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


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

# *MÉMOIRE DE MASTER RECHERCHE*

**En**
**Informatique**

**Option**
***Réseaux et Systèmes Distribués***

# Thème

# Approche à base d'alliances dans les graphes pour la réduction de la congestion dans les VANETs

**Présenté par : Mlle Maouche Nadira et M. Oudia Jugurta**

**Soutenu le 01 Juillet 2017 devant le jury composé de :**

| | | | |
|---|---|---|---|
| **Président** | **M. Saadi** | **Maître Ass. A** | **U. A/Mira Béjaia.** |
| **Rapporteurs** | **H. Slimani** | **Maître de conf. A** | **U. A/Mira Béjaia.** |
| | **K. Ouazine** | **Doctorante "LMD"** | **U. A/Mira Béjaia.** |
| **Examinateur** | **M. Moktefi** | **Maître Ass. B** | **U. A/Mira Béjaia.** |
| **Examinatrice** | **M. Sadou** | **Doctorante "LMD"** | **U. A/Mira Béjaia.** |

Béjaia, Juillet 2017.

# ⁕ Remerciements ⁕

***Avant tout, nous remercions Dieu de nous avoir donné le courage et la foie pour mener à bien ce travail, malgré tous les obstacles.***

***Nos plus vifs et profonds remerciements vont au Dr H. SLIMANI qui fut pour nous un superviseur attentif et disponible malgré ses responsabilités nombreuses. Sa compétence, sa clair voyance, son humanisme, son dynamisme, sa rigueur et sa patience nous ont beaucoup appris, nous lui témoignons notre respectueuse gratitude.***

***Nous remercions Mlle K. OUAZINE pour l'aide qu'elle nous a apportée pendant toute la durée de réalisation de ce mémoire.***

***Nos plus sincères remerciements s'adressent également au membres de jury : M. SAADI, M. MOKTEFI et Mlle SADOU pour avoir accepté d'examiner notre travail.***

***Que toute personne qui, d'une manière ou d'une autre, nous a encouragé et aidé à l'aboutissement de ce modeste travail, trouve ici l'expression de nos sincères reconnaissances.***

***Nadira et Jugurta.***

# ⁕ *Dédicaces* ⁕

***Louange à Dieu, le miséricordieux, sans lui rien de tout cela n'aurait pu être.***

***O*n dédie ce modeste travail :**

***À* nos trop chers parents : Votre amour a laissé en nous une empreinte indélébile.**

**Nous vous prions de trouver en ce travail le fruit de vos efforts, le sacrifice des plus profitables années de vos vies, pour nous voir réussir.**

**Que Dieu nous accorde la grâce de vous avoir encore à nos côtés pour longtemps afin que vous soyez témoins de notre reconnaissance.**

***À* tout ceux que nous aimons.**

# Table des matières

# Table des figures

# Liste des tableaux

# Liste des abréviations

**MANET :** Mobile Ad hoc Network.
**VANET :** Vehicular Ad hoc Network.
**RSU :** Road Side Unit.
**OBU :** On-Board Unit.
**V2V :** Vehicle to Vehicle.
**V2I :** Vehicle to Infrastructure.
**I2I :** Infrastructure to Infrastructure.
**DSRC :** Dedicated Short-Range Communications.
**WAVE :** Wireless Access in Vehicular Environment.
**AODV :** Ad-hoc On-Demand Distance Vector Routing.
**OLSR :** Optimized Link State Routing Protocol.
**ZRP :** Zone Routing Protocol.
**SADV :** Static-node-assisted Adaptative data Dissemination in Vehicular networks.
**MIBR :** Mobile Infrastructure Based VANET Routing protocol.
**MGRP :** Mobile Gateway Routing Protocol.
**IAGR :** Infrastructure Assisted Geo-Routing.
**COIN :** Clustering for Open Inter-vehicular communication Networks.
**ADA2RS :** Approach based Defensive Alliance for Reducing RSUs Saturation.
**RREQ :** Route REQuest.
**RREP :** Route REPlay.
**RERR :** Route ERReur.

# Introduction générale

Ces dernières années ont connu un développement important dans le domaine des télécommunications sans fil [44]. Le nombre d'applications augmente de jour en jour pour améliorer notre vie quotidienne que ce soit dans nos sociétés, nos voitures, etc. L'une des applications qui a suscité beaucoup d'intérêt aux chercheurs est le système de transport intelligent, connu sous le nom de VANETs (Véhiculaire Ad hoc Networks) [17].

Un VANET est un type de réseau ad hoc mobile (MANET) qui a des caractéristiques plus spécifiques telles que la mobilité élevée, les changements de topologie, et la haute densité du réseau [41]. De plus, un VANET est composé principalement des unités mobiles (véhicules) et des unités fixes (Road Side Units "RSUs"). Ces éléments qui constituent le réseau utilisent des communications de type "vehicle to vehicle" (V2V) ou bien de type "vehicle to infrastructure" (V2I) afin d'échanger des informations et des données liées à la sécurité et au confort des usagers de la route [17].

En raison de ces caractéristiques particulières des VANETs, beaucoup de chercheurs se sont concentrés sur des axes de recherche bien spécifiques tels que l'acheminement des paquets (routage), la qualité de service (QoS), et la sécurité des données [59].

Le routage est une méthode d'acheminement des informations vers la bonne destination à travers un réseau de connexion donnée. Il consiste à assurer une stratégie qui garantit, à tous moments, un établissement de routes qui soient fiables et efficaces entre n'importe quelle paire de nœuds appartenant au réseau. Plusieurs protocoles de routage ont été développés dans la littérature pour les VANETs. Parmi ces protocoles, on cite : *Clustering for Open Inter-vehicular communication Networks* (COIN) [8] proposé par Blum et al. et *Cluster-Based Flooding* (LORA-CBF) [50] établi par Santos et al. qui se basent sur le principe du clustering pour l'acheminement des informations. En outre, Borsetti et Gozalvez ont proposé une autre protocole appelé *Infrastructure Assisted Geo-Routing for cooperative vehicular networks* [10] en exploitant les infrastructures de bord de route "RSUs" qui forment un backbone pour le routage des informations captées par les

véhicules. Malgré leurs performances, ces protocoles restent impuissant devant certaines situations liées à la densité du réseau et au nombre de véhicules qui communiquent au même temps. Généralement ce genre de situations conduit à la congestion dans le reseau et ainsi à la saturation des RSUs. Plusieurs stratégies ont été proposées pour réduire la congestion dans les VANETs comme l'ajustement des débits des émetteurs (véhicules) en fonction de l'état des récepteurs (buffers des RSUs) [55]. Cependant, ces stratégies de lutte contre la congestion sont confrontées à certains problèmes comme le retard de transmission des paquets d'urgence. C'est pour cela, il est toujours important et intéressant d'introduire d'autres techniques qui améliorent d'avantage la QoS dans les VANETs. Dans ce sens, nous proposons dans ce mémoire une nouvelle approche basée sur le concept d'alliances défensives dans les graphes afin de mettre en oeuvre une stratégie de cooperation entre les RSUs pour mieux gérer les échanges d'information dans les VANETs.

Le travail est structuré en quatre chapitres, où chaque chapitre est abordé par une petite introduction qui offre une lecture en diagonale de ce qui est à présenter dans le chapitre, et se termine par une conclusion qui est un bilan de ce qui a été présenté. Dans ce qui suit nous donnons une brève description des quatres chapitres et conclusion.

- Le chapitre un est consacré aux généralités sur les réseaux véhiculaires ad hoc (VANETs), où nous avons présenté les différents composants d'un VANET et les technologies de transmission utilisées pour sa mise en place. De plus, nous avons cité quelques caractéristique et quelques applications des VANETS.
- Le chapitre deux est dédié au routage de l'information dans les réseaux ad hoc et plus précisément dans les VANETs. Dans ce cadre, nous avons établi un état de l'art en présentant les principaux protocoles de routage dans les VANETs tout en effectuant une étude comparative entre eux.
- Dans le chapitre trois, nous présentons une nouvelle approche, nommée "ADA2RS" (Approach based Defensive Alliance for Reducing RSUs Saturation), basée sur le concept d'alliances défensives dans les graphes en vue de réduire la congestion dans VANETs.
- Le quatrième chapitre, fait l'objet d'une proposition de deux modèles analytiques qui se basent sur les chaînes de Markov, l'un pour l'approche IAGR *Infrastructure Assisted Geo-Routing for cooperative vehicular networks* [10] et l'autre pour notre approche ADAR2S. Ainsi, à l'aide de ces deux modèles, une étude comparative montre que notre proposition réduit le nombre de paquets perdus. De plus une préparation de l'environnement de simulation est présentée, en perspective d'effectuer d'autres tests.

- Le document se termine par une conclusion où des perspectives futures seront données.

Chapitre 1

# Généralités sur les réseaux véhiculaires ad hoc (VANETs)

## 1.1 Introduction

Ce chapitre a pour objectif de donner une vue d'ensembles des VANETs. Il présente dans la première section les réseaux véhiculaires mobiles de manière générale, les différents modes de communication, ses composants, ainsi une présentation des technologies de transmission. Ensuite, la deuxième section définit les caractéristique des VANETs. La troisième section présente quelques défis et contraintes des VANETs. Enfin, la quatrième section expose les différentes possibilités d'applications de ces réseaux.

## 1.2 Réseaux véhiculaires ad hoc (VANETs)

Dans cette partie, nous allons présenter des définitions des réseaux mobiles ainsi des types de communication dans les VANTETs.

**Définition 1.2.1.** [40] Un *réseau mobile ad hoc*, appelé généralement MANET (Mobile Ad hoc Network), consiste en une grande population relativement dense d'unités mobiles qui se déplacent dans un territoire quelconque et dont le seul moyen de communication est l'utilisation des interfaces sans fil, sans l'aide d'une infrastructure préexistante ou d'administration centralisée.

**Définition 1.2.2.** [41] *Un réseau véhiculaire* appelé généralement (Vehicular Ad hoc Network), est une nouvelle technologie émergente des réseaux Ad hoc mobiles (MANETs) pour 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 portées. Chaque véhicule est équipé d'une antenne radio et d'un ensemble de capteurs pour assurer les différentes types de

communications. Ainsi les VANETs sont considérés comme des systèmes de transports intelligents (Intelligent Transportation Systems - ITS).

### 1.2.1 Types de communication dans les VANETs

Dans les réseaux VANETs, nous trouvons principalement, les entités fixes *(les RSUs)* et les entités mobiles (les véhicules). Pour pouvoir échanger les différentes informations et données liées à la sécurité et au confort des usagers de la route, ces différentes entités doivent établir des communications entre elles. Pour cette raison, nous distinguons trois principaux types de communications : vehicle to vehicle (V2V), vehicle to infrastructure (V2I) et infrastructure to infrastructure (I2I) [17] (voir Figure 1.1).

#### 1.2.1.1 Communication vehicle to vehicle (V2V)

Ce type de communication fonctionne à l'aide des dispositifs installés dans les véhicules appelés *OBU (On-Board Unit)*. Il est semblable au type de communication entre les nœuds mobiles de réseau MANET. La communication entre deux véhicules se fait directement, en mode ad hoc inter-véhicules. Les véhicules n'ont pas besoin de faire appel aux infrastructures pour pouvoir communiquer entre eux. Deux véhicules peuvent communiquer directement si chaque véhicule est à portée de l'autre, sinon ils font appel à des autres véhicules, qui vont jouer le rôle d'un pont (intermédiaires) pour router l'information à plusieurs saut.

#### 1.2.1.2 Communication vehicle to infrastructure (V2I)

La communication vehicle to infrastructure (V2I) est aussi appelée une communication en mode infrastructure qui est assurée grâce aux différentes entités du réseau VANET. En effet, les *OBUs (On-Board Unit)* des véhicules communiquent avec les *RSUs (Road Side Unit)* placées aux bords des routes pour envoyer leurs informations aux autres véhicules. Ce mode de communication assure une connectivité relativement forte par apport à la communication en mode V2V (vehicle to vehicle).

#### 1.2.1.3 Communication infrastructure to infrastructure (I2I)

C'est une communication hybride pour acheminer l'information entre un véhicule qui est a portée d'une station fixe *(RSU)* dans une zone géographique quelconque et un autre véhicule qui est a portée d'une autre station fixe qui se situe dans une autre zone, en

utilisant une communication par exemple V2I2I2V (vehicle-émetteur to infrastructure-1 to infrastructure-2 to vehicle-destinataire).

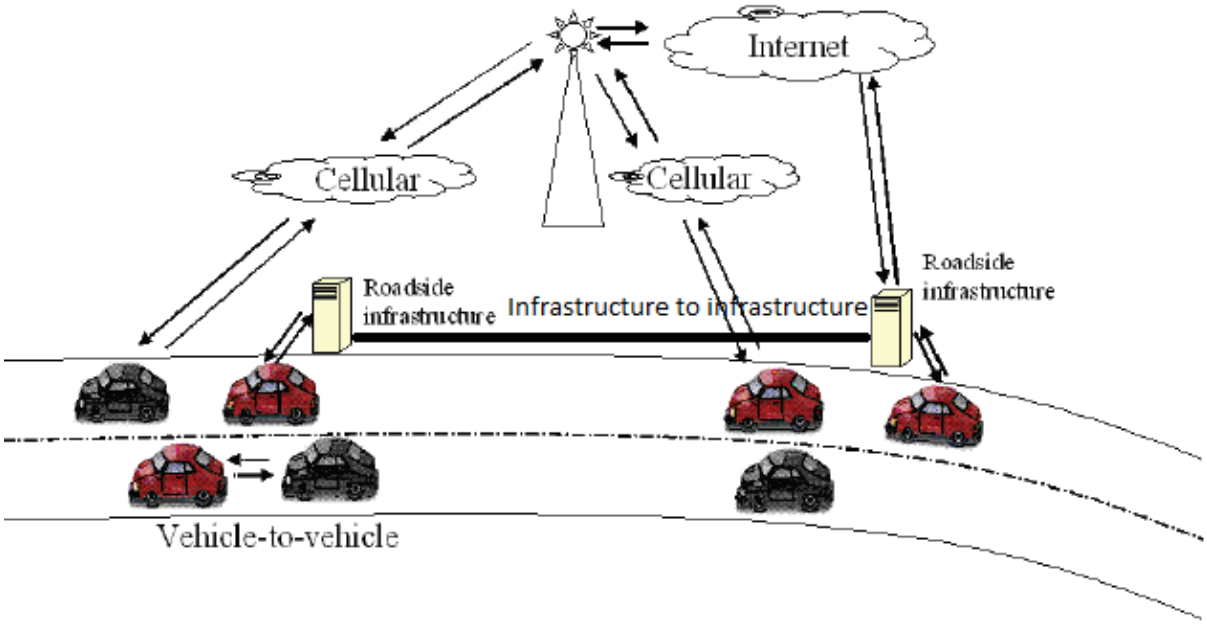



FIGURE 1.1 – Modèle d'un réseau VANET et de communications [17].

### 1.2.2 Composants des VANETs

Les services proposés dans les VANETs permettent de distinguer plusieurs types de communications entre les principaux composants qui sont : *On-Board Unit (OBU)* et *Road Side Unit (RSU)* [17].

#### 1.2.2.1 Road Side Unit (RSU)

Les infrastructures RSUs sont installées au bord des routes. Elles peuvent être principalement, des feux de signalisation, des lampadaires ou autres qui sont équipés de moyens de transmission, de reception et de traitement de données. Leur principale responsabilité est la gestion du trafic et des véhicules. Aussi, ces infrastructures représentent des points d'accès au réseau et aux différentes informations sur la circulation.

#### 1.2.2.2 On-Board Unit (OBU)

Les OBUs sont des unités embarquées dans les véhicules intelligents, elles regroupent un ensemble de composants matériels et logiciels de hautes technologies (GPS, radar, caméras, différents capteurs et autres). Leurs rôles est d'assurer la localisation, la réception, le calcul, le stockage et l'envoi des données dans le réseau. Chaque unité OBU est composée d'une interface spéciale pour la connexion à des autres *OBUs* (véhicules) et d'un périphérique réseau pour une communication sans fil avec les unités de bord de route (*RSUs).*

### 1.2.3 Technologies de communication

Dans le monde d'aujourd'hui, les technologies dédiées aux réseaux sans fil sont nombreuses. Ces technologies de communication sont utilisées pour renforcer la sécurité routières, diminuer les embouteillages, et aussi pour assurer le confort des passagers et des conducteurs. Dans ce qui suit nous exposerons quelques technologies existantes comme la $3^e$ génération (3G) et $4^e$ génération *(4G, Long Term Evolution (LTE))* fournies par les opérateurs téléphoniques mobiles, le Wi-Fi, le WiMax et le DSRC/WAVE [20].

