République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A/Mira de Béjaia
Faculté des Sciences Exactes
Département d'Informatique

MÉMOIRE DE MASTER RECHERCHE

En
Informatique

Option
Réseaux et Systèmes Distribués

Thème

Contrôle de congestion dans les réseaux VANETs

Présenté par :

$\mathcal{M}^{me}$ **AMZAL née ATMAOUI Souhila**
$\mathcal{M}^{lle}$ **AMIR Ouassila**

Soutenu le 29/06/2017 devant jury composé de :

Présidente	$\mathcal{M}^{me}$ **KHOULALENE Nadjet**	**M.A.A**	**U. A/Mira Béjaia.**
Encadreur	**Dr BOULFEKHAR Samra**	**M.C.A**	**U. A/Mira Béjaia.**
Examinatrice	$\mathcal{M}^{me}$ **ZIDANI Ferroudja**	**M.A.A**	**U. A/Mira Béjaia.**
Examinatrice	$\mathcal{M}^{me}$ **LAARBI Wahiba**	**M.A.A**	**U. A/Mira Béjaia.**

Béjaia, Juin 2017.

⁕ *Remerciements* ⁕

Tout d'abord, nous remercions la grâce du dieu, pour nous avoir guidés et éclairés sur la bonne voie du savoir pour continuer ce travail et atteindre les objectifs tracés.

Nous tenons à manifester notre gratitude et reconnaissance envers notre encadreur Madame BOULFEKHAR Samra pour nous avoir aidés et orientés durant la réalisation de ce travail.

Nous remercions chaleureusement l'ensemble des membres du jury d'avoir accepté d'être examinateurs de ce mémoire.

Nous remercions tous nos professeurs, de l'université Abderrahmane Mira de Bejaia, qui nous ont permis d'acquérir plus de connaissances durant nos études, spécialement Madame YAICI.

Ainsi, nous adressons de tout nos cœur nos remerciements à nos chers parents, nous leurs sommes infiniment reconnaissantes pour leur soutien illimité. Qu'ils trouvent dans ce travail le fruit de leurs sacrifices.

Enfin, nous terminons en remerciant tous les amis qui ont aidé à l'accomplissement de ce modeste travail.

⁕ *Dédicaces* ⁕

Je dédie ce modeste travail
À toute ma famille, notament mes parents, qui m'ont comblé de leur soutien et m'ont voué un amour inconditionnel.
À mon cher mari, que ce travail soit témoignage de ma reconnaissance. Sans tes conseils et ton encouragement ce travail n'aurait vu le jour. Tes sacrifices, ton soutien moral m'ont permis de réussir mes études.
À mes deux chers frères : Reda et Sofiane.
À toute la famille YESSAD, challeureusement à ma sœur Lydia YESSAD, qui a était toujours à mes cotés.
À ma précieuse binôme Ouassila.
À toute la famille AMZAL, grand et petit.
À tout mes ami(e)s, spécialement YOUSFI Thilleli, BOUGHANI Lydia, RABIA Amel et BELMEHDI Ouacila.

$\mathcal{M}^{me}$ AMZAL née ATMAOUI Souhila

⁕ *Dédicaces* ⁕

Pour l'expression d'un profond respect et de reconnaissance, je dédie ce modeste travail à mes chers et tendres parents qui m'ont entouré de leur amour, leurs soutien moral et matériel et qui m'ont offert tant de courage et de conseils et aussi mon oncle et sa femme. Que le bon Dieu les protège.

À toute ma famille, notamment, mes bien aimé : mes frères, ma sœur, cousins et cousines, qui mon toujours soutenue.

À ma chère binôme Souhila avec qui je partage ce travail.

À mes ami(e)s : Thilleli, Lydia, Nabila, Lynda, Djahida, Nassima, qui ont été compréhensive et tolérantes avec moi.

$\mathcal{M}^{lle}$ AMIR Ouassila

Table des matières

Table des figures

Liste des tableaux

Liste des algorithmes

Liste des abréviations

ACK	acknowledgement
AIFS	Arbitration InterFrame Space
ATB	Adaptive Traffic Beacon
AWT	Average Waiting Time
BRR	Beaton Reception Rate
BSM	Basic security messages
CAM	Co-operative Awareness Messages
CCH	Control Channel
CMDI	Channel Monitoring and Decision Interval
CR	Collision Rate
CSMA/CA	Carrier Sense Multiple Access / Collision Avoidanee
DSRC	Dedicated Short Range Communication
EDCA	Enhanced Distributed Channel Access
FCC	Federal Communications Commission
GPS	Global Positioning System
IEEE	Institute of Electrical and Electronics Engineers
IPCS	Incremental-Power Carrier-Sensing
MAC	Medium Access Control
MANET	Mobile Ad hoc NETwork
NS-2	Network Simulator version 2
Nam	Network Animator
OSI	Open System Interconnexion
Otcl	Object-oriented Tool Command Language
PDR	Packet Delivery Ratio
PULSAR	Periodically Updated Load Sensitive Adaptive Rate

Qds	Qualité de Service
Qos	Quality Of Servie
RSU	Road Side Units
SCH	Service Channel
SNR	Signal to Noise Ratio
STI	Système de Transport Intelligent
TCL	Tool Command Langage
TCP	Transmission Control Protocol
VANET	Vehicular Ad Hoc NETwork
VC	Vehicular Communication
VSC	Vehicul Security Communication
V2V	Vehicular-to-Vehicular
V2I	Vehicular-to-Infrastructure
WAVE	Wireless Ability in Vehicular Environments

Introduction générale

L'essor des nouvelles technologies et les progrès récents survenus dans les communications sans fil et les systèmes de transport intelligents ont permis de réduire les risques dans le domaine de transport de façon significative en agissant simultanément sur la prévention des accidents ; la réduction des dégâts en cas de collision ; la gestion des secours et enfin la protection des usagers. Ce nouveau domaine de recherche appelé " réseau ad hoc véhiculaire " ou " VANET : Véhicular Ad hoc NETwork " représente un atout majeur pour assurer la sécurité routière. Cependant, les réseaux ad hoc véhiculaires sont un type de MANET (Mobile Ad hoc NETwork) et sont désignés afin de permettre un échange de petite à moyenne portée entre véhicules. En effet, dans les réseaux VANETs, les nœuds sont caractérisés par une forte dynamique et une mobilité, en plus du taux élevé de changements de topologie et de la variabilité de densité.

Les véhicules sont équipés de moyens de communication radio qui leur permettent de communiquer entre véhicules (V2V : Vehicle-to-Vehicle) ou véhicules à infrastructure (V2I : Vehicle-to-Infrastructure), qui se font entre des unités montées sur les véhicules et des unités placées sur les bords des autoroutes ; la combinaison des deux types de réseaux forme des réseaux de communications hybrides. Si un véhicule détecte une anomalie sur la route, il transmet un message d'alarme vers les véhicules voisins à portée radio. Les véhicules récepteurs analysent et évaluent le message et peuvent prendre les mesures qui s'imposent c'est-à-dire ralentir. Dans ce cas, l'échange de messages a permis de prévoir un problème avant que le véhicule ne soit en mesure de le détecter.

Par ailleurs, le standard pour ces communications est celui de l'IEEE, 802.11p, qui permet une augmentation de la puissance d'émission sur les canaux et utilise la bande radio large de 75 MHz située à 5.9Ghz. Cette largeur est divisée en un canal de contrôle (CCH) et six canaux de service (SCH). Grace à ces communications, le conducteur reçoit un message d'avertissement, en cas de dangers éventuels. Cette alerte peut être un message de sécurité périodique (balise), qui contient des informations concernant la position, la direction et la vitesse des véhicules voisins, ou un message évènementiel, envoyé pour prévenir les autres véhicules des différentes urgences et catastrophes sur la route. Ces messages de sécurité sont diffusés via un canal, dit canal de contrôle (CCH). Parfois, cette diffusion, d'une façon illimitée, engendre la densité de ce dernier, ce qui introduit la notion de congestion, qui reste un critère à satisfaire dans la qualité de service (QdS). Cependant, des niveaux élevés de retard sont constatés et des pertes de paquets sont causées par les stratégies de routage, en raison de la saturation des files d'attente des canaux. Pour cette raison, plusieurs algorithmes de contrôle de congestion fiables et efficaces ont été proposés, dans la littérature, afin d'éviter l'encombrement du canal CCH au niveau de la couche physique, et le retard du message de sécurité événementiel.

Notre travail consiste à révéler les points forts et faibles de certains de ces algorithmes, tout en les évaluant selon quelques critères de la qualité de service, dans le but de pouvoir trouver une nouvelle proposition pour minimiser les problèmes de congestions dans les VANETs. Nous avons pris le soin de proposer un nouvel algorithme basé sur le temps d'occupation des messages dans les canaux, l'affectation des différentes priorités et la réduction du débit de transmission, tout en garantissant la qualité de service (QoS), qui demeure un défi dans ces réseaux. En effet, cette proposition a été simulée au moyen du simulateur NS-2 pour donner des résultats de simulation très intéressant en termes de perte de paquets, le taux de transmission, ainsi que le délai.

Ce mémoire est organisé en trois chapitres :
Dans Le premier chapitre, nous donnons un aperçu général sur les réseaux sans fil, à savoir les réseaux ad hoc et les réseaux de capteur. Puis nous abordons les réseaux Ad Hoc véhiculaires (VANET), leurs architectures, applications, caractéristiques et

enfin leurs standardisation.
Dans Le deuxième chapitre, nous traitons le problème de congestion des VANETs puis nous discutons certains travaux de recherche concernant les mécanismes de détection et de contrôle de congestion. Une comparaison des différentes approches est ensuite présentée pour mettre en évidence leurs avantages et inconvénients.
Le troisième chapitre est consacré à la présentation de notre contribution pour le problème de contrôle de congestion, en détaillant les étapes de l'algorithme et en le simulant sous l'outil de simulation NS-2. Nous terminons avec des paramètres et métriques à calculer afin d'analyser et d'évaluer sa performance dans l'environnement VANET.
En raison de la limite de nombre de pages, nous tenons en compte l'annexe, qui est consacré à la suite de l'étude critique de certains protocoles de contrôle de congestion, cités dans le tableau récapitulatif du deuxième chapitre.

En fin de ce mémoire, une conclusion générale est donnée, résumant les apports essentiels de notre travail et dégageons quelques perspectives envisagées pour la solution proposée.

Chapitre 1

Généralités sur les réseaux VANETs

1.1 Introduction

L'évolution récente de la technologie dans le domaine de la communication sans fil permet d'étendre la notion de mobilité pour permettre l'accès à l'information et à la communication, n'importe où et n'importe quand. Avec l'émergence des réseaux VANETs ayant comme objectif principal l'amélioration de la sécurité routière, et grâce à des capteurs installés au sein de véhicules, ou bien situés au bord des routes et des centres de contrôle, les communications véhiculaires permettront aux conducteurs d'être avertis suffisamment tôt de dangers éventuels.

Dans ce chapitre, nous présentons d'abord les réseaux ad hoc de manière générale, puis, nous parlons sur les réseaux de capteur, et enfin nous abordons les réseaux VANETs, leurs définition, leurs architectures de communication, leurs caractéristiques, enfin nous décrivons leurs applications ainsi que les différents types de services offerts par ces derniers.

1.2 Réseaux ad hoc

Les réseaux ad hoc, nommés MANET (Mobile Ad hoc Network), sont composés de systèmes informatiques divers, appelés nœuds, ayant la possibilité de communiquer, de manière autonome par ondes radio. Ces réseaux sont dits ad hoc, dans la

mesure où ils ne nécessitent pas d'infrastructure fixe. Ils peuvent exister temporairement pour répondre à un besoin ponctuel de communication [16].

Exemple d'illustration :
L'entité A et C sont hors de portée directe de transmission, B se comporte comme un intermédiaire pour l'envoi du message de A vers C, dans ce cas B est un relaie, voir Figure 1.1.

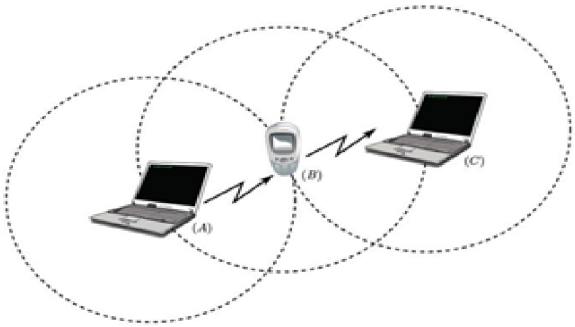

FIGURE 1.1 – Transmission d'un message dans un réseau ad hoc [16].

1.3 Réseaux de capteur

Les réseaux de capteurs sont souvent composés d'un nombre très important des nœuds appelés capteurs. Un capteur (Sensors Networks) est un dispositif de taille extrêmement réduite, avec des ressources très limitées, autonomes, capable de traiter des informations et de les transmettre, via les ondes radio, à une autre entité (capteurs, unité de traitements, etc.) sur une distance limitée à quelques mètres. Un capteur analyse son environnement, et propage les données récoltées aux capteurs appartenant à sa zone de couverture [2].
Les réseaux de capteur ne définissent pas une architecture préexistante puisque les capteurs peuvent se trouver fixés à un endroit précis ou mobile, formant ainsi un réseau sans infrastructure prédéfinie. Un tel réseau ne se limite pas à un domaine particulier mais il peut s'adresser à une diversité de secteurs comme la biologie, la

chimie, l'environnement, ainsi que la surveillance et même la télésurveillance personnelle, etc.

1.4 Réseaux ad hoc véhiculaires

1.4.1 Définition

Les réseaux ad hoc véhiculaires, nommés VANETs (Vehicul Ad Hoc NETwork) ne sont qu'une application des réseaux MANETs, dont un nœud est un véhicule comportant des interfaces réseaux, des calculateurs ainsi que des capteurs capables de collecter et de traiter les informations. Ils constituent le noyau d'un Système de Transport Intelligent (STI) et permettent d'établir des communications entre véhicules, ou bien, avec une infrastructure située aux bords des routes. Pour la mise en place d'un tel réseau, certains équipements électroniques doivent être installés, au sein des véhicules, comme les dispositifs de perception de l'environnement (radars, caméras), les systèmes de localisation de Global Positioning System (GPS), et bien sûr les plateformes de traitement. Ce qui introduit la notion de "véhicule intelligent", voir Figure 1.2 [26].

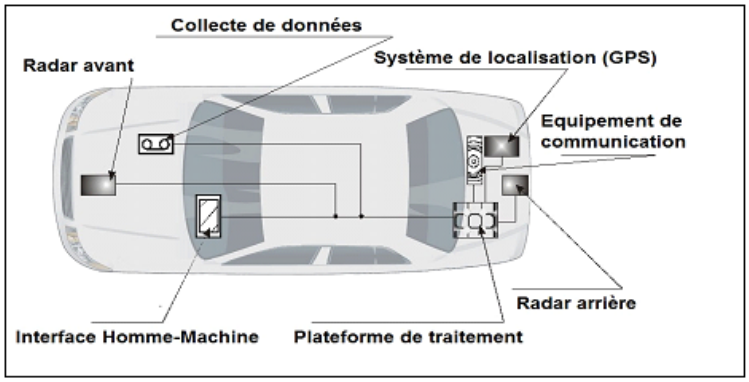

FIGURE 1.2 – Éléments constituant le véhicule intelligent [26].

1.4.2 Architectures de communication dans les réseaux VANETs

Dans les réseaux VANETs, on peut distinguer trois architectures de communication :

1.4.2.1 Communication de véhicule à véhicule (V2V)

Dans ce mode, aucune infrastructure n'est utilisée, aucune installation n'est nécessaire sur les routes, chaque véhicule est équipé pour communiquer directement avec un autre véhicule, s'il se situe dans sa zone radio, voir la partie A, Figure 1.3 [21].

1.4.2.2 Communication de véhicule avec utilisation d'infrastructures (V2I)

Ce mode de communication permet une meilleure utilisation des ressources partagées et démultiplie les services fournis (accès à Internet, échange de données de voiture-à-domicile, communications de voiture-à-garage de réparation pour le diagnostic distant, etc.) grâce à des points d'accès RSU (Road Side Units) situés aux bords des routes, voir la partie B, Figure 1.3 [25].

