nous avons ensuite décrit les entités présentes dans un réseau sans fil véhiculaire ainsi que leurs rôles, et leur type de communication (V2V, V2I). Nous avons notamment remarqué que les communications véhicule-à-véhicule (V2V) soulèvent des contraintes de performances réseau (délai, routage multi-saut, topologie dynamique) et un besoin de confiance (absence d'infrastructure). C'est pourquoi nous nous intéressons aux communications V2V dans un environnement sans infrastructure, c'est-à-dire un réseau sans fil ad hoc véhiculaire (VANET).

Les véhicules peuvent être dans des environnements de déplacement radicalement différents comme l'urbain ou l'autoroutier. Le milieu autoroutier a retenu notre attention, car il présente d'un côté un modèle de mobilité plus prédictible (pas de priorité à droite, de feux tricolores, etc.), mais de l'autre les vitesses les plus élevées. À cause de la vitesse, la moindre erreur sur autoroute peut provoquer des accidents graves et des suraccidents.

Afin de mieux comprendre les réseaux sans fil véhiculaires, nous avons détaillé leurs caractéristiques : énergie, communication, mobilité, géolocalisation, topologie, et pénétration du marché.

Pour déployer ce type de réseau et les applications potentielles, nous avons analysé les technologies d'accès possibles. Après une description des systèmes intra-véhiculaires et des systèmes extra-véhiculaires, nous avons expliqué le choix technologique fait par la communauté scientifique : DSRC. En effet, la technologie DSRC présente toutes les caractéristiques nécessaires au bon déploiement des applications de sécurité du trafic routier.

Les communications véhiculaires sont normalisées à travers l'ensemble de standards IEEE 1609. Cet ensemble de standards définit les différentes couches du modèle OSI pour les communications sans fil véhiculaires. Nous avons donc détaillé le rôle et le fonctionnement de chaque couche du standard IEEE 1609. Ainsi, dans la suite de cette thèse, nous nous intéressons à un réseau d'interconnexion dans lequel chaque véhicule est doté d'un équipement DSRC qui respecte le standard IEEE 1609.

Un exemple d'application de sécurité routière est l'application d'alerte de danger local (LDW). Le LDW vise notamment à éviter le suraccident sur autoroute. Pour cela, elle propose l'envoi d'un message d'alerte lorsqu'un accident est détecté. Les véhicules se dirigeant vers la zone de danger reçoivent l'alerte et peuvent donc agir en conséquence. Les conducteurs avertis ralentiront et pourront changer de voie ou d'itinéraire par exemple. Mais que se passerait-il si un véhicule malicieux parvenait à envoyer de fausses alertes de danger ? En effet, grâce à cette attaque, un véhicule malveillant peut détourner le trafic routier, entraîner des embouteillages ou des accidents. C'est notamment à cette question que le chapitre suivant vise à répondre.

La sécurité des véhicules et des messages est primordiale dans les VANETs. À plus forte raison dans notre contexte où certaines applications sont critiques et mettent en balance la vie des usagers. En effet, les véhicules agissent en fonction des informations envoyées par les véhicules à proximité. Avec une telle dépendance se crée un besoin de confiance. Mais cette confiance ne peut être acquise que par l'ajout de mécanismes de sécurité. C'est pourquoi nous détaillerons dans le chapitre suivant les services de sécurité ainsi que les attaques potentielles dans les VANETs.

2 Sécurité des réseaux sans fil véhiculaires

Les applications de sécurité du trafic routier, présentées dans le chapitre 1, utilisent les messages d'alerte pour informer le conducteur de situations potentiellement dangereuses (conditions de route dégradées, freinage d'urgence d'un autre véhicule, obstacle, etc.). Si ces alertes sont envoyées à tort, ou à outrance, alors l'utilisateur n'y prêtera plus d'attention. L'alerte elle-même peut devenir une menace, et provoquer des accidents à cause des réactions (inutiles, inappropriées, inadaptées) des utilisateurs. Ainsi, un attaquant pouvant injecter des messages falsifiés dans le VANET, pourra causer la « désensibilisation » de l'utilisateur ou des accidents, contrairement à l'objectif d'amélioration du trafic routier. Ce dysfonctionnement peut aussi venir d'un équipement défectueux qui génèrerait des informations erronées. Par exemple, un capteur peut détecter un obstacle sur la route, alors qu'il s'agit simplement une obstruction partielle du capteur. Devant la criticité d'utilisation des VANETs, les mécanismes de sécurité doivent donc adresser deux types de problème : le dysfonctionnement ou l'utilisation malveillante.

À titre d'illustration, supposons le scénario suivant : à la suite d'un accident sur autoroute, un véhicule accidenté diffuse un message d'alerte afin de prévenir les automobilistes arrivant dans la zone de danger. Dès réception de ce message, les conducteurs vont changer de voie, ralentir ou bien changer d'itinéraire. Un véhicule malveillant peut donc envoyer une fausse alerte afin d'influencer le trafic routier et provoquer des accidents. Pour décourager tout attaquant, et se prémunir de telles situations, un moyen est d'exiger un service d'authentification et d'intégrité. Ainsi chaque véhicule pourra authentifier les autres véhicules et vérifier que l'information n'a pas été modifiée par un véhicule intermédiaire. Un schéma de confiance sera alors installé.

Le but de ce chapitre est de faire un état de l'art de la sécurité des réseaux sans fil véhiculaires. Pour pouvoir sécuriser un VANET, il est nécessaire de connaître les menaces possibles. Ainsi, nous détaillons les modèles d'attaquant et les attaques possibles dans la section 2.1. Pour s'en prémunir, des services de sécurité sont nécessaires. Nous les présentons avec les mécanismes de sécurité associés. Notre contexte nous amène à porter ensuite notre attention sur l'application d'alerte de danger local.

Après avoir détaillé les attaques sur cette application, nous analysons les moyens et les stratégies permettant d'y remédier.

Dans la section 5.2 du délivrable D1.1 du projet SeVeCom [KRO 06], le service d'authenticité est marqué comme « important » ou « très important » dans 100 % des 52 applications listées. Le service d'intégrité est aussi important, mais à quoi bon être assuré de l'intégrité d'une donnée si l'on n'est pas certain de l'identité de l'expéditeur ? Le service d'authenticité apparaît donc comme la pierre angulaire de la sécurité des VANETs. C'est pourquoi nous examinons le standard IEEE 1609.2 en nous focalisant sur les procédures nécessaires à l'authentification.

Au-delà des problèmes de sécurité, les VANETs soulèvent des contraintes temporelles. Par exemple, avec un environnement fortement dynamique, caractérisé par une topologie très changeante, et des connexions de courtes durées, le déploiement d'une solution de sécurité doit faire face à des contraintes de temps et des configurations spécifiques. C'est pourquoi nous introduisons la problématique d'impact des mécanismes de sécurité sur la prédictibilité des systèmes embarqués temps réel que sont les équipements WAVE/DSRC.

2.1 Attaques dans les réseaux sans fil véhiculaires

2.1.1 Modèles d'attaquant

Afin de mieux cerner les attaques possibles sur un VANET, il est nécessaire de définir les modèles d'attaquant possibles. Ainsi, nous pourrons déterminer les mécanismes pouvant répondre à la sécurisation des réseaux véhiculaires. Nous définissons les critères de classification d'attaquant suivants [RAY 07]:

1. *Actif* ou *Passif* : Un attaquant passif ne peut qu'écouter clandestinement le canal de transmission. Cette attaque peut être conduite par un voisinage curieux, mais aussi pour une entreprise qui cherche à créer des profils de conducteurs. Un attaquant actif peut générer, modifier, rejeter ou rejouer des messages afin de disséminer de fausses informations. Le but d'un attaquant actif est de s'octroyer des privilèges afin d'améliorer son environnement de conduite. Ainsi, il peut usurper l'identité d'un véhicule de secours pour faciliter son déplacement.

2. *Interne* ou *Externe* : Un attaquant interne est un membre authentifié du réseau qui peut communiquer avec les autres membres du réseau. Comme il fait partie du réseau, il possède déjà quelques avantages comme les clés publiques utilisées par les autres véhicules. Un attaquant interne peut causer plus de dommages au réseau que l'attaquant externe qui a un accès limité au système.

3. *Malicieux* ou *Rationnel* : Un attaquant malicieux cherche à prouver une capacité ou une réussite personnelle. Pour cela, il cherche à détecter des zones de vulnérabilité et à les exploiter pour perturber le système, ou blesser des membres du réseau. Des attaquants qui causent délibérément des accidents de la route sont considérés comme malicieux. Par conséquent, l'attaquant malicieux

est prêt à tout pour arriver à ses fins quels que soient les coûts et les conséquences. Par opposition, l'attaquant rationnel vise l'accomplissement d'une tâche spécifique sur le réseau en défaveur (ou en faveur) d'une personne identifiée. Les attaques rationnelles sont plus prévisibles que les attaques malicieuses.

4. *Mal intentionné* ou *Involontaire* : Un attaquant est dit mal intentionné s'il vise délibérément à remettre en cause le bon fonctionnement du réseau. Ce type d'attaquant est à distinguer d'un attaquant involontaire qui peut par exemple lancer (sans le vouloir) une attaque à partir d'un capteur défectueux.

5. *Indépendant* ou *Collaboratif* : Les attaquants peuvent agir indépendamment les uns des autres ou bien collaborer. Lorsqu'ils collaborent, les attaquants s'échangent des messages et coopèrent afin de rendre l'attaque plus efficace. Par exemple, des véhicules attaquants collaboratifs annoncent un embouteillage fictif pour convaincre les véhicules honnêtes. Ces derniers vont alors changer de chemin, libérant ainsi la voie pour les attaquants [RAY 07].

6. *Local* ou *Étendu* : Un attaquant peut avoir une portée d'action limitée, même s'il contrôle plusieurs entités (OBU ou RSU). On dit qu'il est local parce que la portée limitée des OBU et des RSU, rend l'attaque limitée. Un attaquant étendu contrôle plusieurs entités qui sont éparpillées sur le réseau, ce qui lui confère une portée étendue.

2.1.2 Attaques de base

L'attaque délibérée ou non d'un VANET repose sur un but précis. Nous dressons une liste des attaques évidentes ou faisables et qui constituent un risque non négligeable en cas de réalisation. En raison de l'impossibilité d'envisager toutes les attaques possibles dans les réseaux véhiculaires, nous nous limitons aux exemples les plus significatifs dans notre contexte :

1. *Attaque sur la vie privée* : Dans cette attaque, l'entité malveillante essaie d'obtenir l'identité ou des informations personnelles d'un utilisateur du réseau. Cela peut également se traduire par tracer l'activité et les déplacements de cet utilisateur. Pour identifier et tracer une victime, l'attaquant peut utiliser toute chaîne de caractères identificatrice dont la récurrence est constatée dans les échanges de la victime. Cette chaîne de caractères peut être une adresse IP, une adresse MAC, des informations d'identification d'un certificat, etc. Au-delà des chaînes de caractères, l'empreinte radio de la victime peut également être utilisée: on parle alors d'attaque de la couche physique. D'après les modèles d'attaquants, l'attaquant peut être *Interne* ou *Externe*, *Mal intentionné*, *Passif* et *Indépendant*.

2. *Attaque sur la cohérence de l'information* : Dans cette attaque, l'entité malveillante porte atteinte à la cohérence des informations acheminées dans le réseau en les modifiant ou en injectant des informations erronées. L'intention de l'attaquant est d'altérer la perception qu'ont ses victimes des conditions de circulation (position, vitesse, direction). Ce faisant, l'attaquant peut par exemple provoquer un changement d'itinéraire de ses victimes. Sur la Figure 2-1 qui illustre ce cas, un attaquant (M) diffuse des informations de trafic erronées amenant les victimes A et B à changer

de voie. Dans cette attaque, l'attaque est *Interne* ou *Externe*, *Intentionnelle*, *Active* et *Indépendante*.

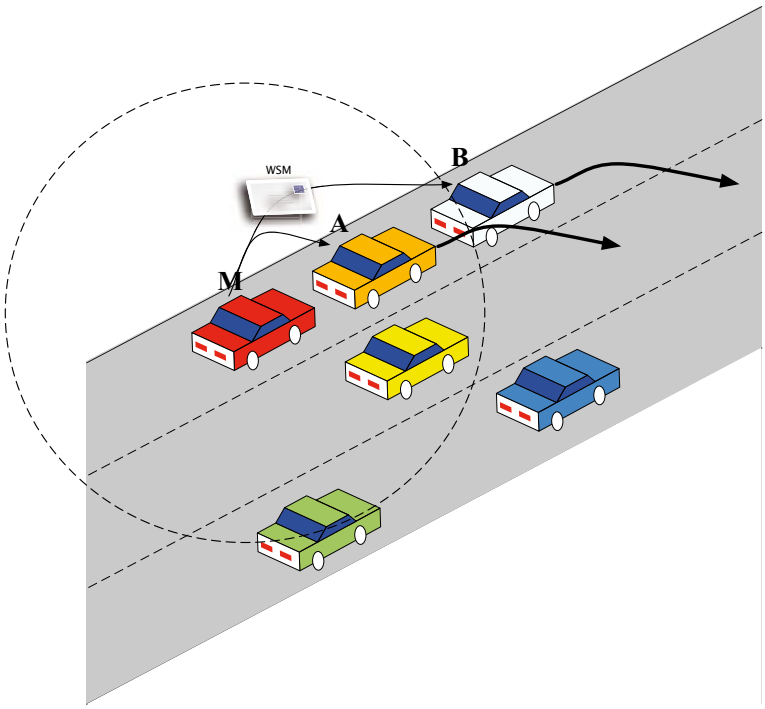

Figure 2-1. Attaque sur l'incohérence de l'information

3. *Usurpation d'identité ou de rôle* : Dans cette attaque, l'entité malveillante utilise une fausse identité ou de fausses lettres de créance pour se faire passer pour une entité légitime ou pour jouir des privilèges de cette dernière. La Figure 2-2 illustre un cas où l'attaquant M usurpe l'identité du véhicule A pour récupérer des données du véhicule B. L'attaquant peut être *Interne* ou *Externe*, *Malicieux* ou *Rationnel*, *Mal intentionné*, *Actif* et *Indépendant*.

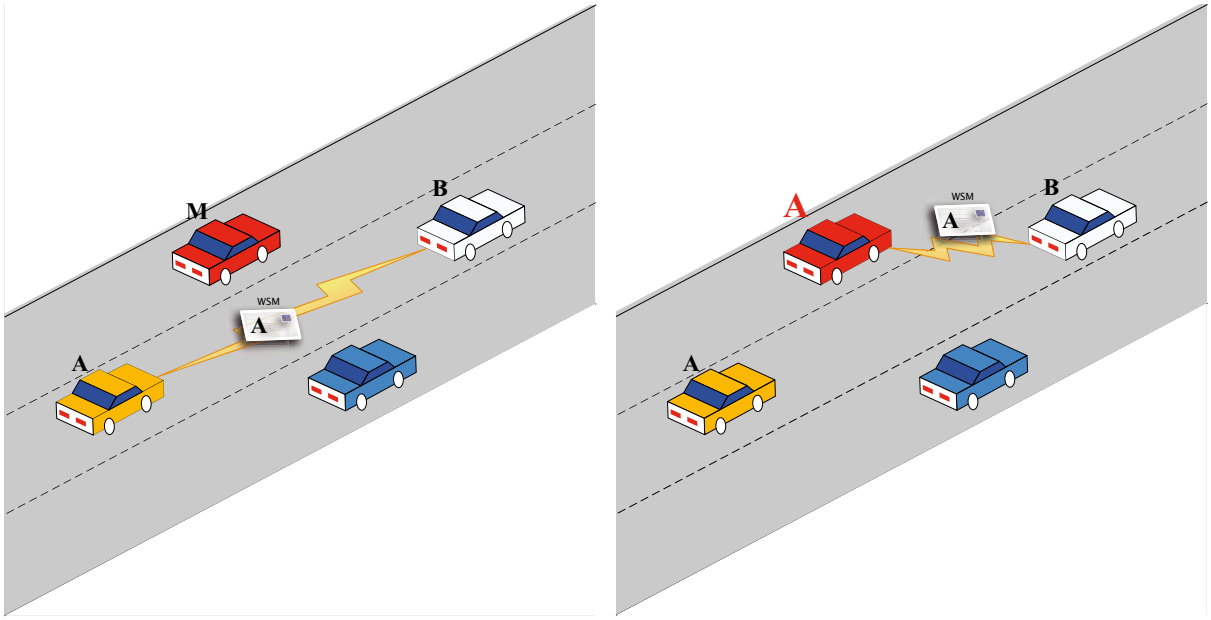

Figure 2-2. Usurpation d'identité ou de rôle

4. *Déni de service (DoS)* : Dans ce type d'attaque, l'entité malveillante empêche l'accès normal aux services du réseau. Ce type d'attaque peut être généré en brouillant le canal radio, en surchargeant ou en épuisant les ressources du réseau par des requêtes abondantes, en exploitant la vulnérabilité des protocoles, ou en ayant une attitude non coopérative (refus de relayer des paquets par exemple). La Figure 2-3 illustre une attaque par déni de service aboutissant à une collision, car l'attaquant M empêche l'échange de messages critiques entre le véhicule accidenté B et le véhicule A. L'attaquant peut être *Interne* ou *Externe*, *Mal intentionné*, *Actif* et *Indépendant*.

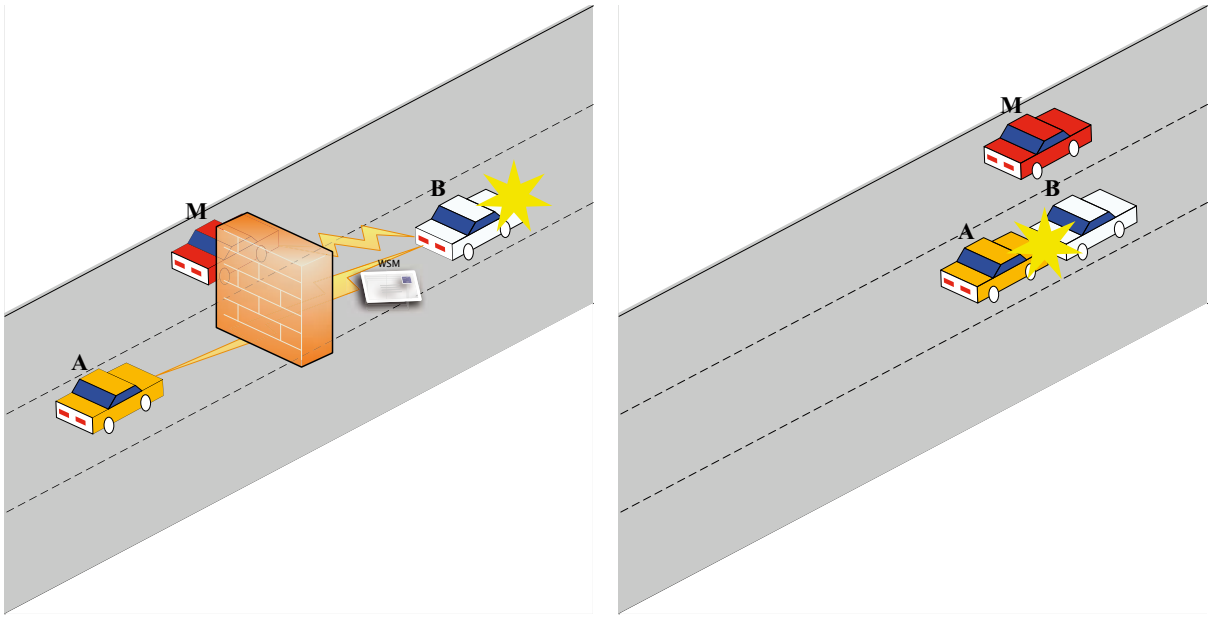

Figure 2-3. Déni de service

5. *Écoute clandestine du réseau* : Dans cette attaque, l'entité malveillante collecte les données transmises dans le réseau afin d'en extraire une information dont elle pourrait tirer profit. Un exemple d'attaque est un attaquant qui espionne une transaction commerciale, typiquement un paiement électronique à un péage, en vue d'en extraire les informations bancaires. L'attaquant peut être *Interne* ou *Externe*, *Mal intentionné*, *Passif* et *Indépendant*.

2.1.3 Attaques complexes

Après avoir listé des attaques de base, nous présentons trois attaques complexes. Une attaque complexe est une combinaison d'attaques de base.

1. *Véhicule caché* : C'est un exemple de falsification des informations de positionnement, et une variante du « Sybil attack ». Dans le protocole de distribution des messages d'alerte, si un véhicule diffusant l'alerte détecte un voisin mieux positionné que lui pour diffuser, alors il arrête d'émettre. Ce protocole permet de réduire la congestion du canal radio. La Figure 2-4 illustre cette attaque. L'attaquant M fait donc croire qu'il est en meilleure position (M') afin d'être le seul à émettre l'alerte. Mais il ne va pas diffuser l'information d'alerte, rendant le véhicule en danger B « caché » des autres véhicules (A).

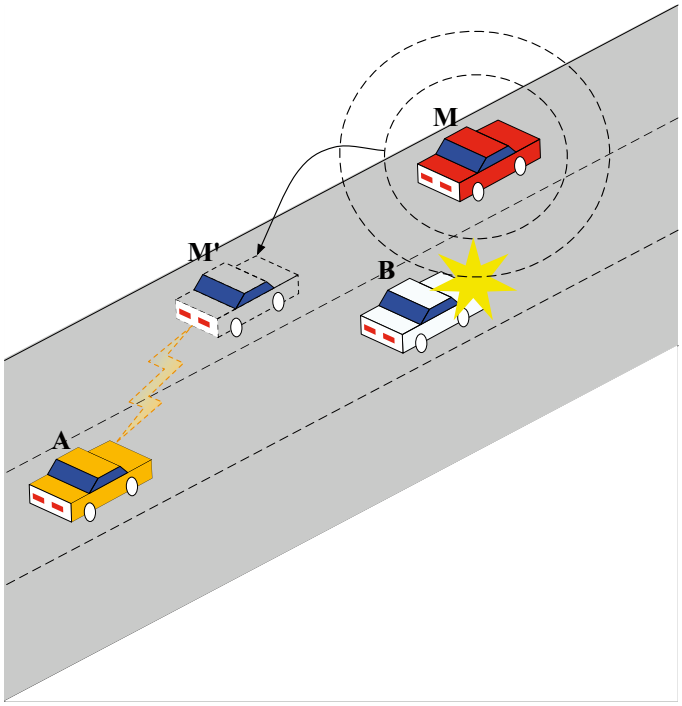

Figure 2-4. Attaque du véhicule caché

2. *Tunnel* : Comme le signal GPS connaît des pertes (dans un tunnel ou dans certaines zones perturbatrices), un attaquant peut exploiter cette perte de positionnement temporaire. En effet, il peut envoyer de fausses données dès la sortie du « tunnel » avant que le véhicule victime ne reçoive une mise à jour de position authentique.

3. *Wormhole* : Un attaquant qui contrôle plusieurs entités éloignées, peut établir un tunnel entre ces entités et peut ainsi injecter des données d'un endroit à l'autre. Il diffuse ainsi des informations erronées (mais signées) à divers endroits. C'est un exemple d'attaque *Étendue*.

2.2 Services de sécurité et mécanismes

À partir des types d'attaque possible, les réseaux sans fil véhiculaires doivent déployer des services de sécurité tels que la confidentialité, l'authenticité, l'intégrité, la non-répudiation, la disponibilité, le respect de la vie privée et le contrôle d'accès. Avant de détailler ces services et leurs mécanismes associés, nous définissons les termes suivants :

- Attaque de sécurité : Action compromettant la sécurité de l'information possédée par une organisation ou une entité.

- Mécanisme de sécurité : Mécanisme conçu pour détecter, prévenir ou contrer une attaque de sécurité.

- Service de sécurité : Service améliorant la sécurité des systèmes informatiques et des transferts d'information d'une organisation. Ces services sont conçus pour contrer les attaques de sécurité, et ils utilisent un ou plusieurs mécanismes de sécurité.

Nous classons les services de sécurité selon deux catégories : proactifs et réactifs. L'approche proactive vise à accroître la sécurité en appliquant des mécanismes préventifs. L'approche réactive détecte et réagit aux attaques. Le but des approches réactives est de compenser les faiblesses des approches proactives. La Figure 2-5 illustre des mécanismes de sécurité associés à ces deux approches. Nous les détaillons dans la section suivante.

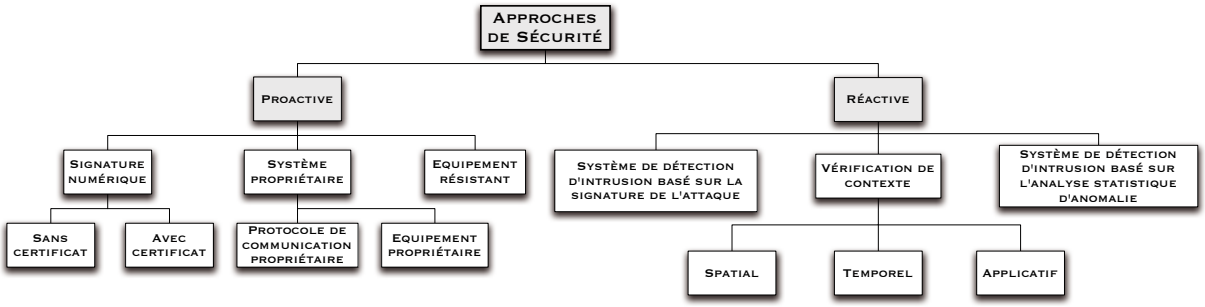

Figure 2-5. Mécanismes de sécurité

2.2.1 Confidentialité

La confidentialité est le fait d'assurer que l'information n'est accessible qu'aux entités qui y sont autorisées. La confidentialité est donc la protection des données transmises contre les attaques passives (écoute clandestine). Deux niveaux de protection sont identifiables :

- le service global qui protège toutes les données transmises entre deux utilisateurs pendant une période donnée (par l'établissement d'un circuit virtuel par exemple) ;

- le service plus restreint qui protège un message par l'ajout de champ(s) spécifique(s) à l'intérieur de ce message.

Les applications de sécurité du trafic routier ne peuvent atteindre leurs objectifs que si le maximum (si ce n'est la totalité) de véhicules coopère étroitement à leur mise en œuvre. Dans ce contexte, il n'est donc pas question de discriminer l'accès aux informations diffusées dans le réseau suivant que le véhicule est authentifié ou non. Dans les applications de sécurité du trafic routier, le principe de confidentialité serait en effet contre-productif dans la mesure où les véhicules non authentifiés (et donc ne pouvant déchiffrer ces services) feraient courir, du fait de leur non-information, un risque important d'accident aux véhicules authentifiés (qui eux, peuvent déchiffrer ces services). À la différence des applications de confort qui ont généralement une vocation commerciale et peuvent, de ce fait, appliquer la confidentialité pour assurer l'accès discriminé aux services, les applications de sécurité du trafic routier doivent impérativement être accessibles à tous les véhicules du réseau, qu'ils soient authentifiés ou non; et ce, dans l'intérêt de la sécurité de tous.

Afin d'assurer ce service, le mécanisme proactif utilisé est le chiffrement des données. Le chiffrement peut être réalisé par la cryptographie symétrique ou asymétrique. Dans le cas de la cryptographie symétrique, les parties prenantes doivent partager une clé secrète. Le chiffrement et le déchiffrement sont alors réalisés avec cette clé. Le standard IEEE 1609.2 utilise le chiffrement *Advanced Encryption Standard in CCM mode* (AES-CCM [DAE 02]) comme algorithme de cryptographie symétrique. Un des problèmes majeurs de la cryptographie symétrique est l'établissement d'un canal sécurisé pour la distribution de la clé privée.

Le standard IEEE 1609.2 utilise la cryptographie asymétrique pour l'échange de la clé secrète grâce à l'algorithme de chiffrement *Elliptic Curve Integrated Encryption Scheme* (ECIES) [CER 00-2]. Dans le cas de la cryptographie asymétrique, chaque véhicule a une paire de clés : publique/privée. La clé privée n'est connue que du véhicule émetteur, tandis que la clé publique est partagée avec toutes les entités du réseau.

2.2.2 Authenticité

L'authenticité est le service de sécurité primordial pour un fonctionnement sécurisé des VANETs. En effet, toutes les applications déployées dans les VANETs ont besoin d'avoir confiance en l'information. Cette confiance est assurée par l'authenticité. Par exemple, dans le cas d'un message (tel un signal d'alerte), la fonction du service d'authenticité est d'assurer au destinataire que le message a bien pour origine la source dont il prétend être issu. L'authenticité est assurée par des mécanismes proactifs d'authentification. Il existe deux types d'authentification : l'authentification des messages et l'authentification des entités (identification).

Une des principales particularités, dans le contexte d'opération des applications de sécurité du trafic routier, réside dans l'obligation pour toute entité générant et diffusant des messages d'alerte ou de contrôle (WSMs), d'y adjoindre une preuve d'authenticité (par exemple une signature). Cette restriction est faite pour éviter que des entités malveillantes ou non authentifiées ne puissent générer et diffuser des WSMs sans qu'il soit possible d'en vérifier l'authenticité.

Une première approche de mise en œuvre de l'authentification consiste à utiliser des clés de groupe symétriques (en anglais, *symmetric group keys*). Cette approche ne peut malheureusement concerner qu'un très petit nombre de véhicules placés sous la même autorité. Pour des déploiements à grande échelle, cette approche présente deux inconvénients majeurs:

- il suffit de compromettre un véhicule pour compromettre la sécurité de tout le réseau,
- les véhicules ayant la clé peuvent se faire passer les uns pour les autres. Ce qui empêche toute confidentialité et non-répudiation.

Une deuxième approche d'authentification consiste à utiliser des clés symétriques individuelles (en anglais, *symmetric pairwise keys*). Cette approche souffre d'une mise à l'échelle intrinsèquement difficile puisque le nombre de clés à gérer augmente de manière linéaire avec le nombre de véhicules du réseau.

Reste donc la cryptographie à clé publique qui, dans le contexte des réseaux véhiculaires, est la seule à pouvoir permettre la réalisation de l'authentification tout en satisfaisant les exigences de mise à l'échelle, de non-répudiation et de confidentialité. Ainsi, chaque véhicule se voit assigner une paire de clés publique/privée. Chaque véhicule va signer numériquement ses messages et sera ainsi authentifié auprès des récepteurs. Néanmoins, les clés publiques doivent être délivrées et signées par une autorité de confiance [RAY 07]. Comme illustrée par la Figure 2-6, la signature numérique peut être délivrée avec ou sans certificat :

- *Sans certificat* : La signature numérique est un concept basé sur l'application de signature numérique ou de fonction de hachage des messages. Ce concept assure l'authenticité, l'intégrité et la non-répudiation du message. La signature numérique est communément réalisée par le biais de la cryptographie asymétrique. Le message est signé avec la clé privée de l'émetteur, tandis que le récepteur vérifiera l'intégrité et l'authenticité du message en utilisant la clé publique correspondante à l'émetteur. Si l'on suppose que la clé privée n'est connue que de son possesseur, alors un véhicule ne pourra pas usurper l'identité d'un autre véhicule. Mais si l'émetteur utilise la même clé pour signer plusieurs messages, alors le récepteur peut lier ces messages à un seul émetteur. D'un côté, cela soulève un problème de vie privée, mais de l'autre cela réduit le coût de vérification des signatures. En effet, si le délai entre les deux messages est faible, alors le véhicule récepteur peut éviter de revérifier la signature. L'avantage de la signature sans certificat est qu'elle nécessite peu de prérequis. En effet, les véhicules doivent pouvoir recevoir et stocker les paires de clés, et ils doivent avoir la puissance de calcul nécessaire pour créer et vérifier des signatures. C'est pourquoi ce concept est facilement déployable. L'inconvénient est qu'il ne protège pas des attaques de création de messages, de déni de service ou de réplication (« *Sybil attack*»).

- *Avec certificat* : Afin d'améliorer le concept de signature numérique, les signatures peuvent être combinées avec un certificat numérique délivré par un tiers de confiance. Ainsi, le récepteur d'un message pourra s'assurer que l'émetteur a bien utilisé sa clé privée pour signer le message. L'hypothèse de base avec les certificats est que les véhicules doivent être capables de vérifier les certificats, car le certificat atteste l'authenticité de la paire de clés publique/privée. Avec la solution des infrastructures à clé publique auto-organisées (*Public Key Infrastructure*, PKI), un véhicule doit signer le message avec sa clé privée et inclure le certificat de l'autorité de certification (*Certification Authority*, CA) :

  $$V \rightarrow * : M, Sig_{\Pr K_V}[M \mid T], Cert_V$$

  où V désigne le véhicule émetteur, * représente tous les récepteurs du message M, | est l'opérateur de concaténation, et T est l'horodatage qui assure la fraîcheur du message. La signature numérique $Sig_{\Pr K_V}[M \mid T]$ assure l'authentification, l'intégrité et la non-répudiation. $Cert_V$ est le certificat associé à la clé publique de V délivrée par le CA. Le récepteur du message doit vérifier la clé publique de V à partir du certificat et vérifie ensuite la signature numérique de V à partir de la clé publique (certifiée). Afin de réaliser ces opérations, le récepteur doit avoir préalablement la clé publique du CA.

Un avantage du certificat est qu'il peut empêcher, ou du moins réduire, l'attaque de réplication de nœud. Bien sûr, dans ce cas, il faut supposer qu'un véhicule ne peut utiliser qu'un seul certificat à la fois. Pour délivrer des certificats, il est nécessaire d'avoir un système de gestion et de distribution des certificats. De plus, les véhicules doivent pouvoir avoir accès à ce système de manière permanente, sporadique ou une seule fois (durant la construction du véhicule par exemple). La fréquence d'accès dépend de la conception des VANETs. Plus la fréquence d'accès est élevée, plus le système sera flexible.

Le concept de signature avec certificat permet donc de se protéger des attaques externes comme l'injection de fausses alertes par un utilisateur non authentifié. De plus, les véhicules qui ne se comportent pas bien peuvent être identifiés puis révoqués. Le certificat joue aussi un rôle de contrôle d'accès. Par exemple, seuls les messages accompagnés du certificat valide seront écoutés. La révocation s'effectue par l'ajout du certificat dans une liste des certificats révoqués (*Certificate Revocation List*, CRL). Les inconvénients d'un tel système sont la nécessité d'une infrastructure, et que malgré l'ajout de certificats, le réseau n'est toujours pas protégé des attaques d'injection par des utilisateurs authentifiés.

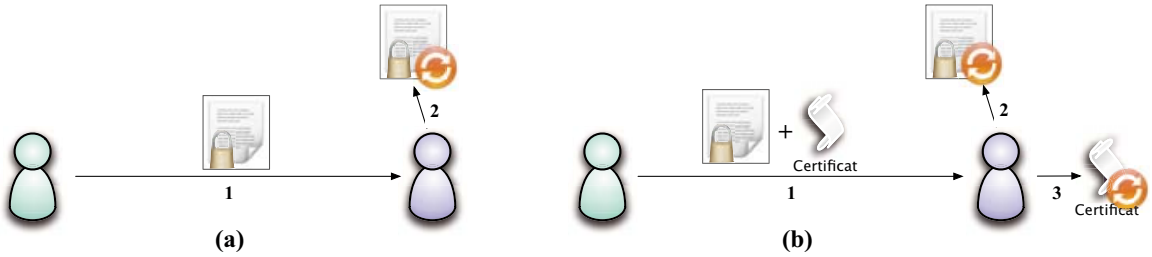

Figure 2-6. Signature numérique : (a) sans certificat ; (b) avec certificat

2.2.3 Intégrité

L'intégrité se divise en deux concepts : l'intégrité des messages et l'intégrité physique :

- Intégrité des messages : Fonction permettant d'assurer que l'information n'a pas subi d'altération.
- Intégrité physique : Fonction permettant d'assurer que le matériel (destiné aux opérations cryptographiques, à l'envoi de messages, à la collecte d'informations, etc.) n'a pas subi d'altération.

Le service d'intégrité des messages assure que les messages envoyés sont rapidement reçus, sans duplication, insertion, modification, réorganisation ou répétition. À l'instar de la confidentialité, l'intégrité s'applique à un flux de messages, un seul message, ou à certains champs à l'intérieur d'un message. Là encore, la meilleure solution est la protection totale du flux.

Les mécanismes proactifs utilisés pour assurer l'intégrité des messages sont les chaînes de hachage (SHA1 [NIS 02], MD5 [RIV 92]), et le *Message Authentication Code* (MAC) [ISO 99]. Ces mécanismes s'appuient sur des fonctions mathématiques à sens unique. Ces fonctions dépendent d'une clé secrète, et produisent un condensé du message original. Ces fonctions mathématiques sont telles

qu'il est difficile de retrouver un message à partir de son condensé ou de produire deux messages ayant le même condensé. De plus, la moindre modification du message original entraine un changement dans le condensé.

