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

Mémoire de Master

En Recherche Opérationnelle

Spécialité : Modélisation mathématique et Évaluation des Performances des Réseaux

Thème :

Controle de congestion dans les VANETs

Réalisé par :
M^{r} AREZKI Bachir
M^{elle} ASSAHLI Lynda

Devant le jury composé de :

Présidente	M^{elle}	Nadjette	REBOUH	Université de Béjaia
Promotrice	M^{me}	Samira	OUYAHIA	Université de Béjaia
Examinatrice	M^{me}	Feroudja	ZIDANI	Université de Béjaia

Promotion 2015/2016.

Résumé

Dans nos jours, les réseaux véhiculaires jouent un rôle significatif. C'est un domaine très intéressant pour toutes les sociétés de recherche et d'industrie. En effet, l'objectif de ces réseaux est d'améliorer la sécurité et la sûreté des passagers et de fournir de nombreux services et facilités aux usagers routiers. Cela nécessite une communication fiable et continue sans déconnexion mais ce n'est pas toujours le cas car ces réseaux souffrent parfois du problème de congestion. Dans ce travail, nous nous intéressons au problème de congestion dans les VANETs. De ce fait, on propose un modèle général à base de chaînes de Markov pour le contrôle de congestion. Il se base sur l'adaptation du débit de transmission après l'affectation des priorités et le calcul du taux d'occupation du canal (en se basant sur les acquittements reçus). L'évaluation des performances est faite par les chaînes de Markov (analytiquement) et par simulation.

Mots clés : *VANETs, Contrôle de congestion, Chaînes de Markov, adaptation du débit de transmission, affectation des priorités, taux d'occupation du canal, acquittements.*

Abstract

In these days vehicular networks plays a significant role. This is a very interesting domain for all research organizations and industry. Indeed, the objective of these networks is to improve the safety and the security of passengers and provide many services and facilities to the road users. This requires a reliable and continuous communication without disconnection but this is not always the case because these networks sometimes experience network congestion problems. In this work, we address the problem of congestion in VANETs. Therefore, we propose a general model based on Markov chains for congestion control. It is based on the adaptation of the transmission rate after the allocation of priorities and the calculated channel occupancy rate (based on the acknowledgments received). The Performances evaluation is done by Markov chains (analytically) and with simulation

Key words : *VANETs,congestion control, Markov chains, adaptation of transmission rate, assignment of priorities, rate occupancy of the channel, acknowledgments.*

Remerciements

À l'issu de ce travail, nous tenons à remercier en premier lieu le bon dieu tout puissant qui nous a donné la force de réaliser ce modeste travail.

Nous adressons par la même occasion nos sincères remerciements à nos parents qui ont su parfaitement nous accompagner durant nos études universitaires tant sur le plan matériel, financier que moral. Qu'ils trouvent ici l'assurance de notre totale reconnaissance et notre profonde humilité.

Une mention spéciale à Mme OUYAHIA Samira, notre promotrice, qui grâce à ses connaissances et à l'assistance particulière dont elle nous a fait bénéficier, elle nous a permis d'être rigoureux et méthodiques dans la réalisation de ce mémoire.

Nous remercions énormément M^{elle} REBOUH.Nadjette de nous avoir fait l'honneur de présider notre soutenance.

Nous remercions également Mme ZIDANI Feroudja de nous avoir fait l'honneur en acceptant d'examiner notre travail et faire partie de notre jury.

Nous ne saurons clôturer cette page sans exprimer notre reconnaissance et sympathie à tous ceux qui par leurs critiques, leurs suggestions, leurs obsérvations et leurs conseils ont contribué d'une manière ou d'une autre à la réalisation de ce mémoire.

dédicaces

Je dédie cet humble travail à :

◇ *Mes très chèrs* ***parents*** *pour leur soutien moral et matériel.*

◇ *Ma chère sœur , Fairouz.*

◇ *La mémoire de mes grands-parents.*

◇ *Ma binôme Lynda avec qui je partage ce travaill.*

◇ *Mes amis pour m'avoir aidé à décompresser chaque fois que la pression outrepassée les limites du tolérable.*

A. Bachir

dédicaces

Je dédie ce modeste travaill à mes parents qui mon soutenue, je suis vraiment reconnaissante pour leur amour, compréhension, et leur support inconditionnell.

À mes frères bien aimés MOHAND, KARIM et MASSINISSA qui mont toujours soutenue.

À la mémoire de mes grands-parents.

À mon binôme Bachir avec qui je partage ce travaill.

À ma cousine et toute ma famille et tous mes amies.

A. Lynda

Table des matières

Table des matières **i**

Table des figures **v**

Liste des tableaux **vi**

Introduction générale **3**

1 Généralités sur les VANETs **1**

1.1 Définition d'un réseau VANET 1

1.2 Caractéristiques des VANETs 2

1.2.1 Forte mobilité et topologie du réseau 2

1.2.2 Capacité de traitement, d'énergie et de communication 3

1.2.3 Caractéristiques inhérentes au canal radio 3

1.2.4 Connectivité et partitionnement de réseau 3

1.2.5 L'environnement de déplacement et modèle de mobilité 3

1.2.6 Collecte d'informations 3

1.2.7 Broadcast storm (tempête de diffusion) 4

1.2.8 Qualité de service 4

1.3 Les architectures de communication 4

1.3.1 Communication de véhicule à véhicule (V2V) 4

1.3.2 Communication de véhicule à Infrastructeures(V2I) 6

1.3.3 Communication Hybride 7

1.4 Les technologies utilisées dans la communication véhiculaire 7

1.4.1 Les solutions radio existantes 8
1.4.1.1 WPAN (Wireless Personal Area Network) 8
1.4.1.2 WLAN (Wireless Local Area Network) 9
1.4.1.3 WMAN (Wireless Metropolitan Area Network) 10
1.4.1.4 WWAN (Wireless Wide Area Network) 10
1.4.2 Utilisation de la norme 802.11 pour les communications inter-véhicules 12
1.5 Standards de communication sans fil véhiculaire 13
1.5.1 IEEE 1609.1 13
1.5.2 IEEE 1609.2 15
1.5.3 IEEE 1609.3 15
1.5.4 IEEE 1609.4 et IEEE 802.11p 16
1.6 Applications des réseaux VANETs 18
1.6.1 Application de la prévention et de la sécurité routière 18
1.6.2 Application de gestion de trafic 18
1.6.3 Application de confort et de divertissement 18
1.7 Les contraintes liées aux VANETs 19
1.7.1 Canal radio partagé et limité 19
1.7.2 Faible bande passante 19
1.7.3 Les interférences 19
1.7.4 Tolérance aux pannes 19
1.7.5 La congestion dans les VANETs 19
1.8 Conclusion 20

2 État de l'art sur le problème de congestion dans les VANETs 21

2.1 Introduction 21
2.2 Définition de la congestion 22
2.3 Les méthodes de détection de la congestion dans les VANETs 22
2.3.1 La détection orientée événement 22
2.3.2 La détection à base de mesures 23
2.4 Mécanisme de contrôle de congestion dans les VANETs 23

2.4.1 Architecture cross-layer pour le contrôle de congestion dans les VANETs 23
2.4.2 Contrôle de congestion par la manipulation de files d'attente MAC . . . 25
2.4.2.1 Le gel de file d'attente (Queue freezing) . . . 25
2.4.2.2 Paramètres de QoS adaptatifs . . . 25
2.4.3 Contrôle de congestion via un contrôle de puissance de transmission dynamique . . . 25
2.5 Les stratégies de contrôle de congestion dans les VANETs . . . 26
2.6 Classification des stratégies de contrôle de la congestion basée sur les paramètres et les moyens . . . 27
2.6.1 Stratégie basée sur le débit de transmission . . . 27
2.6.2 Stratégie basée sur la puissance . . . 29
2.6.3 Stratégie basée sur CSMA/CA . . . 30
2.6.4 Stratégie basée sur la priorité et l'ordonnancement . . . 30
2.6.5 Stratégie hybride . . . 31
2.7 Tableau récaputilatif des protocoles étudiés . . . 32
2.8 Conclusion . . . 32

3 Modèle de contrôle de congestion en fonction de la fenêtre de congestion 29
3.1 Introduction . . . 29
3.2 Présentation du modèle de contrôle de congestion . . . 29
3.2.1 Assignement de priorité . . . 32
3.2.2 Calcul de la taille de la fenêtre de congestion . . . 32
3.2.2.1 Définition de la fenêtre de congestion . . . 32
3.2.3 Application des chaînes de Markov . . . 33
3.2.4 Adaptation du débit de transmission . . . 34
3.3 Implémentation du modèle proposé . . . 34
3.3.1 Présentation de NETBEANS . . . 34
3.3.1.1 Valeurs et paramètres utilisés . . . 35
3.3.1.2 Etape 1 : Assignement de priorité . . . 36
3.3.1.3 Etape 2 : Calcul de la taille de la fenêtre de congestion . . . 37
3.3.1.4 Etape 3 : Modélisation par les chaînes de markov . . . 38
3.4 Conclusion . . . 39

Conclusion générale **40**

Bibliographie **42**

Table des figures

1.1 Hiérarchie des réseaux sans fil 2

1.2 Architecture de communication V2V 5

1.3 Architecture de communication V2I 6

1.4 Architecture de communication Hybride 7

1.5 Les solutions radio existantes 12

1.6 Le modèle DSRC/WAVE : IEEE 1609 13

1.7 Modules du standard IEEE 1609.1 14

1.8 Canaux du standard IEEE 802.11p 17

2.1 Architecture Cross-layer pour le contrôle de congestion 24

3.1 Algorithme de contrôle de congestion 30

3.2 Organnigramme du modèle proposé 31

3.3 La taille de la fenêtre de congestion 33

3.4 La chaîne de Markov 34

3.5 Connexion entre les véhicules 36

3.6 Nombre de messages de haute priorité perdus 37

3.7 Nombre de messages de haute priorité perdus après l'assignement de priorité . . 38

3.8 Tableau de changement d'état de la congestion 38

3.9 Le graphe de transition 39

Liste des tableaux

1.1 *Comparaison entre différentes technologies de réseau WPAN* 9

1.2 *Comparaison entre différentes technologies de WLAN* 10

1.3 *Comparaison entre différentes technologies de WWAN* 11

2.1 *Tableau récaputilatif des protocoles étudiés* 33

3.1 *Les paramètres de la simulation* 35

Tableau des abréviations :

Abréviation	Signification
ACK	**ACK**nowledgement
AIFS	**A**rbitrary **I**nter **F**rame **S**pace
AMRC	**A**daptive **M**AC **M**essage **R**ate **C**ontrol
AVOCA	**A** **V**ehicle **O**riented **C**ontrol **C**ongestion **A**lgorithm
BLR	**B**oucle **L**ocal **R**adio
BRR-EPA	**B**roadcast **R**eception **R**ates and **E**ffects of **P**riority **A**ccess
CABS	**C**ontext **A**ware **B**eacon **S**cheduling
CCA	**C**hannel **C**lear **A**ssessment
CCH	**C**ontrol **CH**annel
CDMA	**C**requency **D**oppingMpreadApectrum
CMDI	**C**hannel . **M**onitoring and **D**écision **I**ntervalle
CSMA/CA	**C**arrier **S**ense **M**ultiple **A**ccess/**C**ollision **A**voidance
D-FPAV	**D**istributed- **F**air **P**ower **A**justements for **V**ehicular environments
DBFC	**D**istributed **B**eacon **F**requency **C**ontrol
DPBS	**D**ynamic **P**riority - **B**ased **S**cheduling
DVB-S	**D**igital **V**ideo **B**broadcasting -**S**atellite
FDF	**F**irst **D**eadline **F**irst
FIFO	**F**irst **I**n **F**irst **O**ut
GPRS	**G**eneral **P**acket **R**adio **S**ervice
GSM	**G**lobal **S**ystem for **M**obile communication
HCCA	**H**ybrid **C**ontrolled **C**hannel **A**ccess
IDE	**I**ntégré **D**éveloppement **E**nvironnement
IEEE	**I**nstitute of **E**lectrical and **E**lectronics **E**ngineers
IPCS	**I**ncrémental **P**ower **C**arrier **S**ensing
ITS	**I**ntelligent **T**ransportation **S**ystems
LSF	**L** **S**elected **F**irst
LTSF	**L**ongest **T**otal **S**tretch **F**irst
LWT	**L**ongest **W**ait **T**ime
MAC	**M**edium **A**ccess **C**ontrol
MQIPF	**M**aximum **Q**uality **I**ncrement **F**irst
ODRC	**O**n-**D**emand **R**ate **C**ontrol
OFDM	**O**rthogonal **F**requency **D**ivision **M**ultiplexing
OBU	**O**n- **B**oard **U**nits

PDA	**P**uersonal **D**igital **A**ssistant
QoS	**Q**uality of **S**ervice
QSTA	**M**aximum **R**equest **F**irst
RSU	**R**oad **S**ide**U**nits
SCH	**S**ervice **CH**annels
SDF	**S**mallest **D**ata-size **F**irst
TDMA	**T**ime **D**ivision **M**ultiple **A**ccess
UBPFCC	**U**tility-**B**ased **P**acket **F**orwarding and **C**ongestion **C**ontrol
UMTS	**U**niversal **M**obile **T**elecommunication **S**ystem
V2I	**V**éhicule -à- **I**nfrastructure
V2V	**V**éhicule -à- **V**éhicule
WAVE	**W**ireless **A**bility in **V**ehicular **E**nvironments
Wi-Fi	**Wi**reless **Fi**delity
WLAN	**W**ireless **L**ocal **A**rea **N**etwork
WMAN	**W**ireless **M**etropolitan **A**rea **N**etwork
WME	**W**ave **M**anagement **E**ntity
WPAN	**W**ireless **P**ersonel **A**rea **N**etwork
WWAN	**W**ireless **W**ide **A**rea **N**etwork

Introduction générale

De nos jours, avec le confort et les services que nous offre la possession d'un véhicule, chaque famille possède au moins un véhicule. Cette situation a conduit à une grande augmentation du trafic routier causant de multiples problèmes.

En effet, la circulation en voiture est devenue, dans certaines villes, une épreuve quotidienne à cause des embouteillages qui provoquent du stress, de la pollution, de la perte du temps et d'énergies, etc. Mais le problème le plus important est celui de la sécurité routière (accidents).

