République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur

et de la Recherche Scientifique

Université Larbi Ben M'hidi

Oum El Bouaghi

Faculté des Sciences Exactes et des Sciences de la Nature et de la Vie

Département des Mathématiques et d'Informatique

MEMOIRE : De fin d'études pour l'obtention du diplôme de

MASTER EN INFORMATIQUE

Option : architecture distribuée

Thème :

CONTRÔLE DE MESSAGES POUR LES RÉSEAUX VÉHICULAIRES

Présenté par :

Chaima Bouhaik

Souaad Salmi

Dirigé par :

Mr .Boubakeur Achichi

2023 /2024

Remerciements

Nous tenons tout d'abord à remercier

Dieu le Tout-Puissant et Miséricordieux de nous

Grâce à la volonté et à la force qui m'ont été accordées, j'ai pu achever ce projet de fin d'études. Nous tenons aussi à remercier notre encadrant,

Dr. Boubakeur Achichi,

pour ses précieux conseils, encouragements, sa disponibilité et son aide tout au long de la réalisation de ce travail. Nos remerciements vont également aux membres du jury pour l'honneur qu'ils nous ont fait en acceptant d'examiner ce travail. Nous remercions également nos très chers parents de nous avoir toujours donné le courage et d'être l'une des raisons qui nous poussent à nous battre face à chaque obstacle. Nos remerciements vont à tous ceux qui nous ont aidés, de près ou de loin, à réaliser ce travail.

Dédicaces

Pour l'expression d'un profond respect et de reconnaissance, je dédie ce travail à mes parents qui n'ont entouré de leur amour, leur soutien moral et matériel et qui m'ont offert tant de courage et de conseils

A toute ma famille, notamment, mes frères, qui mon toujours soutenue

Je tiens également à remercier chaleureusement mon superviseur, [boubakeur achichi], qui n'a ménagé aucun effort pour m'offrir conseils et soutien durant cette recherche.

J'espère que cette réussite sera une fierté pour nous tous et le début d'une nouvelle étape pleine de succès et de prospérité."

Chaima.B

Dédicaces

Dans un profond sentiment de respect et de gratitude, je souhaite dédier ce travail à mes parents, mon marié, mes enfants :djana line, alaa bayane, sadjed abderrahmane et À toute ma famille.

Je tiens également à exprimer ma sincère gratitude envers mon encadreur,

[Boubakeur Achichi],

qui a déployé des efforts considérables au long de cette recherche.

J'espère que cette réussite sera une source de fierté pour nous tous et le point de départ d'une nouvelle étape empreinte de succès et de prospérité

Souaad.S

Dédicaces

Pour l'expression d'un profond respect et de reconnaissance, je dédie ce travail à mes parents qui n'ont entouré de leur amour, leur soutien moral et matériel et qui m'ont offert tant de courage et de conseils

A toute ma famille, notamment, mes frères, qui mon toujours soutenue

Je tiens également à remercier chaleureusement mon superviseur, [boubakeur achichi], qui n'a ménagé aucun effort pour m'offrir conseils et soutien durant cette recherche.

J'espère que cette réussite sera une fierté pour nous tous et le début d'une nouvelle étape pleine de succès et de prospérité."

Chaima.B

Résumé

Vehicular Ad-Hoc Network (reseau Ad-Hoc de vehicules) ou vanet, est une forme de MANET, pour fournir des communications au sein d 'un groupe de véhicules a porté les uns des autres et entre les véhicules et les équipements fixes, usuellement appelés équipements de la route. Ces réseaux se caractérisent par une grande dynamique et une mobilité variable, souffrant notamment de problèmes de congestion dus au grand nombre de messages de communication envoyés via le canal de contrôle. Plusieurs algorithmes ont été développés pour gérer ce problème, en se basant sur diverses mesures. Cependant, ces algorithmes diffèrent dans leur traitement de certaines mesures, ce qui a conduit à des résultats efficaces dans la résolution du problème de congestion d'une part, mais a peut-être négligé d'autres mesures, qui restent un sujet de recherche important dans ce domaine. Dans cette contribution, nous allons étudier le problème de congestion dans les réseaux VANET, ces mécanismes de détection et de contrôle, ensuite nous proposons un algorithme de contrôle de congestion dans les réseaux VANETs.la solution proposée repose sur une combinaison de deux approches : l'événementiel et l'évaluation, avec la planification des messages.

Mots-clés : VANET, contrôle de messages, message périodiques, planification des messages.

Abstract

Vehicular Ad-Hoc Networks (VANETs), also known as Mobile Ad-Hoc Networks (MANETs) for vehicles, are designed to facilitate communication between vehicles within range of each other and between vehicles and roadside equipment. These networks are characterized by high dynamism and variable mobility, and they often suffer from congestion problems due to the large number of communication messages sent through the control channel. Several algorithms have been developed to manage this problem, based on various metrics. However, these algorithms differ in their treatment of certain metrics, which has led to effective results in solving the congestion problem on the one hand, but may have neglected other metrics, which remain an important research topic in this area. In this paper, we will study the congestion problem in VANETs, its detection and control mechanisms, and then propose a congestion control algorithm for VANETs. The proposed solution is based on a combination of two approaches: event-driven and evaluation-driven, with message scheduling.

Keywords: VANET, congestion control, periodic messages, message scheduling

ملخص

شـبكات المركبـات المخصصـة والمعروفـة باسـم (VANETs)، هـي نـوع مـن أنـواع الشـبكات MANETsمصـممة لتسـهيل الاتصـال بـين المركبـات الموجـودة في نطـاق بعضـها الـبعض وبـين المركبـات والمعـدات عـلى جانـب الطريـق .تتميـز هـذه الشـبكات بديناميكيـة عاليـة وحركيـة متغيـرة، وغالبًـا مـا تعـاني هـذه الشـبكات مـن مشـاكل الازدحـام بسبب الكم الهائل من رسائل الاتصال المرسلة عبر قناة التحكم .

تـم تطـوير العديـد مـن الخوارزميـات لإدارة هـذه المشـكلة، بنـاءً عـلى معـايير مختلفـة ومـع ذلـك، تختلـف هـذه الخوارزميـات في معالجتهـا لمعـايير معينـة، ممـا أدى إلى نتـائج فعالـة في حـل مشـكلة الازدحـام مـن ناحيـة، ولكـن قـد تكـون قـد أهملـت معـايير أخـرى، والتـي تظل موضوعًا بحثيًا مهمًا في هذا المجال .

في بحثنـا هـذا، سـنقوم بدراسـة مشـكلة الازدحـام في شـبكاتVANETs ، وآليـات الكشـف والـتحكم الخاصـة بهـا، ثـم نقتـرح خوارزميـة تحكـم في الازدحـام لشـبكات VANETs ، اذ يعتمد الحل المقترح على مزيج من:

الطريقة القائمة على الأحداث والطريقة القائمة على التقييم، مع جدولة الرسائل.

الكلمات المفتاحية: VANET، التحكم في الازدحام، الرسائل الدورية، جدولة الرسائل

Liste des abréviations

STI : systèmes de transport intelligent

VANET : Vehicular Ad Hoc NETwork

l'OBU : On-Board Unit

RSU : Road Side Units

GPS : Global Positioning System

V2V : Vehicular-to-Vehicular

V2I : Vehicular-to-Infrastructure

IEEE : Institute of Electrical and Electronics Engineers

DSRC : Dedicated Short Range Communication

SCH: Service Channel

CCH : Control Channel

WAVE : Wireless Ability in Vehicular Environments

TCP : Transmission Control Protocol

MAC : Medium Access Control

ATB : Adaptative trafic beacon

AODV : Ad hoc On-demand Distance Vector

DSDV : Destination-Sequenced Distance Vector

DSR :Dynamic Source Routing

GSR :Global State Routing

MPR : Multi-Point Relaying

OLSR : Optimized Link State Routing

ZRP :Zone Routing Protocol

CSMA / CA : Carrier Sense Multiple Access / Collision Avoidanee

Listes des figures

Table des matières

Introduction Générale

Les incidents de la circulation représentent un défi majeur pour la santé publique, entraînant chaque année des millions des décès c'est pour cette raison que des nombreux pays à mettre en place des mesures visant à réduire ces incidents et à développer la sécurité routière.

L'émergence des villes intelligentes et des systèmes de transport intelligents a mis en lumière les réseaux de véhicules AD hoc (vanet). Dans ces réseaux, toutes les véhicules sont équipés de technologie de communication sans fil, ce qui facilite un échange d'informations crucial pour améliorer la sécurité routière, gérer le trafic et fournir divers services aux utilisateurs des routes.

Pour assurer le bon fonctionnement des VANET, la diffusion régulière de messages de balises par les véhicules joue un rôle essentielles telles que la position, la vitesse et l'état du véhicule. Ils facilitent la détection mutuelle des véhicules, la cartographie du réseau routier et la prise de décisions adaptées à l'environnement de conduite.

Cependant, la propagation incontrôlée des messages de balises peut entraîner une congestion importante du réseau, réduisant son efficacité et nuisant aux performances des applications, ce problème devient particulièrement critique dans les zones à forte densité de véhicules, où le volume élevé de message transmis simultanément fait statuer saturer les canaux de communication.

La gestion des messages balises constitue donc un défi crucial pour assurer le bon fonctionnement des VANET. Il est essentiel de développer des mécanismes régulateurs pour contrôler la quantité et la fréquence des messages diffusés, afin d'optimiser l'utilisation des ressources réseau, maintenir des performances acceptables et garantir la priorité de transmission des messages d'urgence, tout en préservant l'importance des messages balises.

Ce mémoire se compose de trois chapitres distincts :

Le chapitre initial offre une perspective globale sur les réseaux véhiculaires, en définissant les VANET, leurs éléments, les types de messages transmis, les modes de communication spécifiques, et tout ce qui concerne ce domaine.

Les techniques de contrôle de congestion dans les VANET sont présentées dans le deuxième chapitre.

Enfin, le troisième chapitre met l'accent sur notre contribution : un algorithme de gestion de la congestion pour garantir une livraison rapide des messages de sécurité événementiels, tout en préservant l'importance des messages de balise transmis.

En terminant ce travail, nous présentons une conclusion globale qui résume les contributions essentielles de ce mémoire ainsi que les perspectives.