Pour assurer l'intégrité physique, les véhicules doivent être équipés d'un équipement robuste dit *Tamper Proof Device* (TPD). Le TPD est un équipement résistant au sabotage (ou manipulation). Un TPD peut se décliner de plusieurs façons : accès difficile aux composants ou auto-destruction. Son premier objectif est de sécuriser les communications internes aux véhicules en empêchant la récupération de données de capteurs par exemple. Son deuxième objectif est de participer à la sécurisation des communications externes. En effet, cet équipement peut abriter les paires de clés et les certificats, ainsi qu'une boite noire (pour permettre la reconstitution de scénarii d'accidents par exemple). Mais cet équipement n'est pas, à lui seul, capable de sécuriser les communications externes. On peut donc envisager une combinaison de messages signés avec certificat et un TPD. Néanmoins, la manipulation des capteurs n'est toujours pas protégée, car un attaquant peut mettre une lampe chauffante à proximité d'un capteur de température par exemple.

2.2.4 Non-répudiation

En raison de l'impact que peuvent avoir les applications de sécurité routière sur la sécurité des biens et des personnes, il est indispensable que toute entité générant ou modifiant des messages d'alerte soit toujours identifiable avec certitude. En d'autres termes, toute entité, après avoir émis un message, ne doit pas pouvoir ensuite nier cette action. Assurer la non-répudiation pour les applications de sécurité routière va donc éliminer toute possibilité, pour une entité malveillante d'injecter des informations erronées, et ce sans être confondue.

S'agissant de la mise en œuvre de la non-répudiation, la signature numérique, qui est majoritairement utilisée pour réaliser l'authentification entre des parties étrangères sans qu'il soit besoin de recourir à une entité de confiance en ligne, peut aussi la garantir. Pour ce faire, une signature doit être systématiquement ajoutée aux messages générés ou modifiés. À la différence des applications de sécurité routière qui se distinguent par une exigence forte de non-répudiation, les applications de confort peuvent s'en passer dans la plupart des cas; à l'exception notable de certaines applications sensibles comme celles impliquant des transactions financières.

2.2.5 Disponibilité

L'objectif de la disponibilité est de garantir un accès permanent à un service ou à des ressources. De nombreuses attaques peuvent entraîner une perte ou une réduction de la disponibilité du réseau ou d'un service applicatif. Il n'existe aucun moyen de contrer un déni de service sur le canal radio provoqué par un attaquant ayant les moyens de brouiller efficacement la totalité du spectre radio. Néanmoins, des techniques proactives comme le saut de fréquence [RAY 07], le changement de canal (parmi les sept à disposition dans DSRC), ou bien le changement de technologie (DSRC, Ultra-TDD, etc.) [RAY 05], permettent de se prémunir contre des attaquants ayant des capacités plus réduites. En effet, pour être efficace, un attaquant devra être capable de brouiller l'étendue des fréquences utilisées.

2.2.6 Vie privée

De nombreuses opérations présentent des risques d'atteinte à la vie privée, comme le péage automatique ou la reconnaissance automatique des plaques d'immatriculation. De plus, les véhicules diffusent leurs positions de manière régulière ou en cas d'accident. Certaines applications peuvent nécessiter la discrétion sur l'identité des participants qui collaborent : par exemple l'échange d'itinéraire entre deux véhicules de transport de fonds. De plus, les équipements embarqués auront en toute probabilité, la possibilité de garder la trace des préférences des utilisateurs afin de faciliter leur quotidien et d'offrir des services plus personnalisés. Cette tendance va pourtant à l'encontre de la protection de la vie privée de tout un chacun. La protection de la vie privée est donc obligatoire pour permettre l'acceptation des VANETs par les utilisateurs.

La vie privée est un service primordial pour les VANETs. Ces diffusions sont signées avec des clés assignées à chaque véhicule, et accompagnées d'un certificat (ou d'une chaîne de certificat ou d'un condensé) afin d'attester la validité de la clé. Chaque véhicule diffuse aussi régulièrement son certificat. Avec cette redondance d'information, un attaquant peut suivre les déplacements et les communications d'un véhicule. Nous définissons la vie privée comme l'impossibilité de lier une signature numérique à un véhicule ou groupe de véhicules.

Les mécanismes proactifs qui peuvent assurer le service de vie privée sont les pseudonymes, le changement fréquent de clé ou de certificat. Dans [HUA 05], les auteurs proposent le système CARAVAN qui empêche l'utilisation des informations de position et de vitesse communiquées pour traquer un véhicule. Pour ce faire, ils proposent deux solutions : (i) changement fréquent du pseudonyme du véhicule après une période aléatoire de silence, et (ii) la formation de groupes dynamiques de véhicules afin de favoriser l'anonymat. Le véhicule serait donc un membre de groupe dont le chef représente une interface (proxy) avec l'extérieur et qui donne des informations générales sur le groupe. Dans le même esprit, [BER 03] propose un mécanisme dans lequel plusieurs véhicules changent de pseudonymes en même temps pour empêcher tout suivi des véhicules.

2.2.7 Contrôle d'accès

Le contrôle d'accès réseau permet de définir les entités autorisées à se connecter à un réseau en bloquant les utilisateurs non autorisés, en contrôlant l'accès des invités et en garantissant que les utilisateurs se conforment aux politiques de sécurité du réseau. Ce service est nécessaire pour les applications qui distinguent différents niveaux d'accès en fonction de l'entité. Par exemple, l'application de contrôle des feux tricolores autorise seulement les véhicules de secours ou de police à échanger des informations avec les feux tricolores pour faciliter leur déplacement.

Ce service est établi grâce à des politiques d'accès qui spécifient ce que chaque entité est autorisée à faire ou à accéder, dans le réseau. Par exemple, un garage agréé peut être autorisé à accéder pleinement à des diagnostics sans fil, tandis que les autres n'auront qu'un accès limité.

Une autre forme de contrôle d'accès est l'exclusion des véhicules ayant un comportement anormal par rapport au service attendu. Par exemple, un véhicule qui ne respecte pas la fréquence d'envoi des beacons doit être exclu afin de préserver les performances réseau. Un système de détection d'intrusion utilisant une gestion de confiance (système de crédit) ou la révocation de certificat assure ce type de contrôle d'accès. Détaillons le mécanisme réactif de détection d'intrusion qui vise à assurer le respect ou la détection de violation des politiques d'accès. Le système de détection d'intrusion compare les informations reçues à un catalogue de scénarii (répertoriant les situations « normales »). Il existe deux méthodes de détection d'intrusion :

- *Détection basée sur la signature* : Dans cette méthode, le trafic réseau est comparé aux signatures d'attaques connues. Dès qu'une attaque est détectée, alors la contre-mesure adéquate est lancée. Le premier prérequis est la définition des signatures d'attaques. Le second est la capacité d'enregistrement et de mise à jour des signatures d'attaques. Bien entendu, ce type de détection est limité, car seul le trafic réseau est analysé et le contenu applicatif ne l'est pas. Mais le problème principal est la non-prédictibilité des situations possibles dans un VANET. Le système de détection d'intrusion est aussi limité par la taille du « catalogue » et sa faible réactivité face aux nouvelles attaques.

- *Détection basée sur l'anomalie statistique* : La détection basée sur l'anomalie statistique est basée sur l'hypothèse qu'il y a une définition du comportement normal du système de communication. Les déviations de ce système sont statistiquement analysées et lorsqu'un seuil est atteint, alors le système de sécurité en conclut qu'une attaque est en cours. Là encore, ce concept est limité, car seul le trafic réseau est analysé. L'avantage est qu'il n'a pas besoin d'une base de données des attaques. Il n'y a donc pas de problème de mise à jour. Mais le principal problème réside dans la définition du comportement « normal », sachant qu'un VANET propose de nombreuses conditions « normales ».

Un autre concept réactif pour le contrôle d'accès et l'exclusion de véhicules malveillants est la « vérification de plausibilité » ou « vérification de contexte ». Dans les applications de sécurité du trafic routier, les mécanismes de sécurité doivent détecter les fausses informations et les inconsistances du système. Ainsi, lors de réception d'un message, un véhicule évalue la validité de l'alerte avant de réagir. Le principe est que chaque véhicule collecte des informations de différentes sources pour créer une « vue courante » de son environnement. Les sources d'informations sont les messages d'alerte, les données des capteurs, etc. Ainsi, lorsqu'un véhicule reçoit une alerte de danger local, il peut comparer les informations (localisation, direction, etc.) avec sa « vue courante ». Pour pouvoir effectuer cette comparaison, le véhicule doit être équipé d'un ensemble de règles qui détermine « à quoi l'on peut s'attendre, dans quelle probabilité, dans quelle situation ». Il est évident que cette comparaison doit être faite en temps réel, sans quoi, l'alerte deviendra inutile. Mais le mécanisme de vérification de plausibilité peut aussi être indépendant de l'application. Par exemple, la vérification des messages de contrôle (beacon) peut être utilisée pour détecter la présence de « *sybil attack* ». Un exemple de vérification dépendante de l'application est la réception d'un message d'alerte concernant un embouteillage. Dans cet exemple, une vérification serait de s'assurer que le message ne vienne pas d'un véhicule éloigné du « soi-disant » lieu d'embouteillage.

Il existe trois types de vérification :

- *Vérification spatiale* : Elle vise à empêcher un nœud malicieux (ou défaillant) de mentir sur sa position, car les applications de sécurité routière et le routage dépendent de la fiabilité de l'information de position. La vérification de position contribue aussi à la surveillance du voisinage afin de détecter des situations inhabituelles (véhicules à la même position, etc.).

- *Vérification temporelle* : L'objectif principal de la vérification temporelle est de détecter le rejeu de messages. La différence entre la date de création du message et la date de réception permet de donner un ordre d'idée de l'âge du message. En fonction du résultat, le message peut être rejeté, car trop ancien.

- *Vérification du contexte applicatif* : Chaque application a un ensemble de contraintes. Par exemple, une application d'alerte de danger local ne génère des messages que dans des situations dangereuses. Si ce n'est pas le cas, alors le véhicule rejette la pseudo-alerte. Un exemple de scénario est lorsqu'un véhicule reçoit une alerte de verglas alors que le capteur de température extérieure du véhicule indique +20°C. L'ensemble de contraintes définit qu'il y a un risque de verglas lorsque la température est inférieure à +5°C. Donc dans ce cas, le système doit décider de croire, soit son capteur interne, soit la valeur obtenue par le système de communication. Le véhicule pourra valider l'information en corroborant avec le capteur ABS ou ESP par exemple. Si l'un des capteurs a dû intervenir récemment, cela peut indiquer que le capteur de température est défectueux et que l'alerte est bien valide.

2.2.8 Discussion

Coopérer au sein de réseaux ad hoc véhiculaires présente un risque s'il n'y a aucun contrôle des participants. L'authentification des parties apparaît comme la pierre angulaire d'un réseau ad hoc véhiculaire sécurisé. En effet, comment assurer une quelconque confidentialité et intégrité des messages échangés si, dès le départ, les véhicules ne sont pas sûrs de communiquer avec la bonne entité ?

Nous présentons le Tableau 2-1 et le Tableau 2-2 qui mettent en adéquations les applications, les services de sécurité, les attaques et les mécanismes de sécurité.

Applications		Services de sécurité						
		Confidentialité	Authenticité	Intégrité	Non-répudiation	Disponibilité	Contrôle d'accès	Respect de la vie privée
Sécurité du trafic routier	Alerte post-accident	0	2	2	1	2	0	2
	Alerte coopérative de collision	0	2	2	2	2	0	2
	Freinage d'urgence (feux électroniques)	0	2	2	2	2	0	2
	Alerte angle mort	0	2	2	2	2	0	2
	Alerte véhicule à contre sens	0	2	2	2	2	0	2
Gestion du trafic routier	Train de véhicules	0	2	2	2	1	2	2
	Gestion de trafic intelligent	0	2	1	0	0	0	2
Confort	Messagerie instantanée (V2V)	2	2	2	0	0	0	1
	Paiement électronique	2	2	2	2	1	2	1

Tableau 2-1. Adéquation application/service de sécurité (0 = non pertinent ; 1 = important ; 2 = très important)

Le Tableau 2-1 se base sur le rapport du projet SeVeCom [KRO 06] et détaille l'importance de chaque service de sécurité dans le déploiement d'applications. Nous précisons que le contrôle d'accès signifie ici l'autorisation d'accès à l'application. Les mécanismes de vérification de contexte sont inclus dans le service d'intégrité.

Dans le contexte d'application de sécurité du trafic routier, l'authenticité est le service « très important », suivi (par ordre d'importance décroissante d'après le Tableau 2-1) de l'intégrité, la disponibilité, la vie privée, la non-répudiation, le contrôle d'accès et la confidentialité. Comme évoqué précédemment, cette catégorie d'applications a pour vocation d'informer les véhicules présents dans une zone donnée (proche d'un accident par exemple). La confidentialité n'est donc pas pertinente. Cependant, pour des raisons de responsabilité civile notamment, il est important d'assurer la non-répudiation. En effet, un véhicule provoquant un accident ne doit pas pouvoir s'en décharger. Dans toutes les applications d'alerte, l'authenticité est mentionnée comme « très importante ». Chaque véhicule doit être assuré que l'alerte est émise par un véhicule réel, authentique (l'émetteur a le droit d'envoyer cette alerte), intègre (l'information ne doit pas être modifiée par les véhicules intermédiaires)

et ce tout en assurant une garantie de la vie privée (les véhicules ne doivent pas savoir le modèle exact du véhicule accidenté par exemple).

Dans le contexte d'application de gestion du trafic routier, l'authenticité et le respect de la vie privée tiennent le haut du classement, suivi de l'intégrité, du contrôle d'accès, de la non-répudiation, de la disponibilité et de la confidentialité. Dans cette catégorie d'applications, les véhicules participent à l'amélioration du trafic routier. Par exemple, dans l'application de gestion de trafic intelligent, grâce à l'information microscopique récoltée par chaque véhicule, une cartographie du trafic routier est créée. Il est donc nécessaire d'assurer le respect de la vie privée aux véhicules qui participent à cette application. Dans l'application de train de véhicule (aussi appellée « *platooning* »), il est nécessaire d'assurer un contrôle d'accès. En effet, à long terme nous pouvons imaginer que les autoroutes auront une voie spécifique pour le *platooning*. Mais afin de garantir un niveau de sécurité routière, il est nécessaire d'avoir des véhicules avec une capacité de freinage homogène. C'est pourquoi cette voie ne sera autorisée qu'aux véhicules légers d'un certain type (année de fabrication inférieure à 7 ans par exemple).

Dans le contexte d'application de confort, l'authenticité, la confidentialité et l'intégrité sont les plus importants, suivi du contrôle d'accès, de la non-répudiation, de la vie privée et de la disponibilité. Cela s'explique par la nature même des applications de confort. En effet, il s'agit en général d'applications à but personnel. Par exemple, les informations échangées lors de messagerie instantanée entre deux véhicules sont personnelles et doivent donc être confidentielles. De la même manière, le paiement électronique (télépéage, vidéo à la demande, carburant, etc.) a un but personnel (utile seulement pour un véhicule) et doit être confidentiel, authentifié (c'est bien le bénéficiaire de la carte bleue qui paye par exemple), intègre (le montant prélevé ne doit pas être modifié).

Nous remarquons que, quelle que soit la catégorie d'applications, le service d'authenticité est « très important » dans le déploiement d'applications dans les VANETs.

Attaque / Service	Profilage	Cohérence des données	Usurpation d'identité	DoS	Écoute clandestine	Injection de fausses données
Confidentialité	Chiffrement	n/a	Chiffrement	n/a	Chiffrement	n/a
Authenticité	n/a	Identification et signature des nœuds intermédiaires et de l'émetteur	- Identification - Signature de l'émetteur	n/a	Identification et signature des nœuds intermédiaires et du récepteur	- Identification - Signature de l'émetteur
Intégrité	n/a	- Hachage - TPD	n/a	TPD	n/a	- Attestation des données capteur - Hachage
Non-répudiation	n/a	- Signature - Certificat	- Signature - Certificat	n/a	n/a	- Signature - Certificat
Disponibilité	n/a	n/a	n/a	Saut de fréquence	n/a	n/a
Contrôle d'accès	n/a	- Vérification de plausibilité - IDS	Vérification de plausibilité	- Politique d'accès (groupe d'utilisateur) - Filtrage	Politique d'accès (groupe d'utilisateur)	- Vérification de plausibilité - IDS
Respect de la vie privée	- Pseudonymes - Changement fréquent de clé/certificat	n/a	n/a	n/a	- Pseudonymes - Changement fréquent de clé/certificat	n/a

Tableau 2-2. Mécanisme(s) de sécurité pour assurer un service spécifique en cas d'attaque spécifique

Le Tableau 2-2 décrit les mécanismes employés par les services de sécurité afin de se protéger ou de se prémunir des attaques identifiées en section 2.1. Contrairement au Tableau 2-1, le service de contrôle d'accès contient les mécanismes de vérification de plausibilité. Nous remarquons alors l'importance de ce service dans les réponses aux attaques.

La mention « n/a » signifie que le service n'est pas concerné par l'attaque et qu'aucun mécanisme de sécurité n'est donc pertinent. Par exemple, l'attaque passive d'écoute clandestine ne met pas en danger l'intégrité des données transmises, un mécanisme d'intégrité n'est donc pas pertinent.

Le Tableau 2-2 souligne la difficulté à assurer le service de disponibilité dans les réseaux sans fil ad hoc véhiculaires. En effet, étant donné les contraintes de topologie dynamique, de perturbation de signal, qui pèsent sur ces réseaux, peu de solutions existent. La vie privée est aussi difficile à gérer car parfois en contradiction avec la non-répudiation et soulève des questions juridiques.

Nous remarquons aussi que les mécanismes d'authenticité interviennent dans une majorité d'attaques, mais ne suffisent pas à contrer les attaques. Ainsi, aucun des mécanismes de sécurité ne suffit à lui seul. Leur complémentarité est essentielle pour atteindre un niveau de sécurité répondant aux problématiques que nous venons d'exposer.

2.3 Sécurité de l'application d'alerte de danger local

L'application d'alerte de danger local (LDW) base ses alertes sur les informations collectées par les capteurs locaux à chaque véhicule. Un véhicule pourra ainsi alerter d'un danger (obstacle, accident, etc.).

La sécurité d'un tel système est primordiale, car une information erronée ou falsifiée peut entraîner une dégradation de la sécurité routière. Dans un système hautement dynamique, à forte densité de véhicules, comme les réseaux véhiculaires, les mécanismes de sécurité conventionnels comme la signature numérique et l'équipement robuste ne sont pas suffisants. En effet, ces mécanismes visent à assurer qu'un attaquant ne puisse manipuler le réseau ou une partie du véhicule. Ces protections n'étant pas infaillibles, il existe toujours une possibilité de manipulation. Comme les alertes sont générées à partir de la lecture des capteurs locaux, un attaquant peut détourner le processus de détection en altérant l'environnement physique du capteur. Ainsi, une fausse alerte peut être générée et diffusée. Les protections cryptographiques ne vérifient pas la sémantique de l'information. Une manipulation d'un capteur peut donc entraîner une alerte parfaitement signée et certifiée. C'est pourquoi une approche de vérification de plausibilité de l'information est proposée.

Le mécanisme de vérification de plausibilité peut intervenir à deux niveaux :

- durant le processus de détection (en vérifiant la plausibilité de l'information lue par le capteur)
- durant le processus de décision (en évaluant la plausibilité de l'information reçue)

Si l'attaquant contrôle l'ensemble du véhicule, alors le processus de détection est inutile. Cette solution semble toutefois plus intéressante pour détecter les défaillances matérielles. En effet, supposons qu'un véhicule équipé de trois capteurs de température extérieure reçoit les valeurs +30°C, +29°C, 0°C. Le véhicule détectera, par le biais d'un mécanisme de vote majoritaire, que le capteur n°3 est défaillant et ne l'utilisera plus jusqu'à la prochaine révision du véhicule.

Le processus de détection est aussi intéressant pour déceler la manipulation partielle du véhicule. Si l'OBU détecte l'envoi d'un message indiquant une vitesse nulle et que les capteurs des roues et de vitesse annoncent une vitesse différente d'au moins 2 km/h (chaque équipement admet une incertitude relative qui lui est propre), alors le véhicule aura une suspicion de manipulation malveillante et décidera d'envoyer ou non le message concerné.

Comme notre contexte considère le pire cas où l'attaquant a le contrôle total du véhicule, nous nous intéressons au deuxième niveau qu'est le processus de décision. Cette solution permet d'évaluer la plausibilité de l'information en recoupant l'information avec de multiples sources (voisinage, réputation, capteurs, etc.). Par exemple, sur une route à deux voies à double sens, un véhicule reçoit une alerte indiquant une route barrée. Si le véhicule capte dans son voisinage un autre véhicule arrivant dans le sens opposé et qu'il ne détecte pas de freinage devant lui, alors il mettra en doute l'alerte. Notre but est donc de protéger le processus de décision contre les attaques, notamment l'injection de fausses informations qui peut avoir de graves conséquences.

2.3.1.1 Modèles d'attaque

Lors du déploiement de l'application LDW, il existe quatre menaces au niveau applicatif.

1. *Interférence du trafic routier* : L'application influence le comportement routier et peut être détournée pour entraîner des situations potentiellement accidentogènes. Par exemple, un message d'alerte peut être émis pour dévier le trafic et créer ainsi des embouteillages.

2. *Subversion de la responsabilité* : Lors d'un accident, un attaquant peut vouloir porter de fausses accusations contre un usager de la route ou permettre aux autres attaquants de rester non identifiés.

3. *Dépréciation de la vie privée* : À partir des informations de vitesse et de temps contenues dans un message d'alerte, un attaquant peut générer un profil de déplacement. Il pourra alors revendre l'information ou l'utiliser à des fins malveillantes. Un attaquant pourra par exemple traquer les déplacements d'un convoyeur de fonds afin de lui tendre un piège.

4. *Contrôle à distance de véhicule* : À long terme, on peut supposer une automatisation de la conduite. C'est pourquoi en exploitant les vulnérabilités existantes, il sera possible de prendre le contrôle à distance d'un véhicule. Cela est théoriquement possible, car l'application LDW est connectée au bus électronique interne (pour avoir accès aux lectures des capteurs) et à l'interface sans fil du véhicule.

Nous nous intéressons plus particulièrement à la première menace, car elle peut avoir de graves conséquences sur la sécurité routière. Dans ce type de menace, l'attaque la plus fréquente est

l'injection de fausse alerte (*fake attack*). Il s'agit d'une attaque visant à générer de fausses alertes afin que l'OBU ou le conducteur (selon si le système est automatique ou non) prenne de mauvaises décisions. Tout comme l'attaque de déni de service, l'objectif de cette attaque peut être de créer un accident. La seule différence avec le DoS est le moyen mis en place pour atteindre cet objectif. Dans l'attaque de fausse alerte (cf. Figure 2-7), le véhicule M réfute l'alerte envoyée par B. Sans aucun autre mécanisme de sécurité, le véhicule A fera confiance en M et percutera B (notamment lors de conditions climatiques difficiles). Il est donc nécessaire de vérifier l'information reçue.

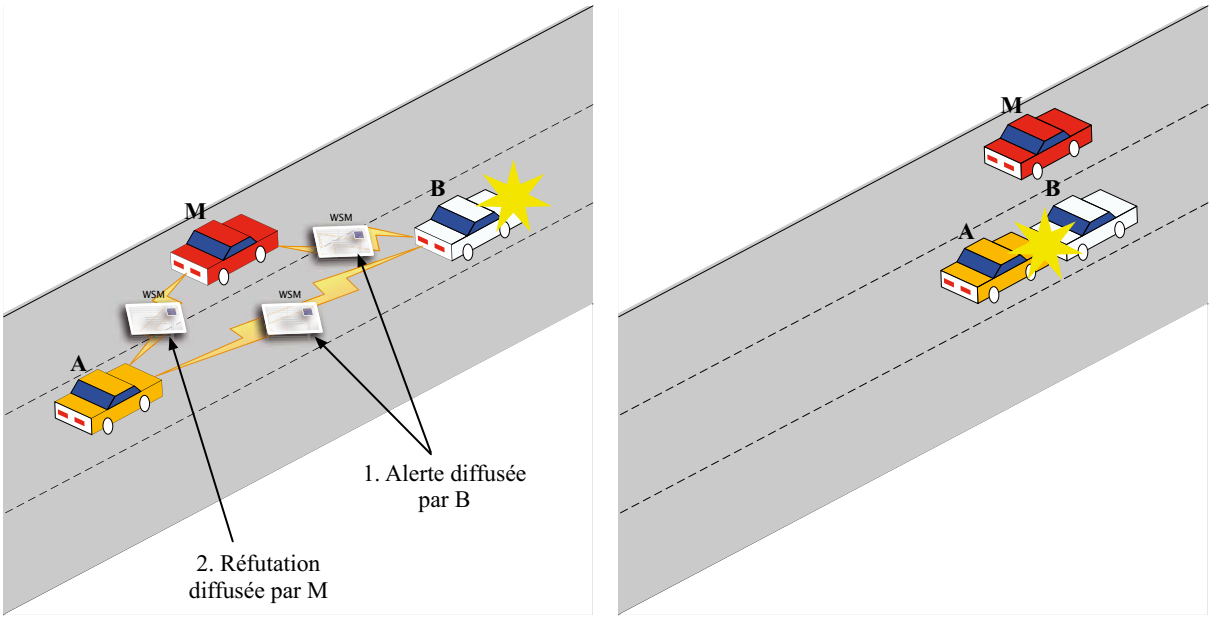

Figure 2-7. Attaque d'injection de fausses informations

2.3.1.2 Mécanismes de sécurité et adéquation au V2V

Dans [GER 06], Gerlach introduit la notion de confiance dans les communications V2V. Cette confiance est établie avec un véhicule sur trois niveaux :

(i) un certificat qui permet la vérification de l'identité du véhicule ;

(ii) un système qui donne un taux de crédibilité des informations en provenance du véhicule suivant l'historique de sa contribution au réseau (système de réputation) ;

(iii) une vérification de la plausibilité au niveau de l'information communiquée et la gestion des conflits en cas de contradiction des informations.

2.3.1.2.1 Système de réputation

Il est possible de vérifier la plausibilité d'un message en adoptant un mécanisme d'écoute des messages combiné à un système de réputation [LO 09]. Un système de réputation établit des relations de confiance entre les participants de manière individuelle. Dans ce système, la décision de considérer ou non une alerte est prise selon ces relations de confiance. Ainsi, une alerte sera prise en compte seulement si l'événement a accumulé suffisamment de crédits. L'hypothèse sous-jacente d'un système

de réputation est que l'analyse du comportement des véhicules indique le degré de confiance des messages qu'ils envoient. Le « comportement » décrit toutes les informations observables d'un véhicule. Cela inclut les déplacements passés, présents, futurs, et les communications. Ces informations sont collectées grâce aux messages de contrôle (beacon). En recevant une séquence de beacons, le véhicule récepteur a suffisamment de données pour permettre une analyse significative. Le résultat de cette analyse conduit à une évaluation du comportement de chaque véhicule. Ces évaluations peuvent être partagées avec les autres véhicules du réseau. Le système de réputation est alors formé.

Ajouter la réputation d'un véhicule dans le processus d'évaluation locale peut apporter une vision plus fine de la situation courante. Mais le système de réputation doit être constamment actif. En effet, quand un message d'alerte est reçu, les contraintes temporelles ne permettent pas une analyse comportementale réactive. Le résultat de l'évaluation de l'émetteur (obligatoirement basée sur le comportement précédent) doit donc déjà être disponible lors de la réception de la prochaine alerte.

Un inconvénient de ce système est que le concept de réputation ne supporte pas le passage à l'échelle dans les réseaux véhiculaires. En effet, un système de réputation nécessite de maintenir à jour les événements et les crédits associés, et ce pour chaque véhicule. La densité des VANETs empêche donc le fonctionnement rapide et efficace d'un système de réputation. De plus, les véhicules qui n'ont jamais participé précédemment ne sont pas susceptibles d'interagir dans le futur. Cette nature transitoire restreint l'utilité des schémas basés sur la réputation. En terme de protection de la vie privée, les systèmes de réputation impliquent une forte identification. Cela vient donc en conflit avec les besoins de vie privée et d'anonymat.

2.3.1.2.2 Contrôle de plausibilité

Chaque véhicule doit vérifier la fiabilité des messages reçus. Hormis la vérification cryptographique, le véhicule doit évaluer si l'information contenue dans le message peut être correcte et réaliste. C'est dans ce but qu'a été proposé le mécanisme de vérification de plausibilité [GOL 04] [SCH 08] [LO 07]. Grâce à ce mécanisme, les véhicules examinent chaque message à partir de leur connaissance actuelle. Par exemple, si un véhicule reçoit un message d'alerte lui indiquant un embouteillage, mais que ses capteurs ne détectent aucun véhicule aux alentours, alors la confiance du message peut être réduite. Pour gérer cette confiance, il existe des techniques telles que les réseaux de neurones.

Néanmoins, cette évaluation du message reçu se fait uniquement à partir des connaissances actuelles propres au véhicule. Afin d'affiner l'évaluation, il serait intéressant de comparer le message avec la perception des autres véhicules. Raya *et al.* [RAY 07] ont proposé d'établir une valeur de confiance pour chaque message envoyé par les autres véhicules. Cette mesure est basée sur plusieurs facteurs statiques (par exemple le type de véhicule : secours, police, etc.), et plusieurs facteurs dynamiques (par exemple la proximité de l'alerte). De plus, les messages émanant de plusieurs entités et se référant au même événement sont regroupés. Ainsi, la confiance est assignée aux événements et non plus seulement aux messages. La crédibilité de l'événement doit être calculée le plus rapidement possible. Pour cela, différentes procédures de calcul sont proposées, chacune basée sur une hypothèse différente :

- Sens de circulation (annonce bidirectionnelle) : Seuls les évènements ayant été annoncés par deux véhicules roulant dans la direction opposée seront considérés. Cette méthode a l'avantage d'utiliser la nature des routes (présence de deux sens de circulation, etc.). De plus, il sera plus difficile pour un attaquant de compromettre les deux directions.

- Confiance basée sur un seuil : Un événement est jugé digne de confiance quand il a été approuvé par un certain nombre de véhicules différents. Bien qu'il serait préférable d'établir ce seuil dynamiquement, à l'heure actuelle, il n'est pas clairement spécifié comment le définir. De plus, si des pseudonymes sont employés, il sera impossible de vérifier que les approbations viennent de véhicules différents. C'est pourquoi la signature MLGS (*Message Linkable Group Signature*) [DOM 09]a été créée afin de répondre à cette problématique.

Schmidt *et al.* [SCH 08] proposent un ensemble de modules d'analyse de comportement afin d'affiner le niveau de confiance des véhicules : analyse de mouvement ; analyse de position par capteurs, radar et lidar ; analyse de la fréquence d'envoi des beacons. Dès qu'un module dépasse un seuil, le véhicule génère une recommandation (positive ou négative) concernant un véhicule. Ainsi les résultats d'analyse sont partagés avec son voisinage. Les recommandations sont ensuite utilisées dans le processus de calcul du niveau de confiance au niveau local. Les auteurs proposent aussi des systèmes d'agrégation de recommandation afin de limiter l'impact sur la bande passante. Ce système est proactif, car les véhicules effectuent une surveillance continue du voisinage. Leur système, nommé VEBAS, est une fusion entre un système de réputation et un contrôle de plausibilité.

Dans [LO 07], les auteurs proposent un contrôle local de chaque message reçu. Le modèle *Plausibility Validation Network* (PVN), vérifie cinq règles avant de considérer le message comme fiable. Il vérifie la duplication de message, la portée de diffusion du message selon le type d'événement (grâce au nombre de sauts depuis la source), la position de l'événement (en recoupant le temps et le nombre de sauts), l'horodatage et la vitesse du nœud émetteur.

Grâce à ces mécanismes de contrôle de plausibilité, les véhicules peuvent évaluer la véracité du message à partir des informations réseau (distance, nombre de sauts, vitesse).

2.3.1.2.3 Consensus

Le mécanisme de consensus vise à évaluer la confiance d'un message par le biais d'informations réseau (mécanismes de plausibilité) et du contenu du message. Le consensus ajoute donc une notion d'évaluation basée sur le contenu lui-même.

Lors de réception d'un message d'alerte, le message (son contenu, son origine, etc.) est analysé et comparé à l'évaluation du véhicule. Un véhicule peut évaluer une situation à partir des données précédemment collectées et obtenir ainsi une estimation de la situation courante. À cause de la criticité en temps du système d'alerte, cette comparaison doit être exécutée en temps réel, sinon l'information d'alerte devient obsolète et donc inutile [LEI 07]. Afin d'affiner le processus de consensus, nous utiliserons les différents modules de contrôle de plausibilité cités précédemment. Nous détaillons le problème de consensus dans le chapitre 4.

2.4 Standard de sécurité : IEEE 1609.2

Le standard IEEE 1609.2 décrit la sécurité dans les VANETs. Il définit les procédures à réaliser à chaque émission et réception de message signé ou chiffré. Il définit aussi le format des messages signés, chiffrés et des certificats.

2.4.1 Format des messages

Comme l'ajout de sécurité entraîne une augmentation de la taille du paquet envoyé, elle influe sur le délai de transfert d'un message (délai entre la génération du message et sa bonne réception). C'est pourquoi nous détaillons le format de certificat et de message signé.

2.4.1.1 Format de certificat

Un certificat est composé des champs suivants :

- *Version du certificat* : 1 octet. Marqué à « 1 » dans le standard actuel.
- *Type d'entité* : 1 octet précisant le type d'entité (OBU, RSU) propriétaire du certificat.
- *ID du signataire* : 8 octets. Condensé du certificat de l'autorité de certification qui délivre ce certificat. Ce champ sert à l'identification de l'autorité émettrice du certificat.
- *Spectre d'applications* : 12 octets. Liste des applications où le certificat est valide.
- *Expiration* : 4 octets. Temps restant (en secondes par rapport au temps universel UTC) avant que ce certificat n'expire. Une valeur égale à 0 implique que le certificat n'expire jamais.
- *CRL* : 4 octets. Identifie le sous-ensemble de certificats auquel ce certificat appartient. En effet, afin d'améliorer la distribution des CRLs, le CA peut fragmenter la CRL. Une valeur égale à 0 implique que le certificat n'apparaitra jamais dans une CRL. Les champs « Expiration » et « CRL » ne peuvent pas être tous les deux à zéro, car un certificat doit toujours avoir une durée de vie limitée et/ou être révocable.
- *Clé(s) publique(s) certifiée(s)* : s'il y a deux clés, une est pour l'authentification et l'autre pour le chiffrement. La taille d'une clé publique certifiée est égale à sa taille actuelle plus un. Par exemple, pour une clé d'authentification de 224 bits (28 octets), la clé encodée ici aura une taille de 29 octets. On retrouve aussi un octet pour la taille de la clé et un octet pour l'algorithme de signature.
- *Signature du certificat* : 64 octets, signature du certificat de l'autorité de certification.

La Figure 2-8 illustre le format de certificat.

<table>
<tr><td>Taille</td><td colspan="4">Champs</td></tr>
<tr><td>1</td><td colspan="2">Version du certificat = 1</td><td colspan="2" rowspan="2"></td></tr>
<tr><td>1</td><td rowspan="11">Certificat non signé</td><td>Type d'entité</td></tr>
<tr><td>8</td><td>ID du signataire</td><td colspan="2" rowspan="2"></td></tr>
<tr><td>1</td><td rowspan="4">Spectre d'applications</td><td>Taille du champ "Nom"</td></tr>
<tr><td>8</td><td>Nom</td><td colspan="2" rowspan="2"></td></tr>
<tr><td>2</td><td rowspan="2">Applications</td><td>Taille du champ "Applications"</td></tr>
<tr><td>1</td><td>Type</td></tr>
<tr><td>4</td><td>Expiration</td><td colspan="2" rowspan="2"></td></tr>
<tr><td>4</td><td>CRL</td></tr>
<tr><td>1</td><td rowspan="3">Clé(s) publique(s) certifiée(s)</td><td>Taille du champ "Clé publique"</td><td colspan="2" rowspan="2"></td></tr>
<tr><td>1</td><td>Algorithme utilisé</td></tr>
<tr><td>29</td><td>Clé publique</td><td>Point de la courbe (dépendant de l'algorithme)</td></tr>
<tr><td>32</td><td rowspan="2">Signature</td><td rowspan="2">Signature ECDSA</td><td>r</td><td colspan="2" rowspan="2"></td></tr>
<tr><td>32</td><td>s</td></tr>
</table>

Figure 2-8. Format de certificat

2.4.1.2 Format de message signé

Tout d'abord l'équipement crée une structure de donnée *ToBeSignedMessage* constituée des éléments suivants :

- *ID application (PSID)*: 4 octets. Application à laquelle le message est destiné. L'application désignée doit faire partie du spectre d'applications défini dans le certificat associé à la clé secrète.

- *4 champs sur 2 octets* : le champ fragmentation indique si le message est fragmenté ; les trois autres champs indiquent si le *ToBeSignedMessage* contient respectivement l'heure de génération, l'heure d'expiration et/ou un emplacement d'utilisation (un message peut n'être utilisé que dans

une zone géographique précise par exemple). Tout comme le PSID, les informations de temps ou de position doivent être en concordance avec le spectre d'utilisation du certificat de la clé.

- *Taille de la charge utile* : 2 octets. Taille des données de l'application.
- *Charge utile* : 32 octets. Données de l'application.
- *Date de génération (optionnel)* : 8 octets. Un émetteur ne peut pas générer deux messages avec la même heure de génération. Ce champ permet d'empêcher l'attaque de rejeu de message.
- *Date d'expiration (optionnel)* : 8 octets.
- *Position (optionnel)* : 11 octets. Position de l'émetteur et zone d'utilisation du message.