#### 1.2.3.1 Réseaux cellulaires

Le principe de fonctionnement repose sur le faite que chaque secteur géographique est découpé en petites zones appelées cellules. Au centre de chaque cellule se trouve une station de base (ou BS : Base Station), comprenant une antenne, un contrôleur et un certain nombre d'émetteurs-récepteurs (équipements). Ensuite, chaque station de base est connectée à un centre de commutation de mobiles ou *MTSO (Mobile Telephone Switching Office)*, gérant plusieurs stations. Généralement, une station est connecté de façon filaire avec un centre de commutation. Ce centre est également connecté au réseau téléphonique public pour permettre d'atteindre les abonnées du réseau. Le réseau cellulaire mobile peut être utilisé pour connecter et transmettre les informations entre les véhicules mais le problème est que chaque élément du VANET doit se doté d'un abonnement chez un opérateur.

#### 1.2.3.2 Wifi et Wimax

Le Wifi est un ensemble de protocoles de communication sans fil régis par les normes du groupe IEEE 802.11 (ISO/CEI 8802-11). Un réseau Wi-Fi permet de relier par ondes

radio plusieurs appareils informatiques (ordinateur, routeur, smartphone, décodeur Internet, etc.) au sein d'un réseau informatique afin de permettre la transmission de données entre eux. Grâce aux normes Wi-Fi, il est possible de créer des réseaux sans fil. En pratique, le Wi-Fi permet de créer des liaisons à haut débit [20]. La portée peut atteindre plusieurs dizaines de mètres en intérieur (généralement entre une vingtaine et une cinquantaine de mètres) s'il n'y a aucun obstacle gênant (mur en béton par exemple) entre l'émetteur et le récepteur. Les technologies Wi-Fi, à travers le standard 802.11, peut être utiliser dans les VANETs. Un protocole Wi-Fi, 802.11p qui définit l'accès sans fil, nommé *(Wireless Access in Vehicular Environment (WAVE))*, a été établi spécialement pour les VANETs en fonction de leurs caractéristiques (véhicules rapides, jusqu'à 160 km/h, temps de latence faible (moins de 50 ms), etc.). En suite une nouvelle technologie nommée, *DSRC (Dedicated Short-Range Communications)* a était développer pour transmettre les informations à courte distance avec un débit théorique allant jusqu'à 6 Mbps/s. Elle est utilisé pour certaines applications liées à l'automobile comme le payement électronique des péages sans s'arrêter. Des bandes dédiées à cette technologie ont été allouées par les organismes de certification, par exemples : aux États-Unis 75 MHz ont été alloués autour des fréquences de 9 GHz, en Europe 25 MHz ont été alloués autour de cette même bande et au Japon 80 MHz ont été alloués autour de la bande 5.8 GHz [40].

De son côté, le WiMax permet une transmission point à point portant sur une zone géographique étendue, c'est pourquoi nous pourrons l'utiliser pour les communications I2I. Mais pour cela, les RSUs nécessitent un bloc de réception/transmission capable d'utiliser à la fois *DSRC* (pour les communications V2I) et le WiMax (pour les communications I2I) [20].

## 1.3 Caractéristiques des VANETs

Les réseaux véhiculaires ont des caractéristiques spécifiques qui les distinguent des autres types de réseaux mobiles (réseaux ad hoc, réseaux de capteurs).

### 1.3.1 Capacité et autonomie d'énergie

Contrairement au contexte des réseaux ad hoc ou des réseaux de capteurs où la contrainte d'énergie, à titre d'exemple, représente une des problématiques traitées dans la littérature, les éléments d'un réseau VANET n'ont pas de limite en terme d'énergie car les *OBUs* utilisent les batteries des véhicules, et les *RSUs* sont déployées sur des feux

tricolores, éclairages publiques et des panneaux qui sont déjà alimentés par une source d'énergie illimitée [2].

### 1.3.2 Changement de topologie

Les réseaux VANETs sont caractérisés par une forte mobilité, liée à la vitesse de déplacement des véhicules. Par conséquent, un véhicule peut rapidement rejoindre ou quitter le réseau en un temps très court, ce qui rend les changements de topologie très fréquents. Les déplacements des véhicules sont structurés par des routes donc il est possible de prévoir l'évolution des déplacements des véhicules grâce à leurs directions et surtout à la connaissance des cartes routières [23].

### 1.3.3 Variation des environnements

L'environnement d'un VANET peut être une route, une autoroute ou une ville (beaucoup plus complexe). De plus, une situation d'embouteillage peut mener à l'encombrement du réseau, tandis qu'une route de campagne peut conduire à la disparition des liens du réseau, surtout la nuit.

## 1.4 Défis et contraintes des VANETs

Les caractéristiques des réseaux de véhicules offrent des challenges techniques importants tel que l'accès au canal, le routage et la dissémination des données, l'auto-organisation, la sécurité, l'adressage, etc.

### 1.4.1 Sécurité

La sécurité est un défi majeur ayant un grand impact sur le futur déploiement des réseaux véhiculaires ainsi que leurs applications. Dans ce contexte, le développement des mécanismes de sécurité instituant les relations de confiance entre les entités communicantes et garantissantes le contrôle d'accès aux services de même que la sécurité des transferts de données, s'avère d'une importance capitale [48].

### 1.4.2 Accès au canal

Les réseaux de véhicules utilisent des communications radio. Par conséquent, il est important de concevoir des solutions MAC spécifiques aux réseaux de véhicules. Des protocoles qui permettent d'apporter de la qualité de service et de gérer les priorités en résolvant les problèmes d'interférences radio, des problèmes de multi-trajets des ondes, les irrégularités électromagnétiques, de l'allocation de ressources distribuées dans une topologie dynamique, etc [60].

### 1.4.3 Routage et la dissémination

Les véhicules doivent définir un protocole de routage pour pouvoir communiquer entre eux. En effet, quand les terminaux ne sont pas à une portée de transmission radio directe, le routage *unicast* est exigé pour établir la communication entre deux véhicules ou entre un véhicule et une infrastructure fixe. Chaque véhicule peut donc prendre le rôle d'un émetteur, récepteur ou routeur. La dissémination d'information quant à elle, consiste à acheminer une information d'une source vers une ou plusieurs destinations, en assurant un délai d'acheminement réduit, une grande fiabilité et une meilleure utilisation des ressources [62].

## 1.5 Domaines d'application des VANETs

Les applications VANETs sont venues répondre à des des problématiques liées à la sécurité des usagers de la route et l'amélioration des performances des réseaux routiers suite à l'augmentation du nombre de véhicules. Pour se tourner par la suite vers différents autres domaines d'applications comme : application de sécurité routière et de gestion du trafic, et application de confort.

### 1.5.1 Application de sécurité routière et de gestion du trafic

Les applications de sécurité qui visent à améliorer la sécurité des passagers sur les routes en avisant les véhicules de toute situation dangereuse. Ces applications se basent en général sur une diffusion de messages d'information permettant aux conducteurs d'avoir une connaissance de l'état de la route et des véhicules voisins [10]. A titre d'exemple, en cas d'accidents les véhicules qui se dirigent vers le lieu de l'accident sont avertis que les conditions de la circulation se trouvent modifiées et qu'il est nécessaire de redoubler

la vigilance. Les messages d'alertes et de sécurité doivent être de taille réduite pour être transmis le plus rapidement possible et doivent être émis à des périodes régulières. Les applications de gestion de trafic sont axées sur l'amélioration des conditions de circulation dans le but de réduire les embouteillages et les risques d'accidents. Elles consistent à fournir aux conducteurs des informations qui leurs permettent d'adapter leurs parcours à la situation du trafic routier. Ces applications visent à équilibrer la circulation des véhicules sur les routes pour une utilisation efficace de la capacité des routes et des carrefours et à réduire par conséquent les pertes humaines, la durée des voyages et la consommation d'énergie, etc.

### 1.5.2 Applications de confort

Les applications de confort sont développées principalement pour divertir les passagers, et aussi à des actions publicitaires et d'informations. Les applications de divertissements permettent un accès Internet par exemple. Cet accès peut être effectué à des points stratégiques, comme les stations essences, ou en remontant le réseau jusqu'à une *RSU* qui serait connecté. En plus de permettre la connexion Internet, il serait possible par exemple de télécharger du contenu, comme des jeux, de la musique ou des videos à ces points stratégiques et de pouvoir les partager ensuite sur le réseau. C'est donc l'accès à Internet, le partage et la messagerie inter-véhicule ou encore les jeux en réseau ou hors ligne, qui seraient permis sur le réseau. Les applications publicitaires sont destinées aux commerciaux présents sur les bords des routes. Ainsi, les hôtels, restaurants, stations essences et autres commerces pourraient annoncer aux véhicules, dans un certain rayon autour de leurs commerces, leurs présence à proximité. Les utilisateurs pourraient ainsi, lorsque nécessaires, consulter le type de commerce présent autour d'eux et sélectionner celui correspondant à leurs besoins. Ces applications peuvent aussi être informatives. Par exemple, nous trouvons des applications de gestion du stationnement, en ville ou dans un stationnement sous-terrain, afin d'informer le conducteur des places disponibles prêt de sa position via les données fournies par une RSU [2].

## 1.6 Conclusion

Dans ce chapitre, nous avons présenté les principaux concepts du réseau VANET ainsi leur caractéristiques et leur applications.

Dans le chapitre suivant, nous allons présenté un état de l'art des protocoles de routage dans les VANETs.

Chapitre 2

# Etat de l'art : routage et congestion dans les VANETs

## 2.1 Introduction

Dans ce chapitre, nous allons analyser le problème de routage de l'information dans les réseaux véhiculaires mobiles (VANETs) et nous allons présenter des protocoles de routage que nous retrouvions principalement dans la littérature et leurs fonctionnements ainsi que leurs points faibles.

## 2.2 Le routage dans les VANETs

### 2.2.1 Classification des protocoles de routage

Le routage de l'information consiste à acheminer des messages du nœud source vers un(des) nœud(s) destinataire(s), à travers un réseau. L'acheminement peut se faire de deux manières différentes, directement avec un seul saut (single-hop) quand la source et la destination sont connectées directement l'une avec l'autre ou par étapes avec plusieurs sauts (multi-hop), dans ce cas, la communication se fait via des nœuds intermédiaires positionnés entre la source et la destination. Lors d'une communication multi-sauts, le chemin est choisi en fonction de divers facteurs tels que sa longueur, sa bande passante ou encore sa durée de vie [40]. Plusieurs classifications ont été proposées dans la littérature pour les protocoles de routage dans les VANETs. Dans ce qui suit, nous présentons quelques classification possibles dans VANETs donnée par Venkatesh et all. [61] (voir Figure 2.1).

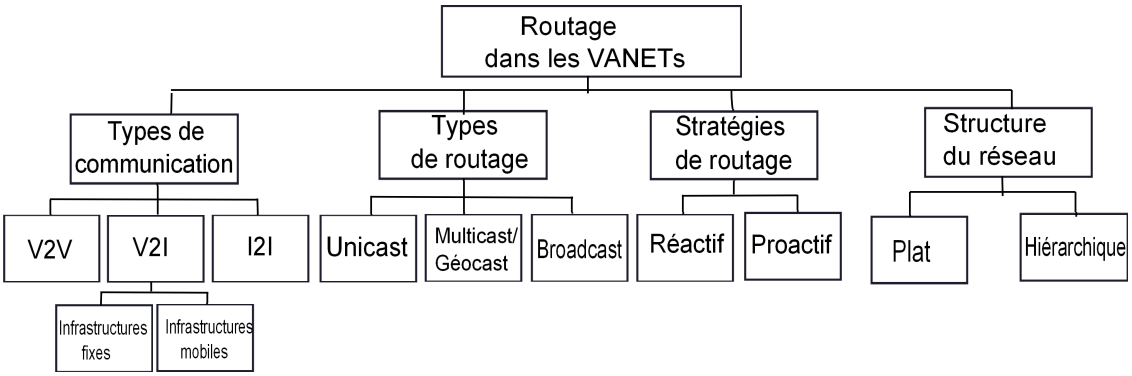



FIGURE 2.1 – Routage dans les VANETs [61].

#### 2.2.1.1 Types de routage

Haas [25] a expliqué les différents types de protocoles de routage selon le nombre et la localisation des destinataires (comme le montre la Figure 2.2).

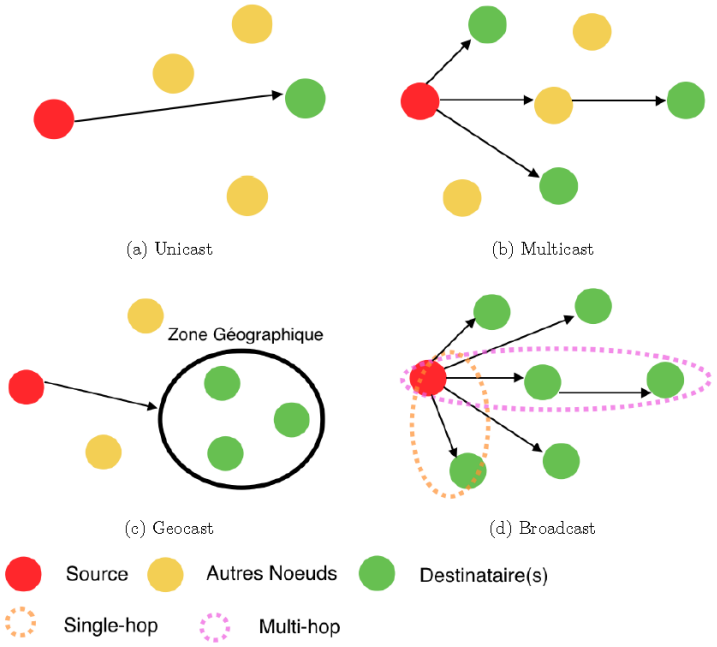



FIGURE 2.2 – Types de routage dans les réseaux [25].

1. *Routage Unicast* : l'information transite d'un nœud source vers un seul nœud destinataire, soit à un seul saut ou bien multi-sauts.

2. *Routage Multicast/Geocast* : l'information est transmise d'un nœud source vers plusieurs nœuds destinataires précis *(Multicast)*, ou à tous les destinataires présents dans une zone géographique donnée (Geocast).
3. *Routage de type Broadcast* : l'information du nœud source est envoyée à tous les nœuds présents autour de ce dernier.

#### 2.2.1.2 Stratégies de routage

Selon Sharef et al. [54], il existe deux principales stratégies qui sont utilisées par plusieurs protocoles de routage, à savoir le routage proactif et le routage réactif.

**Routage proactif**

Les nœuds maintiennent en permanence les tables de routage afin de connaître la topologie du réseau en tout temps (état des liens). Deux principaux protocoles reviennent dans la littérature d'une façon récurrente : *Dynamic destination-Sequenced Distance Vector (DSDV)* [15] et *Optimized Link State Routing Protocol (OLSR)* [29].

- *Dynamic destination-Sequenced Distance Vector (DSDV) :* Chaque nœud possède la table de routage complète (état des liens) ensuite si un nœud veut émettre, il utilise l'algorithme de Bellman afin de trouver le chemin optimal vers le nœud destinataire. La mise à jour des tables se fait en fonction du temps (de façon périodique grâce à des timers), ou en fonction d'événement (mauvais débit de connexion, délais trop élevés, liens qui disparaissent, etc.).
- *Optimized Link State Routing Protocol (OLSR) :* Ce protocole définit des nœuds nommés multi-relais, seuls ces nœuds possèdent les tables de routage complètes. Cela réduit la diffusion excessive et le gaspillage de la bande passante par rapport au protocole *DSDV*.

**Routage réactif**

Les nœuds construisent une table de routage seulement lorsqu'un nœud voisin en fait la demande ou qu'il doit démarrer une transmission, c'est ce que nous appelons le routage à la demande. Les protocoles les plus connus sont : *Ad-hoc On-Demand Distance Vector Routing (AODV)* [47] et *Dynamic Source Routing (DSR)* [31].

- *Ad-hoc On-Demand Distance Vector Routing (AODV) :* Ce protocole a été développé pour les MANETs. Lorsqu'un nœud doit commencer une transmission, le principe d'*AODV* consiste à diffuser un paquet de découverte de façon broadcast.

La destination va utiliser le chemin emprunté par le premier paquet de découverte qui l'a atteint. Il envoie alors un paquet réponse afin d'annoncer ce chemin à la source, l'envoi de données peut alors commencer. En cas de disparition d'un lien sur le chemin choisi, un paquet d'erreur est envoyé à la source.

– *Dynamic Source Routing (DSR) :* Le protocole*DSR* reprend le principe du protocole *DSDV*, mais il construit les tables de routages de façon réactive, et se base sur l'état des liens. En effet, la modification de la table se fait seulement lorsque l'état des liens varie. De plus, il copie les IDs des nœuds traversés dans l'en-tête du message pour permettre au message de retrouver son chemin vers la source. Le protocole *DSR* peut ainsi choisir des routes alternatives s'il les considère comme meilleures et possède ainsi une réactivité plus rapide que celle d'*AODV* en cas de perte de liaison avec un nœud.