1.4.2.3 Communication hybride

Ce mode est une combinaison des communications véhicules à véhicules avec les communications de véhicules à infrastructures. Il est utilisé dans le but d'élargir les zones de communication et minimiser l'installation des infrastructure, voir Figure 1.3.

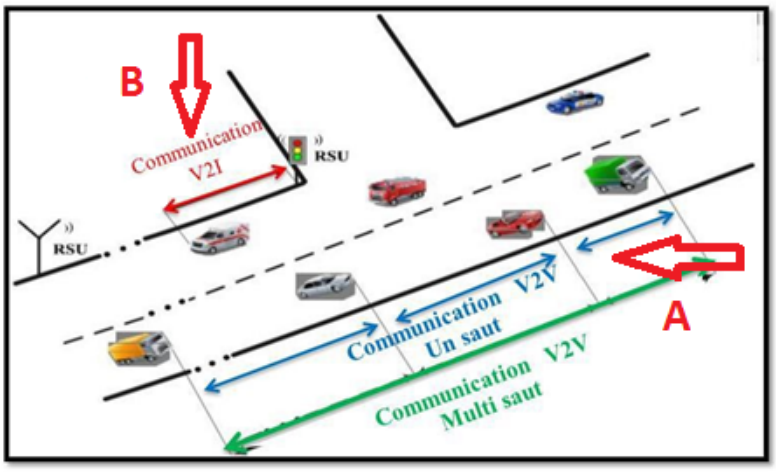

FIGURE 1.3 – Illustration de l'architecture de communication [7].

1.4.3 Caractéristiques des réseaux VANETs

Les réseaux véhiculaires se distinguent d'autres réseaux sans fil par des caractéristiques spécifiques, telle que :

1.4.3.1 Capacité d'énergie et de stockage

Contrairement au contexte des réseaux MANET, où la contrainte d'énergie représente un défi pour les chercheurs, les éléments du réseau VANET disposent suffisamment d'énergie qui peut alimenter les différents équipements électroniques d'une voiture intelligente. Donc, les nœuds sont censés avoir une grande capacité de traitement et de stockage de données [24].

1.4.3.2 Topologie, mobilité et connectivité

Les réseaux VANETs sont caractérisés par la forte mobilité des nœuds (véhicules), liée à la vitesse des voitures qui est très importante dans les autoroutes. Par conséquent, un nœud peut rejoindre ou quitter le réseau en un temps très court,

ce qui rend les changements de topologie très fréquent.
La connectivité nécessite la connaissance des positions des nœuds et de leurs mouvements qui sont tellement difficiles à prévoir de garder en vue la nature et le mode de déplacement de chaque véhicule [22].

1.4.3.3 Modèle de mobilité

Les réseaux VANETs se caractérisent par un modèle de mobilité dynamique dû à l'importante vitesse des nœuds qui réduit considérablement les durées de temps pendant lesquelles les nœuds peuvent communiquer.

1.4.4 Applications et services des réseaux VANETs

Les applications des réseaux VANETs surveillent les différents types de messages échangés, tel que les conditions des véhicules, l'environnement des routes, l'approche des véhicules et les conditions météorologiques pour rendre le réseau plus sûre et plus efficace. Dans ce qui suit, nous examinons brièvement certaines applications et services existantes dans ces réseaux :

1.4.4.1 Applications pour la sécurité routière

Le but ultime des applications de sécurité dans les VANETs est d'éviter et de diminuer le nombre d'accidents des véhicules, par conséquence, de réduire le délai de transmission et d'assurer la fiabilité. Ces applications utilisent la communication véhicule à véhicule, par échange de messages, qui peuvent être classés en deux types : périodiques, dit balises, et événementiels. La permutation de messages de balises est de nature préventive, pour éviter l'apparition de situations dangereuses, qui peuvent contenir des informations sur la position, la direction et la vitesse des véhicules. Par contre les messages événementiels peuvent être générés à la suite d'une situation dangereuse ou lorsqu'une situation anormale est détectée, avec une priorité élevée et sans aucun retard. Les deux messages de sécurité sont diffusés via un canal, dit canal de contrôle (CCH). La densité de ce dernier engendre la notion de congestion [10].

1.4.4.2 Applications d'efficacité

Il s'agit d'une catégorie dans laquelle les applications connaissent l'emplacement du véhicule, afin d'améliorer leur mobilité dans la voie publique. Les conducteurs ont besoin de l'information fournie, pour prendre des décisions pendant le voyage, ce qui le rend plus sécurisé. Elles peuvent être classées en deux modèles : les applications pour contrôler les carrefours et les intersections, et les applications pour réduire et éviter les embouteillages [9].

1.4.4.3 Applications de confort

La conduite sera plus confortable et agréable, pendant le voyage, grâce aux informations envoyées par les services de véhicules. Ce type d'application comprend les renseignements météorologiques, les nouvelles sur le stationnement disponible dans un parking, les informations touristiques, etc [9].

1.4.5 Défis liés aux réseaux VANETs

Étant donné les caractéristiques des VANETs, certaines défis seront résumées en ces points :

1.4.5.1 Qualité de service

La qualité de service dans les réseaux VANETs représente un défi majeur, non encore résolu, dû aux caractéristiques et aux contraintes strictes liées aux VANETs, comme la congestion qui est un problème associé à la circulation des véhicules. Nous estimons étudier ce problème en faveur des applications de sécurité, qui va être détaillée dans le prochain chapitre.
La qualité de service (QdS), dite aussi Quality of Service (QoS), est définie par un ensemble de besoin à assurer par le réseau pour le transport du trafic d'une source à une destination, qui peuvent être traduit par des paramètres mesurables tels que le délai, la bande passante, la congestion etc.
Ainsi, elle correspond à la performance globale d'un réseau, qu'il soit téléphonique

ou informatique, perçue par les utilisateurs du réseau. L'objectif de la QoS est d'atteindre un meilleur comportement de la communication, pour que le contenu de cette dernière soit correctement acheminé, et les ressources du réseau sont utilisées d'une façon optimale [17].

*** Critères de la qualité de service**

Afin de bien évaluer les travaux de recherche étudiés, nous avons établi certains critères de QoS, compte tenu des besoins et contraintes liés aux VANETs. De ce fait, nous nous intéresserons, au coût en termes de fiabilité, la bande passante, le délai de transmission, la gigue et la congestion.

1. **Fiabilité**
   Dans le contexte des services de diffusion VANET, la fiabilité est définie comme la capacité du réseau, de sorte que tous les nœuds mobiles sont concernés à recevoir les messages diffusés, dans la durée d'opération spécifiée [23].
2. **Bande passante**
   La bande passante définit la capacité de transmission de la couche physique, en termes de quantité d'informations (en bits/s), qui peuvent être transmise sur une voie de diffusion. Le débit représente l'occupation réelle de la bande passante, qui peut être affecté par plusieurs facteurs comme, entre autres, la densité des nœuds, la fiabilité du médium de transmission sans fil et le type de protocole utilisé pour la gestion de l'accès au médium (MAC) [34].
3. **Taux de perte**
   Le taux de perte des paquets est le rapport entre le nombre de paquets perdus, et le nombre total des paquets envoyés. Taux de perte = nombre de paquets perdus/nombre de paquets émis.
4. **Délai de transmission**
   Le délai de transmission est une métrique très importante, car la plupart des applications recommandent une communication rapide. Elle représente le moment de transmettre un paquet avec succès.
5. **Gigue**
   La gigue est la variation du délai des paquets reçus au fil du temps. Elle vient

du fait que les conditions réseau ne sont pas toujours stables et peuvent varier d'un instant à l'autre [17].

6. **Congestion**
   La congestion se produit généralement dans les goulots d'étranglement du réseau, où le débit des données entrant dépasse le débit disponible sortant. Lorsqu'un réseau est dans cet état, la demande du trafic est élevée, mais peu de débit utile est disponible. Des niveaux élevés de retard sont constatés et des pertes de paquets sont causées par les routeurs qui les rejettent parce que leurs files d'attente sont pleines. La qualité générale du service est donc extrêmement mauvaise.

1.4.5.2 Routage

Trouver une stratégie de routage stable qui garantit l'échange d'informations à jour, maximisant la fiabilité et minimisant les retards est un défi technique important lors de la conception d'une architecture pour la communication des véhicules. Dans les VANET, les liens pour la communication véhicule-véhicule et véhicule vers l'infrastructure ont tendance à être courts, en raison de la mobilité intrinsèque à haut débit des nœuds et de la présence d'obstacles. Par conséquent, beaucoup d'efforts sont consacrés à la définition de stratégies de routage efficaces. Les protocoles VANET spécifiques sont apparus au cours des dernières années, mais la plupart d'entre eux sont basés sur des réseaux ad hoc mobiles antérieurs [33].

1.4.5.3 Sécurité

La sécurité des réseaux sans fil vise à garantir essentiellement la confidentialité, l'intégrité et la disponibilité des services. Dans les réseaux VANETs la sécurité ne touche pas seulement des données échangées lors des communications, mais aussi, il peut toucher directement à la sécurité humaine. Cependant, les exigences de sécurité dans les VANETs sont intrinsèques et uniques en raison de la taille du réseau, des changements de topologie fréquents, de la mobilité élevée et des différentes classes d'applications et de services [9].

1.4.6 Standardisation et normalisation dans les réseaux VANETs

Les standards des réseaux VANETs sont définis, comme suite [8, 31] :
En 1999, la commission fédérale des communications aux États-Unis (Federal Communications Commission : FCC) avait alloué pour la communication véhiculaire (VC) la bande de fréquence à 5.9 Ghz avec une largeur de bande de 75 MHz (5.850 GHz -5.925 GHz). Cette largeur est divisée en 7 canaux. Un canal de contrôle (CCH) et six canaux de service (SCH). Le canal de contrôle est réservé à la transmission des messages de gestion, ou il est utilisé pour transmettre des messages de très haute priorité comme les messages liés à la sécurité routière. Les six autres canaux sont, quant à eux, dédiés à la transmission des données des différents services annoncés sur le canal de contrôle. Cette communication est connue sous le nom DSRC (Dedicated Short Range Communication).

En 2003, le groupe de travail de l' IEEE a repris ces travaux pour définir un nouveau standard dédié aux communications inter-véhiculaire, nommé WAVE (Wireless Ability in Vehicular Environments) et aussi connu sous le nom d'IEEE 802.llp. cette dernière fait partie de l'architecture IEEE 1609. Ce standard est inspiré, au niveau MAC, des deux standards IEEE 802.11a et IEEE 802.11e.

La famille des standards IEEE 1609 pour WAVE, se décompose en quatre standards : pour la gestion des ressources (IEEE 1609.1 -WAVE Resource Manager), pour la sécurisation des messages (IEEE 1609.2 WAVE Security Services for Applications and Management Messages), pour les services de niveau réseau et transport incluant l'adressage, le routage (IEEE 1609.3 -WAVE Networking Services), et pour la coordination et la gestion des sept canaux DSRC (IEEE 1609.4-WAVE Multi-Channel Operation).

1.5 Conclusion

Un réseau VANET représente un cas d'application particulier des réseaux MANET. Leur objectif principal est d'améliorer la sécurité routière, par l'utilisation de

la technologie des communications et de l'émergence de dispositifs sans fil à faible coût.

Ce chapitre a été axé sur la présentation des réseaux AD Hoc, les réseaux de capteurs sans fil ainsi que les VANETs, et leur description, en détaillant leurs architectures de communication et caractéristiques, et expliquant leur différentes applications et services et enfin leur contraintes et standards existants. Dans le chapitre suivant, nous allons étudier le problème de congestion dans les réseaux VANETs, ses mécanismes de détection et de contrôle, ainsi que des détails sur les protocoles spécifiques et leur fonctionnement.

Chapitre 2

Étude et contrôle de congestion dans les réseaux VANETs

2.1 Introduction

Comme dans tout système de communication, les réseaux ad hoc véhiculaires, de type V2V, doivent respecter certaines contraintes, en termes de qualité de service. Citons la congestion, qui est un défi important pour l'amélioration des performances dans ce domaine. Comme nous l'avons précisé dans le chapitre précédent, le présent chapitre sera consacré à la présentation et l'étude du problème de congestion, dans le besoin de réduire les pertes de paquets ainsi que le délai de transmission. Pour cela, nous commençons par une description du problème, puis, nous passons en revue sur les mécanismes de détections de la congestion ainsi que ceux du contrôle de cette dernière, en donnant des aperçus sur quelques approches ou stratégies et nous concluons par une comparaison entre les protocoles analysés.

2.2 Contrôle de congestion

La plupart des applications dans les VANETs visent à fournir des informations sur le voisinage local, donc elles sont plus sujettes à la congestion, par rapport à d'autres réseaux sans fil. En raison de leurs caractéristiques particulières telles que le taux de transmission, la mobilité élevée, la nature de diffusion de message, etc.

Il est intéressant de noter que le concept de base de la congestion reste le même que celui utilisé dans les réseaux de communication, dans lequel un nœud du réseau est congestionné lorsque la capacité du réseau est inférieure à la charge des canaux. Toutefois, lorsque la bande passante est disponible, les pertes de paquets peuvent encore se produire en raison de la corruption de bit aléatoire, de l'erreur de canal et de l'échec de l'itinéraire. En outre, l'utilisation des pertes de paquets n'est pas suffisante pour déterminer le niveau de contention dans les canaux. Par conséquents, d'autres paramètres de réseau devraient être pris en compte pour contrôler la congestion.

Généralement, tous les réseaux utilisent le protocole TCP (Transmission Control Protocol) pour éviter le problème de congestion, mais en raison des caractéristiques des réseaux ad hoc(la mobilité élevée et les communications sans fil multi-hop, etc.), des environnements différents, des protocoles distincts et une architecture différente qui entraînent une augmentation de perte ou de retard des paquets, les stratégies de contrôle de congestion TCP ne sont pas efficaces.
Particulièrement, dans les VANETs, les messages événementiels (arrêt d'urgence d'un véhicule, collision, etc.) doivent être envoyés avec un délai minimum, une priorité élevée et un taux de perte proche de zéro. Si un grand nombre de véhicules diffusent des messages de balise (les informations sur la vitesse, météo, etc.) à haute fréquence d'une manière périodique, le canal de communication sera facilement congestionné. Pour assurer une livraison rapide et fiable des messages de sécurité, il est très important de garder le canal de contrôle (CCH) libre [5, 35].

La Figure 2.1 montre une vue schématique d'une architecture de contrôle de congestion de plusieurs couches dans les réseaux VANETs. Cependant, une entité de gestion est considérée pour détecter et contrôler la congestion.
La partie détection consacre certaines informations de la couche application pour repérer l'occurrence de congestion dans le réseau. En outre, la congestion peut être détectée en détectant la saturation du canal dans la couche physique et en mesurant certains paramètres, comme le niveau d'utilisation du canal.
La partie contrôle peut être effectuée de différentes manières dans différentes couches du réseau :
- La couche application peut contribuer au contrôle de congestion, en accordant

les taux de génération de messages de différentes applications et en réduisant les charges du trafic ainsi que la congestion dans les réseaux.
- La couche réseau peut collaborer par des algorithmes de routage intelligents qui rediffusent efficacement les messages.
- Les messages d'hiérarchisation et de planification à la couche MAC peuvent considérablement aider à contrôler la congestion dans les VANETs.