Le message signé en lui-même contient les éléments suivants :

- *Version de protocole* : 1 octet. Marqué à « 1 » dans le standard actuel.
- *Type* : 1 octet. Type de sécurité appliquée à ce message.
- *Information du signataire* : taille variable. Le premier octet indique si le message contient le certificat complet (125 octets pour un OBU) ou seulement un condensé (8 octets pour un OBU). Les octets restants représentent le certificat (cf §2.4.1.1).
- *ToBeSignedMessage* : Structure précédemment détaillée.
- *Signature numérique* : deux fois la taille de la clé (56 octets pour une clé de 224 bits ; 64 octets pour une clé de 256 bits), résultat du calcul de la signature numérique avec l'algorithme de signature ECDSA (à partir de la structure *ToBeSignedMessage*).

Taille	Champs		
1	Version de protocole = 1		
1	Type		
1	Information du signataire	Type (certificat ou condensé)	
125		Certificat	
4	Message non signé (*ToBeSignedMesage*)	ID application	
2		Fragmentation	
2		Taille de la charge utile	
32		Charge utile	
8		Date de génération	
8		Date d'expiration	
4		Position	Latitude
4			Longitude
3			Élévation et précision
28	Signature	Signature ECDSA	r
28			s

Figure 2-9. Format de message signé

Si le message signé est un WSM, alors des champs peuvent être omis. En effet, le champ PSID et la taille des données de l'application sont redondants, car déjà présents dans l'entête du WSM. Comme illustré par la Figure 2-9, le message signé généré par un OBU, pour une application et utilisant une clé d'authentification de 224 bits, a une taille de 251 octets (254 octets pour un WSM).

Il est possible de signer et de chiffrer un même message. Dans ce cas, le message est d'abord signé puis chiffré. Au niveau du récepteur le processus est inversé. Nous détaillons dans les sections

suivantes les différentes procédures appliquées pour réaliser ces actions au niveau des émetteurs et récepteurs.

2.4.2 Procédures de signature numérique

Les messages d'alerte relatifs aux applications de sécurité du trafic routier ne sont pas chiffrés, mais simplement signés avec le certificat de l'émetteur. Chaque message signé comprend un horodatage (obtenu à partir de l'horloge interne de l'OBU, elle-même synchronisée avec l'équipement de positionnement) afin d'éviter les attaques de rejeu en vérifiant l'absence du message dans le cache des messages récemment reçus. L'algorithme de signature, spécifié par le standard, est l'algorithme de signature numérique à clé publique ECDSA (*Elliptic Curve Digital Signature Algorithm* [JOH 01]) en combinaison avec la fonction de hachage SHA-1 [NIS 02].

Pour permettre aux véhicules de signer des messages, ils doivent posséder un certificat numérique. Lorsqu'un véhicule signe un message, il doit inclure le certificat ou la chaîne de certificats, c'est-à-dire le certificat de l'entité ayant délivré le certificat du véhicule, le certificat de l'entité ayant accrédité l'entité qui a délivré le certificat du véhicule, et ainsi de suite jusqu'au certificat racine qui est délivré par une autorité supérieure telle qu'une agence gouvernementale responsable des immatriculations (préfecture).

À la réception d'un message signé, chaque véhicule destinataire doit vérifier le certificat racine utilisé pour autoriser le certificat de l'émetteur. Le récepteur doit aussi s'assurer qu'aucun certificat présent dans la chaîne n'a été révoqué. Pour vérifier la révocation d'un certificat, un véhicule parcourt une (ou plusieurs) liste(s) de révocation de certificats. Les CRL et les certificats racines sont stockés localement et doivent être mis à jour périodiquement [LAU 06].

2.4.2.1 Génération de signature numérique

Pour générer un message signé, l'entité doit avoir accès aux informations et services suivants :

- Une clé de signature.
- Le certificat associé à cette clé.
- Un générateur de nombre aléatoire.
- Une implémentation cryptographique logicielle ou physique qui supporte l'algorithme de signature.
- La position et l'heure courante et une estimation de l'erreur de position et d'heure.

Une fois ces hypothèses validées, l'entité qui génère un message signé suit les étapes suivantes :

1. Créer la structure *ToBeSignedMessage*.

    a. Si l'horodatage est inclus, positionner le champ correspond à « 1 » et ajouter la date de génération du message.

b. Si la date d'expiration est incluse, positionner le champ correspondant à « 1 » et ajouter la date d'expiration du message.

c. Si l'information de position est incluse, positionner le champ correspondant à « 1 » et ajouter la position actuelle.

d. Remplir le champ PSID.

2. Signer la structure *ToBeSignedMessage*.

3. Créer le message signé en complétant les champs indiquant le type d'algorithme de signature utilisé, et l'envoyer.

2.4.2.2 Vérification de signature numérique

Un véhicule qui reçoit un message signé exécute les étapes suivantes pour authentifier la signature :

1. Vérifier que le message a un format correct.

2. Vérifier que le message a été généré récemment et qu'il ne correspond pas à un message précédemment reçu. Cette vérification est faite en comparant l'horodatage du message avec l'heure courante et en comparant avec le cache des messages récemment reçus.

3. Si la position de l'émetteur est incluse dans le message, la comparer avec la position courante du récepteur afin d'assurer une portée raisonnable.

4. Si le message contient le condensé du certificat, vérifier que le certificat complet associé au condensé est présent dans le cache des certificats reçus.

5. Si le certificat contient une zone géographique, vérifier que l'émetteur est bien dans cette zone.

6. Vérifier que l'application cible est en concordance avec le spectre applicatif du certificat.

7. Vérifier que le certificat n'est pas dans une CRL.

8. Vérifier que la signature utilise bien ECDSA avec une clé de 224 ou 256 bits.

2.4.3 Procédures de chiffrement

Comme la cryptographie symétrique est moins consommatrice (en terme de CPU) que la cryptographie asymétrique, le standard IEEE 1609.2 utilise une combinaison de la cryptographie symétrique et asymétrique pour le chiffrement. Le chiffrement suit deux étapes :

1. L'émetteur sélectionne une clé symétrique et l'utilise pour chiffrer le message avec un algorithme symétrique.

2. L'émetteur chiffre la clé symétrique avec un chiffrement asymétrique en utilisant la clé publique du destinataire.

À titre d'exemple, les messages d'application de transaction financière sont généralement unicast et envoyés en utilisant la pile IP (cf. Figure 1-4). Ces messages transportent des données personnelles et sont donc chiffrés avec un algorithme de chiffrement symétrique et une clé aléatoire. Cette clé aléatoire est à son tour chiffrée en utilisant l'algorithme de chiffrement asymétrique. L'émetteur d'un message chiffré doit donc connaître la clé publique du destinataire du message. Cette clé publique est connue grâce au certificat délivré par le destinataire (par exemple lorsque le destinataire a signé un message récemment reçu). Un message chiffré peut être envoyé à plusieurs destinataires, mais une clé publique pour chaque destinataire doit être connue. Ainsi, il est impossible d'envoyer un message chiffré à un destinataire inconnu.

Avec cette approche, la majeure partie des opérations cryptographiques sont réalisées avec un algorithme symétrique. Dans la version actuelle du standard, un algorithme symétrique (AES-CCM avec une clé de 128 bits) et un algorithme asymétrique (ECIES) sont spécifiés.

2.4.3.1 Génération de message chiffré

L'émetteur d'un message chiffré doit suivre les étapes suivantes :

1. Récupérer la clé publique du destinataire dans le cache de certificat (on rappelle que le certificat contient la clé publique).
2. Vérifier que le certificat n'est pas révoqué.
3. Générer une clé aléatoire symétrique.
4. Chiffrer le message en utilisant cette clé aléatoire symétrique et l'algorithme AES-CCM.
5. Chiffrer la clé aléatoire symétrique avec ECIES et la clé publique du destinataire.
6. Créer un paquet qui contient le message chiffré et la clé chiffrée et l'envoyer.

2.4.3.2 Vérification de message chiffré

Le destinataire du message chiffré suit les étapes suivantes :

1. Utiliser sa clé privée pour déchiffrer la clé symétrique en utilisant ECIES.
2. Utiliser la clé symétrique précédemment récupérée pour déchiffrer le message en utilisant AES-CCM.

Le standard IEEE 1609.2 spécifie les procédures afin d'assurer la confidentialité, l'authenticité et l'intégrité. Concernant les autres services de sécurité, aucun consensus n'est défini à l'heure actuelle.

2.5 Exigences de performance

Afin d'assurer les communications de sécurité routière dans les VANETs, les exigences applicatives doivent être prises en compte, et les exigences de sécurité satisfaites. Les protocoles de communication sécurisée utilisés par les applications de sécurité du trafic routier sont conçus afin de satisfaire ces exigences. En dehors des exigences de sécurité, il est essentiel qu'ils répondent aussi aux exigences de performance, sans quoi ils ne seront pas applicables dans le contexte routier. Dans les VANETs, les conditions environnementales impactent la fiabilité, la latence et l'efficacité du canal radio. Ces conditions sont par exemple la vitesse, la densité du trafic réseau ou la portée de transmission. La densité du trafic réseau dépend de la fréquence d'envoi des messages, de la taille des messages et de la densité du trafic routier. Il est donc important de bien choisir ces paramètres. Par exemple, si un message d'alerte arrive après que le conducteur l'a déjà détecté par lui-même (délai d'envoi supérieur à 700 ms), alors le conducteur ne fera plus confiance au système. Dans les protocoles utilisés, d'autres paramètres influencent la taille du message et le délai de communication : la taille des informations cryptographiques (clé, certificat, signature, hachage, etc.) et le temps nécessaire au processus d'authentification.

Dans notre contexte d'applications sensibles au délai, le coût de la sécurité doit être maitrisé. Nous nous intéressons donc à la fréquence d'appel des services de sécurité. La signature numérique, le hachage, la vérification des certificats sont des exemples de services proactifs appelés pour chaque message transmis. Sachant qu'un message (beacon) est émis toutes les 100 millisecondes, nous comprenons l'impact que peut avoir un mécanisme consommateur (en temps et en calcul). A contrario, la gestion des pseudonymes, la distribution des clés, des certificats et des listes de révocation, sont des exemples de services de sécurité proactifs appelés moins fréquemment (de l'ordre de la minute dans le pire des cas).

Le coût de la sécurité est donc la somme des coûts des mécanismes proactifs et des mécanismes réactifs. À partir de ce constat, nous nous intéressons aux services de sécurité proactifs, et plus particulièrement à l'authentification. En effet, les services à forte fréquence ont besoin d'être les plus économes en temps possible. La génération et la vérification de signature numérique sont appelées pour chaque message émis dans le VANET. Il est donc primordial de comprendre l'impact de ces mécanismes sur les performances des applications.

De plus, grâce à l'application LDW, un conducteur peut anticiper un freinage d'urgence. Le véhicule pourra donc s'arrêter avant l'obstacle et ainsi éviter de provoquer ou d'aggraver une situation d'accident. Néanmoins, il faut s'assurer que l'ajout des mécanismes de sécurité tels que l'authentification n'augmente pas la distance de freinage de manière significative.

2.6 Conclusion

Ce chapitre pose le problème de la sécurité des VANETs au sens général. Afin de comprendre comment sécuriser un VANET, nous avons détaillé les modèles d'attaquant et d'attaque les plus représentatifs dans notre contexte.

Nous avons ensuite décrit les mécanismes permettant d'assurer les sept services de sécurité conventionnels : la confidentialité, l'authenticité, l'intégrité, la non-répudiation, la disponibilité, le contrôle d'accès et le respect de la vie privée. Dans les applications véhiculaires, certains mécanismes sont plus particulièrement employés : l'authenticité, l'intégrité et le contrôle d'accès [KRO 06].

L'authenticité est importante dans toutes les applications de sécurité du trafic routier, car ce service permet, entre autres, de se prémunir des attaques externes (à l'exception du DoS). De plus, l'authenticité est un prérequis aux autres services de sécurité. En effet, grâce à la signature numérique avec certificat, un véhicule et ses messages sont identifiables. La non-répudiation et le contrôle d'accès pourront alors être mis en place.

Dans la deuxième partie de ce chapitre, nous avons centré notre étude sur une application sensible au délai : l'application d'alerte de danger local. Après avoir explicité les attaques possibles sur cette application, nous avons présenté les mécanismes de sécurité les mieux adaptés. Puisque les communications véhiculaires sont régies par l'ensemble de standards WAVE/DSRC IEEE 1609, nous avons détaillé le standard axé sur la sécurité : le IEEE 1609.2.

Enfin, nous avons introduit le problème de performance associé à l'ajout de mécanismes de sécurité. Comme l'ensemble des services de sécurité ne peut pas être réduit à un unique protocole, les VANETs auront plusieurs mécanismes de sécurité. Ainsi, les mécanismes doivent être choisis avec précaution afin de garantir un coût minimal en terme de temps de calcul et de communication. De plus, les applications peuvent avoir des exigences temporelles. Les mécanismes de sécurité doivent alors respecter les contraintes applicatives.

L'ajout d'un mécanisme de sécurité a donc un coût. Ce coût peut être exprimé en terme de :

- *Temps de calcul* : Temps de traitement (génération de signature, vérification de signature, chiffrement, déchiffrement, vérification de certificat, etc.).

- *Bande passante du réseau* : Nombre de messages, taille de message.

Afin d'améliorer le coût des mécanismes de sécurité, il est indispensable d'en connaître le coût actuel. En plus d'être un prérequis essentiel dans notre contexte, l'authenticité est appelée pour chaque message émis et reçu. Il est donc potentiellement le plus consommateur. Mais quel est le coût de l'authentification ? Quel est son impact dans l'application de LDW ? C'est notamment à ces questions que le chapitre suivant vise à répondre. Nous analyserons plus particulièrement l'impact de l'authentification sur la prédictibilité du système DSRC.

Le mécanisme de vérification de plausibilité combiné à un consensus semble prometteur, car il propose un propriété d'adaptation au contexte pour éviter l'attaque la plus fréquente : l'injection de fausses alertes. Ce dernier point fera l'objet d'une attention toute particulière dans le chapitre 4.

3 Surcoût de l'authentification : Analyse du protocole ECDSA

Un réseau sans fil véhiculaire a besoin de nombreux services de sécurité afin d'assurer son bon fonctionnement. Dans le chapitre précédent, nous avons souligné l'importance du service d'authentification dans le déploiement de VANETs sécurisés. Le standard IEEE 1609.2, régissant la sécurité des communications sans fil véhiculaires, spécifie que l'authentification doit être assurée par un mécanisme de signature numérique : le protocole ECDSA (*Elliptic Curve Digital Signature Algorithm*) [ANS 98].

Le chapitre précédent nous a sensibilisés sur le problème de performance quant à l'ajout de mécanismes de sécurité. Nous allons donc analyser le surcoût de l'authentification dans les VANETs. Afin de calculer ce surcoût, nous explicitons les paramètres et le fonctionnement du protocole ECDSA. Dans un premier temps, nous étudions l'impact d'ECDSA sur le temps de calcul. En effet, le temps nécessaire à la génération/vérification de signature numérique doit être évalué afin de comprendre son impact dans les VANETs. Dans un second temps, nous analysons l'impact d'ECDSA sur les performances réseau. Nous nous intéressons plus particulièrement au délai de transfert d'un message, car les applications de sécurité du trafic routier y sont sensibles.

Dans le contexte critique d'application telle que l'alerte de danger local (LDW), le temps de calcul et de transfert de l'alerte ont un impact sur la réaction du conducteur. Si l'on considère que le conducteur doit freiner, l'ajout de mécanismes d'authentification peut alors avoir un impact sur la distance de freinage. En effet, sans mécanisme de sécurité, le véhicule ayant une vitesse de 130 km/h s'arrêtera en 96 mètres. Grâce à l'application LDW, le conducteur pourra anticiper et ainsi réagir plus tôt que s'il n'avait pas eu d'équipement DSRC. Mais en ajoutant un temps de traitement (à l'émission et à la

réception), ce gain (en terme de temps et donc de distance entre le véhicule et l'obstacle) peut être réduit. En effet, l'ajout de mécanisme de sécurité impose un surcoût :

- Temporel : Temps de calcul (signature numérique, certificat, hachage, etc.).
- Charge de communication : Les messages signés ou chiffrés ont une taille supérieure aux messages non sécurisés. Chaque mécanisme de sécurité entraîne un échange de message (vérification de certificat, récupération de CRL, envoi de la clé privée, etc.).
- Financier : Les équipements dédiés à la sécurité ajoutent un coût financier à la production de chaque unité DSRC. La gestion de systèmes de sécurité peut être chère (mise en place de serveurs de stockage de CRL, etc.).

C'est pourquoi nous avons besoin d'analyser analytiquement et par simulation l'impact d'ECDSA sur le délai de transfert d'un message et sur la distance de freinage.

3.1 Paradigme général du surcoût de la sécurité

Avant d'analyser le surcoût de l'authentification à proprement parler, nous décrions le paradigme général du surcoût de la sécurité. Comme nous l'avons vu dans le chapitre 2, la sécurité peut être définie comme un ensemble de services. Chacun de ces services est à son tour composé d'un ensemble de mécanismes de sécurité. Ainsi le surcoût temporel de la sécurité correspond à la somme des délais pour chaque service. De la même manière, le délai d'un service est égal à la somme des temps de traitement de chaque mécanisme qui le compose. Nous obtenons ainsi la formule suivante :

$$D_{sécurité} = \sum_{i=1}^{n} D_i = \sum_{i=1}^{n} \sum_{j=1}^{m} D_i^j$$

où n est le nombre de service, m le nombre de mécanismes, D_i le délai du service i, D_i^j le délai du mécanisme j appelé par le service i.

Nous pourrons définir le surcoût temporel de la sécurité comme :

$$D_{sécurité} = D_{confidentialité} + D_{authentification} + D_{intégrité} + D_{non-répudiation} + D_{vie\ privée} + D_{disponibilité} + D_{contrôle\ accès}$$

Dans la suite de cette thèse, nous nous intéressons au surcoût de l'authentification ($D_{authentification}$) et détaillons l'ensemble des mécanismes associés (définis dans le standard IEEE 1609.2). À la fin de ce chapitre, nous aurons la formule qui définit ce surcoût.

3.2 Protocole ECDSA

Neal Koblitz et Victor S. Miller ont été les premiers à proposer l'utilisation des courbes elliptiques dans la cryptographie. Cela a donné lieu à la cryptographie des courbes elliptiques (ECC, *Elliptic Curve Cryptography*), qui est une cryptographie asymétrique basée sur la structure algébrique des courbes elliptiques dans un corps fini. L'existence d'une loi de groupe abélien sous-jacente aux points d'une courbe elliptique fournit des propriétés adéquates à leur usage en cryptographie. La loi de groupe définie par la courbe elliptique est ainsi relativement facile à calculer. Toutefois, le problème du logarithme discret reste difficile, car il n'existe pas à l'heure actuelle d'algorithme efficace pour le résoudre (contrairement aux groupes multiplicatifs définis dans les corps finis simples [GAL 07]).

Ainsi, la sécurité d'ECDSA repose sur l'impossibilité de résoudre le logarithme discret dans un sous-groupe d'une courbe elliptique. Vanstone a proposé en 1992 l'algorithme ECDSA qui est défini par le standard X9.62 [ANS 98]. ECDSA est une extension du protocole DSA (*Digital Signature Algorithm*) aux courbes elliptiques afin d'avoir, à niveau de sécurité équivalent, une clé publique plus courte que RSA et DSA. Par exemple, d'après les expérimentations faites par Johnson et Menezes [JOH 98], une clé DSA (ou RSA) de 1024 bits équivaut à une clé ECDSA de 160 bits pour un niveau de sécurité de 10^{11} années MIPS.

Le Tableau 3-1, élaboré par le RSA Laboratories, donne une estimation des ressources nécessaires pour casser les trois systèmes ECC, RSA et DSA pour différentes tailles de clé [HED 06]. Pour mieux évaluer l'efficacité des ECC, le Tableau 3-2 présente une comparaison des temps de calcul en millisecondes pour une signature et une vérification de signature sur un ordinateur équipé d'un processeur Pentium III 900 MHz avec 256 Mo de RAM [WAL 02]. Nous remarquons que le temps de calcul d'une vérification avec ECDSA est supérieur à celui pour RSA. Comme nous le verrons lors de nos expérimentations, ce temps peut être réduit en opérant des modifications au niveau matériel.

Année MIPS	**RSA/DSA Taille des clés**	**ECC Taille des clés**	**Rapport des tailles des clés**
10^4	512	106	5 :1
10^8	768	132	6 :1
10^{11}	1024	160	7 :1
10^{20}	2048	210	10 :1
10^{78}	21000	600	35 :1

Tableau 3-1. Comparaison des niveaux de sécurité pour ECC, RSA, DSA

	RSA			**DSA**			**ECDSA**		
Taille des clés (bits)	680	1368	2704	680	1368	2704	112	160	224
Signature	10	45	270	10	20	80	5	5	25
Vérification	0	2	8	10	30	110	25	75	95

Tableau 3-2. Comparaison du temps de calcul pour RSA, DSA, ECDSA

Avant d'analyser le surcoût d'ECDSA dans les VANETs, nous détaillons ses paramètres et son fonctionnement.

3.2.1 Paramètres

Pour utiliser le protocole ECDSA, les parties doivent s'accorder sur un ensemble d'éléments qui définissent la courbe elliptique : les paramètres de domaine. Chaque participant génère ses paramètres de domaine et les envoie avec sa clé publique. Mais cette opération consiste à compter le nombre de points de la courbe, ce qui est consommateur en temps et difficile à implémenter. Le NIST et le SECG ont donc publié les paramètres de domaines pour les courbes elliptiques [CER 00-2] [NIS 99]. Ainsi, toute implémentation du standard IEEE 1609.2 doit supporter le protocole de signature numérique ECDSA sur les courbes elliptiques P-224 et P-256.

Pour établir la clé publique d'ECDSA, le protocole doit tout d'abord spécifier une courbe elliptique et un point de cette courbe. Bien qu'en principe chaque clé ait sa propre courbe elliptique, en pratique, il est plus efficace d'avoir un nombre restreint de courbes. En effet, cette approche permet de réduire la taille du certificat, car seul l'identifiant de la courbe est donné et non pas la description complète de la courbe.

3.2.2 Fonctionnement

L'algorithme de Johnson décrit le fonctionnement d'ECDSA et comprend la génération de la clé publique, la génération de la signature et la vérification de la signature. L'Algorithme 3-1 présente ces trois phases.

Dans l'Algorithme 3-1, $H(m)$ est la valeur de hachage du message obtenue avec un algorithme de hachage cryptographique (SHA-224 par exemple). Nous remarquons que cet algorithme repose essentiellement sur l'opération de multiplication scalaire d'un point de la courbe elliptique utilisée en $a.3$, $b.2$ et $c.4$ ($Q = dP$).

Le protocole ECDSA a un coût en temps de calcul et en temps « réseau », car il ajoute un temps de traitement à chaque message. En effet, un message est signé avant d'être émis, puis vérifié à la réception. De plus, la taille du message est agrandie, car une signature et un certificat y sont ajoutés. Il est établi qu'un message plus grand a une probabilité de collision plus élevée. Ainsi, ECDSA a un impact sur le temps de calcul au niveau de chaque véhicule, mais aussi sur le délai de transfert du message.

a. Génération de clé publique

1. Définir l'ensemble des paramètres de domaine
   q : cardinalité du champ de Galois F_q
   $a, b \in F_q$: paramètres de la courbe elliptique E
   $P \in E$: point de E
   n : ordre de P (n nombre premier supérieur à 2^{160})
   $h = \frac{ord(P)}{ord(E)}$ où $ord(X)$ est l'ordre de X
2. Tirer un nombre aléatoire $d \in [1, n-1]$ comme clé privée
3. Calculer la clé publique $Q = dP$

(E, Q, P, n) sont publiques.

b. Génération de signature

entrée : message m et (d,Q)

1. Tirer un nombre aléatoire $k \in [1, n-1]$
2. Calculer $\mathrm{k}\times\mathrm{G} = (\mathrm{x}_1, \mathrm{y}_1)$ et $\mathrm{r} = \mathrm{x}_1 \mathrm{mod n}$
   si $r = 0$ aller en 1
3. Calculer $\mathrm{s} = \mathrm{k}^{-1}(\mathrm{e} + \mathrm{d}\times\mathrm{r})\mathrm{mod n}$ avec $\mathrm{e} = \mathrm{H(m)}$
   si $\mathrm{s} = 0$ aller en 1
4. La signature de m est (r,s).

c. Vérification de signature

entrée : $(\mathrm{r}, \mathrm{s}), \mathrm{m}, \mathrm{Q}$

1. Vérifier $\mathrm{r}, \mathrm{s} \in [1, \mathrm{n}\text{-}1]$
2. Calculer $w = s^{-1} (\mathrm{mod}\ n)$
3. Calculer $u_1 = e\times w\ (\mathrm{mod}\ n)$ et $u_2 = r\times w\ (\mathrm{mod}\ n) \mathrm{u}_2 = \mathrm{r}\times\mathrm{w mod n}$ avec $\mathrm{e} = \mathrm{H(m)}$
4. Calculer $\mathrm{X}_1 = \mathrm{u}_1\times\mathrm{G} + \mathrm{u}_2\times\mathrm{Q}$ et $V = X_1 (\mathrm{mod}\ n)$
5. Si $\mathrm{V} = \mathrm{r}$ alors la signature est acceptée.

Algorithme 3-1. Algorithme de Johnson pour ECDSA

3.3 Analyse du temps de calcul

Dans cette section, nous analysons l'impact d'ECDSA sur le temps de calcul. À partir de l'Algorithme 3-1, nous présentons la complexité en temps d'ECDSA, et validons cette étude par le biais d'expérimentations.

3.3.1 Complexité d'ECDSA

Le protocole ECDSA utilise les opérations sur les courbes elliptiques suivantes :

- Addition de deux points : $P + Q$
- Doublement d'un point : $2P$
- Multiplication scalaire d'un point : kP

L'opération de base dans la génération et la vérification de signature ECDSA est la multiplication scalaire dans le corps des courbes elliptiques. Dans les sections suivantes, nous analysons donc la complexité en temps de la multiplication scalaire. Mais cette dernière utilise les opérations de

multiplication modulaire et d'inversion modulaire. C'est pourquoi nous détaillons la complexité de ces trois opérations afin d'évaluer la complexité en temps d'ECDSA.

3.3.1.1 Multiplication scalaire

Dans ECDSA, la multiplication scalaire d'un point de la courbe par un nombre aléatoire est utilisée dans la génération et la vérification des signatures numériques [NEG 05]. Cette opération est la plus consommatrice en temps parmi celles impliquées dans la génération/vérification des signatures [JAR 07]. Il s'agit de l'opération *a*.3, *b*.2, *c*.4 de l'Algorithme 3-1. À partir d'un nombre aléatoire *k* et d'un point *P* de la courbe, il faut calculer la multiplication scalaire *kP* sur la courbe elliptique. Il existe notamment deux algorithmes pour calculer *kP* : « addition et doublement » ou Montgomery. Ces algorithmes requièrent plusieurs multiplications, additions, et éventuellement une inversion de coordonnées. Les auteurs de [OKE 01] ont montré la supériorité (en temps) de l'algorithme de Montgomery dans les environnements contraints comme les équipements mobiles. Ainsi l'efficacité d'ECDSA repose en grande partie sur l'arithmétique sur les courbes elliptiques et l'arithmétique dans le corps sous-jacent [JAR 07]. L'Algorithme 3-2 pour la multiplication scalaire de Montgomery, prend en entrée un point $P = (x, y)$ en coordonnées affines, et un entier $k = \sum_{i=0}^{n-1} k_i 2^i$ de *n* bits de longs en représentation binaire, et calcule $Q = kP = (x_3, y_3)$ en utilisant la méthode de Montgomery [NEG 04].

Entrée : $P = (x, y) \in E, k = (k_{n-1} \dots k_0)_2$

Sortie : $Q = kP$

Algorithme :

$x_1 \leftarrow x$; $z_1 \leftarrow 1$; $x_2 \leftarrow x^4 + b$; $z_2 \leftarrow x^2$
Pour i de $n-1$ à 0 faire
    si $k_i = 0$ alors
        $u \leftarrow z_1$; $z_1 \leftarrow (x_1 z_2 + x_2 z_1)^2$; $x_1 \leftarrow x z_1 + x_1 x_2 u z_2$
        $u \leftarrow x_2$; $x_2 \leftarrow x_2^4 + b z_2^4$; $z_2 \leftarrow u^2 z_2^2$
    sinon si $k_i = 1$ alors
        $u \leftarrow z_2$; $z_2 \leftarrow (x_2 z_1 + x_1 z_2)^2$; $x_2 \leftarrow x z_2 + x_2 x_1 u z_1$
        $u \leftarrow x_1$; $x_1 \leftarrow x_1^4 + b z_1^4$; $z_1 \leftarrow u^2 z_1^2$
    fin si
fin pour
$x_3 \leftarrow x_1 / z_1$
$y_3 \leftarrow (x + x_1/z_1)\,[(x_1 + x z_1)(x_2 + x z_2) + (x^2 + y)(z_1 z_2)]/(x z_1 z_2) + y$
Retourner (x_3, y_3)

Algorithme 3-2. Multiplication scalaire de Montgomery

Afin d'affiner notre étude de la complexité, nous détaillons dans les sections suivantes les opérations de multiplication et d'inversion modulaire.

3.3.1.2 Multiplication modulaire

Afin d'effectuer la multiplication scalaire dans le corps des courbes elliptiques, la multiplication modulaire est utilisée. Il s'agit de l'opération la plus critique en terme de temps. À partir d'un message de *n* bits, un entier *m* de *n* bits appelé modulo, et deux opérandes de *n* bits *x* et *y*, le problème est le calcul de $xy \pmod m$.

L'algorithme de Montgomery pour la multiplication modulaire [GUA 03] est considéré comme le plus rapide quand *x*, *y* et *m* sont grands [OKE 01]. L'idée principale de Montgomery est de réduire la taille des résultats intermédiaires à une taille fixe de $n + 1$ bits. Cela est obtenu grâce à une phase de réduction ne nécessitant pas de divisions, mais uniquement des décalages. L'Algorithme 3-3 présente l'algorithme de Montgomery pour la multiplication modulaire (*b* étant la base) [MEN 01].

Entrée : $m = (m_{n-1} \dots m_1 m_0)_b$, $x = (x_{n-1} \dots x_1 x_0)_b$, $y = (y_{n-1} \dots y_1 y_0)_b$ avec $0 \leq x, y < m$
$R = b^n$ avec $pgcd(m, b) = 1$ et $m' = m^{-1} \pmod b$

Sortie : $A = xyR^{-1} \pmod m$

Algorithme :
$A \leftarrow 0$ (Notation : $A = (a_{n-1} \dots a_1 a_0)_b$)
Pour i de 0 à $n - 1$ faire :
    $u_i \leftarrow (a_0 + x_i y_0) m' \pmod b$
    $A \leftarrow (A + x_i y + u_i m)/b$
    Si $A \geq m$ alors
        $A \leftarrow A - m$
    fin si
fin pour
Retourner *A*

Algorithme 3-3. Algorithme de Montgomery pour la multiplication modulaire

Nous remarquons que si les opérations (addition modulaire, multiplication, addition, décalage) sur *A* sont considérées comme faites en temps constant, alors la complexité en temps est *O(n)* et la complexité en espace est *O(n)* [KOR 93][KAI 05].

3.3.1.3 Inversion modulaire

L'inversion modulaire est une autre opération consommatrice en temps pour la multiplication scalaire, et est aussi utilisée en *b*.3 et *c*.2 de l'Algorithme 3-1. L'inversion de Montgomery est un algorithme pour calculer $x^{-1} \pmod m$ [SAV 05]. Les principales opérations utilisées dans le cadre de l'inversion de Montgomery sont :

- le calcul du PGCD de deux nombres
- la multiplication de Montgomery (cf. Algorithme 3-3)
- la comparaison

L'inverse d'un entier $x \in [1, m-1]$ est j tel que $j = x^{-1}b^n (\mathrm{mod}\, m)$ où m est premier et $n = log_2 m$ est la taille en bit. La complexité en temps de l'inversion modulaire de Montgomery est *O(n)* [MA 08].

3.3.1.4 Complexité en temps

Nous définissons les opérations d'addition, de doublement, de multiplication scalaire, de multiplication modulaire, d'inversion modulaire et d'élévation au carré dans le corps des courbes elliptiques comme les fonctions *P+Q*, *2P*, *kP*, *MUL*, *INV*, *SQR*. La fonction de hachage est notée *HASH*. Le temps nécessaire à l'exécution d'une opération *OP* est noté T_{OP}. Le Tableau 3-3 définit le temps de calcul des trois opérations de base [NIK 08].

Opération	**Temps de calcul**
P+Q	$T_{P+Q} = T_{SQR} + 4\times T_{MUL}$
2P	$T_{2P} = 4\times T_{SQR} + 2\times T_{MUL}$
kP	$T_{kP} = n\times(T_{P+Q} + T_{2P})$

Tableau 3-3. Temps de calcul

D'après l'Algorithme 3-1, la génération et la vérification de signature ECDSA sont obtenues par des multiplications modulaires, exponentiation au carré, inversion modulaire et hachage. Ainsi la complexité en temps d'ECDSA est définie à partir de $T_{MUL}, T_{SQR}, T_{INV}$ et T_{HASH}. Les équations suivantes définissent le temps de génération et de vérification d'une signature numérique [PET 09].

Le temps de génération d'une signature numérique est calculé ainsi :

$$T_{sign} = 2\times T_{MUL} + T_{INV} + T_{kP} + T_{HASH} = (6n+2)\times T_{MUL} + T_{INV} + 5n\times T_{SQR} + T_{HASH} \quad (3.1)$$

Le temps de vérification d'une signature numérique est calculé ainsi :

$$T_{verif} = 2\times T_{MUL} + T_{INV} + 2\times T_{kP} + T_{HASH} = (12n+2)\times T_{MUL} + T_{INV} + 10n\times T_{SQR} + T_{HASH} \quad (3.2)$$

Nous remarquons que la vérification utilise deux multiplications scalaires. La vérification est donc deux fois plus consommatrice en temps que la génération de signature.

Le temps de hachage T_{HASH} est présent dans les deux équations précédentes. Nous analysons donc la complexité de l'opération de hachage. Le standard DSRC spécifie SHA-224 et SHA-256 comme algorithmes de hachage. Leur complexité est en $O(M\times n)$ où *M* est la taille du message à traiter.

Comparativement au coût temporel de la multiplication modulaire, les opérations d'addition et de soustraction modulaire sont négligeables et sont donc omises. Le protocole ECDSA est alors réduit aux opérations de multiplication modulaire, d'inversion modulaire et de hachage. Comme la multiplication et l'inversion modulaire de Montgomery sont toutes deux en $O(n)$ et que le hachage est en $O(M\times n)$, alors la complexité en temps totale d'ECDSA est en $O(n) + O(M\times n)$.

3.3.2 Paramètres et hypothèses d'expérimentation

Le temps de calcul correspond aux processus réalisés par chaque véhicule lors de l'émission ou de la réception d'un message signé. Ce surcoût est dû aux opérations de sécurité que sont la génération et la vérification de signature numérique. Le surcoût de calcul inclut :

(i) Sélection du certificat : Avant de signer un message, un certificat doit être sélectionné à partir d'un ensemble de certificats valides afin d'assurer l'anonymat [RAY 07].

(ii) Signature du message : À la réception d'un message à sécuriser, le hachage du message est calculé et signé grâce à la clé privée associée avec le certificat sélectionné. Ensuite, cette signature et le certificat sont envoyés (avec le message) à la couche inférieure pour transmission. Dans le cas d'ECDSA, la signature a deux composants *r* et *s* (cf. Figure 2-9).

(iii) Vérification du certificat : Dans le cas d'un schéma de certification basé sur les CRLs, à la réception d'un message, le certificat est considéré valide s'il n'est pas présent dans une CRL.

(iv) Vérification du message : Lors de réception d'un message signé, le hachage du message reçu est à nouveau calculé, et utilisé avec la signature *s* afin d'obtenir *r*. La valeur de *r* est comparée avec celle présente dans la signature.

Si l'on suppose que chaque véhicule est équipé de CRL(s) à jour, alors la vérification de certificat (iii) sera rapide, car il s'agit d'une recherche dans une liste. Dans le cas contraire, la vérification peut nécessiter une série d'échange de paquets et même d'un accès à une infrastructure. De plus, les surcoûts (i) et (iii) sont dépendants des mécanismes de certification employés dans les VANETs. Cependant, ils ne sont pas standardisés à l'heure actuelle. C'est pourquoi nous nous intéressons principalement aux surcoûts (ii) et (iv).

3.3.2.1 Environnement d'expérimentation

Il existe trois bibliothèques cryptographiques principales : MIRACL (*Multiprecision Integer and Rational Arithmetic C/C++ Library*) [MIR 00], OpenSSL et Crypto++. Abusharekh et Gaj [ABU 07] les ont comparées et ont conclu que MIRACL offre les meilleures performances pour les opérations sur les courbes elliptiques. ECDSA a donc été implémenté avec MIRACL, et ce, en respectant l'Algorithme 3-1.