Nous pouvons noter que des techniques de type hybride existent (réactif et proactif), par exemple, le protocole *ZRP* (*Zone Routing Protocol*) [25] qui crée des groupes de nœuds (cluster). Ainsi le routage se fait de façon réactive au sein d'un groupe (même cluster), et il se fait de façon proactive entre les différents groupes (entre les chefs des clusters). Comme les VANETs ont une topologie dynamique donc c'est difficile de maintenir la topologie, c'est pour cela que le routage réactif est le plus adapté et le plus utilisé.

#### 2.2.1.3 Structure de réseau

**Routage à plat**

Dans un réseau utilisant un routage à plat tous les nœuds ont les mêmes tâches et les mêmes responsabilités. Ils sont donc dans le même niveau d'importance. Ce type d'architecture ne convient pas pour les réseaux de grande taille en raison du traitement naif des paquets de contrôle. Ce comportement engendre un flux de contrôle important et non optimisé. Ce pendant, le routage à plat pourra être utile lorsque la topologie est très dynamique [44].

**Routage hiérarchique**

En contrepartie au routage à plat, le routage hiérarchique attribue la fonction de de relier les paquets à certains nœuds élus d'une façon organisée. Ainsi, le réseau est organisé d'une manière hiérarchique sous forme de clusters. Chaque cluster regroupe plusieurs nœuds qui sont représentés par un cluster Head qu'ils ont déjà élu. Le rôle des clusters

Head est de router les paquets depuis/vers les nœuds de leurs clusters. Tandis que, les autres nœuds se contentent de relier leurs paquets vers le cluster Head associé [44].

### 2.2.2 Description de quelques protocoles représentatif

Dans cette partie, nous présentons quelques protocoles de routages dans les VANETs.

#### 2.2.2.1 Fonctionnement du protocole AODV

Le protocole *Ad-hoc On-Demand Distance Vector Routing (AODV)* [47] utilise trois types de messages afin de construire et de contrôler l'état des liens lors d'une communication : RREQ (route request), RREP (route replay) et RERR (route erreur). Le message de type requête (RREQ) est diffusé par le nœud source afin de découvrir le réseau. Le message de réponse (RREP) est initié par le nœud destinataire ou par un nœud qui a reçu RREQ et il connaît le chemin jusqu'à la destination afin de rapporter à la source les informations à propos du chemin choisi. Ce concept est illustré dans la Figure 2.3.

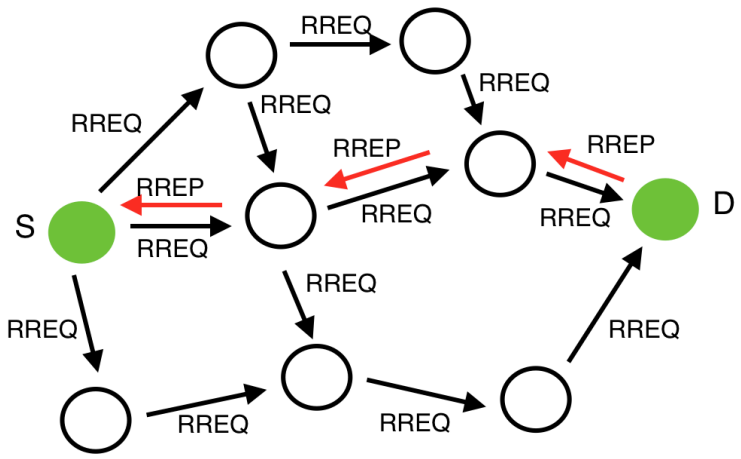



FIGURE 2.3 – Fonctionnement de*AODV*[44]

Un paquet, qu'il soit de données ou de contrôle (par exemple les messages RREP et RREQ utilisés pour établir la route), possède un numéro d'identification unique. Ce numéro est dépendant du temps : le paquet avec le numéro le plus élevé est le paquet le plus récent. Nous appelons cela le numéro de séquence. Ce procédé est très utile pour le routage de l'information. Par exemple, si le nœud source reçoit plusieurs réponses, il choisira celle qui possède la route la plus à jour (c'est-à-dire celle qui a le numéro de

séquence le plus élevé). De plus, dans le cas de réseaux VANETs où la mobilité est élevée et l'état des liens est souvent modifié, ce procédé est très utile. Le protocole *AODV* utilise le principe des numéros de séquences afin de contrôler si les liens utilisés pour atteindre la destination sont mis à jour. Chaque nœud possède un numéro de séquence qu'il incrémente à chaque fois qu'il reçoit des informations utiles de la part des messages RREQ, RREP ou RRER. Cela permet à chaque nœud du réseau de valider si la route qu'il connait vers la destination est bien la bonne. Lors de la réception d'un message RREQ ou RREP, les nœuds exécutent une série de vérification afin de mettre à jour leurs tables de routage. Ces décisions sont prises en fonction du numéro de séquence ainsi que du nombre de sauts entre le nœud et la destination. La Figure 2.4 illustre les décisions prises par un nœud lorsque un lien est coupé [47].

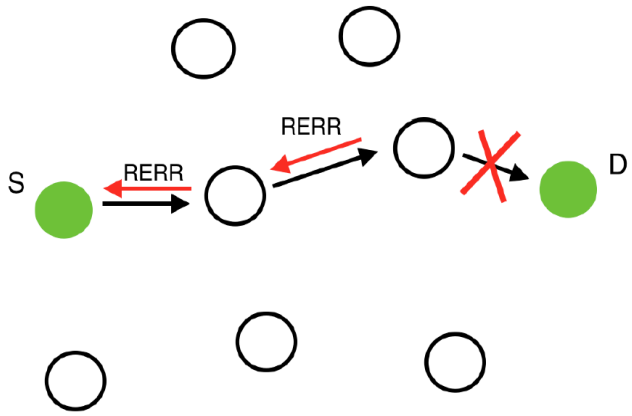



FIGURE 2.4 – Principe de détection d'un lien défaillant [44]

#### 2.2.2.2 Adaptation du protocole AODV pour les VANETs

Les chercheurs ont tenté d'améliorer les performances des protocoles présentés précédemment afin de mieux les adaptés aux réseaux véhiculaires mobiles qui présentent des spécificités qui leurs sont propres. Ainsi, des protocoles tels que Predicted *AODV (PR-AODV)* et *PR-AODVM* (M pour maximiser le nombre de nœuds) [42] ont été créés. Ces protocoles sont des modifications du protocole *AODV* pour les VANETs. Ils utilisent les informations de localisation ainsi que la vitesse des différents véhicules afin d'évaluer la durée de vie du lien. Cela permet ainsi au réseau de créer une nouvelle route avant la fin de la vie du lien, contrairement au protocole *AODV* qui attendra que la liaison soit coupée avant de chercher une nouvelle route. Le protocole *PR-AODVM* consiste à

choisir la route avec la plus grande durée de vie, contrairement au *PR-AODV* qui choisit de façon plus classique la route la plus courte ou la plus rapide.

#### 2.2.2.3 Solutions pour le routage dans les VANETs

Comme les protocoles déjà utilisés dans les MANETs, que nous avons expliquer dans la section précédente, n'ont pas été retenu pour les VANETs. Les protocoles des MANETs ne sont pas adaptés aux VANETs parce qu'un réseau véhiculaire est très dynamique donc la prédiction des routes n'est pas toujours facile à calculer et peut être faussée. Ces protocoles ne sont pas en mesure de découvrir, de conserver et d'actualiser les routes assez rapidement. C'est pour cela que les chercheurs ont développé de nouveaux protocoles dédiés aux VANETs. Ces derniers sont basés sur deux types de communication, véhicule to véhicule (V2V) ( purement ad hoc) et véhicule to infrastructure (V2I).

**Routage basé sur les véhicules (ad hoc)**

Ce sont des protocoles purement ad hoc qui fonctionnent sans l'aide des infrastructures fixes. La majorité de ses protocole se base sur le principe de groupes (clusters), aussi appelé *Cluster-based Routing* qui est une technique efficace sur les autoroutes [34]. Cette technique consiste à créer des sous-réseaux virtuels tel que le montre la Figure 2.5. Chaque groupe élit à sa tête un nœud leader (cluster head), qui va s'occuper de gérer la coordination et le management des communications inter et intra-groupes.

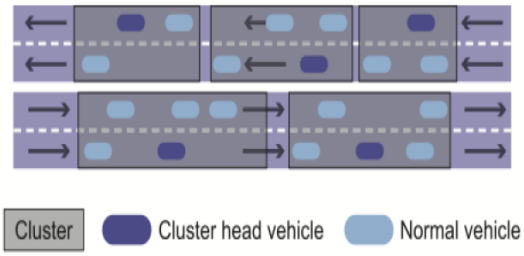



FIGURE 2.5 – Regroupement dans les VANETs [34].

Les deux principaux protocoles basés sur les groupes dans les VANETs sont *Clustering for Open Inter-vehicular communication Networks (COIN)* [8] ainsi que le protocole *Location Routing Algorithm with Cluster-Based Flooding (LORA-CBF)* [50]. Le protocole

*COIN* élit la tête du groupe en fonction des données de déplacement du véhicule et prend en compte la distance entre les véhicules. Le deuxième, *LORA-CBF* définit, en plus des têtes de groupes, des nœuds ponts qui sont chargés de faire la liaison entre les différents groupes, tandis que le nœud tête ne gère que la distribution du message dans le groupe. Les protocoles basés sur le regroupement sont souvent de bonne qualité, à une condition que le réseau ne soit pas trop dynamique et trop surchargé, c'est-à-dire sur autoroute où les véhicules qui roulent dans le même sense peuvent maintenir la topologie pour une durée. En effet, en ville, il est difficile de maintenir les différents groupes car la topologie change surtout dans les intersections et aussi les protocoles d'accueil d'un nouveau membre dans un cluster sont gourmands en coût de gestion du réseau (overhead) qui veut dire qu'un véhicule change de direction va obligatoirement changer de cluster.

Ensuite, Durresi et al. [21] ont développé un protocole nommé *BROADCOMM* qui donne la priorité à la diffusion des messages d'urgences. Ce protocole est conçu pour les communications inter-véhicules de capteurs et basé sur le routage géographique *(geo-cast)*. Les capteurs installés dans les voitures recueillent continuellement des informations importantes qui doivent être diffusé immédiatement dans un rayon donné (calculé en fonction de la distance entre le point d'un accédant par exemple et les véhicules qui doivent connaître l'information). Le protocole *BROADCOMM* crée des clusters temporaires et les messages sont disséminés en utilisant l'inondation qu'entre les têtes de groupes qui se chargent de la retransmission de l'information au sein de leurs groupes respectifs.

### Routage basé sur les infrastructures

#### Infrastructures fixes

Le principe de *Static-node-assisted Adaptative data Dissemination in Vehicular networks (SADV)* [19] est que les véhicules acheminent l'information à une *RSU* la plus proche qui garde le message en mémoire jusqu'à ce qu'elle détecte un chemin vers la destination. Le protocole *SADV* suppose la présence de *GPS* dans les véhicules, aussi chaque véhicule diffuse périodiquement des messages de position et chaque *RSU* est équipée d'une carte numérique contenant des informations sur la route et les véhicules à sa portée.

La Figure 2.6 illustre ce mécanisme de transfert de paquet. Lorsque "A" veut envoyer un message à la destination qui se trouve au nord, il achemine le paquet vers le véhicule B. Ensuite, comme B ne trouve pas de véhicule à sa porté à l'instant $t_0$ (cas de la Figure 2.6 (a)), donc il livre le paquet à l'*RSU* qui le couvre. Cette infrastructure va sauvegarder les paquets dans son buffer jusqu'à ce qu'elle trouve un véhicule qui se déplace vers la destination. A l'instant $t_1$, l'infrastructure *RSU* détecte un véhicule $C$ qui se déplace vers

la destination donc elle lui transmet le paquet (cas de la Figure 2.6 (b)). Donc les RSUs ne servent que d'unités de stockage de données pendant un certain temps.

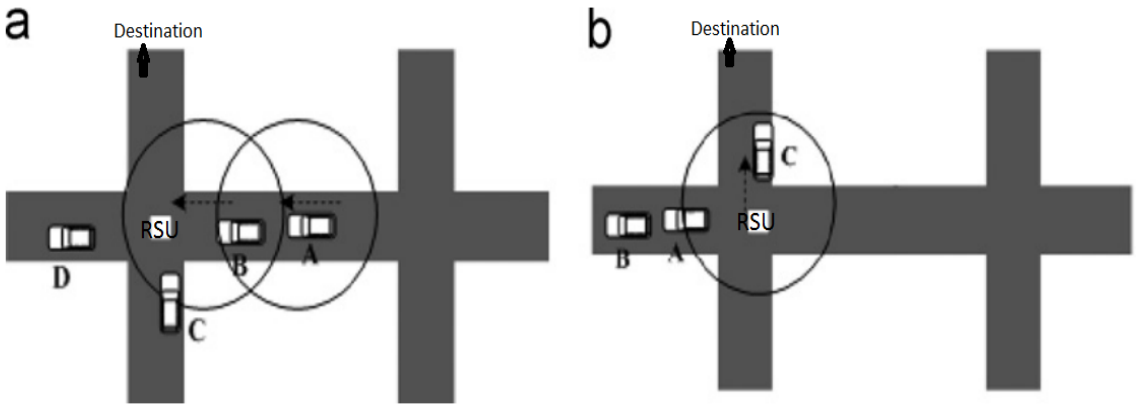



FIGURE 2.6 – Routage à l'aide d'une *RSU* [19].

Le problème du protocole *SADV* est si tout les véhicules choisissent la même *RSU* pour lui acheminer leurs informations au même temps, cela peut engendrer une congestion et le débordement du buffer de la *RSU*.

Le protocole *Infrastructure Assisted Geo-Routing for cooperative vehicular networks (IAGR)* [10] est conçu pour tirer parti de l'infrastructure fixe, où les *RSUs* sont déployées pour rendre la communication des véhicules plus fiables et réduire les retards indésirables survenus lors de la transmission des données, en particulier dans les applications de sécurité. Ces *RSUs* sont reliées entre elles par une bande passante importante et forment un réseau dorsal fiable où toutes les unités *RSUs* peuvent être intégrées dans une unité appelée passerelle backbone en raison du fait qu'elles sont connectées au réseau principale. Chaque véhicule connait les *RSUs* qui sont à sa porté car l'algorithme suppose la présence de cartes numériques et de serveurs de localisation des véhicules donc à chaque fois qu'un véhicule entre dans une zone de couverture d'une *RSU*, tout les deux mettent à jour leurs tables local de routage.

Le routage se fait comme suit :

1. Un véhicule envoie le paquet à l'infrastructure *RSU* la plus proche de lui.
2. A la réception du paquet par cette *RSU*, elle calcule le chemin le plus proche vers la destination, ensuite elle émit le paquet.

La Figure 2.7 montre l'avantage de l'infrastructure fixe où les *RSUs* sont combinées en un seul nœud et le véhicule source envoie un paquet de données.

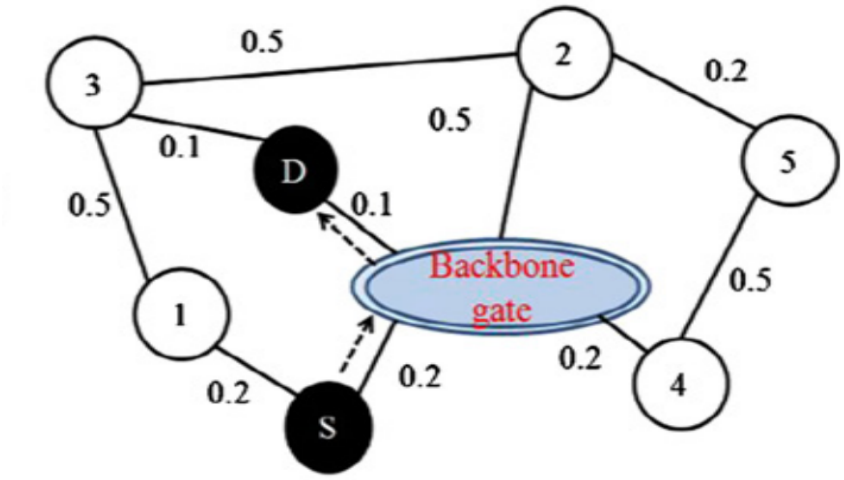



FIGURE 2.7 – Routage à base des *RSUs* [10].

Cependant, ce protocole ne prend pas en compte la densité du réseau.

