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

Université A/Mira de Béjaïa

Faculté des Sciences Exactes

Département d'Informatique

Mémoire De Fin de cycle

En vue d'obtention du diplôme de master professionnel en informatique spécialité : Administration et Sécurité des Réseaux Informatiques

Thème

Etude comparative des protocoles de dissémination de données dans les VANETs

---

Réalisé par :

- M^elle BOUZRAA Sylia
- M^elle LASSOUAG Samira

Soutenu devant le jury composé de :

Présidente	**M^me OUYAHIA.S**	**U.A/MiraBéjaïa.**
Examinatrice	**M^me BELKHIRI.L**	**U.A/MiraBéjaïa.**
Examinatrice	**M^me AIT HACENE.S**	**U.A/MiraBéjaïa.**
Encadreuse	**M^me ZIDANI.F**	**U.A/Mira Béjaïa.**

2016/2017

Dédicaces

Je dédie mon travail à mes très chers et
respectueux parents

Qui m'ont soutenu tout au long de ma vie ainsi qu'à mes chères sœur
Kahina,Nadira,Aichouche et Siham

À mes neveux Maria, Adem et Imane

À mes beaux-frères Khelifa et Redouane

À mes grands-parents, mes cousins et cousines, Oncles et tantes

À mon binôme Sylia ainsi que sa famille

À mes ami(e)s et collègues,
À toutes personnes qui m'a aidé et
encouragé de prêt Ou de loin tout au long de
mes études

Samira

Je dédie mon travail à mes très chers et
respectueux parents,
À mes frère Karim Moukhtar et Yanis et ma
sœur Samia, mon beau-frère et belles sœurs
Yasmine et Sassa et neveux,
À ma précieuse famille, mes cousins et cousines,
Oncles et tantes, À mon fiancé Tarik et toutes la
famille LAMARA,
À mon binôme Samira ainsi que sa famille

À mes amis et collègues
Et à toutes les personnes qui m'ont aidé et encouragé de prêt
Ou de loin tout au long de mes études

Sylia

Remerciements

Nous tenons dans un premier temps à remercier et rendre grâce au bon Dieu le tout puissant qui nous a donné le courage et la volonté pour mener à bien ce modeste travail.

Nous tenons à exprimer tout d'abord notre vif remerciement pour notre encadreuse Mme **ZIDANI Ferroudja**, de nous avoir encadré pour réaliser ce travail par la disponibilité de son temps précieux, ses encouragements, ses aides, ses conseils avisés, sa gentillesse...
Nous tenons, également, à remercier vivement les membres du jury pour l'honneur qu'ils nous ont fait en acceptant de juger ce travail. Nos remerciements vont aussi à tous nos enseignants et toutes les personnes qui nous ont soutenus jusqu'au bout, et qui n'ont pas cessé de nous donner des conseils très importants en signe de reconnaissance.
Nos sincères remerciements s'adressent à nos parents, nos frères, nos sœurs ainsi qu'à toute la famille pour leur encouragement inconditionnels et surtout pour la confiance qu'ils nous accordent.

Enfin, Nous remercions tous ceux qui ont contribué de près ou de loin à l'élaboration de notre travail, en particulier tous nos ami(e)s pour leur soutien et leur présence à nos côtés.

Samira&Sylia

Table des matières

Table des figures

Liste des tableaux

Liste d'abréviation

AC Access Control.

ACK Tame d'Acquittement.

ADCD Satrategie de Dissemination adaptée aux Données Classifiées.

CGM Consumer Generated Media

CSMA/CA Carrier Sense Multiple Access with Collision Avoidance.

DAB Digital Audio Broadcasting.

DDT Distance Defer Transfer.

DGPS Differential Global Positioning System

DMB Digital Multimedia Broadcasting.

DPP Directional Propagation Protocol.

DSRC Dedicated Short-Range Communication

DVB-H Digital Video Broadcast handheld.

DVB- T Digital Video Broadcast terrestrial.

EDCA Enhanced Distributed Channel Access.

EDGE Enhanced Data for)Evolution

FCC Federal Communication Commission.

GPS Global Positioning System.

GSM Global System for Mobile communication

IEEE Institute of Electrical and Electronics Engineers.

ITSA Intelligent Transportation Society of America.

IVC Inter-Vehicle Communication.

IVG Inter- Vehicle Geocast .

LTE Long Term Evolution.

MAC Medium Access Control.

MANET Mobile Ad hoc Networks.

MDDV Mobility- centric Data Dissemination algorithm for Vehicular networks.

MHVB MultiHop Vehicular Broadcast

OAPB Optimized Adaptive Arotocol Aroadcast

OBU On-board Unit.

ODAM Optimized Dissemination of Alarm Messages

RBM Role-Based Multicast.

RDS Radio Data System.

RSUs Road Side Units.

STEID Spatio- Temporal Information Dissemination.

STI Society of Technology Industrials.

TGP Task Group P.

TMC Traffic Message Channel.

TRADE TRack Detection.

TTL Time To Live.

UMB Urban Multi-Hop Broadcast protocol.

UMTS Universal Mobile Telecommunications System.

VANET Vehicular Ad hoc Networks.

V2I Vehicle to Infrastructure.

V2V Vehicle to Vehicle.

WAVE Wireless Access in Vehicular Environment.

WIFI Wireless Fidelity.

WSMP Wave Short Message Protocol.

Introduction générale

Depuis quelques années, le besoin d'être connecté est devenu fondamental pour l'homme. Ce besoin pose de plus en plus de défis pour la technologie moderne l'obligeant à plus d'innovation et de créativité. Ainsi, de nouvelles technologies sont apparues comme les réseaux sans fil, et les réseaux Ad Hoc.

Actuellement, Grâce aux avancées technologiques, il est possible de doter les véhicules d'un moyen de localisation tel que le GPS « Global Positioning System », d'une OBU *« Onboard Units »* implémentant le standard WAVE/DSRC et d'une carte réseau afin de former un réseau dynamique nommé réseau ad hoc véhiculaire (VANET). Tous ces équipements permettent de traiter et de transmettre l'information aux autres véhicules. Les réseaux véhiculaires sont majoritairement composés de véhicules intelligents qui communiquent entre eux et/ou avec des unités de bords de route (RSUs), lorsque celles-ci sont déployées.

Tout comme les réseaux ad hoc mobiles (MANETs), les réseaux ad hoc véhiculaires utilisent exclusivement les communications sans fil, mais leurs caractéristiques les rendent plus complexes que les réseaux MANETs. En effet, la forte mobilité des véhicules, l'étendue des zones à couvrir, ainsi que leur densité font que la topologie du réseau est hautement dynamique, ce qui affecte la qualité des connexions entre les véhicules et les rend irrégulières.

Les services qu'ils proposeront auront pour objectif premier de diminuer le nombre d'accidents de la route, d'améliorer le trafic routier et de l'optimiser grâce à leurs applications de sûreté et de gestion du trafic. En plus, ces réseaux pourront fournir des applications ludiques, qui participent à l'amélioration du confort au sein du véhicule. Ces applications nécessitent le partage de données entre utilisateurs, avec une certaine qualité de service. Cependant, les caractéristiques des réseaux VANETs compliquent la dissémination et l'acheminement des données.

Notre étude s'étale sur trois chapitres ;

Dans le premier chapitre nous commençons dans un premier temps par définir les réseaux Ad Hoc, leurs principales caractéristiques ainsi que leurs contraintes, puis nous donnons une vue d'ensemble sur les réseaux Ad Hoc véhiculaires (VANET) ; à savoir les entités communicantes, les standards de communication, l'architecture de communication, leurs caractéristiques ainsi les différents types d'application de ces réseaux.Nous terminons par quelques problèmes lies aux VANTEs.

Dans le deuxième chapitre, nous présentons la notion de dissémination et leurs techniques, puis nous décrivons les stratégies liées aux applications d'urgences et de confort.

Dans le troisième chapitre nous présentons une description des principaux défis liés à la dissémination de l'information de sécurité dans un réseau de véhicules. Par la suite, nous exposons une classification des différents mécanismes qui ont été présentés dans la littérature, selon deux approches de conception, à savoir, l'approche de conception de haut niveau et l'approche de conception bas niveau. Nous nous concentrons particulièrement sur les mécanismes de sélection du prochain nœud relai et les techniques utilisées. Nous présentons également une classification des métriques utilisées pour évaluer les performances des protocoles de dissémination, et les paramètres de simulation utilisés lors de cette évaluation.

Enfin, nous terminons cette étude par une conclusion générale.

Chapitre 1 : Vue d'ensemble sur les réseaux ad hoc véhiculaires

1.1. Introduction

De nos jours, les véhicules sont considérés autrement que de simples moyens de transport, bien plus. Grâce aux avancées technologiques récentes, une multitude de nouvelles fonctionnalités sont associées aux véhicules, ce qui les dote d'une source d'intelligence de par leurs interactions avec l'environnement routier. En exploitant leurs récentes capacités de communication, la création d'un réseau permet de rendre plus agréable le temps qu'on passe à bord, tout en améliorant la sécurité routière. Dans ce contexte, les réseaux ad hoc véhiculaires (VANETs) participent en permettant le partage, de manière collaborative, de différents types de données entre les véhicules. Dans ce chapitre, nous commençons dans un premier temps par définir les réseaux Ad Hoc, leurs principales caractéristiques ainsi que leurs contraintes, puis nous donnons une vue d'ensemble sur les réseaux Ad Hoc véhiculaires.

1.2. Définitions

1.2.1. Les réseaux Ad hoc

Les réseaux ad hoc sont des réseaux sans-fil capables de s'organiser spontanément et de manière autonome dans l'environnement dans lequel ils sont déployés sans infrastructure définie préalablement. La tâche de la gestion du réseau est repartie sur l'ensemble d'entités communicantes par liaison sans-fil, ces entités sont souvent appelées «nœuds». Dans ces réseaux, les entités envisagées sont des terminaux légers et de taille réduite qui fonctionnent sur batterie, donc elles ont des capacités de traitement et de mémoire limitées [1].

Les réseaux ad hoc, dans leur configuration mobile, sont connus sous le nom de MANET (pour Mobile Ad-hoc Networks).

La figure 1.1 montre un exemple de transmission d'un message dans un réseau ad hoc entre deux équipements distants A et C, comme ces deux derniers ne peuvent pas communiquer directement à cause de la portée limitée du support de transmission utilisés, alors ils utilisent l'équipement B comme relai.

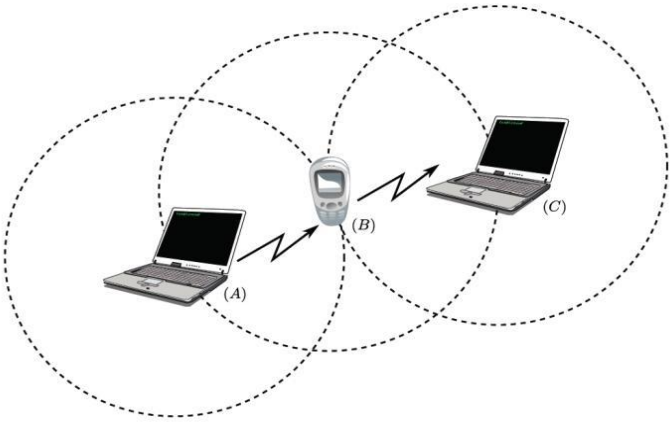

Figure 1-1 : Exemple de transmission d'un message dans un réseau ad hoc [1].

L'entité A veut communiquer avec C. Puisqu'elles sont hors de portée directe de transmission, A transmet son message vers B, qui à son tour le relai vers C.

A. Caractéristiques des réseaux Ad Hoc [2] [3] [4]

Les réseaux mobiles Ad Hoc présentent plusieurs caractéristiques à savoir :

- **Absence d'infrastructure**

Les nœuds d'un réseau Ad Hoc travaillent dans un environnement pair à pair totalement distribué, ce qui leur permet de se déplacer librement. Ces nœuds agissent en tant que routeurs pour relayer des communications ou générer leurs propres donnés.

- **Routage par relais**

Dans un réseau Ad Hoc, un terminal peut communiquer directement avec les terminaux ses voisins. Lorsqu'une machine veut communiquer avec une autre se trouvant hors de sa portée, chaque nœud actif du réseau sert de routeur pour ses voisins.

On reprend l'exemple précédant de la figure 1.1, la machine A, veut communiquer avec la machine C se trouvant hors de son champ de réception. Pour aboutir, la connexion réseau va donc utiliser la machine B se trouvant à portée de réception des machines A et C des réseaux Ad Hoc.

- **Topologie dynamique**

Une particularité très importante qui distingue les réseaux mobiles Ad Hoc des réseaux filaires est la mobilité de ses nœuds. Les nœuds sont libres de se déplacer arbitrairement, des routes peuvent se créer et disparaître très souvent, ce qui provoque des changements fréquents dans la topologie du réseau. Ces modifications doivent être

prises en compte par le protocole de routage. Cette caractéristique rend la topologie de ce type de réseau sans fil très dynamique.

- **L'hétérogénéité des nœuds**

Un nœud mobile peut être équipé d'une ou plusieurs interfaces radio ayant des capacités de transmission variées et opérant dans des plages de fréquences différentes. Cette hétérogénéité de capacité peut engendrer des liens asymétriques dans le réseau. De plus, les nœuds peuvent avoir des différences en terme de capacité de traitement (CPU, mémoire), de logiciel, de taille (petit, grand) et de mobilité (lent, rapide). Dans ce cas, une adaptation dynamique des protocoles s'avère nécessaire pour supporter de telles situations.

- **La taille des réseaux**

Elle est souvent de petite ou moyenne taille (une centaine de nœuds) ; le réseau est utilisé pour étendre temporairement un réseau filaire, comme pour une conférence ou des situations où le déploiement du réseau fixe ne sont pas approprié. Cependant, certaine applications des réseaux Ad Hoc peuvent nécessiter une utilisation allant jusqu'à des dizaines de milliers de nœuds.

- **Multi-sauts**

Les réseaux Ad Hoc utilisent souvent des sauts multiples pour éviter les obstacles, minimiser la consommation d'énergie ou pour joindre un nœud qui n'est pas dans la portée de communication de l'émetteur.

B. Les contraintes liées aux réseaux Ad Hoc [3] [4] [5] [6] [7]

Les réseaux mobiles Ad Hoc exposent plusieurs contraintes suivantes :

- ### Bande passante limitée

La communication dans les réseaux Ad Hoc se base sur le partage d'un médium de transmission (les ondes radio), ce qui induit que la bande passante réservée pour un hôte soit modeste.

- ### Contrainte d'énergie

Les nœuds mobiles sont destinés à être portables et mobiles et donc à être alimentés par des sources d'énergie autonomes comme les batteries ou les autres sources consommables (exemple d'énergie solaire). La durée de vie des batteries est limitée, ce qui se répercute par conséquent sur les services et les applications supportées par chaque nœud. Le paramètre d'énergie doit être pris en considération dans tout le contrôle fait par le système.

- Liens unidirectionnels

Un lien unidirectionnel représente la possibilité qu'un nœud soit entendu (à portée d'ondes) par un autre mais pas l'inverse. Cela arrive notamment lorsque les puissances d'émission sont différentes suivant les émetteurs (mode de propagation des ondes). Ce qui pose un problème des acquittements que l'on ne peut pas envoyer.

- Sécurité physique limitée

Les réseaux mobiles Ad Hoc sont très sensibles aux attaques extérieures par rapport aux réseaux filaires classiques. Les données envoyées transitent par des équipements d'utilisateurs inconnus ce qui pose un problème de confidentialité et nécessite l'utilisation d'outils de cryptage et de sécurisation des données.

- Interface radio multiple

Lorsqu'un nœud possède plusieurs interfaces radio, les protocoles deviennent tout de suite beaucoup plus complexes, car chaque interface possède sa propre zone de couverture.

- Changement de topologie

La mobilité des nœuds provoque des changements fréquents dans la topologie du réseau. La réactivité du dispositif mis en place face à ces modifications a un impact direct sur la qualité du service proposé à l'utilisateur.

- Interférences

Les liens radio ne sont pas isolés, ce qui fait que le taux d'erreur de transmission dans les réseaux radio est plus élevé que dans les réseaux filaires. Cela est dû généralement aux problèmes d'interférences qui peuvent être de natures diverses, à savoir :

- Le nombre limité de canaux disponibles.
- Les fréquences d'émissions sont proches, ainsi, les émetteurs travaillent à des fréquences proches peuvent interférer entre eux.
- Les bruits produits par l'environnement (certains équipements électriques, certains moteurs...).
- Les phénomènes d'atténuation, réflexion et des chemins multiples qui rendent le signal incompréhensible en le déformant.

- La mobilité des nœuds et maintenance des routes

La mobilité continue des nœuds crée un changement dynamique de topologie. Par exemple, un nœud peut joindre le réseau, changer de position ou quitter le réseau. Ce déplacement a naturellement un impact sur la morphologie du réseau et peut modifier le comportement du canal de communication. Ajoutons à cela, la nature des

communications (longues et synchrones, courtes et asynchrones,...). Les algorithmes de routage doivent ainsi résoudre ces problèmes et supporter la maintenance et prendre en charge en un temps limité la reconstruction des routes tout en minimisant l'over head généré par les messages de contrôle.

1.2.2. Les réseaux VANETs (Vehicular Ad hoc NETwork) [28]:

Les réseaux VANETs sont en effet une partie émergente des réseaux sans fil, ils ont une forme de Mobile Ad-hoc Network (MANET) où les nœuds mobiles sont des véhicules intelligents, on parle de la notion de « véhicule intelligent » quand un véhicule est équipé de dispositifs de communications sans fil, cartes réseau et de capteurs. Et tous cela, afin de fournir des communications au sein d'un groupe de véhicules à portée les uns des autres et entre les véhicules et les équipements fixes à portée, usuellement appelés équipements de la route ou (RSU).

Figure 1-2 : Un exemple des réseaux VANET [5].

A. Nœuds d'un réseau VANET

Un nœud d'un réseau VANET est un véhicule équipé de terminaux tels que les calculateurs, les interfaces réseaux ainsi que des capteurs qui sont capables de collecter les informations et de les traiter comme s'est illustré par la figure 1.5.

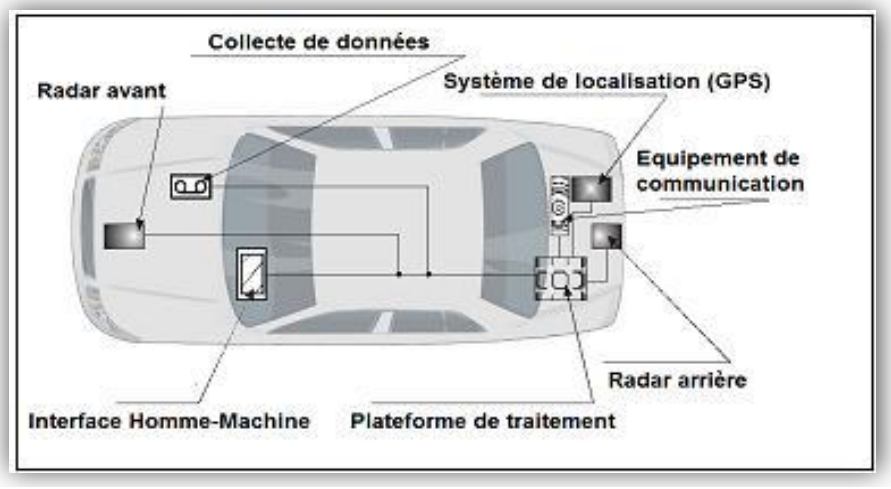

Figure 1-3 : Les éléments constituant le véhicule intelligent [9].