Nos expérimentations ont été réalisées sur un ordinateur équipé d'un processeur Pentium D 3,4 GHz, de 1 Go de RAM, et du système d'exploitation Mandriva 2008. Chacune des expérimentations a été exécutée 500 fois afin de lisser les interférences dues aux interruptions du système. La section 3.3.3.1 présente les résultats de ces expérimentations.

3.3.2.2 Calcul des distances

Dans notre contexte de réseau véhiculaire, il ne faut pas oublier que les véhicules se déplacent relativement vite. Durant la phase de génération ou de vérification d'une signature numérique, un

véhicule V se déplace d'une distance notée D_V (en mètres) en fonction de sa vitesse v_V (en km/h). Le temps T (en millisecondes), dû à la sécurité, est égal à T_{sign} ou T_{verif} ou $T_{sign} + T_{verif}$, selon s'il l'on désire la distance parcourue par l'émetteur ou le récepteur. La distance parcourue est calculée ainsi :

$$D_V = \frac{1}{3600} \times v_V \times T \tag{3.3}$$

Ensuite, nous analysons l'impact du temps de calcul sur la distance de freinage dans la section 3.3.3.2. Pour calculer la distance de freinage (en mètres), à partir des équations de mouvement, nous utilisons la formule suivante :

$$D_{Freinage} = \frac{(\frac{5}{18} \times v^2)}{2 \times \mu g} = \frac{(\frac{5}{18} \times v^2)}{2 \times a} \tag{3.4}$$

où g est l'accélération gravitationnelle ($g = 9{,}81\ m/s^2$), μ est le coefficient de friction entre les pneus et la route ($\mu = 0{,}7$ dans le cas de pneus en bon état), a est le coefficient de décélération ($a = 6{,}8\ m/s^2$ pour une route sèche). La fraction $\frac{5}{18}$ permet de convertir la vitesse v des km/h en m/s. À titre d'exemple, un véhicule roulant à 130 km/h s'arrêtera en 95,82 mètres.

3.3.3 Résultats

Nous présentons les résultats des expérimentations en nous focalisant sur l'aspect temporel et spatial.

D'un point de vue temporel, nous analysons l'impact de la taille de la clé d'authentification sur le temps de calcul. Cela nous permet d'appréhender le surcoût de l'authentification sur le temps de calcul, mais aussi le choix de la taille de la clé d'authentification.

D'un point de vue spatial, nous traduisons le temps de calcul en distance de freinage. Nous analysons alors l'impact de la taille de la clé d'authentification sur la distance de freinage. Nous introduisons un mécanisme de consensus « naïf » afin de mettre en lumière les conséquences d'une mauvaise utilisation de l'authentification.

3.3.3.1 Impact de la taille de la clé d'authentification sur le temps de calcul

Les expérimentations nous permettent d'analyser le temps de calcul nécessaire pour chaque opération d'ECDSA. De manière globale, nous obtenons les temps de génération et de vérification d'une signature numérique.

Taille de la clé (bit)	T_{MUL} **(µs)**	T_{INV} **(µs)**	T_{kP} **(µs)**	T_{HASH} **(µs)**
224	1,23	18,91	2468,71	8,47
256	1,39	22,01	3297,23	10,09

Tableau 3-4. Temps de calcul sur un Pentium D 3,4 GHz

Taille de la clé (bit)	Génération de signature (ms)	Vérification de signature (ms)
224	2,50	4,97
256	3,33	6,63

Tableau 3-5. Temps de génération et de vérification d'une signature sur un Pentium D 3,4 GHz

L'utilisation dc la courbe elliptique P-224 (respectivement P-256) signifie qu'ECDSA est utilisée avec une clé d'authentification de 224 bits (respectivement 256 bits). Dans le Tableau 3-4, l'opération T_{kP} est équivalente au temps de génération d'une signature numérique. Cela confirme que la multiplication scalaire est l'opération la plus coûteuse d'ECDSA. Si nous reportons les valeurs du Tableau 3-4 dans l'équation (3.1) et (3.2), alors nous retrouvons les valeurs du Tableau 3-5. Les équations de temps de calcul sont donc validées.

Le Tableau 3-5 donne les temps de génération et de vérification d'une signature numérique. Nous remarquons qu'utiliser P-256 au lieu de P-224 dans la génération de signature entraine une augmentation de 33,2 % du temps de calcul. De la même manière, le surcoût de P-256 est de 33,4 % du temps de calcul pour une vérification de signature numérique.

L'analyse théorique d'ECDSA montre une complexité linéaire dépendante de la taille de la clé d'authentification. Dans le Tableau 3-5, le temps de calcul augmente avec la taille de la clé. Ces résultats valident notre étude de la complexité.

3.3.3.2 Impact de la taille de la clé d'authentification sur la distance de freinage

Dans notre contexte d'application d'alerte de danger local, le temps calcul consommé par un véhicule récepteur a indéniablement un impact sur la distance de freinage du véhicule. Prenons à titre d'exemple, un véhicule qui reçoit une alerte d'accident à 100 mètres devant lui. Les conditions climatiques sont mauvaises (brouillard épais, de nuit), et le conducteur ne voit pas à 100 mètres devant lui. Le conducteur ne réagira donc qu'au moment où l'alerte lui sera délivrée. Mais un OBU ne délivre l'alerte qu'après avoir vérifié la signature numérique attachée à celle-ci. Nous analysons donc l'impact de l'authentification sur la distance de freinage.

D'après la Figure 3-1 et la Figure 3-2, nous remarquons qu'à une vitesse de 130 km/h, la génération d'une signature numérique augmente la distance de freinage de 0,09 mètre pour P-224 et 0,12 mètre pour P-256. Choisir P-256 au lieu de P-224 entraine une augmentation de 30 cm pour une génération.

D'après la Figure 3-1 et la Figure 3-2, nous remarquons qu'à une vitesse de 130 km/h, la vérification d'une signature numérique augmente la distance de freinage de 0,18 mètre pour P-224 et 0,24 mètre pour P-256. Choisir P-256 au lieu de P-224 entraine une augmentation de 60 cm pour une vérification.

Mais, comme expliqué dans le chapitre 2, dans la majorité des situations, le véhicule ne fera pas confiance à une seule et unique alerte. Il est donc intéressant d'analyser l'impact du temps de calcul

sur la distance de freinage lorsqu'un mécanisme de consensus « naïf » est mis en place (cf. §4.3.2.1). Prenons le cas où le véhicule attend de recevoir au moins n alertes (pour le même événement) lorsque n est égal au nombre de véhicules devant lui et à portée de communication. La Figure 3-3 illustre cette situation pour un véhicule roulant à 130 km/h et ayant un ensemble de voisins allant de 1 à 200. Cet ensemble correspond à une densité maximale de 111 veh/km/voie, ce qui est réaliste dans le cas d'autoroutes à trois voies et plus [KOT 99] [ELH 08]. Nous remarquons que $n = 21$ (pour P-256) et $n = 28$ (pour P-224) suffisent à augmenter la distance de freinage de plus de 5 mètres (soit la taille moyenne d'une voiture). Cela souligne l'importance du temps de calcul et des mécanismes de sécurité déployés.

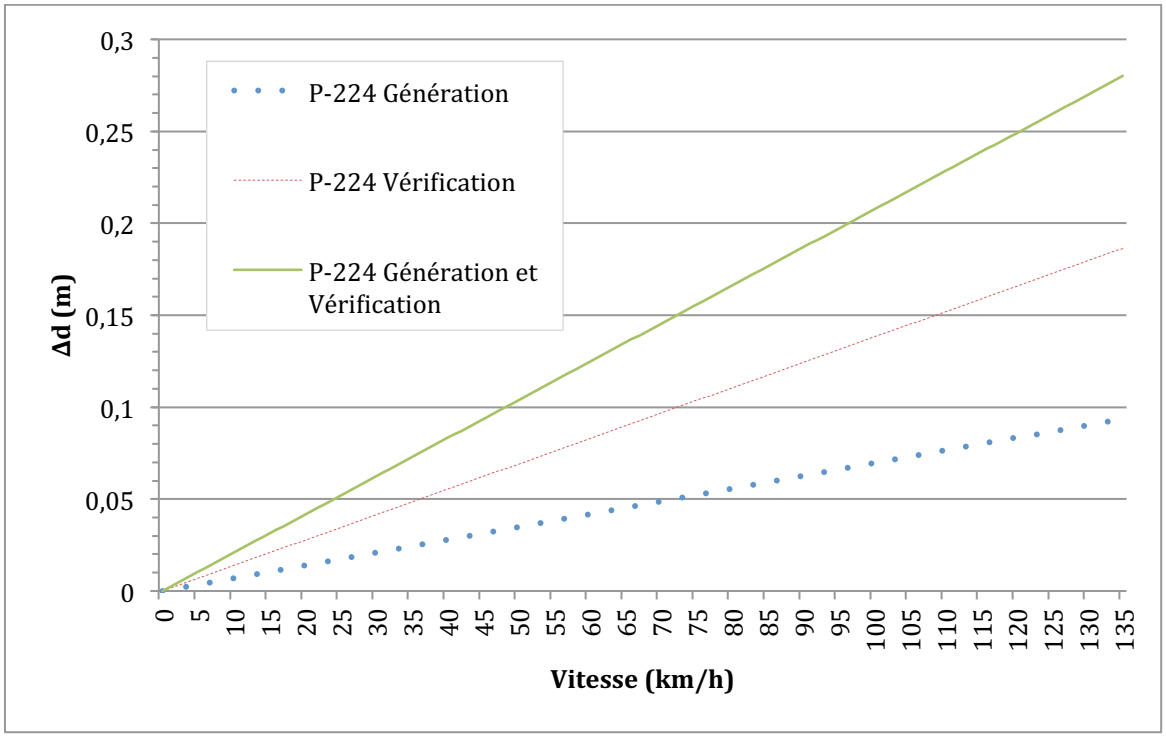

Figure 3-1. P-224 : Surcoût de l'authentification sur la distance de freinage (Δd)

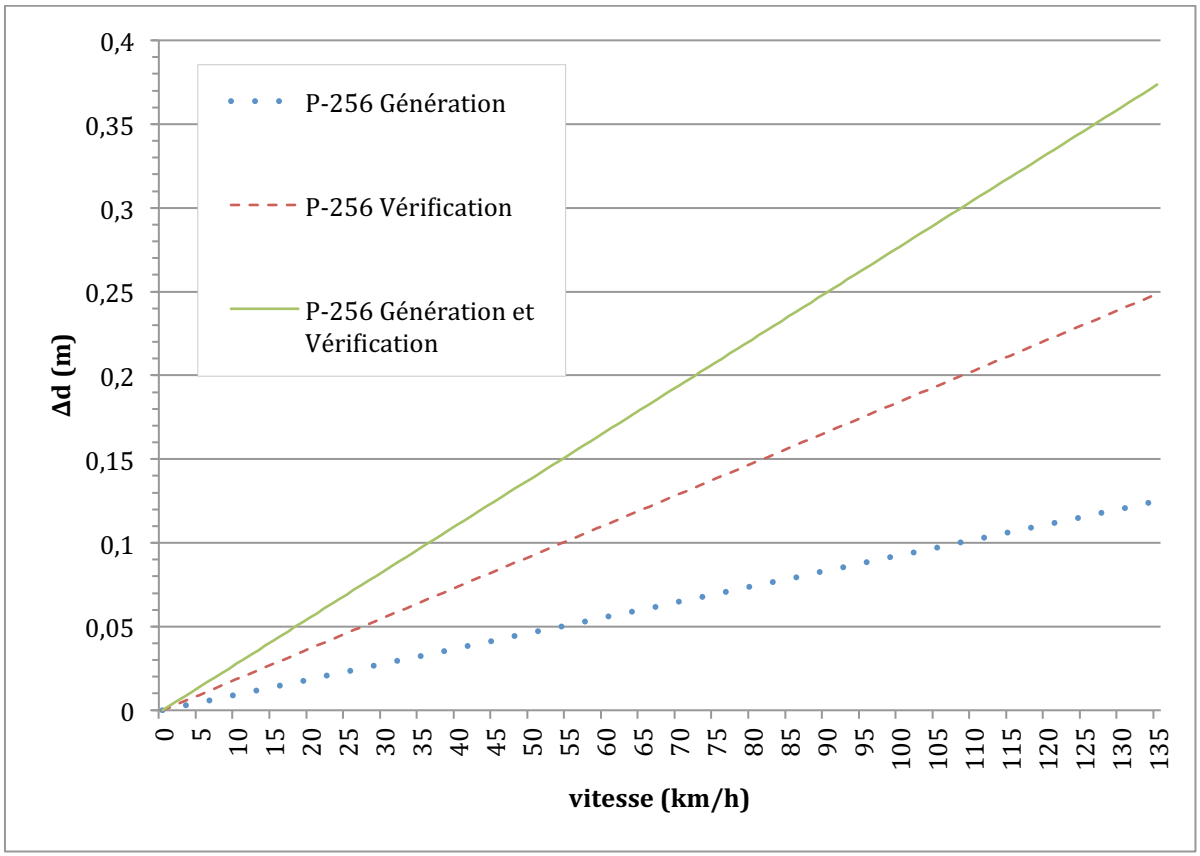

Figure 3-2. P-256 : Surcoût de l'authentification sur la distance de freinage (Δd)

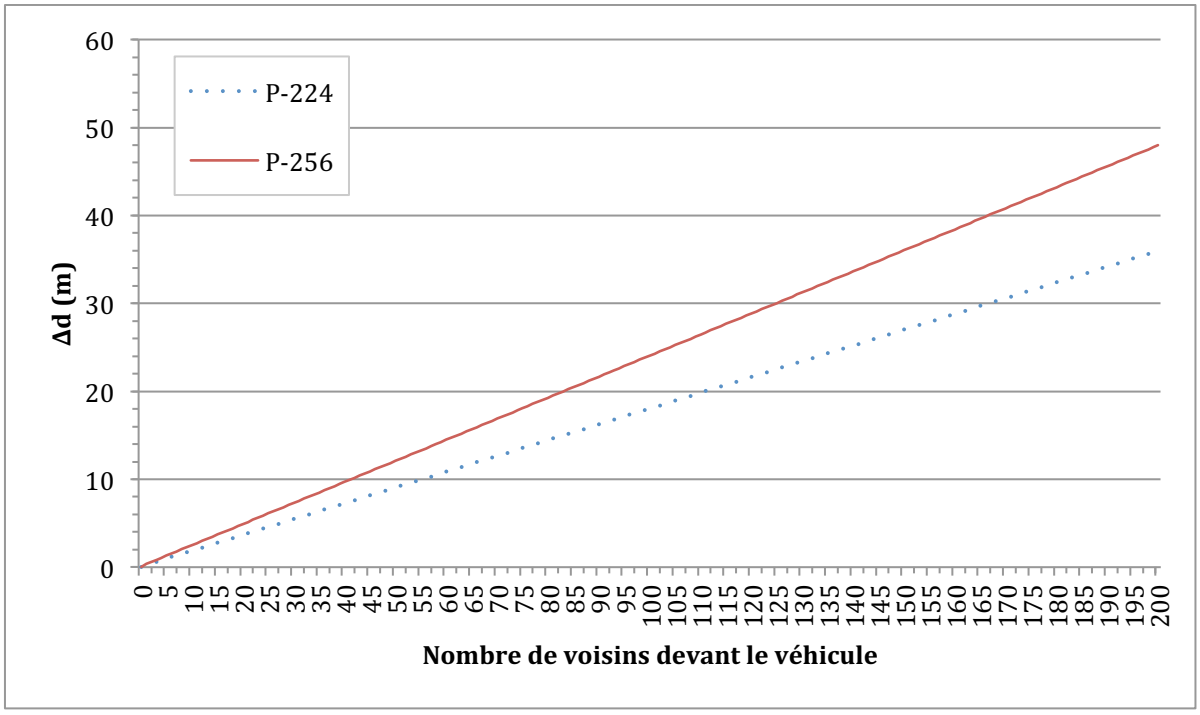

Figure 3-3. Consensus naïf : Impact du nombre de voisins sur la distance de freinage (Δd)

3.3.4 Discussion

Ajouter une signature numérique et un certificat à chaque message de sécurité au nom de la sécurité, crée inévitablement un surcoût qui peut être plus important que le message lui-même. Pour réduire le surcoût, la cryptographie à courbes elliptiques (ECC) est préférée à RSA [RAY 07]. Dans la section 3.3, nous avons analysé l'impact du temps de calcul de signatures ECDSA dans les VANETs. Nous avons plus précisément étudié son effet temporel et spatial. Nous avons aussi introduit un mécanisme de consensus « naïf » afin d'observer les conséquences de génération/vérification de plusieurs messages. Nous retenons que le temps de calcul peut avoir un impact important sur la distance de freinage et doit donc être maîtrisé.

Une solution pour réduire ce surcoût est de signer seulement certains messages (à fréquence régulière). Par exemple, chaque véhicule ne signe qu'un message sur trois. Chaque émetteur et récepteur économise donc respectivement 2 générations et 2 vérifications.

Dans la littérature sur l'authentification dans les VANETs, les signatures NTRU [HOF 98] ont retenu l'attention de la communauté scientifique. En effet, à processeur égal, elles sont plus rapides à calculer que ECDSA. De plus, le cryptosystème NTRU est le seul à résister aux algorithmes quantiques, comme celui de Shor [SHO 97]. Ce qui signifie que si la Physique permet un jour de réaliser le moindre ordinateur quantique, toutes les clés RSA/DSA/ECDSA tomberaient[1]. Néanmoins, les signatures NTRU sont moins compactes et ne sont pas mentionnées dans le standard actuel.

Une amélioration « physique » est de mettre en place un crypto-processeur spécialement conçu pour la génération et la vérification de signature numérique ECDSA avec P-224 et P–256 [JAR 07]. Ainsi on peut espérer un gain significatif sur le temps de calcul.

Une amélioration « mathématique », proposée par la société Certicom, est un algorithme permettant une diminution de 40 % du temps de vérification de signature [ANT 05].

3.4 Analyse du délai de transfert

Après avoir détaillé le surcoût de l'authentification sur le temps de calcul, il est nécessaire d'analyser l'impact de ce service de sécurité sur le délai de transfert d'un message. En effet, un message signé a une taille supérieure à un message non signé. Nous rappelons que la méthode d'accès au support employée dans les VANETs est CSMA/CA (cf §1.5.4). Ainsi, il est établi qu'un message plus grand a une probabilité plus grande de collision. Ainsi, le délai de transfert est augmenté. Dans notre contexte d'application d'alerte de danger local, le délai de transfert est un paramètre sensible. En effet, un véhicule attend après les alertes afin de prévenir le conducteur. Quelques secondes de trop peuvent être fatales.

[1] Pour l'instant, le plus puissant ordinateur quantique jamais réalisé ne sait factoriser que les entiers de 1 à 17, il y a donc encore le temps !

Le terme « délai de transfert » désigne le temps que met un paquet pour être acheminé d'une source vers une destination. Il est égal à la somme des délais sur les liens qui forment ce chemin. Dans le cadre de l'application LDW, les messages sont diffusés à un saut de l'émetteur. Le délai de transfert est donc ici calculé sur un seul saut. Ce temps prend en compte principalement deux étapes : le délai dans la file d'attente des nœuds le long du chemin et le délai de propagation du paquet sur le médium physique. Le problème de la synchronisation des horloges a été mis en relief dans de nombreux travaux, car elle est nécessaire pour la bonne réception des signaux radio, le positionnement (satellite) et les applications de transactions par exemple. Dans le cadre de cette thèse, nous allons supposer que toutes les horloges des entités sont parfaitement synchronisées, et ce, notamment grâce à un équipement de positionnement satellite.

Afin de calculer le surcoût de l'authentification sur le délai de transfert, nous analysons dans un premier temps l'impact sur la taille des messages envoyés.

Le surcoût réseau inclut :

(i) Augmentation de la taille des paquets : Le paquet contient le message, le certificat de la clé utilisée pour signer le message, et la signature.

(ii) Dissémination des informations de révocation : Dans les schémas de révocation basés sur les CRLs, ces listes de révocation doivent être disséminées depuis l'infrastructure vers chacun des véhicules du réseau (potentiellement récepteurs de messages signés à partir de certificats présents dans ces listes).

De la même manière qu'en section 3.3, nous ne considérons que l'opération de signature numérique et étudions donc le surcoût (i) seulement.

3.4.1 Format des messages

D'après la Figure 2-9, un message signé comporte un certificat et une signature. Ainsi le surcoût de l'authentification en terme de taille de message est égal à la somme des deux éléments.

Tout d'abord, quand Alice signe un message avec sa clé privée, rien ne garantit qu'Alice soit une personne de confiance. Le certificat assure cette confiance. La Figure 2-8 montre que la taille du certificat dépend de :

- La taille du point de la courbe (dépendant de l'algorithme utilisé pour générer la clé publique) : S_{pu} (bits) ;
- La taille de la signature utilisée pour signer le certificat : $S_{sigcert}$ (bits).

Ainsi la taille du certificat S_{cert} (octets) est définie par :

$$S_{cert} = \frac{S_{pu}}{8} + 1 + \frac{S_{sigcert}}{8} \times 2 = \frac{S_{pu}}{8} + 1 + \frac{S_{sigcert}}{4} \quad (3.5)$$

Ensuite, pour assurer le service d'authenticité, le message est signé et la signature est attachée au message. La taille de la signature S_{sign} (octets) dépend de la courbe elliptique utilisée $S_{sigmess}$ (bits) et est définie par :

$$S_{sign} = \frac{S_{sigmess}}{8} \times 2 = \frac{S_{sigmess}}{4} \tag{3.6}$$

À partir des deux équations précédentes, lorsque ECDSA est employé, le surcoût global est S_{ov} (octets) :

$$S_{ov} = S_{cert} + S_{sign} = \frac{S_{pu}}{8} + 1 + \frac{S_{sigcert}}{4} + \frac{S_{sigmess}}{4} \tag{3.7}$$

Nous obtenons ainsi la taille totale d'un message signé (WSM) en octets :

$$S_{WSM} = \frac{S_{sigmess}}{8} \times 2 + \frac{S_{sigcert}}{8} \times 2 + \frac{S_{pu}}{8} + 1 + 32 + 20 + 53 = \frac{S_{sigmess}}{8} + \frac{S_{sigcert}}{8} + \frac{S_{pu}}{8} + 106 = S_{ov} + 105$$

où 32 est la taille de l'entête du certificat.

À partir du Tableau 3-6, nous obtenons la taille du surcoût global de l'authentification en fonction de la clé d'authentification choisie pour la signature du certificat, pour la clé publique et pour la signature du message. Par exemple, un certificat signé avec P-256, une clé publique P-224 et un message signé avec P-224 donne un WSM de 254 octets. Le surcoût minimum est donc de 141 octets.

Clé publique S_{pu} (bits)		Signature certificat $S_{sigcert}$ (bits)		Signature message $S_{sigmess}$ (bits)		S_{ov} (octets)	S_{WSM} (octets)
224	256	224	256	224	256		
✓		✓		✓		141	246
✓		✓			✓	149	254
✓			✓	✓		149	254
✓			✓		✓	157	262
	✓	✓		✓		145	250
	✓	✓			✓	153	258
	✓		✓	✓		153	258
	✓		✓		✓	161	266

Tableau 3-6. Surcoût de la taille en fonction de la clé d'authentification

3.4.2 Paramètres influents

Le surcoût de la communication dépend notamment de paramètres de niveau application et de niveau liaison de données. L'application impose une fréquence d'envoi des messages et une réponse en un temps donné. Par exemple le LDW impose l'envoi de messages d'alerte toutes les 100 millisecondes. L'application impose aussi des services de sécurité et un niveau de sécurité. Par exemple, le LDW impose un service d'authentification avec une clé de 224 bits minimum. Ainsi, l'application impacte la taille des messages envoyés. Cela influence donc le comportement de la couche liaison de données.

Il existe aussi des paramètres environnementaux (comme la densité de véhicules à portée de communication) qui influencent la couche liaison de données. En effet, plus la densité est forte, plus il y a de véhicules souhaitant accéder au canal et donc la probabilité de collision augmente. La distance entre les véhicules a aussi une importance, car il y a une augmentation des interférences radio. Les interférences ont un impact fort sur la probabilité de bonne réception des messages [ELB 05].

Il est clairement établi que la taille d'un paquet est liée à la probabilité de collision. Plus un message a une taille importante, plus la probabilité de collision augmente. Ainsi, il existe une taille de paquet optimale pour chaque scénario [BAS 10]. Cette taille optimale dépend des caractéristiques du protocole, de la bande passante disponible et est fortement influencée par le taux d'erreur de bit (BER, *Bit Error Rate*).

La couche MAC utilisée par DSRC a aussi un ensemble de paramètres (DIFS, EIFS, AIFS, taille du buffer, temps de garde) qui influencent le délai de transfert.

3.4.3 Modèle analytique du délai de transfert

Le délai de transfert est défini comme le temps écoulé entre la génération du message et sa correcte réception au niveau application. Cela inclut le délai d'attente dans les files d'attente et le temps de service de la couche MAC et physique (backoff, délai de transmission, délai de propagation, etc.). De nombreux modèles d'analyse du délai de la couche MAC ont été proposés pour les protocoles IEEE 802.11.

Le délai de transfert d'un message M est noté $T_{tx}(M)$. Le surcoût du délai de transfert dû à l'authentification est donc noté $T_{aut}(S_{ov})$. Nous utilisons le modèle de Vinel [VIN 09] afin d'établir le délai de transfert du message, car ce modèle est le plus précis que nous ayons analysé. En effet, ce modèle prend en compte l'environnement des VANETs, où il n'y a pas d'acquittement, ni de retransmissions dans le contexte d'application d'alerte de danger local. Ainsi le délai de transmission est défini par :

$$T_{aut}(S_{ov}) = \frac{W-1}{2}[\sigma P_e + T_S P_s + T_C P_c] + (1-\pi)^{n-1}(1-e)T_S + (1-(1-\pi)^{n-1}(1-e))T_C \qquad (3.8)$$

où T_S et T_C sont respectivement la durée d'une transmission réussie et d'une collision. Ces durées dépendent de la taille du message, des paramètres de la sous-couche MAC (DIFS, EIFS) et de

paramètres de la couche physique (préambule, délai de propagation). Le délai de transmission devient donc :

$$T_{tx}(S_{ov}) = \frac{W-1}{2}\left[\sigma P_e + \left(T_h + \frac{S_{ov}\times 8}{D_R} + DIFS + \delta\right)P_s + \left(T_h + \frac{S_{ov}\times 8}{D_R} + EIFS + \delta\right)P_c\right]$$
$$+(1-\pi)^{n-1}(1-e)\left(T_h + \frac{S_{ov}\times 8}{D_R} + DIFS + \delta\right) \quad (3.9)$$
$$+(1-(1-\pi)^{n-1}(1-e))\left(T_h + \frac{S_{ov}\times 8}{D_R} + EIFS + \delta\right)$$

Dans l'équation (3.9), les paramètres sont :

- W : Taille de la fenêtre de contention
- σ : Durée d'un intervalle de temps (slot time)
- P_e : Probabilité d'avoir le canal libre pour transmettre
- T_h : Durée du préambule et du PLCP
- D_R : Débit de transmission
- δ : Délai de propagation équivalent au temps mis par le signal à la vitesse de la lumière (300000000 m/s). Sur une distance de 300 mètres (cf. portée de communication), ce délai est négligeable et donc fixé à 1 µs.
- P_s : Probabilité de succès de transmission
- P_c : Probabilité de collision
- π : Probabilité d'avoir un véhicule prêt à transmettre dans un slot de temps
- n : Nombre total de véhicules
- e : Probabilité de corruption d'un message à cause d'interférence (bruit)

3.4.4 Paramètres et hypothèses de simulation

Afin d'analyser le surcoût de l'authentification sur le délai de transfert, nous utilisons un simulateur réseau : *Network Simulator 2* (ns-2) [NS2] sous sa version 2.34. Les couches MAC et physique respectent les spécifications du standard IEEE 802.11p [IEE 10]. Le Tableau 3-7 liste les paramètres de simulation utilisés.

Paramètre	Valeur
Modèle de propagation	Nakagami (m=3)
Délai de propagation δ (µs)	1
Intervalle de temps σ (µs)	13
Taille de paquet S_A (octets)	73, 198, 254, 262
Densité de véhicules β (veh/km/lane)	[1 ; 45]
DIFS (µs)	64
EIFS (µs)	248
SIFS (µs)	32
Fréquence d'arrivée de paquet λ (sec)	0,1
CWMin	15
Débit D_R (Mbit/sec)	6
Largeur de bande (MHz)	10
Longueur de préambule (µs)	32
Taille de l'entête PLCP (µs)	8
Durée d'un symbole (µs)	8
Niveau de bruit de fond (dBm)	-99
Seuil de détection (dBm)	-99
SINR pour capture du préambule (dB)	5
SINR pour capture du message (dB)	10
Taille de la file d'attente de la couche MAC (paquets)	50
Vitesse de véhicule (m/s)	v_1=27,7 v_2=30,5 v_3=36,1
Portée de communication (mètres)	300

Tableau 3-7. Paramètres de simulation

Afin de simuler l'impact de la sécurité et du choix de la clé d'authentification, nous utilisons quatre tailles de paquets S_A :

- 73 octets pour un paquet sans sécurité ;
- 198 octets pour un paquet certifié ;
- 254 octets pour un paquet signé avec P-224 et certifié ;
- 262 octets pour un paquet signé avec P-256 et certifié.

Dans nos simulations, nous utilisons le modèle de propagation probabiliste Nakagami (*m=3*) [NAK 58] [PAR 92], car les travaux de Taliwal *et al.* concluent qu'il est le plus adapté à l'environnement véhiculaire [TAL 04]. En effet, ce modèle prend en compte les effets d'affaiblissement de signaux et estime la puissance du signal reçu pour des environnements multichemins. Il est représenté comme une fonction avec deux paramètres Ω et *m*, où Ω est la puissance moyenne du signal reçu et *m* le coefficient d'atténuation. Par exemple, avec une portée de communication de 500 mètres, la probabilité de réception d'un paquet décroit à partir de 200 mètres, tandis qu'avec un modèle de propagation déterministe (*Two-ray ground*) cette probabilité tombe à zéro dès que la distance de 500 mètres est atteinte.

D’après l’Observatoire Européen de la Sécurité Routière [ERS 07] et l’Observatoire National Interministériel de la Sécurité Routière [ONI 10], les autoroutes assurent 28 % du trafic routier français, et 30,7 % des accidents se produisent sur ligne droite. Nous considérons donc le scénario suivant : sur une autoroute à 3 voies dans un sens de direction, des véhicules traversent un tronçon de 5 km en ligne droite. Chacune des voies a une vitesse distincte notée v_i où i est le numéro de la voie. Ces vitesses sont fixées selon la vitesse moyenne sur les autoroutes françaises (cf. Tableau 3-7).

Durant leur passage sur ce segment, certains véhicules (tirés aléatoirement) s’arrêtent (à une position aléatoire) à cause d’un obstacle ou d’un incident sur le véhicule. Le véhicule arrêté envoie alors un message d’alerte toutes les 100 ms. Le véhicule émetteur est marqué comme « en danger ». Les véhicules récepteurs ne retransmettent pas directement l’alerte. Cependant, un véhicule qui détecte un voisin « en danger », émet une alerte pour ce dernier. Après un délai aléatoire, le véhicule repart.

Les véhicules entrent dans le système selon la densité β en véhicule par kilomètre et par voie. Elle dépend du nombre de voies N_L, du coefficient de pénétration du marché γ ($\gamma = 1$ dans notre cas, car nous supposons que 100 % des véhicules sont équipés d’un système DSRC), de la portée de communication R (en kilomètre), du nombre de véhicules N_{TX} présents dans le cercle de rayon R. Elle est calculée grâce à l’équation suivante [WIS 05]:

$$\beta = \frac{N_{TX}}{2\gamma N_L R} \tag{3.10}$$

Nous supposons une densité uniforme de véhicule que nous faisons varier de 1 à 45 veh/km/voie (soit d’un trafic fluide à un embouteillage).

Dans ns-2, tous les nœuds sont générés au début de la simulation et participent au trafic réseau, et ce, même s’ils ne devraient pas. Les nœuds sont générés à l’extrémité gauche de la Figure 3-4 et se déplacer vers l’extrémité droite. Afin d’éviter cet « effet de bordure » indésirable, seuls les véhicules présents dans la zone représentée par le carré noir sont considérés. À partir de la portée de communication fixée à 300 mètres, nous ne considérons pas le premier et le dernier kilomètre de route. Ainsi, nous fixons le carré noir comme l’ensemble du segment autoroutier restant.

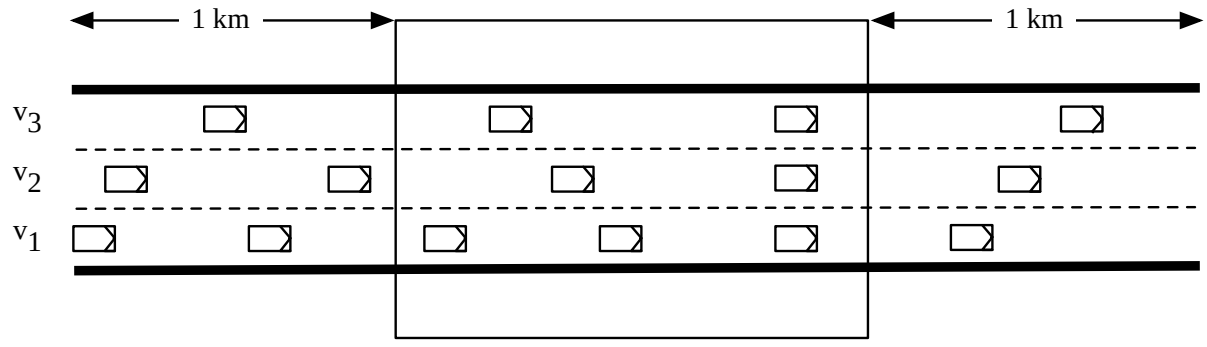

Figure 3-4. Scénario de simulation sur autoroute

3.4.5 Résultats

De la même manière qu'en section 3.3.3, nous présentons les résultats de simulation (avec un intervalle confiance de 95 %) en nous focalisant sur l'aspect temporel et spatial. Nous appréhendons ainsi le surcoût de l'authentification sur le délai de transfert et la distance de freinage, mais aussi l'impact de la taille de la clé d'authentification. Nous introduisons à nouveau un mécanisme de consensus « naïf » afin de mettre en lumière les conséquences d'une utilisation inappropriée de l'authentification.

3.4.5.1 Impact de la taille de la clé d'authentification sur le délai de transfert

La Figure 3-5 présente l'impact de la densité de véhicules sur le délai de transfert d'un paquet. La courbe « *WSM payload* » représente l'envoi d'un message non signé, ni certifié (73 octets). La courbe « *WSM+certificat* » représente un message non signé mais certifié (198 octets). Les courbes P-224 et P-256 représentent un message signé et certifié avec une taille de clé de 224 bits (pour un total de 254 octets) et 256 bits (pour un total de 262 octets) respectivement.

Dans un premier temps, nous remarquons que proportionnellement aux autres cas, un message sans sécurité (*WSM Payload*) est peu influencé par la densité de véhicules. Cela s'explique par la petite taille des paquets échangés et donc du nombre faible de collisions. En effet, plus petite est la taille d'une trame, plus faible est la probabilité de collisions.

L'ajout de sécurité (certificat seul ou certificat et signature) triple le délai de transfert d'un message quand $\beta < 30$ veh/km/voie. Ce délai se voit multiplier par quatre dans les scénarios à forte densité ($\beta > 30$ veh/km/voie). Si nous observons l'impact de la taille de la clé d'authentification (P-224 ou P-256), alors nous remarquons que choisir P-256 au lieu de P-224 entraine une augmentation de 3 % à 8 % du délai de transfert. Par exemple, avec une densité de 35 veh/km/voie, le délai de transfert est de 2 ms pour un WSM.

Cela peut sembler faible à première vue, mais n'oublions pas que la signature numérique ne sera pas le seul mécanisme déployé. En effet, la Figure 3-6 montre l'impact du délai de transfert lorsqu'un mécanisme de consensus « naïf » est employé. Nous remarquons qu'avec une densité de 35 veh/km/voie le surcoût de communication est alors de 120 ms. Afin d'illustrer l'importance de cette valeur, nous rappelons que le délai maximum de déclenchement d'un airbag est de 10 ms par exemple.

