REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

Ministère de l'enseignement supérieur et de la recherche scientifique

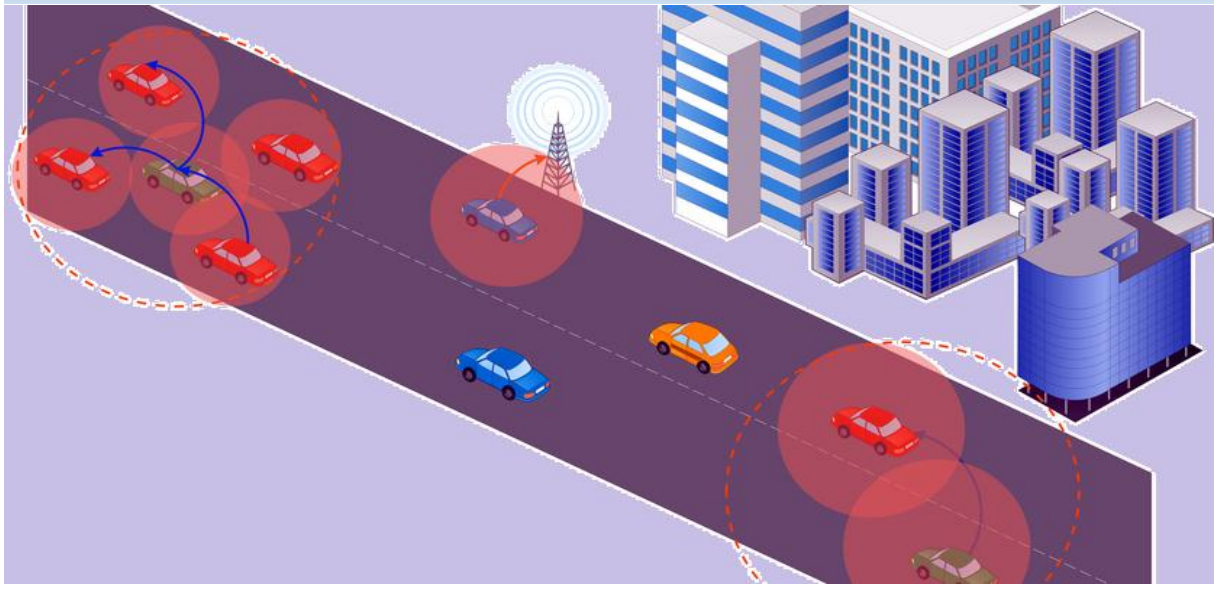
Université Mouloud MAMMERI de Tizi-Ouzou
Faculté de Génie Electrique et Informatique
Département d'Informatique

Mémoire de fin d'études

En vue de l'obtention du diplôme de Master en Informatique
Option : Réseaux, Mobilités et Systèmes Embarqués

Thème :

Conception et réalisation d'une approche collaborative pour la détection d'une conduite agressive dans les Réseaux Ad hoc Véhiculaires (VANET).



Proposé et dirigé par :

Promotrice : Mme OUBABAS Sarah

Co-Promotrice : Mme AOUDJIT Rachida

Réalisé par :

Mlle AISSAOUI Thinhinane

Mlle BEN HOCINE Lydia

Année universitaire : 2019 / 2020

Remerciements

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

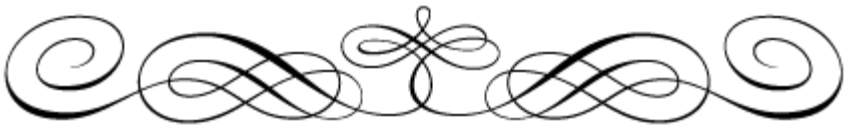
Nous tenons à remercier tout d'abord Mme AOUDJIT Rachida pour l'honneur qu'elle nous a fait en acceptant de nous encadrer, ses précieux conseils ont permis une bonne orientation dans la réalisation de ce modeste travail.

Nous tenons également à remercier les membres du jury pour l'honneur qu'ils nous ont fait en acceptant de juger notre travail, et d'avoir consacré leur temps pour sa lecture.

Nous tenons notre profonde gratitude à l'ensemble du corps enseignant qui a contribué à notre formation.

Enfin nous tenons à rendre hommage à toutes nos familles et nos amis(es) pour le soutien qu'ils nous ont apporté durant toutes ces années d'étude.

Dédicaces



Merci Allah de m'avoir donné la capacité d'écrire et de réfléchir, la force d'y croire, la patience d'aller jusqu'au bout du rêve. Je tiens à dédier ce modeste travail :

A mes chers parents, aucune dédicace ne saurait exprimer mon respect, mon amour éternel et ma considération pour les sacrifices que vous avez consenti pour mon instruction et mon bien être. Que ce modeste travail soit l'exaucement de vos vœux tant formulés, le fruit de vos innombrables sacrifices, bien que je ne vous en acquitterai jamais assez.

A mes très chers grands parents, Je vous remercie pour tout le soutien et l'amour que vous me portez depuis mon enfance et j'espère que votre bénédiction m'accompagne toujours

A ma chère sœur Sarra et à mon chère frère Abderrahmane, En témoignage de mon affection fraternelle, de ma profonde tendresse et reconnaissance.

A touts les membres de la famille « BEN HOCINE » et « BENSAID » pour leur soutien tout au long de mon parcours universitaire.

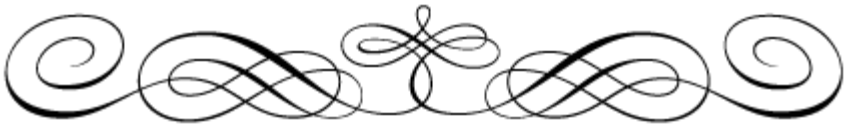
A mes chers amis spécialement Melissa Oussaid et Assia Arrarbi qui ont été toujours un pilier pour moi.

A la personne qui a partagé tous le travail, ma chère amie et binôme Aissaoui Thinhinane, je n'aurais pas souhaité quelqu'un de mieux avec qui faire ce projet et clore ensemble nos années d'études, je te souhaite une vie pleine de bonheur et de succès et que Dieu, le tout puissant, te protège et te garde.

Et à tous ceux qui ont contribué de prés ou de loin pour que ce projet soit possible, je vous dis merci.

Lydia.

Dédicaces



Avant tout propos, je tiens à rendre grâce à Allah qui m'a guidé sur la bonne voie et m'a donné la force dans les moments difficiles d'éditer ce mémoire. Ensuite, Je tiens à dédier ce modeste travail :

A ma famille, elle qui m'a doté d'une éducation digne, son amour et soutien ont fait de moi ce que je suis aujourd'hui.
Particulièrement, à :

Ma très chère mère, qui a œuvré pour ma réussite, de par son amour, son soutien, tous les sacrifices consentis et ses précieux conseils, pour toute son assistance et sa présence dans ma vie, reçois à travers ce travail aussi modeste soit-il, l'expression de mes sentiments et de mon éternelle gratitude.

Mon cher père, qui peut être fier et trouver ici le résultat de longues années de sacrifices

Mon cher oncle Ali ainsi que sa chère épouse Samia qui m'ont aidé et encouragé tout au long de mon parcours et qui ont toujours été présents pour moi.

Mon cher frère Idir et ma chère sœur Dihia, qui m'ont encouragé et soutenu dans mes moments de détresse.

Ma chère grand-mère ainsi que mes oncles et tantes, mes cousins et cousines et toute la famille « AISSAOUI » et la famille « NAIT CHALLAL ».

A mes très chères amies Samia OUKACI et Sarah AOUDJEHANE, qui m'ont écouté, encouragé et soutenu tout au long de mon parcours et qui sont toujours là pour moi.

A ma très chère amie et binôme BEN HOCINE Lydia, avec qui j'ai partagé des belles années d'études et avec qui j'ai eu l'honneur de les terminer avec ce mémoire. Merci pour ta compréhension, tu es toujours là quand j'en ai besoin, je te souhaite du fond de mon cœur une vie pleine de bonheur, de la joie et de la réussite.

A toutes les personnes qui me sont chères, celles que j'aime et celles qui m'aiment et que je n'ai pas citées, je leur souhaite à tous beaucoup de courage, de chance et de succès.

Thinhinane.

Résumé :

Avec la croissance continue du marché automobile, la sécurité routière devient un domaine de recherche populaire. La demande de sécurité routière, a été au centre des préoccupations ces dernières années. Les réseaux ad hoc de véhicules (VANET) ont été la technologie clé en cours de recherche en raison de ses nombreuses possibilités d'application liées à la sécurité routière. Une étude sur les accidents de la route indique que l'erreur humaine est la cause de plus de 90% des accidents et c'est dû principalement aux infractions routières commise lors de sa circulation.

Dans ce mémoire, nous proposons une nouvelle technique pour utiliser les VANET afin d'anticiper des situations potentiellement dangereuses dû à un excès de vitesse ou à un non-respect de la distance entre les véhicules. Pour ce faire, nous proposons une nouvelle approche collaborative utilisant un réseau ad hoc de véhicules (VANET) basé sur le concept de la hiérarchisation, c'est-à-dire, organisé en groupes de nœuds, qui représentent des véhicules intelligents, ces derniers communiquent entre eux par le biais des massages afin de repérer tout véhicule malhonnête ayant commis une infraction pendant le trajet.

L'approche proposée fonctionne sous un système de contrôle basé sur seuil qui permet aux véhicules de coopérer pour produire la signature des preuves contre toute infraction commise.

Les conducteurs accusés sont signalés au serveur de police afin de prendre les contre-mesures appropriées et ce grâce à un système de facturation automatique des contraventions routières.

Mot clés : VANET, clustering, infraction routière.

Abstract :

With the continued growth of the automotive market, road safety is becoming a popular area of research. The demand for road safety has been at the center of concerns in recent years. Ad hoc vehicle networks (VANET) have been the key technology being researched because of its many application possibilities related to road safety. A study on road accidents indicates that human error is the cause of more than 90% of accidents and this is mainly due to traffic violations committed while driving.

In this thesis, we propose a new technique for using VANETs to anticipate potentially dangerous situations due to excessive speeding or failure to respect the distance between vehicles. To do this, we propose a new collaborative approach using an ad hoc network of vehicles (VANET) based on the concept of clustering, that is to say, organized in groups of nodes, which represent intelligent vehicles, the latter communicate with each other through massages in order to identify any dishonest vehicle having committed an offense during the journey.

The proposed approach operates under a threshold-based control system that allows vehicles to cooperate to produce signature evidence against any offense committed.

Charged drivers are reported to the police server in order to take appropriate countermeasures through an automatic billing system for traffic tickets.

Keywords : VANET, clustering, traffic violation.

Glossaire des acronymes :

$: Dollar.

$US : Symbole du Dollar Américain (United State).

% : Pour Cent.

ABS : Anti blocking system.

ACC : Adaptative Cruise Control.

ACDM : Algorithme de Calcul de la Distance Minimale.

ADAS : Advance Driving Assist System.

ADDV : Algorithme de Détection de Dépassement de la Vitesses.

AFIL : Alerte de Franchissement Involontaire de Ligne.

AP : Access Point.

CA : Certification Authority (**AC** : Autorité de Certification).

CH : Cluster Head.

CNIL : Commission Nationale de l'Informatique et des Libertés.

CSW : Collision Warning Systems

CVR : Système Conducteur-Véhicule-Route.

D : Distance entre deux véhicules.

D_L : Distance limitée par la loi entre deux véhicules.

DSRC : Dedicated Short Range Communication.

ECC : Elliptic Curve Cryptography

ESP : Electronic Stability Program.

GMSM : Modèle d'ombre de mélange.

GPRS : General Packet Radio Service.

GPS : Global Positioning System.

I2V : Infrastructure to Vehicular.

IEEE : Institute of Electrical and Electronics Engineers.

IGMM : Infinite Gaussian Mixture Model (modèle de mélange gaussien infini).

IHM : Interface Homme-Machine

ITS : Intelligent Transport System (**STI** : Système de Transport Intelligent).

ITS-S : Station de Système de Transport Intelligent.

IVC : Inter Vehicle Communication.

MANET : Mobile Ad hoc Network.

OBU : On Board Unit.

OMNeT++ : Objective Modular Network Test-bed in C++.

OMS : Organisation Mondiale de la Santé.

OSM : Open Street Map.

PMV : Panneaux à Messages Variables.

RDS : Radio DATA System.

RLC : Reputation Label Certificate.

RSA : Rivest Shamir Adleman

RSU : Road Side Unit.

SIG : Système d'Information Géographique.

SUMO : Simulation of Urban Mobility.

TIC : Technologie de l'Information et de la Communication.

TMC : Transport Management Center.

TraCI : Traffic Control Interface.

TWS : Tailgate Warning Sensor (capteur d'avertissement de talonnage).

V : Vitesse entre deux véhicules.

V2I : Vehicular to Infrastructure.

V2V : Vehicular to Vehicular.

VANET : Vehicular Ad hoc Network.

Veins : Vehicles in network simulation.

V_L : Vitesse limitée par la loi entre deux véhicules.

VSN : Vehicular Sensor Network.

Liste des figures :

Chapitre I : Généralités sur les réseaux véhiculaires (VANET).

Chapitre II : Amélioration de la sécurité routière grâce aux réseaux véhiculaires.

Chapitre III : Description de l'approche proposée.

Chapitre IV : Implémentation et Simulation.

Liste des tableaux :

Sommaire :

Chapitre III : Description de l'approche proposée.

Chapitre IV : Implémentation et Simulation.

Introduction Générale

Introduction générale :

Depuis plusieurs années, les gouvernements, constructeurs automobiles et consortiums d'industriels, ont fixé la réduction des accidents de la route comme une priorité majeure. Afin de réussir ce challenge, une idée novatrice a été de rendre les véhicules et les routes plus intelligents par le biais des communications sans fil. En effet, les véhicules actuels génèrent et analysent déjà une quantité de données importante, mais ne diffusent rien. Avec des communications sans fil, l'environnement du véhicule et le « champ de vision » du conducteur sont accrus.

Avec l'avènement des technologies sans fil telles que la 4G, le Wifi, le Bluetooth, etc. les communications sans fil sont devenues omniprésentes et peu onéreuses. C'est pourquoi, afin de déployer ces applications, un type de réseau a émergé : le réseau sans fil véhiculaire. Une des principales composantes d'un tel réseau est la communication inter-véhicules. Le réseau est alors appelé réseau sans fil ad hoc véhiculaire (VANET).

Au cours de ces dernières années, les VANET ont fait l'objet de recherches approfondies par les chercheurs, les universités et les industries. C'est pourquoi l'industrie automobile a connu une évolution et les véhicules ne sont plus considérés comme des systèmes thermomécaniques contrôlés par quelques composants électroniques. Les véhicules d'aujourd'hui sont des systèmes complexes qui sont contrôlés par des systèmes embarqués ou des réseaux d'ordinateurs. Plusieurs facteurs ont contribué à cette évolution dans le monde de l'industrie automobile telle que la haute densité automobile en particulier dans les grandes villes et les menaces de sécurité routière potentielles.

Dans les réseaux véhiculaires (VANET), les véhicules sont équipés de dispositifs de communication sans fil, appelés unités embarquées (OBU), pour permettre les différents types de communications : véhicule à véhicule (V2V) et véhicule à infrastructure (V2I).

Les VANET et les communications véhiculaires amélioreront considérablement la sécurité, l'efficacité et la commodité du transport. En effet, ils ont contribué efficacement à l'amélioration de la sécurité routière tout en changeant la façon de conduire des chauffeurs et en facilitant les services d'urgence.

Bien qu'initialement conçus pour améliorer la sécurité routière, les VANET peuvent en outre offrir des services commerciaux, informatifs et de divertissement aux conducteurs et aux passagers, augmentant ainsi également les revenus des constructeurs automobiles et de divers prestataires de services.

Les VANET permettent aux véhicules de communiquer facilement entre eux et également avec des infrastructures fixes. Grâce à une communication ad hoc véhicule-infrastructure et véhicule-véhicule, le conducteur peut être averti plus tôt et plus précisément des situations de circulation.

Les réseaux véhiculaires jouent un rôle clé dans la conception de systèmes de gestion du trafic dans les villes intelligentes. Ils sont considérés comme une technologie prometteuse pour la collecte de données sur le trafic qui facilite les applications d'efficacité et de sécurité routière grâce aux systèmes de transport intelligents (STI). En effet, le nombre croissant de véhicules sur les routes des grandes villes a posé de nombreux défis aux autorités en matière de congestion routière, d'accidents de la route et de risques sanitaires. Pour faire face à ces problèmes, les villes du monde entier concentrent leurs efforts sur l'utilisation de technologies avancées et innovantes pour rendre leurs systèmes de gestion du trafic « plus intelligents ».

Dans notre travail, nous avons proposé une nouvelle approche collaborative pour la détection de conduite agressive en utilisant un réseau ad hoc de véhicules (VANET) où les véhicules s'organisent en clusters. Chaque cluster est géré par un chef appelé Cluster-Head (CH) tandis que toutes les opérations des clusters sont gérées par les unités coordinatrices RSU. Les véhicules coopèrent pour dénoncer tout véhicule ayant violé les règles (limitation de vitesse et distance de sécurité) fixées par les services de l'autorité. Pour s'y faire, on a conçu deux algorithmes utilisant les informations collectées lors de l'échange périodique des messages entre les véhicules du réseau afin de pouvoir calculer la vitesse moyenne des véhicules voisins et la distance séparant un véhicule d'un autre, et ainsi détecter les conducteurs enfreignant la loi.

Pour mieux faciliter le système de pénalisation et de facturation de ces véhicules, un serveur de police est mis en place, afin de délivrer automatiquement une amende à chaque véhicule ayant commis une infraction routière et cela se fera avec l'aide et la collaboration des véhicules ayant détecté ladite infraction. Cependant, vu l'importance des informations échangées entre les différents nœuds du réseau (véhicules, RSU, serveur de police…) et l'ouverture de l'environnement VANET, un véhicule ayant une mauvaise intention, peut émettre des messages d'alerte dont le contenu est falsifié, et pour y remédier, nous avons proposé une approche qui se base sur la signature numérique à seuil qui est considérée comme étant une primitive cryptographique pour la génération et la signature de clés distribuées, ce nouveau paradigme peut offrir de nombreux avantages, en particulier en termes de sécurité.

Afin de mener à bien notre travail, nous avons établi un plan qui s'articule sur quatre parties essentielles encadrées par une introduction générale et une conclusion générale :

Le premier chapitre fait l'objet d'une présentation de quelques généralités sur les réseaux sans fil, ensuite sur les réseaux véhiculaires VANET incluant les différents types d'applications ainsi que leurs rôles.

Le deuxième chapitre porte sur les différents types de systèmes de transport intelligent ayant comme objectif principal l'amélioration de la sécurité routière.

Le troisième chapitre présente d'une manière très détaillée l'approche proposée qui permet de garantir la sécurité routière tout en détectant les alertes frauduleuses des conducteurs compromis.

Le quatrième chapitre est une implémentation de l'approche proposée suivie d'une simulation qui permettra d'observer les résultats obtenus.

Chapitre I :

Généralités sur les réseaux véhiculaires (VANET)

I.1. Introduction :

Les accidents de la route anéantissent des milliers de vies humaines, causent des tragédies sociales et engendrent des pertes économiques et financières fort importantes. En effet, chaque année, plus de 1,35 million de personnes perdent la vie dans des accidents de la route. On recense en plus de 20 à 50 millions de blessés, nombre d'entre eux gardant une invalidité à la suite de leurs blessures [1].

Selon l'OMS, les accidents de la circulation routière sont la cause, chaque année, de millions de morts et de blessés dans le monde. La route est devenue ainsi la neuvième cause de mortalité au monde en 2004 (OMS, 2009) et à ce rythme elle passera à la cinquième place en 2030. La route est la première cause de mortalité au monde en 2012 qui a touché en priorité des personnes âgées de 15 à 29 ans (OMS, 2015).

Cette augmentation du nombre de décès a poussé de nombreux pays à prendre des mesures visant la réduction des accidents et la mise en place de mécanismes capables de rendre les routes moins dangereuses pour les différents types d'usagers. Afin de réussir ce challenge, l'idée première a été de rendre les véhicules et les routes plus intelligents par le biais des communications sans fil. Grâce à des véhicules à l'écoute de leur environnement, plus de 75 applications potentielles ont été identifiées [2].

Ce chapitre a pour objectif d'appréhender la notion de réseau sans fil véhiculaire et de définir le contexte de notre travail. Nous présentons dans un premier temps une vue générale sur les réseaux sans fil ainsi que leur architecture, ensuite nous allons aborder les VANET ainsi que leurs objectifs. Enfin, nous décrivons l'architecture et les caractéristiques des réseaux sans fil véhiculaires ainsi que quelques types d'applications dans les VANET.

I.2. Les réseaux sans fil :

I.2.a. Définition d'un réseau sans fil :

Un réseau sans fils (en anglais Wireless network) est un réseau dans lequel les différents éléments participants (ordinateur portable, téléphone portable…etc.) ne sont pas raccordés entre eux par un média physique. La transmission des données se fait via les ondes hertziennes (radio ou infrarouge). Ceci permet aux utilisateurs de se déplacer dans un périmètre de couverture pouvant aller d'une dizaine de mètres à quelques kilomètres.

I.2.b. Architecture des réseaux sans fil :

➢ Mode infrastructure :

Ce mode désigne un réseau composé d'une infrastructure permettant l'échange d'information entre les différentes stations du réseau. Cette infrastructure est basée sur un matériel spécifique qui fournit un ensemble de services. Ce matériel est appelé un point d'accès (AP), appelé aussi station de base. Les stations de base sont munies d'une interface de

communication sans fil avec les sites mobiles qui se trouvent dans sa zone géographique ou sa couverture radio. Voir la figure *Fig. I.1*.

Fig. I. 1 : *Mode infrastructure.*

➢ Mode sans infrastructure ou réseau ad hoc :

Ce mode n'a pas besoin de point d'accès pour fonctionner, ce sont les stations elles-mêmes qui entrent en communication sans s'appuyer sur un équipement extérieur. Tous les nœuds d'un réseau de ce type se comportent comme des routeurs et prennent part à la découverte et à la maintenance des chemins de communication entre les différentes machines. Ce type de réseau s'organise lui-même. Voir la figue *Fig. I.2*.

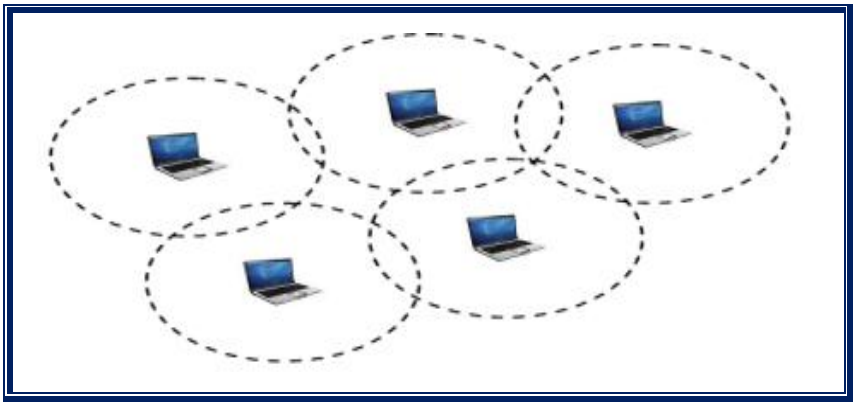


Fig. I. 2 : *Mode sans infrastructure.*

I.3. Les réseaux ad hoc MANET :

Un réseau mobile ad hoc, appelé généralement Mobile Ad hoc Network (MANET), est un ensemble de nœuds mobiles qui se déplacent dans un territoire quelconque d'une manière autonome et coopérative, sans l'utilisation d'une infrastructure préexistante ou d'une administration centralisée. Les ondes radio qui se propagent entre les différents nœuds mobiles sont le seul moyen de communication. Dès qu'un ensemble de nœuds mobiles se trouve à portée radio les uns des autres, alors le réseau se forme spontanément mais de manière provisoire.

I.4. Les réseaux véhiculaires :

Les réseaux véhiculaires sont une nouvelle classe émergente des réseaux sans fil, les VANET constituent une sous-classe des MANET tel qu'il est illustré dans la figure *Fig. I.3*.

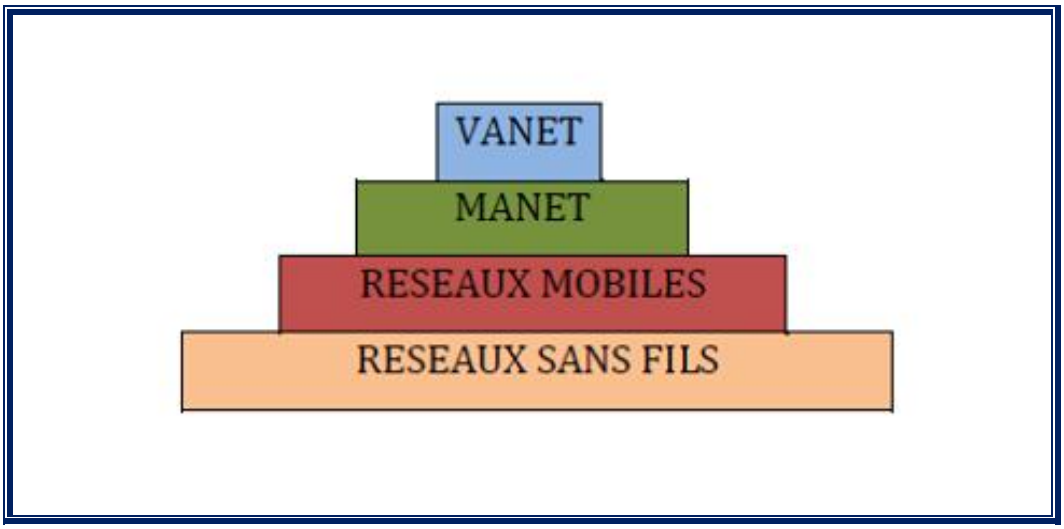


Fig. I. 3 : *Hiérarchie des réseaux sans fil.*

Dans un réseau VANET, les nœuds peuvent être des véhicules ou des infrastructures fixes appelées RSU (Road Side Unit) installées le long des routes. Les différents nœuds du réseau disposent d'équipements (Calculateurs, carte réseaux et capteurs) leur permettant de communiquer via des technologies sans fil d'où le nom de véhicule intelligent qui permet au véhicule de communiquer et de collecter des informations concernant son environnement. Voir la figure *Fig. I.4*.

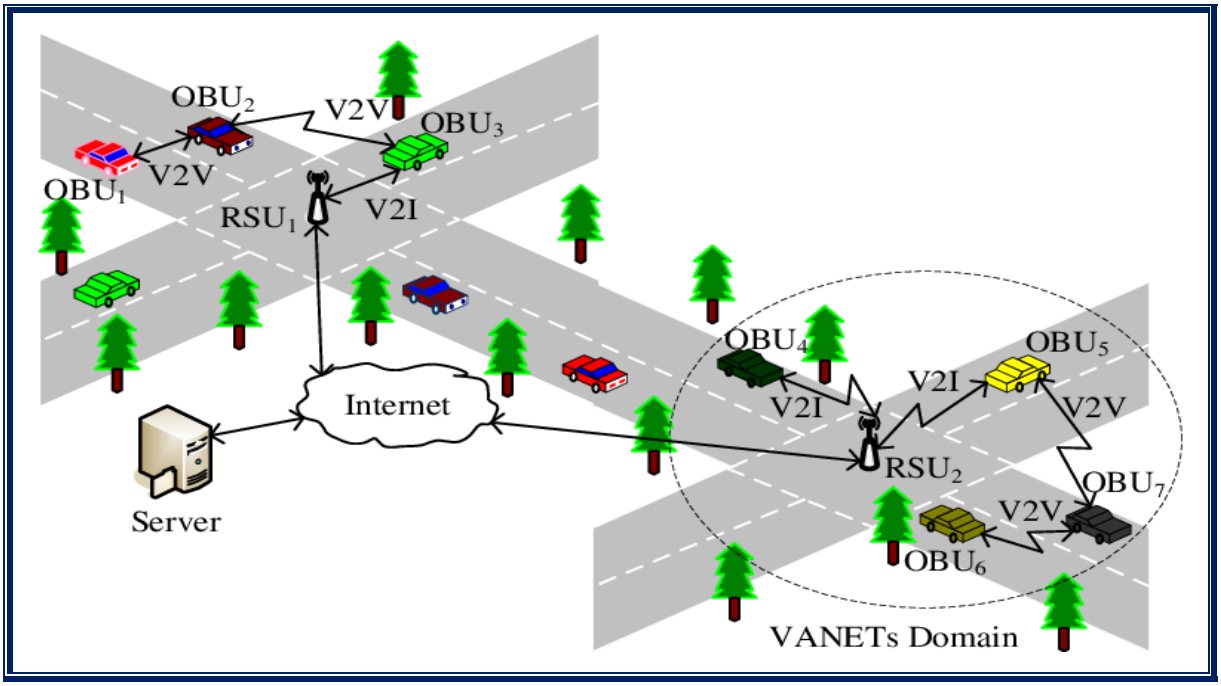


Fig. I. 4 : *Exemple d'un réseau véhiculaire.*

I.4.a. Les entités communicantes :

Un réseau véhiculaire se compose principalement de trois entités comme indiqué sur la figure *Fig. I.5*.

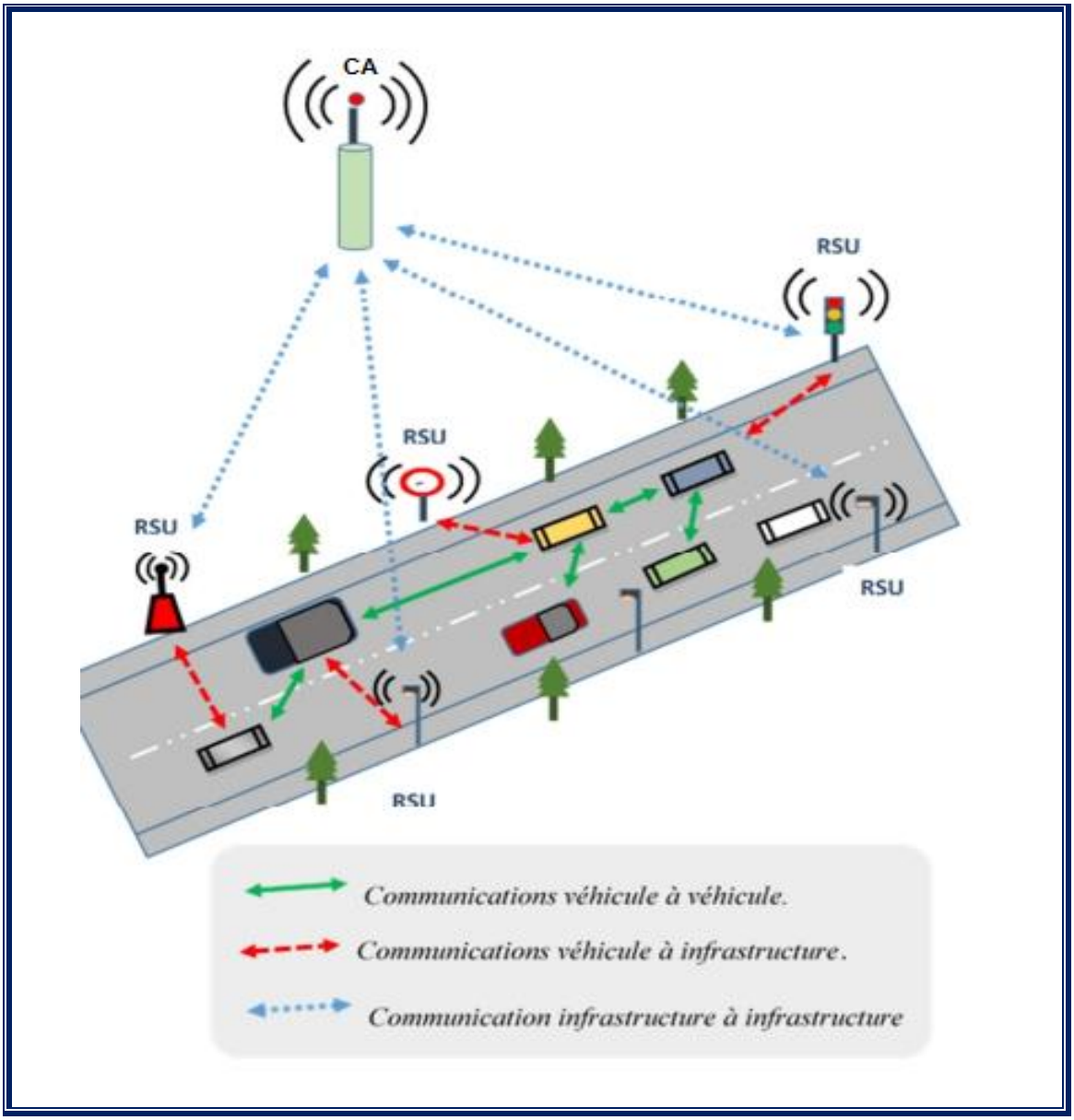


Fig. I. 5 : *Les entités communicantes dans les VANET.*

➢ CA (Certification Authority) :

Dite AC en français (Autorité de Certification). C'est une source d'authenticité de l'information. Elle assure la gestion et l'enregistrement de toutes les entités sur le réseau (RSU et OBU). La CA est sensée connaître toutes les vraies identités des véhicules et au besoin les divulguer pour les forces de l'ordre. Aussi, la CA dans certains travaux se charge de la délivrance et l'attribution des certificats et des pseudonymes de communications.

➢ RSU (Road Side Unit) :

Ces entités sont les subordonnés des CA. Ce sont des infrastructures installées au bord des routes qui peuvent être principalement des feux de signalisation, des lampadaires ou autres. Leur principale responsabilité est de soutenir la CA dans la gestion du trafic et des véhicules en diffusant les conditions du trafic, météorologiques ou spécifiques de la route (Vitesse maximale, autorisation de dépassement, etc.). Elles peuvent jouer aussi le rôle d'une station de base en relayant l'information envoyée par un véhicule. Les RSU représentent également des points d'accès au réseau.

➢ OBU (On-Board Unit) :

Les centrales de calcul qui dispose d'interfaces filaires et sans fil. Les véhicules intelligents, comme montré dans la figure *Fig. I.6*, sont des véhicules équipés d'une unité nommée On-Board Unit (OBU). Cette unité regroupe un ensemble de composants matériels et logiciels de hautes technologies (GPS, radar, caméras, différents capteurs et autres). Son rôle est d'assurer la localisation, la réception, le calcul, le stockage et l'envoi des données sur le réseau. Les équipements du véhicule forment un système de communication utilisant une technologie de communication nommée DSRC [4].

Les véhicules modernes sont équipés d'un ensemble de processeurs connectés à une plateforme de traitement des données.

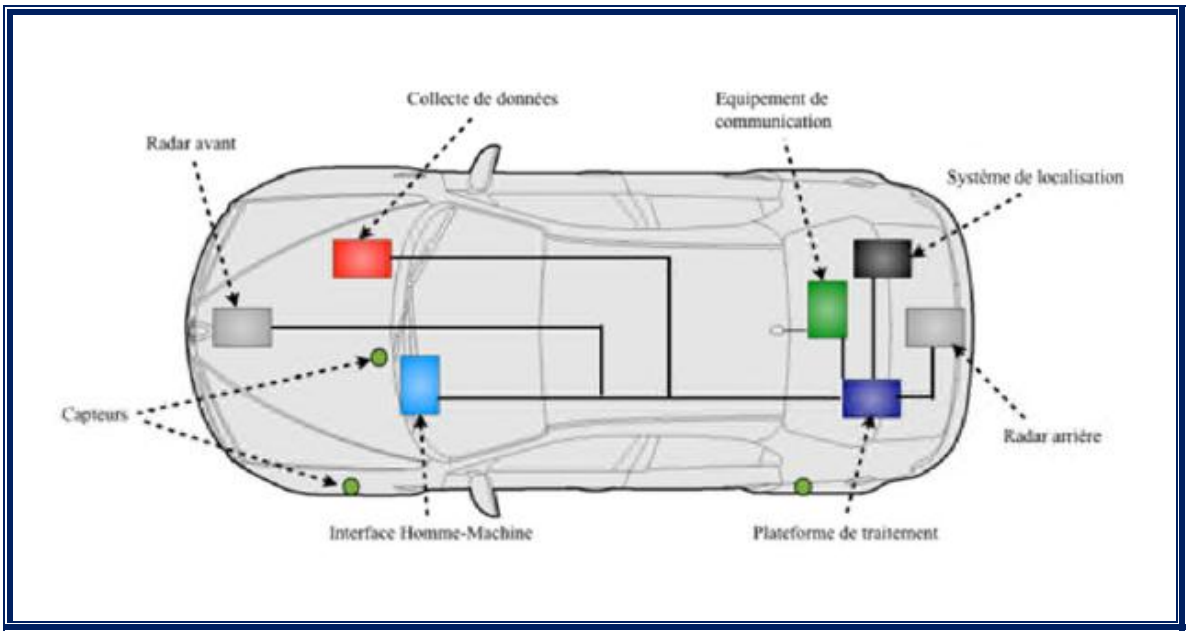


Fig. I. 6 : *Composants d'un véhicule intelligent.*

En plus de ces 3 principaux composants, se rajoutent deux autres équipements essentiels :

➢ L'équipement personnel :

Les équipements personnels sont les équipements qui peuvent être apportés par les utilisateurs à l'intérieur de leurs véhicules. Cela peut être un téléphone portable, un ordinateur portable ou encore un GPS autonome. Ces équipements peuvent interagir avec le véhicule. De nos jours, en activant l'interface Bluetooth du téléphone portable, on peut utiliser son téléphone portable par commande vocale (en utilisant les microphones intégrés au véhicule) ou par le biais de l'interface Homme-Machine (IHM) du véhicule. Voir la figure *Fig. I.7.*

Fig. I. 7 : *L'interface Homme-Machine d'un véhicule intelligent.*

➢ L'équipement central :

L'équipement central se situe du côté « serveur ». Il est transparent pour l'utilisateur. Cet équipement central pourra être un serveur de stockage, un point d'entrée à un réseau filaire (Internet) ou un serveur de transaction (Télépéage par exemple).

I.4.b. Les objectifs des VANET :

Les réseaux VANET sont basés sur la communication et l'échange d'information entre les véhicules, entre les véhicules et des éléments de la route (Exemples : les RSU, les panneaux de signalisations, les feux d'intersections, etc.) ou des éléments de réseaux externes (Satellites, antennes, internet), voir la figure *Fig. I.8* ci-dessous. Leurs deux principaux objectifs se résument en la sécurité et le confort des usagers.

