République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Abderahmane Mira de Béjaïa
Faculté des Sciences et Exactes
Département de Recherche Opérationnel

Mémoire de fin d'études

En Recherche Opérationnel

Option

Modélisatin Mathématique et Evaluation des Performances des Réseaux

Thème

Techniques de contrôle de congestion dans les réseaux véhiculaires

Présenté par

Melle BAAZIZ Thiziri
Melle MAOUCHE Rima

Soutenu le 03/07/2018, devant le jury composé de :

Présidente	**Mme BELKHIRI Ouiza**	**M.A.A.**	**Univ. de Béjaia**
Rapporteur	**Mme BOULFEKHAR Samra**	**M.C.A.**	**Univ. de Béjaia**
Examinatrice	**Mme ZIDANI Ferroudja**	**M.A.A.**	**Univ. de Béjaia**
Examinatrice	**Mlle LAKAOUR Lamia**	**Doctorante**	**Univ. de Béjaia**

Promotion 2017 – 2018

TABLE DES MATIÈRES

TABLE DES FIGURES

LISTE DES TABLEAUX

Liste des abréviations

ACK : acknowledgement

AIFS : Arbitration InterFrame Space

ATB :Adaptive Traffic Beacon

BSM : Basic security messages

CCH : Control Channel

CMDI : Channel Monitoring and Decision Interval

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

NS-2 : Network Simulator version 2

OSI : Open System Interconnexion

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

Les réseaux Véhiculaires ad hoc (VANETs) ne sont qu′une application des réseaux Ad Hoc mobiles(MANET). Ils constituent le noyau d′un Système de Transport Intelligent(STI) ayant comme objectif principal l′amélioration de la sécurité routière. En effet, 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. Les réseaux VANETs sont conçus pour permettre des communications sans fil fiables entre les noeuds mobiles à haute vitesse. Afin d′améliorer la performance des applications dans ce type de réseaux et garantir un environnement sûr et confortable pour ses utilisateurs, la Qualité de Service (QoS) doit être supportée dans ces réseaux. Le délai ainsi que les pertes de paquets sont deux principaux indicateurs de QoS qui augmentent de manière significative en raison de la congestion dans les réseaux. En effet, la congestion du réseau entraîne une saturation des canaux ainsi qu′une augmentation des collisions de paquets dans les canaux. Par conséquent, elle doit être contrôlée pour réduire les pertes de paquets ainsi que le délai, et améliorer les performances des réseaux véhiculaires. Le contrôle de congestion dans les réseaux VANETs est une tâche difficile en raison des caractéristiques spécifiques des VANETs, telles que la grande mobilité des nœuds à haute vitesse, le taux élevé de changement de topologie, etc. Le contrôle de congestion dans les réseaux VANets peut être effectué en ayant recours à une stratégie qui utilise l′un des paramètres suivants : le taux de transmission, la puissance de transmission, la priorisation et l′ordonnancement, ainsi que les stratégies hybrides. Les stratégies de contrôle de congestion dans les réseaux VANETs doivent faire face à quelques défis tels que l′utilisation inéquitable des ressources, la surcharge de communication, le délai de transmission élevé, et l′utilisation inefficace de la bande passante, etc. Par conséquent, il est nécessaire de développer des nouvelles approches pour faire face à ces défis et améliorer les performances des réseaux VANETs.

Notre travail consiste à révéler les points forts et faibles de certains protocole de contrôle de congestion dans VANETs, tout en les évaluant selon quelques critères de la qualité de service(fiabilité,bande passante,taux de perte,délai de transmission,gigue), 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 protocole de contrôle de congestion fondé sur l′affectation des priorité aux messages diffusés selon leurs utilités. Il vise à adapter le taux de transmission et la puissance d′émission afin de fournir une meilleur qualité de service et améliorer la sécurité routière. Notre mémoire s′étale sur trois chapitres :

Dans le premier chapitre, nous avons introduit les réseaux VANETs en donnant les définitions, les caractéristiques, les techniques de communication et tout ce qui relève de ce domaine.

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. Dans le deuxième chapitre, nous présentons quelques solutions ou bien quelques stratégies pour le contrôle de la congestion dans les VANETs.

Dans le dernier chapitre nous avons présenté un protocole de contrôle de congestion, ainsi nous avons dégagé les diagrammes appropriés à ce protole.

En fin de ce mémoire, une conclusion générale est donnée, résumant les apports essentiels de notre travail.

CHAPITRE 1

GÉNÉRALITÉS SUR LES RÉSEAUX VANETS

1.1 Introduction

Les réseaux sans fil véhiculaires sont considérés comme un élément clé des futurs systèmes de transport intelligents " Intelligent Transportation Systems (ITS) ". Ils représentent une technologie prometteuse, qui une fois mise en oeuvre, offrira la possibilité de déployer une large variété d'applications. Certaines de ces applications visent á améliorer la sécurité routiére. D′autre visent á rendre les déplacements des usagers de la route plus confortables. Dans ce chapitre,nous avons définit les réseaux VANETs,puis on a présenté leurs caractéristiques, leurs composantes, leurs applications, ainsi que les défits que rencontrent les réseaux VANETs.

1.2 Définition d′un réseau véhiculaire

Un réseau véhiculaire sans fil (VANET : Vehicular Ad hoc NETworks) est un réseau de communication entre véhicules intelligents équipés de calculateurs, de périphériques réseaux et de différents types de capteurs.

Les VANET font parti de la famille des réseaux mobiles MANETs [1] . Dans un réseau VANET, les noeuds sont les véhicules intelligents appartenant au réseau. Par rapport á un réseau ad hoc classique, les VANETs sont caractérisés par une forte mobilité des noeuds rendant la topologie du réseau fortement dynamique[1].

1. MANETs : Mobile Ad hoc NETworks ; est un système autonome composé des noeuds mobiles dynamiques interconnectés par des liens sans fil et sans infrastructure.

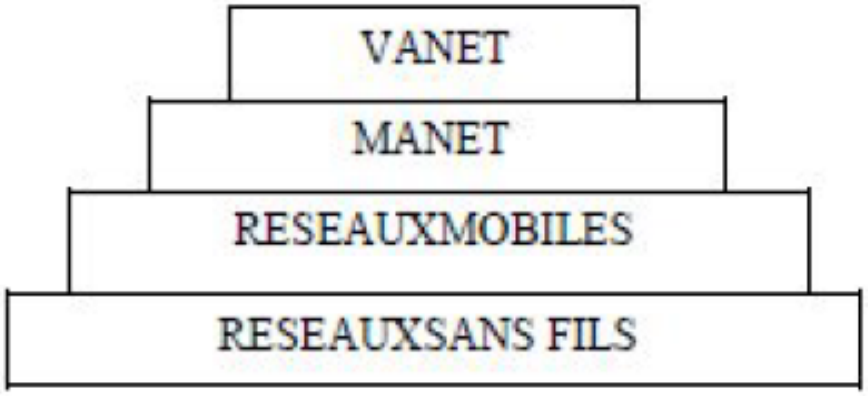

FIGURE 1.1 – Hiérarchie des réseaux sans fil[1]

1.3 Composants d'un réseau véhiculaire

Un réseau VANET est constitué de trois entites[2] :

1.3.1 Autorité de Confiance (CA)

Autorité de Confiance (CA) , c'est une source d'authenticité de l'information . Elle assure la gestion et l'enregistrement de toutes les entités sur le réseau RSU et OBU .La CA doit connaitre toutes les vraies identités des véhicules. Dans certains travaux la CA se charge de la délivrance et l'attribution des certificats et des pseudonymes de communication [2].

1.3.2 Road Side Unit (RSU)

Ce sont les subordonnées des CA .Elles sont installées au bord de la route. Elles peuvent être : des feux de signalisation, des lampadaires ou autre. Leurs principale responsabilité est de soutenir la TA dans la gestion du trafic et des véhicules. Elles représentent des points d'accès au réseau et aux différentes informations sur la circulation [2].

1.3.3 On-Board Unit (OBU)

Ce sont des unités embarquées dans les véhicules intelligents, elles regroupent un ensemble de composants matériels et logiciels de hautes technologies (GPS, radar, caméras, différents capteurs et autres).Elles assurent la localisation, la réception, le calcul, le stockage et l'envoi des données

sur le réseau. Ce sont des émetteurs-récepteurs qui assurent la connexion du véhicule au réseau [2].

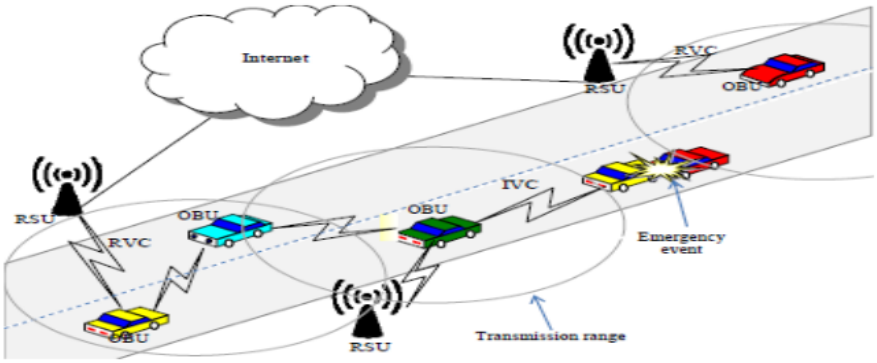

FIGURE 1.2 – Composants d'un réseau véhiculaire[2]

1.4 Architectures des réseaux véhiculaires

Dans les réseaux VANET, on trouve principalement, les entités fixes qui constituent l'infrastructure (RSU et CA) et les entités mobiles (les véhicules). Pour pouvoir échanger les informations liées á la sécurité et au confort des usagers de la route. Ces différentes entités doivent établir des communications entre elles ; pour cela , on distingue trois modes de communication :véhicule á véhicule (V2V), véhicule à infrastructure (V2I), communication hybride[3].

1.4.1 Communication de véhicule á véhicule (V2V)

L'architecture (V2V), comprend uniquement des communications opportunistes entre les véhicules. Quand un véhicule rencontre d'autres véhicules á proximité (i.e.des nœuds voisins), les utilisateurs peuvent alors communiquer et échanger des contenus pendant les durées de contacts V2V La communication V2V n'est pas coûteuse et offre un débit de transmission important. En revanche, cette communication pose des défis tels que les faibles fréquences de contactsentre les véhicules dans un milieu à faible densité, les faibles durées de contacts en raison de la vitesse et de la qualité du lien, et la sélection des nœuds relais[3].

1.4.2 Communication de véhicule à infrastructure (V2I)

L'architecture (V2I), fonctionne sous l'hypothése que les utilisateurs doivent continuellement accéder á un serveur centralisé qui gère leurs interactions avec d'autres utilisateurs, même lorsque

les véhicules sont physiquement proches. Dans une telle architecture, il n′y a pas d′interaction directe entre les véhicules. Dans la littérature, cette communicationest connue sous le nom de véhicule−à−infrastructure (V2I) . Les véhicules communiquent indirectementpar l′intermédiaire des infrastructures existantes telles que les *RSU*s et les réseaux cellulaires. Jusqu′a ce jour, les RSUs sont peu déployés en raison de leur coût élevé. De plus les réseaux cellulaires sont surchargés avec l′augmentation de la demande et ne couvrent pas toutes les zones (e.g. tunnels ou zones rurales)[3].