**Infrastructures mobiles**

Le protocole *Mobile Infrastructure Based VANET Routing protocol (MIBR)* [30] est conçu pour surmonter la restriction des coûts de déploiement des *RSUs*. Des protocoles, comme *Infrastructure Assisted Geo-Routing* [10], utilisent les *RSUs* comme moyen pour acheminer les paquets entre n'importe qu'elle source à n'importe qu'elle destination. Le protocole *MIBR* exploite le concept de passerelle mobile où les *RSUs* sont remplacées par des bus qui formeraient entre eux un réseau backbone, la partie du réseau supportant la grande majorité du trafic grâce à ces performances de transmissions. Dans ce modèle, les bus sont équipés de récepteurs/transmetteurs *WiMax* qui permettent des débits et des rayons de transmissions plus élevés. Cependant, l'efficacité du *WiMax* en cas de grande mobilité est réduite. Les bus étant limités à une vitesse ne dépassant souvent pas 90 km/h, le modèle est considéré comme réaliste. Le protocole sélectionne alors la route avec le minimum de sauts et passant par les nœuds, bus, les plus proches de la destination.

La Figure 2.8 montre le mécanisme de sélection de l'itinéraire dans lequel le véhicule source S envoie des paquets au véhicule D. Les bus et les voitures, travaillent ensemble

pour effectuer le processus d'acheminement. Souvent, les bus ont des priorités plus élevées lors de la phase de transfert du *MIBR* par conséquent la stratégie de transfert est appelée *Bus First*. En première stratégie d'autobus, le véhicule d'expédition tente d'abord de sélectionner le bus en tant que prochain transitaire et s'il n'y a pas de bus disponible dans la table voisine du véhicule expéditeur, il sélectionne la voiture à sa portée.

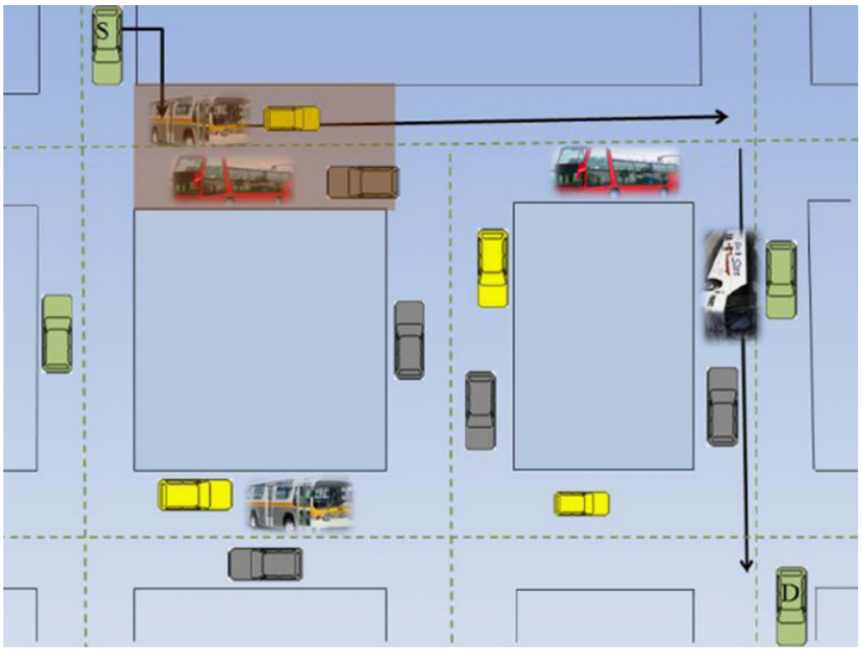



FIGURE 2.8 – Routage basé sur les infrastructures mobiles [30].

Le résultat de la simulation montre une amélioration significative de la performance en termes de taux de livraison de paquets et de débit de transmission. Cependant, aucune infrastructure fixe n'est simulée.

*Mobile Gateway Routing Protocol (MGRP)* [46] va encore plus loin en intégrant au réseau backbone formé par les bus, les taxis, les véhicules de sécurités, les véhicules professionnels, etc. que nous appelons les passerelles mobiles. Dans ce modèle, la communication se fait à l'aide des technologies Wifi pour les communications V2V et V2I (entre véhicule et passerelle mobile par exemple bus), et grâce à la 3G pour le réseau backbone (entre les passerelles mobiles). De plus, un contrôleur (base station) est connecté aux antennes du réseau 3G afin d'optimiser les communications en donnant les positions des véhicules pour trouver le meilleur chemin vers la destination.

#### 2.2.2.4 Analyse des protocoles

Les VANETs ont des spécificités qui leurs sont propres. Les protocoles de routages de l'information, créés afin d'optimiser les délais ainsi que le taux de livraison des paquets dans ce type de réseaux, ne prennent pas malheureusement en compte souvent la totalité de ces caractéristiques. Donc les protocoles que nous avons étudié dans la section précédente ont des limitations, par exemple :

- Lors de la définition d'un réseau véhiculaire mobile, nous utilisons des infrastructures de communication fixes placées en bord de route, spécifiques aux communications pour les VANETs [10]. Or, Luo et al. [30] et Pan et al. [46], dans leurs protocoles de routage *MIBR* et *MGRP* respectivement, utilisent des infrastructures différentes qui sont mobiles. Luo et al. [30] considèrent les bus comme infrastructures de communication pour les VANETs et Pan et al. [46] ont ajouté les taxis et les véhicules d'urgences comme des infrastructures mobiles qui soutiennent les bus pour le routage de l'inforamtion. Ce type de solution pourrait être un support supplémentaire aux infrastructures fixes, mais ne devrait pas être considéré comme un remplacement.
- Pan et al. [46] utilisent les bus et les taxis comme véhicules intermédiaires pour atteindre des infrastructures du réseau cellulaire mobile qui n'est pas spécifique aux VANETs et nécessite un coût de déploiement supplémentaire, obligeant ces véhicules (bus et taxis) à se munir d'un abonnement adéquat auprès d'un opérateur de réseau cellulaire mobile (3G ou 4G).
- Le nombre de véhicules simulés n'est pas très important, par exemple Borsetti and Gozalvez [9] ont simulé 12 véhicules et 3 *RSUs*, mais dans la réalité le nombre de véhicules est très important.
- Le nombre de communications simultanées ne sont pas pris en considération par les chercheurs. Les protocoles existants sont utilisés pour une communication initiée par une seule source (un seul véhicule emit à la fois). Par exemple si le protocole *Infrastructure Assisted Geo-Routing* [10] est utilisé pour le routage de l'information dans une ville où le nombre de véhicules est très important et nous supposons que plusieurs véhicules sélectionnent simultanément la même *RSU* qui est à leurs portés pour router l'information, alors la *RSU* peut être saturer parce que la quantité de données reçu dépasse sa capacité de traitement et de retransmission. Aussi c'est le même cas pour le protocole *MIBR* [30] qui utilise les bus comme infrastructures mobiles.
- Le choix de la *RSU* pour router une information est négligé par les protocoles que nous avons déjà présenté, si à l'instant $t$, un véhicule qui veut envoyer un message

peut communiquer avec plusieurs *RSUs* (à porté de plusieurs *RSUs*) alors le choix de la *RSU* est très important par exemple il faut router vers celle qui n'est pas trop sollicité à cet instant $t$.

Afin de mieux analyser les protocoles de routage dans les VANETs, nous présentons un tableau 2.1 récapitulatif des protocoles cités ci-dessus.

| Protocole | Infrastructure | Topologie | Chemin | Métrique |
|---|---|---|---|---|
| PR-AODV | non | plat | à la source | plus court chemin |
| PR-AODVM | non | plat | à la source | plus court chemin + prédiction des chemins |
| COIN | non | hiérarchique | saut par saut | plus court chemin + clustering |
| LORA-CBF | non | hiérarchique | saut par saut | plus court chemin |
| SADV | fixe | hiérarchique | saut par saut | plus court chemin + position |
| IAGR | fixe | hiérarchique | saut par saut | plus court chemin + plus proche RSU |
| MIBR | mobile | hiérarchique | saut par saut | plus court chemin + plus proche infrastructure (bus) |
| MGRP | mobile | hiérarchique | saut par saut | plus court chemin + plus proche infrastructure (bus, taxis) |

TABLE 2.1 – Tableau récapitulatif des protocoles de routage pour les VANETs

## 2.3 Congestion et saturation des *RSUs* dans les VANETs

Les problèmes de congestion sont fréquents à différentes échelles, il n'est pas rare qu'un réseau soit ralenti quelques secondes, voir quelques minutes suite à un gros pic

dans le trafic de données. Heureusement, il existe plusieurs solutions pour prévenir la congestion et la mettre hors état de nuire. Voici quelques méthodes qui permettent de gérer une congestion réseau.

### 2.3.1 Ajustement du débit

Les chercheurs Cen et al. [14, 65] ont proposé une solution basée sur réduction du taux (débit) d'envoie des nœuds sources, les véhicules dans notre cas. Ces chercheurs ont utilisé la technique suivante : les nœuds destinataires envoient des messages périodiques qui comportent une estimation du taux de perte des paquets aux nœuds sources afin d'ajuster leur débit (taux) d'emission par rapport aux estimations reçues. Mais l'utilisation de cette technique dans les VANETs engendre un retard des messages d'urgences.

### 2.3.2 Le buffer (mémoire tampon)

**Définition 2.3.1.** *Le buffer* aussi appelé *mémoire tampon* est la mémoire utilisée pour le stockage temporaire de données lors du transfert d'informations afin de compenser la différence de débit ou la vitesse de traitement entre les divers éléments du réseau à savoir les véhicules, les bus, les *RSUs*, etc.

Le stockage dans le buffer est la méthode la plus utilisée puisque chaque équipement de transmission (véhicules et *RSUs*) possède son propre buffer. L'équipement va accumuler la surcharge de trafic dans son buffer. Les buffers sont idéals pour absorber un pic de trafic passager, mais si la surcharge dure trop longtemps, le buffer sera à son tour surchargé (débordé) et les données seront alors perdues. Et aussi nous peuvons considérer le buffer comme une file d'attente de capacité limité donc il faut définir une méthode pour que le buffer écrase le surplus de données. La méthode la plus connue est le buffer circulaire qui fonctionne en *FIFO* (*First In First Out*). Lorsque le buffer est plein et que de nouveaux éléments arrivent, les nouvelles données sont supprimées. Les chercheurs Setton et al. [51] ont remarqué qu'il y a une importante perte de paquets donc ils ont essayé de developer une nouvelle méthode basée sur l'approche du contenu prioritaire où chaque paquet a un niveau de priorité lorsqu'un nœud routeur reçoit des paquets, il compare à chaque fois le niveau de priorité de chaqu'un des paquets puis il traite et achemine le paquet le plus prioritaire en premier. Mais cela engendre un problème lorsque plusieurs paquets reçus par le même routeur ont le même niveau de priorité. Ensuite les chercheurs Nzouonta et al. [43] ont proposé une amélioration par apport à la discipline de la file d'attente de chaque nœud. Les disciplines *FIFO* et LIFO (*Last In First Out*) avec *DropTail* (suppression à la

fin de la file) et *FrontDrop* (suppression à la fin de la file) sont basculés dynamiquement en fonction de la charge du trafic et le taux d'occupation du buffer. Par defaut la discipline *FIFO* est la plus utilisée, mais si une congestion a été détectée alors la discipline devient *LIFO* avec *FontDrop*. Le principe est que les paquets stockés sont ignorés et les nouveaux paquets sont traités directement. Si la congestion est sévère alors les paquets ignorés seront supprimés.

## 2.4 Conclusion

Dans ce chapitre, nous avons presenté les protocoles de routage, utilisés dans les réseaux ad hoc, existants dans la literature, leurs classifications et leurs adaptations pour les reseaux VANETs. Ensuite, nous avons étudié et analyser les nouveaux protocoles développés pour les VANETs selon les deux types de communications : sans infrastructure (purement ad hoc) et avec infrastructure. Enfin, nous avons parlé du problème de la congestion et la saturation dans les VANETs. Dans notre étude nous intéressons à ce problème de saturation et la perte de paquets de données au niveau des infrastructures *RSUs* que nous allons détaillé dans le chapitre suivant.

Chapitre 3

# Un schéma de déploiement des RSUs sous forme d'alliance défensive pour les VANETs

## 3.1 Introduction

Dans notre étude, nous considérons que les RSUs qui sont connectés entre elles via une technologie de transmission radio, peuvent être soit : des feux tricolors, des panneaux de signalisations, éclairages publiques, etc., équipés des moyens de receptions, de traitements et de transmissions de données, donc nous les considérons comme des routeurs. Dans ce chapitre, nous proposons une solution pour la congestion et la saturation des RSUs en se basant sur le concept d'alliances dans les graphes. Le chapitre est organisé comme suit : d'abord nous donnons quelques généralités sur les alliances. Ensuite, nous modélisons un VANET par un graphe. Enfin, nous proposons un algorithme nommé "ADA2RS" (Approach based Defensive Alliance for Reducing RSUs Saturation) pour équilibrer et stabiliser la charge des RSUs dans un VANET en utilisant un nouveau concept d'alliances défensives de traitement de données.

## 3.2 Généralités sur les alliances

Dans cette section, nous allons définir les alliances dans les graphes et leurs classifications dans la littérature.

### 3.2.1 Alliances

Le mot *alliance* signifie un lien ou une connexion entre des individus, des familles, des états, ou des parties [45]. Les alliances dans les graphes ont été présentées et étudiées pour la première fois par Kristiansen et al. [33]. Ils ont défini trois types d'alliances qui ont été extensivement étudiées ces deux dérnières décennies. Ces types d'alliances sont appelés *alliances défensives* [28, 27], *alliances offensives* [49, 22] et *alliances puissantes ou duales* [12, 11]. Une généralisation de ces alliances appelée $k$-alliances (ou $r$-alliances), introduite par Shafique et Dutton [52, 53], a reçu une attention particulière ces dernières années. Pour plus de détails sur les propriétés et les applications des $k$-alliances en pratique, les lecteurs peuvent consulter [64, 45].

Dans cette partie, nous présentons des définitions correspondantes aux $k$-alliance défensive, $k$-alliance offensive et $k$-alliance puissante respectivement tout en donnant des exemples d'illustration.

**Définition 3.2.1.** Soit un graphe $G = (V, E)$,

- un ensemble $A \subseteq V$ est une *$k$-alliance défensive* dans $G$, avec $k \in \{-\Delta, ..., \Delta\}$, si

$$|N_A(v)| \geq |N_{\bar{A}}(v)| + k, \ \forall \ v \in A;$$

- un ensemble $A \subset V$ est une *$k$-alliance offensive* dans $G$, avec $k \in \{2 - \Delta, ..., \Delta\}$, si

$$|N_A(v)| \geq |N_{\bar{A}}(v)| + k, \ \forall \ v \in \partial A;$$

- un ensemble $A \subset V$ est une *$k$-alliance puissante* (powerful) dans $G$, avec $k \in \{-\Delta, ..., \Delta - 2\}$, s'il est au même temps une $k$-alliance défensive et une $(k+2)$-alliance offensive ;

où :

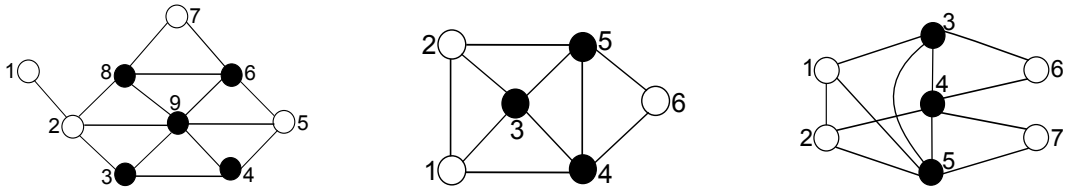
✓ $\Delta$ : représente le degré maximum dans un graphe.
✓ $N_A(v)$ : représente le voisinage ouvert du sommet $v$ dans l'ensemble $A$.
✓ $\partial A$ : représente la frontière de l'ensemble $A$.
✓ $\bar{A} = V - A$ : représente le complémentaire de $A$ dans $V$.

**Remarque 3.2.1.**

- Une alliance $A$ d'un certain type est dite *critique* ou *minimale*, si aucun sous-ensemble de $A$ n'est une alliance du même type.
- Une alliance $A$ d'un certain type est dite *globale*, si $A$ forme un ensemble dominant dans le graphe $G$ ; *i.e.* chaque sommet du graphe $G$ est soit dans $S$ ou adjacent à un sommet dans $S$.