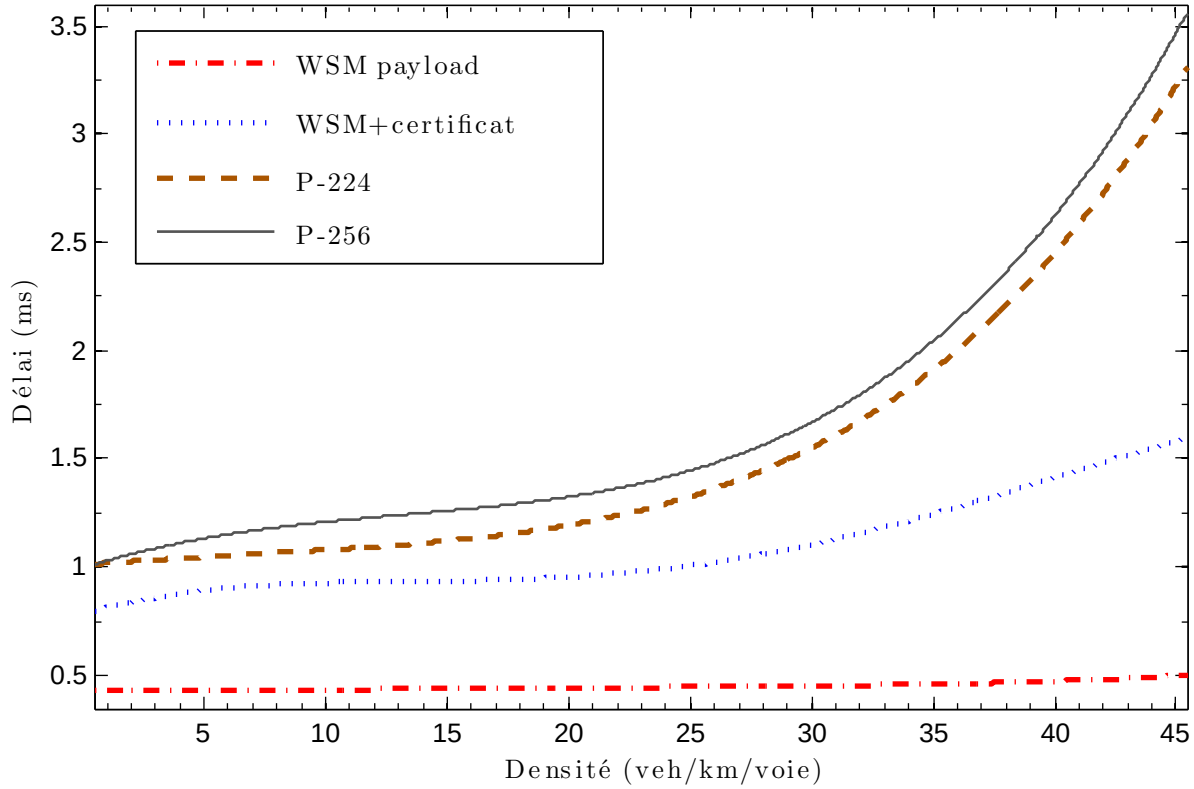

Figure 3-5. Surcoût de communication : Impact de la densité sur le délai de transfert d'un message pour différentes tailles de paquet

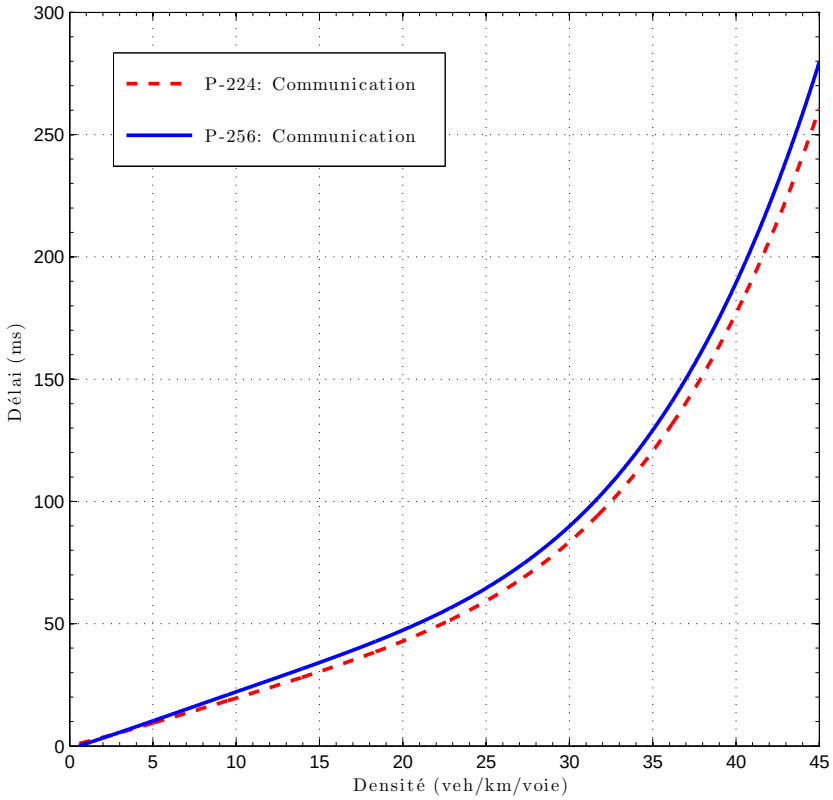

Figure 3-6. Surcoût de communication : Impact de la densité sur le délai de transfert d'un message (consensus naïf)

3.4.5.2 Impact de la taille de la clé d'authentification sur la distance de freinage

Notre contexte de réseaux sans fil véhiculaire entraine que chaque seconde correspond à une distance parcourue (en direction d'un danger potentiel). La Figure 3-7 présente l'impact de la densité de véhicule sur la distance de freinage. Nous considérons le cas où le véhicule se situe sur la voie numéro 3 et a donc une vitesse de 130 km/h. La courbe « *WSM Payload* » montre qu'un message sans sécurité a, comparativement aux autres cas, un faible impact sur la distance de freinage initiale (nous rappelons qu'à partir de l'équation (3.4), un véhicule à 130 km/h s'arrête en 95,82 m). Nous remarquons aussi qu'ajouter un mécanisme de sécurité entraine une augmentation de la distance de freinage. Dans le cas d'une densité faible, la distance de freinage est augmentée au plus de 0,04 m. Pour l'envoi d'un message, elle est augmentée jusqu'à 0,1 m dans les scénarii à forte densité. Nous remarquons que, à l'échelle d'un message, le choix de la clé d'authentification (P-224 ou P-256) a un très faible impact sur la distance de freinage. Cependant lorsqu'un mécanisme de consensus « naïf » est employé, la différence entre P-224 et P-256 est de l'ordre d'un demi-mètre. Plus généralement, comme le montre la Figure 3-8, à 35 veh/km/voie, le surcoût de communication entraîne une augmentation de la distance de freinage de 5 mètres.

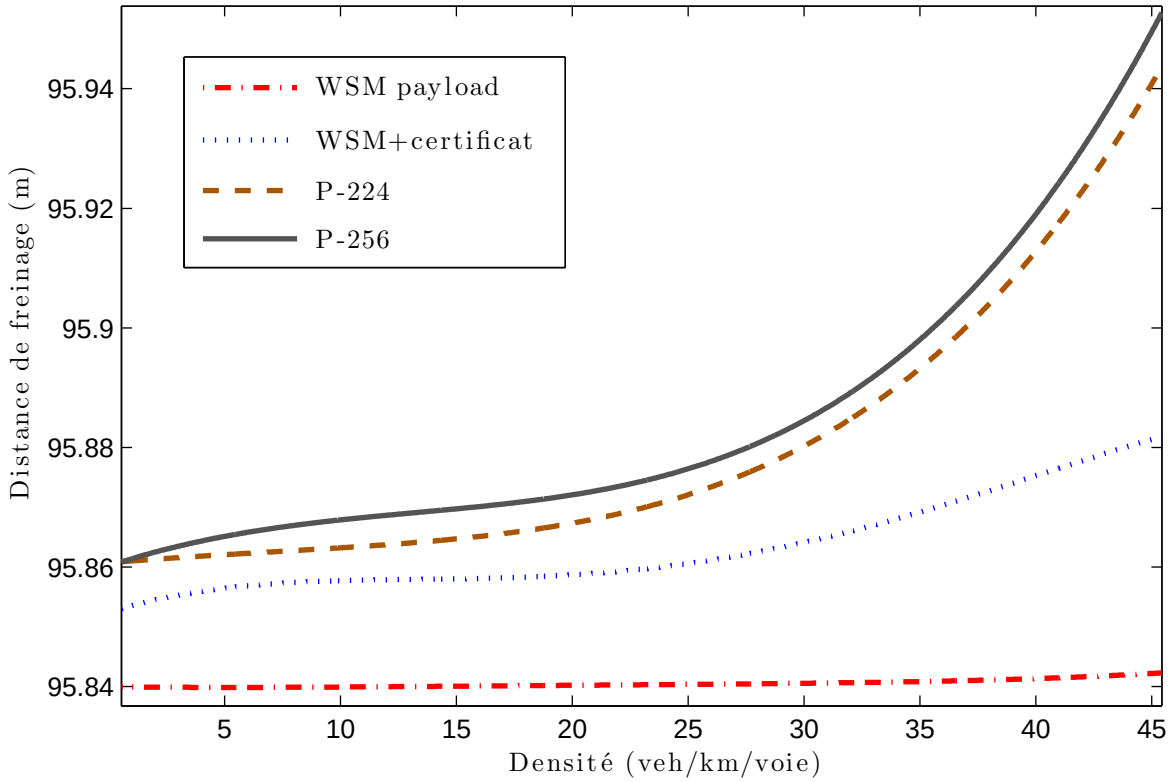

Figure 3-7. Surcoût de communication : Impact de la densité sur la distance de freinage pour un message (différentes tailles)

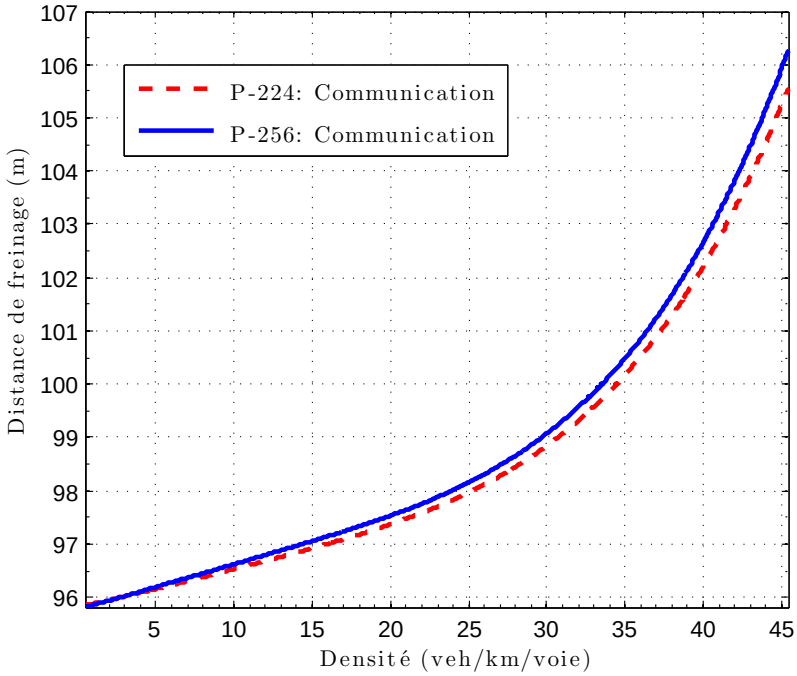

Figure 3-8. Surcoût de communication : Impact de la densité sur la distance de freinage (consensus naïf)

3.4.6 Discussion

Comparativement au temps de calcul, la communication a moins d'influence sur la distance de freinage. Nous étudions plus en détail cet aspect dans la section 3.5.

Là encore, le choix de la clé d'authentification a un impact et doit donc être judicieusement choisie. Par exemple, le niveau de sécurité désiré ou bien le nombre de véhicules dans son voisinage direct peuvent être des facteurs de choix.

Afin de réduire l'impact de l'authentification sur le délai de transfert, l'utilisation de clé de groupe ou du protocole TESLA (protocole de diffusion d'authentification connu dans les MANETs) ont été envisagés [RAY 07].

Une clé de groupe est une information secrète qui doit être connue uniquement par les membres courants du groupe. Cette clé appelée aussi clé de chiffrement du trafic (TEK, *Traffic Encryption Key*) est établie entre les membres du groupe soit par distribution, soit par accord. L'avantage des clés de groupe est qu'elles économisent un surcoût de message. Mais l'établissement de clé de groupe et la mise à jour des membres du groupe, requièrent plus de messages que l'approche par signature numérique. Le surcoût dépend donc du nombre de véhicules et de la dynamique du réseau.

Le protocole TESLA est une alternative à la cryptographie asymétrique [PER 02]. En effet, TESLA utilise la cryptographie symétrique, la divulgation de la clé retardée et une synchronisation d'horloge afin d'assurer une asymétrie suffisante pour l'authentification. L'analyse de performance de TESLA dans les VANETs [HAA 09] a démontré que la taille inférieure des paquets (comparativement à ceux

dans le cas d'ECDSA) entraine un pourcentage de réception supérieur. Néanmoins, la divulgation de la clé entraine l'envoi d'un message supplémentaire. Cela a deux conséquences :

- Le risque de congestion réseau est augmenté.
- Pour vérifier un message d'alerte, il faut attendre de recevoir correctement deux paquets (le message d'alerte et le paquet contenant la clé).

Enfin, à des distances supérieures à 200 mètres, le protocole ECDSA présente de meilleures performances que TESLA (ce qui est important pour la détection de collision par exemple).

3.5 Combinaison du temps de calcul et du délai de transfert

Après avoir analysé l'impact de l'authentification sur le temps de calcul et le délai de transfert séparément, nous les additionnons pour obtenir le surcoût global de l'authentification. En effet, le surcoût global en temps de l'authentification d'un message *M* est défini comme la somme du temps de calcul (génération et vérification de signature numérique) et du temps de transfert du message signé. Ce surcoût est donné par l'équation suivante :

$$T_{ov}(M) = T_{sign}(M) + T_{tx}\left(Sign_{PrK_V}[M]\right) + T_{verif}(M) \tag{3.11}$$

où :

- $T_{sign}(M)$: Temps de génération d'une signature numérique pour le message *M*.
- $T_{verif}(M)$: Temps de vérification d'une signature numérique pour le message *M*.
- $Sign_{PrK_V}[M]$: Signature du message *M* obtenue avec la clé privée de l'émetteur *V*. Elle inclut le certificat du CA qui a délivré la clé.
- $T_{tx}\left(Sign_{PrK_V}[M]\right)$: Temps pour transmettre la signature $Sign_{PrK_V}[M]$.

Comme nous nous intéressons au surcoût de l'authentification, nous ne considérons que le délai de transfert du surcoût S_{ov}. Nous le définisson comme $T_{tx}(S_{ov}) = T_{tx}(M_0 + S_{ov}) - T_{tx}(M_0)$ ou M_0 est le message initial non signé. Comme $T_{tx}(S_{ov}) = \frac{S_{ov}}{D_R}$ où D_R est le débit de transmission et S_{ov} défini par l'équation (3.7), le surcoût temporel global est donc calculé ainsi :

$$\begin{aligned} T_{ov}(M) &= T_{sign}(M) + T_{tx}(S_{ov}) + T_{verif}(M) \\ &= (6n+2)T_{MUL} + T_{INV} + 5nT_{SQR} + T_{HASH} \\ &+ \frac{W-1}{2}\left[\sigma P_e + \left(T_h + \frac{S_{pu} + 2\times\left(S_{sigcert} + S_{sigmess}\right) + 8}{D_R} + DIFS + \delta\right)P_s\right. \\ &\left. + \left(T_h + \frac{S_{pu} + 2\times\left(S_{sigcert} + S_{sigmess}\right) + 8}{D_R} + EIFS + \delta\right)P_c\right] \end{aligned} \tag{3.12}$$

$$+(1-\pi)^{n-1}(1-e)\left(T_h+\frac{S_{pu}+2\times\left(S_{sigcert}+S_{sigmess}\right)+8}{D_R}+DIFS+\delta\right)$$
$$+\left(1-(1-\pi)^{n-1}(1-e)\right)\left(T_h+\frac{S_{pu}+2\times(S_{sigcert}+S_{sigmess})+8}{D_R}+EIFS+\delta\right)$$
$$+(12n+2)T_{MUL}+T_{INV}+10nT_{SQR}+T_{HASH}$$

La Figure 3-9 illustre la proportion du temps de calcul (« *processing* ») dans le surcoût global de l'authentification. Nous remarquons que 80 % du surcoût est dû au temps de calcul.

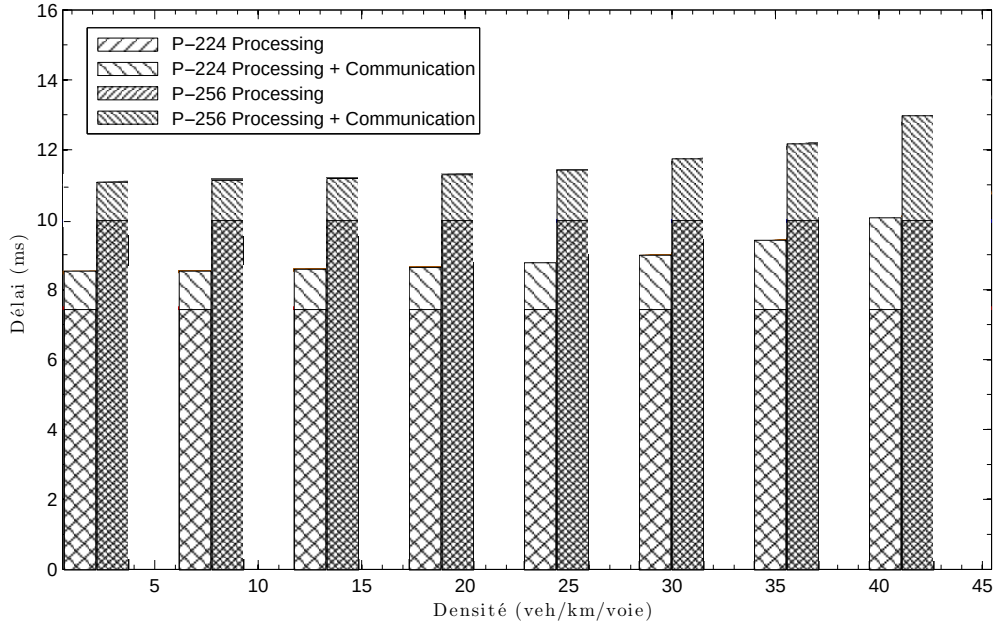

Figure 3-9. Proportion du temps de calcul par rapport au surcoût global

3.5.1 Impact sur le délai de transfert

La Figure 3-10 présente l'utilisation d'un consensus « naïf » et la différence entre le temps de calcul et le délai de transfert (communication). Plus la densité augmente, plus le nombre de messages à vérifier est important. Nous remarquons que le temps de calcul est supérieur au délai de transfert. Par exemple, pour une densité de 35 veh/km/voie, le délai de transfert est de 100 ms, tandis que le temps de calcul est de 400 ms. Cela donne un total de 500 ms. Utiliser P-256 à la place de P-224 engendre un impact plus important sur le temps de calcul que sur le délai de transfert. En effet, les courbes de communication sont sensiblement différentes, alors qu'il y a un écart important entre les courbes de calcul. Par exemple, à 35 veh/km/voie, la différence entre P-224 et P-256 est de 150 ms pour le temps de calcul, et de moins de 10 ms pour le délai de communication.

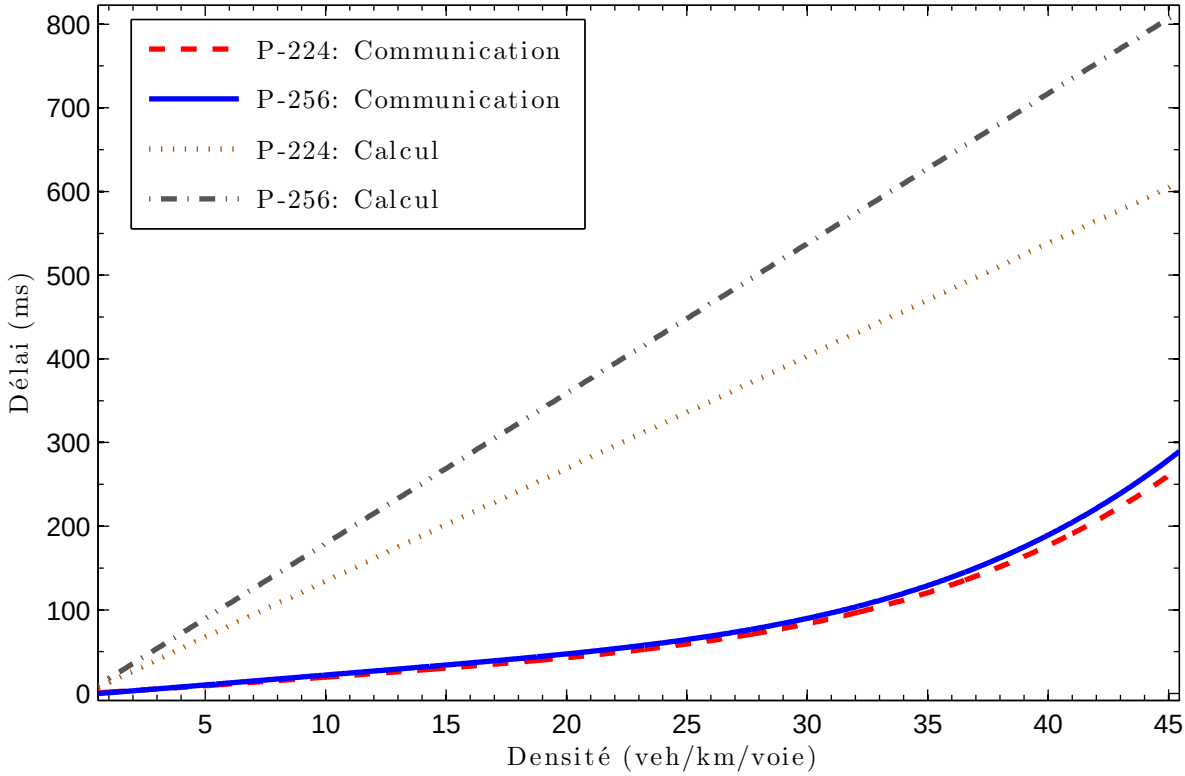

Figure 3-10. Surcoût de communication : Calcul vs. Communication (consensus naïf)

3.5.2 Impact sur la distance de freinage

De la même manière que les sections précédentes, nous analysons l'impact global sur la distance de freinage. La Figure 3-11 présente le surcoût du temps de calcul et de communication et son impact sur la distance de freinage. La courbe « *no message* » représente la distance de freinage sans le traitement de WSM. Nous remarquons que l'authentification d'un message ajoute 0,3 m à la distance de freinage pour P–224 et 0,4 m pour P–256. Cependant, la partie « réseau » semble peu influente sur un seul message. Mais l'on sait que l'authentification ne sera pas déployée seule et que le consensus sera présent.

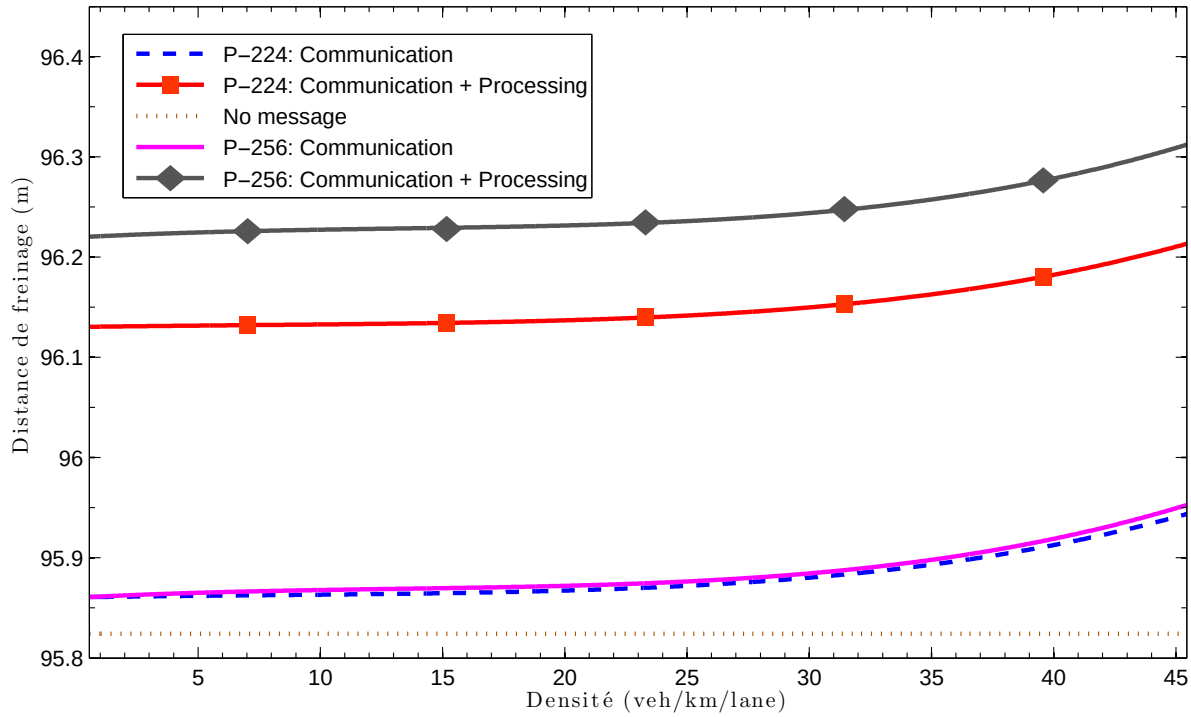

Figure 3-11. Impact de la densité sur la distance de freinage : Proportion du temps de calcul par rapport au surcoût global

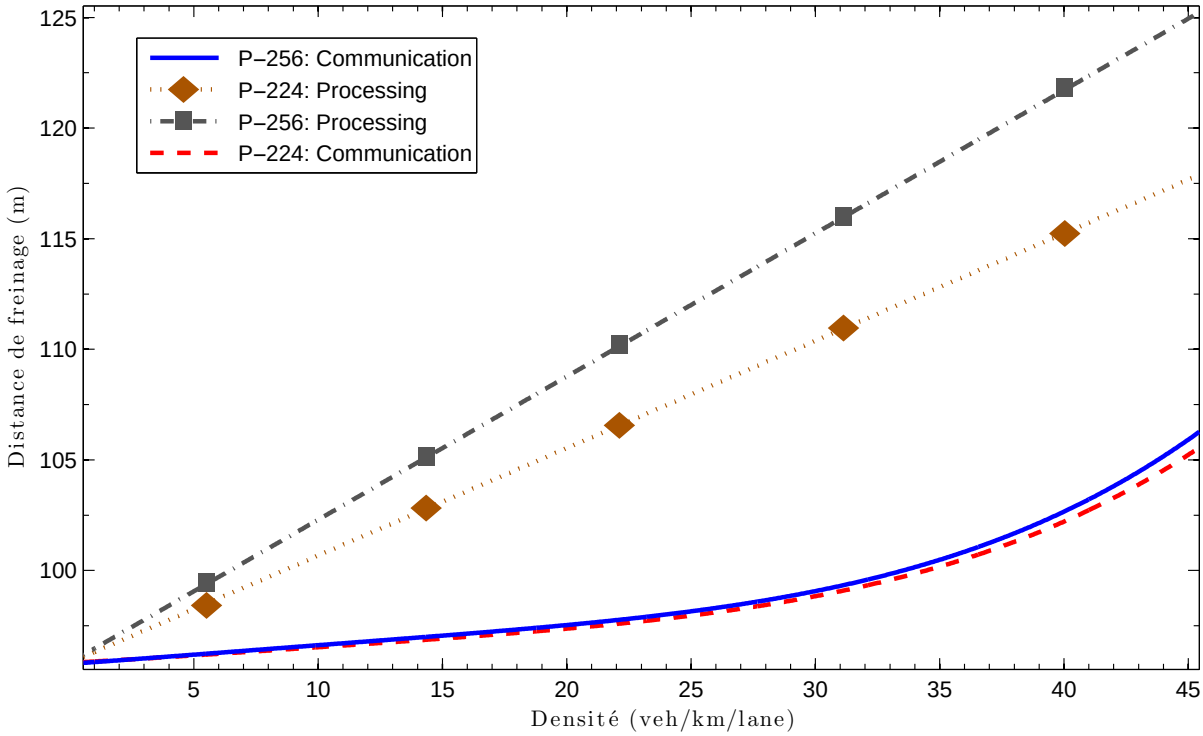

Figure 3-12. Surcoût global : Impact de la densité sur la distance de freinage (consensus naïf)

La Figure 3-12 montre l'impact d'un consensus « naïf » sur la distance de freinage. Pour une densité de 35 veh/km/voie, la communication ajoute 5 mètres à la distance de freinage, tandis que le calcul (« *processing* ») ajoute 17 mètres. Nous obtenons un total de 22 mètres (soit plus d'un cinquième de la

distance de freinage initiale). L'utilisation de P-256 au lieu de P-224 ajoute, dans cet exemple, 5 mètres à la distance de freinage. Une telle différence peut entraîner une collision. Ces résultats démontrent l'importance d'une méthode de décision cohérente avec les objectifs applicatifs, mais aussi avec les performances réseau attendues.

3.6 Conclusion

L'ajout de mécanismes de sécurité amène un surcoût qui affecte les performances des communications V2V et des applications de sécurité du trafic routier. Dans ce chapitre, nous avons analysé le surcoût global du protocole ECDSA. Pour ce faire, nous avons tout d'abord étudié le protocole ECDSA afin de calculer sa complexité en temps.

Nous avons ensuite analysé le surcoût de l'authentification sur le temps calcul et le délai de transfert. Les résultats obtenus par expérimentations et simulations ont montré que le surcoût « calcul » a un impact temporel supérieur au surcoût « réseau ». Cependant, le surcoût « calcul » est très dépendant de l'architecture physique choisie (processeur, implémentation d'ECDSA). Les axes d'amélioration du temps de calcul d'ECDSA sont d'ordre mathématique (méthode de calcul plus rapide) ou architectural (processeur spécialisé).

Au niveau du délai de transfert d'un message, l'impact de l'authentification est faible. Néanmoins, une amélioration peut se faire au niveau du certificat (ne pas l'apposer à chaque message par exemple).

De manière globale, nous avons souligné l'importance de l'authentification et l'impact que peut avoir le choix de la clé d'authentification tant sur le délai que sur la distance de freinage. En effet, selon les exigences applicatives, la distance de freinage est augmentée d'au moins la longueur moyenne d'une voiture dans les scénarii à forte densité. Nous avons aussi mis en lumière l'impact de la taille de la clé d'authentification afin d'adapter ce paramètre de sécurité aux exigences applicatives.

Introduit au chapitre 2, nous avons vu ici que le mécanisme de consensus peut avoir un fort impact sur la distance de freinage et soulève donc de nombreux challenges. Par exemple, à densité moyenne, le consensus entraine une augmentation de la distance de freinage supérieure à 5 mètres. Ainsi, comment définir les paramètres de consensus afin de réduire l'impact de ce mécanisme sur le délai et la distance de freinage ? Comment s'intègre le consensus dans la formule globale de surcoût de l'authentification ? C'est notamment à ces questions que le chapitre suivant répondra.

4 Consensus dans les réseaux sans fil véhiculaires

Dans les réseaux sans fil ad hoc, un problème majeur est l'établissement de la confiance. En effet, dans un environnement sans infrastructure, comment être certain de pouvoir faire confiance aux autres entités ? Depuis quelques années, le problème de la confiance est un sujet de recherche actif dans les MANETs et les VANETs [BIS 10] [FEN 07] [TAJ 10] [ZHA 11]. Dans le contexte des VANETs, le besoin de confiance en l'information reçue est exacerbé, car le véhicule récepteur prendra une décision à partir de cette information. Par exemple, un véhicule roulant à 130 km/h reçoit l'information qu'un véhicule est arrêté sur sa voie. Il va donc prendre la décision de changer de voie et de ralentir. Malheureusement, comme nous l'avons souligné dans les chapitres 2 et 3, un véhicule authentifié peut générer de fausses alertes. Ainsi, dans notre exemple, le véhicule va peut être prendre une mauvaise décision, c'est-à-dire, changer de voie, ce qui l'amènera sur un danger réel.

Pour éviter ce genre de situation, une méthode consiste à recevoir la même alerte de plusieurs véhicules afin de corroborer l'alerte initiale. Le véhicule récepteur ne prendra ainsi une décision non plus à partir d'un unique message, mais d'un ensemble de messages. Ce mécanisme est appelé *consensus*.

Le but de ce chapitre est d'analyser le surcoût du consensus dans les VANETs et de proposer une méthode de décision dynamique afin de réduire l'impact du consensus. Ainsi, après avoir défini les notions de confiance et de consensus, nous présentons le fonctionnement général du consensus et nous nous focalisons sur le processus de décision. Nous proposons ensuite une modélisation des méthodes de décision dans la section 4. Ainsi, à partir d'un modèle conceptuel, nous pouvons en déduire un modèle analytique pour calculer le surcoût de la méthode de décision (appelé *délai de décision*). Dans la section 5, nous analysons la méthode de décision proposée par Ostermaier *et al.* [OST 07]. Nous

l'étendons en section 6 en proposant une méthode de décision dynamique qui prend en compte l'état du réseau (nombre de voisins, historique de transmission, probabilité de collision), l'environnement local (capteurs, informations reçues par les voisins), et le contenu de l'information en elle-même. Nous explicitons en détail la méthodologie pour définir les paramètres du consensus. En section 7, nous intégrons le consensus dans la formule du surcoût global de la sécurité et explicitons l'impact du consensus.

4.1 Définition

Nous définissons tout d'abord la notion de confiance avant de présenter la notion de consensus qui est un mécanisme répondant au besoin de confiance. Nous détaillons aussi les travaux existants sur ces deux notions.

4.1.1 Notion de confiance

« Confiance : Espérance ferme que l'on place en quelqu'un, en quelque chose, certitude de la loyauté d'autrui. » Dictionnaire de l'Académie française.

À partir de cette définition, nous distinguons deux types de confiance : la confiance en la personne (l'entité) et la confiance en l'information (la donnée, l'alerte).

Dans la majorité des travaux réalisés sur la notion de confiance, la confiance d'un véhicule envers les données (*data trust* ou *content trust* en anglais) est exclusivement basée sur les relations de confiance précédemment établies entre les entités du réseau (*entity trust* en anglais). Ainsi, toute nouvelle relation de confiance en une donnée reçue est établie uniquement à partir de la confiance que l'on a en l'entité qui produit cette donnée. Les systèmes de réputation actuels fonctionnent avec ce type de confiance [BUC 08]. Cependant, dans l'« *entity trust* » (aussi appelée confiance centrée sur l'entité, *entity-centric trust* en anglais), les relations de confiance évoluent généralement lentement dans le temps. Une fois établies, elles changeront après de nombreuses opérations (révocation de certificat, surveillance, vote). La notion d'« *entity trust* » fait donc preuve d'une réactivité lente.

De nombreux systèmes de réseaux mobiles sont fortement centrés sur la donnée dans leur fonctionnement (*content-centric trust* en anglais) et opèrent dans des environnements éphémères (durée de vie courte, connectivité entre les entités courtes). Dans ce contexte, il est plus approprié d'établir une confiance en la donnée plutôt qu'en l'entité qui la diffuse. Par exemple, dans les VANETs, l'identité des véhicules n'est pas une information importante comparée aux alertes ou aux informations sur le trafic.

Dans de tels scénarii, et contrairement aux schémas traditionnels d'établissement de la confiance, le niveau de confiance associé à la donnée n'est pas le même que celui associé au véhicule qui a généré celle-ci. Plus précisément dans les VANETs, les véhicules ont des niveaux prédéfinis de confiance (les véhicules de police sont plus fiables que les véhicules privés), mais :

(i) Différents événements reportés par le même véhicule peuvent avoir un niveau de confiance différent (dû à la distance de l'événement ou l'heure de l'alerte par exemple).

(ii) Le même événement rapporté par plusieurs véhicules (qui ont un niveau de confiance prédéfini différent) doit avoir un unique niveau de confiance (qui va différer du niveau de confiance de base des dits véhicules).

(iii) Un événement rapporté par un véhicule requiert une vérification par les autres véhicules et par conséquent son niveau de confiance va différer de celui du véhicule initiateur de l'alerte.

En d'autres termes, la question suivante se pose naturellement : comment les VANETs peuvent être efficaces et de confiance quand leurs caractéristiques opérationnelles de base ne sont pas satisfaites avec les notions existantes de confiance ? Une technique pour répondre à ces besoins est l'établissement de la confiance basée sur la donnée [RAY 09].

La logique *content-centric trust* étend les notions traditionnelles de confiance et les méthodes d'établissement de la confiance selon trois axes. Tout d'abord, contrairement à la confiance traditionnelle, les relations de confiance entre les entités représentent seulement un des paramètres pour établir la confiance de la donnée. Deuxièmement, les relations de confiance centrée sur la donnée sont par définition éphémères et doivent être établies et rétablies fréquemment en fonction des changements perçus dans le réseau. Par exemple, une alerte (accident, verglas), qui doit être délivrée aux récepteurs le plus rapidement possible, ne doit pas être diffusée plus longtemps que le temps de l'alerte réelle. Troisièmement, la confiance ne découle pas d'une unique source de donnée et elle est généralement dépendante de l'application.

Nous déduisons la confiance centrée sur la donnée (l'alerte) de plusieurs éléments de preuve (alertes émanant de plusieurs véhicules). Ainsi, chaque alerte a un niveau de confiance selon sa fraîcheur et son emplacement géographique par exemple. L'alerte et son niveau de confiance serviront d'entrée à la méthode de décision (*classifier*/*decision maker* que nous présentons en section 4.6).