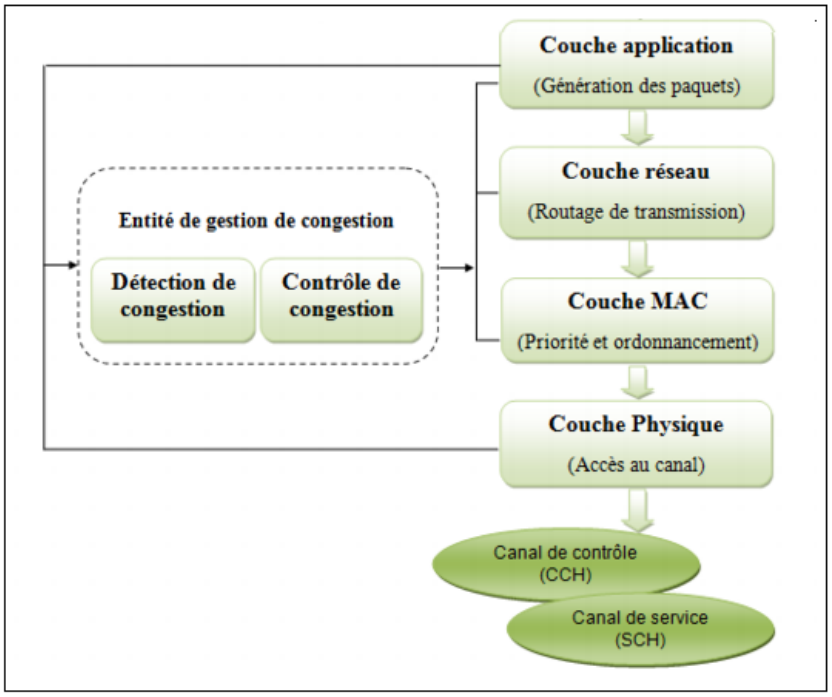

FIGURE 2.1 – Architecture de contrôle de congestion entre les couches [38].

2.3 Mécanismes de détection de congestion dans les réseaux VANETs

Dans les VANETs, la détection de congestion peut être effectuée en utilisant certaines méthodes, comme la détection basée sur des événements ou la détection basée sur des mesures, définies ci-après.

2.3.1 Méthodes basées sur des événements

Cette méthode de détection surveille les messages de sécurité déclenchés par un événement et décide du lancement d'un algorithme de contrôle de congestion, si cette dernière est produite dans le réseau. Cet algorithme diminue l'émission des messages de balise et toutes les files d'attente de transmission MAC, à l'exception de la file d'attente du canal de contrôle (CCH), pour garantir la délivrance des messages événementiels, avec un délai minimum [11].

2.3.2 Méthodes basées sur des mesures

Chaque dispositif surveille périodiquement le niveau d'utilisation du canal. La congestion est indiquée lorsque le nombre de messages dans les files d'attente ou le temps d'occupation des canaux mesuré dépasse un seuil prédéfini. Dans ce cas, les nœuds émetteurs sont notifiés, afin de diminuer leurs vitesse de transmission et les messages de balise seront immédiatement réduits, dans le but d'assurer la performance du message de sécurité événementiel [13].

2.4 Mécanismes de contrôle de congestion dans les réseaux VANETs

Les solutions existantes peuvent être classées en fonction des stratégies ou des moyens par lesquels la congestion est contrôlée, ce qui est pratiquement définie dans ce qui suit.

2.4.1 Classification selon des stratégies

Les stratégies de contrôle de congestion dans les VANETs comprend trois classes : proactives, réactives et hybrides, suivant les phases de leur traitements [12, 27] :

2.4.1.1 Stratégies proactives

Les stratégies proactives sont basées sur certaines informations, telles que le nombre de véhicules voisins, les modèles de génération de données et les paramètres de transmission. Cette stratégie peut être considérée comme une solution de contrôle d'encombrement qui ajuste les paramètres de transmission, avant que les canaux ne soient encombrés. Elle est efficace pour la maîtrise de la congestion dans les environnements de véhicules, où les messages de sécurité sont envoyés aux canaux de communication radio, qui sont sérieusement menacés par la congestion du canal.

2.4.1.2 Stratégies réactives

Les stratégies réactives contiennent les informations sur l'état de congestion du canal. En effet, ces stratégies peuvent être considérées comme des solutions de contrôle de congestion après son apparition dans les réseaux. Si son occurrence est détectée dans les canaux, les paramètres de transmission sont réglés pour diminuer leur charge.

2.4.1.3 Stratégies hybrides

Les stratégies hybrides utilisent les avantages des stratégies proactives et celle des stratégies réactives. Par exemple, elles ajustent la puissance d'émission proactive et le taux de transmission de manière réactive pour contrôler la congestion dans un canal.

2.4.2 Classification selon des paramètres et des moyens

Éviter et contrôler la congestion est d'une importance fondamentale dans les VANETs. Pour cela nous allons présenter, dans ce qui suit, les différents paramètres et moyens sur lesquels a été basé ce contexte. Nous notons que c'est la classification la plus utilisée dans la documentation.

2.4.2.1 Solutions basées sur le taux de transmission

Ce type de solutions ajustent dynamiquement le taux de transmission ou le taux de génération des paquets pour contrôler les charges des canaux dans les réseaux. Les performances des VANETs s'améliore en augmentant le taux de transmission car les applications de sécurité peuvent recevoir de nouvelles informations sur l'état des véhicules voisins, mais l'augmentation du taux de transmission conduit à une utilisation de bande passante élevée, donc, le canal peut être saturer.
Dans la littérature, plusieurs protocoles de contrôle de congestion ont été proposés. Parmi ces protocoles, il existe une catégorie qui permet d'améliorer les performances des VANETs en termes de taux de transmission des paquets, que nous présentons ci après.

1. **Traffic Information Systems : Efficient Message Dissemination via Adaptive Beaconing**
   Dans [28], Sommer et al. Ont proposé l'approche ATB (Adaptive Traffic Beacon) pour augmenter l'envoi des messages dans le réseau et éviter la surcharge des canaux. ATB est une approche entièrement distribuée, qui ajuste dynamiquement le taux de transmission, afin de calculer l'intervalle de diffusion des messages, en fonction de deux phases :

   (a) **Qualité du canal**
   La qualité du canal (C) est déterminé à l'aide de trois mesures : le rapport signal/bruit (SNR), le nombre des véhicules voisins et le dernier état évalué dans le réseau.
   Tout d'abord, un nœud examine le nombre de collisions sur le canal, en

dérivant une valeur K. Ensuite, il mesure continuellement le rapport signal/bruit (SNR) sur le canal, en dérivant une valeur S ; si la voiture est loin, le SNR sera très petite. Enfin, il étudie les massages d'autres nœuds et détermine le nombre de voisins N, y compris lui même.
Cependant, un nœud détermine la valeur de la qualité globale du canal C en combinant linéairement les valeurs K, S et N, dans un intervalle de [0,1], sachant que la valeur inférieure représente une meilleure qualité du canal.

(b) **Utilité des messages**
L'utilité des messages (P) est calculé en fonction de l'âge des messages, de la distance entre les véhicules et des positions d'événements.
D'abord, un nœud indique la distance D_e d'un véhicule qui subi l'événement. Ensuite, il détermine l'âge A du message. Ce qui permet de diffuser les informations plus rapidement. Calculer la valeur d'utilité P revient à combiner les deux valeurs D_e et A, qui peut également varier de 0 à 1. Sachant que les valeurs inférieures décrivent les messages de priorité plus élevée.

*** Discussion**

L'approche ATB peut empêcher les collisions du canal pendant la diffusion des messages. Par ailleurs, la diffusion de l'information d'une manière entièrement distribuée (ATB) fait face à des défis strictes, dans le contexte d'environnements très dynamiques et hétérogènes (VANET). Toutefois, cette approche ne tient pas en compte le paramètre de la couche MAC, car elle calcule la probabilité et le délai de réception des balises. En outre, certaines applications de sécurité ne sont pas satisfaisantes en raison de la réduction du taux de balisage qui entraîne l'absence d'informations requises pour fonctionner efficacement.

2.4.2.2 Solutions basées sur l'énergie et la puissance d'émission

Les solutions basées sur l'énergie et la puissance de transmission est accordée pour diminuer les collisions des canaux. Les applications de sécurité envoient généralement leurs messages de sécurité avec une grande plage de transmission pour couvrir une zone plus grande, de sorte qu'un plus grand nombre de nœuds peuvent recevoir ces messages. Cependant, si la congestion se produit dans les réseaux, certains véhicules devraient réduire leur puissance d'émission pour réduire les collisions des canaux. Nous présentons ci-après quelques protocoles réalisés dans ce contexte.

1. **Cross-layer congestion control model for urban vehicular environments**

   R Jabbarpour et al. [20] ont traité le problème de congestion, qui est affectée par la bande passante limitée dans la norme IEEE 802.11p. Ils ont classé les mécanismes de contrôle de congestion en trois classes, à savoir réactifs, proactifs et hybrides, en fonction de la manière dont ils l'empêchent, en ajustant les paramètres de transmission.

   Ils ont proposé un modèle de contrôle de congestion multicouches transversales, basé sur une valeur de seuil dynamique, qui peut être utilisée pour atténuer les deux inconvénients, à savoir, l'exigence d'un modèle de communication qui mappe les niveaux de puissance d'émission ; la nécessité d'estimer avec précision la quantité de trafic généré via la couche application, en tenant compte à la fois de la puissance d'émission et du taux de génération de trafic simultanément.

   Pour ce faire, les auteurs se sont concentrés sur l'application, le contrôle d'accès au medium (MAC) et les couches physiques. Les messages liés à la sécurité dans cet algorithme sont classés dans les messages balises et événementiels. Ces messages sont diffusés dans un domaine spécifique avec une priorité élevée dans un temps limité. Les messages perdus ou les retards simples peuvent entraîner la perte de vies. Pour cette raison, la priorité devrait être envisagée dans les réseaux de véhicules.

   Chaque couche du modèle de communication a ses propres responsabilités pour diminuer la congestion dans les VANETs, avec l'utilisation de la bande

passante et la hiérarchisation comme suit :

(a) La couche application peut être utilisée pour réduire le nombre de paquets générés et diminuer la congestion dans diverses conditions.

(b) Dans la couche de transport, des services de communication de bout en bout, tels que le protocole TCP et UDP (User Datagram Protocol), peuvent être fournis pour les applications réseau en utilisant les protocoles sur cette couche.

(c) La couche réseau est capable de réduire la congestion et la charge de la chaîne en utilisant des algorithmes intelligents de routage et de diffusion

(d) Dans la couche MAC, les algorithmes de planification et de mise en file d'attente peuvent être utilisés pour fournir différentes priorités pour différents paquets pour atténuer la congestion. Par conséquent, les paquets à faible priorité peuvent être supprimés pour réduire la charge des canaux dans des conditions congestionnées.

(e) Dans la couche physique, la congestion peut être détectée en détectant et en assignant un seuil prédéfini pour le canal dans cette couche, qui est la première étape du contrôle de la congestion dans tous les réseaux.

Ce modèle de couche se compose de deux modules pour alléger la congestion dans le centre de détection de congestion.
Dans le premier module, les messages événementiels sont priorisés lorsqu'un danger critique ou une situation anormale est détecté sur la route.
Dans le deuxième module, le seuil de la charge du canal est attribué dynamiquement en fonction des propriétés de charge et de transmission de balise. La congestion est détectée chaque fois que la charge de canal mesurée dépasse la valeur de seuil prédéfinie. Un seuil dynamique est utilisé à la place d'un paramètre fixe pour utiliser la bande passante de manière optimale.
Un algorithme Dynamic Distributed Fair Transmit Power Adjustment pour VANET (DD-FPAV) qui ajuste la puissance d'émission et le taux de génération de paquets est proposé pour atteindre les trois principaux objectifs, à savoir le contrôle de congestion, l'hiérarchisation et l'utilisation efficace de la bande

passante. Cet algorithme sert d'algorithme de contrôle de congestion dans le centre de contrôle. L'algorithme est basé sur une affectation MBL dynamique par rapport aux conditions urbaines (trafic élevé et faible).
La valeur du seuil de charge de la chaîne est calculée dynamiquement dans DDFPAV en fonction des conditions routières différentes, telles que les conditions de trafic élevées et faibles, et la présence de messages événementiels au lieu d'utiliser des valeurs prédéfinies et fixes.

*** Discussion**

L'algorithme DD-FPAV proposé soulage les problèmes d'encombrement et améliore l'utilisation de la bande passante dans les VANET, même si la densité de véhicule est élevée. DD-FPAV produit une meilleure probabilité de réception pour les messages balisés et événementiels. En outre, l'algorithme DD-FPAV surpasse les approches existantes en termes de taux de livraison moyen dans le trafic faible et de délai moyen de messages balises et de événementiels dans des conditions de trafic élevées

2.4.2.3 Solutions basées sur CSMA/CA

Les solutions basées sur CSMA / CA contrôlent la congestion en déterminant la capacité d'accès au canal de chaque nœud dans la couche MAC, en ajustant la taille de la fenêtre de conflit (contention) et le délai d'attente (Arbitration InterFrame Space : AIFS), ces derniers jouent un rôle important pour réduire les collisions des canaux. Ce qui suit est une catégorie de protocoles s'attaquant à ce problème.

1. **Establishing strict priorities in IEEE 802.11p WAVE vehicular networks**
   Barradi et al. [4] ont présenté une stratégie de contrôle de congestion de la couche MAC pour soutenir les deux capacités manquantes : les priorités strictes et les acquittements des messages diffusés de l'algorithme EDCA (Enhanced Distributed Channel Access), qui garantit sans délai le transfert de message de sécurité de haute priorité sur le canal de contrôle (CCH). Ce dernier est chargé

de trier les paquets en quatre files d'attente distinctes identifiées par leurs index (AC [3], AC [2], AC [1] et AC [0]). Sachant que : AC [3] concerne les informations d'urgence (accidents, obstacles, etc.) et les informations générées par les voitures ; AC [2] concerne les informations de présence et de vitesse annoncées par les véhicules ; AC [1] concerne les informations envoyées par les véhicules demandant de l'aide lorsqu'ils ne présentent aucun risque pour d'autres véhicules et AC [0] concerne les informations visant à établir de nouvelles connexions non liées à la sécurité sur les canaux de service.
Ce système ajuste la taille de la fenêtre de contention et l'AIFS, en empruntant deux étapes principales, citées ci-dessous.

(a) **Standard WAVE**

Le protocole d'EDCA offre des capacités de différenciation du trafic parmi les quatre files d'attente, en leur attribuant un ensemble spécifique de paramètres, tel que l'AIFS (Arbitrage Inter Frame Space), qui définit l'intervalle du temps minimum, que le medium doit être détecté pour qu'un nœud décide s'il est libre ; la fenêtres de contention (CW), qui génère un nombre aléatoire pour le mécanisme de retour et la limite TXOP (transmit opportunity), qui définit l'intervalle du temps le plus long pour la possibilité d'émission de trames.

La durée de l'AIFS pour chaque file d'attente AC est définie comme suit :
$AIFS[AC] = SIFS + AIFSN[AC]$ * *temps de fente*
Où $SIFS$ est le temps qui sépare les échanges de tramesson et son ACK ; $AIFSN[AC]$ (numéro $AIFS$) décrit le nombre minimum de slot à attendre avant de démarrer le compte à rebours et le temps de fente est la durée d'un intervalle de temps de couche physique.

(b) **Priorités strictes**

Dans le pire des cas, un cadre de classe k de priorité supérieure doit attendre $AIFS[k]$ plus grand, avant d'être transmis. Dans le meilleur des cas, un cadre de classe inférieure k-1 doit attendre $AIFS[k-1]$, en supposant que l'intervalle aléatoire sélectionné est nul.

Les auteurs ont proposé d'établir que les messages AC [3] ont une priorité strictement plus élevée que les messages AC [2] et que ces derniers, à leur tour, ont une priorité strictement plus élevée que les messages AC [1]. Étant donné que les messages AC [1] ne sont pas aussi critiques pour la sécurité que les messages correspondant à AC [2] et AC [3] et n'aient pas une priorité strictement plus élevée que les messages AC [0].

*** Discussion**

Cette stratégie ajuste les gammes de la taille de fenêtre de contention et $AIFS$ et fournit les ACK des messages diffusés dans le canal de contrôle pour assurer leur transmission. Mais, ces accusés de réception provoquent plus de collisions dans les réseaux, en raison de l'ajout de charges supplémentaires sur les canaux. Le retard, la gigue et la perte de paquet se réduisent pour les messages de sécurité dans des conditions fortement denses. Par ailleurs, cette stratégie n'est pas efficaces pour les messages à faible priorité.