- Slimani et Kheddouci [56] ont étudié les propriétés mathématiques des $k$-alliances défensives, offensives et puissantes (globales) dans le cas où chaque membre (à l'intérieur et / ou à l'extérieur de l'alliance) a autant de défenseurs que les attaquants, ce qui correspond à une situation critique et sensible. En introduisant et en utilisant un nouveau concept de sommets saturés, ils ont présenté des résultats théoriques consistant principalement en bornes atteintes pour la cardinalité de chaque $(-1)$-alliance puissante globale minimale limite (MGBPA) en termes uniquement de l'ordre et de la taille du graphe.

**Exemple 3.2.1.** Dans cet exemple, nous donnons quelques exemples de $k$-alliances présentés comme suit :




(a) 0-alliance défensive. (b) 1-alliance offensive globale. (c) $(-1)$-alliance puissante globale [45].

FIGURE 3.1 – Exemple de $k$-alliances.

Dans la figure ci-dessus, les sommets noirs forment une alliance dans chaque graphe.

- Dans la Figure 3.1 $(a)$, l'ensemble $A = \{3, 4, 6, 8, 9\}$ représente une 0-alliance défensive, qui est non globale car le sommet 1 n'est pas dominé.
- Dans la Figure 3.1 $(b)$, l'ensemble $A = \{3, 4, 5\}$ représente une 1-alliance offensive globale.
- Dans la Figure 3.1 $(c)$, l'ensemble $A = \{3, 4, 5\}$ représente une $(-1)$-alliance puissante globale.

## 3.3 Modélisation d'un VANET par une alliance défensive (globale et/ou saturée)

Dans les VANETs, les infrastructures RSUs peuvent être déployées d'une manière à couvrir partiellement les zones de la route ou bien d'une manière à couvrir totalement les zones de la route.

### 3.3.1 Dispositions réelles de VANETs

Nous étudions deux dispositions réelles de VANETs : la première concerne le cas où les RSUs sont déployées de manière à couvrir partiellement les zones de la route comme le montre la Figure 3.2, et la deuxième est consacrée au cas où les RSUs sont déployées de manière à couvrir totalement les zones de la route comme le montre la Figure 3.3. Pour chaque cas, nous avons spécifié dans la figure correspondante la zone de couverture de chaque RSU par un cercle. Un véhicule peut communiquer avec une RSU s'il est à la portée de cette dernière (une communication V2I). Par ailleurs, un véhicule peut être à la portée de deux ou plusieurs RSUs s'il est situé dans l'intersection de leurs zones de couverture, et donc le véhicule a la possibilité/choix de communiquer avec l'une des RSUs. De plus, un véhicule quelconque peut communiquer avec n'importe quel autre véhicule qui est à sa portée (une communication V2V). D'autre part, les RSUs sont reliés par une technologie de communication sans fil de sorte que chaque RSU peut communiquer avec toutes les autres RSUs soit à un saut ou à plusieurs sauts (une communication I2I).

#### 3.3.1.1 Cas 1 : quand les RSUs sont déployées de manière à couvrir partiellement les zones de la route

Nous rencontrons ce cas lorsque les RSUs ne sont pas suffisamment déployées en nombre ou en puissance. Dans cette situation, les infrastructures RSUs déployées ne couvrent pas toutes les zones de la route comme les zones A et B de la Figure 3.2. Ainsi, les véhicules qui se positionnent dans ces zones ne peuvent utiliser que les communications V2V pour router leurs informations.

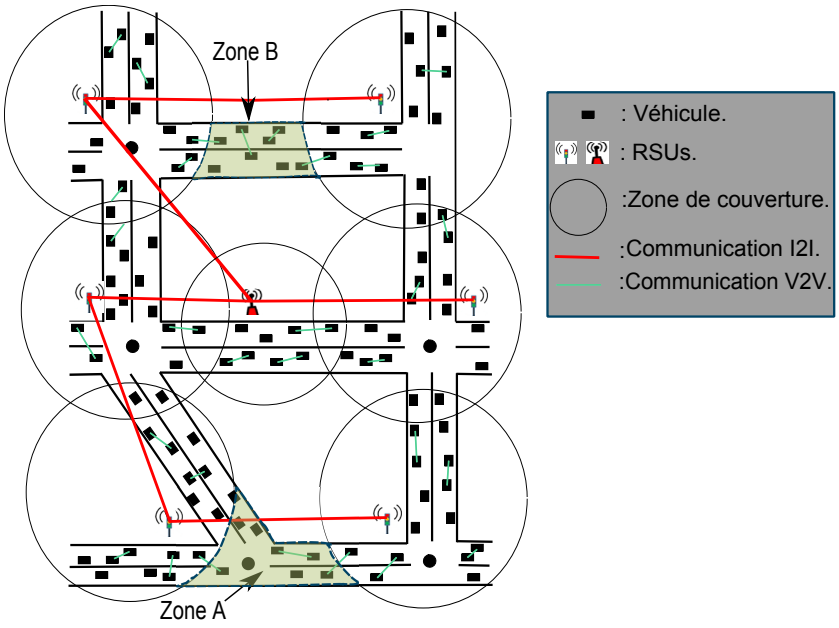



FIGURE 3.2 – Disposition réelle d'un VANET ayant des RSUs qui couvrent partiellement les zones de la route

#### 3.3.1.2 Cas 2 : quand les RSUs sont déployées de manière à couvrir totalement les zones de la route

Dans ce cas, les infrastructures RSUs sont déployées de manière à couvrir toutes les zones de la route. Ainsi, chaque véhicule est à porté au moins d'une (ou plusieurs) RSU(s) pour router ses informations (paquets de données).

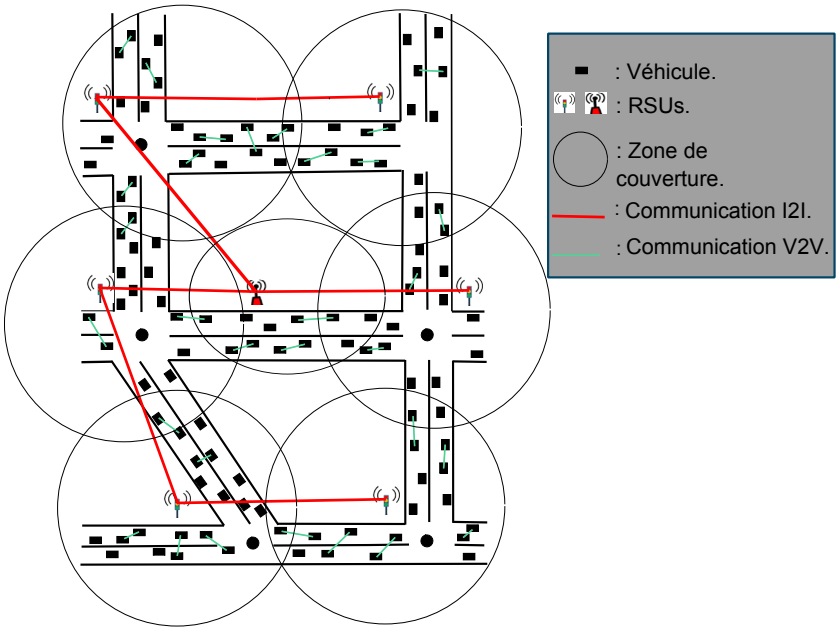



FIGURE 3.3 – Disposition réelle d'un VANET ayant des RSUs qui couvrent totalement les zones de la route.

### 3.3.2 Modélisation d'un VANET par un graphe

Un VANET peut être modéliser par un graphe $G = (V, E)$ où $V$ est l'ensemble des nœuds représentants les véhicules roulants sur la route du VANET et les RSUs déployées au long de cette route, et $E$ est l'ensemble des arrêtes reliant V2V, V2I ou I2I qui représentent les déférents types de communications possibles entre les nœuds. Plus spécifiquement, il existe une arête entre deux nœuds représentants deux véhicules (ou un véhicule et une RSU) si ces derniers sont à porté. De plus, les arêtes reliant chaque couple de RSUs sont obtenues à partir des liaisons pré-définies I2I comme indiquées sur les Figures 3.2 et 3.3. L'ensemble $A \subset V$ constitué des nœuds représentants les RSUs forme une infrastructure multiple et fixe qui gère les échanges d'informations du VANET.

**Cas 1 :** La Figure 3.4 représente le graphe qui modélise le cas où les infrastructures RSUs sont déployées de manière à couvrir partiellement les zones de la route du VANET. Notons que dans ce cas, l'ensemble $A$ des nœuds RSUs n'est pas un ensemble dominant car il y a des nœuds véhicules (appartenant aux zones A et B) qui ne sont adjacents à aucun noeud RSU, ceci est due au fait que les véhicules correspondants ne sont à porté d'aucune RSU.

$$\exists\, j \in (V - A), \forall\, i \in A : (v, i) \notin E. \tag{3.1}$$

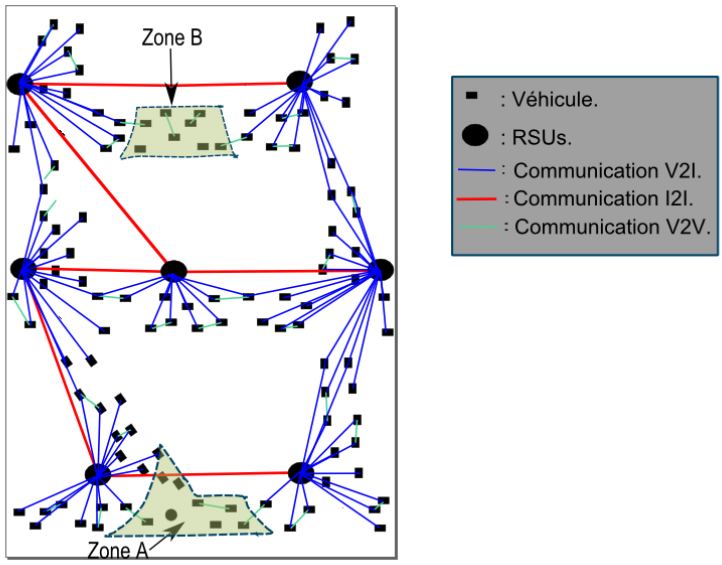



FIGURE 3.4 – Modélisation par un graphe du VANET ayant des RSUs qui couvrent partiellement les zones de la route

**Cas 2 :** La Figure 3.5 représente le graphe qui modélise le cas où les infrastructures RSUs sont déployées de manière à couvrir totalement les zones de la route du VANET. Notons que dans ce cas, l'ensemble $A$ des nœuds RSUs est un ensemble dominant car chaque nœud véhicule est adjacent à au moins un noeud RSU, ceci est due au fait que chaque véhicule est à porté d'une (ou plusieurs) RSU(s).

$$\forall\ j \in (V - A), \exists\ i \in A : (v, i) \in E. \tag{3.2}$$

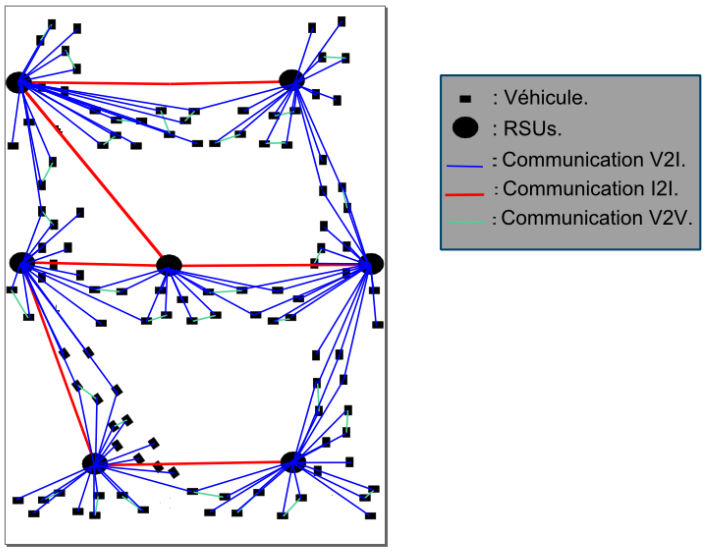



FIGURE 3.5 – Modélisation par un graphe du VANET ayant des RSUs qui couvrent partiellement les zones de la route

### 3.3.3 Représentation des RSUs d'un VANET par une alliance défensive

En s'inspirant des concepts d'alliances dans les graphes (Définition 3.2.1), nous allons définir une nouvelle variante d'alliance défensive en vue d'une application pratique dans les VANETs, que nous appellerons *alliance défensive de traitement de données* formée par l'ensemble des infrastructures RSUs. Une propriété importante d'une alliance défensive de traitement de données est que chaqu'une de ses RSUs peut être soutenue par ses voisines RSUs dans un VANET pour traiter le surplus des paquets qu'elle a reçus.

Avant de donner la définition d'une alliance défensive de traitement de données, nous allons présenter comment se fait le traitement des données par une RSUs. Dans un VANET, à l'instant $t$ donné, chaque véhicule $j$ possède un débit $D_j^i(t)$ qui représente la quantité de données (paquets) que $j$ veut émettre à une RSU notée $i$. Pour le traitement de ces données, chaque RSU possède une file d'attente de capacité limitée appelée *buffer* ou *mémoire tampon* [43] qui enregistre les paquets en attentes de traitement qui lui ont été destinés, comme le montre la Figure 3.6.

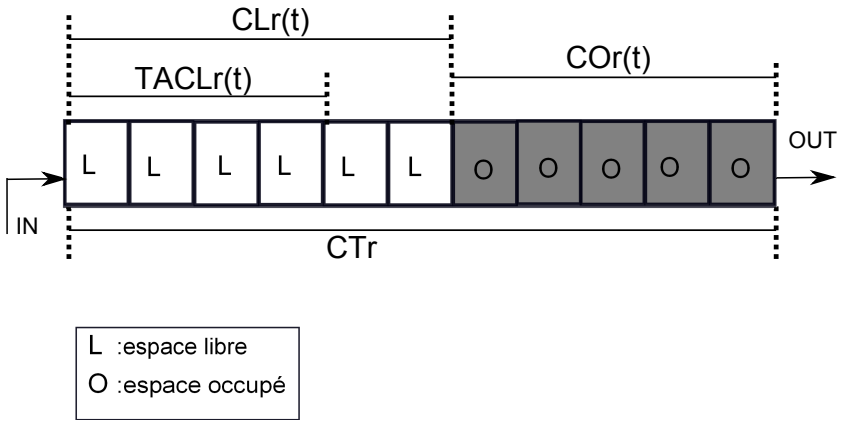



FIGURE 3.6 – File d'attente d'une RSU à un instant $t$

Une file d'attente d'une RSU à un instant $t$, s'il n'est pas saturée (partiellement occupée), est composée d'un espace libre et d'un espace occupé. Dans notre cas, nous avons décomposé l'espace libre d'une file d'attente d'une RSU en deux parties telles que donné dans la Figure 3.6 : l'espace libre 1 qui est conservé et ne peut être consacré que pour les besoins de traitement de cette RSU et l'espace libre 2 qui correspond à l'espace qui peut être confier à des voisins de cette RSU dans l'alliance qui sont en manque d'espace.

Pour la définition d'une alliance défensive de traitement de données, nous avons besoin de définir les paramètres suivants :

$CT_r$ : capacité théorique de la file d'attente de la $r$ème RSU.

$CO_r(t)$ : capacité occupée à l'instant $t$ par les paquets en attente de traitement reçus par la $r$ème RSU.

$CL_r(t)$ : capacité libre de la file d'attente à l'instant $t$, calculée par l'équation suivante : $CL_r(t) = CT_r - CO_r(t)$.

$TACL_r(t)$ : capacité totale libre à l'instant $t$ que l'RSU $r$ peut confier à ses voisins RSUs dans l'alliance $A$ en fonction de leurs besoins, calculée par : $TACL_r(t) = \alpha CL_r(t)$, où $\alpha$ est un paramètre d'entrée qui défini pour chaque RSU le pourcentage de son espace libre à confier à ses voisins RSUs dans l'alliance $A$. Dans notre cas, nous avons fixé $\alpha = \frac{2}{3}$.

$ACL_r^i(t)$ : capacité libre que l'RSU $r$ peut confier à son voisin RSU $i$ à un instant $t$, qui est calculée par l'équation suivante :

$$ACL_r^i(t) = \frac{AIDE_i^r(t)}{\sum_{k \in N_A(r)} AIDE_k^r(t)} TACL_r(t),$$

où $AIDE_i^r$ représente l'espace libre demandé par $i$ à son voisin $r$.

**Définition 3.3.1.** Soit $G = (V, E)$ un graphe et $A \subset V$. L'ensemble $A$ des RSUs est une *alliance défensive de traitement de données* dans un VANET à l'instant $t$, si

$$\sum_{r \in N_A(i)} ACL_r^i(t) + CL_i(t) \geq \sum_{j \in N_{\bar{A}}(i)} D_j^i(t), \ \forall \ i \in A. \tag{3.3}$$

De plus, si l'ensemble $A$ est dominant alors l'alliance défensive $A$ est dite globale.
Si pour un certain $i \in A$, $\sum_{r \in N_A(i)} ACL_r^i(t) + CL_i(t) = \sum_{j \in N_{\bar{A}}(i)} D_j^i(t)$, alors le noeud $i$ ($RSU_i$) est dit *saturé*. On dit que $A$ est une *alliance défensive saturée de traitement de données*, si tous ses nœuds sont saturés.