Parmi les travaux menés sur l'établissement de la confiance, nous citons à titre d'exemple ceux sur l'inférence bayésienne (*Bayesian Inference*) [HOW 05], la théorie de Dempster-Shafer (DST, *Dempster-Shafer Theory*) [SHA 02], l'entropie [SUN 06], et la transitivité [THE 06]. Directement liés aux VANETs, et par conséquent sera notre base de travail, les travaux d'Ostermaier *et al.* [OST 07] proposent d'utiliser le mécanisme de consensus pour assurer le besoin de confiance de type *content-centric*.

4.1.2 Notion de consensus

« Accord exprès ou tacite établi entre les membres d'un groupe, d'un parti, d'une conférence diplomatique, sur l'action à mener, la politique à suivre. » Dictionnaire de l'Académie française.

D'après la définition, le consensus permet de prendre une décision à partir d'un ensemble d'informations. Les principaux avantages des systèmes de réputation, que sont l'auto-organisation et la

décentralisation, sont aussi valables pour le consensus. Mais le consensus offre en plus une simplicité, un passage à l'échelle et une réactivité forte au changement de situation [DOT 07]. L'application du consensus sur un ensemble fini d'événements permet de calculer la plausibilité des messages, et ainsi, permet de détecter et de prévenir les mauvais comportements dans les VANETs. Un des objectifs du consensus est d'assurer que les véhicules légitimes pourront filtrer les messages erronés avec une probabilité élevée.

Parmi les travaux menés sur cette notion, nous citons ceux de Golle *et al.* [GOL 04] qui proposent de valider les données reçues à partir d'un modèle de comportement et un modèle d'attaquant. Chaque véhicule utilise ces modèles pour détecter les inconsistances et en rechercher la cause. Le véhicule choisira alors l'explication qui lui semble la plus plausible pour contrer ces inconsistances. Cependant, leurs modèles sont principalement basés sur la lecture des capteurs du véhicule. Ils utilisent simplement les communications V2V pour vérifier la position géographique des voisins (et supposent une communication parfaite, négligeant les délais, les pertes et les collisions).

Ostermaier *et al.* proposent d'utiliser un schéma de vote comme mécanisme de consensus afin d'évaluer la plausibilité des informations transitant sur un VANET [OST 07]. Ils proposent quatre schémas de vote et analysent les performances pour l'application d'alerte de danger local. Nous les détaillons en section 4.3.2 et mettons en exergue leurs limites en section 4.5.3.

Une étude récente [HYU 10] propose d'examiner six sources d'informations différentes pour détecter les faux messages et calculer une valeur de *confiance en l'événement*. Les six sources sont :

1. Le résultat de vérification de signature numérique.

2. L'emplacement géographique de la source.

3. Les capteurs locaux au véhicule.

4. Les messages des autres véhicules : Y a-t-il une contradiction entre les alertes ?

5. La validation par une infrastructure (RSU).

6. La réputation de l'émetteur.

Ce modèle de validation d'alerte est basé sur deux composants : le *seuil* et la *certitude de l'événement* (CoE, *Certainty of Event*).

Le seuil est défini par la *courbe du seuil*. L'importance d'un événement dépend de la distance entre l'événement et le conducteur. La courbe du seuil décroit donc avec la distance et présente trois aspects :

- Un seuil élevé permet la validation de faux messages.

- Un seuil bas permet d'éviter la suppression d'alertes valides.

- L’annonce de l’événement doit être retardée afin d’éviter de notifier trop tôt le conducteur.

Cette contradiction amène à proposer un seuil qui diminue au fur et à mesure que le conducteur s’approche du lieu de l’événement.

La *courbe CoE*, quant à elle, définit le CoE et augmente lorsque le véhicule s’approche de l’événement (car le nombre de messages rapportant l’événement augmente). Le CoE n’est calculé qu’après avoir vérifié les sources 1, 2, 3 ou 5. Une approche de calcul linéaire consiste à faire la somme de la valeur de réputation (source 6) multipliée par le nombre de messages reçus (source 4). Si l’on considère que tous les véhicules ont une réputation égale à 1, alors le CoE est la somme des messages reçus pour l’événement.

L’OBU alerte le conducteur lorsque la courbe CoE croise la courbe de seuil. Ainsi, cela permet une notification plus rapide pour les alertes proches, et de laisser plus de temps au conducteur pour réagir. Un véhicule va donc agréger les six sources d’informations pour évaluer la validité de l’alerte.

Afin de minimiser l’utilisation du processeur et le temps de calcul, le modèle propose une priorisation des sources en fonction de l’application. En effet, toutes les sources ne sont pas forcément pertinentes pour certaines applications. Par exemple, la validation par un RSU n’est pas réalisée dans le cadre de l’application d’alerte de freinage électronique (*Emergency Electronic Brake Lights*) [ZAN 08].

Cependant, une limite de ce modèle est qu’il ne considère que la distance entre le véhicule et le lieu de l’événement. Nous pouvons donc le raffiner en ajoutant des paramètres, qui nous semblent importants, comme la vitesse ou la criticité de l’alerte par exemple.

4.2 Consensus et application de sécurité du trafic routier : Fonctionnement du LDW

L’alerte de danger local (LDW, cf. §1.1.3 et §2.3) est une application coopérative qui fonctionne selon trois processus : détection, dissémination et décision. Nous détaillons chacun des processus avant de nous focaliser sur le processus de décision.

4.2.1 Processus de détection

L’hypothèse la plus importante qui régit le fonctionnement de l’application LDW est la détection automatique de danger sur la route. Ce n’est pas une tâche évidente et soulève de nombreuses questions [ADL 06] [DOE 05]. Dans le cadre de cette thèse, nous supposons que chaque véhicule peut détecter un danger de deux manières : grâce à ses capteurs (radar ou lidar par exemple), ou bien à partir d’une série de messages d’informations (*beacons*) envoyés par le véhicule « en danger ». En effet, à partir de deux *beacons*, le véhicule récepteur peut en déduire l’arrêt du véhicule émetteur (vitesse à zéro, position géographique identique). Dans la suite, nous appellerons *événement* le fait de détecter la présence ou l’absence d’un danger.

4.2.2 Processus de dissémination de l'alerte

Après un événement, le véhicule détecteur génère un message d'alerte (aussi appelé *alerte*) et le diffuse. Les véhicules récepteurs stockent l'information et peuvent la relayer aux autres véhicules présents dans la zone de danger. En combinant toutes les informations reçues pour chaque événement, chaque véhicule est capable d'avoir un état courant de la route devant lui. Deux types de messages sont considérés : le *message d'alerte* et le *message de révocation*. Lorsqu'un événement est détecté, un message d'alerte est généré. Lorsqu'un véhicule passe à proximité d'un lieu d'un événement précédemment détecté (par un autre véhicule) et qu'il ne détecte rien, il envoie un message de révocation afin de prévenir que l'événement a peut-être disparu (embouteillage terminé, risque de verglas terminé).

4.2.3 Processus de décision

Le processus de décision utilise en paramètre d'entrée les messages collectés durant la phase de dissémination. Néanmoins, les événements rapportés par les autres véhicules ne nécessitent pas d'être évalués constamment. Cela n'est nécessaire que lorsque le véhicule s'approche du danger et se situe dans la *zone de décision*. C'est à ce moment-là que l'application de LDW doit décider s'il faut prévenir le conducteur ou réagir (dans le cas de véhicule autonome ou de situation fortement dangereuse, c'est-à-dire qu'il est sûr et certain que la réaction est humainement impossible dans le temps imparti). Ainsi, prendre une mauvaise décision durant ce processus est une des menaces les plus sérieuses dans ce type d'application.

4.2.4 Diagramme d'états

La Figure 4-1 présente les différents états dans lesquels un OBU peut être lorsqu'un mécanisme de consensus est utilisé. Nous retrouvons les trois processus : détection, dissémination et décision. Dans l'état *idle*, le véhicule ne fait rien (si ce n'est se déplacer et émettre des *beacons*). Lorsqu'un risque est détecté, l'OBU passe dans l'état *envoi alerte*. Tant que le risque est détecté, l'OBU va émettre un message d'alerte à une certaine fréquence (définie par l'application, 100 ms pour le LDW). La cible de cette alerte peut être lui-même (le véhicule s'arrête à cause d'une panne par exemple), un autre véhicule, ou l'environnement (verglas, nid de poule, obstacle). Lorsque le risque disparaît, l'OBU revient en état *idle*. L'état *réception alerte* est atteint lorsqu'un OBU reçoit un message d'alerte. Si l'OBU récepteur reçoit un message de fin d'alerte ou qu'il a dépassé le lieu du danger, alors il repasse à l'état *idle*. Si par contre il reçoit *assez* d'alertes (en fonction des paramètres du consensus), alors il passe dans l'état *décision*. Nous verrons qu'une difficulté est de définir ce « *assez* ». Une autre possibilité de transition est quand le délai maximum de l'application est dépassé. En effet, les applications de sécurité du trafic routier ont des contraintes temporelles fortes et nécessitent une réaction avant un délai T_{MAX}. Ce délai est inférieur à 500 ms pour les applications les plus contraintes, et égal à trois secondes pour les autres [KAR 06]. Dans la Figure 4-1, T représente le temps entre la première réception de l'alerte et l'heure actuelle. Dans l'état *décision*, l'OBU déclenche sa méthode de décision et applique le résultat (émission, alerte du conducteur, freinage, etc.).

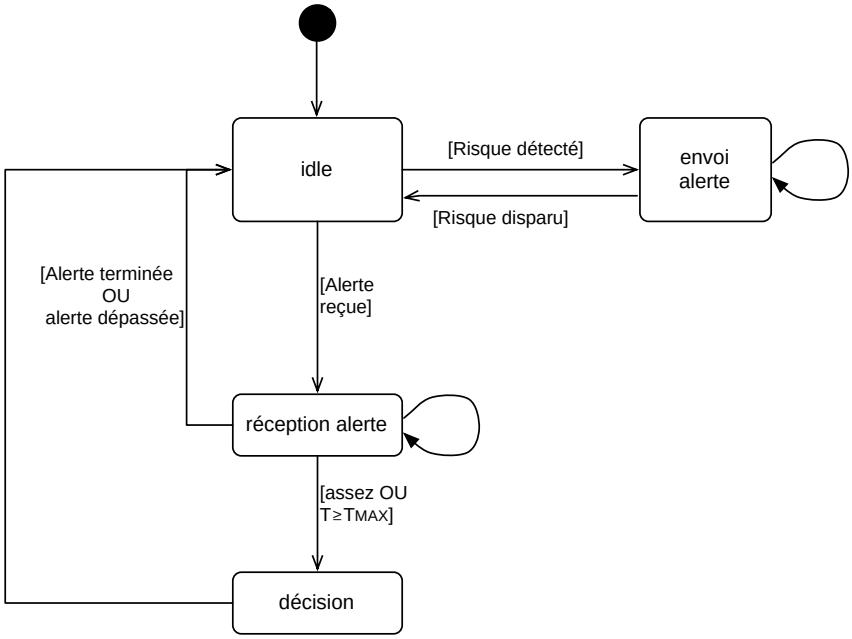

Figure 4-1. Diagramme d'états-transitions du consensus

4.2.5 Schéma des zones

Nous avons évoqué précédemment la notion de zone de décision. La Figure 4-2 représente les différentes zones que nous considérons pour l'application d'alerte de danger local. Le véhicule A est arrêté sur la voie du milieu. Le véhicule B se situe dans la *zone de détection*, c'est-à-dire que ses capteurs peuvent détecter A. Le véhicule C est à *portée de communication* de B, et va donc recevoir l'alerte émise par B. C doit prendre une décision avant la *distance de sécurité*. Afin de prendre en compte le temps de réaction du conducteur en cas d'alerte sonore ou visuelle, nous laissons une zone entre la *zone de décision* et la distance de sécurité : la *zone d'information et de réaction*. Un des objectifs est d'analyser le délai de décision pour affiner la taille de la zone de décision.

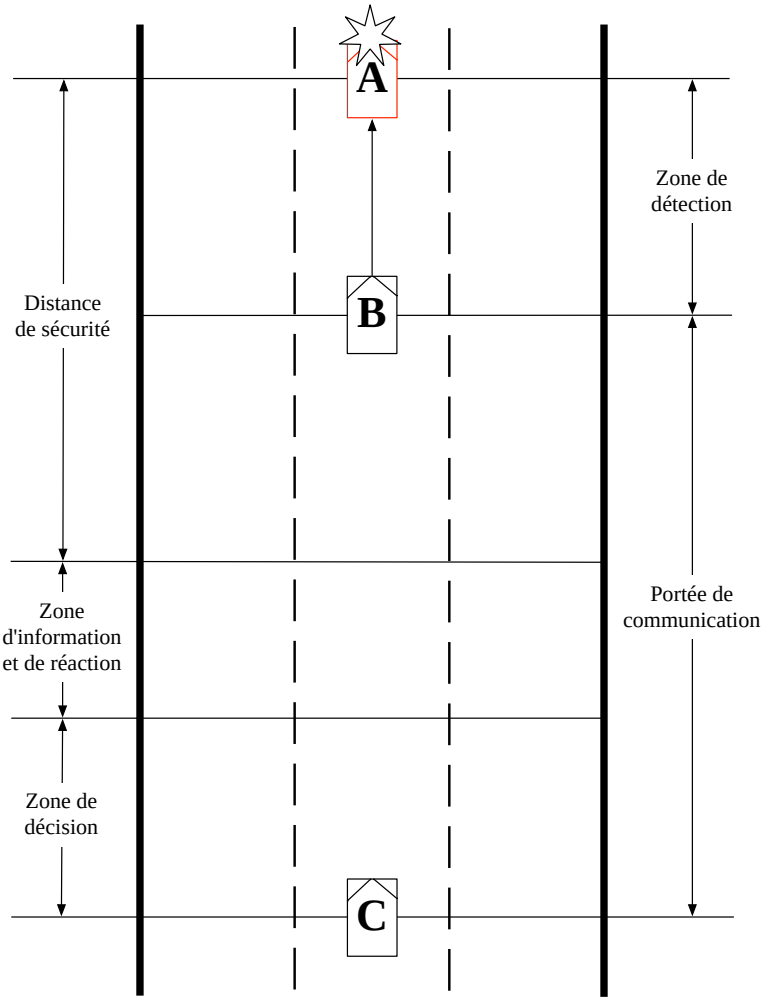

Figure 4-2. Définition des zones pour l'application LDW

4.3 Analyse du processus de décision

Dans la section précédente, nous avons présenté la machine à états d'un OBU. Nous détaillons maintenant les règles de transition, et plus particulièrement celle qui amène à la prise de décision.

Nous analysons plus précisément le processus de décision car il est le plus critique. En effet, la détection ne nécessite pas, *a priori*, de communication avec d'autres véhicules. La dissémination se fait en diffusion et ne présente donc pas d'autre problème que l'accès au support. La décision, quant à elle, nécessite des communications V2V et un traitement local. De plus, le processus de décision est celui qui va influencer la décision finale du conducteur.

Le besoin d'un processus de décision vient de trois raisons. La première est que les erreurs de détection, et donc la dissémination de fausses informations, ne peuvent pas être exclues. La deuxième raison est que l'état de l'événement peut changer, et ainsi, les messages reçus présentent un état inconsistant (cela peut être le cas lorsqu'un événement vient de disparaître par exemple). La troisième raison est que des attaquants internes peuvent disséminer de fausses alertes de danger local.

Un processus de décision utilise une méthode de décision. Lorsqu'un véhicule entre dans la phase de décision, il fait appel à une méthode de décision avec des paramètres en entrée. Ces paramètres sont le résultat du processus de dissémination. Trois critères sont identifiés pour choisir la méthode de décision la plus appropriée.

4.3.1 Critères

Les trois critères principaux pour le choix d'une méthode de décision sont :

(i) Réactivité : L'environnement de communication et le trafic routier sont très dynamiques. La méthode de décision doit pouvoir être capable de réagir rapidement aux changements (connectivité, topologie). Par exemple, le temps nécessaire avant que tous les véhicules approchant détectent la disparition d'un événement précédemment annoncé doit être le plus court possible afin de minimiser le nombre de mauvaises décisions.

(ii) Robustesse : Les messages reçus ne reflètent pas toujours l'état actuel de l'environnement (involontairement ou délibérément). Il est crucial que les méthodes de décision soient aussi robustes que possible contre les fausses informations (ou obsolètes) afin d'assurer la prise de bonnes décisions.

(iii) Passage à l'échelle : Selon les spécificités de l'alerte et du trafic, le nombre d'alertes envoyées pour un même événement peut varier significativement. Cela influence directement sur le nombre de messages qui peuvent être employés par le récepteur pour le processus de décision. La méthode de décision doit pouvoir être employée dans la plupart des situations.

4.3.2 Analyse des méthodes de décision

Nous présentons un ensemble de méthodes de décision existantes : naïve, *Freshest Message*, *Majority Wins*, *Majority of Freshest X*, *Majority of Freshest X with Threshold* [OST 07] [PET 10]. Nous appelons « *bonne décision* » le fait de réagir lorsqu'il y a un vrai danger (ou de ne pas réagir lorsqu'il y a faux danger). Inversement, nous appelons « *mauvaise décision* », le fait de réagir lorsqu'il y a un faux danger (ou de ne pas réagir alors qu'il y a un vrai danger).

4.3.2.1 Naïve

Dans cette méthode de décision, le véhicule récepteur d'une alerte doit attendre de recevoir une alerte (concernant le même événement) de la part de tous les voisins présents dans sa portée de communication (cf. Figure 4-3 (a)). Cette méthode de décision assure le plus haut niveau de protection contre l'attaque d'injection de fausses alertes. Elle est même suroptimale, car dans le contexte d'une majorité de nœuds honnêtes, nous allons voir que d'autres méthodes suffisent. Le délai de décision est intrinsèquement lié au nombre de voisins. Nous pouvons donc déjà souligner un problème de passage à l'échelle.

De plus, les véhicules suivant le véhicule B (N4, N9, N6) ne pourront pas envoyer l'alerte en raison de leur position. Une amélioration est donc de ne considérer que les véhicules se situant devant le véhicule B, c'est-à-dire dans la zone grisée de la Figure 4-3 (b) (N1, N2, N3, N5, N7, N8, A).

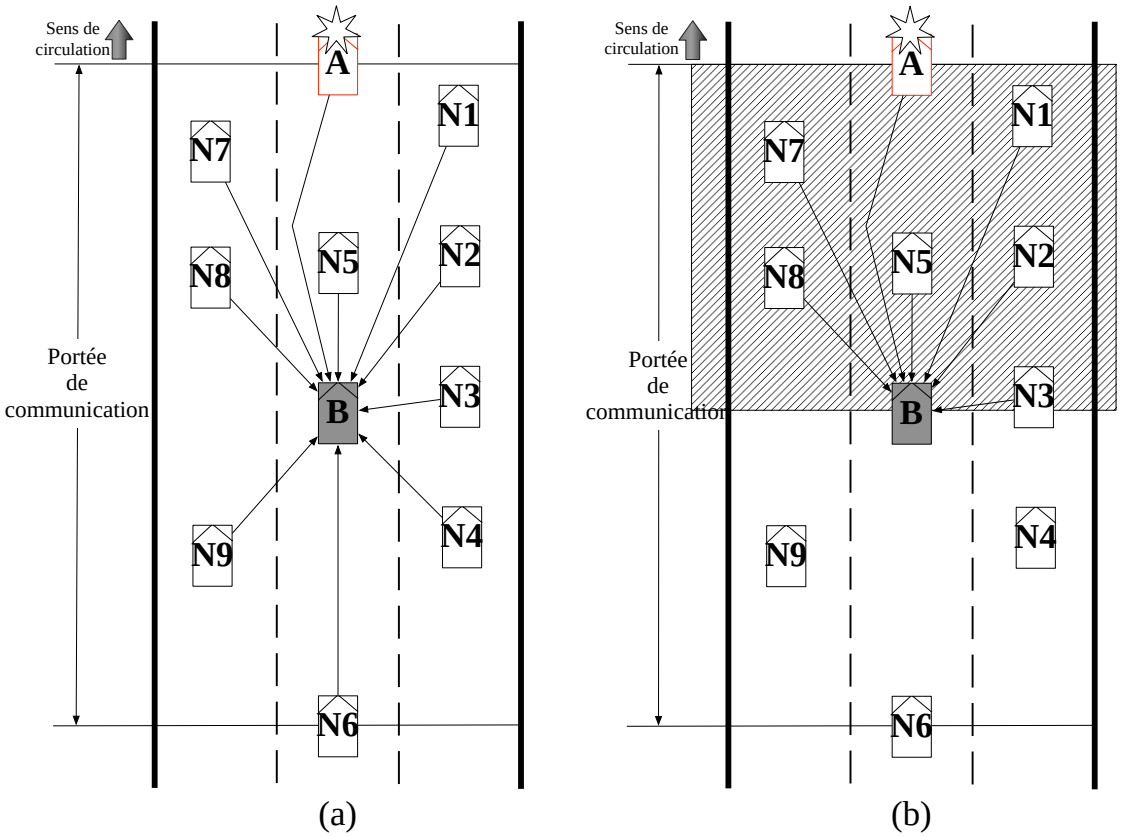

Figure 4-3. Méthode de décision (a) naïve ; (b) naïve ahead

4.3.2.2 *Freshest Message*

Dans cette méthode, quand une décision doit être prise, seul le message le plus récemment reçu est considéré. Si c'est un message d'alerte, alors une décision positive est prise. Si c'est un message de révocation, alors une décision négative est prise. Il est admis que cette méthode de décision ne procure aucune protection contre les attaques. Cependant, elle assure une adaptabilité forte dans le cas de scénarii sans attaquants, résultant ainsi peu de mauvaises décisions.

4.3.2.3 *Majority Wins*

Cette méthode de décision effectue un vote local à partir de tous les messages reçus (concernant la même alerte). Seuls les messages distincts comptent. Par conséquent, un seul message par véhicule est considéré. Si la majorité des messages sont des alertes, alors une décision positive est prise. Sinon, une décision négative est prise pour l'alerte concernée. Il est admis que cette méthode de décision assure une protection contre les attaques de type injection de fausses données dans les scénarii avec attaquants collaboratifs (en conservant une majorité de véhicules honnêtes). La Figure 4-4 illustre le cas où le véhicule B prendra une décision dès qu'il aura reçu un message identique de la majorité des véhicules situés devant lui (ici quatre). Cette méthode provoque de mauvaises décisions lorsque le

danger disparaît, et ce, tant que le nombre d'alertes est supérieur au nombre de révocations. Nous appelons cette période de temps : *la phase d'adaptation de fin d'alerte*. De la même manière, il existe une *phase d'adaptation de début d'alerte* car la majorité n'est pas encore atteinte.

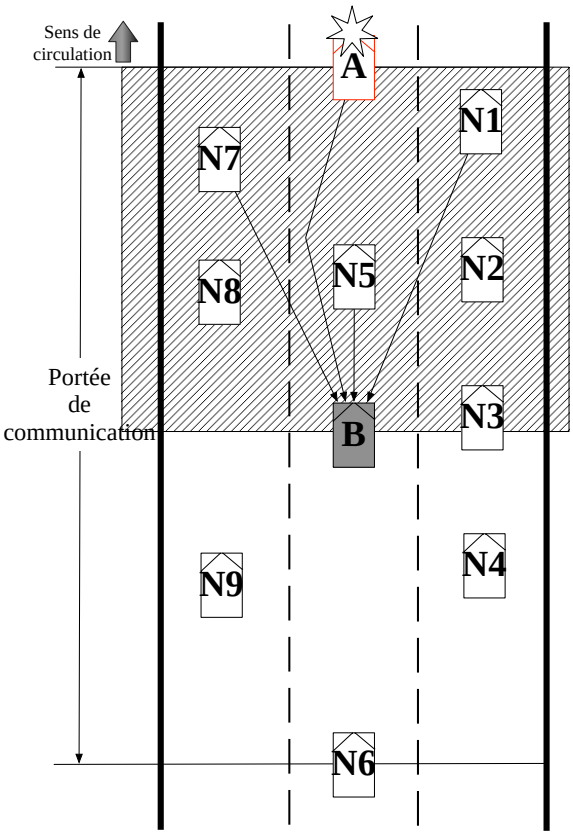

Figure 4-4. Méthode de décision *Majority Wins*

4.3.2.4 *Majority of Freshest X*

Cette méthode de décision est une combinaison des deux méthodes précédentes. Pour prendre une décision, un véhicule effectue un vote en ne considérant que les *X* plus récents distincts messages (concernant la même alerte). Ainsi, cette méthode permet de réduire les phases d'adaptation de début et de fin, en restant « sensible » aux nouvelles alertes (ou révocations). Elle démontre une bonne protection contre l'attaque de type *flip attack* où l'attaquant génère un message inverse à celui envoyé par les véhicules légitimes. Elle présente cependant des faiblesses en présence d'attaques de type *fake attack* avec un pourcentage de mauvaises décisions entre 5 % et 10 % [OST 07].

4.3.2.5 *Majority of Freshest X with Threshold*

Cette méthode de décision étend la précédente en ajoutant un seuil de déclenchement (*Threshold*). Ainsi, lorsque le nombre de messages distincts reçus dépasse le seuil, la décision est prise selon la méthode §4.3.2.4. Si le seuil n'est pas atteint, une réponse négative est prise.

Dans le cas de scénarii sans attaquants, les performances de cette méthode de décision sont moins bonnes que la méthode « *Majority of Freshest X* ». Cela est dû au seuil qui ajoute une phase d'adaptation au début de l'alerte, durant laquelle tous les véhicules prennent une mauvaise décision.

Toutefois, grâce à l'utilisation du seuil, cette méthode permet de réduire le pourcentage de mauvaises décisions lors d'attaques de type *fake attack* (0 % jusqu'à 35 % d'attaquants) [OST 07].

4.4 Modélisation générique de méthode de décision

Pour définir les méthodes de décision, il est intéressant d'avoir une modélisation générique. Le modèle générique est composé de deux modèles : le modèle conceptuel et le modèle analytique. À partir du modèle conceptuel qui définit le fonctionnement général, nous désirons extraire un modèle analytique qui définit une formule de calcul du délai de décision.

4.4.1 Modèle conceptuel

Afin d'avoir une vision claire des méthodes de décision, nous proposons une modélisation conceptuelle des méthodes de décision. La Figure 4-5 illustre le modèle conceptuel générique. Le modèle conceptuel est représenté par un système composé de modules (M1 à Mj). Chaque module est représenté par une boîte qui a les caractéristiques suivantes : un nom, une description textuelle du fonctionnement, des paramètres d'entrée et de sortie, et un temps de traitement.

Pour définir l'enchaînement logique des modules et faire apparaître le paramètre de temps, nous ajoutons des transitions. Les transitions entre les modules sont représentées par des flèches. Ces flèches peuvent avoir une (ou plusieurs) condition(s) afin d'orienter le modèle selon les paramètres de sortie du module.

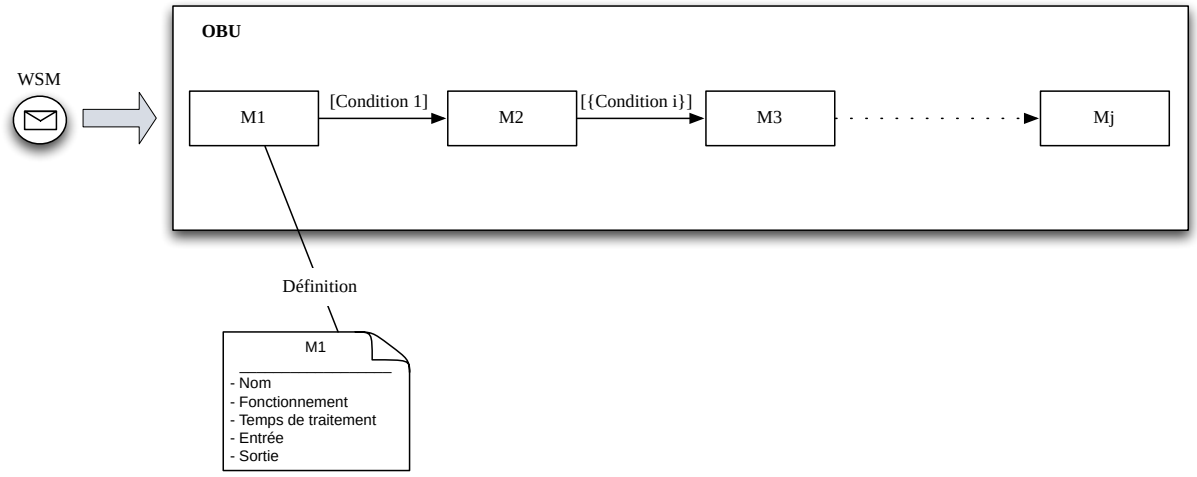

Figure 4-5. Modèle conceptuel générique

4.4.2 Modèle analytique

Lorsqu'un véhicule doit prendre une décision et qu'il doit exécuter le mécanisme de consensus, il va devoir recevoir un certain nombre de messages avant d'établir sa décision finale. Ce temps, appelé « délai de décision », va impacter la distance de freinage, mais aussi le délai d'authentification. En effet, si un véhicule doit attendre X messages (ce qui induit un temps $X \times T_{tx}$) avant de prendre sa décision, il va devoir vérifier X signatures numériques (ce qui induit un temps $X \times T_{verif}$). C'est pourquoi, à partir du modèle générique, nous souhaitons calculer le délai de décision de la méthode de décision représentée.

Chaque module a une fonction particulière et un délai associé. Ainsi, le délai de décision correspond à la somme des délais de chaque module qui compose le modèle conceptuel. Soit un système de décision composé de j modules ayant chacun un délai D_j, le délai de décision $Délai_{decision}$ est défini par :

$$Délai_{decision} = \sum_{k=1}^{j} D_k \tag{4.1}$$

Nous établissons les notations utilisées pour définir la formule de calcul du consensus. L'alerte d'un événement i rapportée par le véhicule V_k est notée e_k^i. Le type de l'événement i est noté $\lambda(i)$ et a une valeur. Par exemple, un message d'alerte est égal à +1, tandis qu'un message de révocation égal à -1. Nous définissons la fonction de confiance de l'événement $f: \Theta \times \Lambda \rightarrow [0,1]$. Cette fonction a deux arguments : $\lambda(i)$ et $\tau(V_k)$, où $\tau(V_k)$ est la confiance de base du véhicule (comme nous l'avons évoqué précédemment, un véhicule de secours peut avoir un niveau de confiance plus élevé). La confiance en l'événement est donc : $f(\tau(V_k), \lambda(i))$.

Afin de prendre en compte le cas où un véhicule serait révoqué, nous définissons une fonction s, qui retourne le statut de révocation actuel du véhicule. Ainsi à partir de l'ensemble des véhicules Υ, nous avons $s: \Upsilon \longrightarrow [0,1]$, où $s(V_k) = 0$ implique que le véhicule V_k est révoqué, et $s(V_k) = 1$ implique que le véhicule est légitime. Nous combinons ces arguments dans une fonction qui retourne une valeur comprise entre 0 et 1 :

$$F\left(e_k^i\right) = G(s(V_k), f(\tau(V_k), \lambda(i))) \tag{4.2}$$

Si V_k ne signale pas l'événement i, alors $F\left(e_k^i\right) = 0$. Ces valeurs sont calculées localement pour chaque message reçu et sont utilisées comme une fonction poids par la méthode de décision.

4.5 Analyse de la méthode de décision « *Majority of freshest X with Threshold* »

La méthode « *Majority of freshest X with Threshold* » offre un bon compromis entre l'adaptabilité de la méthode « *Freshest X* » et la robustesse de la méthode « *Majority Wins* ». Nous détaillons dans cette section le modèle conceptuel et analytique.

4.5.1 Modèle conceptuel

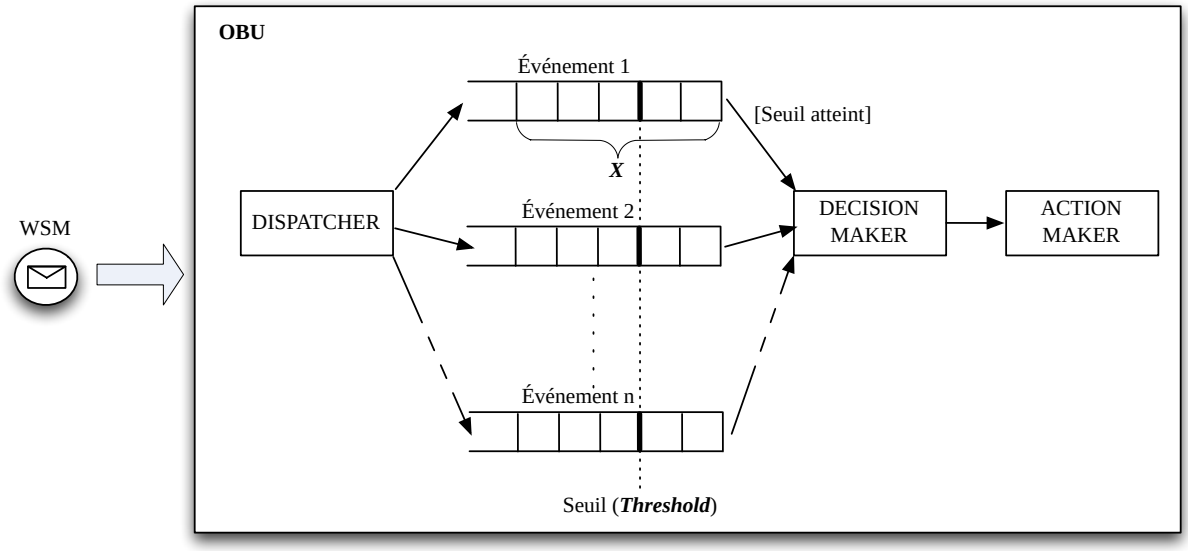

Figure 4-6. Modèle conceptuel de la méthode de décision « *Majority of freshest X with Threshold* »

Nous appliquons la modélisation conceptuelle et explicitons les modules *dispatcher*, *decision maker* et *action maker*. La Figure 4-6 représente le modèle conceptuel de cette méthode de décision.

Lorsqu'un véhicule reçoit un message d'alerte (WSM, cf §1.2.2), celui-ci passe par un module appelé *dispatcher* qui trie les WSMs dans la file de l'événement correspondant. Nous considérons une file d'attente par événement. Toutefois, nous supposons que notre processeur peut gérer toutes les files d'attente en même temps (le problème de gestion d'ordonnancement entre les files dépasse le cadre de cette thèse).

Le module *decision maker* surveille les files et lance le processus de décision dès que le seuil est atteint. Il prendra ainsi la décision sur les *X* derniers messages reçus pour cet événement. La décision est alors donnée au module *action maker* qui fera l'action. L'action peut être une *action réseau* (diffusion de l'alerte) ou une *action véhicule* (avertissement du conducteur, freinage).

4.5.2 Modèle analytique

Nous présentons dans un premier temps comment calculer le consensus. Ensuite, nous analysons le délai de décision et l'impact sur la distance de freinage.

Soit d_i le niveau de confiance calculé à partir de l'ensemble des messages reçus pour l'événement *i*. L'OBU calcule le score avec la fonction suivante :

$$d_i = \sum_{k=1}^{N_{TX}} F(e_k^i)_X \text{ , si } X > Threshold \quad (4.3)$$

où N_{TX} est le nombre de véhicules équipés du système DSRC présents dans le rayon de communication *R* (cf. §3.4.4). Si le résultat est positif, alors l'OBU prend une décision, sinon l'alerte est rejetée.

Nous définissons le délai de décision comme le temps entre la première réception de l'alerte et la prise de décision. À partir de l'Équation 4.1, nous obtenons la formule suivante :

$$Délai_{décision} = D_{dispatcher} + D_{decision\_maker} \quad (4.4)$$

Le *dispatcher* ne fait que trier les messages et son délai est négligeable par rapport à celui du *decision maker*. Nous intégrons le temps d'attente avant décision dans le délai du *decision maker*. Nous considérons que le véhicule récepteur a constamment un message à réceptionner. Ainsi, nous ne considérons pas le délai d'attente entre plusieurs réceptions (qui correspond à un temps mort). La loi d'inter-arrivée des messages n'est pas évidente à déterminer, car le délai dépend de nombreux paramètres de niveau physique, MAC, applicatifs (loi d'inter-arrivée au niveau de l'émetteur) ou encore environnementaux (densité de véhicule). Avec cette hypothèse, le délai de décision dépend du temps de calcul, du temps de communication et de *X*. Il est défini par :

$$Délai_{décision} = X \times (T_{tx} + T_{vérif}) \text{ avec } X > Threshold \quad (4.5)$$

Sans le mécanisme de consensus, le véhicule décide à partir d'un seul message. Le surcoût temporel de cette méthode de décision est donc :

$$T_{decision\_ov} = (X - 1) \times (T_{tx} + T_{vérif}) \quad (4.6)$$

La Figure 4-7 montre l'impact des paramètres *X* et *Threshold* sur le délai de décision (en unité T_{ov} où $T_{ov} = T_{tx} + T_{vérif}$).