1.4.3 Communication hybride

L′architecture hybride, comprend á la fois des communications V2V et des communications V2I . L′infrastructure peut être utilisée d′une manière optionnelle ou quand elle est présente. Dans les zones où l′infrastructure est inexistante, cette architecture opte pour des communications directes entre les véhicules[4].

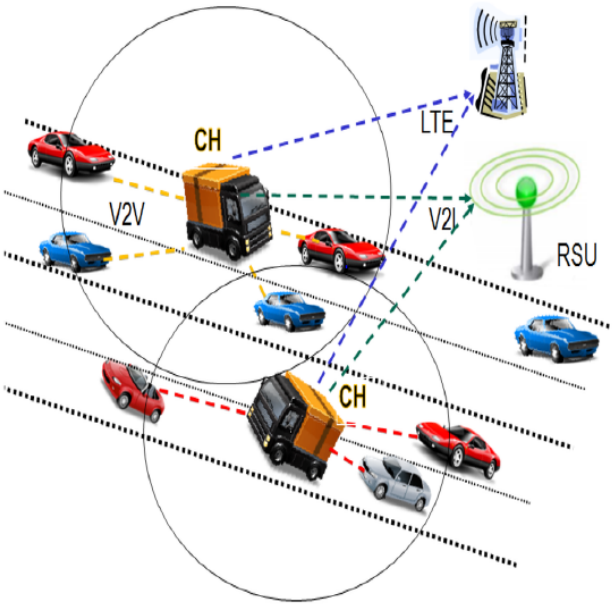

FIGURE 1.3 – Architecture de communication Hybride dans un réseau VANET[4]

1.5 Caractéristiques des réseaux véhiculaires

En plus des caractéristiques des réseaux ad hoc mobiles classiques, les VANETs ont la particularité d′avoir une très grande mobilité (les noeuds mobiles circulent à très grande vitesse). La topologie dynamique provoque de nombreuses reconfigurations (mise à jour des tables de

routage,*etc*) , et soulève par conséquent des problèmes de performances. Après cet apercu, nous détaillons, dans cette section, les caractéristiques des VANETs[3].

1.5.1 Potentiel énergétique

La différence des réseaux sans fil traditionnel soù la contrainte d′énergie représente un facteur limitant important, les entités des VANET disposent de capacités énergétiques suffisantes qu′elles tirent du système d′alimentation des véhicules. Même en cas d′arrét du moteur et donc d′arrêt du système d′alimentation, il est possible pour une plateforme embarquée de recourir au dispositif de batteries dont seul un véhicule peut disposer. Les plateformes embarquées dans les véhicules étant pleinement alimentés, elles peuvent bénéficier de capacités de calcul plus massives et de multiples interfaces de communication[3].

1.5.2 Environnement de communication et le modéle de mobilité

Les réseaux véhiculaires imposent la prise en compte d′une plus grande diversité environnementale. Du fait de la mobilité des véhicules, il est en effet possible de passer d′un environnement urbain caractérisé par de nombreux obstacles à la propagation des signaux, à un environnement périurbain ou autoroutier présentant des caractéristiques différentes. En plus de cette diversité environnementale, les réseaux véhiculaires se distinguent également des réseaux sans fils ordinaires par un modèle de mobilité dont une des traductions les plus évidentes est l′importante vitesse des nœuds qui réduit considérablement lesdurées de temps pendant les quelles les nœuds peuvent communiquer[3].

1.5.3 Modèle de communication

L′une des applications clés des VANET sétant la prévention et la sécurité routiére. Les types de communication s′axent sur diffusion de message d′une source vers plusieurs distinataires.Bien entendu ,les véhicules peuvent aussi, communiquer point à point. Dans le cas de diffusion , les véhicules sont plus ou moins concernés en fonction de leurs positions géographiques et leurs degrés d′implication dans lévenement routier. Par exemple, un véhicule sur une route parallèle à une autoroute ne sera pas concerné par l′information d′un accident sur l′autoroute. Nous retrouvons ainsi deux modèles de communication dominants: la diffusion totale et la diffusion multipoints vers une zone géographique définie(geocast,unicast). L′avantage de la diffusion est qu′avec un taux de

pénétration faible, un message peut atteindre six kilométres (avec un rayon de communication de milles métres)[3].

1.5.4 La taille du réseau

Étant donné les avancées importantes réalisées dans le domaine des communications sans fil et les bas coûts des équipements associés, les véhicules qui intègrent déjà massivement des systèmes GPS et des équipements Bluetooth, seront très probablement équipés et ce, tout aussi massivement, de plateformes de communication leur permettant de constituer de véritables réseaux. Ce faisant, et compte tenu de l'importance sans cesse grandissante de la densité et du parc des véhicules, on peut s'attendre à ce que la taille des réseaux véhiculaires dont les déploiements restent encore très confidentiels, soit d'une tout autre ampleur. L'importance potentielle de la taille des réseaux véhiculaires constitue donc une caractéristique majeure à prendre en compte dans la conception de ces réseaux[3].

1.5.5 Topologie du réseau et connectivité

Un véhicule peut rapidement rejoindre ou quitter le réseau en un temps très court, ce qui rend les changements de topologie trés fréquents, de plus, des problèmes telles que le partitionnement du réseau fréquent apparaitre, essentiellement quand le systéme $DSRC$(Dedicated Short Range Communications) n'est pas largement répondu et équipé dans la majorité des véhicules. Une seconde raison de partitionnement du réseau inter véhiculaire est que la probabilité de formation d'une chaine ininterrompu de véhicule à portée radio décroit exponentiellement. Les solutions (proposées doivent alors prendre en considération cette contrainte spatiotemporelle où la connectivité est un des paramètresclés, avec un diamètre de réseau limité. L'hétérogéneité des nœuds en termes de vitesse (les bus ont par exemple une vitesse régulière est inférieure aux véhicules particuliers) offre des information supplémentaires à prendre en compte dans l'élaboration des solutions et des architectures pour les réseaux de véhicules. Par ailleurs, les propriétés inhérentes aux VANET, notamment en termes de taille, ouvrent des problématiques de passage à l'échelle[5].

1.6 Applications des réseaux VANETs

Les principales applications des réseaux VANET peuvent être classées en trois catégories [6]

1.6.1 Applications de gestion du trafic routier

Les applications de gestion de trafic sont axées sur l'amélioration des conditions de circulation dans le but de réduire les embouteillages et les risques d'accidents. Elles fournissent aux conducteurs un support technique leur permettant d'adapter leur parcours à la situation du trafic routier. Ces applications visent à équilibrer la circulation des véhicules sur les routes pour une utilisation efficace de la capacité des routes et des carrefours et à réduire par conséquent les pertes humaines, la durée des voyages et la consommation d'énergie[6].

1.6.2 Applications de confort

Cette catégorie comporte toutes les applications qui participent au confort du conducteur et qui ne relèvent pas de la gestion du trafic ni de la sécurité routiére.Ces applications se présentent, donc, en tant que services fournis au conducteur. Parmi ces applications, citons les panneaux d'annonces locales : d'ordre commercial comme les offres des restaurants, la présence des stations service à proximité, ou culturel comme des informations touristiques relatives à la localisation du véhicule. Il y a aussi des services télématiques comme le péage à distance sur les autoroutes, le paiement automatique dans les stations-service. La vie des usagers pourra aussi être facilitée par le contrôle à distance de véhicule de manière électronique (vérification du permis de conduire, contrôletechnique, plaque d'immatriculation) pour les services compétents (police, douane, gendarmerie)[6].

1.6.3 Applications de sécurité du trafic routier

Ils visent à améliorer la sécurité des passagers sur les routes en avisant les véhicules de toute situation dangereuse. Ces applications se basant en général sur une diffusion, périodique ou non, de messages informatifs permettant aux conducteurs d'avoir une connaissance de l'état de la route et des véhicules voisins. Des exemples répandus de services dans cette catégorie d'application sont, l'avertissement des collisions, les avertissements sur les conditions de la route, l'assistance dépassement et changement de voie, etc[7].

1.7 Défis liés aux réseaux VANETs

Les réseaux VANETs rencontrent plusieurs défis, dont on peut citer :

1.7.1 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 dite aussi Quality of Service (QoS), est définie par un ensemble de besoins 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 de transmission, 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[8].

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

- **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 á recevoir les messages diffusés, dans la durée d′opération spécifiée[9] .
- **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′accés au médium (MAC)[31].
- **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.
- **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.
- **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[8].

– **Congestion** On peut définir la congestion comme étant une situation où les usagers des transports ne peuvent pas se déplacer comme ils y sont habitués. C'est un phénomène généralisé lorsque la capacité d'une infrastructure est saturée.

1.7.1.1 Routage et dissémination

Les véhicules doivent définir un protocole de routage pour pouvoir communiquer entre eux. En effet, quand les terminaux ne sont pas á une portée de transmission radio directe, le routage unicast est exigé pour établir la communication entre deux véhicules ou entre un véhicule et une infrastructure fixe. Chaque véhicule peut donc prendre le rôle d'un émetteur, récepteur ou routeur. La dissémination d'information quant à elle, consiste à acheminer une information d'une source vers une ou plusieurs destinations, en assurant un délai d'acheminement réduit, une grande fiabilité et une meilleure utilisation des ressources[12].

1.7.1.2 Sécurité

La sécurité dans les réseaux véhiculaires ad hoc est cruciale, car elle affecte la vie des gens. Il est essentiel, par exemple, que l'information vitale ne puisse pas être modifiés ou supprimés par un attaquant. Les communications passant par un véhicule du réseau ainsi que des informations sur les véhicules et leurs conducteurs doivent être garantis et protégés de façon à assurer le bon fonctionnement des systèmes de transport intelligents[6].

1.8 Normes et standardisations dans les réseaux VANETs

L'utilisation des normes et des standards permet de simplifier le développement des produits, réduire les couts, et permet aux utilisateurs de comparer les produits de concurrence. On trouve une multitude de normes qui se rapporte à l'accès sans fil dans les environnements véhiculaires. Ces normes sétendent des protocoles qui s'appliquent é léquipement de transmission et protocoles de transmission en passant par les spécifications de sécurité, l'acheminement des paquets, et les protocoles d'interopérabilité[14] [8] .

1.8.1 Dedicated Short Range Communications (DSRC)

Les standards des réseaux VANETs sont définis, comme suite : 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 è la sécurité routière. Les six autres canaux sont, quant à eux, dédiés á 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).