2.4.2.4 Solutions basées sur la priorité et l'ordonnancement

Les solutions basées sur la priorité et l'ordonnancement contrôlent la congestion en définissant une priorité pour chaque message, puis en les programmant dans les files d'attente de contrôle CCH ou de service SCH. Les priorités sont définies de telle sorte que les messages de sécurité hautement prioritaires ont plus de chances d'acquérir les canaux et de transférer avec moins de retard. Quelques protocoles reliés à de telles application seront montrés ci-dessous.

1. **A Cooperative Congestion Control Approach within VANETs : Formal Verification and Performance Evaluation**
   Bouassida et al. [6] ont présenté une nouvelle stratégie qui contrôle la congestion dans les VANETs, afin de programmer de manière dynamique et coopérative la transmission des messages, en fonction de leurs priorités. Cette approche est divisée en trois étapes, à savoir :

(a) **Affectation des priorités**

Les messages recevront une priorité par la mise en route de l'application. Les paquets de priorité moyenne et faible sont retardés pour permettre l'envoi des paquets de priorité élevée sans délai. La priorité d'un paquet est composée de trois champs : Le facteur statique, défini en fonction du contexte du message ; le facteur dynamique, défini en fonction de l'état du réseau (densité) et la taille du message. Ces champs sont combinés pour obtenir l'indicateur de priorité global (Priorité du message = facteur dynamique * Priorité du message statique / taille du message).

(b) **Planification des messages**

Chaque nœud planifie ses messages en fonction de leurs priorités dans le canal approprié, soit de contrôle (CCH) ou de service (SCH). Le canal de contrôle est principalement utilisé pour transmettre les messages de balise, les messages à priorité élevée ou pour transférer les messages de service lorsqu'il est libre. Cette stratégie transfère sans délai les messages de priorité élevée et reprogramme les messages de priorité moyenne et faible dans les canaux. Par contre, SCH est disponible pour les applications de sécurité avec une priorité inférieure.

(c) **Transmission coopérative**

Le processus de transmission des messages envoie le message de priorité plus élevée dans le canal correspondant, chaque fois qu'il est libre. Cependant, l'envoi de paquets de priorité élevée via le canal de contrôle est préemptif par rapport aux paquets envoyés via le canal de service. En effet, afin d'envoyer des paquets de priorité élevée avec un délai minimum, l'émission de paquets de priorité inférieure est bloquée, même si leur canal correspondant est libre. Cette technique de transmission coopérative est divisée en deux mécanismes principaux :

i. **Partage de bande passante**

Afin de ne pas saturer la bande passante fournie et de permettre une transmission fiable des messages d'urgence, la bande passante offerte

à l'application VANET par 10 Mhz est égale à la moitié de la bande passante totale.

ii. **La prochaine sélection de redirection pour le cas de communication multi-sauts**
Dans le cas des communications inter-véhicules multi-hop, le choix du prochain expéditeur est essentiel pour améliorer les performances de l'architecture de communication. Le prochain expéditeur devrait être choisi comme nœud moins congestionné dans le voisinage.

*** Discussion**

La stratégie proposée est la meilleur en terme de taux de livraison de paquets d'avertissement, car il essaye de garder le canal CCH libre des messages de balise. Ces résultats ont confirmé que le contrôle de congestion avec l'adoption de l'algorithme de retransmission est l'une des meilleures solutions pour la diffusion des applications de sécurité événementielles dans un réseau dense. En utilisant la stratégie proposée, les charges du réseau diminuent et les ressources sont efficacement utilisées. Cependant, les frais généraux de communication augmentent en raison de l'échange du contexte des messages entre les véhicules voisins. En outre, le problème de la diffusion n'est pas pris en compte.

2.4.2.5 Solutions hybride

Dans les solutions hybrides, deux ou plusieurs paramètres et moyens sont utilisés comme le réglage de la vitesse de transmission, et l'ajustement de la taille de la fenêtre de conflit et de l'$AIFS$, la définition d'une priorité appropriée pour chaque message et la planification dans les canaux sont combinés pour éviter la saturation des canaux dans les VANETs. Nous présentons, dans ce qui vient, certains algorithmes réalisés dans ce contexte.

1. **A Robust Congestion Control Scheme for Fast and Reliable Dissemination of Safety Messages in VANETs**

Djahel et al. [14] ont introduit une stratégie de contrôle de congestion qui garantit la fiabilité et la diffusion économique des messages de sécurité, en contrôlant le taux, la puissance de transmission et la priorité des messages de balise. Cette dernière consomme une grande quantité de la bande passante du canal de contrôle, qui entraîne une congestion. La stratégie proposée comprend trois phases, présentées ci-après, dans le but d'identifier l'état de congestion dans le réseau et faciliter la diffusion des messages événementiels.

(a) **Affectation prioritaire et planification des messages**
Lorsqu'un véhicule reçoit un message diffusé par les unités routières (RSU), la couche MAC classe ces messages par ordre de priorité dans trois niveaux (bas, moyen et haut) en fonction de leur degré d'importance et de danger, tandis que la planification des messages de sécurité sont triés selon leur type de contenu. Ce dernier se compose de trois types, comme indiqué ci-dessous.

i. **Message d'urgence**
Ce type de message est envoyé en cas d'accidents, de conditions météorologiques, etc. On lui attribue la priorité de niveau supérieur (HL).

ii. **Message d'avertissement**
Ce message est envoyé pour annoncer un événement important sur la route, mais pas un danger immédiat (critique). On lui attribue une priorité de niveau moyen (ML).

iii. **Annonce sur l'information routière**
Ce type de message contient les informations sur les embouteillages dans certains segments routiers, afin de diriger le conducteur vers la route la plus rapide et la moins congestionnée. On lui attribue la priorité de niveau le plus bas (LL).

Dans le cas de recevoir de nombreux messages de même type de contenu, une deuxième métrique est alors utilisée pour déterminer le niveau de priorité d'un message. Cette métrique utilise un champ baptisé (Hop cpt) à

l'en-tête de paquet de message de sécurité, afin d'accélérer la transmission des nouveaux messages d'urgence. Ce choix est dû aux raisons suivantes :

i. Une valeur de (Hop cpt) inférieure signifie que le danger est très proche du véhicule récepteur. Ainsi, ce message doit être transmis très rapidement vers ses voisins afin d'éviter d'autres dommages.

ii. Une plus grande valeur (Hop cpt) indique que le danger est relativement éloigné du véhicule récepteur.

(b) **Détection de congestion**
La congestion est détectée en mesurant le temps d'attente moyen AWT (Average Waiting Time), le taux de collision CR (Collision Rate) et le taux de réception des balises BRR (Beaton Réception Rate). Si les valeurs de ces mesures dépassent les seuils prédéfinis, la congestion est détectée dans le canal de contrôle.

(c) **Ajustement dynamique de puissance et du taux de transmission**
Lorsqu'un véhicule vérifie que le réseau est encombré, il ajuste la charge de balise afin de conserver une certaine quantité de la bande passante pour la transmission des messages événementiels nécessitant un faible délai de transmission. La charge de balise peut être réduite soit par la réduction de la puissance d'émission, en fonction du taux de collision et l'état des véhicules voisins ; soit par la diminution de leur vitesse de transmission. Ensuite, le véhicule partage la puissance et le débit de transmission calculés avec les véhicules voisins pour diminuer la charge du canal de contrôle. La vue schématique de la stratégie proposée est illustrée dans la Figure2.2.

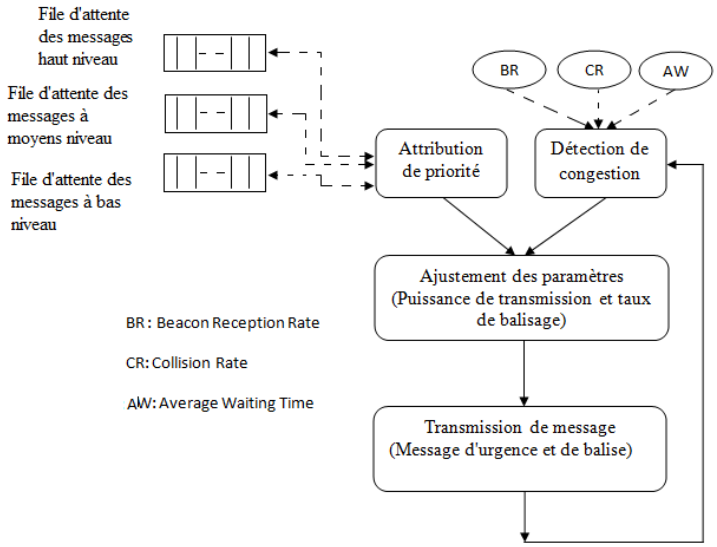

FIGURE 2.2 – Aperçu global sur le système de contrôle de congestion [14].

*** Discussion**

Cette stratégie améliore le taux de réception des messages d'urgence et augmente la sécurité et la fiabilité des VANETs. Cependant, le retard de cette stratégie est important en raison de la détection de la congestion. En outre, l'échange d'informations entre les véhicules voisins ajoute une surcharge de communication élevée dans les canaux et le partage de la même fraction de la bande passante n'est pas souvent souhaitable pour différentes applications de sécurité.

2.5 Tableau récapitulatif

Après avoir étudier et analyser les protocoles, cités précédemment et ceux figurant dans les annexes, il nous est apparu qu'une étude comparative est esti-

mable. La table 2.1, illustre cette étude selon les fonctions, caractéristiques et critères d'évaluation de la Qos, détaillées dans le chapitre précédent.

Protocoles	Paramètres	Fonctionnements	Classes	Efficacité	Fiabilité	Priorité d'accès	Délai	Puissance de transmission	Débit
[36]	Taux de transmission	– Diffusion fiable – Diffusion efficace	Proactif	Oui	Oui	Non	Non	Oui	Non
[30]	Taux de transmission	– Évaluation de la charge du canal – Adaptation tarifaire	Proactif	Non	Oui	Non	Non	Non	Oui
[28]	Taux de transmission	– Evaluation de la qualité du canal – Calcul d'utilité du message	Proactif	Non	Oui	Oui	Non	Non	Non
[37]	Énergie et puissance d'emission	– Calcul de la probabilité de transmission	Réactif	Oui	Non	Non	Non	Oui	Oui
[32]	Énergie et puissance d'emission	– Définition d'un seuil – Accord des priorités aux messages balises ou événementiels	Réactif	Non	Oui	Non	Oui	Oui	Oui
[20]	Énergie et puissance d'emission	– Algorithme D-FPAV	Réactif	Non	Non	Oui	Non	Oui	Non

[4]	CSMA/CA	– Ajustement de la taille de la fenêtre de contention et l'AIFS	Réactif	Non	Non	Oui	Oui	Non	Oui
[15]	CSMA/CA	– Mécanisme de détection de porteuse d'énergie (IPCS)	Proactif	Non	Oui	Non	Non	Oui	Oui
[12]	Priorité et ordonnancement	– Détection et contrôle de congestion – Retransmission des messages	Réactif	Non	Oui	Oui	Non	Non	Non
[6]	Priorité et ordonnancement	– Affectation des priorités – Planification des messages – Transmission coopérative	Proactif	Non	Oui	Oui	Non	Non	Non
[29]	Priorité et ordonnancement	– Planification des messages	Proactif	Non	Oui	Oui	Oui	Non	Non
[14]	1. Puissance d'émission 2. Taux de transmission 3. Priorité des messages	– Affectation prioritaire – Planification des messages – Détection de congestion – Ajustement dynamique de la puissance	Hybride	Oui	Non	Oui	Non	Non	Oui

[3]	1. Taux de transmission 2. puissance d'émission	– Contrôle de puissance d'émission à partir D-FPAV – Contrôle du taux de transmission à partir EELBL-F	Hybride	Oui	Non	Non	Non	Oui	Oui
[18]	Contrôler la transmission des paquets dans la couche transport	– Protocole AVOCA	hybride	Non	Oui	Non	Non	Oui	Oui

TABLE 2.1 – Comparaison entre les solutions étudiées.

Notre étude des travaux basés sur les taux de transmission montre que les solutions proposées ajustent le taux de transmission en fonction de la condition du canal et la diffusion fiable des messages pour contrôler la congestion, ces solutions nécessitent, cependant, que les véhicules puissent envoyer ces messages avec une priorité élevé et un délais très petits. Par contre les stratégies basées sur la puissance ajustent dynamiquement la puissance d'émission pour contrôler la charge des canaux. Mais ces solutions nécessitent une diffusion efficace des messages, afin de réduire le délai de transmission et la priorité des messages événementiels ne sont pas prise en considération. En effet les solutions basées sur CSMA/CA contrôlent la congestion en déterminant les valeurs appropriées pour la taille de la fenêtre de contention et l'$AIFS$ pour l'accès au canal. Dans les solutions basées sur la priorité et l'ordonnancement, les messages de sécurité hautement prioritaires ont plus de chance de se transférer dans les canaux. Enfin, les stratégies hybrides utilisent tout ou quelques paramètres et moyens de stratégies antérieures pour contrôler la congestion dans les VANETs. A l'issue de cette étude comparative, nous avons pu appréhender les enjeux majeurs qui entourent la congestion dans les VANETs.

2.6 Conclusion

Il existe de nombreuses techniques proposées pour améliorer la QoS dans les VANETs, où l'une d'entre elles est le contrôle de congestion, qui est un problème majeur associé à la circulation des véhicules. Dans ce chapitre, nous avons étudié le problème de congestion dans les VANETs, en faveur des applications de sécurité, et nous avons cité quelques algorithmes efficaces, proposés par certains chercheurs. A l'issue d'une étude comparative entre ces travaux, il nous est apparu qu'une proposition pourrait être une nouvelle solution au problème de congestion, dont souffre les réseaux VANETs, qui sera l'objectif du prochain chapitre.

Chapitre 3

Nouvel algorithme de contrôle de congestion dans les VANETs

3.1 Introduction

La majorité des protocoles de contrôle de congestion dans les réseaux VANETs, vu dans le chapitre précédent, ont tous des parties incomplètes et nécessitent des améliorations, car parfois le traitement d'un problème peut générer un autre problème. Pour cela et pour fournir une qualité de service encore meilleure, nous avons proposé un algorithme de contrôle de congestion appartenant à la classe de la priorité et l'ordonnancement des messages, en fonction du temps d'occupation, de la réduction du débit et d'un seuil pour la détection de congestion.

Dans le chapitre présent, nous allons présenter le fonctionnement de cet algorithme, puis, nous allons évaluer ses performances au moyen du simulateur NS-2, en donnant les différents métriques et paramètres et en discutant les résultats obtenus, pour les comparer avec ceux obtenus dans le protocole de Darus et al [12], intitulé "Congestion control algorithm for eventdriven safety messages in vehicular networks".

3.2 Principe de fonctionnement de l'algorithme proposé

Les problèmes de congestion font partie d'une réalité des réseaux de communications. Cependant, cette communication véhicule un message de balise ou un message événementiel, qui seront diffuser dans le canal CCH. Nous allons proposé un nouvel algorithme, afin d'éviter l'encombrement du canal CCH au niveau de la couche physique, et le retard du message de sécurité événementiel.

Notre algorithme fonctionne en trois étapes, à savoir :

1. Affectation des priorités
2. Détection de congestion
3. Contrôle de congestion

Dans ce qui suit, nous allons présenter les détails de ces étapes, ainsi, le diagramme de notre algorithme de contrôle de congestion dans les réseaux VANETs, voir la Figure 3.1.

3.2.1 Affectation des priorités

Dans cette phase, chaque véhicule possède deux variables locales, à savoir, la variable K, initialisée à nul, indiquant le niveau d'utilisation du canal de contrôle (CCH).

La variable S, initialisée à val, indiquant un seuil et présentant l'approche de la congestion, sachant que la capacité du canal est à 100% et val est inférieur à cette capacité.

Tous les véhicules peuvent recevoir les deux types de message, définis précédemment, soit balise ou événementiel. Selon le type d'un message, son utilité est calculée par l'affectation d'un temps d'occupation dans le canal et une priorité. La Table 3.1 résume cette procédure.