L'approche que nous proposions dans la sous-section suivante se base sur le principe de l'alliance défensive de traitement de données et procède de manière à éviter autant que possible qu'il y ait des sommets saturés ou l'alliance soit saturée.

### 3.3.4 Algorithme

Dans cette partie, nous allons présenter une solution détaillée pour le problème de la congestion et la saturation des infrastructures RSUs dans les VANETs qui est basée sur l'alliance de traitement de données. Notre algorithme complètement distribué procède de manière à éviter la saturation de l'alliance formée par les RSUs et ainsi réduire la probabilité qu'il y est congestion dans le réseau. Nous allons définir quelques paramètres et notations que nous utiliserons dans notre algorithme.

- RSUPATH ($D_v^i(t)$) : est un message envoyé par un véhicule $v$ aux RSUs pour leur demander un chemin vers la destination.
- Dataemi($v$) : est une valeur booléene qui est à vrai si le message est transféré du véhicule $v$ vers une RSU, faux sinon.
- $|N_A(v)|$ : est un entier qui représente le nombre des RSUs qui sont à portées du véhicule $v$ à l'instant de la recherche d'un chemin optimal.
- $ACK_i^v()$ : est un message envoyé par une RSU $i$ au véhicule $v$ pour l'informer qu'elle est prête à recevoir les données à émettre par $v$.
- $ACK_i^v$ : est une valeur booléene qui est à vrai si l'RSU $i$ a envoyé $ACK_i^v()$ au véhicule $v$, faux sinon.
- $SomD_i(t)$ : est une variable qui sauvegarde la somme des débits reçus par une RSU $i$ à l'instant $t$ et elle est mise à jour à chaque fois qu'un véhicule $k$ n'est plus à portée de l'infrastructure $i$, donc $SomD_i(t + \Delta t) = SomD_i(t) - D_k^i(t)$.
- $ClibreA_i(t)$ : est une variable qui sauvegarde la somme des capacités allouées par l'ensembles des voisins de l'infrastructure $\text{RSU}_i$ à l'instant $t$.

- $ABESION_i(AIDE_i^r(t))$ : est un message envoyé par une $\text{RSU}_i$ qui a besoin d'un soutien de la part de ses voisins dans l'alliance.
- $ALOUER(ACL_r^i(t))$ : est un message envoyé par une RSU $r$ à l'RSU $i$ pour répondre au message $ABESION_i(AIDE_i^r(t))$ pour lui dire que $r$ vous soutien avec une capacité $ACL_r^i(t)$.
- $SATURER_i^v()$ : est un message envoyé par l'RSU $i$ pour avertir le véhicule $v$ qu'elle est saturée. Donc $v$ doit éventuellement acheminer ses données vers un autre véhicule ou bien une autre RSU.
- $DATA()$ : c'est les données que $v$ veut envoyer.
- $compte_i$ : est une variable entière, initialisée à zero à chaque fois qu'une RSU demande de l'aide à ces voisins RSUs, et à chaque reception du message $ALOUER(ACL_r^i(t))$ la variable est incrémenté (calcule le nombre de réponses d'aide).

**Algorithm 1** Algorithme distribué pour éviter la saturation des RSUs dans les VANETs.

**Lors de la reception des données par un véhicule** $v$ ;

$v$ envoie RSUPATH $(D_v^i(t))$ aux RSUs à sa portée ;
$N := |N_A(v)|$ ;
$Dataemi := faux$;

**Lors de la réception de RSUPATH** $(D_v^i(t))$ **par une RSU** $i$ ;

$ACK_i^v := faux$ ;
$SQDE_i(t) := SomD_i(t) + (D_v^i(t))$ ;
**if** $SQDE_i(t) \leq CL_i(t)$ **then**
    $i$ envoie $ACK_i^v()$ à $v$ ;
    $ACK_i^v := vrai$ ;
**else**
    $ClibreA_i(t) := CL_i(t)$ ;
    $compte_i := 0$ ;
    $AIDE_i^r := SQDE_i(t) - CL_i(t)$ ;
    L'RSU $i$ envoie $ABESION_i(AIDE_i^r(t))$ à ces voisins RSUs ; // $r \in \{1, ..., |N_A(i)|\}$
**end if**

**Lors de la réception de** $ABESION_i(AIDE_i^r(t))$ **par une RSU** $r$ ;

$TACL_r(t) = \alpha CL_r(t)$ ;
$ACL_r^i(t) := \frac{AIDE_i^r(t)}{\sum_{k \in N_A(r)} AIDE_k^r(t)} TACL_r(t)$ ;
$r$ envoie $ALOUER(ACL_r^i(t))$ à $i$ ;

**Lors de la réception de** $ALOUER(ACL_r^i(t))$ **par une RSU** $i$ ;

$compte_i + +$;
$ClibreA_i(t) := ClibreA_i(t) + ACL_r^i(t)$ ;
**if** $((SQDE_i(t) \leq ClibreA_i(t))\ et\ (ACK_v = faux))$ **then**
    $i$ envoie $ACK_i^v()$ à $v$ ;
    $ACK_i^v := vrai$ ;
**end if**
**if** $((compte_i = |N_A(i)|)\ et\ (ACK_v = faux))$ **then**
    $i$ envoie $SATURER_i^v()$ à $v$ ;
**end if**

**Lors de la réception de** $ACK_i^v()$ **par un véhicule** $v$ ;

**if** $Dataemi = faux$ **then**
    $v$ envoie $DATA()$ à $i$ ;
    $Dataemi := vrai$ ;
**end if**

**Lors de la réception de** $SATURER_i^v()$ **par un véhicule** $v$ ;

$N - -$ ;
**if** $((Dataemi = faux)\ et\ (N = 0))$ **then**
    $v$ envoie $DATA()$ au véhicule le plus proche à sa portée ;
**end if**

Cette approche se base sur la coopération des RSUs, qui forme une alliance défensive, pour faire face ensemble d'une manière efficace au traitement des données qui leur seront destiner. Plus spécifiquement :

- Quand un véhicule $v$ demande s'il peut envoyer ses données captées à une RSU $i$, cette dernière vérifie d'abord l'espace libre dans son buffer pour ensuite décider s'elle va autoriser le véhicule à lui transmettre ses données (dans le cas de disponibilité d'un espace suffisant), ou bien elle envoie une demande d'aide à ses voisines RSUs (dans le cas d'un espace insuffisant ou de saturation).
- Dans le cas d'envoie d'une demande d'aide par une RSU $i$, chacune des voisines de cette dernière dans l'alliance détermine la capacité dont elle peut aider cette RSU $i$. Ainsi, en recevant par l'RSU $i$ de l'aide de la part de (certaines de) ses voisines, sa capacité devient plus puissante pour faire face au débit des données rentrantes et ainsi éviter sa saturation et donc la perte de données.

## 3.4 Conclusion

Dans ce chapitre, nous avons proposé une approche basée sur le concept d'alliances défensives dans les graphes en vue de réduire la congestion dans les réseaux véhiculaires. Dans le chapitre suivant, nous allons effectuer des simulations pour tester et évaluer le protocole proposé.

Chapitre 4

# Évaluation de performances et simulation

## 4.1 Introduction

Dans ce chapitre, nous proposons deux modèles analytiques qui se basent sur les chaînes de Markov, l'un pour l'approche IAGR et l'autre pour notre approche ADA2RS. A l'aide de ces deux modèles, nous effectuons une étude comparative en estimant la perte de paquets de chacun des deux protocoles. De plus, en perspective d'effectuer d'autres tests, une préparation de l'environnement de simulation est présentée.

## 4.2 Rappel sur les chaînes de Markov

Les chaînes de Markov est une technique de modélisation statistique des processus aléatoires, pour laquelle l'état du système change par progression. Le système est composé d'un ensemble d'états et de probabilités de transition entre ces états. Le processus commence avec un état initial et se déplace successivement d'un état à un autre. Si le système est actuellement à l'état $E_i$, alors il se déplace à $E_j$ dans l'étape suivante avec une probabilité, notée $P_ij$. Cette probabilité ne dépend pas de tout l'historique des différents états mais il dépend seulement de l'état actuel du système ($E_i$). C'est pour cela qu'on dit que la probabilité de transition entre deux états dépend entièrement des circonstances de l'état d'origine de la transition et non de l'historique antérieur du processus. Compte tenu d'une séquence d'états $E_1, E_2, ..., E_n$, la propriété Markov est donnée comme suit [35] :

$$P = (E_{n+1} = x | E_n = x_n, ..., E_1 = x_1) = P(E_{n+1} = x | E_n = x_n). \tag{4.1}$$

Les applications des chaînes de Markov sont très nombreuses, comme : génétique des populations, mathématiques financières, réseaux, simulation, etc. [35].

## 4.3 Modèle analytique pour IAGR

Dans cette section, nous proposons un modèle analytique qui se base sur les chaînes de Markov pour représenter le système de routage de l'information utilisé dans le protocole IAGR (*Infrastructure Assisted Geo-Routing for cooperative vehicular networks*). Pour cela il est nécessaire de définir l'ensembles des états et des probabilités de transitions que nous utiliserons.

| **Notations** | **Descriptions** |
|---|---|
| $n$ | Nombre de véhicules dans le VANET. |
| $m$ | Nombre d'RSUs dans le VANET. |
| $p$, $q$ | Probabilités de choix de changement d'etat. |
| $I$ | État initial (un véhicule veut communiquer). |
| $TRSU_i$ | État de transmission avec succès vers un l'RSU $i$. |
| $TV_j$ | État de transmission avec succès vers un véhicule $V_j$. |
| $Pe$ | État de perte de paquets. |
| $S$ | État de transmission avec succès vers destination. |

TABLE 4.1 – Tableau des paramètres utilisés dans le modèle analytique

Ainsi, le modèle analytique du protocole IAGR qui se base sur le principe qu'un véhicule choisi en priorité les RSUs pour le routage de l'information est donné comme suit :

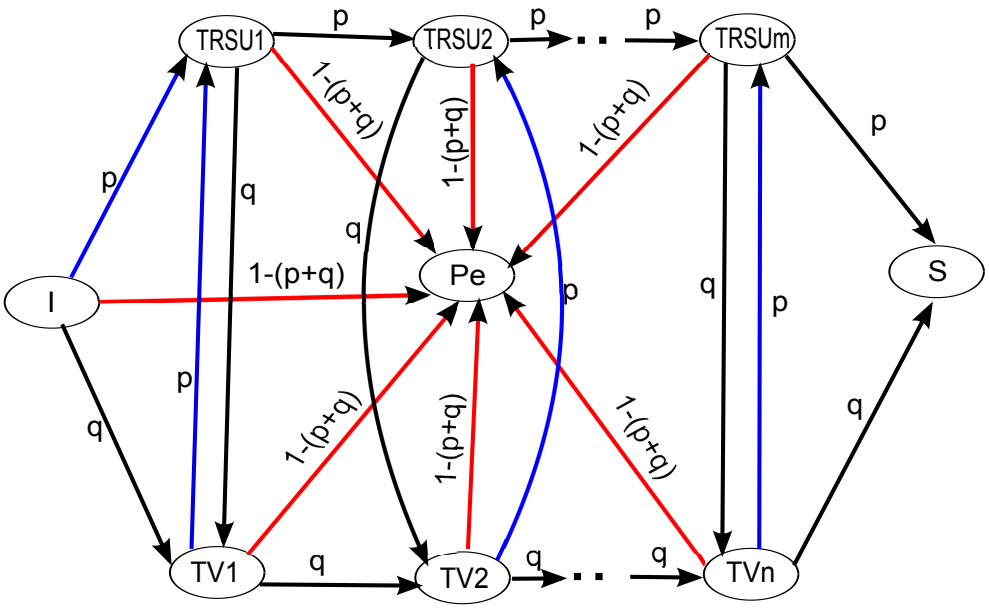



FIGURE 4.1 – Modèle analytique pour IAGR

Donc la probabilité qu'un paquet soit transmit avec succès à l'une des RSUs est égale à $p$. Mais si le véhicule ne trouve pas d'RSU à sa portée, il choisit un véhicule le plus proche à lui pour lui acheminer le paquet avec une probabilité égale à $q$. Par ailleurs, un paquet peut être perdu et cela avec une probabilité égale $1-(p+q)$. Puisque l'envoie de données (informations) est toujours privilégié vers une RSU, alors on suppose que $q \leq p$ et $p+q \leq 1$.

## 4.4 Modèle analytique pour ADA2RS

Dans cette section, nous proposons un autre modèle analytique qui se base aussi sur les chaînes de Markov pour représenter le système de routage de l'information utilisé dans notre protocole "ADA2RS" (Approach based Defensive Alliance for Reducing RSUs Saturation). Nous utilisons les mêmes paramètres que ceux donnés dans le Tableau 4.1. Par ailleurs, pour montrer le principe de la coopération entre les RSUs de l'alliance pour le routage des données, nous avons regroupé tous les états $TRSU_i$ dans un seul état nommé $TRSUs$ en ajoutant un paramètre $\mu$ qui représente le nombre d'RSUs saturées (qui demandent de l'aide). Ainsi, nous obtenons le système des états suivant :

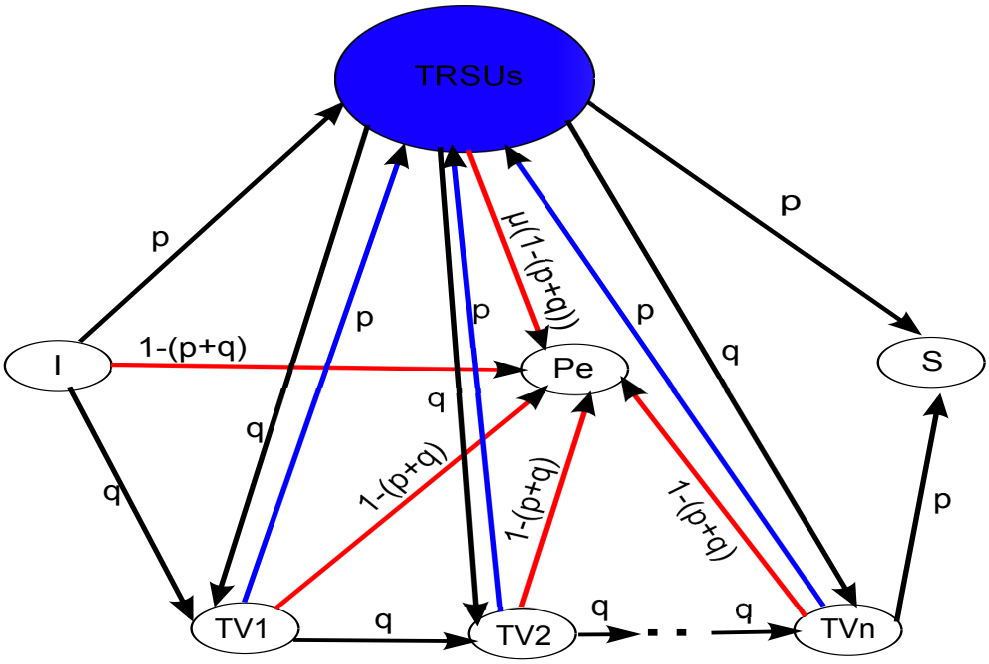



FIGURE 4.2 – Modèle analytique pour ADA2RS

**Expliquer brièvement le fonctionnement**

## 4.5 Etude comparative entre IAGR et ADA2RS

Dans cette section, en utilisant les deux modèles analytiques ci-dessus, nous effectuons une comparison entre les deux protocoles IAGR et ADA2RS. Pour cela, nous calculons la probabilité de perte de paquets $P(Pe) = P(I \to Pe)$ pour les deux modèles.