B. Les composants d'un réseau véhiculaire [10]

Les principaux composants qui constituent un réseau véhiculaire sont les suivants :

- **Les usagers routiers** : dans les réseaux véhiculaires, les conducteurs et les passagers peuvent participer aux communications. Ces utilisateurs peuvent jouer le rôle de consommateur, de fournisseur de contenus ou les deux à la fois. De nos jours, le nombre d'accidents de la route et d'infractions à la circulation augmente en raison de l'utilisation des équipements mobiles et des équipements embarqués dans les véhicules. Par conséquent, il est nécessaire de prévoir un mécanisme qui réduit sensiblement l'interaction du conducteur avec les dispositifs de bord lors du partage de contenus. À titre d'exemple, une architecture a été proposée qui consiste à partager automatiquement des informations détectées par les capteurs dans les véhicules.
- **L'équipement mobile** : les véhicules sont équipés d'On-Board Units (OBUs) permettant de détecter les utilisateurs à proximité, de communiquer et de partager des contenus avec eux. Pendant ces dernières années, plusieurs projets européens et internationaux ont montré, avec des prototypes et des expérimentations, la faisabilité et l'importance des communications véhiculaires dans le cadre de plusieurs applications.
- **L'infrastructure :** certaines applications conçues pour les réseaux véhiculaires sont centralisées ou utilisées par l'infrastructure quand cette dernière existe. Globalement, les infrastructures qui peuvent être utilisées dans les réseaux véhiculaires sont les Road Side Units (RSUs) et les réseaux cellulaires. D'une part, les RSUs offrent des communications à courte portée et restent peu déployées en raison de leur coût élevé. D'autre part, les réseaux cellulaires offrent des communications à longue portée les plus souvent coûteuses.

C. Types de messages dans les VANETs [11]

Les entités forment un réseau sans fil véhiculaire vont générer et s'échanger des messages. En fonction de l'application et du contexte environnemental, un véhicule peut envoyer (ou recevoir) un message de contrôle, d'alerte ou « autre ».

- Message de contrôle

Un message de contrôle est généré à intervalle régulier. Conventionnellement, chaque véhicule émet un message de contrôle toutes les 100 ms. Ce message, appelé aussi «beacon», contient la position, la vitesse, la direction et l'itinéraire du véhicule émetteur. Grâce aux messages de contrôle, chaque véhicule se crée une vue locale de son voisinage. Le véhicule peut aussi prédire et anticiper des situations accident ogènes ou de congestion. Le message de contrôle est l'équivalent du message HELLO des protocoles de routage. Chaque véhicule se fait donc connaître de son voisinage direct. Bien entendu, les messages de contrôle ne sont pas transférés et utilisent une diffusion à un saut.

- Message d'alerte

Le message d'alerte est généré lorsqu'un événement est détecté. Cela peut être la détection d'un accident, d'un obstacle ou la réception d'un autre message d'alerte. Les messages d'alerte contiennent en particulier les coordonnées du lieu de l'accident et les paramètres de la zone de retransmission, ils doivent être de taille réduite pour être transmis-le plus rapidement possible.

- Autres messages

Ce type de message contient tous les messages qui ne sont pas des messages d'alerte ou de contrôle. Ces messages ne sont généralement pas répétés à intervalle régulier. En effet, cela peut être par exemple un message de transaction financière ou l'envoi de courrier électronique.

Tous les messages reçus seront stockés dans un « cache des messages récemment reçus ». Chaque message se verra associé une durée de vie dans le cache.

D. Applications des réseaux de véhicules [12]

Les principales applications des réseaux VANET (voir la figure 1.6) peuvent être classifiées selon le service offert en trois grandes catégories, chaque catégorie peut avoir diverses classes, et au niveau de chaque classe plusieurs applications peuvent être distinguées. Les contraintes de ces applications sont différentes comme par exemple la vitesse de propagation de l'information. Dans le cas d'un accident, il faut prévenir les usagers dans un temps borné alors que la diffusion de publicités n'a pas cette contrainte de temps mais elle sera par contre plus consommatrice de bande passante.

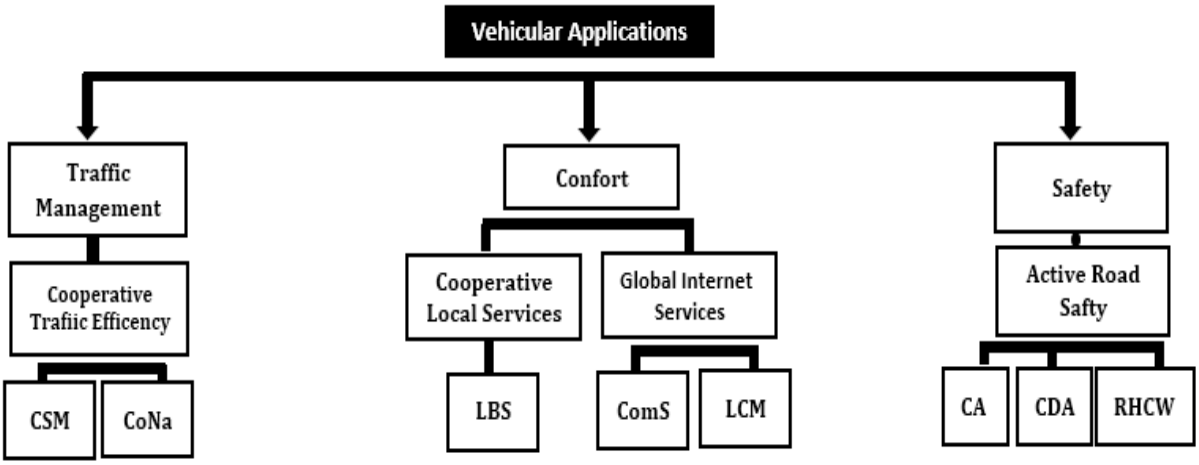

Figure 1-4 : La classification des applications dans les VANETs [12].

Nous allons donc décrire dans les paragraphes suivants deux applications :

➢ Applications de sécurité routière (safety)

- Alerter en cas d'accidents

Ce service permet, dans le cas d'un accident, d'avertir les véhicules se dirigeant vers le lieu de l'accident que les conditions de circulation se trouvent modifiées et qu'il est nécessaire de redoubler de vigilance (voir. figure 1.7). Il est nécessaire, également, en cas de densité réduite de véhicule de pouvoir conserver l'information pour pouvoir la retransmettre si un véhicule entre dans la zone de retransmission. Les messages de sécurité devront être émis à des périodes régulières. Ainsi le ou les nœuds désignés pour la retransmission des messages émettront des alertes à un instant régulier. Les messages devront être de taille réduite pour être transmis le plus rapidement possible. Les messages devront comporter les coordonnées du lieu de l'accident et les paramètres de la zone de retransmission.

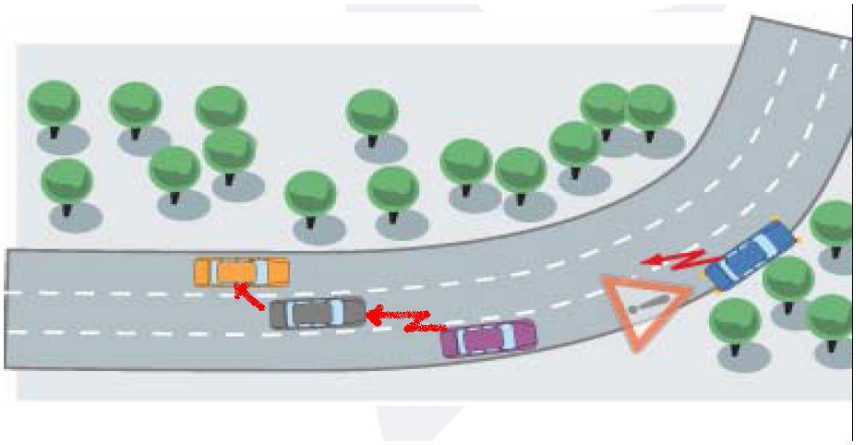

Figure 1-5 : vehicule en panne [13].

- Alerter en cas de ralentissement anormal (bouchon, travaux, intempéries, etc)

Ce service permet d'avertir les automobilistes de situations de circulation particulières (voir. figure 1.8). Quelque soit la nature des difficultés de circulation, il renseigne l'automobiliste qu'il est nécessaire de ralentir. Le message d'alerte est émis par un véhicule qui détecte les difficultés de circulation (freinage important par exemple, déclenchement des feux de détresse, pluie). Un véhicule banalisé effectue des travaux peut également être à l'origine du message d'alerte. Comme pour le message d'alerte informant d'un accident, un ralentissement doit être transmis aux autres véhicules de façon efficace et rapide.

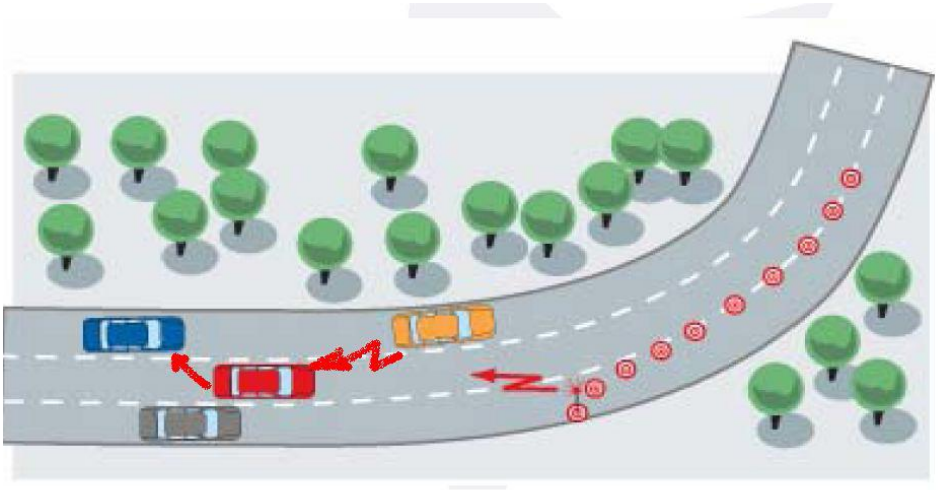

Figure 1-6 : travaux sur les routes [13].

- La conduite collaborative

La conduite collaborative est un concept qui améliore considérablement la sécurité du transport routier (réduction du nombre de victimes, voir. Figure 1.9). Cette innovation est basée sur un échange de renseignements entre des véhicules munis d'instruments (ex : capteurs) leur permettant de percevoir ce qui les entoure et de collaborer en groupes. Ces groupes de véhicules ou réseaux ponctuels, peuvent élaborer une stratégie de conduite collective qui exigerait peu ou pas d'interventions de la part des conducteurs. Depuis ces dernières années, différentes architectures de véhicules automatisés ont été proposées, mais la plupart d'entre elles n'ont peu ou pas investi le problème de communication inter véhicules. On peut aussi, sur le même principe, échanger des informations de trafic et de travaux afin de fluidifier le réseau routier en

indiquant par exemple des itinéraires. La signalisation automatique est aussi envisageable avec l'avertissement de passage de véhicule d'urgence, ou encore l'avertissement d'une panne d'un feu tricolore.

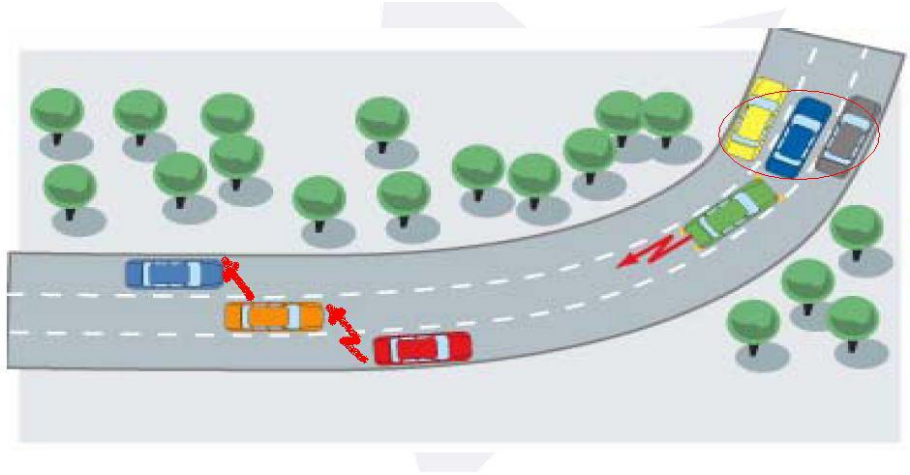

Figure 1-7 : Risque de collision [13].

➢ Applications de confort (confort)

- Réseaux collaboratifs

Les réseaux collaboratifs sont en train de se développer en particulier avec les réseaux pairs-à pairs. On peut imaginer une chaîne de radio ou de « télévision distribuée » où chaque véhicule va partager les musiques et vidéos qu'il a en sa possession pour construire un programme de diffusion continu. Les cartes collaboratives (wiki) et les petites annonces peuvent être des services distribuées à base de réseaux collaboratifs. Un serveur relai (dit « proxy-cache ») peut permettre la navigation sur Internet même dans des zones sans connexion à Internet. Un système de distribution de publicités et d'informations pratiques (concerts, restaurants…) peut être mise en place à l'entrée des villes.

- Internet dans les transports

Aujourd'hui, les hotspots (zone wifi à accès Internet) sont de plus en plus développés dans les villes, en particulier avec les initiatives des communautés. Ainsi, les passagers dans la voiture pourront jouer en réseaux, ou encore même naviguer sur Internet (voir. figure 1.10).

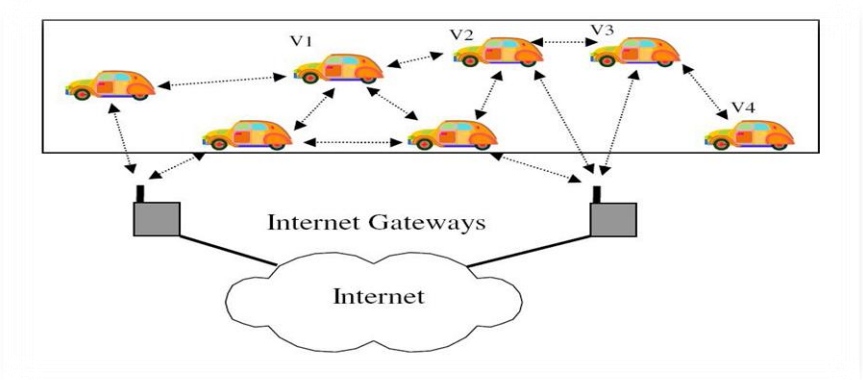

Figure 1-8 : Accès à Internet [13].

- **Gestion des espaces libres dans les parkings**

Ce service permet de rassembler des informations sur la disponibilité de l'espace de stationnement dans les parkings et de coordonner entre les automobilistes afin de les guider vers les espaces libres (voir. Figure 1.11).

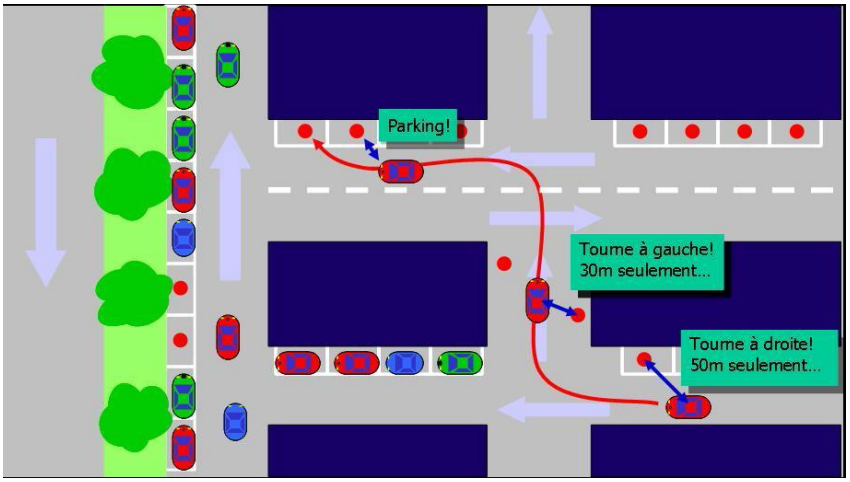

Figure 1-9 : Parking intelligent [13].

E. Technologies de communication

Afin de déployer les applications proposées pour les réseaux véhiculaires, différentes technologies de communication existent. Ces technologies peuvent être divisées principalement en trois catégories [14] :

- **Radio diffusion numérique**

tels que Radio Data System (RDS)/Traffic Message Channel(TMC), Digital Audio Broadcasting(DAB)/Digital Multimedia Broadcasting (DMB) et DVB

Terrestrial(DVB-T)/DVB-Handheld (DVB-H), dans laquelle les informations sont fournies aux utilisateurs d'une manière unidirectionnelle.

- **Réseaux cellulaires**

Nous pouvons citer comme exemple l'Enhanced Data Rates for GSM Evolution(EDGE), UMTS, Long Term Evolution (LTE) et WiMax qui dominent le domaine des communications mobiles et offrent des couvertures très larges mais nécessitent en revanche une infrastructure.

- **Device-to-Device**

Cette catégorie permet une communication directe entre les véhicules en utilisant des technologies telles que le Wifi et Dedicated Short-Range Communications (DSRC).

F. Standardisation et normalisation dans un VANET [15]

Le standard IEEE 802.11-2012 [19], anciennement nommé IEEE 802.11p [20], introduit de nouvelles spécificités à la couche physique, ainsi qu'à la sous-couche MAC, afin d'améliorer la communication dans les VANETs. L'IEEE 802.11p utilise le canal de communication DSRC [15], Dedicated Short Range Communication, qui est spécialement conçu pour les applications à portée moyenne et sensibles au délai, afin de s'adapter à la mobilité des véhicules et de proposer un faible taux d'erreurs, à savoir 10−6 lors d'une vitesse de 160 km/h. Le débit proposé varie de 3 Mbit/s à 27Mbit/s, avec une portée de transmission théorique allant jusqu'à 1000 mètres. Par ailleurs, l'utilisation d'accusé de réception (ACK) est ainsi non utilisée pour l'envoi de données par diffusion, afin de réduire la charge du canal de communication. Cependant, le taux de délivrance des messages peut en souffrir, car un véhicule source n'a plus aucune garantie par rapport à la réception de son message.

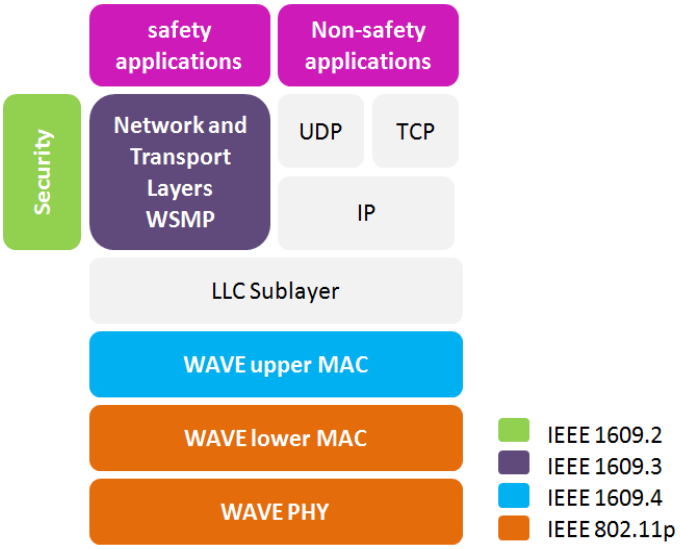

Figure 1-10 : La pile protocolaire WAVE [29].