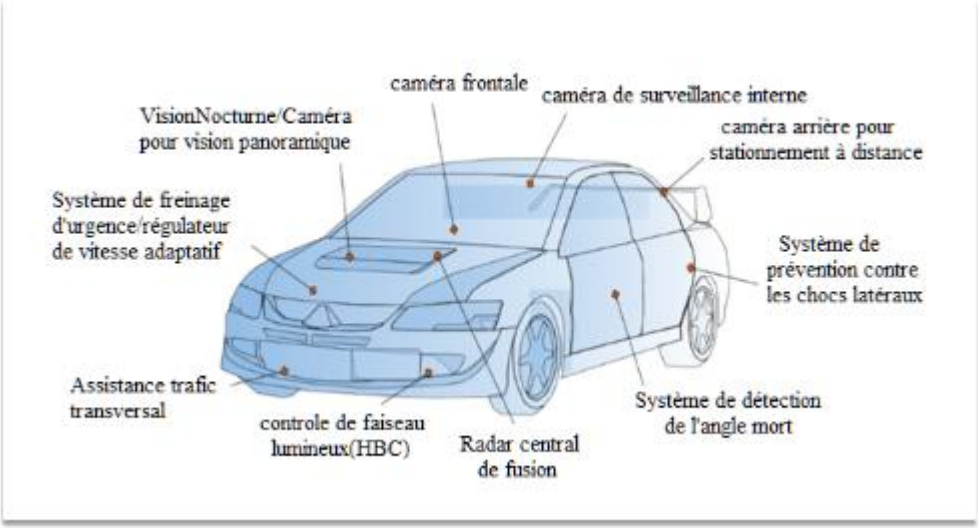
Chapitre 01

1. INTRODUCTION

L'incorporation de l'intelligence dans le domaine automobile vise à améliorer l'expérience utilisateur et les conducteurs au quotidien. Ces applications potentielles sont énormes, incluant, mais sans s'y limiter, le confort, la sécurité et le divertissement. Les idées portent un seul nom : les systèmes de transport intelligents (ITS). Il s'agit d'un terme général qui désigne l'introduction de technologies innovantes d'information et de communication dans le secteur des transports rendant ainsi les systèmes intelligents en raison de leur capacité à effectuer des tâches telles que la perception par les sens (comme la vue), le stockage de la mémoire, la communication entre différents composants, le traitement des données reçues ou la génération de décisions basées sur celles-ci ainsi que l'adaptabilité aux changements de l'environnement. Dans ce chapitre, nous commençons par examiner les réseaux VANETS. Nous définissons les composantes de ces réseaux, les types de messages qui y sont échangés, la manière dont ils communiquent (y compris leurs caractéristiques associées), ainsi que les normes et enjeux.

2. DEFINITION D'UN RESEAU VEHICULAIRE :

Un VANET relève de la classification des réseaux mobiles MANET ; les nœuds de ce réseau sont des véhicules, se distinguent par leurs caractéristiques individuelles ; principalement une grande mobilité. Cela confère un haut niveau de dynamisme au réseau dont la topologie subit des modifications fréquentes et drastiques. Chaque véhicule est doté d'ordinateurs de bord, d'interfaces réseau et de capacités de capteurs pour l'acquisition et l'analyse des données. Un tel scenario souligne le concept de « véhicule intelligent » [1]. La figure 1.1 modélise un véhicule intelligent.



La Figure 1.1 : Exemple de véhicule intelligent

Ce type de réseau aide les voitures à communiquer entre elles et également avec les infrastructures de bord de routes sur lesquelles elles se trouvent.

La Figure 1.2 : Exemple d'un réseau véhiculaire.

3. LES COMPOSANTS D'UN RESEAU VANET :

Afin de mettre en œuvre ce genre de réseau, plusieurs éléments essentiels sont requis afin de permettre la communication entre ces nœuds :

3.1- Les véhicules intelligents : sont équipés de radars et de caméras pour observer leur environnement, de systèmes de localisation GPS et de plateformes de traitement disponibles.

3.2-L'OBU (on board unit) : (connus sous le nom d'entités embarquées) le système central d'un véhicule intelligent est constitué d'une unité de traitement qui interagit avec différentes mémoires de stockage, des interfaces de communication sans fil, des interfaces de contrôle du véhicule et des GPS. Grâce à des éléments logiciels, il est en mesure de repérer les utilisateurs à proximité et de recueillir des données à partir du GPS afin de les présenter.

3.3-RSU : road side unit : Ces dispositifs sont installés le long des routes (connus sous le nom d'entités de bord de routes) et jouent le rôle de points d'accès aux communications. Cela s'explique par le fait qu'ils communiquent aux utilisateurs, les informations sur la situation du trafic, garantissant ainsi un échange bidirectionnel. Son déploiement est restreint en raison de ses capacités de communication à courte portée limitées et de son coût élevé [2].

3.4- Le serveur principal : L'utilisateur ne voit pas le serveur et il peut être un serveur de stockage, un point d'entrée de réseau filaire (Internet) ou un serveur de transactions.

3.5- Autorité Centrale (CA) : cet élément est responsable de l'authenticité des informations, gestion et de l'enregistrement de toutes les entités présentes sur le réseau, qu'elles soient RSU ou OBU, l'AC doit être au courant de : l'identité du véhicule et dans certains cas, de la délivrance et de la distribution de licences de communication et de pseudonymes [4].

4. TYPES DE MESSAGES DANS LES RESEAUX VEHICULAIRES :

Les véhicules produisent et communiquent divers types de messages, tels que des messages de contrôle, d'alerte et autres...

4.1- le message de contrôle :

En fournissant des informations sur la position, la vitesse, la direction et l'itinéraire des véhicules émetteurs, les balises de contrôle ont la capacité de réguler et d'améliorer le trafic routier. Ces données permettent à chaque nœud d'avoir une vision locale de son environnement. Chaque voiture envoie généralement un message de contrôle toutes les 100 millisecondes, ce qui permet de prévoir les risques potentiels ou les embouteillages. [5]

4.2- le message d'alerte :

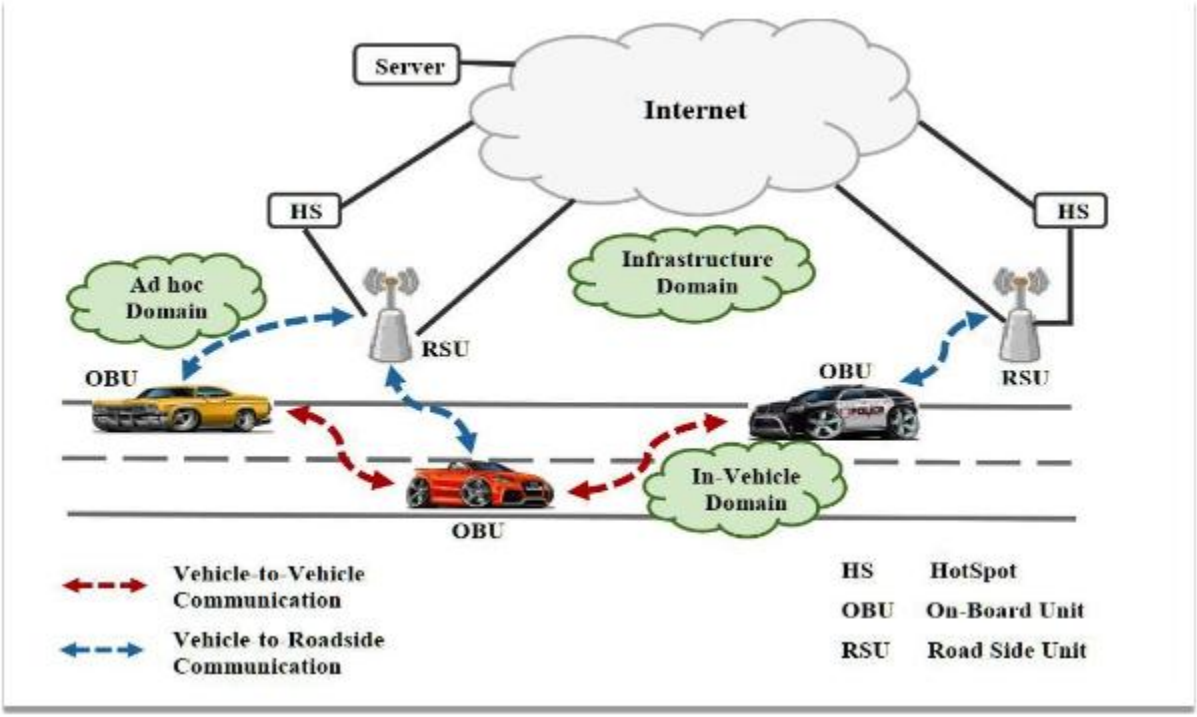
Lorsque des événements tels que des accidents ou des obstacles sont repérés, des alertes sont activées afin de prévenir et de sécuriser le trafic routier. Ces messages incluent les informations de contact de l'événement ainsi que les paramètres de la zone de diffusion. Il est essentiel qu'ils soient régulièrement diffusés et rediffusés, tout en étant de taille. diminuée afin d'être transmise rapidement.

4.3-Autre messages :

Ce genre de message englobe tous les messages qui ne sont ni des contrôles ni des avertissements. Ils visent à améliorer la satisfaction des utilisateurs et ne transmettent généralement pas régulièrement. Cela peut englober, notamment, des opérations financières ou l'envoi d'e-mails.

5. LES MODES DE COMMUNICATION DANS LES VANETS :

Les messages mentionnés précédemment sont transmis lorsqu'une communication est mise en place entre des entités fixes comme l'infrastructure (RSU) et des entités mobiles comme les véhicules. Sur le plan architectural, il y a trois types de communication : la communication entre véhicules (V2V), la communication entre véhicules et infrastructures (V2I) et la communication hybride. [4].



La Figure 1.3: les modes de communication dans les vanets [6]

5.1-communication de véhicule a véhicule (V2V):

La flèche rouge sur la figure 1.3 illustre une architecture décentralisée ou V2V, qui ne se limite qu'à une communication opportuniste entre les véhicules. Quand les véhicules sont proches les uns des autres, ils ont la possibilité de communiquer et de partager du contenu lors d'une interconnexion V2V [2]. Prenons l'exemple d'un accident qui se produit quelques kilomètres devant vous. Le véhicule impliqué signalera les véhicules

qui s'approchent de la zone de l'accident. L'information sera transmise aux véhicules suivants, etc. [7].

Malgré sa rentabilité et son taux de transmission élevé, cette méthode comporte également certains désavantages, tels que : [8]

- Les sauts multiples entraînent des délais de transmission plus élevés.
- Les nœuds sont très mobiles, ce qui entraîne des déconnexions fréquentes.
- Une sécurité routière restreinte.

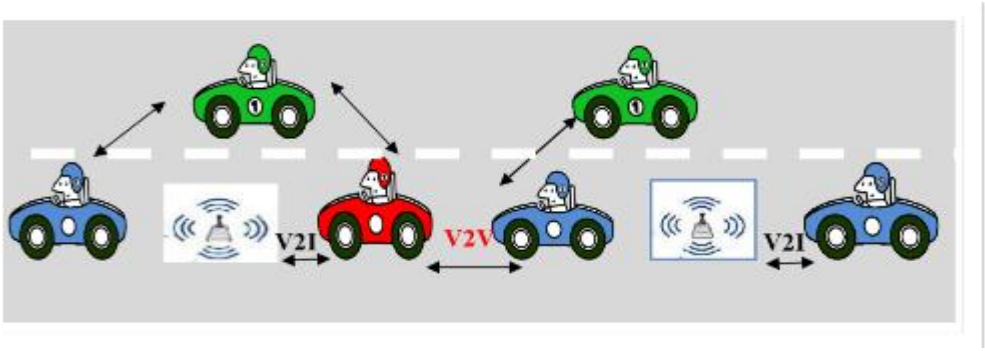
5.2- communication de véhicule à infrastructure (V2I) :

Selon la figure 1.3 (La flèche bleu), les architectures centralisées ou (V2I), reposent sur l'idée que les utilisateurs doivent constamment accéder à un serveur centralisé qui gère leurs interactions avec les autres utilisateurs, même lorsque les véhicules sont proches.