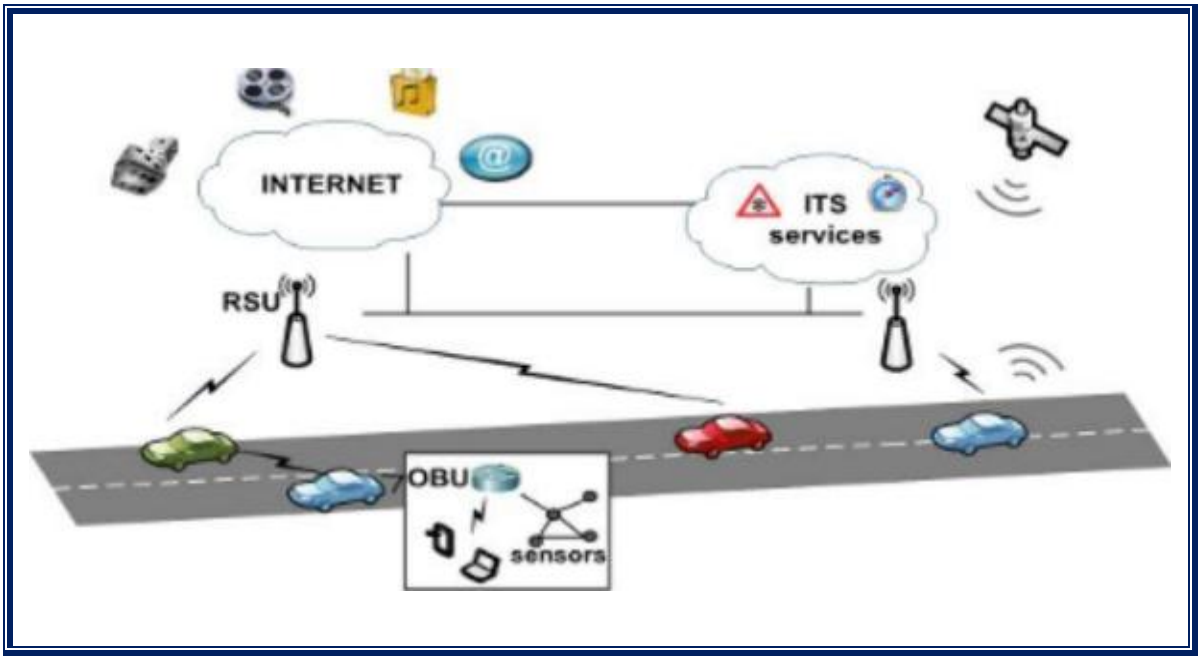


Fig. I. 8 : *L'objectif des VANET.*

➢ Sécurité des usagers :

- ✓ **Prévention sur les accidents :** Les accidents deviennent plus rapidement détectables et l'intervention devient plus rapide, cela peut minimiser le risque de décès après un accident.

- ✓ **Anticipation du trafic :** Les véhicules sont informés par les routes où il y'a des embouteillages, ils peuvent donc emprunter un autre chemin, cela peut permettre de rendre les routes plus fluides.

- ✓ **Préventions d'un véhicule prioritaire :** Permet d'aviser les conducteurs d'un passage de véhicules prioritaires (Exemple : ambulances, véhicules de police…).

- ✓ **Anticipation d'un danger quelconque :** Les véhicules peuvent s'échanger entre eux des préventions de dangers liés aux routes pour mieux les anticiper.

➢ Confort des usagers :

- ✓ Les réseaux VANET peuvent communiquer avec les infrastructures externes comme internet, donc la capacité d'accéder à des loisirs comme les téléchargements de flux multimédias, lecture des emails …etc.
- ✓ Possibilité de jouer en réseau entre les passagers des voitures, téléchargement et partage de fichier tel que les cartes.
- ✓ La régulation des flux de véhicules, permet de réduire le nombre d'embouteillages.
- ✓ Le guidage par GPS permettant un déplacement plus facile, et l'auto-localisation qui permet de trouver les véhicules volés.

I.5. Architectures des VANET :

Dans les réseaux VANET, on trouve principalement, les entités fixes qui constituent l'infrastructure (RSU et CA) et les entités mobiles (les véhicules). Pour pouvoir échanger les 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, on distingue trois types de communications : véhicule à véhicule (V2V), véhicule-infrastructure et la communication hybride qui combine entre les deux premières communications. Comme illustré dans la figure *Fig. I.9.*

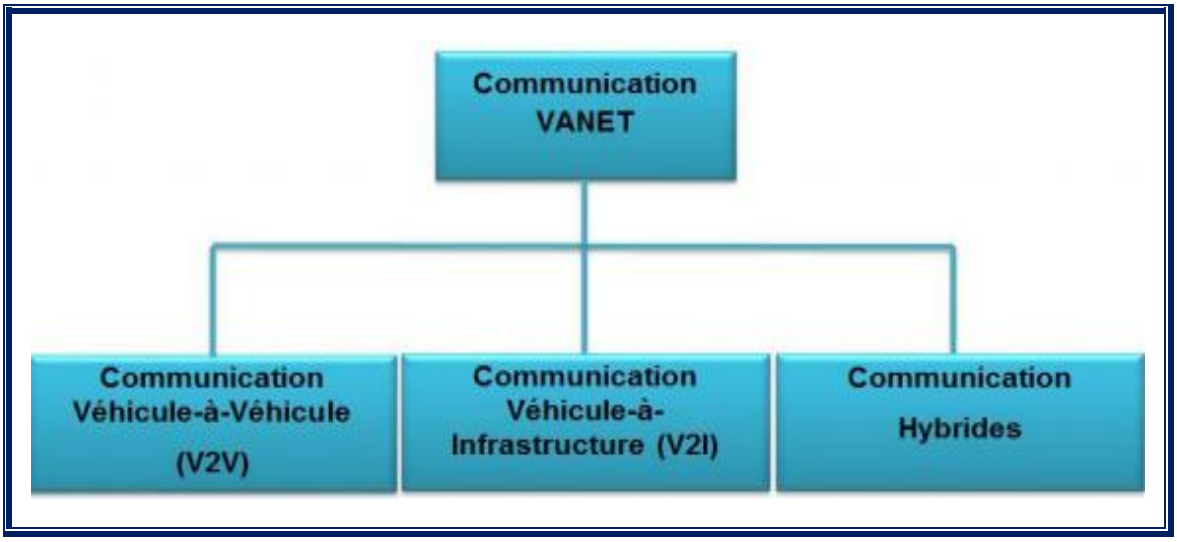


Fig. I. 9 : *Les déférents modes de communication dans les VANET.*

➢ Communication Véhicule à Véhicule :

L'architecture de communication inter-véhicules (V2V ou IVC pour Inter Vehicle Communication) est composée uniquement d'OBU (véhicules légers, poids lourds, véhicules de secours, etc.). Elles forment alors un réseau mobile sans avoir besoin d'un élément de coordination centralisé. Cette situation est plausible et essentielle si certains équipements RSU deviennent indisponibles (en panne ou hors de portée). Dans ce cas, le réseau doit continuer de fonctionner. Les véhicules doivent alors collaborer pour assurer la disponibilité du service. Ce mode de fonctionnement est communément appelé « ad hoc » et est utilisé par les VANET.

L'architecture V2V en mode ad hoc peut aussi être utilisée dans les scénarios de diffusion d'alerte (freinage d'urgence, collision, ralentissement, etc.) ou pour la conduite coopérative. En effet, dans le cadre d'applications de sécurité routière, les réseaux à infrastructure montrent leurs limites, surtout en terme de délai.

Prenons l'exemple d'un véhicule en difficulté sur la chaussée qui diffuse un message d'alerte. Il semble plus rapide d'envoyer l'information directement aux autres véhicules plutôt que de la faire transiter par une station de base. En effet, un véhicule peut communiquer directement avec un autre véhicule s'il se situe dans sa zone radio, ou bien par le biais d'un protocole multi-sauts qui se charge de transmettre les messages de bout en bout en utilisant les nœuds voisins qui les séparent comme des relais.

Une autre raison de l'existence de ce type d'architecture de communication vient du fait de la densité des réseaux routiers. En effet, le million de kilomètres d'une route particulière nécessitent, par exemple, un nombre important de RSU, ce qui entraine un cout financier non négligeable.

Même si les RSU sont déployées plus densément que prévu, elles ne seront pas toutes opérationnelles durant la phase de déploiement incrémental. Les communications V2V seront donc aussi utiles durant cette période d'installation. Nous comprenons ainsi que le V2V joue un rôle primordial afin d'assurer une disponibilité du service.

L'architecture V2V permet les communications critiques (alerte de danger local entre plusieurs véhicules proches, alerte d'un véhicule de secours se rapprochant, alerte de violation de feux tricolores).

Dans ce mode, les supports de communication utilisés sont caractérisés par une petite latence et un grand débit de transmission. Les communications V2V sont très efficaces pour le transfert des informations concernant les services liés à la sécurité routière, mais elles ne garantissent pas une connectivité permanente entre les véhicules. Voir la figure *Fig. I.10*.

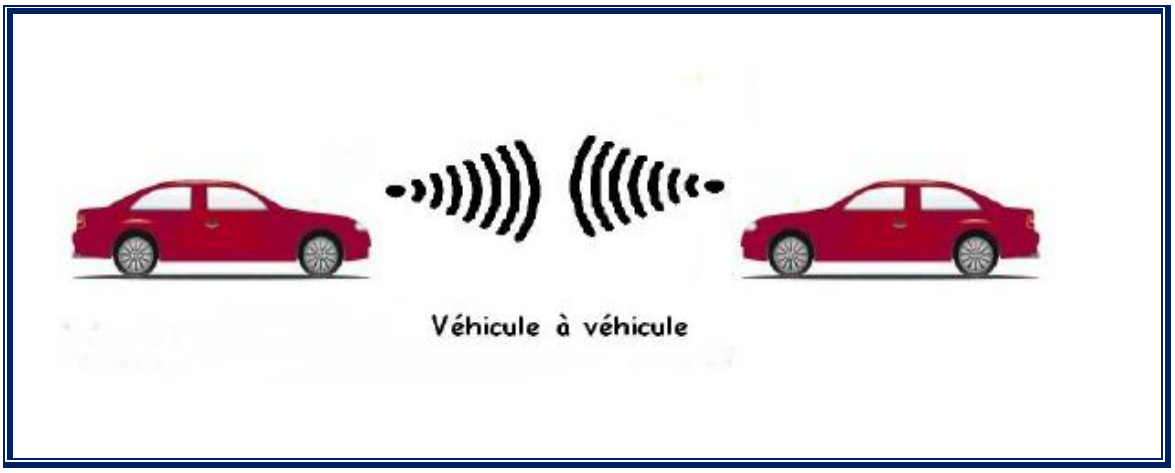


Fig. I. 10 : *Mode de communication V2V.*

➢ Mode de communication Véhicule Infrastructure :

Ce mode de communication permet une meilleure utilisation des ressources partagées et démultiplie les services fournis.

- ✓ L'architecture Véhicule-à-Infrastructure (V2I) est composée de RSU, auxquelles les véhicules accèdent pour les applications de sécurité, de gestion et de confort. Les RSU sont administrées par un ou plusieurs organismes publics ou bien par des opérateurs autoroutiers. Un véhicule qui informe le service de voirie au sujet d'un obstacle est un exemple de communication unidirectionnelle V2I, de l'OBU vers la RSU.

- ✓ L'architecture I2V dans le cas de communication Infrastructure-à-Véhicule. Un panneau de signalisation équipé d'une RSU qui envoie une information aux véhicules passant à proximité est un exemple de communication I2V.

Dans ce qui suit, par V2I, nous englobons toutes les communications Véhicule-Infrastructure, quelle que soit la direction du trafic de données. Voir la figure *Fig. I.11*.

Fig. I. 11 : *Mode de communication Véhicule-Infrastructure (V2I ou I2V).*

➢ Mode de communication hybride :

La combinaison de ces deux types d'architecture de communication permet d'obtenir une architecture hybride intéressante. En effet, les portées des infrastructures étant limitées, l'utilisation de véhicules comme relais permet d'étendre cette distance. Dans un but économique et en évitant de multiplier les bornes à chaque coin de rue, l'utilisation de sauts par véhicules intermédiaires prend toute son importance. Néanmoins, les communications inter-véhiculaires souffrent de problèmes de routage lors de transmission longue distance. Dans de telles situations, l'accès à une infrastructure peut améliorer les performances réseaux. Nous comprenons donc la complémentarité des deux types de communication et l'intérêt d'une architecture hybride. Voir la figure *Fig. I.12*.

Fig. I. 12 : *Mode de communication hybride.*

Un cas particulier de l'architecture hybride est le réseau VSN (Vehicular Sensor Network). En effet, ce type de réseau émerge en tant que nouvelle architecture de réseaux de véhicules. Le VSN a pour objectif la collecte et la diffusion proactive en temps réel des données relatives à l'environnement dans lequel évoluent les véhicules, et ce, plus particulièrement en zone urbaine. En effet, les voitures sont munies de plus en plus de capteurs de toutes catégories (caméras, capteurs de pollution, capteurs de pluie, capteurs d'état des pneumatiques, ESP, ABS, géolocalisation satellite, etc.).

Les informations délivrées par ces équipements peuvent être utiles pour l'obtention d'états sur le trafic routier (embouteillages, ralentissements, vitesse moyenne du trafic, etc.), sur les places de parking disponibles, pour des informations plus générales telles que la consommation moyenne de carburant et le taux de pollution, ou encore pour des applications de surveillance (grâce aux caméras embarquées sur des véhicules).

I.6. Caractéristiques des VANET :

Les VANET sont une catégorie des MANET permettant la communication entre les véhicules. En plus des caractéristiques des réseaux ad hoc mobiles classiques, les VANET ont la particularité d'avoir une très grande mobilité (les nœuds mobiles circulent à très grande vitesse). La topologie dynamique provoque de nombreuses reconfigurations (mise à jour des tables de routage, etc.), et soulève par conséquent des problèmes de performances. Après cet aperçu, nous détaillons, dans cette section, les caractéristiques des VANET.

➢ Capacité et autonomie d'énergie :

À la différence des réseaux sans fil traditionnels où la contrainte d'énergie représente un facteur limitant important, les réseaux véhiculaires sans fil disposent d'une source énergétique importante grâce au système d'alimentation véhiculaire, qui se renouvèle dans le temps, ce qui implique que ce type de réseau ne souffre pas de problème d'énergie.

➢ Environnement de communication :

Contrairement aux environnements des réseaux Ad-hoc mobiles qui sont souvent stables et limités en espace (Bâtiment, aéroport ou aérogare et centre commercial). Les réseaux VANET sont caractérisés par la grande diversité de leurs environnements qui sont déployés dans la nature à grande échelle. Passant du milieu urbain qui présente différents obstacles (immeubles) qui peuvent réduire la qualité de transmission radio, à un environnement autoroutier affecté principalement par les très grandes vitesses des véhicules.

➢ Topologie et connectivité :

Les réseaux VANET sont caractérisés par une connectivité irrégulière et relativement faible, liée directement à la vitesse des véhicules, leurs déplacements aléatoires et leurs comportements face à des obstacles, qui peuvent réduire considérablement les durées des

communications. En effet, un véhicule peut rapidement rejoindre ou quitter un groupe de véhicules, ce qui rend les changements de topologie très fréquents et très dynamiques, constitués de plusieurs groupes séparés, ceci entraîne une réorganisation de la topologie du réseau [5].

➢ Modèle de mobilité :

Le modèle de mobilité des réseaux VANET est lié à la diversité environnementale et les infrastructures routières. Mais dans une certaine mesure, il est possible de prévoir l'évolution des déplacements des véhicules grâce à leurs vitesses, leurs directions et surtout la connaissance des cartes routières. Car les déplacements des véhicules sont structurés par les routes et les rues.

Le mode de mobilité des réseaux VANET est affecté par la vitesse des véhicules et leurs déplacements aléatoires, qui peuvent réduire considérablement les durées de communications et leurs comportements face à des obstacles.

➢ Modèle de communication :

Les réseaux véhiculaires ont été imaginés principalement pour les applications liées à la sécurité routière (Ex. diffusion de messages d'alerte). Dans ce type d'application, les communications se font presque exclusivement par reliages successifs d'une source vers une multiplicité de destinataires. Le modèle de transmission en Broadcast ou en Multicast est donc appelé à dominer largement dans les réseaux véhiculaires, ce qui n'est par exemple pas sans conséquence sur la charge du réseau et le modèle de sécurité à mettre en œuvre [6].

➢ Technologies de communications :

Pour mettre en place les différentes communications entre les entités du réseau VANET, diverses technologies ont été conçues, pour offrir les différents services et augmenter la portée des communications et des bandes passantes. Ainsi, une norme de communication appelée DSRC a été adoptée. Sa couche physique est basée sur la norme IEEE 802.11a.

Plus tard, L'IEEE s'inspira de cette norme pour créer la norme actuellement utilisée 802.11p. Cette norme définit essentiellement les services de sécurité et le format des messages [5].

➢ Taille du réseau :

Etant donné les avancées importantes réalisées dans le domaine des communications sans fil et les bas coûts des équipements associés, les véhicules qui intègrent déjà massivement des systèmes GPS et des équipements Bluetooth, seront très probablement équipés et ce, tout aussi massivement, de plateformes de communication leur permettant de constituer de véritables réseaux [6].

Ce faisant, et compte tenu de l'importance sans cesse grandissante de la densité et du parc des véhicules, on peut s'attendre à ce que la taille des réseaux véhiculaires dont les déploiements restent encore très confidentiels, soit d'une tout autre ampleur. L'importance potentielle de la taille des réseaux véhiculaires constitue donc une caractéristique majeure à prendre en compte dans la conception de ces réseaux.

I.7. Type d'applications dans les VANET :

Après avoir présenté l'utilité des réseaux sans fil véhiculaires, nous détaillons les applications qui peuvent être déployées sur ce type de réseau. Un consortium d'industriels (General Motors, Daimler Chrysler, Toyota, Nissan, Volkswagen, Ford, BMW) a établi un rapport qui fait actuellement autorité, et qui liste plusieurs types d'applications [2]. Nous pouvons distinguer trois classes d'applications : le confort, la gestion et la sécurité du trafic routier. Voir la figure *Fig. I.13*.

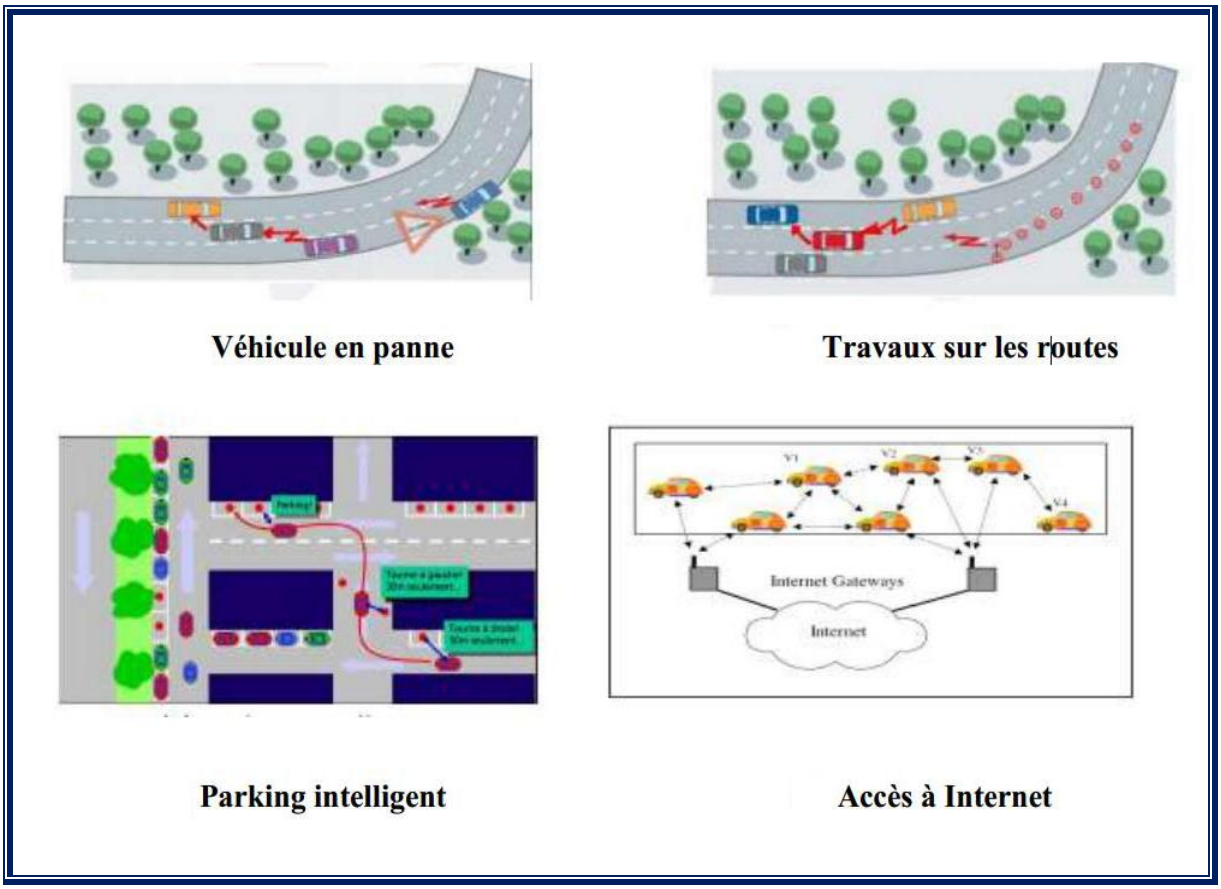


Fig. I. 13 : *Applications des réseaux de véhicules.*

➢ Applications liées au confort :

Comme certains voyages peuvent parfois être longs, dû au trajet et/ou aux congestions sur la route, les réseaux VANET contribuent à l'amélioration du confort du conducteur de véhicule en l'occupant durant ses voyages, ces services comprennent entre autres les panneaux d'annonces locales : d'ordre commercial comme les offres de restaurants, la

présence de stations-service à proximité, ou culturel comme des informations touristiques relatives à la localisation du véhicule , il y a aussi l'accès à Internet qui permet aux passagers de s'échanger des musiques, vidéos ou d'accéder à des jeux comme illustré dans la figure *Fig. I.14*.

On pourra également procéder à la vérification à distance des permis de conduire, des plaques d'immatriculation par les autorités compétentes (police, douane, gendarmerie), le paiement électronique au niveau des points de péage et dans les stations-service (ce qui peut faciliter la vie des handicapés).

A tous ces services s'ajoutent aussi le chat inter-véhicule qui représente une communication point à point entre deux conducteurs qui voyagent ensemble ainsi ils peuvent s'échanger des messages ou partager des données (vidéos, musique, itinéraire, jeux en réseau).

Fig. I. 14 : *Les systèmes embarqués contribuant au confort du conducteur.*

➢ Applications d'optimisation et d'amélioration du trafic routier :

Outre les services liés aux applications de confort, les réseaux sans fil véhiculaires contribuent également à l'optimisation et à l'amélioration du trafic routier en fournissant des informations sur l'état des routes. En effet, un véhicule peut être informé sur l'état de la circulation de son trajet actuel ou futur à partir des messages échangés par les différentes entités du réseau, ce qui donne la possibilité au conducteur de décider quelle route il peut suivre lorsque le trafic est dense sur un trajet et éviter ainsi la congestion. De plus et grâce à l'échange des informations entre les véhicules, il y aura la possibilité de créer le passage pour les voitures d'urgence, ou de proposer d'autres itinéraires aux véhicules qui sont dans une zone de congestion dans le but d'optimiser le trafic et de le rendre fluide. Voir la figure *Fig. I.15.*

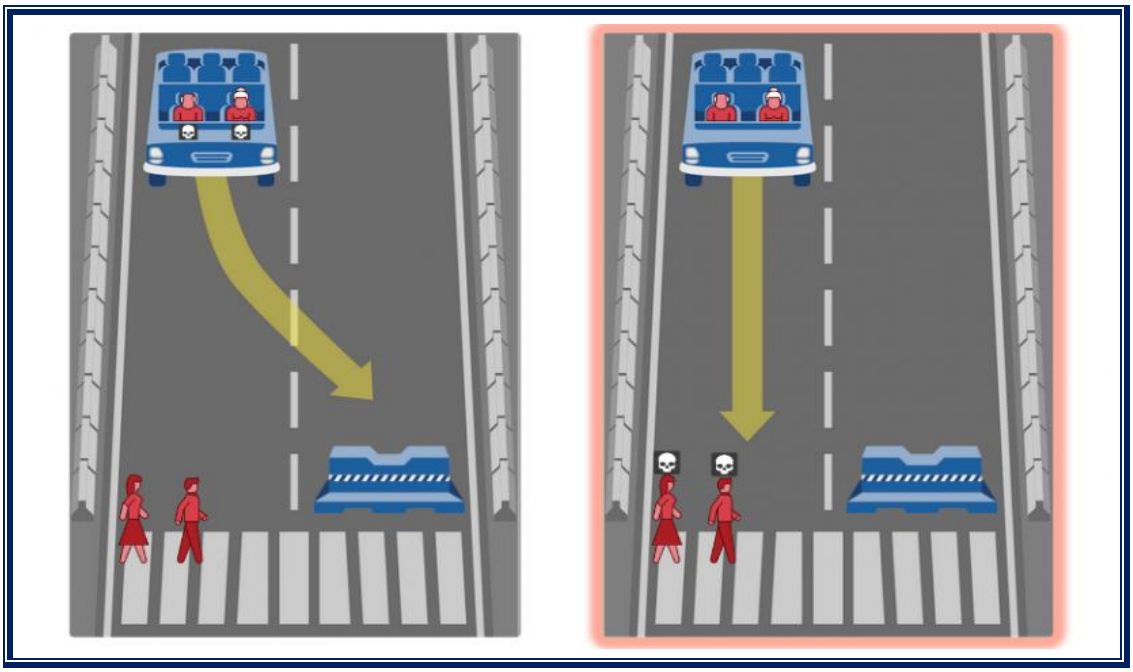


Fig. I. 15 : *Optimisation du trafic routier.*

➢ Applications de prévention et de sécurité du trafic routier :

Comme les applications de préventions et de sécurité du trafic routier ont un impact direct sur la sécurité des personnes et des biens, les conducteurs peuvent être avertis des accidents ou autres situations dangereuses (alerte pour les travaux routiers, informations météorologiques) en recevant des messages d'alerte diffusés entre les différentes entités afin d'être plus vigilant et de réduire leur vitesse comme illustré sur la figure *Fig. I.16*. Comme ces applications contribuent à la diminution du nombre d'accidents sur les routes alors elles aident à préserver la vie humaine.

Un service de ces applications qui est un service SOS est déjà déployé dans les véhicules haut de gamme. En cas d'accident, lors du déclenchement de l'airbag (c'est-à-dire dans les dix millisecondes qui suivent la collision), un message est émis afin de prévenir le centre de secours le plus proche. Ce service permet d'économiser de précieuses minutes dans le processus d'arrivée des secours.

Dans cette catégorie, on retrouve les applications qui utilisent les informations des autres véhicules : l'alerte d'état de la route (verglas, obstacle), l'aide au dépassement (calcul des distances, vérification de l'angle mort), l'alerte de freinage ou de collision en amont du trajet. On remarque donc que les applications de sécurité du trafic routier ont un rôle majeur dans la réduction du nombre d'accidents. On remarque aussi que cette catégorie d'applications a des contraintes temporelles fortes. En effet, si l'alerte de danger arrive trop tard, alors le conducteur ne pourra pas anticiper. Nous perdons ainsi les bénéfices de telles applications.

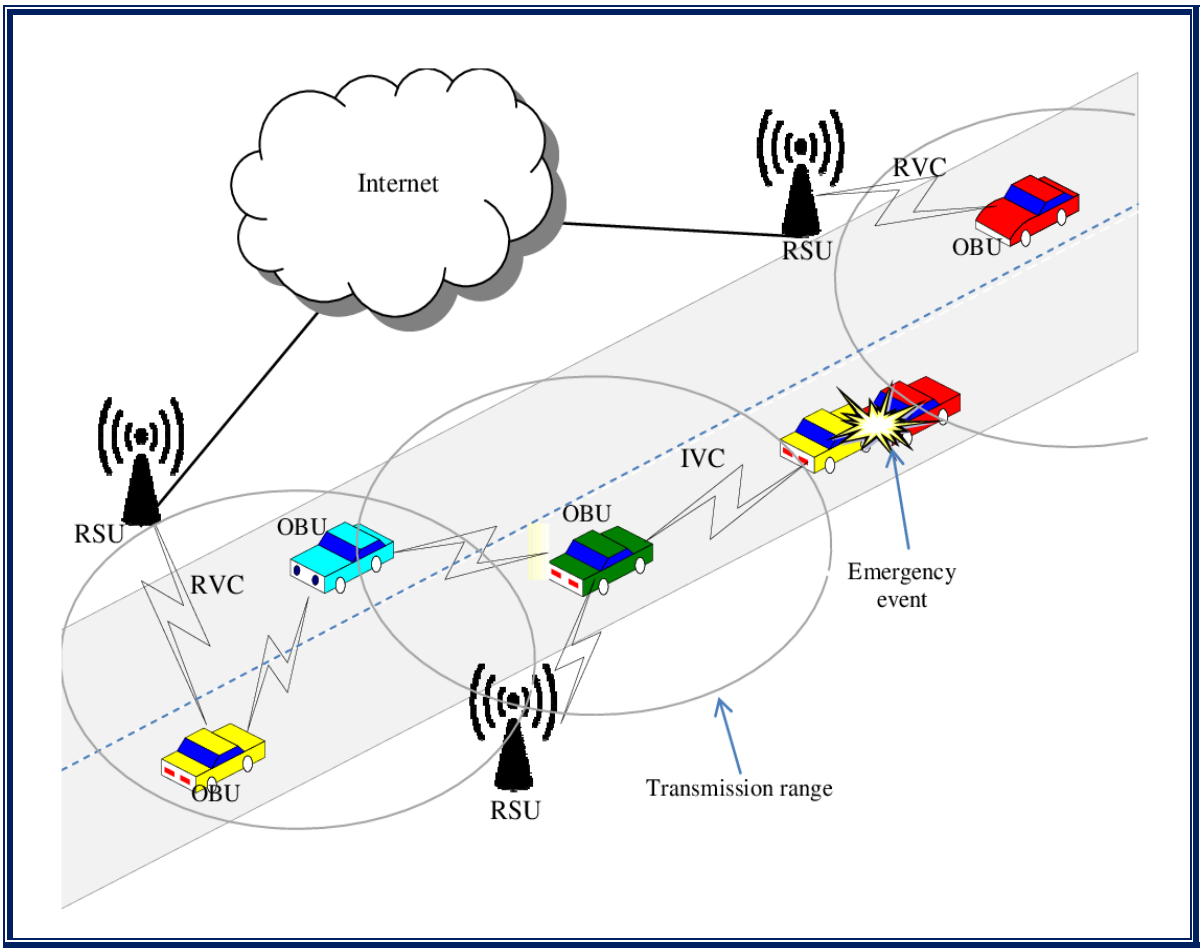


Fig. I. 16 : *Prévention et amélioration de la sécurité routière.*

I.8. Conclusion :

Les VANET sont une particularité des réseaux MANET où les nœuds mobiles sont des véhicules (intelligents) équipés de calculateurs. Grâce à la technologie des ITS, nos véhicules vont embarquer des applications ayant pour but l´échange de messages vitaux avec les unités de l'infrastructure routière afin d'assurer la sécurité des usagers de la route. Comme il sera possible, aussi et à partir de son véhicule, de consommer des services sur Internet ou sur le Cloud.

Dans ce chapitre, nous avons défini, en premier lieu, les réseaux sans fil ainsi que leur architecture, ensuite nous avons présenté les réseaux véhiculaires VANET et nous avons décrit les entités présentes dans un réseau sans fil véhiculaire ainsi que leurs rôles, et puis leurs principaux objectifs. Nous avons notamment vu l'architecture et les composants essentiels des VANET ainsi que les différents modes de communication existants.

Par la suite, afin de mieux comprendre les réseaux sans fil véhiculaires, nous avons détaillé leurs caractéristiques et identifié les applications déplorables dans un réseau sans fil véhiculaire, et les avons classés en catégories.

Dans ce qui suit, nous allons parler de l'impact des réseaux Ad hoc véhiculaires « VANET » sur la prévention et l'amélioration de la sécurité routière.

Chapitre II :

Amélioration de la sécurité routière grâce aux réseaux véhiculaires.

II.1. Introduction :

Au cours de ces dernières années, les progrès des communications sans fil ont ouvert de nouveaux domaines de recherche, offrant une connectivité réseau dans des environnements où les solutions câblées ne sont pas possibles. Parmi ceux-ci, les réseaux ad hoc de véhicules (VANET) qui attirent de plus en plus l'attention en raison des diverses applications importantes pour le trafic, contrôle et amusement pour les passagers. Les villes intelligentes aimeraient planifier comment minimiser leurs problèmes de transport en raison de l'augmentation de la population qui produit des routes encombrées. Les VANET facilitent la résolution de ce problème en améliorant la mobilité des véhicules, en augmentant la sécurité routière et en cherchant également à avoir des villes plus durables.

Au début du développement des technologies véhiculaires, l'objectif principal était d'avoir des routes plus efficaces et plus sûres. De nos jours, en raison du développement massif des technologies sans fil et de leur application dans les véhicules, il est possible d'utiliser le système de transport intelligent (STI) qui changera notre façon de conduire, améliorera la sécurité routière et facilitera les services d'urgence.

Les VANET permettent aux véhicules de communiquer facilement entre eux et également avec des infrastructures fixes. Cela améliorera non seulement la sécurité routière, mais augmentera également de nouvelles opportunités commerciales telles que l'info-divertissement pour les passagers.

II.2. Les systèmes de transport intelligents :

Le système de transport intelligent (STI, ou "Intelligent Transport System", ITS) est un nouveau type d'application des technologies de l'information et de la communication (TIC), basé sur la communication inter-véhicules (IVC). Les véhicules compatibles IVC fournissent des informations actualisées sur les conditions de la circulation. Les STI peuvent être utilisés pour minimiser les accidents de la route, la congestion et améliorer l'efficacité du trafic. Ils jouent un rôle important dans l'économie d'un pays en réduisant la consommation de carburant et la gestion efficace du temps des individus. Les stations de système de transport intelligent (ITS-Ss) avec la disposition de la communication sans fil est un nouveau domaine de recherche en croissance pour réduire les accidents de la route, la congestion et améliorer l'efficacité du trafic.

Le réseau ad hoc véhiculaire (VANET) est une composante importante des STI. VANET utilise les mécanismes STI pour fournir des informations fiables sur l'emplacement, la vitesse, le cap et les conditions routières du véhicule. L'augmentation de la population et le manque de gravité de la conduite entraînent des embouteillages, des accidents de la route et des retards inutiles dans les déplacements.

La figure *Fig. II.1* montre l'un des scénarios de non-gravité au volant. Pour le mieux-être de la société, il devrait y avoir une utilisation positive de la technologie dans les systèmes de transport pour réduire les encombrements, les accidents, et améliorer la sécurité routière et l'efficacité du trafic.

Fig. II. 1 : *Scénario sans système de transport intelligent.*

Les systèmes de transport intelligents sont utilisés depuis plus de 20 ans, ils progressent rapidement sur le marché et devraient probablement équiper une plus grande proportion du parc de véhicules dans les 10 à 15 prochaines années [7]. Les STI recouvrent l'application de l'électronique, de l'informatique et des technologies de communication aux véhicules et aux routes, ils désignent les nouvelles technologies appliquées aux réseaux de transport pour améliorer la conduite, la gestion et l'exploitation ainsi que pour apporter de nouveaux services aux utilisateurs.

De nombreux systèmes encouragent l'utilisation de moyens de transports multimodaux et réduisent le temps passé sur la route, réduisant ainsi le nombre et la gravité des collisions, les encombrements et la pollution. Voir la figure *Fig. II.2*.

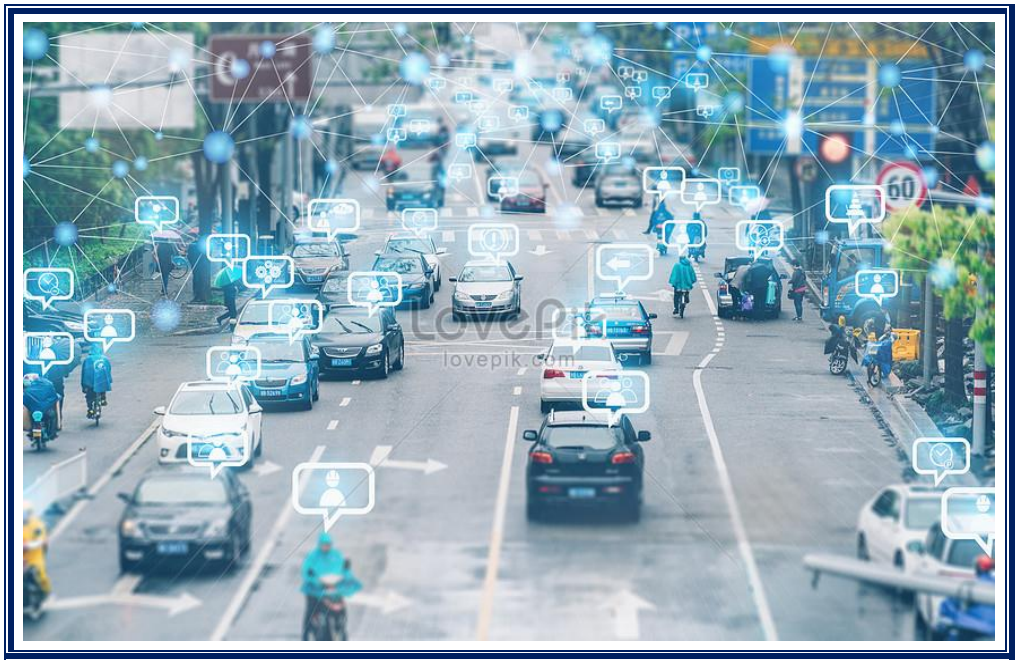


Fig. II. 2 : *Scénario avec système de transport intelligent.*

Il est probable qu'une plus grande pénétration des STI contribuera à améliorer l'attractivité des véhicules par rapport aux transports en commun, par exemple, ce qui aurait un impact négatif sur la sécurité en raison du transfert modal opéré (plus de véhicules en circulation => nombre d'accidents accru). Certains systèmes peuvent également avoir une incidence négative sur certains aspects du comportement des conducteurs par une adaptation comportementale.