Le standard IEEE 802.11-2012 [19], anciennement nommé IEEE 802.11p [20], introduit de nouvelles spécificités à la couche physique, ainsi qu'à la sous-couche MAC, afin d'améliorer la communication dans les VANETs. L'IEEE 802.11p utilise le canal de communication DSRC [15], Dedicated Short Range Communication, qui est spécialement conçu pour les applications à portée moyenne et sensibles au délai, afin de s'adapter à la mobilité des véhicules et de proposer un faible taux d'erreurs, à savoir 10^{-6} lors d'une vitesse de 160 km/h. Le débit proposé varie de 3 Mbit/s à 27Mbit/s, avec une portée de transmission théorique allant jusqu'à 1000 mètres. Par ailleurs, l'utilisation d'accusé de réception (ACK) est ainsi non utilisée pour l'envoi de données par diffusion, afin de réduire la charge du canal de communication. Cependant, le taux de délivrance des messages peut en souffrir, car un véhicule source n'a plus aucune garantie par rapport à la réception de son message.

G. Architectures de communication

Selon la manière avec laquelle les usagers routiers sont en mesure d'accéder et de partager les contenus, les réseaux véhiculaires peuvent être classés en trois types d'architectures [20] :(*i*) centralisée, (*ii*) décentralisée et (*iii*) hybride.

- **Architecture centralisée (communicationVéhicule-à-Infrastructure V2I)**

L'architecture centralisée, comme illustré dans la figure 1.13, fonctionne sous l'hypothèse que les utilisateurs doivent continuellement accéder à un serveur centralisé qui gère leurs interactions avec d'autres utilisateurs, même lorsque les véhicules sont physiquement proches. Dans une telle architecture, il n'y a pas d'interaction directe entre les véhicules. Dans la littérature, cette communication est connue sous le nom de vehicle-to-infrastructure (V2I). Les véhicules communiquent indirectement par l'intermédiaire des infrastructures existantes telles que les RSUs et les réseaux cellulaires. Jusqu'à ce jour, les RSUs sont peu déployés en raison de leur coût élevé. De plus les réseaux cellulaires sont surchargés avec l'augmentation de la demande et ne couvrent pas toutes les zones (e.g. tunnels ou zones rurales).

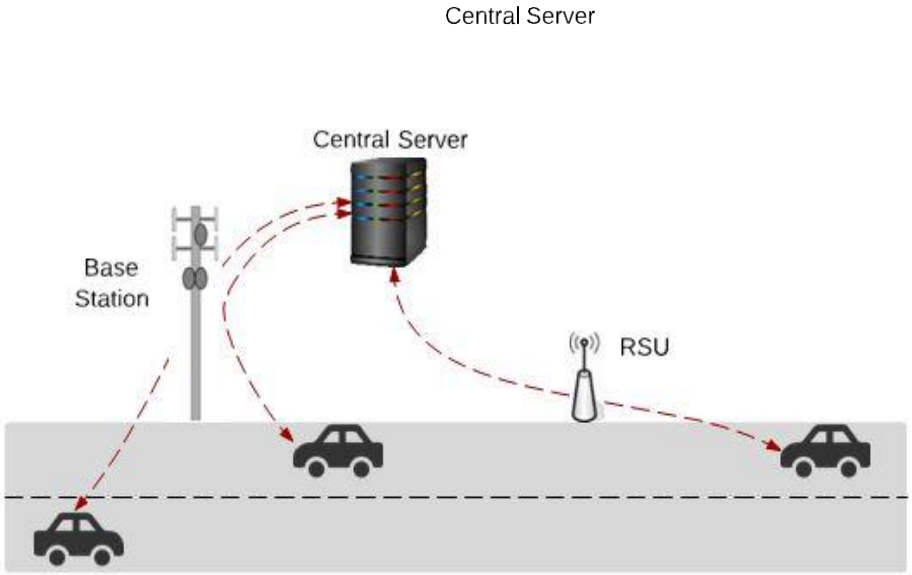

Figure 1-11 :Architecture centralisée[20].

- Architecture distribuée (communication Véhicule-à-Véhicule V2V)

L'architecture décentralisée illustré sur la figure 1.14, comprend uniquement des communications opportunistes entre les véhicules. Quand un véhicule rencontre d'autres véhicules à proximité (i.e. des nœuds voisins), les utilisateurs peuvent alors communiquer et échanger des contenus pendant les durées de contacts V2V. La communication V2V n'est pas coûteuse et offre un débit de transmission important. En revanche, cette communication pose des défis tels que les faibles fréquences de contacts entre les véhicules dans un milieu à faible densité, les faibles durées de contacts en raison de la vitesse et de la qualité du lien, et la sélection des nœuds relais.

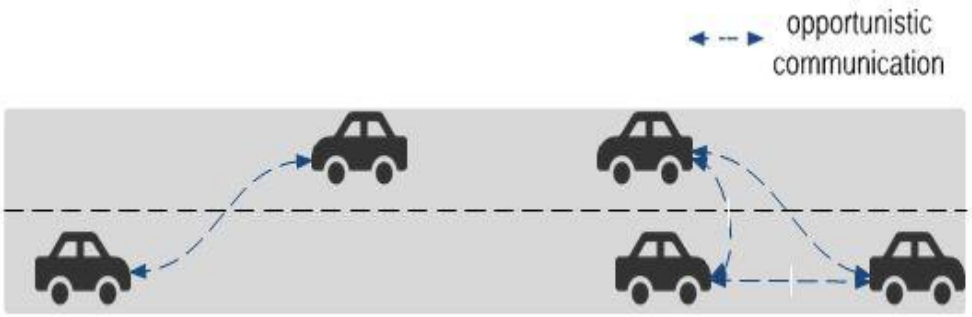

Figure 1-12 : Architecture centralisée [20].

- **Architecture hybride**

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

H. Les problématiques dans les VANETs

Les VANETs ont l'avantage de ne pas être conditionnés par les problématique liées à l'espace mémoire, à la capacité de calcul et à l'énergie. Cependant, ils souffrent de l'imposante quantité de données à envoyer et de l'étendue des zones géographiques à couvrir. Celles-ci combinées à la dispersion et la forte mobilité des véhicules, à l'absence ou à l'insuffisance d'infrastructure, ainsi qu'à la densité variable du réseau, créent plusieurs problématiques à la dissémination des données. Ci-dessous nous listerons quelques unes :

- **Problématiques liées à la densité variable et aux connexions sporadiques**

La densité des véhicules dans un VANET est très variable, elle peut être très faible, comme dans le cas d'une route de campagne à faible fréquentation ou très forte dans un réseau urbain fortement encombré. Ceci a un impact sur le taux de délivrance et les délais de l'acheminement des données. En effet, dans les situations de faible densité, les déconnexions sont fréquentes, ce qui peut causer de longs délais de transmission et de faibles taux de livraison de messages. De façon similaire, au cours de situations avec de forte densités, la concurrence pour l'accès au canal de communication est forte, causant des collisions de messages et donc beaucoup de pertes et de faibles taux de délivrance de messages [21] [22].

- **Partage des ressources du canal**

Les VANETs ne disposent pas de coordinateur pour l'allocation de la bande passante aux véhicules. Il devient alors la responsabilité de chaque véhicule à gérer ces ressources de manière équitable. Ceci peut augmenter les temps d'attentes avant l'accès au canal et la latence des messages.

- **Établissement de relations de confiance**

La problématique de la modélisation de la confiance pour les membres d'un VANET est délicate et unique en son genre. Dans certains scénarios, les véhicules circulent à des vitesses très élevées, comme sur une autoroute, les réactions des conducteurs devant des situations dangereuses et imminentes doivent être rapides et efficaces, ce qui rend la vérification en temps réel de la fiabilité des informations provenant d'autres véhicules nécessaire mais non triviale. En effet, les VANETs sont des systèmes *décentralisés* et *ouverts*, souvent sans infrastructures dédiées. Les membres peuvent rejoindre ou quitter les ilots en composant le réseau lui-même sans passer par une entité centrale. Par conséquent, le mécanisme de confiance à utiliser doit être distribué par essence [23].

- **Incitation à la coopération**

La dissémination de données dans les VANETs est effectuée, le plus souvent, de manière collaborative, afin de remédier à la non présence constante d'infrastructure et de supporter la mobilité des véhicules. Pour cela, il est primordial que les véhicules acceptent de coopérer et de transmettre les messages de leurs voisins.

- **Le passage à l'échelle**

Le nombre de véhicules croît de manière significative. La quantité d'information collectée et échangée au sein des VANETs fait de même. Cela impose que toute solution proposée pour les VANETs considère dés sa conception la problématiques du passage à l'échelle.

1.2.3. Conclusion

L'objectif de ce chapitre est de présenter les réseaux véhiculaires comme un nouveau paradigme de réseau. Nous avons exposé leurs caractéristiques ainsi que les différentes architectures de communication possibles. Les réseaux véhiculaires offrent une multitude d'applications allant de la sécurité de la route au confort et au divertissement des usagers routiers et qui peuvent être classée en fonction de leur impact sur le trafic routier et leurs exigences en termes de délais et de services. Dans le chapitre suivant, nous nous intéresserons à la dissémination des données dans les vanets.

Chapitre 2 : Dissémination de données dans les VANETS

2.1. Introduction

Tout au long de ce chapitre, nous nous intéressons à la problématique de la dissémination des données dans les réseaux ad hoc véhiculaires (VANETs).Ce mecanisme vise à permettre la réception des informations envoyées par tous les véhicules concernés, tout en respectant les durées de validité de celles-ci. La condition est de ne pas inonder le réseau de doublons ou d'informations inutiles, comme cela peut être le cas durant une diffusion générale. L'acheminement de données doit faire face aux difficultés induites par la densité variable du réseau, la forte mobilité des véhicules, l'absence ou l'insuffisance d'infrastructure, ainsi que l'étendue des zones géographiques à couvrir.

Dans ce chapitre, nous présentons d'abord la dissémination de manière générale, puis Ses techniques et leurs stratégies liées aux applications d'urgence et de confort.

2.2. Définition de la dissémination

La dissémination d'information consiste à acheminer une information d'une source vers une ou plusieurs destinations, en assurant un délai d'acheminement réduit, une grande fiabilité et une meilleure utilisation des ressources. Les destinations ciblées par l'opération de dissémination peuvent être caractérisées par la position, l'adresse IP (voir. Figure 2.1), la région géographique ou autre (voir. Figure 2.2) [26].

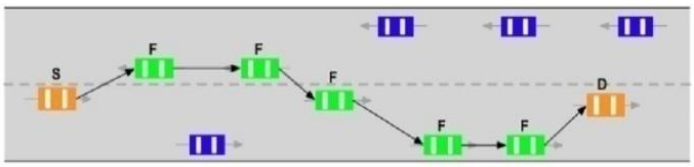

Figure 2-1: Communication à destination unique (unicast).

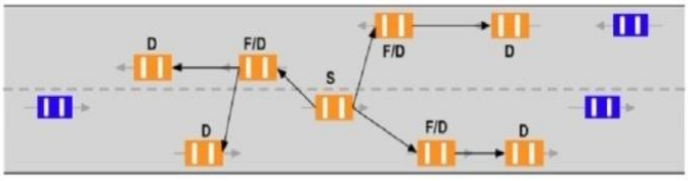

Figure 2-2: Diffusion limitée aux véhicules à deux sauts radio.

Dans les réseaux MANETs, les protocoles de routage utilisent l'inondation pour la découverte et la maintenance des routes. L'inondation est le protocole le plus naïf pour la diffusion dans les réseaux ad hoc. Dans celui-ci chaque nœud rediffuse systématiquement le paquet reçu une seule fois. Le problème, aussi connu dans [26] comme "the broadcast storm problem" est que cette rediffusion systématique cause inutilement une consommation excessive de bande passante vu que chaque nœud va recevoir plusieurs fois la même information via le canal sans fil. De plus, dans le cas de réseaux ad hoc denses, le fait que chaque nœud rediffuse systématiquement génère un nombre important de collisions qui ne seront pas corrigés par la couche MAC (absence d'ACK lors de la diffusion). Ce qui réduit donc l'efficacité et la fiabilité de la diffusion. Pour éviter ce phénomène, la solution la plus souvent retenue est d'écarter un certain nombre de pairs par une heuristique [27]. Toutefois, d'autres types de diffusion mieux adaptés aux environnements IVC sont désormais possible notamment le multicast et la géo-diffusion [30]. Le multicast est utilisé par des applications qui souhaitent transmettre des informations vers plus d'une destination. Un nœud voulant recevoir les données, doit d'abord joindre un groupe multicast. Les messages envoyés sont alors reçus par tous les membres du groupe. La géo-diffusion quant à elle adopte le même principe de fonctionnement, à la différence qu'au lieu de joindre explicitement un groupe multicast, les nœuds sont implicitement membres du même groupe s'ils sont dans la même zone géographique. Le groupe devient dans ce cas groupe géocast. Dans ce type de concept, la terminologie suivante est utilisée [13] :

- Groupe géocast : les membres d'un groupe sont définis par leur localisation géographique.
- Zone géocast : c'est l'espace géographique où l'ensemble des nœuds mobiles membre d'un groupe géocast sont localisés. Entrer dans la zone revient à joindre le groupe et vice versa.
- Zone de relayage (forwarding zone) : représente la zone où les paquets de données sont relayés.

Chaque groupe géocast dispose d'une zone de relayage, et seuls les nœuds se trouvant à l'intérieur peuvent relayer les paquets. Une zone géocast peut être incluse dans une zone de relayage (voir. figure 2.3) ou non (voir. figure 2.4).

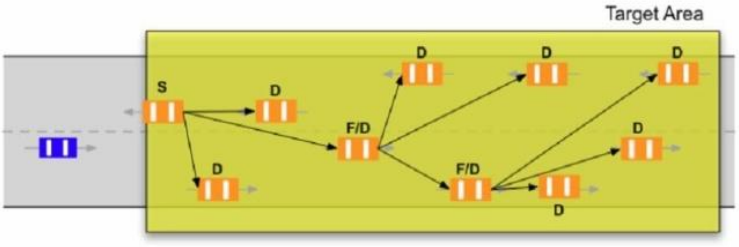

Figure 2-4 : Géo-diffusion [13].

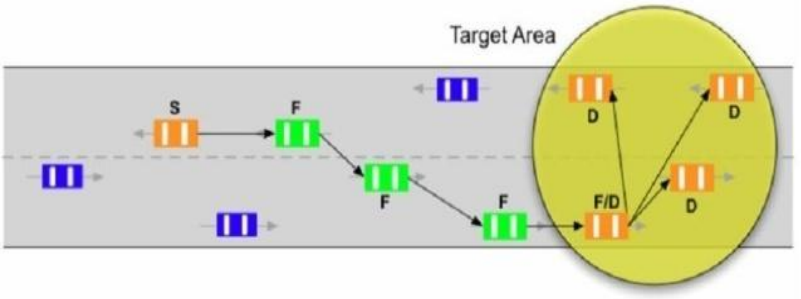

Figure 2-3 : Géo-diffusion avec zone distance de diffusion [13].

Lors de ce relayage d'informations, le réseau peut être partitionné et ainsi la chaine de communication rompue. Un mécanisme nommé "opportunistic forwarding" [27] permet de résoudre ce problème en sauvegardant le message au niveau du nœud en attendant l'arrivée d'un nouveau nœud voisin. Lorsqu'un nœud arrive et qu'il satisfait les conditions de transmission, la communication reprend et le message est transféré à ce nouveau voisin.

2.3. Techniques de dissémination

Une solution de dissémination efficace pour les VANETs doit absolument prendre en considération les caractéristiques de ces dernières, comme la taille du réseau, la vitesse des véhicules, la connexion intermittente du réseau qui cause son partitionnement en de nombreux ilots, ainsi que les différents besoins des applications en termes de qualité de service. Dans la littérature, plusieurs stratégies ont été proposées. Chacune d'elles, peut nécessiter un ou plusieurs sauts pour l'acheminement de ses données, ainsi que le déploiement ou non d'infrastructure, comme les unités de bords de route (RSUs). Néanmoins, toutes les stratégies se basent sur la coopération des véhicules du réseau pour relayer les messages. C'est pour cette dernière raison qu'une multitude de

modèles incitatifs ont été proposé en parallèle aux stratégies de diffusion, comme il est illustré dans la figure 2.5 .

En plus de la motivation des véhicules à coopérer, il existe un deuxième mécanisme, complémentaire au précédent, dont l'objectif est d'attester de la validité des messages reçus et **Figure 2-5** : Classification des techniques de dissémination existantes [28].

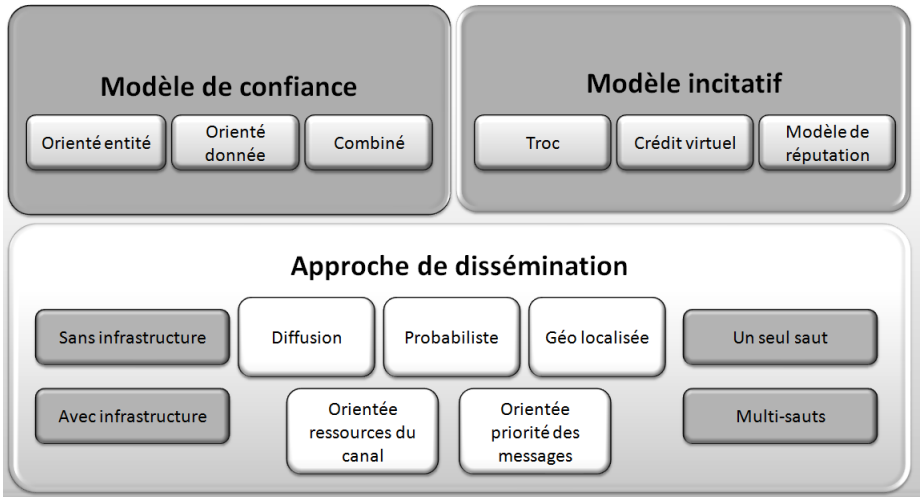

Figure 2-5 : Classification des techniques de dissémination existantes [28].

En plus de la motivation des véhicules à coopérer, il existe un deuxième mécanisme, complémentaire au précédent, dont l'objectif est d'attester de la validité des messages reçus et d'exclure du réseau les véhicules dont le comportement est malicieux. Ci-dessous, nous détaillons les différentes stratégies de dissémination, les modèles incitatifs, ainsi que les modèles de confiance existants. Ces trois éléments représentent un ensemble complémentaire de mécanismes qui doivent être mis en place pour l'élaboration d'une solution complète et efficace de dissémination de données dans les VANETs.

2.3.1. Modèles incitatifs à la coopération

La plupart des solutions de dissémination considèrent la coopération des véhicules présents dans le réseau comme acquise, ce qui n'est pas vérifié à cause de la présence potentielle de véhicules égoïstes. Ces derniers préfèrent réserver leurs ressources uniquement pour leurs besoins personnels et refusent donc les demandes de retransmission des messages de leurs voisins. Cette attitude baisse l'efficacité des solutions à acheminer les données dans les VANETs. Pour cette raison, il est primordial d'accompagner une solution de dissémination de données par un modèle incitatif à la coopération, afin de s'assurer de la participation de tous les véhicules à la

retransmission des données. Trois approches peuvent être utilisées pour motiver les véhicules à coopérer [29] :

- **Le Troc**

Dans cette approche, chaque véhicule tient une table retraçant le comportement des autres véhicules à son égard, un véhicule n'accepte de coopérer et de retransmettre le message d'un autre à condition de réciprocité que ce dernier ait déjà fait de même [30]. Cependant, la forte mobilité des véhicules et les changements fréquents de topologie dans les VANETs ne permettent pas l'établissement de solides relations entre les véhicules, ce qui peut affaiblir les performances de cette approche.