Dans cette structure, les voitures ne communiquent pas directement, elles communiquent plutôt à travers les infrastructures existantes telles que les RSU et les réseaux cellulaires. Le principal inconvénient de cette méthode réside dans la durée et les frais élevés d'installation et de maintenance des stations RSUs. En outre, l'augmentation de la demande peut entraîner une saturation des réseaux cellulaires qui ne couvrent pas toutes les zones, comme les tunnels ou les zones rurales [2].

5.3- communication hybride :

La fusion de ces deux types de communication (V2V et V2I) permet d'élargir la zone de communication et de diminuer les coûts liés à l'installation des infrastructures [9].



La Figure 1.4 : communication hybrides (V2V, V2I). [10]

6. LES CARACTERISTIQUES DES VANETS :

La distinction entre les réseaux véhiculaires ad hoc (VANETs) et les autres réseaux mobiles réside dans plusieurs caractéristiques spécifiques. Voici les caractéristiques principales à prendre en compte pour toute solution spécifique: [8,9,11]

6.1- Gestion de l'énergie et du Stockage :

Les VANETs résolvent les problèmes d'énergie et de stockage qui se posent dans les réseaux mobiles ad hoc. Les véhicules intelligents qui les transportent alimentent directement les dispositifs électroniques, qui sont équipés de différentes interfaces de communication telles que le wifi et le Bluetooth.

6.2- modèle de mobilité :

En raison de la vitesse élevée des nœuds, la mobilité dans les réseaux véhiculaires est très dynamique, ce qui restreint la durée de leurs communications. Il est difficile de prédire les mouvements des nœuds car ils sont influencés par les décisions des conducteurs. Toutefois, les nœuds ont tendance à se déplacer de façon structurée, respectant des routes établies en fonction du nombre de voies disponibles.

6. 3- topologie et connectivité :

Il est courant de constater des variations de topologie dans les VANETs, ce qui permet aux véhicules d'entrer ou de sortir rapidement du réseau, avec des vitesses qui varient en fonction de l'environnement et des informations recueillies par les conducteurs. Par exemple, sur les routes, des vitesses de 120 km/h ont un impact sur la qualité et la durée des échanges entre les véhicules, en raison des modifications rapides de la topologie provoquée par le mouvement des véhicules.

7- LA STANDARDISATION ET LA NORMALISATION DANS LES RESEAUX VANETS :

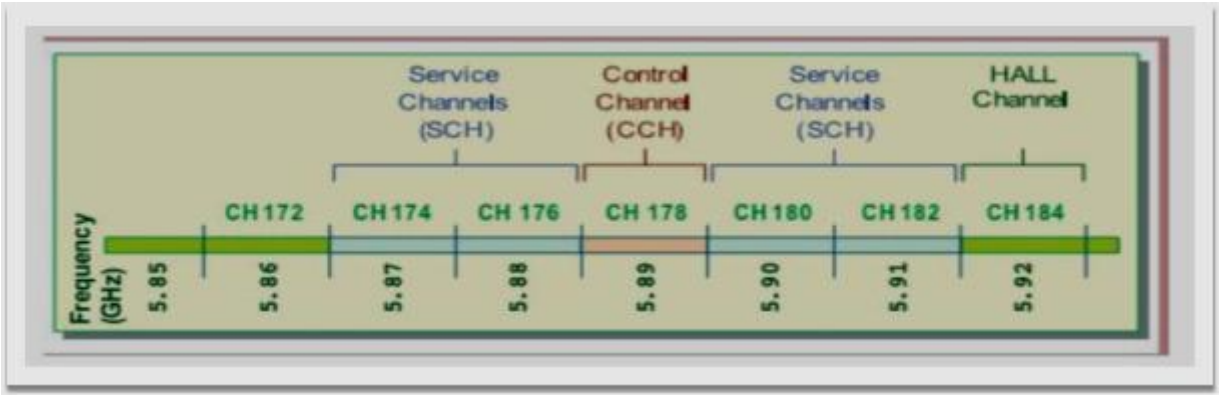
Il est essentiel de respecter les normes de communication afin de favoriser la connexion entre les entités au sein des réseaux de véhicules. Dans cette partie, nous exposons succinctement les normes et les standards de communication employés dans ces réseaux. [3,12]

7.1-DSRC : Dedicated Short Range Communications

Le DSRC, également connu sous le nom de Communication Sans Fil Dédiée à Courte ou Moyenne Portée, est un système de communication sans fil qui peut être unidirectionnel ou bidirectionnel. Son objectif principal est de faciliter les échanges entre véhicules (V2V) et entre véhicules et infrastructures (V2I).

Le système DSRC comprend un terminal de communication (OBU) pour chaque véhicule, tandis que les terminaux fixes situés le long des routes et faisant partie de l'infrastructure sont appelés RSU (Road Side Unit). Au lieu de s'appuyer sur un dispositif particulier pour chaque type d'application, les OBU et les RSU sont des points d'entrée pour toutes les applications mises en place dans les réseaux véhiculaires.

DSRC est un standard de communication radio basé sur la norme IEEE 802.11p, également appelée WAVE (Wireless Access for Vehicular Environments). La transmission avec cette technologie peut atteindre 1000 mètres, avec une bande de fréquence de 5,9 GHz et une largeur de bande totale de 75 MHz (5,850 GHz - 5,925 GHz), répartis en 7 canaux de 10 MHz chacun. Le fonctionnement de ces canaux est divisé en un canal de contrôle et six canaux de service, comme le montre la figure 1.5.



La Figure 1.5 : la norme DSRC

7.2- WAVE : Wireless Access for Vehicular Environment

Un nouveau standard a été créé par le groupe de travail de l'IEEE pour intégrer l'accès sans fil dans l'environnement des véhicules, appelé WAVE ou IEEE 802.11p. Ce standard met en place une structure multicanaux afin de faciliter les échanges pour les applications de sécurité et d'autres services des systèmes de transport intelligents (STI). Il est possible de distinguer deux éléments essentiels : la couche physique du WAVE et la couche MAC du WAVE.

a) La couche physique du WAVE :

WAVE tire sa couche physique de l'IEEE 802.11a. Sur une distance de 1000 mètres, elle peut fournir un débit allant de 6 à 27 Mb/s, avec une modulation de type OFDM (Orthogonal Frequency Division Multiplexing). 7 canaux de communication d'une longueur de 10 MHz sont utilisés pour cette couche physique, chacun situé dans la zone des 5.9 GHz.

b) La couche MAC du WAVE :

La couche MAC du protocole WAVE ressemble à celle du protocole 802.11e, mais la qualité de service (QoS) est spécifiquement élargie. Les messages sont répartis en 4 catégories d'accès (AC : Catégories d'accès), chacune ayant une priorité différente (AC0 étant la plus basse et AC3 la plus élevée). Chaque classe possède une file d'attente distincte, ce qui implique qu'un paquet qui entre dans l'une de ces files doit attendre au moins un temps avant d'être transmis, en fonction des paramètres de contention établis.

8- LES DEFIS LIES AUX RESEAUX VANETS :

8.1- La qualité de service (QoS) : Les utilisateurs des réseaux VANET sont satisfaits grâce à l'efficacité du service. Il vise à assurer la fiabilité des communications pour des applications indispensables comme la sécurité

routière, en assurant des transmissions rapides, fiables et sécurisées qui répondent aux variations du trafic et des conditions urbaines. [13,04]

Pour les applications multimédia, il est primordial d'avoir ces paramètres QoS, car ils sont également liés à la couche MAC des réseaux VANET.

8.2- Routage et dissémination :

Afin de simplifier les échanges entre les véhicules dans les réseaux VANET, il est indispensable d'adopter des protocoles de routage. Lorsque les appareils ne peuvent pas se connecter directement par transmission radio, le routage unicast devient très important pour la communication entre véhicules ou entre un véhicule et une infrastructure fixe. Chaque véhicule peut être utilisé comme émetteur, récepteur ou routeur. Le transfert des données de leur source vers une ou plusieurs destinations doit être effectué de manière efficace, en respectant un délai minimum, une fiabilité élevée et une utilisation optimale des ressources.

8. 3- Sécurité :

L'intégrité des données transmises et la protection des systèmes de transport intelligents contre les attaques sont des éléments essentiels pour garantir la sécurité des VANET. La sécurité des échanges entre les véhicules et la préservation des données personnelles des conducteurs sont indispensables pour cela.

8.4- Congestion :

En général, la congestion survient aux endroits où le trafic est plus demandé que la capacité disponible du réseau. Cela conduit à des retards importants et à des pertes de paquets, car les routeurs refusent les paquets lorsque leurs files d'attente sont remplies. La congestion entraîne une grave dégradation de la qualité de service dans son ensemble.

9. CONCLUSION :

Dans ce chapitre, nous examinons les diverses manières dont les échanges d'informations entre les véhicules peuvent contribuer à l'amélioration de la sécurité routière. Ils améliorent également l'expérience de voyage en offrant une variété de services. Les VANET sont un nouveau domaine de recherche qui englobe différentes disciplines. Comme les messages échangés entre les véhicules jouent un rôle essentiel dans la diffusion de l'information, il est essentiel de s'assurer que ces informations soient reçues en temps voulu. La congestion des canaux constitue l'un des principaux défis des réseaux VANET. Ainsi, dans le prochain chapitre, nous aborderons les méthodes pour gérer la congestion dans les réseaux.

Chapitre 02

1. INTRODUCTION

Il est essentiel de mettre en place des méthodes de gestion de la congestion afin de garantir la continuité des services réseaux. L'objectif de ces technologies est d'éviter la suraccumulation de données à des points précis du réseau, ce qui pourrait entraîner des ralentissements ou même une interruption du flux de données. En réduisant les délais et les pertes de paquets, la gestion de la congestion s'avère être une approche efficace pour garantir la qualité de service (QoS). La régulation de la congestion permettra aux VANETs d'améliorer considérablement leurs performances, assurant ainsi un environnement plus agréable.

Nous abordons dans ce chapitre la définition de contrôle de la congestion, les diverses techniques de détection de la congestion, ainsi que les mécanismes de contrôle qui y sont liés, et on précise les contrôles au niveau couche Mac.