Les administrations routières devront continuer de déployer leurs propres systèmes STI sur les réseaux routiers. Il est primordial que les systèmes, là où les administrations routières sont les principales responsables, soient déployés de manière coordonnée par lesdites administrations. Cette nécessité souligne le besoin, au moins sur un plan général, en stratégies et en visions communes.

Le déploiement de systèmes de transport intelligents, s'accroît rapidement à travers le monde. Ces systèmes sont déployés et installés à bord des véhicules et intégrés aux infrastructures routières. Nombre d'entre eux sont des systèmes associés qui utilisent une technologie embarquée et une technologie déployée en bord de route ou sur la route.

Certains de ces systèmes fonctionnent déjà depuis plusieurs années dans de nombreux pays, tandis que d'autres sont encore en voie de développement. C'est pourquoi certains présentent des résultats bien documentés et d'autres seulement des résultats théoriques, souvent fondés sur des essais de simulation.

Les STI et les technologies connexes ont largement été acceptés par les secteurs publics et privés comme une manière avancée d'atteindre un objectif de mobilité durable tout en améliorant la qualité de vie.

Les STI répondent aux problématiques de sécurité routière et de congestion du trafic. Ils fournissent aussi une assistance évoluée prenant en compte l'environnement et les risques sur les routes. Ils peuvent sauver des vies et permettre d'économiser du temps et de l'argent, tout en contribuant à réduire les menaces qui pèsent sur notre environnement. Les systèmes de transport intelligents proposent des solutions intéressantes pour :

- Réaliser une gestion du trafic à partir de données dynamiques pour diminuer les congestions.

- Etablir un système de gestion de la circulation qui permet l'intervention rapide en cas d'incidents.

- Réduire le temps de déplacement (Travel Time) sans modifier ni le chemin ni les moyens utilisés.

II.3. Objectifs et avantages des STI :

On fait souvent la différence entre un système de transport intelligent et un service de transport intelligent : les systèmes sont utilisés par des gestionnaires, opérateurs ou entreprises de transports, et sont donc transparents pour les usagers, alors que les services de transports intelligents sont destinés directement aux usagers en leur permettant d'adapter leurs comportements (de choix modal, d'itinéraire, de conduite) à l'information qu'ils reçoivent.

II.3.a. Les objectifs des STI :

Les STI sont adressés aux utilisateurs, qu'ils soient usagers de transports, gestionnaires, ou autorités organisatrices de transports afin de leur proposer différents services. Ces derniers sont illustrés en figure *Fig. II.3.*

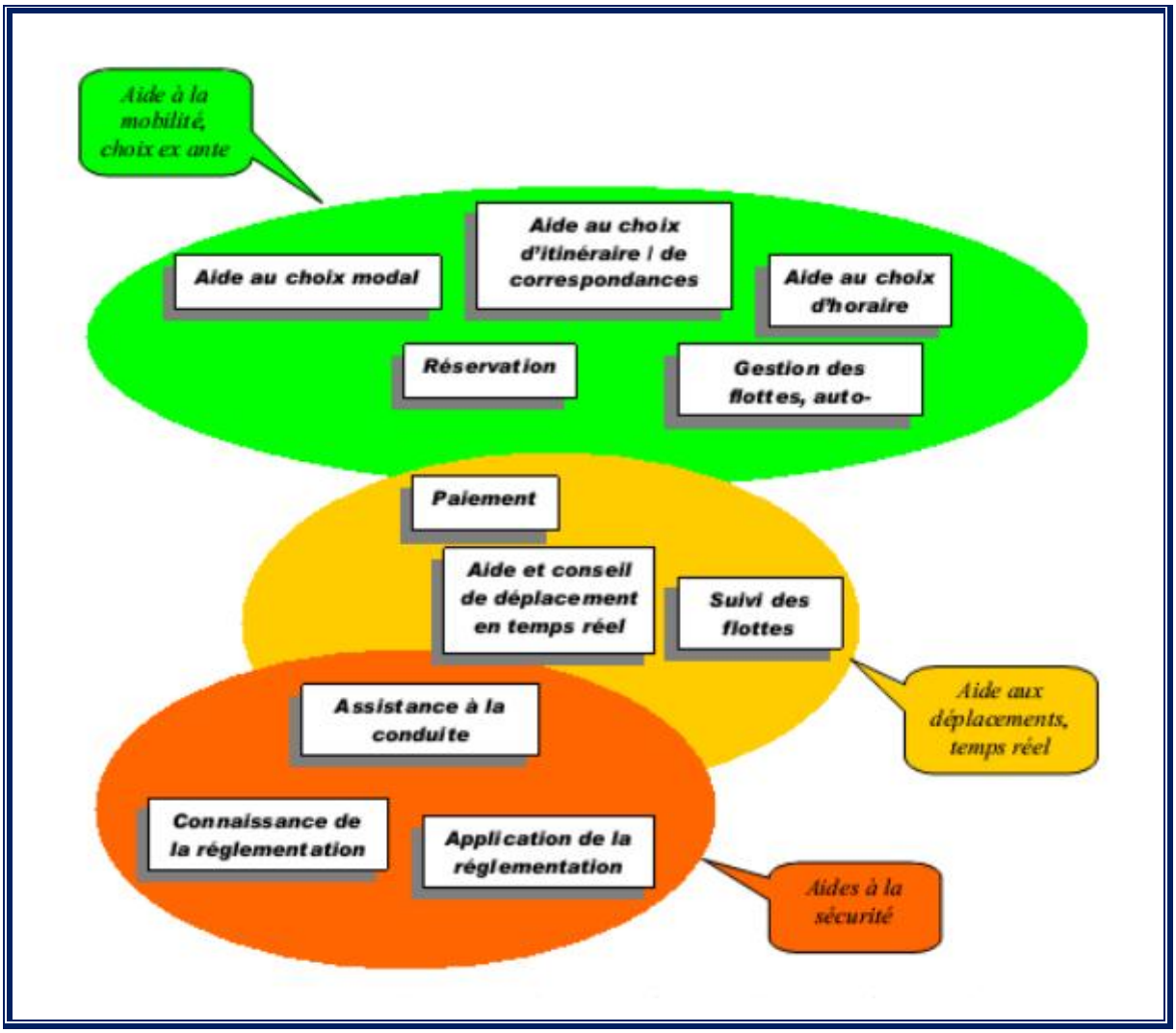


Fig. II. 3 : *Présentation schématique des STI en fonction du service fourni à l'usager.*

On y ajoute également :

- L'amélioration de l'efficacité énergétique des transports.
- Le développement durable ou la diminution de la pollution et la maîtrise de la mobilité.
- Le développement des services et des enjeux industriels et commerciaux.

II.3.b. Les avantages tirés de quelques projets STI :

Améliorer les temps de parcours, réduire la congestion, augmenter la sécurité, diminuer les nuisances environnementales et bien plusieurs autres objectifs de la politique publique sont atteints directement ou indirectement grâce aux STI et leurs services rendus aux utilisateurs. Dans ce qui suit, on montre un certain nombre des avantages tirés des projets STI mis en œuvre au Canada, aux États-Unis, en Europe et au Japon.

➢ Transports plus fiables :

Grâce aux projets STI, la ponctualité du transport en commun a passé de 12 à 23% ; ce qui implique la réduction des délais d'attente des passagers jusqu'à 50%. Par exemple, la ponctualité des autobus urbains de Kanas City (Missouri) a été améliorée de 12%, ce qui a conduit à la réduction de ses parcs d'autobus de 9% [8].

Les systèmes de paiement électronique mise en place ont marqué un gain de 90% que d'habitude. Ils ont augmenté la perception du péage de 3 à 30% [8].

➢ Productivité économique améliorée :

Les exploitants de véhicules commerciaux canadiens estiment l'économie de 55 millions de dollars annuellement, et la génération de 20 millions de dollars en exportations par année depuis 1993 grâce à l'utilisation du système COMPAS (système de gestion de la circulation autoroutière). Alors que, le département américain des transports estime que l'utilisation des STI permet aux fournisseurs d'économiser 35% des investissements d'infrastructure et la réduction de 25% des coûts de cycle de vie du réseau de transport pour la prochaine décade, soit 30 milliards de dollars [8].

➢ Amélioration de la sécurité :

L'utilisation du système de trafic routier COMPAS à Toronto, sur certaines sections de l'autoroute 401, a enregistré une réduction de la durée des incidents entre le moment où ils surviennent et celui où ils sont éliminés de 86 à 30 minutes, une diminution du retard moyen par incidents de 537 véhicules-heures, une prédiction d'environ 200 accidents par année due à l'affichage de messages d'incident au moment où ceux-ci surviennent, entraînant des économies de 10 millions de dollars [8].

L'expérience aux États-Unis révèle une réduction du nombre d'accidents allant de 15 à 62%. Plus précisément, le projet FAST-TRAC à Oakland (Michigan) a entraîné une réduction de 89% des accidents de virage à gauche, une réduction de 27% du nombre total de blessures et une réduction de 100% des blessures graves [8].

Le projet Guidestar TMS à Minneapolis a permis une réduction de 25% des accidents, une augmentation de 35% de la vitesse moyenne à l'heure de pointe et un accroissement de la capacité routière de 22% [8].

Le comté de Fulton (Géorgie) a réduit le délai moyen d'intervention en cas d'incendie de 7,5 à 4,5 minutes [8].

➢ Économie de temps et gains d'efficacité opérationnelle :

Réduction de délais globaux de 5,3 millions de véhicules-heures par année et la consommation de carburant de 11,3 millions de litres par année grâce à l'utilisation du système COMPAS [8].

Au Japon, ils ont prouvé que l'application des STI permet une diminution de la consommation annuelle de carburant et qui peut arriver jusqu'à 11% annuellement [8].

A Indiana, ils ont enregistré un gain de 14 millions $US par année en coût d'exploitation et équipement dû à la régulation assistée par ordinateur pour les chasse-neiges [8].

En Oklahoma, ils ont révélé une réduction des coûts d'exploitation à chaque poste de péage de 176 000 $ à 16 000 $ par année en utilisant le système de perception électronique du péage (PIKEPASS) [8].

A New York, le temps d'attente des véhicules dans les voies de péage a passé de 15 minutes à moins de 30 secondes depuis l'utilisation de système de péage E-Z pass [8].

➢ Réduction des effets sur l'environnement :

Des émissions de gaz à effet de serre de 3100 tonnes par année grâce à l'utilisation du système de gestion routier COMPAS [8].

Une récente étude commandée par la table des transports, dans le cadre du processus national sur le changement climatique du Canada, sur les effets de sept applications STI sur les émissions de gaz à effet de serre, a estimé la réduction annuelle de ces émissions en 2010 à 763 milliers de tonnes. Cette réduction représente 0,5 pour cent des émissions totales de gaz à effet de serre attribuable au transport en 1995. Les réductions connexes dans la consommation de carburant sont estimées à près de 300 millions de litres [8].

➢ Réduction des accidents en zone rurale :

À l'aide des services 911 et autres services de gestion des véhicules d'urgence, des systèmes anticollisions, des fonctions de prévisions météo, etc. [8].

➢ Réduction du fardeau administratif et des coûts d'exploitation :

Grâce à l'amélioration de l'efficacité des systèmes au moyen de fonctions automatisées et de transactions électroniques.

➢ Amélioration de la surveillance et de la gestion des flux de trafic et des incidents reliés au transport des marchandises dangereuses.

II.4. Types des technologies ITS :

Les systèmes de transport intelligents sont divisés en trois catégories différentes :

II.4.a. Les systèmes installés au niveau de l'infrastructure :

Les systèmes implantés uniquement sur l'infrastructure se composent essentiellement de : capteurs en bord de route qui recueillent les informations, et d'un équipement en bord de route qui émet des alertes et des conseils. Les avantages de ces systèmes résident dans la détection de phénomènes qui échappent aux capteurs embarqués à bord des véhicules comme les conditions météorologiques, les obstacles ou le trafic au-delà d'une courbe ou à une certaine distance. Des données variables peuvent être fournies sur des panneaux au bord de la route et l'information peut être transmise à tous les véhicules à proximité potentiellement affectés. Parmi, les applications de ce type de système, nous citons les suivantes :

➢ Application automatisée du code de la route :

Détection et enregistrement automatiques à l'aide de caméras et de capteurs des infractions au code de la route telles que :

- ✓ Le dépassement des limitations de vitesse.
- ✓ Le non-respect des feux rouges.
- ✓ Une combinaison du dépassement des limitations de vitesse et du non-respect des feux.
- ✓ Le contrôle des distances de sécurité dans les tunnels.
- ✓ Les heures de conduites des chauffeurs routiers.
- ✓ Les véhicules non immatriculés.
- ✓ Les véhicules non assurés.
- ✓ Les véhicules dont le propriétaire n'a pas réglé une amende.

Parmi les autres solutions à base de caméras qu'il est possible de mettre en œuvre, citons, le contrôle de l'accès des véhicules, la détection des infractions liées aux zones restreintes (dépassement de la hauteur ou du poids limite autorisés), les infractions des véhicules en mouvement, les conseils afférents au retardement d'un déplacement, les outils de classification des véhicules, etc.

Des photos sont prises automatiquement des véhicules / conducteurs qui enfreignent les règles et une amende est adressée aux propriétaires / conducteurs.

➢ Gestion dynamique du trafic et avertisseurs de danger locaux :

Ceci comprend :

- ✓ La gestion dynamique du trafic.
- ✓ Les panneaux à messages variables.
- ✓ Les signalisations électroniques de limites de vitesse variables.
- ✓ Le contrôle et les signaux des rampes d'accès.
- ✓ Le contrôle des ponts et des tunnels.

Les systèmes de gestion dynamique du trafic et avertisseurs de dangers locaux servent à accroître la sécurité et le flux du trafic en cas de perturbations provoquées par des incidents, des encombrements et une météo défavorable. Le système donne des informations aux conducteurs sur la vitesse, l'utilisation des voies, le choix d'itinéraire, les opérations de jonction, etc. à l'aide de panneaux à messages variables (PMV), afin d'améliorer la sécurité et l'utilisation du réseau. Voir la figure *Fig. II.4* ci-dessous.

Fig. II. 4 : *Panneau à messages variables (PVM).*

Les systèmes sont exploités de manière automatique, semi-automatique ou manuelle à partir de centres de contrôle du trafic qui s'appuient sur des systèmes de surveillance fixes ou des capteurs mobiles disposés sur place. Il existe trois catégories de PMV en fonction des types de messages communiqués : Les « messages à caractère réglementaire », les « messages d'avertissement de danger » et les « messages informatifs ».

Les systèmes de gestion dynamique du trafic utilisent généralement des messages à caractère réglementaire, accompagnés parfois de messages d'avertissement de danger et de messages informatifs. Les utilisations dans les cas d'autoroutes de liaison, les situations de réseau et de modification d'itinéraire sont également considérées comme des domaines distincts sur le plan fonctionnel.

➢ Contrôle de signalisation aux intersections :

Il consiste à contrôler les mouvements de circulation d'une intersection par le biais de signaux lumineux, réglés en vertu de séquences fixes de durée déterminée ou de manière automatique en fonction des besoins réels, contrôlés par des capteurs. Cette approche comprend également le contrôle d'intersections signalisées au sein d'un réseau (contrôle du réseau de signalisation) afin d'optimiser les performances du réseau en fonction de certains critères et d'installations de contrôle de la signalisation routière évolutives. Voir la figure *Fig. II.5*.

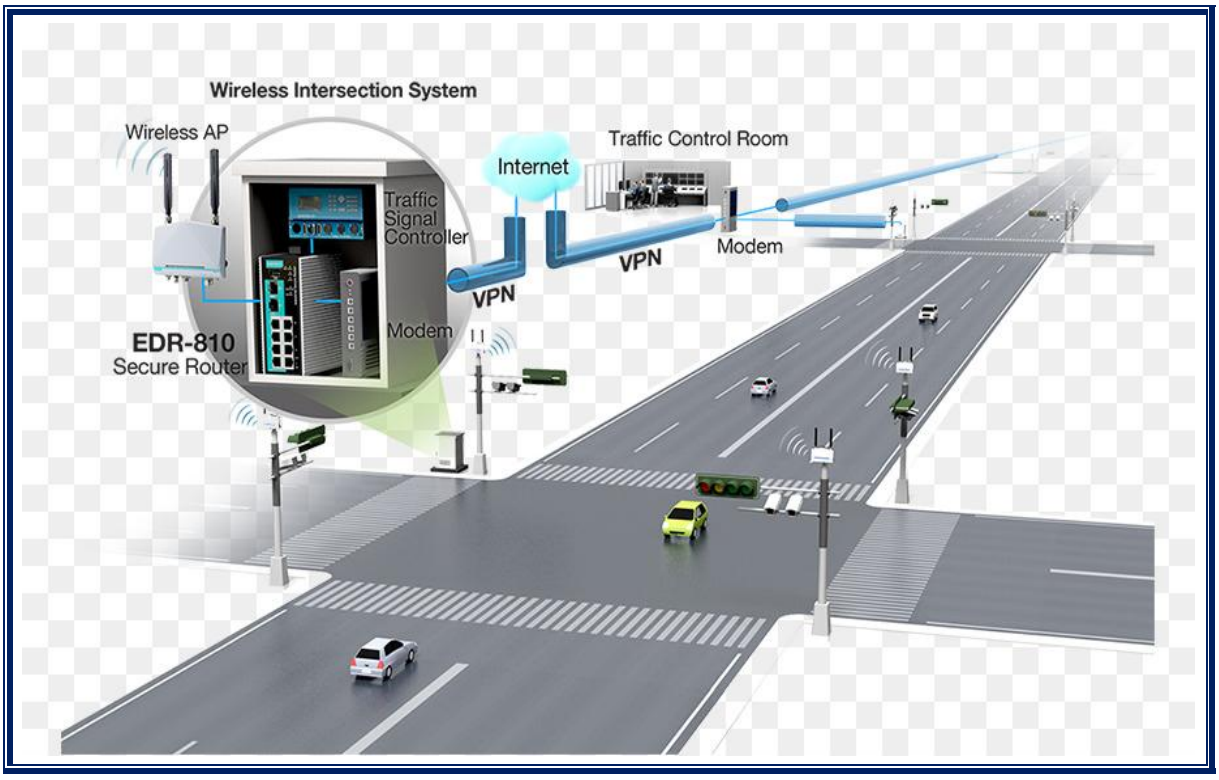


Fig. II. 5 : *Système d'intersection sans fil.*

Le système peut contribuer à une réduction des choix de vitesse inappropriés lors de certaines manœuvres ou des violations de feu rouge et, en conséquence, du nombre de collisions.

- ✓ **Systèmes d'informations sur la circulation :**

  Ces systèmes comprennent :

  - Information en temps réel sur les itinéraires et la circulation.
  - Canal de messages sur la circulation routière (TMC).
  - Guidage routier.
  - Panneaux d'information dynamiques d'itinéraires.
  - Avertissements hivernaux.
  - Transmission d'informations routières (RDS).
  - Systèmes de gestion des incidents et de la circulation.

Ces systèmes, aident le conducteur à arriver à bon port de manière plus rapide et plus sûre. Les informations en temps réel sur les itinéraires et la circulation comprennent l'ensemble des informations permettant d'organiser et d'optimiser les flux de circulation et d'informer et de conseiller (généralement le conducteur) contribuant dès lors à une amélioration de la sécurité et de l'efficacité routières. Les informations transmises aux véhicules peuvent être personnalisées. Voir la figure *Fig. II.6*.

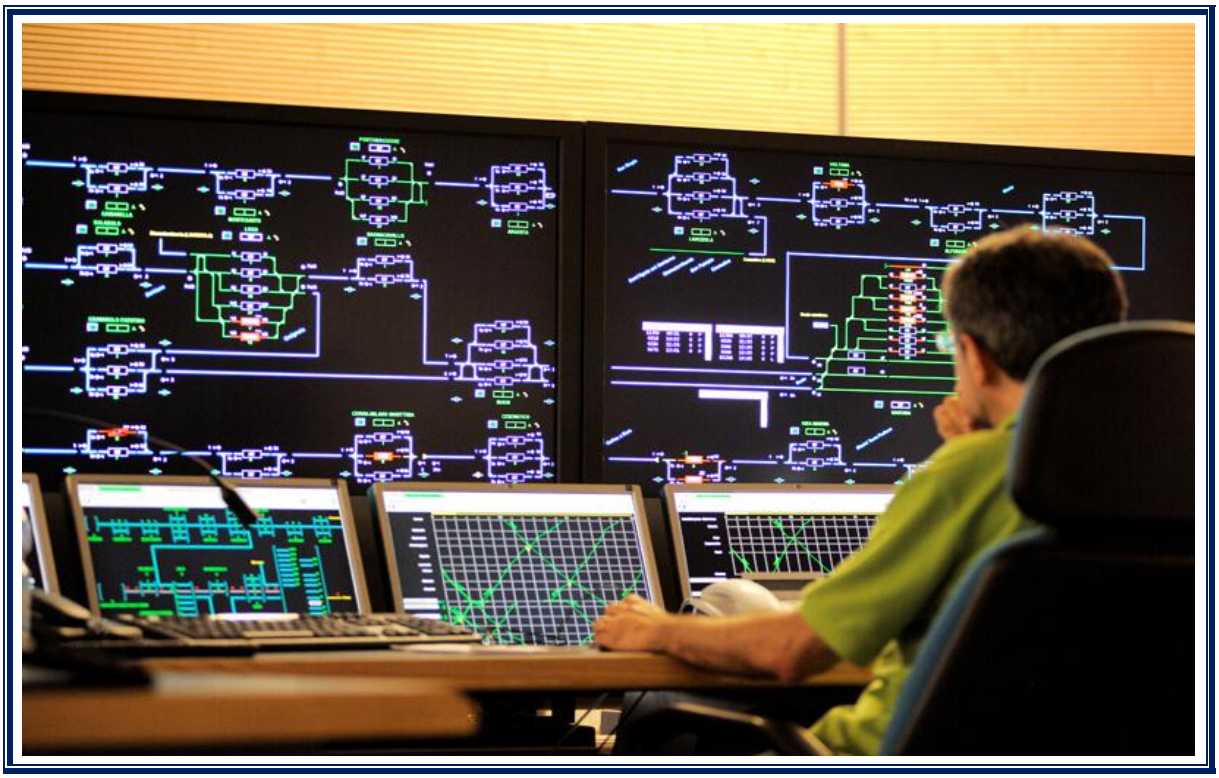


Fig. II. 6 : *Systèmes de contrôle.*

Les systèmes communiquent au conducteur des informations sur la circulation (encombrements) et les conditions météo afin de l'aider à choisir l'itinéraire le plus efficace ou à le préparer à faire face à une situation qui l'attend plus loin sur la route. La précision des informations sur l'état de la circulation est importante pour le maintien de la crédibilité de la fonction et il est par conséquent essentiel que ces systèmes puissent assurer des prévisions à court terme.

La sécurité peut être améliorée non seulement grâce à une prompte réaction aux incidents, mais également à leur prévention, permise par l'harmonisation des flux de circulation. Ces progrès peuvent être obtenus grâce aux signaux des rampes d'accès, au contrôle des voies, aux déviations et, plus généralement, à la gestion du trafic.

- ✓ **Systèmes de gestion de trafic :**

Il a été tenté d'influer sur la vitesse des véhicules par le biais d'une gestion du trafic en fonction des conditions météo et de l'application de limitations de vitesse variables, dans le cadre, notamment, de l'utilisation de systèmes de gestion du trafic basés sur les conditions météo, afin de réduire les limitations de vitesse dans de mauvaises conditions de circulation.

II.4.b. Les systèmes Embarqués :

Les technologies embarquées pour la sécurité recouvrent essentiellement des capteurs embarqués qui recueillent des données et des dispositifs embarqués qui émettent des alertes ou qui prennent partiellement le contrôle du véhicule. L'avantage de ces systèmes est qu'ils peuvent avertir le conducteur des dangers potentiels ou se substituer dans une certaine mesure au conducteur pour commander le véhicule afin de chercher à éviter les collisions. Les avantages ne se manifestent que pour les véhicules dotés de l'équipement embarqué.

En outre, il est important de faire prendre conscience aux conducteurs de la portée de la réduction du danger dont le système est capable afin d'éviter une confiance excessive dans ces dispositifs embarqués. Parmi les applications on cite :

➢ Les ADAS :

Les ADAS (Advance Driving Assist System) est le terme anglais pour désigner les systèmes avancées d'assistance et d'aide à la conduite. Ces derniers sont des systèmes électroniques ayant accès aux organes de restitution, motricité, freinage et direction du véhicule, permettant ainsi au conducteur de bénéficier d'une assistance et/ou de déléguer temporairement la conduite à un copilote automatique dans certaines conditions de circulation (voir la figure *Fig. II.7*). Cet automate peut généralement être activé ou désactivé selon la volonté du conducteur. Les ADAS interviennent sur les différentes phases de conduite, avant la collision, ils participent à la sécurité primaire du véhicule (ou sécurité active).

Fig. II. 7 : *Les système ADAS.*

Des capteurs, ultrasons, caméras, Radars, GPS ont donc été intégrés dans le véhicule pour percevoir l'environnement immédiat et permettre la mise en œuvre de systèmes informatifs ou de systèmes actifs (actions sur les freins, moteur, direction) [10].

Les systèmes d'aide à la conduite fournissent aussi de nouvelles fonctionnalités intéressantes pour le transport routier comme par exemple : le platooning, la détection d'obstacles, la gestion des distances, la planification des trajectoires et des trajets, la détection de la pluie pour l'activation automatique des essuie-glaces et l'Alerte de Franchissement Involontaire de Ligne (AFIL). Dans ce contexte, la connaissance de la localisation et la vitesse des objets mobiles représentent une information clé. Voir la figure *Fig. II.8*.

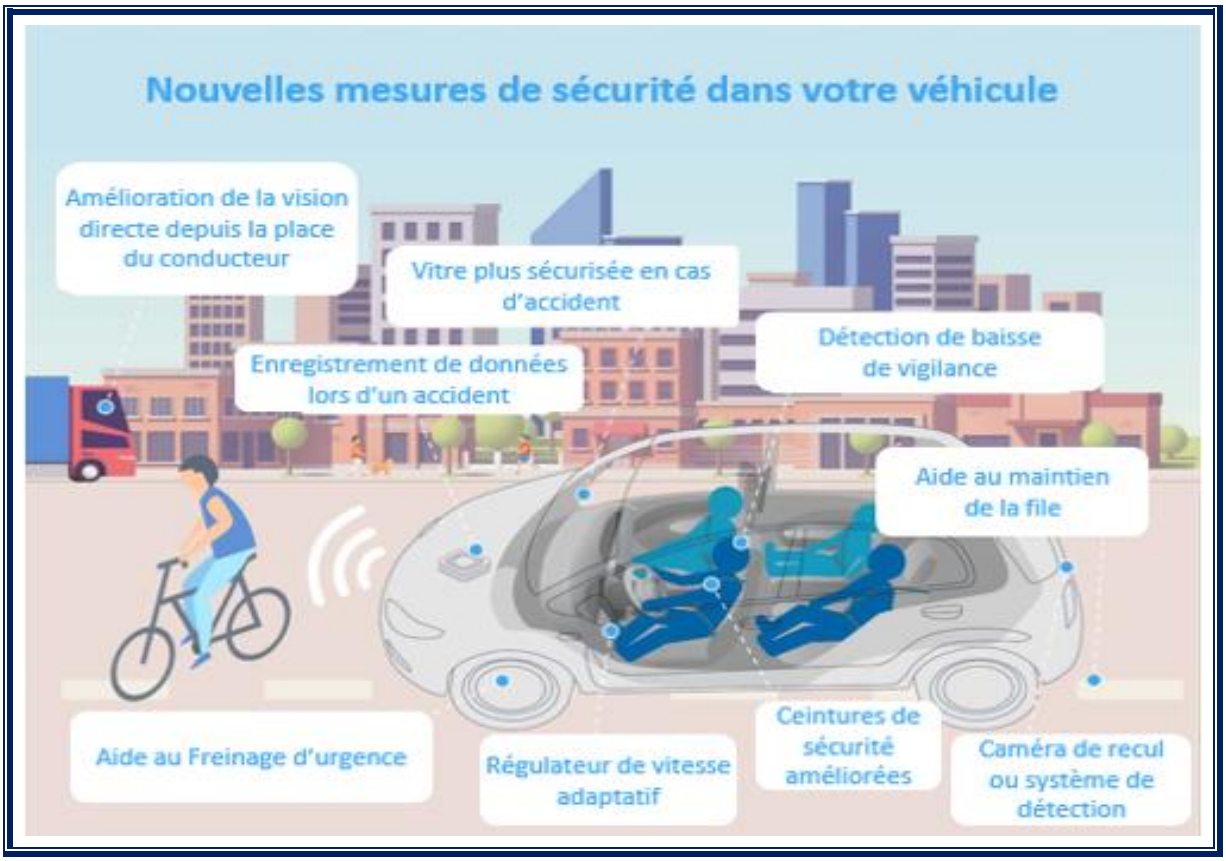


Fig. II. 8 : *Les fonctionnalités des ADAS.*

✓ **Les technologies ADAS :**

- **Capteurs d'imagerie :** Modules de caméras, les caméras gamme 3D, le visage du pilote et les trackers regard, capteur de la route d'état de surface, détecteurs lasers, détecteurs infrarouges (caméra infrarouge).

- **Capteurs de distance :** Capteurs infrarouges, radar, capteur de collision par l'avant, capteur de collision par l'arrière, capteur de collision latérale et capteurs anticollision.

- **Les cartes numériques :** Système de Positionnement Global (Cartes GPS), Système d'Information Géographique (SIG).

- **Les dispositifs de communication :** Communication sans fil et diffusion météorologique locale.

- **Tachymètres :** Indicateur de vitesse, thermomètres, horloges, la vitesse de la roue.
- **Capteurs mécaniques :** Capteurs mécaniques de l'état du moteur, capteurs de pression des pneus, capteurs de l'état des pneumatiques.
- **Autres capteurs :** Pollution, détection de la pluie, etc.

La figure *Fig. II.9* montre les différentes technologie ADAS répandues :

Fig. II. 9 : *Les technologies ADAS.*

➢ Direction active et contrôle dynamique du châssis :

La direction active est un système contrôlé électroniquement à l'aide d'un système de direction variable et d'une direction assistée. Deux éléments différents sont associés, à savoir : l'angle de direction du volant et l'angle de correction communiqué par un contrôleur via une boîte de vitesse spéciale.

Le contrôle dynamique du châssis est un système d'amortissement et de suspension actif qui minimise le roulis du châssis et le tangage en ajustant la garde au sol en fonction de la vitesse, permettant l'adaptation de la garde au sol suivant deux hauteurs différentes comprenant une fonction indépendante de stabilisateur horizontal (Cf. également les contrôles dynamiques de stabilité (ESP).

➢ Régulateur de vitesse adaptatif :

Le régulateur de vitesse adaptatif, parfois désigné avec le sigle AAC (Adaptative Cruise Control), est une version évoluée du régulateur de vitesse. Il ne permet pas uniquement de maintenir une vitesse de croisière : il est également capable de calculer et de conserver une distance de sécurité avec le véhicule qui le précède sur la même voie.

Principe :

Le régulateur automatique de vitesse contrôle la distance qui sépare le véhicule du véhicule qui le précède dans une certaine plage de vitesse (voir la figure *Fig. II.10*) et est doté d'une capacité limitée à décélérer (25 % de la capacité maximale de freinage). La vitesse définie par le conducteur est maintenue dans la limite du possible, tout en demeurant adaptée et en tenant compte de la distance qui sépare le véhicule de celui qui le précède et ce, afin de maintenir une distance de sécurité. En raison des performances limitées des capteurs, le régulateur automatique de vitesse ignore les obstacles immobiles et s'avère incapable de gérer les situations d'arrêt-redémarrage. Les systèmes de régulation automatique de la vitesse sont cependant désormais dotés de nouvelles capacités, plus complètes.

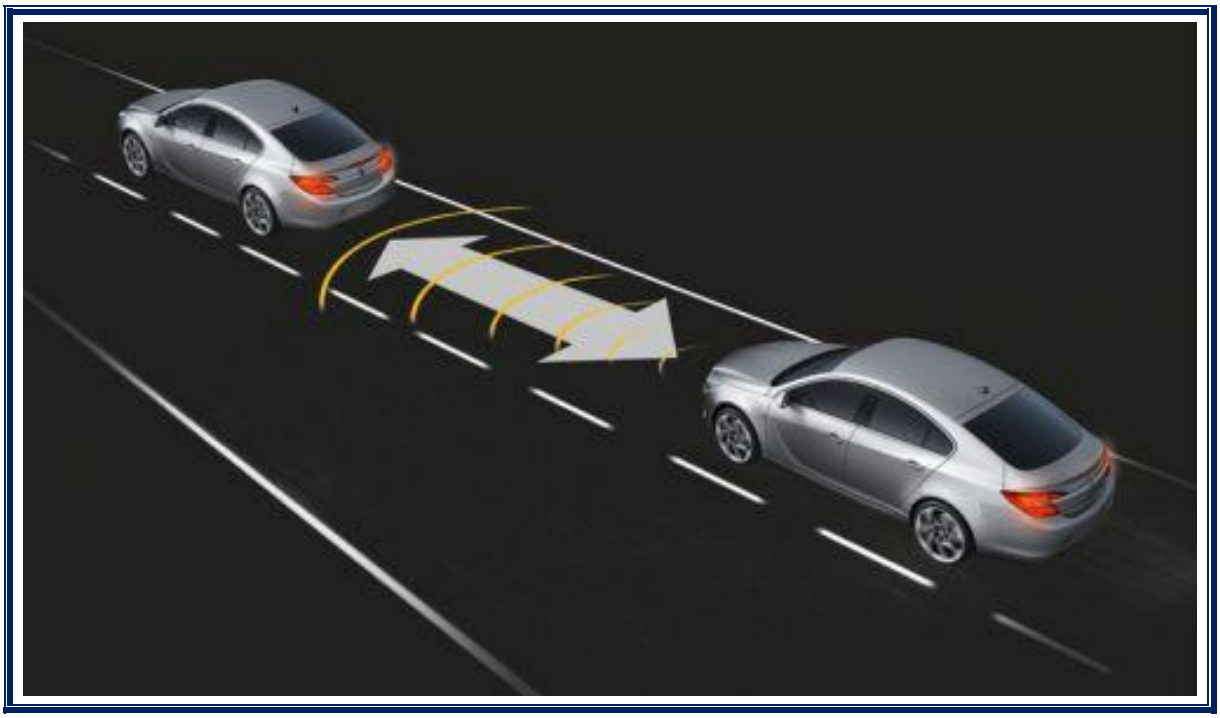


Fig. II. 10 : *Régulateur de vitesse.*

➢ Enregistreur d'événements ou de collisions, ou boîte noire :

Les enregistreurs d'événements recèlent un potentiel d'amélioration de la sécurité routière en permettant d'augmenter la précision des reconstitutions d'accidents et en ouvrant le bénéfice de l'accès à leurs données aux chercheurs, aux accidentologues et aux constructeurs. Les enregistreurs d'accidents enregistrent les paramètres physiques du véhicule sur un court intervalle de temps juste avant et juste après un incident ou un accident [11]. La liste suivante représente les dix éléments à stocker en priorité dans un enregistreur d'événements :

- ✓ Accélérations longitudinale et latérale et direction principale de la force.
- ✓ Localisation géographique du choc.
- ✓ Port ou non de la ceinture pour chaque siège.
- ✓ Nombre d'occupants et position.
- ✓ Données avant le choc.
- ✓ Heure précise du choc.

- ✓ Données relatives au renversement.
- ✓ Données relatives au mouvement de lacet.
- ✓ Informations relatives au système de freinage anti blocage, au contrôle de la traction et au contrôle de la stabilité.
- ✓ Données relatives aux coussins gonflables, par exemple éventuelle désactivation, instant du déploiement, étape du déploiement, etc.

Comment ça marche ?

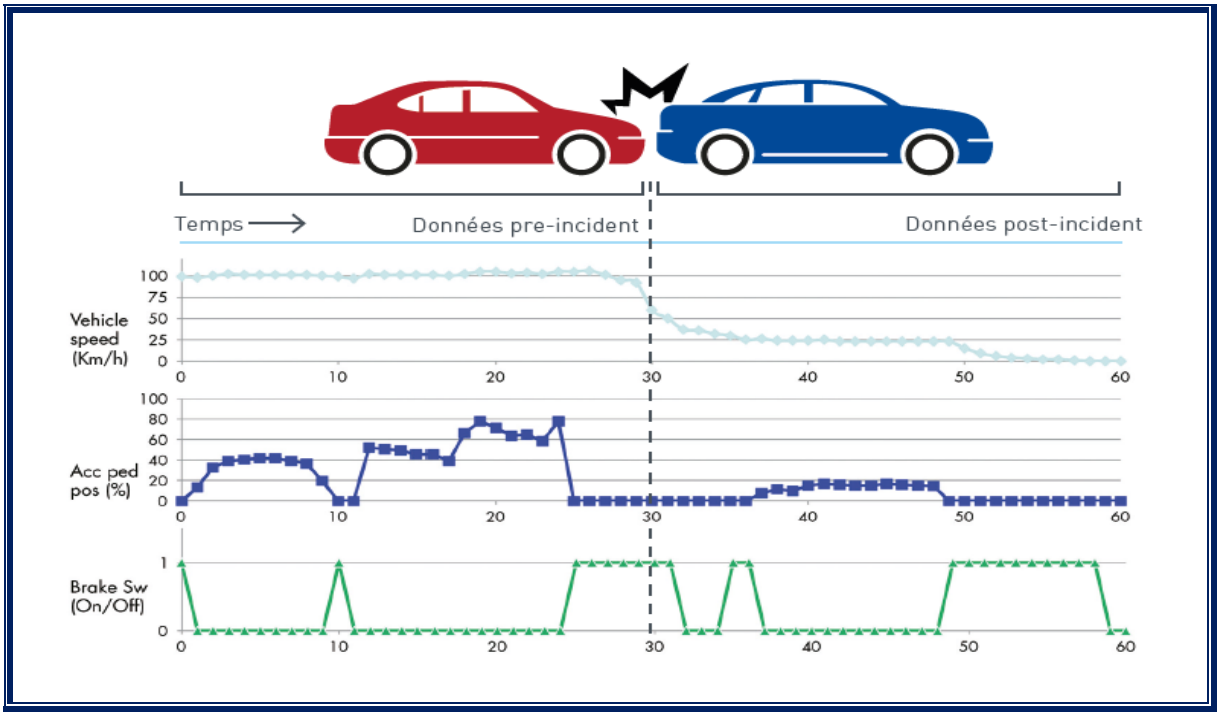


Fig. II. 11 : *Graphique des données pré-incident et post-incident de l'Enregistreur.*

Dans cet exemple (illustré dans la figure *Fig. II.11* ci-dessus), la décélération brusque du véhicule a déclenché l'enregistreur des données de la route. Comme le montre ce graphique : la pédale d'accélération a été relâchée avant l'incident, et le conducteur a freiné pendant l'événement [12].