- **Les crédits virtuels**

La majorité des modèles incitatifs utilisent des crédits virtuels qui servent à monétiser la coopération des véhicules. Chaque transmission de message fait bénéficier le véhicule relayeur d'une récompense donnée par le véhicule émetteur. Le maintien d'un tel système nécessite le déploiement d'infrastructures ou la disposition dans les véhicules d'équipements spécifiques, afin de gérer le calcul et la distribution des récompenses [31] [32]. Les limites de cette approche concernent le calcul des coûts et récompenses, qui souvent peut être basé sur des estimations, ainsi que sur la distribution des crédits, qui peut souffrir de la mobilité des véhicules.

- **Les modèles de réputation**

Cette dernière approche mesure la coopération des véhicules à travers des réputations, chaque véhicule relayant un message verra sa réputation mise à jour par le véhicule émetteur. Une réputation de haute valeur ouvre l'accès à des privilèges sur le réseau [33]. Tout comme l'approche basée sur le troc, celle-ci souffre de la mobilité et des changements de topologie dans les VANETs qui ne permettent pas la construction fiable de réputation.

2.3.2. Stratégies de dissémination

- **Diffusion**

L'une des approches les plus utilisées pour la dissémination de données dans les VANETs est celle utilisant la diffusion. Elle peut être utilisée à un seul saut comme à plusieurs sauts. Un message envoyé par un véhicule émetteur par diffusion est transmis à tous ses voisins directs, puis est retransmis encore une fois par chacun de ses récepteurs, jusqu'à atteindre le (ou les) destinataire(s). Cette approche ne nécessite aucune information préalable sur les voisins du véhicule, ce qui lui permet d'ignorer l'inexistence ou l'inexactitude des informations sur la topologie du réseau. Elle augmente le taux de délivrance et améliore la vitesse d'acheminement des données, car

un véhicule destinataire reçoit plusieurs copies du message, arrivant au travers de plusieurs routes. Néanmoins, cette approche augmente aussi la compétition pour l'accès au canal de communication et l'utilisation de la bande passante, ce qui ne lui permet pas le passage à l'échelle au risque de générer une forte congestion du réseau [28].

Les auteurs de l'étude [35] proposent un protocole de diffusion multi-sauts pour les environnements urbains, nommé UMB (Urban multi-hop broadcast protocol), qui vise à remédier aux problèmes liés à la diffusion massive. Pour l'envoi d'un message, un véhicule émetteur l'envoie par diffusion à ses voisins directs, puis seul le véhicule le plus éloigné le rediffuse. À la rencontre d'une intersection, des véhicules sont sélectionnés comme répéteurs et sont chargés de rediffuser l'information sur les différents segments de l'intersection.

Les auteurs de la solution [36] utilisent la même approche de dissémination. Un message est envoyé par diffusion afin d'atteindre un certain groupe de véhicules. Cependant, à partir de la seconde transmission du message, uniquement les véhicules sur les bords sont sélectionnés comme relayeurs. Les critères de sélection des relayeurs dans ces deux approches concernent principalement leurs positions géographiques. Ceci n'est pas suffisant pour répondre aux problèmes spécifiques au VANETs, comme par exemple l'adaptation à la densité changeante du réseau, car aucune relation entre le nombre de relayeurs et la densité n'est donnée.

– **Probabiliste**

Ce type d'approche, tente de diminuer les messages redondants générés en calculant les probabilités de rencontres entre deux véhicules avant de décider du chemin de dissémination d'une information, sans pour autant nécessiter la connaissance de la topologie du réseau. Un véhicule utilisant cette approche peut se baser sur ses connaissances , son historique de rencontres avec les autres véhicules, ainsi que sur les informations qu'il a pu collecter sur la mobilité et les localisations des autres véhicules du réseau.

La solution [37] utilise cette approche probabiliste. Les décisions concernant les choix des véhicules relayeurs pour la retransmission d'un message se basent sur les probabilités de rencontres du (ou des) véhicule(s) destinataire(s). Alors que dans les solutions [38] et [40], les véhicules récepteurs d'un message calculent eux-mêmes leur probabilité de retransmission, en se basant sur la distance les séparant du véhicule émetteur. Plus cette distance est grande plus leur probabilité de retransmission est importante. Les auteurs de la solution [41] utilisent le critère de la distance entre un véhicule récepteur et un véhicule source pour calculer la probabilité de retransmission et y ajoutent un paramètre concernant la densité locale du réseau, soit le nombre de voisins directes du véhicule récepteur, afin de réduire le nombre de véhicules relayeurs lorsque la densité est forte.

- **Géographique**

Cette approche de dissémination se base sur les informations de localisation des véhicules contenues dans les messages de contrôle, diffusés périodiquement dans le réseau, lorsqu'elle suit une approche pro-active [42], ou alors diffusés à la demande, lors d'une approche réactive [43]. Chaque véhicule tient régulièrement à jour une table contenant l'historique des localisations de ses voisins, afin de pouvoir acheminer ses messages par le chemin le plus court et donc, réduire leur délai d'acheminement. Pour ce fait, lors d'une dissémination, le véhicule le plus proche du (ou des) destinataire(s) est sélectionné lors de chaque saut. Cette approche permet aussi de cibler un groupe de véhicules grâce à leurs coordonnées géographiques, comme font les applications visant à avertir les conducteurs des risques de collision en intersection, par exemple.

- **Orientée ressources du canal**

Sachant que, les ressources du canal de communication sont limitées, l'accès au canal et l'allocation de ses ressources deviennent un problème d'optimisation. Cependant, ce problème risque d'être complet à cause de toutes les variantes qui doivent être prises en considération et du peu d'informations sur le réseau mises à la disposition du véhicule. Des solutions proposent alors des algorithmes basés sur des heuristiques, tel l'étude [44] qui propose un routage de données accès sur la prise en compte de l'historique des rencontres du véhicule émetteur avec les autres véhicules du réseau. Cela dans le but d'estimer les congestions potentielles ainsi que la densité du réseau, puis de les prendre en considération afin d'améliorer le taux de délivrance et de limiter le nombre de messages doublons. Dans la solution [45], chaque nœud tient une table avec des informations sur le débit et les conditions du canal afin de choisir par quel nœud relayeur il est préférable de transmettre son message. Cependant, ces solutions nécessitent des échanges de messages entre les véhicules pour maintenir un contrôle sur l'utilisation des ressources du canal.

Une autre solution [46], améliore le taux de réception des messages d'urgences en leur allouant une partie de la bande passante disponible. Dans cette solution, chaque nœud envoie en premier un signal sous forme d'impulsion, puis le message d'urgence.

- **Orientée priorité des messages**

Pour répondre aux différents besoins en qualité de service des multiples applications des VANETs, des solutions de dissémination proposent une adaptation de la dissémination par rapport à l'importance du contenu des messages échangés. Afin de ne

pas supprimer systématiquement tous les nouveaux messages entrants en cas de congestion du réseau. La solution [47] remédie à ce problème en fixant des priorités pour l'accès au canal de communication d'après les catégories d'accès ACs, fixées par EDCA [48], pour chaque message. Une autre solution [49], alloue des jetons aux files d'attente formées par les messages souhaitant l'accès au canal. Elle gère l'accès au canal en pondérant le nombre de jetons offerts par rapport à la densité du canal et à la priorité des messages.

Tout comme cette dernière, la solution [50] ordonnance les messages à envoyer sur la base des ressources disponibles du canal et de l'importance du message, en utilisant un système de files d'attentes où une plus grande priorité est donnée aux messages les plus urgents.

Dans ce qui suit nous allons expliquer quelques protocoles de la dissémination des messages d'urgence et des messages de confort avec leurs différentes contraintes. Mais d'abord on défini le mécanisme DDT« Distance Defer Transfer » que l'on retrouve dans de nombreux protocoles.

➢ DDT

Pour disséminer le plus rapidement possiblel'nformation, [51] propose de relayer l'information par les nœuds les plus éloignés, en supposant que les nœuds intermédiaires écoutent simplement le message. Pour élire ce nœud le plus éloigné, les récepteurs calculent la distance de l'émetteur grâce à la position insérée dans le message. Un temps d'attente inversement proportionnel à cette distance est alors enclenché avant la réémission. Ainsi, le premier à réémettre sera le nœud le plus éloigné et les autres nœuds annuleront leur réémission à la réception du message rediffusé. La formule 1 montre le calcul effectué pour borner le délai d'attente.

$$WT(d) = -\frac{MaxWT}{Range} \cdot \hat{d} + MaxWT$$
$$\hat{d} = \min\{d, Range\}$$

Équation 1 : calcul du délai d'attente dans DDT.

Où d est la distance de l'expéditeur original, MaxWT: temps d'attente maximum, portée(Range): portée de transmission.

➢ Dissémination de messages d'urgence

Un message d'urgence est caractérisé par son lieu de génération, sa zone de pertinence et sa durée de validité. Le protocole de dissémination doit donc assurer la

contrainte spatiale et temporelle. En effet, il faut que tous les véhicules proches de l'alerte soient avertis de l'incident mais aussi qu'ils soient informés le plus tôt possible pour qu'ils aient le temps d'agir en conséquence. Deux approches sont alors possibles, soit une diffusion assistée par des points d'infrastructure le long de la route soit une diffusion complètement distribuée avec une propagation de voitures en voitures avec un mécanisme de sauvegarde/réémission (store and forward)[29]. Nous allons dans cette partie résumer quelques solutions proposées.

I. STEID (Spatio-Temporal Information Dissemination) [53]

Ce protocole propose de résoudre les besoins en termes de fiabilité spatiale et temporelle. STEID s'assure que tous les véhicules à l'intérieur de la zone d'alerte soient informés et dans un délai suffisant pour réagir. Pour cela STEID s'exécute sur un réseau hybride de type 802.11 et de type cellulaire comme on peut le voir dans la figure2.6.

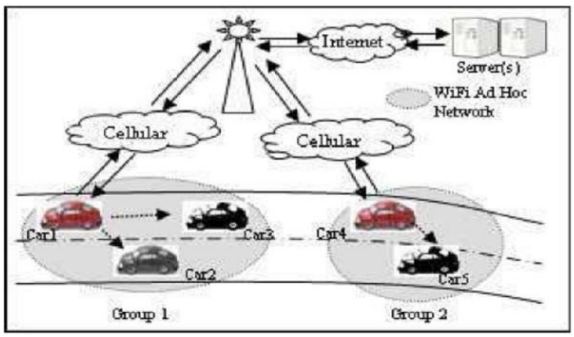

Figure 2-6 : fonctionnement général de STEID[53].

L'idée générale de cette architecture est d'utiliser la communication wifi pour transférer l'ensemble des alertes dans le cluster car il est peu couteux et il s'affranchi bien du facteur d'échelle. Le réseau cellulaire est quant à lui il est utilisé pour améliorer la fiabilité quand le réseau est partitionné en plusieurs morceaux.

Pour former un cluster, la solution propose que chaque voiture sur la route avertissement périodiquement sa présence en émettant un message "Hello" en utilisant l'interface WiFi. A chaque cluster est élu un responsable qui va gérer l'ensemble du trafic à l'intérieur de celui-ci, il joue le rôle d'un "serveur". Il est aussi responsable de la communication entre les autres clusters. La solution propose d'utiliser DDT pour la.

Réémission du message. Pour augmenter la fiabilité, l'auteur propose d'ajouter au message "Hello" des informations concernant le nombre d'alertes actives ainsi que la position de l'alerte la plus proche. Cela permet via un algorithme de synchroniser les

alertes avec les nœuds voisins. Le principal inconvénient de la solution est l'émission périodique de messages qui pose des problèmes de passage à l'échelle. De plus, il ne propose ni l'algorithme d'élection, ni le maintien de nœud élu du cluster.

J. DPP (Directional Propagation Protocol)

Dans [53], l'auteur propose une solution purement ad hoc pour la dissémination de messages d'alerte. Ce protocole, nommé DPP, utilise une direction pour la propagation de l'information. Le protocole prend en compte le phénomène de regroupement de véhicules (nommé aussi cluster) qui se produit sur les axes routiers. A l'intérieur des clusters sont élus un véhicule de tête (header) et un véhicule de queue (trailer). Ce sont eux qui vont gérer la propagation des messages entre les différents clusters. A l'intérieur d'un cluster, les véhicules n'acquittent pas les messages alors que d'un cluster à l'autre, les messages sont acquittés pour assurer une fiabilité. Pour la gestion de la fragmentation du réseau, le message peut être enregistré dans les nœuds de tête et de queue pour une future réémission jusqu'à ce que le message soit acquitté par un autre cluster.

Un inconvénient de cette solution est que l'auteur ne propose pas d'algorithme d'élection des véhicules de tête et de queue alors que ce problème n'est pas trivial (utilisation de messages Hello, ou autre). Il ne propose pas non plus l'algorithme de formation et de maintien des clusters. Un autre inconvénient est que l'auteur étudie uniquement la solution dans un environnement de type autoroute et il ne compare pas son protocole avec d'autres solutions.

K. Ah-IVC (disseminating messages among highly mobile hosts based on Inter-vehicle Communication)

La solution proposée dans [54] permet la dissémination dans une zone locale autour de l'initiateur. Si le message atteint un seuil de nombre de sauts alors le message n'est pas réémis. Une zone de pertinence est définie dans le message pour informer les conducteurs concernés. Pour augmenter la vitesse de propagation du message, l'auteur propose d'utiliser le mécanisme où le délai d'attente pour la réémission est inversement proportionnel à la distance de l'émetteur [51].

L'inconvénient de la solution est qu'elle ne prend pas en compte la fragmentation du réseau et que le choix de limiter la propagation au nombre de sauts n'est pas toujours un critère pertinent.

L. OAPB (Optimized Adaptive Protocol Broadcast)

Les auteurs de [55] proposent une méthode de diffusion de messages d'urgence censée éviter le problème de la « tempête de diffusion ». Dans un protocole comme DDT, la sélection des véhicules qui retransmettent effectivement le message est fondé sur la distance qui les sépare de l'émetteur. Dans [55], une stratégie de sélection différente est mise en place afin d'écarter un maximum de véhicules de l'acte de retransmission. Selon les auteurs, leur méthode permettrait d'obtenir un taux de véhicules atteints de l'ordre de 90-100% à 400 mètres de l'émetteur. La stratégie utilisée est basée sur l'attribution d'une probabilité de retransmission à chaque véhicule récepteur. La valeur de cette probabilité n'est cependant pas la même pour tous les véhicules : chaque véhicule calcule sa propre probabilité de retransmission qui dépend directement de son voisinage local à deux sauts (obtenu en supposant l'émission périodique de messages HELLO). En effet, les formules qui déterminent la valeur de cette probabilité (données dans l'article) utilisent le nombre de voisins à un seul saut, celui à deux sauts global et via chacun des voisins à un seul saut. Il peut arriver que ces nombres soient identiques pour plusieurs véhicules ; dans ce cas, pour éviter qu'ils retransmettent le message au même moment, un mécanisme dérivé de DDT est mis en place pour éviter cela. Celui-ci utilise une formule différente propre à [55] pour le calcul du temps d'attente avant retransmission.

Les simulations réalisées par les auteurs se sont limitées à un nombre de véhicules maximum, ce qui ne paraît pas très réaliste. D'autre part, l'émission périodique de messages HELLO consomme des ressources non négligeables.

M. ODAM(Optimized Dissemination of Alarm Messages)

Les auteurs de [56] proposent un protocole conçu pour la diffusion de messages d'alerte généralisant le concept de DDT et censé pallier phénomène de partitionnement du réseau de véhicules, éviter de recourir à la détermination du voisinage (aspect présent dans d'autres solutions) et être d'une grande fiabilité. La solution proposée consiste à diffuser le message selon le mécanisme de DDT ; une formule pour le calcul du temps d'attente avant retransmission, similaire à celle de [54], est donnée dans l'article. Lorsqu'un véhicule retransmet le message, il devient « relai » et continue de l'émettre périodiquement jusqu'à ce qu'il reçoit le même message d'un véhicule situé derrière lui. Le message est diffusé dans des zones restreint est dites « zones à risque » qui sont, comme le montre la figure 2.8, les demi-portions de routes sur lesquelles les véhicules circulent en direction de l'incident ayant causé le message d'alerte.

Sur la figure 2.8, un véhicule endommagé (x) diffuse un message d'alarme. Si le véhicule (a) a été pris comme relais, alors (C) ne peut être atteint car il était hors de la portée de transmission de (a). Contre, si (b) ont été sélectionnés comme relais, alors (c)

serait atteints et informés. Un relais est désigné comme le véhicule ayant la valeur minimale du délai de veille calculé. Le véhicule qui reçoit un message d'alarme ne devrait pas le retransmettre immédiatement mais il doit attendre pendant un délai différé. La valeur du délai de retard est inversement proportionnelle à la distance entre l'expéditeur et le récepteur. À l'expiration de cette période, si un nœud ne fonctionne pas il reçoit une autre alarme du même message, provenant d'un autre nœud, puis retransmet le message. Par là, il est choisi comme relais. Le problème est que la nécessité de faire retransmettre périodiquement le message par certains véhicules s'avère délicat pour le passage à l'échelle ; de plus, la restriction de la zone de diffusion limite les applications potentielles du protocole.

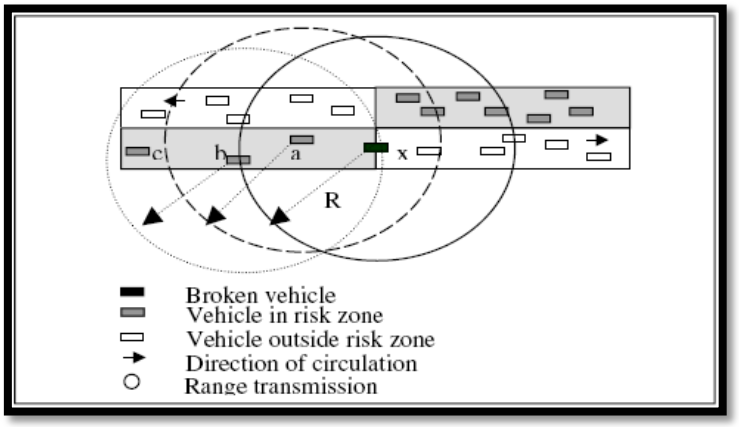

Figure 2-7 : Diffusion limitée aux zones à risque.

N. MHVB (MultiHop Vehicular Broadcast)

Ce protocole consiste à inonder une zone géographique avec un message d'urgence tout en veillant à limiter les risques de collision et l'utilisation de la bande passante Pour cela, la diffusion du message au sein du réseau de véhicules suit une méthode similaire au protocole DDT à la différence que chaque véhicule qui reçoit le message continue par la suite à l'émettre périodiquement tant qu'il n'est pas trop éloigné de son émetteur original. Les délais d'attente entre les retransmissions sont modulés en fonction de l'environnement (densité véhiculaire, distance à l'émetteur).Lorsqu'un véhicule doit diffuser un message d'urgence, il émet celui-ci périodiquement en indiquant sa position original (à la première émission) dans l'en-tête du message. Lorsqu'un autre véhicule reçoit le message à diffuser (après un ou plusieurs sauts), il suit les étapes suivantes [57] :

- ✓ Il enregistre le message reçu dans sa base de données locale.

