Optimisation de routage dans les réseaux véhiculaires par la prédiction de rupture de lien

Soumia Bourebia

▶ **To cite this version:**

Soumia Bourebia. Optimisation de routage dans les réseaux véhiculaires par la prédiction de rupture de lien. Réseaux et télécommunications [cs.NI]. Université de Haute Alsace - Mulhouse, 2019. Français. NNT : 2019MULH3003 . tel-03650636

HAL Id: tel-03650636

https://theses.hal.science/tel-03650636

Submitted on 25 Apr 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

UNIVERSITÉ HAUTE-ALSACE

UNIVERSITÉ DE HAUTE-ALSACE

IRIMAS UNIVERSITÉ HAUTE-ALSACE

ÉCOLE DOCTORALE MATHÉMATIQUES, SCIENCES DE L'INFORMATION ET DE L'INGÉNIEUR

INSTITUT DE RECHERCHE EN INFORMATIQUE, MATHÉMATIQUES, AUTOMATIQUE ET SIGNAL

THÈSE Présentée par :

Soumia BOUREBIA

soutenue le : 05 décembre 2019

pour obtenir le grade de : **Docteur de l'université de Haute-Alsace**

Discipline/ Spécialité : Informatique

OPTIMISATION DE ROUTAGE DANS LES RÉSEAUX VÉHICULAIRES PAR LA PRÉDICTION DE RUPTURE DE LIEN

Thèse dirigée par :

M. LORENZ Pascal Professeur des Universités, Université de Haute-Alsace, Mulhouse

RAPPORTEURS :

M. FOUCHAL Hacène Professeur des Universités, Université de Reims Champagne Ardenne, Reims

M. CHALHOUB Gérard Maître de conférences HDR, Université de Clermont Auvergne, Clermont-Ferrand

EXAMINATEUR :

M. GUYENNET Hervé Professeur des Universités, Université de Franche-Comté, Besançon

---

CO-DIRECTEUR DE THÈSE :

M. HILT Benoit Maître de Conférences HDR, Université de Haute-Alsace, Mulhouse

CO-ENCADRANT DE THÈSE :

M. DROUHIN Frédéric Maître de Conférences, Université de Haute-Alsace, Mulhouse

INVITÉ :

M. BINDEL Sébastien Maître de conférences, Université de Haute-Alsace, Mulhouse

Remerciements

Ce travail de thèse a été mené au sein du Groupe de Recherche en Réseaux et Télécommunications du laboratoire IRIMAS de l'Université de Haute-Alsace (UHA, France), et financé par le gouvernement algérien.

Vous étiez nombreux à m'accompagner tout au long de cette aventure :

Tout d'abord, j'aimerais exprimer ma grande reconnaissance et gratitude à mon directeur de thèse, Monsieur Pascal Lorenz et à mon co-directeur, Monsieur Benoît Hilt. Merci de votre encadrement, de votre assistance, de votre savoir, de votre orientation et vos conseils précieux ainsi que pour être disponibles en dépit de vos nombreuses charges. Je remercie vivement Monsieur Lorenz de m'avoir accueillie au sein de son groupe de recherche et d'avoir mis à ma disposition les moyens nécessaires pour mener à bien mes travaux de thèse.

Je remercie mon co-encadrant de thèse, M. Frédéric Drouhin, Maître de conférences au laboratoire IRIMAS de l'Université de Haute-Alsace, pour tous ses conseils, son soutien, ses encouragements et de m'avoir supportée tout au long de cette thèse. J'ai beaucoup apprécié et pris un grand plaisir à travailler avec lui.

Tous mes remerciements vont également à monsieur Sébastien Bindel, Maître de conférences à l'Université de Haute-Alsace, pour l'aide qu'il m'a apportée, ses précieux conseils, sa patience, son encouragement et le partage de son savoir.

Je tiens aussi à remercier Monsieur Jean-Philippe Lauffenburger, professeur à l'Université de Haute-Alsace, de nous avoir rendu visite à plusieurs reprises et de m'avoir invitée à régulièrement à son laboratoire pour effectuer ces travaux de recherche. Pendant mon doctorat, j'ai également eu la chance de travailler avec Monsieur Jonathan Ledy et Madame Hind Laghmara. Je les remercie

de leurs collaborations et de leurs contributions à ce travail.

Je remercie Monsieur Hacène Fouchal, Professeur des Universités de l'Université de Reims, et Monsieur Gérard Chalhoub, Maître de conférences à l'Université de Clermont Auvergne, pour leur intérêt et d'avoir accepté de rapporter mon travail. Je les remercie pour les différentes remarques et corrections qu'ils ont suggérées et qui ont permis d'augmenter la qualité de ce mémoire de thèse. Je remercie aussi Monsieur Hervé Guyennet, Professeur des Universités travaillant à l'Université de Technologie de Franche-Comté, pour avoir accepté d'examiner mon travail et de faire partie de mon jury.

Je remercie également tous les membres et ex-membres du GRTC de m'avoir soutenue et de m'avoir aidée en me fournissant l'information et l'aide nécessaire pour tous les problèmes rencontrés (liés au travail ou autre) pendant mon séjour à Colmar. Je voudrais exprimer particulièrement toute mon amitié et ma gratitude à Karima et Dorine pour leur grande gentillesse et leur bonne humeur.

Merci à mes très chères amies Afifa, Hasna, Leila et Anissa pour tous les moments que nous avons partagés ensemble. Merci à vous d'être toujours là pour moi.

Je tiens également à remercier Monsieur Florian Kohler, ainsi que tous mes amies et mes enseignants qui m'ont toujours encouragée et m'ont donné de précieux conseils quand j'en avais besoin.

Merci à tous ceux qui ont contribué de près ou de loin à l'aboutissement de ce travail.

Enfin, les mots les plus simples étant les plus forts, j'adresse mes remerciements les plus chaleureux et toute mon affection à mes chers parents, à mes frères et à ma soeur pour avoir fait de moi ce que je suis aujourd'hui, d'avoir toujours cru en moi et de m'avoir soutenue tout au long de mes études.

Table des matières

Table des figures

Liste des tableaux

Chapitre 1

Introduction générale

Sommaire

1.1 Contexte général

Au cours des dernières années, les progrès réalisés dans les technologies des communications sans fil ont donné lieu à une variété de nouveaux domaines de recherche. Leurs objectif consiste à étendre la connectivité aux environnements où des solutions câblées ne sont pas toujours possibles. Dans cette perspective, les réseaux véhiculaires (VANET : *Vehicular Ad hoc NETworks*) sont l'un des domaines de recherche pertinent. Les chercheurs se sont investis dans ce domaine et les résultats sont repris aujourd'hui par des entreprises automobiles et les autorités publiques, qui ont pris l'engagement de rendre la conduite routière plus sûre et plus efficace. En effet, les applications des VANET ne se limitent pas seulement à la sécurité routière, mais englobent aussi bien l'optimisation du trafic automobile comme le contrôle de la congestion des flux, les applications de divertissement comme par exemple l'information d'événements d'une ville ou encore les places de stationnement possibles.

Les réseaux véhiculaires sont considérés comme une variante des réseaux mobiles ad hoc (MANET : *Mobile Ad hoc NETwork*). En effet, les véhicules équipés d'interfaces radio sans fil

peuvent communiquer avec leurs voisins directs à condition que ces derniers soient à portée de leurs transmissions radio. En outre, deux nœuds éloignés l'un de l'autre peuvent s'appuyer sur des nœuds intermédiaires pour acheminer les messages ou peuvent utiliser un ensemble d'unités stationnaires. Dans le cadre des VANET, ces infrastructures sont appelées unités de bord de route (*RSU : Road Side Unit*).

Les VANET partagent plusieurs caractéristiques avec les MANET malgré des différences notables. Les particularités des VANET sont la grande mobilité, l'évolution rapide de la topologie du réseau et la volatilité des liens de communication causée par l'instabilité du canal de transmission. Le principal challenge pour le domaine des VANET est de concevoir des protocoles de routage pour contrôler le processus de transfert des paquets au travers des nœuds du réseau compte tenu de la volatilité des liens de communications. Construire un protocole de routage robuste est considéré comme une problématique cruciale pour les VANET.

De nombreux protocoles de routage dédiés aux MANET ont été modifiés afin d'être adaptés à l'échange d'information dans le cadre des VANET. L'une des techniques consiste à détecter la rupture de lien avant que celle-ci ne se produise. En couplant des protocoles de routage avec des métriques de détection de rupture de lien (*MDRL*), ces protocoles sont capables de détecter ces ruptures avant qu'elles ne se produisent et de rechercher des routes alternatives afin de pallier cette défaillance tout en exploitant le lien de communication avant la rupture effective. Malgré leurs diversité, les *MDRL* existantes ne sont pas toujours capables d'identifier l'état d'un lien (c.-à-d. les ruptures des liens) dans le cas d'une communication véhiculaire. Une *MDRL* pour les VANET doit prendre en considération de nombreux paramètres tels que la puissance de signal reçu (RSSI) ainsi que tous les aspects caractérisant la communication : l'état du canal de propagation et la mobilité des nœuds. Elle doit également être capable de prédire les ruptures de lien avant la perte d'un paquet au niveau de la couche application et informer le protocole de routage d'une rupture imminente.

Dans cette thèse, la thématique de ***"l'optimisation de routage dans les VANET par la prédiction de la rupture d'un lien"*** est abordée. L'objectif principal de cette thèse est de développer un indicateur de rupture de lien capable de détecter une rupture entre deux véhicules qui communiquent et d'informer la couche de routage afin qu'une route alternative soit préparée avant la rupture effective du lien. Le but final est donc d'améliorer le routage dans les réseaux véhiculaires.

1.2 Contribution

Ce travail de thèse a pour objectif de répondre et résoudre la problématique de routage dans les VANET. Les contributions principales peuvent être résumées par les deux points suivants.

Développement d'un indicateur de rupture de lien pour les VANET Le processus de détection de rupture de lien peut être réalisé à différents niveaux. Dans l'étude présentée ici, le processus de détection est effectué au niveau de la couche physique. Les informations fournies par celle-ci lors de la réception des paquets sont utilisées pour développer un nouvel indicateur. Ces informations sont issues du processus de décodage OFDM (*Orthogonal Frequency Division Multiplexing*). L'intérêt d'utiliser le processus de décodage OFDM est qu'il produit des informations utiles pour la détection de rupture de lien, notamment des erreurs de décodage spécifiques lorsque le lien se dégrade. Ces erreurs de décodage ont été exploitées dans le cadre de la détection des ruptures des liens. Le premier travail consiste à étudier et analyser le comportement de ces erreurs au fur et à mesure de la communication et selon plusieurs scénarios. Suite à cette analyse, un modèle mathématique de détection de rupture de lien basé sur la théorie des fonctions de croyance est proposé. Cet indicateur appelé LBFI pour *Link Breakage Forecasting Indicator* fournit une meilleure détection de rupture de lien par rapport aux indicateurs existants.

Amélioration du protocole de routage AODV Dans la deuxième partie de cette thèse, l'indicateur de rupture de lien LBFI est intégré au protocole de routage AODV. Le mécanisme de détection traditionnel de AODV est remplacé par l'indicateur de rupture de lien LBFI. Cet indicateur est capable de détecter une rupture et d'informer AODV afin d'opérer le processus de maintenance de route au travers d'une recherche d'une route alternative tout en optimisant l'utilisation du lien actuel. Le nouveau protocole AODV-LBFI améliore le taux de réception de paquets, minimise les délais de bout en bout et augmente la stabilité des routes.

1.3 Organisation de manuscrit

Les grandes lignes de ce manuscrit sont décrites ci-dessous.

Chapitre 2 Ce chapitre présente une vue d'ensemble des VANET. Il décrit les architectures de communications et les caractéristiques des VANET. En outre, il illustre les différentes applications VANET, les normes et les standards. Il présente également une classification des protocoles de routage et les problématiques de recherche dans ce domaine.

Chapitre 3 Ce chapitre décrit tout d'abord les différents effets de perturbation du canal de propagation dans les VANET ainsi que les différents modèles disponibles. Par la suite, il présente un état de l'art sur les indicateurs prédictifs de rupture de lien. Enfin, ce chapitre met le point sur le processus de décodage des trames OFDM et qui sert à développer l'indicateur LBFI.

Chapitre 4 Le quatrième chapitre est consacré à la présentation de l'outil mathématique utilisé pour construire l'indicateur de rupture de lien. Les principes de base de la théorie des fonctions de croyance ainsi que ses fonctionnalités utilisées dans la solution proposée sont détaillés dans ce chapitre.

Chapitre 5 Le cinquième chapitre est consacré à la présentation de la première contribution. Dans ce chapitre, l'indicateur prédictif de rupture de lien, appelé LBFI (*Link Breakage Forecasting Indicator*), basé sur la théorie des fonctions de croyance, est décrit en détail. Cet indicateur a fait l'objet d'une publication dans la revue internationale "Wireless Networks" [4].

Chapitre 6 Le sixième chapitre est consacré à la présentation de la deuxième contribution. Dans ce chapitre, le détail de l'implémentation de l'indicateur prédictif de rupture de lien (LBFI) dans le protocole de routage AODV est présenté ainsi que les résultats obtenus. Cette contribution a fait l'objet d'un papier de conférence dans la conférence "IEEE Global Communications Conference, 2019".

Conclusion Enfin, une conclusion générale et des perspectives de recherche sont proposées.

Chapitre 2

Les réseaux véhiculaires (VANET)

Sommaire

2.1 Introduction

L'idée du développement d'un système de transport intelligent a passionné les chercheurs depuis longtemps [5, 6]. Au cours des dernières années, ce domaine a connu des progrès considérables (apparition des applications de sécurité routière, applications de confort, etc.). Plusieurs facteurs ont conduit à ce progrès, notamment l'adoption de la technologie IEEE 802.11p. Les réseaux véhiculaires ou Vehicular Ad hoc NETwork (VANET) désignent un réseau qui relie les véhicules mobiles entre eux et les véhicules et unités de bord de route (*RSU - Road Side Unit*). Les VANET visent principalement à fournir des informations relatives à la sécurité et à la gestion du trafic. Un autre type d'application fourni des services de divertissement visant à améliorer le confort des usagers.

Dans ce chapitre, l'ensemble des notions nécessaires pour comprendre le contexte de cette thèse sont présentées. Une présentation générale des réseaux véhiculaires est fournie. D'abords, les caractéristiques, les domaines d'application et les architectures de communication pour les réseaux véhiculaires sont détaillés. Les normes et les standards sont abordés ensuite. Enfin, les problématiques et les divers axes de recherche ainsi que les mécanismes de routage VANET sont décrits.

2.2 Les réseaux véhiculaires

Les évolutions récentes dans le domaine des communications et réseaux sans fil ont donné naissance à un nouveau type de réseau mobile connu sous le nom de VANET, et qui vise à améliorer la sécurité et l'efficacité routière. Les VANET, qui sont constitués de nœuds mobiles (véhicules), peuvent être considérés comme un cas particulier des MANET (*Mobile Ad hoc NETworks*). Ils se caractérisent tous les deux par le mouvement et l'auto-organisation des nœuds, mais ils diffèrent également par certains points, comme les composants de l'infrastructure réseau et la topologie très dynamique.

Un VANET utilise le support sans fil pour assurer la communication entre les véhicules en mouvement. Le déplacement des nœuds dans un VANET est relié à des contraintes de structure des routes. Ils se caractérisent également par une grande puissance de calcul et d'énergie et possèdent plusieurs architectures de réseau. Dans ce qui suit, nous détaillons leurs caractéristiques, architectures de communication ainsi que les activités de recherche et de normalisation dans ce

domaine.

2.3 Caractéristiques des réseaux véhiculaires

La conception des protocoles véhiculaires ainsi que les applications dédiées aux VANET nécessitent la prise en considération de plusieurs contraintes liées à la nature de ce type de réseaux. Les protocoles conçus pour les MANET ne peuvent pas être utilisés directement dans les VANET. En effet, les MANET sont basés sur des caractéristiques de faible mobilité, des mouvements aléatoires des nœuds et un changement lent dans la topologie de réseau [7]. Nous présentons ci-dessous les principales caractéristiques qui doivent être considérées pour la mise en œuvre des protocoles efficaces pour les réseaux VANET [8] :

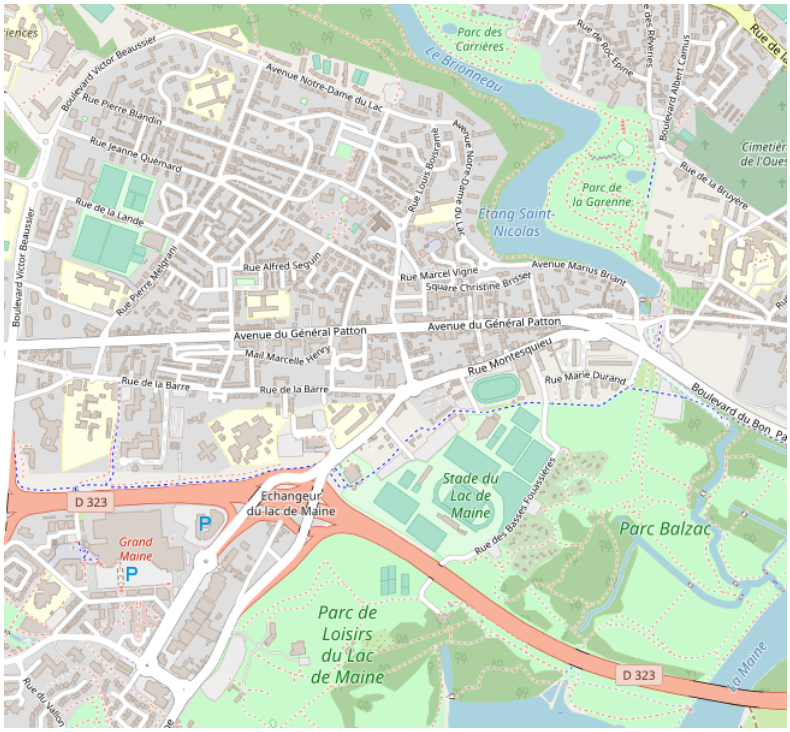


FIGURE 2.1 – Exemple de réseau routier

La mobilité Comme illustré dans la figure 2.1, la topologie des VANET est dynamique mais n'est pas aléatoire. Le mouvement des véhicules est restreint par un ensemble de contraintes de structure des routes (comme : les intersections, les autoroutes, les directions possibles, le nombre de voies, etc) et des contraintes imposées par les infrastructures routières (comme : les feux

de signalisation et les limites de vitesse). L'environnement VANET peut être urbain, rural ou autoroutier, ce qui impacte la transmission des signaux dans le canal sans fil.

La connectivité La volatilité des liens entre des véhicules est le résultat de la topologie dynamique du réseau. Les liens de communication entre les nœuds sont fréquemment perturbés, deux nœuds échangeant des données peuvent se déconnecter à tout moment.

La consommation d'énergie Contrairement aux MANET, la limite des ressources énergétiques et de calcul n'est pas imposée directement dans le cadre des VANET. En effet, les batteries et les alternateurs permettent d'avoir une capacité énergétique nécessaire pour supporter des applications nécessitant des calculs importants.

Support de l'infrastructure À la différence des MANET, les VANET peuvent profiter d'une infrastructure. Grâce aux unités de bord de la route, les véhicules peuvent étendre leur connectivité en profitant des liens entre les infrastructures.

2.4 Architectures de communication

Les communications dans les VANET peuvent être représentées par trois architectures : (i) la communication véhicule-véhicule ou ad hoc (V2V), et qui permet au véhicule de communiquer avec d'autres véhicules directement, (ii) la communication véhicule-infrastructure (V2I), et qui permet l'échange d'informations entre les véhicules et les unités de bord de la route, (iii) une architecture hybride, et qui englobe les deux architectures de communication V2V et V2I.

2.4.1 Architecture Véhicule-à-Véhicule (V2V)

Une architecture décentralisée (Fig 2.2) permet la communication directe entre les véhicules sans avoir besoin de soutien d'infrastructures fixes, et peut être utilisée principalement pour des applications de sécurité et de diffusion. La communication peut être unicast, multicast (par exemple dans le cas d'un cluster de véhicules échangeant des informations routières) ou même broadcast (dans le cas d'avertissements d'accident). La communication V2V est un véritable challenge, la connectivité entre les véhicules n'est pas permanente, étant donné que les véhicules se déplacent à des vitesses différentes, ce qui peut entraîner des modifications rapides de la topologie du réseau.

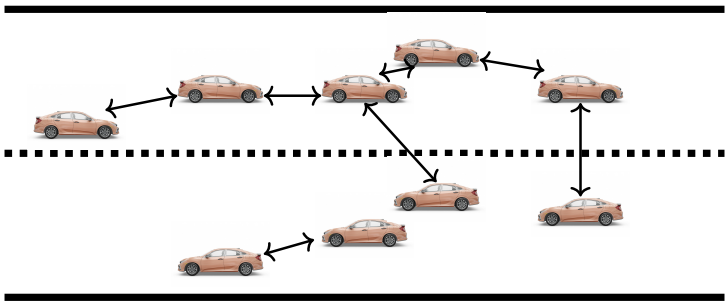


FIGURE 2.2 – Architecture V2V

2.4.2 Architecture Véhicule-Infrastructure (V2I)

Une architecture centralisée (Fig 2.3) permet la communication entre les véhicules et les infrastructures routières (RSU), principalement dans le cadre de la collecte d'informations et de données. Les infrastructures routières peuvent collecter des données et avertir les véhicules en temps réel de l'état des routes, des embouteillages, des accidents, des zones de construction et de la disponibilité des places du stationnement, etc.

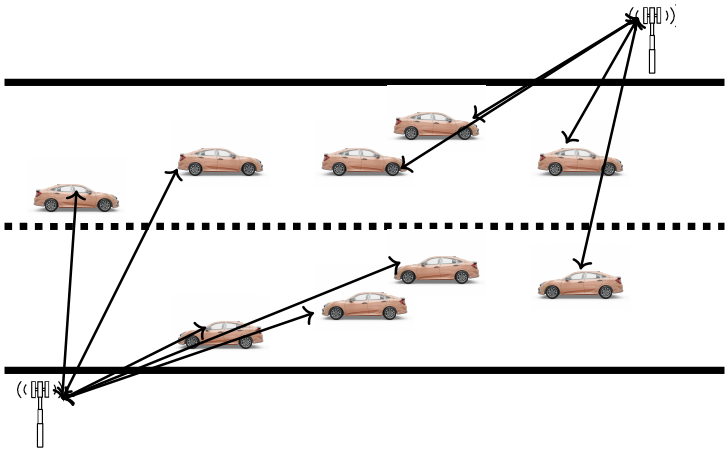


FIGURE 2.3 – Architecture V2I

2.4.3 Architecture hybride

Cette architecture (Fig.2.4) mélange à la fois l'architecture V2V et l'architecture V2I. Ainsi, selon la distance, un véhicule est capable de communiquer avec l'infrastructure routière, que ce soit par un ou plusieurs sauts. Les véhicules communiquent entre eux selon une architecture

V2V lorsqu'ils se trouvent à proximité l'un de l'autre, et échangent essentiellement leurs observations du trafic ou transmettent des messages multi-hop, ou encore des données provenant éventuellement de zones plus larges, transmises précédemment par RSU.

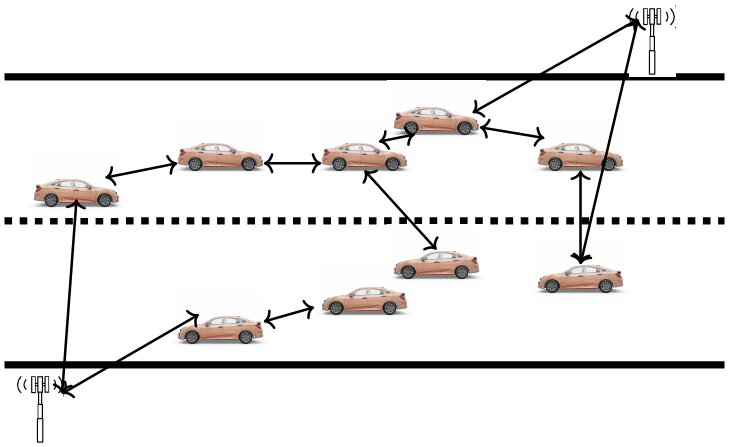


FIGURE 2.4 – Architecture hybride

2.5 Domaines d'application

La réduction des risques d'accidents de la route et l'amélioration de la sécurité et l'efficacité du trafic sont les objectifs premiers des applications VANET. Aujourd'hui, les VANET possèdent une large gamme d'applications qui peuvent être divisées en trois catégories selon [9, 10] : (i) applications de sécurité routière (ii) applications de gestion de trafic, (iii) applications d'information et de divertissement. Dans cette section, les diverses applications supportées par les VANET sont abordées, les détails de chaque application et ses contraintes sont décrits.

2.5.1 Applications de sécurité routière

Les applications de sécurité routière agissent de manière préventive en avertissant les conducteurs à l'avance des risques potentiels [11, 12]. Quelques exemples de ces applications sont présentés ici :

Applications de détection et d'alerte de pré-collision Périodiquement, des données sont échangées entre les véhicules et l'infrastructure afin de prévenir de collisions. Ces données incluent des informations détaillées concernant la localisation, la vitesse et même l'état du conducteur afin de

pouvoir éviter ou diminuer la gravité d'un accident [13]. Ces systèmes permettent de compléter les systèmes d'aide à la conduite des véhicules qui ne tiennent compte que de l'environnement immédiat du véhicule.

Applications d'alerte en cas d'urgence Un véhicule d'urgence, une ambulance par exemple, annonce sa présence sur la route aux autres véhicules de son voisinage afin de libérer une voie de circulation. La diffusion des messages d'alertes dans le réseau permet aux véhicules de visualiser localement leur environnement en identifiant les véhicules en situation d'urgence.

Applications d'avertissements de collision aux intersections Ces applications visent à détecter les risques de collision pour les véhicules qui approchent d'un carrefour routier ou en cas d'accès à une bretelle [13].

Applications d'alertes Ce type d'application permet de diffuser un événement particulier tel que la perte de contrôle du véhicule ou même un accident aux véhicules alentours, qui pourraient être non visibles du fait d'une obstruction de la vue du conducteur (virage, bâtiments, etc.). À la réception de ces informations, les véhicules aux alentour déterminent la validité de l'événement et avertissent les autres conducteurs afin d'agir de façon appropriées [14].

2.5.2 Applications de gestion du trafic

Les applications de gestion du trafic sont principalement orientées vers l'amélioration et la coordination du trafic, l'assistance routière ainsi que la mise à jour des localisations et cartes, etc. Selon [9], les applications de gestion du trafic peuvent être classées selon deux groupes typiques : la gestion de la vitesse et la navigation coopérative.

La gestion de la vitesse Le but est de réduire les accidents, de rouler à une vitesse appropriée en fonction des conditions de circulation du moment et de maximiser la sécurité. Les applications de gestion de la vitesse sont destinées à aider le conducteur, par un contrôle de la vitesse de son véhicule de manière à assurer une conduite en toute sécurité et à éviter les arrêts inutiles.

La navigation coopérative Cette classe regroupe l'ensemble des applications qui visent à augmenter l'efficacité du trafic, en contrôlant la circulation des véhicules grâce à la collaboration

entre les véhicules et entre ces derniers et les infrastructures en bord de route.

2.5.3 Applications d'information et de divertissement

Ces applications visent à améliorer le confort du conducteur et des passagers. Elles ont pour but de fournir aux usagers du divertissement et des services tels que l'accès internet, le streaming audio et vidéo. Par exemple, des services offerts par des entreprises pourront être entièrement disponibles dans les véhicules grâce à la communication V2I. De plus, le partage et la diffusion vidéo en temps réel peuvent être effectués par la communication V2V. Ce qui rend les longs voyages plus confortables et agréables. En raison des différentes exigences de qualité de service de cette catégorie d'applications en termes de bande passante et de délai, il est extrêmement difficile de garantir des communications fiables et en temps réel pour les applications sensibles au délai sans affecter le débit des applications sensibles.

Le tableau 2.1 résume l'ensemble des caractéristiques de chaque type d'applications des VANET. En effet, les applications de divertissement se caractérisent principalement par des contenus de taille variée tels que : des fichiers images, audio ou vidéos, et qui exigent une bonne qualité de service. Cependant, compte tenu de la topologie extrêmement dynamique des VANET, la qualité de service quant à ces contenus s'avèrent souvent détériorée en raison soit de perte d'informations, soit de délais de transmissions trop importants au regard du contenu. Pour pallier ces problèmes, certains travaux se basent sur les RSU comme solution [15], d'autres proposent des protocoles de routage qui favorisent la qualité de service comme dans le cas du streaming vidéo [16, 17], etc.

Application	**Caractéristiques de contenu**	**Exigence**
Application d'information et de divertissement	Contenu varié (texte, image, audio, vidéo)	Qualité de service
Application de gestion routière	Contenu de petite taille (texte)	Sensible au délai
Application de sécurité routière	Contenu de petite taille (texte)	Très sensible au délai

TABLE 2.1 – Caractéristiques des applications pour les VANET

Les applications de la gestion routière et les applications de sécurité, quant à elles, nécessitent un délais de transmission des données (*End to End Delay - E2ED*) quasiment en temps

réel compte tenu de la criticité des informations. En effet, comme les VANET se caractérisent par leurs vitesse élevée, des contraintes de mobilité et du comportement des conducteurs, la conception de ce type d'applications présente un challenge. Plusieurs problèmes freinent la transmission rapide des messages de sécurité. L'un des problèmes bien connu dans le domaine des réseaux VANET est le problème de la connectivité. Comme les liens de communication ne sont pas stables, des ruptures peuvent arriver à tout moment ce qui entraîne la perte des paquets dans le réseaux et des grands délais de transmission. Dans ce contexte, plusieurs travaux ont été menés pour résoudre ce problème, certains visent à déterminer l'état de lien de communication [3, 18], d'autres proposent des protocoles de dissémination des messages de sécurité [19, 20].

2.6 Normes et standards

Plusieurs standards de communication sans fil ont été élaborés afin de définir une norme de communication qui sera utilisée par les applications VANET. Ils répondent aux exigences d'accès radio requises dans le cadre d'une communication véhicule à véhicule, d'une communication véhicule à infrastructure ou d'une communication infrastructure à infrastructure. Ces standards sont principalement conçus pour assurer l'interopérabilité entre les équipements.

2.6.1 L'architecture ITS

L'architecture ITS est illustrée dans la Figure 2.5. Elle est maintenue et supportée par l'institut européen des normes de télécommunications (ETSI)[21]. Cette architecture définit quatre couches qui sont : la couche *application*, la couche *facilités*, la couche *réseaux et transport* et la couche *technologies d'accès*. Cette architecture possède également deux plans : le plan de gestion et le plan de sécurité. ITS intègre plusieurs technologies de communications : *WIFI*, *ITS-G5* (IEEE 802.11p), *Bluetooth*, *cellulaire* et *WiMax*. L'utilisation de la couche réseau et transport dépend du type d'application. Les applications de confort qui se basent sur une architecture de communication V2I utilisent les protocoles IPv6 et TCP/UDP, dans le cas des communication V2V. ITS définit une nouvelle couche appelée *facilités* [22], son principale rôle est de fournir des fonctionnalités pour l'exécution des applications (support d'application), de fournir des données pour l'exécution des applications (support d'information) et d'offrir des services pour la communication (support de communication).

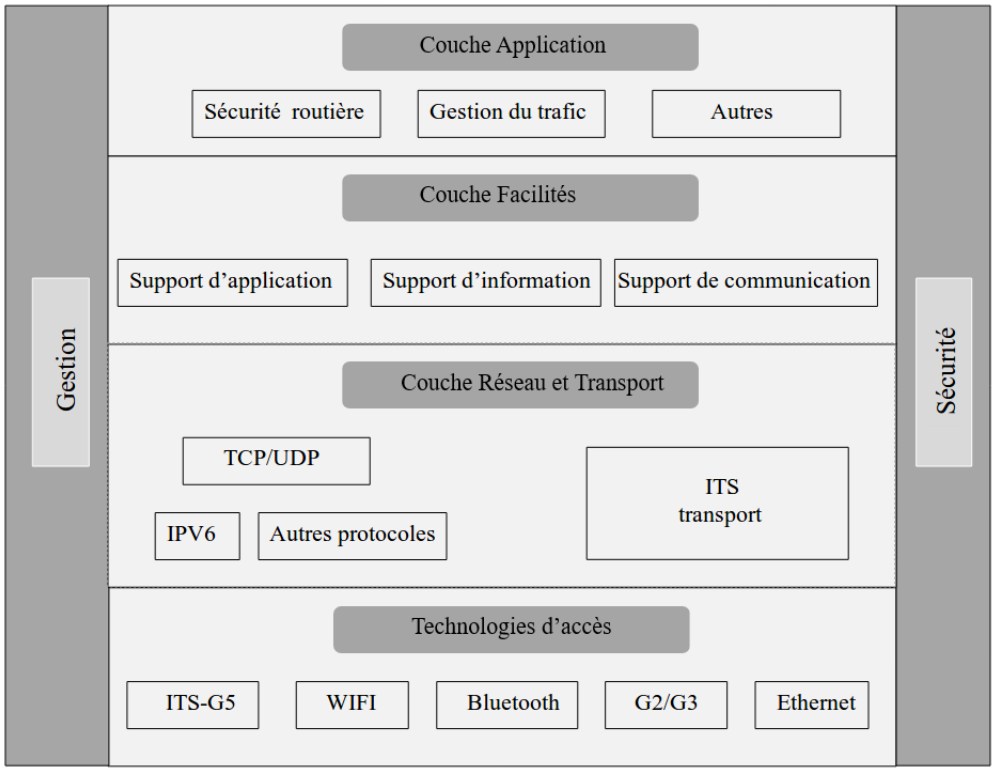


FIGURE 2.5 – Architecture ITS

2.6.2 Communications dédiées à courte portée

Les communications dédiées à courte portée ou *Dedicated Short Range Communication* (DSRC) ont été développées en Europe et au Japon en 2003, principalement pour supporter les communications véhicule à véhicule et véhicule à infrastructure [23]. Il s'agit d'un service de communication à courte portée basé sur la norme IEEE 802.11p, dérivée de la norme IEEE 802.11a [24]. Les fréquences exploitées par le DSRC se répartissent dans la bande de fréquences de 5,9 GHz, et se composent de sept canaux dont chacun a une largeur de bande de 10 MHz (un canal de contrôle et six canaux de service). Les canaux 174 et 176 peuvent être combinés afin de former le canal 175 de 20 Mhz, tel est le cas aussi pour les canaux 180 et 182 qui forment le canal 181. Le canal de contrôle est réservé à la transmission des messages de gestion du réseau et aux messages de très haute priorité tels que les messages liés à la sécurité routière. La transmission des données de service est assurée par les six autres canaux.

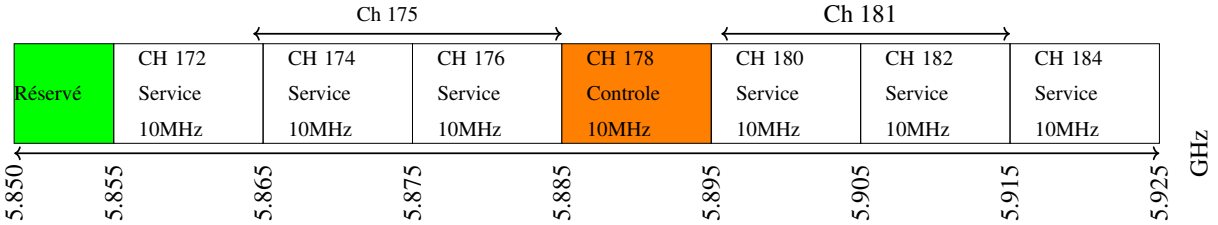


FIGURE 2.6 – Désignation des canaux DSRC

2.6.3 L'architecture WAVE

Le standard WAVE (*Wireless Access Vehicular Environment*) définit une architecture et un ensemble complémentaire standardisé de services et d'interfaces qui facilitent la communication sécurisée en mode V2V et V2I. Combinées, ces normes forment la base de toute une gamme d'applications destinées à l'environnement des transports, y compris des applications de sécurité, de navigation, de gestion du trafic et autres. La Figure 2.7 représente l'architecture WAVE résultant de la combinaison de l'amendement IEEE 802.11p (802.11p est la base de DSRC) et des quatre standards IEEE1609.1, 1609.2, 1609.3 et 1609.4 tels que définis par le groupe de travail WAVE IEEE 1609 pour la spécification des couches supérieures des communications [25].

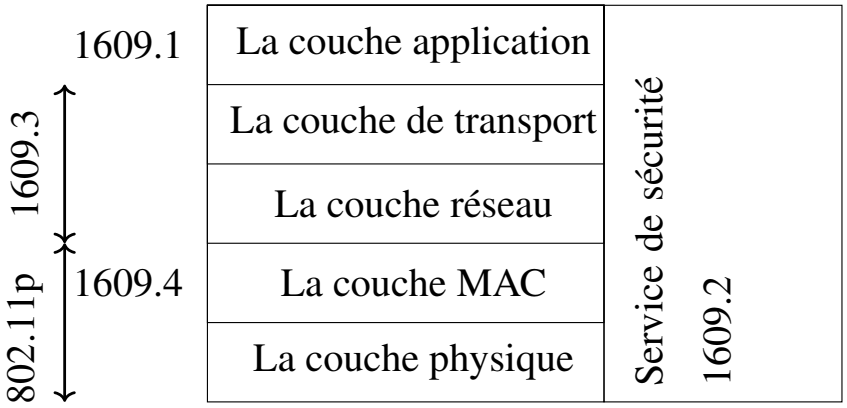


FIGURE 2.7 – Architecture WAVE

— **IEEE1609.1 :** ce standard spécifie les services et interfaces de l'application WAVE. Il précise les formats adéquats de messages de commande et les réponses, ainsi que les formats de stockage des données qui doivent être utilisés par les applications pour communiquer entre les composants de l'architecture,

— **IEEE1609.2 :** ce standard représente les services de sécurité des applications et des messages de gestion. Il décrit le format des paquets de sécurité, le cryptage ainsi que l'authentification, correspondant aux messages de sécurité et de gestion des données,

— **IEEE1609.3 :** cette norme décrit les services de la couche réseau et de la couche transport, y compris l'adressage et le routage,

— **IEEE1609.4 :** ce standard définit tous les mécanismes nécessaires permettant l'accès aux canaux de transmission, la coordination et l'acheminement des données,

— **IEEE Standard 802.11p :** ce standard est un amendement à l'IEEE 802.11 destiné à intégrer l'accès sans fil dans les environnements véhiculaires (WAVE). Il apporte les modifications nécessaires à la norme 802.11 pour supporter les systèmes de transport intelligents (STI). Dans le cadre de la communication à grande vitesse, les échanges de données entre véhicule et véhicule (V2V) et la communication véhicule et unités de bord de la route (V2I) peuvent être réalisés grâce à la bande de fréquence 5,9 GHz. correspondant au IEEE 802.11p. Ce standard s'appuie sur fonctionnement du standard 802.11a au niveau physique et le standard 802.11e au niveau accès canal. Toutefois, il englobe des techniques visant à répondre aux différentes exigences de communication dans un réseau VANET [26]. La communication dans les environnements à forte mobilité selon le standard IEEE 802.11p ne nécessite pas l'authentification de l'accès avant la transmission de données.