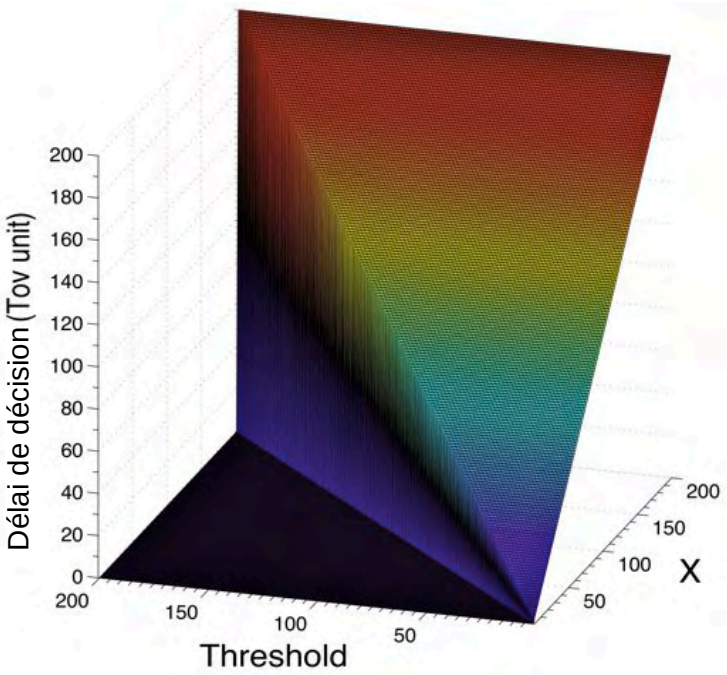

Figure 4-7. Impact des paramètres *X* et *Threshold* sur le délai de décision

Nous remarquons que si le seuil est élevé, alors X est grand et le processus de décision est retardé. Avant de démarrer le processus de décision, c'est-à-dire choisir la décision, le véhicule doit attendre $Threshold \times (T_{tx} + T_{vérif})$.

Si X est grand, alors le surcoût en temps de calcul (pour la vérification des signatures numériques) est important. Un X élevé procure une robustesse plus importante, mais une réactivité plus faible.

En augmentant le délai de décision du véhicule, cela réduit la distance entre le véhicule et le danger. Le surcoût sur la distance de freinage (en mètres) est défini par :

$$\Delta D_B = D_B^1 - D_B^0 = X \times (v_{V_k} \times (T_{tx} + T_{vérif})) = v_{V_k} \times Délai_{decision} \quad (4.7)$$

où D_B^0 est la distance de freinage initiale du véhicule (cf. Équation 3.4), D_B^1 est la distance de freinage totale incluant les mécanismes de sécurité, v_{V_k} est la vitesse du véhicule V_k.

La Figure 4-8 montre l'impact du paramètre X sur la distance de freinage. La tendance exponentielle s'explique par le fait que plus le nombre de véhicules est important dans la portée de communication, plus la probabilité de collision est importante et par extension le délai de transfert est important. Nous remarquons qu'à partir de $X = 180$ (c'est-à-dire une densité $\beta = 100$ veh/km/voie), la distance de freinage est doublée. Le paramètre X doit donc être choisi avec précaution.

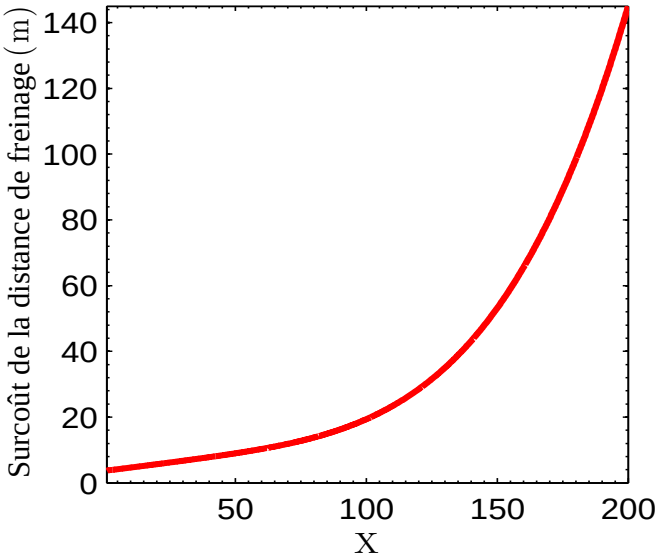

Figure 4-8. Impact du paramètre X sur la distance de freinage

4.5.3 Limites

Les résultats de simulation ont démontré que la méthode « *Majority of freshest X with Threshold* » est la plus adaptée pour prévenir l'attaque d'injection de fausses alertes dans le LDW, car elle présente une probabilité de mauvaise décision proche de zéro.

Cependant, une limite de cette méthode de décision (et de celles présentées en section 4.3.2) est qu'elle ne considère que le nombre de voisins à portée de communication directe pour prendre une

décision. En effet, cette méthode n'analyse pas le contenu de l'alerte, et l'OBU stockera donc des messages potentiellement inappropriés. Il y a donc un gaspillage des ressources de l'OBU.

Dans leur étude [OST 07], les auteurs ne se sont pas intéressés à la problématique de surcoût du consensus. De plus, ils ont laissé en suspens la question du choix des paramètres du consensus *X* et *Threshold*. Afin d'accroître la réactivité du processus de décision, nous proposons d'ajuster dynamiquement les paramètres du consensus.

4.6 Méthode de décision dynamique

Afin de répondre aux limites présentées en section 4.5.3, nous proposons une méthode de décision dynamique. Nous détaillons dans cette section le modèle conceptuel et analytique.

4.6.1 Modèle conceptuel

Nous appliquons la modélisation conceptuelle et proposons d'ajouter les modules *filter*, *classifier* ainsi qu'une modification du *decision maker*. La Figure 4-9 représente le modèle conceptuel de notre méthode de décision. Les flèches en gras illustrent un changement dynamique.

1. *Filter* : Ce module est utilisé pour le filtrage des paquets « inappropriés ». Nous entendons par « inapproprié », un paquet qui informe d'un événement ne concernant pas le véhicule. Ce filtrage peut être fait selon plusieurs critères :

    a. Distance : Si le véhicule est trop éloigné du danger par exemple. Notons que cette vérification peut être évitée si un protocole de routage geocast [EIC 06] [SUN 04] basé sur la distance est utilisé.

    b. Voie : En fonction du type d'événement et de la dimension de l'obstacle, le véhicule peut rejeter le message si l'incident est sur une voie différente de la sienne (dans le cas d'une autoroute notamment). Ainsi, il n'y aura pas d'action du véhicule, mais une *action réseau* est autorisée, comme la diffusion d'une alerte par exemple.

    c. Chemin : L'alerte est inadaptée car l'incident n'est pas sur le chemin prévu. Mais si le véhicule passe à proximité et peut détecter le danger, il peut être intéressant de ne pas rejeter l'alerte afin de prévenir les autres véhicules.

    Ce module a donc pour rôle de réduire le nombre de paquets stockés, le nombre de files d'événement, le nombre de vérifications de signature numérique (consommation de temps processeur et d'énergie moindre), et d'éviter la prise de décision inappropriée.

2. *Classifier* : Ce module est utilisé pour marquer les paquets et a pour rôle de calculer la criticité de l'alerte. Pour ce faire, il utilise plusieurs critères :

    a. Distance entre le véhicule et l'obstacle.

b. Vitesse : Une vitesse élevée nécessite un temps de réaction plus court.

c. Cap : Est-ce que le véhicule se dirige vers l'obstacle ?

d. Route, chemin : Est-ce que le chemin prévu du véhicule passe par l'obstacle ?

e. Temps estimé d'arrivée dans la zone de danger : À partir de la vitesse et du chemin prévu, le véhicule peut estimer l'heure d'arrivée dans la zone.

f. Heure de première diffusion de l'alerte.

g. État du véhicule : Pression des pneus, états des pneus, poids, usure des plaquettes de frein, etc.

h. État de la route : Mouillée, enneigée, etc.

i. Conditions environnementales : Altitude, jour/nuit, montée/descente.

j. Facteurs humains : Âge, sexe, fatigue calculée grâce à la durée de conduite sans arrêt, statistiques de réactions antécédentes.

Son but est de fournir l'information de criticité au module *decision maker* afin d'influencer les paramètres du consensus pour cet événement. Dans le problème d'ordonnancement entre les files d'événements, ce calcul peut aussi être utilisé. Nous détaillons le calcul de la criticité en section 4.6.2.2.

3. *Decision maker* : Ce module récupère la valeur de criticité et change dynamiquement les paramètres *X* et *Threshold*. À chaque réception de WSM, le *decision maker* récupère la valeur de criticité et l'état du voisinage courant pour calculer les nouveaux paramètres du consensus. Il réagit ensuite à partir des nouvelles valeurs *X* et *Threshold*.

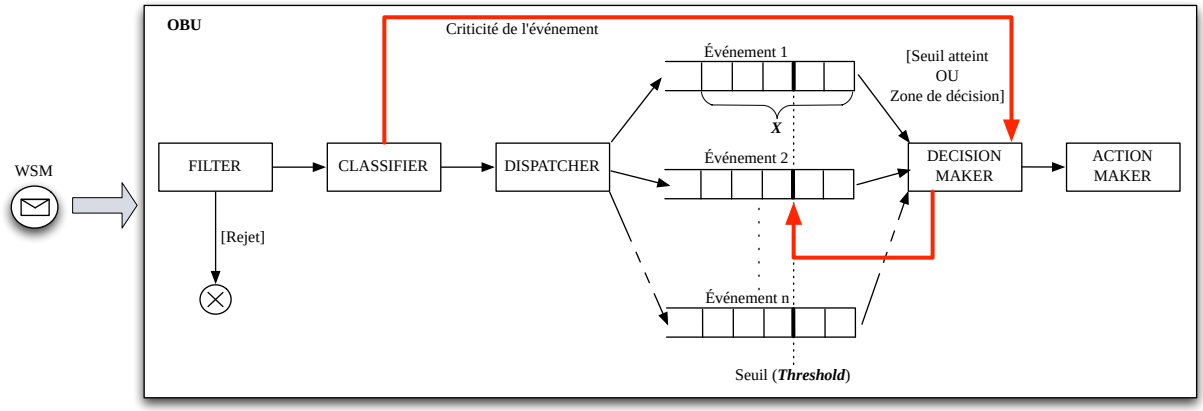

Figure 4-9. Modèle conceptuel de méthode de décision dynamique

4.6.2 Modèle analytique

Le délai de décision et l'impact sur le surcoût de la sécurité dépendent du calcul de *X* et *Threshold*. Dans un premier temps, nous formalisons ce qui se passe dans notre système. Nous proposons des formules pour fixer dynamiquement les paramètres du consensus.

La formule de calcul du niveau de confiance d_i est la même que pour la méthode « *Majority of Freshest X with Threshold* ». La différence est dans la définition des paramètres du consensus. Définir *X* et *Threshold* revient à un problème d'optimisation de multiples paramètres en fonction du contexte. Ce type de problème est particulièrement présent dans les domaines du traitement du signal, du traitement d'image, ou en analyse financière. Le système étudié est alors souvent représenté par un filtre de Kalman.

Le filtrage (à ne pas confondre avec notre module *filter*) consiste à estimer l'état d'un système dynamique, c'est-à-dire évoluant au cours du temps, à partir d'observations partielles, généralement bruitées. Typiquement, on dispose d'une suite Y_1, Y_2,…, Y_n d'observations, obtenues après traitement préalable du signal brut recueilli au niveau des capteurs. Chaque observation Y_n est reliée à l'état inconnu I_n par une relation du type $Y_n = h(I_n) + B_n$ où B_n est un bruit, qui modélise l'erreur d'observation.

De la même manière, nous représentons notre système (l'OBU), et plus précisément le module *decision maker*, comme un filtre de Kalman. Notre méthode de décision est donc vue comme une fonction de filtrage. Ce filtre a des paramètres d'entrée, de bruit, et une valeur de sortie (cf. Figure 4-10). Nous supposons que chaque véhicule a une connaissance totale de l'environnement, c'est-à-dire du voisinage, de leurs coordonnées et de la topologie du réseau. Nous supposons aussi que le processus de dissémination utilise un protocole de routage de diffusion à un saut.

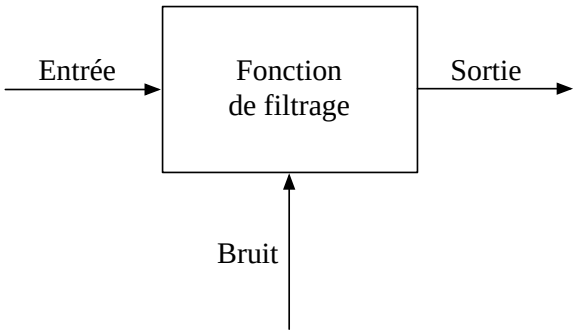

Figure 4-10. Modèle type d'un filtre

Si nous discrétisons les événements reçus par un OBU sur une ligne temporelle, nous obtenons la Figure 4-11. Au temps t_i, le véhicule reçoit le message A_i (qui peut être une alerte ou une révocation) émanant d'un véhicule élément de l'ensemble $\overline{V^{t_i}}$.

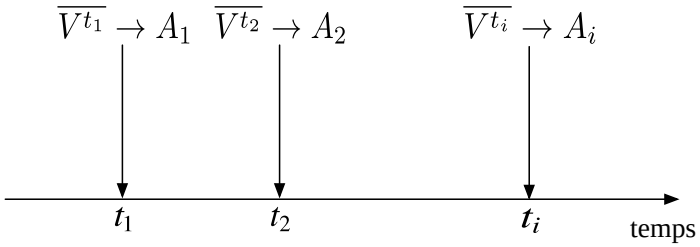

Figure 4-11. Discrétisation des événements

En entrée du filtre, nous avons :

- $\overline{V^t} = \{V_1, \dots, V_k\}$: Ensemble des voisins du véhicule à l'instant *t*.
- $\left|\overline{V^t}\right|$: Cardinal de l'ensemble, c'est-à-dire le nombre de voisins devant le véhicule.
- A_i : *i*-ième message reçu pour l'alerte concernée.
- $|\overline{A_t}|$: Nombre de messages reçus pour l'alerte concernée au temps *t*.
- $|\bar{T}|$: Ensemble des temps de réception des messages *A*.
- ξ^t : Résultat de la fonction d'observation ξ au temps *t*.

La fonction ξ permet de calculer la proportion de messages reçus par rapport au nombre de voisins. À chaque réception, le véhicule calcule la fonction ξ au niveau du *dispatcher*. L'ensemble des valeurs de la fonction ξ, noté $\bar{\xi}$, forme donc les observations nécessaires à la fonction de filtrage (dans le *decision maker*).

Le paramètre de bruit est le pourcentage d'attaquants qui lancent des attaques d'injection de fausses alertes. Ce pourcentage est compris entre 0 et 49 %, car nous considérons une majorité de véhicules honnêtes.

Dans un premier temps, la fonction d'observation est définie par :

$$\xi^1 = \frac{1}{\left|\overline{V^{t_i}}\right|} \tag{4.8}$$

La décision est prise à partir d'un seul message et en fonction du nombre de voisins.

Mais plus le véhicule s'approche de la zone de détection, plus le nombre de messages reçus pour cet événement est important, car le voisinage augmente. Au lieu d'utiliser la formule ξ^1, nous agrégeons les messages reçus pour le même événement. Lors de la deuxième réception, nous avons $\xi^2 = \frac{2}{\left|\overline{V^{t_1}} \cup \overline{V^{t_2}}\right|}$. Par interpolation, nous obtenons : $\xi^k = \frac{k}{\left|\bigcup_{j=1}^{k} \overline{V^{t_j}}\right|}$. La décision est prise à partir de l'ensemble des messages reçus. Le problème est donc de trouver le « meilleur » *k*, ce qui équivaut à trouver le *X* de la méthode de décision d'Ostermaier.

À partir des données en entrée (séquence de valeurs $\bar{\xi}$, criticité $C_{\lambda(i)}$) et du bruit, nous observons la sortie du filtre. Les valeurs de sortie sont *X* et *Threshold*.

En entrée, une séquence de valeurs croissantes représente l'approche d'un danger potentiel. À partir de l'ensemble $\bar{\xi}$, la fonction de filtrage doit reconnaître, parmi une séquence de *k* valeurs, une sous-séquence de valeurs croissantes. *k* est alors vu comme la taille de la fenêtre des valeurs considérées pour la détection (cf. Figure 4-12).

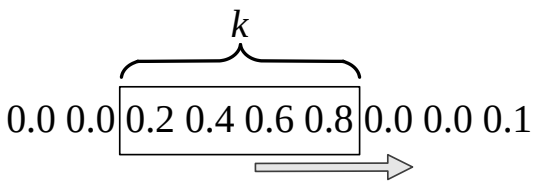

Figure 4-12. Exemple de fenêtre glissante

Après avoir détecté l'événement, il faut définir comment réagir et quand (quel est le délai maximum ?).

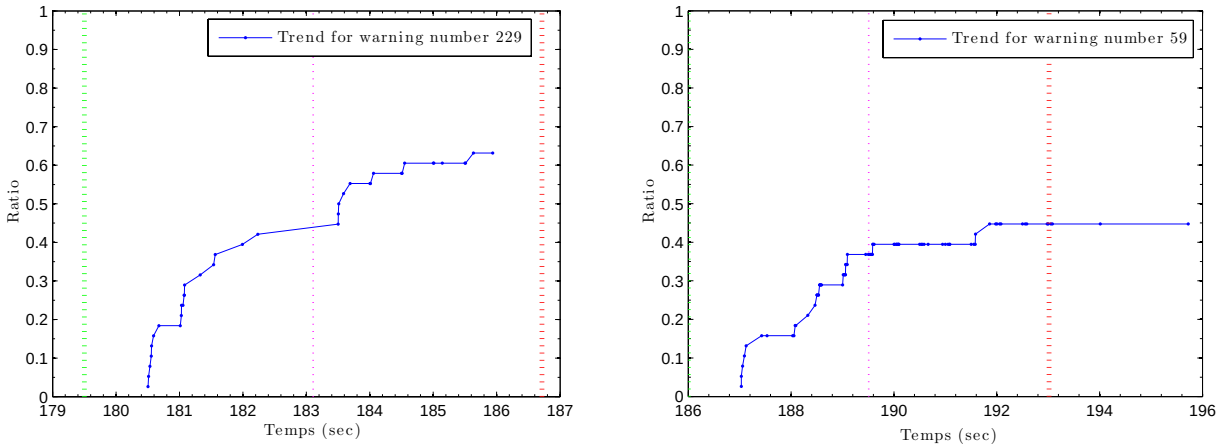

Figure 4-13. Exemples de séquence d'observations

La Figure 4-13 montre deux exemples de séquence d'observations utilisée en paramètre d'entrée du filtre. Dans cet exemple, la densité est de 20 veh/km/voie et l'on observe un véhicule se dirigeant vers deux obstacles (n°229 et n°59). Le ratio représente la valeur ξ^k. Un ratio de 0,5 équivaut à recevoir un message de 50 % des voisins. La ligne verticale verte représente l'apparition du danger, et la ligne verticale rouge représente le moment de collision du danger. Dans la Figure 4-13 gauche, le véhicule arrive à un ratio de 0,6 avant d'atteindre la zone de collision. Il en est autrement dans la Figure 4-13 droite où le véhicule atteint un ratio de 0,45 au moment de la collision. Atteindre la majorité n'est donc pas si évident. L'arrêt de réception d'alerte peut s'expliquer de deux façons. La première est que l'alerte est terminée avant d'arriver sur le danger. La deuxième est que le véhicule entre dans la zone de détection du danger.

Pour savoir comment réagir, c'est-à-dire positionner *X* et *Threshold*, il faut avoir une fonction de coût. Cette fonction permet de définir le point de collision si le véhicule ne change pas son état actuel (vitesse, direction). Pour prendre en compte la dangerosité de l'événement, la fonction de coût utilise

la criticité calculée par le *classifier* et influence le choix des paramètres pour réagir dans les temps (avant le franchissement de la distance de sécurité).

4.6.2.1 Calcul du paramètre *Threshold*

Nous fixons le seuil à un pourcentage du voisinage courant se situant devant le véhicule. Nous définissons le paramètre *Threshold* par la formule suivante :

$$Threshold = p \times \frac{Ahead(N_{TX}(t),R)}{2} \quad (4.9)$$

La fonction $Ahead(N_{TX}(t), R)$ retourne le nombre de voisins devant le véhicule courant à l'instant *t* et dans la portée de communication *R*. Cette fonction peut être combinée à une carte routière et aux coordonnées géospatiales (obtenues par un système de positionnement par satellite par exemple).

Dans l'Équation 4.4, le paramètre *p* est un pourcentage. Ainsi le seuil est fixé à un pourcentage du nombre de véhicules dans son voisinage à un saut. Pour fixer ce pourcentage, nous proposons d'utiliser un système d'apprentissage. Au départ, le véhicule a une confiance totale envers les autres véhicules. Lorsque le véhicule détecte qu'il a réagi alors qu'il n'y avait pas de menace réelle, il met à jour une *valeur de méfiance*. Cette valeur représente le pourcentage moyen de fausses alertes. Le véhicule devient donc de plus en plus méfiant. La valeur de méfiance influence le choix du paramètre *p* de l'Équation 4.9.

4.6.2.2 Calcul du paramètre *X*

En cas de densité de véhicule non homogène, il faut modifier dynamiquement le paramètre *X*. Ce paramètre permet un ajustement entre les deux besoins contradictoires d'adaptabilité et de robustesse. Nous le définissons par :

$$X = \frac{(2 \times C_{\lambda(i)})^{pc}}{C_{\lambda(i)}} \times \frac{Ahead(N_{TX}(t),R)}{2} \quad (4.10)$$

où $pc \in [0; 1]$ est un entier représentant le paramètre de précaution.

Pour calculer la criticité $C_{\lambda(i)}$, nous proposons la formule suivante :

$$C_{\lambda(i)} = \begin{cases} 1 & \text{si } \Delta T_i > T_{dist\_sécurité} \\ 1 + \frac{1}{\Delta T_i} & \text{si } T_{dist\_sécurité} > \Delta T_i > T_{collision} \end{cases} \quad (4.11)$$

où :

- $T_{collision}$: Instant de collision estimé si le véhicule ne change pas sa vitesse ou se trajectoire. Cette variable est calculée à partir de la distance restante entre l'obstacle et le véhicule.

- $\Delta T_i = T_{collision} - T_i$ (c'est le temps restant avant collision),

- $T_{freinage} = \frac{v}{a}$ (c'est le temps de freinage calculé à partir de la vitesse et de la décélération),

- $T_{réaction}$: Temps de réaction du conducteur (entre 0,7 et 1,5 secondes en moyenne [GRE 09]),

- $T_{dist\_sécurité} = T_{freinage} + T_{réaction}$ (c'est le temps écoulé durant la distance de sécurité).

Plus la criticité est élevée, plus *X* est faible car il est urgent de prendre une décision. Dans un premier temps, afin de conserver une dimension raisonnable pour un modèle analytique simple, nous ne considérons que la distance et la vitesse afin de calculer la criticité. Bien entendu, ce paramètre peut prendre en compte tous les critères cités en section 4.6.1.

4.6.2.3 Calcul du délai du consensus

Tout comme pour la méthode de « *Majority of Freshest X with Threhsold* », le délai de décision dépend des valeurs *X* et *Threshold*. Nous notons :

- $W()$: La fonction qui calcule le nombre de messages utilisés par la méthode de décision.

- $\left|Q_{e_k^i}\right|$: Messages présents dans la file d'attente.

- ω : Un booléen représentant un deuxième paramètre de précaution, mais moins flexible que *pc*, car de type « tout ou rien ». Si $\omega = 1$, alors le module de décision prend une décision à partir des messages présents dans la file d'attente, et ce, même si le seuil n'est pas atteint.

- T_{MAX} : Le délai maximum accordé par l'application avant d'avoir des conséquences critiques (pour le véhicule ou pour les voisins du véhicule). T_{MAX} est calculé à partir de la vitesse, de la distance entre le véhicule et le danger et des besoins applicatifs.

$$Délai_{décision} = (Threshold + W(X)) \times T_{ov} \tag{4.12}$$

$$W(X) = \begin{cases} X - Threshold \text{ , si } \left|Q_{e_k^i}\right| \geq X \text{ avant } T_{MAX} \\ \omega \times \left(\left|Q_{e_k^i}\right| - Threshold\right) \text{ , si } T_{MAX} \text{ atteint} \end{cases} \tag{4.13}$$

Chacun des modules a un délai qui correspond au temps de traitement du paquet. Nous détaillons le délai de chaque module:

1. *Filter* : Il vérifie le contenu du paquet. Comme les paquets ne sont pas chiffrés, il n'y aura aucune opération cryptographique à réaliser pour pouvoir lire le contenu. Si l'information se révèle fausse, le paquet est rejeté. Nous pouvons envisager l'ajout d'un module de "recommandation" qui donnerait des bonus/malus aux émetteurs. Nous considérons le délai comme négligeable, car il s'agit d'opérations simple (comparaison entre les informations locales et celles de l'alerte).

2. *Classifier* : Tout comme le module *filter*, il vérifie le contenu du paquet et calcule la criticité en comparant l'état actuel du véhicule et les informations de l'événement. Nous considérons donc aussi son délai comme négligeable.

Comparativement à la méthode de décision « *Majority of Freshest X with Threshold* », le délai n'est donc pas augmenté significativement (comparaison, calculs simples). Le principal délai vient donc de l'attente par le *decision maker* pour prendre la décision.

4.6.3 Analyse et discussion

La Figure 4-14 présente l'impact de la criticité et du paramètre de précaution sur X lorsque $N_{TX}(t) = 100$. Quand la criticité augmente et que le paramètre de précaution est égal à zéro (précaution privilégiée), alors X décroit. Lorsque $pc = \frac{\ln(C_{\lambda(i)})}{\ln(2\times C_{\lambda(i)})}$, alors la limite inférieure de X est $\frac{Ahead(N_{TX}(t),R)}{2}$. Cela assure une robustesse dans les scénarii avec attaquants collaboratifs.

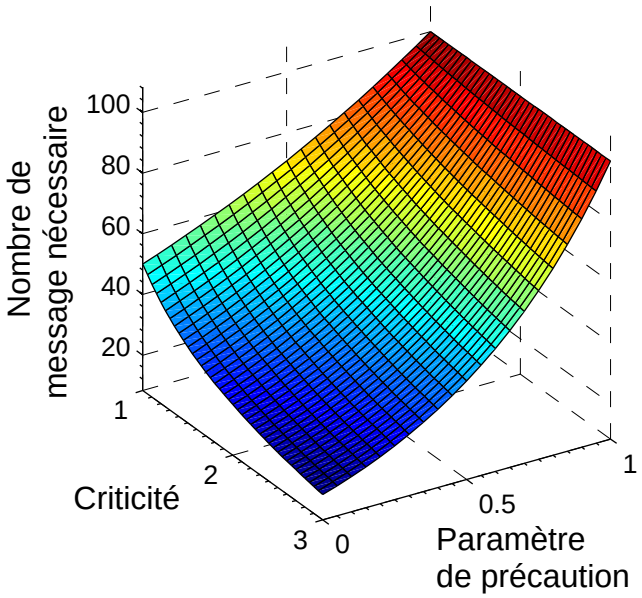

Figure 4-14. Impact de la criticité et du paramètre de précaution sur X ($N_{TX}(t)$=100)

Le paramètre X doit prendre en compte les contraintes temporelles de l'application. Cette contrainte est définie par x_{MAX} qui est le nombre maximum de messages que peut vérifier un véhicule avant de dépasser le délai maximum de l'application T_{MAX}. Grâce à notre formule du surcoût de l'authentification obtenue au chapitre 3, la valeur du paramètre x_{MAX} est facilement obtenue. Nous faisons apparaître x_{MAX} dans l'Équation 4.10, ce qui nous donne :

$$X = \min\left(\left(\frac{(2\times C_{\lambda(i)})^{pc}}{C_{\lambda(i)}} \times \frac{Ahead(N_{TX}(t),R)}{2}\right), x_{MAX}\right) \quad (4.14)$$

Mais la contrainte temporelle définie par x_{MAX} réduit le niveau de sécurité, car il réduit le nombre de messages nécessaire pour la prise de décision dans les scénarii à forte densité. Cette contrainte annule

le besoin de $\frac{Ahead(N_{TX}(t),R)}{2}$ messages, et par conséquent, les véhicules malicieux pourront injecter de fausses alertes. Il est clairement établi qu'un compromis entre la sécurité et les performances doit être pris.

Nous étudions la question de la terminaison afin d'établir si le consensus est toujours atteint. À partir du calcul de la limite de *X* lorsque N_{TX} tend vers $+\infty$, nous remarquons que sans l'ajout d'une borne (représentée par le *min* dans l'Équation 4.14), le véhicule n'atteindra jamais le consensus, car il réclamera toujours un message de plus. Cela sera le cas lorsqu'un véhicule se dirige sur un embouteillage. Plus il va avancer, plus il aura de voisins dans sa portée de communication et le *X* augmentera. C'est pourquoi il faut obliger la prise de décision avant la fin de la zone de décision ou bien lorsque le délai maximum autorisé par l'application risque d'être atteint.

Grâce au paramètre de précaution *pc*, la distance parcourue entre la première réception de l'alerte et le moment de décision est bornée, car la distance de freinage est prise en compte dans la formule. Par rapport à une réaction immédiate dès la première alerte reçue, le consensus reporte l'instant de freinage afin de collecter le maximum de preuves sur l'événement, tout en conservant la distance de freinage nécessaire pour éviter une collision.

4.7 Intégration du consensus dans la formule du surcoût de la sécurité

D'après la formule du surcoût global de la sécurité donnée en section 3.1, nous y ajoutons le délai du mécanisme de consensus $D_{consensus}$. Le délai du consensus équivaut au délai de décision de la méthode de décision employée.

Dans un souci de lisibilité, nous n'écrivons pas tous les services de sécurité listés au chapitre 2 et les représentons par « ... » dans les Équations 4.15 et 4.16. Nous obtenons la formule suivante :

$$D_{sécurité} = D_{authentification} + D_{consensus} + D_{confidentialité} + \cdots \quad (4.15)$$

Mais le consensus utilise l'authentification pour chaque message engagé dans le processus de décision. Nous considérons l'authentification comme un paramètre du délai du consensus.

$$D_{sécurité} = D_{consensus} + \cdots = \sum_{i=1}^{N_E} X_i \times \left(D_{authentification} + D_{filter} + D_{classifier} + D_{decision\_maker}\right) + \cdots \quad (4.16)$$

N_E est le nombre total d'événements que subit le véhicule et X_i est la valeur de *X* pour l'événement *i*. Nous remarquons donc que le mécanisme d'authentification a un impact sur le mécanisme de consensus et de manière générale sur toutes les applications nécessitant la collecte d'informations.

4.8 Conclusion

Avec des applications ayant un impact direct sur la vie des usagers et des communications ad hoc, les VANETs ont besoin d'instaurer une confiance entre les entités du réseau. Afin de répondre à ce besoin, nous analysons dans ce chapitre le mécanisme de consensus. Le consensus permet de vérifier la plausibilité d'une alerte en collectant des informations de multiples sources. Le véhicule prend alors une décision en fonction du résultat de la méthode de décision. Le consensus dépend donc principalement de la méthode de décision qui fixe les paramètres du consensus. Ce chapitre contient deux contributions : l'analyse du surcoût du consensus et une proposition de méthode de décision dynamique et multisources.

Afin de répondre à la problématique d'établissement de la confiance et de son surcoût dans les VANETs, nous avons tout d'abord défini les notions de confiance, de consensus et effectué un état de l'art des solutions existantes. Nous avons détaillé les trois processus du consensus : détection, dissémination et décision.

Nous nous sommes ensuite focalisés sur le processus de décision, car c'est durant cette phase que la réaction à l'alerte sera prise. Il est donc primordial de prendre la meilleure solution possible pour le véhicule concerné. Nous avons détaillé cinq méthodes de décision. La méthode *« Majority of Freshest X with Threshold »* a particulièrement retenu notre attention, car elle a démontré de bons résultats de simulation.

Nous avons ensuite décidé d'établir un modèle conceptuel et analytique de méthode de décision. Ainsi, à partir d'un ensemble de modules, nous pouvons calculer le délai moyen de décision. Nous avons appliqué cette modélisation à la méthode *« Majority of Freshest X with Threshold »* et obtenu une formule du délai de décision.

Après avoir soulevé des axes d'amélioration, nous avons proposé une méthode de décision dynamique. Les paramètres de consensus sont fixés en fonction de l'environnement réseau et du contenu des alertes. Nous avons formalisé notre méthode par le biais d'un filtre de Kalman et proposé une méthodologie pour définir ses paramètres.

Enfin, nous avons intégré le consensus dans la formule globale du surcoût de la sécurité.

Une perspective à court terme consiste à effectuer une validation par simulation de notre méthode de décision. Nous souhaitons cependant lever l'hypothèse d'identifiant global unique d'événement (*Globally Unique Identifier*, GUID) qui nécessite une synchronisation (temporelle, spatiale) entre les véhicules. En effet, pour stocker les messages dans une file d'attente spécifique à l'événement, le véhicule doit être capable d'identifier l'événement concerné. Pour cela, nous proposons un système d'apprentissage qui permet d'évaluer la probabilité de fausses alertes (que nous appelons *bruit*). Ainsi, le véhicule calcule le niveau de bruit et ne réagira que lorsque le nombre de messages reçus (quel que soit l'événement) dépasse le bruit. Faisons une analogie avec « l'appel de phare ». Lorsqu'un conducteur détecte un événement, il fait un appel de phare pour avertir les véhicules se dirigeant sur l'endroit. Le conducteur récepteur de cet appel de phare ne connaît pas le lieu exact de l'événement, il

sait simplement qu'il doit faire attention. Au début, le récepteur fera pleinement confiance et réagira dès le premier appel de phare. Par la suite, lorsqu'il aura parcouru une certaine distance sans avoir observé le moindre événement, il en déduira qu'il s'agissait d'une fausse alerte (ou que l'événement a disparu). Ainsi, la prochaine fois qu'il recevra un appel de phare, il attendra d'en recevoir plusieurs avant de réagir. Dans notre cas, le but est de calculer le niveau moyen de bruit et de le faire évoluer dans le temps. Ce niveau moyen de bruit est vu comme le seuil de déclenchement de réaction et sera utilisé pour définir p (cf. Équation 4.9).

5 Conclusion et perspectives

Dans un futur proche, les véhicules sont appelés à devenir de plus en plus intelligents, et ce, notamment grâce à l'ajout de communication sans fil. Ainsi, par le biais de communication véhicule à véhicule, les véhicules seront à l'écoute de l'environnement et partagerons des informations. Cependant, afin d'être accepté par le grand public, il est nécessaire d'assurer un niveau de sécurité suffisant. Pour cela, il faut déployer une multitude de services de sécurité (confidentialité, authentification, intégrité, respect de la vie privée, contrôle d'accès, disponibilité, non-répudiation). Mais, l'ajout de service de sécurité rend le système plus complexe et potentiellement plus consommateur de ressources (réseau, temps, énergie). Il est donc primordial de maîtriser le coût de chacun de ces services. Pour répondre à cette problématique, cette thèse a été consacrée à l'étude du surcoût de l'authentification et du consensus dans la sécurité des réseaux sans fil véhiculaires. C'est à notre connaissance le premier travail à poser un paradigme général du surcoût de la sécurité dans les VANETs et étudiant séparément puis conjointement l'authentification et le consensus. Dans ce chapitre de conclusion, nous présentons une mise en perspective de nos contributions ainsi que de nouvelles pistes à explorer.

5.1 Contributions

Dans un premier temps, nous avons effectué un état de l'art détaillé consacré à notre travail : les réseaux sans fil véhiculaires d'une part, et la sécurité de ces réseaux d'autre part. L'analyse de la littérature sur la sécurité des réseaux sans fil véhiculaires fait apparaître le service d'authentification comme la pierre angulaire des applications de sécurité du trafic routier.

Afin de répondre à la problématique du surcoût de la sécurité, notre première contribution consiste à étudier le protocole responsable de l'authentification dans les VANETs : ECDSA. Le service

d'authentification est décomposé en trois étapes : génération de signature numérique, transfert du message signé, vérification de signature numérique.

Dans un premier temps, nous nous sommes intéressés au *temps de calcul*, c'est-à-dire au temps nécessaire pour la génération et la vérification des signatures numériques. Nous avons analysé la complexité d'ECDSA et effectué des expérimentations afin d'évaluer chacune des opérations mathématiques employées dans cet algorithme.

Dans un second temps, nous avons complété la formule du surcoût de la sécurité avec la partie « communication », c'est-à-dire le *délai de transfert*. Nous avons ainsi étudié le standard IEEE 1609 qui régit les communications sans fil véhiculaires afin d'appréhender en détail l'ensemble des couches de la pile de communication. En terme de délai de transfert, le surcoût de la sécurité se traduit principalement par une taille de paquet plus grande (et donc un risque de collision plus important). Nous avons défini analytiquement le délai de transfert d'un message et analysé par simulation l'impact de l'authentification sur le délai de transfert.

Ainsi, nous avons proposé une formule du surcoût de l'authentification qui prend en compte le temps de calcul et le temps réseau. Nous nous sommes focalisés sur l'application d'alerte de danger local, car elle soulève des contraintes temporelles fortes, et a un impact direct sur la distance de freinage et donc sur l'usager et le trafic routier. Nous avons remarqué qu'en plus du mécanisme d'authentification en lui-même, le choix de la clé d'authentification a aussi un impact temporel et spatial.