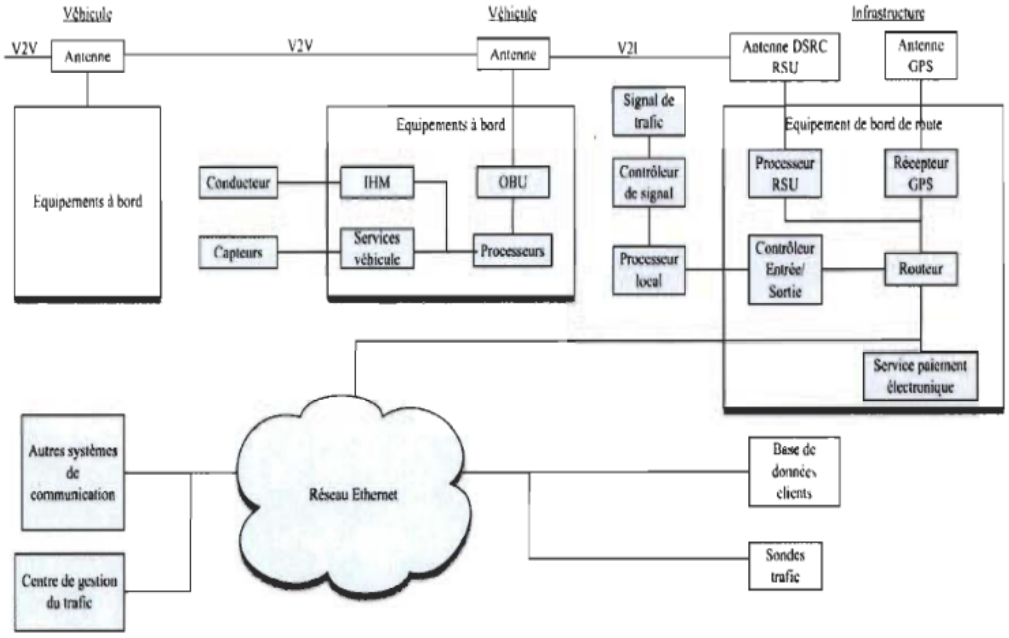

FIGURE 1.4 – Exemple d′architecture d′ un réseau DSRC[8]

1.8.2 La norme IEEE 802.11p

En 2003, le groupe de travail de l′ IEEE a repris ces travaux pour définir un nouveau standard dÂ´edié 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.[26]

1.8.3 Wireless Access in Vehicular Environnements (WAVE)

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).

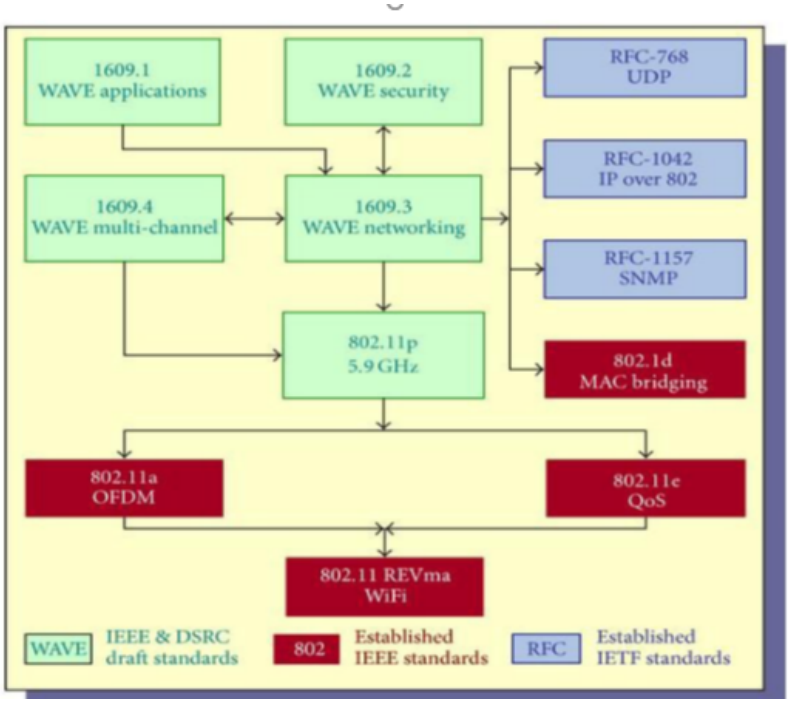

FIGURE 1.5 – La repartition des canaux [14]

1.9 Conclusion

Dans ce chapitre, nous avons présenté les réseaux véhiculaires VANETs qui ne sont qu'une particularité des réseaux MANETs. Nous avons signalé également leurs composantes, leurs caractéristiques, leurs différentes applications, leurs modes de communication,ainsi que les défis liés à ce type de réseaux à savoire :routage et dissémination,sécurité,qualité de service(fiabilité,la bande passante, taux de perte, congestion). Cette derniéres est l'objet du deuxiéme chapitre.

CHAPITRE 2

TECHNIQUES DE CONTRÔLE DE CONGESTION

2.1 Introduction

Afin de garantir la fiabilité et la sécurité des communications véhiculaires et d′améliorer les performances des réseaux VANETs, la qualité de service (QoS) doit être prise en charge. Le contrôle de la congestion est un moyen efficace qui devrait être utilisé pour setenir la QoS ; en contrôlant la congestion, le retard et la perte des paquets vont être diminués et par conséquent les performances des VANETs seront améliorés, ce qui permet d'avoir un environnement plus sûr et plus fiable pour les utilisateurs de VANETs.

Ce chapitre sera consacré pour le contrôle de congestion à savoir sa définition, les différentes méthodes de détection de congestion ainsi que les mécanismes de contrôle de congestion, puis nous allons conclure par un tableau récapitulatif qui fait une comparaison entre les protocoles étudiés.

2.2 Contrôle de congestion

1. La congestion se produit dans les canaux lorsque ces derniérs sont saturés par les noeuds en concurrence pour acquérir ces canaux. En effet, en augmentant la densité du véhicule, le nombre de collisions des canaux augmente l'occurrence de congestion dans le réseau. L'apparition de la congestion augmente le retard et la perte des paquets (en particulier pour les messages de sécurité), ce qui réduit les performances des VANETs. En langage courant, la congestion est l′incapacité d′atteindre une destination dans un temps satisfaisant à cause des vitesses relatives ou imprévisibles de la circulation. C′est un cas où la demande dépasse

l′offre.

2. La congestion du réseau se traduit généralement par des dépassements du tampon du routeur, lorsque les nœuds envoient plus de paquets que le réseau ne peut en gérer ; la congestion s′explique par le fait que la capacité du canal est inférieure á la charge du réseau.

   Divers algorithmes empêchent la congestion du trafic en établissant des contrôles sur les systémes d′envoi de messages. 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 entrainent une augmentation de retard ou de perte des paquets, les stratégies de contrôle de congestion TCP ne sont pas efficaces. Dans les VANETs, les messages événementiels (arrêt d′urgence d′un véhicule, collision, etc.) doivent être envoyés avec un dèlai 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 maniére périodique, le canal de communication sera facilement congestionné. Pour assurer une livraison rapide et fiable des messages de sécurité, il est trés important de garder le canal de contrôle (CCH) libre[15, 16].

   La Figure 2.1 montre une vue schématique d′une architecture de contrôle de congestion de plusieurs couches dans les réseaux VANETs. Telle qu′une entité de gestion est considéré pour détecter et contrôler la congestion.

– **La partie détection** : utilise des informations venant de la couche application pour détecter la congestion dans le réseau. Ainsi, la congestion peut étre détectée en écouttant le canal dans la couche physique ; en mesurant certains paramétres, comme le niveau d′utilisation du canal.
– **La partie contrôle** : peut être effectuée de différentes maniéres dans différentes couches du réseau :
– La couche application : peut contribuer au contrôle de congestion, en ajustant les taux de génération de messages de différentes applications et en réduisant les charges du trafic et la congestion dans les réseaux.
– La couche réseau : peut collaborer par des algorithmes de routage intelligents qui rediffusent efficacement les messages.
– La couche MAC : utilise la hiérarchisation et l′ordonnancement des messages pour contrôler la congestion dans les VANETs.

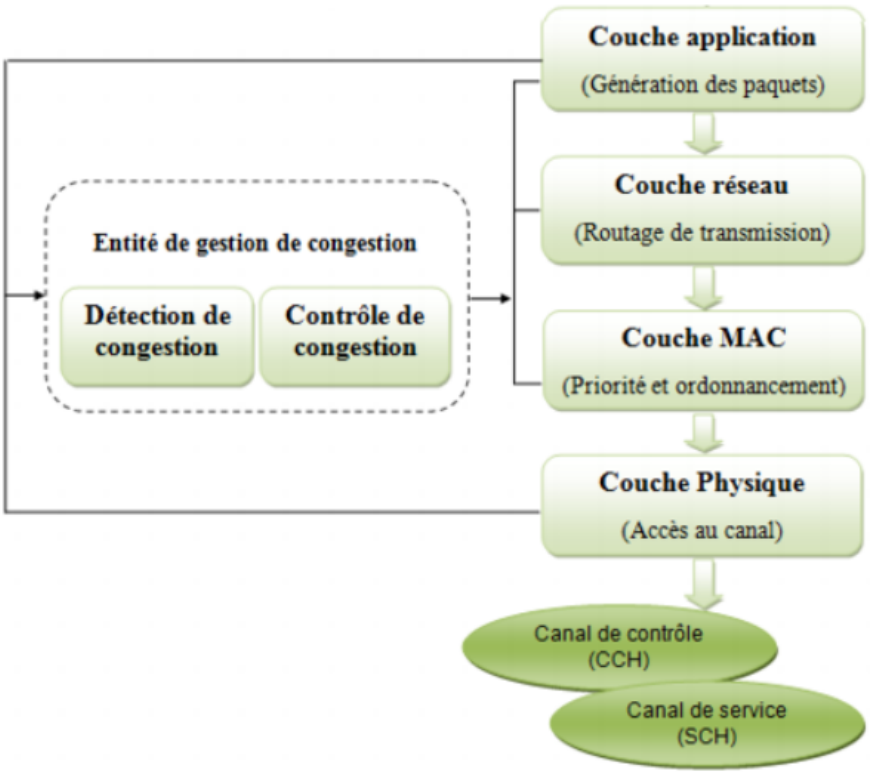

FIGURE 2.1 – Architecture de contrôle de congestion dans les VANETs[18].

2.3 Méthodes de détection de la congestion dans les VANETs :

La détection de congestion dans les réseaux VANETs peut se réaliser en utilisant deux méthodes à savoir : la détection basée sur des événements (event-driven detection), la détection basée sur des mesures (measerement-based detection).

2.3.1 Méthodes basées sur des événements

La méthode de détection basée sur des événements surveille les applications de sécurité et décide de lancer un algorithme de contrôle de congestion quand un message de sécurité d'une priorité élevé est détecté. 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. Par exemple, quand un noeud détecte un message de sécurité de type EEBL-F (Emergency Electronic Brake

Light with Forwarding) généré soit par sa couche application ou reçu d′un autre noeud, il lance immédiatement le contrôle de congestion pour garantir la qualité de service des applications de sécurité[18][19].

2.3.2 Méthodes basées sur des mesures

Les méthodes de détection basées sur des mesures, détectent la congestion en surveillant périodiquement le niveau d′utilisation du canal, en mesurant certains param‘etres à savoir : le nombre des messages dans les files d′attente et le temps d′occupation des canaux. On compare les valeurs de ses paramétres avec des seuils prédéfinis pour pouvoir décider l′occurrence de la congestion dans le réseau. Les seuils prédéfinis ont un impact significatif sur les performances du réseau pour contrôler les canaux de communication et détecter la congestion. Par exemple, si la taille de la file SCHs (Service Channels) dépasse un certain Seuil, on considére qu′il y ′a une congestion dans le réseau. Ainsi, le noeud détecté contrôle la congestion par la réduction du débit de transmission. D′autre part, chaque noeud mesure localement le temps d′occupation du canal de son CCH (Control Channel) ; si ce temps dépasse le seuil, ce noeud bloque la transmission des messages beacon (les messages périodiques) pour contrôler la congestion. Aussi on peut détecter la congestion quand le niveau d′utilisation du canal dépasse un seuil prédéfini estimé en se basant sur le processus de transmission de paquets dans la couche MAC du standard WAVE[18].