2.7 Les problématiques dans les VANET

Les VANET sont progressivement intégrés dans la vie quotidienne et contribuent à promouvoir les systèmes de transport intelligent (*ITS - Intelligent Transport System*) ainsi que le concept de ville intelligente (*Smart-City*). Il est donc indispensable avant tout de définir les principaux en-

jeux qu'il faut impérativement résoudre. Dans la suite, un résumé des principales problématiques des VANET est présenté, en se focalisant en particulier sur l'aspect routage.

Sécurité Garantir la sécurité des informations échangées dans les VANET est un aspect très important. Des informations erronées peuvent être acheminées dans le réseaux. En effet, la communication sans fil est très vulnérable du fait que les attaques peuvent être menées sans nécessiter des accès physiques à l'infrastructure réseau. Il est donc essentiel de concevoir des VANET aussi robustes que possible et de les protéger contre les attaques réseaux.

Limitation de bande passante La plage de fréquences réservée au VANET est limitée. Seulement 75 MHz (de 5,850 à 5,925 GHz) sont alloués au DSRC, ainsi la congestion des canaux peut se produire facilement dans les environnements à haute densité. Il est donc nécessaire d'optimiser efficacement l'utilisation de la bande passante.

La connectivité et le routage La mobilité élevée des véhicules, l'état du canal de transmission ainsi que la topologie qui évolue rapidement provoquent des ruptures fréquentes [27][3]. Afin d'éviter la perte des paquets échangés, il est nécessaire de trouver un moyen pour étendre la connexion entre les véhicules ou détecter les ruptures des liens avant leurs arrivées. De ce fait, la conception des protocoles de routage pour les VANET est une tâche difficile. Un protocole de routage VANET doit réussir à acheminer tous les paquets tout en respectant certains délais [28], notamment dans le cadre de la sécurité routière. Il doit donc être capable de prévoir les ruptures des liens et de réagir avant la perte des paquets.

Dans cette thèse, la problématique de connectivité et de routage est au centre de nos préoccupations. Vu que l'échange de données est l'objectif principal de tout réseau, il est donc important de trouver des moyens efficaces pour effectuer cet échange.

Les protocoles de routage sont conçus afin d'acheminer tous les types d'information et sont considérés comme capables de s'adapter à toute situation. Cependant dans le cas des VANET, les protocoles de routages existants sont inadaptables à cause de ces caractéristiques, et plus précisément de la forte mobilité des nœuds ainsi que les phénomènes de propagation. Ci-dessous, un état de l'art sur les protocoles de routage VANET est présenté.

2.7.1 Protocoles de routage dans les VANET

Les VANET permettent la création de réseaux auto-organisés entre des véhicules en fonction de leurs besoins. Afin d'établir une communication réussie, un chemin doit être initié entre l'émetteur et le destinataire pour acheminer les paquets. Cette opération nécessite des protocoles de routage efficaces.

Un protocole de routage définit le paradigme de communication entre deux nœuds. Il détermine la manière d'établir une route, assure le routage des paquets et la maintenance des routes. De nombreux protocoles de routage existent pour les VANET, et peuvent être classés selon deux grandes familles (Figure 2.8) :

— les protocoles topologiques : le routage des paquets s'effectue en se basant sur les connaissances disponibles sur les liens qui relient les nœuds du réseaux,

— les protocoles géographiques : ils utilisent les informations de localisation (GPS, Galiléo) des nœuds pour acheminer les paquets.

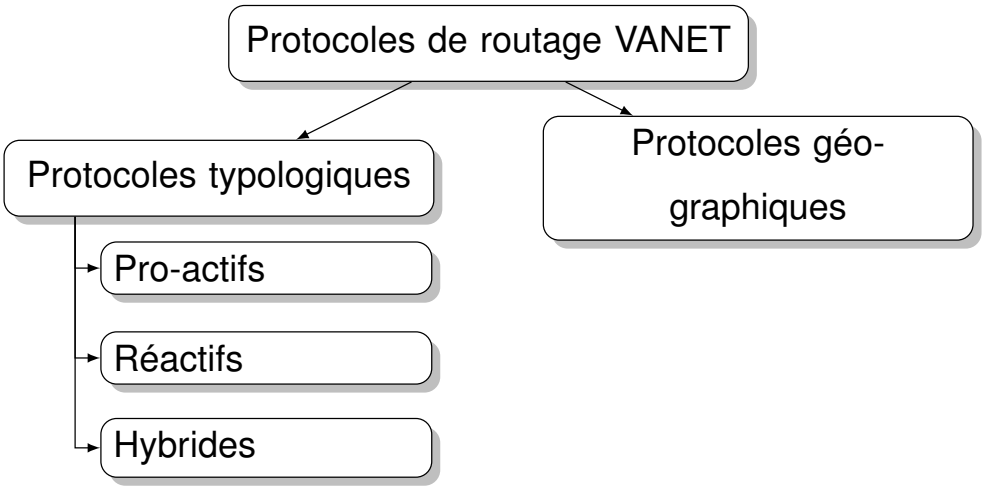


FIGURE 2.8 – Classification des protocoles de routage VANET

2.7.1.1 Les protocoles topologiques

Considérés comme des protocoles de routages conventionnels, cette famille de protocole utilise les informations disponibles sur les liens pour acheminer les paquets. En fonction de la stratégie de routage utilisée, l'ensemble des protocoles appartenant à cette famille peuvent être classés selon trois catégories (Figure 2.8) : pro-actif, réactif et hybride.

Les protocoles pro-actifs Un protocole pro-actif est un protocole piloté par des tables de routage où il enregistre les informations sur la topologie du réseau et les informations concernant le routage. Le principal avantage de cette approche de routage réside dans l'absence de découverte de route puisque tous les chemins possibles reliant les nœuds du réseau entre eux sont enregistrés dans les tables de routage. Pour réagir aux changements dans la topologie du réseau et tenir à jour les informations de routage, chaque nœud propage périodiquement des mises à jour de routage à ses voisins. La méthode de collecte et de gestion des informations de routage ainsi que le type de données contenues dans ces tables forment la différence essentielle entre les différents protocoles pro-actifs. La nécessité de mettre à jour constamment les tables de routage de chacun des nœuds dans le réseau demeure un des problèmes des protocoles de routage pro-actifs. Leurs performances dans les réseaux à topologie dynamique comme les VANET se retrouvent réduites [29, 30]. Il existe plusieurs protocoles pro-actifs, quelques exemples de ces protocoles sont :

— *OLSR (Optimised Link State Routing)[31]* : c'est l'un des protocoles de routage ad hoc proactifs les plus importants. OLSR introduit le concept de relais multipoints (MPR). L'utilisation des MPR minimise l'inondation des messages de contrôle. OLSR utilise trois types de messages : (i) Messages de contrôle de topologie (TC) ; (ii) Messages de contrôle HELLO ; (iii) Messages de déclaration à interfaces multiples (MID),

— *DSDV (Destination Sequenced Distance Vector)[32]* : Dans DSDV, chaque nœud cherche à maintenir une table de routage pour pouvoir atteindre tout autre nœud. La table de routage contient des informations telles que : la liste des destinations possibles, le nombre de sauts pour atteindre chacune des destinations et le numéro de séquence de chaque destination. Pour maintenir la cohérence de la table de routage dans une topologie qui change rapidement, chaque nœud du réseau transmet périodiquement les derniers changements de sa table de routage à ses voisins.

Les protocoles réactifs Le routage réactif est un routage à la demande dans lequel les routes ne sont pas mises à jour en fonction de l'évolution de la topologie du réseau. À la différence des protocoles de routage pro-actifs, la découverte des routes est initiée uniquement lorsqu'un nœud source souhaite communiquer ou envoyer des données à un autre nœud de la destination.

Le routage réactif vise à réduire la charge sur le réseau puisque seules les routes utilisées doivent être maintenues. L'inconvénient de ce type de routage est le temps nécessaire pour établir une route. Les fonctions essentielles d'un algorithme de routage à la demande sont la découverte et la maintenance des routes une fois établies. Plusieurs protocoles de ce type ont été proposés. Les protocoles de routage réactifs les plus répandus sont :

— *AODV (On Demand Distance Vector)[33]* : le protocole réactif le plus exploité. Lorsqu'une source S souhaite établir une route, un paquet de demande de route (RREQ) est envoyé au réseau pour construire un chemin/une route vers une destination, D. Un paquet RREP (Route Reply) est alors renvoyé par D à S, lorsque D reçoit le RREQ. Si la demande de route traverse des chemins bidirectionnels, le RREP est envoyé en utilisant l'inversion du chemin.

— *DSR (Dynamic Source Routing)[34]* : est un protocole réactif, tout comme AODV, les routes ne sont créées que lorsqu'elles sont nécessaires. L'entête des paquets de DSR contient l'adresse de tous les nœuds intermédiaires ainsi que l'adresse de la destination. En effet, grâce au chemin complet présent dans l'entête de chaque paquet, il est possible d'identifier où se situent les ruptures de route.

La force principale des protocoles réactifs réside dans le fait qu'ils nécessitent moins de paquets de contrôle que les protocoles pro-actifs, mais il faut tenir compte du temps d'établissement de la route lorsqu'il n'existe pas de route, ou lorsqu'une route est interrompue suite à des ruptures de lien [29].

les protocoles hybrides Les protocoles de routage hybrides regroupent des protocoles qui combinent le routage réactif et le routage pro-actif. Ainsi, ils bénéficient des avantages de ces deux types protocoles. Les nœuds proches collaborent entre eux afin de diminuer les coûts de découverte des routes en maintenant de façon pro-active les routes vers les nœuds à proximité et en recourant à une stratégie réactive pour déterminer les routes vers les nœuds éloignés. Un exemple des protocoles de routage hybrides classiques est le protocole *ZRP* :

— *ZRP (Zone Routing Protocol)[35]* : est un protocole de routage hybride. ZRP définit au-

tour de chaque nœud une zone qui contient les nœuds voisins. Des algorithmes de routage pro-actifs et réactifs sont utilisés par les nœuds pour transférer les paquets, respectivement, dans et en dehors de leurs zones. C'est un routage par zone. Un système pro-actif est utilisé dans la zone déterminée pour chaque nœud. Une approche de routage réactif est utilisée pour les nœuds situés au-delà de cette zone. Ce routage vise à combiner les avantages des deux familles de routage (réactif et pro-actif). Cependant, le ZRP n'est pas assez efficace dans le cas d'un environnement urbain et d'une forte mobilité de nœuds tel que les VANET [36].

2.7.1.2 Les protocoles géographiques

Cette famille de protocole utilise les informations sur la position des nœuds pour effectuer le routage. Une zone cible contenant la destination est déterminée par le biais d'un système de géolocalisation (GPS, Galiléo par exemple). Le fonctionnement des protocoles de routage géographiques peut être divisé en deux étapes. Lors de la première étape, le paquet est retransmis sur un chemin de routage construit à l'intérieur d'une zone spécifiée, appelée "Zone de transfert". Dans la deuxième étape, le paquet est diffusé vers les nœuds de la région cible (région de géo-diffusion). Tout comme d'autres familles de protocoles, la découverte de routes dans les protocoles géographiques peut être réactive ou pro-active. Un exemple de protocole de routage géographiques est :

— *GPSR (The Greedy Perimeter Stateless Routing)[37]* : Il s'agit d'un protocole de routage unicast qui utilise une stratégie de transmission basée sur la position pour envoyer des messages vers une destination connue. Dans GPSR, chaque nœud achemine son paquet à son voisin immédiat qui est géographiquement le plus proche du nœud de destination. La transmission peut échouer s'il n'y a pas de nœuds dans la direction de la destination.

Le choix de la famille de protocoles la plus adaptée aux VANET est une problématique courante. Plusieurs recherches ont été menées afin de résoudre ce problème. Des comparaisons entre les diverses familles de protocole ont été effectuées [38, 39, 40]. Certaines études [40] ne prennent pas en compte un environnement de simulation réaliste (les obstacles ne sont pas pris en compte dans l'environnement de propagation des ondes) ce qui peut donner des résultats erronés

(optimistes). Dans [41], une étude réaliste des différents protocoles de routage est effectuée. Elle souligne que la catégorie des protocoles de routage réactifs est la plus adaptée aux réseaux VANET. Les auteurs montrent également que parmi les protocoles de cette famille, AODV présente les meilleurs résultats, spécialement en terme de taux de paquets reçus.

Bien que le protocole AODV possède de meilleures performances par rapport aux autres protocoles de routage, ces performances restent modestes [30]. Les auteurs montrent également que les défaillances des routes causées par les ruptures des liens sont la principale cause de dégradation des performances du routage AODV dans les VANETS. En effet, à cause du déplacement des véhicules et de la présence des obstacles, les liens entre les nœuds sont instables. Il est donc nécessaire qu'un protocole de routage puisse s'adapter et réagir lorsque les ruptures des liens se produisent. Plusieurs optimisations du protocole AODV ont été proposées. Chacune vise à améliorer le taux de réception de paquets. Les auteurs de [42] utilisent un indicateur de rupture de lien basé sur la puissance de réception pour fournir une extension du protocole de routage AODV permettant la maintenance préventive des routes. Une autre version du protocole AODV appelée *PPAODV* (*Préventive Prédictive AODV*) utilise l'indicateur de rupture de lien présenté dans [43]. L'intensité du signal reçu est approchée à l'aide d'une interpolation de Lagrange afin de détecter la rupture des liens avant qu'elle ne se produise. PPAODV recherche de nouveaux itinéraires avant que l'actuel ne tombe en panne grâce au message d'erreur envoyé avant la rupture. Les auteurs de [44] proposent un AODV préventif (PrAODV) qui est basé sur deux mécanismes de prévention. Le premier consiste à planifier une redécouverte de route à l'avance, le second consiste à prévenir à l'avance la source du risque de rupture. Le processus d'échange de messages HELLO appelé le Ping-Pong est utilisé pour informer la source lorsqu'un lien est rompu. La réception d'un paquet dont l'intensité du signal est inférieure à un seuil prédéfini entraîne l'envoi d'un message Ping vers le nœud voisin. Ce nœud voisin répond ensuite par un message Pong dans un délai spécifié. Si la période spécifiée s'est écoulée sans réception d'une réponse, un message d'alerte sera transmis à la source. Quand la source reçoit un message d'alerte, elle déclenche un processus de découvert de route.

Le principal problème de ces versions du protocole AODV est qu'elles se basent sur des indicateurs de rupture de lien incapables de donner une détection adéquate de rupture de lien dans un milieu VANET. En effet, ces solutions utilisent les paquets correctement reçus au niveau de la couche MAC pour détecter les ruptures. Leurs réactivités diminuent lorsque le lien se dégrade

[45]. Un autre type d'indicateur de rupture de lien utilise le processus de décodage de paquets au niveau de la couche physique pour déterminer l'état du lien [3, 46]. Les paquets reçus ainsi que les paquets rejetés en raison d'erreurs de décodage sont pris en compte dans l'algorithme de détection. Les résultats de ces travaux montrent une grande réactivité par rapport à d'autres techniques. Cependant, ils souffrent de quelques problèmes qui seront détaillés dans le chapitre 5.

Dans cette thèse, la détection de rupture de lien est au centre de notre préoccupation. Un indicateur prédictif de rupture de lien basé sur les décodage des paquets au niveau physique est proposé pour l'anticipation des ruptures dans les VANET (chapitre 5). Ensuite, l'indicateur est implémenté dans le protocole AODV. Le mécanisme de prédiction de rupture de lien utilisé par AODV est étudié et analysé et le nouveau mécanisme de détection de rupture basé sur le décodage des paquets au niveau physique est proposé et implémenté dans AODV. Le protocole AODV est décrit en détail dans le chapitre 6.

2.8 Conclusion

Ce chapitre a introduit les réseaux véhiculaires (VANET). Le contexte général et les connaissances nécessaires pour comprendre le cadre de cette thèse ont été présentés. Les caractéristiques et les applications pratiques des réseaux VANET ainsi que les architectures de communication et les standards conçus pour les VANET ont été détaillés. Ensuite, les défis et les problèmes existants des réseaux VANET ont été abordés.

Ce travail de thèse porte sur l'optimisation du routage dans les réseaux véhiculaires en prenant en compte la prédiction de rupture d'un lien. Pour ce faire, le prochain chapitre est dédié à l'introduction de la problématique rupture de lien dans les VANET et les différentes approches utilisées dans le processus de détection de rupture des liens.

Chapitre 3

Rupture de lien dans les VANET

Sommaire

3.1 Introduction

Le caractère extrêmement dynamique des réseaux véhiculaires provoque l'instabilité de la connectivité des liens entre les nœuds. Des ruptures de lien peuvent se produire à tout moment

et causer la perte des paquets. Dans de telles situations, pour rester efficaces les protocoles de routage qui ont pour objectif d'assurer une connectivité optimale sans perte de paquets doivent se doter de mécanismes permettant la détection des ruptures des liens, qui devraient être capables de prédire les changements soudains qui pourraient survenir sur un lien de communication et d'informer le protocole de ces changements.

Ce chapitre est divisé en trois grandes parties. Dans la première partie les principales contraintes de propagation des ondes qui peuvent influencer la communication au sein des réseaux VANET sont présentées. Dans la deuxième partie, un état de l'art sur les techniques de détection de rupture de lien est introduit. Cette thèse est restreinte aux travaux de détection de rupture de lien. Pour cela, l'état de l'art se concentre sur les approches existantes dans la littérature qui visent à anticiper la défaillance des liens. Dans la troisième partie, les aspects techniques du décodage des paquets OFDM sont présenté. ils sont la base de notre contribution.

3.2 Effets de perturbation de canal de transmission et modélisation

La propagation des ondes radio dans les réseaux sans fil est affectée par un certain nombre de phénomènes physiques comme l'atténuation du signal en fonction de la distance (*pathloss*), l'effet de masquage (*shadowing*) et l'évanouissement (*fading*). Ces effets perturbent le canal de propagation et provoquent des variations de la puissance du signal. De nombreux travaux ont étudié l'impact de la modélisation réaliste du canal sur la transmission des données dans les environnements sans fil [47, 48, 49]. Ils montrent que l'intensité des perturbations sur le canal de transmission a une grande influence sur la connectivité ce qui impacte largement le routage. Ainsi, l'élaboration d'un modèle de propagation radio précis doit refléter de manière adéquate les effets de perturbation du canal [50]. Dans la suite, chaque effet est défini et des exemples de modélisations sont présentés.

3.2.1 Atténuation du signal en fonction de la distance (Path loss)

Le *Path loss* correspond à l'atténuation de la puissance des ondes électromagnétiques en fonction de la distance entre l'émetteur et le récepteur. Plusieurs modèles représentant l'effet de *PathLoss* existent dans la littérature. Deux modèles sont décrits ici : *Free space* et *Two Ray*

Ground.

-Free space Le modèle de propagation en espace libre repose sur l'hypothèse qu'une antenne d'émission et une antenne de réception sont localisées dans un milieu sans obstacle (*Line of Sight*) ni absorbants ni réfléchissants. En particulier, toute influence d'obstacles est totalement absente. L'équation de Friis (3.1) calcule la puissance du signal reçu en espace libre à une distance R de l'émetteur.

$$\frac{P_r}{P_t} = G_r G_t \left(\frac{\lambda}{4\pi R}\right)^2. \tag{3.1}$$

où :

- λ représente la longueur d'onde du signal.
- R est la distance parcourue.
- G_t et G_R sont les gains des antennes émettrices et réceptrices.

-Two Ray Ground Le modèle *Free space* considère seulement l'affaiblissement de signal lié à la distance entre l'émetteur et le récepteur. Le modèle *Two Ray Ground* incorpore l'effet de réflexion sur le sol. La surface du sol est caractérisée par un coefficient de réflexion R qui dépend des propriétés du matériau de la surface et du type de polarisation des ondes. Les antennes d'émission et de réception sont respectivement de hauteur h_t et h_r et sont séparées par la distance de d mètres. La puissance de signal reçue est alors définit par la formule 3.2.

$$P_r(d) = \left(\frac{P_t G_t G_r h_t^2 h_r^2}{d^4 L}\right). \tag{3.2}$$

3.2.2 Effet de masquage (Shadowing)

Le *Shadowing* ou l'effet de masquage représente l'effet des obstacles sur l'atténuation du signal. La modélisation du *Shadowing* s'effectue souvent suivant une distribution log-normale. Un modèle représentant le *Shadowing* est le modèle *Log distance path loss* qui est présenté ci dessous.

-Log distance path loss Ce modèle est utilisé pour prédire l'affaiblissement des ondes dans une grande variété d'environnements. Ce modèle englobe les effets de masquage aléatoires dus au blocage du signal par le relief, les arbres, les bâtiments, etc. Il s'exprime par l'équation :

$$P_l(d) = P_l(d_0) + 10nlog_{10}(\frac{d}{d_0}) + X. \tag{3.3}$$

$P_l(d_0)$ est l'affaiblissement sur le trajet à une distance d_0 depuis l'émetteur. $P_l(d)$ est l'affaiblissement sur le trajet à une distance arbitraire d, n est l'exposant d'affaiblissement sur le trajet qui dépend du type d'environnement (c.-à-d. environnement avec ou sans obstacles). X est une variable aléatoire à distribution gaussienne de moyenne nulle avec un écart-type σ pour représenter l'effet de masque.

3.2.3 Fading

Le *Fading* résulte de la réception de multiples répliques du signal transmis au récepteur due à quatre principaux mécanismes de propagation des ondes : la réflexion, la diffraction, la réfraction et la diffusion (figure 3.1).

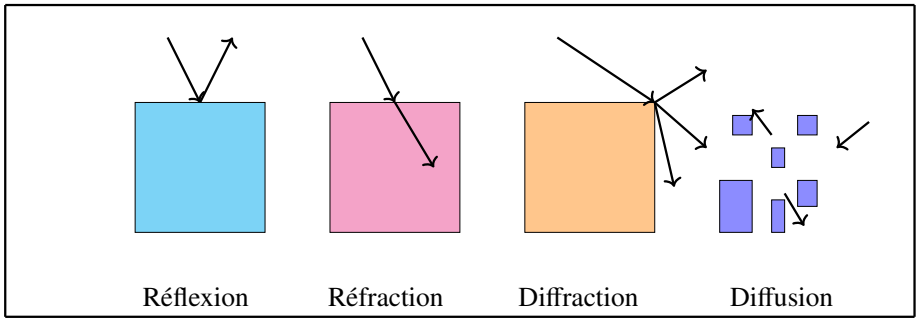


FIGURE 3.1 – Phénomènes de perturbation

La réflexion Lorsque l'onde électromagnétique tombe sur un objet de grande taille par rapport à la longueur de l'onde, l'obstacle reflète une partie de l'énergie de l'onde avec le même angle d'arrivée.

La réfraction Ce phénomène se produit chaque fois qu'une onde traverse un matériau.

La diffraction Ce phénomène se produit lorsqu'une onde atteint un bord ou une surface courbe d'un objet où elle se divise ensuite en une multitude d'ondes diffractées.

La diffusion Ce phénomène se produit lorsqu'une onde rencontre un ensemble d'obstacles de dimensions inférieures à sa longueur d'onde provoquant une superposition de diffractions élémentaires. L'onde est alors réfléchie dans toutes les directions.

Les modèles couramment utilisés pour simuler l'effet de fading sont : Rice, Rayleigh et Nakagami.

-Rice Ce modèle modélise la propagation des ondes dans un environnement avec un trajet dominant en terme de puissance. La densité de probabilité de Rice est utilisée pour décrire l'amplitude du signal reçu :

$$P_z(Z) = \frac{Z}{\sigma^2} exp(-\frac{z^2 + A^2}{2\sigma^2}) I_0(\frac{Z.A}{2\sigma^2}). \tag{3.4}$$

Où Z l'amplitude de signal, A l'amplitude du trajet prédominant et I_0 la fonction de Bassel d'ordre 0. Le facteur $K=\frac{A^2}{2\sigma^2}$ représente le degré de l'évanouissement.

-Rayleigh Ce modèle utilise la distribution de Rayleigh pour modéliser la variation rapide de l'amplitude signal. Ce modèle représente la propagation des ondes dans un environnement multi-trajets. L'amplitude du signal reçu est décrite par la formule (3.5) :

$$P_Z(Z) = \frac{Z}{\sigma^2} exp(\frac{Z^2}{2\sigma^2}). \tag{3.5}$$

Avec Z l'amplitude du signal et σ la puissance moyenne du signal.

-Nakagami Ce modèle de propagation est défini dans [51]. Le modèle Nakagami est une modélisation mathématique générale d'un canal radio avec effet d'évanouissement. Il possède de nombreux paramètres configurables pour permettre une représentation plus proche du canal de communication sans fil. Il permet de modéliser un canal en espace libre parfait, un canal à évanouissement moyen et même un canal à évanouissement important dans les milieux urbains. La distribution de Nakagami est définie par la fonction de densité de probabilité (3.6) :

$$P_Z(Z) = \frac{2m^m Z^{2m-1}}{\Gamma(m)\Omega^m} exp(-\frac{mZ^2}{\Omega}), m > 0.5. \tag{3.6}$$

Avec Γ est la fonction Gamma, *m* représente le degré d'évanouissement et Ω est la puissance du signal reçu.

3.2.4 L'effet Doppler

L'effet Doppler ou le décalage Doppler (figure 3.2) est la variation de la fréquence ou de la longueur d'onde d'un mobile qui se déplace par rapport à la source de l'onde. Pour illustrer le principe du décalage Doppler, un exemple courant est celui du changement de tonalité lorsqu'un véhicule produisant un son approche puis s'éloigne d'un observateur. Au regard de la fréquence émise, la fréquence reçue est plus élevée lors de l'approche, identique au moment du passage, et plus faible lors de l'éloignement. L'effet de Doppler est modélisé par le modèle de Jakes.

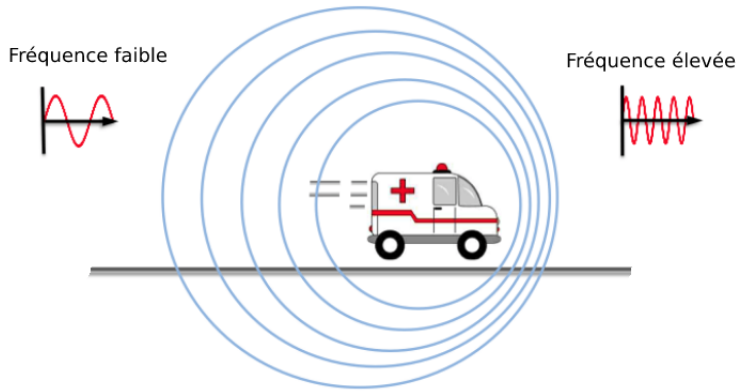


FIGURE 3.2 – Effet de Doppler

-Modèle de Jakes Ce modèle modélise le décalage de fréquence d'une onde provoqué par l'effet de Doppler à l'aide de la formule (3.7) :

$$S(f) = \frac{1}{\pi f_d \sqrt{1 - (\frac{f}{f_d})^2}}, |f| <= f_d \tag{3.7}$$

Avec f la fréquence de travail et f_d la fréquence de translation maximale.

Après avoir présenté les différents effets de perturbation du canal qui peuvent être présents dans un réseau VANET et les modèles de propagation modélisant ces effets, nous présentons dans la section suivante un état de l'art sur les indicateurs de rupture de liens. À noter que cet état de l'art introduit la catégorie des indicateurs de rupture de lien seulement, sans aborder les estimateurs de qualité de lien.

3.3 Détection de rupture de lien

La détection des ruptures de lien se fait en exploitant des mesures de ce lien. Les mesures de lien sont réalisées en récupérant des informations utiles provenant des paquets échangés dans le réseau (c.-à-d. acquittements reçus, données extraites des paquets reçus), elles concernent le RSSI, les erreurs de décodage, etc. À partir des mesures de lien, des métriques de détection sont construites pour produire une information d'anticipation de la rupture d'un lien. Le plus souvent, ces métriques sont conçues selon une technique simple comme la comparaison avec un seuil [52] ou en utilisant des techniques plus complexes comme l'apprentissage [3].

3.3.1 Classification des métriques

La conception d'un indicateur de rupture d'un lien ou d'un estimateur de l'état d'un lien se base sur un ensemble des informations/métriques. Ces dernières peuvent être classées selon deux grandes familles :

Métrique physique Dans cette famille de métriques, l'évaluation d'un lien se fait en se basant sur des informations extraites à partir de la couche physique. Elle possède l'avantage de fournir des observations immédiates sur l'état du lien dès la réception d'un paquet.

— ***RSSI (Received Signal Strength Indication)*** la mesure du RSSI donne l'information sur la puissance de réception d'un signal reçu, autrement dit son intensité,

— ***SNR (Signal to Noise Ratio)*** est calculé comme le ratio entre la puissance du signal reçu et le bruit. Il s'agit d'une mesure qui est largement utilisée pour évaluer les liens,

— ***Erreurs de décodage des paquets*** le processus de décodage des paquets au niveau de la couche physique aboutit à des erreurs de décodage lorsque le lien subit une dégradation.

Ces erreurs peuvent être utilisées pour évaluer l'état de lien [46][3].

Métrique logique Cette famille englobe les métriques indépendantes du matériel. Elles peuvent être classées en trois groupes :

— ***PRR*** est considéré comme la métrique la plus simple. Elle est calculée au niveau du récepteur et peut être utilisée comme référence pour l'évaluation des mesures physiques. Une métrique construite à base d'informations physiques est considérée comme bonne si elle corrèle avec le PRR,

— ***RNP (Required Number of Packet Transmissions)*** est calculée au niveau expéditeur. L'idée de RNP est de calculer le nombre moyen de retransmissions requis pour une bonne réception d'un paquet, pour ce faire une fenêtre temporelle est utilisée,

— ***Score*** ce type de métrique part sur l'idée d'utilisation de plusieurs métriques différentes, chacune pour évaluer une priorité du lien.

Comme mentionné avant, cette thèse porte sur l'optimisation de routage par la détection de la rupture d'un lien. Pour cela, la section suivante présente un état de l'art sur l'ensemble des travaux connexes les plus populaires sur les indicateurs de rupture de lien.

3.3.2 État de l'art sur les indicateurs de rupture de lien

De nombreux travaux exploitent l'information fournie par la puissance du signal reçu (*RSSI*) afin de détecter une rupture de lien. Les auteurs de [52] introduisent une métrique permettant de prédire une rupture de lien. Cette métrique a été utilisée pour améliorer les performances du protocole AODV. Elle consiste à comparer les valeurs de l'intensité du signal reçu à un seuil appelé *Pr-THRESHOLD*. Si la puissance du signal entrant est inférieure au seuil, le lien est considéré comme instable et est susceptible de subir une situation de rupture. Bien que les résultats expérimentaux montrent de bonnes performances, ils supposent que tous les nœuds ont la même puissance de transmission et que la perte du signal dépend entièrement de la distance qui sépare les nœuds (pathloss). Dans ce travail les aspects de modélisation de la propagation du signal sont insuffisants, ce qui conduit à des performances surévaluées.

D'autres auteurs, dans [53] proposent un algorithme pour prédire le temps de rupture de lien entre deux nœuds, qu'ils utilisent pour améliorer le protocole DSR. L'algorithme évalue le temps de rupture d'un lien en fonction de la puissance du signal des trois derniers paquets reçus. Les auteurs de [54] ont également proposé une autre méthode pour évaluer la probabilité de rupture de lien dans les réseaux véhiculaires à l'aide de RSSI. Chaque véhicule du réseau vérifie périodiquement les signaux reçus de ses voisins et mesure la distance, la vitesse et l'accélération de son prochain saut. En utilisant ces valeurs, le nœud prédit si le lien va rompre.

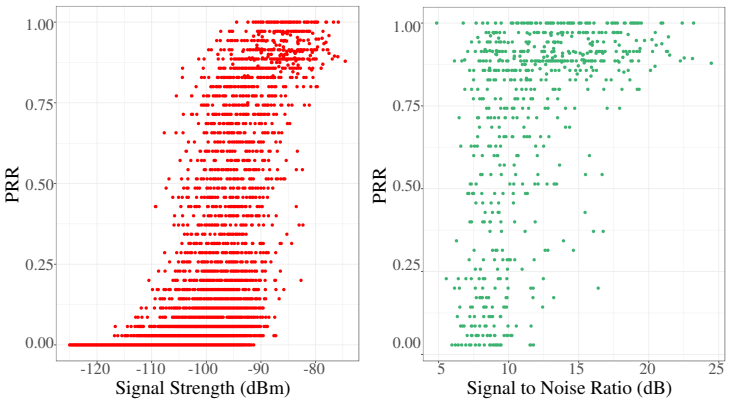
Dans [55] le principe de définition d'un seuil est utilisé pour détecter des ruptures de lien. La détection est faite si l'intensité du signal reçu est en dessous d'un seuil appelé *preemptive threshold*. Ce seuil est défini en fonction de la région autour d'une source. Les auteurs de [43] utilisent également le RSSI pour déterminer si un lien est en train de rompre. Si un nœud reçoit un signal en dessous d'un seuil donné, il collecte trois valeurs RSSI consécutives de son prédécesseur et utilise l'interpolation de Lagrange pour calculer une nouvelle intensité du signal reçu. Si cette intensité tombe en dessous du seuil, une rupture est détectée.

Un deuxième type d'indicateur se base sur l'information fournie par le SNR pour prédire les ruptures des liens. Les auteurs de [56], proposent un protocole de routage capable de basculer entre les routes selon une interpolation de Lagrange du rapport signal sur bruit et de la surcharge de la couche MAC (*Media Access Control*).

D'autres indicateurs de rupture de lien fonctionnent au niveau de la couche physique et utilisent les informations du processus de décodage des paquets OFDM (Orthogonal Frequency-Division Multiplexing) [46, 3]. De telles approches permettent l'obtention des informations sur la raison du succès ou de l'échec du processus de réception du paquet. Contrairement aux indicateurs basés sur RSSI et SNR qui nécessitent la bonne réception de paquets, ils fournissent des informations sur un paquet entrant depuis sa détection jusqu'à son décodage complet. Dans [46], les auteurs ont conçu un indicateur empirique de l'état du lien appelé Indicateur de prévision de l'état du lien (*Link State Forecasting Indicator - LSFI*), qui se base sur les erreurs de décodage liées au processus de réception d'une trame OFDM. En supposant que chaque erreur de décodage peut être considérée comme une source imparfaite pour prédire la rupture d'un lien, les auteurs de [3] ont amélioré ce travail en proposant un indicateur appelé LSFI-BF (*Link State Forcasting Indicator Belief Function*) qui fait une prédiction probabiliste résultant de la fusion des erreurs de décodage de trame OFDM avec la théorie de Dempster-Shafer.

Discussion Les techniques de prédiction de rupture de lien présentées ci-dessus sont basées sur la couche physique. Elles utilisent des informations fournies par la puissance de signal reçu, le rapport signal bruit et le processus de décodage des paquets au niveau physique. Les deux premières catégories soulèvent certaines questions car elles estiment l'état de lien en se basant sur une interprétation du RSSI ou du SNR qui ne peuvent détecter avec précision la rupture d'un lien. Le principal inconvénient de ces approches est qu'elles ne fournissent qu'un instantané de la qualité du signal sans corrélation avec le taux de réception des paquets (PRR) [57].

La figure 3.3 présente le résultat d'une étude qui montre le niveau de corrélation des informations de la couche physique (RSSI et SNR) avec le PRR [45]. Une simple lecture des valeurs du RSSI et du SNR ne suffit pas pour déterminer avec précision le PRR.



(a) RSSI vs PRR (b) SNR vs PRR

FIGURE 3.3 – Corrélation du SNR et RSSI avec le PRR

Les techniques basées sur le RSSI et le SNR n'utilisent que les paquets reçus avec succès à la couche MAC et ne prennent pas en compte les paquets qui sont rejetés au niveau de la couche physique. Elles ignorent toute information collectée au niveau de la couche physique. La deuxième catégorie d'indicateurs de rupture de lien profite du processus de décodage des trames OFDM au niveau de la couche physique pour anticiper les ruptures des liens. Les paquets sont analysés au niveau du bit et les paquets rejetés, en raison d'erreurs de décodage, sont également pris en compte dans l'algorithme de détection. Les résultats de ces travaux montrent une grande réactivité par rapport à d'autres techniques.

Le travail présenté dans cette thèse est inspiré de cette catégorie d'indicateur basée sur les

erreurs de décodage OFDM. Une étude des deux indicateurs de rupture de lien conçus spécialement pour les réseaux véhiculaires *LSFI* et *LSFI-BF* est effectuée dans le chapitre 5. Dans la prochaine section, le processus de décodage OFDM ainsi que les erreurs qui peuvent résulter du décodage des paquets seront expliqués. Cette section présente la base de notre contribution.

3.4 Le décodage d'une trame OFDM

La technique de codage de paquets OFDM (Orthogonal Frequency Division Multiplexing) est utilisée dans les normes IEEE 802.11a, g, p. Nous considérons ici le standard IEEE802.11p, qui est dédié aux communications véhiculaires. Un paquet OFDM est composé de trois parties, comme illustré à la figure 3.4. La première, appelée Préambule (preamble), contient douze symboles OFDM (dix symboles courts et deux symboles longs), ces symboles sont utilisables par le récepteur pour la détection du signal, la synchronisation temporelle, l'estimation de décalage de canal (c.-à-d. le processus de caractérisation du canal). La seconde, appelée Entête (header), ne contient qu'un seul symbole OFDM, et fournit des informations sur la longueur de la partie de données, le type de modulation et de codage utilisé. La dernière, appelée Charge (payload), contient une trame MAC [58].

Au niveau du récepteur, le processus de réception peut être divisé en deux étapes. La première étape est la détection de trame reçue par rapport au seuil d'énergie requis pour déclencher le processus de décodage. Une fois que la trame a été correctement détectée, l'étape de décodage est enclenchée, sinon la trame est considérée comme perdue. Au cours de cette étape, la trame OFDM est décodée selon l'ordre suivant : les symboles courts, les symboles longs, l'entête et les données.