Nous avons ensuite analysé l'impact du temps de calcul et l'avons comparé au délai de transfert d'un message. Nous avons remarqué que 80 % du surcoût de l'authentification d'un message vient du temps de calcul. Nous avons souligné que le temps de calcul est dépendant de l'implémentation de l'OBU choisie (présence d'un crypto-processeur, algorithme de multiplication modulaire, etc.). Pour un message, le surcoût peut sembler faible, mais cela est dû à la petite taille du paquet.

Cependant, les réseaux véhiculaires soulèvent de nombreux problèmes de sécurité et l'authentification ne sera pas le seul service déployé. Ainsi, dans notre deuxième contribution, nous complétons notre formule du surcoût de la sécurité avec un nouveau mécanisme. Étant donné le contexte des réseaux ad hoc véhiculaires, un problème majeur est l'établissement de la confiance. En effet, un véhicule authentifié peut générer de fausses informations. C'est pourquoi, après avoir détaillé la notion de confiance, nous avons introduit le mécanisme de consensus. Grâce à une méthode de décision, le consensus permet d'analyser l'événement afin de prendre la meilleure décision pour le conducteur. Ce mécanisme ajoute cependant un nouveau délai : le *délai de décision*. Nous l'avons analysé ainsi que son impact sur la distance de freinage. Nous avons souligné l'implication d'un tel mécanisme dans le surcoût global de la sécurité.

Nos deux premières contributions ont permis d'établir un paradigme général du surcoût de la sécurité. Nous avons établi les formules régissant le surcoût de l'authentification et du consensus. Ainsi, en fonction des besoins de l'application, un concepteur d'application ou de solutions de sécurité peut connaître le surcoût de sa méthode et ainsi ajuster les paramètres en conséquence (taille de la clé,

niveau de sécurité). Nous avons aussi analysé l'impact de la sécurité sur les performances applicatives (notamment la distance de freinage).

Afin de réduire le surcoût du consensus, notre troisième contribution consiste à proposer une méthode de décision dynamique qui prend en compte le contenu de l'alerte et l'environnement réseau. À partir d'un modèle conceptuel et analytique, nous avons proposé une méthode pour définir les paramètres du consensus.

5.2 Perspectives

Les contributions de cette thèse ont apporté des réponses à certains problèmes, mais il reste des pistes à explorer. Chacune de ces pistes est une perspective possible dans la continuité de cette thèse.

5.2.1 À court et moyen terme

- *Poursuite des simulations* : Dans un premier temps, nous pouvons valider la méthodologie proposée pour déterminer dynamiquement les paramètres du consensus. Pour cela, à partir du modèle sans attaquant que nous avons, nous désirons lancer une série de simulations avec un pourcentage d'attaquants allant jusqu'à 49 %. Le but premier est d'évaluer le niveau moyen de bruit et de tester le comportement de notre méthode de décision. Le second objectif est de proposer plusieurs méthodes de décision et de les comparer, car nous pensons qu'une unique méthode de décision ne peut pas répondre à toutes les situations. Il est donc parfois intéressant de changer de méthode de décision en fonction du contexte. Les premiers résultats de simulation sont encourageants [PET 11] et notre méthode dynamique démontre une augmentation de la confiance grâce à la prise en compte de l'environnement réseau, de l'événement, et des contraintes temporelles applicative.

- *Analyse de l'impact de la sous-couche MAC* : Dans un second temps, il serait intéressant d'analyser l'impact de la sous-couche MAC sur le délai nécessaire pour recevoir les X messages. En effet, dans le standard IEEE 802.11p/WAVE, l'OBU écoute et émet sur les canaux de contrôle (CCH) et les canaux de services (SCH) de manière alternée. Les messages relatifs aux applications de sécurité du trafic routier sont émis sur le CCH. Ainsi, les OBUs vont entrer en compétition pour émettre l'alerte lors du CCH. Nous définirons analytiquement la probabilité d'avoir X messages en un temps donné (T_{safety} par exemple).

- *Détermination du comportement par la théorie des jeux* : Dans notre troisième contribution, nous avons vu que la méthode de décision influence le nombre de messages émis sur le réseau. En effet, un véhicule peut prendre la décision de diffuser l'alerte à son tour. Ainsi, la méthode de décision impacte la contention du canal et peut donc venir mettre à mal le consensus ou allonger le temps nécessaire pour atteindre le consensus au niveau du véhicule suivant. Dans la continuité, nous pourrons utiliser la théorie des jeux pour déterminer le comportement optimal du véhicule en fonction des autres pour atteindre le meilleur niveau de sécurité routière.

- *Analyse du surcoût du mécanisme de certification* : La formule de l'authentification proposée ne prend en compte que les mécanismes de génération, de transfert et de vérification de signature numérique. Or, dans le service d'authentification, il y a aussi un mécanisme de certification. Il serait donc intéressant de l'analyser afin de voir son implication. Ce dernier est composé de la distribution de certificat, de la vérification de certificat et de la révocation de certificat. Parmi ces processus, celui responsable de la vérification est potentiellement le plus consommateur, car il est appelé avant chaque vérification de signature numérique. Les processus de distribution et de révocation sont appelés moins fréquemment. Nous pourrons donc nous intéresser à la vérification de certificat. Le mécanisme de certification n'est pas clairement défini dans le standard IEEE 1609, mais il est fait état d'utilisation de listes de révocation (CRL). Cependant, les CRLs ne seront pas forcément à jour et il sera nécessaire de réclamer une mise à jour de CRL. Cela pose un souci dans le cadre des VANETs car aucune infrastructure n'est présente. Nous pouvons donc imaginer le cas où les voisins doivent transmettre la demande de mise à jour au RSU le plus proche. Il y a donc ici une utilisation du réseau ad hoc de manière « temporaire » et à courte portée (inférieur à 2 kilomètres par exemple). Dans ce cas, le mécanisme de certification vient ajouter un nouveau délai et entraine une augmentation de la charge du réseau.

- *Optimisation de la gestion des certificats* : D'après le standard IEEE 1609.2, un certificat, couvrant une seule application pour un OBU, et utilisant une clé d'authentification de 224 bits, a une taille de 125 octets. Il a été prévu la possibilité d'utiliser une version plus courte du certificat : un condensé. Un condensé de certificat est une référence vers le certificat. Il est donc inutile pour un récepteur qui n'a pas précédemment reçu le certificat complet. On peut se demander dans quel cas utiliser un certificat complet plutôt qu'un condensé de certificat. Quand une série de messages est envoyée pour une même application, il est possible d'inclure le certificat complet dans le premier message et seulement le condensé pour le reste de la série. Néanmoins, si le récepteur manque le premier message, alors le service ne pourra pas être assuré avec succès. De plus, cette technique n'est pas applicable dans le cas de diffusion des messages d'alerte. En effet, la nature transitoire des liens de communication d'un réseau sans fil véhiculaire fait que chaque message émis est potentiellement le premier reçu par les véhicules récepteurs. Il faut donc inclure le certificat complet à chaque envoi. Pour réduire la consommation de bande passante, une technique consiste à inclure le certificat complet à fréquence régulière, et ce, en fonction de la fréquence d'émission des WSMs. Par exemple, un véhicule émet un WSM toutes les 100 ms. Si un message sur trois contient le certificat complet, alors un véhicule devra attendre au maximum trois WSMs avant de pouvoir authentifier correctement l'émetteur. On économise ainsi $125 \times 3 - (125 + 8 + 8) = 516$ octets. Il y a clairement un compromis à prendre entre la consommation de bande passante et la latence d'authentification. Actuellement, aucun consensus ne se dégage et c'est un sujet de recherche actif.

5.2.2 À long terme

À long terme, nous pouvons explorer deux axes : le respect de la vie privée et l'optimisation de notre modélisation de méthodes de décision.

- *Analyse du surcoût de la vie privée* : Tout d'abord, nous pourrions compléter la formule globale en étudiant le respect de la vie privée, car ce service est primordial pour que les VANETs soient acceptés par le public. Cela ajoute une gestion des pseudonymes, et vient mettre à mal le système de réputation et la gestion des certificats. En effet, ne pouvant instaurer d'historique, car les identifiants des véhicules changent fréquemment, le véhicule est obligé de vérifier le certificat à chaque message reçu (ce qui met à mal l'amélioration proposée précédemment). Une idée serait d'utiliser la théorie des jeux pour modéliser le service de respect de la vie privée dans les VANETs. Ainsi, à partir de cette modélisation, nous pourrions en déduire son impact sur le temps et l'intégrer dans notre formule globale du surcoût de la sécurité.

- *Modélisation des méthodes de décision par le biais d'automates cellulaires* : Ensuite, afin d'optimiser notre modèle générique des méthodes de décision, nous pourrions étudier la possibilité d'utiliser les automates cellulaires. En effet, cet outil mathématique est un modèle déterministe qui permet d'analyser l'évolution d'un système auto-organisé dans le temps et l'espace. Les automates cellulaires sont notamment employés pour modéliser le trafic routier. Nous pourrions utiliser le modèle de Nagel et Schreckenberg pour modéliser l'environnement d'un véhicule. Ainsi le véhicule sera placé au centre de la matrice et le voisinage sera représenté par le modèle de Moore étendu. En fonction de l'état des cellules voisines, la cellule centrale change d'état. Cela correspond donc tout à fait à notre principe de consensus.

- *Réduction du surcoût de la sécurité* : Pour conclure, nous avons remarqué que 80 % du surcoût d'authentification est dû au temps de calcul. Les axes d'amélioration proposés sont une architecture physique dédiée ou un nouvel algorithme pour la multiplication modulaire. Néanmoins, la solution d'un crypto-processeur n'est pas viable, car elle est trop onéreuse (il faut compter 8000$ pour un IBM-4764 par exemple). Le projet PRESERVE, lancé au premier trimestre 2011, a pour but d'établir une architecture de sécurité pour les VANETs en combinant les projets SeVeCom (axé sur la sécurité V2V), Preciosa (axé sur le respect de la vie privée) et Evita (axé sur la création d'un TPD pour les communications internes au véhicule), en ayant à l'esprit le problème de passage à l'échelle et de coût (processeur, production, énergie, réseau).

Le projet PRESERVE démontre bien que la problématique du surcoût de la sécurité, traitée dans le cadre de cette thèse, est plus que jamais d'actualité et que de nombreux challenges restent à résoudre.

Bibliographie

[ABU 07] Abusharekh A., Gaj K., “Comparative Analysis of Software Libraries for Public Key Cryptography”, *Software Performance Enhancement for Encryption and Decryption (SPEED’07)*, pp. 3–19, Amsterdam, the Netherlands, June 2007.

[ADL 06] Adler C., Strassberger M., “Putting Together the Pieces - A Comprehensive View on Cooperative Local Danger Warning”, *13th ITS World Congress and Exhibition on Intelligent Transport Systems and Services (ITS’06)*, pp. 1–8, London, UK, October 2006.

[AGU 08] Aguado M., Matias J., Jacob E., Berbineau M., “The WiMAX ASN Network in the V2I Scenario”, *68th IEEE Vehicular Technology Conference (VTC’08)*, pp. 1–5, Calgary, Canada, September 2008.

[ANS 98] ANSI, “Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm”, ANSI X9.62-1998.

[ANT 05] Antipa A., Brown D.R.L., Gallant R.P., Lambert R.J., Struik R., Vanstone S.A., “Accelerated Verification of ECDSA Signatures”, *12th International Workshop on Selected Areas in Cryptography (SAC’05)*, pp. 307–318, Kingston, Canada, August 2005.

[AST 07] ASTM International, “E2213-03 - 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”, 2007.

[BAS 10] Basagni S., Petrioli C., Petroccia R., Stojanovic M., “Choosing the Packet Size in Multi-hop Underwater Networks”, *IEEE International Conference OCEANS*, pp. 1-9, Sydney, Australia, May 2010.

[BER 03] Beresford A.R., Stajano F., “Location privacy in pervasive computing”, *IEEE Pervasive Computing*, pp. 46–55, 2003.

[BIS 10] Biswas S., Misic J.V., “Establishing Trust on VANET Safety Messages”, *2nd International ICST Conference on Ad Hoc Networks (ADHOCNETS'10)*, pp. 314-327, Victoria, Canada, August 2010.

[BLI 02] Blincoe L., Seay A., Zaloshnja E., Miller T., Romano E., Luchter S., Spicer R., “The Economic Impact of Motor Vehicle Crashes”, U.S. Department of Transportation National Highway Traffic Safety Administration, Technical Report, 2002.

[BLU 04] Blum J.J., Eskandarian A., Hoffman L.J., “Challenges of Intervehicle Ad Hoc Networks”, *IEEE Transactions on Intelligent Transportation Systems*, vol. 5, no. 4, pp. 347–351, December 2004.

[BUC 08] Buchegger S., Mundinger J., Le Boudec J.Y., “Reputation Systems for Self-Organized Networks”, *IEEE Technology and Society Magazine*, vol. 27, no. 1, pp. 41–47, 2008.

[CAL 06] CALM Project (Continuous Air interface for Long and Medium distance), Available: http://www.isotc204wg16.org/concept.

[CAR 07] CARE, Community Road Accident Database, 2007.

[CER 00-1] Certicom Research, “Standards for efficient cryptography, SEC 1: Elliptic Curve Cryptography”, Version 1.0, September 2000.

[CER 00-2] Certicom, “Standards for Efficient Cryptography, SEC2: Recommended Elliptic Curve Parameters”, 2000.

[COM 09] COMeSafety consortium, “D31: European ITS Communication Architecture: Overall Framework Proof of Concept Implementation”, COMeSafety European Specific Support Action Public Deliverable, December 2009.

[COM 10] Com2REACT, European project, www.com2react-project.org.

[DAE 02] Daemen J., Rijmen V., “The Design of Rijndael: AES - The Advanced Encryption Standard”, Springer, ISBN 3-540-42580-2, 2002.

[DOE 05] Doetzer F., Kosch T., Strassberger M., “Classification for traffic related inter-vehicle messaging”, *5th IEEE International Conference on ITS Telecommunications (ITST’05)*, pp. 1–4, Brest, France, June 2005.

[DOM 09] Domingo-Ferrer J., Wu Q., “Safety and Privacy in Vehicular Communications”, *Lecture Notes In Computer Science*, vol. 5599, pp. 173–189, 2009.

[DOT 07] Dötzer F., “Security Concepts for Robust and Highly Mobile Ad-hoc Networks”, *PhD thesis*, Technical University of Munich, September 2007.

[DRA 07] Drawil N., “Improving the VANET Vehicles’ Localization Accuracy Using GPS Receiver in Multipath Environments”, *Master Thesis*, University of Waterloo, 2007.

[EIC 06] Eichler S., Schroth C., Kosch T., Strassberger M., “Strategies for Context-Adaptive Message Dissemination in Vehicular Ad Hoc Networks”, *2nd International Workshop on Vehicle-to-Vehicle Communications (V2VCOM’06)*, pp. 1–9, San Jose, USA, July 2006.

[ELB 05] El Batt T., Goel S., Kukshya V., Holland G., Krishnan H., Parikh J., “Communications Performance Evaluation of Cooperative Collision Warning Applications”, Document IEEE 802.11-05/0764r0, July 2005.

[ELH 08] El Hmam M.S, Jolly D., Abouaissa H., Benasser A., “Modélisation hybride du flux de trafic”, *Méthodologies et Heuristiques pour l'Optimisation des Systèmes Industriels (MHOSI’08)*, pp. 193–198, Janvier 2008.

[ERS 07] European Road Safety Observatory, “Traffic Safety Basic Facts”, 2007.

[FEN 07] Feng Y., “Adaptive Trust Management in MANET”, *International Conference on Computational Intelligence and Security (CIS’07)*, pp. 804–808, Harbin, China, December 2007.

[GAL 07] Galice S., “Modèle dynamique de sécurité pour réseaux spontanés”, Institut National des Sciences Appliquées de Lyon, Thèse de Doctorat, 2007.

[GER 06] Gerlach M., Steglich S., Arbanowski S., Wegdam M., Teunissen H., “Trustworthy ap- plications for Vehicular Environments”, *IEEE Vehicular Technology Magazine*, vol. 1, no. 2, pp. 9–15, 2006.

[GOL 04] Golle P., Greene D., Staddon J., “Detecting and Correcting Malicious Data in VANETs”, *1st ACM International Workshop on Vehicular Ad Hoc Networks (VANET’04)*, pp. 29–37, Philadephia, USA, September 2004.

[GRE 09] Green M., “Perception-reaction time: Is Olson (& Sivak) all you need to know?”, *Collision The International Compendium for Crash Research*, vol. 4, pp. 88–93, 2009.

[GUA 03] Guan D.J., “Montgomery Algorithm for Modular Multiplication”, 2003, Available: http://isl.cse.nsysu.edu.tw/note/montg.pdf.

[HAA 09] Haas J.J., H-C. Chu, K. P. Laberteaux, “Real-World VANET Security Protocol Performance”, *28th IEEE conference on Global telecommunications (GLOBECOM’09)*, pp. 1–7, Hawai, USA, November 2009.

[HED 06] Hedabou M., (2006) “Amélioration et sécurisation des calculs arithmétiques pour la cryptographie basée sur les courbes elliptiques”, *Thèse de l’Institut National des Sciences Appliquées de Toulouse*, Octobre 2006.

[HED 97] Hedrick J.K, Tomizuka M., Varaiva P., “Control issue in automated highway systems”, *IEEE Control System Magazine*, vol. 14, no. 6, pp. 21–32, 1997.

[HOF 98] Hoffstein J., Pipher J., Silverman J.H., “NTRU : a ring based public key cryptosystem”, *Lecture Notes In Computer Science*, vol. 1423, pp. 267–288, 1998.

[HOW 05] Howson C., Urbach P., “Scientific Reasoning: the Bayesian Approach (3rd edition)”, Open Court Publishing Company, ISBN 978-0812695786, 2005.

[HUA 05] Huang L., Sampigethaya K., Matsuura K., Poovendran R., Sezaki K., Caravan M.L., "Providing Location Privacy for VANET", *3rd International Conference on Embedded Security in Cars (ESCAR'05)*, Cologne, Germany, November 2005.

[HUB 05] Hubaux J.P., "Vehicular Networks: How to Secure Them", *MiNeMa Summer School*, Klagenfurt, Germany, July 2005.

[HYU 10] Hyun-Jin Kim T., Studer A., Dubey R., Zhang X., Perrig A., Bai F., Bellur B., Iyer A., "VANET Alert Endorsement Using Multi-Source Filters", *7th ACM International Workshop on Vehicular Ad Hoc Networks (VANET'10)*, pp. 51–60, Chicago, USA, September 2010.

[IEE 07] IEEE, "Trial Use Standard for Wireless Access in Vehicular Environments (WAVE) - Architecture", March 2007.

[IEE 10] IEEE Standard 802.11p, "IEEE Standard for Information technology--Telecommunications and information exchange between systems--Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments", 2010.

[IEE 99] IEEE Standard 802.11a, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: High-speed Physical Layer in the 5 GHz Band", 1999.

[ISO 03] International Organization for Standardization, "Traffic and Traveller Information (TTI)–TTI messages via traffic message coding Part 1: Coding protocol for Radio Data System–Traffic Message Channel (RDS-TMC) using ALERT-C", ISO 14819-1, 2003.

[ISO 99] ISO/IEC, "Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 1: Mechanisms using a block cipher", ISO/IEC 9797-1, 1999.

[JAR 07] Järvinen K., Skyttä J., "Final Project Report: Cryptoprocessor for Elliptic Curve Digital Signature Algorithm (ECDSA)", 2007.

[JOH 01] Johnson D., Menezes A., Vanstone S., "The Elliptic Curve Digital Signature Algorithm (ECDSA)", *International Journal of Informatics Security*, vol. 1, no. 1, pp. 36–63, 2001.

[JOH 98] Johnson D.B., Menezes A.J., "Elliptic Curve DSA (ECDSA): An Enhanced DSA", 7th conference on USENIX Security Symposium (SSYM'98), vol. 7, 1998.

[KAI 05] Kaihara M.E., Naofumi Takagi N., "A Hardware Algorithm for Modular Multiplication/Division Based on the Extended Euclidean Algorithm", *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E88–A, pp. 3610–3617, 2005.

[KAR 06] Kargl F., Ma Z., Schoch E., "Security Engineering for VANETs", *4th Workshop on Embedded Security in Cars (ESCAR'06)*, pp. 1–10, Berlin, Germany, 2006.

[KOB 87] Koblitz N., “Elliptic Curve Cryptosystems”, *Mathematics of Computation*, vol. 48, pp. 203–209, 1987.

[KOR 93] Kornerup P., “High-radix Modular Multiplication for Cryptosystems”, *11th Symposium on Computer Arithmetic*, pp. 277–283, Windsor, Canada, July 1993.

[KOT 99] Kotsialos A., Papageorgiou M., Meßner A., “Integrated Optimal Control of Motorway Traffic Networks”, *American Control Conference (ACC’99)*, vol. 3, pp. 2183–2187, San Diego, USA, June 1999.

[KRO 06] Kroh R., Kung A., Kargl F., “VANETS Security Requirements Final Version”, Technical report, Secure Vehicle Communication (Sevecom), September 2006.

[LAU 06] Laurendeau C., Barbeau M., “Threats to security in DSRC/WAVE”, *5th International Conference on Ad-hoc Mobile and Wireless Networks (ADHOC-NOW’06)*, vol. 4104, pp. 266–279, Ottawa, Canada, August 2006.

[LEI 07] Leinmuller T., Schoch E., Maihofer C., “Security Requirements and Solution Concepts in Vehicular Ad Hoc Networks”, *4th Annual Conference on Wireless on Demand Network Systems and Services (WONS’07)*, pp. 84–91, Obergurgl, Tyrol, Austria, January 2007.

[LIN 08] Lin X., Lu R., Zhang C., Zhu H., Ho P.H., Shen X., “Security in vehicular ad hoc networks”, *IEEE Communications Magazine*, vol. 46, no. 4, pp. 88–95, April 2008.

[LO 07] Lo N.W., Tsai H.C., “Illusion Attack on VANET Applications – A Message Plausibility Problem”, *IEEE Globecom Workshops*, pp. 1–8, Washington DC, USA, November 2007.

[LO 09] Lo N.W., Tsai H.C., “A Reputation System for Traffic Safety Event on Vehicular Ad Hoc Networks”, *EURASIP Journal on Wireless Communication and Networking*, vol. 2009, pp. 1–10, September 2009.

[LOC 07] Lochert C., Scheuermann B., Caliskan M., Mauve M., “The feasibility of information dissemination in vehicular ad-hoc networks”, *4th Annual Conference on Wireless On-demand Network Systems and Services (WONS’07)*, pp. 92–99, Obergurgl, Tyrol, Austria, January 2007.

[MA 08] Ma S., Hao Y., Pan Z., Chen H., “Fast Implementation for Modular Inversion and Scalar Multiplication in the Elliptic Curve Cryptography”, *2nd International Symposium on Intelligent Information Technology Application (IITA’08)*, vol. 2, pp. 488–492, Shangai, China, December 2008.

[MAT 05] Matheus K., Morich R., Paulus I., Menig C., Lübke A., Rech B., Specks W., “Car-to-car communication – market introduction and success factors”, *5th European Congress and Exhibition on Intelligent Transport Systems and Services (ITS’05)*, pp. 1–10, Hannover, Germany, June 2005.

[MEN 01] Menezes A.J., Van Oorschot P.C., Vanstone S.A., “Handbook of Applied Cryptography”, CRC Press, 2001.

[MIL 86] Miller V.S., “Use of Elliptic Curves in Cryptography”, *Advances in Cryptology (CRYPTO’85), Lecture Notes in Computer Science*, vol. 218, pp. 417–426, 1986.

[MIR 00] “MIRACL User's Manuel”, Shamus Software Limited, April 2000, Available : http://www.shamus.ie/uploads/docs/userman.pdf.

[NAK 58] Nakagami M., “The m-Distribution, a general formula of intensity of rapid fading”, *Symposium on Statistical Methods in Radio Wave Propagation*, pp. 3–36, Los Angeles, USA, June 1958.

[NEG 04] Negre C., “Opérateurs Arithmétiques pour la Cryptographie Basée sur les Courbes Elliptiques”, *Thèse de l’Université de Montpellier II*, Septembre 2004.

[NEG 05] Negre C., “Scalar Multiplication on Elliptic Curves Defined over Fields of Small Odd Characteristic”, *Lecture Notes in Computer Science*, vol. 3797, pp. 389–402, 2005.

[NHT 08] NHTSA, “Traffic Safety Fact Sheet”, 2008.

[NIK 08] Nikooghadam M., Bonyadi M.R., Malekian E., Zakerolhosseini A., “A Protocol for Digital Signature Based on the Elliptic Curve Discrete Logarithm Problem”, *Journal of Applied Sciences*, vol. 8, pp. 1919–1925, 2008.

[NIS 02] National Institute of Standards and Technology, “Fips 180-2, Secure Hash Standard, Federal Information Processing Standard (fips)”, Publication 180-2, 2002.

[NIS 99] National Institut of Standards and Technology, “Recommended Elliptic Curves for Federal Government Use”, 1999.

[NS2] The network simulator - ns-2. http://nsnam.isi.edu/nsnam/.

[OKE 01] Okeya K., Sakura K., “Efficient Elliptic Curve Cryptosystems from a Scalar Multiplication Algorithm with Recovery of the *y*-Coordinate on a Montgomery-Form Elliptic Curve”, *3th International Workshop on Cryptographic Hardware and Embedded Systems (CHES’01)*, pp. 126–141, Paris, France, May 2001.

[ONI 10] Observatoire National Interministériel de la Sécurité Routière, “La sécurité routière en France : Bilan de l’année 2009”, 2010.

[OST 07] Ostermaier B., Dötzer F., Strassberger M., “Enhancing the Security of Local Danger Warnings in VANETs - A Simulative Analysis of Voting Schemes”, *2nd International Conference on Availability, Reliability and Security (ARES'07)*, pp. 422–431, Vienna, Austria, April 2007.

[PAP 09] Papadimitratos P., La Fortelle A., Evenssen K., Brignolo R., Cosenza S., “Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation”, *IEEE Communications Magazine*, vol. 47, no. 11, pp. 84-95, November 2009.

[PAR 92] Parsons J.D., “The Mobile Radio Propagation Channel”, Éditions Wiley, 1992.

[PER 02] Perrig A., Canetti R., Tygar J.D., Song D., “The TESLA broadcast authentication protocol”, *RSA CryptoBytes*, vol. 5, no. 2, 2002.

[PET 09] Petit J., “Analysis of ECDSA Authentication Processing in VANETs”, *3rd IFIP International Conference on New Technologies, Mobility and Security (NTMS’09)*, pp. 388–392, Cairo, Egypt, December 2009.

[PET 10] Petit J., Mammeri Z., “Analysis of Authentication Overhead in Vehicular Networks”, *3rd Joint IFIP Wireless and Mobile Networking Conference (WMNC’10)*, pp. 1–6, Budapest, Hungary, October 2010.

[PET 11] Petit J., Mammeri Z., “Dynamic Consensus for Secured Vehicular Ad hoc Networks”, *7th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob’11)*, pp. 1–8, Shangai, China, October 2011.

[RAO 09] Rao A., “Performance Evaluation of Secure Communication in Vehicular Networks”, Indian Institute of Technology Delhi, Master Thesis, January 2009.

[RAY 05] Raya M., Hubaux J.P., “The Security of Vehicular Ad Hoc Networks”, *3rd ACM Workshop on Security of Ad hoc and Sensor Networks (SASN’05)*, pp. 11–21, Alexandria, USA, November 2005.

[RAY 07] Raya M., Hubaux J.P., “Securing Vehicular Ad Hoc Networks”, *Journal of Computer Security - Special Issue on Security of Ad Hoc and Sensor Networks*, vol. 15, no. 1, pp. 39–68, 2007.

[RAY 09] Raya M., “Data-Centric Trust in Ephemeral Networks”, *PhD thesis*, no. 4423, EPFL, June 2009.

[REA 06] REACT : Reaction to Emergency Alerts using voice and Clustering Technologies, European project, 2006.

[REI 02] Reichardt D., Miglietta M., Moertti L., Morsink P., Schulz W., “CarTALK 2000-safe and comfortable driving based upon inter-vehicle communication”, *IEEE Intelligent Vehicle Symposium (IV’02)*, Versailles, France, June 2002.

[RES 08] Resendes R., “The New ‘Grand Challenge’ - Deploying Vehicle Communications”, *5th ACM International Workshop on Vehicular Internetworking (VANET’08)*, San Francisco, USA, September 2008.

[RIT 09] RITA/ITS, “IEEE 1609 - Family of Standards for Wireless Access in Vehicular Environments (WAVE)”, http://www.standards.its.dot.gov/fact_sheet.asp?f=80, September 2009.

[RIV 92] Rivest R., “The MD5 Message Digest Algorithm”, RFC1321, April 1992.

[SAV 05] Savaş E., Nasser M., Gutub A.A.A., Koç Ç.K., “Efficient Unified Montgomery Inversion with Multibit Shifting”, *Journal of Computers and Digital Techniques*, vol. 152, no. 4, pp. 489–498, July 2005.

[SCH 08] Schmidt R.K., Leinmüller T., Schoch E., Held A., Schäfer G., “Vehicle Behavior Analysis to Enhance Security in VANETs”, *4th IEEE Workshop on Vehicle to Vehicle Communications (V2VCOM’08)*, Eindhoven, the Netherlands, June 2008.

[SHA 02] Shafer G., “Dempster-Shafer Theory”, University of Kansas, Lawrence, Kansas, USA, 2002.

[SHO 97] Shor P.W., “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer”, *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, October 1997.

[STA 03] Staulinger M., “Electronic Vehicle Identification Using Active Infrared Light Transmission”, *10th World Congress on Intelligent Transport Systems and Services (ITSS’03)*, Madrid, November 2003.

[SUN 04] Sun Q., Garcia-Molina H., “Using Ad-hoc Inter-vehicle Networks for Regional Alerts”, Technical report, Stanford University, 2004.

[SUN 06] Sun Y., Yu W., Han Z., Ray Liu K.J., “Information theoretic framework of trust modeling and evaluation for ad hoc networks”, *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 305–317, February 2006.

[TAJ 03] Tajima T., Sugawara T., “Our tackling on further advancement of information uplinking function”, *10th World Congress on Intelligent Transport Systems and Services (ITSS’03)*, Madrid, November 2003.

[TAJ 10] Tajeddine A., Kayssi A., Chehab A., “A Privacy-Preserving Trust Model for VANETs”, *10th IEEE International Conference on Computer and Information Technology (CIT '10)*, pp. 832–837, Washington DC, USA, July 2010.

[TAL 04] Taliwal V., Jiang D., Mangold H., Chen C., Sengupta R., “Empirical Determination of Channel Characteristics for DSRC Vehicle-to-Vehicle Communication”, *1st ACM International Workshop on Vehicular Ad Hoc Networks (VANET’04)*, pp. 88, Philadephia, USA, September 2004.

[TCH 08] Tchepnda C., “Authentification dans les Réseaux Véhiculaires Opérés”, *Thèse Ecole Nationale Supérieure des Télécommunications*, Décembre 2008.

[THE 06] Theodorakopoulos G., Baras J.S., “On trust models and trust evaluation metrics for ad hoc networks”, *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 318–328, February 2006.

[VIN 09] Vinel A., Andreev S., Koucheryavy Y., Staehle D., “Estimation of a Successful Beacon Reception Probability in Vehicular Ad-hoc Networks”, *ACM International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly (IWCMC)*, pp. 416–420, Leipzig, Germany, June 2009.

[VSC 05] Vehicle Safety Consortium, “Task 3 Final Report - Identify Intelligent Vehicle Safety Applications Enabled by DSRC”, Vehicle Safety Communications Project, 2005.

[WAL 02] Walter J., “The Role of ECDSA in Wireless Communication (implementation and evaluation of ECDSA on constrained devices)”, *Master Thesis*, University of California, 2002.

[WIS 05] Wischhof L., Ebner A., Rohling H., Lott M., Halfmann R., “Self-Organizing Traffic Information System”, Inter-Vehicle-Communications Based on Ad Hoc Networking Principles : The Fleetnet Project, pp. 233–272, 2005.

[ZAN 08] Zang Y., Stibor L., Reumerman H.J., Chen H., “Wireless Local Danger Warning Using Inter-Vehicle Communications in Highway Scenarios”, *14th European Wireless Conference (EW’08)*, pp. 1–7, Prague, Czech Republic, June 2008.

[ZEN 09] Zeng X., Tao C., Chen Z., “The application of DSRC Technology in Intelligent Transportation System”, *IET International Communication Conference on Wireless Mobile & Computing (CCWMC’09)*, Shangai, China, November 2009.

[ZHA 11] Zhang J., “A Survey on Trust Management for VANETs”, *25th International Conference on Advanced Information Networking and Applications (AINA’11)*, pp. 1–8, Singapore, March 2011.

Annexes

I Liste des abréviations

3G : **3**ème **G**énération.

ACID : **A**pplication **C**lass **Id**entifier.

ACM : **A**pplication **C**ontext **M**ark.

ADAS : **A**dvanced **D**river **A**ssitance **S**ystem.

AES : **A**dvanced **E**ncryption **S**tandard.

CA : **C**ertificate **A**uthority.

CALM : **C**ommunication **A**rchitecture for **L**and **M**obile environment.

CBR : **C**onstant **B**it **R**ate (cf. ATM).

CCH : **C**ontrol **Ch**annel.

CCW : **C**ooperative **C**ollision **W**arning.

CME : **C**ALM **M**anagement **E**ntity.

CRC : **C**ontrôle de **R**edondance **C**yclique (**C**yclic **R**edundancy **C**heck).

CRL : **C**ertificat **R**evocation **L**ist.

CSMA/CD : **C**arrier **S**ense **M**ultiple **A**ccess / **C**ollision **D**etection.

DAB : **D**igital **A**udio **B**roadcasting.

DGPS : **D**ifferential **G**lobal **P**ositioning **S**ystem.

DMB : **D**igital **M**ultimedia **B**roadcasting.

DSRC : **D**edicated **S**hort **R**ange **C**ommunication.

DVB-H : **D**igital **V**ideo **B**roadcasting **H**andheld.

DVB-T : **D**igital **V**ideo **B**roadcasting **T**errestrial.

ECDSA : **E**lliptic **C**urve **D**igital **S**ignature **A**lgorithm.

ECIES : **E**lliptic **C**urve **I**ntegrated **E**ncryption **S**cheme.

ETSI : **E**uropean **T**elecommunication **S**tandards **I**nstitute.

FCC : **F**ederal **C**ommunications **C**ommission.

FIFO : **F**irst-**I**n **F**irst-**O**ut.

GNSS : **G**lobal **N**avigation **S**atellite **S**ystem.

GPRS : **G**lobal **P**acket **R**adio **S**ervice.

GPS : **G**lobal **P**ositioning **S**ystem.

GSM : **G**lobal **S**ystem **M**obile communication.

GUID : **G**lobally **U**niquer **Id**entifier.

IETF : **I**nternet **E**ngineering **T**ask **F**orce.

IP : **I**nternet **P**rotocol.

IR : **I**nfra**R**ouge.

ISO : **I**nternational **O**rganization for **S**tandardization.

ITS : **I**ntelligent **T**ransportation **S**ystem.

ITU : **I**nternational **T**elecommunication **U**nion.

ITU-T : **I**nternational **T**elecommunication **U**nion, **T**elecommunications Standardization Sector.

IVC : **I**nter **V**ehicle **C**ommunication.

LAN : **L**ocal **A**rea **N**etwork.

MAC : **M**edium **A**ccess **C**ontrol.

MAN : **M**etropolitan **A**rea **N**etwork.

MANET : **M**obile **A**d hoc **Net**work.

NTIC : **N**ouvelles **T**echnologies d'**I**nformation et de **C**ommunication.

PKI : **P**ublic **K**ey **I**nfrastructure.

QoS : **Q**uality **o**f **S**ervice.

RCP : **R**esource **C**ommand **P**rocessor.

RDS : **R**adio **S**ystem **D**ata.

RFC : **R**equest **F**or **C**omments.

RM : **R**esource **M**anager.

RMA : **R**esource **M**anager **A**pplication.

RTK : **R**eal **T**ime **K**inematic.

RTT : **R**ound **T**rip **T**ime.

SCH : **S**ervice **Ch**annel.

TCP : **T**ransport **C**ontrol **P**rotocol.

TEK : **T**raffic **E**ncryption **K**ey.

TMC : **T**raffic **M**essage **C**hannel.

TPD : **T**amper **P**roof **D**evice.

UDP : **U**ser **D**atagram **P**rotocol.

UMTS : **U**niversal **M**obile **T**elecommunication **S**ystem.

UTM : **U**niversal **T**ransverse **M**ercator.

V2I : **V**ehicle-to-**I**nfrastructure.

V2V : **V**ehicule-to-**V**ehicule.

VANET : **V**ehicular **A**d hoc **Net**work.

VSN : **V**ehicular **S**ensor **N**etwork.

WAN : **W**ide **A**rea **N**etwork.

WAVE : **W**ireless **A**ccess for the **V**ehicular **E**nvironment.

WiFi : **W**ireless **F**idelity.

WiMAX : **W**orldwide **I**nteroperability for **M**icrowave **A**ccess.

WSA : **W**AVE **S**ervice **A**dvertisement.

WSM : **W**AVE **S**hort **M**essage.

WSMP : **W**AVE **S**hort **M**essage **P**rotocol.