2.4 Mécanismes de contrôle de la congestion

Les mécanismes de contrôle de congestion peuvent améliorer les performances des réseaux VANETs et fournir des communications plus fiables en contrôlant les charges des canaux. La congestion doit être contrôlée dans les réseaux pour atteindre une utilisation efficace de la bande passante. La congestion doit également être contrôlée pour réduire la perte des paquets et améliorer l′équité et la compatibilité des réseaux avec divers protocoles et normes. Les mécanismes de contrôle de la congestion dans les VANETs sont classées soit par stratégies (proactives, réactives, hybrides), soit par les paramétres et les moyens par lesquels la congestion est contrôlée, d′où on distingue deux types de classification cités ci-dessous :

2.4.1 Classification selon les stratégies

Les stratégies de contrôle de la congestion dans les réseaux VANETs peuvent être classées en fonction de divers critéres, en fonction de la maniére dont les stratégies décident de prévenir ou de contrôler la congestion, les stratégies de contrôle de congestion dans les réseaux VANETs peuvent être classées en trois classes, y compris les stratégies proactives, réactives et hybrides[18] [21][24].

2.4.1.1 Stratégies proactives

Ces stratégies basées sur certaines informations telles que le nombre de véhicules voisins et les modéles de génération de données, les paramétres de transmission sont réglés de telle sorte que l′occurrence de la congestion sera empêchée. En d′autres termes, les stratégies proactives peuvent être considérées comme des solutions de contrôle de congestion en boucle ouverte qui ajustent les paramétres de transmission avant que les canaux ne soient congestinés. Les stratégies proactives estiment la charge du canal en utilisant un modéle de systéme. Ensuite, pour fournir les performances souhaitées pour le niveau d′application, le mécanisme d′optimisation est utilisé pour obtenir les valeurs correctes pour les paramétres de transmission afin d′éviter l′occurrence de congestion dans les canaux. Les stratégies proactives sont efficaces pour le contrôle de la congestion dans les environnements véhiculaires car ces environnements sont ceux où les messages de sécurité sont principalement envoyés aux canaux de communication radio qui sont menacés par la congestion. Les stratégies proactives réduisent les charges des canaux pour éviter la congestion des canaux en ajustant les paramétres de transmission[18][21].

2.4.1.2 Stratégies réactives

Ces stratégies utilisent l′information des conditions de collision des canaux pour décider la maniére dont elles doivent effectuer le contrôle de congestion en ajustant les paramétres de transmission. En effet, les stratégies réactives peuvent être considérées comme des solutions de contrôle de congestion en boucle fermée qui contrôlent la congestion aprés son apparition dans les réseaux.Par conséquent, ces stratégies mesurent certains paramétres du canal (le niveau d'utilisation du canal, le nombre de messages dans les files d'attente et temps d'occupation du canal), et comparent les valeures de ces paramétres avec un seuil prédéfini pour détecter l'apparition de la congestion dans les réseaux. Si l'occurrence de congestion est détectée dans les canaux, les paramétres de transmission sont réglés pour diminuer la charge des canaux et contrôler la congestion. Ainsi, les stratégies réactives réduisent la charge des canaux en obtenant localement le retour des réseaux

véhiculaires. Ces stratégies contrôlent les charges des canaux aprés la détection de l'occurrence de congestion, il est nécessaire de récupérer le réseau à partir de cette situation critique. Cependant, la reprise du réseau conduit à diminuer les performances des applications de sécurité dans ces situations critiques[18][21].

2.4.1.3 Stratègies hybrides

Ces stratégies combinent les avantages des stratégies proactives et réactives.A titre d'exemple, ces stratégies ajustent la puissance de transmission de manière proactive dans le but de réduire les charges des canaux afin d'éviter la congestion,et ajustent le taux de transmission de manière réactive,aprés avoir mesurer les paramétres du canal, à savoir le nombre des messages dans la file d'attente et le temps d'occupation du canal,en comparant ces mesures avec des seuils prédéfinis,on peut détecter la congestion puis la réduire [18][21].

2.4.2 Classification selon les paramétres et les moyens

En se basant sur les paramètres et les moyens pour contrôler la congestion dans les réseaux VANETs,les stratégies de contrôle de congestion peuvent être classées en cinq classes : stratégies basées sur le taux de transmission, stratégies basées sur la puissance d′émission, Les stratégies basées sur CSMA / CA, et celles basées sur la hiérarchisation et l′ordonnancement, et les stratégies hybrides. Les stratégies basées sur le taux de transmission ajustent le débit de transmission en fonction de la condition du canal pour contrôler la congestion. Les stratégies basées sur la puissance d′émission ajustent dynamiquement la puissance de transmission (portés) pour contrôler la charge des canaux. Les stratégies CSMA / CA contrôlent la congestion en déterminant les valeurs appropriées pour la taille de la fenêtre de contention et AIFS pour contrôler l′accès au canal. Les stratégies d′hiérarchisation et d′ordonnancement contrôlent la congestion en définissant une priorité pour chaque message, puis en les ordonnant dans les files d′attente de contrôle ou de service conformément à CCH et SCH, respectivement, dans ces stratégies, les messages de sécurité hautement prioritaires ont plus de chance d′être transférés dans les canaux. Enfin, les stratégies hybrides utilisent tout ou une partie des paramètres et des moyens des stratégies pour contrôler la congestion dans les VANETs. Ces stratégies sont discutées en détail ci-dessous :

2.4.2.1 Stratégies basées sur les taux de transmission

Ces stratégies ajustent dynamiquement le débit de transmission ou le taux de génération de paquets pour contrôler les charges des canaux et la congestion dans les réseaux. Les performances des VANETs s′améliorent en augmentant le taux de transmission car les applications de sécurité peuvent recevoir de nouvelles informations sur l'état des véhicules voisins, envoyer leur propre statut aux véhicules voisins et mettre á jour leurs informations pour fonctionner efficacement. En outre, un taux de balisage élevé dans le réseau, en particulier lorsque la densité du réseau est élevée, conduit á une utilisation élevée de la bande passante et par conséquent á une congestion dans le canal de contrôle. Par conséquent, la performance des applications de sécurité est réduite .Il convient également de noter que lorsque le débit de transmission augmente, le canal peut se saturer en raison de l′augmentation des charges du canal[22].

Tielert et al.[23] ont présenté une stratégie basée sur l′adaptation de débit pour contrôler la congestion dans les réseaux véhiculaires qui s′appelait contrôle PULSAR (Periodically Updated Load Sensitive Adaptive Rate). 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). Dans cette stratégie, la portée de transmission est sélectionnée en fonction de la charge du canal qui dépend de l'environnement de conduite. La puissance de transmission est également considérée comme fixe en fonction des exigences de l′application. La stratégie PULSAR contrôle la congestion en trois étapes principales : Dans la première étape, lévaluation de la charge du canal est effectuée en utilisant le taux d′occupation du canal (CBR) qui est une mesure de rétroaction appropriée pour maximiser le nombre de paquets reçus, pour détecter la congestion. Dans la deuxième étape, une adaptation tarifaire (réglage de débit de transmission) est effectuée, lorsqu′une nouvelle mesure CBR arrive à la fin de chaque intervalle (CMDI), PULSAR compare la valeur mesurée par rapport à la valeur cible. Etant 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 débit de transmission sélectionné est partagé entre les véhicules voisins situés dans la portée de communication.

Par conséquent, dans cette stratégie, les véhicules voisins contribuent au processus de contrôle de la congestion. La stratégie PULSAR diffuse équitablement les informations de congestion entre les véhicules voisins sur des multi-sauts de sorte que les nœuds cachés sont considérés. Cependant,

dans cette stratégie, les exigences de l′application de sécurité ne sont pas prises en compte. De plus, le partage des informations de congestion entraîne une charge supplémentaire pour les canaux.

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 sécuritè, mais les exigences relatives de ces dernières ne sont pas prises en compte (la priorité, la fiabilité, etc.). 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.

2.4.2.2 Stratégies basées sur la puissance de transmission

Dans ces stratégies la puissance de transmission (portée) est réglée pour diminuer les congestions du canal. Pour assurer l′équité aux VANETs, tous les noeuds devraient avoir une possibilité similaire de communiquer avec d′autres véhicules voisins. Les applications de sécurité envoient généralement leurs messages de sécurité avec une portée de transmission élevée pour couvrir une plus grande zone de sorte qu'un plus grand nombre de noeuds peut recevoir ces messages de sécurité. Cependant, si la congestion se produit dans le réseau, certains véhicules devraient réduire leur puissance de transmission pour réduire les collisions des canaux. Ainsi, la chance de communiquer avec les véhicules voisins est réduite et l′objectif d′équité dans les VANETs est violé. De plus, une puissance d′émission élevée conduit à augmenter la collision du canal et la saturation du canal[24][25].

Torrent-Moreno et al.[10] ont proposé une stratégie D-FPAV (Distributed Fair Power Adjustment for Vehicular Networks) qui est une stratégie d′ajustement de la puissance de transmission entièrement distribuée et localisée pour les environnements véhiculaires. D-FPAV fournit une puissance de transmission efficace pour les messages pilotés par les événements en diminuant les charges de balisage dans le canal de contrôle. En utilisant D-FPAV, les messages pilotés par les événements ont une priorité plus élevée que les messages de balise à transférer dans le canal de contrôle. Cette stratégie considére que les taux de réception de balisage ne diminuent pas aux nœuds voisins. Cette stratégie contrôle la congestion en ajustant équitablement la gamme de messages de balise en fonction de la densité du véhicule. Dans D-FPAV, chaque véhicule nécessite l′information globale sur l′état des véhicules voisins situés dans la gamme de détection de porteuse. Sur la base de cette connaissance, les véhicules ajustent la portée de transmission maximale pour les messages de balise de sorte que la charge de balisage ne dépasse pas un seuil prédéfini fixe. Ensuite, la puissance

de transmission ajustée est diffusée aux véhicules voisins situés dans la plage de détection de porteuse. Un temps d'occupation de canal équitable est obtenu en utilisant D-FPAV. Cependant, la réduction de la portée de transmission de balisage réduit la distribution de messages de balise à des distances plus lointaines. Par conséquent, les applications de VANETs qui ont utilisé l'information des messages de balise peuvent faire face au manque d'informations essentielles pour fonctionner efficacement. De plus, la collecte de l'information globale sur les véhicules environnants est une tâche difficile dans les VANETs, et l'échange de la puissance d'émission ajustée entre les véhicules voisins entraîne une charge supplémentaire dans les canaux.

Les étapes de cette stratégie sont définies comme suit :

- 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.
- Equilibrer 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).
- 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.
- 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 paramétres 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.

2.4.2.3 Stratégies basées sur CSMA / CA

La stratégie CSMA / CA est une stratégie d'évitement des collisions utilisée comme stratégie de contrôle de congestion par défaut dans IEEE 802.11p. Cette stratégie détermine la capacité

d′accés au canal de chaque noeud dans la couche MAC en ajustant la taille de la fenêtre contention et l′AIFS (Arbitrage Inter Frame Space). Ces derniers jouent des rôles importants pour réduire les collisions du canal et éviter l′occurrence de la congestion dans les canaux. En outre, dans la stratégie CSMA / CA, le mécanisme de retrait exponentiel est utilisé pour contrôler la congestion. Cependant, lorsque le taux de génération de message est élevé, le mécanisme de retour exponentiel n′est pas exécuté efficacement dans les réseaux VANETs en raison de la suppression des messages avant transmission[22][24].