➢ Les systèmes anti collisions :

Le système anti collision est un dispositif de sécurité routière. Installé sur une voiture, il veille en permanence à ce que le véhicule n'entre en collision avec un autre ou avec un piéton. Fonctionnant avec des capteurs ou des radars qui détectent les menaces, ces derniers avertissent le conducteur en signalant le danger comme illustré sur la figure *Fig. II.12*. Même si cette technologie est en cours de se généraliser, quelques conditions sont à respecter pour que le dispositif soit performant.

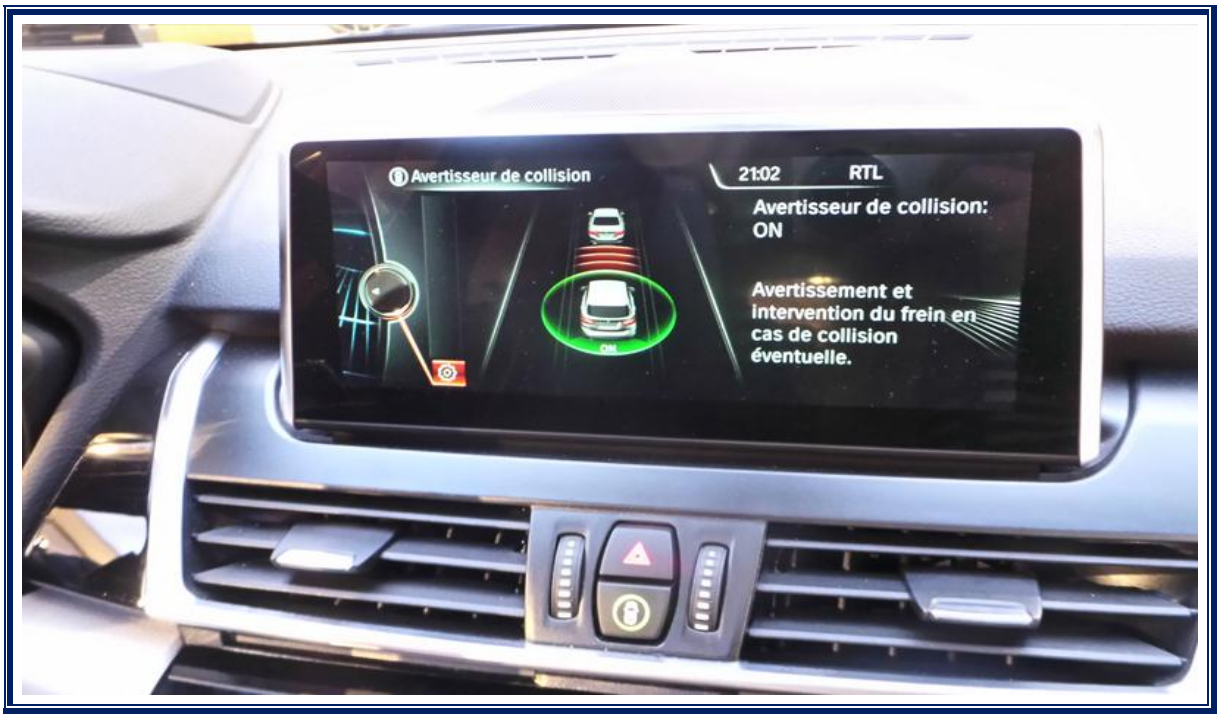


Fig. II. 12 : *Les systèmes anti collisions.*

Principe :

Ce dispositif de sécurité routière fonctionne à l'aide de radars placés sur la calandre et une caméra installée au dos du rétroviseur. Ces derniers émettent des signaux constants qui détectent tous les mouvements et objets. Ensuite, ils les transmettent à un ordinateur lié au système. Ce dernier calcule la distance qui sépare une voiture de l'obstacle ou d'un autre véhicule. Si les calculateurs détectent un risque d'accident, ils envoient des informations au conducteur sous forme de signaux sonores ou de signal lumineux clignotant sur l'affichage tête haute du pare-brise. Dans le cas où vous ne réagissez pas, alors que le danger est imminent, le système prend l'initiative et effectue rapidement un freinage automatique.

Le dispositif anti collision ne peut marcher que si la différence de vitesse entre les deux voitures est inférieure à 25 km/h. Si vous roulez à une vitesse inférieure à 30 km/h, la collision peut être entièrement évitée. Si vous roulez à vive allure, le système peut réduire l'impact de l'accident à 75 %.

II.4.c. Les systèmes coopératifs :

Les systèmes de sécurité coopératifs font appel à la fois aux systèmes installés sur l'infrastructure et aux systèmes embarqués reliés entre eux par des moyens de communication. L'avantage de ces systèmes est que l'information est reçue depuis l'infrastructure (par exemple limites de vitesse, état de la circulation de la route) et qu'elle est transmise de manière dynamique au moment opportun aux véhicules individuels. L'information peut également être transmise en sens opposé, c'est-à-dire du véhicule vers l'infrastructure, par exemple pour avertir automatiquement les services d'urgence lorsqu'un véhicule est impliqué dans une collision.

Ces services ne peuvent être fournis qu'aux véhicules qui sont équipés des dispositifs embarqués. Les cartes numériques et les technologies permettant de repérer très précisément une localisation sont également considérées comme des technologies coopératives dans la mesure où l'information liée à la sécurité peut être combinée à des cartes stockées dans l'équipement embarqué et une aire de service plus importante peut être déterminée comparé aux informations fournies par l'infrastructure.

Les questions spécifiques aux systèmes coopératifs recouvrent : la nécessité de préserver un équilibre entre la sécurité, la fiabilité et le coût du système ; et la normalisation de l'interface homme-machine(IHM). Les applications liées à cette de catégories sont :

➢ eCall :

Le dispositif « eCall » résulte d'une proposition législative de la Commission européenne ayant conduit à un règlement UE du 29 avril 2015. Son but est d'apporter une assistance rapide aux conducteurs en cas d'accidents graves de la route. Il s'agit d'une fonctionnalité d'appel d'urgence, embarquée dans les véhicules, déclenchée automatiquement, quand les capteurs embarqués détectent un accident grave tel qu'il est illustré sur la figure *Fig. II.13*, ou bien manuellement via un bouton logé dans le véhicule comme indiqué dans la figure *Fig. II.14*. Une fois déclenché, le système compose le numéro d'appel d'urgence, établit une connexion téléphonique avec le centre de réception d'appels approprié et lui transmet un ensemble de données concernant l'accident, notamment l'heure de celui-ci et la localisation précise du véhicule accidenté [9].

Fig. II. 13 : *Le système eCall déclenché automatiquement.*

Fig. II. 14 : *Le système eCall déclenché manuellement.*

Le dispositif « eCall » suppose que 3 éléments soient présents simultanément : un module embarqué dans les véhicules pour initier des appels d'urgence « eCall » ; des centres de réception d'appel d'urgence capables de traiter les données spécifiques « eCall » transmises avec l'appel d'urgence ; des réseaux de téléphonie mobile capables de transmettre les appels d'urgence « eCall » vers un centre de réception d'appels capable de traiter les données spécifiques « eCall » comme illustré dans la figure *Fig. II.15* ci-dessous.

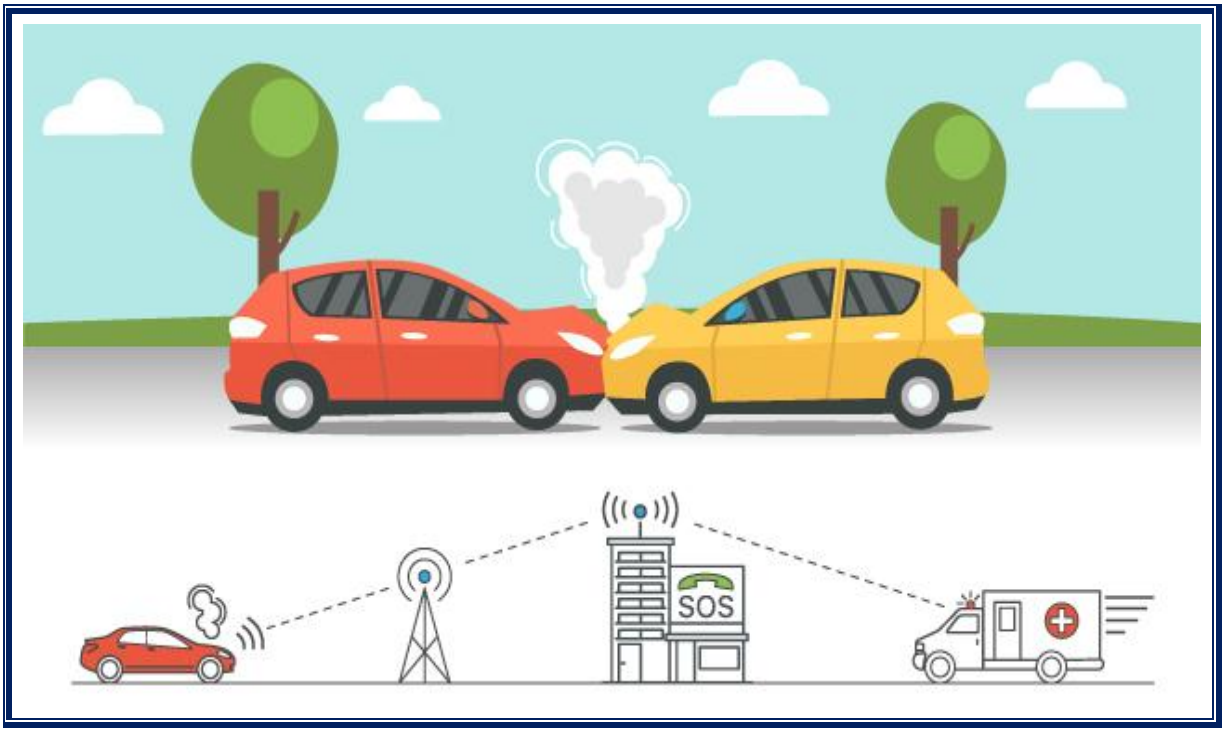


Fig. II. 15 : *Fonctionnement du système eCall.*

Tout en apportant des avantages en matière de sécurité, le système eCall optimise l'efficacité de la chaîne d'intervention en réduisant les temps de réponse. La disponibilité de soins médicaux au profit de personnes se trouvant dans un état critique (ou sévère) immédiatement après une collision, peut permettre de réduire le taux de décès de manière significative. Cette approche est connue en tant que principe de l'heure d'or en médecine d'urgence, ce qui signifie qu'une heure après une collision, le taux de décès des personnes victimes de défaillances cardiaques ou respiratoires ou d'hémorragie massive est pratiquement de 100 %.

➢ Alerte, adaptation intelligente et ajustement de la vitesse :

Le système d'alerte de dépassement de la vitesse aide le conducteur à respecter les limites de celle-ci (voir la figure *Fig. II.16*). La plupart des systèmes utilisent une caméra qui peut lire l'information sur les panneaux de la limitation de la vitesse et ainsi informer les conducteurs des limites de cette dernière par l'entremise d'un écran sur le tableau de bord.

D'autres systèmes utilisent des cartes numériques sur les vitesses stockées avec le dispositif de navigation GPS qui affichent la limite de la vitesse et avertissent les conducteurs par un signal visuel ou sonore lorsqu'il y a dépassement de la limite. Les systèmes les plus récents intègrent les données provenant de ces deux sources, soit une caméra et une carte numérique sur les vitesses avec GPS.

Fig. II. 16 : *Adaptation intelligente de la vitesse.*

Le niveau auquel le système intervient pour contrôler la vitesse du véhicule peut être l'un des suivants :

- ✓ **Conseil :** le conducteur est informé de la limitation de la vitesse et de son éventuel dépassement.
- ✓ **Sélection volontaire par le conducteur** : le conducteur a le choix de l'activer ou de le désactiver, le respect des limitations devient dès lors volontaire.
- ✓ **Obligatoire :** le système ne permet aucun dépassement des limitations de la vitesse.

II.5. Enjeux et défis des ITS :

Les formidables évolutions des STI posent de multiples défis : défis humains, technologiques, scientifiques, commerciaux et économiques. Sans omettre ceux, probablement plus difficiles, d'ordre social, institutionnel et politique.

➢ Homme et machine :

La majorité des systèmes STI embarqués qui procurent un avantage en sécurité peuvent également introduire un élément de risque ; il faut tendre vers un ratio risque-avantage acceptable afin de contribuer valablement aux objectifs de sécurité routière.

➢ Normalisation et certification :

Des pans entiers de technologies STI sont toujours dépourvus de normes. Cette situation peut être bénéfique à l'évolution des technologies (par la latitude qu'elle laisse à la recherche), mais peut aussi se révéler une source d'incompatibilité entre équipements. Il faudra qu'à terme les fabricants de systèmes s'accordent sur un cadre architectural et explorent les avantages d'applications uniformes et normalisées. Des spécifications européennes engendreront d'appréciables économies d'échelle.

Le développement d'une charpente légale de certification des produits est également indispensable. Des procédures d'essai doivent être élaborées, qui permettront l'auto certification vis-à-vis de normes nationales.

Il faudra trouver un équilibre et une complémentarité entre les services offerts par le gestionnaire public et l'opérateur privé. Les échanges de données et les méthodes, procédures et protocoles devront être formalisés.

➢ Responsabilités :

Comment, en cas de dysfonctionnement susceptible de causer un accident, partager les responsabilités entre le constructeur automobile, le fournisseur de logiciels ou de services, l'opérateur de communications, le gestionnaire routier et le conducteur ?

Et que dire d'un dysfonctionnement qui mettrait en cause la protection de la vie privée, à cause de la possibilité de suivi autorisée par les systèmes STI ?

➢ Protection de la vie privée :

Le développement des STI doit se réaliser dans le respect des libertés individuelles et sans déresponsabiliser le conducteur. Mais la protection de la vie privée risque d'être mise à mal, par exemple par la localisation précise des véhicules, par leur identification automatique, ou encore par la « boîte noire ». Il faudra définir, à partir de la jurisprudence, les recommandations à appliquer aux nouveaux services, en tenant compte des règles existantes concernant, par exemple, les péages autoroutiers ou la télé-billettique.

➢ Sécurité des informations :

Puisque l'information constitue la base de la majorité des STI, il faudra garantir une extrême fiabilité des serveurs d'informations, qui devront résister aux pannes, virus et autres piratages informatiques.

➢ Adaptation du conducteur :

La propagation des STI entraîne une transformation profonde des usages et des pratiques en matière de conduite automobile, en particulier les systèmes d'information et d'assistance (ADAS).

De nombreuses fonctions des STI sont conçues pour faciliter et sécuriser la tâche de conduite :

- ✓ Alléger les processus d'orientation,
- ✓ Réduire le niveau de stress et la charge mentale du conducteur,
- ✓ Favoriser l'anticipation vis-à-vis de situations critiques,
- ✓ Pallier certaines latences de réaction et incertitudes de décision.

Mais les interrogations demeurent sur l'acceptabilité des STI par les conducteurs et sur les modifications de comportement qu'ils risquent d'engendrer.

Il sera nécessaire d'instaurer un observatoire qui analysera les effets psychologiques et comportementaux résultant d'un rendement amélioré et d'un confort accru. L'analyse s'étendra aux effets d'une perte potentielle de certaines aptitudes, aux conflits entre l'individu et le système, aux difficultés qu'éprouveront certains segments de la population et à tout autre effet secondaire, difficile à pronostiquer mais pouvant influencer le niveau de sécurité.

Il faut replacer le conducteur au centre de la conception des STI. Les systèmes d'aide à la conduite, entre autres, doivent être conçus à partir des besoins et des usages. Les fabricants doivent s'assurer de leur pertinence et identifier en amont leurs effets potentiellement négatifs afin d'en limiter les conséquences.

➢ Comportement :

On l'a vu, les STI offrent le potentiel de simplifier et de standardiser la conduite, de détecter les faiblesses du comportement du conducteur et de compenser celles-ci. Le risque existe toutefois que plusieurs tâches en viennent à se concurrencer, au point que le conducteur ne soit plus à même de traiter toutes les informations pertinentes qui s'offrent à lui. Cette « surcharge de tâches » (overload en anglais) est essentiellement visuelle.

Le phénomène inverse est tout aussi plausible et tout aussi risqué : l'underload se traduit par un état de vigilance réduite ou de « désactivation » (assoupissement). Il peut être provoqué par un dispositif STI qui remplit certaines tâches à la place du conducteur, en combinaison avec des conditions de conduite monotones. « L'hypnose de l'autoroute » est un exemple d'underload.

Une autre adaptation comportementale contre-productive peut être induite lorsque le conducteur adopte un comportement plus risqué parce qu'il perçoit un gain de sécurité fourni par un système STI. Exemple : au début de l'introduction de l'ABS, certains conducteurs avaient tendance à accélérer dans des conditions défavorables. Tout bien considéré, l'ABS a modifié le type d'accidents plutôt que d'en réduire le nombre.

➢ Les dérives potentielles :

Les assureurs plaident pour un contrôle électronique des véhicules et des conducteurs. Pour inciter les jeunes conducteurs à rouler prudemment, une compagnie française d'assurances avait envisagé, en 2005, un système de localisation permanente des véhicules : grâce à un GPS embarqué, l'assureur aurait pu déterminer, toutes les deux minutes, la vitesse pratiquée et le type de route emprunté par son client [8]. En contrepartie d'un rabais sur le montant de la prime, les conducteurs s'engageaient à ne pas dépasser les limitations. En novembre 2005, la Commission nationale de l'informatique et des libertés (CNIL) a refusé la création d'un tel dispositif, considérant qu'il débouchait sur un fichier individualisé des infractions, démarche interdite pour une entreprise privée. La CNIL a également estimé que l'atteinte à la liberté était disproportionnée par rapport aux avantages attendus.

II.6. Potentiel des STI sur la sécurité routière :

Une autre manière de classer les systèmes selon leur incidence sur la sécurité consiste à étudier quel domaine de la sécurité routière est affecté par le système : exposition, risque d'accident ou conséquences des accidents [7].

Pratiquement l'ensemble des systèmes ont une incidence sur la sécurité en influant sur les risques de collision. Il est probable, par exemple, qu'une pénétration accrue de nombreux systèmes STI embarqués rende l'utilisation de la voiture plus attractive que celle des transports en commun. Cette conséquence aurait un impact négatif sur la sécurité en modifiant le choix modal (augmentation du trafic => accroissement du nombre de collisions). Cet impact n'est suffisamment visible pour aucun système embarqué seul.

Il est important de noter que l'estimation de l'impact s'appuie souvent sur des études pilotes réalisées à petite échelle en des lieux spécifiques ou auprès de catégories spécifiques de conducteurs. C'est pourquoi elles ne peuvent être considérées comme concluantes, mais comme reflétant les connaissances actuelles d'un système particulier. Les effets combinés d'un certain nombre de systèmes ne devraient pas être calculés comme la somme des effets des systèmes considérés individuellement – il est impossible d'empêcher deux fois une même collision. Les effets nets de l'interaction entre différents systèmes sur la sécurité routière demeurent cependant inconnus.

II.7. Conclusion :

En conclusion, actuellement, certains pays testent, évaluent et mettent en œuvre la technologie de sécurité STI en vue de réduire le nombre de collisions et d'améliorer la sécurité sur les routes. Les systèmes embarqués, les systèmes installés sur l'infrastructure et les systèmes coopératifs semblent prometteurs en termes de prévention et de minimisation des collisions et des dommages consécutifs à ces dernières.

Les progrès des technologies de l'information ont alimenté le développement de technologies de détection en vue de déterminer le danger potentiel et de localiser avec précision le véhicule, en plus de la communication sans fil et des technologies de numérisation des cartes routières. Ces progrès technologiques ont permis la création de nouvelles mesures en faveur de la sécurité de la circulation qui fournissent en temps réel des informations détaillées pour répondre aux besoins de chaque conducteur.

Dans le prochain chapitre, nous allons aborder les différents travaux qui ont été déjà faits afin de réduire les accidents de la route et d'améliorer la sécurité routière. Nous allons proposer une approche qui permet de dénoncer tout véhicule enfreignant les règles des autorités compétentes et de détecter toute collaboration de véhicules pour une alerte frauduleuse.

Chapitre III :

Description de l'approche proposée

III.1. Introduction :

Dans le cadre des accidents de la route, les causes humaines arrivent loin devant les causes météorologiques ou techniques. La plupart du temps, c'est à une combinaison de causes que l'on assiste.

En effet les infractions routières commises par les conducteurs lors de leur trajet contribuent en grande partie à l'augmentation régulière du nombre de décès et de blessures dus aux accidents routiers dans le monde. Parmi les infractions qui accentuent ce risque, la vitesse et le non-respect de la distance sont les plus fréquentes et les plus dangereuses.

Dans le contexte de ce chapitre, notre objectif est de faciliter la tâche aux autorités policières dans la détection et la pénalisation des infractions routières. Classiquement, un agent de la circulation doit identifier un véhicule enfreignant toute règle de circulation, soit manuellement, soit en utilisant des appareils tels que des capteurs de vitesse et des caméras. Puis le flic suit ledit véhicule et demande au conducteur de s'arrêter, ensuite il inspecte manuellement le véhicule et il délivre un ticket de violation portant l'identité du véhicule, l'identité du conducteur, la nature de la circulation et les amendes qui y sont associées. Ce système est considéré comme étant lent et exigeant en main-d'œuvre. Pour pallier aux lacunes du système classique et surtout minimiser les erreurs humaines et le danger pour la vie des policiers, nous avons proposé un protocole de détection collaborative de conduite agressive qui se focalise à déceler les conducteurs ayant dépassé la vitesse limitée et/ou la distance autorisée par la loi de la route et les signaler auprès des autorités, et cela en s'appuyant sur un réseau VANET.

III.2. Travaux connexes :

III.2.a. Le dépassement des vitesses autorisées :

Les méthodes disponibles pour la détection des véhicules qui dépassent les vitesses autorisées peuvent être classées en deux types. La première catégorie est la méthode intrusive, basée sur les tubes routiers pneumatiques, les capteurs piézoélectriques et les détecteurs à boucle inductive. La deuxième catégorie est la méthode non intrusive, basée sur le traitement d'images vidéos, les capteurs infrarouges, les radars micro-ondes et les capteurs ultrasoniques.

Les principaux composants du détecteur à boucle inductive sont un câble d'extension de boucle, une boucle et un détecteur. Des emplacements spécifiques sont sélectionnés pour placer les détecteurs de boucle sur les bords de la route pour compter le nombre de véhicules qui traversent. La vitesse du véhicule peut être calculée en fonction de la période pendant laquelle un véhicule occupe le détecteur. Cependant, le principal inconvénient de cette méthode est l'installation de ces détecteurs.

Pour l'installation, les détecteurs nécessitent un grand nombre de coupes sur les revêtements routiers. Ainsi, les principales difficultés résident dans la méthode basée sur l'induction et son déploiement ainsi que sa maintenance. De plus, les modèles de communication des détecteurs de boucle sont unidirectionnels, c'est-à-dire du véhicule à l'infrastructure, mais pas l'inverse.

De nombreuses recherches ont été effectuées sur les STI pour améliorer l'efficacité de la détection des véhicules circulant à grande vitesse, en revanche ces recherches sont bien moindres dans le domaine des réseaux véhiculaires VANET.

QuocChuyenDoan, Tahar Berradia et Joseph Mouzna apportent le concept d'équipement routier pour communiquer avec les véhicules. La présence d'équipements routiers et de véhicules dans le réseau aide les auteurs à proposer une méthode de calcul de la vitesse du véhicule. Les unités routières en bordure de route jouent le rôle de détecteurs de boucle, elles collectent les données et comptent le nombre de véhicules qui la traversent au cours d'une certaine période. Le principal inconvénient de ce schéma est la conception du réseau. Les auteurs ont sélectionné des RSU dans une position telle que la couverture de celle-ci ne devrait pas se chevaucher avec celle des autres et il ne devrait pas non plus y avoir d'écart entre les plages de couverture de deux RSU adjacentes. Ce modèle donne un bon résultat dans leur propre environnement, mais n'a pas pu être appliqué aux réseaux où le nombre d'RSU est assez minime. Le système proposé est également coûteux, car le nombre d'RSU nécessaires est plus élevé [13].

Nehal Kassem, Ahmed E Kosba et Moustafa Youssef ont proposé un système de détection et d'estimation de vitesse basé sur les fréquences radio (ReVISE). Ce système fonctionne sur le fait que la présence et le mouvement des objets affectent la force du signal sans fil dans un environnement RF. Par conséquent, il estime que ce changement dans la force du signal est dû aux véhicules qui le traversent. Sur la base de ce changement de signal et de la période de changement, les auteurs comptent la vitesse des véhicules. Le système proposé ne s'applique qu'à la zone d'intérêt. Une fois qu'un véhicule franchit la zone du signal RF, il ne peut pas être retracé [13].

Ainsi, pour surmonter les points mentionnés, un schéma de détection de véhicule a été proposé par les auteurs Rajendra Prasad Nayak, Srinivas Sethi et Sourav Kumar Bhoi. Ce schéma utilise l'algorithme PHVA pour contrôler les véhicules à grande vitesse dans les régions avec ou sans RSU. Son principal objectif est de détecter les véhicules à grande vitesse, de réduire le nombre d'accidents et d'assurer la sécurité des voyageurs ainsi que des piétons [13].

III.2.b. Le non-respect de la distance de sécurité :

L'utilisation de données vidéos pour accroître la sensibilisation des conducteurs a été abordée dans plusieurs travaux dont le but était d'améliorer la perception visuelle des conducteurs des véhicules circulant dans la voie opposée. À cette fin, une technologie ADAS a été développé pour la détection de dépassement de distance autorisée en s'appuyant sur la technologie VANET. Le système partage des informations avec des véhicules circulant dans la même direction et dans la même voie après que le véhicule suivant ait lancé la demande de transmission d'un flux vidéo entre le véhicule de tête et le véhicule suivant.

La combinaison d'images provenant de plusieurs caméras pour améliorer la conscience visuelle du conducteur est une approche étendue utilisée dans les processus de détection d'objets. Les avantages de l'utilisation de caméras synchronisées, comme une détection améliorée des routes plus fluide grâce à la combinaison de champs visuels, ont été élucidés lorsque cette approche a été comparée à des approches basées sur une seule caméra pour obtenir des informations 3D à partir d'une carte de disparité. Voir la figure *Fig. III.1*.

Fig. III. 1 : *Détection améliorée de la route d à l'aide d'une caméra synchronisée.*

Le comportement de conduite du conducteur a également été enregistré et évalué à l'aide de différentes technologies basées sur la vision, y compris des caméras. Par exemple, A. Houchin, J. Dong, N. Hawkins et S. Knickerbocker ont analysé des données vidéos et ont constaté que les temps de progression et les distances d'arrêt dépendaient du type du véhicule. La progression moyenne était d'environ 2 secondes lorsqu'une voiture suivait et 3 secondes lorsqu'un camion suivait [14].

La prévention des collisions par l'arrière a été abordée dans plusieurs travaux axés sur la mise en œuvre des ADAS. Par exemple, un travail récent a présenté un ADAS basé sur la vision stéréo utilisant un appareil mobile capable de détecter les véhicules et les voies.

Une autre étude a proposé un nouveau système d'avertissement de collision basé sur le temps (CSW pour Collision Warning Systems) qui a alerté le conducteur du véhicule de tête d'une collision arrière imminente. Le système était basé sur le calcul des paramètres suivants : le temps jusqu'à la dernière seconde d'accélération (T_{lsa}) pour le véhicule de tête et le temps jusqu'à la dernière seconde de freinage (T_{lsb}) pour le véhicule suivant. Les valeurs ont été comparées et un avertissement a ensuite été transmis au conducteur en cas de dépassement d'un certain seuil [14]. Une fois le conducteur averti, il peut prendre des mesures pour prévenir ou atténuer les conséquences d'une collision arrière (appuyer sur l'accélérateur, klaxonner ou faire clignoter les feux de freinage pour alerter le conducteur suivant). Après une série d'expériences et de tests, il a été conclu que parmi les trois actions précitées, le scénario dans lequel le véhicule de tête accélère montre une amélioration significative des résultats dans la prévention des collisions arrières. Cependant, pour que le conducteur accélère complètement, il ne doit pas y avoir d'obstacles à venir, ce qui rend cette méthode inutile dans de nombreux scénarios de circulation urbaine.

Il existe également des travaux qui se concentrent sur les systèmes de détection, de surveillance et d'alerte des comportements de talonnage (illustré sur la figure *Fig. III.2*).

Fig. III. 2 : *Comportement de talonnage d'un conducteur du véhicule.*

Pour décourager le talonnage, un capteur d'avertissement de talonnage (TWS) à faible coût a été présenté. L'appareil a averti le conducteur s'il était impliqué dans le talonnage ou si une collision était imminente. Il se composait d'un capteur électronique optique compact monté à l'avant du véhicule [14].

Un travail supplémentaire a été en mesure de suivre de manière robuste des objets (à partir d'une plate-forme mobile) dans un environnement complexe en utilisant le modèle de mélange gaussien infini (IGMM). La méthode a combiné l'approche déterministe non basée sur un modèle avec le modèle d'ombre de mélange gaussien (GMSM) pour supprimer les ombres. La stratégie de suivi a été encore améliorée en calculant la similitude des histogrammes de couleur.

Tous les systèmes d'évitement de collisions arrières présentés dans cette section ont collecté des informations à l'aide de capteurs ou de caméras montés dans le véhicule arrière. Cependant, une caméra d'aide au stationnement arrière située dans le véhicule de tête a été utilisée pour collecter les données pertinentes, car les caméras d'aide au stationnement arrière sont déjà de série dans de nombreuses voitures neuves. Voir la figure *Fig. III.3*.

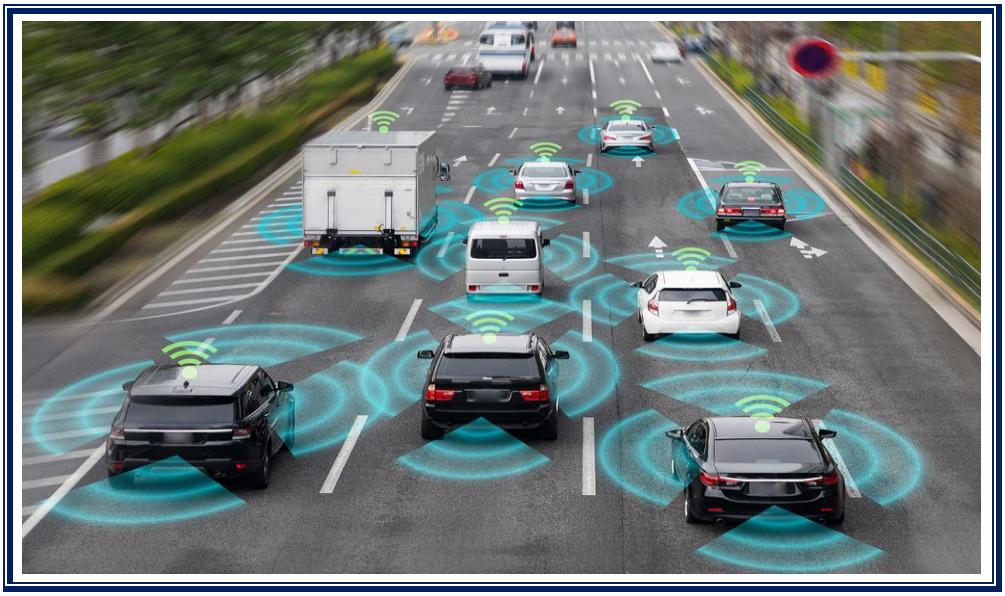


Fig. III. 3 : *Exemple d'un système anticollision.*

Conformément à ce travail, ils ont contribué à la recherche dans le domaine en élaborant le système coopératif pour promouvoir le respect de la distance de sécurité (Tailigator) de manière discrète. Le système détecte la distance au véhicule suivant au moyen de la détection d'objets et de la stéréoscopie optique.

Afin de permettre au conducteur de communiquer avec le véhicule suivant, les composants du système résident dans le véhicule de tête. Si une certaine valeur seuil concernant la distance entre les deux véhicules est dépassée, le véhicule de tête affiche un message dans le pare-brise arrière indiquant que la distance de sécurité requise a été violée. Ce message est destiné au conducteur du véhicule suivant. La figure *Fig. III.4* illustre l'idée.

Fig. III. 4 : *Message affiché au véhicule de talonnage.*

III.3. Infractions routières et conséquences :

Les infractions routières, aussi désignées comme des infractions au code de la route, sont tellement multiples qu'il n'est pas rare d'en commettre une. Un mauvais stationnement ou un homicide involontaire, les amendes et peines encourues ne sont bien évidemment pas du même ordre, mais il est généralement possible d'alléger la sanction.

Plusieurs types d'infractions routières peuvent être constatées : infraction aux règles de sécurité routière, sanctions relatives au permis de conduire ou sanctions relatives aux véhicules, celles-ci sont considérées selon leur gravité comme des contraventions ou des délits.

➢ Les infractions donnant lieu à une contravention :

Les infractions routières sanctionnées d'une contravention sont les moins graves. On parle de contravention lorsque l'infraction routière concerne :

- ✓ Le stationnement ;
- ✓ L'excès de vitesse ;
- ✓ Le non-respect de la distance de sécurité ;
- ✓ Le non-respect du feu tricolore ;
- ✓ Une conduite en état d'ivresse avec un taux d'alcool inférieur à 0,80 g/l ;
- ✓ Le téléphone au volant ou l'utilisation d'oreillettes, d'écouteurs ou de casques audio ;
- ✓ Le défaut de contrôle technique d'un véhicule ;
- ✓ Le surnombre de passagers, etc.

➢ Les infractions qualifiées de délit :

Si les simples contraventions n'entraînent en général que des conséquences minimes, les infractions routières qualifiées de délit sont quant à elles sanctionnées bien plus sévèrement. Dans ce cas, un passage par le tribunal correctionnel est systématique, accompagné par une peine pouvant aller jusqu'à la restriction de liberté. Les faits qualifiés de délit sont :

- ✓ Homicide involontaire par conducteur ;
- ✓ Blessures involontaires par conducteur ;
- ✓ Conduite avec un taux d'alcoolémie supérieur à 0,80 grammes par litre de sang ;
- ✓ Conduite sous l'emprise de stupéfiants ;
- ✓ Refus d'obtempérer ;
- ✓ Conduite sans permis ou après retrait du permis ;
- ✓ Certaines infractions contraventionnelles en cas de récidive.

Le facteur humain apparaît dans plus de 90% des accidents de la route. En effet, d'après une étude menée en septembre 2018 par l'Observatoire National Interministériel de la Sécurité Routière (ONISR), la plupart des chocs ou accidents sont dus à un non-respect de la distance de sécurité ainsi qu'au non-respect de la vitesse moyenne autorisée. Voir la figure *Fig. III.5*.

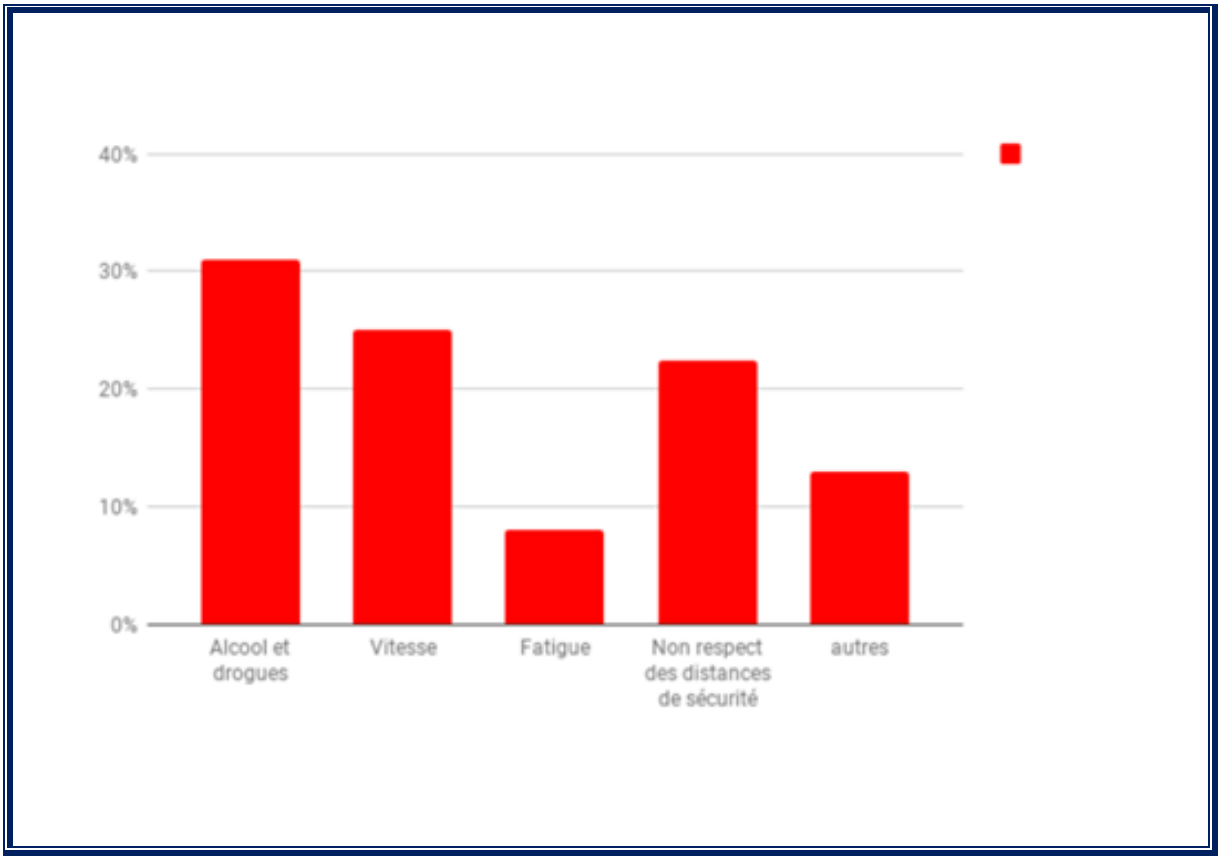


Fig. III. 5 : *ONISR : Taux d'accidents routiers en fonction des causes.*

Voici un exemple du conducteur, comme illustré sur la figure Fig. III.6, roulant un peu vite et ne respectant pas la distance de sécurité (voiture rouge), à ce rythme-là, le moindre freinage de la part du conducteur de la voiture orange provoquera un accident et mettra les voitures dans la zone de couverture globale (ellipse en pointillé rouge) en danger potentiel (voitures jaunes). Les voitures vertes étant à une distance éloignée du véhicule anormal peuvent éviter le danger.