✓ Il calcule la distance qui le sépare de l'émetteur original (celui qui a envoyé le message pour la première fois). Si cette distance est supérieure à un certain seuil, la procédure s'arrête ici.

✓ Il calcule la distance qui le sépare de l'émetteur (celui dont il a reçu le message).

✓ Il attend un temps d'attente calculé de telle sorte que les véhicules les plus éloignés de l'émetteur retransmettent le message plus tôt que les véhicules plus proches.

✓ S'il reçoit le même message d'un ou plusieurs autres véhicules, il détermine leurs positions relatives par rapport à lui-même, calcule une zone de non-retransmission, et s'il se trouve à l'intérieur de celle-ci, il annule sa propre retransmission. Sinon, il retransmet le message périodiquement.

Étant donné un retransmetteur, la forme de la zone de non-retransmission est illustrée par la figure suivante :

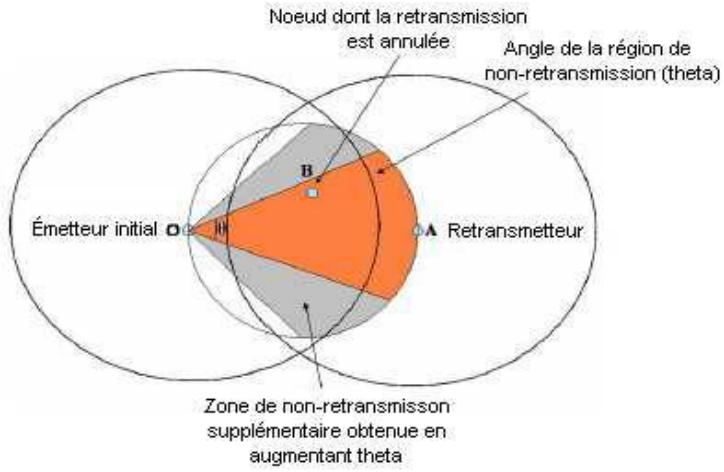

Figure 2-8 : Forme de la zone de non-retransmission dans MHVB[57].

Mettre comme vecteur de position relative du nœud A à O et B comme vecteur de position relative du nœud B à O et θ comme L'angle de la région arrière du feu, pour que B revient en arrière lorsqu'il reçoit le message retransmis de A voici les conditions suivantes :

$$(mod\ a) < (mod\ b) \qquad (1)$$

$$\frac{a.b}{(mod\ a).\ (mod\ b)} \geq \cos\theta \qquad (2)$$

(mod a) et (mod b) sont les positions relatives absolues des nœuds A et B respectivement de l'expéditeur original O.

Pour améliorer l'efficacité de la méthode, chaque véhicule module sa période d'attente entre deux retransmissions en fonction de la densité de circulation. Pour cela,

il compte le nombre de véhicules qui l'entourent et détecte s'il se trouve dans une zone congestionnée en vérifiant les trois conditions suivantes :

- ✓ Le nombre de véhicules dénombrés excède un certain seuil.
- ✓ Le nombre de véhicules dénombrés au devant et le nombre de véhicules dénombrés à l'arrière excèdent tous les deux un certain seuil.
- ✓ La vitesse du véhicule est inférieure à un certain seuil.

Lorsque ces trois conditions sont remplies, le véhicule modifie sa période d'attente par défaut avec une nouvelle valeur inversement proportionnelle au nombre de véhicules dénombrés. Ainsi, plus la circulation devient dense, plus la période d'attente va augmenter, permettant ainsi de réduire l'utilisation de la bande passante et le risque de collisions.

L'inconvénient de ce protocole est que de nombreux véhiculent vont retransmettre le message périodiquement, ce qui augmente fortement la charge du réseau.

O. MHPFH (Protocole de diffusion multi-hop à fuseau horaire)

Le protocole proposé par les auteurs de l'article [58] présente plusieurs nouvelles fonctionnalités clés. Tout d'abord, il utilise une approche de transmission de messages axée sur le segment pour réduire le nombre de véhicules relais. En outre, des emplacements temporels multi-hop distincts sont attribués pour les messages d'avertissement afin de surmonter les interférences avec les messages de sécurité à un seul saut. En outre, le mécanisme proposé gère le scénario de reconnaissance inconnue (ACK), ce qui réduit efficacement les retransmissions inutiles des messages d'avertissement.

- ➢ Scénario de transmission d'alertes d'urgence routière

La figure **2.10** illustre un exemple typique du scénario de déploiement VANET d'autoroute considéré. Supposons que chaque véhicule soit équipé d'un système de positionnement global différentiel (DGPS) qui puisse mesurer avec précision sa propre position sur la route. Généré par un véhicule marqué comme «véhicule d'avertissement d'urgence» « emergency warning vehicle », un message d'avertissement doit être envoyé à d'autres véhicules dans le sens de propagation indiqué « emergency warning message propagation direction ». Comme le montre la figure **2.10**, plusieurs messages d'avertissement distincts peuvent être transmis dans un VANET. Étant donné que la portée de transmission d'un véhicule est limitée, c'est préférable d'employé une technique de transmission de paquets multi-hop afin de s'assurer que le message d'avertissement atteindra les véhicules situés à de longues distances de l'expéditeur, c'est-à-dire le «véhicule d'avertissement d'urgence».

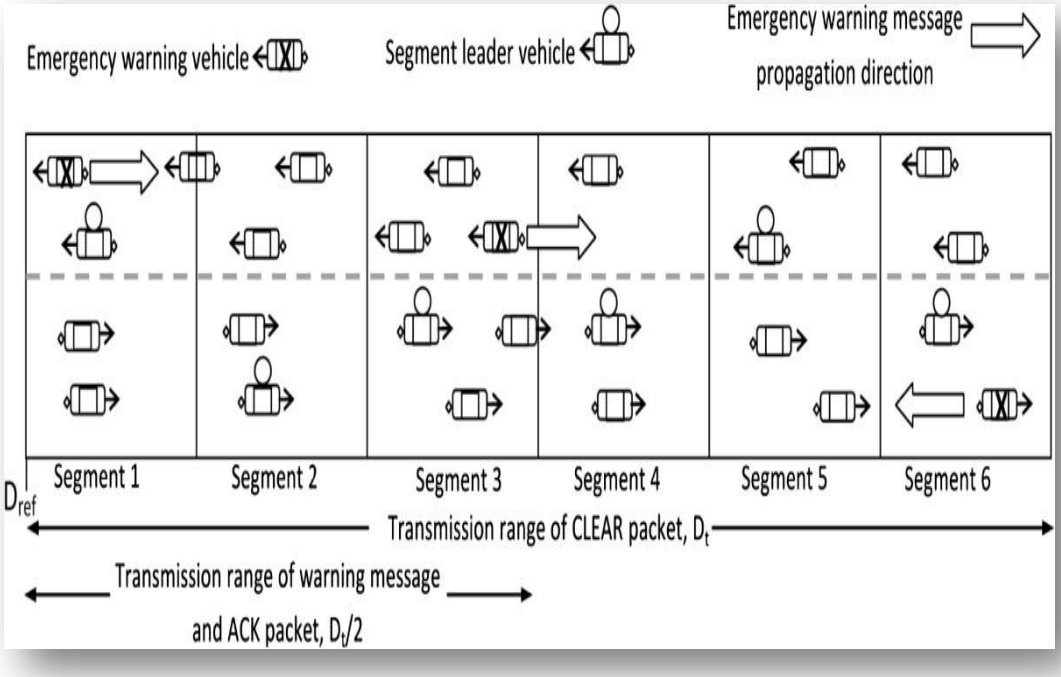

Figure 2-9 : Diffusion de messages d'avertissement sur une autoroute via un VANET [12].

Pour faciliter une diffusion efficace du message d'urgence, il faut diviser l'autoroute en segments de longueur fixe D_C et désignons un véhicule dans un segment en tant que «chef de segment» « segment leader vehicle ». Ceci est illustré à la figure 2.10. Ainsi, que chaque véhicule connaît sa propre position D_V par rapport à un point de référence D_{ref} sur l'autoroute. Ce point de référence peut être incorporé da ns les cartes ou transmis en tant que message diffusé par les nœuds d'infrastructure fixe sur l'autoroute. Les auteurs ont proposés dans Algorithme 1 un schéma pour chaque véhicule de sélectionner son leader de segment. Chaque véhicule v trouve son numéro de segment actuel k selon la formule suivante :

$$K = \frac{D_V - D_{ref}}{D_C}$$

Sur la base des données DGPS, chaque véhicule peut déterminer le point final de son segment actuel$D_{end}[K]$. Avec sa propre position D_v et la vitesse Sv, chaque véhicule peut également déterminer le temps restant qu'il restera dans le segment actuel Tv, rem. Les informations sur les positions et les vitesses des autres véhicules dans le même segment sont reçues via les messages de sécurité périodiques. Avec cette information, chaque véhicule peut également calculer le temps restant pendant lequel les autres véhicules restent dans leurs segments respectifs

Algorithm 1: Segment leader selection

```
1  Algorithm SegmentLeaderSelection()
2      Vehicle v computes its segment number by (1).
3      Vehicle v finds the current segment leader using
       FindSegmentLeader();
4      if T_{v,rem} ≤ T_exp and MY_STATUS = Leader then
5          Vehicle v sets MY_STATUS := Retired;
6          Vehicle v finds the next segment leader using
           FindSegmentLeader();
7      if Vehicle v receives a BSM from the same segment
       with MY_STATUS = Retired and LEADER_ID
       equal to the node_ID of vehicle v then
8          Vehicle v sets MY_STATUS := Leader;
9          Vehicle v sets LEADER_ID equal to the
           node_ID of vehicle v;
10     if Vehicle v receives no BSM from the same segment
       with MY_STATUS = Leader for a time period
       t > T_exp then
11         Vehicle v determines the segment leader using
           FindSegmentLeader();
12     if Vehicle v receives a BSM from the same segment
       with MY_STATUS = Leader or Vehicle v moves to a
       new segment then
13         Vehicle v sets MY_STATUS := Regular;
14 Procedure FindSegmentLeader()
15     foreach Vehicle w in the k^th segment do
16         T_{w,rem} = (D_end[k] − D_w) / S_w;
17     Vehicle v selects segment leader of the k^th segment
       as: w* = arg max_{w∈k^th segment} T_{w,rem};
18     Vehicle v sets its LEADER_ID field equal to the
       node_ID of w*;
```

Figure 2-10 : algorithme segment leader selection [58].

Au début, il faut sélectionner le véhicule leader du segment comme celui ayant le plus long temps restant dans son propre segment, en utilisant la procédure Find Segment Leader (). Notez que le leader du segment peut être dans n'importe quelle voie d'une autoroute. Les véhicules sélectionnés en tant que leaders seront les leaders du segment pour toute la durée qu'ils sont présents dans ces segments. Lorsqu'un leader de segment se rend compte qu'il se déplacera vers un autre segment dans un certain temps T_{exp} (sa valeur peut être considérée comme un multiple de l'intervalle de synchronisation = 100 ms), ce véhicule marque son statut de «Retraité» pour le temps

restant de sa présence Dans le segment actuel. Ce véhicule est également responsable de la nomination d'un nouveau chef de segment, c'est-à-dire celui avec le temps restant le plus élevé actuel dans le segment. Le leader du segment à la retraite notifie ce rendez-vous au nouveau chef de segment et à tous les autres véhicules dans le segment actuel. Pour mettre en œuvre le mécanisme ci-dessus, les auteurs ont proposés que chaque véhicule ajoute deux nouveaux champs dans le cadre de ses messages de sécurité périodiques. Le champ MY_STATUS indique l'état actuel d'un véhicule, qui peut avoir des valeurs de «Régulier», «Leader» et «Retraité». Le champ LEADER_ID contient l'ID du nœud du leader du segment actuel. Comme décrit dans l'Algorithme 1, lorsqu'un véhicule reçoit un message de sécurité périodique d'un véhicule leader du même segment (avec MY_STATUS = Leader), le champ LEADER_ID dans ce message contient l'ID de nœud de la voie.

Lorsqu'un chef de segment se retire, il trouve le nouveau segment leader et envoie le message de sécurité avec l'ID de nœud de ce nouveau leader dans le champ LEADER_ID. Après avoir reçu le message de sécurité périodique du même segment avec MY_STATUS = Retiré, chaque véhicule correspond à son propre ID de nœud avec la valeur de champ LEADER_ID. Si un véhicule reconnaît une correspondance, il se définit comme le nouveau leader et modifie son champ MY_STATUS sur Leader.

Un véhicule dans un segment peut ne pas recevoir un message de sécurité périodique d'un véhicule leader du même segment pour un temps$t > T_{exp}$. Dans ce cas, ce véhicule trouvera le leader en utilisant Find Segment Leader (). De même, si un véhicule entre dans un segment vide, il attendra $t = T_{exp}$ avant de se désigner comme leader de ce segment. Il se peut aussi que deux véhicules à proximité se considèrent comme les leaders du segment actuel. Dans ce cas, le véhicule qui reçoit le message de sécurité périodique avec MY_STATUS = Leader changera son MY_STATUS en Régulier et deviendra un véhicule «régulier». Cet arrangement garantit qu'il y aura toujours un seul segment leader dans n'importe quel segment de route.

Dans le protocole proposé, la taille du segment est sélectionnée comme une valeur beaucoup plus petite que la plage de transmission du message de sécurité. Il en résulte un taux de réception élevé des messages de sécurité et, par conséquent, une diffusion fiable des informations de leader dans un segment. De plus, la taille du segment est considérée comme une valeur fixe, car elle est une tâche difficile à adapter et à faire consensus sur la valeur d'une taille de segment dans un réseau ad hoc [59]. Cependant, il existe un certain nombre de techniques dans la littérature telles que le contrôle de la puissance d'émission et le contrôle du taux de génération de paquets qui peuvent être utilisés pour réduire le trafic de messages de sécurité dans un segment à densités de véhicule plus élevées [60, 61, 62, 63]. Néanmoins, ce document est hors de portée de ce

document, axé sur la diffusion efficace des messages multi-hop. Enfin, il convient de noter que si un segment ne pouvait pas élire un chef de segment pendant une certaine période pendant laquelle le message d'avertissement est également diffusé.

➢ Dissémination pour des applications de confort

Les applications de confort sont généralement plus consommatrices de bande passante avec par l'exemple le téléchargement de fichier. La propagation de message est donc sans contrainte de délai mais doit optimiser la bande passante. Une spécificité des applications de confort est que le contenu du message peut aussi être dynamique et se modifier lors du passage de nœud en nœud (par exemple pour mettre à jour une information).

A. SODAD(Segment-Oriented Data Abstraction and Dissemination)

Ce protocole combine une diffusion locale périodique et une couche application de sauvegarde et réémission de messages. La diffusion locale se base sur la construction de l'information par l'intermédiaire d'une fonction agrégation. Chaque route est fragmentée sous forme de segments comme on peut le voir dans la figure 2.11. Les informations reçues sont enregistrées dans une base de données et lors de la diffusion d'un message, les informations les plus récentes et les plus pertinentes de la zone sont sélectionnées et sont insérées dans le message à diffuser [64].

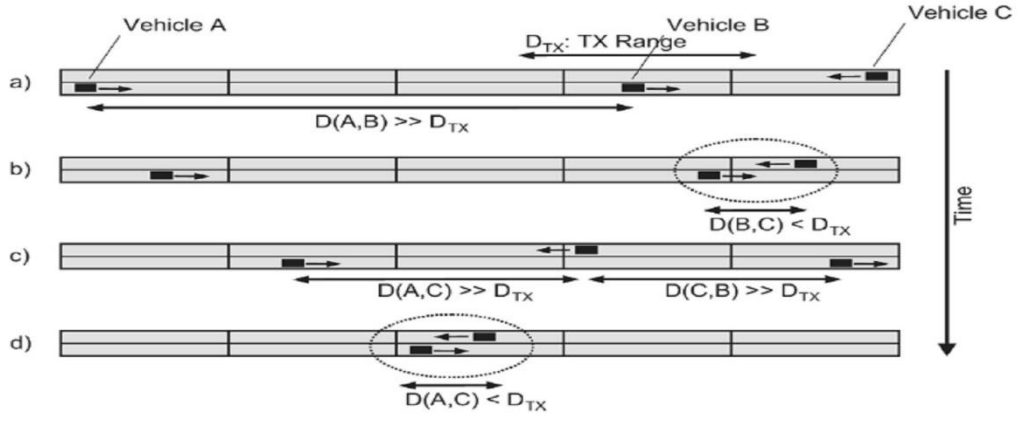

Figure 2-11 : Fragmentation des routes et connectivité au cours du temps.

L'auteur présente aussi un autre mécanisme qu'il appelle la diffusion adaptative. La vitesse à laquelle un véhicule envoi des messages s'adapte à l'environnement actuel en observant deux types d'événements. Si le nœud a reçu de vielles informations alors le temps entre chaque diffusion va être diminué. A l'inverse, si le nœud reçoit des

informations identiques à celle qu'il a enregistrée alors le délai de diffusion va augmenter.

B. MDDV (Mobility-Centric Data Dissemination Algorithm for Vehicular Networks)

Le protocole proposé dans cet article [65] est un algorithme de diffusion qui est contrairement aux autres algorithmes géographiques, considère que les véhicules ne disposent pas des positions des véhicules voisins. Le réseau routier est modélisé comme un graphe orienté où les nœuds représentent les intersections, les liens et les segments routiers. Un poids est associé à chaque lien pour refléter la distance et la densité de trafic correspondante. MDDV utilise une trajectoire de relayage spécifiée comme le chemin ayant la plus petite somme des poids d'une source vers la 'région destination' dans le graphe orienté.

C. UMB(Urban MultiHop Broadcast Protocol)

Le protocole proposé dans cet article [67] est un algorithme de diffusion qui modifie la couche d'accès 802.11 pour l'adapter au contexte des IVC dans le but de réduire les collisions et d'utiliser efficacement la bande passante. Cette adaptation utilise un mécanisme de RTS/CTS couplé au mécanisme de type DDT qui permet d'éviter le problème de la station caché en mode de diffusion. UMB comprend deux phases : la première appelée diffusion directionnelle où la source sélectionne un nœud dans la direction de diffusion pour effectuer le relayage des données sans aucune information sur la topologie, et la deuxième diffusion aux intersections, pour disséminer les paquets dans toutes les directions, en installant des répéteurs vers tous les segments de route.

D. RBM (Role-Based Multicast)

Dans [68], les auteurs proposent un protocole de multicast où chaque nœud maintient deux listes : une liste de voisins et une liste des nœuds émetteurs. En fonction des contenus de ces deux listes, un nœud décide ou pas de rediffuser le message après un certain temps. Dans cette approche, le protocole suppose l'existence d'une couche liaison qui maintient la liste des nœuds voisins.

E. TRADE (TRack DEtection)

Dans [51], les auteurs ont proposé ce protocole de diffusion. Son objectif est de garantir une meilleure fiabilité avec un nombre de rediffusions limité. Un véhicule doit

alors désigner parmi ses voisins, en fonction de leurs déplacements, ceux qui assurent la retransmission des messages.