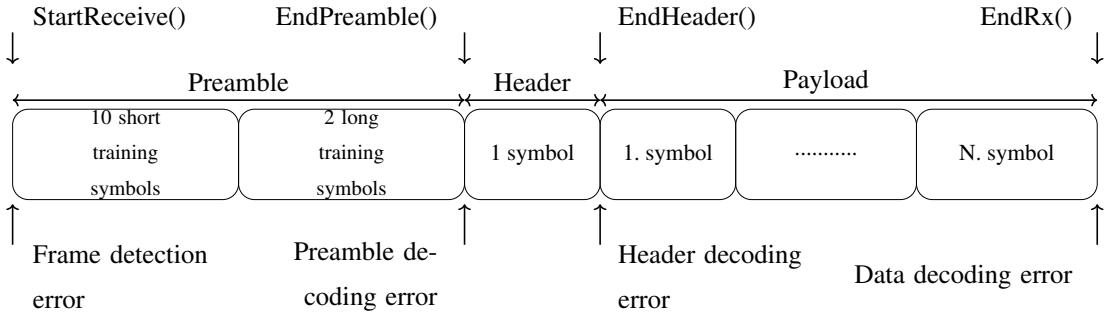


FIGURE 3.4 – Procéssus de décodage OFDM

Dans le cadre de cette thèse, le modèle PhySimWifi [59] est utilisé avec le simulateur ns-3. PhySimWifi contient une implémentation de la couche physique de la norme IEEE802.11p basée sur OFDM, comprenant tout le traitement du signal au niveau du bit et effectuant les phases de traitement d'un véritable émetteur-récepteur OFDM. En outre, le simulateur des réseaux ns-3 permet l'association de différents modèles de propagation d'une onde électromagnétique à une couche physique. Ceci permet de créer un processus de transmission de données réaliste dans un environnement sans fil. Le processus de réception des paquets OFDM s'effectue dans PhySimWifi en quatre phases : StartReceive (1), EndPreamble (2), EndHeader (3) et EndReceive (4) comme illustré dans la figure 3.4.

La phase StartReceive Cette phase est déclenchée à la réception du premier bit d'un paquet. Si la puissance du signal reçu est inférieure au seuil de détection d'énergie, le paquet sera rejeté, et une erreur de détection de trame OFDM sera générée. Si l'état du récepteur est différent de IDLE ou CCA BUSY, alors le paquet est également rejeté, mais pour des raisons d'interférence. Cette erreur est appelée erreur d'interférence. Sinon, la phase suivante, réception préambule sera déclenchée.

La phase EndPreamble Similairement à la phase StartReceive, dans la phase EndPreamble, si l'état du récepteur est RX ou TX, alors le paquet est rejeté pour des raisons d'interférence (erreur d'interférence du preamble). Sinon, une vérification du signal détecté pour un rapport signal/bruit supérieur à 4 dB est effectuée. Si c'est le cas, l'estimation de canal est lancée et l'événement EndHeader est prévu.

L'échec du test SNR génère un paquet rejeté qui est représenté par une erreur appelée erreur de décodage de préambule (EDP).

La phase EndHeader Dans cette phase, l'estimation initiale du canal est appliquée et l'en-tête du signal est décodé. Le contenu de l'en-tête est utilisé pour déterminer la modulation et le taux de codage, la longueur de trame et les bits de parité [1]. Si le décodage de l'en-tête est réussi, la

1. Un bit de parité, ou bit de contrôle, est un bit ajouté à une chaîne de code binaire pour garantir que le nombre total de bits dans la chaîne est pair ou impair. Les bits de parité sont utilisés comme la forme la plus simple de code de détection d'erreur.

phase de décodage EndRx se déclenche. Sinon, le paquet est rejeté et une erreur d'interférence se produit.

Si l'état du canal est différent de SYNC ou si le contenu de l'en-tête n'est pas plausible, alors le paquet est rejeté et l'événement associé est une erreur de décodage de l'entête.

La phase EndRx Dans cette étape les symboles codant les données sont finalement décodés. L'estimation initiale de canal est appliquée à tous les échantillons OFDM. Ensuite, les bits sont réorganisés dans leur format d'origine. Si les bits réarrangés correspondent aux données transmises, le paquet est considéré comme bien reçu et un événement RxOk se produit.

Sinon une erreur se produit, appelée erreur de décodage des données (EDD).

3.4.1 machine d'état de la couche physique

La couche physique distingue cinq états différents (figure 3.5). L'état TX qui correspond à l'état actif lorsque la couche physique transmet un paquet. L'état IDLE, représente l'état actif de la couche physique s'il n'y a pas de réception en cours et lorsque l'intensité cumulée du signal est inférieure au seuil *CcaModelThreshold*. L'état CCA_BUSY est similaire à l'état IDLE sauf que le signal est supérieur au seuil du modèle *CcaModelThreshold*. L'état SYNC reflète la situation dans laquelle le préambule a été détecté ou le canal a été verrouillé, et donc le canal n'est pas accessible. Et finalement l'état RX correspond à l'état actif du récepteur lors du décodage de la partie payload d'un paquet.

3.4.2 Classification des erreurs de décodage

Comme expliqué dans la section précédente, l'échec d'une phase de décodage génère une erreur spécifique. Le tableau 3.1 résume l'ensemble des erreurs qui peuvent être générées au cours du processus de décodage d'une trame OFDM. On distingue trois types de familles d'erreurs selon la cause de l'échec de décodage. Erreur d'interférence, erreur d'énergie de détection insuffisante et erreur de décodage. Ces erreurs peuvent être utilisées pour détecter les ruptures des liens. Dans la section suivante le lien entre ces erreurs et les ruptures sera expliqué.

Une étude des erreurs de décodage a été effectuée afin de déterminer quelles erreurs pouvaient être exploitées pour anticiper une rupture d'un lien. Pour cela un scénario d'éloignement de deux véhicules a été utilisé et la figure 3.6 montre un histogramme cumulatif des erreurs de décodage des paquets :

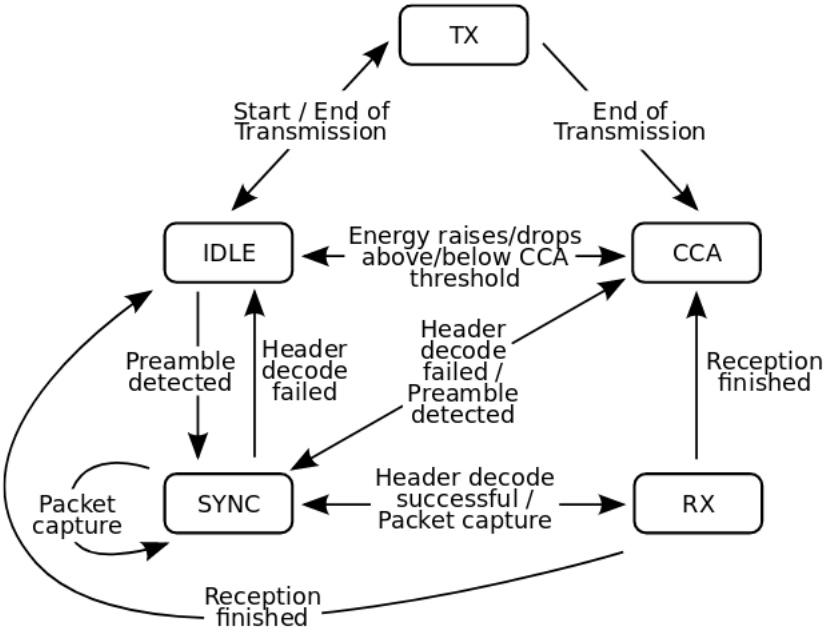


FIGURE 3.5 – la machine d'état de la couche physique [1]

Étape de décodage	Erreur de décodage
StartReceive	- Erreur de détection de trame OFDM - Erreur d'interférence
EndPreamble	- Erreur de décodage de préambule (EDP) - Erreur d'interférence
EndHeader	- Erreur de décodage de l'entête - Erreur d'interférence
EndRx	- Erreur de décodage de données (EDD)

TABLE 3.1 – Erreurs de décodage d'une trame OFDM

— Les erreurs liées au décodage du préambule (Erreur de Décodage du Préambule - *EDP*),

— les erreurs liées au décodage des données (Erreur de Décodage des Données - *EDD*),

— Les erreurs d'interférences. Néanmoins ces erreurs ne peuvent pas être utilisées puisqu'elles dépendent des interférences et donc de la densité des nœuds,

— Les erreurs de détection. Néanmoins ces erreurs ne peuvent pas non plus être utilisées puisqu'il est impossible d'identifier l'expéditeur et donc le lien concerné du fait du rapport signal sur bruit (*SNR*),

— Les erreurs de décodage de l'entête. Ces erreurs sont quant à elles très rares comme le montre la figure 3.6.

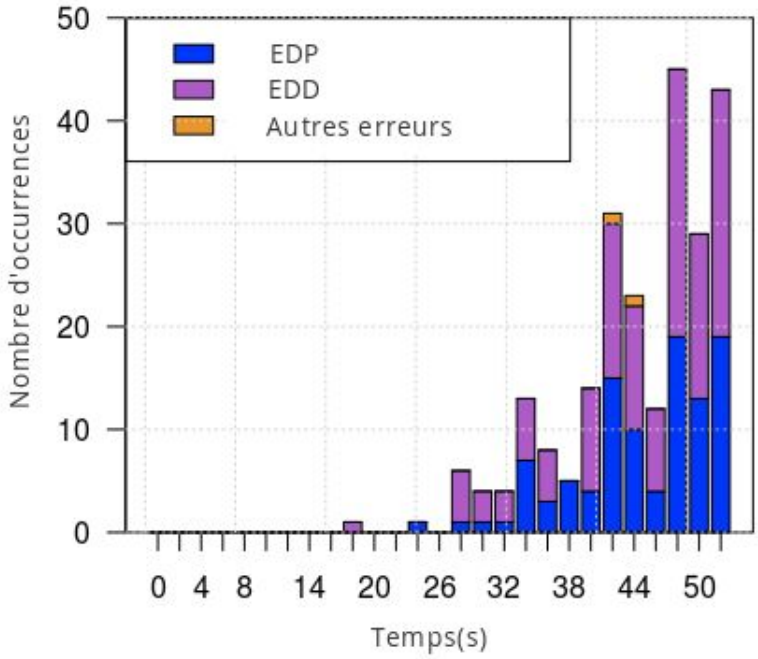


FIGURE 3.6 – Erreurs de décodage OFDM (scénario d'éloignement de deux véhicules)

Comme résultat de cette étude et en fonction de leurs fréquences d'apparition, les erreurs utilisées dans notre détection seront donc les erreurs liées au décodage du préambule (*EDP*) et les erreurs liées au décodage des données (*EDD*). Ces résultats viennent confirmer les résultats obtenus par les auteurs des papiers [3, 46].

3.5 Des erreurs de décodage OFDM vers la détection de rupture de lien

La rupture d'un lien est traduite par la perte d'un paquet de données au niveau de la couche réseau. La figure 3.7, montre l'état d'une communication au niveau de la couche réseau en fonction du nombre de retransmissions de paquet au niveau physique. Afin d'illustrer la rupture de

lien, cette image est effectuée à partir des données d'un scénario d'éloignement de deux véhicules. La retransmission d'un même paquet sept fois au niveau de la couche physique correspond à la perte du même paquet au niveau de la couche réseau. Cette retransmission est pilotée par la couche MAC. Tant que la couche MAC ne reçoit pas d'accusé de réception (ACK), elle continue à retransmettre le paquet un certain nombre de fois (au maximum sept retransmissions dans le cas standard).

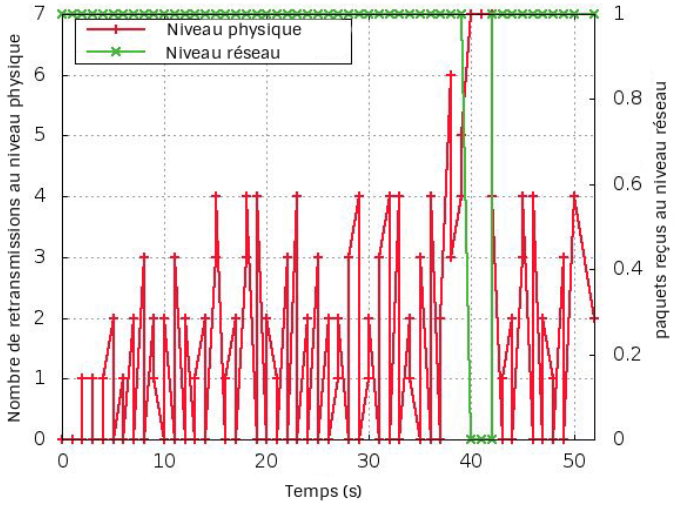


FIGURE 3.7 – Nombre de retransmission de paquet au niveau physique versus la perte de paquet au niveau de la couche réseau

Une détection de rupture de lien est caractérisée par un temps de prédiction (appelé aussi délai de prédiction) qui correspond au temps entre la détection et la vraie rupture. Ce temps doit donc être utilisable par le protocole de routage. En effet, il doit être le plus petit possible mais suffisamment long pour qu'un protocole de routage puisse prendre une décision et entreprendre une action corrective (recherche d'une nouvelle route).

3.6 Conclusion

Le présent chapitre a fait l'objet d'état de l'art sur la détection d'une rupture de lien. D'abord les différents effets de propagation impactant la transmission dans les VANET ont été introduits, et des exemples des modèles de propagation de chaque effet ont été présentés. Par la suite, un aperçu sur les différentes approches et techniques utilisées dans la littérature pour la détection

de rupture de lien dans les réseaux ad-hoc sans fil ont été présentées, tout en mettant l'accent sur leurs avantages et leurs limites. À la fin, le décodage des trames OFDM est détaillé et une classification des erreurs de décodage qui seront utilisées dans la partie contribution est fournie.

Notre travail de thèse porte sur l'optimisation du routage par la détection de rupture de lien. Pour ce faire, nous dédions le prochain chapitre à l'introduction de l'outil mathématique qu'on a utilisé pour développer notre approche.

Chapitre 4

Théorie des fonctions de croyance

Sommaire

4.1 Introduction

Dans le cas du développement de systèmes intelligents qui interagissent avec le monde réel, la modélisation des imperfections des données est un problème difficile à résoudre. Pour que ces systèmes agissent de manière robuste, il faut qu'ils soient capables de faire face aux différentes

formes d'incertitudes que peuvent leur soumettre le monde réel, au travers des données qui ne sont pas toujours cohérentes. Il existe une variété de cadres mathématiques permettant la manipulation des imperfections de données [60]. La théorie des probabilités est la théorie prédominante et elle est largement appliquée pour ce type de problématique. D'autres cadres incluent la théorie des ensembles flous [61], la théorie des possibilités [62], la théorie des fonctions de croyance [63], etc.

Dans le cadre de cette thèse, la théorie des fonctions de croyance a été adoptée. Ce choix sera expliqué dans la section 4.3. La théorie de croyance, aussi connue sous le nom de théorie de Dempster-Shafer (TDS) ou théorie de la preuve, permet le raisonnement avec l'incertitude. Elle permet de modéliser les imperfections de données et le conflit généré par des sources de données. La TDS utilise des outils performants de fusion des données (règles de combinaison) qui rendent possible la combinaison de multiples données, afin de produire des informations plus cohérentes, précises et utilisables que celles fournies par des sources de données individuelles. Les sources de données peuvent être : un expert du domaine, un capteur, etc. Dans la TDS, chaque source exprime sa connaissance et son ignorance sur une question posée sous le format des fonctions de masses, et qui seront combinées afin de mettre en évidence les croyances communes et assurer une prise de décision plus fiable.

Ce chapitre présente le cadre mathématique de notre contribution. Dans une première partie, nous présentons les différents cadres théoriques de manipulation de données imparfaites : sous-ensembles flous, probabilités, possibilités et fonctions de croyance. Par la suite nous expliquons notre choix du cadre mathématique à utiliser (théorie des fonctions de croyance).

Dans une deuxième partie, nous détaillons les concepts de la théorie des croyances, suivie d'une description des modèles de représentation d'information (modèles de masse), des règles de combinaison et critères de prise de décision.

4.2 Difficultés liées à la fusion de données

Le processus de fusion de données soulève certains problèmes particuliers. La majorité de ces problèmes découlent principalement des données à fusionner (problème d'imperfection des données), des conflits entre les données ainsi que de la nature des systèmes étudiés (figure (4.1)).

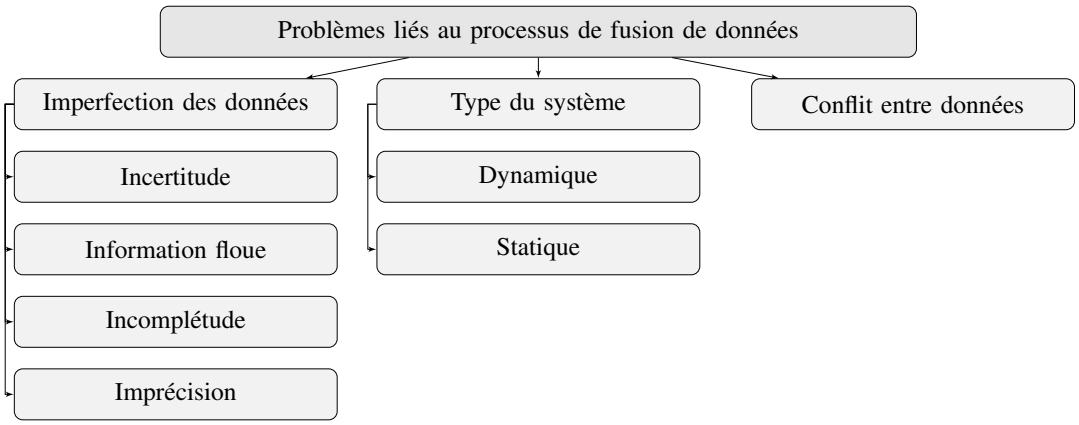


FIGURE 4.1 – Problèmes liés au processus de fusion de données

Imperfection des données Les mesures fournies par des capteurs sont toujours affectées par un certain niveau d'imprécision et d'incertitude. Il est important donc qu'un outil de fusion de données soit capable de modéliser et de prendre en compte ces imperfections, imprécisions et incertitudes afin de réduire leur effet sur le processus de décision. Selon [64], l'imperfection d'une donnée peut être associée à : (i) l'incertitude liée au degré de justesse et d'exactitude d'une mesure, (ii) l'imprécision qui est relative à des défauts quantitatifs, (iii) l'incomplétude qui désigne un manque partiel de données, (iv) l'information floue issue des intervalles des valeurs mal définis. Ainsi, une information floue constitue une information imprécise.

Type de système Le phénomène étudié peut être indépendant ou dépendant du temps statique ou dynamique. Dans ce dernier cas, l'outil de fusion de données doit être capable d'incorporer des historiques récents des mesures dans le processus de fusion. Cela joue un rôle essentiel dans la validité des résultats de la fusion.

Conflit entre les données Il est problématique de fusionner des données contradictoires, surtout lorsque le système de fusion est fondé sur un grand nombre d'observations. Pour éviter de produire des résultats contre-intuitifs, tout outil de fusion de données doit posséder des mécanismes de manipulation des données conflictuelles.

4.3 Cadres mathématique pour la fusion de données

La théorie des probabilités Elle est connue comme le cadre le plus ancien de manipulation des données imparfaites. Elle constitue la base mathématique de l'étude des phénomènes aléatoires, c'est-à-dire des phénomènes dont l'issue n'est pas prévisible à l'avance (phénomène dont on ne peut pas prédire avec certitude son résultat). La théorie des probabilités se base sur un ensemble des lois permettant la description du comportement du phénomène observé. Une probabilité associée à un événement exprime le degré de véracité en cet événement. L'inconvénient de la théorie des probabilités classique est qu'elle n'est pas capable de modéliser d'ignorance et l'imprécision des données. Cependant, lorsque cette théorie est appliquée à un phénomène bien défini, les résultats obtenus peuvent être optimaux.

Théorie des ensembles flous Développée par Zadeh en 1965 [61], cette théorie décrit un raisonnement avec des informations imparfaites. Plus précisément, elle permet la modélisation et le traitement d'informations floues. Dans la théorie des ensembles flous, chaque élément possède un degré d'appartenance à un ensemble défini. Contrairement à la théorie classique des ensembles, qui définit l'appartenance d'éléments à un ensemble en termes binaires (un élément appartient ou non à l'ensemble) en fonction d'une condition. La théorie des ensembles flous permet l'évaluation progressive de l'appartenance d'un élément à un ensemble ; elle est décrite à l'aide d'une fonction d'appartenance évaluée dans l'intervalle [0, 1]. La théorie des ensembles flous offre des règles de combinaison conjonctives et/ou disjonctives. L'élément qui a le plus haut degré d'appartenance à l'ensemble flou sera sélectionné comme le plus crédible.

Théorie des possibilités Initialement introduite par Zadeh [62] et développée par la suite par Dubois et Prade [65], cette théorie est une extension de la théorie des ensembles flous. Cependant, elle est dédiée au traitement d'informations incomplètes au lieu d'informations floues. Similairement à la théorie des fonctions de croyance, la théorie des possibilités permet une représentation de l'ignorance en partant sur le principe que toute hypothèse est possible.

Théorie des fonctions de croyance Également connue sous le nom de théorie de Dempster-Shafer est l'un des principaux outils disponibles pour raisonner avec des données incertaines et imprécises. Cette théorie, introduite par Dempster [63] et développée plus tard par Shafer [66],

étend la théorie de la probabilité et de la possibilité. Elle repose sur deux fondements principaux : (i) la représentation de l'information à combiner sous forme de fonctions de masses, cette étape repose sur la modélisation des connaissances d'une source pour un problème en attribuant une probabilité à chaque élément de l'ensemble des solutions possibles au problème, (ii) une règle de combinaison pour fusionner les fonctions de masse, cela permet d'obtenir une fonction de croyance représentative de toutes les connaissances disponibles. Cette théorie a été utilisée dans de nombreux domaines y compris les réseaux véhiculaires [67, 3]. Les principes de base de la théorie des croyances seront expliqués dans la suite.

Le choix de l'outil mathématique pour la combinaison de données imparfaites ne se révèle pas toujours évident. Il repose sur les spécificités du système étudié ainsi que sur le type de données traitées. Dans le cadre de cette thèse, nous avons fait le choix de la théorie des croyances comme outil de combinaison de données. Ce choix découle des caractéristiques et des fonctionnalités qu'elle offre, à savoir : la possibilité pour chaque source de fournir de l'information à différents niveaux de détail (à travers des fonctions de masses), la possibilité de représenter l'ignorance totale ou partielle, la variété des règles de combinaison selon le type de données traitées et leur consistance.

Dans la suite de ce chapitre, nous présentons les concepts de base de la théorie de croyance et les fonctionnalités qui seront utilisées dans le cadre de ce travail.

4.4 Théorie des fonctions de croyance et l'imperfection des données

La théorie des fonctions de croyance représente un cadre complet de manipulation et traitement de données imparfaites et qui permet d'extraire une information fiable à partir d'un ensemble d'informations incertaines. Cette imperfection peut prendre deux formes :

— l'incertitude qui se définit par le manque de précision de l'information fournie,

— le conflit qui découle de deux sources d'information qui peuvent fournir des croyances contradictoires à propos d'un même phénomène.

L'expression de l'incertitude est importante et nécessaire quand il s'agit de combiner des informations provenant de sources différentes. Souvent les informations qui viennent d'un capteur

ne sont pas exactes mais entachées d'incertitude, sans compter d'autres informations qui viennent d'autres capteurs et qui pourraient être en contradiction. Il est alors important d'une part de représenter cette incertitude et d'autre part de pouvoir la gérer pour produire une information avec un degré minimal d'incertitude ou du moins de la mesurer.

Prenons un exemple simple basé sur la consultation de deux médecins (M_1) et (M_2) pour le diagnostic d'une maladie. Chaque médecin examine le patient et selon les symptômes observés décrit l'affection du patient. Supposons que les médecins hésitent entre deux maladies (A_1) et (A_2). Dans ce cas la théorie de croyance permet de modéliser cette hésitation sous forme d'incertitude :

$m_{M1}(A_1) = 1/4$	$m_{M2}(A_1) = 0$
$m_{M1}(A_2) = 1/2$	$m_{M2}(A_2) = 1/2$
$m_{M1}(\Omega) = 1/4$	$m_{M2}(\Omega) = 1/2$

La colonne de gauche modélise l'opinion du premier médecin (M_1) qui croit à 25% que la maladie est A_1 et à 50% que c'est la deuxième maladie (A_2). Il exprime également une ignorance $m_{M1}(\Omega)$ de 25% qui veut dire qu'il ne sait pas de quelle maladie souffre le patient. D'autre part, le médecin (M_2) est totalement sûr que ce n'est pas la maladie A_1, mais que ça peut être la maladie (A_2) à 50% ou non à 50% ($m_{M2}(\Omega)$=1/2).

Cette représentation permet à chaque source d'exprimer son degré d'incertitude à propos des observations d'un phénomène donné.

L'utilisation de la théorie des fonctions de croyance consiste à l'application des étapes illustrées dans la figure 4.2 :

— La représentation de l'information,

— La combinaison des masses,

— La prise de décision.

Le formalisme et la définition concernant chaque étape seront présentés dans les sections suivantes.

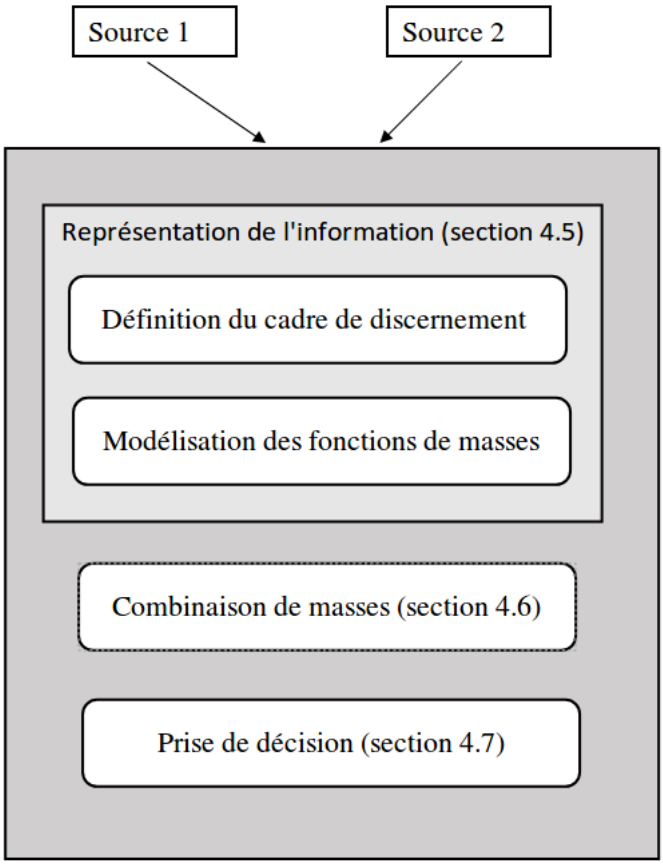


FIGURE 4.2 – Processus de fusion de données selon la TDS

4.5 Représentation de l'information

4.5.1 Cadre de discernement

La première étape pour modéliser un problème avec la théorie de croyance est la définition de cadre du discernement.

Soit $\Omega = \{ \omega_1, \omega_2, ..., \omega_n \}$ un ensemble fini, appelé cadre de discernement. Chaque hypothèse ω_i est une réponse possible à la question ou au problème considéré. Le référentiel 2^Ω contient toutes les combinaisons possibles d'éléments de Ω (sous ensemble A de Ω) :

$$2^\Omega = \{A, A \subseteq \Omega\} = \{\emptyset, \{\omega_1\}, \{\omega_2\}, \{\omega_1, \omega_2\}, ..., \Omega\} \tag{4.1}$$

Chaque élément de 2^Ω représente une proposition. Une proposition peut être un singleton (comme ω_1) ou un ensemble de singletons (comme $\{\omega_1, \omega_2\}$). L'élément $\emptyset$ représente le conflit

alors que l'élément Ω qui est le cadre de discernement représente l'ignorance.

Exemple En reprenant l'exemple du diagnostic de maladie, un patient montre des symptômes qui peuvent être dus à l'une des deux maladies A_1 ou A_2 . Il faut donc déterminer de quelle maladie souffre ce patient. Le cadre de discernement est donc défini par :

$\Omega = \{ A_1, A_2 \}$.

Le référentiel 2^Ω est alors défini par :

$$2^\Omega = \{\emptyset, \{A_1\}, \{A_2\}, \Omega\} \tag{4.2}$$

4.5.2 Fonction de masse

Après avoir défini l'ensemble des solutions possibles au problème traité sous la forme d'un cadre de discernement, l'étape suivante consiste en la représentation des croyances vis-à-vis des solutions possibles. Chaque expert du domaine représente son degré de croyance en chaque solution possible par une fonction de masse (ou *BBA* pour Basic Belief Assignment) m. La connaissance exprimée par un agent à propos de chaque hypothèse est décrite par une fonction de masse, désignée par $m(.)$. Elle permet d'associer à chaque élément de l'ensemble 2^Ω (4.2) une valeur dans l'intervalle [0,1]. Une fonction de masse est alors définie par :

$$m : 2^\Omega \rightarrow [0, 1] \tag{4.3}$$

L'ensemble des masses attribuées aux propositions doit respecter la condition suivante :

$$\sum_{A \subseteq \Omega} m(A) = 1 \tag{4.4}$$

Chaque élément qui possède une masse non nulle ($m(.) \neq 0$) est connu comme un élément focal [1]. Les fonctions de masse possibles sont :

— *m(A)* désigne la croyance associée à l'hypothèse A,

1. Un élément focal est un élément qui possède un degré de croyance c.-à-d : $m(\omega) = p$, $\omega \in \Omega$, $p \in [0,1]$

— $m(\Omega)$ correspond au niveau d'ignorance et de méconnaissance,

— $m(\emptyset)$ représente le degré de conflit. Ce conflit existe quand des croyances sont attribuées à des hypothèses contradictoires.

4.5.3 Fonctions de masse particulières

Indépendamment de la représentation, il y a certaines fonctions de masses qui sont particulièrement importantes qui sont décrites ci-dessous.

Fonction de masse certaine Une fonction de masse m est dite *certaine*, si : $\forall$ A et $B \in \Omega$, $m(A)=1$, $m(B)=0$. Autrement dit, une masse certaine est une masse qui attribue toute croyance à une proposition. Cela signifie qu'il y a un seul élément focal.

Fonction de masse normale (standard) Une fonction de masse m est dite *Normale* si : $m(\emptyset)=0$. Autrement dit, une masse avec un conflit égal à 0 est une fonction de masse normale.

Fonction de masse vide Une fonction de masse est dite *Vide*, si : $m(\Omega)=1$. Autrement dit, une fonction de masse vide représente l'ignorance totale de l'état de système.

Fonction de masse simple Une fonction de masse est dite *Simple* si :

$m(\Omega)= p$

$m(A)= 1\text{-}p$, $A \in \Omega$

$m(B)= 0$, $B \neq A \in \Omega$

$p \in [0,1]$

Autrement dit une fonction de masse simple est une fonction de masse qui s'exprime sur deux propositions (une solution et l'ignorance).

Fonction de masse dogmatique Une fonction de masse est dite *Dogmatique* si : $m(\Omega)= 0$. Autrement dit le cadre de discernement n'est pas un élément focal.

Fonction de masse bayésienne Une fonction de masse est dite *Bayésienne* si tous les éléments focaux sont des singletons :

$m(A) \neq 0 \Rightarrow |A|=1, A \in \Omega$.

Exemple de répartition de masse selon les différents types des BBA Un exemple de répartition des masses sur le cadre de discernement $\Omega = \{ A_1, A_2 \}$ selon les différents types des fonctions de masses présentées précédemment est donné par le tableau 4.1 :

TABLE 4.1 – Exemple de masses

Fonction de masse	$\emptyset$	A_1	A_2	Ω
Certaine	0	1	0	0
Normal	0	0.2	0.3	0.5
Vide	0	0	0	1
Simple	0	0	0.75	0.25
Dogmatique	0.4	0.2	0.4	0
Bayésienne	0	0.2	0.5	0

4.5.4 Modèles de masse

La théorie des croyances par son aspect applicatif s'appuie sur la construction des fonctions de masses. Cette étape se révèle difficile, car elle représente la base des étapes suivantes. Elle consiste à la mise en œuvre d'un modèle de masse qui décrit le comportement des masses. Si le modèle de masse est mal construit, alors les résultats finaux sont erronés. De nombreux travaux sur cette théorie sont focalisés sur la combinaison des fonctions de masses et le raisonnement associés (c.-à-d. les règles de combinaison, la prise de décision) [68, 69], mais peu de travaux se sont intéressés aux modèles de masse eux-mêmes.

La mise en place d'un modèle de fonction de masses approprié à un problème spécifique reste un challenge considérable. Puisque le modèle de masse dépend de l'application et de la perception du système étudié, il est difficile (voir impossible) de trouver un modèle universel pour représenter les masses [70]. Dans la littérature, plusieurs modèles de masse sont disponibles et les auteurs de [71] citent les plus utilisés. Les auteurs de [72] utilisent les réseaux de neurones pour définir leur modèle de masse. Le modèle proposé est assez performant spécialement dans le

cas du traitement d'images. Dans [73], une méthode basée sur Fuzzy-Cmeans est proposée pour construire le modèle de fonction de masse. D'autres modèles reposent sur des statistiques pour construire les fonctions de masse [74], certains se basent sur les probabilité [75] et il existe aussi d'autres modèles qui se basent sur l'opinion des experts des domaines. Chacun de ces modèles est construit selon des exigences et des contraintes spécifiques en fonction de l'application pour laquelle il est conçu et présente donc des avantages et des inconvénients.

Cette section est consacrée à la présentation de deux modèles de masse, le premier est de modèle de *Rombaut* qui a été utilisé pour la détection de rupture de lien dans les réseaux véhiculaires [3], et qui représente le point de départ de ce travail de thèse. Le deuxième modèle est le modèle *Non-antagoniste*, c'est le modèle qui est utilisé dans notre contribution, le choix de ce modèle sera justifié dans le chapitre 5.

Modèle de masse de Rombaut Présenté pour la première fois par [76], ce modèle exprime la croyance d'un expert par une fonction de masse sur une hypothèse (4.5), son complément (les autres hypothèses qui existent dans le cadre de discernement) (4.6) et l'ignorance (4.7) simultanément. Avec ce modèle, une source peut donc exprimer une croyance sur toutes les hypothèses à la fois ce qui introduit un auto-conflit (c.-à-d. la source est en conflit avec elle-même.). Le conflit généré par ce modèle rend compliqué l'étape de décision expliquée par la suite.

$$m(\omega) = p_1 \quad p_1 \in [0, 1]. \tag{4.5}$$

$$m(\overline{\omega}) = p_2 \quad p_2 \in [0, 1]. \tag{4.6}$$

$$m(\Omega) = 1 - p_1 - p_2 \quad p_1, p_2 \in [0, 1]. \tag{4.7}$$

Le modèle de Rombaut possède l'avantage de permettre à une source d'exprimer des croyances simultanément sur l'ensemble de toutes les solutions possibles. Cela permet de voir l'avis de la source à propos de chaque solution. D'autre part, ce modèle présente des inconvénients. Le fait de permettre aux sources d'exprimer leurs croyances sur tout l'ensemble Ω produit une masse de conflit importante après la combinaison ce qui peut influencer l'étape de la prise de décision.

Modèle de masse Non-antagoniste Tout comme le modèle Rombaut, ce modèle exprime une croyance sur toutes les propositions. Toutefois, il a la propriété d'éviter l'auto-conflit car il ne permet pas de soutenir simultanément une hypothèse et son complément. Un exemple est présenté dans [77]. Les fonctions de masse sont présentées dans la figure 4.3.

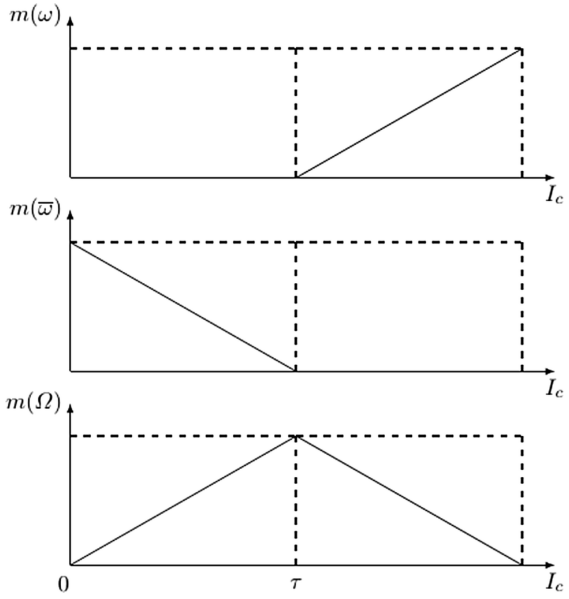


FIGURE 4.3 – Modèle Non antagoniste : fonction de masse d'une hypothèse (haut), fonction de masse de complément de l'hypothèse (milieu) et fonction de masse de l'ignorance (bas).

Elles respectent ce modèle et s'expriment au travers du modèle mathématique suivant :

$$m(\omega) = \begin{cases} 0 & I_c \in [0, \tau] \\ \Phi_1(\alpha_0, I_c) & I_c \in [\tau, 1] \end{cases} \tag{4.8}$$

$$m(\overline{\omega}) = \begin{cases} \Phi_2(\alpha_0, I_c) & I_c \in [0, \tau] \\ 0 & I_c \in [\tau, 1] \end{cases} \tag{4.9}$$

$$m(\Omega) = \begin{cases} 1 - \Phi_2(\alpha_0, I_c) & I_c \in [0, \tau] \\ 1 - \Phi_1(\alpha_0, I_c) & I_c \in [\tau, 1] \end{cases} \tag{4.10}$$

Où I_c est l'indice de confiance, α_0 est un coefficient lié à la fiabilité de la source et Φ_1, Φ_2 sont des fonctions sélectionnées qui varient entre $[0, \tau]$ et $[\tau, 1]$.

Le modèle de masse Non-antagoniste possède l'avantage de réduction de la masse de conflit, comme il ne permet pas à une source d'exprimer sa croyance sur tout l'ensemble Ω, mais sur deux éléments de Ω seulement (c.-à-d. une solution et l'ignorance). Cette propriété élimine la possibilité de l'auto-conflit des sources (qui est présente dans le modèle de Rombaut) et par conséquence réduit la masse de conflit après la combinaison des sources. Le modèle Non-antagoniste présente la particularité d'être piloté par un point de transition appelé τ, et qui permet à une source de basculer ses croyances d'une hypothèse à son complément. Ce point de transition est difficile à définir.

4.6 Combinaison des masses

La combinaison de données imparfaites (c.-à-d. données imprécises, incomplètes et incertaines) afin de générer des informations de meilleure qualité a depuis toujours motivé la communauté scientifique pour développer des techniques de fusion de données : la théorie des ensembles flous [78], les réseaux Bayésiens [79], la théorie de croyance [63], etc. Ces techniques visent à investiguer la redondance et la complémentarité des informations pour améliorer la prise de décision et faciliter le processus d'inférence [2].