Types de message	Temps d'occupation	Priorités	Exemples
Événementiel	Supérieur	Haute	– Accident – Route barrée – Dangers éventuels
Balise 1	Moyenne	Moyenne	– Vitesse – Ceinture de sécurité
Balise 2	Inférieur	Basse	– Météo – Direction

TABLE 3.1 – Exemples sur le calcul d'utilité d'un message.

3.2.2 Détection de congestion

Dans cette phase, la fonction de détection est de surveiller le canal de communication CCH, en fonction de la variable K, qui est incrémentée à chaque accès au canal.

Le nœud détecte que le canal CCH est encombré une fois la variable K dépasse le seuil prédéfinie S (val).

3.2.3 Contrôle de congestion

Cette phase est une suite des tests présentée sous forme d'algorithme, voir Algorithme 1. Le premier test consiste à vérifier la condition ($k <= val$) pour détecter la congestion. Le deuxième test consiste à vérifier l'arrivé du message de sécurité événementiel, pour appliquer la politique du premier arrivé le premier servi. Dans le

cas échéant, ajuster la vitesse de transmission de balise et de les supprimer selon les priorités inférieurs.

Algorithm 1 Algorithme expliquant la troisième phase de la solution.

```
if (K <= val) then
  if (Arrivé du message événementiel) then
    Appliquer la politique (Le premier arrivé le premier servi) ;
  else
    Ajuster la vitesse de transmission des messages de balise ;
    Supprimer les messages de balise selon la priorité inférieur ;
  end if
else
  Accès au canal de contrôle CCH ;
end if
```

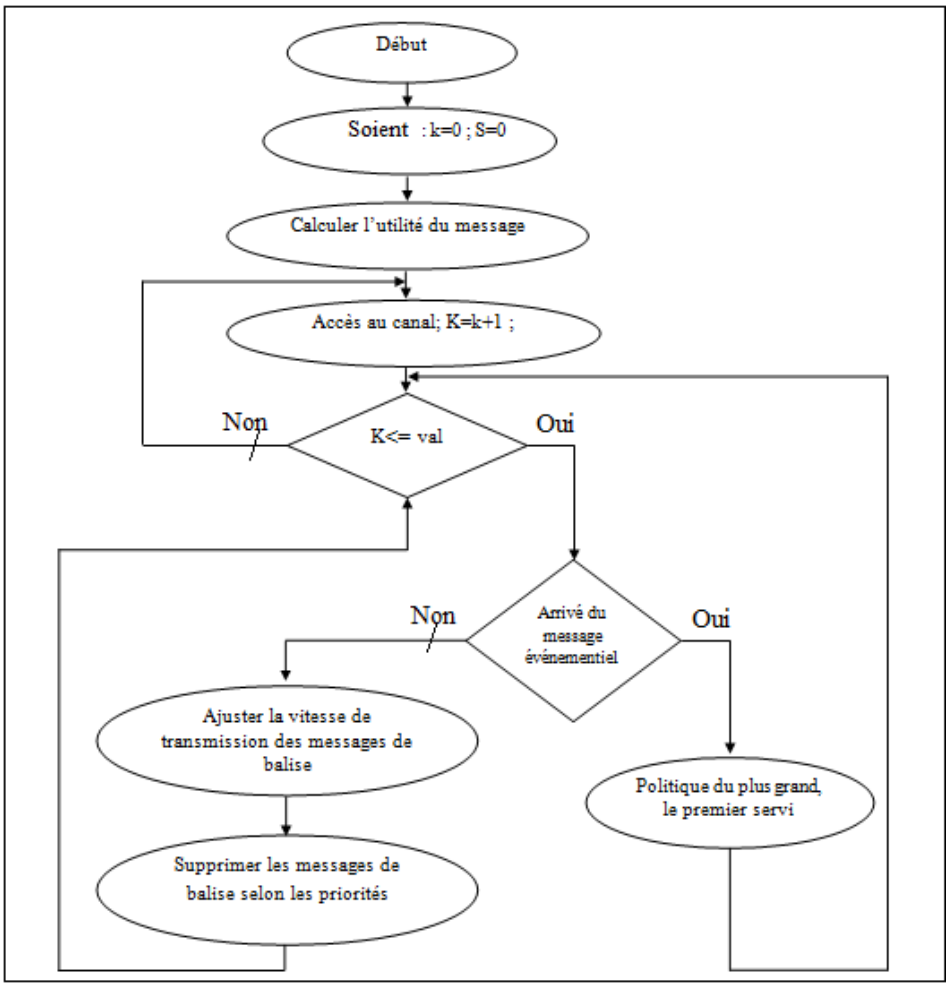

FIGURE 3.1 – Diagramme proposé pour le contrôle de congestion.

3.3 Evaluation de performances de notre algorithme

Le but de toute simulation est de tester les systèmes réalisés avant qu'ils soient mis en marche afin de déterminer les conditions exactes de leur fonctionnement,

évaluer leurs performances et prévoir les différents états liés à ces systèmes et donc de bien réagir et prendre des décisions.

Dans cette section, nous présentons le simulateurs NS-2, que nous avons utiliser pour évaluer les performances de notre algorithme. Puis, nous décrivons les paramètres de simulation et nous discutons les résultats obtenus.

3.3.1 Présentation du simulateur NS-2

NS-2 (Network Simulator version 2) est un outil de simulation "Open Source" qui appartient à la famille des simulateurs événementiel "Event-Driven". Ce simulateur a était conçu pour la recherche spécialisée dans le domaine des réseaux informatiques, plus particulièrement, les protocoles de communication filaire et non filaire. Il dispose d'un nombre important de modèles de protocoles de toutes les couches du modèle OSI allant de la couche physique à la couche Application.

Comme les autres simulateurs de réseaux, NS-2 a été développé en utilisant deux langages de programmation : le langage C++, qui définit les mécanismes internes des objets de simulation (le noyau du simulateur) et le langage Otcl (Object-oriented Tool Command Language) qui est responsable de la configuration et la liaison de ces objets ainsi que l'ordonnancement des événements "Events Scheduling". Il joue le rôle d'une interface entre l'utilisateur et le noyau du simulateur à travers le script TCL (Tool Command Langage). Cette architecture, illustrée dans la Figure 3.2, est introduite afin de permettre une exécution rapide grâce au langage C++ pour le détail d'implémentation des protocoles, en plus de la possibilité de modifier la configuration de manière rapide et interactive à travers le langage OTCL [1].

Les fonctionnalités qu'offre ce dernier à travers l'étude et l'élaboration de scripts qui font appel à des outils comme : Nam (Network Animator) qui visualise la simulation ou encore Xgraph qui permet de représenter les traces de la simulation sous forme de courbe.

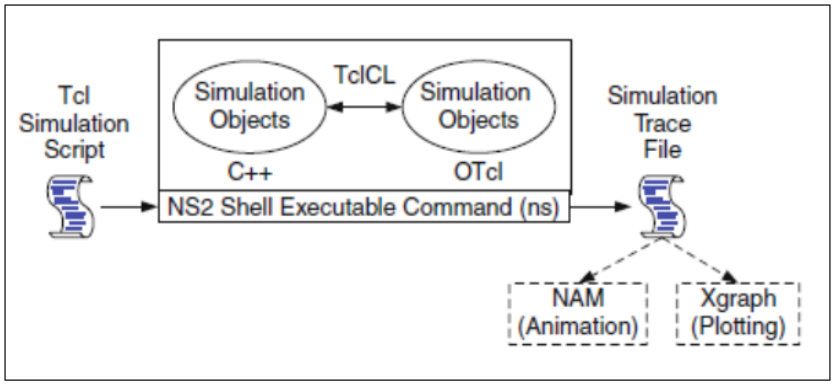

FIGURE 3.2 – Architecture de base de NS-2 [19].

3.3.2 Paramètres de simulation

Notre proposition a été simulée sous le simulateur NS-2. Cette simulation a été réalisée avec huit (8) nœuds, dont quatre (4) nœuds représentent des capteurs, qui sont placés dans un véhicule et qui permettent d'envoyer des messages de balises. Deux (2) autres nœuds représentent des véhicules permettant de délivrer des messages événementiels et le (7) représente le véhicule destinataire. Chaque capteur possède une portée radio d'environ 1m et un débit de 10Mb. Afin de mesurer les pertes de paquets par un véhicule, lors d'une transmission, nous nous sommes basés sur un seul véhicule pour l'accès à son canal CCH. Les paramètres fixés pour la réalisation des simulations sont définis dans la Table 3.2.

Paramètres	**Valeurs**
Nombre de nœuds	8
Type du trafic	CBR,UDP
Débit de données	1 Mbps
Délais de propagation	10 ms
Taille max des canaux	100 paquets
Taille des paquets	500 bit
Seuil	70 paquets
Durée de simulation	40s
Zone de déploiement	NAM

TABLE 3.2 – Paramètres de simulation de notre solution.

Notre proposition est basée sur l'accès au canal de contrôle CCH, afin d'éviter la surcharge des messages de balise au niveau de la couche physique et donner la priorité au message événementiel au niveau de la couche MAC. Dans ce cas, la mobilité, la densité, le nombre et la vitesse des véhicules ne sont pas pris en considération.

La simulation a débuté par la transmission des messages de balise par différents capteurs (1, 2, 3, 4), qui sont placés au sein d'un véhicule, d'une manière périodique, avec un intervalle de temps $Dt = 0.005s$. Une variable k surveille la surcharge du canal CCH avec un seuil (qui sera définit lors de la simulation).

À un instant donné T, un autre véhicule (5 ou 6) envoie un message événementiel à un autre véhicule (destinataire (7)), indiquant un danger. De ce fait, les capteurs diminuent leurs vitesses de transmission à 50 % de la vitesse précédente. La Figure 3.3 illustre le début de la simulation.

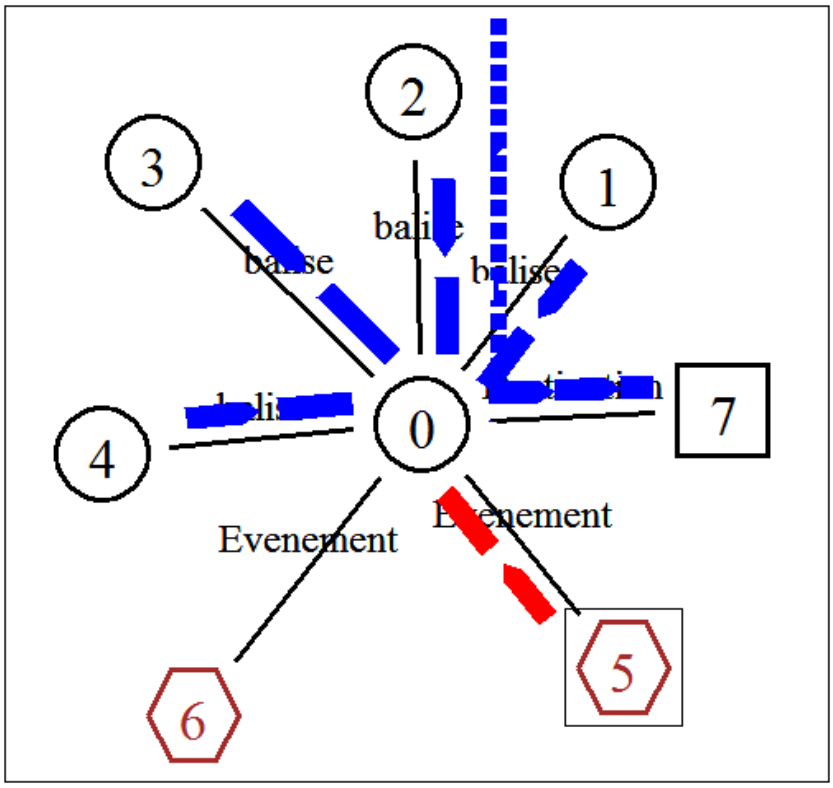

FIGURE 3.3 – Illustration du début de simulation.

3.3.3 Métriques de performance

Afin d'évaluer les performances de notre protocole, nous utilisons les métriques de simulation suivantes :

- **Perte de paquets :** C'est la perte ou bien le retard des paquets qui conduit à un gaspillage de la bande passante et un taux d'erreurs élevé des paquets de données lors de leur réceptions.
- **Délai de transmission :** C'est le temps écoulé entre l'envoi d'un paquet par un émetteur et sa réception par un récepteur.
- **Taux de paquets délivrés :** C'est le rapport entre le nombre de paquets

de données reçus par les destinations et le nombre de données émis par les sources.

3.3.4 Résultats et discussions

Dans cette section, nous intéressons à l'étude des performances de l'algorithme proposé, nous allons les présenter sous forme de graphiques puis nous interprétons les résultats obtenus.

1. **Perte de paquets**
   Pour fixer une variable de seuil S, nous nous procédons par l'essai de plusieurs simulation, en fonction de deux valeurs (70, 80), par rapport au nombre de paquets perdus.
   Cependant, les valeurs inférieurs à 70 engendre le problème d'énergie des capteurs et les valeurs supérieurs conduit à des pertes de paquets élevées.
   La Figure 3.4 représente le nombre de messages de balise perdus pour libérer le canal CCH.

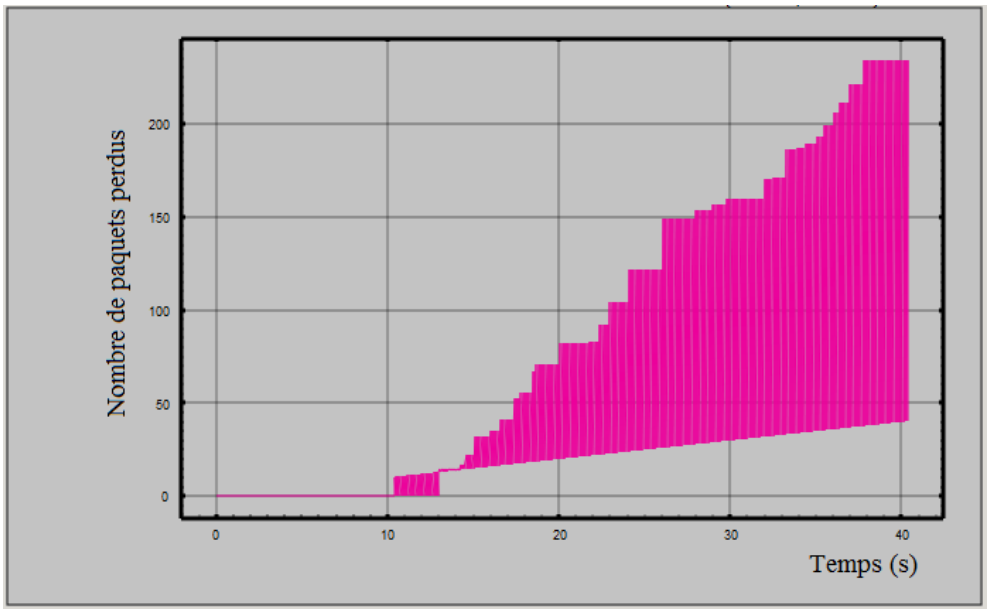

FIGURE 3.4 – Nombre de paquets perdus par seconde avec $S_1 = 70$.

* Après 10 secondes de simulation, nous remarquons une augmentation de perte de paquets de messages de balise, suite à l'affectation de la valeur de seuil ($S_1 = 70$). Puis, à partir de la 35eme seconde, cette perte se stabilise à 260 pq/s.

* Après avoir affecter au seuil la valeur ($S_2 = 80$), on obtient la Figure 3.5 , dont on remarque 310 paquets perdus. Alors, nous déduisons que l'augmentation du seuil engendre une perte élevée de paquets.