- **Probabilité de pertes de paquets par le protocole IAGR**

$$\begin{aligned} P_1 = P(Pe) &= (1-(p+q)) + [q(1-(p+q)) + 2q(1-(p+q)) + \cdots + nq(1-(p+q))] + \\ &\quad [p(1-(p+q)) + 2p(1-(p+q)) + \cdots + mp(1-(p+q))] \\ &= (1-(p+q)) + q(1-(p+q))[1+2+\cdots+n] + \\ &\quad p(1-(p+q))[1+2+\cdots+m] \\ &= (1-(p+q))[1+q\frac{n(n+1)}{2} + p\frac{m(m+1)}{2}]. \end{aligned}$$

- **Probabilité de pertes de paquets par le protocole ADA2RS**

$$\begin{aligned} P_2 = P(Pe) &= (1-(p+q)) + [q(1-(p+q)) + 2q(1-(p+q)) + \cdots + nq(1-(p+q))] + \\ &\quad (\mu p(1-(p+q)) + \\ &= (1-(p+q)) + q(1-(p+q))[1+2+\cdots+n] + (\mu p(1-(p+q)) + \\ &= (1-(p+q))[1+q\frac{n(n+1)}{2} + (p\mu)]. \end{aligned}$$

- **Estimation de la différence de perte de paquets entre les deux protocoles**
  Pour estimer la différence de perte de paquets entre les deux protocoles, nous calculons la différence entre les probabilités $P_1$ et $P_2$ dont le résultat est donné comme suit :

$$diff = P_1 - P_2 = p(1-(p+q))[\frac{m(m+1)}{2} - \mu]. \tag{4.2}$$

  Puisque le terme $p(1-(p+q)$ est toujours positif, alors le signe de $diff$ est donné par $\frac{m(m+1)}{2} - \mu$.
  - ▷ **Cas où $\mathbf{m = 1}$ et $\mu = 1$** : cette situation correspond au cas où il existe une RSU et elle a besoin de l'aide (saturée). Dans ce cas, on a $diff = P_1 - P_2 = 0$. Ainsi, dans ce cas particulier, les protocoles ont une même probabilité de perte de paquets.
  - ▷ **Cas où $\mathbf{m > 1}$ et $\mu \in \{\mathbf{0}, \mathbf{1}, \ldots, \mathbf{m}\}$** : cette situation plus générale correspond au cas où il existe au moins deux RSUs avec au moins une (ou aucune n') a besoin de l'aide. Dans ce cas, on a

$$0 < p(1-(p+q))\frac{m(m-1)}{2} \leq diff = P_1 - P_2 \leq p(1-(p+q))\frac{m(m+1)}{2}.$$

    Ainsi dans ce cas, dès qu'il y a au moins deux RSUs, le concept d'alliance entre ces dernières prend effet et ainsi la coopération entre elle engendre une réduction de perte de paquets.

## 4.6 Préparation de l'environnement de simulation

Dans les réseaux VANETs, il existe deux types de simulateur : un simulateur de mobilité, et un simulateur de réseau. Les simulateurs de trafic routier sont utilisés pour la réalisation de teste sur des cartes géographiques et la génération de la mobilité souhaitée (nombre et types de véhicules, la vitesse des véhicules, événement de la route, etc.). Tandis que les simulateurs réseaux sont utilisés pour l'evaluation des performances des protocoles

de routage. Dans ce travail, nous avons utilisé comme environnement de simulation du trafic routier : OSM (*Open Street Map*) pour la recuperation des données géographiques d'une partie de la carte et SUMO *Simulation of Urban Mobility* pour la visualisation et la simulation de ce réseau routier. D'autre part, nous avons utilisé NS-2 (Network simulator) comme un simulateur de réseau.

### 4.6.1 Simulateur de trafic routier

#### OSM (Open Street Map)

OpenStreetMap (OSM) [6] est un projet international fondé en 2004 dans le but de créer une carte libre du monde. Cette carte collecte des données dans le monde entier sur les routes, voies ferrées, les rivières, les forêts, les bâtiments et bien plus encore. Un utilisateur de OSM peut exporter une zone de cette carte (sous fichier.osm) pour l'utiliser et l'integer dans d'autres applications et simulateurs (voir la Figure 4.3).

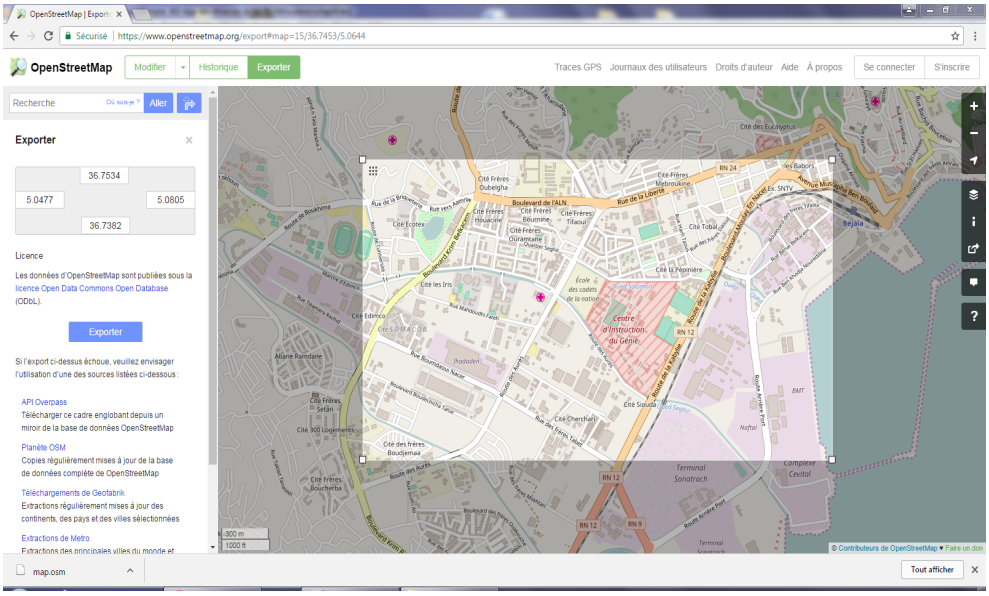



FIGURE 4.3 – Open Street Map

#### SUMO (Simulation of Urban Mobility)

SUMO [7] est développé par les employés de l'institut des systèmes de transports dans le centre aéronautique Allemand. Il permet de simuler le trafic routier. De plus, il permet l'importation de cartes provenant de Google Earth ou bien de OSM (comme dans

notre cas). Ainsi, les routes sont présenté sous forme de voies et le comportement des véhicules est vivant comme le changement de voie de circulation. Il y a des intersections a base des règles de circulation et de priorité connu dans le code la route (voir Figure 4.4).

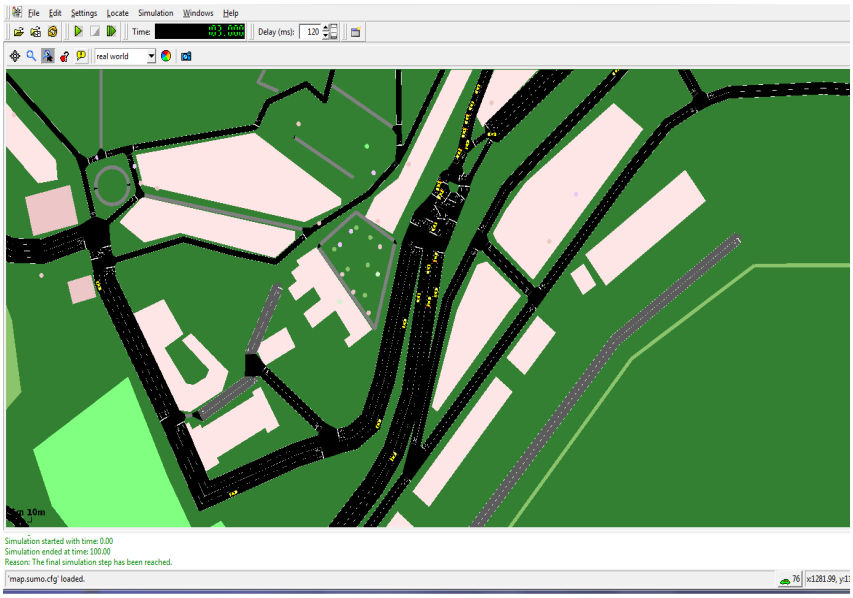



FIGURE 4.4 – SUMO

### 4.6.2 Simulateur réseau

Dans notre étude nous allons utiliser le simulateur de reseaux NS-2 qui est développé dans le cadre du projet VINT [4] avec la collaboration de plusieurs acteur (LBL, Xerox et UCB, etc.). Le choix de ce simulateur est motivé par sa large utilisation par la communauté scientifique pour l'evaluation des nouveaux protocoles, algorithmes et modèles. D'ailleurs, il est considéré, aujourd'hui, comme un standard de références dans le domaine de la simulation des réseaux. De plus il est un simulateur de réseaux libre (Open source), orienté objet et codé avec le langage C++ qui sert à décrire le fonctionnement interne des composants de la simulation. Le simulateur NS-2 est basé sur deux langages :

- Une librairie d'objets réseaux et de protocoles écrits en C++ (noeuds, protocole de routage, fil d'attente, liaisons, etc.).
- Un interpréteur script Otcl [5] utilisé pour décrire une simulation. Chaque simulation définit la topologie du réseau, les protocoles, la durée de simulation, etc.

NS-2 intègre aussi des outils d'analyse et de visualisation comme le NAM (Network Animator) qui est un outil d'animation invoqué à la fin de la simulation en exploitant le fichier trace généré afin d'afficher une vue graphique de la simulation (voir Figure 4.5).

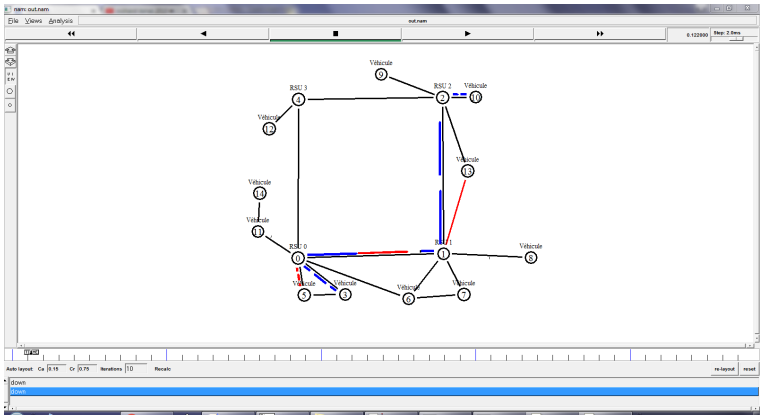


FIGURE 4.5 – Outil NAM

## 4.7 Méthodologie de simulation du protocole proposé

Le processus de simulation d'un VANET passe par plusieurs étapes comme le montre la Figure 4.6.

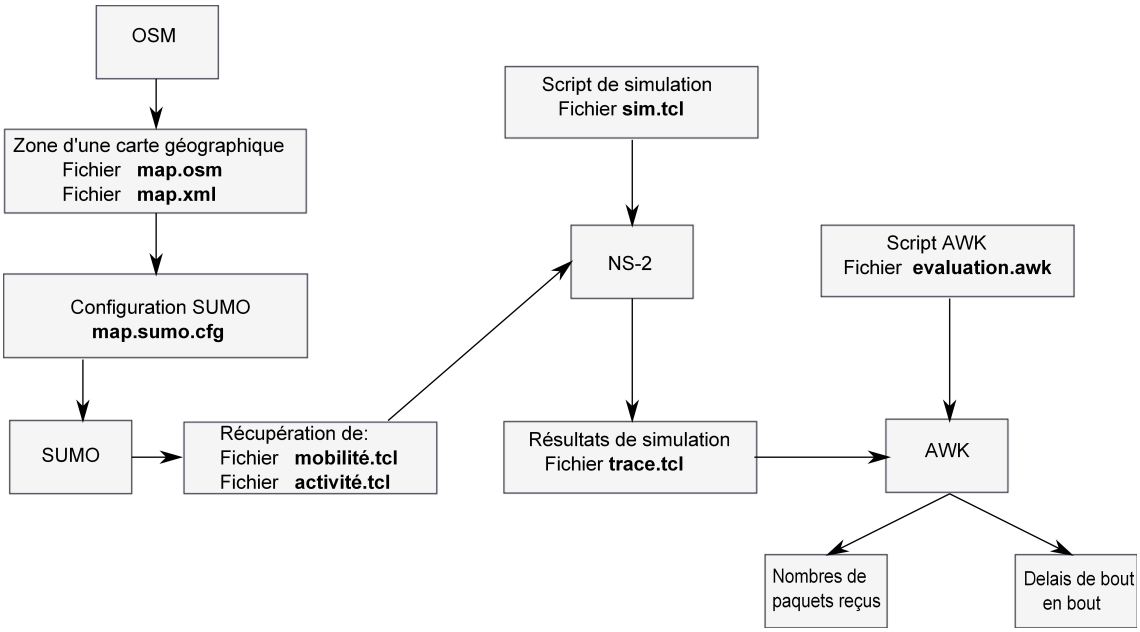



FIGURE 4.6 – Schéma récapitulatif des étapes de la simulation.

La Figure 4.6 montre les principales étapes de simulations dans VANETs qui sont :

*Etape*1 : **Préparation de la carte avec OSM** : dans cette étape, nous avons importé une carte de la ville de Bejaia (Aamriw) avec OSM. Après la configuration et l'intégration de cette carte dans SUMO, nous avons obtenu un fichier **map.sumo.cfg** que nous allons executer avec une commande de console (CMD).

*Etape*2 : **Integration des RSUs à SUMO** : dans cette étape, il faut intégré les RSUs à SUMO.

*Etape*3 : **Execution du fichier map.sumo.cfg** : dans cette étape, nous obtenons un trafic (véhicules) sur la map et la position fixe des RSUs. A la fin de cette étape, un fichier **mobilité.tcl** qui comporte la position de chaque véhicule à chaque instant (voir la Figure 4.7)

```
$node_(0) set X_ 959.06
$node_(0) set Y_ 1725.67
$node_(0) set Z_ 0
$ns_ at 1.0 "$node_(0) setdest 959.06 1725.67 0.00"
$ns_ at 2.0 "$node_(0) setdest 959.36 1724.26 1.44"
$node_(1) set X_ 1081.91
$node_(1) set Y_ 1662.2
$node_(1) set Z_ 0
$ns_ at 2.0 "$node_(1) setdest 1081.91 1662.2 0.00"
$ns_ at 3.0 "$node_(0) setdest 960.01 1721.21 3.12"
$ns_ at 3.0 "$node_(1) setdest 1082.14 1659.67 2.54"
$ns_ at 4.0 "$node_(0) setdest 961.32 1716.32 5.08"
$ns_ at 4.0 "$node_(1) setdest 1082.54 1655.32 4.37"
```

FIGURE 4.7 – Extrait du fichier de mobilité généré par SUMO.

*Etape*4 : **Execution du script sim.tcl en lui integrant le fichier mobilité.tcl** : dans cette étape, nous allons executer le fichier **sim.tcl** avec le simulateur NS-2 et a la fin de la simulation nous allons obtenir fichier **trace.tr** qui comporte tout les événement survenus durant la simulation. Ce fichier sera utilisé pour traiter les résultats de simulation et de calculer les métriques de performances comme le délai d'acheminement et le taux de perte de paquets.

*Etape*5 : **Analyse des résultats** : grace au fichier **evaluation.awk**, écrit en langage C, nous pouvons extraire du fichier **trace.tr** les résultats de la simulation généré par NS-2.

## 4.8 État d'avancement de la simulation

Pour l'instant nous avons préparé l'environnement de simulation. Nous avons configuré SUMO en lui integrant une carte géographique importé de *Open Street Map* (OSM) et nous avons généré un trafic sur le simulateur du trafic urban (SUMO). Comme résultat de la simulation du trafic, nous avons obtenu un fichier **mobilité.tcl** qui comporte les positions des véhicules à chaque instant et qui sera le fichier d'entré pour le simulateur réseau NS-2. Dans les prochaines étapes, nous allons intégrer notre approche à NS-2 et nous executant quelques tests et simulations afin d'avoir les résultats de la simulation. En fin, nous ferons une étude comparative des résultats obtenu des teste de notre approche et ceux du protocole IAGR.

## 4.9 Conclusion

Dans ce chapitre, nous avons proposé deux modèles analytiques qui se basent sur les chaînes de Markov pour comparer les deux approches IAGR et ADA2RS. Les résultats de comparaison obtenus ont montré l'efficacité et la performance de notre approche par rapport à l'approche IAGR en termes de pertes de paquets. Pour plus de comparaisons, notamment avec d'autres approches (protocoles), des tests et simulations supplémentaires sont envisagées.

# Conclusion et perspectives

Le développement des réseaux véhiculaires est en plein essor [44]. D'ailleurs aujourd'hui, il existe plusieurs technologies de transmission de données d'un véhicule à un autre ou vers une infrastructure. Mais malgré cela, il existe toujours des insuffisances liées à la congestion et à la saturation des RSUs dans les VANETs. Ainsi, la préoccupation des chercheurs est de développer de nouvelles techniques de routage de l'information afin de réduire justement la congestion et améliorer la qualité de service dans ce type de réseau.