2. CONTROLE DE CONGESTION

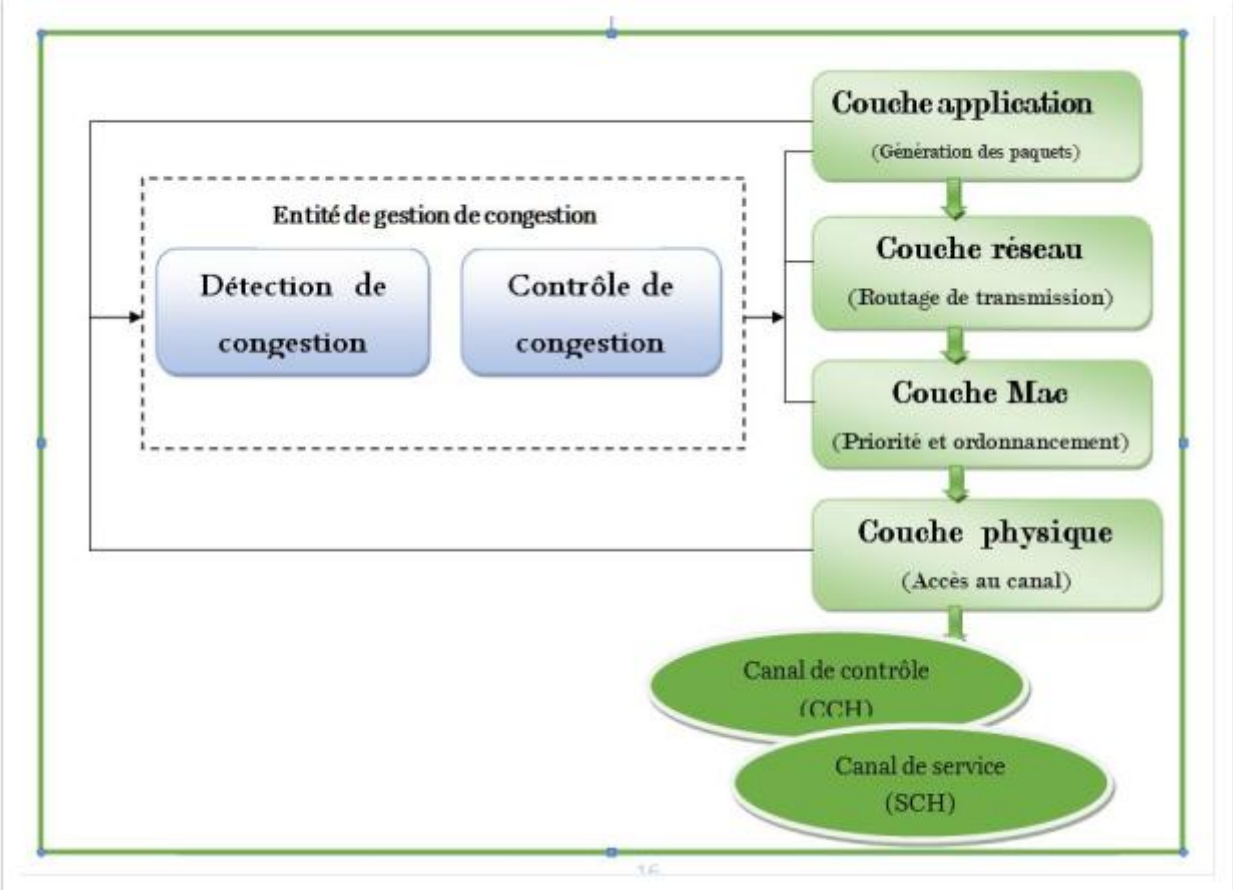
La congestion se manifeste lorsque le nombre de paquets dans le réseau dépasse une certaine limite, en raison du volume d'informations à échanger, ce qui peut mener à une saturation.

En général, chaque réseau partage plusieurs ressources entre ses utilisateurs, entraînant une concurrence pour ces ressources. Il est nécessaire de régler les paramètres du réseau pour maîtriser la charge et éviter la saturation des canaux.

En effet, si la capacité du réseau est inférieure à la charge qu'il supporte, les paquets peuvent être perdus en raison de la congestion, ce qui réduit considérablement le débit du réseau.

Par conséquent, il est essentiel de contrôler la congestion pour prévenir cette situation et assurer la livraison des données dans les réseaux.

De plus, le contrôle de la congestion améliore l'utilisation de la bande passante, la réactivité et l'équité dans l'utilisation des ressources du réseau.



La Figure 2.1 : Architecture de contrôle de congestion entre les couches. [17]

L'architecture du système de contrôle de congestion entre les couches dans les VANets est illustrée dans la figure 2.1. L'objectif de cette architecture est de repérer et de superviser la congestion.

La détection des embouteillages : analyse les données issues de la couche d'application afin de détecter les embouteillages dans le réseau. De plus, il est possible de repérer la congestion en observant le canal au niveau de la couche physique et en étudiant différents paramètres tels que le taux d'utilisation du canal.

Le contrôle de la congestion : peut être effectué de différentes façons à différents niveaux du réseau, comme indiqué ci-dessous :

- En ce qui concerne la couche d'application, il est envisageable de jouer un rôle dans la gestion de la congestion en adaptant les taux de génération de messages pour diverses applications, ce qui permet de diminuer la charge de trafic et la congestion des réseaux.

- En ce qui concerne la couche réseau, il est possible de gérer la congestion en utilisant des algorithmes de routage intelligents qui rediffusent les messages de manière efficace et gèrent la congestion. La mise en priorité et la planification des messages sont réalisées à l'échelle MAC.

En ce qui concerne la couche MAC, elle joue un rôle essentiel dans la gestion de la congestion dans les VANets. Il est également possible d'utiliser le contrôle et la gestion des canaux afin de transmettre les messages de manière adéquate.

3. METHODES DE DETECTION DE LA CONGESTION DANS LES VANETS :

Dans les vanets, il existe deux méthodes de détection de congestion, une détection basée sur les évènements, et une autre basée sur les mesures.

3.1-méthodes basées sur les évènements : (event driven detection) :

Ces méthodes surveillent activement les applications de sécurité et déclenchent un algorithme de contrôle de congestion dès qu'un message de sécurité à haute priorité est détecté. Cet algorithme ajuste le taux d'émission des balises et réduit les files d'attente de transmission MAC, à l'exception de celle du canal de contrôle (CCH), pour assurer une livraison rapide des messages critiques.

Par exemple, lorsqu'un nœud identifie un message de sécurité de type EEBL-F (Emergency Electronic Brake Light with Forwarding), que ce soit via sa couche application ou en le recevant d'un autre nœud, il déclenche immédiatement le contrôle de congestion. Ce processus garantit que les messages de sécurité sont priorisés et livrés avec un minimum de délai, permettant ainsi de répondre rapidement aux situations d'urgence tout en maintenant la qualité de service des applications de sécurité.

Le déclenchement de cet algorithme implique plusieurs actions spécifiques :

Réduction du taux d'émission des balises : Les balises, normalement utilisées pour la communication régulière entre les nœuds, Ils sont réduits en fréquence d'émission pour libérer de la bande passante.

Ajustement des files d'attente de transmission MAC : Les files d'attente de transmission, à l'exception de celle utilisée pour le canal de contrôle, sont ajustées pour favoriser les messages de sécurité. Cela inclut une priorité moindre pour les messages ordinaires.

Priorisation du canal de contrôle (CCH) : La file d'attente du canal de contrôle est préservée pour assurer une transmission sans délai significatif des messages à haute priorité, notamment ceux liés à la sécurité. [23,24]

3.2- méthodes basées sur les mesures : (measurement based detection) :

Ces méthodes surveillent la congestion en effectuant des vérifications périodiques du canal et en évaluant divers paramètres comme le nombre de messages en attente, le temps d'occupation du canal et le niveau d'utilisation. Ces mesures sont ensuite comparées à des seuils prédéfinis qui jouent un rôle crucial dans l'évaluation de la congestion au sein du réseau. Par exemple, lorsqu'une file de canaux de service (SCHs) dépasse un seuil déterminé, cela indique la présence de congestion. Dans ce cas, le nœud correspondant réduit le débit de transmission pour atténuer cette congestion. De plus, chaque nœud peut mesurer localement le temps d'occupation de son canal. Ces mesures sont ensuite comparées

Les seuils préétablis jouent un rôle fondamental dans l'évaluation de la congestion au sein du réseau. Par exemple, lorsqu'une file d'attente de canaux de service (SCHs) franchit un certain seuil, cela signale la présence d'une congestion. Dans une telle situation, le nœud concerné réduit son débit de transmission pour alléger la congestion. En outre, chaque nœud a la capacité de mesurer localement le temps d'occupation de son canal de contrôle (CCH). Si ce temps dépasse une valeur seuil prédéfinie, La transmission des messages de balises (messages périodiques) peut être interrompue par le nœud afin de mieux gérer la congestion.

On peut également détecter la congestion lorsque le niveau d'utilisation du canal dépasse un seuil spécifique, généralement calculé en fonction du processus de transmission des paquets au niveau de la couche MAC du standard WAVE (Accès sans fil dans les environnements automobiles).

Ces approches de détection basées sur les mesures présentent plusieurs avantages significatifs :

1. Elles assurent un équilibre optimal dans l'utilisation des ressources réseau en surveillant activement les files d'attente et le temps d'occupation du canal, ce qui permet d'ajuster efficacement les taux de transmission afin d'éviter les congestions.
2. Elles garantissent une transmission efficace des données en comparant les mesures actuelles aux seuils prédéfinis. Ainsi, le réseau peut réagir rapidement aux signes de congestion, assurant que les données critiques sont transmises avec un minimum de retard.
3. En détectant les congestions, elles évitent les retards et les pertes de paquets en ajustant automatiquement le débit de transmission. Cela favorise l'amélioration de la fiabilité globale des échanges.
4. Elles assurent une réactivité rapide aux situations de congestion en surveillant en continu et en appliquant des seuils précis. Ainsi, les nœuds peuvent rapidement détecter les problèmes potentiels et prendre des mesures adéquates pour minimiser l'impact sur les performances globales du réseau. [24]

4. MECANISMES DE CONTROLES DE LA CONGESTION :

L'optimisation de la charge des canaux à travers des mécanismes de contrôle de la congestion améliore les performances des réseaux VANET, créant des systèmes de communication plus fiables. Gérer efficacement la bande passante est crucial pour éviter la congestion, réduire la perte de paquets, et améliorer l'équité ainsi que la compatibilité entre différents protocoles et normes.

Les mécanismes de contrôle de la congestion dans les VANET peuvent être classés en fonction de leurs stratégies (proactives, réactives, hybrides) et des paramètres ainsi que des méthodes utilisés pour gérer et réguler la congestion. Les stratégies proactives cherchent à anticiper la congestion avant qu'elle ne se produise, tandis

que les stratégies réactives interviennent après avoir détecté la congestion. Les stratégies hybrides combinent ces deux approches pour offrir une solution équilibrée.

4.1- Classification selon les stratégies :

Selon leurs stratégies (proactives, réactives, hybrides) ou les paramètres et méthodes utilisés pour gérer et réguler la congestion, les mécanismes de contrôle de la congestion dans les VANET peuvent être classés. Les stratégies proactives visent à prévoir la congestion avant sa survenue, tandis que les stratégies réactives interviennent après sa détection. Ces deux approches sont combinées dans les stratégies hybrides afin de proposer une solution équilibrée.