Pour résoudre ces problèmes, de nombreuses initiatives ont été prises par les gouvernements, les associations et les constructeurs automobiles. Parmi lesquelles, on trouve l'invention des véhicules intelligents.

Au début des années 1990, les véhicules intelligents sont apparus sous le nom de ITS (Intelligent Transportation Systems). Ils consistent à intégrer les nouvelles technologies de l'information et de la communication afin de rendre le système routier plus efficace et plus sûr en réduisant au maximum le nombre d'accidents. De plus, ces systèmes permettent, aussi, d'offrir de nouveaux services aux usagers des routes en rendant la route plus agréable et plus confortable.

Cette technologie permet aux véhicules équipés de capteurs d'établir des liens et des communications entre eux afin de détecter l'environnement proche et d'avertir les conducteurs des autres véhicules voisins le plutôt possible en cas de risques d'accident, et cela avec ou sans infrastructures installées aux bords des routes. Cet ensemble de véhicules et de technologies constituent les réseaux VANETs (Vehicular Ad-Hoc NETwork), une des applications les plus prometteuses dans le domaine des automobiles.

Les VANETs qui sont une technologie importante et nécessaire pour l'amélioration de notre vie soufrent d'un problème qu'on peut dire handicapant qui est la congestion de réseau. Cette congestion bloque l'envoi des messages et provoque des retards de transmission, cela parfois nous mènera même aux accidents à cause du manque d'informations et de la mauvaise estimation de l'état des routes.

En fait, la majorité des accidents peuvent être évités si les conducteurs sont alertés juste à temps avant la présence de la collision. Dans ce travail, nous visons à étudier comment améliorer la communication entre les véhicules par le contrôle de la congestion.

Notre travail est composé de trois chapitres. Dans le premier chapitre, nous introduisons les réseaux VANETs, leur domaines d'applications et leur contraintes et faiblesses.

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

Enfin, dans le dernier chapitre, nous étudions et évaluons l'impact de l'utilisation de la fenêtre de congestion pour l'adaptation du débit de transmission pour contrôler la congestion dans les VANETs par l'utilisation des chaines de markov. Nous implémentons cette solution avec le langage JAVA et nous présentons les résultats à la fin du chapitre.

Nous cloturons ce mémoire par une conclusion et quelques perspectives.

1

Généralités sur les VANETs

Notre mémoire s'intéresse au contrôle de congestion dans les réseaux VANETs. Dans ce chapitre, nous allons introduire les réseaux VANETs et éclairer un peu sur ce vaste domaine. Ce chapitre est composé de Cinq sections qui sont organisées de sorte que nous commençions par donner une définition d'un réseau VANET, ensuite dans la section 1.2 et 1.3 nous introduisons les caractéristiques et les architectures de communication de ces réseaux. Dans 1.4 et 1.5, nous présentons les solutions radio existantes et les domaines d'application de ces réseaux. Enfin, pour conclure et ouvrir un passage vers le deuxième chapitre, nous terminons par donner les contraintes liées aux VANETs parmi lesquelles, on trouve la congestion des réseaux.

1.1 Définition d'un réseau VANET

Dans les réseaux sans fil, on trouve plusieurs sous ensembles de réseaux, dont on cite les réseaux Ad Hoc mobiles(MANETs) et parmi les cas particuliers de MANETs on trouve les VANETs (Vehicular Ad-Hoc NETworks). La figure FIG 1.1, nous présente la hiérarchie des réseaux sans fil. Les réseaux véhiculaires (VANETs) sont une projection des systèmes de transport intelligents (Intelligent Transportation Systems -ITS) équipés de calculateurs, de périphériques réseaux et de différents types de capteurs. Ils permettent d'établir des communications entre

véhicules ou bien avec une infrastructure située aux bords des routes afin d'offrir les services suivants[1] :

- *Une conduite collaborative sécurisée :* transmission des messages d'urgence (freinage, collision, danger quelconque, etc.)
- *Une conduite plus conviviale et confortable pour le conducteur et ses passagers :* partage de contenu, publicité, tourisme et internet.
- *Une centrale d'informations sur l'état de l'environnement dans lequel évolue le véhicule :* état de la route, informations sur l'environnement (place de parking, embouteillages).
- *Un environnement de conduite plus optimisé :* allumage automatique de l'éclairage sur les routes quand il y a du trafic .

FIG. 1.1 – Hiérarchie des réseaux sans fil

1.2 Caractéristiques des VANETs

Les VANETs se distinguent des MANETs par un certain nombre de caractéristiques spécifiques dont on peut citer :

1.2.1 Forte mobilité et topologie du réseau

C'est le facteur qui rend les réseaux véhiculaires différents par rapport aux autres réseaux sans fil. La vitesse d'un véhicule varie selon l'environnent et selon les informations reçues par le conducteur, ce qui cause un changement de la topologie du réseau. Par exemple sur l'autoroute, la vitesse peut atteindre 120 Km/h, ceci a une grande influence sur la qualité et la durée de vie

des communications entre les véhicules suite au changement rapide de topologie causé par la mobilité des véhicules[3].

1.2.2 Capacité de traitement, d'énergie et de communication

Dans les réseaux ad hoc mobiles, on est toujours confronté au problème d'énergie car les ressources d'énergie sont limitées (batteries). Par contre dans un réseau VANET, les véhicules ne souffrent pas de ce problème vue qu'ils n'ont pas de limite en terme d'énergie et ils disposent d'une grande capacité de traitement. Ils peuvent aussi avoir plusieurs interfaces de communication : Wifi, Bluetooth, etc[4].

1.2.3 Caractéristiques inhérentes au canal radio

Auparavant, dans les MANETs, les échanges de données se font dans la plupart des cas dans un environnement libre sans obstacles ou dans des espaces externes fermés. Les communications dans les réseaux véhiculaires s'éffuctuent dans des conditions défavorables pour l'éttablissement des liens radio à cause de nombreux obstacles, surtout en zones urbaines. Parmis ces obstacles, nous citons les forêts, les montagnes, les batiments, etc. Ces obstacles ont comme conséquence une grande dégradation de la qualité de la puissance des signaux [3].

1.2.4 Connectivité et partitionnement de réseau

Le changement rapide de la topologie du réseau et la forte mobilité des véhicules causent la disparition de certains chemins et ainsi, le partitionnement du réseau peut souvent survenir [1]

1.2.5 L'environnement de déplacement et modèle de mobilité

Les véhicules se deplacent aléatoirement dans le réseau MANET, alors que dans le réseau VANET les déplacements des véhicules sont dépendants des infrastructures routières (limitation de vitesse, ronds-points, carrefours, etc.).

1.2.6 Collecte d'informations

La collecte d'informations se fait en utilisant différents capteurs de toutes catégories (caméras, capteurs de pollution, capteurs de pluies, capteurs de l'état de la route et de voiture, etc.) qui permettent au conducteur à bord, de son véhicule de disposer d'un certain nombre d'informations et d'une meilleure visibilité pour pouvoir réagir d'une manière adéquate aux changements de son environnement proche.

1.2.7 Broadcast storm (tempête de diffusion)

L'epineux problème du broadcast storm a été considéré depuis longtemps dans les réseaux MANET et multiples solutions ont été proposées. Ce problème se pose en particulier dans les protocoles de routage qui inondent le réseau avec les paquets de contrôle à la recherche de routes. Les retransmissions successives des paquets causent de sérieuses redondances qui saturent le réseau. Dans le cas des réseaux véhiculaires, le problème du broadcast storm se pose également au niveau application. En effet, les principaux services proposés pour les réseaux véhiculaires sont des services de sécurité qui se basent presque exclusivement sur les retransmissions de proche en proche des données. De plus, le problème du broadcast storm est aggravé dans les réseaux à forte densité notamment dans des scénarios tels les embouteillages et les files d'attente aux intersections[4].

1.2.8 Qualité de service

La demande en qualité de service dépend des applications supportées. La principale contrainte des applications de sécurité est la latence. La validité des informations étant limitée dans le temps, les messages doivent parvenir à destination dans des délais courts pour être considérés comme pertinents. Dans le cas des applications de gestion de trafic, il s'agit essentiellement de la définition d'algorithmes d'agrégation des données qui permettent d'inclure autant d'informations de trafic que possible dans les paquets diffusés[6].

1.3 Les architectures de communication

L'architecture des VANETs peut être divisée en trois modes de communication, les communications Véhicule-à-Véhicule (V2V), les communications Véhicule-à-Infrastructure (V2I) et hybride. Dans cette section, nous présentons le principe de chaque mode.

1.3.1 Communication de véhicule à véhicule (V2V)

La communication de véhicule à véhicule se deroule suivant un mode décentralisé. Les VANETs sont basés sur la communication inter-véhicules sans utilisation d'infrastructures. En effet, un véhicule peut communiquer directement avec un autre véhicule s'il se situe dans sa zone radio, ou bien à l'aide d'un protocole multi-sauts, ou ses derniers se chargent de transmettre les messages de bout en bout en utilisant les véhicules voisins qui les séparent comme des relais. Dans ce mode, les supports de communication utilisés sont caractérisés par une petite latence et un grand débit de transmission. Les communications V2V sont très efficaces pour

le transfert des informations concernant les services liés à la sécurité routière, mais elles ne garantissent pas une connectivité permanente entre les véhicules[7]. La figure FIG 1.2 nous présente l'architecture de communication V2V.

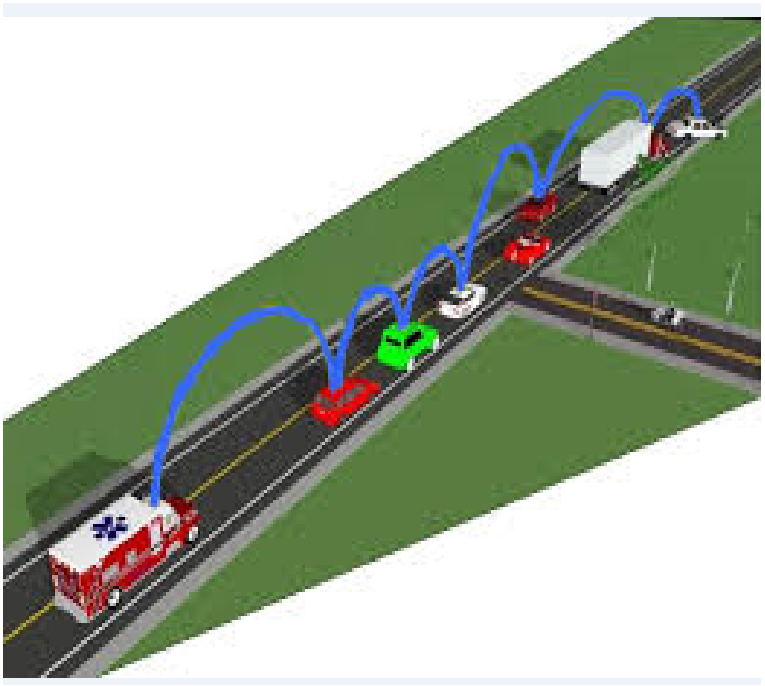

FIG. 1.2 – Architecture de communication V2V

1.3.2 Communication de véhicule à Infrastructeures(V2I)

Dans ce mode de communication, les véhicules se connectent à des stations fixes pour acquérir ou transmettre l'information. Cette sorte de communication favorise l'utilisation des ressources partagées et multiplie les services fournis comme (accès à Internet, échange de données de voiture-à-domicile, communications de voiture-à-garage de réparation pour le diagnostique distant, etc.). Les points d'accès connus sous le nom RSU (Road Side Units) ou bien (Unités Latérales de la Route) se situent aux bords des routes (les feux tricolores, les intersections, les stops, etc.) et qui ont pour rôle l'amelioration de la conduite pour une securité routière. La figure Fig 1.3 nous présente l'architecture de communication V2I.

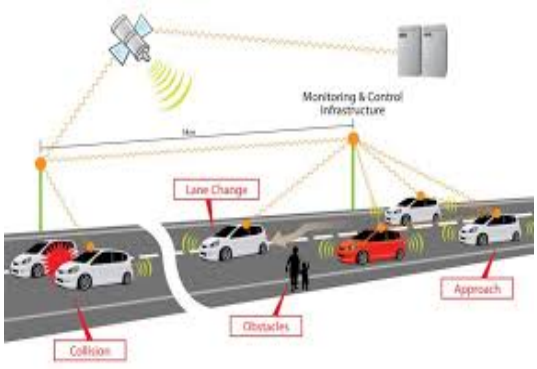

FIG. 1.3 – Architecture de communication V2I

1.3.3 Communication Hybride

Ce mode de communication combine entre (V2V) et (V2I) pour rendre plus vaste la zone de communication et dans un but economique pour minimiser le budjet concernant l'installation des infrastructures.

La figure FIG 1.4 nous présente l'architecture de communication hybride.

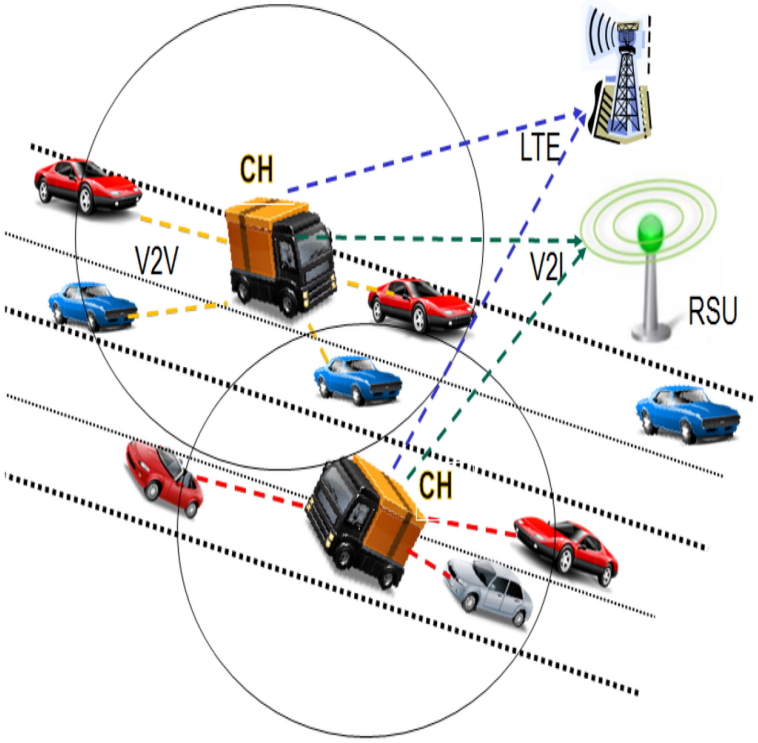

FIG. 1.4 – Architecture de communication Hybride

1.4 Les technologies utilisées dans la communication véhiculaire

Dans cette partie, nous allons présenter les technologies de communication qui existent dans les réseaux VANETs et les différents moyens de les mettre en œuvre.