Dans la literature, plusieurs protocoles de routage utilisent les infrastructures RSUs qui sont connectées pour le routage de l'information dans un VANET. Mais les solutions proposées sont souvent confrontées à des problèmes de saturation de ces RSUs, ce qui engendre une perte de paquets et un retard de livraison de l'information. Pour remédier à cela, nous avons proposé une nouvelle approche qui se base sur un nouveau concept d'alliances défensives dans les graphes qui est formée par l'ensemble des RSUs dans un VANET. L'approche est nommée "ADA2RS" (Approach based Defensive Alliance for Reducing RSUs Saturation) qui se base sur le principe de coopération entre ces RSUs afin de minimiser la perte et le temps de livraison des paquets. Pour évaluer notre proposition, nous avons établi deux modèles analytiques qui se basent sur les chaînes de Markov avec lesquels nous avons comparer notre protocole ADA2RS avec le protocole IAGR. Les résultats de comparaison obtenus ont montré l'efficacité et la performance de notre approche par rapport à l'approche IAGR en termes de pertes de paquets. De plus nous avons préparer l'environnement de simulation pour effectuer plus de comparaisons, notamment avec d'autres approches (protocoles).

Nous pensons, à travers ce travail, que nous avons apporté une contribution relative à la qualité de service dans les VANETs. Cette contribution a permis d'améliorer le routage qui se base sur les infrastructures RSUs. A l'issue de cette contribution, plusieurs perspectives se sont dégagées. parmi elles nous citons :

- Effectuer des tests et des simulations en prenant en considération différentes situations et comparaisons avec plusieurs protocoles dédiés aux VANETs.
- Appliquer l'approche proposée pour le traitement de problèmes posés dans d'autres types de réseaux et systèmes distribués.
- Appliquer de nouvelles techniques de graphes telles que les ensembles sécurisés dans l'étude des VANETs.

# Bibliographie


[1] http://www-igm.univ-mlv.fr/~beal/Enseignement/Polytechnique/Td9/graphe.html, (Consulté le 02 février 2017).

[2] Projet smartpark : Parking made easy. http://smartpark.epfl.ch., (Consulté le 02 février 2017).

[3] https://fr.wikipedia.org/wiki/Routage, (Consulté le 04 février 2017).

[4] http://www.isi.edu/nsnam/vint/, (Consulté le 20 mai 2017).

[5] http://www.otcl-tclcl.sourcefrouge.net/otcl/, (Consulté le 20 mai 2017).

[6] http://openstreetmap.fr/quest-ce-quopenstreetmap, (Consulté le 29 mai 2017).

[7] M. Behrish, L. Bieker, J. Erd-mann, and D. Krajzewiez. Sumo : Simulation of urban mobility. *In Proceedings of SIMUL 2011, The 3rd International Conference on Advances in System Simulation*, (2011).

[8] J. Blum, A. Eskandarian, and L. Hoffman. Mobility management in ivc networks. *In Intelligent Vehicles Symposium Proceedings IEEE, pp. 150-155*, (2003).

[9] D. Borsetti and J. Gozalvez. Infrastructure-assisted geo-routing for cooperative vehicular networks. *IEEE transaction in Vehicular Networking Conference (VNC), pp. 255-262*, (2010).

[10] D. Borsetti and J. Gozalvez. Infrastructure-assisted geo-routing for cooperative vehicular networks. *In Vehicular Networking Conference (VNC), IEEE, pp.255-262*, (2010).

[11] R.C. Brigham, R.D. Dutton, T.W. Haynes, and S.T. Hedetniemi. Powerful alliances in graphs. *Discrete Math. 309 (8), pp. 2140-2147*, (2009).

[12] R.C. Brigham, R.D. Dutton, and S.T. Hedetniemi. A sharp lower bound on the powerful alliance number of $c_m \times c_n$. *Congr. Numer. 167 , pp. 57-63*, (2004).

[13] I. Broustis and M. Faloutsos. Routing in vehicular networks : feasibility, modeling, and security. *In International Journal of Vehiculer Technology*, (2008).

[14] S. Cen, P.C. Cosman, and G.M. Voelker. End-to-end differentiation of congestion and wireless losses. *IEEE/ACM Transactions on Networking, 11(5), 703-717.*, (2003).

[15] C.E.Perkins and P. Bhagwat. Highly dynamic destination-sequenced distance-vector routing (dsdv) for mobile computers. *In Proceedings of the Conference on Communications Architectures, Protocols and Applications, pp. 234-244*, (1994).

[16] Y.Z. Chen and A.L. Liestman. A zonal algorithm for clustering ad hoc networks. *International Journal of Foundations of Computer Science, 14(2), pp. 305-322*, (2003).

[17] J. Choi, S. Jung, Y. Kim, and M. Yoo. A fast and efficient handover authentication achieving conditional privacy in v2i networks. *In Proceedings of the 9th International Conference on Smart Spaces and Next Generation Wired pp. 291-300, Petersburg, Russia*, (2009).

[18] T. Cui, L. Chen, and T. Ho. Energy efficient opportunistic network coding for wireless networks. *INFOCOM 2008. The 27th conference on computer communications. IEEE. pp. 1022-1030*, (2008).

[19] Y. Ding and Li Xiao. Sadv : Static-node-assisted adaptive data dissemination in vehicular networks. *Vehicular Technology, IEEE Transactions on, 59(5) pp. 2445-2455*, (2010).

[20] R. Dipankar and M. Gerla. Emerging wireless technologies and the future mobile internet. *thése doctorat, Cambridge University Press*, (2011).

[21] M. Durresi, A. Durresi, and L. Barolli. Emergency broadcast protocol for intervehicle communications. *In Proceedings 11th International Conference In Parallel and Distributed Systems, 2, pp. 402-406*, (2005).

[22] O. Favaron, G. Fricke, W. Goddard, S.M. Hedetniemi, S.T. Hedetniemi, P. Kristiansen, R.C. Laskar, and R.D. Skaggs. Offensive alliances in graphs. *Discussiones Mathematicae Graph Theory, 24 (2), pp. 263-275*, (2004).

[23] M. Fiore, J. Harri, F. Filali, and C. Bonnet. Vehicular mobility simulation for vanets. *In Proceedings of the 40th Annual Simulation Symposium, pp. 301-309, Norfolk*, (2007).

[24] T. Ghosh and S. Mitra. Congestion control by dynamic sharing of bandwidth among vehicles in vanet. *International Conference on Intelligent Systems Design and Applications (ISDA), pp. 291-296*, (2012).

[25] Z.J. Haas. A new routing protocol for the reconfigurable wireless networks. *IEEE 6th International Conference on Universal Personal Communications Record, 2, pp. 562-566*, (1997).

[26] T. Haynes, T. W. Hedetniemi, S., and P.J. Slater . Domination in graphs. *Journal of Combinatorial Theory, Series B, 34(1), pp. 65-76*, (1998).

[27] T.W. Haynes, S.T. Hedetniemi, and M.A. Henning. Global defensive alliances in graphs. *Discrete Applied Mathematics, 157(2), pp. 211-218*, (2003).

[28] C.J. Hsua, F.H. Wang, and Y.L. Wang. Global defensive alliances in star graphs. *Discrete Applied Mathematics, 157 (8), pp. 1924-1931*, (2009).

[29] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L. Viennot. Optimized link state routing protocol for ad hoc networks. *In Proceedings Of Multi Topic Conference Technology for the 21st Century, pp. 62-68*, (2001).

[30] J.Luo, X.Gu, T.Zhao, and Wei Yan. A mobile infrastructure based vanet routing protocol in the urban environment. *International Conference In Communications and Mobile Computing, 3, pp. 432-437*, (2010).

[31] D.B. Johnson and D.A. Maltz. Dynamic source routing in ad hoc wireless networks. *Proceedings In Mobile Computing Systems and Applications, pp. 90-100*, (1999).

[32] k. Ait Ali. Modélisation et étude de performance dans les réseaux vanets. *Thése doctorat, école doctorale des sciences pour l'ingénieur et microtechniques, université de technologies Belfort, Montbeliard*, (2013).

[33] P. Kristiansen, S.M. Hedetniemi, and S.T. Hedetniemi. Alliances in graphs. *J. Combin. Math. Combin. Comput. 48, pp. 157-177*, (2004).

[34] F. Li and Y. Wang. Routing in vehicular ad hoc networks : A survey. *Vehicular Technology Magazine, pp. 12-22*, (2007).

[35] N.M Li. Markov chain sampling methods for dirichlet process mixture models. *Journal of computational and graphical satatistics, 9(2) pp. 249-265*, (2000).

[36] Z. Lin, L. Xu D. Wang, and J. Gao. A coloring based backbone construction algorithm in wireless ad hoc network. *Proceeding of the GPC 2006, pp. 509-516*, (2006).

[37] J. Luo, X. Gu, T. Zhao, and W. Yan. A mobile infrastructure based vanet routing protocol in the urban environment. *International Conference In Communications and Mobile Computing, 3, pp. 432-437,*, (2010).

[38] H. Moustafa and Y. Zhang. Vehicular networks : techniques, standards and applications. *CRC Press*, (2009).

[39] H. Moustafa and Y. Zhangr. Vehicular networks : techniques, standards and applications. *Auerbach publications*, (2009).

[40] P. Muhletharler. *802.11 et les réseaux sans fil.* Edition Eyrolles, 1er ed. , Paris, (2002).

[41] V. Namboodiri, M. Agarwal, and L. Gao. A study on the feasibility of mobile gateways for vehicular ad-hoc networks. *In Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks, VANET, pp. 66-75, New York, USA*, (2004).

[42] V. Namboodiri, M. Agarwal, and L. Gao. Study on the feasibility of mobile gateways for vehicular ad-hoc networks. *In Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks, pp. 66-75, New York, USA*, (2004).

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

[44] R. Olivier. *Le routage de l'information dans les réseaux vÃ©hiculaires mobiles, université LAVAL.* PhD thesis, (2016).

[45] K. Ouazine, H. Slimani, and A. Tari. Alliances in graphs : parameters, properties and applications-a survey. *AKCE Int. J. Graphs Comb.,*, (2017), http ://dx.doi.org/10.1016/j.akcej.2017.05.002.

[46] H. Pan, R. Jan, A. Jeng, C. Chen, and H Tseng. Mobile-gateway routing for vehicular. *Networks. In IEEE VTSI APWCS*, (2011).

[47] C.E. Perkins and E.M. Royer. Ad-hoc on-demand distance vector routing. *Kluwer Academic Publishers In Mobile Computing, pp. 153-181*, (1996).

[48] M. Raya and J-P. Hubaux. The security of vehicular ad hoc networks. *proceeding of The Third ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN'05), Alexandria, VA, USA, 15(1), 39-68*, (2005).

[49] J.A. Rodríguez-Velázquez and J.M. Sigarreta. Global offensive alliances in graphs. *Electronic Notes in Discrete Mathematic, 25, pp. 157-164*, (2006).

[50] R.A. Santos, A. Edwards, R. M. Edwards, and N.L. Seed. Performance evaluation of routing protocols in vehicular ad-hoc networks. *International Journal of Ad Hoc and Ubiquitous Computing, 1(1/2) ,80-91*, (2005).

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

[52] K.H. Shafique and R.D. Dutton. Maximum alliance-free and minimum alliance-cover sets. *Congr. Numer. 162, pp. 139-146*, (2003).

[53] K.H. Shafique and R.D. Dutton. A tight bound on the cardinalities of maximum alliance-free and minimum alliance-cover sets. *J. Combin. Math. Combin. Comput. 56, pp. 139-145*, (2006).

[54] B.T. Sharef, R.A. Alsaqour, and M. Ismail. Vehicular communication ad hoc routing protocols. *A survey. Journal of Network and Computer Applications, 40(0), pp. 363-396*, (2014).

[55] X. Shen, X. Cheng, R. Zhang, B. Jiao, and Y. Yang. Distributed congestion control approaches for the ieee 802.11 p vehicular networks. *IEEE Intelligent Transportation Systems Magazine, 5(4), pp. 50-61*, (2013).

[56] H. Slimani and H. Kheddouci. Saturated boundary k-alliances in graphs. *Discrete Applied Mathematics, 185, pp. 192-207*, (2015).

[57] P.K. Srimani and Z. Xu. Distributed protocols for defensive and offensive alliances in network graphs using self-stabilization. *In Proceedings of the International Conference on Computing : Theory and Applications, pp. 27-31, Kolkata, India, March*, (2007).

[58] M.Te Sun, Wu chi Feng, T.H. Lai, K. Yamada, H. Okada, and K. Fujimura. Gps-based message broadcast for adaptive inter-vehicle communications. *In Vehicular Technology Conference, 2000. IEEE-VTS Fall VTC 2000. 52nd, 6, pp. 2685-2692*, (2000).

[59] Y. Toor, P. Muhlethaler, A. Laouiti, and A.D.L. Fortelle. Vehicle ad hoc networks : Applications and related technical issues. *IEEE Communications Surveys and Tutorials, 10(3), pp. 74-88*, (2008).

[60] M. Torrent-Moreno, D. Jiang, and H. Hartenstein. Broadcast reception rates and effects of priority access in 802.11-based vehicular ad-hoc networks. *In Proceedings Of the 1st ACM International Workshop on Vehicular Ad hoc Networks, pp. 10-18*, (2004).

[61] Venkatesh, A.Indra, and R.Murali. Routing protocols for vehicular ad-hoc networks (vanets). *Emerging Trends in Computing and Information Sciences*, (2014).

[62] N. Wisitpongphan, O. Tonguz, J. Parikh, F. Bai, P. Mudalige, and V. Sadekar. On the broadcast storm problem in ad hoc wireless network. *The 3rd International Conference on BROADNETS, IEEE, pp. 1-11*, (2006).

[63] J. Wu, M. Cardei, F. Dai, and S.H. Yang. Extended dominating set and its applications in ad hoc networks using cooperative communication. *IEEE Transactions on Parallel and Distributed Systems, 17(8), pp. 851-863*, (2006).

[64] I.G. Yero and J.A. Rodríguez-Velázquez. Defensive alliances in graphs : a survey. *arXiv :1308.2096v1 [math.CO]*, (2013).

[65] Y. Yi and S. Shakkottai. Hop-by-hop congestion control over a wireless multi-hop network. *IEEE/ACM Transactions on Networking, 15(1), pp. 133-144*, (2007).

# RÉSUMÉ

Les réseaux véhiculaires mobiles, ou Vehicular Ad-hoc Networks (VANETs), ont reçu une attention particulière de part des scientifiques en raison de leur importance dans la vie quotidienne. Dans les VANETs, nous trouvons principalement, des entités fixes (RSUs) et des entités mobiles (véhicules). Pour pouvoir échanger différentes informations et données liées à la sécurité et au confort des usagers de la route, ces différentes entités doivent établir des communications entre elles. Lors de ces communications, le problème majeur est lié à la congestion et à la saturation des RSUs. Pour remédier à ce problème, nous avons proposé dans ce mémoire, une nouvelle approche de coopération entre les RSUs d'un VANET en vue de réduire sa congestion et donc d'éviter au mieux la saturation de ces RSUs. Cette approche, appelée "ADA2RS" (Approach based Defensive Alliance for Reducing RSUs Saturation), se base sur le concept d'alliances défensives dans les graphes qui assure une collaboration efficace entre les RSUs. De plus nous avons proposé deux modèles analytiques qui se basent sur les chaînes de Markov pour comparer notre protocole ADA2RS avec le protocole IAGR. Les résultats de comparaison obtenus ont montré l'efficacité et la performance de notre approche par rapport à l'approche IAGR en termes de pertes de paquets. Pour plus de comparaisons, notamment avec d'autres approches (protocoles), des tests et simulations supplémentaires sont envisagées.



**Mots clés :** VANET, Congestion, RSU, Saturation, Alliance défensive de traitement de données, Chaîne de Markov, Modèle analytique.



# ABSTRACT

Vehicular Ad-hoc Networks (VANETs) have received special attention from scientists because of their importance in daily life. In VANETs, we mainly find fixed entities (RSUs) and mobile entities (vehicles). In order to exchange information and data relating to the safety and comfort of road users, these different entities must establish communications between them. In these communications, the major problem is related to congestion and saturation of RSUs. To solve this problem, we proposed in this paper a new approach of cooperation between the RSUs of a VANET with a view to reducing its congestion and thus to avoid as much as possible the saturation of these RSUs. This approach, called "ADA2RS" (Approach based Defensive Alliance for Reducing RSUs Saturation), is based on the concept of defensive alliances in graphs that ensures efficient collaboration between RSUs. In addition, we proposed two analytical models based on Markov chains to compare our ADA2RS protocol with the IAGR protocol. The comparison results obtained showed the efficiency and the performance of our approach compared to the IAGR approach in terms of packet loss. For further comparisons, in particular with other approaches (protocols), additional tests and simulations are envisaged.



**Key words :** Vehicular ad hoc network (VANET), Congestion, Road side unit (RSU), Defensive alliance of data processing, Markov Chain, Analytical model.