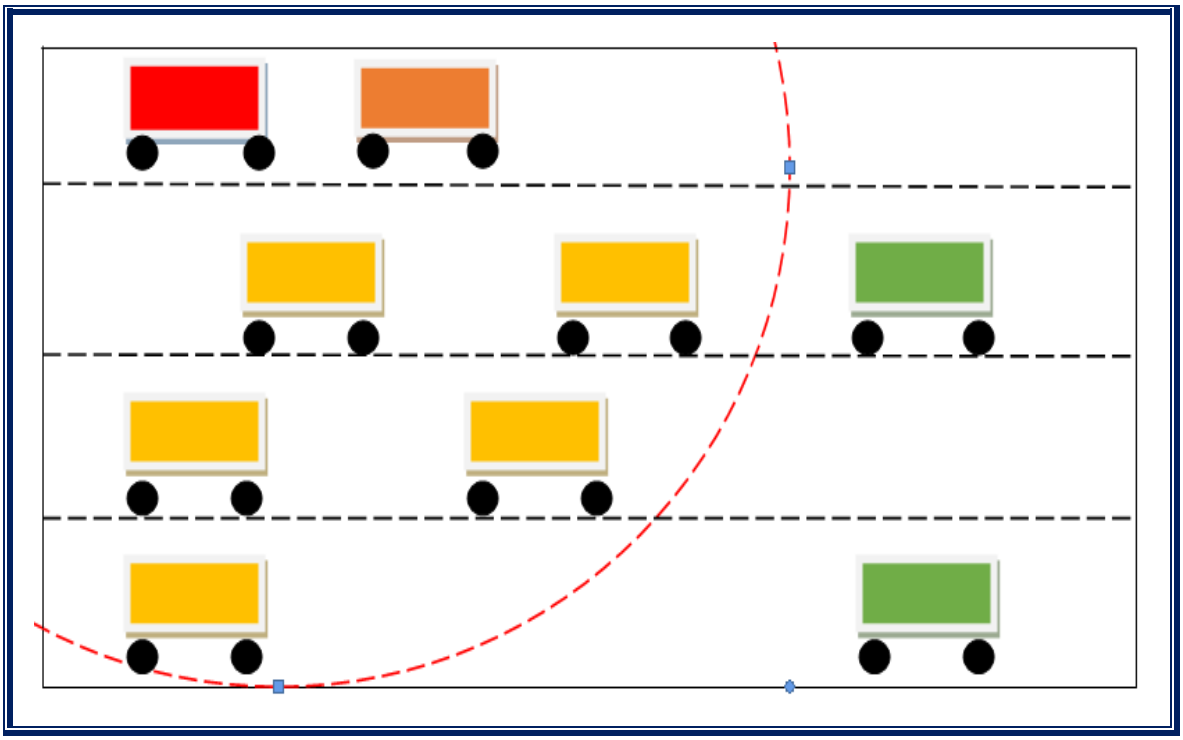


Fig. III. 6 : *Danger causé par le non-respect de la distance de sécurité.*

A partir du graphe et de l'exemple mentionnés ci-dessus, on peut constater que le non-respect de la vitesse et de la distance autorisée sont les facteurs déclencheurs les plus élevés et les plus aggravants des accidents routiers.

Dans le but d'améliorer la sécurité des conducteurs et des piétons sur les routes, nous proposons un système qui repose sur les VANET.

III.4. Vue globale sur le système utilisé :

Les véhicules ne respectant pas la vitesse autorisée et la distance minimale, doivent être contrôlés. Ainsi, diverses organisations gouvernementales, institutions universitaires et industries automobiles ont entamé diverses recherches et projets pour réduire les risques d'accidents et assurer la sécurité des passagers et des conducteurs. Des projets récents ont été déjà mis en œuvre et d'autres sont en cours dont l'objectif principal est d'assurer la sécurité et les services aux personnes.

Désormais, le réseau ad hoc de véhicules (VANET) est un élément clé des systèmes de transport intelligents (STI ou ITS en anglais). Il est utilisé pour soutenir leur développement. Les principaux composants des VANET sont les véhicules, les nœuds d'infrastructure (par

exemple, la RSU) et les autorités de certification (AC). Les RSU reçoivent des informations des véhicules qui passent et les envoient au serveur du réseau. Les RSU servent également de pont entre les véhicules et les serveurs ainsi que les AC. L'architecture VANET de base est illustrée sur la figure *Fig. III.7*.

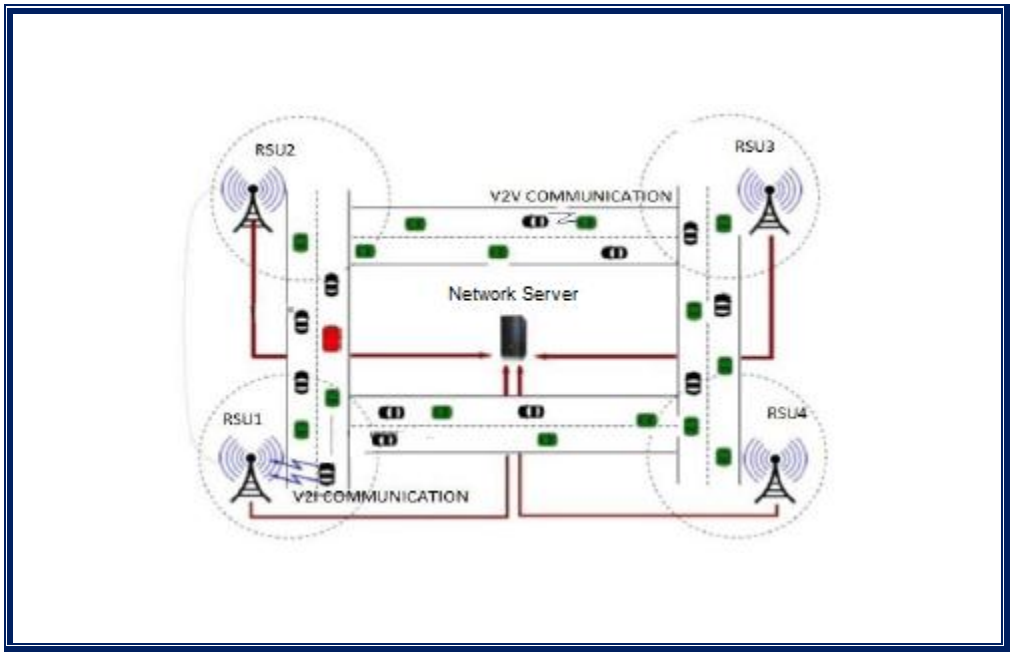


Fig. III. 7 : *Architecture VANET montrant la communication véhiculaire sous RSU 1.*

Lors de la circulation routière, si un véhicule relève de la couverture d'une RSU, cette dernière informe le véhicule des conditions routières ainsi que des informations de circulation sur cette zone.

Chaque véhicule constituant le réseau est équipé de dispositifs de communication sans fil, appelés unités embarquées (OBU), pour permettre les différents types de communications : véhicule à véhicule (V2V) et véhicule à infrastructure (V2I), d'un système de positionnement global (GPS) pour identifier son propre emplacement et de capteurs, etc.

Durant leur trajet, les conducteurs s'échangent diverses informations concernant l'état de leurs véhicules (position...etc.) via des messages, le contenu de ces derniers va permettre aux véhicules récepteurs de détecter les conduites agressives (l'excès de vitesse et le non-respect de la distance de sécurité) et de les déclarer aux autorités policières. Pour ce faire, on propose l'approche suivante.

III.5. L'approche proposée :

Dans ce qui suit, nous présentons les différentes phases qui constituent notre approche afin de détecter et dénoncer tout véhicule enfreignant les règles de la route, plus spécifiquement le non-respect de la vitesse limitée et de la distance de sécurité minimale.

L'organisation de notre réseau est basée sur le concept de la hiérarchisation connue sous le nom de clustering en anglais. Voir la figure *Fig. III.8*.

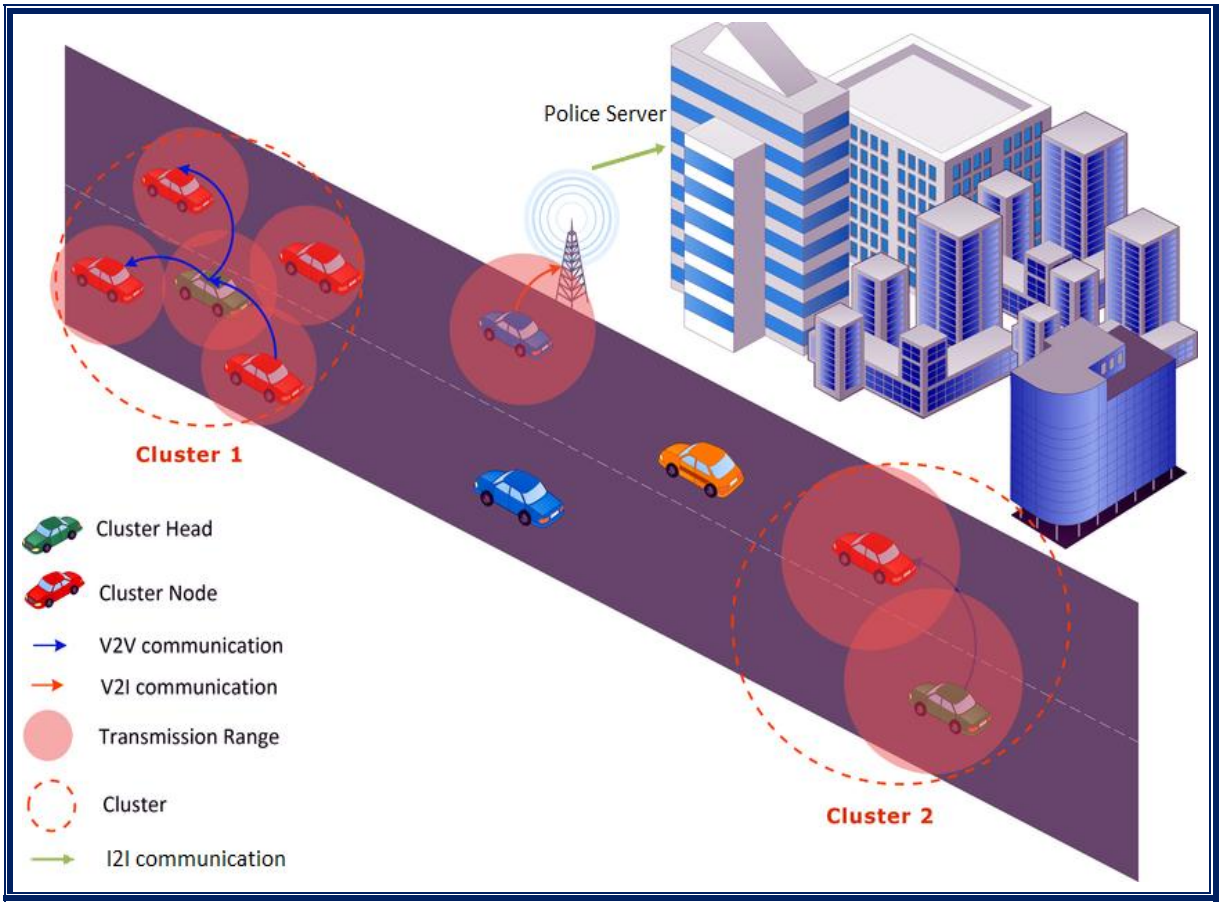


Fig. III. 8 : *Architecture VANET proposée.*

III.5.a. Le Processus de clustering :

Pour la réalisation de notre réseau, le protocole Leach était le point phare sur lequel on s'est appuyé pour concevoir notre algorithme. En effet, des modifications ont été nécessaires afin de l'adapter aux caractéristiques de notre réseau VANET.

La hiérarchisation du réseau organise le réseau en groupes de nœuds appelés cluster. Dans notre algorithme, les nœuds peuvent avoir l'un des rôles suivants : Cluster-head (CH) ou Cluster-Member (CM). Le CH sert de coordinateur local pour son cluster, effectuant des communications intra-cluster, et de passerelle pour communiquer avec la RSU. Le CM rejoint un cluster pour devenir membre de ce dernier. Cette organisation présente de nombreux avantages dont la facilité de gestion et la diminution de messages échangés entre les véhicules du réseau.

Dans cette section, nous décrirons les différentes étapes de l'algorithme de clustering. Pour ce faire, nous définissons deux étapes :

➢ Etape 1 : Election du CH :

Le but de cette étape est l'élection des Cluster-Head afin d'entamer la formation des clusters dans l'étape suivante.

Cette étape commence par la prise de décision locale pour devenir Cluster-Head. Chaque véhicule V_i choisit un nombre aléatoire compris entre 0 et 1, si ce nombre est inférieur à une valeur seuil $S(V_i)$, le véhicule devient Cluster-Head. Le seuil $S(V_i)$ est définie comme suit :

$$S_{V_i} = \frac{P}{1 - P * (r \ mod \ \frac{1}{P})}$$

Où :

P : pourcentage désiré de cluster-Head pendant un round.

r : numéro du round.

➢ Etape 2 : Formation des clusters :

Une fois qu'un véhicule soit élu CH, il diffuse un message dit message d'invitation (advertisment en anglais) pour inviter les véhicules qui lui sont adjacents à rejoindre son cluster.

Ensuite chaque véhicule ayant reçu le message d'invitation, décide de son appartenance à un cluster. A la réception du premier message d'invitation le véhicule se met en attente d'autres invitations pendant une courte période, une fois que ce temps est écoulé sans avoir reçu d'autres messages, il adhère au cluster du CH l'ayant invité en premier, cependant, s'il y'a eu réception d'autre invitations de la part de plusieurs CH, le véhicule va choisir celui qui a la plus grande puissance de transmission afin de le rejoindre. Ainsi la formation des clusters est faite.

Ces 2 étapes forment un processus qui sera répété chaque période de 10 secondes, appelé round, dans le but d'altérer le rôle du CH entre les véhicules du réseau.

III.5.b. Protocole de détection de conduite agressive :

Comme nous l'avons décrit précédemment, l'approche proposée repose sur un VANET organisé en clusters, les étapes énumérées ci-dessous du protocole permettent de détecter une infraction commise par les conducteurs des véhicules et de la signaler au serveur de police.

➢ Etape 01 : Détection d'une infraction routière :

On suppose qu'un véhicule enfreigne la distance de sécurité ou dépasse la vitesse autorisée par la loi, une infraction sera détectée par les véhicules adjacents et un message contenant une photo de la plaque d'immatriculation liée à l'heure et à la géolocalisation où il a été repéré sera envoyé au Cluster-Head.

➢ Etape 02 : Le test de confiance :

Une fois que le CH reçoit un message d'alerte de l'un de ses membres, il effectue un test, appelé test de confiance, qui a pour but de vérifier si le véhicule alertant est digne de confiance

ou non. Ce test se fait en comparant la valeur de confiance T_i de ledit véhicule à un certain seuil T fixé à l'avance. Si $Ti < T$ alors le message est ignoré sinon, le CH va générer un message de dénonciation du véhicule qui a commis la contravention afin de l'envoyer à la RSU la plus proche.

➢ Etape 03 : envoi du message au serveur de police :

La RSU à son tour s'en charge de communiquer le message au serveur de police.

L'organigramme du processus de détection automatique d'une infraction routière est illustré sur la figure Fig. III.9.

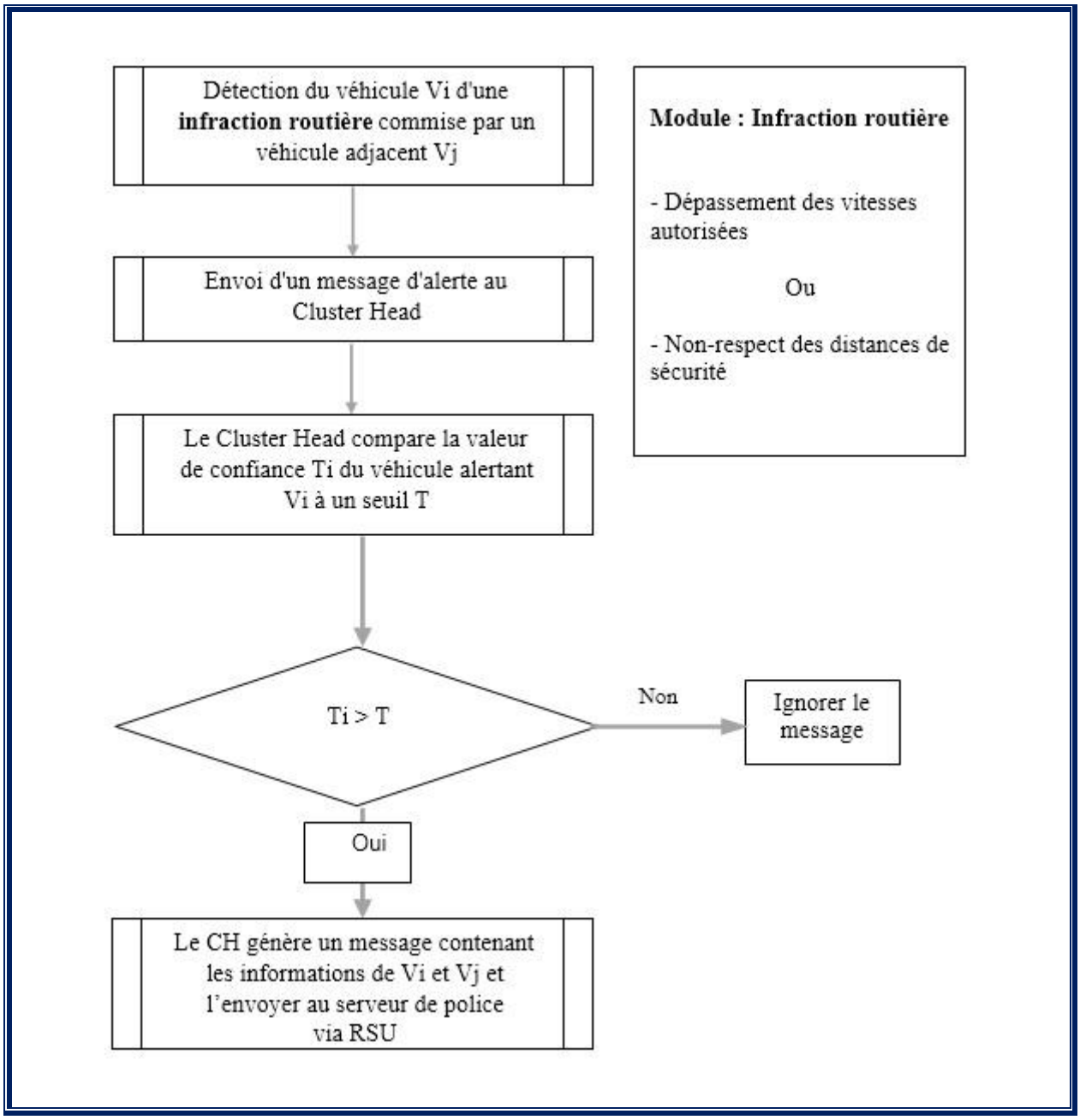


Fig. III. 9 : *Organigramme de détection automatique d'une infraction routière.*

III.5.c. Détection d'une infraction routière :

➢ Algorithme de dépassement des vitesses autorisées :

Problème posé :

On suppose qu'un ensemble de véhicules circulent sur une voie qui est limitée à 80km/h, à un moment donné, l'un de ces véhicules enfreigne la vitesse autorisée en roulant à une vitesse moyenne de 100km/h ou plus (comme indiqué sur la figure *Fig. III.10*) sachant que la route ne dispose ni de radar ni de présence d'agents de police. Comment faire pour dénoncer cet acte ?

Fig. III. 10 : *Grand excès de vitesse.*

L'objectif de cet algorithme est de détecter les véhicules à grande vitesse et réduire le nombre d'accidents afin d'assurer la sécurité des voyageurs ainsi que celle des piétons.

✓ Algorithme de détection de dépassement des vitesses (ADDV) :

La motivation derrière les réseaux ad hoc de véhicules (VANET) est d'améliorer la sécurité routière et l'efficacité de la conduite. Leurs applications s'appuient sur le principe d'échange de messages entre les nœuds du réseau. Notre approche est basée sur ce principe.

En effet les informations décrivant l'état d'un véhicule à un instant donné (géolocalisation, instant, etc.) seront encapsulées dans des messages dits message « **Hello** » et seront échangés périodiquement, chaque 2 secondes, entre les différents membres d'un cluster, cela va permettre à chaque fois de calculer la vitesse actuelle de l'un des véhicules voisins dans le réseau, ainsi, en cas de dépassement de la vitesse limitée par la loi, un message

dit message d'alerte, contenant les informations du véhicule contrevenant, est envoyé au serveur de police en transitant par le Cluster-Head (CH) et la RSU.

- ✓ **Fonctionnement de l'algorithme :**

L'échange du message « **Hello** » permet à un véhicule de calculer la vitesse moyenne avec laquelle roule son voisin, le contenu de ce message est le suivant :

$\boldsymbol{Hello\_Message} = \{\boldsymbol{ID\_Vehicule}, \boldsymbol{Position\_X}, \boldsymbol{Position\_Y}, \boldsymbol{Position\_Z}\}$ Où :

- $\boldsymbol{ID\_Vehicule}$: est l'identifiant du véhicule dans le réseau ;
- $\boldsymbol{Position\_X}, \boldsymbol{Position\_Y}, \boldsymbol{Position\_Z}$: sont les coordonnées GPS (X, Y, Z) ;

L'envoi d'un message de type « **Hello »** à un instant T_1 suivi d'un autre message du même type à un instant T_2 avec un écart de 2 secondes permet au véhicule récepteur d'estimer la vitesse moyenne du véhicule source durant ce laps de temps.

Pour pallier le problème posé précédemment, la voiture va jouer le rôle d'un agent de police ou d'un radar, en comparant la vitesse calculée V avec V_L représentant la vitesse autorisée sur la voie où les véhicules circulent, s'il y'a dépassement de celle-ci, ladite voiture s'en charge alors de dénoncer le chauffard auprès du serveur de police en passant par le CH et la RSU.

Algorithme : algorithme de détection de dépassement des vitesses.

Entrée : données des messages Hello, vitesse limitée V_L.

Sortie : action effectuée sur le véhicule émetteur.

Type $Hello\_Tab = structure$;
    ID : int ;
    X, Y, Z: $double$;
    T : $time\_t$;
End ;

Var $helloTab = fichier\ de\ Hello\_Tab$;
H : $enregistrement\ de\ type\ Hello\_Tab$;
i, ID : int ;
$isTrue$: $bool$;
$X_1, Y_1, Z_1, X_2, Y_2, , Z_2, V$: double ;
T_1, T_2 : $time\_t$;

Begin

$isTrue = false$;

$i = 0$;

$ID =$ *récupérer l'id du msg reçu* ;

X_1, Y_1, Z_1 : *récupérer les coordonnées du msg reçu* ;

T_1 : *récupérer l'instant actuel lors de la réception du msg Hello* ;

while $((i < helloTab.size()) \&\& (isTrue == false))$

If $(H.ID == ID)$

$isTrue = True$;

// Récupérer les informations stockées lors de la précédente réception.

$X_2 = H.X$; $Y_2 = H.Y$; $Z_2 = H.Z$; $T_2 = H.T$;

//Ensuite, mettre à jour la table en modifiant les anciennes valeurs par les nouvelles reçues ;

else

$i = i++$;

End if ;

End while ;

if $(!isTrue)$

$H.ID = ID$;

// Stocker les informations reçues dans $helloTab$;

$H.X = X_1$; $H.Y = Y_1$; $H.Z = Y_1$; $H.T = T_1$;

$helloTab.insert\ (\ helloTab.end()\ , H)$;

else

$V = sqrt((X_2 - X_1)^2 + (Y_2 - Y_1)^2 + (Z_2 - Z_1)^2) / (T_2 - T_1)$;

if $(V > V_L)$

// Envoyer un message d'alerte contenant les informations du véhicule en question au CH pour que ce dernier puisse le dénoncer au serveur de police en transitant par la RSU ;

End if ;

End if ;

End.

- ✓ **Les étapes détaillées de l'algorithme ADDV :**

Lorsqu'un véhicule récepteur reçoit un message de type « **Hello** », il va d'abord vérifier s'il y a eu au préalable un échange de message entre les deux véhicules, et cela se fait en parcourant les éléments du fichier $helloTab$, qui sont de type « enregistrement », tout en comparant l'identifiant ID reçu à ceux déjà enregistrés. Si l'ID du véhicule n'est pas présent dans le fichier alors les données : ID, coordonnée GPS (X_1, Y_1, Z_1) et le temps T_1 (nous avons pris en considération le retard de transmission du message comme négligeable) seront rajoutées au fichier. Dans le cas contraire , i.e. il y a une correspondance d'identifiant et donc une communication a déjà été établie, alors les données seront stockées temporairement pour que le véhicule puisse récupérer, les données stockées précédemment, dans les variables : les coordonnées GPS(X_2, Y_2, Z_2) et le temps T_2, et met à jour le fichier d'enregistrement.

Suite à ça, la vitesse moyenne du même véhicule peut être calculée telle que mentionnée dans l'algorithme **ADDV** où (X_1, Y_1, Z_1) et (X_2, Y_2, Z_2) sont les coordonnées représentant les positions reçues aux instants T_1 et T_2 respectivement.

Maintenant, la vitesse calculée va être comparée avec V_L représentant la vitesse maximale autorisée sur cette voie et qui était attribuée par la RSU auparavant, si elle est supérieure à V_L, alors un message d'alerte sera envoyé au cluster Head « CH », ce dernier va effectuer le test de confiance suivant :

If ($T_i >= T$) then
    // Envoyer un message pour dénoncer le véhicule auprès du serveur de police via la RSU ;
else
    // Ignorer le message ;
End ;

Explication :

Si le degré de confiance T_i du véhicule dénonciateur est supérieur ou égal au seuil *T*, le CH va générer un message afin de l'envoyer à la RSU la plus proche, cette dernière à son tour s'en charge de le communiquer au serveur de police, sinon il va ignorer le message.

Remarque :

A l'issue de chaque round, le fichier $helloTab$ sera vidé en utilisant l'instruction $helloTab.clear()$ pour éviter la surcharge de ce dernier.

➢ Algorithme de calcul de la distance de sécurité :

Problème posé :

Dans cet exemple, on suppose qu'un ensemble de véhicules sont en circulation moyenne et haute densité sur une voie particulière comme illustré sur la figure *Fig. III.11*.

Supposons que l'un de ces véhicules enfreigne la distance minimale et se rapproche de très près du véhicule de tête, à un moment donné, ce dernier pourrait freiner subitement, ce qui pourrait par la suite provoquer une collision par l'arrière et engendrer des dégâts assez graves. Comment procéder afin de dénoncer le responsable de cet acte ?

Fig. III. 11 : *Exemple de non-respect de la distance de sécurité minimale.*

Nous proposons un algorithme qui est utilisé principalement pour calculer la distance entre les véhicules dans un réseau VANET. Son objectif est de détecter les véhicules ne respectant pas la distance de sécurité minimale entre deux véhicules adjacents afin de réduire le nombre de collisions et ainsi le nombre d'accidents afin d'assurer la sécurité routière.

✓ Algorithme de calcul de la distance minimale (ACDM) :

Dans cet algorithme, les informations nécessaires pour calculer la distance entre les véhicules sont les mêmes que celles utilisés dans l'algorithme de détection de dépassement des vitesses (ADDV), i.e. : l'identifiant et la géolocalisation.

Pour éviter de surcharger le réseau, l'algorithme de calcul de la distance utilisera les mêmes messages **Hello** échangés précédemment pour calculer à la fois la vitesse et la distance.

✓ **Fonctionnement de l'algorithme :**

Inversement à l'algorithme **ADDV**, dans cet algorithme l'envoi d'un seul message de type **Hello** à un instant *T* par un véhicule émetteur vers un autre véhicule adjacent permet à ce dernier d'estimer la distance entre lui et le véhicule émetteur à cet instant précis.

Pour pallier le problème posé précédemment, la voiture va jouer le rôle d'un agent de police, en comparant la distance calculée *D* avec la distance limitée D_L exigée par la loi, s'il y a infraction de cette dernière, ladite voiture s'en charge alors de dénoncer le chauffard auprès du serveur de police en passant par le CH et la RSU.

Algorithme : algorithme de calcul de la distance minimale.

Entrée : données des messages Hello, distance limitée D_L.

Sortie : action effectuée sur le véhicule émetteur.

Var $X_1, Y_1, X_2, Y_2, Z_1, Z_2, D : double$;

Begin

// Le véhicule ayant reçu le message Hello récupère ses coordonnées GPS.

$X_1 = getX$;

$Y_1 = getY$;

$Z_1 = getZ$;

// Ensuite le véhicule récupère les coordonnées GPS du véhicule émetteur du message Hello.

$X_2 = X$;

$Y_2 = Y$;

$Z_2 = Z$;

// Enfin le véhicule récepteur calcule la distance les séparant.

$D = sqrt((X_2 - X_1)^2 + (Y_2 - Y_1)^2) + (Z_2 - Z_1)^2)$;

If $(D < D_L)$

Envoyer un message d'alerte contenant les informations du véhicule en question au CH pour que ce dernier puisse le dénoncer au serveur de police en transitant par la RSU ;

End if ;

End.

- ✓ **Les étapes détaillées de l'algorithme ACDM :**

Lorsqu'un véhicule récepteur reçoit un message de type « **Hello** », il va d'abord récupérer ses propres coordonnées dans les variables (X_1, Y_1, Z_1) et il récupère également les coordonnées du véhicule émetteur dans les variables (X_2, Y_2, Z_2) au même instant.

Par la suite, il procède au calcul de la distance entre lui et le véhicule émetteur du message « **Hello** » en utilisant la formule de calcul des distances [15] telle qu'elle est définie dans l'algorithme **ACDM**.

Une fois que la distance *D* est calculée, elle va être comparée avec la distance limitée D_L exigée par la loi et qui était attribuée par la RSU auparavant. Si elle est inférieure à D_L, alors un message d'alerte sera envoyé au Cluster-Head « CH », ce dernier va effectuer le même test de confiance que celui de l'algorithme **ADDV**.

Par la suite, si la tâche de dénonciation du véhicule auprès de la RSU est exécutée, cette dernière s'en charge de communiquer le message de dénonciation de ce véhicule au serveur de police.

III.5.d. Contrainte de la solution proposée :

Comme tout protocole, il y a certaines contraintes que l'on doit prendre en compte. En effet, même si les réseaux Ad hoc véhiculaires (VANET) apportent d'énormes avantages à la société, ils soulèvent de nombreux défis où les problèmes de sécurité et de confidentialité sont les plus critiques.

Afin de remédier aux contraintes rencontrées, nous concevons un système de contrôle basé sur le schéma de cryptage à seuil.

III.5.e. Cryptage des données :

Afin d'améliorer la sécurité de notre réseau VANET et d'assurer la confidentialité et l'intégrité des informations transmises entre ses différentes entités, les messages échangés doivent être cryptés, c'est-à-dire les rendre inintelligibles. Pour ce faire, nous allons utiliser un schéma de cryptage basé sur les courbes elliptiques (ECC, Elliptic Curve Cryptography en anglais) et la signature de Schnorr.

L'utilisation des courbes elliptiques en cryptographie permet l'adoption de nouveaux crypto systèmes. Les courbes elliptiques sont bien adaptées à la cryptographie à clé publique. Cette cryptographie repose sur la difficulté de résoudre le problème du logarithme discret sur le groupe des points d'une courbe elliptique.

Ce qui fait la différence des algorithmes de chiffrement à base de courbes elliptiques par rapport aux algorithmes basés sur les entiers comme RSA ou El-Gamal est que, pour les vaincre, il faut résoudre le logarithme discret sur le groupe de la courbe elliptique, et non un problème analogue sur les entiers. Ces groupes sont plus difficiles à manipuler, ils peuvent différer beaucoup les uns des autres si on change les paramètres [16].

En cryptographie, le protocole d'authentification de Schnorr (souvent abrégé protocole de Schnorr) est une preuve à divulgation nulle de connaissance décrite en 1989 par Schnorr dont la sécurité repose sur la difficulté du problème du logarithme discret et servant à prouver la connaissance d'un logarithme discret. Ce protocole peut être dérivé en une signature numérique en rendant la preuve non interactive par « l'heuristique de Fiat-Shamir » [17].

Dans la conception de notre approche, nous allons utiliser le nouveau schéma de cryptage des signes basé sur le crypto système à courbe elliptique et le schéma de signature de Schnorr en utilisant l'idée du cryptage authentifié. Ce schéma de chiffrement de signe n'utilise pas la fonction de hachage unidirectionnelle.

Le tableau suivant résume les principales notations utilisées dans cette approche :

Notation	***Description***
v_i	Identifiant du véhicule i
$K_{v_i}, \widehat{K}_{v_i}$	La clé privée et la clé publique du véhicule v_i
$K_{v_j}, \widehat{K}_{v_j}$	La clé privée et la clé publique du véhicule v_j
$K_{v_k}, \widehat{K}_{v_k}$	La clé privée et la clé publique du véhicule v_k
$K_c, \widehat{K}_c$	La clé privée et la clé publique du cluster C
$K_c^i, \widehat{K}_c^i$	La part de clé privée et publique du véhicule v_i
$K_s, \widehat{\mathrm{K}}_s$	La clé publique et la clé privée du serveur police
$K_{RSU}, \widehat{\mathrm{K}}_{RSU}$	La clé publique et la clé privée de la RSU
B_k	Facture du conducteur v_k
$\mathcal{E}_k$	Preuve d'une infraction routière du véhicule v_k
σ_{B_k}	Signature numérique de la facture
C_k	montant de la facture du conducteur v_i
$< L_{v_k}, T_{v_k} >$	< Géolocalisation, Instant > de l'infraction du véhicule v_k
$< t, n >$	schéma de contrôle du seuil
E_p	courbe elliptique
Q	point de base sur E_p
q	grand nombre premier
p	Nombre d'éléments du champs de la courbe E_p.

Tableau III. 1 : *Notations.*

La procédure de ce schéma contient trois phases : la phase d'initialisation, la phase de cryptage des signatures et la phase de vérification et de récupération des messages [18].

➢ La phase d'initialisation :

Notre schéma requiert un coordinateur RSU, qui est responsable de la génération des paramètres. La RSU choisit un point de base Q, appelé le point générateur d'une courbe elliptique E_p, d'un ordre premier de q, où q est un grand premier (q ≥ 160 bits). Le choix de Q est souvent aléatoire.

Dans le cadre de notre travail, chaque véhicule $v_i \in C$ choisit un entier aléatoire $\hat{K}_{v_i} \in [1, q-1]$ comme clé privée et calcule la clé publique correspondante, représentée par un point :

$$K_{v_i} = \hat{K}_{v_i} \cdot Q$$

Et envoie K_{v_i} à la RSU. Enfin, cette dernière publie les paramètres p, q, Q, K_{v_i}.

➢ La phase de cryptage de données :

Supposons qu'un message $m \in [1, p-1]$ sera crypté par $v_i \in C$, puis envoyé au véhicule $v_j \in C$. Dans ce cas, chaque véhicule $v_i \in C$ code tout message m comme un point P_m de la courbe elliptique E_p, l'opérations de cryptage est faite ainsi :

- ✓ **Étape 1 :** le signataire v_i choisit un entier aléatoire $k \in [1, q-1]$ et calcule :

$$y_1 = k \cdot Q$$

Et

$$y_2 = k \cdot K_{v_j}$$

- ✓ **Étape 2 :** le signataire v_i génère le cryptage de la signature $< r, s >$ en calculant :

$$r = m \cdot (y_2)_x \ mod \ p$$

Et

$$s = k - \hat{K}_{v_i} \cdot r \ mod \ q$$

Où $(y_2)_x$ est une coordonnée x du point y_2.

Enfin, le signataire v_i envoie le cryptage (r, s) et y_1 au récepteur v_j via un canal de transmission.

Comme indiqué dans les équations de cryptage de la signature, le cryptage des signes (r, s) inclut non seulement le message *m* (caché dans *r*), mais inclut également la signature par la clé privée $\hat{K}_{v_i}$ du signataire v_i.

➢ Phase de vérification et de récupération des messages :

Une fois que v_j a reçu le cryptage de la signature (r, s), il peut vérifier sa validité et récupérer le message *m* en procédant comme suit :

✓ **Étape 1 :** il calcule :

$$y_1' = r \cdot K_{v_i} + s \cdot Q$$

et

$$y_2' = \hat{K}_{v_j} \cdot y_1'$$

✓ **Étape 2 :** il vérifie si $y_1 = y_1'$ est correct. Si c'est correct, le cryptage des signes (r, s) est valide, sinon il n'est pas valide.

✓ **Étape 3 :** dans le cas où le cryptage des signes est valide, il récupère le message *m* par :

$$m = r \cdot (y_2')_x^{-1} \; mod \; p$$

III.5.f. Initialisation du système :

Pour accéder au système, certains paramètres envoyés par la RSU doivent être stockés dans l'OBU des véhicules se trouvant dans sa portée de communication comme illustré sur la figure *Fig. III.12*. Par exemple, chaque véhicule V_i aura une valeur unique pour s'identifier auprès du serveur de police. De plus, comme l'OBU devra vérifier la signature de la facture de la contravention routière, elle enregistre la clé publique du serveur de police K_s. Il devra également générer une clé paire $<K_i, \widehat{K}_i>$, où la clé publique K_i est liée à son identifiant et partagée avec le serveur de police, les véhicules du même cluster ainsi que la RSU tandis que la clé privée $\widehat{K}_i$ est conservée secrète.