Dans un premier temps, nous nous attachons donc à présenter les différentes solutions radio existantes avec leurs caractéristiques. Ensuite, dans un deuxième temps, nous explicitons un choix possible de technologie de communication pour les réseaux de véhicules.

1.4.1 Les solutions radio existantes

Un système de communication comprend tous les éléments capables de véhiculer de l'information (son, données informatiques, vidéo, etc.) d'une source vers une ou plusieurs destinations. Depuis la naissance des réseaux sans fil, les communications sont passées de la communication analogique filaire vers une communication numérique sans fil. De nombreuses techniques existent pour échanger de l'information par liaison radio qui sont classées suivant leur débit et leur portée.

1.4.1.1 WPAN (Wireless Personal Area Network)

Les réseaux sans fil personnels ou WPAN (appelés également réseaux individuels sans fil ou réseaux domestiques sans fil) sont caractérisés par :

- Communication à courte portée (de l'ordre de quelques dizaines de mètres).
- Basse consommation énergétique.
- À bas prix.
- Petits réseaux personnels.
- Communication des appareils au sein d'un espace personnel.

Ils sont le plus souvent utilisés dans le cadre de l'informatique vestimentaire (ou Wearable Computing) qui consiste à faire communiquer entre eux des matériels présents sur une personne (par exemple une oreillette et un téléphone portable). Ils sont, également, utilisés pour relier des équipements informatiques entre eux : par exemple pour relier une imprimante ou un assistant personnel PDA (Personal Digital Assistant) à un ordinateur de bureau. Plusieurs technologies sont utilisées pour les WPAN dont on trouve le IEEE 802.15.1 [5] ou bluetooth, HomeRF, ZigBee et infrarouge. La principale technologie utilisée est le Bluetooth. Elle fut proposée par Ericsson en 1994 et fournit un débit de transmission radio théorique de 1 Mbit/s pour une portée maximale d'une trentaine de mètres.

Ci dessous un tableau TAB 1.2 qui résume toutes ces technologies :

Technologie	**Norme**	**Débit théorique**	**Portée (m)**	**Bande de fréquence (GHz)**	**Observation**
Bluetooth	IEEE 802.15.1	1 Mbits/s	Une trentaine	2,4 - 2,4835	-Bas prix -L'émission de puissance dépend de la réglementation
HomeRF	Consortium (Intel,HP, siemens Motorola)	10 Mbits/s	50	2,4-2,4835	-Permet de relier des PC portables, fixes et d'autres terminaux.
ZigBee	IEEE 802.15.4	20 - 250 kbits/s	100	2,4-2,4835	-Très bas prix,

TAB. 1.1 – *Comparaison entre différentes technologies de réseau WPAN*

1.4.1.2 WLAN (Wireless Local Area Network)

Le réseau local sans fil (WLAN) est un réseau permettant de couvrir l'équivalent d'un réseau local d'entreprise, soit une portée d'environ une centaine de mètres. Il permet de relier entre-eux les terminaux présents dans la zone de couverture. Il existe plusieurs technologies concurrentes qui sont :

- Le Wifi (ou IEEE 802.11)
- hiperLAN2 (High Performance Radio LAN 2.0)

Ils font le pont entre la téléphonie et l'informatique et possèdent de nombreux avantages :

- Ils permettent de rendre mobiles les équipements informatiques.
- Ils autorisent des débits compatibles avec les applications informatiques actuelles.
- Ils utilisent des bandes de fréquences libres de droit d'utilisation.
- Ils ne nécessitent que peu ou pas d'infrastructure.
- Ils ont une mise en œuvre aisée.

Il faut, malgré tout, pondérer tous ces avantages par le fait que les communications radio sont moins fiables que les filaires à cause des interférences radio, des problèmes de multi-trajets des ondes, des irrégularités électromagnétiques, etc. De plus, les WLANs sont moins sûrs que les réseaux filaires.

Ci dessous un tableau TAB 1.2 qui résume les technologies de WLAN :

Technologie	**Norme**	**Débit théorique (Mbits/s)**	**Portée (m)**	**Bande de fréquence (GHz)**	**Observation**
Wifi	IEEE 802.11	2 - 54	35 -50 (indoor) des centaines (outdoor)	2,4 - 2,4835 5	-Elle comporte plusieurs déclinaisons IEEE 802.11 a/b/g
- *HiperLAN 1* - *HiperLAN 2*	ETSI	19 - 20 25	50 200	5	- La vitesse de déplacement de l'utilisateur ne peut excéder 10 m/s - accès aux réseaux ATM
HiperLINK 2	ETSI	155	150 - 200	17,2 - 17,3	-Permet des liaisons fixes entre 2 points
DECT	ETSI	2	300	1880 - 1900 MHz	-Technique d'accès TDMA

TAB. 1.2 – *Comparaison entre différentes technologies de WLAN*

1.4.1.3 WMAN (Wireless Metropolitan Area Network)

Les réseaux métropolitains sans fil ou WMAN, est également connu sous le nom de boucle locale radio (BLR), étaient à l'origine prévus pour interconnecter des zones géographiques difficiles d'accès à l'aide d'un réseau sans fil. Actuellement, ces réseaux sont utilisés dans certaines villes américaines (San Francisco) pour fournir un accès Internet aux habitants. Les réseaux basés sur la technologie IEEE 802.16 ont une portée de l'ordre de plusieurs dizaines de kilomètres (50 kms de portée théorique annoncée) et un débit de transmission radio théorique pouvant atteindre 74 Mbit/s pour IEEE 802.16-2004 [13] plus connue sous le nom commercial de WiMAX. C'est également dans cette catégorie que peuvent être classés les réseaux téléphoniques de la troisième génération utilisant la norme UMTS (Universal Mobile Telecommunication System) pour transmettre de la voix et des données. Cette norme UMTS propose des débits de transmission radio théoriques pouvant aller jusqu'à 2 Mbit/s sur des distances de plusieurs kilomètres [4].

1.4.1.4 WWAN (Wireless Wide Area Network)

Les réseaux sans fil étendus ou WWAN regroupent notamment les différents réseaux cellulaires de première et deuxième génération mais également les réseaux satellitaires. Les réseaux cellulaires téléphoniques reposent sur des technologies comme GSM (Global System for Mobile

Communication) et GPRS (General Packet Radio Service). Les réseaux satellites s'appuient quant à eux sur les normes comme DVB-S (Digital Video Broadcasting-Satellite) pour transmettre l'information et proposent des débits élevés (de l'ordre de 40 Mbit/s pour la norme DVB-S).

Ci dessous un tableau TAB 1.3 qui résume les technologies de WWAN :

Technologie	**Norme**	**Débit**	**Portée (km)**	**Bande de fréquence**	**Observation**
GSM	Européenne	9.6 Kbits/s	0.3 - 30	[890-915] MHz [935-960] MHz [1710-1785] MHz [1805-1880] MHz	-Utilise une commutation de circuits -Système très sécurisé
GPRS	Européenne	$\leqq$ 120 kbits/s	0.3 - 30	[890-915] MHz [935-960] MHz [1710-1785]MHz [1805-1880]MHz	Utilise une commutation de paquets Prise en charge des applications de données à moyens débits
UMTS	Européenne (ETSI)	$\leqq$ 2 Mbits/s	0.3 - 30	2 GHz	Offre un accès à Internet et à ses serveurs web Supporte des applications audio et vidéo basse définition Fonctionne en mode paquet et circuit
CDMA 2000	Américaine (TIA)	$\leqq$ 2 Mbits/s		2 GHz	-Utilise la technique d'étalement de bande
EDGE	Européenne	59.2 kbits/s	0.3 - 30	2 GHz	-Utilise la commutation de circuit
IS 95	Américaine	1,2288 Mbits/s		[800-900] MHz [1800-1900] MHz	Utilise la technologie CDMA

TAB. 1.3 – *Comparaison entre différentes technologies de WWAN*

La figure FIG 1.5 montre les solutions radio existantes

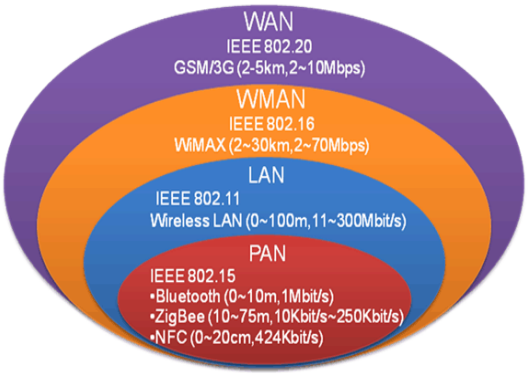

FIG. 1.5 – Les solutions radio existantes

1.4.2 Utilisation de la norme 802.11 pour les communications inter-véhicules

La norme IEEE 802.11 [11] est un standard international décrivant les caractéristiques d'un réseau local sans fil (WLAN). La norme IEEE 802.11 est en réalité la norme initiale offrant des débits de 1 ou 2 Mbps. Des révisions ont été apportées à la norme originale afin d'optimiser le débit (c'est le cas des normes 802.11a, 802.11b, 802.11g et 802.11p [12], appelées normes 802.11 physiques) ou bien préciser des éléments afin d'assurer une meilleure sécurité ou une meilleure interopérabilité. Par rapport au modèle OSI, le IEEE 802.11 ne concerne qu'une partie de la couche de liaison de données 2 et la couche physique 1 et reste donc entièrement compatible avec les couches supérieures (dans le but de valider le choix de la norme IEEE 802.11, nous avons procédé à de nombreux tests en condition réelle dans des véhicules. Lors de ces expérimentations, nous avons utilisé des véhicules équipés d'un kit composé d'un PC portable, d'un récepteur GPS, d'une carte IEEE 802.11b et d'une antenne externe. Cette plateforme de tests nous a permis d'effectuer des tests mettant en place des réseaux allant de deux à six véhicules. Ces expériences nous ont permis d'évaluer les performances de la norme ainsi que de comprendre les problèmes qui surviennent lors de la communication inter véhicules. Les premiers résultats obtenus lors de ces tests sont encourageants. En particulier, ils montrent la bonne performance de la norme 802.11 avec des pertes ou des délais relativement faibles. Nous avons également constaté que la distance est un facteur de perte alors que la vitesse et l'accélération ne sont que peu influentes sur la communication. Les résultats expérimentaux ont révélé aussi la faisabilité du réseau ad hoc pour étendre la zone de couverture des points d'accès).

1.5 Standards de communication sans fil véhiculaire

L'IEEE a étendu sa famille de protocoles 802.11 en ajoutant le 802.11p, s'inspirant pour cela du standard ASTM E2213-03 [29], lui-même basé sur le 802.11a [28]. Ce protocole modifie la couche physique et la couche MAC pour s'adapter aux réseaux de véhicules, en conformité avec la bande DSRC. En complément, l'IEEE a défini la famille de protocoles 1609, dite WAVE, pour l'accès sans fil dans les réseaux de véhicules. Ce standard, structuré en quatre composantes (1609.1 à 1609.4), définit l'architecture, le modèle de communication, la structure de gestion, la sûreté et l'accès physique. Comme l'illustre la figure 1-4, 802.11p et WAVE spécifient une pile protocolaire complète. Le modèle DSRC/WAVE utilise deux piles. Une pile pour les applications de sécurité routière et une plus ■ classique ■ pour les deux autres catégories d'applications.

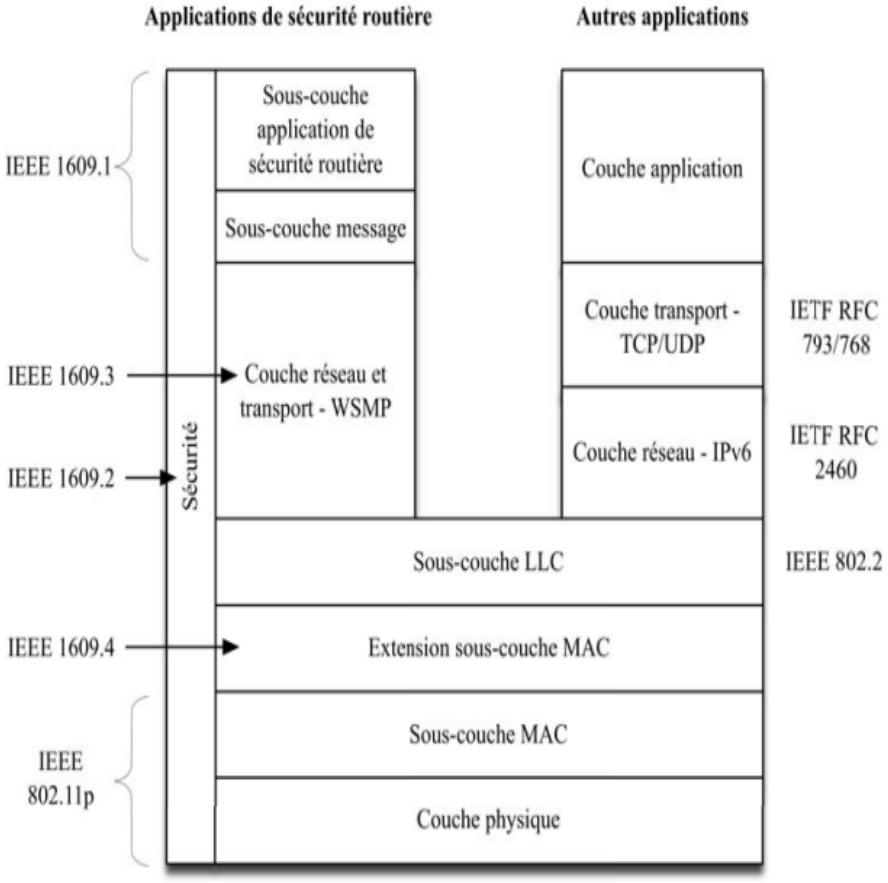

FIG. 1.6 – Le modèle DSRC/WAVE : IEEE 1609

1.5.1 IEEE 1609.1

Le standard IEEE 1609.1 se positionne au niveau de la couche application et définit les formats de messages et le mode de stockage des données utilisées par la couche application. Ce

standard définit un gestionnaire de ressources qui autorise des applications de l'équipement de bord de route (RSU) à communiquer avec les On-Board Units (OBU) des véhicules à proximité. Il décrit trois composants de la couche application qui seront inclus dans un OBU :

- *Resource Manager Applications (RMA) :* Entité distante qui utilise le RM pour communiquer avec le RCP.
- *Resource Manager (RM) :* Le gestionnaire des ressources relaie le message du RMA vers le RCP. Le RM assure les services qui permettent au RMA de contrôler les interfaces présentes dans l'OBU.
- *Resource Command Processor (RCP) :*Il exécute les commandes données par le RMA et fournit une réponse au RMA via le RM.