Dans le contexte de la théorie des croyances, le processus de combinaison est une étape fondamentale représentant le cœur du processus de raisonnement. Ainsi, la théorie de croyance est fondée en grande partie sur les règles de combinaison. Chaque élément de preuve est représenté par une fonction de masse. Des règles de combinaison sont donc utilisées pour fusionner toutes les fonctions de masse afin d'obtenir une fonction de masse significative faisant la synthèse de toutes les preuves disponibles. Ils existent de nombreuses règles de combinaison des masses [80], chacune possède des conditions et contraintes pour pouvoir l'utiliser. Ces contraintes sont reliés à la nature des données utilisées (c.-à-d. données dépendantes ou indépendantes), à la nécessite de gestion de conflit, etc.

Deux fonctions de masse m_1 et m_2 définies sur un même cadre de discernement Ω et dérivées de deux sources d'information distinctes, peuvent être combinées en utilisant les règles de

2. Opération qui consiste à admettre une proposition en raison de son lien avec une proposition préalable tenue pour vraie.

combinaison conjonctives ou disjonctives ou mixtes. Dans ces cas de figure, il est primordial de garantir une indépendance des sources d'informations. Si cette hypothèse ne peut être satisfaite, la règle de combinaison prudente peut être utilisée [69] . Voici les règles de combinaison les plus utilisés.

La règle de combinaison conjonctive Introduit par Smets [81], le résultat de la combinaison conjonctive reflète l'agrégation des informations provenant des sources examinées et produit des fonctions de masse non standard (c.-à-d. $m(\emptyset) \neq 0$.). Formellement, la combinaison conjonctive de deux fonctions de masse m_1 et m_2 indépendantes peut être exprimée par l'équation (4.11) :

$$m_{\textcircled{\cap}}(A) = \sum_{B \bigcap C = A} m_1(B).m_2(C) \tag{4.11}$$

$$m_{\textcircled{\cap}}(\emptyset) = \sum_{B \bigcap C = \emptyset} m_1(B).m_2(C) \tag{4.12}$$

$m(A)$ est le degré de preuve qu'un élément spécifique de Ω appartient à l'ensemble A. Selon la règle conjonctive, il est égal à la somme du produit des preuves soutenant l'hypothèse telle que $A = B \cap C$ avec $m(B)$ et $m(C)$ représentant les croyances issues de différentes sources affirmant la validité de l'hypothèse initiale (c.-à-d. l'hypothèse A). $m(\emptyset)$ représente le degré de conflit entre les sources.

La combinaison conjonctive possède les propriétés suivantes :

— *L'associativité et la commutativité :* $m_1 \textcircled{\cap} m_2 = m_2 \textcircled{\cap} m_1$ et $(m_1 \textcircled{\cap} m_2) \textcircled{\cap} m_3 = m_1 \textcircled{\cap} (m_2 \textcircled{\cap} m_3)$,

— *Non-idempotente :* la combinaison des sources en interaction (c.-à-d. sources dépendantes) est impossible puisque : $m_1 \textcircled{\cap} m_1 \neq m_1$,

— *Un élément neutre :* qui est la masse vide $m(\Omega)$ représentant l'ignorance,

— *Représentation du niveau de conflit :* en cas de combinaison de sources conflictuelles ou

non fiables, une masse non standard est générée, c.-à-d. $m(\emptyset) > 0$.

Illustration de la règle de combinaison conjonctive Supposons deux sources qui expriment leurs croyances sur une trame de discernement $\Omega = \{l, \bar{l}\}$. La combinaison conjonctive est donc calculée selon le tableau 4.2 :

$\textcircled{\cap}$	$m_1(l)$	$m_1(\bar{l})$	$m_1(\Omega)$
$m_2(l)$	$m_1(l) * m_2(l)$	$m_1(\bar{l}) * m_2(l)$	$m_1(\Omega) * m_2(l)$
$m_2(\bar{l})$	$m_1(l) * m_2(\bar{l})$	$m_1(\bar{l}) * m_2(\bar{l})$	$m_1(\Omega) * m_2(\bar{l})$
$m_2(\Omega)$	$m_1(l) * m_2(\Omega)$	$m_1(\bar{l}) * m_2(\Omega)$	$m_1(\Omega) * m_2(\Omega)$

TABLE 4.2 – La règle de combinaison conjonctive

En appliquant l'équation (4.11), les masses sont :

— La masse de l est calculée en faisant la somme des preuves validant l'hypothèse l (cellules rouges),

— La masse de $\bar{l}$ est calculée en faisant la somme des preuves validant l'hypothèse $\bar{l}$ (cellules bleues),

— La masse de conflit est calculée en faisant la somme des preuves en contradiction (cellules vertes),

— La valeur de la dernière cellule représente le niveau d'ignorance des sources (cellule en noir).

La règle de Dempster Connue aussi sous le nom de la somme orthogonale de Dempster, elle est représentée par le symbole $\oplus$. Cette règle normalise la règle conjonctive en masquant le conflit. La combinaison orthogonale de deux masses m_1 et m_2 indépendantes est décrite par l'équation (4.13), d'après [82] :

$$m_{\oplus}(A) = \frac{1}{1-k} \sum_{B \bigcap C = A} m_1(B).m_2(C), m_{\oplus}(\emptyset) = 0 \tag{4.13}$$

$m_{\oplus}(\emptyset)$ correspond à la masse du conflit après combinaison, qui en raison du processus de normalisation est alors égale à 0. k est la masse conflictuelle qui indique le degré de contradiction entre les sources fusionnées et qui est donnée par l'équation (4.14), d'après [82] :

$$m_{\oplus}(\emptyset) = \sum_{B \bigcap C = \emptyset} m_1(B).m_2(C). \tag{4.14}$$

Si les sources sont complètement en désaccord (conflit total entre les sources), ce qui implique que $k = 1$, la combinaison est alors impossible.

La combinaison orthogonale possède les propriétés suivantes :

— *L'associativité et la commutativité :* $m_1 \oplus m_2 = m_2 \oplus m_1$ et $(m_1 \oplus m_2) \oplus m_3 = m_1 \oplus (m_2 \oplus m_3)$,

— *Non idempotente :* la combinaison des sources en interaction (c.-à-d. : sources dépendantes) est impossible puisque : $m_1 \oplus m_1 \neq m_1$,

— *Un élément neutre :* la masse de l'ignorance *m(Ω)*.

Illustration de la règle de combinaison orthogonale Pour appliquer la règle orthogonale, il faut passer par les mêmes étapes illustrées dans le tableau 4.2. Cependant la masse de conflit est distribuée sur les autres masses comme décrit dans l'équation (4.13). Les masses normalisées sont donc calculées par :

$$m(l) = \frac{\sum_{A \cap B = l \neq \emptyset} m_1(A).m_2(B)}{1 - \sum m_{\emptyset}} \tag{4.15}$$

$$m(l) = \frac{\sum_{A \cap B = \bar{l} \neq \emptyset} m_1(A).m_2(B)}{1 - \sum m_{\emptyset}} \tag{4.16}$$

La règle de combinaison prudente Les règles de combinaison présentées ci-dessus exigent l'indépendance des sources qui fournissent les informations. Toutefois, dans certaines situations,

les sources ne peuvent pas être traitées comme indépendantes, par exemple, lorsque les experts partagent des informations (c.-à-d. les opinions de différents experts fondées sur des expériences qui se chevauchent ne peuvent être considérées comme des sources indépendantes). Par conséquent, il y a un grand besoin de règles de combinaison tolérant la dépendance d'une information combinée. Dans ce contexte, parmi les différentes règles proposées, une règle de combinaison a été introduite par Denoeux [69]. Elle permet de combiner deux fonctions de croyance m_1 et m_2 définies sur le même cadre de discernement et provenant de deux sources dépendantes. La règle prudente est représentée par l'équation (4.17).

$$m_{1\wedge 2}(A) = (m_1 \wedge m_2)(A). \tag{4.17}$$

Où $\wedge$ représente l'opérateur minimum.

Le calcul de la combinaison prudente de deux masses m_1 et m_2 se fait en trois étapes :

— *Calcul des fonctions de communalité :* la fonction de communalité q associée à une fonction de masse m est calculée en utilisant l'équation (4.18) :

$$q(A) = \sum_{B \supseteq A} m(B), A, B \subset \Omega \tag{4.18}$$

— *Calcul des fonctions de poids :* la fonction de poids w associée à m est calculée en se basant sur l'équation (4.19) :

$$w(A) = \begin{cases} \frac{\prod_{B\supseteq A, |B| \notin 2N} q(B)}{\prod_{B\supseteq A, |B| \in 2N} q(B)}, si |A| \in 2N \\ \frac{\prod_{B\supseteq A, |B| \in 2N} q(B)}{\prod_{B\supseteq A, |B| \notin 2N} q(B)}, sinon, \end{cases} \tag{4.19}$$

Où, $|A|$ et $|B|$ sont les cardinalités des deux propositions A et B. 2N est l'ensemble des nombres pairs naturels. Cette équation est détaillée dans le tableau 4.3, agrémenté

d'exemples.

— *Calcul de $m_1 \wedge m_2$:* calcul du résultat de la combinaison à partir de l'équation (4.20) :

$$(m_1 \wedge m_2)(A) = \bigcirc_{A \subset \Omega} A^{w_1(A) \wedge w_2(A)} \tag{4.20}$$

Comme les autres opérateurs de combinaison la règle prudente possède plusieurs propriétés :

— *L'associativité et la commutativité :* $m_1 \wedge m_2 = m_2 \wedge m_1$ et $(m_1 \wedge m_2) \wedge m_3 = m_1 \wedge (m_2 \wedge m_3)$

— *Idempotente :* : $m_1 \wedge m_1 = m_1$.

— *Un élément neutre :* la masse de l'ignorance *m(Ω)*.

Illustration de la règle prudente Supposons deux sources m_1 et m_2 qui expriment leurs croyances sur la trame de discernement Ω={ l,$\bar{l}$ }. La combinaison prudente est donc calculée selon le tableau 4.3 :

m_1	q_1	w_1	m_2	q_2	w_2	$w_1 \wedge w_2$	$m_1 \wedge m_2$
$m(\emptyset)$	1	1	$\emptyset$	1	1	1	$(1-(w_1 \wedge w_2)_l)*$ $(1-(w_1 \wedge w_2)_{\bar{l}})$
$m_1(l)$	$m_1(l)+m_1(\Omega)$	$\frac{q_1(\Omega)}{q_1(l)}$	$m_2(l)$	$m_2(l)+m_2(\Omega)$	$\frac{q_2(\Omega)}{q_2(l)}$	$min(w_1,w_2)_l$	$(1-(w_1 \wedge w_2)_l)*$ $(w_1 \wedge w_2)_{\bar{l}}$
$m_1(\bar{l})$	$m_1(\bar{l})+m_1(\Omega)$	$\frac{q_1(\Omega)}{q_1(\bar{l})}$	$m_2(\bar{l})$	$m_2(\bar{l})+m_2(\Omega)$	$\frac{q_2(\Omega)}{q_2(\bar{l})}$	$min(w_1,w_2)_{\bar{l}}$	$(1-(w_1 \wedge w_2)_{\bar{l}})*$ $(w_1 \wedge w_2)_l$
$m_1(\Omega)$	$m_1(\Omega)$		$m_2(\Omega)$	$m_2(\Omega)$			$(w_1 \wedge w_2)_l * (w_1 \wedge w_2)_{\bar{l}}$

TABLE 4.3 – Illustration de la combinaison prudente

En utilisant l'équation (4.18) pour les communalités (deuxième et cinquième colonnes du tableau) :

— Pour les masses non vides (c.-à-d. $m_1(l)$, $m_1(\bar{l})$, $m_2(l)$, $m_2(\bar{l})$), la communalité est calculée en ajoutant la masse de l'ignorance à la masse non vide, par exemple : $q_1(l)=m_1(l)+m_1(\Omega)$,

— Pour les masses de l'ignorance (c.-à-d. $m_1(\Omega)$ et $m_2(\Omega)$) la communalité est égale à la masse de l'ignorance, par exemple : $q_1(\Omega)=m_1(\Omega)$

En utilisant l'équation (4.19) pour les poids (troisième et sixième colonnes du tableau) :

— Pour les masses non vides (c.-à-d. $m_1(l)$, $m_1(\bar{l})$, $m_2(l)$, $m_2(\bar{l})$), les poids sont calculés par fractionnement de la communalité de l'ignorance (c.-à-d. $q(\Omega)$) par la communalité de la masse pour laquelle le poids est calculé, par exemple : $w_1(l)=\frac{q_1(\Omega)}{q_1(l)}$,

— Pour les masses de l'ignorance (c.-à-d. $m_1(\Omega)$ et $m_2(\Omega)$), le poids n'est pas calculé puisque la fonction des poids s'applique à chaque élément $A \in 2^{\Omega}\ \{\ \Omega\ \}$

Pour calculer la septième colonne le minimum entre les poids calculés pour chaque ligne est choisi.

En utilisant l'équation (4.20) pour calculer le résultat final de la dernière colonne. Chaque ligne représente de résultat de la combinaison conjonctive des $A^{w_1(A)\wedge w_2(A)}$.

Application numérique En reprenant l'exemple de diagnostic de maladies, considérons la répartition suivante des masses sur le cadre de discernement $\Omega=\{\ A_1\ ,\ A_2\ \}$:

— **Les masses selon la source 1 (médecin 1) :**
$m_1(A_1) = 0.25$
$m_1(A_2) = 0.6$
$m_1(\Omega) = 0.15$

— **Les masses selon la source 2 (médecin 2) :**
$m_2(A_1) = 0.4$
$m_2(A_2) = 0.43$
$m_2(\Omega) = 0.17$

Supposons que nos sources sont indépendantes, le résultat de combinaison des masses selon les deux règles orthogonale et conjonctive sont représentés dans le tableau 4.4 :

	Combinaison Conjonctive	Combinaison Orthogonale
$m(A_1)$	0,20	0,31
$m(A_2)$	0,42	0,65
$m(\Omega)$	0,03	0,04
$m(\emptyset)$	0,35	0

TABLE 4.4 – Résultat de combinaison selon les deux règles conjonctive et orthogonal

Supposons maintenant que nos sources partagent certaines informations ou possèdent un niveau de dépendance. Le résultat de combinaison selon la règle prudente est le suivant :

$m(A_1)$=0.14

$m(A_2)$=0.24

$m(\Omega)$=0.06

$m(\emptyset)$=0.56

Le résultat de combinaison donné par la règle conjonctive considère l'hypothèse A_1 comme la peu probable et favorise la deuxième hypothèse (A_2) mais produit aussi une masse de conflit représentant le degré de discorde entre les sources. D'une autre part, la combinaison Orthogonale impose une normalisation des masses qui fait converger le résultat vers l'hypothèse la plus défendue par les deux fonctions de masse (A_2).

Quant à la combinaison prudente, elle aussi favorise l'hypothèse A_2 par rapport à l'hypothèse A_1. Les trois règles favorisent l'hypothèse la plus défendue par les sources.

Comme mentionné précédemment, le choix de la règle de combinaison dépend de plusieurs facteurs qui sont : le type des données, le type du système et d'autres paramètres. D'une part, le besoin de gestion du conflit dans un système nécessite l'utilisation d'une règle de combinaison normalisée comme la règle de combinaison orthogonale. D'autre part, la dépendance entre les sources de données impose l'utilisation d'une règle supportant les sources dépendantes.

4.7 La prise de décision

La combinaison des différentes preuves produit des masses qui prennent en compte toutes les informations disponibles. L'étape suivante consiste à décider quelle hypothèse répond à la

question posée. Pour ce faire, plusieurs critères de décision peuvent être utilisés. Dans la suite, deux exemples de critères de décision sont présentés :

Le maximum de plausibilité La plausibilité d'un élément A ⊆ Ω, correspond à la partie de la croyance qui pourrait être attribuée à A et est définie par la fonction (4.21) :

$$Pl(A) = \sum_{B \cap A \neq \emptyset} m(B) \tag{4.21}$$

La plausibilité prend en compte toute la masse qui peut éventuellement être accordée à un état (c.-à-d. hypothèse). La plausibilité d'un état reflète donc le degré de possibilité de cet état. Ce critère est considéré comme trop optimiste, puisque en cas d'une masse $m(\Omega)$=1, la plausibilité de chaque $A \subseteq \Omega$ est égale à 1 ($Pl(A) = 1$). Ce qui n'aide pas à la décision.

Le maximum de crédibilité La fonction de crédibilité quantifie la croyance totale en A ⊆ Ω (c.-à-d. la partie de la croyance qui est attribuée à A) et est définie sur le cadre de discernement Ω par la fonction (4.22) :

$$Cr(A) = \sum_{\emptyset \neq B \subseteq A} m(B) \tag{4.22}$$

Dans le cas de la sélection entre des hypothèses de singletons, cela revient au choix de l'hypothèse avec la masse maximale, puisque la crédibilité d'une hypothèse singleton est égale à sa masse (c.-à-d. $Cr(A) = m(A)$ si |A|=1). La crédibilité reflète donc en quelque sorte le degré de certitude du système. De fait, elle ne considère que la masse directement associée à un élément focal et à ses sous-ensembles. Le critère de maximum de crédibilité a été choisi comme critère de décision dans cette thèse.

Exemple Reprenons l'exemple de la diagnostic de maladie. La décision du médecin basée sur les masses fournies par la combinaison prudente et selon les différents critères expliqués au-dessus se résume dans les points suivants :

-Décision selon les critère de maximum de la plausibilité

$Pl(A_1)=m(A_1)+ m(\Omega)=0.14+0.56=0.7$

$Pl(A_2)=m(A_2)+ m(\Omega)=0.24+0.56=0.8$

Le résultat de diagnostic de maladie selon le critère de maximum de plausibilité est la maladie A_2.

-Décision selon les critère de maximum de la crédibilité

$Cr(A_1)=m(A_1)=0.14$

$Cr(A_2)=m(A_2)=0.24$

Le résultat de diagnostic de maladie selon le critère de maximum de crédibilité est la maladie A_2.

4.8 Conclusion

Dans ce chapitre, les notions fondamentales de la théorie des fonctions de croyance ont été présentées. La théorie des fonctions de croyance a pour objectif de gérer tous types d'imperfections de données, y compris les conflits. Elle permet également la représentation de l'incertitude comme ignorance partielle ou totale. Les fonctions de croyance autorisent les sources à produire des informations à divers niveaux de précision en manipulant des sous-ensembles plutôt que des singletons. Ces avantages rendent cette théorie un des outils performant de présentation et de combinaison des données et de prise de décision.

Chapitre 5

Détection de rupture de lien dans les VANET

Sommaire

5.1 Introduction

La problématique principale des VANET est la connectivité entre les nœuds. En raison de changements réguliers de topologie, d'une densité variable de nœuds et de fluctuations du canal de transmission, les réseaux véhiculaires connaissent des fréquentes ruptures de liens. Ainsi, un des challenges dans les VANET est d'anticiper les ruptures des liens. Le canal de transmission VANET subit des fluctuations causées par l'environnement à l'entour. Cette volatilité rend difficile la tâche de prédiction de rupture des liens. Ce chapitre correspond à la première contribution de cette thèse et a fait l'objet d'une publication dans la revue *"Wireless Networks"*. La contribution est la conception d'un indicateur de rupture de lien pour les réseaux véhiculaires. L'indicateur proposé est appelé LBFI pour *Link Breakage Forecasting Indicator*. L'objectif est de prédire la rupture de lien avec un temps utile qui permet au protocole de routage de prendre une décision. Cet indicateur est mesuré du côté récepteur et exploite à la fois les paquets bien décodés et les paquets non décodés. L'indicateur repose sur des événements de décodage OFDM (*Orthogonal Frequency Division Multiplexing*) et utilise le mécanisme de fusion de données connu sous le nom de la théorie de Dempster-Shafer pour prévoir les ruptures.

Ce chapitre est organisé en quatre grandes parties. La première présente une analyse détaillée de deux indicateurs de rupture des liens conçus pour les VANET qui se basent aussi sur d'erreurs de décodage des trames OFDM. La deuxième partie introduit le nouvel indicateur (LBFI).

La troisième partie présente l'environnement de simulation utilisé pour évaluer LBFI. Dans la dernière partie du chapitre les paramètres des simulations ainsi que les résultats sont décrits.

5.2 Indicateurs de détection de rupture de lien basés sur les erreurs de décodage OFDM

Avant de présenter notre indicateur de rupture de lien, nous présentons dans cette section une analyse des deux indicateurs de rupture de lien publiés et conçus pour les VANET qui utilisent les erreurs de décodage OFDM pour prévoir les ruptures. Le premier indicateur [46] est empirique, le deuxième utilise un outil mathématique (DST) pour fusionner les erreurs et prédire la rupture [3].

5.2.1 Prédiction de la rupture d'un lien par une approche empirique

Un indicateur de rupture de lien appelé *LSFI* (*Link State Forecasting Indicator*) est proposé dans [46]. Afin de prédire une rupture de lien, une analyse quantitative et qualitative d'erreurs de décodage des paquets est effectuée [46]. Les erreurs de décodage sont stockées dans une file d'attente temporaire, circulaire de type FIFO et de taille fixe. Puis, à partir des observations du contenu de cette file d'attente, quatre métriques sont construites :

La somme maximale d'erreurs EDP et EDD ***($Max_{EDP+EDD}$)*** Cette métrique est utilisée pour détecter la première perte d'un paquet au niveau réseau. Le résultat de cette métrique peut être l'un des trois états suivants : (i) l'état de lien est connecté, si $Max_{EDP+EDD} = 0$. (ii) l'état de lien est transitoire, si $0 < Max_{EDP+EDD} < 7$. (iii) l'état de lien est déconnecté si $Max_{EDP+EDD} \geq 7$.

La différence entre le nombre des EDP et EDD ***($EDP - EDD$)*** Selon [46], lorsqu'un lien se dégrade, les erreurs de décodage de préambule deviennent plus importantes en terme de quantité que les erreurs de décodage des données.

La fluctuation Cette métrique présente la vitesse de fluctuation du lien. La fluctuation est calculée ainsi : le nombre d'alternance entre les erreurs de tout type et RxOk [1] est divisé par la durée d'observation. Cette métrique peut donner l'une des deux indications suivantes : (i) le lien est stable, si $fluctuation = 0$. (ii) le lien est fluctuant, si $fluctuation \,!= 0$.

La fiabilité de la couche physique Cette métrique calcule le nombre des RxOk consécutives dans la FIFO. Le résultat de la métrique peut être : (i) le lien est fiable, si $\sum_{FIFO} RxOk \geq 3$. (ii) le lien n'est pas fiable, si $\sum_{FIFO} RxOk < 3$.

Les métriques décrites au-dessus sont combinées selon des formules logiques pour déduire l'état de lien, celui peut être connecté, transitoire ou déconnecté.

Un bon indicateur de rupture de lien doit non seulement être capable de détecter les ruptures de lien mais ne doit pas non plus produire des fausses détections (c.-à-d. une indication de rupture alors qu'il y a pas de vraie rupture) ni de cas ratés (c-à-d : détection tardive d'une rupture). L'indicateur présenté dans [46] souffre des temps de prédiction fluctuants. Selon la figure 5.1 ces

1. C'est l'événement associé au bon décodage d'un paquet au niveau physique (décodage sans erreur).

temps peuvent atteindre jusqu'à 18 secondes, de plus le nombre de faux positifs [2] est élevé. Les auteurs ont testé l'indicateur sur un ensemble de 550 scénarios, le nombre de fausses détection ainsi que les cas ratés sont présentés dans le tableau 5.1. La détection fournie par *LSFI* résulte de l'ensemble des métriques que nous avons mentionné ci-dessus. Ces métriques sont incapables d'identifier l'état du lien.

D'abord, l'hypothèse affirmant que les erreurs de décodage de préambule deviennent plus importantes en terme de quantité lorsque le lien se dégrade n'est pas valable dans tous les cas. En effet, une étude effectuée montre que dans certains cas (scénarios) les erreurs de décodage de données sont les erreurs dominantes lorsque le lien se dégrade. De plus, la métrique de fluctuation calculée au niveau physique permet de décrire une fluctuation du lien mais pas une déconnexion. Enfin, la métrique de fiabilité de la couche physique se base sur une quantification des *RxOk* consécutives, cette métrique ne peut pas décrire la fiabilité de la couche physique comme le canal de transmission VANET est très fluctuant et que son état change rapidement.

Nombre de scénarios	Fausses détections	Cas ratés
550	166	5

TABLE 5.1 – Nombre de fausses détections et de cas raté pour LSFI [2]

5.2.2 Prédiction de la rupture d'un lien par la théorie des croyances

Les auteurs de [3] ont abordé le problème de la détection de rupture de lien dans les réseaux véhiculaires. Pour cela et de la même manière que LSFI, ils ont utilisé les erreurs de décodage OFDM, les EDP et les EDD pour construire leur indicateur appelé LSFI-BF (*Link State Forecasting Indicator based on Belief Functions*). LSFI-BF utilise la théorie de croyance [63] pour fusionner deux sources de donnée (c.-à-d. erreur de décodage de préambule et de donnée EDP et EDD) afin de calculer une probabilité de rupture d'un lien entre deux véhicules. L'estimation des fonctions de masses est faite en utilisant le modèle de masse de Rombaut (expliqué dans la section 4.5.4, du chapitre 4). Comme représenté dans la Figure 5.2 les fonctions de masse des deux sources d'EDP et EDD sont exprimées sur la trame de discernement $\Omega = \{Comloss, \overline{Comloss}\}$ où *Comloss* et $\overline{Comloss}$ sont les convictions que le lien respectivement va rompre ou non. Chaque

2. fausses détections

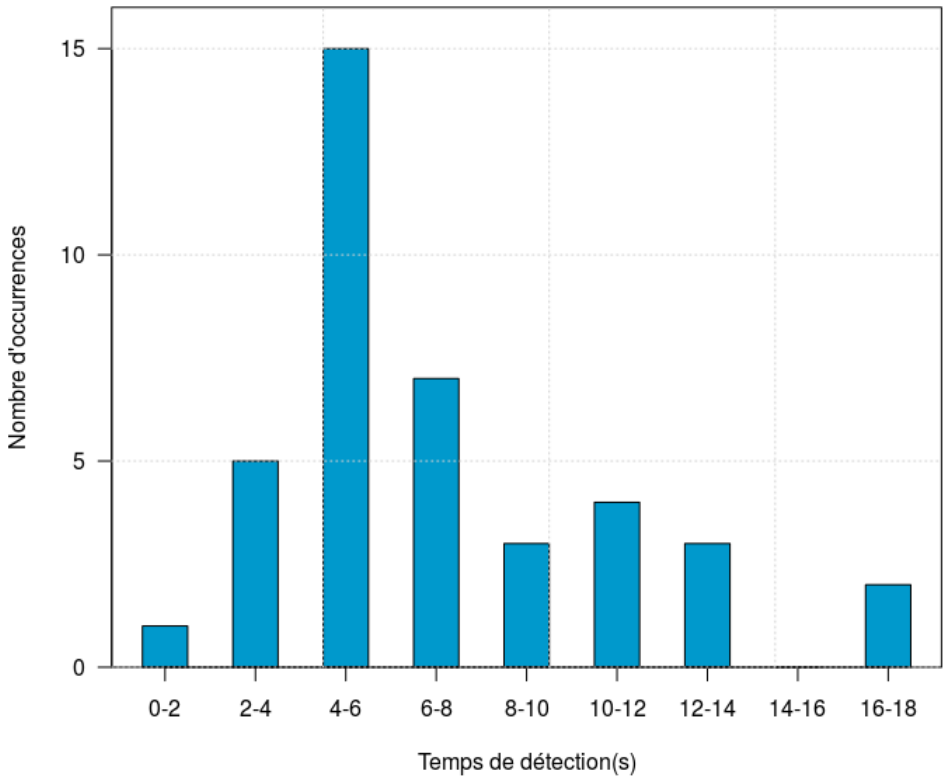


FIGURE 5.1 – Temps de prédiction pour LSFI [2]

source exprime un degré de croyance dans les deux hypothèses *Comloss*, $\overline{Comloss}$ en même temps.

Le modèle de masse utilisé dans [3] est présenté dans la figure 5.2. Il donne une estimation de l'état d'un lien selon le nombre d'erreurs consécutives. Comme expliqué dans la section précédente, la couche MAC peut retransmettre un paquet jusqu'à sept fois (selon le standard IEEE 802.11). L'évolution des masses d'EDP et EDD varie selon le nombre d'erreurs instantanées. Cela signifie que l'indicateur est calculé à l'apparition de chaque erreur de décodage, sans tenir compte de l'état du lien calculé précédemment. L'indicateur déclenche immédiatement une alerte de rupture de lien dès que le nombre d'EDP ≥ 1 et le EDD ≥ 2.

D'autre part, les fonctions de masse utilisées favorisent le conflit entre les sources. En effet, l'attribution de deux masses opposées (*Comloss* et $\overline{Comloss}$) à chaque source rend la source contradictoire avec elle-même et donc engendre une masse conflictuelle importante après combinaison. La figure 5.3 montre la masse conflictuelle résultante des différentes combinaisons

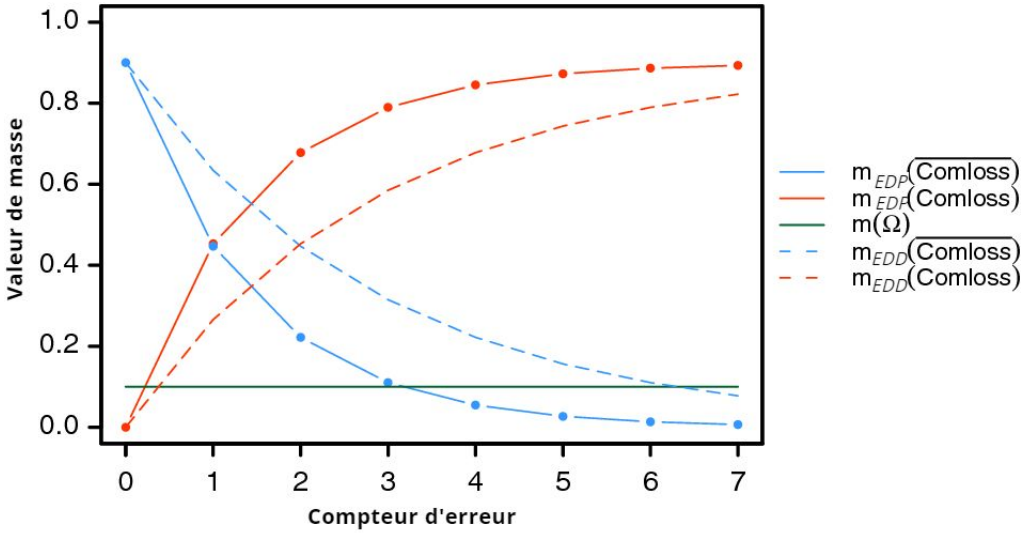


FIGURE 5.2 – Modèle de Rombaut [3]

possible des deux source EDP et EDD selon le modèle de LSFI-BF. Ainsi, même si les deux sources EDD et EDP sont en accord (c.-à-d. les deux sources ont la même vision à propos de l'état d'un lien), le conflit demeure important.

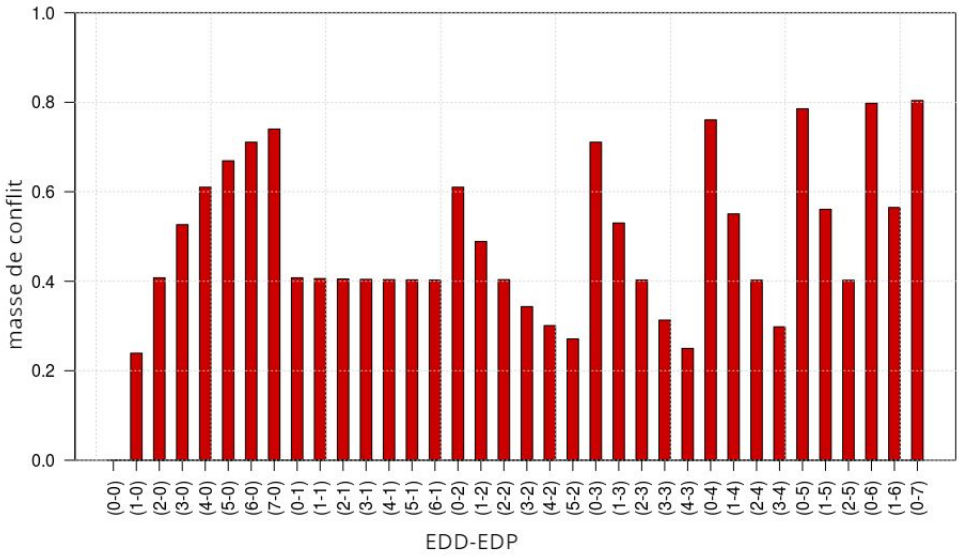


FIGURE 5.3 – Masse de conflit en fonction des couples (EDD-EDP)

LSFI-BF souffre aussi de temps de détection longs, surtout lorsque la vitesse des véhicules est inférieure à 9 m/s. Comme le montre la figure 5.4 ses performances sont fortement influencées

par la vitesse des véhicules. Plus la vitesse est faible, plus le temps de détection est long et variable. Les temps de détection ne dépassent pas quatre secondes pour des vitesses supérieures à 9 m/s, alors que les temps de détection pour des vitesses inférieures à 9 m/s sont variables et peuvent atteindre 20 secondes.

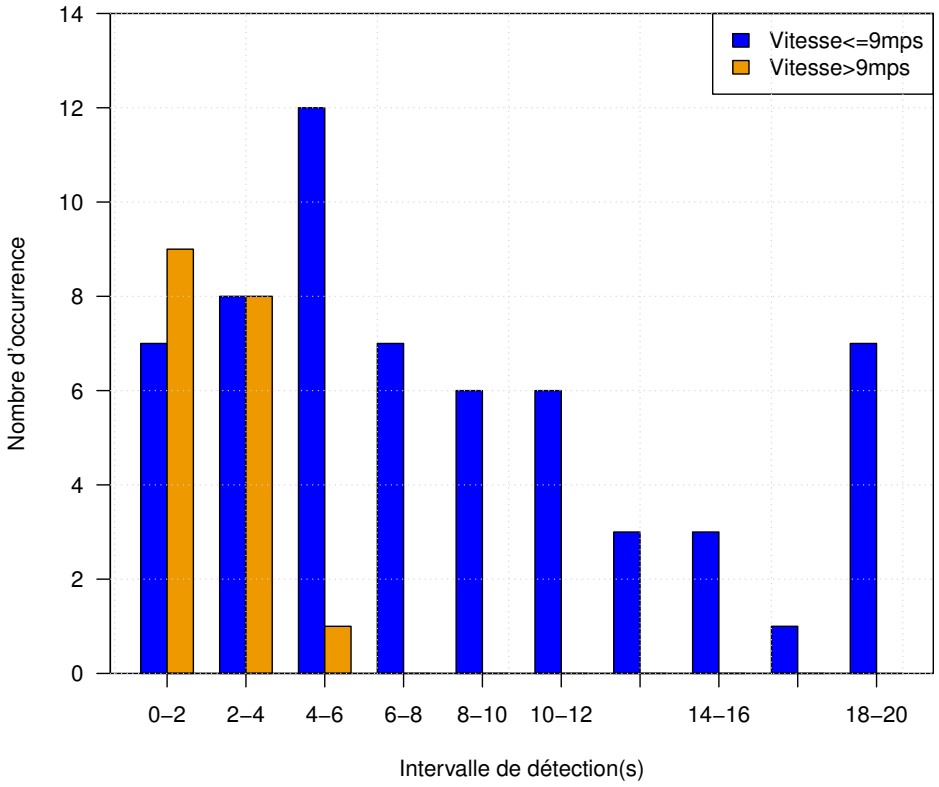


FIGURE 5.4 – Distribution des temps de détection du LSFI-BF dans une situation d'éloignement de deux véhicules

La principale raison de ces importantes variations des temps de détection peut être déduite du modèle de masse qui a été utilisé (figure 5.2). Dès que le couple d'erreurs (EDD, EDP) atteint une condition spécifique, nombre d'EDD cumulé ≥ 2 et nombre d'EDP cumulé ≥ 1 (figure 5.5), LSFI-BF indique une rupture de lien. Nous appelons un tel couple qui vérifie la condition précédente un couple d'erreurs de détection ou DEC pour *Detection Error Couple*. Cela signifie que la raison principale des temps de détections longs, des fausses détections [3] et des détections

3. Une fausse détection est une indication de rupture de lien sans vraie rupture.

manquées [4] est l'apparition trop tôt ou trop tardive d'un DEC.

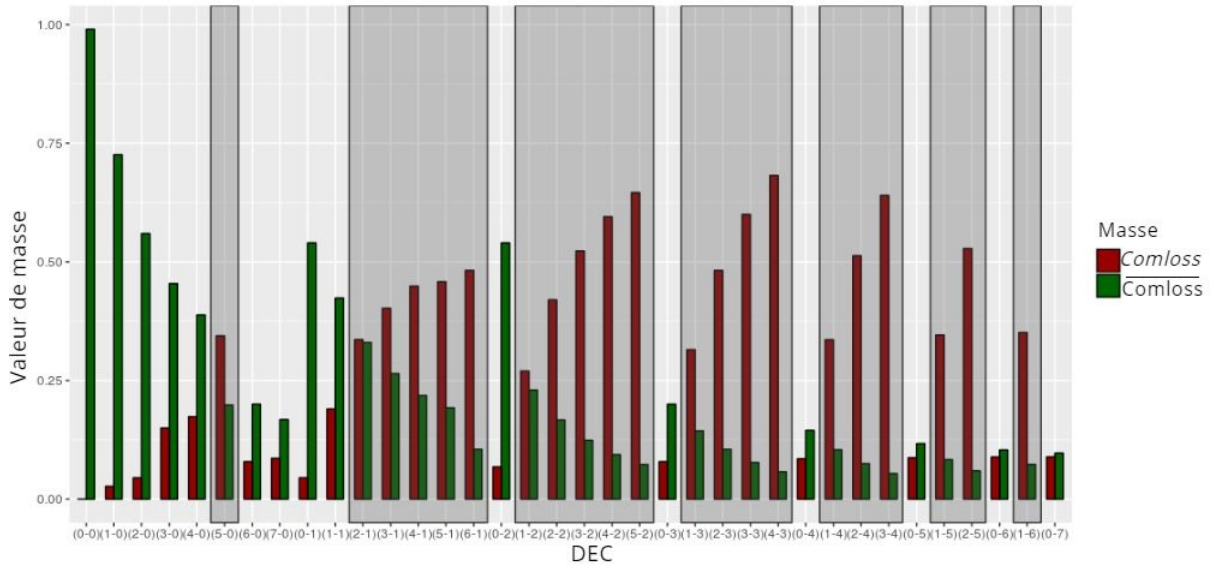


FIGURE 5.5 – Comportement des masses selon les valeurs du couple DEC. Les zones en gris montrent les masses de $\overline{Comloss}$ et de $Comloss$ pour les couples d'erreurs DEC.