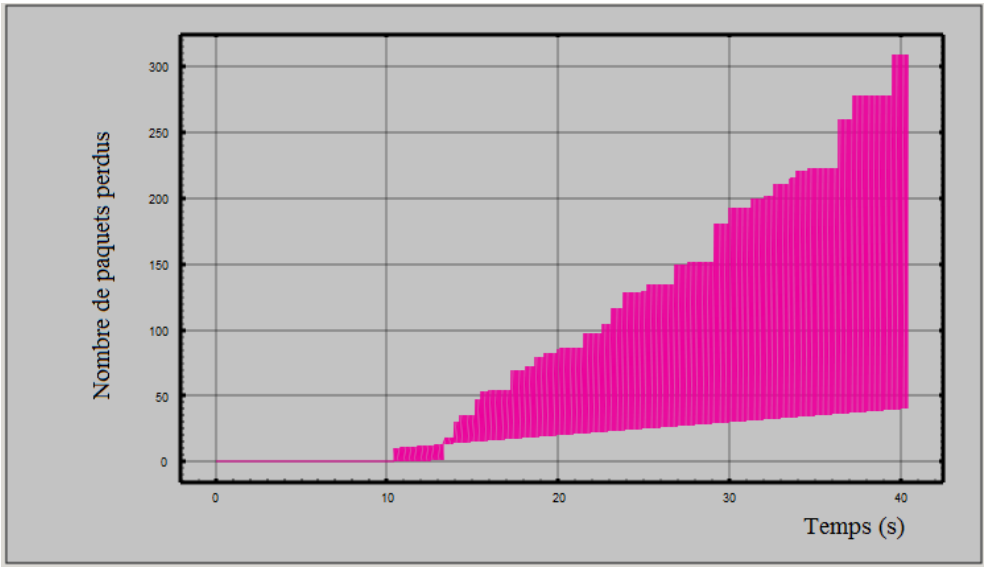

FIGURE 3.5 – Nombre de paquets perdus par seconde avec $S_2 = 80$.

Après avoir comparer les deux résultats de perte de paquets par rapport à S_1 et S_2, nous remarquons que nombre de paquets perdus de S_1 est inférieur au nombre de paquets perdus de S_2.

Notre objectif vise à minimiser la perte de paquets, alors, nous fixons la valeur la plus adéquate pour le seuil à $S = 70$ pour calculer le taux ainsi que le délai de transmission.

2. **Délai de transmission**

   La Figure 3.6 illustre le retard des paquets de type événementiel.

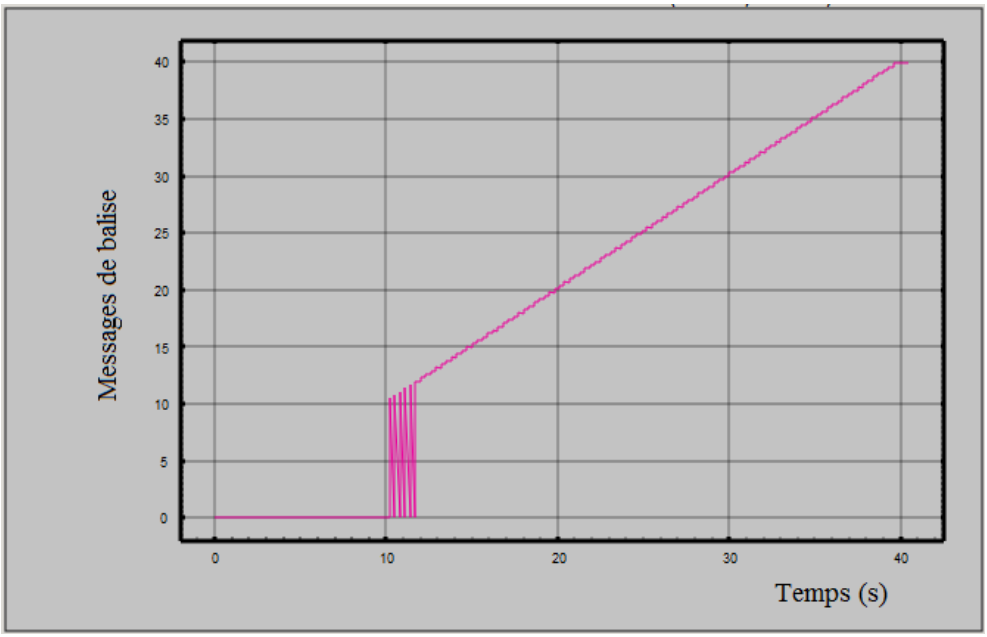

FIGURE 3.6 – Délais de transmission d'un message événementiel.

En raison d'envoi des messages de balise, d'une manière illimité, ce graphe montre que le délai de paquets augmente.
Cependant, la performance des messages de sécurité événementielle, de notre algorithme, est bonne en terme du temps (40ms).
Sachant que, dans la littérature, le cas le plus défavorable est 60ms [12].

3. **Taux de transmission**
   La Figure 3.7 illustre le taux de transmission des paquets reçu d'un véhicule.

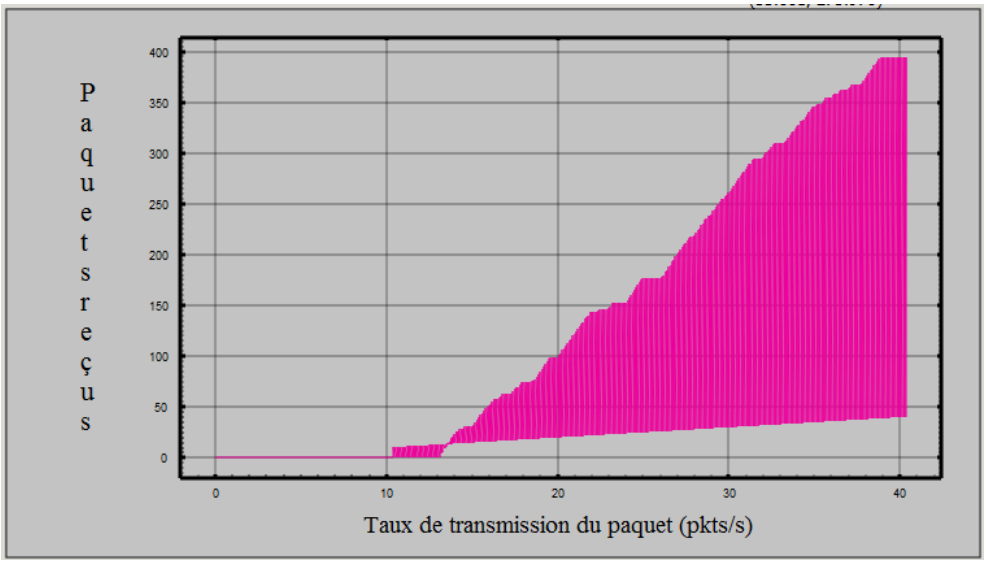

FIGURE 3.7 – Taux de transmission d'un paquet par seconde.

Chaque point de la courbe correspond à la combinaison de la vitesse de transmission des paquets et sa puissance. Par ailleurs, à l'instant 10s, le taux de transmission augmente jusqu'à l'atteinte de 390 paquets/s. Pour ce fait, notre algorithme permet de répondre à l'efficacité.

3.4 Conclusion

Divers algorithmes évitent le problème de congestion dans les VANETs et le retard du délai du message événementiel. Mais ces algorithme réclament plus de perfectionnement. Pour cela, dans ce chapitre, nous avons proposé un algorithme de contrôle de congestion proactif de la classe priorité et ordonnancement. Nous avons évalué ses performances par le simulateur NS2 et nous avons obtenu des résultats intéressants en termes de nombre de paquets perdus, du délai de transmission ainsi que du taux de transmission.

Nous estimons comparer notre algorithme avec le protocole de Doris et all [12], présenté dans l'annexe. Mais en raison de la limite de temps, nous n'avons pu atteindre ce point.

Conclusion et perspectives

Les réseaux VANETs sont un cas particulier des réseaux ad hoc Mobile MANET. Ces réseaux appartiennent à un nouveau domaine de recherche qui s'annonce vaste et riche en possibilité de développement d'applications.

Dans ce mémoire, nous avons proposé l'amélioration des systèmes de communication des réseaux ad hoc véhiculaires pour la qualité de service. Plus particulièrement, nous cherchons à mieux contrôler la congestion dans ces réseaux pour rendre cette communication plus sécurisée.

Notre objectif a été axé sur l'étude et l'analyse de ce problème. Pour se faire, nous avons présenté, dans un premier lieu, les différentes généralités sur les réseaux VANETs, afin de comprendre le contexte de notre travail. Par la suite, nous avons résumé, selon quelques paramètres et moyens, certains travaux de recherche menés dans cet axe. Enfin, nous avons présenté un algorithme pour contrôler la congestion avant son apparition dans le canal CCH. Puis, nous l'avons simulé sous NS-2 pour présenter les résultats obtenus. Cet algorithme se base sur l'affectation prioritaire, le calcul du taux de transmission, l'ajustement du débit de transmission et la surveillance de l'occupation du canal, en se basant sur un seuil prédéfini.

En guise de perspective, nous souhaitons faire une comparaison avec d'autre protocole, de la même classe, pour tester l'efficacité de notre algorithme. Ainsi, nous envisageons à modéliser la mobilité des VANETs, à l'aide du modèle SUMO. Ces modèles doivent prendre en considération les contraintes de la mobilité véhiculaire, pour que la simulation soit proche de la réalité. Sachant que la mobilité se traduit

par la possibilité que certaines entités peuvent passer d'une cellule à une autre sans perdre la liaison.

Chapitre A

ANNEXES

Etude critique de certains protocoles de contrôle de congestion dans les réseaux VANETs

A.1 Introduction

Dans cette présente annexe, nous allons donner quelques aperçus sur certains protocoles, visant à palier au problème de congestion dans les VANETs. Par ailleurs, comme nous l'avons préciser dans le chapitre 2, ces protocoles peuvent appartenir à deux types de classes, à savoir, des classes basées sur des stratégies et d'autres basées sur des paramètres et moyens. Nous notons que dans ce qui suit, nous allons se concentrer sur la deuxième classification.

A.2 Solutions basées sur le taux de transmission

1. **Efficiency and Reliability of One-Hop Broadcasting in Vehicular Ad Hoc Networks**
   Dans [36], Ye et al ont ajouté une nouvelle couche pour communiquer avec la couche MAC, en modifiant la norme WAVE, pour contrôler la congestion dans les VANETs. Ils ont distingué deux paramètres, la fiabilité, qui est définie comme le nombre moyen des nœuds qui reçoivent des paquets avec succès et l'efficacité, qui est définie comme le taux de livraison des paquets diffusés aux

nœuds voisins. Ce protocole se déroule en deux phases principales ; une diffusion efficace, qui est le nombre prévu des nœuds auxquels une source délivre ses paquets par unité de temps et une diffusion fiable, qui contient un récepteur centralisé, qui analyse la probabilité de recevoir un paquet de référence d'une source, avec succès ; un émetteur centralisé, qui calcule le nombre des nœuds pouvant recevoir un paquet de référence, avec succès.

*** Discussion**

L'algorithme proposé contrôle la congestion avec une stratégie qui permet d'atteindre une diffusion efficace presque optimale lorsque les nœuds de réseau ont une mobilité élevée (95 % de l'efficacité optimale en simulation) et garantit une transmission optimale en fonction de la densité des nœuds, de la puissance d'émission, de la longueur du paquet et d'autres paramètres du système VANETs. Cependant, le protocole proposé nécessite une prise en compte des contraintes liées au taux de transmission des messages de sécurité, pour éviter les collisions dans les canaux et transférer ces messages sans délai. Citons les occurrences de collision par transmissions simultanées, problème de terminal caché, le scénario de communication étudiée est un scénario de voie unique, de sorte que les véhicules peuvent simplement diffuser une seule donnée qui n'est pas courante dans les VANETs.

2. **Design Methodology and Evaluation of Rate Adaptation Based Congestion Control for Vehicle Safety Communications**

   Tielert et al. [30] ont proposé le système PULSAR (Periodically Updated Load Sensitive Adaptive Rate), adapté à la vitesse de la charge du canal, d'une manière périodique. Ce protocole est destiné à la communication sécurisé des véhicules (Vehicul Security Communication : VSC), qui est basé sur les communications à court terme dédiées (DSRC) et dominé par des émissions de messages de sécurité de base (BSM) et messages de sensibilisation coopérative (CAM). Les auteurs prennent en considération les principes de conception et les exigences pour les VSC, en introduisant la méthodologie de conception globale qui prend en compte la gamme de transmission, qui est sélectionnée en fonction de la charge du canal, dépendant de l'environnement de conduite. La stratégie PULSAR contrôle la congestion dans trois étapes principales. Dans la première

étape, évaluer la charge du canal pour détecter la congestion et un seuil, à l'aide du rapport d'occupation de canal (CBR), qui est une mesure de rétroaction appropriée pour maximiser le nombre de paquets reçus. La deuxième étape est l'adaptation tarifaire, lorsqu'une nouvelle mesure CBR arrive à la fin de chaque CMDI, PULSAR compare la valeur mesurée par rapport à la valeur cible. Étant donné que CMDI (Channel Monitoring and Decision Interval) est un intervalle de surveillance et de décision du canal de longueur fixe. Si le CBR mesuré dépasse un seuil prédéfini, le taux de transmission diminue. Cependant, s'il est inférieur au seuil, le taux de transmission augmente linéairement. Enfin, dans la dernière étape, le taux de transmission sélectionné est partagé entre les véhicules voisins situés dans la plage de communication.+++

*** Discussion**

Le protocole PULSAR proposé est un algorithme distribué qui réalise l'équité locale en prenant en compte les taux des voisins pour assurer la transmission des messages. Cet algorithme est capable de fonctionner dans l'espace disponible pour les ajustements définis par les applications de sécurité, mais les exigences relatives de ces dernières ne sont pas prises en compte (la priorité, la fiabilité, etc.). En outre, le partage de l'information sur la congestion entraîne une charge supplémentaire dans les canaux. Le réglage du taux de transmission en fonction de charge des canaux conduit à une diminution des performances des messages de sécurité événementiels, la priorité des paquets n'est pas prise en compte.

A.3 Solutions basées sur l'énergie et la puissance d'émission

1. **Congestion Control to Achieve Optimal Broadcast Efficiency in VANETs**

   Dans les VANETs, chaque véhicule diffuse périodiquement des messages contenant des informations de localisation et de vitesse sur ses voisins, à un seul saut. Si la mesure de densité des nœuds augmente, les interférences vives réduisent l'efficacité de la diffusion. Fei Ye et al. [37] ont fourni une stratégie de contrôle

de congestion et de puissance, qui maximisent l'efficacité des massages, en fonction de trois paramètres : la probabilité de transmission optimale en fonction de la densité des nœuds, la puissance d'émission et la longueur des paquets. Cette stratégie diminue la puissance d'émission dans le réseau avec une densité élevée, qui entraîne une réduction de la probabilité de réception des paquets à une distance proche. Elle est très utile pour les applications de sécurité qui doivent avoir plus d'effets sur les véhicules environnants, au lieu de véhicules plus lointains.

*** Discussion**

La stratégie proposée utilise une stratégie de contrôle de congestion et de puissance en maximisant la diffusion efficaces des massages. Cette stratégie garantie au pire des cas au moins 95 % de performance optimale, même lorsque les nœuds de réseau ont une mobilité élevée. Les simulations montrent que les résultats analytiques prédisent avec précision la dynamique du système. Cependant, le réglage de la puissance d'émission dans les VANETs n'est pas une solution évolutive pour contrôler la congestion dans le canal, le retard et la priorité des messages ne sont pas considérées.

2. **Distributed Fair Transmit Power Adjustment for Vehicular Ad Hoc Networks**

   Dans [32], Moreno et Al. Ont proposé une stratégie entièrement distribuée pour contrôler la charge des canaux en fonction de l'ajustement de puissance de transmission des nœuds, intitulée D-FPAV (Distributed Fair Power Adjustment for Vehicular Networks). Il est formellement prouvé d'atteindre l'équité et d'équilibrer la pertinence entre les messages balises et événementiels. D-FPAV fournit une puissance d'émission efficace et une priorité plus élevée pour les messages événementiels, en diminuant la charge de balise dans le canal de contrôle. Dans cette stratégie, chaque véhicule réclame l'information générale sur l'état des véhicules voisins situés dans la plage de sens de porteuse. Sur la base de cette connaissance, les véhicules adaptent la plage de transmission maximale pour les messages de balise de sorte que la charge de balisage ne dépasse pas le seuil predefine. Ensuite, la plage de transmission ajustée est diffusée sur les véhicules voisins situés dans la zone de détection des porteurs.