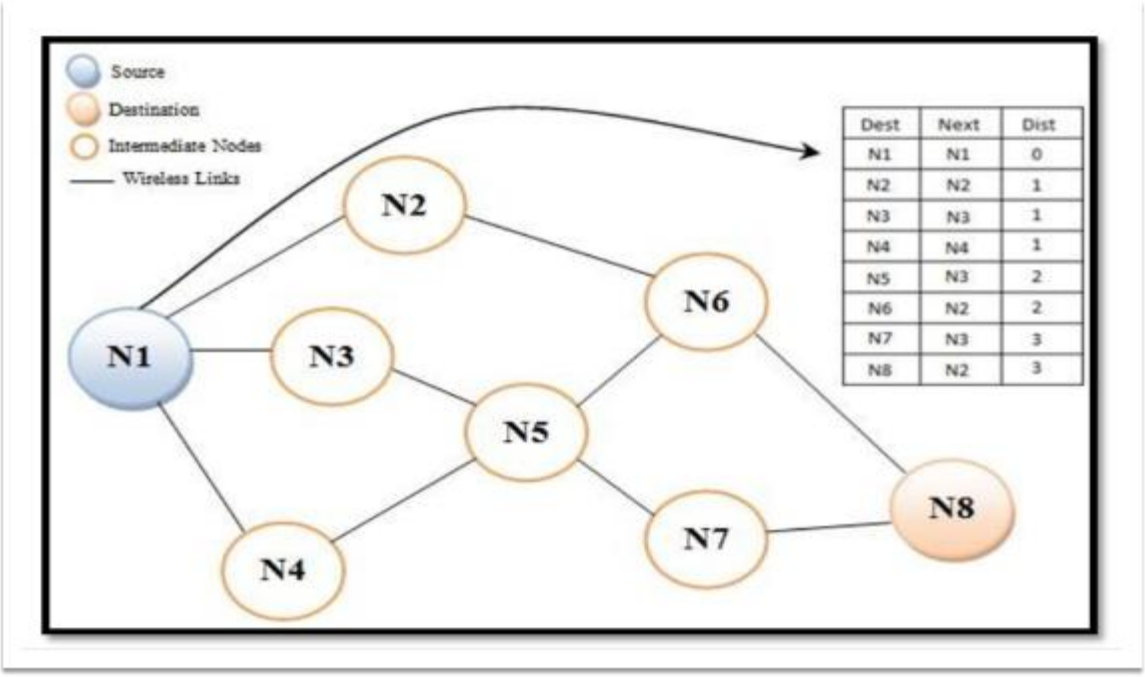
4.1.1- contrôle de congestion proactif :

Les protocoles de routage proactifs maintiennent une table de routage complète qui inclut tous les itinéraires possibles vers les destinations prévues. Ainsi, chaque fois que la topologie du réseau change, le protocole de routage met à jour la table de routage en recalculant les chemins disponibles.

Avantages : Il y a toujours un itinéraire disponible vers chaque destination dans le réseau.

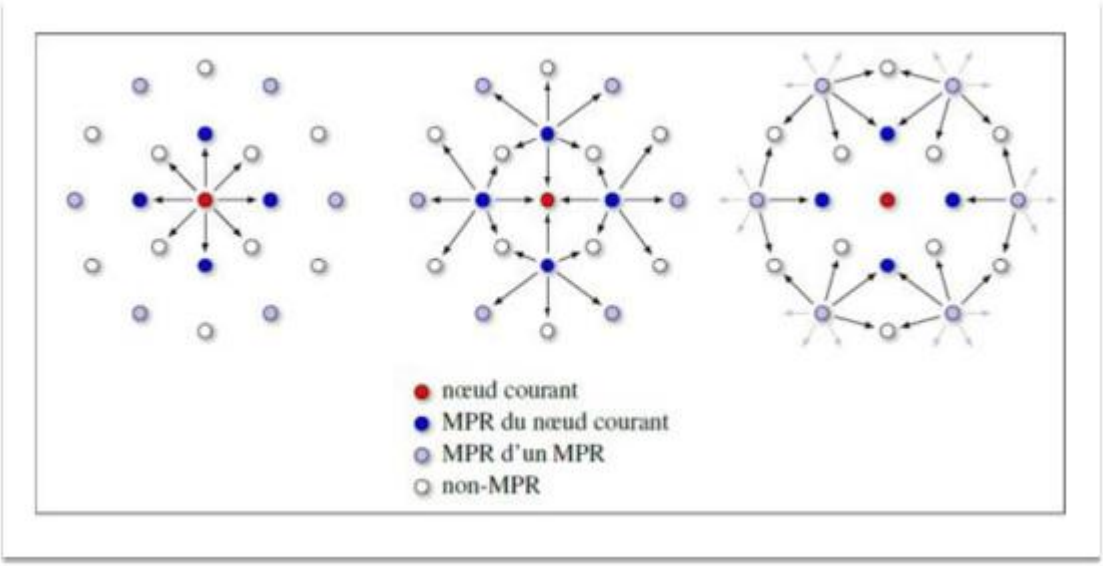
Inconvénients : Il est nécessaire de communiquer régulièrement des informations sur les changements de topologie du réseau. Cela entraîne un volume important de signalisations.

Exemples sur les protocoles proactifs : DSDV, GSR, OLSR.



La Figure 2.2 : exemple DSDV

ü OLSR (Optimized Link State Routing) [15] [25]



La Figure 2.3 : Exemple OLSR

4.1.2. Contrôle de congestion réactif : [5,15 ,28, 29]

Les stratégies réactives fonctionnent comme des solutions de contrôle de congestion en boucle fermée, intervenant après l'occurrence de la congestion dans les réseaux. Ces protocoles

fonctionnent en créant une table de routage contenant au moins un chemin vers le(s) nœud(s) cible(s). À chaque nouvelle communication, cette table est recalculée afin de déterminer un chemin vers la destination.

Les bénéfices :

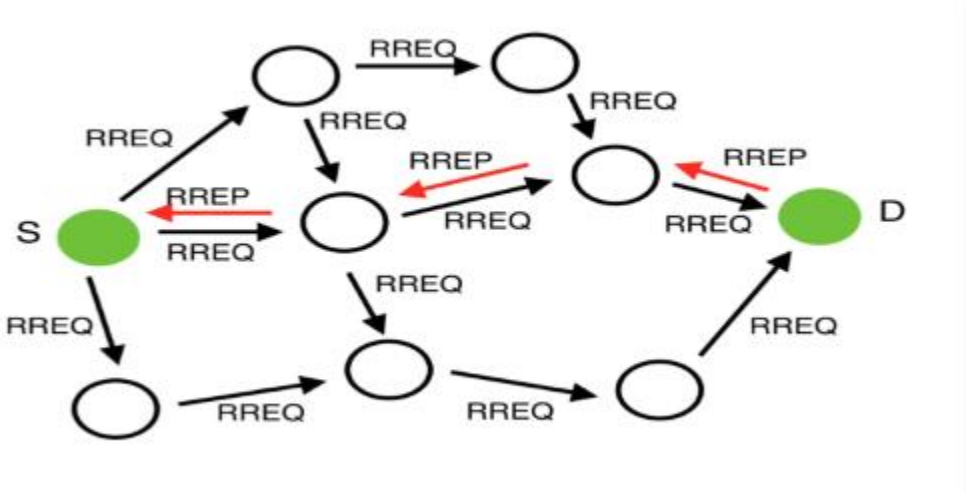
L'utilisation d'un paquet de routage périodique n'est pas requise ; les nœuds mobiles ne conservent pas ou peu d'informations sur la topologie globale du réseau, seules les informations sur les routes actives sont conservées. À première vue, les protocoles réactifs génèrent une quantité de signalisations moindre.

Les désavantages :

Le retard dans la construction (ou la reconstruction) des routes est causé par la mise en place de protocoles réactifs, ce qui rend la création de routes optimales moins facile.

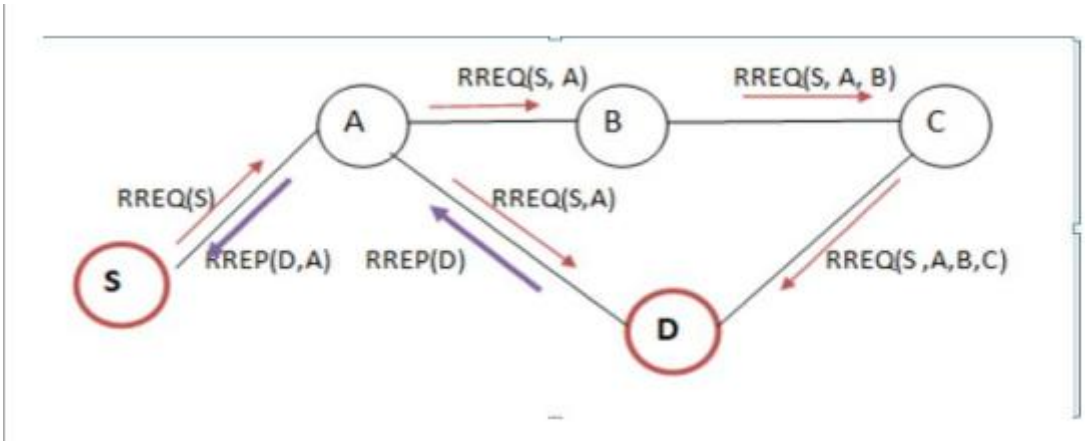
La problématique de l'évolutivité réside également dans le fait qu'elle repose sur des diffusions aveugles pour explorer les chemins.

Exemples sur les protocoles réactifs : DSR, AODV [25]



La Figure 2.4 : Exemple de fonctionnement de l' AODV.

ü DSR (Dynamic Source Routing) : [26]



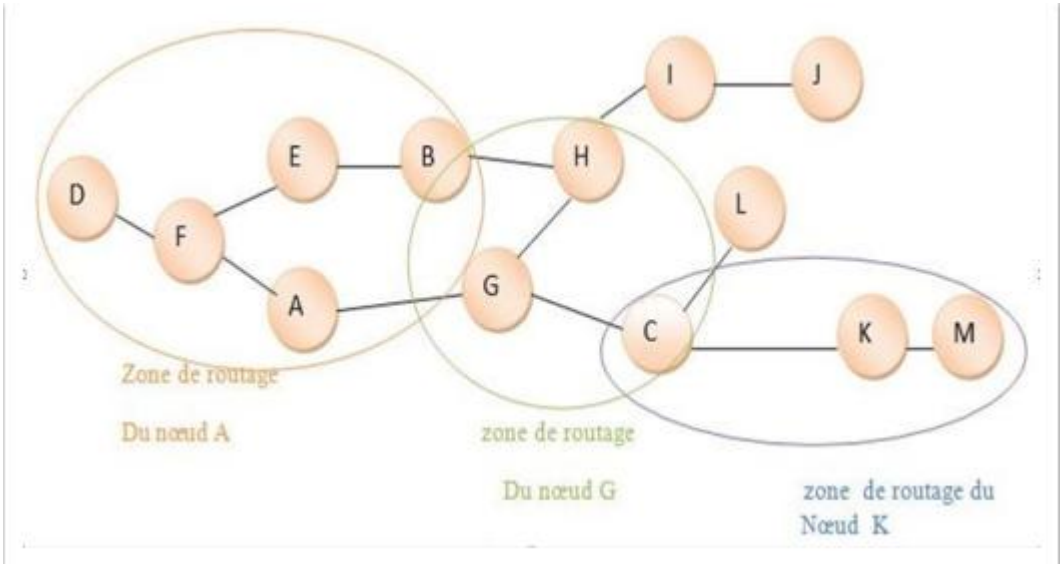
La Figure 2.5 : Exemple de fonctionnement de DSR

4.1.3. Contrôle hybride :[15,29]

Ce protocole combine les principes des deux catégories précédentes pour gérer la congestion : il utilise une approche proactive pour identifier les voisins proches (jusqu'à deux ou trois sauts), garantissant ainsi des chemins immédiatement disponibles dans le voisinage immédiat. Au-delà de cette zone, le protocole hybride adopte des techniques réactives pour la découverte des routes. Cette méthode divise le réseau en plusieurs zones, optimisant ainsi la recherche réactive de chemins : lorsqu'un nœud reçoit une requête de recherche réactive, il peut rapidement déterminer si la destination est à proximité. Si tel est le cas, il redirige la requête vers d'autres zones sans perturber son propre secteur. Un exemple courant de protocole de routage hybride est le ZRP.