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

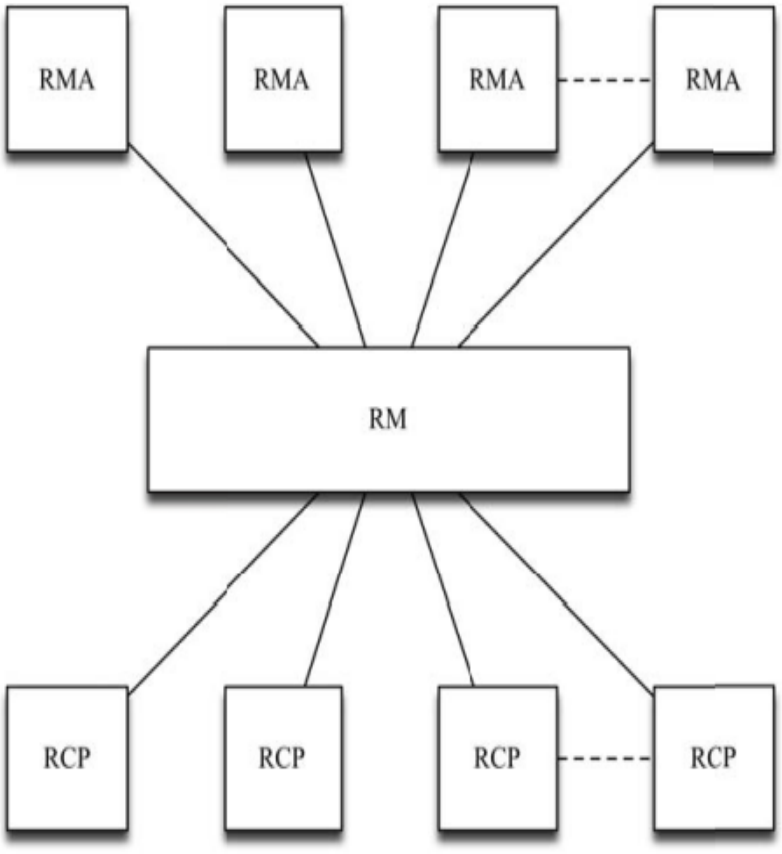

FIG. 1.7 – Modules du standard IEEE 1609.1

1.5.2 IEEE 1609.2

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

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

1.5.3 IEEE 1609.3

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

D'après la Figure 1-4, la couche réseau utilise le protocole IPv6 pour ses caractéristiques de mobilité, de qualité de service et son espace d'adressage important. En effet, cette dernière caractéristique est primordiale dans un système avec plus de 500 millions de véhicules dans le monde. Le protocole IPv6 est utilisé pour les applications financières par exemple. D'un autre côté, le protocole WSMP est présenté comme une alternative à IPv6 [30]. Dans WSMP, les messages sont routés avec un identifiant de classe d'application (Application Class IDentifier, ACID) et une marque de contexte applicatif (Application Context Mark, ACM) en lieu et place de l'adresse IP et de l'identificateur de flux (flow label). Le WSMP permet aussi le contrôle de la puissance de transmission, du canal et du débit. Les applications de sécurité routière comme l'alerte de danger local (LDW) utilisent le WSMP car elles nécessitent une latence faible.

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

1.5.4 IEEE 1609.4 et IEEE 802.11p

Le standard IEEE 802.11p définit la couche physique du système DSRC. La technologie DSRC est définie dans la bande de fréquence des 5.9 GHz sur une largeur de bande totale de 75 MHz (5.850 GHz – 5.925 GHz). Comme illustrée par la figure 1-6, cette largeur de bande est segmentée en 7 canaux de 10 MHz chacun. Ces canaux se répartissant fonctionnellement en 1 canal de contrôle (CCH) et 6 canaux de service (SCH), chacun pouvant offrir des débits allant de 6 à 27 Mbit/s. Optionnellement, des canaux peuvent être configurés sur une largeur de bande de 20 MHz, ce qui permet d'obtenir des débits pouvant aller jusqu'à 54 Mbit/s. La portée de transmission d'un système DSRC peut atteindre les 1000 mètres.

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

- Le canal de rendez-vous est un canal que chaque équipement doit consulter à intervalle régulier. Le canal de contrôle (CCH) est le canal de rendez-vous du standard IEEE 1609.4. Les autres canaux sont des canaux de services (SCH). Le canal de contrôle est notamment réservé à la transmission des messages de gestion du réseau (basculement entre canaux, annonces de services, etc.).
- Le concept de répartition dans le temps suppose que tous les équipements ont accès à une source commune de temps afin d'être synchronisés. Cette source de temps est disponible dans des systèmes globaux de positionnement comme le GPS (cf. §1.3.4). En l'absence de récepteur GPS, un équipement peut être synchronisé en recevant des signaux de temps depuis un autre équipement. Une fois les OBU synchronisés, l'IEEE 1609.4 impose un ordonnancement entre le CCH et les SCH afin d'assurer un service garanti aux applications de sécurité routière et un service minimum aux autres types d'applications.

Le standard IEEE 1609.4 a une forte relation avec le mécanisme EDCA de la sous-couche MAC. EDCA (Enhanced Distributed Channel Access) est basé sur CSMA/CA et est utilisé dans les réseaux WiFi supportant le standard IEEE 802.11e. EDCA assure un accès au support distribué et différencié en utilisant huit niveaux de priorité utilisateurs pour quatre catégories d'accès (Voix, Video, Best Effort, Background). Ce mécanisme permet ainsi d'attribuer une priorité à chaque message. Par exemple, un message d'application de sécurité du trafic routier aura une priorité supérieure à celle d'un message d'application de confort [27].

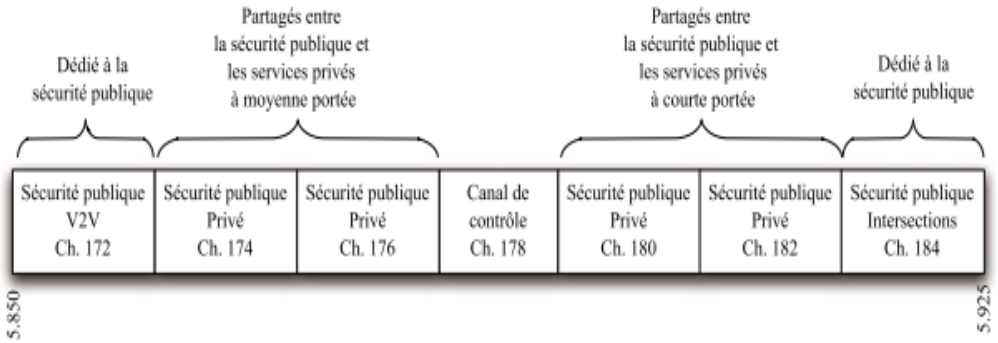

FIG. 1.8 – Canaux du standard IEEE 802.11p

1.6 Applications des réseaux VANETs

Il existe de nombreuses applications pour ces VANETs, et elle peuvent être classées en trois catégories générales[8].

1.6.1 Application de la prévention et de la sécurité routière

La sécurité routière est devenue une priorité dans la plupart des pays développés, Cette priorité est motivée par le nombre croissant d'accidents sur ses routes associés à un parc de véhicules de plus en plus important. Les VANET permettent de prévenir les collisions et les travaux sur les routes, de détecter les obstacles (fixes ou mobiles) et de distribuer les informations météorologiques par l'envoi de messages d'alerte et de sécurité. A titre d'exemple, alerter un conducteur en cas d'accidents, permet d'avertir les véhicules qui se dirigent vers le lieu de l'accident que les conditions de circulation se trouvent modifiées et qu'il est nécessaire de redoubler la vigilance. Les messages d'alerte doivent être de tailles réduites pour être transmis le plus rapidement possible et doivent être émis à des périodes régulières.

1.6.2 Application de gestion de trafic

Les applications de gestion de trafic sont orientées vers l'amélioration des conditions de circulation dans le but de réduire les embouteillages et les risques d'accidents. Elles permet aux conducteurs d'accéder aux informations leur permettant de connaitre l'etat de la route et 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, etc.

1.6.3 Application de confort et de divertissement

Les applications de confort ou de divertissement dont l'objectif est de rendre les voyages plus agréables en permettant aux passagers de communiquer soit avec d'autres véhicules ou avec des stations fixes comme l'accès à internet, la messagerie, le chat inter – véhicule, etc. Les passagers dans la voiture peuvent jouer en réseau, télécharger des fichiers MP3, envoyer des cartes à des amis, etc.

1.7 Les contraintes liées aux VANETs

Bien que les réseaux VANETs sont considérés comme étant le moyen le plus efficace pour éviter les emboutilliages, minimiser la consommation de carburant et réduire le temps passé sur les routes, on trouve plusieurs contraintes dans ces réseaux dont on peut citer :

1.7.1 Canal radio partagé et limité

Un canal radio à fréquences précises est utilisé par tous les nœuds, le flux d'information est donc limité et le débit de transmission diminue surtout dans les centres villes.

1.7.2 Faible bande passante

Le partage du canal limite la bande passante dont dispose chaque véhicule pour partager les informations.

1.7.3 Les interférences

Les réseaux VANETs utilisent les transmissions radio pour transmettre l'information, ce qui rend les communications exposées aux interférences radio. Ces dernières sont de nature diverse comme : le rapprochement des fréquences d'émission (interférences entre deux véhicules), les bruits de l'environnement (équipements électriques, moteurs, etc.), et les phénomènes de réflexion, atténuation et dispersion qui déforment le signal. Ces interférences font augmenter le taux d'erreurs de transmission d'un message, et le rendent incompréhensible par le récepteur [2].

1.7.4 Tolérance aux pannes

La tolérance aux pannes est un mécanisme permettant d'assurer le bon fonctionnement du système et de remplir les spécifications requises malgré la présence de dysfonctionnement dans ses composants [9].

1.7.5 La congestion dans les VANETs

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.

Par définition, cette capacité correspond au nombre d'usagers par unité de temps qui transitent en un lieu déterminé.

les véhicules intelligents sont dotés de capteurs permettant la communication permanente entre eux, ce qui veut dire que la congestion du trafic routier provoque une congestion dans le réseau de communication des véhicules et peut même être saturé. C'est ce qu'on appelle la congestion dans les réseaux véhiculaires. Cette congestion peut provoquer la perte ou bien le retard des paquets ; elle conduit aussi à un gaspillage de la bande passante et un taux d'erreurs élevé des paquets de données lors de leur réceptions [10].

1.8 Conclusion

Dans ce chapitre, nous avons présenté des généralités sur les réseaux Vanets (définition, standards, contraintes, etc.).

Le chapitre suivant sera consacré aux protocoles de congestion dans les Vanets.

2

État de l'art sur le problème de congestion dans les VANETs

2.1 Introduction

Dans le premier chapitre, nous avons défini les réseaux véhiculaires et nous avons éclairé quelques points sur leur caractéristiques, architectures, applications, etc. A l'apparition des réseaux véhiculaires et avec leur adaptations dans les véhicules intelligents, la route devient de plus en plus sécurisée mais le problème de congestion de réseau peut survenir à n'importe quel moment [18]. Les congestions se forment lorsqu'un équipement du réseau est incapable d'absorber le flot de données entrant. Pour éviter ou contrôler les congestions, plusieurs mécanismes peuvent être mis en place à différents niveaux :

Au niveau de la source : le contrôle à la source interdirait que de nouvelles connexions s'établissent sur un chemin déjà saturé.

Au niveau du réseau : l'équilibrage de la charge du réseau permettrait aux routeurs de détourner certains paquets afin qu'ils évitent la saturation d'une portion du réseau.

Au niveau des routeurs : les routeurs pourront privilégier certains flots, et détruire préventivement des paquets provenant de flots ayant tendance à congestionner le réseau.

Dans ce chapitre, nous commencerons par définir la congestion (routière et de réseau), puis, nous présenterons les différents mécanismes et stratégies (apprcohes)de contrôle de la congestion des VANETs et nous terminerons le chapitre par une comparaison entre ces approches.

2.2 Définition de la congestion

La congestion est un phénomène physique concernant la façon dont les véhicules empêchent la progression des uns et des autres au fur à mesure que la demande d'un espace routier s'approche de la capacité maximale de celui-ci, de même qu'un phénomène relatif ayant impact sur les attentes des usagers vis-à-vis des performances d'un réseau routier. 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. Cette définition identifie la caractéristique centrale de la congestion. Cependant, elle laisse beaucoup à désirer en tant que définition opérationnelle puisqu'elle n'offre que peu d'aperçus des éléments multiples, complexes et communicants entre eux, qui aboutissent à cette incohérence entre l'offre et la demande.

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. Une liaison réseau saturée est une liaison qui doit transmettre plus de trames que ne le permet son support physique. Divers algorithmes empêchent la congestion du trafic en établissant des contrôles sur les systèmes d'envoi de messages.

2.3 Les méthodes de détection de la congestion dans les VANETs

Dans les VANETs, la détection de la congestion peut être réalisée en utilisant l'une des deux types de méthodes :" détection orientée événement (event-driven detection) " et " détection basée sur des mesures (measurement-based detection) ".