L'algorithme 2 montre le pseudo-code pour la stratégie D-FPAV, et les étapes de cette stratégie sont définies comme suit :

(a) **Pertinence des messages de sécurité**
Les messages événementiels devraient pouvoir accéder au canal de contrôle avec un court délai et devraient avoir une faible probabilité de collision même lorsqu'ils sont transmis avec une puissance élevée. D'autre part, les balises sont moins pertinentes à des distances plus élevées. Ainsi, une stratégie d'allocation de ressources est nécessaire pour obtenir une hiérarchisation claire, ou un équilibre, parmi les messages en fonction de leur pertinence pour la sécurité.

(b) **Équilibrer les messages de balises et événementiels**
Compte tenu de la pertinence pour les messages de sécurité, la quantité de charge résultant du balisage devrait être limitée ; il est souhaitable d'éviter un nombre élevé de collisions de balises et laisser une bande passante disponible pour gérer des situations d'urgence inattendues avec la fiabilité nécessaire. Ainsi, de concevoir un " mécanisme de contrôle de congestion " qui permet de conserver la charge des messages périodiques sous une valeur maximale spécifique à tous les nœuds du réseau. Ce seuil, appelé Max Beaconing Load (MBL).

(c) **Garder la charge de balisage sous MBL**
Le seuil MBL peut être considéré comme un moyen pour définir le niveau de priorisation entre les messages balisés et événementiels.

(d) **L'équité avec une faible complexité**
Les réseaux de véhicules sont composés de nœuds hautement mobiles. Par conséquent, le mécanisme d'ajustement de puissance ne peut pas être basé sur une stratégie qui converge vers des paramètres de puissance stables sur une période de temps relativement longue. Donc, il doit pouvoir réagir rapidement aux changements d'exigences et d'emplacements des nœuds.

Algorithm 2 Algorithm D-FPAV (Algorithm for node u_i)

Input : Status of all nodes in $CS_{MAX}(i)$

Output : A power setting $P(A)_i$ for node u_i, such that the resulting power assignment in an optimal solution to BMMTxP

(a) Basesd on the Status of the nodes in $CS_{MAX}(i)$, compute the maximum common tx power level P_i s.t. the MBL threshold is not violated at any node in $CS_{MAX}(i)$

(b) i. Broadcast P_i to all nodes in $CS_{MAX}(i)$

ii. Receive the messages with the power level from nodes u_j such that $u_i \in CS_{MAX}(j)$; store the received values in P_j

(c) Compute the final level : $PA(i) = \min\{P_i, \min_{j:u_i \in CS_{MAX}(j)}\{P_j\}\}$

*** Discussion**

L'algorithme D-FPAV contrôle la congestion en diminuant la puissance de transmission des messages de balise. Cependant, la réduction de la plage de transmission de balisage réduit la transmission de ces messages dans des distances plus éloignées et fait face au manque d'informations essentielles pour le fonctionnement efficaces des applications de sécurité dans les VANETs. De plus, l'échange de la puissance d'émission réglée entre les véhicules voisins entraîne une charge supplémentaire dans les canaux et le gaspillage de bande passante causée par une affectation fixe de MBL.

A.4 Solutions basées sur CSMA/CA

1. **Effective Carrier Sensing in CSMA Networks under Cumulative Interference**

   Liqun Fu et Al. [15] ont proposé un mécanisme de détection de porteuse d'énergie IPCS (Incrémental-Power Carrier-Sensing) pour éviter les collisions causées par les nœuds cachés. Ce mécanisme garantit des transmissions sans collision dans les réseaux CSMA et surveille chaque augmentation du niveau de puissance dans le réseau, puis le compare avec le seuil prédéfini. En effet, IPCS présente trois contributions majeures listées comme suit :

(a) **Le concept Safe Carrier-Sensing Range**

Ce concept peut garantir des transmissions sans collision dans les réseaux CSMA sous le modèle d'interférence cumulative. Lorsqu'un nœud récepteur (i) est constitué par la puissance cumulative reçue de tous les autres nœuds, un ensemble de liaisons transmetteurs simultanés est considéré comme étant interférentiel si les SINR (Signal-to-Interference-plus-Noise Ratios) de récepteurs de tous ces liens sont supérieurs au seuil.

(b) **Le concept Incremental-Power Carrier-Sensing**

Les auteurs montrent que ce concept (dit aussi IPCS) est un mécanisme simple qui surveille la puissance. Cette puissance consiste à une somme des pouvoirs reçus de tous les autres émetteurs. Il est impossible de déduire de ce pouvoir absolu la séparation exacte du nœud de chacun des autres émetteurs. Cela entraîne une réutilisation spatiale insuffisante.

Par ailleurs, IPCS est capable de détecter et de séparer les puissances de transmission des véhicules transmis simultanément dans le réseau. Ensuite, en fonction du niveau de puissance d'émission reçue, ce mécanisme détecte l'état du repos des canaux et détermine la plage de détection du support.

*** Discussion**

Le mécanisme IPCS proposé peut garantir des transmissions sûres sans collision et réaliser le concept de gamme de détection de porteur de manière simple. Au lieu de surveiller la puissance. L'IPCS peut stimuler la réutilisation spatiale de débit de réseau de plus de 60 % par rapport au mécanisme de détection de support conventionnel, mais, les bruits d'arrière-plan ne sont pas pris en compte. Ainsi, ce mécanisme est très difficile pour l'application dans les environnements réels.

A.5 Solutions basées sur la priorité et l'ordonnancement

1. **Congestion Control Algorithm for Event- Driven Safety Messages in Vehicular Networks**

   Pour contrôler la congestion dans les VANETs, en fonction de la priorité des messages, Darus et al. [12] ont introduit un algorithme qui se concentre sur la priorité unique des messages événementiels, afin d'assurer une livraison rapide et fiable et d'avoir la possibilité de programmer les nœuds ayant les mêmes paquets de priorité élevée.

   L'algorithme proposé est divisé en deux parties essentielles : La détection et le contrôle de la congestion, en utilisant la méthode basée sur des événements et celle basée sur des mesures (comme nous l'avons définies ci-haut). La retransmission des messages est réalisée en fonction de deux types de diffusion : forward and makeup. Si le nœud source a détecté un message de sécurité piloté par événement, il l'envoi au nœud le plus proche appelé (forward/ makeup). Dans la deuxième phase, le forward/ makeup retransmettra les messages de sécurité événementiels à tous les véhicules dans la gamme de communication recevant leurs messages. Les plages de transmission sont définies à 400 mètres. Les étapes de l'algorithme de contrôle de congestion proposé sont démontrées sous forme d'un organigramme, voir FigureA.1.

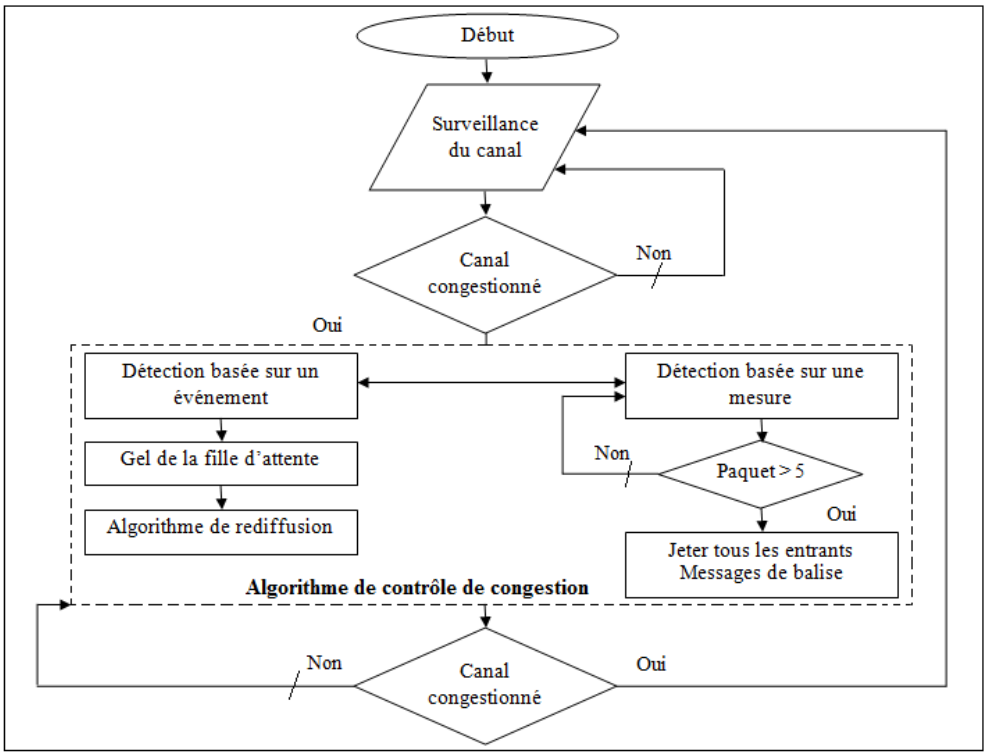

FIGURE A.1 – L'algorithme de contrôle de congestion [12].

*** Discussion**

Le contrôle de congestion proposé est le meilleur en terme de taux de livraison de paquets d'avertissement, avec l'adoption de méthode de retransmission, qui est l'une des meilleures solutions pour la diffusion des messages de sécurité événementiels dans un réseau dense. Cet algorithme réserve une partie de la bande passante pour les messages d'urgence. Cependant, la réservation d'une partie de cette dernière engendre la perdre de la totalité de bande passante dans les conditions normales de VANETs. Cette stratégie ne considère pas le retard qui est un facteur critique pour les messages de sécurité.

2. **Priority-Based Inter-Vehicle Communication for Highway Safety Messaging Using IEEE802.11e**

   C.Suthaputchak. [29] a proposé une stratégie de contrôle de congestion axée sur les priorités, qui utilise les communications entre véhicules pour accroître la

fiabilité de la diffusion des messages de sécurité entre les véhicules. Les messages de priorité supérieure sont retransmis plusieurs fois plus que des messages de priorité inférieure afin d'augmenter la livraison et améliorer leur fiabilité.
Dans cette stratégie, comme le montre la figure A.2, quatre files d'attente internes sont supposées pour chaque véhicule. Chaque message qui arrive au MAC depuis la couche supérieure est mappé dans une priorité. Des exemples de priorités des massages dans la messagerie de la sécurité routière sont présentés dans la Table A.1. Chaque message sera mis en file d'attente en fonction de sa priorité. Il existe un contrôleur de chasse virtuel, qui suit la chute interne. Le gestionnaire de collision virtuelle permettra de transmettre des messages de priorité plus élevée avant les messages de priorité inférieure, avec une politique non préemptive. Pour chaque priorité, il existe différentes valeurs des paramètres suivants : $CWmin[i]$, $CWmax[i]$,$AIFS[i]$ et $TXOP[i]$. Par conséquent, le message de priorité supérieure accède au canal plus rapidement que les messages à priorité inférieure. Une fois que le véhicule gagne le canal, il transmet seulement 1 unité de données de service MAC.

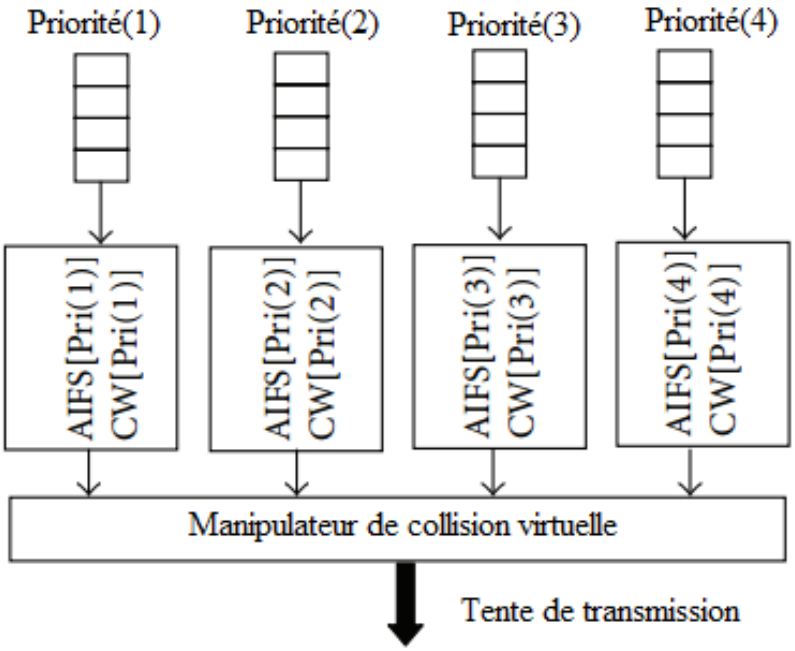

FIGURE A.2 – Files d'attente de chaque véhicule [29].

Priorités	**Types**	**Exemples**
Priorité(1)	Accident	– Capteur airbag – Capteur du corps du véhicule – Capteur thermique
Priorité(2)	Possibilité d'accident	– Saut – État de surface
Priorité(3)	Alerte	– Avertissement de travaux routiers – Traffic de congestion

Priorité(4)	Autre	– Conditions météorologiques

TABLE A.1 – Exemples de priorités des massages dans la messagerie de la sécurité routière [29].

*** Discussion**

La stratégie proposée offre une meilleure performance pour les messages de priorité et améliore le retard et le taux de transmission dans les réseaux à haute densité, pour augmenter la fiabilité de la communication. Cette stratégie applique le mécanisme de retransmission afin de fournir une fiabilité proportionnelle pour chaque message prioritaire. Cependant, le taux d'occupation et la bande passante des messages lors de retransmission ne sont pas prise en compte.

A.6 Solutions hybride

1. **Efficient Congestion Control in VANET for Safety Messaging**
   La vue conceptuelle d'un schéma de contrôle de congestion dans les VANETs utilisant le taux et la puissance de transmission a été proposée par Mughal et al [3]. Les auteurs ont sélectionné deux techniques :
   (a) **Technique de contrôle de la puissance**
   Distribute Fair Power Assignment for Vehicular Networks (D-FPAV) permet de maintenir le pouvoir d'émission. Ainsi, la gamme de transmission des messages de sécurité périodiques (balises) est contrôlée en gardant la charge du réseau au-dessous d'un seuil spécifié appelé MBL (Maximum Beaconing Load), la bande passante restante est implicitement réservée aux messages événementiels. Le D-FPAV est fondé sur un critère d'équité stricte. Selon ce critère, aucun émetteur ne devrait augmenter son pouvoir d'émission s'il affecte la capacité de transmission / réception d'un

autre nœud. La description de l'algorithme est présenté dans les étapes suivantes, voir Algorithme 2.

- **Première étape**
  Chaque nœud u_i calcule le niveau de puissance optimal P_i, qui est basée sur la vue locale de chaque nœud, de telle sorte que P_i ne dépasse pas le seuil MBL.
- **Deuxième étape**
  A l'étape b.i, la puissance calculée P_i est Diffusé à tous les nœuds dans la plage maximale de détection des porteurs $CS_{MAX}(i)$ (Carrier Sense). A l'étape b.ii, le nœud reçoit et stocke la valeur P_i d'autres nœuds dans $CS_{MAX}(i)$.
- **Troisième étape**
  Le nœud u_i définit P_i comme puissance minimale calculée parmi les niveaux de puissance reçus.