Ce protocole permis de tirer à tirer parti des bénéfices des deux approches antérieures en intégrant une architecture de découpage du réseau. Néanmoins, il maintient certains désavantages des approches proactive et réactive

ZRP (Zone Routing Protocol):



La Figure 2.6 : Exemple de fonctionnement de ZRP

4.2- Classification selon les paramètres et les moyens :

On peut classer les techniques de gestion de la congestion pour les réseaux VANET en fonction de divers critères. Le critère principal de cette classification repose sur la façon dont les mécanismes de contrôle ajustent les paramètres de transmission. En général, cinq classes principales peuvent être distinguées :

* Stratégies basées sur le taux de répartition

* Stratégies reposent sur la capacité d'émission

* les stratégies basées sur csma/ca

* basées sur la hiérarchisation et l'ordonnancement

* les stratégies hybrides.

4.2.1. Stratégies basées sur le taux de transmission :

De manière dynamique, les stratégies modifient le débit de transmission ou le taux de génération des paquets pour contrôler la congestion. Nous présentons ici un protocole particulier employé dans cette situation :

Adaptive Traffic Beacon (ATB) : ce protocole est employé afin de modifier de manière dynamique l'intervalle de diffusion des messages en fonction de la qualité du canal et de l'utilité des messages diffusés.

La qualité du canal et l'utilité des messages sont évaluées en utilisant des mesures comme le signal/bruit (SNR), le nombre de véhicules et l'état du réseau, la protection et l'efficacité.

Cependant, malgré ses avantages, cette approche rencontre des défis dans les environnements très dynamiques et hétérogènes. Elle pourrait notamment ne pas intégrer de manière optimale les paramètres spécifiques de la couche MAC, limitant ainsi sa capacité à réagir efficacement aux variations rapides des conditions du réseau. De plus, la réduction du taux de balisage peut poser des problèmes pour certaines applications critiques nécessitant des informations fréquentes et précises pour fonctionner de manière optimale.

4.2.2. Stratégies reposent sur la puissance d'émission:

La puissance de transmission est régulée de manière dynamique par ces stratégies afin de contrôler la charge des canaux. Généralement, Les applications de sécurité envoient leurs messages à une distance considérable pour couvrir une vaste zone, ce qui permet à de nombreux nœuds de les recevoir. Toutefois, en cas de congestion du réseau, il est nécessaire que certains véhicules diminuent leur émission afin de réduire les collisions sur les canaux. un protocole permis lesquelles sont développés dans ce contexte est présenté ci-dessous. : [31]

- Cross layer congestion control model for urban vehicular environments :

  Ce modèle est conçu pour gérer et réduire la congestion du trafic dans les zones urbaines en exploitant la communication entre différentes couches du réseau dans les véhicules et l'infrastructure. En combinant

des informations en temps réel issues de différentes sources comme les véhicules et les systèmes d'infrastructure, le modèle émet des choix éclairés afin d'optimiser le flux de circulation, diminuer les délais de déplacement et renforcer la sécurité routière. En employant des méthodes comme la collecte de données, la communication d'informations, la gestion adaptative des incendies de circulation et la modélisation prédictive, ce modèle vise à améliorer l'efficacité globale du trafic urbain.

4.2.3. Stratégies basées sur CSMA / CA:

Les paramètres clés tels que la taille de la fenêtre de contention et l'intervalle AIFS (arbitration inter frame space) sont employés afin de contrôler l'accès au canal dans le protocole CSMA/CA, couramment employé dans les réseaux sans fil. Contrairement au CSMA/CD utilisé dans les réseaux câblés, le CSMA/CA vise à prévenir les collisions plutôt qu'à les détecter après leur occurrence.

Fonctionnement de CSMA/CA

Écoute du Canal :

Avant de transmettre des données, chaque nœud vérifie si le canal est déjà utilisé par d'autres transmissions. Si une activité est détectée, le nœud retarde sa transmission pour éviter une collision. Sinon, il attend un intervalle de temps aléatoire avant de commencer à transmettre pour s'assurer que le canal reste libre. Cet intervalle est déterminé par la fenêtre de contention.

RTS/CTS (Request to Send/Clear to Send) :

Le protocole utilise un mécanisme appelé RTS/CTS (Request to Send/Clear to Send) pour coordonner les transmissions entre les nœuds.
Un nœud envoie un paquet RTS au destinataire avant d'envoyer des données afin de solliciter la permission de transmettre.

Si le destinataire répond avec un paquet CTS, cela indique qu'il est prêt à recevoir des données, et la transmission peut alors avoir lieu.

Dans le cadre du protocole CSMA/CA, Lorsqu'une collision est détectée ou que le canal est déjà occupé, le nœud en attente entre dans une phase de backoff, durant laquelle il suspend sa tentative de transmission pendant un laps de temps aléatoire. Cette fenêtre de contention croît de manière exponentielle à chaque échec de transmission, ce qui contribue à diminuer les risques de collisions répétées. De plus, le protocole utilise l'Interval AIFS (Arbitration Inter-Frame Space) pour déterminer le temps d'attente après la libération du canal, avant qu'un nœud ne recommence à transmettre. Ce délai peut varier selon les classes de service attribuées, permettant par exemple aux données critiques de bénéficier d'un accès plus rapide au canal par rapport à d'autres types de données moins prioritaires

CSMA/CA présente plusieurs avantages significatifs dans les réseaux sans fil. Tout d'abord, et grâce à l'utilisation de l'écoute du canal et d'un dispositif de réparation, ce protocole diminue considérablement les risques de collisions ; En outre, en modifiant l'intervalle AIFS et la période de contention., CSMA/CA permet de prioriser certains types de trafic, comme les données critiques, assurant ainsi leur transmission rapide et efficace. En environnement partagé, où de nombreux nœuds utilisent le même canal, CSMA/CA régule efficacement l'accès pour minimiser les interférences. Cependant, ce protocole peut introduire des retards dus au processus d'écoute et d'attente, ce qui peut poser problème pour les applications nécessitant des transmissions en temps réel.

4.2.4. Stratégies basées sur la hiérarchisation et l’ordonnancement :

Approches basées sur la hiérarchisation et l'organisation : L'objectif de ces approches de gestion de la congestion est d'évaluer l'efficacité de la classification des messages en fonction des canaux de contrôle (CCH) et de service (SCH). Les messages critiques reçoivent une priorité élevée, facilitant ainsi leur accès et leur transmission, ce qui réduit les retards et prévient la

saturation des canaux. En organisant l'ordre de transmission des messages, ces stratégies réduisent les collisions et améliorent l'utilisation des réseaux VANET. Il est essentiel de gérer de manière méthodique les priorités afin d'éviter les embouteillages et de garantir la fluidité des communications.. Parmi les algorithmes utilisés à cette fin, on trouve FIFO, LWT, MRF, FDF, SDF, LTSF, MQIF et D S, chacun offrant des avantages spécifiques adaptés aux besoins du réseau.

Par exemple, FIFO privilégie les premiers messages arrivés, tandis que LWT accorde la priorité aux messages en attente depuis plus longtemps. Une approche innovante proposée par C.Suthaputchak se concentre spécifiquement sur l'amélioration de la diffusion des messages de sécurité en attribuant des priorités ajustées pour un accès plus rapide aux canaux. Cependant, il est essentiel de noter que ces stratégies peuvent améliorer la fiabilité pour les messages prioritaires sans nécessairement prendre en compte la bande passante disponible ou le taux d'occupation lors des retransmissions.

4.2.5. Stratégies hybrides :

Ces méthodes combinent diverses techniques pour une gestion efficace de la congestion dans les réseaux VANET. Elles règlent le débit et la puissance de transmission, contrôlent la taille de la fenêtre de contention et accordent des priorités adéquates à chaque message tout en organisant leur transmission dans les canaux, afin d'éviter la saturation et les dysfonctionnements

Une étude récente menée par Huang et ses collaborateurs ont mis au point L'algorithme AVOCA (algorithme de contrôle de congestion basé sur les véhicules), ce qui permet d'optimiser la transmission des paquets en fonction des variations de la couverture du réseau. AVOCA surveille de manière régulière les performances de la couche de transport et modifie constamment les paramètres de gestion des embouteillages pour maintenir un débit optimal lorsque les véhicules entrent ou sortent des zones de couverture grâce à cette approche innovante .

5.LES PRINCIPAUX PROTOCOLES MAC PROPOSES POUR LES VANETS:

5.1. MCTRP : Multi Channel Token Ring Protocol

Le protocole Token Ring Multi Channels Bi et ses collaborateurs ont développé un système utilisant des anneaux et des jetons sur plusieurs canaux de communication distincts. L'objectif est de créer une approche MAC déterministe permettant une organisation autonome des nœuds du réseau en anneaux, visant à améliorer la bande passante et réduire les délais. Chaque nœud est équipé de deux radios : une connectée en permanence au canal 178 du système 'WAVE' pour les transmissions entre anneaux, et une autre sur l'un des six autres canaux 'WAVE' pour les communications internes à l'anneau, quel que soit le type de message. Cependant, le protocole présente des contraintes, notamment en termes de robustesse. Le MCTRP dépend fortement de la présence des nœuds sur les anneaux. Par exemple, si le leader d'anneau se déplace, s'éloigne ou quitte la portée du réseau, tous les nœuds connectés à cet anneau seront déconnectés, ce qui rend le MCTRP plus adapté aux réseaux avec une mobilité limitée. De plus, le protocole requiert une connexion continue entre chaque nœud de l'anneau, car le jeton doit circuler de manière chronologique d'un nœud à l'autre. Cette exigence est complexe à satisfaire dans les réseaux véhiculaires, souvent instables et imprévisibles, ce qui complique la mise en œuvre du MCTRP dans des contextes réels.

5.2. DMMAC :

Selon [14], Lu et ses collègues ont introduit un nouveau protocole d'accès au canal pour les réseaux véhiculaires, nommé DMMAC, qui utilise la technologie WAVE. Ce protocole vise à assurer une transmission sans collision des messages de sécurité pendant l'intervalle CCHI (Contrôle Channel Interval), divisé en deux parties distinctes : CCHI pour le canal de contrôle et SCHI pour les canaux de service. DMMAC combine les techniques TDMA (Accès multiple par répartition dans le temps) et CSMA/CA (Accès multiple avec écoute de porteuse et évitement de collision).

SCHI est réservé aux messages d'information, tandis que CCHI est destiné aux messages de sécurité. Les deux sous-intervalles de CCHI, ABF et CRP, sont séparés par une frontière flexible ajustée en fonction du nombre de nœuds dans la portée. ABF permet la diffusion de messages de sécurité à plusieurs points, similaire au CCH dans WAVE.

5.3. STDMA :

D'après [14], STDMA est une variante du protocole MAC basée sur le TDMA, conçue pour assurer des délais de transmission optimaux pour les messages critiques en matière de sécurité, tout en minimisant les risques de collisions. La trame de STDMA est constituée d'un ensemble prédéfini de créneaux synchronisés par le temps GPS pour tous les nœuds du réseau. Chaque nœud sélectionne un groupe spécifique de créneaux auxquels il peut accéder. Voici une explication détaillée de l'organisation des messages utilisée par ce protocole : Une fois les créneaux attribués, chaque nœud transmet ses données et éventuellement un message d'urgence pendant son créneau assigné, conformément au fonctionnement standard du TDMA. Cependant, STDMA présente des contraintes qui peuvent le rendre inadapté dans certaines situations.