2.3.1 La détection orientée événement

La méthode de détection orientée événement surveille les applications de sécurité et décide de lancer le contrôle de congestion quand un message de sécurité d'une priorité élevée est détecté. Par exemple, quand un nœud 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 nœud, il lance immédiatement le contrôle de congestion pour garantir la qualité de service des applications de sécurité [19].

2.3.2 La détection à base de mesures

Les méthodes de détection, basées sur les mesures, détectent la congestion en vérifiant périodiquement le canal et en mesurant quelques paramètres tels que le nombre de messages dans les files, le temps d'occupation du canal et le niveau d'utilisation du canal. Les valeurs de ces paramètres sont comparées avec des seuils prédéfinis pour prendre la décision de 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 considère qu'il y a une congestion dans le réseau. Ainsi, le nœud détecté contrôle la congestion par réduire le débit de transmission. Cependant, dans un autre travail, chaque nœud mesure, localement, le temps d'occupation du canal de son CCH (Control Channel). Quand ce temps dépasse le seuil, le nœud bloque la trasmission des messages beacon (les messages périodiques) pour contrôler la congestion. la congestion peut être détectée 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 [21].

2.4 Mécanisme de contrôle de congestion dans les VANETs

Plusieurs mécanismes peuvent être mis en place pour contrôler la congestion dans les VANETs dont on peut citer :

2.4.1 Architecture cross-layer pour le contrôle de congestion dans les VANETs

Les approches concrètes de contrôle de congestion sont intégrées au niveau de chaque couche de la pile protocolaire, comme le montre la figure FIG 2.1 de [24] :

- ***Couche d'application :*** la retransmission contraintes de messages basée sur l'application peut aider à réduire la charge du trafic et de la congestion.
- ***Couche Réseau :*** les algorithmes de routage de retransmission intelligents et effectifs sont utiles pour atténuer le problème de la congestion en limitant le trafic expédié.

- ***Couche MAC :*** la différenciation de la priorité au niveau de la couche MAC est l'approche principale pour résoudre le problème de la congestion dans les VANETs.
- ***Couche Physique :*** utilise les fonctions de détection et de mesure du canal, par exemple le Channel Clear Assessment (CCA) de l'IEEE 802.11 peut contribuer à la détection de la congestion.
- ***Channel :*** la conception de canaux dédiés pour différentes applications, comme l'architecture CCH / SCH de WAVE, facilite la différenciation de priorité entre les applications de sécurité et applications qui ne sont pas de sécurité. Cependant, CCH en WAVE est encore utilisé par les applications de multiples priorités.

  Dans ce travail, nous nous concentrons sur la couche MAC, et nous présentons les méthodes de détection de la congestion ainsi que deux approches de contrôle de congestion [24].

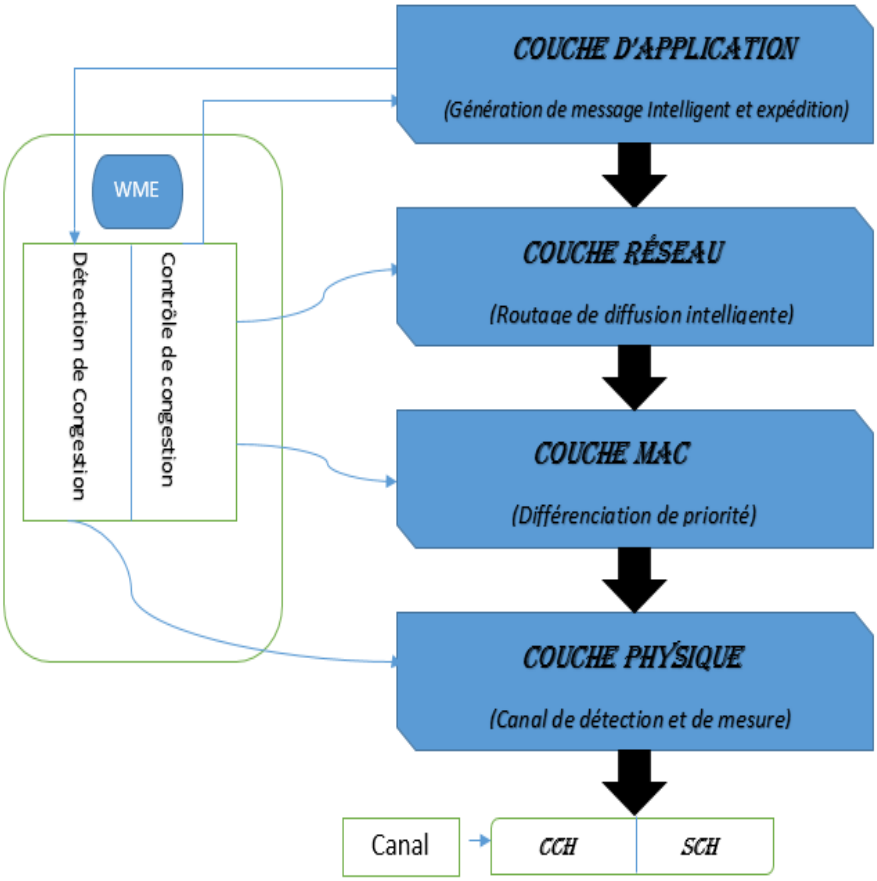

FIG. 2.1 – Architecture Cross-layer pour le contrôle de congestion

2.4.2 Contrôle de congestion par la manipulation de files d'attente MAC

L'idée principale est d'affecter la priorité absolue au message de sécurité sur le reste du trafic par la manipulation des files d'attente, du trafic de priorité inférieure, des transmissions MAC, ou de réserver dynamiquement une fraction de la bande passante pour le trafic de priorité la plus élevée avec des paramètres de qualité de service adaptatifs. Les priorités d'accès aux canaux sont statiquement différenciées par les paramètres de qualité de service associés à chaque file d'attente. Selon le schéma WAVE MAC, la plus courte valeur AIFS et la plus petite taille de la fenêtre de contention peuvent statistiquement fournir une probabilité plus élevée d'accès au canal pour le trafic qui leur est assigné.

Deux approches de contrôle de congestion basées sur la manipulation de files d'attente MAC sont envisagées :

2.4.2.1 Le gel de file d'attente (Queue freezing)

Lors de la détection du message de sécurité avec la méthode de détection orientée événement, chaque nœud applique une force brutale pour le gel de toutes les files d'attente de transmission MAC, sauf pour la file d'attente de sécurité avec la plus haute priorité.

2.4.2.2 Paramètres de QoS adaptatifs

Différemment de la première approche, cette approche réserve dynamiquement une fraction de la bande passante pour les applications de sécurité, même si aucun message EEBL-F n'est détecté [24].

2.4.3 Contrôle de congestion via un contrôle de puissance de transmission dynamique

Le contrôle de la puissance de transmission du trafic habituel sur HCC, qui est généralement des messages de diffusion mono saut périodique, peut limiter le niveau d'utilisation du canal et réserve dynamiquement une fraction de la bande passante pour les applications de sécurité. L'idée originale de [22] est de contrôler la puissance de transmission des messages de faible priorité et maintenir la puissance de transmission du trafic de priorité la plus élevée.

2.5 Les stratégies de contrôle de congestion dans les VANETs

Une stratégie de contrôle de la congestion peut être : proactif, réactif et hybride, suivant la phase de traitement de la congestion.

- ***La stratégie proactive :*** dans les stratégies proactives, en se basant sur quelques informations telles que le nombre de véhicules voisins et le modèle de génération de données, les paramètres de transmission sont ajustés de sorte que l'occurrence de la congestion soit prévenue, i.e. ; les paramètres de transmission sont ajustés avant que le canal soit congestioné. Les stratégies proactives sont efficaces pour le contrôle de la congestion dans l'environnement véhiculaire car dans ces environements les messages de sécurité sont, principalement, envoyés sur des canaux de communication radio sujets à la congestion. De ce fait, ces stratégies réduisent la charge du canal pour éviter sa congestion en ajustant les paramètres de transmissions [17].
- ***La stratégie réactive :*** les stratégies réactives emploient les conditions de congestion des canaux pour décider comment elle devraient mener le contrôle de la congestion en ajustant les paramètres de transmission. Ces stratégies contrôlent la congestion après son occurrence dans le réseau. De plus, ces stratégies vérifient les canaux périodiquement et mesurent quelques paramètres des canaux (exemple le niveau d'utilisation, nombre de messages dans la file d'attente, temps d'occupation) et comparent ces valeurs avec des seuils prédéfinis pour détecter l'occurrence de la congestion dans le réseau. Si une congestion de canaux est détectée, les paramètres de transmission seront ajustés pour diminuer la charge des canaux et contrôler la congestion. Brièvement, les stratégies réactives réduisent la charge des canaux en obtenant, localement, des informations à partir des réseaux de véhicules [17].
- ***La stratégie hybride :*** ces stratégies utilisent les avantages des stratégies réactives et proactives. Par exemple, ces stratégies ajustent la puissance de la transmission d'une façon proactive et le débit de la transmission d'une façon réactive pour contrôler la congestion dans les canaux [17].

Par ailleurs, d'autres classes de contrôle de congestion, suivant d'autres critères, peuvent exister dans les VANETs :

2.6 Classification des stratégies de contrôle de la congestion basée sur les paramètres et les moyens

Le contrôle de la congestion dans les réseaux VANETs peut être effectué en ayant recourt à une stratégie qui utilise l'un des paramètres suivants : le débit de transmission, la puissance de transmission, la priorisation, l'ordonnancement ainsi que des stratégies hybrides.

2.6.1 Stratégie basée sur le débit de transmission

En raison de l'impact significatif du débit de transmission sur les performances des réseaux, cette stratégie ajuste dynamiquement le débit de transmission ou le taux de génération de paquets pour contrôler la charge du canal et la congestion dans le réseau. Les performances des VANETs sont améliorées par l'augmentation du débit de transmission car les applications de sécurité peuvent recevoir des informations actualisées sur les véhicules voisins, envoyer leur propre états aux véhicules voisins et mettre à jours leur informations pour fonctionner efficacement. En outre, un débit de transmission élevé, des messages périodiques dans le réseau en particulier lorsque la densité du réseau est élevée, conduit à une utilisation élevée de la bande passante et par conséquent congestionne le canal de contrôle. Donc, les performances des applications de sécurité sont réduites à cause de l'anarchie de livraison des messages de sécurité. Il faut, aussi, noter que lorsque le débit de transmission augmente, le canal peut être saturé à cause de l'augmentation de la charge du canal. Ci dessous, quelques protocoles qui appartiennent à cette classe :

Dans [27], les auteurs ont modifié le standard WAVE pour ajouter une nouvelle couche qui communique avec la couche MAC pour contrôler la congestion dans les réseaux véhiculaires. Ils considèrent deux paramètres, à savoir la fiabilité et l'efficacité pour mesurer les performances de diffusion des messages périodiques dans les VANETs. L'efficacité est définie comme le taux de livraison des paquets envoyés aux véhicules voisins et la fiabilité est définie comme étant le nombre moyen de nœuds qui ont bien reçu les paquets diffusés. En effet, ce travail vise l'efficacité et la fiabilité des messages périodiques diffusés en obtenant un débit de transmission de paquets optimal et en se basant sur la densité des véhicules. Toutefois, les contraintes liées au débit de transmission strict des messages de sécurité, qui doivent être considérées pour éviter les collisions dans le canal et transférer ces messages sans retard, ne sont pas prises en considération. Bien que le canal "fading" est considéré comme la seule source de défaillance des paquets, l'occurrence de la collision par des transmissions simultanées et le problème du nœud caché ne sont pas pris en compte.

Dans [20], les auteurs ont introduit une stratégie de contrôle de congestion cross-layer qui augmente le débit de transmission des messages de sécurité orienté événement par rapport aux messages périodiques. Dans cette stratégie, tous les nœuds utilisent la méthode du blocage MAC pour la détection de la congestion dans le canal de contrôle. En effet, si le temps d'occupation du canal dépasse un seuil prédéfini, une congestion se produira dans le canal de contrôle. Ensuite, la couche MAC envoie un message à la couche d'application pour bloquer tous les messages périodiques. Ainsi, la charge du canal est réduite et le canal de contrôle est réservé seulement aux messages de sécurité orienté événement [17].

Un autre travail, nommé On-Demand Rate Control(ODRC) [23], qui contrôle le débit de transmission des applications de sécurité en se basant sur les conditions du réseau telles que l'occurrence de la congestion et les mouvements imprévus de véhicules. Dans ODRC, une probabilité de transmission est calculée en traçant les erreurs des véhicules voisins en se basant sur leur position. ODRC, augmente le débit de transmission quand le véhicule aura des comportements inattendus. D'autre part, le débit de transmission est diminué pour réduire la perte de paquets lorsque la collision se produit. ODRC est un algorithme décentralisé qui améliore les performances de VANETs. Cependant, la priorité des paquets n'est pas prise en compte dans ce protocole.

Utility-Based Packet Forwarding and Congestion Control (UBPFCC) est proposé pour le contrôle de la congestion des applications qui ne sont pas de sécurité. Il ajuste le débit de transmission en se basant sur l'utilité et la taille des paquets. Il assigne dynamiquement la bande passante disponible aux véhicules en se basant sur l'utilité moyenne calculée pour chaque véhicule [17].
La fonction d'utilité est donnée comme suit[14] :

$Y_T(\pi) = \frac{Valeur\ de\ segment\ charg}{Nombre\ total\ des\ valeurs\ de\ segment}$.

En effet, le véhicule avec la plus grande utilité peut consommer une grande partie de la bande passante disponible, alors que les paquets avec une faible utilité risquent d'être jetés à cause de la congestion. L'utilité moyenne est calculée indépendamment dans la couche d'application de chaque nœud en considérant la densité et le mouvement des véhicules. Ensuite, le débit de transmission approprié est déterminé pour le véhicule à partir de l'utilité moyenne calculée. Dû à l'échange de la bande passante entre les véhicules voisins indifféremment de la capacité et de l'état de congestion des véhicules, les canaux sont considérablement surchargés surtout dans les réseaux de haute densité. UBPFCC a besoin d'effectuer la segmentation de route pour calculer la métrique d'utilité. Ce protocole emploie les informations de GPS pour segmentr les routes. A cause de la segmentation, il ne peut pas être utilisé par des applications

de sécurité. En plus, les signaux de GPS peuvent ne pas être reçus dans certains cas tels que les tunnels qui réduisent l'exactitude des informations. De plus, ajuster le débit de transmission en se basant sur l'utilité et la taille des paquets conduit aux diminutions des performances des messages de sécurité orienté événement. Quand une congestion se produit, le paquet avec l'utilité inferieure sera abandonné et la congestion sera reduite.