F. IVG (Inter-Vehicle Geocast)

La méthode proposé dans [69] est une nouvelle méthode de diffusion qui généralise les méthodes précédentes (TRADE et DDT) et permet de surmonter les problèmes de fragmentation du réseau, de fiabilité et de calcul de voisins. Des relais dynamiques sont introduits pour rediffuser périodiquement les messages d'alerte. Ces relais sont désignés en fonction de la distance relative au véhicule source. Une comparaison avec les méthodes TRADE et DDT a été réalisée en utilisant un modèle analytique et des simulations, et a montré les améliorations apportées, et ce indépendamment de l'environnement (rural ou urbain).

Ces protocoles optimisent la dissémination d'information en sélectionnant seulement quelques nœuds pour la retransmission des messages. Ils tentent d'assurer à la fois un délai d'acheminement réduit et une meilleure utilisation des ressources.

G. ADCD (stratégie de dissémination adaptée aux données classifiées)

La solution proposer dans [29] a pour objectif de transmettre les bonnes informations aux bons véhicules et particulièrement lorsqu'il s'agit d'informations de sûreté. ADCD *ne* suppose pas l'existence préalable d'unités de bords de route. Dans ce cas tous les véhicules acceptent de coopérer en partageant leurs données collectées et en acceptant également d'assurer des retransmissions en cas de demande. Cette stratégie permet une récolte régulière des données et une diffusion adaptée, dans le but d'éviter les risques de congestion et de famine dans les zones éloignées.

Dans cette solution les auteurs ont considérés que chaque véhicule doit recevoir les informations locales liées à sa route, ainsi que les informations d'urgence récoltées dans un certain périmètre, qui soit plus large que pour les informations locales, tout en respectant une certaine durée de validité pour les données. Ceci, afin qu'un conducteur soit toujours au courant des conditions actuelles du trafic routier.

La stratégie de dissémination d'ADCD se base sur trois étapes :

–La récolte et la classification des données.

–L'élection des véhicules relayeurs et l'envoi du message.

–La retransmission itérative du message, d'après les caractéristiques de son contenu.

- Récolte et classification des données

Un véhicule peut être équipé de différents capteurs et collecter divers types de données.les auteurs considèrent que chaque information dépend de son lieu de collecte et que sa diffusion n'a de sens qu'aux alentours, cela durant une période de temps limitée afin d'éviter le partage d'informations obsolètes.

Ils ont caractérise chaque information par deux paramètres : la *classe* et le *mode*. La classe d'une information représente son niveau d'importance, elle définie l'étendue géographique de sa zone de dissémination, alors que son mode définit l'échelle de sa

ADCD propose un intervalle [σmin, σmax] pour les paramètres classe et mode. L'information la plus urgente se voit attribuer la valeur maximale pour sa classe et de même concernant le mode d'une information dont la validité dans le temps est la plus longue .Pour illustrer cette approche, le tableau 1 représente une caractérisation de quelques informations pouvant être échangées dans des applications de sûreté et de gestion du trafic routier.

Il faut prendre en considération qu'un véhicule est concerné par la réception d'une information uniquement s'il se trouve dans sa zone de transmission, laquelle est déterminée par sa classe, durant sa période de validité, qui est déterminée par son mode. Pour pouvoir cibler ces véhicules, ils ont considérés des zones de dissémination de forme carrée au tour du point de collecte de chaque information à distribuer, de sorte que l'échelle de la taille de chaque coté du carré corresponde à la classe de l'information.

- Dissémination des données

La figure (2.12) illustre le processus à suivre par un véhicule avant le partage d'une donnée. Pour alléger la charge du canal des informations redondantes, les trois conditions suivantes doivent être respectées :

–Le véhicule a récemment collecté des informations, les quelles sont différentes de ses derniers envois.

–Le véhicule peut retransmettre les mêmes informations une seconde fois si les messages à ce sujet ont atteint leur limite de validité et que l'événement est toujours d'actualité

–Aucun de ses voisins n'a pour l'instant partagé ces mêmes informations.

Une fois ces conditions réunies, un véhicule attend un court instant aléatoire, afin d'éviter les envois simultanés lors de la détection d'un même événement par des véhicules voisins. Si l'information détectée reste différente de celle reçue dernièrement par le véhicule, il procède à sa caractérisation en définissant sa classe et son mode, puis incorpore la date et le lieu de collecte de l'information dans le message.

La manière la plus sûre pour que tous les véhicules reçoivent une information est de l'envoyer par diffusion à plusieurs sauts. Cependant, cette méthode cause un phénomène dit de "broadcast storm" [68] et congestionne le réseau. Nous agissons autrement, en effectuant une seule diffusion aveugle à un seul saut, pour que tous les véhicules voisins directs à la source réceptionnent le message. Puis la retransmission de l'information se fait en prenant en considération sa classe et son mode. Le véhicule source est en charge d'élire les relayeurs pour son message parmi ses voisins directs, sachant que chaque véhicule connait tous ses voisins directs avec leurs coordonnées grâce aux messages HELLO échangés périodiquement. Il a aussi connaissance du nombre de voisins de chacun de ses voisins, soit parce que cette information a été ajouté aux messages HELLO ou alors grâce aux messages échangés pour la conduite collaborative.

Une liste de véhicules élus est alors insérée dans le message, afin de limiter son nombre de retransmissions. Le nombre de relayeurs pour un message dépend de l'importance de son contenu, soit la valeur de son paramètre classe. Plus une information est urgente plus sa transmission doit être complète et rapide.

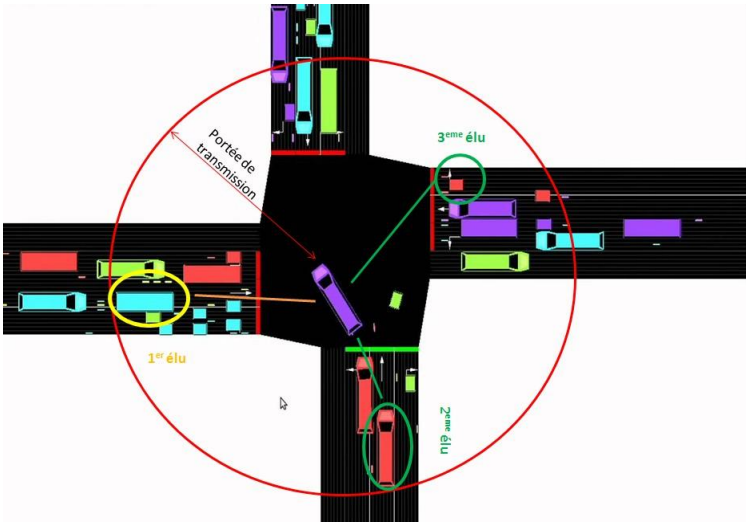

Figure 2-12 : Exemple d'élection de trois véhicules pour la retransmission d'un message [29].

La figure 2.13 illustre un exemple d'élection de véhicules relayeurs pour une information de classe3.Le premier véhicule relayeur élu à sa portée réseau, nous considérons alors le premier angle à 120° couvert. Pour couvrir les deux angles restants, nous choisissons le véhicule dont le nombre de voisins est le plus important dans chacun d'eux. Ce processus d'élection est représenté par l'algorithme 1, il nécessite en entrée le nombre de relayeurs requis sa fin de donner en sortie leurs coordonnées.

- Retransmission itérative

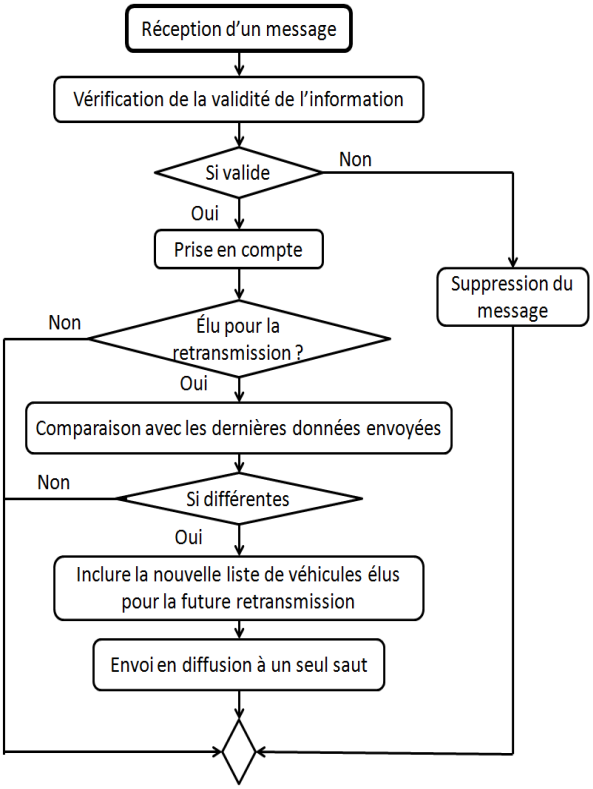

Figure 2-13 : Processus de réception et de retransmission[29].

A la réception d'un message, un véhicule vérifie sa validité par rapport aux caractéristiques spatiales et temporelles de son contenu. Le véhicule compare sa localisation par rapport à la zone de dissémination du message. Celle-ci est calculée par rapport à la classe et aux coordonnées de collecte de l'information. Puis, le véhicule récepteur vérifie si l'information est encore valide dans le temps via son mode et la date de sa collecte. Si le message échoue à une de ces deux vérifications, il se verra éliminé. Sinon le véhicule récepteur prendra en considération l'information et vérifiera s'il est élu pour la retransmission du message. Si oui, il rediffuse le message sans rien changer à ses caractéristiques, mais en actualisant la liste des élus pour la future retransmission. Ceci, à condition que le véhicule élu n'ait pas déjà partagé ces mêmes informations à travers des messages envoyés, qui sont encore valides dans le temps.

Les informations issues des applications de sûreté et de sécurité routière requièrent une dissémination rapide et complète pour tous les véhicules se situant dans la zone cible de dissémination, pendant tout le temps de validité de chaque donnée. A la traduction de ces contraintes par les notions de classes et modes qu'on associe aux différents types de messages, de sorte qu'une classe corresponde à la couverture géographique de la zone de dissémination et qu'un mode à la validité dans le temps de l'information.

2.4. Conclusion

Dans ce chapitre, nous avons introduit quelques protocoles de dissémination de messages d'alerte et de confort qui existe pour les réseaux véhiculaires. Les informations issues de ces applications requièrent une dissémination rapide et complète pour tous les véhicules situé dans la zone cible de dissémination, pendant tout le temps de validité de chaque donnée.

Dans le prochain chapitre, Nous allons faire une étude comparative des solutions de dissémination que nous avons présentée dans ce chapitre.

Chapitre 3 : Etude comparative et synthèse

3.1. Introduction

Plusieurs travaux se sont attaqués au sujet de la dissémination des messages dans les VANETs et une large variété de protocoles ont été proposés. D'après toutes ces propositions une classification à ces protocoles a été constatée. Cette classification se base sur un ensemble de critères que nous allons décrire pour mettre en évidence les principes de conception et les performances de ces protocoles [70, 71, 72].

Dans ce chapitre nous présentons aussi l'ensemble des métriques qui sont utilisées couramment pour comparer les protocoles de dissémination de l'information dans les réseaux véhiculaires. Ensuite, avec ces critères et métriques nous allons faire une comparaison entre ces protocoles.

3.2. Classification des mécanismes de dissémination

La façon la plus simple pour gérer la dissémination de l'information est l'inondation *«Flooding »*. Cette dernière est une stratégie bien connue dans les réseaux sans fil tels que les MANETs ou les VANETs. Elle offre une probabilité élevée que tous les nœuds destinataires reçoivent le message dans l'hypothèse où il existe des chemins en les reliant à la source.

Malheureusement, l'inondation pure est inefficace en particulier dans les réseaux véhiculaires denses, parce que le nombre de collisions devient de plus en plus élevé avec le nombre de nœuds dans la zone. En effet, dans les réseaux denses, l'inondation peut conduire au problème de tempête de diffusion « *broadcast storm problem*» [68] et ses conséquences négatives, notamment le gaspillage de la bande passante, la perte de paquets et les messages retardés.

Comme chaque véhicule rediffuse tous les messages qu'il reçoit, l'inondation en soit conduite à la redondance (plusieurs copies des mêmes messages circulent sur les mêmes liens). L'objectif principal des protocoles de dissémination qui ont été proposés est de réduire la redondance, et par conséquent, améliorer l'utilisation du réseau en sélectionnant de manière distribuée un sous ensemble de nœuds qui rediffusent le message dans la zone de dissémination.

3.2.1. Approche de conception de bas niveau [73]

Les protocoles de dissémination peuvent être classes selon quelques mécanismes de base comme notamment :

- **Balisage**

Il est utilisé pour permettre aux nœuds soit de diffuser des données périodiques et/ou d'échanger des informations d'état (nombre de messages reçus, nombre de messages diffusés, position et vitesse du véhicule ...).

- **Acquittement**

C'est un mécanisme de base pour améliorer la fiabilité. L'acquittement peut être explicite (un paquet ACK est utilisé pour accuser réception) ou implicite (après l'envoi d'un message, un nœud i écoute le canal et quand son voisin j rediffuse le message, le nœud i conclut que le message a été reçu par le nœud j). On notera que l'acquittement explicite engendre une augmentation dans le surcoût, essentiellement en termes de délai.

- **Adaptation de la portée de transmission**

Certains protocoles adaptent dynamiquement la portée de transmission selon la densité du réseau observée/estimée (c'est-à-dire transmettre avec une faible portée lorsque le réseau est dense et une portée élevée lorsque le réseau n'est pas dense).

- **Diffusion multi-canal**

Certains protocoles profitent des canaux disponibles pour diffuser les données sur plusieurs canaux. Il convient de noter que d'une part le nombre de canaux est très limité sous le DSRC et d'une autre part la gestion du multi-canal a un coût.

- **Utilisation d'infrastructure**

Certains protocoles s'appuient partiellement sur l'infrastructure fixe (ex : les RSUs) pour diffuser les données de sécurité tandis que d'autres sont entièrement sans infrastructure.

- **Zone de dissémination**

La zone de dissémination peut être explicite ou implicite. Différents paramètres (tels que la direction et la portée de communication) peuvent être utilisés pour spécifier cette zone. Lorsqu'elle n'est pas spécifiée, la dissémination peut être très coûteuse. Par conséquent, les protocoles existants qui ne spécifient pas la zone de dissémination devraient être adaptés avant leur déploiement.

- **Scénario du trafic**

Certains protocoles sont polyvalents (ils ciblent de multiples formes de trafic) tandis que d'autres sont spécifiques au contexte (par exemple la dissémination dans les zones urbaines ou sur des autoroutes).

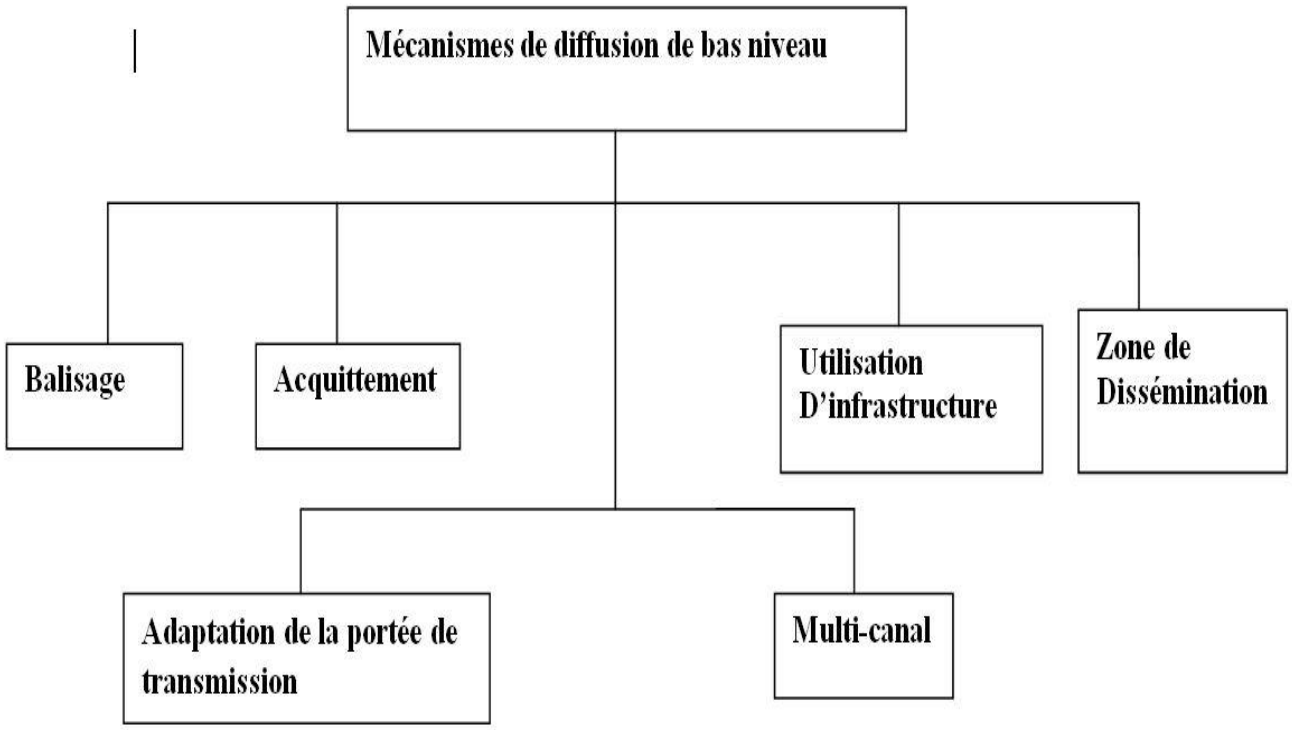

Figure 3-1 : Critères de classification de bas niveau [73].

3.2.2. Approche de conception de haut-niveau

D'après [74], ils ont pu identifier neuf classes de disséminations basées sur les mécanismes utilisés pour guider la rediffusion des messages reçus qui sont les suivantes :

- **Dissémination à base de compteur**

Chaque nœud compte le nombre de fois qu'un paquet est reçu pendant une période déterminée, puis il compare ce nombre avec un seuil prédéterminé pour décider s'il rediffuse le paquet ou le détruit. L'avantage de cette approche est que les nœuds n'ont pas besoins d'échanger les états des voisins pour construire collectivement une décision sur la rediffusion.

- **Dissémination à base de délai**

Chaque nœud reçoit un message à rediffuser, le garde pour un certain temps d'attente avant de décider de le rediffuser. Les temps de maintien sont choisis au

hasard par les nœuds. Le nœud ayant le temps de maintien le plus court a la priorité la plus élevée pour rediffuser le message. Un nœud qui a un message à rediffuser ne le rediffuse pas s'il sait que le message a été rediffusé par un autre nœud voisin.

- **Dissémination à base de distance**

Les messages sont rediffusés en considérant la distance entre l'émetteur et les récepteurs. Lorsqu'un nœud reçoit un message, il ne le rediffuse pas si la distance entre lui et son voisin le plus proche qui a déjà rediffusé le même message est inférieure à un seuil prédéfini. La raison est que si un nœud a reçu un message d'un autre nœud très proche de lui, il y a peu d'avantages dans la couverture supplémentaire obtenue par la rediffusion du message reçu. Par conséquent, les nœuds devraient favoriser la rediffusion lorsque la distance au dernier relai est grande.

- **Dissémination à base de localisation**

Les messages sont diffusés aux nœuds sur la base des positions géographiques de la source et de la destination. Ce mécanisme suppose qu'un service de localisation est disponible pour permettre de localiser les nœuds. Le principe de cette approche est de réduire le nombre de nœuds relais en sélectionnant les nœuds permettant un maximum de progrès dans la direction de dissémination.