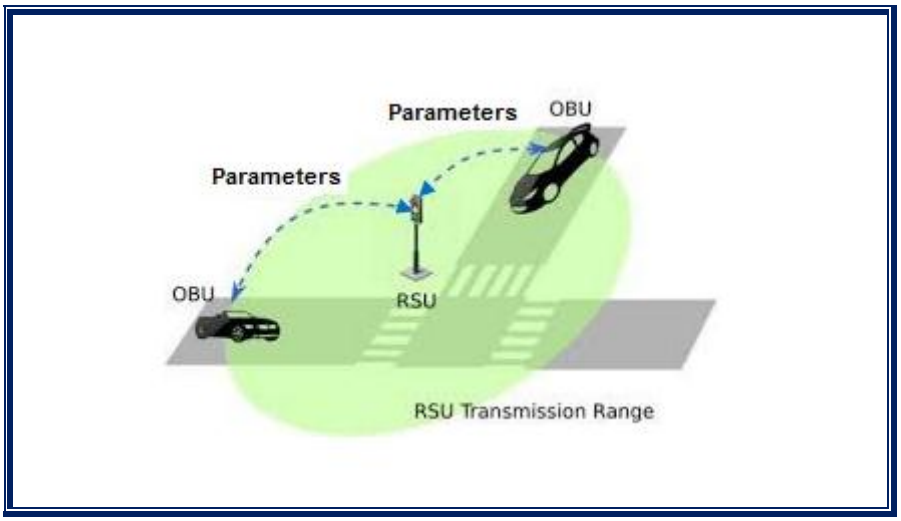


Fig. III. 12 : *Echange des paramètres entre la RSU et les véhicules.*

III.5.g. Signature et vérification des alertes frauduleuses basées sur la cryptographie à seuil :

Pour prouver le mauvais comportement d'un conducteur accusé, le système conserve des preuves contre lui, ces dernières contiendront le type, la géolocalisation, le temps de l'infraction ainsi qu'une photo de sa plaque d'immatriculation. Ces données sont envoyées au serveur de police par les véhicules accusateurs. Après vérification, le serveur de police facture son propriétaire en calculant une amende en fonction de l'infraction commise, tandis qu'une récompense est offerte aux chauffeurs alertant (bonification des points de permis ou un sursis pour les bons conducteurs).

À travers un schéma de seuil $< t, n >$, nous considérons un cluster $C = \{v_1, v_2, \ldots, v_n\}$ de véhicules légitimes, où *n* est le nombre de véhicules dans le Cluster *C*. Par conséquent, la valeur du paramètre *n* dépend du nombre de véhicules dans le cluster sélectionné par l'algorithme de clustering. En ce qui concerne le paramètre *t*, plusieurs travaux ont été effectués pour déterminer si la valeur de *t* doit être variable ou fixe. Le seuil *t* pourrait être défini comme un paramètre variable dont sa valeur évolue dans le temps, comme ce qui a été proposé dans certaines solutions existantes dans la littérature. La valeur du seuil *t* sera alors négociée lors de la formation du groupe (représente 80% du nombre d'éléments du cluster).

Une fois formés, les véhicules du cluster partagent une clé privée (comme indiqué sur la figure *Fig. III.13*) et coopèrent pour produire la signature des preuves contre tout véhicule contrevenant pendant le voyage.

Tout *(t -1)* véhicules ou moins ne peuvent pas reconstruire la clé privée ou forger une signature valide. Même un attaquant qui peut compromettre au plus *(t-1)* véhicules ne peut découvrir aucune information sur la clé privée.

Toutes les opérations du Cluster *C* sont gérées par des unités RSU coordinatrices, qui sont responsables de la distribution partielle des clés, de la collecte et de la vérification partielle des signatures et du calcul des signatures de groupes.

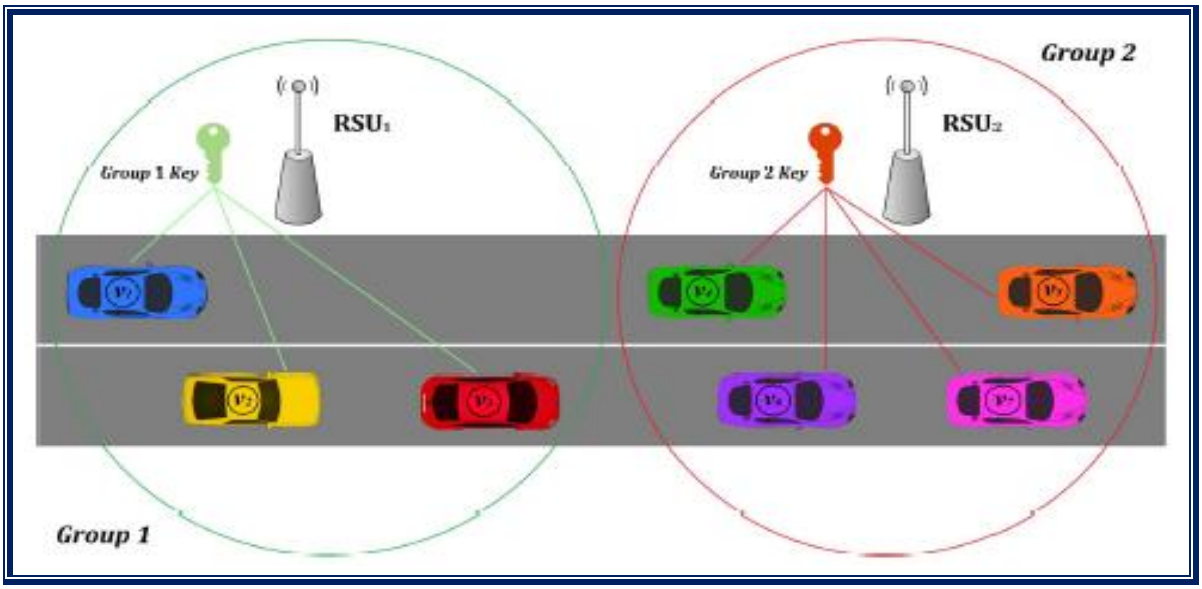


Fig. III. 13 : *Processus de cryptographie dans les systèmes de contrôle à seuil.*

Pour la conception de notre approche proposée, nous allons utiliser un autre nouveau schéma de seuil $< t, n >$ basé sur notre schéma de cryptage de données proposé [18].

Supposons qu'une infraction commise par le conducteur du véhicule $v_k \in C$ a été détectée, par le véhicule $v_i \in C$, en passant sur une géolocalisation L_{v_k} donnée à un instant T_{v_k} donné. Le type de l'infraction peut-être, soit un dépassement de la vitesse autorisée dans cette zone ou bien un non-respect de la distance de sécurité minimale entre les véhicules. Suite à ça, un message d'alerte sera généré et crypté, par le véhicule v_i, en suivant la méthode de cryptage de données citée précédemment. Ensuite, ce message sera envoyé au CH afin de dénoncer cet acte.

Une fois que le CH a décrypté le message reçu, il effectue le test de confiance. Si le véhicule émetteur v_i est digne de confiance, le message d'alerte sera crypté et communiqué au serveur de police via la RSU, sinon il sera ignoré.

Ensuite, au niveau de la RSU, quand un message est reçu, les données : ID du véhicule accusé, le temps et la géolocalisation de l'infraction commise seront stockées dans un fichier d'enregistrement, ensuite le message d'alerte sera retransmis au serveur de police. Cela nous permettra de produire la signature de la preuve $\mathcal{E}_k = < L_{v_k}, T_{v_k} >$ qui est une preuve de l'infraction du véhicule v_k et qui doit être envoyée au serveur de police afin de prouver son mauvais comportement.

A la réception d'un autre message d'alerte, le contenu de ce dernier va être comparé aux informations enregistrées précédemment. Si le message concerne la même infraction, donc il ne sera pas pris en considération et sera directement retransmis au serveur de police. Dans le cas contraire, les informations de la nouvelle infraction seront enregistrées dans le fichier.

Le *Tableau III.2* représente le format du fichier contenant les données des infractions routières.

ID	Tuple < Géolocalisation, Temps >
ID du véhicule accusé v_k	Infraction 1 : $< L_{v_k}, T_{v_k} >$ Infraction 2 : $< L_{v_k}, T_{v_k} >$ . . . Infraction N : $< L_{v_k}, T_{v_k} >$

Tableau III. 2 : *Format du fichier des infractions routières au niveau de la RSU.*

Enfin, au niveau du serveur de police, chaque alerte reçue sera classée selon l'ID du véhicule dénoncé, sa plaque d'immatriculation, le type de l'infraction, le tuple < géolocalisation, temps > et les ID des véhicules dénonciateurs. Le serveur de police attend que la RSU lui fournit la preuve de l'infraction afin de générer la facturation automatique de la contravention routière selon le type de l'infraction commise et de l'envoyer au conducteur du véhicule v_k.

Le *Tableau III.3* représente les informations des infractions routières enregistrées au niveau du serveur de police.

ID	Plaque d'immatriculation	Type de l'infraction	Tuple < Géolocalisation, Temps >	Les ID des véhicules dénonciateurs
ID du véhicule dénoncé v_k	Du véhicule v_k	Dépassement de la vitesse autorisée et/ou non-respect de la distance de sécurité minimale	$< L_{v_k}, T_{v_k} >$ $< L_{v_k}, T_{v_k} >$ . . . $< L_{v_k}, T_{v_k} >$	ID 1 ID 1 . . . ID M

Tableau III. 3 : *Format du fichier des infractions routières au niveau du serveur de police.*

Pour appuyer l'accusation de preuves plus concrètes, le sous-ensemble de *t* véhicules adjacents de v_k l'ayant dénoncé produira alors en collaboration la signature de la preuve $\mathcal{E}_k = < L_{v_k}, T_{v_k} >$ grâce à un schéma de seuil qui passe par les phases suivantes :

➢ Phase de choix des paramètres :

Dans ce schéma de cryptage à seuil, le récepteur est le serveur de police. Cependant, le signataire est changé en un groupe de signataires qui est désigné par $C = \{v_1, v_2, \ldots, v_n\}$. C'est-à-dire que *C* est un ensemble de *n* signataires dans lequel chaque membre peut signer le cryptage de signe partiel.

Tout d'abord, un coordinateur RSU génère la clé privée $\hat{K}_c \in [1, q-1]$ du Cluster *C*, et calcule sa clé publique correspondante K_c, représentée par un point, telle que :

$$K_c = \hat{K}_c \cdot Q$$

Dans cette section, les paramètres p, q, Q, K_{v_i} sont les mêmes que ceux de la sous-section III.5.e de la section III.5. Enfin la RSU publie également K_c et K_s (K_s est la clé publique du serveur de police).

➢ Phase de partage de la part de clé privée :

Dans les étapes suivantes, nous présentons un protocole de partage de la part de clé privée basé sur le partage de secret. La clé privée $\hat{K}_c$ du groupe *C* sera distribuée sur v_i $(1 \leq i \leq n)$.

✓ **Étape 1 :** la RSU génère aléatoirement un polynôme secret *G* de degré (*t - 1)* tel que :

$$G(x) = a_0 + a_1 x + \ldots + a_{t-1} x^{t-1} \; mod \; q$$

Où $$G(0) = a_0 = \hat{K}_c$$

Enfin, elle calcule la part de clé privée $\hat{K}_c^{(i)}$ de tout véhicule $v_i \in C$ telle que :

$$\hat{K}_c^{(i)} = G(i)$$

Et publie la part de clé publique correspondante $K_c^{(i)}$ telle que :

$$K_c^{(i)} = \hat{K}_c^{(i)} \cdot Q.$$

✓ **Étape 2 :** Sur un canal de communication sécurisé, le coordinateur RSU envoie pour chaque véhicule $v_i \in C$ sa part de clé privée $\hat{K}_c^{(i)}$.

➢ Phase de cryptage à seuil :

Supposons que $\mathcal{E}_k \in [1, p-1]$ soit crypté par *t* participants du cluster C pour le récepteur serveur de police. Dans cette phase, le cryptage de signature de groupe (r, s) sera généré. Cette phase comprend quatre étapes :

✓ **Étape 1 :** chaque véhicule $v_i \in C$ ayant détecté une infraction, choisit un nombre aléatoire $c_i \in [1, q-1]$, et calcule Y_i et Z_i tels que :

$$Y_i = c_i \cdot Q$$

et

$$Z_i = c_i \cdot K_s$$

L'ensemble de Y_i et Z_i est envoyé sur un canal de communication sécurisé à un coordinateur RSU à leur portée.

- ✓ **Étape 2 :** A la réception, le coordinateur RSU calcule *Z* et *r* tels que :

$$Z = \sum_{i=1}^{t} Z_i$$

et

$$r = \mathfrak{E}_k \cdot (Z)_x \; mod \; p.$$

où $(Z)_x$ est la coordonnée *x* de *Z*.

Ensuite, le coordinateur RSU diffuse *r* aux véhicules $v_i \in C$.

- ✓ **Étape 3 :** chaque véhicule récepteur calcule x_i et e_i tels que :

$$x_i = \prod_{j=1, j\neq i}^{t} \frac{-j}{(i-j)} mod \; q$$

$$e_i = \hat{\mathrm{K}}_c^{(i)} \cdot x_i \; mod \; q$$

et répond par sa signature partielle s_i telle que :

$$s_i = \; c_i - e_i \cdot \; r \; mod \; q$$

- ✓ **Étape 4 :** lors de la réception d'au moins *t* signatures partielles, le coordinateur RSU calcule Y_i' tel que :

$$Y_i' = r \cdot x_i \cdot K_c^{(i)} + s_i \cdot Q$$

Si $Y_i = Y_i'$ pour toutes les signatures partielles, le coordinateur RSU calcule *s* tel que :

$$s = \sum_{i=1}^{t} s_i \; mod \; q$$

Enfin, $\sigma_E = < r, s, \; Y_1, Y_2, \ldots, Y_t >$ est la signature du groupe C accompagnée de la preuve $\mathfrak{E}_k = < L_{vk}, T_{vk} >$ qui sera cryptée avec la clé publique K_s du serveur de police.

➢ Phase de vérification et de récupération des messages :

Dans cette phase, le serveur de police peut alors vérifier la validité de la signature à l'aide de la clé publique K_c du groupe C et récupérer le message reçu dans le cas d'une signature valide. Pour ce faire, le serveur de police exécute deux étapes :

✓ **Étape 1 :** il calcule Y, Y' *et* Z' tels que :

$$Y = \sum_{i=1}^{t} Y_i$$

$$Y' = r \cdot K_C + s \cdot Q$$

et

$$Z' = \hat{\mathrm{K}}_S \cdot Y'$$

✓ **Étape 2 :** si $Y = Y'$, alors la signature est valide et le serveur de police décrypte $\mathcal{E}_k$ tel que :

$$\mathcal{E}_k = r \cdot (Z')_x^{-1} \, mod \, p$$

où $(Z')_x^{-1}$ est la coordonnées *x* de Z'.

Sinon, la signature n'est pas valide, et le serveur de police prouve que cette alerte est une alerte frauduleuse.

III.5.h. Facturation automatique des contraventions routières :

Dans le cas d'une signature valide, le serveur de police produit la facture de la contravention routière et l'envoie au conducteur du véhicule v_k. La facture est signée par le serveur de police pour garantir son intégrité ainsi que son authenticité (voir la figure *Fig. III.14*).

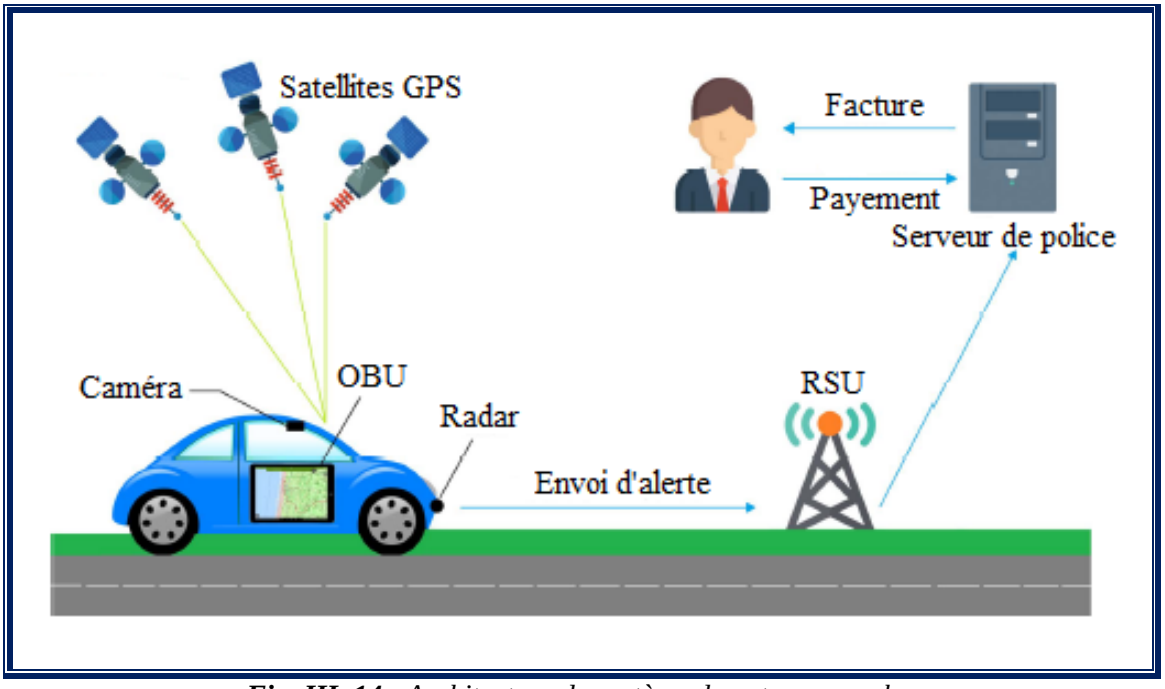


Fig. III. 14 : *Architecture du système de notre approche.*

Pour ce faire, le serveur de police suit plusieurs étapes [18] :

- ✓ **Étape 1 :** le serveur de police génère automatiquement la facture de contravention du véhicule v_k, notée B_k, avec le montant à payer selon le type de l'infraction commise, notée C_k.

- ✓ **Étape 2 :** cette étape consiste à chiffrer la facture à l'aide de la clé publique du véhicule v_k puis à la signer à l'aide de la clé privée du serveur de police $\hat{K}_S$. Pour ce faire, ce dernier s'appuie sur le même schéma de cryptage de données précédent. D'abord, il choisit aléatoirement $c \in [1, q-1]$ et calcule y_1 et y_2 tels que :

$$y_1 = c \cdot Q$$

et

$$y_2 = c \cdot K_{v_k}$$

Ensuite, il calcule *r* et *s* tels que :

$$r = B_k \cdot (y_2)_x \; mod \; p$$

et

$$s = c - \hat{K}_s \cdot r \; mod \; q$$

- ✓ **Étape 3 :** enfin, le serveur de police délivre la signature $\sigma_{B_k} = < r, s, y_1 >$ incorporant la facture de contravention B_k cachée dans *r*.

A la fin du processus de facturation, tout conducteur du véhicule v_k reçoit sa facture de contravention. Avant le paiement, l'OBU authentifie la signature de la facture de contravention à l'aide de la clé publique du serveur de police et récupère le coût de facturation de la contravention routière. Le conducteur procède au paiement si la signature est valable.

- ✓ **Étape 1 :** le véhicule v_k calcule :

$$y_1' = r \cdot K_s + s \cdot Q$$

$$y_2' = \hat{K}_{v_k} \cdot Y_1'$$

- ✓ **Étape 2 :** si $y_1 = y_1'$, la facture de contravention B_k est reconstruite telle que :

$$B_k = r \cdot (y_2')_x^{-1} \; mod \; p$$

où $(y_2')_x^{-1}$ est la coordonnées *x* de $(y_2')^{-1}$.

III.5.i. Format des factures de contravention routière :

Pour se conformer au paradigme de la ville intelligente qui vise à améliorer la sécurité routière et à simplifier les services offerts aux citoyens, le système de facturation automatique des contraventions routières doit facturer les conducteurs accusés au format numérique en adoptant les factures de contravention électroniques comme un service simple et pratique.

Nous proposons une approche pour la facture de contravention routière. Cette dernière est organisée en trois parties comprenant des informations relatives à la facture de contravention ainsi que celles sur la violation de la loi, des informations sur son propriétaire et des informations relatives au serveur de police accompagnées des preuves numériques générées par le groupe de signataires. *Le tableau III.4* illustre le format de la facture de contravention.

Il y a plusieurs aspects de la phase de facturation qui doivent être pris en considération pour produire la facture de contravention finale pour un conducteur contrevenant donné. Cependant, notre approche proposée n'aborde pas les détails de la facturation, par conséquent, elle n'exclut pas d'autres types d'applications.

Informations sur la facture finale de la contravention routière	Identifiant de la facture finale de contravention
	Tuple de géolocalisation sur l'infraction routière
	Montant à payer
	Date d'échéance de la facturation
Informations sur le conducteur	Identifiant du conducteur
	Numéro de la plaque d'immatriculation
	Clé publique
Informations sur le serveur de police	Identifiant du serveur de police
	Clé publique
	Signature de seuil pour la preuve de l'infraction routière

Tableau III. 4 : *Format de la facture de contravention routière.*

III.6. Conclusion :

Dans ce chapitre, nous avons présenté notre approche ainsi que les algorithmes appropriés afin de détecter les véhicules à grande vitesse et les véhicules qui ne respectent pas la distance de sécurité minimale exigée par la loi dans un réseau VANET.

En effet, lorsqu'un véhicule est observé se déplaçant plus vite que la limite de vitesse d'une voie particulière ou bien un véhicule ne respectant pas la distance de sécurité minimale sera dénoncé au Cluster-Head par les véhicules adjacents qui, lui-même, envoie un message au serveur de police via la RSU. En fonction de la fréquence des violations et avec l'aide du serveur de police, des mesures appropriées seront prises sur ce véhicule enfreignant la loi. Ainsi, en appliquant cette approche, nous pouvons réduire le nombre de véhicules qui commettent des infractions routières dans un VANET et donc diminuer le nombre d'accidents.

Bien que ce système semble promettre des avantages évidents, il existe des infractions potentielles importantes telles que les alertes frauduleuses. Dans ce chapitre, nous avons proposé une nouvelle approche de sécurité pour les systèmes de détection des actions frauduleuses. L'un des objectifs principaux de ce travail est de repérer les alertes frauduleuses sur des conducteurs innocents afin de les obliger à payer une amende de contravention routière et gagner illégalement la récompense offerte par les services autoritaires aux véhicules dénonciateurs.

L'approche proposée repose sur des communications V2V et le crypto système à seuil. Il combine des primitives cryptographiques pour protéger la confidentialité des données transmises et renforcer la garantie de leur honnêteté.

Afin d'évaluer l'efficacité de l'approche proposée, nous allons effectuer une simulation afin d'obtenir des résultats que nous allons évaluer et interpréter par la suite.

Chapitre IV :

Implémentation et Simulation

IV.1. Introduction :

Toute nouvelle solution passe par un processus d'évaluation et de validation avant son éventuel déploiement. Le moyen idéal de réaliser cette tâche est de pouvoir effectuer des tests dans des environnements réels. Cependant, de par la nature distribuée, l'environnement et la topologie complexe des réseaux véhiculaires et pour contourner ce problème, la simulation est le moyen le plus largement utilisé. En effet, il est plus facile et moins cher, par le biais de la simulation, de concevoir, d'analyser et d'évaluer les performances de toute solution.

Dans ce chapitre nous commençons par une présentation de la simulation dans les VANET. Nous décrivons ensuite, l'environnement de travail, les outils et les étapes de la simulation.

IV.2. Simulation dans les VANET :

La simulation dans les VANET implique deux différents aspects. Le premier réside aux problèmes liés à la communication entre les véhicules. Un simulateur de réseau, comme OMNeT++, fait face à ces problèmes, il se focalise sur les caractéristiques du protocole du réseau, le deuxième aspect très important est lié à la mobilité des nœuds « véhicules », c'est le simulateur SUMO qui gère la mobilité et le mouvement des véhicules. Ces deux simulateurs sont connectés via un modèle de simulation réseau appelé Veins.

IV.3. Environnement de travail :

IV.3.a. OMNeT++ :

L'environnement de développement intégré OMNeT++ (Objective Modular Network Test-bed in C++) est un espace de simulation modulaire à base de composants Open Source. Son domaine d'application principal est celui des réseaux de communication. Voir la figure *Fig. IV.1*.

OMNeT++ présente une architecture générique et flexible ce qui lui permet aussi d'être efficace dans d'autres domaines tels que les systèmes informatiques, les réseaux de files d'attente, des architectures matérielles, ou même des processus d'affaires.

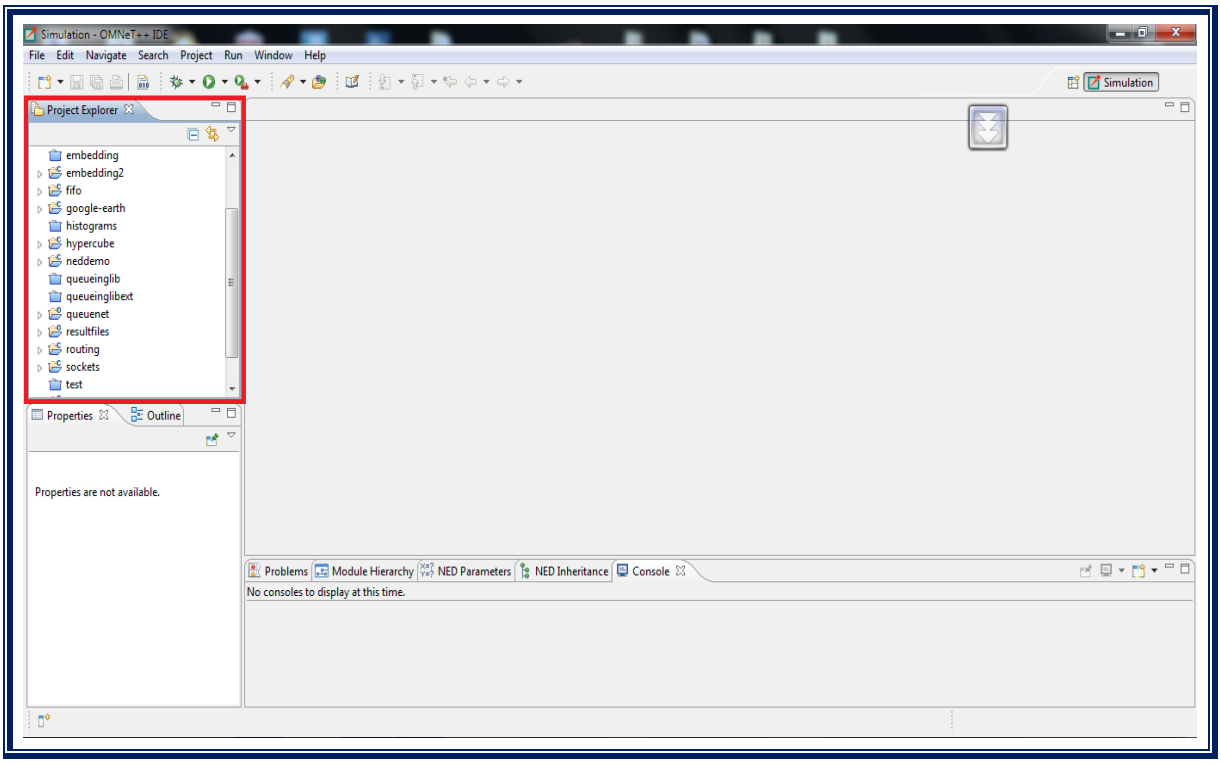


Fig. IV. 1 : *Interface graphique de l'environnement OMNeT++.*

➢ Architecture d'OMNeT++ :

L'architecture de OMNET++ est hiérarchique composée de modules (Voir la figure *Fig. IV.2*). Un module peut être soit un module simple ou bien un module composé. Les feuilles de cette architecture sont les modules simples qui représentent les classes C++. Pour chaque module simple correspond un fichier « .cc » et un fichier « .h ».

Un module composé est constitué de modules simples ou d'autres modules composés connectés entre eux. Les paramètres, les sous modules et les ports de chaque module sont spécifiés dans un fichier « .ned ».

La communication entre les différents modules se fait à travers les échanges de messages. Les messages peuvent représenter des paquets, des trames d'un réseau informatique, des clients dans une file d'attente ou bien d'autres types d'entités en attente d'un service. Les messages sont envoyés et reçus à travers des portes (gates en anglais). Les portes sont les interfaces d'émission et de réception des modules. On ne peut créer des connexions que dans un seul niveau d'hiérarchie des modules. Il est par exemple impossible de créer une connexion directe entre un module et un sous-module d'un autre module de même niveau dans la hiérarchie.

La conception d'un réseau se fait dans un fichier « .ned » et les différents paramètres de chaque module sont spécifies dans un fichier « .ini ». OMNeT++ génère à la fin de chaque simulation deux nouveaux fichiers omnet.vec et omnet.sca qui permettent de tracer les courbes et calculer des statistiques [20].

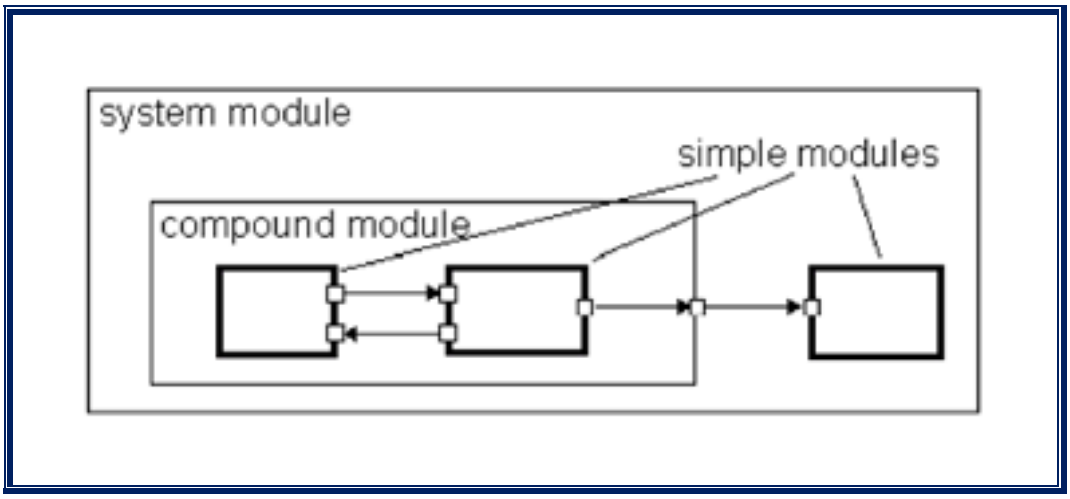


Fig. IV. 2 : *Architecture modulaire du simulateur.*

IV.3.b. SUMO :

SUMO (Simulation of Urban Mobility) est une source ouverte, microscopique, multimodale. Elle permet de simuler la manière dont une demande de trafic donnée qui se compose de véhicules individuels se déplaçant à travers un réseau routier donné.

Le réseau routier, les types de véhicules et les itinéraires des véhicules sont tous configurables et permettent des simulations personnalisées. En outre, l'interface de contrôle du trafic (TraCI) permet à SUMO de communiquer de manière bidirectionnelle avec n'importe quel simulateur de réseau. Ainsi, les résultats du simulateur du trafic affectent le simulateur réseau et inversement. Par défaut, SUMO utilise le modèle de voiture Stefan Krau pour simuler de manière réaliste l'accélération et la décélération de chaque véhicule(Krauss,1997).

De manière plus détaillée, les réseaux routiers SUMO sont définis par un fichier réseau. Dans le fichier réseau, les voies sont définies comme des arêtes dans un graphe dirigé avec des sommets se présentant sous la forme de connexions entre les voies. Les voies individuelles ont des attributs tels que des limitations de vitesse ou des restrictions de virage. Les connexions entre les voies peuvent simplement indiquer un changement de direction ou des intersections à plusieurs voies avec des feux de circulation ou une direction de trafic prioritaire.

Comme la simulation du trafic « SUMO » nécessite la représentation des réseaux routiers et de la demande du trafic à simuler dans un format propre, les deux doivent être importés ou générés à partir de sources différentes. Des réseaux routiers géométriques simples peuvent être générés à l'aide de l'utilitaire NETGEN. Pour modéliser la vie réelle, des données de carte routière provenant de diverses sources telle qu'Open Street Map (OSM) peuvent être importées à l'aide de l'utilitaire NETCONVERT. Il fournit une carte de Google Maps en tant qu'interface pour la visualisation des données cartographiques générées par la communauté. Il est également possible d'ajouter un large éventail de polygones supplémentaires tels que des bâtiments et des rivières. Ces polygones peuvent être importés à l'aide de POLYCONVERT. Ces outils permettent de générer des réseaux routiers réalistes. Voir la figure *Fig. IV.3*.

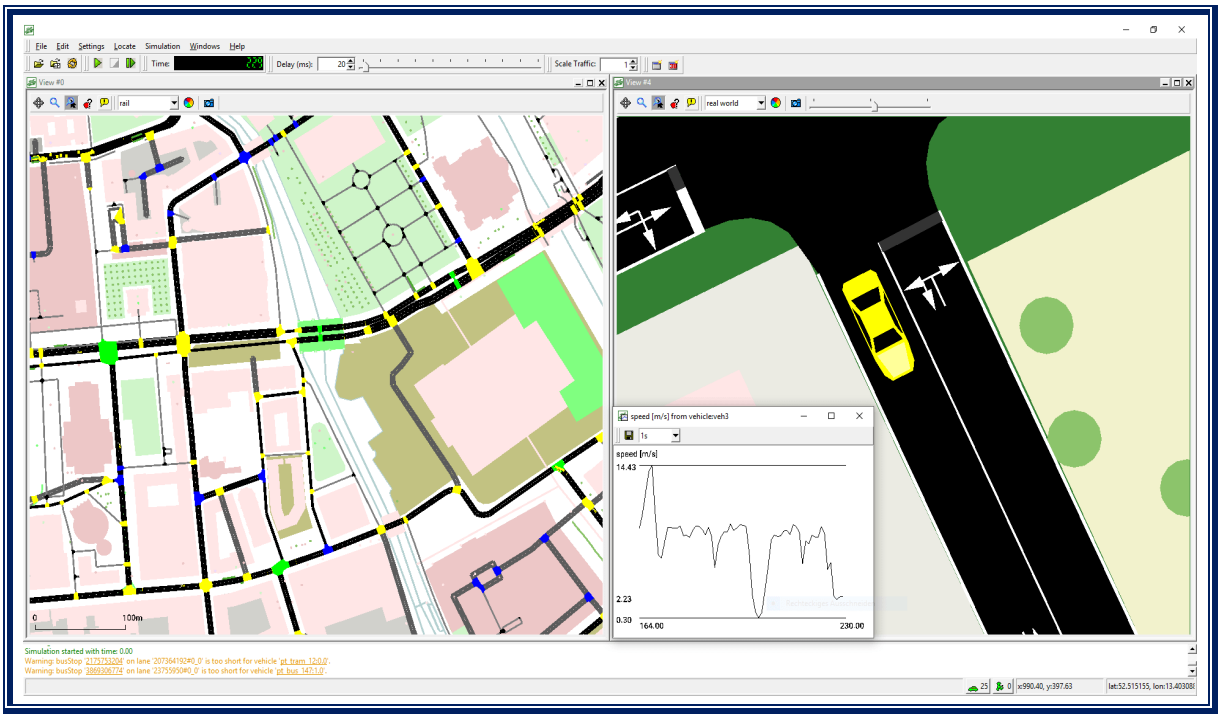


Fig. IV. 3 : *Exemple d'une interface SUMO.*

IV.3.c. VEINS Framework :

Veins (Vehicles in network simulation), le cadre de simulation de réseau de véhicules Open Source, il se présente sous la forme d'une suite de modèles de simulation pour le réseau de véhicules. Ces modèles sont exécutés par un simulateur de réseau basé sur les événements (OMNeT ++) tout en interagissant avec un simulateur de trafic routier (SUMO). D'autres composants de Veins se chargent de la configuration, de l'exécution et du suivi de la simulation.

Cela constitue un cadre de simulation, ce qui signifie que Veins est censé servir de base à l'écriture de code de simulation spécifique à une application. Bien qu'il puisse être utilisé sans modification, avec seulement quelques paramètres modifiés pour un cas d'utilisation spécifique, il est conçu pour servir d'environnement d'exécution pour le code écrit par l'utilisateur. En règle générale, ce code écrit par l'utilisateur sera une application qui doit être évaluée au moyen d'une simulation. Le Framework s'occupe du reste : modéliser les couches de protocole inférieures et la mobilité des nœuds, prendre en charge la mise en place de la simulation, assurer sa bonne exécution et collecter les résultats pendant et après la simulation. Voir la figure *Fig. IV.4.*

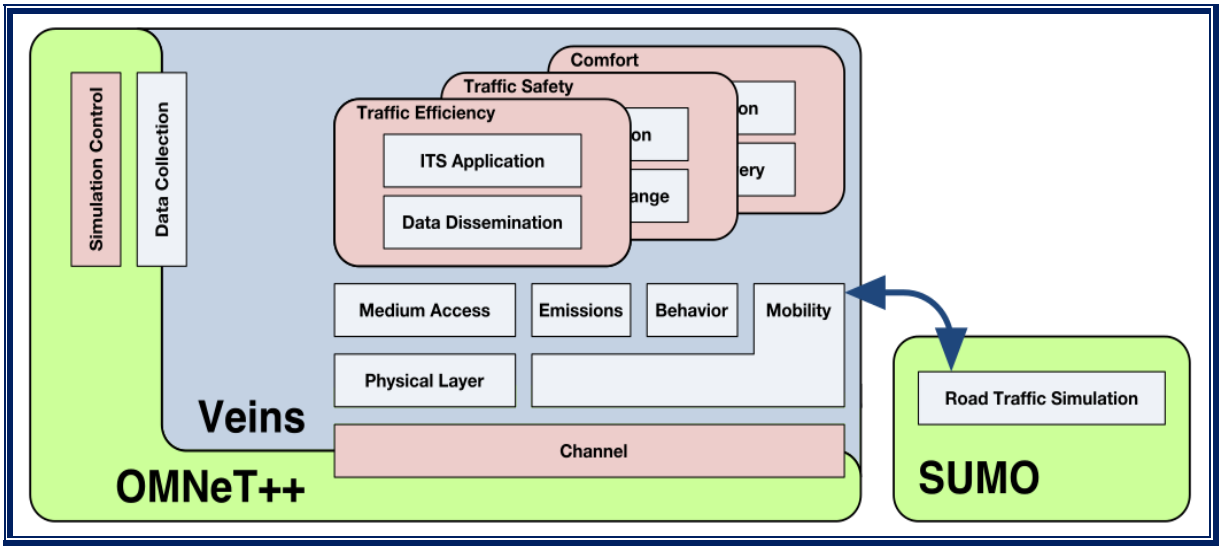


Fig. IV. 4 : *Intégration de SUMO et OMNeT++ par le Framework Veins.*

Comme indiqué précédemment, avec Veins, chaque simulation est réalisée en exécutant deux simulateurs en parallèle : OMNeT ++ (pour la simulation de réseau) et SUMO (pour la simulation du trafic routier). Les deux simulateurs sont connectés via une socket TCP. Le protocole de cette communication a été normalisé sous le nom de Traffic Control Interface (TraCI). Cela permet une simulation bidirectionnelle couplée du trafic routier et du trafic réseau. Voir la figure *Fig. IV.5*.