2.6.2 Stratégie basée sur la puissance

Dans ces stratégies, la puissance de transmission (la portée) est ajustée pour diminuer les collisions des canaux. Pour assurer l'équité dans les VANETs, tous les nœuds doivent avoir la même opportunité pour communiquer avec les véhicules voisins. Les applications de sécurités envoient, généralement, leur messages de sécurité avec une portée de transmission élevée pour couvrir une grande surface de sorte que ces messages soient reçus par le plus grand nombre de véhicules. Cependant, si la congestion survient dans le réseau, certains véhicules devraient réduire leur puissances de transmission pour éviter les collisions du canal. Ainsi, la chance de communication avec les véhicules voisins sera réduite et l'équité dans les VANETs sera violée. En outre, une puissance de transmission élevée conduit à l'augmentation de la collision du canal et sa saturation. Ci dessous quelques protocoles qui suivent ce type de stratégies :

Dans [25], les auteurs ont présenté un nouvel algorithme pour le partage de la bande passante de manière équitable entre les véhicules. Cet algorithme est appelé Fair Power Ajustement for Vehicular environment (FPAV). Les auteurs ont proposé une stratégie de contrôle de congestion qui augmente la probabilité de réception des paquets par les véhicules voisins, de sorte que l'équité soit assurée dans le système. Dans FPAV, l'algorithme contrôle la congestion uniquement pour les messages de sécurité y compris les messages périodiques et les messages d'urgence. L'algorithme FPAV limite la charge de messages périodiques et fournit une puissance de transmission appropriée en se basant sur la densité des véhicules. En effet, pour assurer une utilisation équitable du canal, lorsque le nombre de véhicules actifs augmente, la puissance de transmission est réduite à un seuil prédéfini. En outre, cet algorithme réserve une partie de la bande passante pour les messages d'urgence. Cependant, la réservation de la bande passante peut la gaspiller dans les conditions normales de Vanet.

Distributed Fair Power Ajustements for Vehicular environments (D-FPAV) est un protocole distribué et local d'ajustement de la puissance de transmission. Il fournit une puisance de transmission efficace pour les messages orientés événement en réduisant la charge des messages périodiques sur le canal de contrôle. En utilisant ce protocole, les messages orientés événement

ont une priorité plus élevée d'être transmis sur le canal de contrôle en comparaison avec les messages périodiques. Ce protocole considère que le taux de réception des messages périodiques ne doit pas se diminuer chez les véhicules voisins. Il contrôle la congestion en ajustant équitablement la portée des messages périodiques en se basant sur la densité des véhicules. Dans D-FPAV, chaque véhicule nécessite des informations générales sur l'état des véhicules voisins. En se basant sur cette connaissance, le véhicule ajuste la portée de transmission maximale pour les messages périodiques de sorte que leur charge ne doit pas dépasser un certain seuil prédéfini. Ensuite, la portée de transmission ajustée sera diffusée aux voisins [14].

2.6.3 Stratégie basée sur CSMA/CA

Cette stratégie est une stratégie d'évitement de collision utilisée par IEEE 802.11p (WAVE) en tant que la stratégie par defaut de contrôle de congestion. Cette stratégie détermine la capacité d'accès au canal de chaque nœud dans la couche MAC en ajustant la taille de la fenêtre de contention et AIFS. Ces derniers jouent un rôle important pour réduire les collisions des canaux et éviter leur congestions. En plus, dans cette stratégie, le mécanisme de back-off exponentiel est utilisé pour contrôler la congestion. Cependant, lorsque le taux de génération des messages est élevé et les messages périodiques ont un timeout, le mécanisme de back-off exponentiel ne sera pas efficace dans les VANETs.

Incremental Power Carrier Sensing(IPCS) est un mécanisme approprié pour prévenir la collision causée par les nœuds cachés. Le protocole IPCS garantit une transmission sans interférence dans un réseau basé sur CSMA suivant le modèle physique d'interférence. Ce protocole surveille toute réduction du niveau de puissance dans le réseau et ensuite la compare avec un seuil prédéfini. En effet, ce mécanisme est capable de détecter et séparer les puissances de transmission concurrentes des véhicules dans le réseau. Alors, en se basant sur le niveau de puissance de transmission reçu, ce protocole détecte l'état "idle" des canaux et détermine la portée appropriée (carrier sensing range). Bien que, en utilisant ce protocole, le débit est amélioré mais les bruits de font ne sont pas considérés. Donc, ce protocole n'est pas efficace dans les vrais environnements [17].

2.6.4 Stratégie basée sur la priorité et l'ordonnancement

Cette stratégie contrôle la congestion en assignant des priorités aux messages et en les ordonnançant pour être transférés sur les canaux de contrôle et de service. Les priorités, dans

ce cas, sont définies de sorte que les messages de sécurité avec haute priorité auront plus de chance d'acquérir les canaux et transférés dans de bons délais. En utilisant cette classe, l'accès au canal est contrôlé de sorte que les collisions du canal sont diminuées. Dans cette classe, des niveaux de priorité sont nécessaires pour les différents types de messages générés dans les VANETs. Ensuite, les messages à priorité sont programmés pour le transfert sur les canaux de contrôle et de service. Par conséquent, la saturation et la congestion des canaux peuvent être évitées. Les algorithmes suivants peuvent être employés dans VANETs : First-in-First-out (FIFO), Longest Wait Time (LWT), Maximum Request First (MRF), First Deadline First (FDF), Smallest Data-size First (SDF), Longest Total Stretch First (LTSF), Maximum Quality Increment First (MQIF), Least Selected First (LSF).

Dans [26], les auteurs ont proposé Context Aware Beacon Scheduling (CABS) qui est une stratégie de contrôle de congestion pour les applications de sécurité. En plus, cette stratégie est utilisée pour adresser le problème de taux de messages périodiques élevé dans les réseaux denses qui conduit à la surcharge et la congestion des canaux. Le CABS est une stratégie distribuée qui ordonnance, dynamiquement, les messages périodiques en utilisant des méthodes d'accès aux canaux (exemple TDMA) pour allouer un slot de temps pour l'envoi des messages périodiques. Ces slots de temps sont déterminés en se basant sur l'état du canal et les informations de contexte (exemple la vitesse, la position, la direction des véhicules). Dans cette stratégie, le taux de réception de paquets et le délai d'accès au canal sont réduits grâce à la diminution du taux de messages périodiques [17].

2.6.5 Stratégie hybride

Dans cette stratégie, deux paramètres ou plus sont utilisés pour le contrôle de la congestion. Ajuster le débit et la puissance de transmission, la taille de la fenêtre de contention et AIFS, et définir une priorité propre à chaque message et son ordonnancement sur les canaux sont combinés dans les stratégies hybrides pour éviter la saturation de canal et la congestion dans les VANETs.

Adaptive Message Rate Control (AMRC) est un protocole de contrôle d'adaptation à deux niveaux. Il contrôle la congestion en ajustant le débit de transmission et l'intervalle de contrôle du canal en se basant sur l'utilité des paquets. Dans ce protocole, la scalabilité de communication de véhicules est améliorée, les performances des messages de sécurité sont garanties, et les applications qui ne sont pas de sécurité peuvent acquérir la bande passante autant que possible pour s'exécuter efficacement. Dans ce protocole, en utilisant une procédure

hors ligne, le débit de transmission et l'intervalle de contrôle du canal sont déterminés pour un nombre spécifique de véhicules. Ensuite, en utilisant une procédure en ligne, RSU configure les valeurs déterminées du débit de transmission et de l'intervalle de contrôle du canal pour un nombre spécifique de véhicules. En plus, les valeurs obtenues sont diffusées par les RSUs. AMRC améliore les performances des Vanets [17].

A Vehicle Oriented Congestion Control Algorithm (AVOCA) est un protocole de contrôle de la congestion cross layer. Dans AVOCA, puisque la congestion est contrôlée dans le réseau, les failles de couverture du réseau sont prises en compte. Cet algorithme a été proposé pour répondre au problème de défaillance dans la couche transport lorsque les véhicules entrent 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. Quand un véhicule entre dans une zone de couverture, les performances de la couche de transport dépassent le seuil. Ensuite, AVOCA remet à zéro les paramètres de contrôle de congestion et initie les transmissions de paquets. En revanche, lorsque le véhicule sort de la zone de couverture, les performances de la couche de transport diminuent. Puis, AOVCA gèle les paramètres de contrôle de congestion et bloque les transmissions de paquets. Cet algorithme améliore de manière significative le débit du réseau en tenant compte de l'équité dans l'allocation du canal [17].

2.7 Tableau récaputilatif des protocoles étudiés

Nous resumons dans le tableau TAB 2.1 toutes les approches étudiées :

2.8 Conclusion

Dans ce chapitre, nous avons détaillé le problème de congestion dans les VANETs. Nous avons commencé par une définition générale (routière) puis spéciale (du réseau). Ensuite, nous avons exhibé les méthodes de détection de la congestion dans les VANETs. Par la suite, nous avons présenté les différentes stratégies de contrôle de congestion et étudié quelques protocoles pour chaque stratégie.
Le chapitre suivant sera consacré à notre proposition qui résout le problème de congestion dans les VANETs.

Approche	**Débit de transmission**	**Puissance de transmission**	**Priorité d'accès**	**Seuil de l'écoute de porteuse**	**Fonction d'utilité**	**Rediffusion intelligente**
UBPFCC	OUI	NON	OUI	NON	OUI	NON
Cross-layer CC	NON	OUI	OUI	OUI	NON	OUI
BRR-EPA	NON	OUI	OUI	NON	NON	NON
FPAV	OUI	OUI	OUI	OUI	NON	NON
D-FPAV	NON	OUI	OUI	OUI	NON	NON
ODRC	OUI	NON	NON	NON	NON	NON
IPCS	OUI	OUI	OUI	NON	NON	NON
AMRC	OUI	OUI	NON	NON	OUI	NON
AVOCA	OUI	OUI	NON	NON	NON	NON

TAB. 2.1 – *Tableau récaputilatif des protocoles étudiés*

3

Modèle de contrôle de congestion en fonction de la fenêtre de congestion

3.1 Introduction

La majorité des protocoles de contrôle de congestion dans les réseaux VANETs 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 modèle de contrôle de congestion en fonction de la fenêtre de congestion par l'utilisation des chaînes de Markov.
Dans ce chapitre, nous présenterons le modèle et l'algorithme de contrôle de congestion proposés tout en expliquant ses étapes par une modélisation. Nous terminons par une conclusion.

3.2 Présentation du modèle de contrôle de congestion

Comme nous l'avons dit dans le chapitre 2, il existe plusieurs protocoles et stratégies de contrôle de congestion, parmi lesquels des approches réactives qui se basent sur l'adaptation du débit de transmission. Ces approches ne sont pas vraiment pratiques dans des environements de dynamicité élevée tels que VANETs car elles s'appliquent seulement après la détection de

la congestion. Ce genre d'approches peut conduire à une perte considérable de paquets avant que le système traite la congestion. Pour alléger ce problème, nous proposons dans ce travail un modèle, basé sur les chaines de Markov, qui contrôle la congestion avant son apparition. Le but de ce modèle est de permettre un contrôle de congestion par l'adaptation du débit de transmission en fonction de la fenêtre de congestion. Les différentes étapes de cet algorithme sont illustrées dans la figure FIG 3.1 :

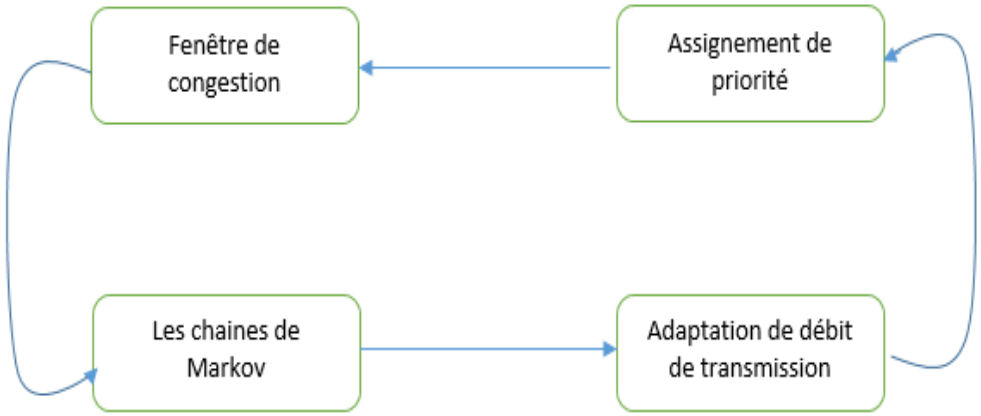

FIG. 3.1 – Algorithme de contrôle de congestion

Après la réception des messages, dans la 1^{re} etape chaque nœud organise les messages (périodiques, orienté événement, etc.) selon leur priorités (faible priorité, priorité moyenne, haute priorité). La deuxième étape de l'algorithme consiste à surveiller la taille de la fenêtre de congestion pour décider de l'état de la congestion du canal. Ensuite, dans la troisième étape, nous utilisons les chaînes de Markov pour modéliser les différents états de la congestion. A la fin, chaque nœud adapte le débit de transmission des messages périodiques en se basant sur l'état de la congestion calculé précédemment (dans l'étape précédente). L'organnigramme sur la figure FIG 3.2 illustre les différentes parties de cette solution.