Barradi et al.[26] ont présenté une stratégie de contrôle de la 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 le transfert sans délai du message de sécurité de haute priorité sur le canal de contrôle(CCH). Cette stratégie ajuste les plages de taille de fenêtre de back-off et AIFS pour différents types de messages dans les VANETs, afin de mettre en œuvre les priorités strictes pour les messages de sécurité. De plus, cette stratégie fournit les accusés de réception pour les messages de sécurité diffusés dans le canal de contrôle afin d′assurer la remise du message de sécurité et d′empêcher la retransmission des messages. Cependant, ces accusés de réception causent plus de collisions dans les réseaux denses en raison de l′ajout de charges supplémentaires sur les canaux congestionnés. Grâce à cette stratégie, le délai, la gigue et la perte de paquets réduisent les messages de scéurité dans des conditions de haute densité. Cependant,pour les messages de faible priorité, les performances des VANETs diminuent.

2.4.2.4 Stratégies basées sur la priorité et l′ordonnancement

Ces stratégies contrôlent la congestion en affectant la priorité aux messages et en les ordonnant pour les transférer dans les canaux de contrôle et de service. Dans ces stratégies, les priorités sont définies de telle sorte que les messages de sécurité prioritaires ont plus de chance d′acquérir les canaux et de les transférer avec moins de retard. En utilisant ces stratégies, l′accès au canal est contrôlé de telle sorte que les collisions sont diminuées. Dans cette classe de stratégies de contrôle de congestion, une hiérarchisation stricte est requise pour les différents types de messages générés dans VANETs. Ensuite, les messages prioritaires sont programmés pour être transférés dans des canaux de contrôle ou de service. Par conséquent, les stratégies basées sur l′établissement de priorités et l′ordonnancement peuvent empêcher la saturation du canal et, par conséquent, l′occurrence de l′encombrement dans les réseaux. Généralement, les stratégies de hiérarchisation et d′ordonnancement sont des stratégies de contrôle d′encombrement proactives très courantes qui

sont employées pour prévenir l'occurrence d'encombrement dans les réseaux[?][27][27].

Certains algorithmes de hiérarchisation et d'ordonnancement qui peuvent être utilisés dans les VANETs sont First-in-First-out (FIFO), Longest Wait Time (LWT) et Maximum Request First (MRF), First Deadline First (FDF), Plus petit format de données (SDF), (LTSF) Longest Total Stretch First,(MQIF) Maximum Quality Increment First, (LSF) Least Selected First et D * S.

L'algorithme FIFO, qui est l'un des algorithmes d'ordonnancement les plus simples, sert d'abord la première demande d'arrivée.

En effet, les premiers paquets arrivant aux files d'attente sont d'abord transférés vers les canaux. L'algorithme LWT donne une priorité plus élevée aux messages qui attendent plus longtemps dans les files d'attente à transférer dans les canaux.

L'algorithme MRF attribue une priorité plus élevée aux messages qui ont été demandés davantage par divers services. Dans l'algorithme FDF, les messages sont planifiés en fonction du délai restant à respecter. L'algorithme SDF a déterminé la plus haute priorité pour les messages de taille inférieure . En LTSF, une mesure étirement est utilisée pour réduire le temps d'attente dans les files d'attente. Cette métrique est définie comme le rapport entre le temps de réponse de la requête et le temps de service demandé[30].

L'algorithme LTSF vise à optimiser la valeur de la métrique d'étirement. Cependant, cet algorithme d'ordonnancement ne peut pas fonctionner efficacement lorsque la taille du système est grande (en particulier lorsque les messages sont diffusés) en raison de l'augmentation du temps de calcul pour calculer la métrique d'étirement pour chaque élément de données . Dans l'algorithme MQIF, les messages sont planifiés en fonction des métriques de qualité de service (QoS) et de qualité des données (QoD). Les métriques QoS et QoD sont définies pour prendre en compte la réactivité et l'inertie des messages de données, respectivement. Enfin, l'algorithme D * S détermine les priorités en fonction de Deadline (D) et Size (S) des messages[30][32].

C.Suthaputchak.[28] a proposé une stratégie de contrôle de congestion axée sur les priorités, qui utilise les communications entre véhicules pour accroitre 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, 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 Table2.1. Chaque message sera mis en file dattente en fonction de sa priorité. Il existe un contrôleur de chasse virtuel, qui suit la chute interne. Le gestionnaire de collision virtuelle permet-

tra 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 $CW_{min}[i]$ $CW_{max}[i]$, 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 seulement1 unité de données de service MAC.

Priorités	**Types**	**Exemples**
Priorité 1	Accident	−Capteur airbag −Capteur du corps du véhicule − Capteur thermique
Priorité 2	Possibilité d′accident. .	− Saut − Etat de surface .
Priorité 3	Alerte	−Avertissement de travaux routiers −Trafic de congestion
Priorité 4	Autre	Conditions Météorologiques

TABLE 2.1 – Les priorités des massages dans la messagerie de la sécurité routiére[28].

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.

2.4.2.5 Stratégies hybrides

Dans les stratégies hybrides, deux ou plusieurs paramètres et moyens sont utilisés pour contrôler la congestion. Le réglage de débit et de la puissance de transmission, l′ajustement de la taille de la fenêtre de contention et de l′AIFS et la définition d'une priorité appropriée pour chaque message et l′ordonnancement dans les canaux sont combinés dans des stratégies hybrides pour éviter la saturation et la congestion des canaux[25].

Huang et al.[29] ont proposé un algorithme de contrôle de congestion orienté véhicule AVOCA (A Vehicle Oriented Congestion Control Algorithm) qui est un algorithme de contrôle de congestion inter−couches. Dans AVOCA, étant donné que la congestion est contrôlée dans le réseau, les trous de couverture du réseau sont pris en compte. Cet algorithme a été proposé pour remédier à

la défaillance de la couche de transport lorsque les véhicules pénètrent dans une zone de couverture. AVOCA utilise un seuil de performance défini dans la couche de transport pour contrôler la transmission de paquets dans cette couche. Lorsqu′un véhicule entre dans une zone de couverture, les performances de la couche de transport dépassent le seuil. Ensuite, l′AVOCA réinitialise les paramètres de contrôle de congestion et initie les transmissions de paquets. D′autre part, lorsque le véhicule quitte la zone de couverture, les performances de la couche de transport diminuent. Ensuite, AVOCA gèle les paramètres de contrôle de congestion et met fin aux transmissions de paquets. Cet algorithme améliore considérablement le débit du réseau en tenant compte de l′équité dans l′attribution des canaux.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.

Après avoir étudier et analyser les protocoles cités précédemment, il nous est apparu qu′une étude comparative est estimable. La table 2.2, illustre cette étude selon quelques exigesnces des applicatins de sècuritè à savoir :efficacitè,fiabilitè,prioritè d'accès.

Protocole	Paramètre	Fonctionn -ement	Fiabilité	Efficacité	Priorité D′accés
PULSAR	Débit de transmis-sion	Diffision équitable des infor-mation aux vé-hicules voisin	Non	Non	Non
D-FPAV	Puissance d′émission	Densité des véhi-cules	Oui	Oui	Oui
EDCA	Taille de la fenétre de back-off et AIFS	Fornit les accusés de reception	Non	Non	Oui
C.SUTHPU TCHAK	CWmin[i] CWmax[i] AIFS[I]	Mécanisme de retrans-mission	Oui	Non	Oui
AVOCA	débit de trans-mission Puissance d′émission	Utilisé un seuil de per-formance défini dans la couche de transport	Non	Non	Non

TABLE 2.2 – Comparaison entre les différents protocoles.

Dans ce tableau,on a effectué une étude comparative entre des protocoles de contrôle de conges-tion appartenant aux differentes stratégies de contrôle de congestion,telle que les protocoles(PULSAR,D−FP

successivemant aux classes des stratégies basées sur (Débit de transmission,Puissance d'émission,CSMA-CA,Priorisation et ordonnancement,Hybrides)selon les exigences des applications de sécurité suivantes(efficacité,fiabilité,priorité d'accés). Pour le protocole PULSAR,on ajuste le débit de transmission pour contrôler la congestion,cependant les exigences de sécurité ne sont pas prises en compte. Le protocole D-FPAV ajuste dynamiquement la puissance d'émission pour contrôler la charge des canaux ,compte tenu pour la fiabilité,l'efficacité de la diffusion des messages,et la priorité d'accés(les messages événementiels sont de priorité plus élevé par rapport aux messages de balise). EDCA détermine la capacité d'accés au canal de chaque noeud dans la couche MAC,en ajustant la taille de la fenétre de contention et AIFS.Dans ce protocole,on tient compte uniquement pour la priorité d'accés des messages. Dans le protocole proposé par C-SUTHPUTCHAK qui est basé sur la priorité et l'ordonnancement,on prend en consédération la priorité d'accés des messages,telle que le messages de sécurité hautement prioritaires ont plus de chance de se transférer dans les canaux.et la fiabilité de la diffusin des messages de sécurité entre les véhicules est aussi prise en consédération. Finalement,le protocole AVOCA ajuste les paramétres de contrôle de congestion afin de répondre au probléme de défaillance dans la couche de transport,sans tenir compte pour aucune exigence des applications de sécurité. D'aprés cette comparaison,on constate que le meilleure protocole est AVOCA,car il ajuste plusieurs paramétres de contrôle de congestion,sans se limiter par les exigences des applicatin de sécurité.

2.5 Conclusion

Dans ce chapitre, nous avons défini le problème de congestion, et nous avons présenté les méthodes de détection de congestion. Puis nous avons abordé les différents mécanismes de contrôle de congestion avec ces différents protocoles utilisés. Comme nous avons effectué une comparaison entre ces protocoles dans tableau récapitulatif. Dans le prochain chapitre, nous allons proposé un protocole de contrôle de congestion tout en expliquant son principe de fonctionnement .

CHAPITRE 3

NOUVEAU PROTOCOLE POUR LE CONTRÔLE DE CONGESTION

3.1 Introduction

Pour faire face aux problèmes de congestion, qui se déclenche à cause de la mobilité élevé des nœuds et le changement de topologie à grande vitesse des réseaux VANETs.Ainsi que l′amélioration de la qualité de service et les performances des VANETs, plusieurs protocoles ont été proposés à savoir : Tielert et al [23], Torrent-Moreno [10],Barradi et al[26],C.Suthapuchak [28],Huang et al[29].

Ces protocoles sont classés selon les paramètres et les mesures par lesquelles la congestion à été contrôlé à savoir : le débit de transmission, la puissance d′émission, la planification et l′ordonnancement, ainsi que les stratégies hybrides qui ajustent tous ou une partie des paramètres ajustés dans les stratégies précédentes. Chaque protocole a des avantages ainsi que des inconvénients et des parties incomplètes qui nécessitent des améliorations.