Le mouvement des véhicules dans le simulateur de trafic routier SUMO se traduit par le mouvement des nœuds dans une simulation OMNeT ++. Les nœuds peuvent alors interagir avec la simulation de circulation routière [21].

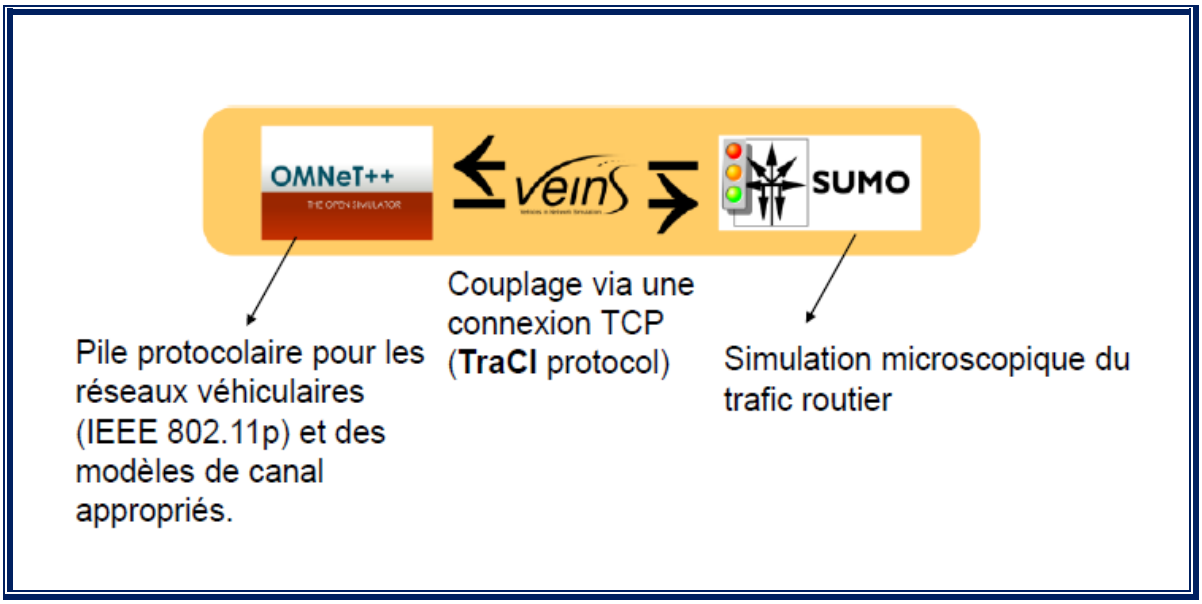


Fig. IV. 5 : *Simulation bidirectionnelle-couplée du trafic routier et du trafic réseau.*

IV.4. Préparation de l'environnement :

La préparation de l'environnement d'implémentation consiste à :

1. Installer le simulateur de réseau OMNeT++ sous le système d'exploitation Windows 7 Professionnel, nous avons utilisé la version 4.4. L'installation est faite comme suit :
   - ✓ Télécharger OMNeT++ à partir du lien : https://omnetpp.org/download/ ;
   - ✓ Extraire le fichier zip, dans le ming.cmd, on fait entrer les commandes : ./configure ensuite make et enfin omnetpp.

2. Télécharger le code source SUMO-0.21.0 à partir du lien : https://www.clubic.com/telecharger-fiche120628-sumo.html et extraire le fichier zip ;

3. Télécharger le code source Veins-3.0 à partir du lien https://veins.car2x.org/download/ et extraire le fichier zip ;

4. Importer les deux fichiers Veins dans le simulateur OMNeT++.

IV.5. Etapes de simulation :

Dans ce qui suit, nous allons décrire les différentes étapes à suivre afin de réaliser notre simulation.

➢ Simulation de l'algorithme de clustering en utilisant OMNeT++ :

Pour commencer notre simulation, la première chose qu'on doit faire est de lancer l'EDI OMNeT++ en tapant omnetpp dans le mingwin, ensuite importer le projet Leach en choisissant dans le menu : File → Import → Exesting project to workspace.

Dans un premier lieu, nous allons entrer dans le cœur du code source de notre projet afin de donner un aperçu sur le déroulement de l'algorithme de clustering, et des algorithmes de détection de la vitesse et de la distance, ensuite nous présenteront un exemple de simulation.

- ✓ **Implémentation de l'algorithme de clustering :**

  - **Etape d'élection du Cluster-Head (CH) :**

D'abord, au niveau de la méthode initialize (), montrée dans la figure *Fig. IV.6*, de la couche de communication netLayer, les nœuds du réseau initient la communication, en créant un message newRoundMessage, ce message va être dupliqué, une copie sera envoyée aux nœuds adjacents et qui sera reçue dans NEW_ROUND, l'autre copie sera envoyée au nœud lui-même et qui va être reçue dans NEW_ROUND_MESSAGE, cela va permettre de répéter le processus chaque 10s (chaque round).

```
void NetLayer::initialize()
{
    // TODO - Generated method body
    numChAdv = 0;
    isCH = false;
    selfId = getParentModule()->getParentModule()->par("ID");
    energy = 1000;

    VL = 23;
    DL = 23;

    NewRoundMsg *newRoundMsg = new NewRoundMsg();
    newRoundMsg->setNodeId(selfId);
    newRoundMsg->setRound(roundNumber);
    newRoundMsg->setKind(NEW_ROUND_MESSAGE);
    NewRoundMsg *copy = newRoundMsg->dup();
    RoutingPacket *routingPkt = new RoutingPacket("routingPkt", ROUTING_PACKET);
    routingPkt->setRoutingPacketType(NEW_ROUND);
    routingPkt->setNodeId(newRoundMsg->getNodeId());
    routingPkt->setTxPower(newRoundMsgTX);
    routingPkt->setSize(newRoundMsgSize);
    routingPkt->encapsulate(copy);
    send(routingPkt, "toMacLayer");
    scheduleAt(simTime()+ roundTime, newRoundMsg);
}
```

Fig. IV. 6 : *OMNeT++ : Méthode initialize ().*

Le message NewRoundMsg destiné aux autres nœuds du réseau va être reçu dans la méthode handleMacPacket (), case : NEW_ROUND. Suite à ça, l'étape de l'élection du CH va commencer. Pour ce faire, chaque nœud génère un nombre aléatoire entre 0 et 1, si le nombre engendré est inférieur à un certain seuil prédéfini, le nœud va s'auto élire CH. Voir la figure *Fig. IV.7*.

```
case NEW_ROUND :{
    NewRoundMsg *newRoundMsgRcv = check_and_cast<NewRoundMsg*>(routingPkt->decapsulate());
    int roundNumber = (double)newRoundMsgRcv->getRound();    //numéro du round
    double r = (double) roundNumber;
    cluster.clear();                        // on réinistialise les clusters
    helloTab.clear();                        // on réinistialise les tables
    energy = energy + 100;
    numChAdv = 0;
    if(isCH)                                // si c'était un CH il devient noeud ordinaire
        isCH = false;

    double chThresholdElection = percentageOfCh/(1-percentageOfCh*(fmod(r,(1/percentageOfCh))));
    double randNumber = (double)(rand()% 1000)/1000.00;
    if(randNumber<chThresholdElection){
        numCluster++;
        isCH = true;
```

Fig. IV. 7 : *OMNeT++ : NEW_ROUND.*

- **Etape de la formation des clusters :**

Le CH élu va envoyer des messages d'invitation aux autres nœuds adjacents pour les inviter à rejoindre son cluster. Voir la figure *Fig. IV.8*.

```
    isCH = true;
    ChadvMsg *chMsg = new ChadvMsg();
    routingPkt->setKind(ROUTING_PACKET);
    routingPkt->setRoutingPacketType(CH_ADV);
    routingPkt->setNodeId(selfId);
    routingPkt->setTxPower(chAdvMsgTX);
    routingPkt->setSize(chAdvMsgSize);
    routingPkt->encapsulate(chMsg);
    send(routingPkt, "toMacLayer");
}
else
    delete routingPkt;
delete newRoundMsgRcv;
break;
```

Fig. IV. 8 : *OMNeT++ : Messages d'invitation des noeuds adjacents.*

Les nœuds voisins recevront ce message dans case : CH_ADV. Après ça, chaque nœud va se mettre en attente d'autres messages d'invitation, cela se fait en s'auto-envoyant un message qui sera délivré qu'après l'écoulement d'un certain laps de temps dit simTime. Voir la figure *Fig. IV.9*.

```
case CH_ADV :{
    if(!isCH){
        numChAdv++;
        if(numChAdv == 1){
            maxRSSI = routingPkt->getRxPower();
            chID = routingPkt->getNodeId();
            cMessage *decisionMsg = new cMessage("decisionMsg", CLUSTER_JOIN_DECISION_MESSAGE);
            delayDecisionExpired = false;
            scheduleAt(simTime()+ delayDecision, decisionMsg);
        }
        else if((routingPkt->getRxPower()> maxRSSI)&&(delayDecisionExpired ==false)){
            chID = routingPkt->getNodeId();
            maxRSSI = routingPkt->getRxPower();
            dataMsgTx = CCAthreshold+chAdvMsgTX-maxRSSI;
        }
    }
    delete routingPkt;
    break;
```

Fig. IV. 9 : *OMNeT++ : CH_ADV.*

Une fois, la période de temps simTime est écoulée, la réception de l'auto-message se fait dans CLUSTER_JOIN_DECISION_MESSAGE, de ce fait, le nœud va décider du cluster qu'il va rejoindre. Dans le cas où il a reçu plusieurs invitations, il choisit son CH en fonction de la plus grande puissance de transmission, sinon, il n'a pas à faire une comparaison et choisit le seul CH qui l'a invité. Ensuite, il lui envoie un message JoinClusterMsg pour rejoindre son cluster. Voir la figure *Fig. IV.10*.

```
case CLUSTER_JOIN_DECISION_MESSAGE :{
    delayDecisionExpired = true;
    JoinClusterMsg *joinClMsg = new JoinClusterMsg();
    joinClMsg->setNodeId(selfId);
    joinClMsg->setChId(chID);
    RoutingPacket* routingPkt = new RoutingPacket("routingPkt", ROUTING_PACKET);
    routingPkt->setRoutingPacketType(JOIN_CLUSTER);
    routingPkt->setNodeId(selfId);
    routingPkt->setTxPower(dataMsgTx);
    routingPkt->encapsulate(joinClMsg);
    send(routingPkt,"toMacLayer");
    delete msg;
    break;
```

Fig. IV. 10 : *OMNeT++ : CLUSTER_JOIN_DECISION_MESSAGE.*

Le CH va recevoir le message JoinClusterMsg dans case : JOIN_CLUSTER, à chaque réception de ce type de message, le nœud émetteur va être inséré dans le cluster du CH en question. Ce mécanisme est répété par tous les CH du réseau afin d'achever l'étape de formation des clusters. Voir la figure *Fig. IV.11*.

```
case JOIN_CLUSTER :{
    if (isCH){
        JoinClusterMsg *joinMsg = check_and_cast<JoinClusterMsg*>(routingPkt->decapsulate());
        if(joinMsg->getChId()==selfId){
            Neighbor N;
            N.neighborId = joinMsg->getNodeId();
            cluster.insert(cluster.end(),N);
        }
        delete joinMsg;
    }else{
        cMessage *creationHelloMsg = new cMessage("creationHelloMsg", HELLO_MSG);
        scheduleAt(simTime()+ delayCreationHelloMsg, creationHelloMsg);
    }
    delete routingPkt;
    break;
```

Fig. IV. 11 : *OMNeT++ : JOIN_CLUSTER.*

✓ **L'implémentation des algorithmes de détection de la vitesse et de la distance :**

Après la formation des clusters, chaque nœud s'auto-envoie un message qui va être reçu dans case : HELLO_MSG, où l'échange périodique des messages Hello va être déclenché. En effet, chaque nœud récupère ses coordonnées GPS ainsi que son ID, ensuite il les encapsule dans un message nommé helloMsg. Ce dernier va être dupliqué, une copie de ce message va lui servir de moyen pour maintenir l'échange périodique du message Hello dans HELLO_MSG_RPT, l'autre copie va être envoyé aux autres nœuds voisins du même cluster pour calculer la distance et la vitesse, et sera reçu dans case : HELLO_MSG. Voir la figure *Fig. IV.12*.

```
case HELLO_MSG :{
    // Dans cette section, on initie l'échange périodique des messages Hello contenants l'id et les coordonnées du noeud.

    double X = getParentModule()->getParentModule()->par("XPOS");
    double Y = getParentModule()->getParentModule()->par("YPOS");
    double Z = getParentModule()->getParentModule()->par("ZPOS");

    HelloMsg *helloMsg = new HelloMsg();
    helloMsg->setNodeId(selfId);
    helloMsg->setCoordinateX(X);
    helloMsg->setCoordinateY(Y);
    helloMsg->setCoordinateZ(Z);

    helloMsg->setKind(HELLO_MSG_RPT);
    HelloMsg *copy = helloMsg -> dup();
    RoutingPacket *routingPkt = new RoutingPacket("routingPkt", ROUTING_PACKET);
    routingPkt->setRoutingPacketType(RECV_HELLO_MSG);
    routingPkt->setNodeId(selfId);
    routingPkt->setTxPower(dataMsgTx);
    routingPkt->encapsulate(copy);
    send(routingPkt, "toMacLayer");
    scheduleAt(simTime()+ delayHelloMsg, helloMsg);
    delete msg;
    break;
}
```

Fig. IV. 12 : *OMNeT++ : HELLO_MSG.*

- **Calcul de la distance entre les nœuds :**

Après que chaque nœud ait reçu le message Hello, il va procéder au calcul de la distance entre lui et le nœud émetteur en fonction de ses coordonnées GPS et celles de ce dernier. Ensuite le résultat va être comparé à la valeur de la distance minimale, s'il n'y a pas eu respect de cette dernière un message d'alerte sera envoyé au cluster-Head. Voir la figure *Fig. IV.13*.

```
case RECV_HELLO_MSG :{
    // Réception des messages Hello et calcul de la vitesse ainsi que de la distance.

    HelloTab H;
    int ID;
    double X1,X2,Y1,Y2,Z1,Z2;
    time_t T1,T2;

    HelloMsg *helloMsg = check_and_cast<HelloMsg*>(routingPkt->decapsulate());
    ID = helloMsg -> getNodeId();
    X2 = helloMsg -> getCoordinateX();
    Y2 = helloMsg -> getCoordinateY();
    Z2 = helloMsg -> getCoordinateZ();
    T2 = time(0);


    X1 = getParentModule()->getParentModule()->par("XPOS");
    Y1 = getParentModule()->getParentModule()->par("YPOS");
    Z1 = getParentModule()->getParentModule()->par("ZPOS");

    D = sqrt((X2-X1)*(X2-X1) + (Y2-Y1)*(Y2-Y1) + (Z2-Z1)*(Z2-Z1));
    if(D < DL){
        MsgDenunciation *msgDenunciation = new MsgDenunciation();
        msgDenunciation->setNodeId(selfId);
        msgDenunciation->setChId(chID);
        msgDenunciation->setDistance(D);
        RoutingPacket* routingPkt = new RoutingPacket("routingPkt", ROUTING_PACKET);
        routingPkt->setRoutingPacketType(MSG_DENUNCIATION);
        routingPkt->setNodeId(selfId);
        routingPkt->setTxPower(memberToChTX);
        routingPkt->encapsulate(msgDenunciation);
        send(routingPkt,"toMacLayer");
    }
```

Fig. IV. 13 : *OMNeT++ : RECV_HELLO_MSG, calcul de la distance.*

.

- **Calcul de la vitesse des nœuds adjacents :**

En ce qui concerne la vitesse, le nœud dispose d'un fichier nommé helloTab, ce dernier représente un fichier contenant l'ID, les coordonnées GPS et le temps de réception de chaque message Hello reçu.

A chaque réception d'un message Hello, le nœud récepteur va parcourir le fichier helloTab, afin de vérifier si le nœud émetteur existe dans ce fichier.

Dans le cas où l'ID de ce nœud figure dans helloTab ; cela veut dire qu'il y a eu déjà un échange de message entre les deux nœuds, suite à ça, le nœud récepteur récupère les coordonnées GPS et le temps de réception du message déjà existant et les met dans des variables temporaires, ensuite il met à jour l'enregistrement en question dans le fichier en remplaçant les anciennes valeurs par les nouvelles valeurs des coordonnées et du temps de réception du dernier message. Par la suite, il calcule la vitesse du nœud émetteur, le résultat sera comparé à la vitesse autorisée, s'il y a eu dépassement alors le nœud va envoyer un message d'alerte au CH afin de le dénoncer.

Dans le cas où l'ID du nœud ne figure pas dans le fichier, cela veut dire que c'est le tout premier message Hello reçu de la part du nœud émetteur, donc il va insérer son ID, ses coordonnées ainsi que le temps de sa réception dans le fichier helloTab. Voir la figure *Fig. IV.14*.

```
unsigned i = 0;
bool isTrue = false;

while((i < helloTab.size()) && (isTrue == false)){
    if(H.helloId == ID){
        // Récupération des coordonnées ainsi que le temps de réception du premiers msg Hello
        isTrue = true;
        X1 = H.X;
        Y1 = H.Y;
        Z1 = H.Z;
        T1 = H.T;

        // Mise à jour de la table en modifiant les valeurs du 1er msg Hello par le 2ème msg Hello.
        H.X = X2;
        H.Y = Y2;
        H.Z = Z2;
        H.T = T2;
    }
    else{
        i++;
    }
}

if(!isTrue){
    H.helloId = ID;
    H.X = X2;
    H.Y = Y2;
    H.Z = Z2;
    H.T = T2;
    helloTab.insert(helloTab.end(),H);
}


   else{

       V = sqrt(((X2-X1)*(X2-X1) + (Y2-Y1)*(Y2-Y1) + (Z2-Z1)*(Z2-Z1))/(T2-T1));
       if(V > VL){
           MsgDenunciation *msgDenunciation = new MsgDenunciation();
           msgDenunciation->setNodeId(selfId);
           msgDenunciation->setChId(chID);
           msgDenunciation->setSpeed(V);
           RoutingPacket* routingPkt = new RoutingPacket("routingPkt", ROUTING_PACKET);
           routingPkt->setRoutingPacketType(MSG_DENUNCIATION);
           routingPkt->setNodeId(selfId);
           routingPkt->setTxPower(memberToChTX);
           routingPkt->encapsulate(msgDenunciation);
           send(routingPkt,"toMacLayer");
       }
   }

   delete msg;
   break;
}
```

Fig. IV. 14 : *OMNeT++ : RECV_HELLO_MSG, calcul de la vitesse.*

NB : Les algorithmes de calcul de la vitesse et de la distance ont été fusionnés lors de l'implémentation pour la répétition, et ainsi éviter la surcharge du réseau.

Le CH récupère le message d'alerte dans case : MSG_DENUNCIATION. Par la suite il devrait vérifier le niveau de confiance du véhicule alertant, si don degré de confiance est supérieur à un certain seuil prédéfini, le CH achemine les données au serveur de police en transitant par la RSU. Dans le cas contraire, le message d'alerte est ignoré. Voir la figure *Fig. IV.15*.

```
case MSG_DENUNCIATION :{
    // Evaluation du niveau de confiance des noeuds dénonciateurs et transmission des requettes à la RSU.
    if(isCH){
        MsgDenunciation *msgDenunciationRcv = check_and_cast<MsgDenunciation*>(routingPkt->decapsulate());
        int chId = msgDenunciationRcv->getChId();
        if(chId == chID){
          /*int ID = msgDenunciationRcv->getNodeId();
            V = msgDenunciationRcv->getSpeed();
            D = msgDenunciationRcv->getDistance();

            Dans cette section on devrait récupérer également le degré de confiance
            du véhicule dénonciateur afin d'évaluer sa crédibilté.
            si son degré de confiance est >= à la norme, son message sera transmis à la RSU.
            sinon, son msg est ignoré.
          */
        }
    }

    delete msg;
    break;
```

Fig. IV. 15 : *OMNeT++ : MSG_DENUNCIATION.*

Dans, l'EDI OMNeT++ illustré dans la figure *Fig.IV.16*, on clique avec le bouton droit sur le projet vanet puis Build Project afin de construire le projet. Ensuite, un autre clic droit sur omnetpp.ini afin de sélectionner Run As OMNeT++ Simulation.

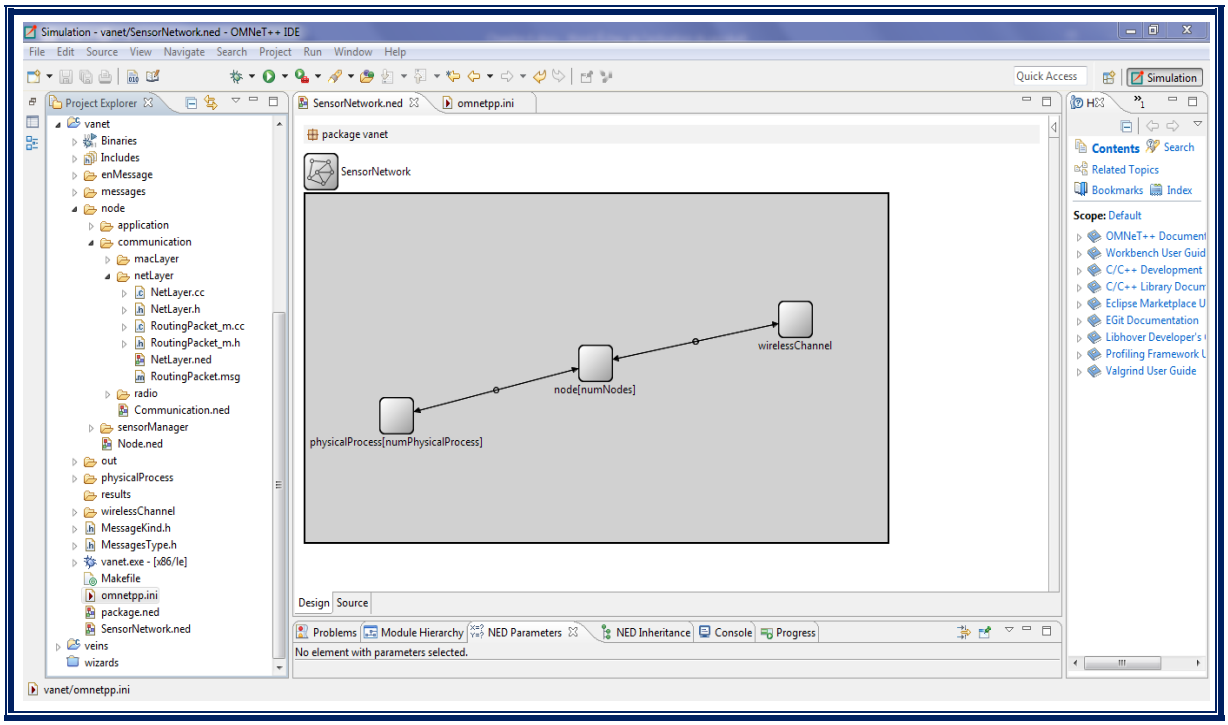


Fig. IV. 16 : *Exécution omnetpp.ini.*

Une autre fenêtre d'exécution OMNeT++ sera lancée comme l'indique la figure *Fig. IV.17*.

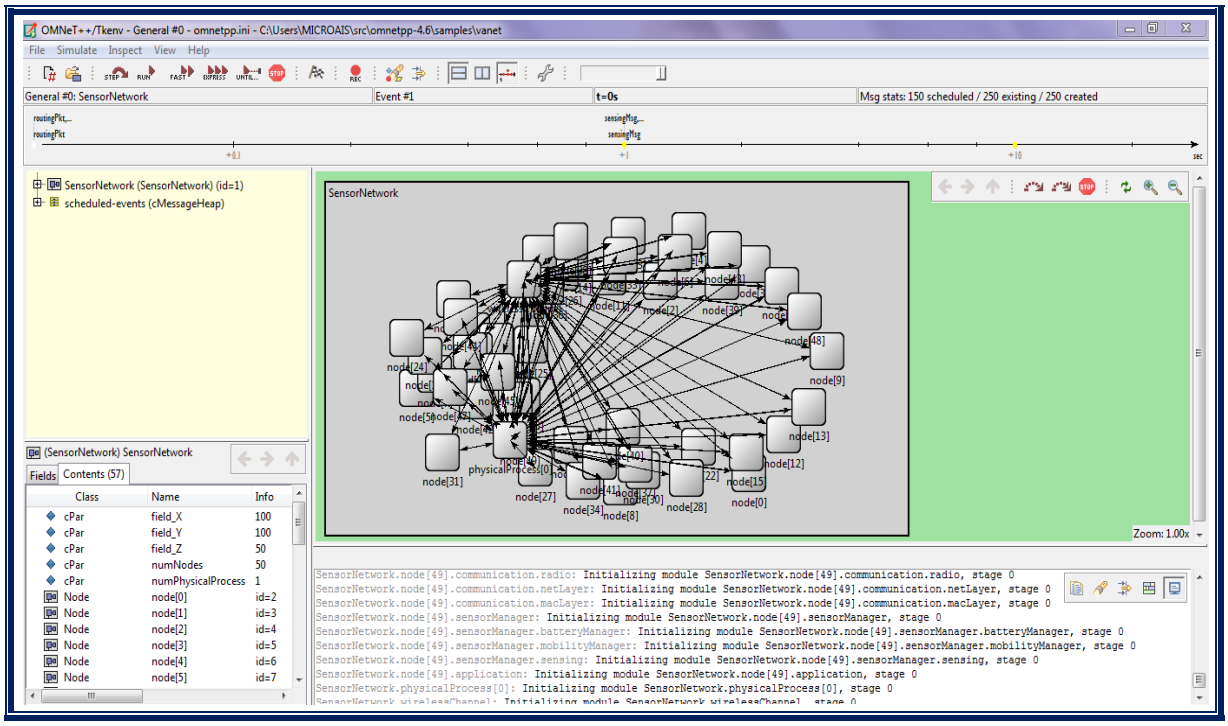


Fig. IV. 17 : *Fenêtre de simulation de OMNeT++.*

Ensuite, on clique sur RUN pour pouvoir démarrer notre simulation comme le montre les figures *Fig. IV.18*, *Fig. IV.19* et ci-dessous.

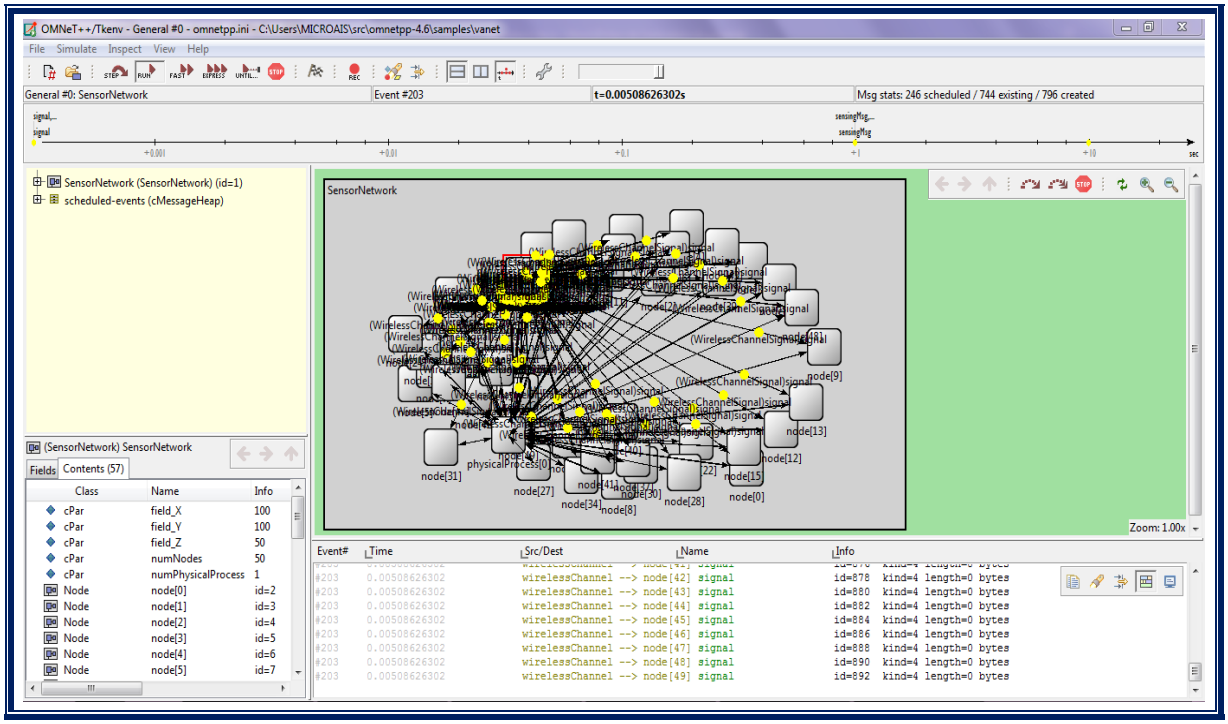


Fig. IV. 18 : *Démarrage de la simulation dans OMNeT++.*

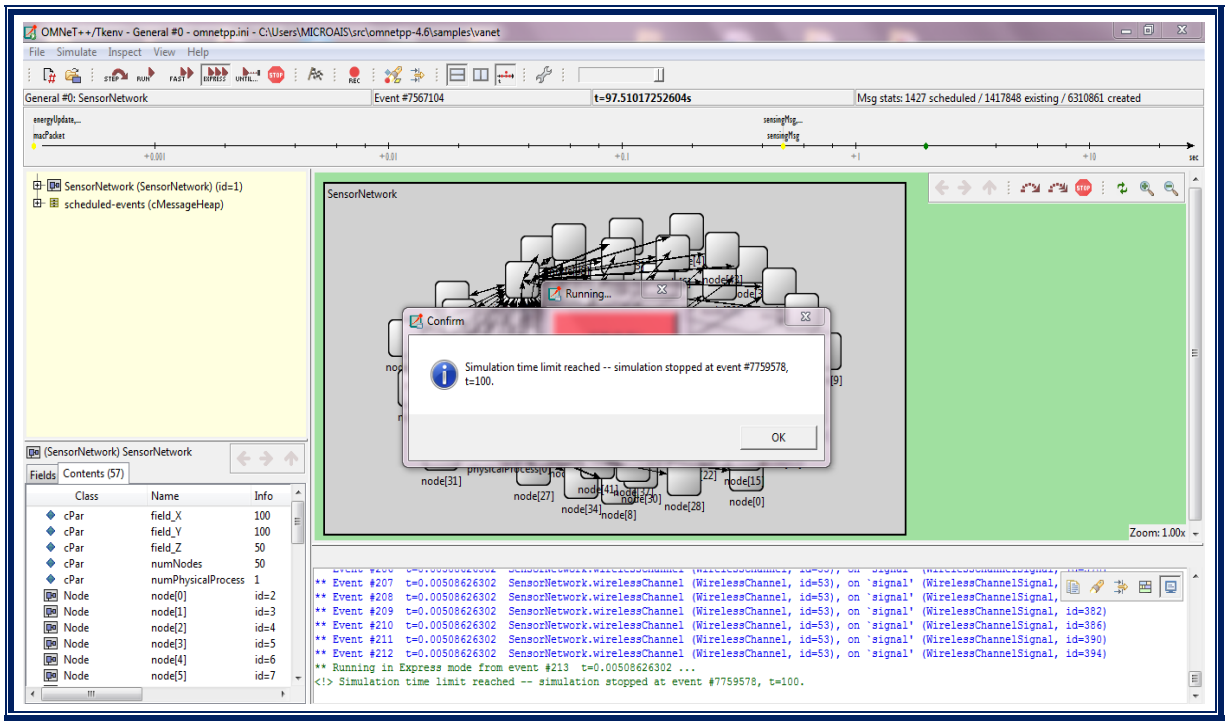


Fig. IV. 19 : *Fin de la simulation dans OMNeT++.*

A la fin de la simulation, on obtient les résultats illustrés dans les figures *Fig. IV.20* et Fig. *IV.21* et qui montrent les clusters formés lors du dernier round, chaque cluster est défini par l'ID de son Cluster-Head, les ID de ses Cluster-Membres ainsi que le nombre d'éléments dans le cluster en question.

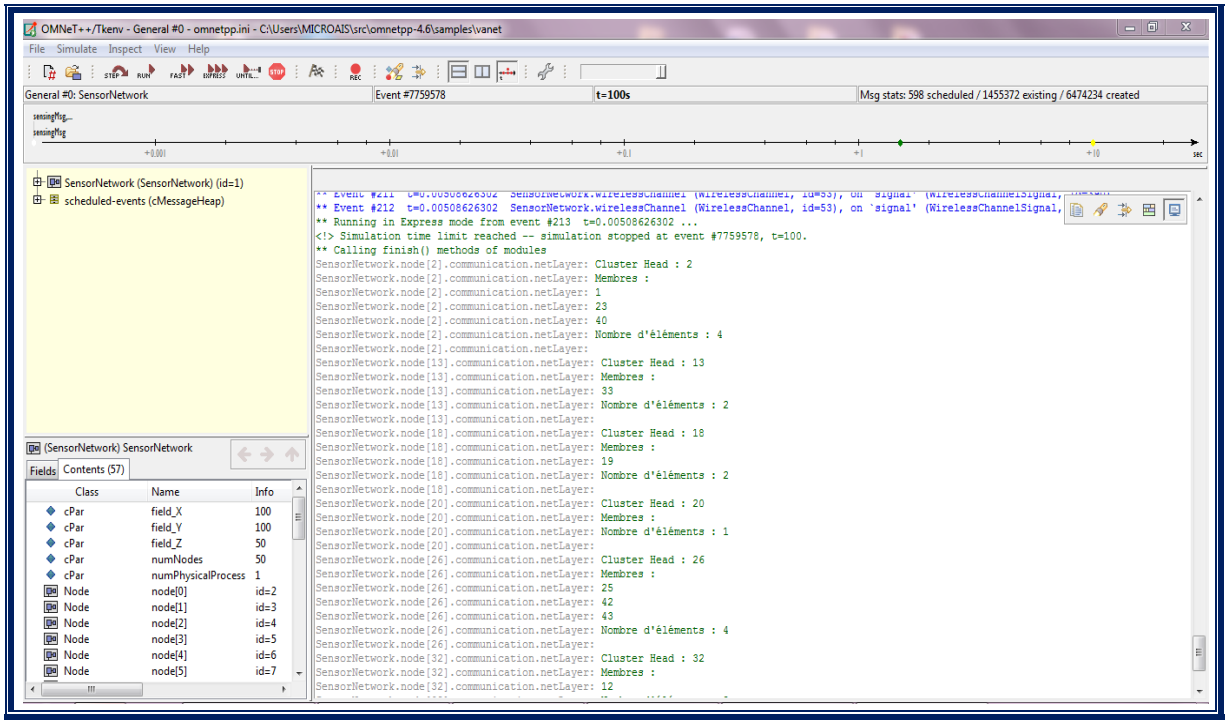


Fig. IV. 20 : *Résultat de simulation de l'algorithme de clustering (1).*

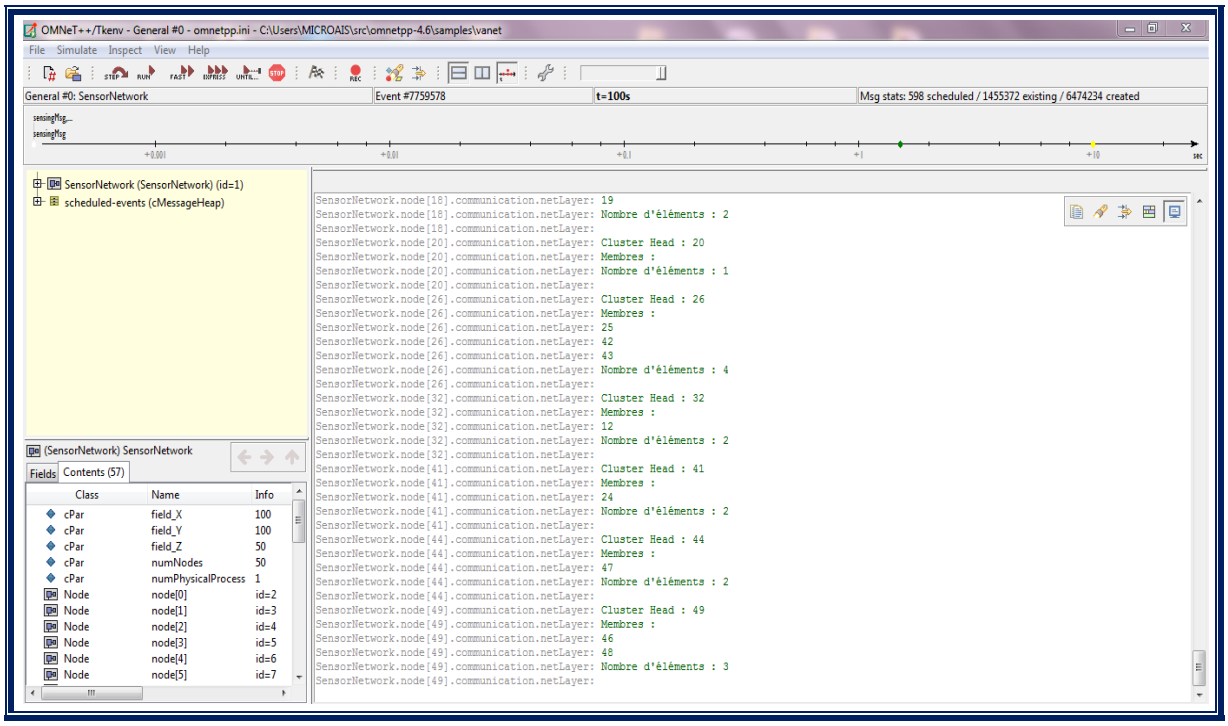


Fig. IV. 21 : *Résultat de simulation de l'algorithme de clustering (2).*

On obtient également les communications établies entre les différents nœuds de notre réseau vanet comme le montre la figure *Fig. IV.22*.