Tous les récepteurs sont des relayeurs potentiels du message, et ils sont en concurrence entre eux pour rediffuser le message reçu, la période de contention est le temps qu'attendent les nœuds avant de rediffuser le message. Dans l'approche à base de localisation, cette période dépend essentiellement de la distance parcourue dans la direction de la dissémination.

- **Dissémination à base de trafic**

Des informations reflétant le trafic (densité, la vitesse du véhicule ...) sont utilisées pour guider les opérations de rediffusion. Il faut remarquer que la densité est le seul paramètre utilisé réellement dans les protocoles à base de trafic existants. L'utilisation d'autres paramètres peut entraîner un coût élevé pour recueillir les données d'état.

- **Dissémination à base de clusters**

Les messages sont diffusés à un groupe de véhicules (par exemple les taxis, les ambulances, peloton de véhicules sur une autoroute) se déplacent sur un chemin commun. Le groupe peut être structuré en un niveau ou en une hiérarchie.

Seulement, les nœuds têtes de clusters « Clusters Heads » rediffusent les messages à l'intérieur de leur cluster.

- **Dissémination probabiliste**

Quand un nœud reçoit un message, il le rediffuse selon une valeur de probabilité. Plus la probabilité de rediffusion est faible, plus le coût est faible (la consommation de

la bande passante) de la dissémination des données, et plus est faible la probabilité de livraison des messages à tous les destinataires. Plus est élevée la probabilité de rediffusion, plus est élevé le coût de la dissémination et plus est élevée la probabilité de livraison du message. Par conséquent, il existe un compromis entre le coût de la dissémination et la probabilité de livraison.

Les protocoles de dissémination existants ont proposé différentes façons pour dériver la probabilité de rediffusion : une valeur fixe pendant toute la durée de vie du réseau, une valeur fixe pendant une certaine période de temps, une valeur qui est fonction du nombre de messages reçus dans un intervalle de temps, une valeur qui est fonction du nombre de voisins à un saut, la distance entre l'émetteur et le récepteur du message, etc. Chaque modèle de calcul de la probabilité de rediffusion a ses avantages (simplicité et flexibilité) et ses inconvénients (surcharge due à la collecte des données utilisées dans le calcul de probabilité). Dans les protocoles existants, le mécanisme basé sur la probabilité est combiné avec d'autres mécanismes (par exemple, la distance ou la densité) pour améliorer la performance de la dissémination.

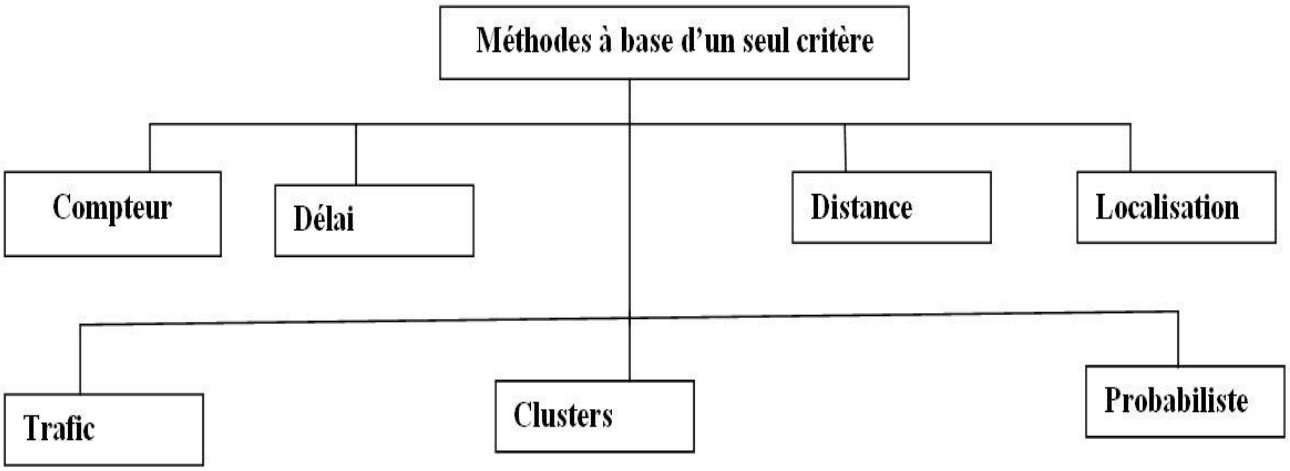

Figure 3-2 : Critères de classification de haut niveau [73].

3.3. Métriques d'évaluation des protocoles de dissémination [73]

Pour évaluer comment un protocole donné fonctionne par rapport à d'autres protocoles ou à la dissémination parfaite, des métriques ont été utilisées. Certaines métriques sont primitives tandis que d'autres peuvent être obtenues à partir d'autres métriques. Il est à noter que la définition de la même métrique peut varier selon les auteurs. En outre, certaines métriques sont plus pertinentes pour évaluer un protocole spécifique que, pour comparer différents protocoles. Il convient également de remarquer

que la performance dépend de nombreux facteurs, notamment de la densité du trafic et de la portée de transmission.

Il existe trois modèles de trafic, appelés régimes de trafic [75], qui impactent significativement les performances des protocoles de dissémination et nécessitent une adaptation de la diffusion : trafic dense, trafic clairsemé et trafic régulier.

- **Régime de trafic dense**

C'est lorsque le trafic est supérieur à une certaine valeur dans ce cas également connu comme *problème de tempête de diffusion « Broadcast Storm problem »* la probabilité de collision entre les nœuds en contention est très élevée, ce qui entraîne la perte ou le retard de paquets.

- **Régime de trafic clairsemé**

Il est observé dans certaines heures de la journée/semaine lorsque la densité de la circulation peut être si faible que la connectivité entre les nœuds devient indisponible et les messages ne peuvent pas atteindre à temps leur destination en raison d'insuffisance de nœuds relayeurs.

- **Régime de trafic régulier**

C'est le régime dominant lorsque le trafic des véhicules est observé. Il se caractérise par un trafic non-homogène (quelques nœuds peuvent avoir quelques voisins, tandis que d'autres ont beaucoup).

Dans la partie suivante nous allons présenter l'ensemble des métriques [73] qui sont utilisées couramment pour comparer les protocoles de dissémination. En général, la valeur moyenne de la métrique est considérée pour l'évaluation/comparaison de performances.

A. Métriques temporelles et spatiales

- *Délai de bout en bout :* c'est le temps écoulé entre la première diffusion du message et sa réception par le dernier récepteur dans la zone. La valeur requise de la métrique dépend de l'application de sécurité considérée.
- *Distance de propagation* : elle mesure à quelle distance de la source le message est diffusé dans la zone. Une distance proche de (ou supérieure) la portée de communication requise par l'application est attendue.
- *Vitesse de propagation (ou vitesse de dissémination) :* elle mesure la vitesse à laquelle le message se propage dans le réseau. Elle s'exprime par la distance parcourue par unité de temps, ou la portion de nœuds qui reçoivent le message par unité de temps.

B. Fiabilité

- L*e taux (ou ratio) de livraison :* il mesure la proportion de véhicules dans la zone d'intérêt qui reçoivent le message. Une valeur proche de 100% est fortement préférable pour rendre réellement les VANETs très efficaces pour le support des applications de sécurité. Le taux de livraison est aussi appelé *Taux (ou ratio) de réception* (ou probabilité de réception).
- *Débit de réception :* c'est le nombre de messages (ou bits) reçus par un nœud dans une période de temps (par exemple en secondes). Cette mesure est particulièrement utile lorsque des données périodiques sont diffusées. Etant donné la période et la taille d'un message, cette mesure permet d'évaluer comment le débit de réception des nœuds est proche du débit optimal requis par l'application.
- *Taux de perte de paquets :* à cause des collisions, certains messages n'atteignent jamais certaines (ou toutes) destinations. Cette métrique, qui s'applique aux messages périodiques et aux messages d'alerte, est utile pour évaluer la fiabilité du réseau.

C. Mesures d'efficacité

- *Taux de Collisions :* comme les nœuds partagent le même canal sans fil, les collisions peuvent se produire lorsque les nœuds rediffusent les messages. Cette métrique donne une indication sur la façon dont les opérations de la rediffusion impactent les performances du réseau.
- *Taux de redondance :* il mesure le nombre de paquets dupliqués par un paquet source. En d'autres termes, la redondance indique combien de fois un paquet est rediffusé pour atteindre les véhicules dans la zone d'intérêt. C'est un indicateur de surcoût. La limite supérieure du taux de redondance est donnée par l'inondation pure. La redondance est un indicateur clé de performance d'un protocole de dissémination. Un bon protocole devrait être en mesure de disséminer l'information à travers toute la zone d'intérêt avec le moins de redondance ou de surcoût.
- *Surcoût de la diffusion du nœud :* au lieu du taux de redondance, certains auteurs utilisent le surcoût de la rediffusion, qui est le nombre de messages rediffusés collectivement dans la zone d'intérêt.
- *Taux de nœuds diffuseurs :* il mesure la proportion de nœuds qui rediffusent un message. C'est un indicateur de l'implication des nœuds dans la rediffusion. La limite supérieure est de 100% (d'inondation pure) ce qui signifie que tous les nœuds rediffusent le message.
- *Taux de rediffusion du nœud* : il mesure le nombre de fois que le nœud rediffuse les messages dans un intervalle de temps donné. Il mesure l'équité dans la rediffusion. Cette mesure peut être utilisée pour détecter les nœuds avec une forte participation dans la rediffusion (par exemple des nœuds avec le rayon de communication plus élevé ou des nœuds qui attaquent le réseau pour diffuser de fausses alertes ...).

- *Utilisation du canal :* elle mesure comment la charge globale de la rediffusion occupe le canal. Dans les applications de sécurité, l'utilisation du canal doit rester faible ce qui signifie que le canal doit être libre de temps en temps pour permettre la diffusion de messages d'alerte.

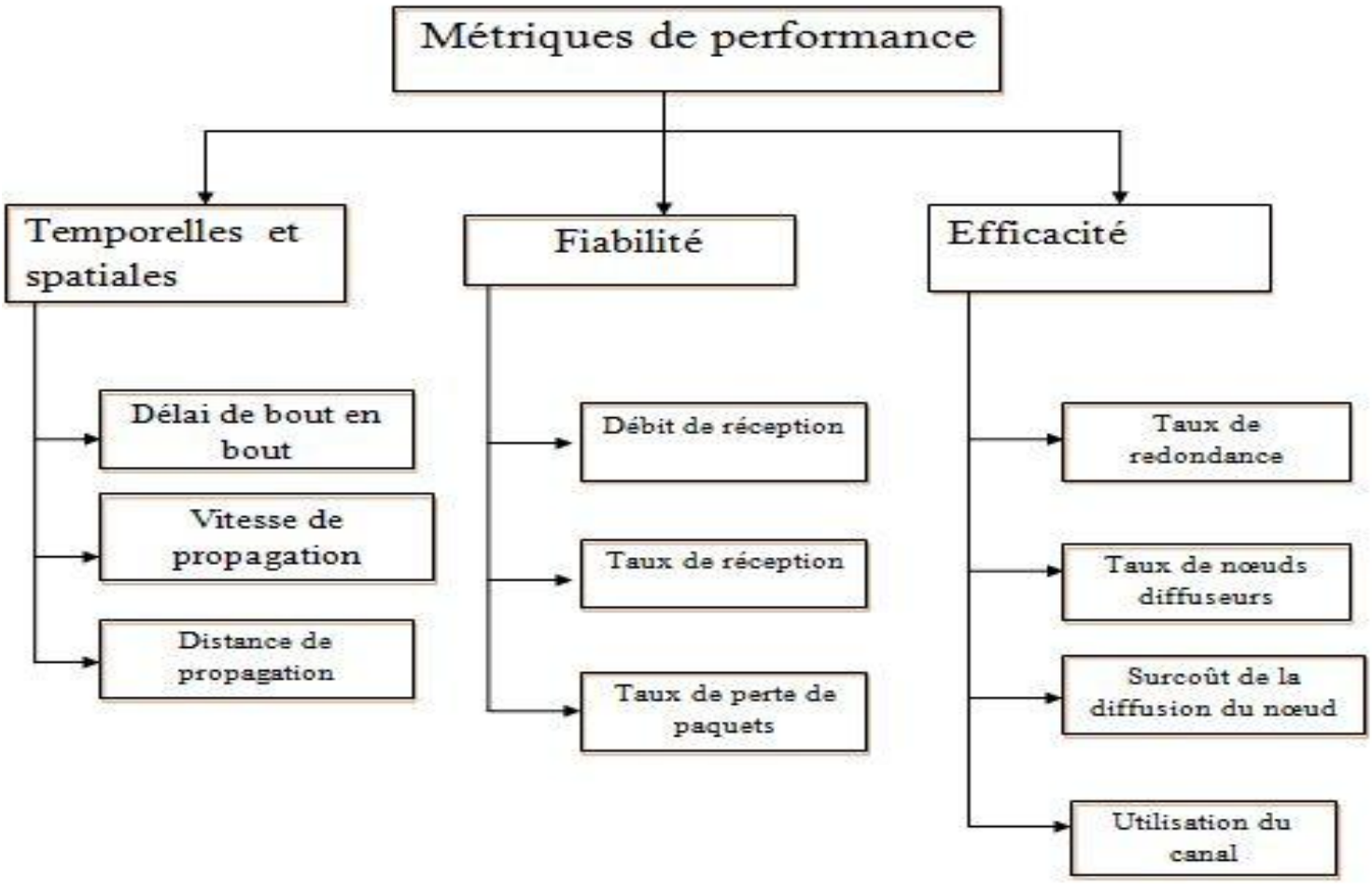

Figure 3-3 : 3.3.Métriques d'évaluation des protocoles de dissémination [73].

Les tableaux 2,3 et 4 suivant donnent une comparaison des protocoles étudié au chapitre deux selon l'approche de bas et de haut niveau et les métriques de la section 3.2.1 respectivement :

Tableau 3-1 : Classification des protocoles de dissémination -Approche de conception de haut-niveau [73].

Critères / Protocol	Localisation	Distance	Cluster	Trafic	Délai	Probabilité	Compteur
ADCD	✓	✓	✓	✓	✓	✓	✓
DPP	✓	✓	✓		✓		✓
DDT	✓	✓			✓		✓
IVC	✓	✓			✓		
IVG				✓	✓	✓	
MDDV					✓		✓
MHFH	✓	✓			✓		
MHVB	✓	✓		✓	✓		✓
OAPB		✓		✓	✓	✓	✓
ODAM	✓	✓			✓		
RBM					✓		
STEID	✓	✓	✓		✓		
SODAD	✓	✓			✓		
TRADE	✓	✓			✓		✓
UBM	✓	✓			✓		

Tableau 3-2 : Classification des protocoles de dissémination -Approche de conception de bas-niveau [73].

Critères / PROTOCOLE	Balisage	Acquittement	Adaptation de la portée	Zone de Dissémination	Utilisation d'infrastructure	Scénario de Trafic
ADCD	✓	I	✓	✓	A	AT/U
DPP	✓	E	✓	✓	-	AT
DDT	✓		✓	✓	A	AT/U
IVC	✓		✓	✓	-	-
IVG	✓		✓	✓	A	U
MDDV	✓		✓	✓	A	AT/U
MHVB	✓		✓	✓	A	AT
OAPB	✓		✓	✓	A	AT/U
ODAM	✓	I	✓	✓	A	AT/U
RBM	✓		✓	✓	-	AT
STEID	✓		✓	✓	A	U
SODAD	✓		✓	✓	-	U
TRADE	✓	I	✓	✓	-	-
UBM	✓	E	✓	✓	D	AT/U

- : Non spécifiée ; D : Direction ; A : Aléatoire ; T : TTL (Time to live) ; E : ACK explicite ; I : ACK implicite ; AT : Autoroute ; U : Urbain.

Tableau 3-3 : Métriques de performance des protocoles de dissémination [73].

PROTOCOLES	Temporelles et Spatiales			Fiabilité			Efficacité			
	Délai de Bout en bout	**Vitesse de Propagation**	**Distance de Propagation**	**Débit de Réception**	**Taux de réception**	**Taux de perte de paquets**	**Taux de Redondance**	**Surcoût du nœud**	**Taux de nœuds diffuseurs**	**Utilisation du canal**
ADCD	✓	✓	✓		✓	✓	✓	✓	✓	✓
DPP	✓	✓	✓							
DDT	✓	✓	✓		✓					
IVC	✓	✓	✓						✓	
IVG	✓	✓	✓						✓	
MDDV			✓			✓				✓
MHFH			✓			✓				✓
MHVB					✓	✓				
OAPB	✓	✓	✓		✓		✓			✓
ODAM				✓	✓	✓				
RBM	✓		✓							
STEID	✓	✓	✓			✓	✓			✓
SODAD	✓	✓		✓			✓	✓		
TRADE	✓		✓							
UBM		✓			✓		✓			

3.3.2. Discussion :

Un grand nombre de protocoles de dissémination ont été proposés dans la littérature ces dernières années. Nous avons fournis trois tables (Tables 3--2, 3-3 et 3-4) comparatives de 13 protocoles de dissémination. Cette classification est basée sur les critères que nous avons présentés. La Table 3-3 et est une synthèse de l'analyse des performances qualitatives des protocoles de dissémination. Elle montre les métriques évaluées par les auteurs.

D'après cette comparaison on a constaté que chaque protocole à ses propres avantages et ses limites, et un compromis entre eux doit être accepté. Il n'existe pas de protocole parfait, et, approcher d'un tel protocole soulève de nombreux défis pour la recherche future. Certains protocoles sont efficaces pour délivrer des messages de confort tandis que d'autres sont efficaces pour délivrer les messages d'alerte. Certains protocoles se comportent bien uniquement sous une densité faible, tandis que d'autres ont un rendement acceptable dans des réseaux denses.

Comme on a vue presque tous les protocoles sont basés sur plusieurs critères où la *localisation*, la d*istance* et le *trafic* sont considérés ensemble pour guider les décisions de rediffusion. Aussi, presque tous les protocoles sont basés sur le délai, ce qui signifie que les nœuds attendent pour une période (aléatoire) de temps avant de tenter de rediffuser. C'est un mécanisme simple et puissant pour réduire la redondance de messages.

Après avoir fait cette comparaison en basée sur des métriques et des critères bien défini, on a pu constater qu'il y'avait des point communs entre ces protocoles on peut trouver une métrique ou un critère qui utilise la majorité des protocoles comme le taux de réception.

Comme indiqué précédemment, les principales exigences des applications de sécurité sont la rapidité et la fiabilité. La table 4 montre que presque tous les protocoles ont rapporté des résultats sur le délai de bout en bout et le ratio de livraison et donnent quelques résultats sur le taux de redondance (qui est une métrique de surcoût).

Pour donner des résultats de performance, la densité est le principal paramètre de simulation qui est utilisé dans tous les articles que nous avons examinés. La *distance* de diffusion est utilisée à peu près dans la moitié des protocoles. *La vitesse* du véhicule est considérée de trois façons : une valeur constante pour tous les véhicules, une valeur aléatoire choisie dans un intervalle ou une valeur aléatoire ne dépassant pas un maximum comme on peut le remarquer sur les tables 3-3, très peu d'articles ont fourni une simulation intensive et "complète". Certains papiers ciblant les applications de sécurité ont présenté des résultats de simulation non pertinente (sans importance) à ces applications, parce que certains auteurs ont mal compris les exigences des applications de sécurité

D'après les tables présentées nous remarquons que chaque protocole a un certain nombre de performances et avec cela nous avons conclus que parmi les protocoles étudier qu'ADCD est le protocole le plus adaptatif.