Pour cela, nous avons proposé un protocole de contrôle de congestion qui appartient aux stratégies fondées sur l′assignation des priorités pour les messages envoyés selon leurs contenus (planification et ordonnancement). Notre protocole ajuste la puissance de transmission et le taux de transmission, en surveillant d′une part, le temps d′attente d′un paquet avant qu′il occupe le canal, et le nombre de paquet à envoyer dans le cas de communication V2I .D′autre part, il contrôle le temps d′attende de paquet reçu avant de le renvoyer, et le nombre de messages reçus au canal dans le cas d′une communication V2V .

Ce chapitre est consacré pour définir le modèle du réseau où notre protocole fonctionne, ainsi que la présentation de son principe fonctionnement.

3.2 Modèle du réseau

Derniérement les VANETs ont attiré beaucoups de chercheurs.L'objectif des VANETs est d'assurer la sécurité de la vie sur les routes. Pour ce fait,les véhicules utilisent deux types de messages :

- Des messages de sécurité périodiques(balises)pour échanger des informations d'état,par exemple :emplacement,vitesse...
- Des messages évenementiels qui sont diffusés en cas de situation d'urgence,par exemple :accident,frinage brutal...

Comme les deux types de messages partagent le même canal de contrôle,ce qui provoque la congestion du canal, et la dégradation des performances des canaux. Le réseau ad−hoc véhiculaire (VANET) est apparu comme une solution possible pour concevoir des réseaux capables de résoudre les problèmes de détection de congestion du trafic . Les premières tentatives ont porté sur la communication de véhicule à véhicule qui a essentiellement une courte portée. Le véhicule peut être équipé de ces dispositifs (OBU) et cela peut servir à des fins de communication à courte portée dédiée ou DSRC. Ce mode est plus simple et attrayant à certains égards, mais prèsente des limites qui justifient l′utilisation d′autres systèmes. Pour commencer, si la densité des véhicules est faible ou si le véhicule en question tombe en panne,le mode de communication $V2V$ cessera d′être efficace. Plus important encore, il ne peut pas résoudre les problèmes d′alerte rapide sur une large gamme de manière à permettre aux véhicules de prendre d′autres itinéraires vers la destination. L′autre possibilité qui offre une plus grande portée et d′autres avantages qui se produisent à partir de plus longue portée est de véhicule à infrastructure ou réseau V2I. Cela a une longue portée et le traitement des données et la transmission du message à une région complète couvrant tous les véhicules . Cependant, pour mettre en œuvre ceci, une grande ressource est nécessaire car les tours de communication ou ce qu′on appelle les unitées latérales de la route(RSU) sont des propositions coûteuses. La portée de ces V2I dépend de leur puissance et / ou un compromis approprié entre l′espacement des tours et la puissance de transmission peut être obtenu en fonction des terrains et des statistiques de densité du véhicule et de la topologie de l′interconnexion des routes.

Nous combinons les bonnes caractéristiques des deux et offrons une meilleure solution pour la détection et le contrôle de la congestion. Dans la figure 3.1 nous présentons un modèle typique d′une route, avec des RSUs embarquées au bord de cette dernière (les feux tricolores, les virages,

les intersections, les stops, etc.) .Cette utilisation combinèe de V2V et V2I est robuste et efficace.

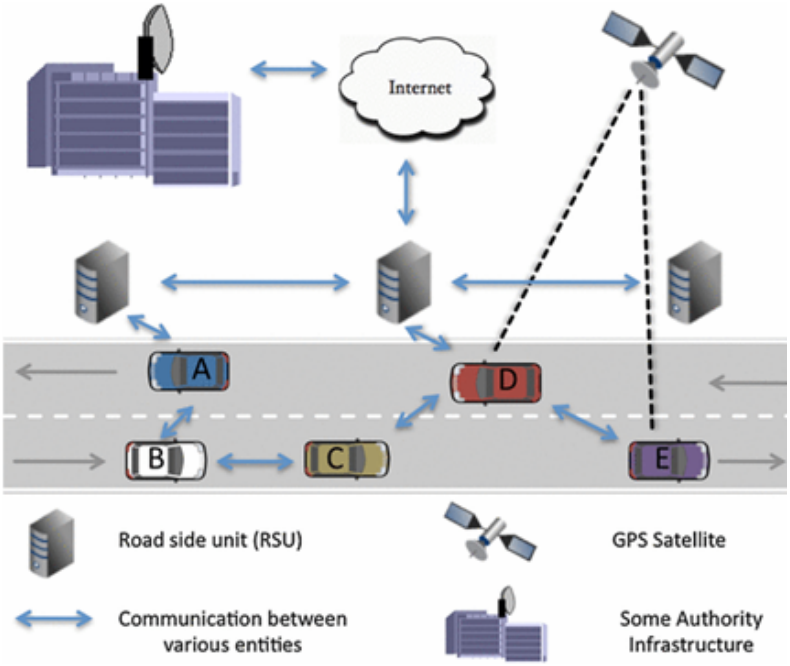

FIGURE 3.1 – Mode de communication hybride[42]

3.3 Principe de fonctionnement du protocole proposé

La congestion du canal est un problème crucial des zones urbaines,dû aux plusieurs raisons tellesque : les accidents routiers,obstacles sur la route,conditions météorologiques etc.

Pour éviter la congetion du canal de contrôle , réduire les retards des paquets et assurer la transmission des messages de sécurité(évenementiels et balises) dans un délai minimun,nous proposons un algorithme pour contrôler la congestion du canal en se basant sur les réseaux véhiculaires ,cet algorithme fonctionne dans un réseau hybride qui combine la communication véhicule à véhicule et véhicule à infrastructure. ses etapes sont détaillées comme suit :

3.3.1 Architecture Communication de véhicule à infrastructure (V2I)

Dite architecture centralisée, où la route est dotée des unités latérales RSUs. Lors d′un accident routier, le véhicule affecté envoie immédiatement un message de sécurité à l′unité côté de la route. Cette dernière rediffuse ce message aux véhicules appartenant à la zone de couverture de la tour, pour que ces véhicules puissent prendre la décision appropriée, dans le but d′éviter la congestion. Tout en appliquant les étapes du notre protocole proposé. Comme le montre la figure ci dessous :

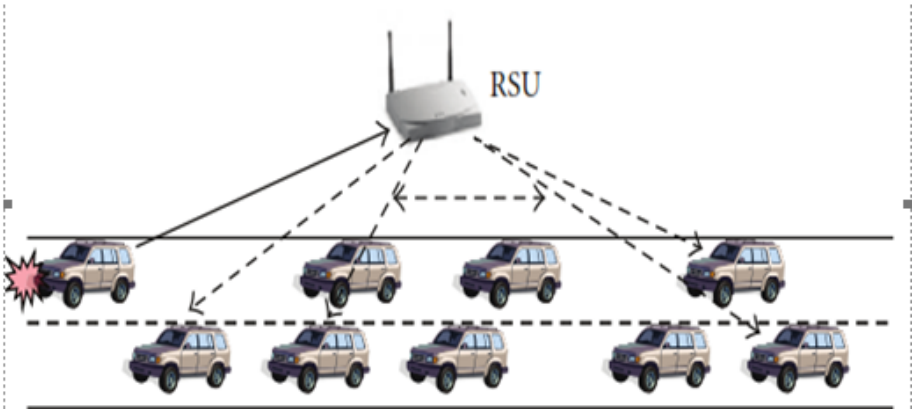

FIGURE 3.2 – Modèle du réseau véhicule à infrastructure

Dans cette architecture, notre protocole fonctionne en trois phases :

- Affectation des priorités aux messages selon leur utilité.
- Détection de la congestion.
- Contrôle de la congestion.

Ces phases seront détaillées au niveau des sous sections suivantes

3.3.1.1 Assignation des priorités aux messages selon leurs contenus

Notre protocole contrôle la congestion en affectant des priorités aux messages de sécurité envoyés des RSU aux véhicules, et en les ordonnant pour les transférer dans les canaux de contrôle et de service. Dans ce protocole, les priorités sont définies de telle sorte que les messages de sécurité prioritaires MP_{max} ont plus de chance d′acquérir les canaux de contrôle et de service, et de les transférer avec moins de retard. Les priorités assignées aux messages sont en fonction de leur contenu (utilité), ce qui nous permet de distinguer trois types de message à savoir :

MP$_{max}$: désigne les messages avec des priorités maximales comme les messages d′urgence : accident, arrêt d′urgence d′un véhicule, route barrée, danger éventuel, etc.

MPM : désigne les messages avec priorités moyennes, comme les messages d′avertissement, la vitesse, ceinture de sécurité, etc.

$\mathbf{MP}_{min}$: désigne les messages avec priorités minimales, telle que les messages périodiques, météorologiques, etc.

3.3.1.2 Détection de congestion

La détection de la congestion au niveau de notre protocole se fait en mesurant périodiquement le niveau d′utilisation du canal, en se basant sur deux paramètres importants à savoir : le temps d′attente d′un paquet avant qu′il occupe le canal et le temps d′occupation du canal, et le nombre de paquet à envoyer (la taille de la file d′attente). Pour chacun des deux paramètres on affecte un seuil prédéfini, telle que le temps d′attente d′un paquet avant qu′il occupe le canal, on lui affecte un seuil α. Et le nombre de paquets à envoyer, on lui affecte un seuil β. Ces seuils prédéfinis ont un impact significatif sur les performances du réseau. Dans notre protocole, lors d′un accident, le véhicule affecté (nœud affecté) envoie un message au RSU pour l′informer sur l′existence d′un accident, de son tour RSU envoie des messages de sécurité pour les véhicules situés dans sa zone de couverture. D′ou chaque véhicule mesure périodiquement les valeurs de ces deux paramètres pour juger l′apparence de la congestion, telle que ,en mesurant localement la valeur du temps d′attente d′un paquet avant qu′il occupe le canal CCH, si elle dèpasse le seuil α on considère qu′il y′a une congestion dans le réseau(détection de congestion). De la même manière pour le nombre de messages à envoyer, si sa valeur dépasse un seuil β, alors il existe une congestion dans le réseau.

3.3.1.3 Contrôle de congestion

Une fois la congestion est détectée par les véhicules appartenant au réseau, le contrôle de congestion selon notre protocole, se fait en quatre étapes, que nous allons détailler en ce qui suit :

- Après la détection de la congestion par le véhicule, ce dernier envoie immédiatement et seulement des messages de sécurité avec priorité MP_{max}, telle que ces messages contiennent trois éléments à savoir : l′utilité du message, et l′adresse de RSU pour lequel on envoie ce message, plus un bit = 1 (qui indique la présence de congestion dans le réseau) .
- RSU renvoie les messages qui ont la priorité MPmax pour seulement les véhicules appartenant à sa porté de transmission avec une puissance de transmission adéquate pour minimiser le nombre de véhicules qui vont recevoir le message (donc, on minimise le nombre de messages reçus),il s′agit donc de l′ajustement de la puissance d′émission. Telle que la forme des messages envoyés reste la même qui garde toujours le bit= 1 pour que les autres véhicules recevant le messages sachent qu′il y a une congestion. Donc la réduction de la puissance d′émission minimise le nombre de messages à transmettre, ce qui aide à la réduction de la congestion au niveau du canal.
- Les RSUs Ajustent la vitesse de transmission des messages avec priorité MPM afin de réduire le nombre de messages diffusés du RSUs au véhicules ,ce qui réduit la possibilité d′avoir la saturation du canal et éviter sa congestion
- - Les RSUs bloque carrément l′envoie des messages avec MP_{min}, après la détection de la congestion, dans le but de garantir la fluidité du canal et de minimiser sa congestion.