5.2.3 Synthèse

Les analyses précédentes peuvent être résumées dans les trois points suivants :

A. L'indicateur LSFI-BF ne repose que sur une observation instantanée d'erreurs de décodage sans prendre en compte ni des informations supplémentaires ni l'historique des liens de communication (c.-à-d. la densité d'erreurs de décodage). Ceci n'est pas suffisant pour détecter une rupture de lien dans un canal de propagation très fluctuant comme celui d'un réseau VANET où l'état du lien peut passer du mauvais à bon et vice versa en un temps très court,

B. Les fonctions de masse utilisées dans [3] introduisent du conflit entre les sources. Elles affectent des masses opposées ($Comloss$ et $\overline{Comloss}$) à chaque source en même temps, ce qui rend une source contradictoire avec elle-même et augmente le conflit après la combinaison. Ainsi, même si le couple d'erreurs est un DEC, le conflit sera important et rendra difficile la prise de décision,

4. Une détection manquée est une détection tardive de rupture de lien.

C. Un autre point important est la règle de combinaison utilisée pour fusionner les informations. Le choix de la combinaison conjonctive pour la fusion des masses n'est pas approprié dans un système où il existe une relation entre les sources. Le choix de la combinaison sera discuté et justifié dans les sections suivantes.

Dans le but de résoudre le problème de prédiction de rupture de lien dans les VANET, un modèle de masse basé sur plusieurs facteurs est proposé dans cette thèse. Pour mettre en place un indicateur performant, le facteur du temps est un élément à prendre en compte. La densité d'erreurs de décodage dans le temps est également calculée pour calibrer les fonctions de masse. Les données suivantes sont prises en compte pour construire le nouvel indicateur appelé *Link Breakage Forecasting Indicator* (LBFI) :

Les erreurs de décodage OFDM Comme expliqué plus haut compte tenu de la répartition d'erreurs, il a été décidé d'utiliser les erreurs de décodage du préambule (EDP) et de décodage des données (EDD).

La densité d'erreurs Cette mesure permet d'estimer la quantité d'erreurs survenues pendant un temps donné sur un lien de communication. Elle permet d'analyser l'historique de l'état du lien.

La vitesse L'analyse des profils d'erreurs de décodage OFDM révèle que la vitesse relative de déplacement des nœuds influe sur la quantité d'erreurs ainsi que sur leurs séquences d'arrivée et sur le nombre maximal d'erreurs consécutives avant une rupture de lien. Plus la vitesse est faible, plus la quantité et le nombre d'erreurs consécutives avant rupture sont importants. La vitesse relative entre les véhicules est prise en compte dans l'indicateur LBFI afin d'améliorer la précision de détection. Un exemple est illustré dans les figures 5.6 et 5.7. La figure 5.6 correspond à un scénario d'éloignement de deux véhicules avec une vitesse relative de $13ms^{-1}$. La figure 5.7 correspond à un scénario d'éloignement de deux véhicules avec une vitesse relative de $5ms^{-1}$. La quantité d'erreurs de décodage EDD et EDP varie d'un scénario à un autre ainsi que leur ordre et temps d'arrivée. Prenons l'exemple du scénario (a), la première erreur qui apparaît est une erreur de décodage des données EDD tandis que, dans le scénario (b) la première erreur de décodage qui apparaît est une erreur de décodage de préambule EDP. On peut remarquer

aussi que pour le scénario (a) l'erreur dominante est l'erreur *EDD* à l'inverse du scénario (b) ou l'erreur dominante c'est *EDP*.

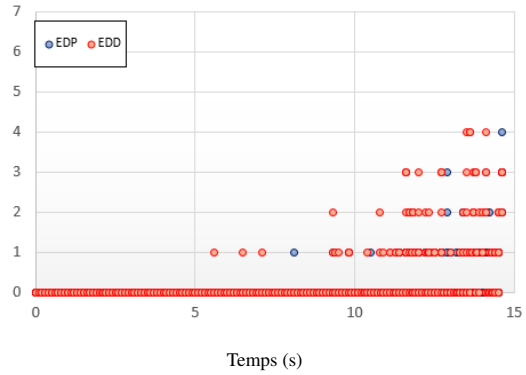


FIGURE 5.6 – scénario (a)

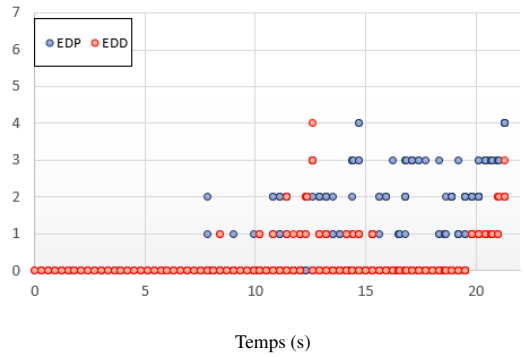


FIGURE 5.7 – scénario (b)

La puissance de réception du signal reçu (*Received Signal Strength Indication* - RSSI) Cette puissance fournit des informations sur l'intensité du signal reçu. Dans les VANET, le RSSI est impacté à la fois par la mobilité des nœuds et par l'environnement. Bien qu'utilisée par certains indicateurs, cette puissance de réception n'est pas suffisante pour anticiper la rupture d'un lien, mais constitue néanmoins une information pertinente.

Les erreurs de décodage OFDM décrites dans le chapitre 4 (c.-à-d. *EDP* et *EDD*) sont des sources de données imparfaites. Tout d'abord, la perte d'un paquet peut être causée par d'autres types d'erreurs, cela révèle l'aspect d'incomplétude de l'information fournie par les deux sources *EDP* et *EDD*. En outre, l'information fournie par chaque source sur l'état d'un lien n'est pas exacte, vu que les deux sources peuvent entrer en conflit. Par exemple dans le cas où une source affirme que le lien risque de se rompre alors que l'autre source affirme l'inverse. Un exemple concret est : un nombre de *EDD* égal à 6 et un nombre de *EDP* égal à 0. La nature imparfaite des sources de données impose l'utilisation d'un mécanisme de fusion de données imparfaites. La théorie des fonctions de croyance permet de manipuler et de traiter tout type d'incomplétude des informations fournies par des sources afin de générer une information plus précise et plus fiable.

Dans la section suivante, un nouvel indicateur de rupture de lien basé sur la théorie de croyance est présenté. L'indicateur utilise la théorie de croyance pour la fusion d'erreurs de décodage OFDM dans le but de prédire les ruptures des liens dans les réseaux VANET.

5.3 Un indicateur de rupture de lien dédié aux VANET

Afin de palier des inconvénients induits par l'utilisation du modèle de masse de Rombaut, un nouveau modèle de masse est proposé dans cette thèse (modèle de masse non antagoniste décrit dans le chapitre 4). Chaque source croit en un seul état à la fois (*Comloss* ou $\overline{Comloss}$). Cette croyance peut être absolue (masse = 1) ou partielle. Dans ce cas, le reste de la croyance est attribué à la troisième proposition qui est l'ignorance. De plus, l'évolution des masses ne repose pas seulement sur le nombre d'erreurs générées, mais aussi sur la valeur d'un point de transition appelée τ. Ainsi le cadre de discernement est définit par : Ω= $\{Comloss, \overline{Comloss}\}$.

5.3.1 Mise en œuvre de fonctions de masse non antagonistes :

Les fonctions de masse pour chaque erreur de décodage (*ED*) sont définies à l'aide du modèle non antagoniste et formalisées par les équations suivantes. Comme le nombre total de retransmissions avant l'abandon d'une trame par la couche MAC est de 7, ce chiffre est la borne supérieure de l'indice de confiance (I_c) de la proposition.

$$m_{ED}(Comloss) = \begin{cases} 0 & I_c \in [0, \tau] \\ \Phi_1(\alpha, I_c) & I_c \in [\tau, 7] \end{cases} \tag{5.1}$$

$$m_{ED}(\overline{Comloss}) = \begin{cases} \Phi_2(\alpha, I_c) & I_c \in [0, \tau] \\ 0 & I_c \in [\tau, 7] \end{cases} \tag{5.2}$$

$$m_{ED}(\Omega) = \begin{cases} 1 - \Phi_2(\alpha, I_c) & I_c \in [0, \tau] \\ 1 - \Phi_1(\alpha, I_c) & I_c \in [\tau, 7] \end{cases} \tag{5.3}$$

— I_c correspond à l'indice de confiance de la proposition $\in$ [0,7] ;

— α est le coefficient de fiabilité des sources EDD et EDP. Dans ce travail, α a la valeur 0.9 (on estime que les sources ne sont pas fiables à 100%),

— $\tau \in$ [0,7] est le point de transition entre *Comloss* et $\overline{Comloss}$.

La figure 5.8, illustre les nouvelles fonctions de masse utilisées pour l'erreur de décodage de préambule (EDP) et l'erreur de décodage de données (EDD). A tout moment, chaque source croit en un seul état (Comloss ou $\overline{Comloss}$). Cette croyance peut être absolue ou partielle. Dans ce cas, le reste de la croyance est attribué à la troisième proposition qui est l'ignorance. De plus, la probabilité de déconnexion ne dépend plus seulement du nombre cumulé d'erreurs de décodage successives, mais aussi de la valeur de τ.

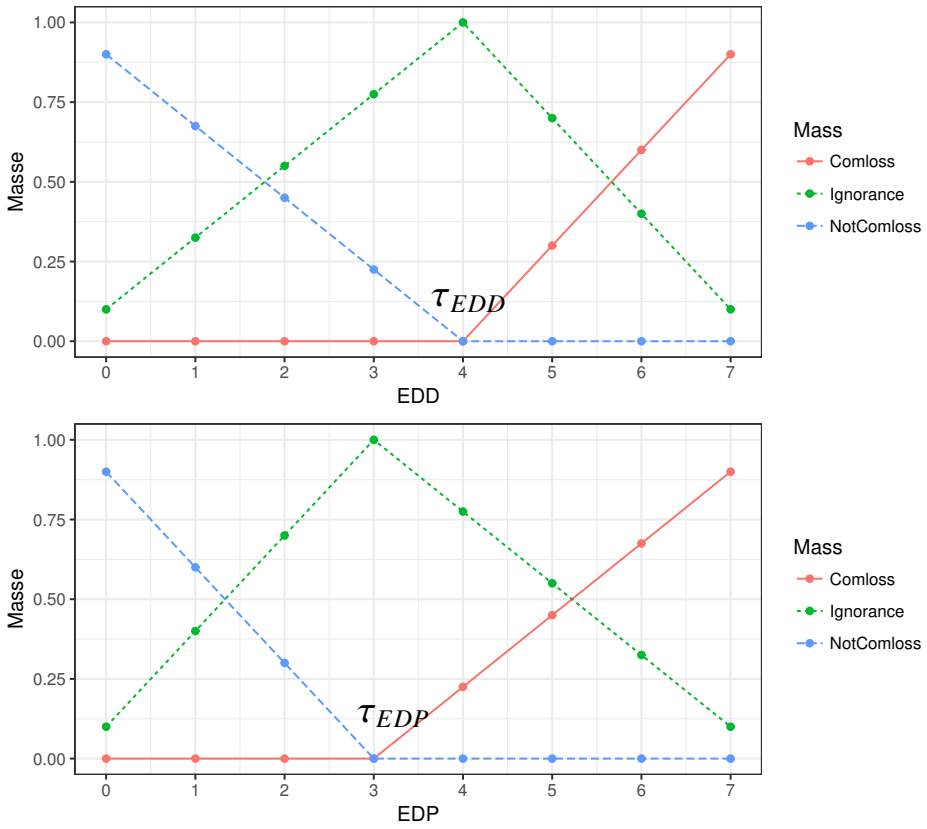


FIGURE 5.8 – Fonctions de masse non antagonistes utilisées pour le calcul de LBFI

Deux valeurs sont calculées pour τ (τ_{EDD} pour la source EDD et τ_{EDP} pour la source EDP). En effet, l'évolution de la quantité d'erreurs consécutives au cours d'une communication n'est pas identique. Le tableau 5.2 montre le nombre maximal d'erreurs EDP et EDD successives avant la première perte d'un paquet au niveau de la couche réseau. Cela a mené à choisir deux valeurs différentes pour τ. À noter que les valeurs du tableau 5.2 sont obtenues à partir d'une analyse des scénarios d'éloignement et de suivi de véhicules à différentes vitesses et distances. Ces valeurs

sont utilisées comme valeurs initiales pour les deux points de transition τ_{EDD} et τ_{EDP}.

Erreur	$Max_{ErreursConscutives}$
EDP	4
EDD	3

TABLE 5.2 – Nombre maximal des EDP et EDD consécutives avant la rupture d'un lien

Afin de garantir une détection plus précise, τ est rendu adaptable aux conditions de lien en exploitant trois informations supplémentaires : la vitesse relative (V) entre véhicules communicants, la densité (D) des paquets non décodés dans une file temporelle et leur puissance de réception (RSSI).

Comme présenté dans la figure 5.8, l'ignorance sur l'état du lien est minimale lorsque $Comloss$ et $\overline{Comloss}$ fournissent une information claire (c'est-à-dire une valeur minimale pour l'un et une valeur maximale pour l'autre). De plus, quand $Comloss$ et $\overline{Comloss}$ se trouvent dans des zones d'incertitude (c'est-à-dire autour de τ), l'ignorance sur l'état du lien atteint son maximum. Ce comportement est plus réaliste et prédictif qu'une ignorance constante et indépendante de l'état du lien observé.

5.3.2 Évolution dynamique des masses

Les erreurs OFDM générées par le processus de décodage de paquets varient en quantité, en séquence temporelle et en nombre d'erreurs consécutives maximales d'un scénario à l'autre. Cette variation dépend fortement de la vitesse relative des voitures et des conditions du canal de transmission. Les temps d'arrivée et la densité d'erreurs qui en résultent sont fortement affectés. Le maximum d'erreurs consécutives pour EDP et EDD avant la rupture d'une liaison est sensible à la vitesse des nœuds et à l'état de canal de transmission. Ainsi, l'utilisation d'une valeur fixe de τ entraîne une réduction des performances de prédiction en augmentant le nombre des cas ratés si τ a une valeur élevée, sinon le nombre de fausses détections sera augmenté et le temps de détection sera allongé si τ a une valeur plus faible. Par conséquent, pour adapter le modèle de masse à la dynamique de l'état du lien, nous rendons τ dynamique.

Mesures pour construire LBFI Pour la conception de LBFI, nous avons besoin d'un ensemble d'informations qui décrivent l'état du lien au cours du temps. Dans cet objectif, nous

avons considéré une structure de sauvegarde de son historique. Les évènements de décodage OFDM (*EED*, *EDP*, *RxOk*) et la puissance de réception des paquets (RSSI), sont sauvegardés dans un tampon de type FIFO indexé par le temps. La taille de la FIFO est de 20 éléments, cette taille a été calibrée lors des tests effectués pour l'indicateur LBFI. La structure du FIFO est illustrée par la figure 5.9.

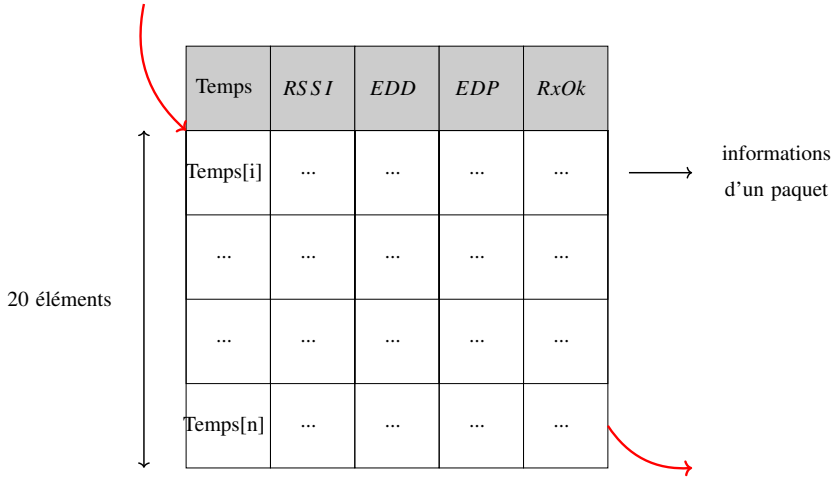


FIGURE 5.9 – Tampon FIFO utilisé pour la construction de LBFI

Le problème du choix de la valeur de τ pour EDP (τ_{EDP}) et EDD (τ_{EDD}) peut être vu comme la sélection d'un sous-ensemble τ_{EDP}, τ_{EDD} de l'ensemble S = {0,1,2,3,3,4,5,6,7} en prenant en compte la puissance de réception, la densité d'erreurs et la vitesse relative :

La puissance de réception (RSSI) Elle représente la valeur moyenne de la puissance de réception des paquets dans le FIFO examinée. Cette information est utilisée dans le calcul des premières valeurs de τ_{EDD} et τ_{EDP}. Le calcul s'effectue sur la base d'une fonction G donnée par l'équation (5.5). Cette formule sera détaillée dans la suite.

La densité d'erreurs (D) Elle représente la somme des densités d'erreurs *EDP* et *EDD* dans la FIFO et est calculée de manière temporelle avec l'équation (5.4), inspirée de [83].

$$D_{nouveau} = \lambda^{(t_n - t_i)} D_{ancien} + 1. \tag{5.4}$$

t_n est l'instant actuel, et t_i est le dernier instant de la mise à jour de la densité (D). λ est un paramètre appelé facteur d'évanouissement qui représente la vitesse à laquelle la densité diminue avec le temps. Il a la valeur 0.9 qui a été déterminée par des tests empiriques. D_{ancien} représente la densité d'erreurs au moment t_i.

Cette fonction permet de calculer la densité d'erreurs dans la file d'attente que nous utilisons et qui considère l'ensemble des vingt derniers évènements de décodage des paquets. La densité D est calculée de façon incrémentale. À l'ajout d'une erreur de décodage dans le tampon FIFO à l'instant t_n, la densité est mise à jour en ajoutant l'erreur à l'ancienne densité affaiblie dans le temps. Notons qu'à l'instant t_0 (instant d'initialisation) la densité D_0 est égale à zéro, puisqu'à cet instant la FIFO est vide (pas d'erreurs). Comme cette fonction dépend du temps écoulé entre la date de la dernière mise à jour de la densité et l'instant présent, elle permet de donner une vue sur l'état du lien. Ainsi, si les erreurs contenues dans le FIFO sont âgées, la densité est faible, et si les erreurs sont récentes, la densité est élevée.

Cette densité est utilisée pour calculer une seconde valeur de τ_{EDD} et τ_{EDP} selon la fonction G exprimée par l'équation (5.5) et qui sera expliquée dans la partie suivante.

La vitesse relative (V) Représente la vitesse relative entre deux véhicules utilisant le lien de communication en cours d'analyse. Nous divisons V en quatre groupes en fonction de la densité d'erreur maximale (D) dans la file d'attente :

— A : vitesse relative $< 3ms^{-1}$,

— B : vitesse relative $\in [3ms^{-1} ; 5ms^{-1}]$,

— C : vitesse relative $\in]5ms^{-1} ; 13ms^{-1}[$,

— E : vitesse relative $\geq 13ms^{-1}$.

Comme nous l'avons déjà mentionné, le profil d'erreurs OFDM dépend de plusieurs facteurs, parmi ces facteurs il y a la vitesse relative entre les véhicules. Pour cela, les quatre classes de vitesse citées ci-dessus sont définies à partir d'un ensemble de données (un jeu de donnée simulant des différents scénarios de communication entre des véhicules). Ces scénarios comportent des situations de déplacement des véhicules à différentes vitesses et distances. Pour chaque classe, le nombre maximal d'erreurs consécutives avant rupture de liaison et une valeur de densité d'er-

reurs ont été déterminés de manière empirique. Cela nous permet de décider quelle est la valeur τ_{EDD} et τ_{EDP} appropriée à prendre en normalisant la valeur de D et la valeur du RSSI dans la plage donnée [0,7].

Pour chaque τ (τ_{EDD} et τ_{EDP}), deux valeurs sont calculées à l'aide des deux indicateurs (D et $RSSI$), et en utilisant la fonction **G** qui normalise la puissance de réception et les valeurs de densité d'erreurs dans l'intervalle [0,7]. De fait, les valeurs numériques des deux attributs sont très fluctuantes. Par exemple, la puissance de réception prend des valeurs négatives, tandis que la densité d'erreurs peut prendre des grandes valeurs positives. L'utilisation de ces valeurs peut avoir des effets considérables sur la performance du modèle de masse. Pour ajuster ces valeurs, nous utilisons la normalisation des données selon la fonction *Min-Max*.

La normalisation *Min-Max* est un processus qui consiste à prendre les données mesurées (calculées) dans ses unités et à les transformer en une valeur comprise entre 0 et 7. La valeur la plus basse (min) est réglée à 0 et la valeur la plus haute (max) est réglée à 7. Cela permet de comparer facilement les valeurs mesurées à l'aide d'échelles ou d'unités de mesure différentes [84]. La fonction de normalisation **G** est donnée par l'équation suivante :

$$G(X,V) = \left(\frac{X - \min_x}{\max_x - \min_x}\right) \times (max_\tau(V) - min_\tau(V)) + min_\tau(V), \tag{5.5}$$

Où :

— X est la valeur à normaliser (densité d'erreurs D ou puissance de réception $RSSI$),

— $\max_x$ est la valeur maximale de X selon les quatre classes de vitesse relative définies précédemment entre les véhicules,

— $\min_x$ est la valeur minimale de X (typiquement 0),

— la plage $[\min_x; \max_x]$ pour D est définie par l'intervalle $[0; max(D, v)]$. Pour le $RSSI$ cet intervalle est défini par $[\min_{FIFO}(RSSI); -90dBm]$,

— $max_\tau(V)$ est la limite maximale de la plage à laquelle X appartiendra après normalisation. Le tableau 5.3 montre les différentes valeurs de $\max_\tau$ selon les groupes de vitesse relative

pour *EDP* et *EDD*. Plus la vitesse des véhicules est élevée, plus le nombre d'erreurs consécutives est faible,

— $min_\tau(V)$ est la limite minimale de la plage à laquelle X appartiendra après normalisation,

— Pour RSSI et D, $\max_\tau$ représente le nombre maximum d'erreurs consécutives avant la première perte de paquets au niveau réseau, ce nombre se varie selon EDD et EDP et selon la vitesse relative.

Classe de vitesse	EDD	EDP
A	4	3
B	4	2
C	2	2
E	1	1

TABLE 5.3 – Nombre maximum d'erreurs consécutives selon un ensemble de données d'apprentissage

Après avoir calculé les valeurs de τ_{EDD} et τ_{EDP} en fonction de la densité D et la puissance de réception $RSSI$, un choix est effectué pour chaque τ. On choisit le maximum des valeurs calculées (c.-à-d. le maximum entre les τ calculés en fonction de la densité et ceux calculés en fonction du $RSSI$) 5.6 :

$$\tau = \max(G(D, V), G(RSSI, V)). \tag{5.6}$$

5.3.3 Choix d'opérateur de combinaison

Dépendance de sources Les deux sources EDP et EDD sont intrinsèquement dépendantes. Il existe toujours une relation entre EDP et EDD qui peut être résumée par les éléments suivants :

— Pour un paquet donné, l'existence d'un type d'erreur élimine la possibilité de l'autre,

— La probabilité d'occurrence d'un certain nombre d'erreurs d'EDD est définie par le nombre d'EDP, et vice versa. Par exemple, si nous avons deux EDD, le nombre maximum d'EDP

que nous pouvons obtenir est inférieur ou égal à cinq pour le même processus de retransmission de paquets à la couche MAC,

— Enfin, ces deux types d'erreurs partagent la même origine, qui est le processus de décodage d'un paquet OFDM unique.

Choix de l'opérateur de combinaison et détection de rupture La dépendance des deux sources conduit à l'utilisation de la règle de la combinaison prudente (Eq. (4.17)). Cette combinaison, décrite théoriquement dans le chapitre 4, conduit aux équations ci-dessous. Le calcul des masses est effectué dans l'ensemble 2^{Ω}={ Ω, $\overline{Comloss}$, $Comloss$, $\emptyset$ }.

La masse de déconnexion ($m(Comloss)$) après la combinaison est déterminée par l'équation (5.7).

$$m(Comloss) = (1 - (w_{EDD} \wedge w_{EDP})_{Comloss}) * (w_{EDD} \wedge w_{EDP})_{\overline{Comloss}} \tag{5.7}$$

La masse de connexion (m($\overline{Comloss}$)) après la combinaison est déterminée par l'équation (5.8).

$$m(\overline{Comloss}) = (1 - (w_{EDD} \wedge w_{EDP})_{\overline{Comloss}}) * (w_{EDD} \wedge w_{EDP})_{Comloss} \tag{5.8}$$

La masse de conflit ($m(\emptyset)$) après la combinaison est déterminée par l'équation (5.9).

$$m(\emptyset) = (1 - (w_{EDD} \wedge w_{EDP})_{Comloss}) * (1 - (w_{EDD} \wedge w_{EDP})_{\overline{Comloss}}) \tag{5.9}$$

La masse de l'ignorance ($m(\Omega)$) après la combinaison est déterminée par l'équation (5.10).

$$m(\Omega) = (w_{EDD} \wedge w_{EDP})_{Comloss} * (w_{EDD} \wedge w_{EDP})_{\overline{Comloss}} \tag{5.10}$$

Avec w une fonction de poids calculée pour chaque source de donnée selon l'équation (4.19)

détaillée dans le chapitre 4. Dans notre cas, le calcul de cette fonction de poids pour chaque masse est effectué de la manière suivante :

La fonction de poids $w_{EDD}(Comloss)$ est déterminée par l'équation (5.11).

$$w_{EDD}(Comloss) = \frac{q_{EDD}(\Omega)}{q_{EDD}(Comloss)} \tag{5.11}$$

La fonction de poids $w_{EDD}(\overline{Comloss})$ est déterminée par l'équation (5.12).

$$w_{EDD}(\overline{Comloss}) = \frac{q_{EDD}(\Omega)}{q_{EDD}(\overline{Comloss})} \tag{5.12}$$

La fonction de poids $w_{EDP}(Comloss)$ est déterminée par l'équation (5.13).

$$w_{EDP}(Comloss) = \frac{q_{EDP}(\Omega)}{q_{EDP}(Comloss)} \tag{5.13}$$

La fonction de poids $w_{EDP}(\overline{Comloss})$ est déterminée par l'équation (5.14).

$$w_{EDP}(\overline{Comloss}) = \frac{q_{EDP}(\Omega)}{q_{EDP}(\overline{Comloss})} \tag{5.14}$$

Le calcul de $w_{EDD} \wedge w_{EDP}(Comloss)$ est effectué par l'équation (5.15).

$$w_{EDD} \wedge w_{EDP}(Comloss) = min(w_{EDD}(Comloss), w_{EDP}(Comloss)) \tag{5.15}$$

Le calcul de $w_{EDD} \wedge w_{EDP}(\overline{Comloss})$ est effectué par l'équation (5.16).

$$w_{EDD} \wedge w_{EDP}(\overline{Comloss}) = min(w_{EDD}(\overline{Comloss}), w_{EDP}(\overline{Comloss})) \tag{5.16}$$

La fonction de poids $q_{EDD}(Comloss)$ est déterminée par l'équation (5.17).

$$q_{EDD}(Comloss) = m_{EDD}(Comloss) + m_{EDD}(\Omega) \tag{5.17}$$

La fonction de poids $q_{EDD}(\overline{Comloss})$ est déterminée par l'équation (5.18).

$$q_{EDD}(\overline{Comloss}) = m_{EDD}(\overline{Comloss}) + m_{EDD}(\Omega) \tag{5.18}$$

La fonction de poids $q_{EDP}(Comloss)$ est déterminée par l'équation (5.19).

$$q_{EDP}(Comloss) = m_{EDP}(Comloss) + m_{EDP}(\Omega) \tag{5.19}$$

La fonction de poids $q_{EDP}(\overline{Comloss})$ est déterminée par l'équation (5.20).

$$q_{EDP}(\overline{Comloss}) = m_{EDP}(\overline{Comloss}) + m_{EDP}(\Omega) \tag{5.20}$$

Pour décider si un lien va rompre, une comparaison entre $\overline{Comloss}$ et $Comloss$ est réalisée

après la combinaison. Si la valeur de $Comloss$ est supérieure à $\overline{Comloss}$, l'indicateur LBFI indique une rupture probable de lien. Le processus de détection de rupture de lien est décrit dans l'algorithme 5.1.

Algorithm 5.1 LBFI (Link breakage forecasting indicator)

Require: Erreurs de décodage OFDM

return État de lien

- Calculer la masse $m(Comloss)$ après combinaison
- Calculer la masse $m(\overline{Comloss})$ après combinaison
- Calculer la masse $m(\Omega)$ après combinaison
- Calculer la masse $m(\emptyset)$ après combinaison

if $Comloss > \overline{Comloss}$ **then**

Détection de rupture d'un lien

else

Le lien est en bon état

end if

La figure 5.10 montre un exemple de détection de rupture de lien pour un scénario d'éloignement de deux véhicules. Comme expliqué dans les sections précédentes, notre référence pour la détection des ruptures de lien est la retransmission d'un paquet sept fois au niveau de la couche physique. Dans l'exemple du scénario présenté dans la figure 5.10, la rupture (première perte de paquet) arrive à 41,4 s. LBFI détecte la rupture à 37,7 s. En effet, la masse de $Comloss$ devient supérieure à la masse de $\overline{Comloss}$ avec des valeurs respectives de 0.30 et 0.28. Le délai de prédiction de notre indicateur est donc de 3.7 secondes.

5.3.4 Synthèse

Le diagramme 5.11 résume le fonctionnement de notre indicateur de rupture de lien (LBFI). À la réception d'un paquet au niveau de la couche physique, le processus de décodage OFDM commence. Les informations sur le type d'erreur générées et la puissance de réception de paquet ($RSSI$) sont extraites et les densités d'erreurs sont mises à jour. Par la suite, le point de transition τ est calculé et les fonctions de masse sont calibrées (comme expliqué dans la section précédente). Dans la phase suivante, les masses sont combinées à l'aide de la règle prudente puis

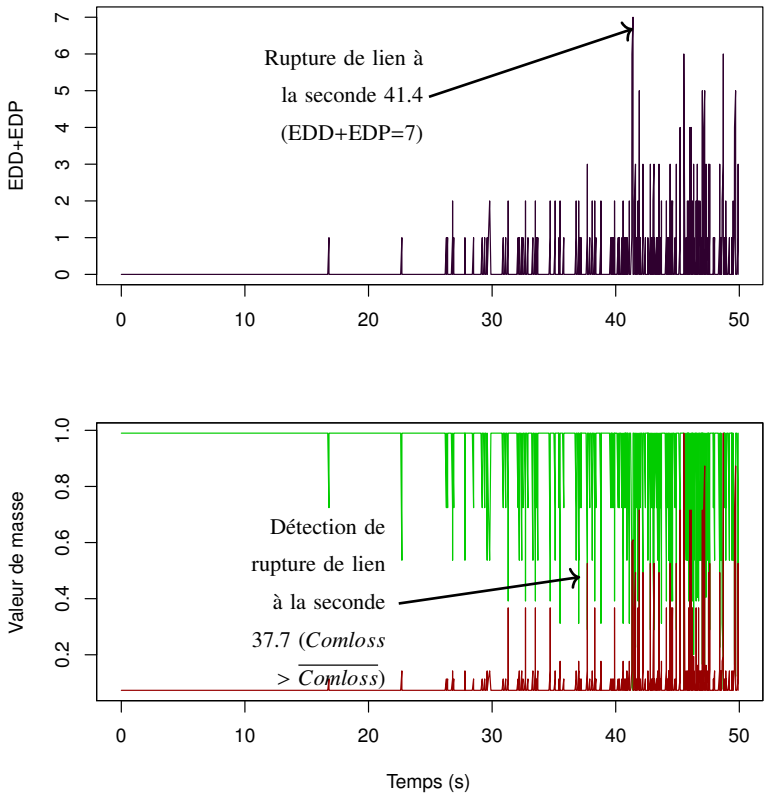


FIGURE 5.10 – Exemple de détection de rupture de lien

la masse de *Comloss* résultante de la fusion des deux sources EDP et EDD est comparée avec la masse $\overline{Comloss}$. Si *Comloss* est supérieure à $\overline{Comloss}$, LBFI déclenche une prédiction de rupture de lien.

Dans la prochaine section, les éléments liés à l'évaluation de cet indicateur ainsi que les performances obtenues sont présentés.

5.4 Évaluation des performances de LBFI

5.4.1 Environnement de simulation

Les expérimentations réelles dans le domaine des VANET basées sur une flotte de véhicules équipés sont très coûteuses en terme de matériel. Il est également nécessaire de pouvoir refaire

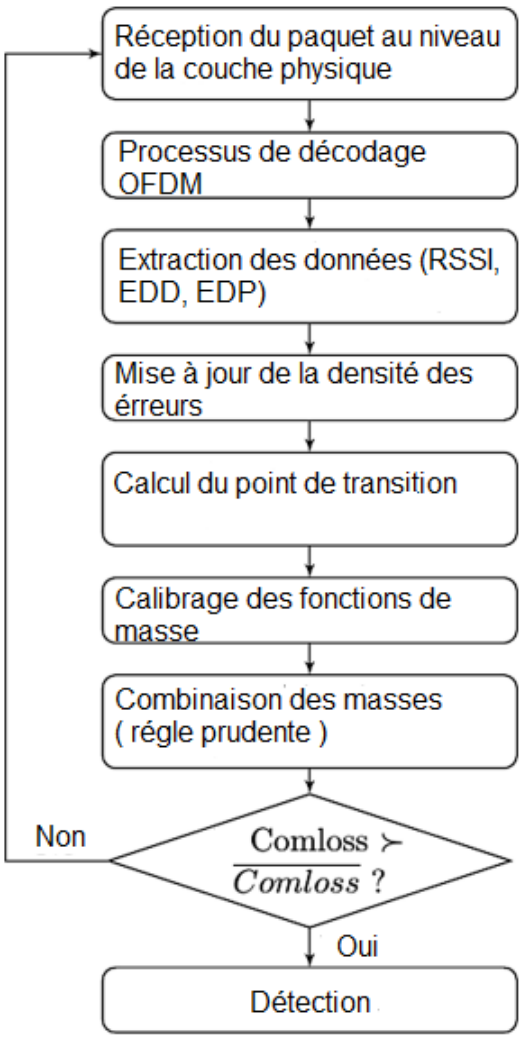


FIGURE 5.11 – Processus de LBFI pour la prédiction de rupture d'un lien

certains tests dans les mêmes conditions (reproductibilité) ce qui est difficile dans le cadre des expérimentations réelles. Les outils de simulation réseaux et plus particulièrement des VANET ont évolué permettant d'avoir des modèles de protocoles de routages et de propagation les plus réalistes possible. Il a donc été choisi (au-delà d'un cadre financier) d'utiliser un simulateur réseau. Il serait très intéressant d'effectuer par la suite des tests grandeur nature afin de confirmer les résultats obtenus par simulation. Les simulations réalisées ici se font avec le simulateur ns-3 [85].

Ns-3 Ns-3 est un simulateur de réseaux à événements discrets ciblant prioritairement le milieu universitaire tant sur les aspects recherche que sur les aspects pédagogiques. Commencé en 2006, le développement du projet ns-3 est un projet *open-source*, il vise à maintenir un environnement public dans lequel les chercheurs peuvent contribuer et partager leurs contributions. Ns-3 ne correspond pas à une extension ou une évolution de Ns-2, mais est un nouveau simulateur qui se distingue par l'utilisation du *Python* ou *C++* comme langage du script au lieu du *OTcl* utilisé par Ns-2. Certains modèles Ns-2 qui sont écrits en *C++* ont déjà été portés sur ns-3. Cependant, les modèles basés sur *OTcl* n'ont pas été portés car il faut une réécriture complète. Les modèles disponibles dans ns-3 se focalisent sur la modélisation du fonctionnement des protocoles et réseaux internet. Ns-3 n'est pas restreint aux systèmes Internet ; en fait, divers usagers l'utilisent pour modéliser des systèmes ne reposant pas sur internet.

Ns-3 est basé sur des bibliothèques pouvant se combiner les unes avec les autres mais également avec des librairies externes. Quelques plates-formes de simulation sont dotées de leurs propres interfaces graphiques intégrant de nombreuses tâches. Contrairement à ceux-ci ns-3 se distingue par des animateurs et des outils d'analyse et de visualisation des données externes tels que *Netanim*. Ns-3 fonctionne en ligne de commande et avec des outils de développement logiciel C++ et Python. Ns-3 est essentiellement disponible sous des systèmes Unix-Like.

Dans cette thèse, le choix du simulateur s'oriente vers ns-3. Les modules présentés ainsi que les fonctionnalités offertes par ce simulateur permettent d'atteindre un haut degré de réalisme. D'autre part, il est doté d'un mécanisme de traçage modifiable. Des fichiers de sortie peuvent être personnalisés selon le besoin de l'utilisateur. Enfin, comme mentionné précédemment ns-3 rend possible l'intégration d'autres logiciels et outils. De ce fait, un module de propagation réaliste a été importé. Ce module développé par le KIT s'appelle Physimwifi [1] dont voici une présentation.

Physimwifi Développé par *Decentrelized System and Network Service Research Group* [86] de l'Institut de Technologie de Karlsruhe (KIT) [87], le module PhysimWifi est une implémentation des mécanismes d'encodage et de décodage ainsi que de propagation de la norme IEEE802.11. Les opérations de codage et de décodage basées sur la technique de multiplexage OFDM dans la bande des 5 GHz y sont implémentées et cela de manière réaliste. Cette implémentation reproduit toutes les étapes de traitement du signal qu'un véritable émetteur-récepteur réaliste lors du

codage/décodage d'une trame. Ainsi, les bits individuels sont explicitement pris en compte et des techniques détaillées des couches basses telles que la modulation OFDM sont mises en œuvre. La prise en compte de la modélisation de cette couche physique, les modèles de propagation du signal existants et nouveaux peuvent facilement être implémentés et connectés au simulateur sans qu'il soit nécessaire de construire des taux d'erreur de bits ou de paquets empiriques.