3.4. Conclusion

Dans ce chapitre nous avons évalué et comparé l'approche de bas niveau et de haut niveau des protocoles de dissémination liées aux messages d'urgences et de confort que nous avons présenter dans le chapitre précédant pour cela nous avons d'abord présenter l'approche de conception de bas niveau et de haut niveau et métriques de performances.

Conclusion générale

Le développement des nouvelles technologies a favorisé une formidable évolution des réseaux véhiculaires. Cette évolution vise à rendre la conduite plus sûre, plus efficace, plus fiable et plus écologique aussi bien du point de vue de l'industrie automobile que des opérateurs de réseaux et services. Les réseaux véhiculaires sont en effet une classe émergente des réseaux mobiles Ad Hoc permettant des échanges de données entre véhicules ou encore véhicules et infrastructure. Ils suscitent un intérêt certain dans le but d'améliorer la sécurité et l'efficacité des transports routiers ainsi que l'amélioration du confort de l'usager en lui fournissant une multitude des services d'information, d'aide à la décision, de guidage et d'accès à internet.

Les applications de sécurité routière et de divertissement, pour lesquelles une grande quantité de contenus peut exister, exigent que les contenus engendrés soient propagés au travers des véhicules et/ou de l'infrastructure jusqu'à atteindre les utilisateurs intéressés tout en respectant les durées de vie potentiellement limitées des contenus. La dissémination de contenus pour ces type d'applications reste un défi majeur en raison de plusieurs facteurs tels que la présence de beaucoup de contenus, la connectivité très intermittente mais encore les intérêts potentiellement hétérogènes des utilisateurs.

Dans ce mémoire nous nous somme tout particulièrement intéressé a la dissémination des données. Les applications de sécurité routière et de divertissement, pour lesquelles une grande quantité de contenus peut exister, exigent que les contenus engendrés soient propagés au travers des véhicules et/ou de l'infrastructure jusqu'à atteindre les utilisateurs intéressés tout en respectant les durées de vie potentiellement limitées des contenus. La dissémination de contenus pour ces type d'applications reste un défi majeur en raison de plusieurs facteurs tels que la présence de beaucoup de contenus, la connectivité très intermittente mais encore les intérêts potentiellement hétérogènes des utilisateurs.

Après avoir présenté quelques approches de dissémination existante pour les VANETS, on a fait une étude comparative basée sur des approches de conception et quelques métriques comme le délai de bout en bout, le taux de réception etc.

En effet, nous avons conclus que parmi les protocoles étudier qu'ADCD est le protocole le plus adaptatif. En présentant une stratégie de dissémination adaptée pour chaque type (classe, mode) de messages, nommée *ADCD*. Cette approche propose un compromis entre le taux de réception, la vitesse de dissémination des messages et le nombre de messages superflus qu'elle peut générer. *ADCD* adapte sa stratégie de dissémination en choisissant le nombre de relayeurs adéquat pour chaque type de message, afin de respecter ses contraintes.

Enfin, Nous avons également acquis un bon aperçu des méthodes de travail d'un chercheur, avec une connaissance approfondie dans ce domaine. Tout au long de ce travail, nous avons développé des nouvelles idées prometteuses qui vont nous permettre dans l'avenir proche d'élargir ce sujet de recherche et s'attaquer aux problématiques plus pointues dans le domaine de réseau de VANET et potentiellement autres réseaux de nature proche avec des solutions plus génériques.

Bibliographie

[1] C. BURGOD, Contribution à la sécurisation du routage dans les réseaux adhoc , Université de Limoges ,Thèse de doctorat, 2009.

[2]RESEAUXADHOC.Généralités.http://www.opera.fr/people/TayebLemlouma/papers/AdHoc_presentation/. Connecté.

[3] A.Gégout, Les réseaux Ad Hoc http ://www.tdf.fr/medias/view/ ?id=704,2005.

[4] R.Meraihi, Gestion de la qualité de service et contrôle de topologie dans les réseaux AdHoc ,PhDthesis, Ecole Nationale Supérieure des Télécommunications de Paris,2005.

[5] J.Vandermeerschen, Hybridation entre les modes Ad Hoc et infrastructuredans les réseaux de type Wifi-Fi, http ://code.ulb.ac.be/dbfiles/media832.pdf,2006.

[6] A.Benoit, Algorithmique des réseaux et des télécoms, http://graal.enslyon.fr/abenoit/reso05/cours/3-adhoc.pdf, 2006.

[7] E.G. Ktur, Ad Hoc Networks, Theirs Simulation, Emulation and real worldExperiments,http ://folk.uio.no/erek/talks/050323odtumanet.pdf, 2009.

[8] C.Chaidet,I.GLassous, Routage QoS et réseau Ad hoc,http://hal.inria.fr/docs/00/07/18/86/PDF/RR-4700.pdf, 2003.

[9] J.P.Hubaux, C.Srdjan and L.Jun,Conférence,The securityand privacy of smart vehicles, IEEE Security & Privacy, 2004.

[10] I.Lequerica,M.G.Longaron, P.M. Ruiz. Drive and Share,Efficient Provisioning of Social Networks in Vehicular Scenarios,IEEECommunications Magazine, pages 90–97, 2010.

[11] R .Coussement ,mécanisme d'aide à la décision pour les ids dans les réseaux vanets ,l'université du québec à trois-rivières,janvier 2014.

[12] N.Bouchemal, R. Naja and S. Tohme, Traffic Modeling and Performance Evaluation in Vehicle to Infrastructure 802.11p Network , in Ad Hoc Networks, M. H. Sherif, A. Mellouk, J. Li and P. Bellavista, Éd. Springer International Publishing, 2013, p. 82-99.

[13] P.MARLIER ,Communications optimisées dans un réseau véhiculaire ad hoc multi-sauts , Université de Technologie de Compiègne, Juillet 2007 .

[14] F.Mezghani, la dissémination de contenus dans les réseaux véhiculaires, Institut National Polytechnique de Toulouse (INP Toulouse), vendredi 9 octobre 2015.

[15] ASTM International, Standard Spécification for Télécommunications 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, April 2009.

[16] Etsi, intelligent transport systems (its) ,european profile standard for the physical and medium access control layer of intelligent transport systems operating in the 5 ghz frequency band, etsi std, 2010.

[17] CEPThttp://www.anfr.fr/fr/l-anfr/organisation/le-cadre-europeen/cept-ecc.html.,

[18] R.Uzc,Ã.tegui,G.Acosta-Marum,Wave:Atutorial,IEEE CommunicationsMagazine, 47(5) :126–133, May 2009.

[19] IEEE 802.11-2012, IEEE Standard for Iinformation technology–Telecommunications and information exchange between systems local and metropolitan area networks–Specific requirements part 11: Wireless lan medium access control (MAC) and physical layer (PHY) specifications, 2012.

[20] F.Mezghani, R.Dhaou, M.Nogueira andA.L.Beylot,Contentdissemination in Vehicular Social Networks : Taxonomy and User satisfaction,IEEECommunications Magazine, 52(12):34–40, 2014.

[21] IEEE 802.11p, Amendment 6: Wireless Access in Vehicular Environments, July 2010.

[22] R. Kumar, M. Dave,A review of various vanet data dissemination protocols,International Journal of U- and E-Service, Science and Technology, 5(3):27–44, 2012.

[23] F.D.Da Cunha, L. A.Vilas, A. CarneiroViana and A.A.F. Loureiro,Data Communication in VANETs : A Survey, Challenges and Applications, Technical report, January 2014.

[24] R. Kumar and M. Dave, A review of various vanet data dissemination protocols,International Journal of U- and E-Service, Science and Technology, 5(3):27–44, 2012.

[26]J. Zhang, A survey on trust management forvanets,In IEEE International Conference on Advanced Information Networking and Applications (AINA' 12), Biopolis, Singapore, 2011.

[27] Y.C. Tseng, S.Y. Ni, Y.S. Chen and J.P. Sheu, The broadcast storm problem in a mobile ad hoc network , Wireless Networks, 8(2/3), p. 153-67, 2002.

[28] S. Buchegger,J.Y.L. Boudec, Performance analysis of the confidant protocol : Cooperation of nodes - fairness in dynamic ad-hoc networks, In The Third ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc' 02), Lausanne, Switzerland, 2002.

[29] N .Haddadou, Réseaux ad hoc véhiculaires : vers une dissémination de données efficace, coopérative et fiable, École Doctorale MSTIC, Université Paris-EST, juin 2014.

[30] N. Benamara, D. Kamal, M. Benamara, D.El Ouadghiria and J.M. Bonninb, Routing protocols in vehicular delay tolerant networks: A comprehensive survey, Computer Communications, 2014.

[31] M.Z. Ashtiani,Q. Dongyu, Achieving fair cooperation for multi-hop ad hocnetworks.,In QBSC, Queen's University Kingston, Canada, May 2010.

[32] L. Buttyán,J.P. Hubaux, Enforcing service availability in mobile ad hoc wans,In ACM MobiHoc, Boston, USA, Aug 2000.

[33] L. Buttyán,J.P. Hubaux, Stimulating cooperation in self-organizing mobile ad hoc networks,ACM/Springer MONET, 8 :579–592, 2003.

[35] S. Ni, Y. Tseng, Y. Che and J. Sheu,The broadcast storm problem in a mobile ad hoc network,In Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking (MobiCom' 99), New York, USA, 1999.

[36] G. Korkmaz, E. Ekici, F. Ozguner, U. Ozguner, Urban multi-hop broadcast protocol for inter-vehicle communication systems, In ACM International Workshop on Vehicular Ad Hoc Networks, New York, NY, USA, 2004.

[37] M. Sun, W. Feng, T.H. Lai, K. Yamada, H. Okadaand K. Fujimura,Gps-based message broadcasting for inter-vehicle communication, In International Conference on Parallel Processing (ICPP' 00), Toronto, Canada, 2000.

[38] C. Palazzi, F,Pezzoniand P. Ruiz,Delay-bounded data gathering in urban vehicular sensor networks, Elsevier Journal of Pervasive and Mobile Computing, Special Issue on Vehicular Sensor Networks and Mobile Sensing over Wide-Scale Deployment Environments, 8(2):180–193, 2011.

[39] N. Wisitpongphan, O.K. Tonguz,J.S. Parikh, P. Mudalige, F. Bai and V. Sadekar, Broadcast storm mitigation techniques in vehicular ad hoc networks, IEEE Wireless Communications, 14(6):84–94.

[40] M.Slavik and I. Mahgoub,Stochastic broadcast for vanet, In IEEE Consumer Communication and Networking Conference (CCNC' 10), Las Vegas, Nevada, USA, 2010.

[41] S. Busanelli, G. Ferrari, and S. Panichpapiboon,Efficient broadcasting in ieee 802.11networksthroughirresponsibleforwarding,InIEEEGlobalTelecommunicationConference (GLOBECOM' 09), Honolulu, Hawai, USA,2009.

[42] M. Bakhouya, J. Gabet and M. Wack.Performance evaluation of dream protocol for inter-vehicle communication. In Wireless Communication, Vehicular

Technology, Information Theory and Aerospace and Electronic Systems Technology, Aalburg, Netherlands, May 2009.

[43] U. Lee,M. Gerla,A survey of urban vehicular sensingplatforms,Elsevier ComputerNetworksJournal,54(4):527–544,March2010.

[44] A. Palma, P.P. Pereir and A. Casaca, Multicast routing protocol for vehicular delay-tolerant networks, In IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob' 12), Barcelona, Spain, October 2012.

[45] P. Liu, Z. Tao, S. Narayanan, T. Korakis and S.S. Panwar,Coopmac : A cooperative mac for wireless lans,IEEE Journal on Selected Areas in Communications,25(2) :340–354, Feb2007.

[46] J.Peng,L. Cheng,A distributed mac scheme for emergency messagedissemination in vehicular adhocnetworks,IEEETransactions on VehicularTechnology,56(6):3300–3308,Nov2007.

[47] M. T.Moreno, D. Jiang and H,Hartenstein, Broadcast reception rates and effects of priority access in 802.11-based vehicular ad-hoc network, In The first ACM Workshop on Vehicular Ad Hoc Networks (VANET' 04), Philadelphia, Pennsylvania, USA, October 2004.

[48] N. Haddadou and A. Rachedi.Dtm^2 : Adapting job market signaling for distributed trust management in vehicular ad hoc networks. In IEEE ICC, Budapest, Hungary, June 2013.

[49] H.Haddadou,A.Rachedi,Y.GhamriDoudane.Advanceddiffusionofclassifieddata in vehicularsensornetwork ,In Wireless CommunicationsandMobileComputing Conference (IWCMC'11), Istanbul, Turkey, July 2011.

[49] M. Gerharz, C. de Waal, M. Frank, A practical view on qualityof-service supportinwirelessadhocnetworks,InThe3rdIEEEWorkshoponApplicationsandServices in WirelessNetworks(ASWN'03),2003.

[50] A. Rahim, M. Yasin, I. Ahmad, Z.S. Khan, and M. Sher. Relevance based approach with virtual queue for vehicular adhoc networks. In International Conference on Computer, Control and Communication (IC4' 09), Karachi, Pakistan,2009.

[51] M.-T.Sun, Gps-based message broadcast for adaptive intervehicle communications,VTC Fall 2000.

[53] T.D.C.Little, A. Agarwal: An Information Propagation Scheme for VANETs, MCL Technical Report 07-01-2005, Department of Electrical and Computer Engineering, Boston University,Boston, USA, July 2005.

[54] L. Briesemeister, L. Schäfers and G. Hommel: Disseminating Messages among Highly Mobile Hosts based on Inter-Vehicle Communication, In Proceedings of the IEEE Intelligent Vehicles Symposium 2000, pages 522–527, Piscataway, NJ, USA, October 2000.

[55] Alshaer, H. and E. Horlait: An Optimized Adaptive Broadcast Scheme for Inter-vehicle Communication. In Proceedings of the IEEE Vehicular Technology Conference (IEEE VTC2005-Spring),pages 2840– 2844, Stockholm, Sweden, May 2005.

[56] A. Benslimane, Optimized Dissemination of Alarm Messages in Vehicular Ad-Hoc Networks (VANET) ,2004.

[57] M.N. Mariyasagayam, T.Osafune, M. Lenardi, Enhanced MultiHop Vehicular Broadcast (MHVB) for Active Safety Applications , 2007.

[58] M,A,Javed,D.T.Ngo,J.Y.Khan,EURASIP Journal on Wireless Communications and Networking2014:179,Awais Javed et al.; licensee Springer,2014.

[59] J.J.Blum, A Eskandarian, A reliable link-layer protocol for robust and scalable intervehicle communications,IEEE Tran,Intell, Transportation Syst 2007, 8(1):4-13.

[60]C,L,Huang,Y,P,Fallah,R,Sengupta,H,Krishnan:Adaptiveintervehicle communication control for cooperative safety systems. IEEE Network 2010, 24(1):6-13.

[61] M.Torrent-Moreno, Mittag J, Santi P, Hartenstein H: Vehicle-to-Vehicle communication: Fair transmit power control for safety-critical information,IEEE Trans,Vehic. Technol 2009, 58(7):3684-3703.

[63] M.Sepulcre, J.H.Gozalvez,H.Hartenstein: Contextual communications congestion control for cooperative vehicular networks,IEEE Trans,WirelessCommun 2011, 10(2):385-389.

[64] L. Wischhof, A. Ebner, et H.Rohling,Information Dissemination in Self-Organizing Intervehicle Networks ,mars 2005.

[65] H.Wu, R.Fujimoto, R.and M.Hunter: MDDV: A Mobilitycentric Data Dissemination Algorithm for Vehicular Networks, In Proceedings of the Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks (VANET '04), pages 47–56, New York, NY, USA, 2004. ACM Press.

[66] G. Korkmaz, E. Ekici, F. Ozguner and U. Ozguner , Urban Multi-Hop Broadcast Protocol for Inter-Vehicle Communication Systems, Proceedings of First ACM Workshop on Vehicular Ad HocNetworks (VANET 2004), p. 76-85, Philadelphia, PA, USA, Octobre 2004.

[67] L. Briesemeister, G. Hommel, « Role-based multicast in highly mobile but sparselyconnected ad hoc networks », Proceedings of the 1st ACM international symposium on Mobile ad hocnetworking& computing, Boston, Massachusetts, 2000.

[68] S. Ni, Y. Tseng, Y. Chen and J. Sheu. The broadcast storm problem in a mobile ad hoc network. In Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking (MobiCom' 99), New York, USA, 1999.

[69] R. Chen, W. L Jin, and A. Regan, Broadcasting Safety Information in Vehicular Networks:Issues and Approaches, IEEE Network, vol. 24, no. 1, pp. 20-25, 2010.

[70] R. Kumar and M. Dave, A Review of Various VANET Data Dissemination Protocols,International Journal of u- and e- Service, Science and Technology, vol. 5, no. 3, pp. 27-44,2012.

[72] S. Panichpapiboon and W. Pattara-Aticom, A review of Information Dissemination Protocols for Vehicular Ad Hoc Networks, IEEE Communications Surveys & Tutorials, vol. 14, no. 3,pp. 784-798, 2012.

[73] A. Berradj and Z. Mammeri, Multi-hop broadcasting in VANETs for safety applications:Review and classification of protocols, International Journal of Business DataCommunications and Networking, vol. 9, no. 4, pp. 86-104, Oct. 2013.

[74] J. J. Blum, A. Eskandarian, and L. J. Hoffman, Challenges of Intervehicle Ad Hoc Networks,IEEE Transactions on Intelligent Transportation Systems, vol. 5, no. 4, pp. 347-351, 2004.

[75] O. Tonguz, N. Wisitpongphan, and F. Bai, DV-CAST: A Distributed Vehicular Broadcast Protocol for Vehicular Ad Hoc Networks, IEEE Wireless Communications, vol.17,no.2,pp.47-56,2010.

Résumé

Les réseaux véhiculaires, connus sous le terme VANETs, sont des réseaux impliquant des communications entre véhicules ou entre véhicules et des unités de bords de route (RSU). Des défis majeurs ont besoin cependant d'être abordés pour offrir une communication sur une route sécurisée et fiable dans des environnements anonymes et quelque fois hostiles à la communication. Comme dans tout système de communication, les réseaux véhiculaires doivent opérer en respectant des contraintes. Ces contraintes sont d'autant plus strictes quand il s'agit de fournir des services de sécurité. Dans ce projet, nous avons classifié et comparé quelques solutions de dissémination existante pour les réseaux véhiculaires selon les approches de conception de bas et de haut niveau et quelque métriques comme le délai de bout en bout, le taux de réception.

Mots clé : VANETs, Dissémination, Métrique.

Abstract

Vehicle networks, known as VANETs, are networks involving communications between two or more vehicles and possibly communication with elements of infrastructure on the road. However, major challenges need to be tackled to provide communication on a secure and reliable route in anonymous environments that are sometimes hostile to communication. As in any communication system, vehicular networks must operate under constraints. These constraints are all the more stringent when it comes to providing safety and comfort services. This project aims to compare some existing dissemination methods for vehicular networks for reliably linking information. These techniques make it possible to respect severe time constraints in order to envisage their use in different applications on the road. To do so, these methods of disseminating information were explained and then design approaches and metrics based on different real-time measurements.

Keybords : VANETS, dissémination,