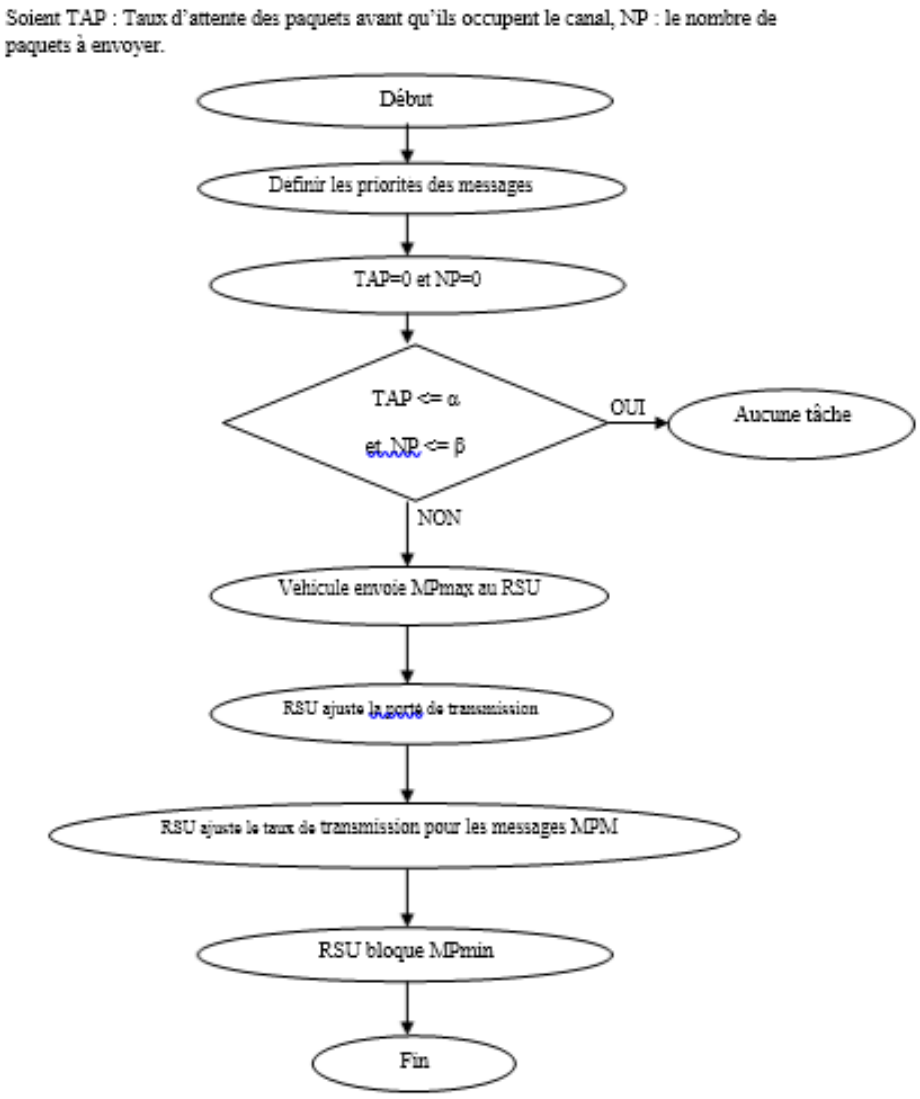

FIGURE 3.3 – Organigramme de contrôle de congestion dans le mode de communication véhicule à infrastructure.

3.3.2 Architecture Communication de véhicule à véhicule (V2V)

Dite architecture distribuée, ou la route contient que des véhicules dotés des OBUs, sans l'existence des unités coté de la route RSU. La vitesse du véhicule devient nulle en cas d'accident. Le message d'avertissement se diffuse continuellement par le véhicule affecté aux véhicules appartenant à sa gamme de transmission. Le véhicule de la gamme reçoit le message d'avertissement transmis par le véhicule concerné, les véhicule obtient les informations sur l'état de la voie et sa situation puis il prend la décision et met également à jour les champs de message et retransmet le message reçu. Comme le montre la figure3.5 .

Dans cette architecture, notre protocole fonctionne en trois phases :

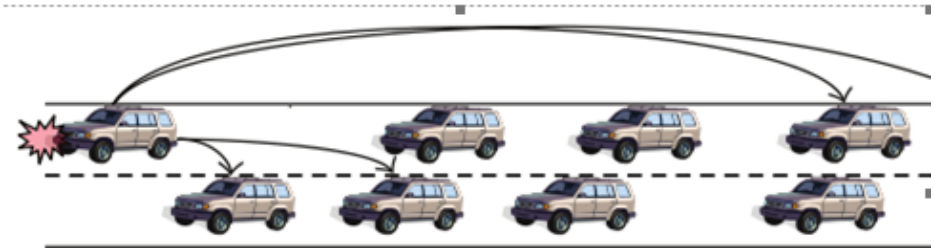

FIGURE 3.4 – Modèle du réseau véhicule à véhicule

– Assignation des priorités selon le contenu des messages.
– Détection de congestion.
– Contrôle de congestion.

Nous allons présenter en détaille chacune des trois phases motionnées précédemment, comme suit :

3.3.2.1 Assignation des priorités aux messages selon leur contenu

Lors d′un accident, le véhicule affecté envoie des messages de sécurité aux autres véhicules voisins, afin de les informer de l′état de la route. On affecte à chaque message une prioritè convenable selon son utilité. Les différentes priorités se divise en trois types, qui sont définit comme suit :

MP$_{max}$: désigne les messages avec des priorités maximales comme les messages d′urgence : accident, arrêt d′urgence d′un véhicule, route barrée, danger éventuel, etc.

MPM : désigne les messages avec priorités moyennes, comme les messages d′avertissement, la vitesse, ceinture de sécurité, etc.

MP$_{min}$: désigne les messages avec priorités minimales, telle que les messages périodiques, météorologiques, etc

3.3.2.2 Détection de congestion

Ici, on mesure le niveau d′utilisation du canal, suivant deux paramètres à savoir : le temps d′attente de paquets reçus avant de les envoyer, et le nombre de messages reçus. On affecte pour ces deux paramètres deux valeurs prédéfinis α, β successivement appelées seuils, telle que si les valeurs mesurées des deux paramètres dépassent ces seuils, on déduit qu′une congestion est survenu. Dans notre protocole, lors d′un accident, le véhicule affecté envoie un message aux véhicules voisins pour les informer sur cet accident, de leur tour ces véhicules rediffusent ses messages de sécurité pour les véhicules voisins ce qui peut provoquer la congestion du canal. D′où chaque véhicule mesure périodiquement les valeurs du temps d′attente de paquets reçus avant de les envoyer ainsi que le

nombre des messages reçus dans le canal, pour juger l′apparence de la congestion, telle que, en mesurant localement la valeur du temps d′attente des paquets reçus au canal CCH avant de les envoyer, si elle dépasse le seuil α on considère qu′il y′a une congestion dans le réseau (détection de congestion).On mesure également le nombre de messages reçus au canal, si sa valeur dépasse un seuil β, alors il existe une congestion dans le réseau.

3.3.2.3 Contrôle de congestion

Après avoir détecter la congestion du canal, le véhicule détectant la congestion et qui appartenant au lieu de la congestion, transmet des messages événementiels pour les véhicules voisins dans le but de les informer de l′existence de congestion. Pour que ces véhicules puissent prendre de bonnes décision pour minimiser cet encombrement. Selon notre protocole la congestion va être diminuée en trois étapes principales détaillées au dessous :

-Eliminer tous les messages avec la priorité MP$_{min}$:

après avoir recevoir les messages qui les informent qu′une congestion existe au niveau du canal de transmission, les véhicules décident immédiatement de bloquer les messages du la priorité minimale MP$_{min}$, Pour libérer le canal un petit peu.

-Ajuster la vitesse de transmission des messages avec la priorité MPM

aprés avoir bloquer les messages de priorité MP$_{min}$,les véhicules doivent minimiser la nombre de messages de priorité moyenne MPM par unité du temps, il s′agit donc de l′ajustement du taux de transmission afin d′assurer la fluidité des messages au niveau du canal.

-Calcul de puissance de transmission optimal : après le blocage des messages de priorité MP$_{min}$, et l′ajustement du taux de transmission, les véhicules passent à l′ajustement de la puissance de transmission, en déterminant le nombre optimal de voisins suivant la distance, la région géographique. Telle que les véhicule détectant la congestion sélectionnent les véhicules appartenant à la zone géographique la où il y′a une congestion, de plus ils affectent une valeur prédéfinie k pour la distance séparant entre le véhicule affecté et les véhicules voisins, on mesure cette distance entre le véhicule affecté et chacun des véhicules appartenant à son voisinage ,si elle dépasse le seuil k ca veut dire ce véhicule n′appartient pas á sa porté de transmission, si elle est inférieure ou égale à k , ca veut dire ce véhicule appartient à la porté de transmission. d′ou on trouve la puissance de transmission optimale.

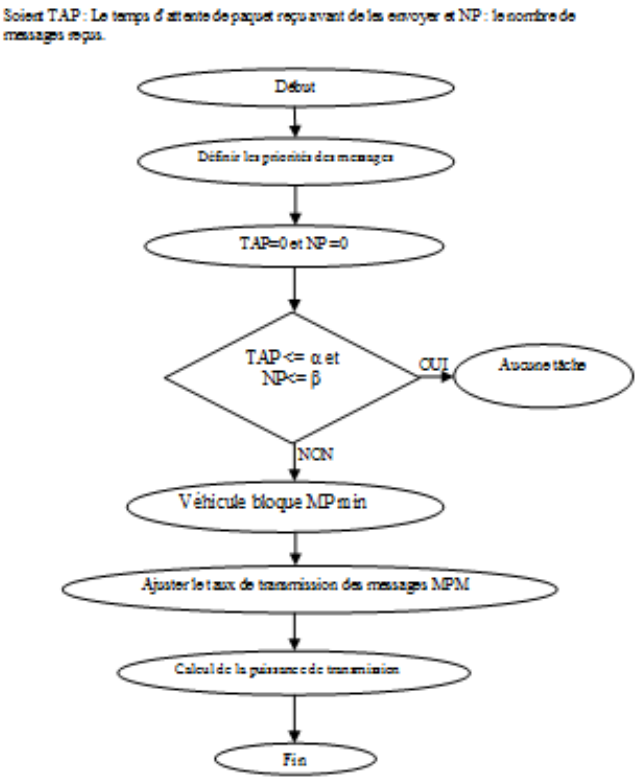

FIGURE 3.5 – Organigramme de contrôle de congestion dans le mode de communication véhicule à véhicule

3.4 Conclusion

Dans ce chapitre, nous avons développé un nouveau protocole de contrôle de congestion, qui appartient à la classe des stratégies réactives. Il est basé sur l′adaptation du taux de transmission ainsi que puissance d′émission en affectant les priorités pour les messages a transmettre, dans le but d′éviter la congestion du canal et améliorer les performances des VANETs. Ce protocole fonctionne dans un réseau hybride qui combine le mode de communication véhicule à véhicule avec le mode de communication véhicule à infrastructure. Nous avons présenté le model de réseau où fonctionne notre protocole, comme nous avons détaillé son principe de fonctionnement, puis on a introduit les organigrammes appropriés à ce protocole.