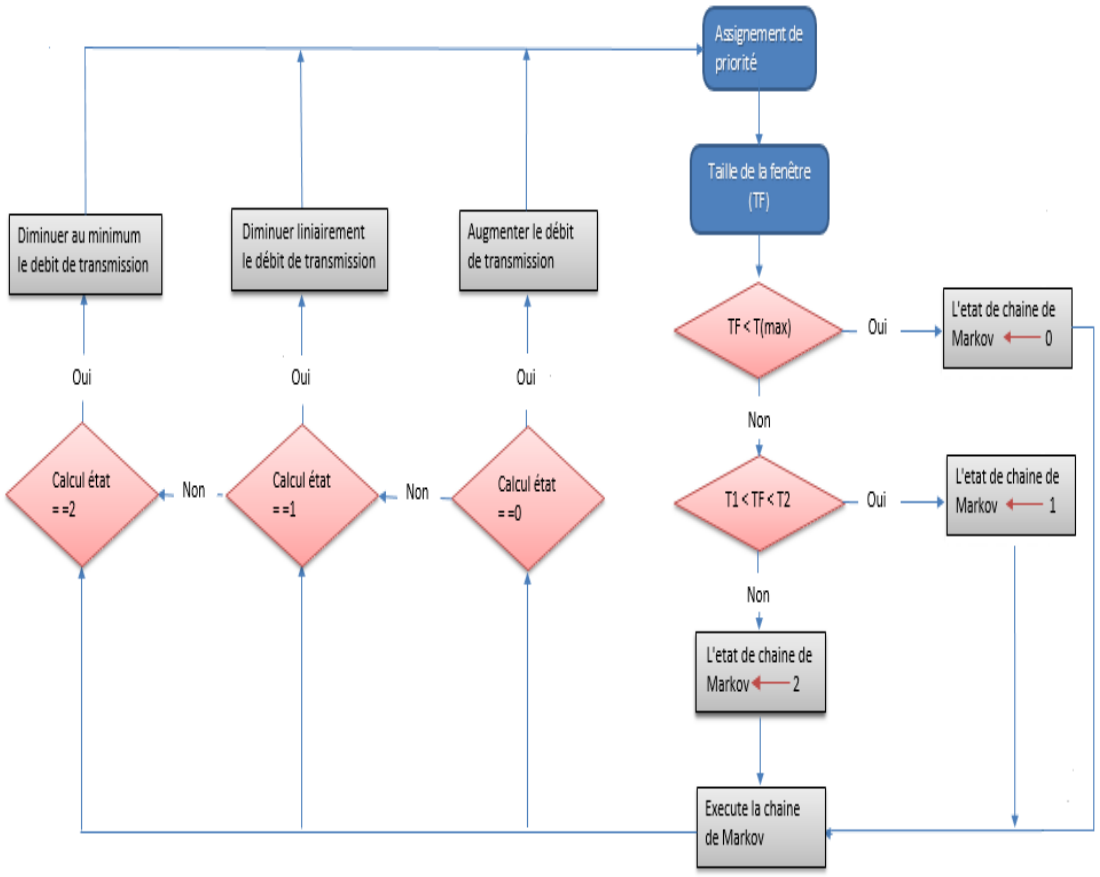

FIG. 3.2 – Organnigramme du modèle proposé

3.2.1 Assignement de priorité

Lorsqu'un véhicule reçoit un message orienté événement par un RSU ou un véhicule voisin détectant une collision, un arrêt d'urgence, etc., nous assignons à ces messages différentes priorités selon leur utilités, ce qui donne naissance à trois files d'attente :

HP : regroupe les messages de haute priorité (messages d'urgence) tels que la présence d'accident, la neige, l'arrêt prématuré d'un véhicule, etc.
MP : regroupe les messages de priorité moyenne tels que les messages d'avertissement, la congestion routière, etc.
FP : regroupe les messages de faible priorité tels que les messages périodiques ou les messages de surveillance du réseau.

Si une file d'attente est pleine, on réorganise ses messages selon la distance séparant le véhicule émetteur et le véhicule récepteur tel que les messages à envoyer pour les véhicules lointains soient déplacés vers la file d'attente de niveau inférieur pour libérer celle de niveau supérieur avec l'hypothèse d'avoir un intervalle de vitesse fixe à ne pas dépasser et avec l'utilisation d'un GPS pour la détection de la position du véhicule récepteur.

3.2.2 Calcul de la taille de la fenêtre de congestion

Pour appliquer cette étape de l'algorithme, nous commençons par la définition de la fenêtre de congestion :

3.2.2.1 Définition de la fenêtre de congestion

Elle permet de calculer le taux d'occupation du canal et représente le nombre de messages qui circulent sur le réseau sans être délivrés par les véhicules. En d'autres termes, elle enregistre les messages à qui un véhicule n'a pas reçu d'aquittement de réception.

Nous envisageons trois cas possible avec les seuils :

- Si la taille de la fenêtre est $< T_1 \Rightarrow$ il n'y a pas de congestion $\Rightarrow$ nous sommes à l'état "0".
- Si la taille de la fenêtre est entre T_1 et $T_2 \Rightarrow$ il y'a une congestion moyenne $\Rightarrow$ nous sommes à l'état "1".
- Si la taille de la fenêtre est entre T_2 et $T_{max} \Rightarrow$ il y'a une forte congestion $\Rightarrow$ nous sommes à l'état "2", (Voir FIG 3.3).

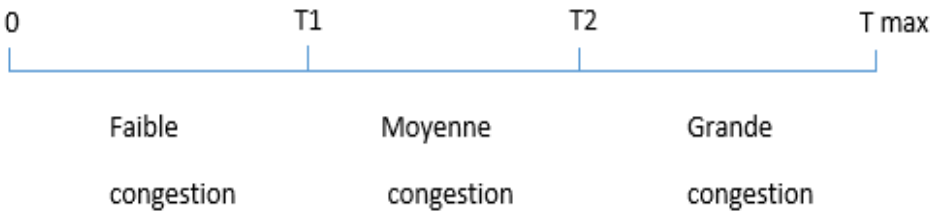

FIG. 3.3 – La taille de la fenêtre de congestion

3.2.3 Application des chaînes de Markov

Dans cette étape, nous utilisons les chaînes de Markov pour estimer la taille de la fenêtre de congestion. Après cette estimation, nous décidons de l'adaptation du débit de transmission. Selon les résultats précédents, nous observons la taille de la fenêtre de congestion pendant des intervalles de temps t_0, t_1, t_2, ..., t_n. Les résultats sont donnés par X_0, X_1, X_2 ... X_n pour t_0, t_1, t_2 ... t_n, tel que X_t est une variable aléatoire.

X_t est représentée par une chaîne de Markov à temps discret. Elle représente la taille de la fenêtre de congestion au moment t. Nous avons trois états $S = 0, 1, 2$

$$\mathrm{S} = \begin{cases} 0 & si\ 1 < \mathrm{X}_t < T_1\,; \\ 1 & si\ \mathrm{T}_1 < X_t < T_2\,; \\ 2 & si\ \mathrm{T}_2 < X_t\ T_{max}. \end{cases}$$

Les probabilités de transition de la chaîne de Markov X_t avec l'espace d'état $\{0, 1, 2\}$ sont données sous forme de la matrice suivante :

P_{ij}=$\{X_{t+1}$=j / X_t=i$\}$.

P_{ij} : est une probabilité de passage de l'état i vers l'état j ou i$\in\{0, 1, 2\}$ et j$\in\{0, 1, 2\}$.

$$\text{T}= \begin{pmatrix} P_{00} & P_{01} & P_{02} \\ P_{10} & P_{11} & P_{12} \\ P_{20} & P_{21} & P_{22} \end{pmatrix}$$

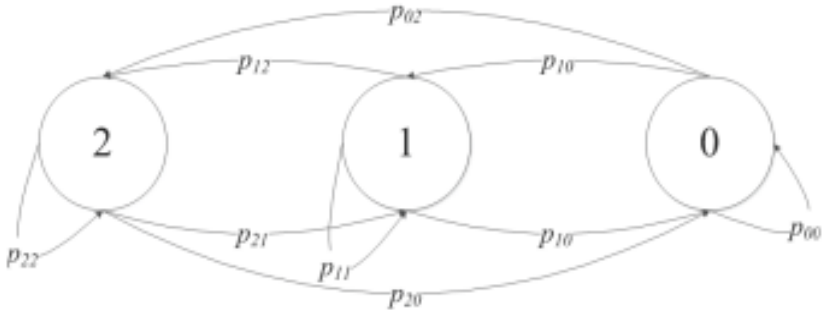

FIG. 3.4 – La chaîne de Markov

3.2.4 Adaptation du débit de transmission

A ce niveau et selon le résultat obtenu par le modèle de chaîne de Markov et l'état de congestion du réseau, nous adaptons le débit de transmission de la manière suivante :

1 -Si le système est à l'état "0", nous augmentons le débit de transmission au maximum.

2 -Si le système est à l'état "1", nous diminuons le débit de transmission linéairement.

3 -Si le système est à l'état "2", nous réduisons le débit de transmission au minimum.

3.3 Implémentation du modèle proposé

Avoir des résultats analytiques de l'algorithme proposé n'est pas possible, pour cela on a opté pour une simulation d'un scénario choisi des réseaux VANETs. Pour arriver à notre objectif, nous avons développé une interface, qui nous permettra de faire la simulation, et tester l'efficacité de la proposition qu'on a apporté dans ce travail. Cela est effectué à l'aide d'un logiciel de programmation appelé NETBEANS.

3.3.1 Présentation de NETBEANS

Cet IDE a été créé à l'initiative de Sun Microsystems. Il présente toutes les caractéristiques indispensables à un environnement de qualité, que ce soit pour développer en Java, Ruby,

C/C++ ou même PHP.

NetBeans est un logiciel OpenSource, il permet de développer et déployer rapidement et gratuitement des applications graphiques Swing, des Applets, des JSP/Servlets, des architectures J2EE, dans un environnement fortement personnalisable.

A coté de la version complète de l'IDE NetBeans, il existe différentes déclinaisons qui se concentrent sur une plateforme ou un langage précis (Java ME, Java : SE + ME + EE, Ruby, C/C++, PHP).

NetBeans contient, en plus du support pour CVS et SubVersion, un support pour ClearCase, mais aussi pour Mercurial. Il permet également de déployer des applications Web, non seulement vers Tomcat et Glassfish qui sont livrés avec le "Pack Web", mais aussi vers JBoss, WebSphere 6.1, WebLogic 9.

NetBeans détient un support de développement d'applications Web avec des améliorations pour l'édition des JSP, la gestion serveur et le support des dernières versions de Tomcat.

Enfin, cet IDE possède un débogueur de grande qualité ainsi qu'une interface graphique améliorée [31].

3.3.1.1 Valeurs et paramètres utilisés

Les valeurs et les paramètres utilisés pour réaliser les simulations et les graphes adéquats de notre algorithme sont récapitulés dans le tableau TAB 3.1.

Taille d'un message	1500 octets
T_{max}	5000 octets
ACK	0.5 s
Nombre de véhicules	10
Surface	120 000 m^2
Taux de transmission	3000 octets/s
Durée de simulation	40 s

TAB. 3.1 – *Les paramètres de la simulation*

3.3.1.2 Etape 1 : Assignement de priorité

Pour cette étape, nous avons classé les messages suivant leur priorité (HP, MP, FP) et nous avons choisi un réseau de 10 véhicules qui envoient un nombre aléatoire de messages qui ont une taille fixe de 1500 octets et un débit de transmission de 3000 octets/s.

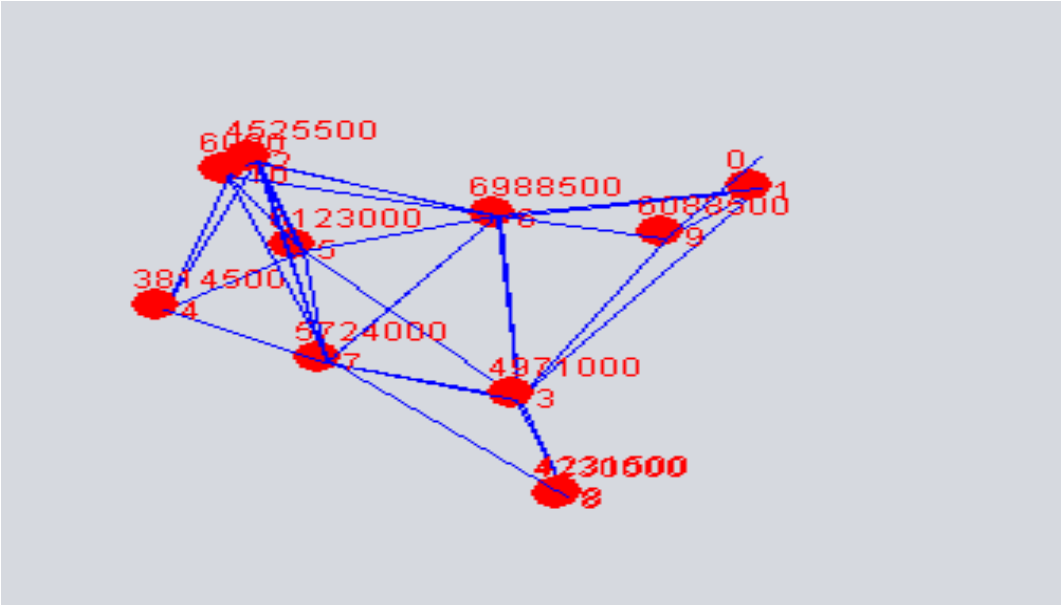

FIG. 3.5 – Connexion entre les véhicules

3.3.1.3 Etape 2 : Calcul de la taille de la fenêtre de congestion

Chaque véhicule manipule une fenêtre de congestion avec une taille maximale $T_{max} = 5000$ octets. Pour chaque messages, un aquittement (ACK) est suggéré pendant un temps maximum (timeout) de 0.5 seconde. La fenêtre de congestion est caractérisée par la perte des paquets, c'est à dire quand elle est saturée, les derniers messages envoyés seront perdues.
Nous nous intéressons aux messages HP et nous cherchons à calculer le nombre de messages perdus (aux quels, nous n'avons pas reçu d'ACK) dans la fenêtre de congestion avec et sans assignement de priorité. Les figures FIG 3.6 et FIG 3.7 illustrent les résultas obtenus.

La figure FIG 3.6 représente le nombre de messages de haute priorité perdus sans assignement de priorité. Après chaque 40 secondes de simulation, nous remarquons une augmentation du nombre de messages perdus.