5.4. VeMAC :

Dans l'article [141], Hassan Aboubakr Omar et ses collègues ont développé une étude sur VeMAC, un protocole MAC déterministe multicanaux conçu pour améliorer les performances en réduisant les collisions. Ce protocole assure des communications point à point et multipoint en utilisant deux récepteurs radio par nœud : l'un dédié au canal de contrôle (c0) et l'autre pouvant se connecter à plusieurs canaux de service (c1 à cm). La synchronisation est assurée par des signaux GPS.

Le canal de contrôle (c0) organise les paquets en plusieurs champs, notamment l'en-tête, l'annonce de service (AnS), l'acceptation de service (AcS), et les applications courtes à haute priorité. Pour éviter les problèmes de terminal caché, chaque message envoyé sur c0 inclut les espaces temps réservés par tous les voisins à un instant précis, facilitant ainsi la planification efficace des transmissions par le récepteur en fonction des disponibilités.

Les fournisseurs, définis comme tout nœud proposant un service sur un canal de service spécifique selon le champ AnS sur c0, sont chargés de l'attribution des slots aux utilisateurs. VeMAC utilise les sept canaux réservés à DSRC (un canal de contrôle et six canaux de service) pour réduire efficacement les collisions. Cependant, ce protocole présente des contraintes telles que le risque de surcharge de débit et les retards dus à la taille importante des paquets de contrôle sur c0, ainsi qu'une rigidité apparente dans des environnements à forte densité.

6. CONCLUSION :

Dans ce chapitre, nous avons établi une définition du problème de congestion et exposé les différentes techniques pour détecter la congestion. Par la suite, nous avons étudié les différents protocoles utilisés pour contrôler la congestion, ainsi les principaux protocoles MAC proposés pour les VANETs seront abordés. Le chapitre suivant exposera notre protocole de gestion de congestion en détaillant son fonctionnement.

Chapitre 03

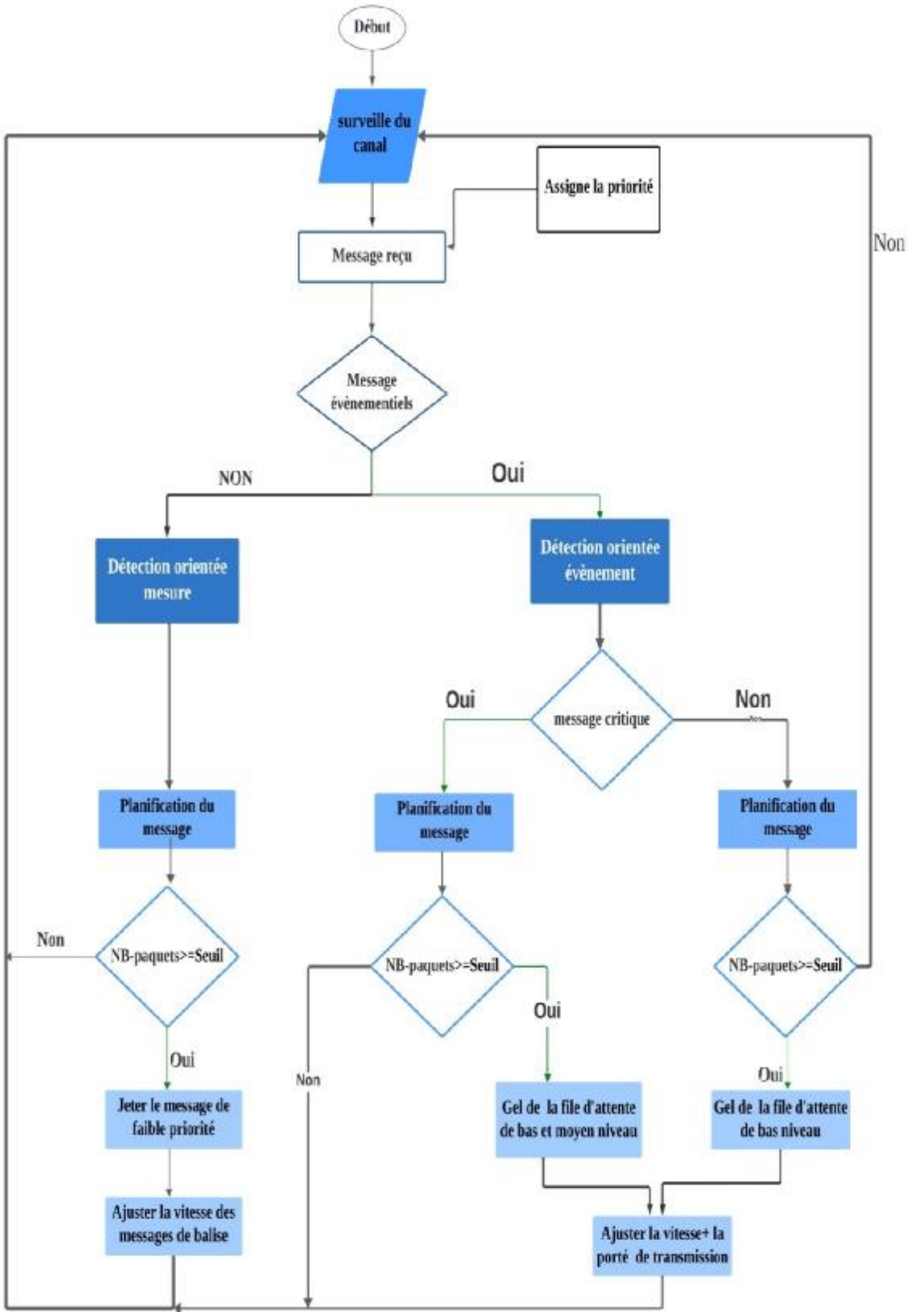
1.INTRODUCTION :

Dans le but de remédier aux lacunes des protocoles de contrôle de congestion déjà en œuvre dans les réseaux VANETs, qui sont souvent incomplets et peuvent entraîner de nouveaux problèmes tout en cherchant à les résoudre, nous avons développé un algorithme de contrôle de congestion au niveau de la couche MAC.

Cet algorithme vise à assurer la transmission sans retard des messages de sécurité événementielle essentiels, comme les alertes d'accidents, et de prendre en compte l'importance des messages de contrôle échangés entre les véhicules.

2. ALGORITHME DE CONTROLE DE CONGESTION PROPOSE :

Au cours de cette étude, nous avons suggéré un algorithme de gestion de la congestion afin de garantir une livraison sans retard des messages de sécurité évènementiels. La Figure 3.1 ci-dessous présente les différentes étapes de l'organigramme de l'algorithme de gestion de la congestion proposé.



La Figure 3.1 : L'organigramme de l'algorithme de contrôle de congestion proposé.

Le processus commence par :

Etape01 : Début et Surveillance du Canal :

Le processus débute par la surveillance continue du canal de communication (Control Channel, CCH). Cette étape implique une écoute active pour détecter les messages entrants. La surveillance permet de déterminer la disponibilité du canal et d'identifier les messages potentiels qui pourraient influencer la planification des messages ultérieurs.

Etape02 : L'affectation De Priorité :

Le diagramme débute par la réception du message, qui est ensuite analysé pour déterminer son type et son importance selon sa priorité. Cette analyse conduit à la création de trois files d'attente :

- File d'attente de niveau supérieur : regroupe les messages prioritaires, tels que ceux relatifs à des accidents, des conditions météorologiques, etc. Ces messages sont considérés comme critiques et reçoivent la priorité la plus élevée.
- *File d'attente de moyen niveau* : regroupe les messages de priorité moyenne, par exemple ceux annonçant des événements importants sur la route qui ne représentent pas un danger immédiat. Ces messages sont classés comme non critiques et reçoivent une priorité moyenne.
- *File d'attente de bas niveau* : regroupe les messages de faible priorité, comme les messages périodiques ou ceux servant à la surveillance du réseau (messages de balise).

- Pour cela, nous avons mis en place une fonction nommée assignPriorityToFIFOQueue(cMessage msg), définie comme suit :

```
void MyApplication::assignPriorityToFIFOQueue(cMessage* msg) {
    // Identifier le type de message et attribuer la priorité en conséquence
    if (msg->getType() == HIGH_PRIORITY_MSG) {
        highPriorityQueue.insert(msg);
    } else if (msg->getType() == MEDIUM_PRIORITY_MSG) {
        mediumPriorityQueue.insert(msg);
    } else if (msg->getType() == LOW_PRIORITY_MSG) {
        lowPriorityQueue.insert(msg);
    }
}
```

Etape03 : Planification Des Message :

En fonction de la priorité attribuée au message (élevée, moyenne, faible), l'organigramme établit la stratégie de planification en fonction du délai de transmission, qui représente le temps maximum autorisé (deadline) pour diffuser le message à tous les véhicules destinataires. Chaque file d'attente ordonne ces messages selon leurs deadlines en ordre croissant."

```
void MyApplication::calculateDSValue(cMessage* msg) {
    simtime_t currentTime = simTime(); // Temps actuel
    simtime_t deadline = msg->getDeadline(); // Définir la deadline de chaque message
    int size = msg->getSize(); // Taille du message en octets
    int DS_Value = (deadline - currentTime) * size; // Calcul de la valeur DS
    // Utilisez DS_Value comme critère pour l'affectation de priorité
}
```

```
void MyApplication::DS_SchedulingAlgorithm() {
    // on deux listes triées D-List et S-List contenant les délais et les tailles de données respectivement
    // on doit parcourir ces listes et calculer les valeurs DS
    int minDS = INT_MAX; // Initialisez à une valeur maximale pour la comparaison
    cMessage* selectedMsg = nullptr; // Message sélectionné à envoyer

    for (auto msg : D_List) { // Parcourez la D-List triée par ordre croissant
        int deadline = msg->getDeadline(); // Récupérez le délai du message
        int size = S_List[msg->getIndex()]; // Récupérez la taille de données correspondante dans la S-List
        int DS_Value = (deadline - simTime().dbl()) * size; // Calcul de la valeur DS

        if (DS_Value < minDS) { // Si la valeur DS est plus petite que la valeur minimale actuelle
            minDS = DS_Value; // Mettez à jour la valeur minimale de DS
            selectedMsg = msg; // Sélectionnez ce message pour l'envoi
        }
    }

    // Envoyez le message sélectionné
    if (selectedMsg) {
        send(selectedMsg, "out");
    }
}
```

Etape 04: détecter et à contrôler la congestion:

Pour gérer la congestion, nous avons opté pour deux méthodes : la détection basée sur les événements et la détection basée sur les mesures.

Les événements sont surveillés par la détection orientée événement: Dès qu'un message de sécurité spécifique à un événement est détecté ou généré, les déclencheurs de messages décident d'activer l'algorithme de contrôle de congestion. Afin de réduire les délais d'envoi des messages de sécurité, le contrôle de congestion active immédiatement la méthode de gel des files d'attente pour les files d'attente de transmission MAC et ajuste la transmission.

Gestion des files d'attente en congestion:

Pour les messages événementiels critiques Si le nombre de paquets reçus dépasse un seuil spécifique (indicateur de congestion), les messages à faible et moyenne priorité sont temporairement gelés.