CONCLUSION GÉNÉRALE

Fournir une communication fiable dans les futurs réseaux en particulier les réseaux véhiculaires(VANET) est un véritable défi. En effet, un réseau VANET est un environnement hostile qui apporte plusieurs défis, dû à des caractéristiques et spécificités propres à ce genre de technologie. Dans ce mémoire de master, nous avons proposé l′amélioration des systèmes de communication dans les réseaux VANETs. Plus particulièrement, nous cherchons à mieux contrôler la congestion dans ces réseaux pour rendre la communication plus fluide pour assurer le bon fonctionnement de ces réseaux. Au commencement, nous avons présenté les réseaux vhéiculaires pour bien comprendre sur quoi notre travail est basé. Ensuite, nous avons présenté quelques stratégies et protocoles utilisés pour le contrôle de la congestion. Car la présence de cette dernière dans les VANETs réduit la fiabilitè de transmission des messages entre les nœuds, ce qui réduit les performances de cesréseaux. La plupart des approches propoées se basent sur l′ajustement du taux de transmission, puissance de transmission, CSMA/CA, priorisation et ordonnancement. Notre protocole proposé pour le contrôle de congestion fonctionne dans un mode de réseau hybride, qui combine entre le mode de communication véhicule à véhicule et le mode de communication véhicule à infrastructure. Donc, notre protocole englobe les bonne caractéristiques des deux modes et offre une meilleure solution pour la détection et le contrôle de la congestion du trafic, Cette utilisation combinée de V2V et V2I est robuste et efficace. Ce protocole se base sur la priorisation et l′ordonnancement des messages selon leurs utilité, ce qui conduit à l′ajustement du taux de transmission et la puissance de transmission , tout en mesurant le temps d′attente d′un paquet avant qu′il occupe le canal ainsi que le nombre de paquets à envoyer dans le cas de communication V2I, puis Le temps d′attente de paquet reçu avant de les envoyer, et le nombre de messages reçus dans le canal CCH dan le cas de communication V2V. .

.

BIBLIOGRAPHIE

[1] R. Mazot, W. Meslem, M. Layouni, and A. Tran, Communication inter véhiculaire. PhD thesis, Arles Avignon, 2013.

[2] S. Busanelli, G. Ferrari, and L. Veltri, "Conférence," in Short-lived Key Management for Secure Communications in VANETs, 2011.

[3] K. Moghraoui, Gestion de l′anonymat des communications dans les réseaux véhiculaires AD HOC sans fil (VANETs). PhD thesis, l′université du Québec à trois-rivieres, 2015.

[4] D. Bektache, Application et Modélisation d′un protocole de communication pour la sécurité routiére. PhD thesis, l′université de Badji Mokhtar Annaba, 2014.

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

[6] FD. Cunha, A. Boukerche, L. Villas, AC. Viana, and AF. Loureiro. Data communication in vanet : a servey, challenges and applications, 2014.

[7] MY. Darous and AB. Kamalrulnizam. Congestion control algorithm for evendriven safety messages in vehiclar networks. vol 03 , pages 99 - 106. In Journal of Advenced Computer Science and Technology Research, 2013.

[8] 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.

[9] 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.

[10] M. Torrent-Moreno, P. Santi, and H. Hartenstein, "Distributed fair transmit power adjustment for vehicular ad hoc networks," 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks, SECON'06, pp. 479-488, 2006.

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

[12] J. Toutouh, S. Nesmachnow, and E. Alba. Fast energy-aware olsr routing in vanets by means of a parallel evolutionary algorithm. vol 16, pages 435− 450. In Springer Science+Business Media, 2000.

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

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

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

[16] 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.

[17] J. Petit, Surcoût de l′authentification et du consensus dans la sécurité des réseaux sans fil véhiculaires. PhD thesis, l′université de Toulouse, 2011.

[18] Y. Zang, L. Stibor, X. Cheng, H.-J. Reumerman, A. Paruzel, and A. Barroso, "Congestion control in wireless networks for vehicular safety applications," Proceedings of the 8th European Wireless Conference, 2007.

[19] M. Y. Darus and K. Abu Bakar, "A review of congestion control algorithm for event-driven safety messages in vehicular networks," International Journal of Computer Science Issues, vol. 8, pages. 49−53, 2011.

[20] M. Sepulcre, J. Mittag, P. Santi, H. Hartenstein, and J. Gozalvez, "Congestion and awareness control in cooperative vehicular systems," Proceedings of the IEEE, vol. 99, pages. 1260−1279, 2011

[21] M. R. Jabbarpour, R. M. Noor, R. H. Khokhar, and C.-H. Ke, "Cross-layer congestion control model for urban vehicular environments," Journal of Network and Computer Applications, vol. 44, pages. 1−16, 2014.

[22] X. Shen, X. Cheng, R. Zhang, B. Jiao, and Y. Yang, "Distributed congestion control approaches for the IEEE 802.11 p vehicular networks," IEEE Intelligent Transportation Systems Magazine, vol. 5, pages. 50-61, 2013.

[23] 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," IEEE Vehicular Networking Conference (VNC), pages. 116−123, 2011.

[24] M. Sepulcre, J. Mittag, P. Santi, H. Hartenstein, and J. Gozalvez, "Congestion and awareness control in cooperative vehicular systems," Proceedings of the IEEE, 2011.

[25] M. Torrent-Moreno, "Inter-vehicle communications : assessing information dissemination under safety constraints," Fourth Annual Conference on Wireless on Demand Network Systems and Services, WONS'07, pages. 59-64, 2007.

[26] M. Barradi, A. S. Hafid, and J. R. Gallardo, "Establishing strict priorities in IEEE 802.11 p WAVE vehicular networks," IEEE Global Telecommunications Conference (GLOBECOM 2010), pp. 1-6, 2010. bibitemM. S. Bouassida2010M. S. Bouassida and M. Shawky, "A cooperative congestion control approach within VANETs : formal verification and performance evaluation," EURASIP Journal on Wireless Communications and Networking, vol. 2010, 11, 2010.

[27] Y. Gui and E. Chan, "Data Scheduling for Multi-item Requests in Vehicle-Roadside Data Access with Motion Prediction Based Workload Transfer," 26th International Conference on Advanced Information Networking and Applications Workshops (WAINA), pages. 569−574, 2012.

[28] C. Suthaputchakun, "Priority-based inter-vehicle communication for highway safety messaging using IEEE 802.11 e," International journal of vehicular technology, vol. 2009, 2009.

[29] Y. Huang, E. Fallon, Y. Qiao, M. Rahilly, and B. Lee, "AVOCA−A Vehicle Oriented Congestion Control Algorithm," ISSC, Trinity College Dublin, 2011.

[30] V. Kumar and N. Chand, "Data Scheduling in VANETs : A Review," International Journal of Computer Science and Communication, vol. 1, pages. 399−403, 2010.

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

[32] R. Baldessari, D. Scanferla, L. Le, W. Zhang, and A. Festag, "Joining forces for vanets : A combined transmit power and rate control algorithm," 6th international workshop on intelligent transportation (WIT), 2010.

[33] J. Toutouh, S. Nesmachnow, and E. Alba. Fast energy-aware olsr routing in vanets by means of a parallel evolutionary algorithm. vol 16, pages 435− 450. In Springer Science+Business Media, 2000.

[34] Manoj Dongre , Narendra Bawane , Traffic Congestion Detection by using VANET to improve Intelligent Transportation System (ITS).International Journal of Network and Communication Scientific Academic Publication , 2015

[35] Ramesh B. Koti and Mahabaleshwar S. K.," Multi Agent Based Congestion Control in VANETs",International Journal of Future Computer and Communication, Vol. 3, 2, April 2014

[36] Mohammad Rezza Jabharpour Sattari, Rafidah Md Noor and Saied Ghahremani." Dynamic Congestion Control Algorithum for VANET", Inertnational Jouranl of software Engineering And its Applications, Vol. 7 , 3 May 2013.

[37] Mohamad Y. Duras, K. Abu Bakar," A review of Congestion Control Algorithms for events Driven Safety message in Vehicular Network", IJCS Vol.8 Issue 5, No.1 sept.2011.

[38] Komchan chaitien, chayaphon Tanwongvarl, Soamsiri Chantaraskul,"Adaptive Multichannel Approach for Congestion Control in Vehicular Safety Communications,2015 IEEE.

[39] By Miguel Sepulcre,Jens Mittiag,Paolo Santi,Member IEEE,"Congestion and Awareness Control in Coorperative Vehicular Systems,Vol.99, 7,july2011|Proceedings of the IEEE.

[40] Alak Roy,Jayasree Chakraborty,"Communication Based Accident Avoidance and Congestion Mechanism in VANETs,2015 (ISACC).

[41] Tianli Hu,Minghui Liwang,Lianfen Huang,Yuliang Tang,"An Enhanced GPSR Routing Protocol based on the buffer length of nodes for the Congestion Problem in VANETs,The 10th International Conference on Computer science and Education(ICCSE)july,2015.Fitzwilliam college Cambridge University,UK.

[42] N. Chaib. La sÃ©curitÃ© des communications dans les rÃ©seaux VANETs. ThÃ©se Magister, UniversitÃ© Elhadj Lakhdar, Batna, 2010.

Résumé :

La détection de la congestion est un problème majeur dans les VANETs, en particulier sur les routes urbaines. Pour cela nous avons besoin de prendre des décisions intelligentes pour éviter la congestion du réseau Ad Hoc véhiculaire. Dans notre mémoire, nous nous intéressons au problème de congestion dans les VANETs. Ce qui nous a conduits à proposer un protocole qui sert à détecter et contrôler la congestion du trafic en utilisant à la fois la communication véhicule 2 véhicule (V2V) et véhicule2 infrastructure (V2I) .
Notre protocole se base sur l'ajustement de taux de transmission et l'adaptation de puissance d'émission après l'affectation des priorités pour les messages diffusés selon leurs utilités, après avoir mesurer le niveau d'utilisation du canal(le temps d'attente d'un paquet , Et le nombre de paquet).Nous voulons évaluer les performances de notre protocole avec le simulateur NS-2,mais le facteur du temps nous a empêcher d'aboutir aux résultats finaux.

Mots clés : VANETs, Contrôle de congestion, priorités et ordonnancement, taux de transmission, puissance de transmission, communication V2V, communication V2I.

Abstract:

The detection of congestion is a major problem in VANETs, especially on urban roads. For that we need to make intelligent decisions to avoid the congestion of the vehicular Ad Hoc network. In our work, we are interested to the problem of congestion in the VANETs. We proposed a protocol that is used to detect and control traffic congestion using both vehicle 2 vehicle (V2V) communication and vehicle2 infrastructure (V2I).
Our protocol is based on the adjustment of transmission rate and the adaptation of transmission power after the allocation of priorities for broadcast messages according to their utility, it measured the level of use of the channel (the waiting time of one package, and the number of package). We want to evaluate the performance of our protocol with the NS-2 simulator, but the time factor prevented us from reaching the final results.

Keywords: VANETs, Congestion Control, Priorities and Scheduling, Transmission Rates, transmission power, V2V communication, V2I communication.