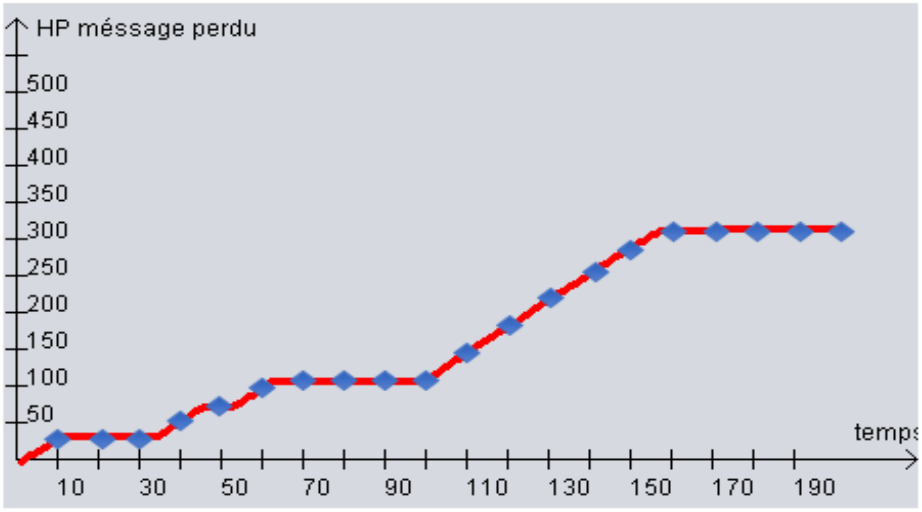

FIG. 3.6 – Nombre de messages de haute priorité perdus

La figure FIG 3.7 représente le nombre de messages de haute priorité perdus avec assignement de priorité. Pendant toute 40 secondes, nous remarquons une légère augmentation du nombre de messages perdus et à partir de la seconde 30, équivalente à 150 pixels sur le graphe, le nombre de messages perdus est stabilisé à 120 messages HP.

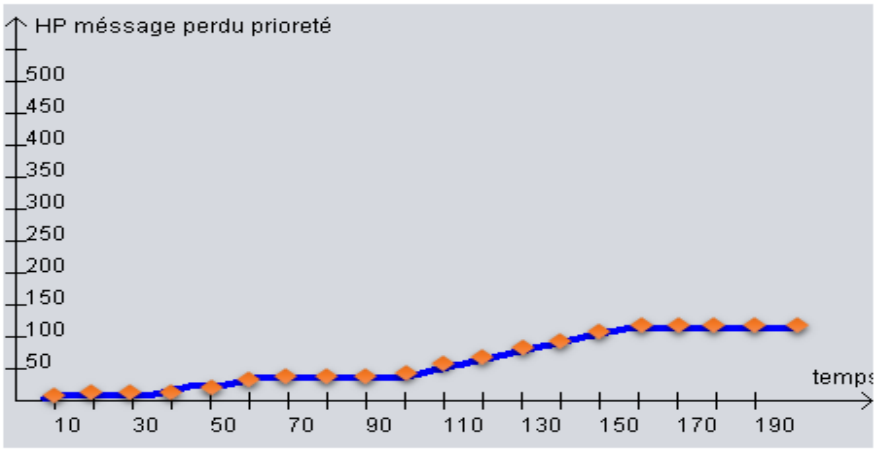

FIG. 3.7 – Nombre de messages de haute priorité perdus après l'assignement de priorité

3.3.1.4 Etape 3 : Modélisation par les chaînes de markov

Le tableau de la figure FIG 3.8 montre le changement d'états de congestion pour les 20 transitions de T_1 à T_{20}.

T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	T11	T12	T13	T14	T15	T16	T17	T18	T19	T20
1	1	1	0	1	0	0	1	0	2	0	2	2	2	2	0	2	2	1	2

FIG. 3.8 – Tableau de changement d'état de la congestion

Le graphe de la figure FIG 3.9 schématise graphiquement les changements d'états de la congestion.

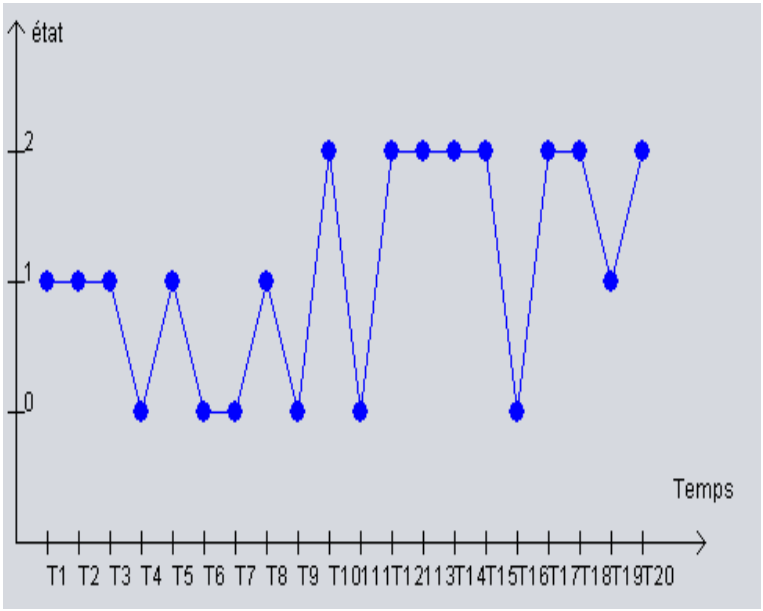

FIG. 3.9 – Le graphe de transition

Ainsi, la matrice de transition, qui correspond aux transitions d'état de la congestion, est obtenue :

$$T = \begin{pmatrix} 1/6 & 2/6 & 3/6 \\ 3/6 & 2/6 & 1/6 \\ 2/7 & 1/7 & 4/7 \end{pmatrix}$$

3.4 Conclusion

Dans ce chapitre, nous avons proposé un modèle de contrôle de congestion à base de chaînes de Markov. Nous avons modélisé la solution et la simulée avec NetBeans. Nous avons obtenu des résultats de simulation en termes de nombre de messages perdus (sans et avec priorité). Reste à comparer ces résultats avec d'autres travaux pour montrer l'efficacité de notre solution.

Conclusion générale

Avec l'introduction des systèmes de transport intelligents, une nouvelle ère s'annonce avec des véhicules plus confortables et plus sécuritaires. La nouveauté consiste à doter les véhicules et l'infrastructure routière de capacités sensorielles, d'intelligence artificielle qui se traduit par la possession d'unités de calcul et de communication pour améliorer la sécurité routière.

Dans ce mémoire de master, nous avons proposé l'amélioration des systèmes de communication des réseaux véhiculaires. Plus particulièrement, nous cherchons à mieux contrôler la congestion dans ces réseaux pour rendre la communication plus fluide et plus sécurisée.

Les réseaux VANETs sont un cas particulier des réseaux ad hoc Mobile (MANETs). Ces réseaux appartiennent à un nouveau domaine de recherche qui s'annonce vaste et riche en possibilité de développement, un domaine dont on connaît que les origines et non les limites.

Pour notre part de recherche, nous avons choisi dans ce mémoire d'étudier le contrôle de la congestion dans ces réseaux. Pour commencer, nous avons présenté les réseaux VANETs pour bien comprendre sur quoi notre travail est basé. Ensuite, nous avons presenté quelques stratégies et protocoles utilisés pour le contrôle de la congestion. La présence de congestion dans les réseaux VANETs réduit la fiabilité de transmission des messages entre les véhicules, ce qui réduit les performances de ces réseaux.

Dans ce travail, nous avons étudié et évalué l'impact de l'utilisation de la fenêtre de congestion pour l'adaptation du débit de transmission pour contrôler la congestion dans les VANETs par l'utilisation des chaînes de markov. Nous avons implémenté cette solution avec le langage JAVA et nous avons présenté les résultats dans le dernier chapitre. Ce modèle se base sur le calcul de la taille de fenêtre de congestion (congestion window) pour connaître l'état de la congestion dans le réseau et à partir d'ici nous avons fixé deux seuils pour classifier la congestion du réseau en trois cas possibles (il n y a pas de congestion, faible congestion et forte congestion). Ensuite, nous avons modélisé cette situation avec une chaîne de markov à trois états. Pour la simulation, nous avons simulé un scénario dont les résultats illustrent l'impact de l'utilisation de la fenêtre de congestion sur le contrôle de congestion .

En guise d perspectives, nous comptons implémenter le modèle proposé et le comparer avec d'autres modèles. En plus, proposer une solution hybride de congestion et inclure le maximum de paramètres pour éviter la congestion.

Bibliographie

[1] D. Bektache, "Application et Modélisation d'un protocole de communication pour la sécurité routière ", thèse de doctorat de l'universite badi mokhtar annaba, 2014 .

[2] A. Aous, M. Hammodi, Y. Benaissa, N. Bensaidane, "Les reseaux véhiculaire",mémoire de licence de l'université des sciences et de la technologie houari boumediene, 2015 .

[3] K. AIT ali, "Modélisation et étude de performances dans les réseaux vanets", thése de doctorat de l'niversité de Technologie de Belfort-Montbeliard, 2012.

[4] M. Jerbi, "Protocoles pour les communications dans les reseaux de vehicules en environnement urbain : Routage et GeoCast bases sur les intersections", thèse de doctorat de L'universite D'evry Val D'essonne, 2008.

[5] Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 15.1 : Wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPANs), New York, 2002.

[6] Y. Toor, P. Mühlethaler, A. Laouiti et A.D.L. .Fortelle, Vehicle ad hoc networks : Applications and related technical issues. IEEE Communications Surveys and Tutorials, pp. 74-88, 2008.

[7] A. Benchabana et R. Bensaci, " Analyse des protocoles de routage dans les reseaux VANETs", Université Kasdi Merbah-Ouargla, Mémoire Master Académique, juin 2014.

[8] Y. Khaleda, M. Tsukadaa, J. Santab, JinHyeock Choia and Thierry Ernsta .(2009). A usage oriented analysis of vehicular networks : from technologies to applications. journal of communications, vol. 4, no. 5, june 2009.

[9] J. C. Laprie : Surete de fonctionnement et tolerance aux fautes : concepts de 17 base. Rapport technique LAAS-88287, Laboratoire d'automatique et d'analyse des systèmes (Toulouse), 1988.

[10] R.T. Malar "congestion control in wirlesse sensor networks based multi-path routing in priority rate ajustement technique", international journal jan, 2010.

[11] IEEE 802.11 Draft Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, New York, 1997.

[12] IEEE 802.11p Amendment, “Wireless Access in Vehicular Environments,” v. D3.0, 2007, work in progress.

[13] IEEE Standard 802.16-2004 : IEEE Standard for Local and Metropolitan Area Networks - Part 16 : Air Interface for Fixed Broadband Wireless Access Systems. New York, 2004.

[14] I. B. Vyas, Review on Congestion Control Algorithm for VANET, International Conference on Quality Up-gradation in Engineering, Science and Technology, 2014 .

[16] A. Adama, ”Protocole de routage basé sur des passerelles, mobiles pour un accès Internet dans les réseaux véhiculaires”, thèse de doctorat de l’université de Montréal, Avril, 2011.

[17] N. Taharkhani, ”Congestion control in vehicular ad hoc networks”, thèse de doctorat de université de montréal, 2015.

[18] F. Chatté, ”Contribution au contrôle de congestion dans les protocoles de transport”, thèse de doctorat de l’niversité de Technologie de Compiegne, 2013.

[19] Y. Zang, L. Stibor, X. Cheng, H.-J. Reumerman, A. Paruzel and A. Barroso . “Congestion Control in Wireless Networks for Vehicular Safety Applications”, In Proceeding The 8th European Wireless Conference, Paris, France, pp. 7, 2007.

[20] J. He, H.-H. Chen, T. M. Chen, and W. Cheng, ”Adaptive congestion control for DSRC vehicle networks,” IEEE communications letters, vol. 14, pp. 127-129, 2010.

[21] M.-Y. Darus and K. Abu Bakar, ”A Review of Congestion Control Algorithm for Event-Driven Safety Messages in Vehicular Networks”, pp. 51-52, 2011

[22] M. Torrent-Moreno, P. Santi, H. Hartenstein, “Fair Sharing of Bandwidth in VANETs In Proceedings of the second ACM In- ternational Workshop on Vehicular Ad Hoc Networks (VANET)”, pp. 49-58, 2005.

[23] C.L. Huang, Y. P. Fallah, R. Sengupta, and H. Krishnan, ”Information dissemination control for cooperative active safety applications in vehicular ad-hoc networks,” IEEE Global Telecommunications Conference, Globecom, pp. 1-6, 2009.

[24] Y. Zang, L. Stibor, X. Cheng, H.J.Reumerman, A. Paruzel and A. Barroso, “Congestion Control in Wireless Networks for Vehicular Safety Applications”, pp. 1-5.

[25] M. Torrent-Moreno, P. Santi, and H. Hartenstein, ”Fair sharing of bandwidth in VANETs,” Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks, pp. 49-58, 2005.

[26] S. Bai, J. Oh, and J.-i. Jung, ”Context awareness beacon scheduling scheme for congestion control in vehicle to vehicle safety communication,” Ad Hoc Networks, vol. 11, pp. 2049-2058, 2013.

[15] F. Ye, R. Yim, S. Roy, and J. Zhang, "Efficiency and reliability of one-hop broadcasting in vehicular ad hoc networks," IEEE Journal on Selected Areas in Communications, vol. 29, pp. 151-160, 2011.

[27] J Petit, "Surcoût de l'authentification et du consensus dans la sécurité des réseaux sans fil véhiculaires", thése de doctorat de l'niversité de toulouse, 2011.

[29] IEEE Standard 802.11a, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications : High-speed Physical Layer in the 5 GHz Band", 1999.

[29] ASTM International, "E2213-03 - Standard Specification for Telecommunications and Information Exchange Between Roadside and Vehicle Systems - 5 GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications", 2007.

[30] RITA/ITS, "IEEE 1609 - Family of Standards for Wireless Access in Vehicular Environments (WAVE)", http : www.standards.its.dot.gov/fact$_s heet.asp?f$=80, $September$2009.

[31] https : www.google.dz/ ?gws$_r d = crei$ = $9QN1V6CVM4f6swHb4YHoCQq$=$netbeans$