(b) **Technique de contrôle du taux de transmission**
Feux de freinage électrique d'urgence avec expédition (Emergency Electric Brake Light with Forwarding : EEBL-F) est une application de sécurité qui utilise le taux de transmission des paquets, afin de maintenir la charge des balises sous un seuil spécifié, en se basant sur une technique de détection de congestion basée sur les mesures. Ces dernières sont calculés selon la formule suivante :
⋇ $Utilisation\ des\ canaux = \frac{\sum(D_{busy}+D_{AIFS}+\overline{D_{Backoff}})}{D_{CCH}} * 100$
La taille de la fenêtre de contention dynamique (CW) est exploitée pour contrôler le taux de transmission du message. Si le niveau d'utilisation du canal dépasse la valeur définie de 95 %, toutes les files d'attente de sortie sont bloquées sauf celles contenant les messages de sécurité événementiels. Dans le cas d'une utilisation de canal de 70 % ou supérieure, la taille de CW est doublée et l'utilisation de 30 % ou moins du canal entraîne une réduction de la taille de CW à la moitié jusqu'à ce qu'elle atteigne une taille de CW minimale prédéfinie.

Sur la base des défis des techniques précédentes, les auteurs proposent une

solution hybride, qui peut utiliser les deux techniques d'une manière dynamique et adaptative. L'approche est illustrée dans la Figure A.3.

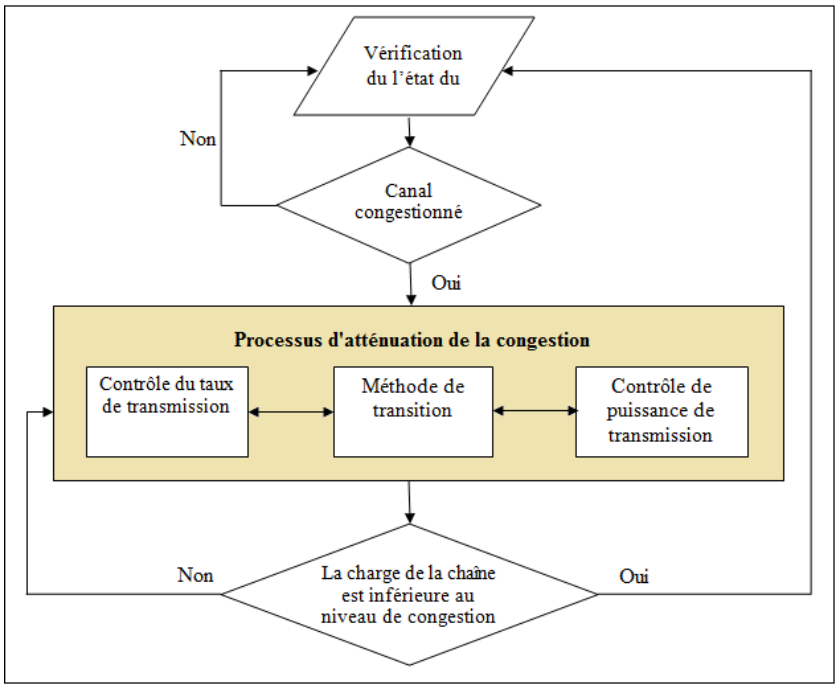

FIGURE A.3 – Schéma de contrôle de congestion sur les flux d'informations [4].

Dans ce schéma, tous les nœuds doivent être informés tout au long de leur état du canal. Chaque fois qu'un canal atteint son niveau de saturation, un nœud peut détecter immédiatement la congestion, alors il déclenche un processus d'atténuation de congestion. Ce dernier décide la technique appropriée à utiliser, soit l'ajustement de la puissance d'émission ou le taux de transmission. Un ensemble complet d'instructions est nécessaire pour exécuter le processus. Une attention particulière est nécessaire pour gérer une transition en douceur entre les deux techniques, car le niveau de puissance croissant / décroissant d'une étape peut avoir un effet différent sur la charge du canal par rapport à l'ajustement du taux de transmission d'un niveau. Cette étape est répétée si nécessaire jusqu'à ce que la charge du canal soit inférieure au niveau de congestion. En attendant, les messages entraînés par l'événement peuvent

être facilement propagés via la bande passante restante avec une pénétration maximale.

*** Discussion**

L'algorithme offre un processus d'atténuation de congestion en fonction de l'ajustement de la puissance de transmission ou du taux. Cependant, il révèle que les techniques de contrôle de la puissance ne satisfont pas les exigences des applications de sécurité dédiés aux balises ; les méthodes utilisées pour mesurer le niveau d'utilisation des canaux dans la technique de contrôle du débit peuvent ne pas être aussi efficaces dans des conditions réelles. Cette stratégie ne considère pas le retard des messages, qui est un facteur critique pour les messages de sécurité.

2. **AVOCA – A Vehicle Oriented Congestion Control Algorithm**

Huang et al. [18] ont proposé un algorithme de contrôle de congestion axée sur les véhicules (AVOCA), qui est un algorithme de contrôle de congestion de couche croisée, utilisant un seuil de performance de la couche transport pour contrôler la transmission de paquets de couche de transport. Puisque la congestion est contrôlée dans le réseau, il considère que les trous de couverture du réseau sont pris en compte. Les autreurs se sont concentrés sur l'optimisation du débit du réseau pour les véhicules de route, tels que les bus de transport public et les trains. Dans un tel environnement, les mécanismes existants de la couche de transport ne permettent pas d'utiliser pleinement la connectivité intermittente lorsque le véhicule entre dans les zones de couverture. Lorsque le seuil de performance de la couche transport est dépassé, indiquant que le véhicule entre dans une zone de couverture sans fil, les paramètres de contrôle de congestion sont rénitialisées et la transmission de paquets est amorcée. Lorsque le véhicule se déplace de la zone de couverture, la performance et le RSS sont inférieurs au seuil ; La transmission de paquets sera terminée et tous les paramètres de contrôle de congestion seront gelés. Dans une configuration partiellement fiable, le paquet final transmis sera un numéro de séquence de transmission avant (TSN) indiquant que tous les paquets en vol doivent être ignorés. Sachant que cette dégradation de la performance résulte du contrôle de congestion orientée réseau et des mécanismes de calcul RTO. Dans le pire des cas, la communica-

tion sera retardée par la valeur spécifiée par RTO.max. Par défaut, RTO.MAX est réglé sur 60 secondes dans TCP et SCTP. L'approche AVOCA supprime la nouvelle forme de blocage de la fenêtre de congestion et améliore le débit, tout en maintenant les politiques d'utilisation équitable d'Internet.

*** Discussion**

L'algorithme AVOCA a été proposé pour répondre au problème de défaillance dans la couche de transport lorsque les véhicules accèdent à une zone de couverture, il gèle le paramètre de contrôle de congestion et bloque les transmissions des paquets. Cet algorithme améliore de manière significative le début jusqu'à 24 % du réseau, en tenant compte de l'équité dans l'allocation du canal. Cependant, la diffusion des messages n'est pas efficace et la priorité d'accès et le délai ne sont pas pris en considération.

A.7 Conclusion

En raison de la limite de nombre de pages, nous avons présenté, dans l'annexe présente, les différentes critiques des protocoles appartenant à la classification basé sur des paramètres et des moyens, pour résoudre le problème de congestion dans les VANETs.

Bibliographie

[1] The network simulator - ns2, disponible sur : http ://www.isi.edu/nsnam/ns/. consulté le : 08-juin-2017.

[2] F. Abdelfatah. Développement d'une bibliothèque de capteur. Mémoire de Master, Informatique Professionnelle et Recherche en Informatique, Université Montpellier2 Science et Technique, Canada, 2008.

[3] H. Hasbullah B. Munir Mughal, A. Ali Wagan. Efficient congestion control in vanet for safety messaging. volume 10, pages 654–659. In International Conference of IEEE on Science and Technology, 2010.

[4] M. Barradi, A. S. Hafid, and J. R. Gallardo. Establishing strict priorities in ieee 802.11p wave vehicular networks. pages 1–6. In International Conference IEEE Global Telecommunications (GLOBECOM 2010), 2010.

[5] MA. Benatia, L. Khoukhi, M. Esseghir, and L. Merghem Boulahia. A markov chain based model for congestion control in vanets. volume 13, pages 1021–1026. In International Conference on Advenced Information Networking and Applications Workshops, 2013.

[6] M.S. Bouassida and M. Shawky. A cooperative congestion control approach within vanets : formal verification and performance evaluation. volume 2010 of *11*, page 13. In EURASIP Journal on Wireless Communications and Networking, 2010.

[7] N. Chaib. *La sécurité des communications dans les réseaux VANETs*. Thèse Magister, Université Elhadj Lakhdar, Batna, 2010.

[8] H. Chehri. *Etude et caractérisation d'un canal de propagation pour les réseaux VANETs*. Mémoire Ingénierie, Université de Quebec, 2014.

[9] FD. Cunha, A. Boukerche, L. Villas, AC. Viana, and AF. Loureiro. Data communication in vanet : a servey, challenges and applications. volume 25, pages 0249–6399. Research Report n° 8498, 2014.

[10] MY. Darous and AB. Kamalrulnizam. Congestion control algorithm for even-driven safety messages in vehiclar networks. volume 03 of *02*, pages 99–106. In Journal of Advenced Computer Science and Technology Research, 2013.

[11] M. Yusof Darus and K. Abu Bakar. A review of congestion control algorithm for event-driven safety messages in vehicular networks. volume 8 of *1*, pages 1694–0814. In Journal of Computer Science Issues, 2011.

[12] M. Yusof Darus and K. Abu Bakar. Congestion control algorithm for eventdriven safety messages in vehicular networks. volume 3 of *2*, pages 99–106. In Journal of Advanced Computer Science and Technology Research, 2013.

[13] M. Yusof Darusa and K. Abu Bakar. Congestion control algorithm in vanets. volume 21 of *7*, pages 1057–1061. In Journal of World Applied Sciences, 2013.

[14] S. Djahel and Y. Ghamri-Doudane. A robust congestion control scheme for fast and reliable dissemination of safety messages in vanets. pages 2264–2269. In International Conference of IEEE Wireless Communications and Networking (WCNC), 2012.

[15] L. Fu, S. Chang Liew, and J. Huang. Effective carrier sensing in csma networks under cumulative interference(3). 2009.

[16] V. Gayraud, L. Nuami, F. Dupont, S. Gombault, and B. Tharon. *La sécurité dans les réseaux sans fil ad hoc*. Thèse de Doctorat, Université Thomsen RI Security Lab, Bretagne, 2003.

[17] K. El Gholami. *La gestion de la qualité de service temps-réel dans les réseaux de capteurs sans fil*. Thèse Doctorat, Université Blaise Pascal - Clermont-Ferrand II, France, 2014.

[18] Y. Huang, E. Fallona, Y. Qiao, M. Rahilly, and B. Lee. Avoca – a vehicle oriented congestion control algorithm. pages 23–24. ISSC, Trinity College Dublin, 2011.

[19] T. Issariyakul and E. Hossain. Introduction to network simulator ns2. *Springer Publishing Company*, 2008.

[20] M. Reza Jabbarpour, R. Md Noor, R. Hafeez Khokhar, and C. Heng Ke. Cross-layer congestion control model for urban vehicular environments. volume 44, pages 1–16. In Journal of Network and Computer Applications, 2014.

[21] S. José, F. Antonio, and S. Artigas Marc. Architecture and evaluation of a unified v2v and v2i communication system based on cellular networks. volume 31 of *12*, pages 2850–2861. In Journal of Computer Communications, 2008.

[22] M. Kaur, S. Kaur, and G. Singh. Vehicular ad hoc network. volume 3, pages 61–64. In Journal of Global Research in Computer Science, 2012.

[23] X. Ma, J. Zhang, and T. Wu. Reliability analysis of one-hop safety-critical broadcast services in vanets. volume 60 of *8*, pages 0018–9545. In Journal of IEEE Transactions On Vehicular Technology, 2011.

[24] Y. Meraihi. *Routage dans les réseaux véhiculaires (VANETs) cas d'un environnement type ville*. Thèse Doctorat, Université M'hamed Bougara, Boumerdès, 2011.

[25] J. Moez. *Protocoles pour les communications dans les réseaux de véhicules en environnement urbain : Routage et GeoCast basés sur les intersections*. Thèse Doctorat, Université Evry-Val d'Essonne, France, 2008.

[26] J. Pierre, H. Srdjan, and C. JunLuo. The security and privacy of smart vehicles. volume 04, pages 1540–7993. In Journal of IEEE Computer Society, 2004.

[27] M. Reza Jabbarpour Sattari, R. Md Noor, and H. Keshavarz. A taxonomy for congestion control algorithms in vehicular ad hoc networks. pages 44–49. In IEEE International Conference on Communication, Networks and Satellite (ComNetSat), 2012.

[28] C. Sommer, O. K. Tonguz, and F. Dressler. Traffic information systems : efficient message dissemination via adaptive beaconing. volume 49, pages 173–179. In Journal of IEEE Communications Magazine, 2011.

[29] C. Suthaputchakun. Priority-based inter-vehicle communication for highway safety messaging using ieee 802.11e. volume 2009 of *423141*, page 12. In Journal of Vehicular Technology, 2009.

[30] T. Tielert, D. Jiang, Q. Chen, L. Delgrossi, and H. Hartenstein. Design methodology and evaluation of rate adaptation based congestion control for vehicle safety communications. pages 116–123. In IEEE Vehicular Networking Conference (VNC), 2011.

[31] Y. Toor, P. Muhlethaler, and A Laouiti. Vehicle ad hoc networks : applications and related technical issues. volume 10 of *3*, pages 74,88, University of Calgary, 2008. In Journal of IEEE Communications Surveys.

[32] M. Torrent-Moreno, P. Santi, and H. Hartenstein. Distributed fair transmit power adjustment for vehicular ad hoc networks(2). 2007.

[33] J. Toutouh, S. Nesmachnow, and E. Alba. Fast energy-aware olsr routing in vanets by means of a parallel evolutionary algorithm. volume 16, pages 435–450. In Springer Science+Business Media, 20.

[34] J. Widmer, R. Denda, and M. Mauve. A survey on tcp-friendly congestion control. volume 01, pages 0890–8044. In Journal of IEEE Network, 2001.

[35] L. Wischhof and H. Rohling. Congestion control in vehicular ad hoc networks. pages 58–63. In IEEE International Conference on Vehicular Electronics and Safety, 2005.

[36] F. Ye, R. Yim, S. Roy, and J. Zhang. Efficiency and reliability of one-hopbroadcasting in vehicular ad hoc networks. volume 29, pages 151–160. In IEEE Journal on Selected Areas in Communication, 2011.

[37] F. Ye, R. Yim, J. Zhang, and S. Roy. Congestion control to achieve optimal broadcast efficiency in vanets. In IEEE xplor on Communication ICC, 2010.

[38] Y. Zang, L. Stibor, X. Cheng, HJ. Reumerman, A. Paruzel, and A. Barroso. Congestion control in wireless networks for vehicular safety applications. page 7, Paris, France, 2007. In International Conference in The 8th European Wireless.

RÉSUMÉ

Les réseaux Ad-Hoc Véhiculaires ont pour objectif l'amélioration de la sécurité et l'efficacité des transports routiers afin de diminuer les accidents et fournir un environnement confortable aux conducteurs et à leurs passagers. Mais, ces réseaux souffrent parfois du problème de congestion.

Dans ce travail, nous avons proposé un nouvel algorithme de contrôle de congestion, basé sur l'affectation des priorités, le calcul du temps d'occupation, la réduction du débit de transmission et la surveillance du canal de contrôle (CCH).

La simulation sous le simulateur NS-2 nous a permis d'obtenir des résultats importants en terme des trois critères de performance, à savoir, l'évolution de taux de transmission, la perte des paquets ainsi que le délai.

Mots clés : VANET, contrôle de congestion, message événementiel, message balise (périodique), sécurité routière, communication V2V.

ABSTRACT

Ad-Hoc Vehicles networks aim to improve the safety and efficiency of road transport in order to reduce accidents and provide a comfortable environment for drivers and their passengers. But, these networks sometimes suffer from the problem of congestion. In this work, we proposed a new congestion control algorithm based on priority assignment, occupancy time calculation, transmission rate reduction, and monitoring of the control channel (CCH). The simulation under the NS-2 simulator allowed us to obtain important results in terms of the three performance criteria, namely, transmission rate evolution, packet loss and delay.

Key words : VANET, Congestion control, Event message, beacon message, road safety, communication v2v.