L'architecture conceptuelle de *PhySimWifi* est représentée par la figure 5.12. Comme le montre ce schéma, les deux modules les plus importants de PhysimWifi sont son module de couche physique appelé PhysimWifiPhy et son module d'émulation de canal de propagation appelé PhysiWifiChannel. Elle montre l'interaction avec la couche *MAC*. Le processus de transmission de paquet commence par une requête *SendPacket()* lancé par la couche *MAC* vers *PhysimWifiPhy*. À ce niveau le paquet est représenté sous forme d'une suite de bits. Le paquet est transmis par la suite au canal sans fil (de type PhySimWifiChannel) pour l'application des effets du canal. Ensuite le paquet est démodulé et le résultat est comparé finalement avec ce qui a été transmis pour vérifier la bonne réception.

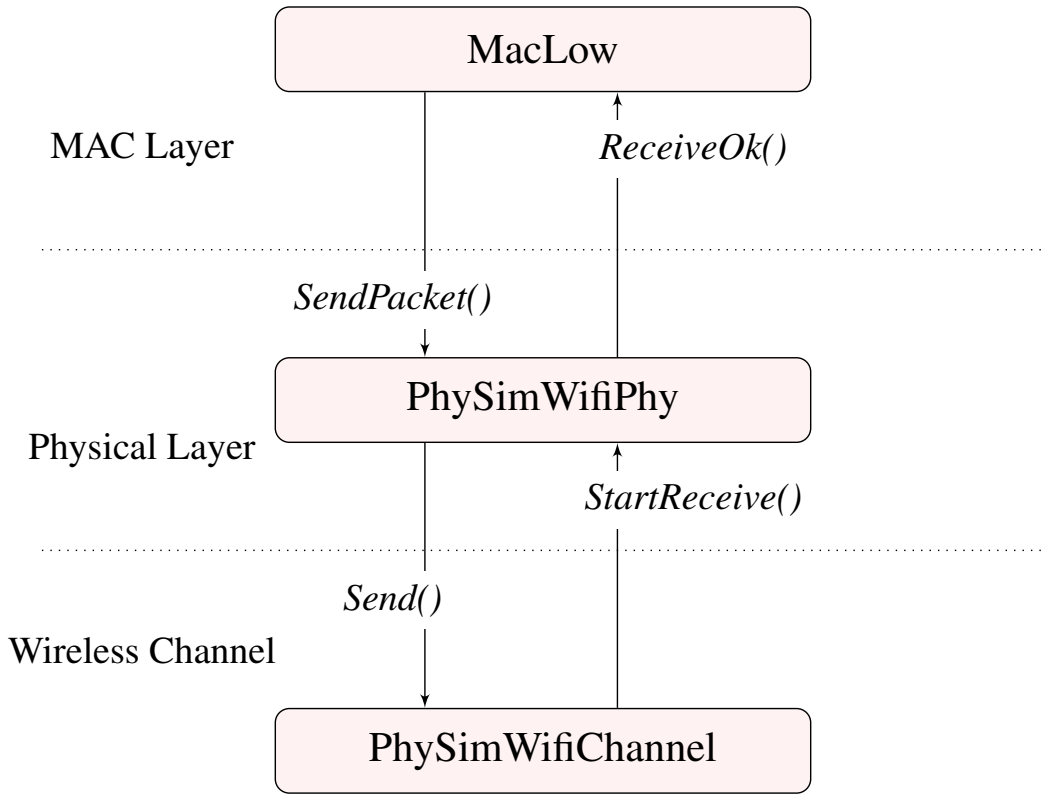


FIGURE 5.12 – Implémentation de PhySimWifi

PhySimWifi prend en compte les trois effets qui influencent la propagation des signaux : l'affaiblissement du signal selon la distance, le *shadowing* et l'effet de *fading* lors de la modélisation du canal de transmission. Voici des exemples de modèles de propagation proposés dans *PhySimWifi* :

— **PhySimFriisSpacePropagationLoss :** représente le modèle de propagation *Friis Space*,

— **PhySimShadowingPropagationLoss :** permet d'appliquer un effet de *shadowing* avec une variable aléatoire normale gaussienne,

— **PhySimRicianPropagationLoss :** permet d'appliquer un effet de fading qui prend également en compte les effets Doppler.

Il existe d'autres modèles de propagation des ondes incorporés dans *PhySimWifi*, et qui peuvent être utilisés pour simuler des différents environnements de propagation des ondes. Dans notre cas, les modèles utilisés sont : *PhysimAbbasLosShadowing* qui permet de simuler l'effet de *Shadowing*, et qui est combiné avec le modèle *PhysimITUA* qui permet de simuler les effets de *Small scale fading*.

5.4.2 Critères d'évaluation

L'indicateur LBFI est conçu pour prédire une rupture de lien en utilisant des informations fournies par la couche physique. Une rupture de lien est définie comme la première perte d'un paquet au niveau de la couche réseau. L'évaluation du LBFI est faite selon les trois critères suivants :

Temps de prédiction Aussi appelé *délai de prédiction*, c'est le temps entre la détection effectuée par LBFI et la vraie rupture de lien c.-à-d. première perte du paquet au niveau de la couche application.

Faux positifs Aussi appelé *fausse détection*, c'est une fausse prédiction de rupture de lien dans laquelle LBFI indique une rupture de lien alors qu'il n'y aura pas de rupture. Les faux positifs peuvent se produire dans des situations de suivi de véhicules qui augmentent l'espace inter-véhiculaire.

Cas raté Aussi appelé *détection manquée*, c'est le fait de détecter une rupture après que celle-ci ait eux lieu (c.-à-d. prédiction tardive d'une rupture de lien) ou de ne pas la détecter même si ce cas n'apparaît pas dans l'indicateur LBFI.

5.4.3 Paramètres de simulation

L'évaluation des performances de l'indicateur a été menée avec le simulateur ns-3 en mettant en place un environnement réaliste de propagation du signal et à l'aide d'un ensemble de scénarios retraçant des conditions de rupture de lien. Nous avons utilisé les scénarios suivants :

Scénario [1] Véhicules qui se croisent à différentes vitesses. Toutes les situations d'éloignement produisent des ruptures de lien qui sont idéales pour évaluer notre indicateur en termes de temps de détection et de nombre de détections manquées (cas raté). Les vitesses utilisées varient dans l'ensemble { $3m.s^{-1}$, $5m.s^{-1}$, $9m.s^{-1}$, $13m.s^{-1}$, $15m.s^{-1}$ }.

Scénario [2] Véhicules qui se suivent à des distances inter-véhicules qui varient en cours de simulation. Dans ces situations, l'apparition d'une rupture de lien dépend de la distance entre les véhicules et des conditions du canal de transmission. Ce type de scénario est utilisé pour évaluer l'indicateur en termes de temps de prédiction et en nombre de faux positifs. Un indicateur de prédiction de rupture de lien performant ne doit pas indiquer des fausses détections. La distance entre les véhicules examinée varie dans l'ensemble $\{60m, 90m, 120m, 150m, 210m\}$.

Scénario [3] Scénario qui fait varier la taille des paquets échangés dans l'ensemble $\{128, 256, 1024\}$ octets pour évaluer l'impact de la taille des paquets. Cette variation de la taille des paquets est appliquée aux scénarios [1] et [2].

Scénario [4] Scénario qui fait varier le débit des données dans l'ensemble $\{10, 20, 100\}$ ms pour évaluer l'impact du débit de données sur LBFI. Cette variation du débit de données est appliquée aux scénarios [1] et [2].

Scénario [5] Scénario qui sert pour évaluer LBFI dans les situations d'interférence. Pour ce faire, un scénario de 12 nœuds a été défini. La vitesse des nœuds se varie dans l'intervalle [$3m.s^{-1}$, $15m.s^{-1}$]. Ce scénario est reproduit 50 fois à l'aide de 50 seeds aléatoires.

Scénario [6] Scénario qui est utilisé pour montrer les performances de LBFI dans des scénarios de mobilité réaliste. L'outil SUMO (Simulation for Urban MObility [88]) est un simulateur de mobilité qui permet de générer une mobilité utilisables par ns-3 à partir des cartographies numériques fournies notamment par OpenStreetMap [89]. OpenStreeMap est un projet visant à construire une base de données géographiques gratuite du monde entier (sous licence ODbL [5]). Son but est de répertorier toutes les caractéristiques géographiques : cartographie des rues, des bâtiments, signalisations, etc. Le scénario utilisé comporte 50 nœuds dans la ville de Strasbourg, France.

Un exemple illustrant un scénario de suivi de deux véhicules à une distance de 90 m est présenté dans la figure 5.13. Au début, la distance est constante, la vitesse relative entre les véhicules est alors est égale à zéro. À la seconde 20, la distance entre les véhicules commence à augmenter (due à l'accélération ou au freinage d'un véhicule). Cette augmentation de la distance engendre un changement dans la vitesse relative qui augmente et qui revient à zéro lorsque la distance est constante. Les situations de suivi des véhicules représentent de bons scénarios de test des faux positifs générés par un indicateur de rupture de lien.

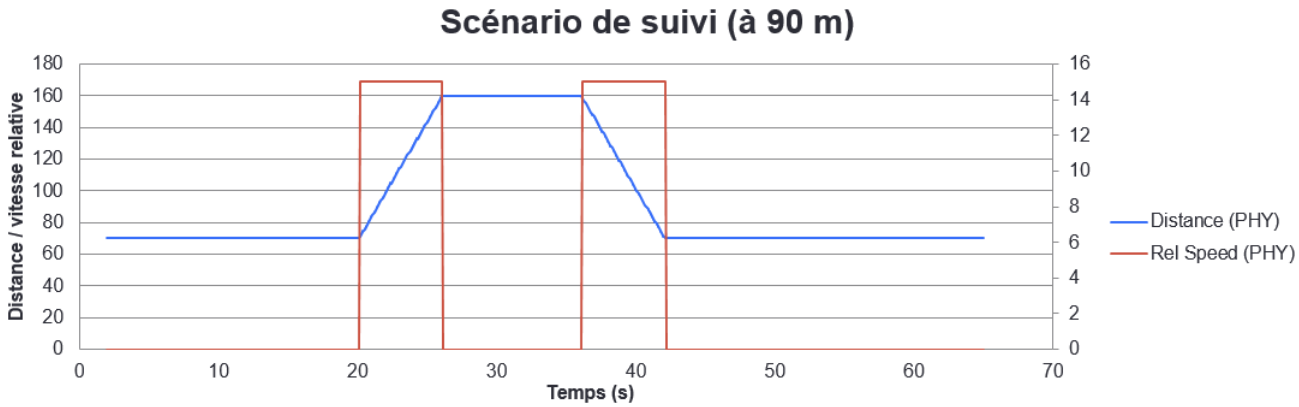


FIGURE 5.13 – scénario de suivi à 90 m

Un autre exemple illustrant un scénario d'éloignement de deux véhicules à une vitesse de $3m.s^{-1}$ est présenté dans la figure 5.14. Au fur et à mesure de la simulation la distance entre les véhicules augmente, tandis que la vitesse reste constante. Les situations d'éloignement des

5. licence libre Open Data Commons Open Database License (ODbL) auprès de la Fondation OpenStreetMap (OSMF), © les contributeurs d'OpenStreetMap

véhicules représentent de bons scénarios de test des cas ratés générés par un indicateur de rupture de lien.

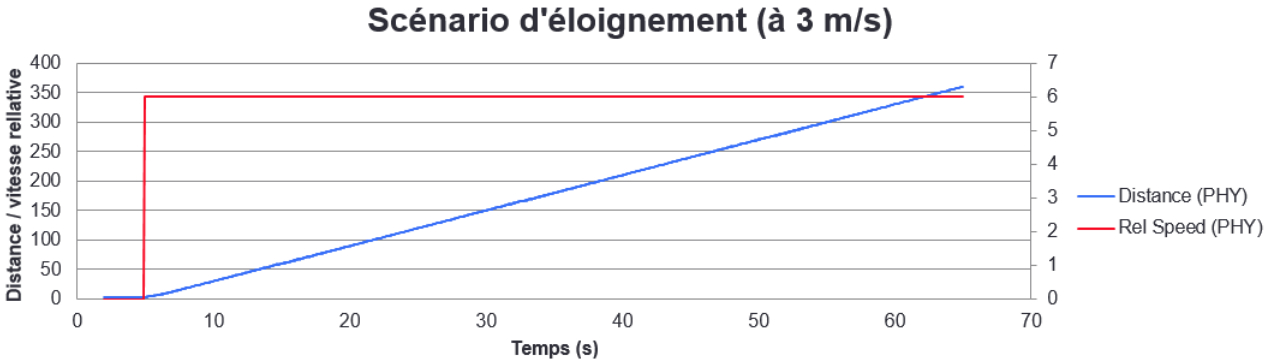


FIGURE 5.14 – scénario d'éloignement à $3m.s^{-1}$

Les simulations ont été effectuées avec le simulateur ns-3 [85] avec différentes graines aléatoires. Une graine aléatoire est un nombre utilisé pour initialiser un générateur de nombres pseudo-aléatoires. Cette fonctionnalité est importante dans un simulateur, parce qu'elle permet de nouvelles conditions de simulation à chaque fois que la graine (le seed) est modifiée. Dans notre cas, elle permet de créer des effets différents de perturbation de canal de transmission. À noter que si la graine n'est pas changée entre deux simulations, les mêmes effets sont observés permettant ainsi d'avoir une reproductibilité dans les simulations. Puisque le canal de propagation affecte la qualité des liens dans les réseaux véhiculaires [90], il est très important de mettre en œuvre une modélisation réaliste de son comportement. Ce qui implique : (i) un affaiblissement de signal en fonction de la distance, (ii) du *shadowing*, (iii) du *fading*, (iv) de l'effet Doppler (voir le chapitre 3, section 3.2). À cette fin, Physimwifi fournit plusieurs modèles de propagation qui peuvent être utilisés pour simuler le comportement d'un canal de propagation réaliste. Tous les paramètres de simulation sont résumés dans le tableau 5.4.

Paramètre	Valeur
Simulateur	Ns-3
Temps de simulation	120 s
Nombre de noeuds	{2, 12, 50}
Couche MAC	802.11p
Modèle de propagation	Pathloss, shadowing, fading, doppler
Vitesse	$3m.s^{-1}$ à $15m.s^{-1}$
Distance	60 m à 210 m
Taille de paquet de données (B)	{128, 256*, 1024}
Temps inter-paquet de données (ms)	{10, 50, 100*}
Débit physique des données (Mb/s)	6

TABLE 5.4 – Paramètres de simulation

5.5 Performance de LBFI

5.5.1 Sensibilité du LBFI aux différentes conditions réseaux

Voici les différents éléments permettant d'évaluer l'efficacité et la robustesse de l'indicateur LBFI dans diverses conditions de réseau :

Impact de la taille des paquets Pour cette étude le scénario [3] est utilisé. L'objectif est de connaître l'influence de la taille des paquets sur les performances de LBFI. La taille des paquets varie dans l'ensemble {128, 256, 1024} octets.

Impact du débit des données Pour cette étude le scénario [4] est utilisé. L'objectif est de tester l'influence de la variation de débit. Comme LBFI se base sur les paquets reçus pour alimenter son algorithme, il est nécessaire de savoir si une variation de débit de données améliore ou dégrade ses performances. Les débits utilisés varient dans l'ensemble {10, 50, 100} ms.

Impact des interférences Pour cette étude le scénario [5] est utilisé. L'objectif est de savoir comment LBFI se comporte dans des situations d'interférence quand la densité des nœuds augmente.

Nous évaluons tout d'abord les temps de prédiction, ensuite le nombre de faux positifs et le nombre de cas ratés. Le réglage des simulations reste le même que dans le tableau 5.4.

A)-Influence des conditions du réseau sur le temps de prédiction

La taille des paquets La figure 5.15 représente la distribution du temps de prédiction pour différentes tailles de paquets allant de 128 octets à 1024 octets, et montre que les paquets de données de taille 1024 octets enregistrent le nombre d'occurrences le plus haut dans l'intervalle [0-2]. La distribution des temps de prédiction des paquets à grande taille (1024 octets) est la plus décalée vers la gauche. La figure 5.16 représente le cumul des pourcentages des occurrences. Elle montre que pour des tailles de paquets différentes l'indicateur à tendance de donner un temps de détection inférieur à 6 secondes.

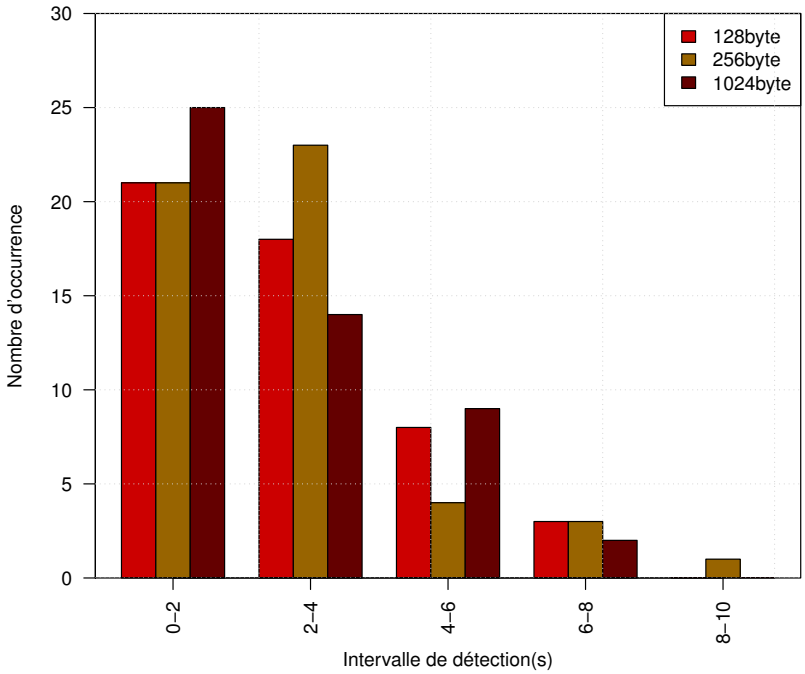


FIGURE 5.15 – Distribution du temps de détection LBFI pour différentes tailles de paquets

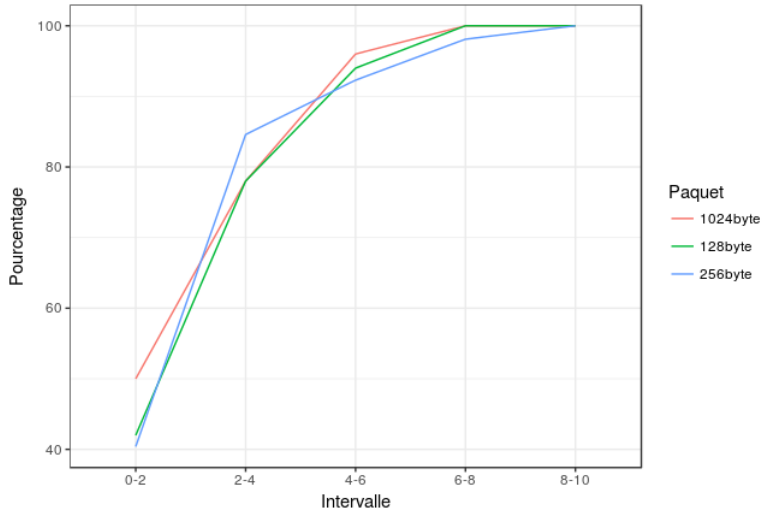


FIGURE 5.16 – Pourcentage cumulé du nombre d'occurrences des temps de détection pour différentes taille de paquet

L'analyse effectuée montre la capacité de notre indicateur à détecter les ruptures de lien même lorsqu'il reçoit un trafic de données avec différentes tailles de paquets et d'en montrer les effets. De plus, cette variation de la taille des paquets affecte favorablement les temps de détections, plus la taille du paquet est grande, plus le temps de détection est court. Plus les paquets sont de grande taille, plus le canal de transmission les impacte en les dégradant, ce qui entraîne une augmentation du nombre d'erreurs et donc de meilleures performances de LBFI. Ces résultats sont encourageants puisqu'ils montrent que la taille des paquets les plus défavorable (taille inférieure à 512 octets), LBFI montre de bonnes performances et que quand cette taille augmente les performances augmentent en même temps.

Débit La deuxième évaluation de performance vise à mesurer l'impact du débit de paquets sur les temps de prédiction. Pour ce faire, une comparaison est effectuée avec trois intervalles de temps inter-paquets (1 paquet toutes les 10 ms, toutes les 50 ms et 1 paquet toutes les 100 ms) et qui correspond aux trois débits 100p/s, 20p/s et 10 p/s. La figure 5.17 représente le cumul des pourcentages d'occurrences des temps de prédiction. Elle montre que plus le débit est élevé plus les temps de prédiction sont courts.

Ces performances s'expliquent par la quantité des informations utilisées pour alimenter l'algorithme de LBFI. Plus LBFI reçoit des paquets (évènements de décodage de paquet), plus les

performances sont améliorées.

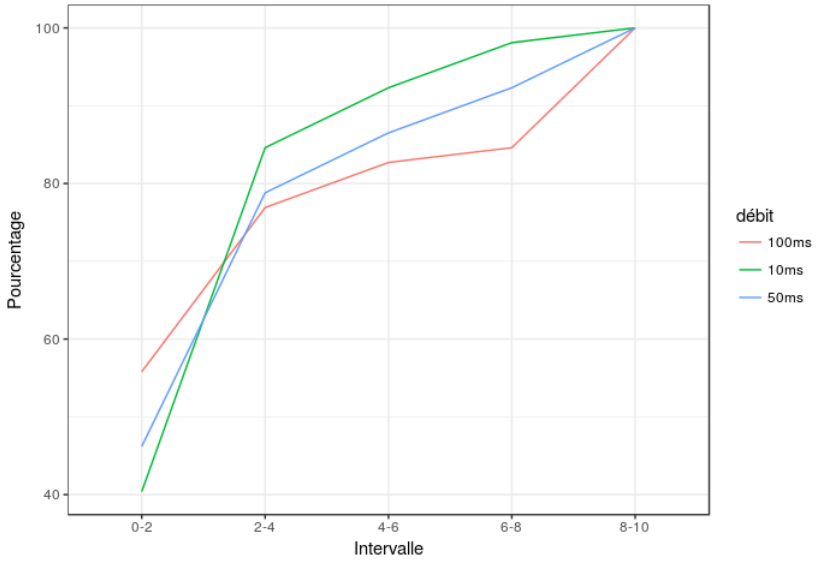


FIGURE 5.17 – Pourcentage de cumul du nombre d'occurrences pour les différents débits

Situation d'interférence Dans les deux premières évaluations présentées, seules des situations avec deux nœuds ont été utilisées. Ces situations ne prennent pas en compte le phénomène d'interférences. L'objectif de cette étude est de montrer la robustesse de l'indicateur par rapport à des situations d'interférence. Dans les communications sans fil, un des impacts majeurs sur les communications est les interférences entre nœuds voisins. Les paquets de données peuvent être rejetés en raison de ces interférences. Afin de simuler de telles situations, le scénario [5] a été utilisé. La figure 5.18 compare les temps de détection dans des situations avec et sans interférences. Les résultats montrent que les temps de détection sont influencés positivement par les interférences. 90% des cas de rupture de lien sont détectés en moins de 4 secondes dans les scénarios avec interférences. Alors que sans interférences, seuls 80% sont détectés au cours de la même période.

Une détérioration de l'état du réseau affecte positivement les temps de détection de LBFI. Ceci est, comme précédemment, dû au fait que l'impact des interférences est de produire une plus grande quantité d'erreurs, ce qui réduit l'incertitude sur la prédiction des défaillances de liaison.

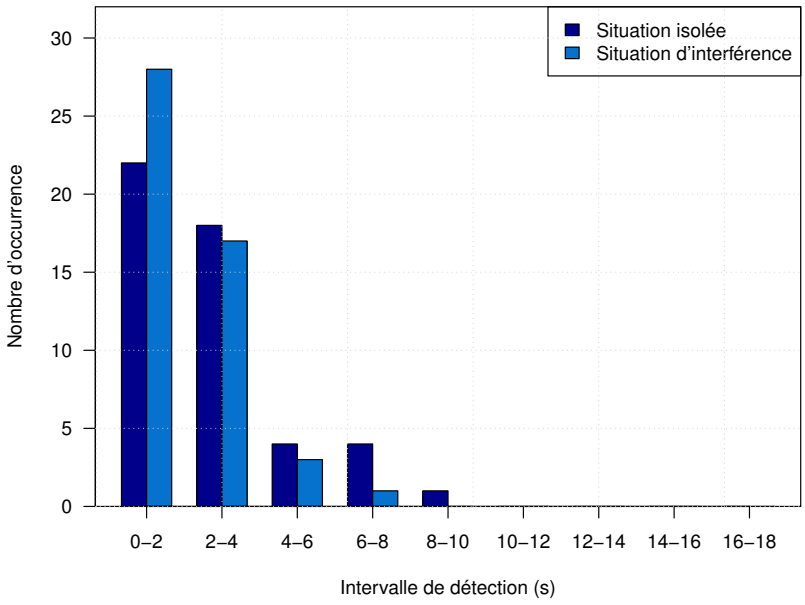


FIGURE 5.18 – Temps de détection LBFI en cas d'interférence

B)-Influence des conditions du réseau sur le nombre de faux positifs et les cas ratés

L'objectif d'un indicateur prédictif de rupture de lien ne réside pas seulement dans le fait de prévoir les ruptures avec un temps utilisable, qui permet au protocole de routage la recherche de nouvelles routes. Mais aussi d'être capable d'une part de différencier entre une rupture de lien au niveau réseau et une fluctuation (perturbation) du lien au niveau physique. Ce qui arrive souvent dans des scénarios de suivi de véhicules où la connectivité est assurée au niveau réseau mais l'état de lien est fluctuant au niveau de la couche physique. D'autre part, l'indicateur doit être capable de prédire les ruptures avant qu'elles ne surviennent (c.-à-d. l'indicateur doit indiquer le minimum possible des cas ratés).

Les figures 5.19 et 5.20 montrent respectivement le pourcentage de cas ratés et de faux positifs produits par l'indicateur en fonction de la taille des paquets et de leur débit. Les cas ratés sont calculés à partir des scénarios d'éloignement des véhicules et les cas de faux positifs sont calculés à partir des cas de suivi de véhicules. Il apparaît clairement que le nombre de cas ratés augmente en augmentant la taille des paquets contrairement au nombre de faux positif qui diminue en augmentant la taille des paquets (figure 5.19). D'une autre part, le nombre de cas

ratés augmente en diminuant le débit contrairement au nombre de faux positif qui diminue en diminuant le débit (figure 5.20). Nous constatons que la faiblesse de LBFI réside dans les débits faibles et une taille des paquets qui va en augmentant. Cet indicateur repose sur le nombre d'erreurs et moins il y a d'erreurs, moins l'indicateur est performant.

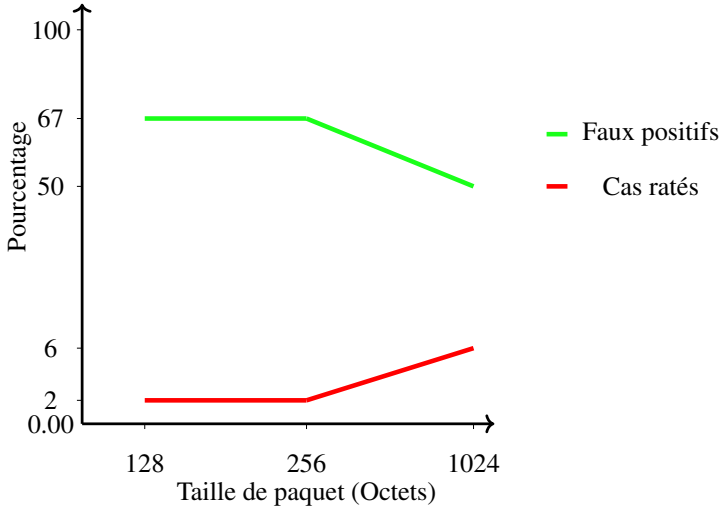


FIGURE 5.19 – Pourcentage des cas ratés et des faux positifs en fonction de la taille des paquets de données

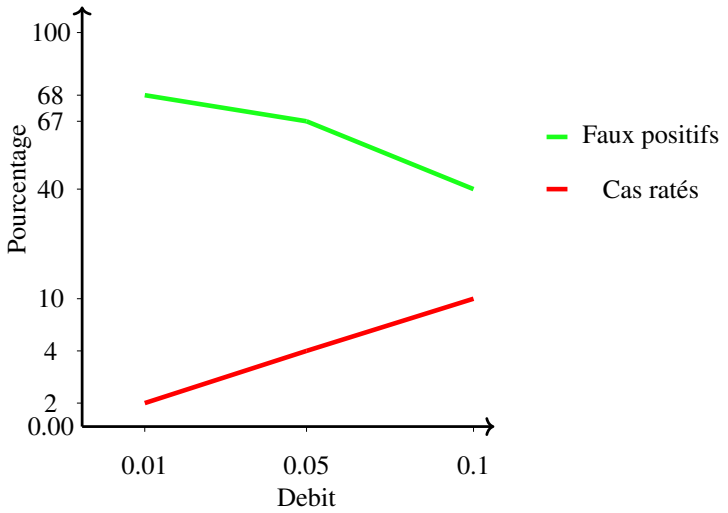


FIGURE 5.20 – Pourcentage des cas ratés et des faux positifs en fonction du débit

Dans le cas de l'existence d'interférence, le nombre de cas raté enregistré est égal à un seul cas raté. Cependant le nombre de fausse est de 67%.

5.5.2 Évaluation de LBFI dans le cas d'une simulation de la mobilité réaliste

Dans cette section, l'efficacité de LBFI est testée dans des scénarios de mobilité réaliste (scénario [6]). L'objectif ici est de démontrer la robustesse du LBFI face à de la mobilité urbaine. Les mêmes modèles de propagation sont utilisés et les communications entre les nœuds en situation de croisement et suivis sont analysées afin de détecter les ruptures de lien et les cas de fausses détections.

La figure 5.21 montre la distribution des temps de détection pour 37 liens de communication. Ces résultats montrent que 84% des temps de détection ne dépassent pas 4 secondes. Le reste est détecté en moins de 7 secondes et un seul cas de détection manquée a été observé. Pour évaluer les performances de LBFI par rapport aux fausses détections, onze liens de communication pour des véhicules en mode suivi ont été également examinés parmi lesquels il n'y a pas de rupture des liens, et donc pas de pertes de paquets au niveau réseau. Le pourcentage de faux positifs générés par LBFI est de 36%.

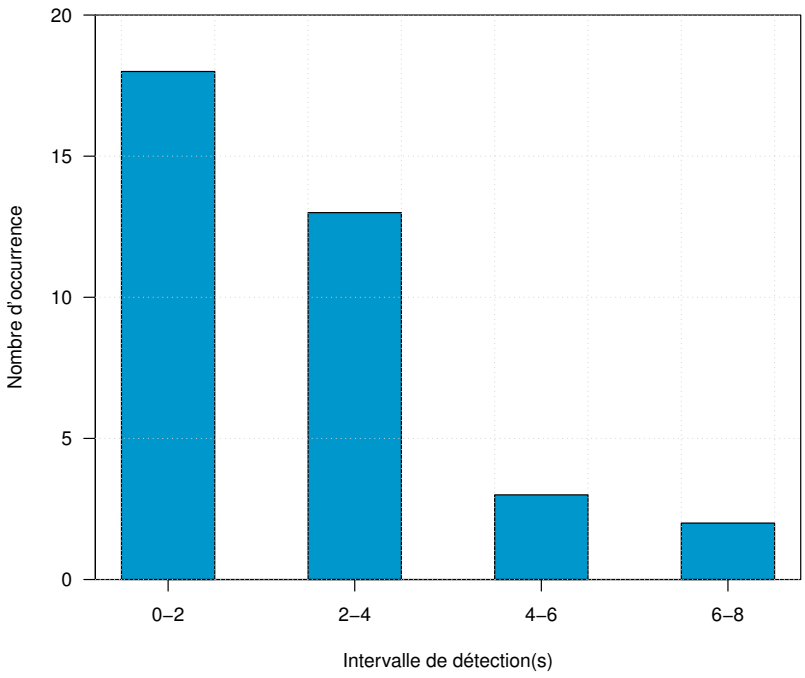


FIGURE 5.21 – Répartition des temps de détection en milieu urbain

LBFI est capable de prédire les ruptures des liens en milieu urbain avec des temps de prédiction qui ne dépassent pas 6 secondes.

Dans la section suivante, les performances de LBFI sont comparées à celles de LSFI-BF.

5.5.3 Comparaison entre LBFI et LFSI-BF

Pour cette expérimentation le scénario [1] est utilisé dans les simulations. Nous traçons la distribution des temps de prédiction pour les deux indicateurs de rupture de liaison. Les résultats sont séparés en deux groupes. Les temps de prédiction pour les véhicules circulant à des vitesses inférieures à $9m.s^{-1}$ (Figure 5.22) et les temps de prédiction pour les véhicules circulant à une vitesse supérieure à $9m.s^{-1}$ (Figure 5.23). Cette expérience rassemble les résultats de 150 scénarios d'éloignement.

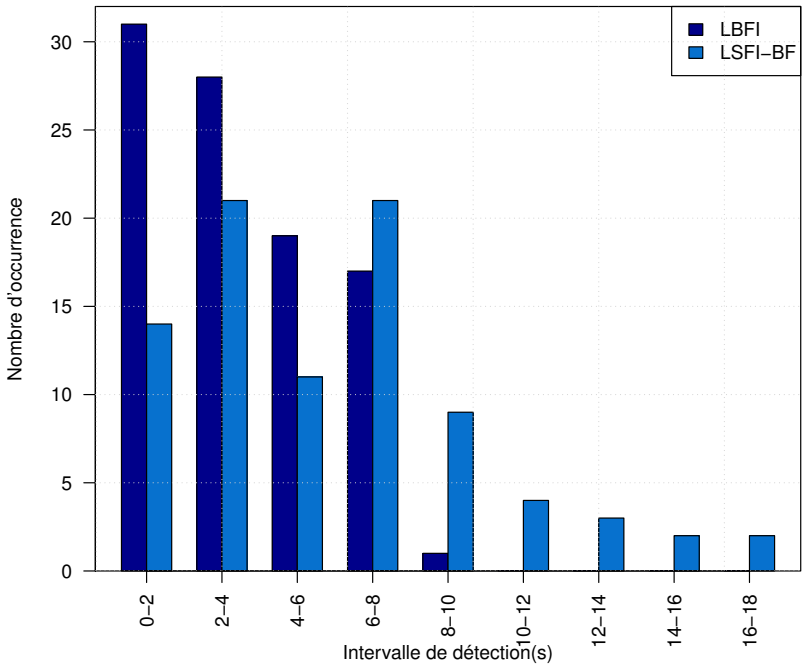


FIGURE 5.22 – Distribution du temps de détection pour des vitesses inférieures à $9m.s^{-1}$

LSFI-BF possède 47,6% de temps de prédiction situés dans un intervalle de temps de 0 s à 8 s, tandis que LBFI a plus de 91% situés dans cet intervalle. En effet, les temps de prédiction produits par LSFI-BF sont grands, cela minimise le temps d'utilisation d'une route par le protocole de routage. Il est donc nécessaire de réduire le temps de détection d'une façon qui permet non

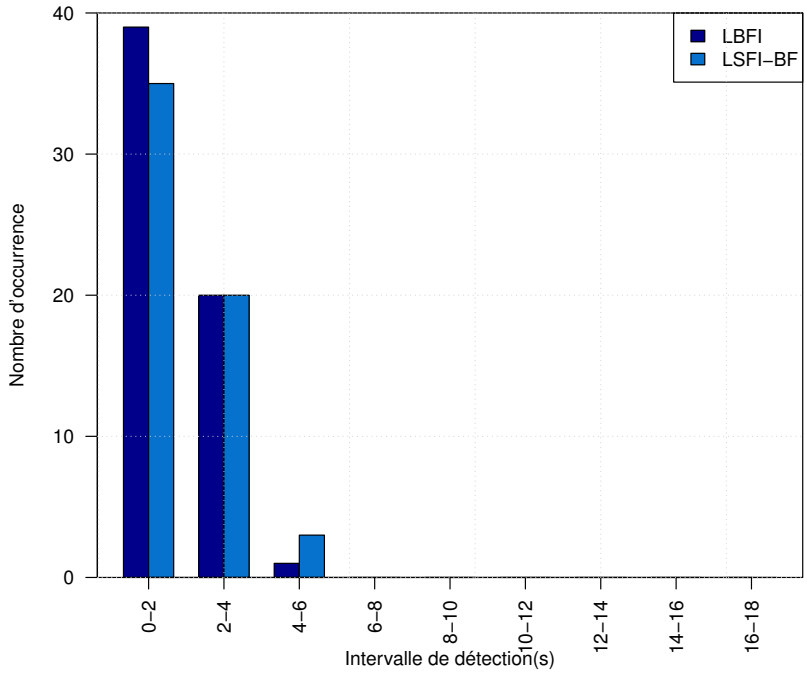


FIGURE 5.23 – Distribution du temps de détection pour des vitesses supérieures à $9m.s^{-1}$

seulement à allonger le temps d'utilisation des routes mais aussi de permettre aux protocoles de rechercher une nouvelle route avant qu'une route ne soit rompue. Dans les situations où la vitesse est supérieure à $9m.s^{-1}$ (Figure 5.23), la distribution des temps de détection est quasiment identique. Notez que pour ces vitesses, les temps de prédiction ne dépassent pas 5 secondes pour les deux indicateurs.

Les performances de LBFI par rapport à LFSI-BF s'expliquent par le modèle de masse utilisé pour estimer la rupture de lien, qui tient en compte plusieurs éléments d'information (la densité d'erreurs, la puissance de réception et la vitesse relative entre les véhicules) contrairement au modèle de masse du LFSI-BF qui repose simplement sur le nombre d'erreurs produites. La densité d'erreurs calculées par l'indicateur fournit un historique du lien. Ceci aide LBFI à prendre des bonnes décisions contrairement au LFSI-BF qui construit sa détection sur l'observation instantanée d'erreurs.

Pour évaluer le nombre de fausses détections et des cas ratés fournis par chaque indicateur, nous testons LBFI sur un ensemble de scénarios de suivi (scénario [2]) et d'éloignement (scénario [1]). Les résultats de simulation sont résumés dans le tableau 5.5. Il montre que notre indicateur

réduit le nombre de faux positifs d'un tiers, tandis que le nombre de détections manquées reste pratiquement identique pour les deux indicateurs. Comme indiqué précédemment, ces résultats sont dus au fait que l'historique des liens est pris en compte dans le calcul de la probabilité de défaillance des liens.