Pour les messages événementiels non critiques : Si le nombre de paquets reçus dépasse ce seuil, les messages à faible priorité sont gelés et la vitesse des messages de balise est ajustée aux messages événementiels non critiques

Ajustement de la transmission : Si les messages sont gelés ou supprimés, il est envisageable d'ajuster la vitesse et la portée de transmission pour diminuer la congestion et améliorer l'efficacité du réseau.

- La détection de la congestion orientée mesure:

Elle consiste à surveiller le canal CCH en fonction de la file d'attente des paquets. Le canal CCH est considéré comme encombré lorsque le nombre de messages dans la file d'attente dépasse un seuil prédéfini. Dans notre algorithme de contrôle de congestion proposé, une action de suppression d'un message balise est entreprise Chaque fois que la longueur de la file d'attente des paquets dépasse ce seuil, cela est suivi d'un ajustement de la vitesse

```
void MyApplication::sendCongestionControlMessage() {
    // Vérifier si la congestion est détectée dans les files d'attente
    if (highPriorityQueue.getLength() > HIGH_CONGESTION_THRESHOLD) {
        sendCongestionControlMessageToMAC(highPriorityQueue);
    } else if (mediumPriorityQueue.getLength() > MEDIUM_CONGESTION_THRESHOLD) {
        sendCongestionControlMessageToMAC(mediumPriorityQueue);
    } else if (lowPriorityQueue.getLength() > LOW_CONGESTION_THRESHOLD) {
        sendCongestionControlMessageToMAC(lowPriorityQueue);
    }
}
```

```
void MyApplication::adjustTransmissionSpeed(cMessage* msg, double speed) {
    // Ajustez la vitesse de transmission du message
    msg->setSpeed(speed); //  la nouvelle vitesse de transmission
}
```

```
void MyApplication::sendCongestionControlMessageToMAC(cQueue& queue) {
    // Envoyer un message de contrôle de congestion à la couche MAC
    if (!queue.isEmpty()) {
        cMessage* congestionMsg = queue.pop();
        send(congestionMsg, "out");
    }
}

void MyApplication::manageCongestion() {
    // Parcours de la file d'attente pour gérer la congestion
    while (!packetQueue.isEmpty()) {
        cMessage* msg = packetQueue.pop(); // Récupérez le prochain message dans la file d'attente
        int priority = msg->getPriority(); // Récupérez la priorité du message

        if (priority == LOW_PRIORITY) {
            EV_INFO << "Congestion detected: Dropping low priority message.\n";
            delete msg; // Supprimez le message de faible priorité
        } else {
            // Ajustez la vitesse de transmission des messages de balises
            if (priority == HIGH_PRIORITY) {
                adjustTransmissionSpeed(msg, HIGH_PRIORITY_SPEED);
            } else if (priority == MEDIUM_PRIORITY) {
                adjustTransmissionSpeed(msg, MEDIUM_PRIORITY_SPEED);
            }
            // Envoyez le message avec la nouvelle vitesse de transmission
            send(msg, "out");
        }
    }
}
```

3. CONCLUSION :

Cette contribution présente notre solution : un algorithme de contrôle de congestion qui combine deux approches, à savoir celle basée sur les événements et celle basée sur les mesures.

Cette combinaison permet d'améliorer significativement le contrôle de la congestion en donnant la priorité aux délais comme critère principal de planification.

Grâce à cette planification, il est possible de gérer efficacement la congestion tout en assurant le traitement en temps opportun des messages critiques.

De plus, elle permet ajuster dynamiquement les files d'attente et la vitesse de transmission en fonction du trafic réseau.

Ce processus vise à assurer une surveillance continue et des ajustements réactifs qui contribuent à maintenir La satisfaction du client dans un contexte réseau en constante évolution et soumis à la contrainte de grande vitesse des nœuds.

Conclusion Générale

CONCLUSION GENERALE

Les avancées technologiques dans le domaine des réseaux et des télécommunications ont apporté de nombreux avantages à divers domaines de la recherche et du développement, notamment dans le secteur des transports. Les réseaux VANETs, une sous-catégorie des réseaux ad hoc mobiles (MANETs), représentent un nouveau champ de recherche prometteur, riche en possibilités pour le développement d'applications innovantes.

Dans ce mémoire, nous avons proposé des améliorations aux systèmes de communication des réseaux ad hoc véhiculaires pour optimiser la qualité de service. Notre objectif principal était de mieux contrôler la congestion dans ces réseaux pour rendre les communications plus fiables et sécurisées.

Pour atteindre cet objectif, nous avons commencé par une étude approfondie des réseaux VANETs afin de bien situer notre travail dans son contexte. Ensuite, nous avons effectué une synthèse des techniques de contrôle de congestion existantes. Enfin, nous avons développé un algorithme destiné à prévenir la congestion sur le canal CCH. Cet algorithme s'appuie sur la surveillance de l'occupation du canal, l'attribution de priorités, et prend en compte les délais des messages. Sur la base d'un seuil prédéfini, il calcule le taux de transmission et ajuste ensuite ce taux pour prévenir la congestion.

Perspectives

Pour les travaux futurs, nous envisageons de simuler l'algorithme proposé afin de vérifier sa pertinence et son efficacité dans des conditions réalistes. Nous prévoyons également de comparer cet algorithme avec d'autres protocoles similaires afin d'évaluer ses performances et d'identifier les éventuelles améliorations à apporter dans les recherches à venir.

Bibliographie

[1] :Saliha BENKERDAGH:Prise en compte des contraintes temporelles dans les réseaux véhiculaires, Thèse de Doctorat, Université de Mostaganem, Décembre 2019

[2]: Farouk Mezghani : La dissémination de contenus dans les réseaux véhiculaires, Thèse de Doctorat, Institut National Polytechnique de Toulouse (INP Toulouse) 2015.

[3] : HERAIZ Aboubakr,MAATOUG Wassim : Simulation d'une approche adaptative de diffusion à un saut dans les réseaux ad-hoc véhiculaires, diplôme de Master Académique 2021/2022

[4] : ZIREG Tahar , BOUAOUD Idir : Routage d'information dans les réseaux Véhiculaires (VANET), diplôme de Master Académique , Université de bouira , 02/07/2023,

[5] : Melle BAAZIZ Thiziri ,Melle MAOUCHE Rima : Techniques de contrôle de congestion dans les réseaux véhiculaires, Université Abderahmane Mira de Béjaïa, 2017/2018.

[6] : Nasrin Taherkhani : Congestion Control in Vehicular Ad Hoc Networks, Thèse de doctorat, École Polytechnique de Montréal, 2015

[7]: Zaater hayet ,Chaib rima : Etude des modèles de mobilité de véhicules et leur simulation, Mémoire de fin d'étude Master, Université de Guelma , 2011.

[8] : Slimane Boucefar, Walid Boucefar : La qualité de service dans les réseaux véhiculaires (VANET), Mémoire de fin d'étude Master, universite mouloud mammeri de tizi-ouzou, 2017.

[9] : Laib said : Contrôle de congestion décentralisé pour les communications de véhicule,Mémoire de Master,universite l'arbi ben mehidi oum el bouaghi, 2020/2021.

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

[11] : Nadia Haddadou, Réseaux ad hoc véhiculaires : vers une dissémination de données efficace, coopérative et fiable, Thèse de doctorat, Université Paris-EST, 2014.

[12] : Saidi Abdessamad, Mamem Wafa : Amélioration des performances du protocole de routage EGyTAR dans les réseaux VANETs, Mémoire de Master, Université Abou Bakr Belkaid– Tlemcen, 2016/2017.

[13]: Nabil OUAZENE : Pour une QoS au niveau de la Couche MAC dans les Réseaux Sans Fil, Mémoire de magistère,Université Hadj Lakhdar – Batna,2009.

[14] Bennai yani athmane, Pr.louiza Bouallouche-Medjkoune,Dr.Samira Yessad, synthèse sur les principaux protocoles Mac proposés pour les vanets, doctoriales de recherche opérationnelle, le 12 et 13 décembre 2018.

[15] : Benmoumene Safaa , Boukhaloua Fatima : Simulation et analyse de protocoles de routage dans les réseaux VANET, Mémoire de Master, univesité IBN KHALDOUN – TIARET, 2019.

[16]: M. A. Benatia, L. Khoukhi, M. Esseghir, L. Merghem Boulahia :A Markov Chain Based Model for Congestion Control in VANETs, University of Pierre and Marie Curie -Paris VI, Paris, France, 2013 27th International Conference on Advanced Information Networking and Applications Workshops.

[17] : Y. Zang, L. Stibor, X. Cheng, H.-J. Reumerman, A. Paruzel, and A. Barroso, ”Congestioncontrol in wireless networks for vehicular safety applications,” Proceedings of the 8th Euro-pean Wireless Conference, 2007.

[18] : Mlle Maouche Nadira et M. Oudia Jugurta, Approche à base d’alliances dans les graphes pour la réduction de la congestion dans les VANETs, master, Université A/Mira de Béjaia, 2017.

[19] : CEN et al.: end-to-end differentiation of congestion and wireless losses: ieee/acm transactions on networking, vol. 11, no. 5, october 2003.

[20] : Yung Yi and Sanjay Shakkottai : Hop-by-hop Congestion Control over a Wireless Multi-hop Network, 133-144, (2007).

[21] : E. Setton, J. Noh, and B. Girod : Congestion distorsion optimized peer-to-peer video streaming. Proceedings IEEE International Conference on Image Processing (ICIP), pp. 721-724, (2006).

[22] : J. Nzouonta, T. Ott, and C. Borcea. Impact of queuing discipline on packet delivery latency in ad hoc networks. Performance Evaluation, 66(12), pp. 667-684., (2006).

[23] : M. Yusof Darus and K. Abu Bakar. A review of congestion control algorithm for event-driven safety messages in vehicular networks. volume 8 of 1, pages 169430814. In Journal ofComputer Science Issues, 2011.

[24] : M. Yusof Darusa and K. Abu Bakar. Congestion control algorithm in vanets. volume 21of 7, pages 105731061. In Journal of World Applied Sciences, 2013.

[25] : Naceur karima , Oukidi mimouna : gestion du trafic routier urbain de la ville de tiaret à l'aide de la technologie vanet, mémoire de master, univesité ibn khaldoun – tiaret 2020-2021

[26] : Guehguih Bachira ,Krika Yousra Djihad : Routage dans les réseaux vanet, mémoire de master, Université Mohamed Sadik Benyahia – JIJEl, 2015/2016.

[27] : ATMAOUI Souhila ,AMIR Ouassila, Contrôle de congestion dans les réseaux VANETs, mémoire de master, Université A/Mira de Béjaia, 2017.

[28] : Jonathan Ledy : Stratégie d'adaptation de liens sur canaux radios dynamiques pour les communications entre véhicules Optimisation de la qualité de service, thèse doctorat, université de poitiers 2006.

[29] : Liana Khamis Qabajeh, Dr. Miss Laiha Mat Kiah, Mohammad Moustafa Qabajeh : A Qualitative Comparison of Position-Based Routing Protocols for Ad-Hoc Networks, IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.2, February 2009.

[30] : C. sommer, O.k. tonguz , f. dressler : traffic information systems: efficient message dissemination via adaptive beaconing. Computer and Communication Systems, Institute of Computer Science, University of Innsbruck, Austria.

[31] : Lokesh M.Gripunje, Deepika Masand, and Shishir Kumar Shandilya : congestion control in vehicular Ad-hoc Networks (vanet's) : a review, vit bhopal university, bhopal, india.