Indicateur	Cas raté (situations d'éloignement)	Faux positif (situations de suivi)
LSFI-BF	2%	96%
LBFI	1,5%	67%

TABLE 5.5 – Comparaison entre LBFI et LSFI-BF

5.5.4 Discussion

Au travers des simulations effectuées nous avons montré la robustesse de notre indicateur de rupture de lien (LBFI) face à différentes situations et variations des paramètres. Les premières expérimentations examinent les performances de LBFI dans des situations de communication de deux nœuds isolés en fonction des paramètres de réseaux (taille des paquets et débit). Les résultats montrent la capacité de LBFI à détecter les ruptures de liens avec des temps de prédictions inférieurs à 8 secondes. L'analyse montre également que le nombre des cas ratés et de faux positifs sont influencés principalement par deux paramètres qui sont le débit et la taille des paquets. Dans le deuxième type d'expérimentations, nous avons montré la robustesse de LBFI dans des situations d'interférences et dans des simulations de mobilité réaliste. L'indicateur donne des temps de détection qui ne dépassent pas 8 secondes. À la fin, nous avons comparé notre indicateur avec LSFI-BF. Les résultats des expérimentations montrent que notre indicateur minimise le temps de prédiction de 18 secondes au maximum pour LSFI-BF à 8 secondes au maximum pour LBFI. Les nombre des cas ratés est amélioré par rapport au LSFI-BF (2% vs 1.5%) et le nombre de faux positifs est diminué d'un tiers (96% vs 67%).

5.6 Conclusion

La détection de rupture de lien est une tâche difficile, en particulier dans les réseaux à haute dynamique (VANET), en raison de la mobilité et du comportement aléatoire du canal de propagation. Dans ce chapitre, une solution basée sur les évènements de décodage OFDM et la théorie

de croyance est présentée. L'indicateur prédictif de rupture de lien appelé LBFI (*Link Breakage Forecasting Indicator*) est proposé. Il utilise la théorie de Dempster-Shafer pour combiner les erreurs issues du décodage des trames OFDM afin de calculer la probabilité de rupture de lien. LBFI prend en compte l'évolution de la densité d'erreurs de décodage des paquets OFDM au cours du temps, ainsi que la puissance de réception des paquets pour calibrer les masses de $Comloss$ et $\overline{Comloss}$. La détection de la rupture est effectuée lorsque la masse de $Comloss$ devient plus importante que la masse $\overline{Comloss}$.

L'indicateur proposé fonctionne bien et est capable de détecter les défaillances de lien avant la perte de paquets. LBFI était évalué et comparé avec un autre indicateur de rupture de lien dans les VANET (LSFI-BF). Les résultats montrent que notre indicateur enregistre un meilleur temps de détection, un pourcentage de détection manquée et fausse que le LSFI-BF. Un tel indicateur peut renforcer les capacités des protocoles de routage à identifier l'état d'une route sélectionné et à agir en conséquence. Cela nous motive à implémenter cet indicateur dans un protocole de routage comme prochaine étape.

Chapitre 6

Optimisation du protocole de routage AODV pour les VANET

Sommaire

6.1 Introduction

Les réseaux véhiculaires possèdent un caractère qui peut être extrêmement dynamique avec une connectivité instable entre les nœuds. Des ruptures de liens sont susceptibles de se produire à tout instant ce qui provoque alors des pertes de paquets. Pour résoudre cette problématique, différents protocoles de routage doivent être équipés des mécanismes permettant la détection des ruptures de routes. L'objectif est d'identifier par avance une rupture de lien et de trouver un chemin alternatif avant que ce lien ne soit plus disponible.

Dans ce chapitre, une modification du protocole de routage AODV est proposée. L'indicateur prédictif de rupture de lien LBFI (*Link Breakage Forecasting Indicator*), présenté au chapitre précédent, remplace le système de détection de rupture de route de AODV. Quand LBFI détecte une rupture de lien à venir, le processus de maintenance de route de AODV pourra opérer avant que cette rupture ne provoque une perte de paquets. Ce chapitre est divisé en trois parties. Dans la première, le fonctionnement standard de AODV est présenté. La deuxième partie détaille les différentes modifications proposées. La troisième partie présente les résultats de leur évaluation par simulation.

6.2 Le protocole réactif AODV

Le protocole de routage AODV [91] est un protocole réactif. Il permet la construction de chemins multi-sauts afin d'acheminer des paquets entre deux nœuds distants. AODV établit des routes à la demande, lorsqu'un nœud (source) souhaite envoyer des paquets de données à un autre nœud (destination), un processus de découverte de route commence.

Dans les réseaux véhiculaires, AODV possède de meilleures performances par rapport aux autres protocoles de routage. En effet, des études [30, 92] comparent les différentes familles de protocoles de routage topologiques (réactif, proactif et hybride) à l'aide de simulations réalistes. L'étude présentée dans [30] compare entre trois protocoles pour chaque famille : réactif (AODV), proactif (OLSR) et hybride (ZRP). Chaque protocole est ainsi évalué en termes de taux de paquets reçus, d'overhead et de délai de transmission de bout en bout. Les résultats de cette étude

relèvent que le protocole AODV est le plus performant pour le routage des paquets dans les réseaux VANET avec un taux de paquets reçu meilleur de 15% par rapport à celui offert par OLSR et ZRP. Cette différence entre les performances des protocoles s'explique par leur gestion des ruptures de route [30].

Le protocole AODV ne maintient pas les routes entre tous les nœuds du réseau, mais uniquement les routes en cours d'utilisation. En effet, chaque route dans la table de routage du protocole AODV possède un *timer* appelé ART (*Active Route Timeout*). ART définit la durée pour laquelle une route est maintenue dans la table de routage après la dernière transmission d'un paquet sur cette route. L'expiration de ART entraîne la suppression de la route de la table de routage. À la demande, les routes sont découvertes et conservées aussi longtemps que nécessaires (c.-à-d. tant qu'il y a des paquets de données à transmettre et qu'il n'y a pas d'erreurs/de rupture dans le chemin établi). AODV mémorise une seule route par destination. Bien que cela réduise la charge sur chaque nœud, il en découle un problème lors des ruptures des routes puisqu'il ne supporte pas le routage multi-chemins. En cas de rupture d'une route active, AODV déclenche un nouveau processus de découverte de route, provoquant ainsi des délais dans la transmission de paquets. Étant donné que AODV arrête l'envoi des paquets sur une route lorsqu'elle est rompue, les paquets sont sauvegardés dans une file d'attente jusqu'à la découverte d'une nouvelle route. Cette procédure peut générer des délais de transmission importants.

6.2.1 Processus de découverte de routes dans AODV

Lorsqu'un nœud source (S) souhaite transmettre des paquets vers une destination (D), il cherche dans sa table de routage une route (c.-à-d. une entrée de table de routage) valide vers la destination. Si une route n'existe pas, AODV déclenche une phase de découverte de route. Le nœud source diffuse un message de demande de route à ses voisins, appelé *Route Request* (RREQ). Un nœud qui reçoit un message RREQ peut-être : i) soit la destination, ii) soit un nœud qui a une route valide vers la destination, iii) soit un nœud qui ne connaît pas de route vers la destination.

Dans le cas où le nœud est soit la destination, soit un nœud connaissant une route vers la destination, il génère un message appelé *Route Reply* (RREP) et le renvoie au nœud qui lui a envoyé le RREQ et ce de proche en proche jusqu'au nœud source du RREQ. Dans le cas où

le nœud n'est pas la destination et ne connaît pas de route vers la destination, celui-ci rediffuse le message RREQ à ses voisins. Le message RREP est renvoyé au nœud source par le chemin inverse utilisé lors de la diffusion des RREQ. Lorsque le message RREP arrive au nœud source, le processus de découverte de route est terminé, la nouvelle route est enregistrée dans la table de routage et la transmission des paquets de données peut commencer.

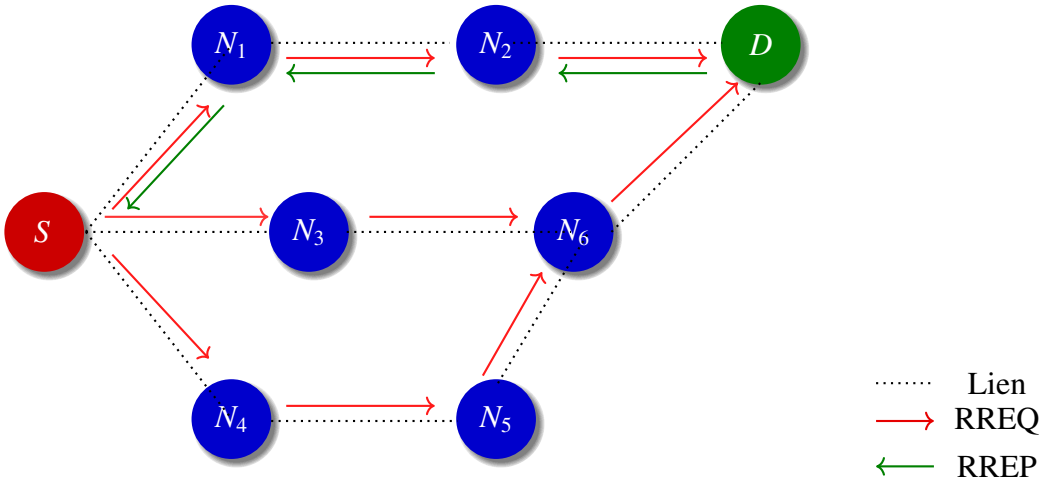


FIGURE 6.1 – Processus de découverte de route

La figure 6.1 montre un exemple de processus de découverte de route déclenché par le nœud S qui souhaite communiquer avec le nœud D. Le nœud source diffuse un message RREQ à ses voisins. Un paquet RREQ est caractérisé par son numéro de séquence et un identifiant de broadcast ($Sequence-number$ et $Broadcast-id$). Le $Broadcast-id$ est incrémenté à chaque fois que la source initialise un nouveau processus de découverte de route. Dans la figure, à la réception de la demande de route, les nœuds N_1, N_3 et N_4 cherchent dans leur table de routage une route valide vers le nœud D. Si une route est trouvée un message RREP est renvoyé à la source. Un nœud peut recevoir de multiples copies du même message RREQ depuis différents voisins. Dans ce cas (messages RREQ redondants), ces derniers sont supprimés en se basant sur $Broadcast-id$ et $Source-address$ (l'adresse du nœud source). Quand aucune route valide n'est trouvée chaque nœud rediffuse le message RREQ à ses voisins après l'incrémentation de nombre du sauts ($Hop-cnt$). Lorsque le RREQ arrive à la destination (D), le nœud D répond par un message RREP. Lorsque la source reçoit ce message RREP, la transmission des paquets de données démarre. En cas de chemins multiples, la sélection du meilleur se base sur le nombre de

sauts (si par exemple plusieurs RREP sont reçus par le nœud source). Le nœud source transfère les paquets vers le nœud de destination en utilisant la route sélectionnée. Cependant, en raison de la mobilité des nœuds, il se peut que certains nœuds se déplacent en dehors de la portée de communication et par conséquent des ruptures de lien se produisent. Ces ruptures ont pour conséquence des pertes de paquets (et donc de données) dans le réseau. Pour faire face à ce problème, AODV possède un mécanisme de maintenance de route.

6.2.2 Processus de maintenance de routes dans AODV

Le processus de maintenance de route consiste à trouver un chemin alternatif lorsque le chemin en cours d'utilisation tombe en panne. Ce processus ne s'exécute que sur les nœuds actifs. La connectivité entre les nœuds est gérée par l'échange des messages HELLO. Un message HELLO est un message RREP particulier dont la destination est égale à la source et le nombre de sauts est égal à zéro. Ainsi, si un nœud ne reçoit pas de paquet HELLO d'un voisin connu au cours d'une certaine période (ALLOWED_HELLO_LOSS * HELLO_INTERVAL ms selon la RFC [33]), la connexion entre eux est considérée comme interrompue. Un message *Route Error* (RERR) est alors envoyé à la source. Ce dernier contient l'adresse de destination qui est devenue injoignable (figure 6.2). Toutes les destinations injoignables seront marquées comme invalides dans les tables de routages des nœuds qui font partie des routes devenues défaillantes. À la réception d'un message RERR, le nœud source arrête l'envoi des paquets de données sur la route concernée vers le prochain saut enregistré et démarre un nouveau processus de recherche de route. Ce mécanisme de maintenance de route présente deux inconvénients principaux :

— La détection de la rupture de lien ne se fait qu'après la perte d'un certain nombre de paquets HELLO. Cela signifie que le lien est rompu avant la détection,

— La transmission de données sera interrompue à partir du moment où la rupture est détectée, jusqu'à ce qu'un autre chemin soit découvert.

Pour pallier ces faiblesses, un système de maintenance basé sur l'indicateur de rupture de lien LBFI est proposé dans la suite de ce chapitre. LBFI surveille la connectivité entre voisins et réalise ainsi une détection anticipée de rupture des liens ce qui permet de notifier à l'avance le nœud source. La section suivante détaille le processus de maintenance de route proposé.

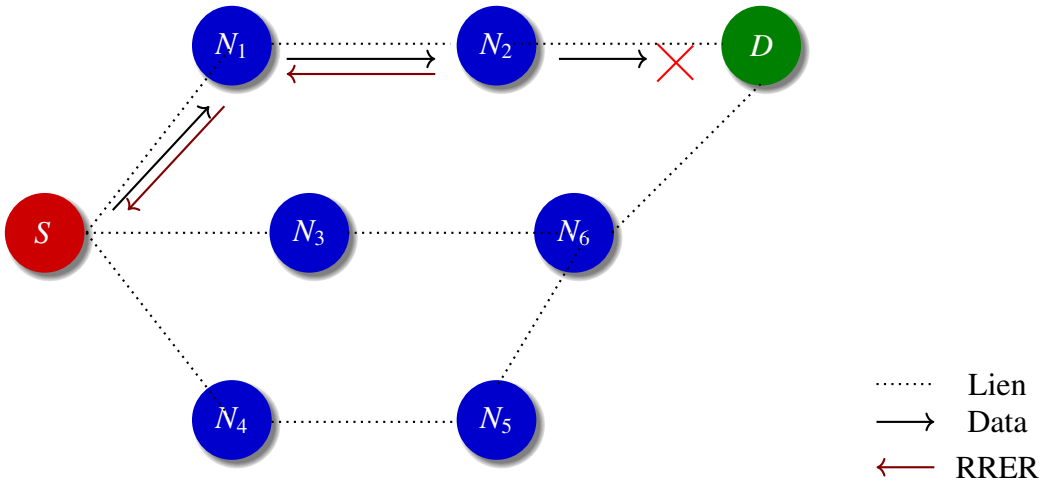


FIGURE 6.2 – Processus de maintenance de route

6.3 AODV basé sur LBFI pour les VANET (AODV-LBFI)

Le mécanisme de détection de rupture de lien du protocole AODV se base sur la réception des messages RERR (qui sont envoyés dans le réseau lorsqu'il y a une perte de message HELLO dans un intervalle de temps). Lorsque ce type de message est reçu, il indique une rupture de route et donc la perte de paquets de données et la mise en attente d'autres paquets jusqu'à l'établissement d'une nouvelle route. L'indicateur prédictif de rupture de lien LBFI présenté dans le chapitre 5 permet de détecter la rupture d'un lien avant qu'elle se produise. L'introduction de LBFI dans le protocole ADOV permet donc d'anticiper les ruptures de lien et donc de minimiser la perte de paquets.

6.3.1 Processus de maintenance de routes de AODV-LBFI

Le processus de maintenance de route de AODV-LBFI se base sur l'indicateur prédictif de rupture de lien (LBFI) présenté dans le chapitre 5. Les messages échangés entre les nœuds qu'ils soient issus du protocole AODV (messages HELLO, RREQ, RREP et même RERR) ou des données échangés permettent à LBFI de détecter une éventuelle rupture du lien entre voisins. Chaque nœud peut ainsi surveiller l'état du lien avec ses voisins qu'il soit nœud émetteur de données ou nœud récepteur (la détection peut être faite au niveau du nœud émetteur comme au niveau du récepteur). Pour autant le nombre de messages entre un nœud émetteur et nœud récepteur n'est pas symétrique. En effet, un nœud recevant des données en plus des messages

de protocoles (RREQ, RREP, HELLO) reçoit quantitativement plus de paquets qu'un nœud ne recevant que les messages du protocole AODV. Cette asymétrie réduit l'efficacité de l'indicateur LBFI. Les messages HELLO sont utilisés pour gérer la table des voisins et alimenter LBFI. La connectivité entre les nœuds est contrôlée par LBFI. Cela signifie que les temps de détection ne sont pas identiques à cause de la quantité d'informations reçue par chaque nœud (le nœud récepteur des paquets de données possède plus d'informations sur l'état du lien, comme il décode plus de paquets que le nœud émetteur et donc plus d'information pour alimenter LBFI.).

Chaque nœud du réseau possède une liste "noire" où il marque les liens qui sont susceptibles de rompre, c'est-à-dire les liens pour lesquels LBFI indique une rupture à venir. Cette fonctionnalité permet aux nœuds d'éviter les messages de demande de route (RREQ) et les messages de réponse de route (RREP) en provenance des liens à risque. Une fois qu'un nœud détecte une rupture de lien, un message RERR est envoyé au nœud source. Lorsque le nœud source reçoit le message d'erreur, il relance le processus de découverte de route. Durant ce processus, la transmission des paquets de données continue, le lien étant encore utilisable jusqu'à la rupture effective. Ce processus permet d'optimiser l'utilisation de la route tout en cherchant une alternative viable. Une fois la nouvelle route trouvée, la transmission des paquets de l'ancienne route s'arrête et elle sera marquée invalide dans la table de routage. Les paquets sont par la suite acheminés vers la destination en utilisant la nouvelle route.

Durant le processus de découverte de route, les messages RREQ sont diffusés dans tout le réseau. Si un nœud (A) reçoit deux messages RREP (ou deux demandes de route RREQ) en provenance d'un nœud (B) qui figure sur la liste noire du nœud A, A considère que son lien avec B ne présente plus de risque de rupture et retire B de sa liste noire. Ce processus minimise la probabilité du choix d'un lien en risque de rupture dans le processus de construction de la nouvelle route.

Exemple de processus de maintenance de route de AODV-LBFI La figure 6.3 illustre un exemple de scénario de maintenance de route effectué par le protocole AODV-LBFI. Le nœud source (S) utilise le chemin I_1-I_2 pour acheminer les paquets de données au nœud destination D (figure 6.3(a)). Tous paquets reçus (paquets de données et paquets de contrôle) sont utilisés pour alimenter l'indicateur LBFI. Quand LBFI indique une rupture de lien à venir, un message d'erreur est envoyé à la source (figure 6.3(b)). Dans le scénario de la figure 6.3(b), LBFI détecte

une rupture à venir entre le nœud I_1 et le nœud I_2. Le nœud détecteur (I_2) marque alors le nœud I_1 dans sa liste noire. Durant le processus de recherche de route les données sont acheminées sur le chemin I_1-I_2 (figure 6.3(c)). À la découverte d'un nouveau chemin, AODV-LBFI bascule de l'ancienne route vers la nouvelle (figure 6.3(d)) .

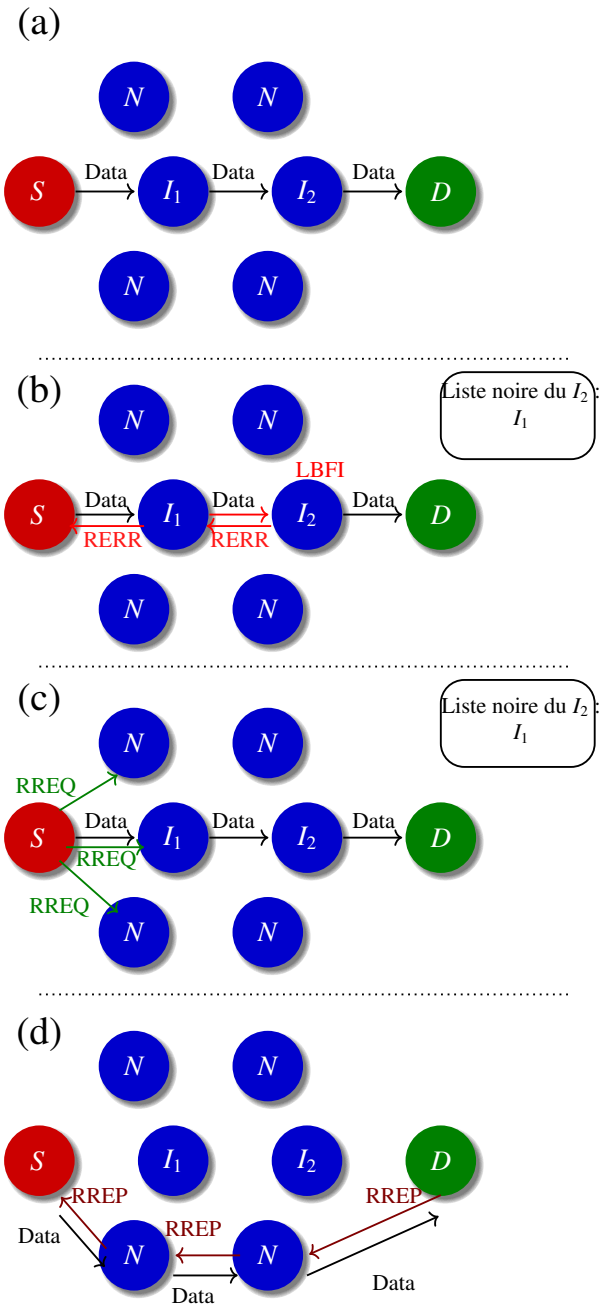


FIGURE 6.3 – Processus de maintenance de route du protocole AODV-LBFI

Le fonctionnement du mécanisme de maintenance de route proposé est décrit par deux algorithmes :

— L'algorithme 6.1 qui décrit le comportement d'un nœud qui détecte une rupture de lien. Si LBFI détecte une rupture d'un lien X, un message d'erreur est envoyé à la source et le lien X est rajouté à la liste noire. Durant le processus de découverte de route, toute réception de messages RREQ ou RREP en provenance d'un nœud inscrit dans une liste noire sera ignorée car ces liens risquent de rompre à tout moment. Un compteur est utilisé pour compter le nombre de messages RREQ et RREP reçus sur le lien X. Si le nombre de messages reçus est supérieur ou égal à 2, le lien X sera supprimé de la liste noire et considéré comme en bon état (pas de risque de rupture),

— L'algorithme 6.2 décrit le comportement du nœud source. Lorsque la source reçoit un message d'erreur (RERR) elle déclenche un processus de découverte de route en diffusant des messages RREQ dans le réseau. Et à la réception d'une réponse de route (RREP) la source bascule de l'ancien chemin vers le nouveau chemin.

L'intégration de LBFI dans AODV permet donc de détecter les ruptures de liens et informer AODV à l'avance afin de trouver une route alternative. Dans la prochaine section, des résultats de simulations sont présentées.

Algorithm 6.1 Nœud détectant une rupture de route

```
if LBFI détecte une rupture de lien avec un nœud voisin (X) then
    - Envoyer un message RRER à la source ;
    - Ajouter le lien X à la liste noire ;
end if
if le nœud reçoit un message (Msg) then
    if (Msg == RREP) || (Msg == RREQ) then
        if compter ≥ 2 then
            - compter=0 ;
            - supprimer le lien X de la liste noire ;
            - traiter le message(Msg) ;
        else
            if le lien X ∈ liste noire then
                - Ignorer(Msg) ;
                - compteur++ ;
            else
                - traiter le message (Msg) ;
            end if
        end if
    end if
end if
```

Algorithm 6.2 Nœud source

```
if le nœud reçoit un message (Msg) then
    if Msg == RERR then
        Diffuser (RREQ) ;
    end if
    if Msg == RREP then
        - Basculer de l'ancien chemin vers le nouveau ;
    end if
end if
```

6.4 Simulations et résultats

Pour évaluer les performances du nouveau protocole AODV-LBFI, des scénarios de mobilité mettant en œuvre des nœuds qui se déplaçent aléatoirement dans une infrastructure routière du type *Manhattan Grid* [1] ont été utilisés. Les simulations sont effectuées à l'aide du simulateur NS3, déjà utilisé précédemment dans l'étude de LBFI. Les résultats ont été produits à partir des séries de simulations mettant en oeuvre des graines de génération de nombre aléatoire différentes. Cinq graines différentes ont été utilisées. Un résumé de l'ensemble des paramètres de simulation est fourni dans le tableau 6.1. Les critères d'évaluation sont : i) le taux de paquet reçu (PDR), ii) le délai de bout en bout, iii) le nombre de paquets de contrôle au regard du nombre de paquets de données, iv) le nombre de changements de route. Ces critères permettent de réaliser une évaluation comparative entre le protocole AODV standard et notre proposition AODV-LBFI.

Paramètre	***Valeur***
Simulateur	NS3
Temps de simulation (s)	80
Nombre de véhicules	{10, 50, 100}
Nombre des nœuds communiquants	10
Couche MAC	802.11p
Modèle de propagation	Path loss, shadowing, fast fading et doppler
Vitesse des nœuds ($m.s^{-1}$)	up to 13
Taille de la zone de simulation (m)	600 X 600
Architecture de routes	Manhattan grid 6X6
Taille de données (octets)	256
Débit de données (paquets/s)	10
Temps inter messages HELLO (s)	1

TABLE 6.1 – Paramètres de simulation

1. Manhattan Grid modélise une architecture de routes urbaines.

6.4.1 Représentation des résultats

Cette section explique le principe des *boîtes à moustaches* qui sont utilisées pour représenter les résultats de cette évaluation. Une boîte à moustaches (aussi appelée *boxplot*) permet de visualiser, d'identifier les valeurs extrêmes et de comprendre la distribution des données. Elle comprend les valeurs minimales et maximales de l'intervalle des valeurs, les quartiles supérieurs et inférieurs et la médiane. Cette collection de valeurs est un moyen rapide pour résumer la distribution d'un ensemble de données. De plus, cette représentation basée sur cinq nombres permet de comparer facilement des ensembles de données.

Pour lire une boîte à moustaches, il faut repérer les éléments suivants (figure 6.4) :

— l'échelle des valeurs de la variable (l'axe vertical),

— la valeur du premier quartile Q_1 (25% des effectifs), qui correspond au trait inférieur de la boîte,

— la valeur du deuxième quartile Q_2 ou la médiane (50% des effectifs), qui correspond au trait à l'intérieur de la boîte,

— la valeur du troisième quartile Q_3 (75% des effectifs), qui correspond au trait supérieur de la boîte,

— les valeurs aberrantes, représentées par des points. Ces valeurs correspondent à une/des observations exceptionnelles, élevées ou faibles.

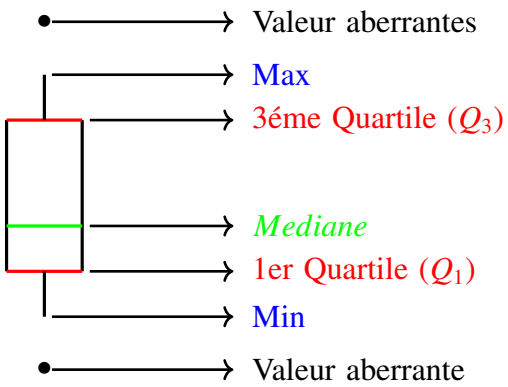


FIGURE 6.4 – Lecture d'une boite à moustaches

Exemple d'interprétation d'un diagramme de boîte à moustaches Les diagrammes de boîtes à moustaches sont utilisés pour montrer les schémas globaux des données analysées. Ils fournissent un moyen utile pour représenter une distribution des données. La figure 6.5 présente un exemple de différentes formes de boîte à moustaches.

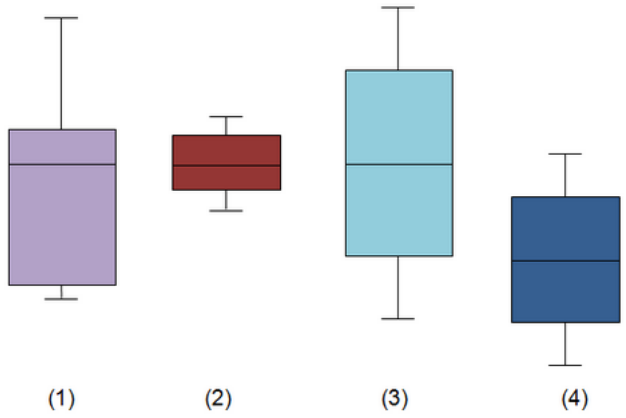


FIGURE 6.5 – Exemple des boîtes à moustaches

Analyse de quelques boîtes à moustaches typiques :

— *La boîte à moustaches est relativement petite*, comme dans les cas (2) et (4). Cela veut dire que les valeurs globales des données sont très proches les unes des autres,

— *La boîte à moustaches est relativement grande*, comme dans les exemples (1) et (3). Cela montre que les valeurs des données sur l'aspect étudié sont très dispersées,

— *Les quatre sections de la boîte à moustaches sont de taille inégale*, les variations des rectangles allant du premier quartile ou troisième quartile témoignent des différences d'un même caractère représenté par des jeux de données. Or, dans l'exemple (1), les quatre sections de la boîte à moustaches sont de tailles inégales. La barre supérieure de la boîte à moustaches dans l'exemple signifie que les valeurs des données varient parmi le groupe du quartile le plus positif, et sont très similaires pour le groupe du quartile le moins positif.

6.4.2 Taux de paquets reçus (PDR)

C'est le rapport entre le nombre de paquets de données reçus et nombre de paquets de données envoyés. Chaque simulation possède dix liens de communication.Le PDR reflète l'efficacité du protocole et est exprimé en pourcentage.

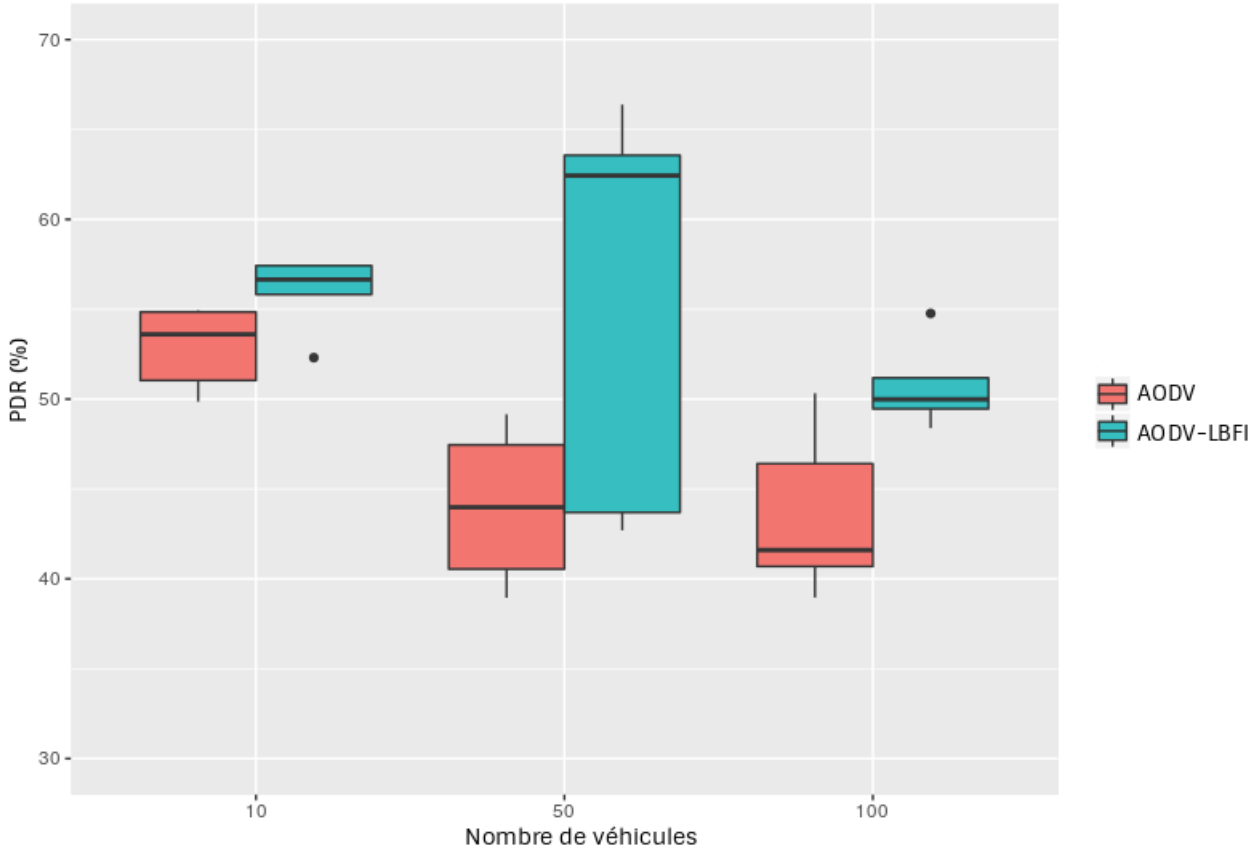


FIGURE 6.6 – Taux de délivrance de paquets en fonction du nombre de véhicules

Comme le montre la figure 6.6, le protocole AODV-LBFI est plus efficace que le protocole AODV pour différentes densités de véhicules. Les taux de réception des paquets avec AODV-LBFI sont plus élevés que ceux avec AODV. Prenons le cas d'une densité des nœuds égale à 10, 75% des valeurs de PDR fournies par le protocole AODV sont inférieures ou égales à 54% et supérieures ou égale à 50%. Pour le protocole AODV-LBFI, 75% des valeurs de PDR sont inférieures ou égales à 58 et supérieures ou égale à 55. Dans le cas d'une densité du réseau égale à 50 nœuds, la valeur maximale des PDR fournie par AODV est égale à 50, tandis que pour AODV-LBFI, cette valeur est égale à 68. 75% des PDR fournis par AODV sont supérieures ou

égales à 39, alors que pour le protocole AODV-LBFI, 75% des PDR sont supérieurs ou égaux à 45. Dans le cas d'une densité égale à 100, la distribution des valeurs de PDR pour le protocole AODV varie dans l'intervalle [40, 51]. Tandis que les valeurs de PDR de AODV-LBFI varient dans l'intervalle [50, 53].

Ce gain découle de la prise en compte d'une rupture de lien à l'aide de l'indicateur prédictif LBFI. Dans ce cas, une route alternative est recherchée tout en continuant d'utiliser la route actuelle. Ce mécanisme permet d'optimiser l'utilisation du chemin actuel et de changer le chemin avant que la rupture ne soit effective.

6.4.3 Délai de bout en bout

Le délai de bout en bout (*End to End Delay* - E2ED) est le délai de livraison d'un paquet depuis son émission par le nœud source jusqu'à sa réception par le nœud destination.

La figure 6.7 présente la distribution cumulative des délais de bout en bout calculée pour les paquets de données reçus pendant le temps de simulation pour les deux protocoles AODV et AODV-LBFI et cela pour différentes densités de réseau (10, 50 et 100 nœuds). On observe que les temps de délivrance des paquets pour AODV-LBFI sont plus courts que ceux du AODV. Dans le cas d'un réseau de 10 nœuds, 86% des paquets de AODV-LBFI ont un E2ED inférieur à 2 secondes, alors que pour AODV 78% des paquets ont un E2ED inférieur à 2 secondes. Pour les réseaux à plus haute densité de nœuds, AODV-LBFI obtient un E2ED inférieur à celui de AODV. Par exemple, dans le cas d'un réseau de 50 nœuds, tous les E2ED de AODV-LBFI sont inférieurs à 5 secondes tandis que avec AODV, les E2ED peuvent atteindre jusqu'à 10 secondes. Pour un réseau de 100 nœuds, 99% des paquets de AODV-LBFI ont un E2ED inférieur à 3 secondes, ce qui est mieux comparé au E2ED de AODV.

Ces bons résultats sont principalement dûs à la capacité de AODV-LBFI à anticiper une future rupture de lien, ce qui lui permet de trouver une nouvelle route avant que la liaison actuellement utilisée ne tombe, contrairement à AODV qui ne réagit que lorsque la liaison est rompue ce qui entraîne un stockage des paquets pendant la recherche de route et donc un délai supplémentaire. À noter que le E2ED n'est calculé que sur les paquets reçus et ne prend pas en compte les paquets perdus.

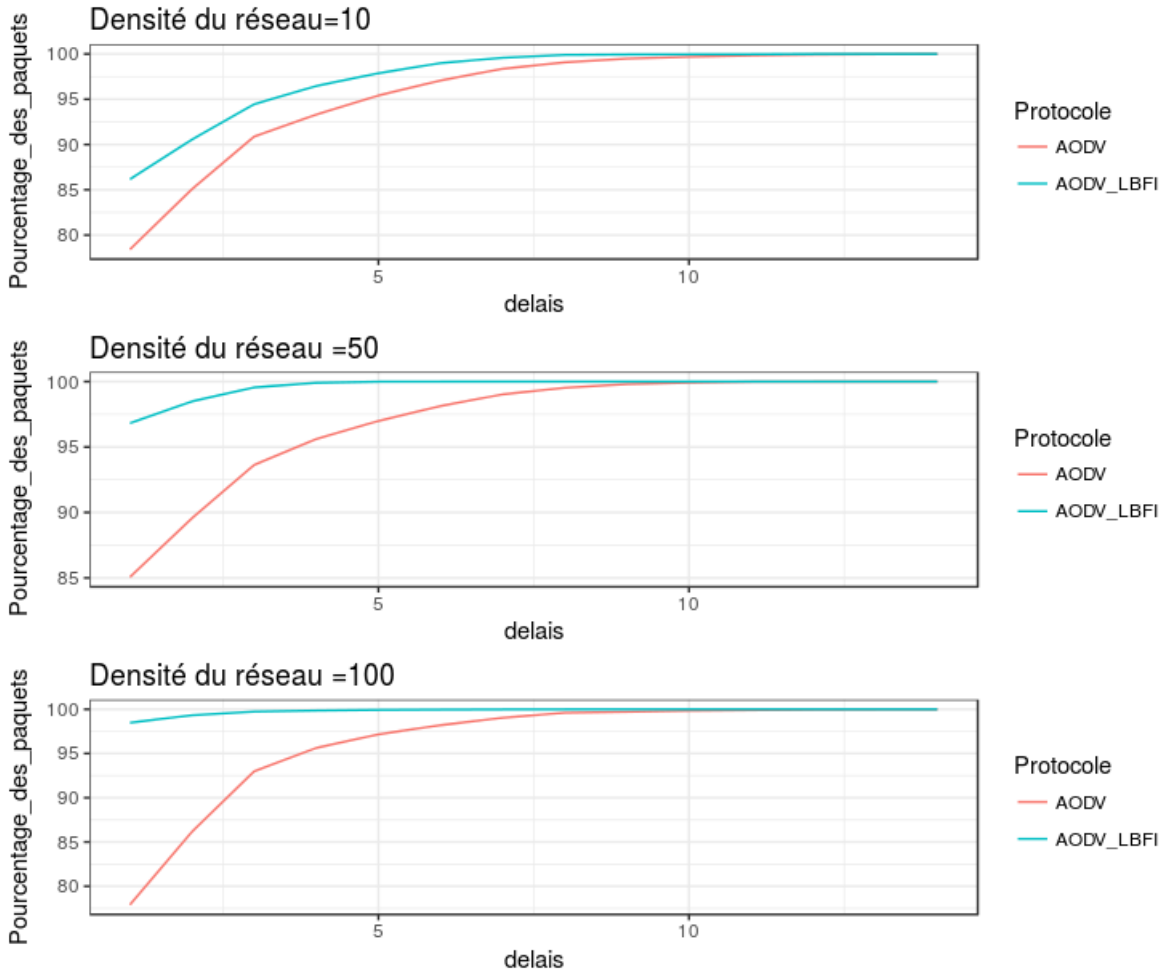


FIGURE 6.7 – Délai de bout en bout pour 10 nœuds, 50 nœuds et 100 nœuds

6.4.4 Overhead

L'*overhead* mesure le nombre de paquets de contrôle au regard du nombre de paquets de données et est exprimé en %. Il reflète le taux de paquets de contrôle utilisés pour construire et maintenir les routes et mesure l'efficacité du routage.

La figure 6.8 montre l'overhead de routage pour les deux protocoles. Dans certains cas, comme dans le scénario avec 50 nœuds, l'overhead de AODV-LBFI dépasse celui d'AODV. En effet, le nombre de messages RERR envoyés augmente avec le nombre de détections de ruptures de liens opérées par LBFI.

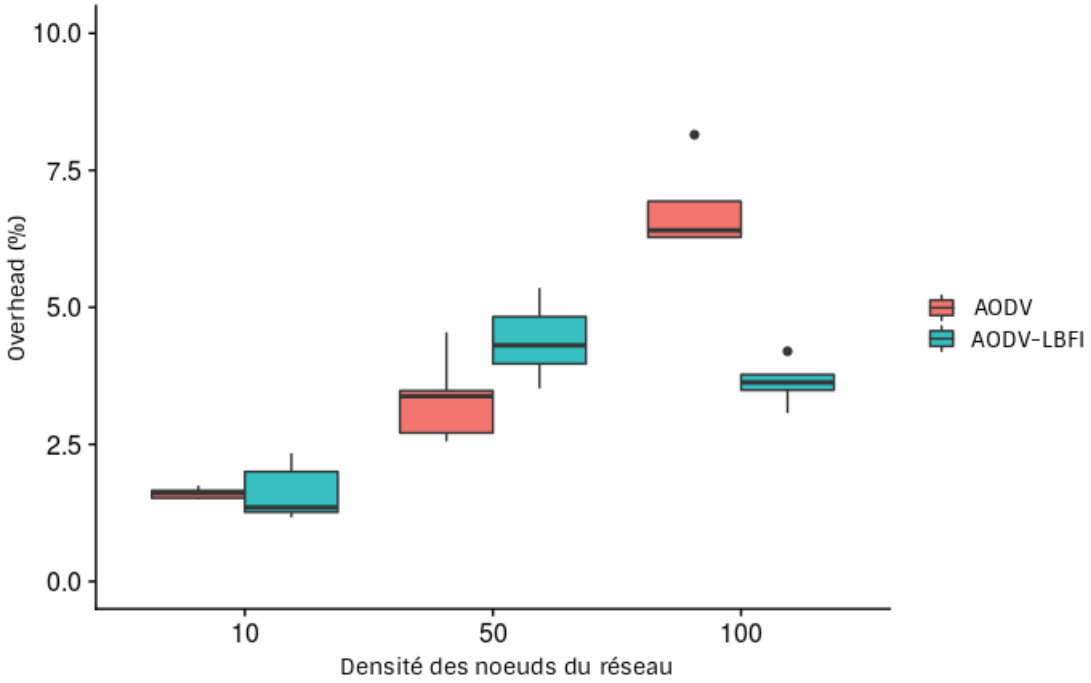


FIGURE 6.8 – L'overhead vs la densité du réseau

6.4.5 Nombre de changements de route

Les changements de route montrent l'efficacité du protocole et reflètent la stabilité des routes utilisées par le protocole. Il a un impact sur l'overhead et sur le délai de livraison des paquets. Le changement de route considéré ici est celui effectué lors du processus de maintenance des routes rompues à cause d'une rupture de lien.

La figure 6.9 montre le nombre moyen de changements de route en fonction de la densité de véhicules. Le nombre de substitutions de routes opérées par AODV-LBFI est inférieur à celui de AODV. Cela découle directement de l'utilisation de LBFI pour détecter les défaillances. Contrairement au système de détection de AODV basé sur les messages HELLO, AODV-LBFI fournit une détection appropriée qui permet une meilleure utilisation de la route et minimise donc le nombre de changements de route.

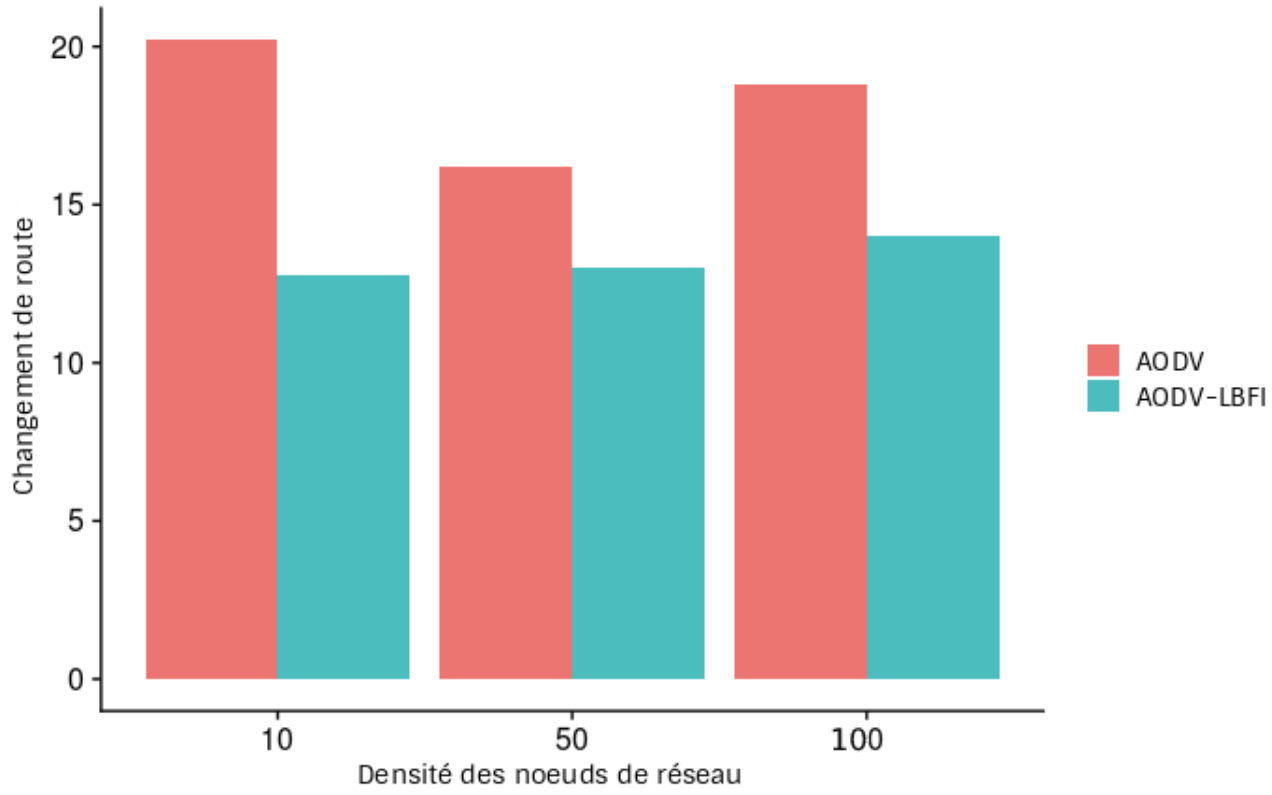


FIGURE 6.9 – Changements de routes vs la densité du réseau

6.5 Conclusion

Dans ce chapitre, une amélioration du protocole AODV a été proposée au travers de l'utilisation de l'indicateur LBFI. Cette nouvelle version de AODV, appelée AODV-LBFI, est fondée sur l'indicateur LBFI qui prédit les ruptures de liens en analysant le trafic entrant d'un nœud. Fonctionnant au niveau de la couche physique, LBFI effectue une analyse approfondie des événements de décodage OFDM et prédit si une rupture de lien va se produire. LBFI a été implémenté dans le protocole ADOV afin de détecter les défaillances des liens locaux avant qu'elles ne se produisent de façon à permettre de découvrir un chemin alternatif avant la rupture effective du lien. Les résultats révèlent que le taux de paquets reçus, le délai de livraison des paquets sont améliorés malgé un overhead de paquets de signalisation plus important. La densité de nœuds influe considérablement sur le délai de bout en bout, vu que l'écart entre les délais de AODV-LBFI et AODV devient plus important lorsque la densité augmente. En termes de stabilité de route, AODV-LBFI

effectue moins de changements de route que AODV. Certaines améliorations restent encore à apporter notamment concernant l'overhead.

Chapitre 7

Conclusion et perspectives

Sommaire

7.1 Conclusion générale

La croissance de la demande de communication sans fil et le développement des appareils sans fil ont mené à des recherches sur des réseaux sans fil auto-organisables, d'où l'apparition des réseaux ad hoc mobiles(textitMANET). Les réseaux véhiculaires (*VANET*) représentent une sous-catégorie des *MANET*. La mobilité est la principale caractéristique de la plupart des nœuds du réseau VANET. Cependant, cette mobilité est restreinte, limitée et contrôlée par un plan routier et des règles de circulation des véhicules (limites de vitesses, feux de signalisation). Du point de vue de la propagation des ondes, les zones urbaines constituées par des bâtiments et autres obstacles influencent la propagation ce qui impacte la communication dans les réseaux véhiculaires.

La communication au sein d'un réseau de véhicule est basée sur des protocoles de routage, qui gère et détermine la méthode de mise en place et la maintenance des chemins entre les noeuds de réseau. Malheureusement, bien que de nombreux protocoles de routage ont été conçus dans les MANET, un bon nombre de ces protocoles ne sont pas adaptés à l'utilisation dans les VANET. Ceci, en raison de la forte mobilité et des conditions du canal de propagation, qui

causent des ruptures de routes et rendent difficile l'acheminement des paquets. Une solution consiste à anticiper les ruptures des routes et informer le protocole de routage à l'avance pour initialiser le processus de maintenance de route.

Les travaux menés dans le cadre de cette thèse sont centrés sur la construction d'un indicateur prédictif de rupture de lien pour les réseaux véhiculaires. L'indicateur proposé dans cette thèse est implémenté par la suite dans le protocole de routage réactif *AODV*, afin de permettre une maintenance prédictive des routes. Cette maintenance prédictive permet de détecter les routes avant que le lien ne se rompe ce qui conduit à augmenter la fiabilité du réseau en termes d'augmentation du taux de délivrance des paquets, de réduction de nombre de changement de route et des délais de bout en bout soit de la source à la destination.

La première contribution de cette thèse est présentée dans le chapitre 5, qui introduisait un nouvel indicateur de rupture de lien pour les VANET appelé Link Breakage Forecasting Indicator *LBFI*. Le processus de détection de rupture de lien peut être réalisé à différents niveaux. Dans cette étude, la couche physique et plus particulièrement le décodage ont été utilisés. Les informations fournies lors de la réception des paquets ont été utilisées pour développer cet indicateur. Ces informations sont issues du processus de décodage Orthogonal Frequency-Division Multiplexing *OFDM*. L'intérêt d'utiliser le processus de décodage OFDM est qu'il produit des informations utiles pour la détection de rupture de lien notamment des erreurs de décodage lorsque le lien se dégrade. Ces erreurs de décodage ont été exploitées dans le cadre d'anticipation de rupture de lien. La première étape est d'étudier et analyser le comportement des indicateurs existants dans la littérature et qui se basent sur le décodage OFDM. Suite à cette analyse, un modèle mathématique de détection de rupture de lien basé sur la théorie des fonctions de croyance a été proposé.

La théorie des fonctions de croyance aussi connue sous le nom de la théorie de Dempster-Shafer est l'un des outils de raisonnement qui tient compte de l'incertitude. Le choix d'utilisation de cette théorie est le résultat d'une analyse de la nature des données utilisées : les erreurs de décodage OFDM, la vitesse des noeuds et la puissance de signal reçu. Les données collectées, qui ne sont pas exactes au sens mathématique du terme possèdent un certain degré d'imperfection. Il était donc nécessaire d'utiliser un outil mathématique permettant la gestion d'imperfection, d'où le choix de la théorie des fonctions de croyance.

La deuxième contribution est présentée dans le chapitre 6. L'indicateur de rupture de lien

LBFI a été mise en oeuvre dans le protocole de routage AODV. Ce nouveau protocole appelé AODV-LBFI a remplacé le mécanisme de détection de rupture traditionnel de AODV par l'indicateur LBFI. L'indicateur proposé ici est capable de détecter une rupture de lien et d'informer AODV afin qu'il puisse opérer un processus de maintenance de route au plus tôt au travers de la recherche d'une route alternative tout en optimisant l'utilisation du lien actuel.

Des simulations ont été réalisées avec NS-3, simulateur des réseaux ad hoc. Ce simulateur sous licence GNU GPLv2 est destiné principalement à la recherche et à l'enseignement. NS-3 était un choix d'outil d'évaluation pertinent dans le cadre de cette étude puisqu'il permet l'utilisation d'un module *PhysimWifi* qui émule toutes les étapes de décodage OFDM. Il a été ainsi montré que l'indicateur de rupture de lien LBFI pour les réseaux véhiculaires donne des meilleures performances par rapport à d'autres indicateurs. Il permet la détection de ruptures de liens dans différents scénarios avec des temps de détection permettant une nouvelle recherche de route optimale, en diminuant le nombre de fausses détection et de cas ratés en comparaison avec d'autres indicateurs existants.

L'évaluation des performances du nouveau protocole AODV-LBFI montre une amélioration en terme de taux de réception de paquet, les délais de bout en bout et la stabilité des routes.

De ce fait, nous avons constaté qu'il est largement adaptable aux environnements des réseaux véhiculaires.

7.2 Perspectives

Les réseaux véhiculaires demeurent un sujet de recherche actuel dans le domaine des communications sans fil compte tenu de l'évolution des technologies et de manière plus générale l'intégration des véhicules dans la ville intelligente (*Smartcity*). Ces aspects reposent sur la communication et sur la fiabilité de la transmission des données. L'indicateur LBFI développé ici qui a été couplé au protocole AODV nécessite un passage de la simulation vers des tests à grandes échelles afin de valider l'ensemble des résultats obtenus. Cet indicateur peut être également utilisé dans les MANET afin de fiabiliser la transmission des données. Il serait intéressant de voir si cette amélioration impacte également ce type de réseau. Un point qui n'a pas été abordé dans cette thèse est l'ajout d'une couche de sécurité dans ces réseaux qui est un élément essentiel dans la communication.

Liste des publications

Article de journal international avec comité de lecture

-Bourebia, S., Laghmara, H., Hilt, B., Drouhin, F., Bindel, S., Ledy, J.,Lauffenburger,J. Lorenz, P. "A belief function-based forecasting link breakage indicator for VANETs". *Wireless Networks*, 2019, 1-16.

Conférence internationale avec comité de lecture

-Bourebia, S., Hilt, B., Drouhin, F. Lorenz, P. "A new AODV based forecasting link breakage indicator for VANETs", *Globcom*, 2019.

Journée de recherche

-Bourebia, S., Hilt, B., Drouhin, F., Bindel, S., Ledy, J.,Lauffenburger,J. Lorenz, P. "Indicateur de rupture de lien pour les réseaux véhiculaires". *jnct2017 : Journées Nationales des Communications Terrestres* 2017.

-Bourebia, S., Hilt, B., Drouhin, F., Bindel, S., Ledy, J.,Lauffenburger,J. Lorenz, P. "Fusion de données pour la détection de rupture de lien dans les VANET". *Journée thématique sur les Réseaux Véhiculaires (REVE)*, 2018.

Références bibliographiques

[1] Stylianos Papanastasiou, Jens Mittag, Erik G Strom, and Hannes Hartenstein. Bridging the gap between physical layer emulation and network simulation. In *2010 IEEE Wireless Communication and Networking Conference*, pages 1–6. IEEE, 2010.

[2] Hanene Gabteni. *Prédiction de rupture de lien dans les VANETs basée sur une modélisation réaliste du canal de transmission*. PhD thesis, Université de Haute Alsace, 2016.

[3] Jonathan Ledy, Frederic Drouhin, Jeremie Daniel, Michel Basset, Benoit Hilt, Hanene Gabteni, and Pascal Lorenz. Data fusion for a forecasting link state indicator in vanets. In *2016 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6. IEEE, 2016.

[4] Soumia Bourebia, Hind Laghmara, Benoit Hilt, Frédéric Drouhin, Sébastien Bindel, Jonathan Ledy, Jean-Philippe Lauffenburger, and Pascal Lorenz. A belief function-based forecasting link breakage indicator for vanets. *Wireless Networks*, pages 1–16, 2019.

[5] Hironao Kawashima. Japanese perspective of driver information systems. *Transportation*, 17(3) :263–284, 1990.

[6] Hannes Hartenstein and Kenneth Laberteaux. *VANET : vehicular applications and internetworking technologies*, volume 1. Wiley Online Library, 2010.

[7] Brijesh Kumar Chaurasia, Md Iftekhar Alam, Arun Prakash, Ranjeet Singh Tomar, and Shekhar Verma. Mpmac : Clustering based mac protocol for vanets. *Wireless Personal Communications*, pages 1–28, 2019.

[8] Imad Eddine TLEMSANI. *Déploiement efficace des RSUs dans les VANETs en utilisant des approches métaheuristiques*. PhD thesis, 15-05-2019, 2018.

[9] Georgios Karagiannis, Onur Altintas, Eylem Ekici, Geert Heijenk, Boangoat Jarupan, Kenneth Lin, and Timothy Weil. Vehicular networking : A survey and tutorial on requirements, architectures, challenges, standards and solutions. *IEEE communications surveys & tutorials*, 13(4) :584–616, 2011.

[10] Hannes Hartenstein and LP Laberteaux. A tutorial survey on vehicular ad hoc networks. *IEEE Communications magazine*, 46(6) :164–171, 2008.

[11] Mihail L Sichitiu and Maria Kihl. Inter-vehicle communication systems : a survey. *IEEE Communications Surveys & Tutorials*, 10(2) :88–105, 2008.

[12] Roberto Baldessari, B Bödekker, A Brakemeier, M Deegener, A Festag, W Franz, A Hiller, C Kellum, T Kosch, A Kovacs, et al. Car to car communication consortium manifesto : overview of the c2c-cc system. *C2C-CC, Version*, 1, 2009.

[13] Jean-Nicola RUSSO. *Risk level assessment for driver and automotive with a Bayesian Network in the context of car communicating*. PhD thesis, Université de Haute Alsace, 2018.

[14] M Maile. Vehicle safety communications–applications (vsc-a) project : Crash scenarios and safety applications. *Mercedes-Benz Research and Development North Amercia, Inc*, 2009.

[15] Abbas Bradai and Toufik Ahmed. Reviv : Selective rebroadcast mechanism for video streaming over vanet. In *2014 IEEE 79th Vehicular Technology Conference (VTC Spring)*, pages 1–6. IEEE, 2014.

[16] Paulo Bezerra, Adalberto Melo, Allan Douglas, Hugo Santos, Denis Rosário, and Eduardo Cerqueira. A collaborative routing protocol for video streaming with fog computing in vehicular ad hoc networks. *International Journal of Distributed Sensor Networks*, 15(3) :1550147719832839, 2019.

[17] Daxin Tian, Chuang Zhang, Xuting Duan, Yunpeng Wang, Jianshan Zhou, and Wei Hao. *A Bio-Inspired Video Transmission Routing Protocol for VANETs in City*, pages 5721–5732. ASCE library.

[18] Eduardo Cambruzzi, Jean-Marie Farines, Raimundo Jose Macedo, and Werner Kraus. An adaptive failure detection system for vehicular ad-hoc networks. In *2010 IEEE Intelligent Vehicles Symposium*, pages 603–608. IEEE, 2010.

[19] Sofiane Zemouri, Soufiene Djahel, and John Murphy. A fast, reliable and lightweight distributed dissemination protocol for safety messages in urban vehicular networks. *Ad Hoc Networks*, 27 :26–43, 2015.

[20] Rene Oliveira, Carlos Montez, Azzedine Boukerche, and Michelle S Wangham. Reliable data dissemination protocol for vanet traffic safety applications. *Ad Hoc Networks*, 63 :30–44, 2017.

[21] ETSI. European telecommunications standards institute etsi. https ://www.etsi.org/.

[22] TCITS ETSI. Intelligent transport systems (its) ; users and applications requirements ; part 2 : Applications and facilities layer common data dictionary. *ETSI TS*, 102 :894–2, 2014.

[23] Abdel Mehsen Ahmad. *Techniques de transmission et d'accès sans fil dans les réseaux ad-hoc véhiculaires (VANETS)*. PhD thesis, Evry, Institut national des télécommunications, 2012.

[24] US Federal Communications Commission et al. R&o fcc 03-324,". *Dedicated Short Range Communications Report and Order*, 2003.

[25] Roberto A Uzcátegui, Antonio Jose De Sucre, and Guillermo Acosta-Marum. Wave : A tutorial. *IEEE Communications magazine*, 47(5) :126–133, 2009.

[26] IEEE. Wireless lan medium access control (mac) and physical layer (phy) specifications and regulations specifications ; amendment 7 : Wireless access in vehicular environments. *IEEE Vehicular Technologie Society*, 2010.

[27] Ranjeet Singh Tomar, Brijesh Kumar Chaurasia, Shekhar Verma, and Rajendra Singh Kushwah. Network connectivity in vanets. In *Proceedings of the Third International Conference on Soft Computing for Problem Solving*, pages 767–775. Springer, 2014.

[28] Surmukh Singh and Sunil Agrawal. Vanet routing protocols : Issues and challenges. In *2014 Recent Advances in Engineering and Computational Sciences (RAECS)*, pages 1–5. IEEE, 2014.

[29] Salim Allal. *Optimisation des échanges dans le routage géocast pour les réseaux de Véhicules Ad Hoc VANETs*. PhD thesis, Paris 13, 2014.

[30] Jonathan Ledy. Conception cross-layer modèle de couche-physique protocoles de routage qualité de service réseaux ad hoc de véhicules simulation systèmes à entrées multiples et à sorties multiples vanets. 2012.

[31] Thomas Clausen, Philippe Jacquet, Cédric Adjih, Anis Laouiti, Pascale Minet, Paul Muhlethaler, Amir Qayyum, and Laurent Viennot. Optimized link state routing protocol (olsr). 2003.

[32] Charles E. Perkins and Pravin Bhagwat. Highly dynamic destination-sequenced distance-vector routing (dsdv) for mobile computers. In *Proceedings of the Conference on Communications Architectures, Protocols and Applications*, SIGCOMM '94, pages 234–244, New York, NY, USA, 1994. ACM.

[33] Request for comment (rfc) aodv. https ://www.ietf.org/rfc/rfc3561.txt.

[34] David B Johnson and David A Maltz. Dynamic source routing in ad hoc wireless networks. In *Mobile computing*, pages 153–181. Springer, 1996.

[35] Zygmunt Haas. The zone routing protocol (zrp) for ad hoc networks. *IETF Internet draft, draft-ietf-manet-zone-zrp-01. txt*, 1998.

[36] TASSOULT Nadia, AMAD Mourad, MOUMEN Hamouma, and KALLA Hamoudi. A survey on vehicular ad-hoc networks routing protocols : Classification and challenges. *Journal of Digital Information Management*, 17(4) :227, 2019.

[37] Brad Karp and Hsiang-Tsung Kung. Gpsr : Greedy perimeter stateless routing for wireless networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking*, pages 243–254. ACM, 2000.

[38] S Azad, Arafatur Rahman, and Farhat Anwar. A performance comparison of proactive and reactive routing protocols of mobile ad-hoc network (manet). *Journal of engineering and applied sciences*, 2(5) :891–896, 2007.

[39] Deepak Kumar, Ashutosh Srivastava, and SC Gupta. Performance comparison of pro-active and reactive routing protocols for manet. In *2012 International Conference on Computing, Communication and Applications*, pages 1–4. IEEE, 2012.

[40] Jerome Haerri, Fethi Filali, and Christian Bonnet. Performance comparison of aodv and olsr in vanets urban environments under realistic mobility patterns. In *Proceedings of the 5th IFIP mediterranean ad-hoc networking workshop*, number i, pages 14–17, 2006.

[41] Jonathan Ledy. Stratégie d'adaptation de liens sur canaux radios dynamiques pour les communications entre véhicules-optimisation de la qualité de service. 2012.

[42] Tom Goff, Nael B Abu-Ghazaleh, Dhananjay S Phatak, and Ridvan Kahvecioglu. Preemptive routing in ad hoc networks. In *Proceedings of the 7th annual international conference on Mobile computing and networking*, pages 43–52. ACM, 2001.

[43] Sofiane Boukli Hacene, Ahmed Lehireche, and Ahmed Meddahi. Predictive preemptive ad hoc on-demand distance vector routing. *Malaysian Journal of Computer Science*, 19(2) :189–195, 2006.

[44] Azzedine Boukerche and Liqin Zhang. A performance evaluation of a pre-emptive on-demand distance vector routing protocol for mobile ad hoc networks. *wireless communications and mobile computing*, 4(1) :99–108, 2004.

[45] Tao Liu and Alberto E Cerpa. Data-driven link quality prediction using link features. *ACM Transactions on Sensor Networks (TOSN)*, 10(2) :37, 2014.

[46] Hanene Gabteni, Benoit Hilt, Frederic Drouhin, Jonathan Ledy, Michel Basset, and Pascal Lorenz. A novel predictive link state indicator for ad-hoc networks. In *2014 IEEE Global Communications Conference*, pages 149–154. IEEE, 2014.

[47] Francisco J Martinez, Chai-Keong Toh, Juan-Carlos Cano, Carlos T Calafate, and Pietro Manzoni. Realistic radio propagation models (rpms) for vanet simulations. In *2009 IEEE Wireless Communications and Networking Conference*, pages 1–6. IEEE, 2009.

[48] Mineo Takai, Jay Martin, and Rajive Bagrodia. Effects of wireless physical layer modeling in mobile ad hoc networks. In *Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing*, pages 87–94. ACM, 2001.

[49] Stefano Marinoni and Hannu H Kari. Ad hoc routing protocol performance in a realistic environment. In *International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL'06)*, pages 96–96. IEEE, 2006.

[50] William H Tranter, Theodore S Rappaport, Kurt L Kosbar, and K Sam Shanmugan. *Principles of communication systems simulation with wireless applications*, volume 1. Prentice Hall New Jersey, 2004.

[51] Qi Chen, Felix Schmidt-Eisenlohr, Daniel Jiang, Marc Torrent-Moreno, Luca Delgrossi, and Hannes Hartenstein. Overhaul of ieee 802.11 modeling and simulation in ns-2 (802.11 ext). In *Proceedings of the 10th ACM Symposium on Modeling, Analysis, and Simulation of Wireless and Mobile Systems, 2007*, 2008.

[52] Qing Li, Cong Liu, and Han-hong Jiang. The routing protocol of aodv based on link failure prediction. In *2008 9th International Conference on Signal Processing*, pages 1993–1996. IEEE, 2008.

[53] Liang Qin and Thomas Kunz. Increasing packet delivery ratio in dsr by link prediction. In *36th Annual Hawaii International Conference on System Sciences, 2003. Proceedings of the*, pages 10–pp. IEEE, 2003.

[54] Won Seok Choi, Jong Wook Nam, and Seong Gon Choi. Hop state prediction method using distance differential of rssi on vanet. In *2008 Fourth International Conference on Networked Computing and Advanced Information Management*, volume 1, pages 426–431. IEEE, 2008.

[55] Tom Goff, Nael Abu-Ghazaleh, Dhananjay Phatak, and Ridvan Kahvecioglu. Preemptive routing in ad hoc networks. *Journal of Parallel and Distributed Computing*, 63(2) :123–140, 2003.

[56] Moussa Ali Cherif, Mohamed Kamel Feraoun, and Sofiane Boukli Hacene. Link quality and mac-overhead aware predictive preemptive multipath routing protocol for mobile ad hoc networks. *International Journal of Communication Networks and Information Security*, 5(3) :210, 2013.

[57] Sebastien Bindel. *Algorithms and applications for mobile communicating multi-level heterogeneous unmanned systems*. Theses, Université de Bordeaux, October 2016.

[58] Jens Mittag, Stylianos Papanastasiou, Hannes Hartenstein, and Erik G Strom. Enabling accurate cross-layer phy/mac/net simulation studies of vehicular communication networks. *Proceedings of the IEEE*, 99(7) :1311–1326, 2011.

[59] Philipp Andelfinger, Jens Mittag, and Hannes Hartenstein. Gpu-based architectures and their benefit for accurate and efficient wireless network simulations. In *2011 IEEE 19th Annual International Symposium on Modelling, Analysis, and Simulation of Computer and Telecommunication Systems*, pages 421–424. IEEE, 2011.

[60] Bahador Khaleghi, Alaa Khamis, Fakhreddine O Karray, and Saiedeh N Razavi. Multisensor data fusion : A review of the state-of-the-art. *Information fusion*, 14(1) :28–44, 2013.

[61] Lotfi A Zadeh. Fuzzy sets. *Information and control*, 8(3) :338–353, 1965.

[62] Lotfi Asker Zadeh. Fuzzy sets as a basis for a theory of possibility. *Fuzzy sets and systems*, 1(1) :3–28, 1978.

[63] Arthur P Dempster. Upper and lower probabilities induced by a multivalued mapping. In *Classic Works of the Dempster-Shafer Theory of Belief Functions*, pages 57–72. Springer, 2008.

[64] Philippe Smets. Imperfect information : Imprecision and uncertainty. In *Uncertainty management in information systems*, pages 225–254. Springer, 1997.

[65] Didier Dubois and Henri Prade. Possibility theory in information fusion. In *Proceedings of the third international conference on information fusion*, volume 1, pages PS6–P19. IEEE, 2000.

[66] GA Sharer. A mathematical theory of evidence. princeton. *Princeton University Press*, 1 :976, 1976.

[67] Véronique Cherfaoui, Thierry Denoeux, and Zohra Leïla Cherfi. Distributed data fusion : application to confidence management in vehicular networks. In *2008 11th international conference on information fusion*, pages 1–8. IEEE, 2008.

[68] Glenn Shafer. Dempster-shafer theory. *Encyclopedia of artificial intelligence*, 1 :330–331, 1992.

[69] Thierry Denœux. The cautious rule of combination for belief functions and some extensions. In *2006 9th International Conference on Information Fusion*, pages 1–8. IEEE, 2006.

[70] Thierry Denœux. Methods for building belief functions. *Methods*, (1/76), 2017.

[71] Hind Laghmara, Christophe Cudel, Jean-Philippe Lauffenburger, and Mohammed Boumediene. Evidential object association using heterogeneous sensor data. In *2018 21st International Conference on Information Fusion (FUSION)*, pages 1285–1292. IEEE, 2018.

[72] Hongwei Zhu and Otman Basir. A scheme for constructing evidence structures in dempster-shafer evidence theory for data fusion. In *Proceedings 2003 IEEE International Symposium on Computational Intelligence in Robotics and Automation. Computational Intelligence in Robotics and Automation for the New Millennium (Cat. No. 03EX694)*, volume 2, pages 960–965. IEEE, 2003.

[73] Alireza Chakeri, Iman Nekooimehr, and Lawrence O Hall. Dempster-shafer theory of evidence in single pass fuzzy c means. In *2013 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)*, pages 1–5. IEEE, 2013.

[74] Astride Aregui and Thierry Denœux. Constructing consonant belief functions from sample data using confidence sets of pignistic probabilities. *International Journal of Approximate Reasoning*, 49(3) :575–594, 2008.

[75] A Appriou. Probabilities and unknowns in multisensor data fusion. *Revue Scientifique*.

[76] M Rombaut. Decision in multi-obstacle matching process using theory of belief. *AVCS*, 98 :1–3, 1998.

[77] Benjamin Mourllion, Dominique Gruyer, R Royere, and Sébastien Théroude. Multi-hypotheses tracking algorithm based on the belief theory. In *2005 7th International Conference on Information Fusion*, volume 2, pages 8–pp. IEEE, 2005.

[78] George J Klir and Baozung Yuan. *Fuzzy sets and fuzzy logic : theory and applications*, volume 574. Prentice Hall PTR New Jersey, 1995.

[79] David Bellot. *Fusion de données avec des réseaux bayésiens pour la modélisation des systèmes dynamiques et son application en télémédecine*. PhD thesis, Université Henri Poincaré-Nancy 1, 2002.

[80] Kari Sentz, Scott Ferson, et al. *Combination of evidence in Dempster-Shafer theory*, volume 4015. Citeseer, 2002.

[81] Philippe Smets. The transferable belief model and other interpretations of dempster-shafer's model. *CoRR*, abs/1304.1120, 2013.

[82] Glenn Shafer. *A mathematical theory of evidence*, volume 42. Princeton university press, 1976.

[83] Gilles Roudiere and Philippe Owezarski. A lightweight snapshot-based ddos detector. In *2017 13th International Conference on Network and Service Management (CNSM)*, pages 1–7. IEEE, 2017.

[84] Ismail Bin Mohamad and Dauda Usman. Standardization and its effects on k-means clustering algorithm. *Research Journal of Applied Sciences, Engineering and Technology*, 6(17) :3299–3303, 2013.

[85] George F Riley and Thomas R Henderson. The ns-3 network simulator. In *Modeling and tools for network simulation*, pages 15–34. Springer, 2010.

[86] https ://dsn.tm.kit.edu/english/index.php. Decentralized systems and network services research group.

[87] http ://www.kit.edu/. Institut de technologie de karlsruhe.

[88] Michael Behrisch, Laura Bieker, Jakob Erdmann, and Daniel Krajzewicz. Sumo–simulation of urban mobility : an overview. In *Proceedings of SIMUL 2011, The Third International Conference on Advances in System Simulation*. ThinkMind, 2011.

[89] Mordechai Haklay and Patrick Weber. Openstreetmap : User-generated street maps. *IEEE Pervasive Computing*, 7(4) :12–18, 2008.

[90] Nouha Baccour, Anis Koubâa, Luca Mottola, Marco Antonio Zúñiga, Habib Youssef, Carlo Alberto Boano, and Mário Alves. Radio link quality estimation in wireless sensor networks : A survey. *ACM Transactions on Sensor Networks (TOSN)*, 8(4) :34, 2012.

[91] Ian D Chakeres and Elizabeth M Belding-Royer. Aodv routing protocol implementation design. In *24th International Conference on Distributed Computing Systems Workshops, 2004. Proceedings.*, pages 698–703. IEEE, 2004.

[92] Jonathan Ledy, AnneMarie Poussard, Rodolphe Vauzelle, Benoît Hilt, and Hervé Boeglen. Aodv enhancements in a realistic vanet context. In *2012 International Conference on Wireless Communications in Underground and Confined Areas*, pages 1–5. IEEE, 2012.

Optimisation de routage dans les réseaux véhiculaires par la prédiction de rupture de lien

Résumé

Les réseaux véhiculaires appelés aussi *Vehicular Ad hoc NETworks* (*VANET*) sont des réseaux mobiles concernant des véhicules. Les réseaux VANET se distinguent des autres types de réseaux ad hoc par certaines caractéristiques et propriétés particulières. En effet, la topologie change constamment en raison de la vitesse élevée des véhicules ainsi qu'en fonction des voies de circulation. La communication (canal de transmission) devient donc instable du fait de la présence de nombreux obstacles notamment en milieu urbain (bâtiments, véhicules, etc.). L'une des problématiques dans ce type de réseau concerne le routage. En effet, les véhicules ou nœuds, ne peuvent pas communiquer directement entre eux sauf s'ils sont voisins. Dans ce cas, lorsqu'un nœud veut envoyer un message à un autre nœud, il utilise des nœuds relais. Dans cette thèse, la problématique d'optimisation du routage est abordé en utilisant une détection de rupture de lien. Afin de détecter la rupture de lien, un indicateur prédictif appelé *Link Breakage Forecasting Indicateur* (*LBFI*) basé sur les erreurs de décodage *Orthogonal Frequency Division Multiplexing* (*OFDM*) est développé. Le processus de détection de rupture est fondé sur l'application de la théorie des fonctions de croyance basés sur différents paramètres dont les erreurs de décodage *OFDM*. L'indicateur est ensuite intégré au protocole de routage *AODV* en remplaçant le mécanisme de détection de rupture de lien traditionnel de *AODV* par LBFI. Lorsqu'une rupture de lien est détecté, une recherche de route est enclenchée tout en continuant l'utilisation de la route actuelle permettant ainsi l'optimisation du routage. Ces travaux sont évalués sur un simulateur de réseaux intégrant notamment une émulation de la couche physique IEEE802.11p intégrant la couche *OFDM*. L'évaluation des performances du protocole ainsi obtenu montre une amélioration du taux de réception de paquet, des délais de bout en bout et une meilleure stabilité des routes notamment par rapport à AODV mais aussi par rapport à un autre protocole de détection de rupture de lien.

Mots-clés:

VANET, rupture de lien, OFDM, théorie des fonctions de croyance, AODV

Abstract

Vehicular Ad hoc NETworks (VANET) are mobile networks involving vehicles. VANET networks are distinguished from other types of ad hoc networks by certain specific characteristics and properties. Indeed, the topology is constantly changing due to the high speed of vehicles and according to the traffic lanes. Thus, communication (transmission channel) becomes unstable due to the presence of many obstacles, especially in urban areas (buildings, vehicles, etc.). One of the challenges in this kind of network concerns routing. In fact, vehicles or nodes cannot communicate directly with each other unless they are neighbors. In this case, when a node wants to send a message to another node, it uses relay nodes. In this thesis, the problem of routing optimization is addressed by using link failure detection. In order to detect link failure, a predictive indicator called Link Breakage Forecasting Indicator (LBFI) based on Orthogonal Frequency Division Multiplexing (OFDM) decoding errors is developed. The process of detecting a link failure is based on the application of belief function theory to various parameters including OFDM decoding errors. The indicator is then integrated into the AODV routing protocol by replacing AODV's traditional link failure detection mechanism with LBFI. When a link failure is detected, a route search is initiated while continuing to use the current route, thus optimizing routing. This work is evaluated using a network simulator that integrates an emulation of the IEEE802.11p physical layer with the OFDM layer. The performance assessment of the protocol shows an improvement in the packet reception rate, end-to-end delays and better route stability, particularly compared to AODV but also compared to another link break detection protocol.

Keywords:

VANET, link breakage, OFDM, theory of belief functions, AODV