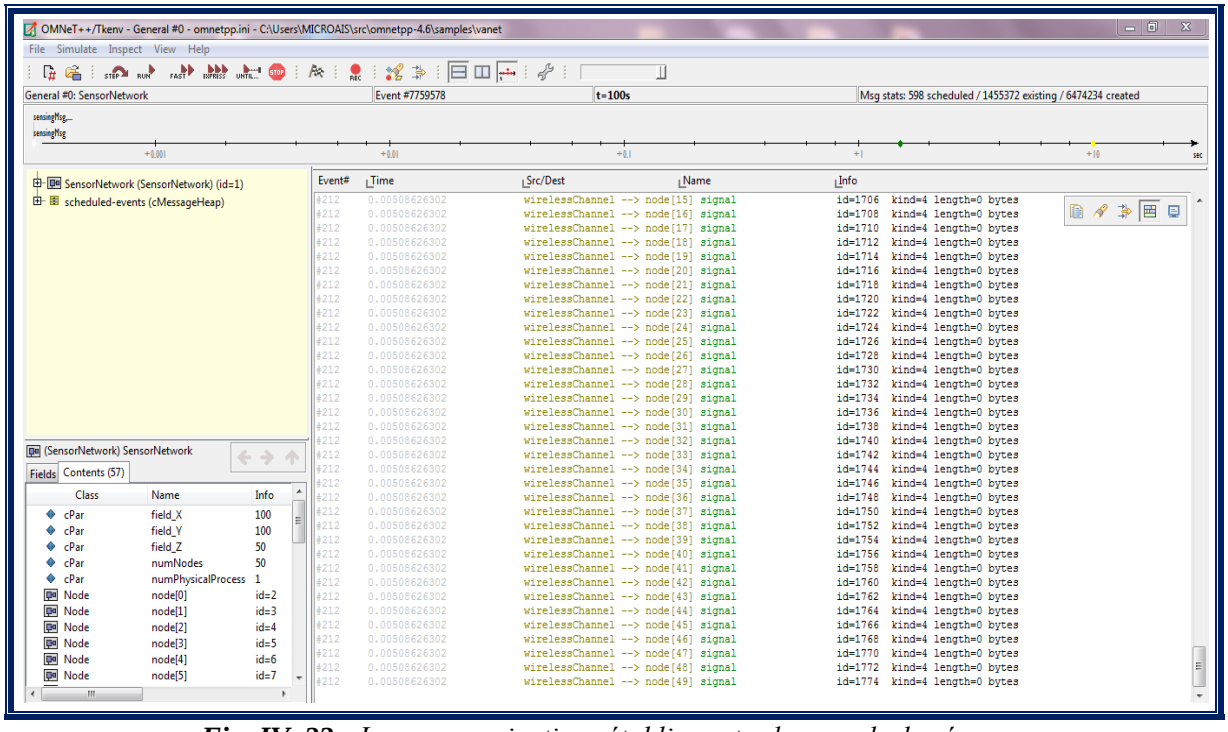


Fig. IV. 22 : *Les communications établies entre les nœuds du réseau.*

En ce qui concerne la suite de l'implémentation, nous n'avons pas pu la terminer à cause de certaines circonstances imprévues qui ont fait retarder notre travail, et c'est pourquoi les communications entre les nœuds du réseau dans OMNeT avec la RSU se trouvant dans Veins n'a pas pu être réalisée. Par contre, nous avons pu créer notre réseau du trafic routier et l'avons simulé dans OMNeT++ et SUMO en utilisant le Framework Veins. Dans ce qui suit, nous montrons les étapes nécessaires afin d'établir cette connexion.

➢ Simulation du trafic routier en utilisant OMNeT++, SUMO et Veins :

SUMO offre la possibilité d'importer des topologies de réseau réelles pour la simulation, ce qui constitue un avantage important, car c'est une possibilité très intéressante. L'utilisateur peut utiliser des scénarios réels et concrets afin d'étudier le comportement d'une communication inter-véhicules donnée. Le simulateur SUMO peut importer des réseaux de plusieurs sources. Cependant, il utilisera le premier site open source des cartes routières OpenStreetMap.

Le projet OpenStreetMap (OSM) a collecté une quantité énorme de données spatiales gratuites et la base de données s'agrandit chaque jour. De nombreuses personnes souhaitent utiliser ces données pour leurs propres projets, mais ont été gênées par l'utilisation d'un format de données non standard dans le projet OSM.

Le mappage des données OSM vers d'autres formats n'est pas une science exacte. Les règles OSM sur la manière de mapper certaines fonctionnalités ne sont souvent pas bien définies et il n'existe pas de contrôle de qualité obligatoire. Cette ouverture permet beaucoup de flexibilité et explique en partie pourquoi OSM a pu collecter autant de données dans un laps de temps aussi court, mais rend l'utilisation des données plus difficile. Lors de l'utilisation ou de l'exportation des données, de nombreuses décisions doivent être prises sur la manière d'extraire les différentes caractéristiques en un élément utilisable pour la tâche à accomplir.

La carte ci-dessous a été obtenue à partir du site officiel d'OpenStreetMap https://www.openstreetmap.org/export#map=17/45.51599/-73.64336&layers=N telle qu'elle est illustrée sur la figure *Fig. IV.*23. La carte sera importée sous forme de fichier « .osm » et enregistrée sous le nom map.osm.

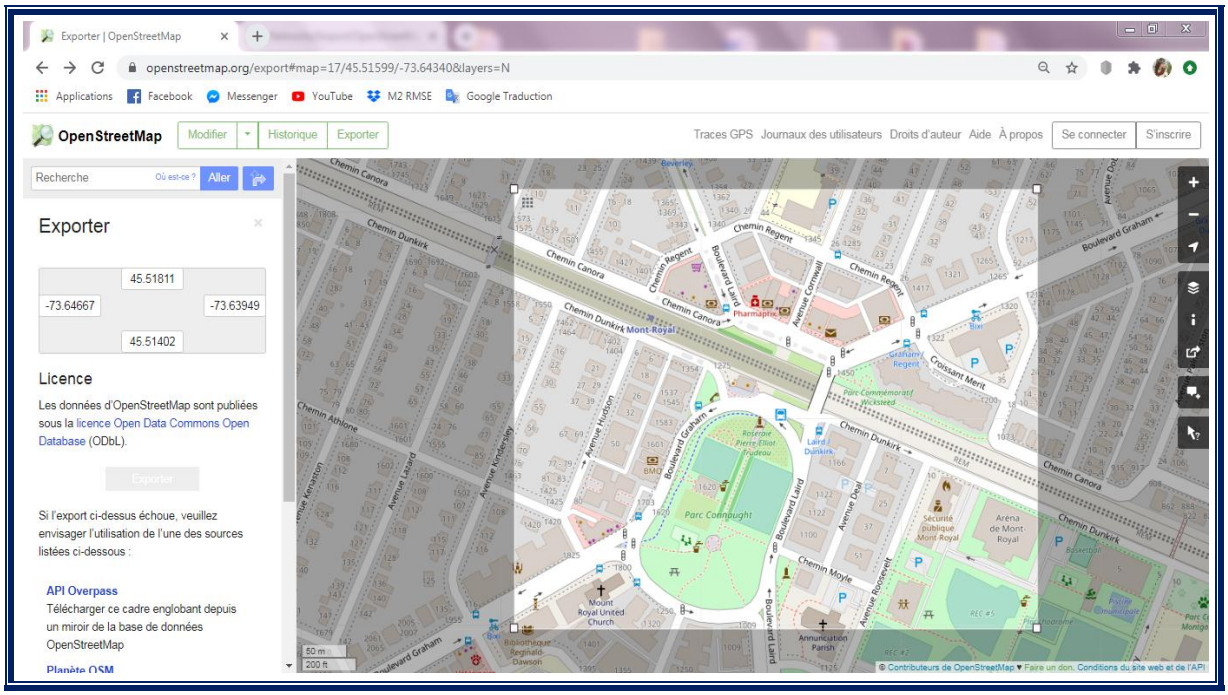


Fig. IV. 23 : *Zone d'étude de la ville de Montréal dans OpenStreetMap.*

✓ Préparation de la carte pour l'utilisation dans SUMO :

On copie le fichier map.osm que nous avons téléchargé précédemment dans le répertoire sumo-1.2.0/bin, puis on la convertie vers un autre format connu par le simulateur SUMO grâce à la commande **netconvert** comme illustré dans la figure IV.24.

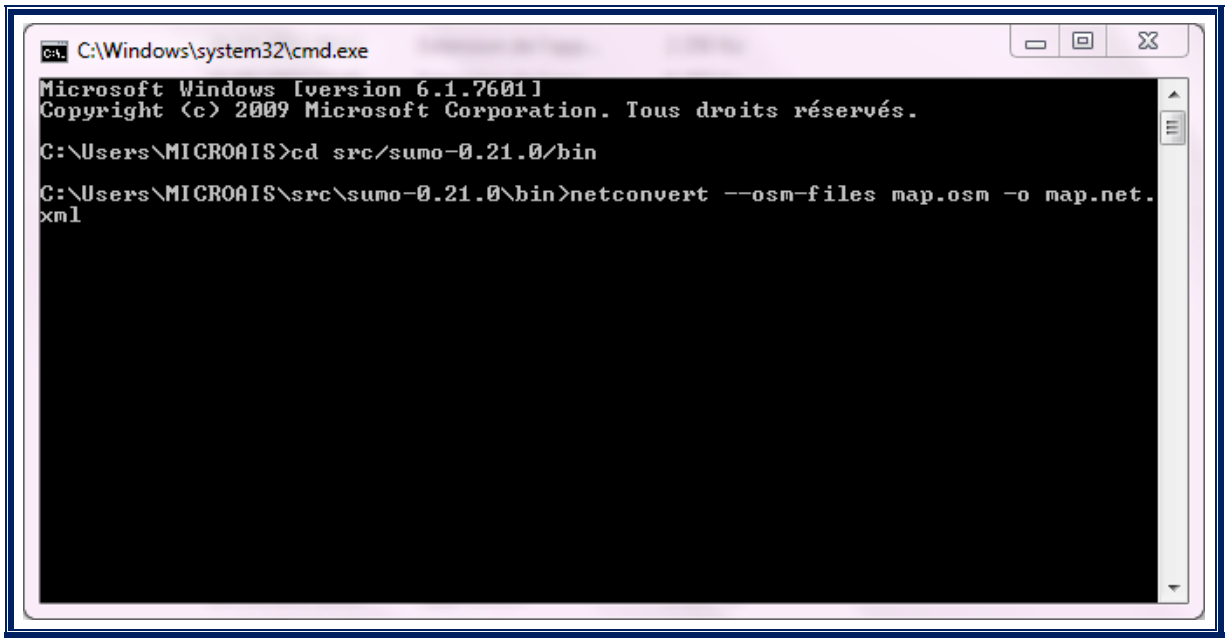


Fig. IV. 24 : *Génération de map.net.xml.*

Les données OSM contiennent non seulement le réseau routier mais également un large éventail de polygones supplémentaires tels que des bâtiments et des rivières. Ces polygones peuvent être importés à l'aide de **polyconvert**, puis ajoutés à une **sumo-gui-configuration.** Cependant, il est nécessaire de créer le fichier « typemap.xml ». Alors, on entre dans le répertoire sumo/bin et on crée un nouveau fichier qu'on nomme typemap.xml où le contenu copié à partir du site web : https://sumo.dlr.de/docs/Networks/Import/OpenStreetMap.html sera collé et enregistré. Voir la figure *Fig. IV.25*.

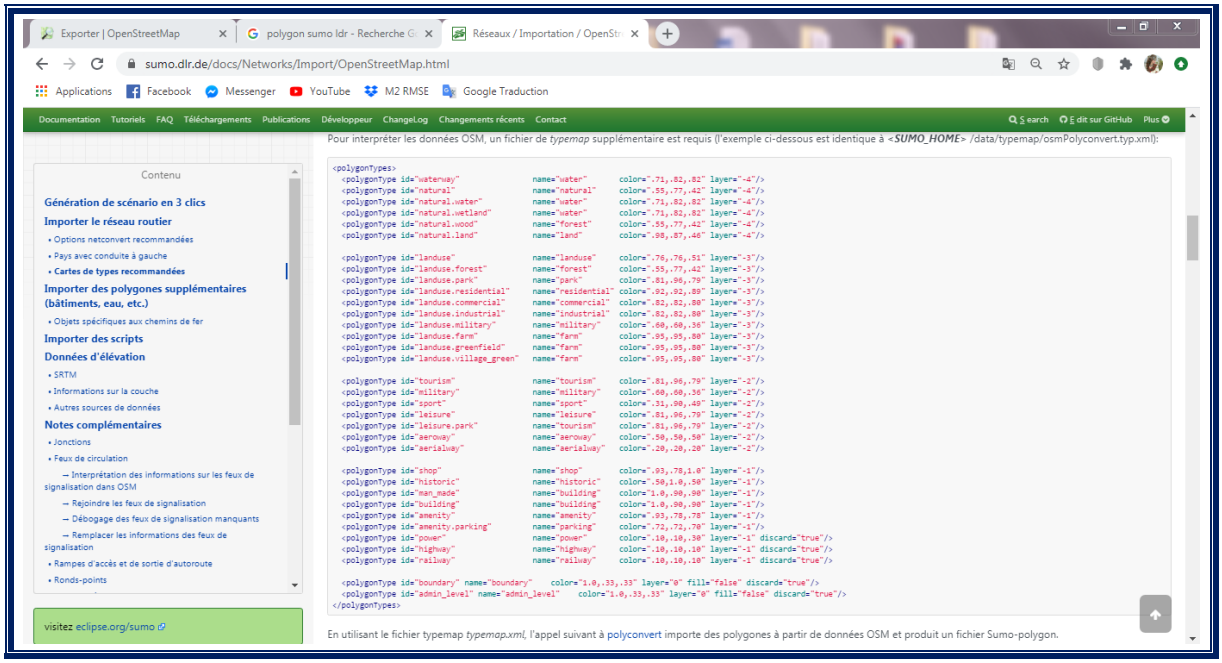


Fig. IV. 25 : *Contenu du fichier typemap.xml.*

En utilisant le fichier typemap.xml, l'appel à **polyconvert** importe des polygones à partir de données OSM et produit un fichier « sumo.poly.xml ». Voir la figure *Fig. IV.26*.

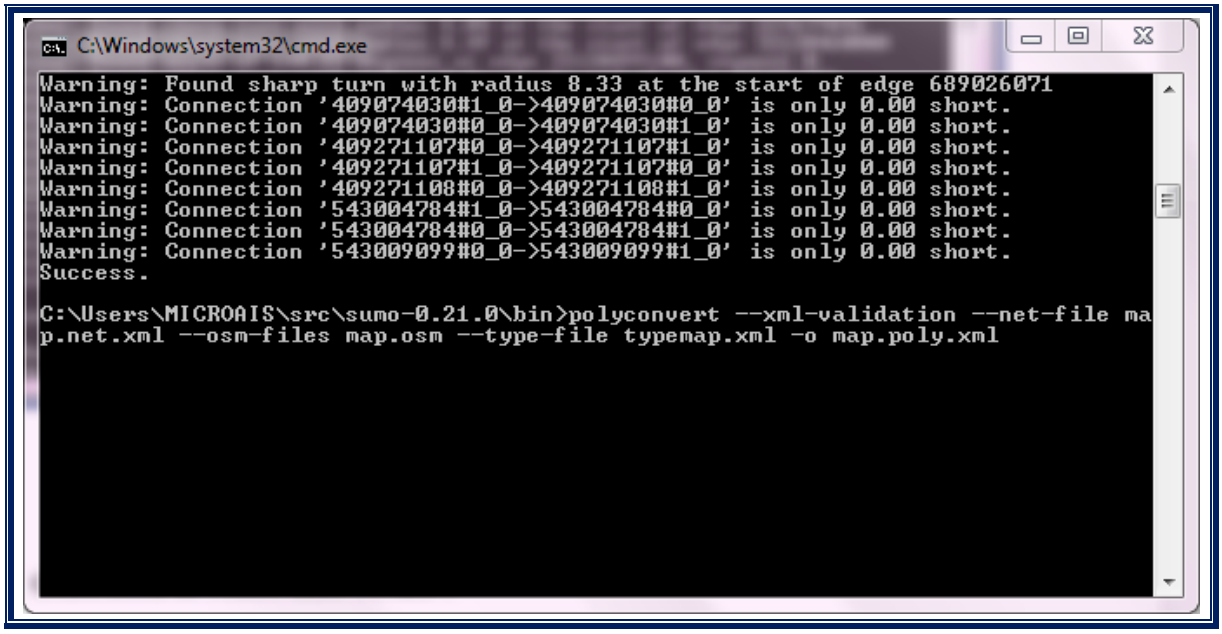


Fig. IV. 26 : *Génération de map.poly.xml.*

✓ **Génération des routes dans SUMO :**

Après avoir défini la topologie du réseau, il ne reste plus qu'à générer la demande de trafic, à savoir la description des itinéraires que les véhicules suivent. Il existe plusieurs méthodes pour générer la demande de trafic dans SUMO :

- Utilisation des définitions de route.
- Utiliser les définitions voyager.
- En utilisant les définitions de fleurs (semblables ci-dessus, mais unir les véhicules avec Voyage similaire dans les groupes).
- En utilisant les définitions des flux aux intersections et au taux de rotation (la cible du lien n'est pas spécifiée, et au lieu de la probabilité de faire des virages aux intersections indiquées).
- Utilisation de routes aléatoires.

Dans notre cas, on utilisera des routes aléatoires. Il existe un script Python développé dans le but de produire des itinéraires aléatoires, son nom est randomTrips.py. Actuellement, c'est la méthode la plus recommandée pour obtenir cette fonctionnalité. Cependant, notez que les résultats ne sont pas toujours tout à fait réalistes. Alors, toujours dans l'invite de commande, on tape la commande nécessaire comme on peut le voir dans la figure *Fig. IV.27*.

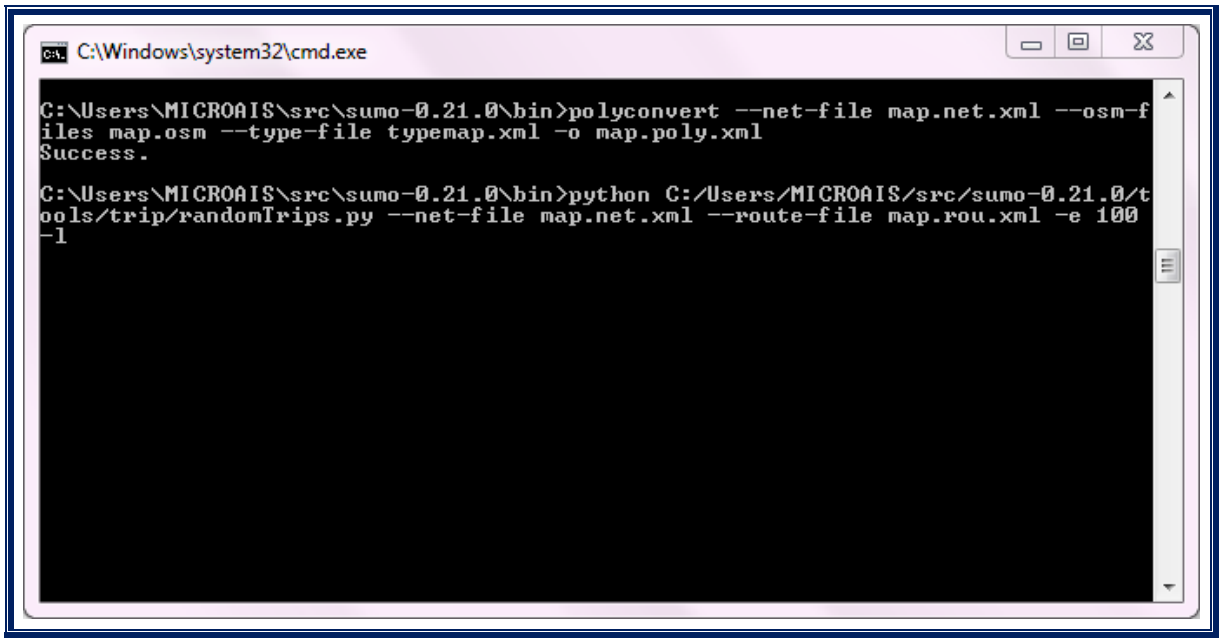


Fig. IV. 27 : *Génération de msila.rou.xml.*

✓ **Préparation des fichiers avant la simulation :**

Maintenant, on copie les fichiers que nous avons générés du dossier SUMO/bin dans le dossier veins-3.0/examples/veins.

Après cela, nous devons éditer les fichiers de configuration de Veins. On entre dans le répertoire veins-3.0/exemples/Veins et on ouvre avec Notepad++ les fichiers « erlangen.launchd.xml » et « erlangen.sumo.cfg » et on écrit le nom des fichiers que nous

avons copiés avant : « map.net.xml », « map.rou.xml » et « map.poly.xml » tel qu'il est illustré sur les figures *Fig. IV.28* et *Fig. IV.29* ci-dessus :

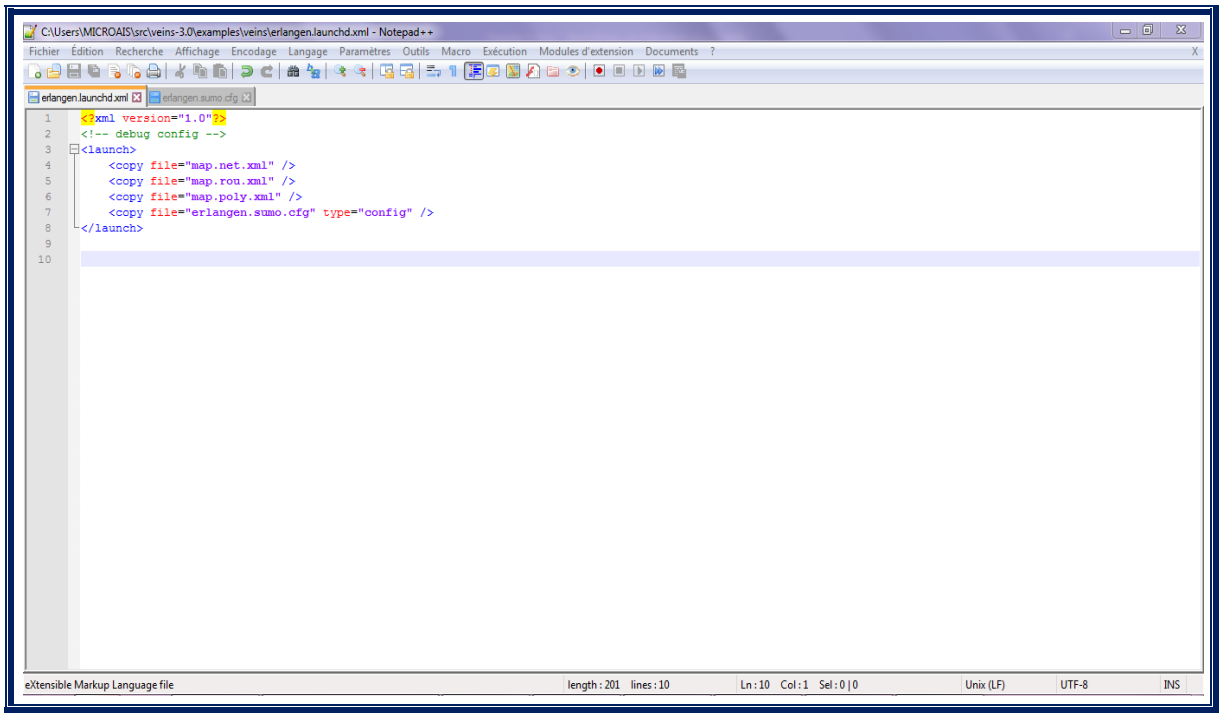


Fig. IV. 28 : *Modification du fichier erlangen.sumo.cfg.*

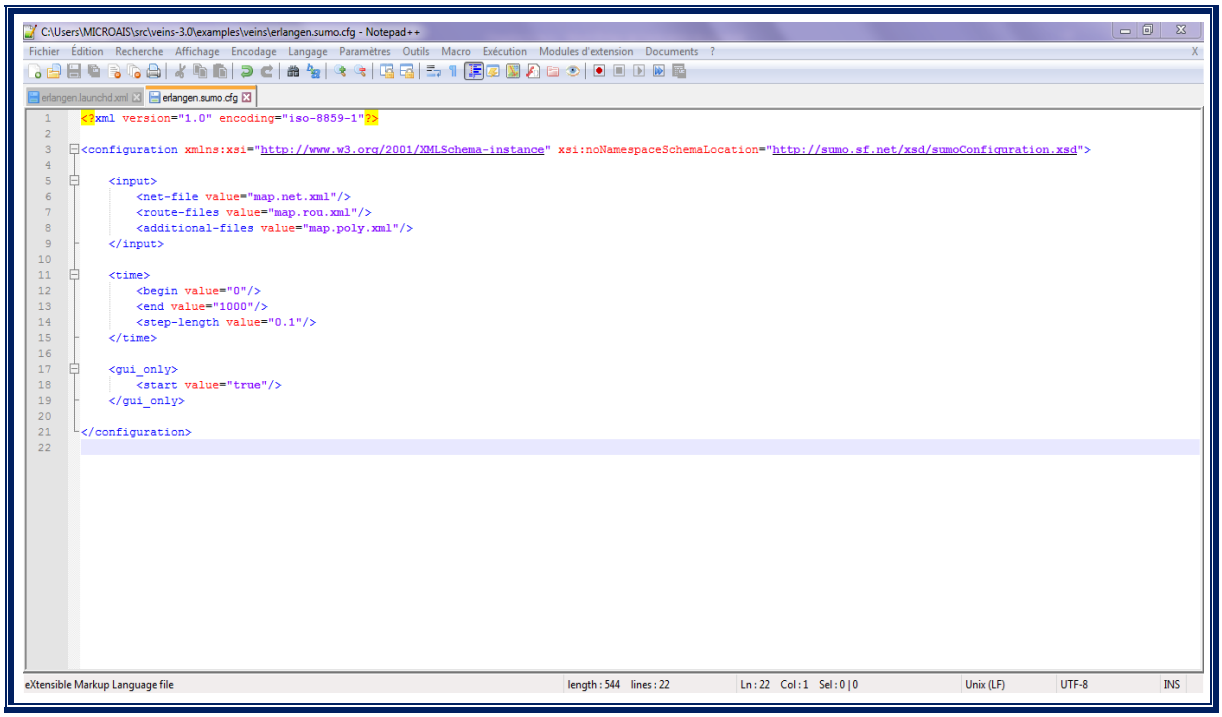


Fig. IV. 29 : *Modification du fichier erlangen.lauchd.xml.*

- ✓ **Lancement de la simulation :**

Avant de lancer la simulation, il est recommandé de nettoyer les variables locales de Veins. Ainsi, dans l'espace de travail OMNeT ++, avec le bouton droit de la souris on clique sur : clean local → clean project → build project.

Pour pouvoir procéder à la simulation on doit exécuter SUMO et OMNeT++ à la fois, c'est pour ça que Veins est livré avec un petit script python qui fait une connexions TCP proxy entre OMNeT++ et SUMO. Pour le faire, ce script commence une nouvelle copie de la simulation de SUMO pour la simulation de chaque OMNeT connexion. Ainsi, dans l'invite de commande ming on tape la commande montrée dans la figure *Fig.IV.30*, et le script va écouter sur le port 9999.

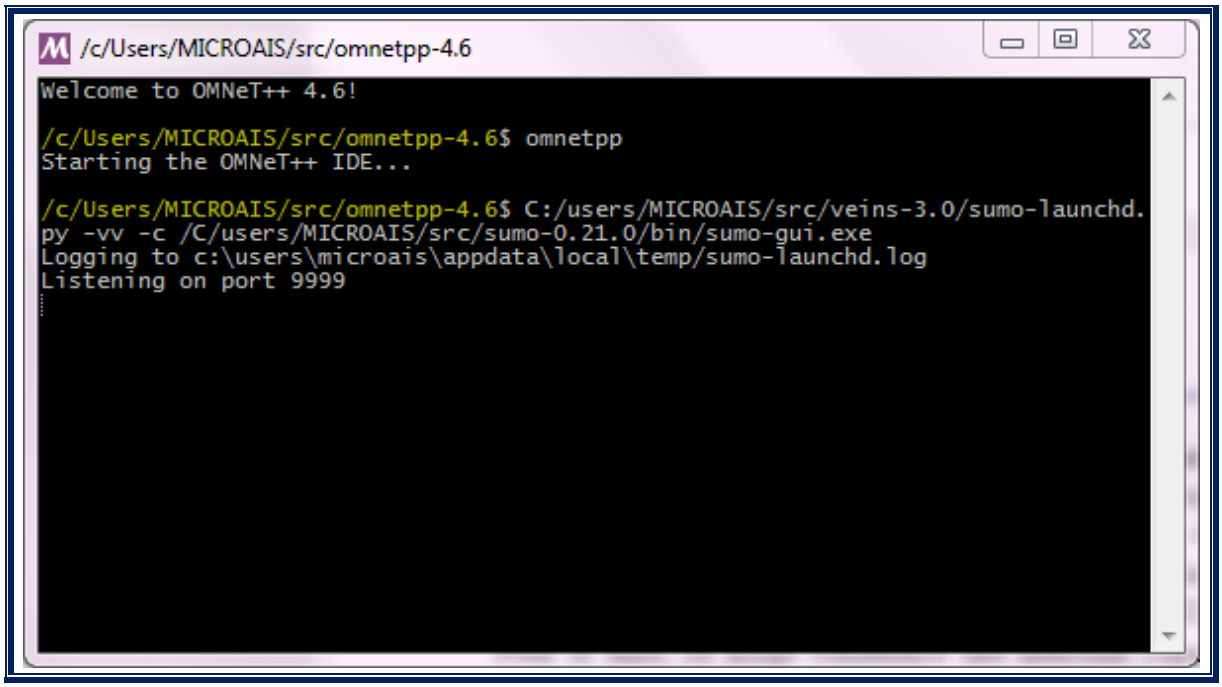


Fig. IV. 30 : *Ouverture et écoute sur le port TCP 9999.*

Dans l'EDI OMNeT++ illustré sur la figure *Fig.IV.31*, on clique avec le bouton droit sur omnetpp.ini afin de sélectionner Run As.

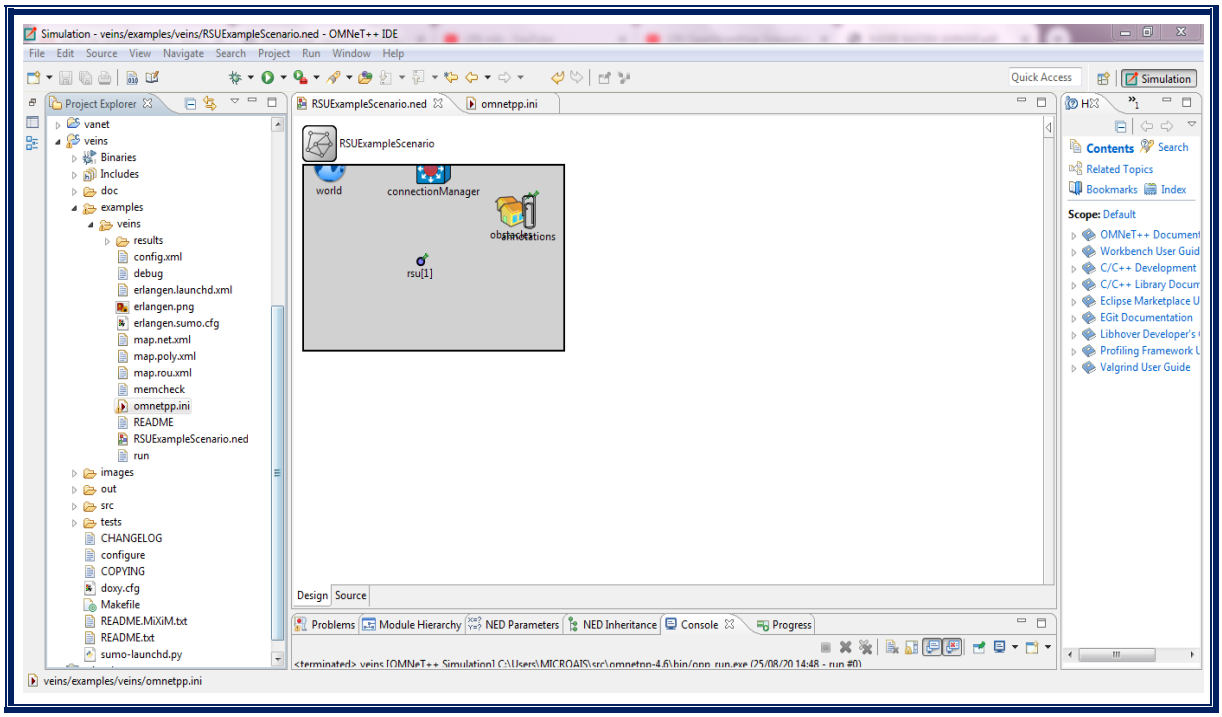


Fig. IV. 31 : *Exécution omnetpp.ini.*

Ensuite, on sélectionne une méthode d'exécution, dans notre cas « nodebug », comme montré sur à la Figure *Fig. IV.32*.

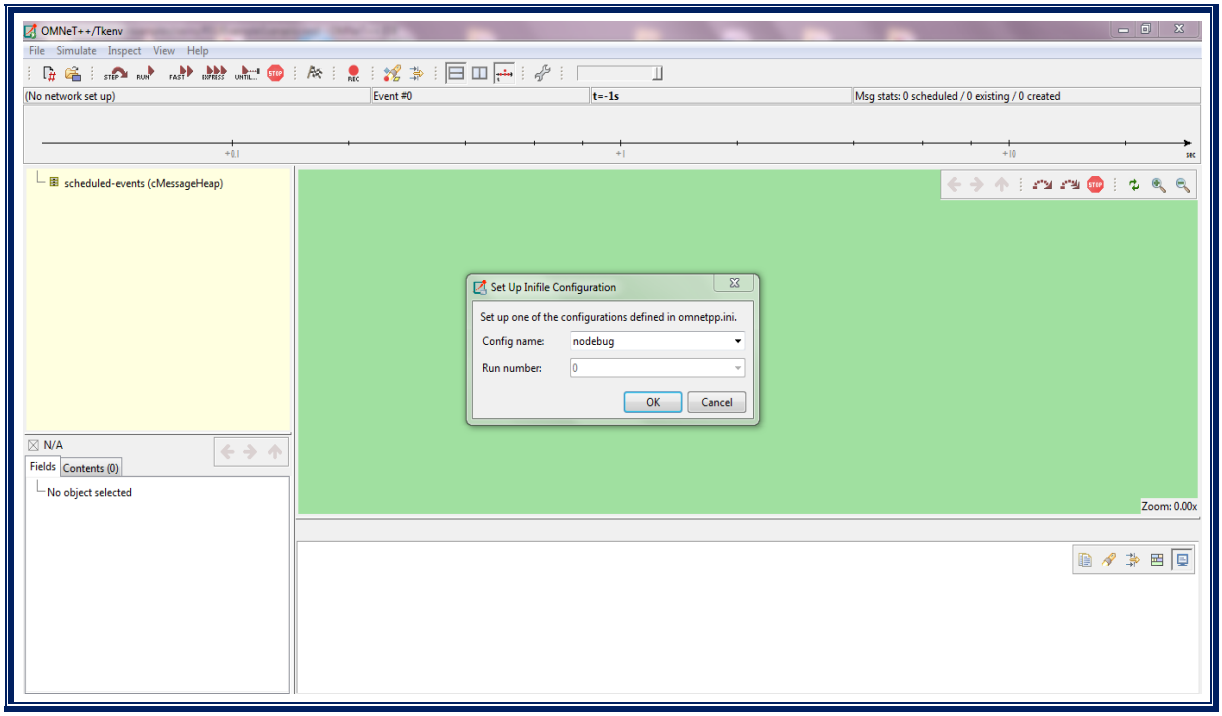


Fig. IV. 32 : *Sélection d'une méthode d'exécution.*

Enfin, on clique sur RUN pour pouvoir démarrer notre simulation comme le montre la figure *Fig. IV.33* ci-dessous.

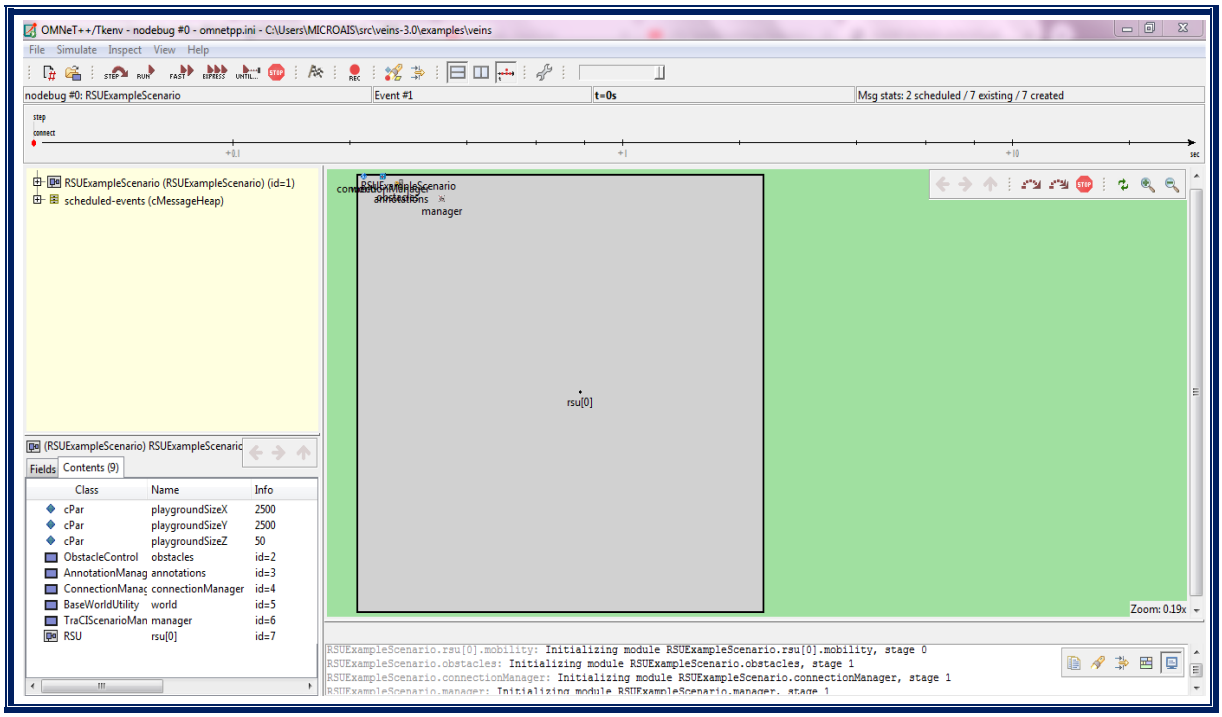


Fig. IV. 33 : *Fenêtre de simulation de OMNet++.*

Une autre fenêtre de SUMO sera lancée automatiquement comme illustré sur la figure *Fig. IV.34*.

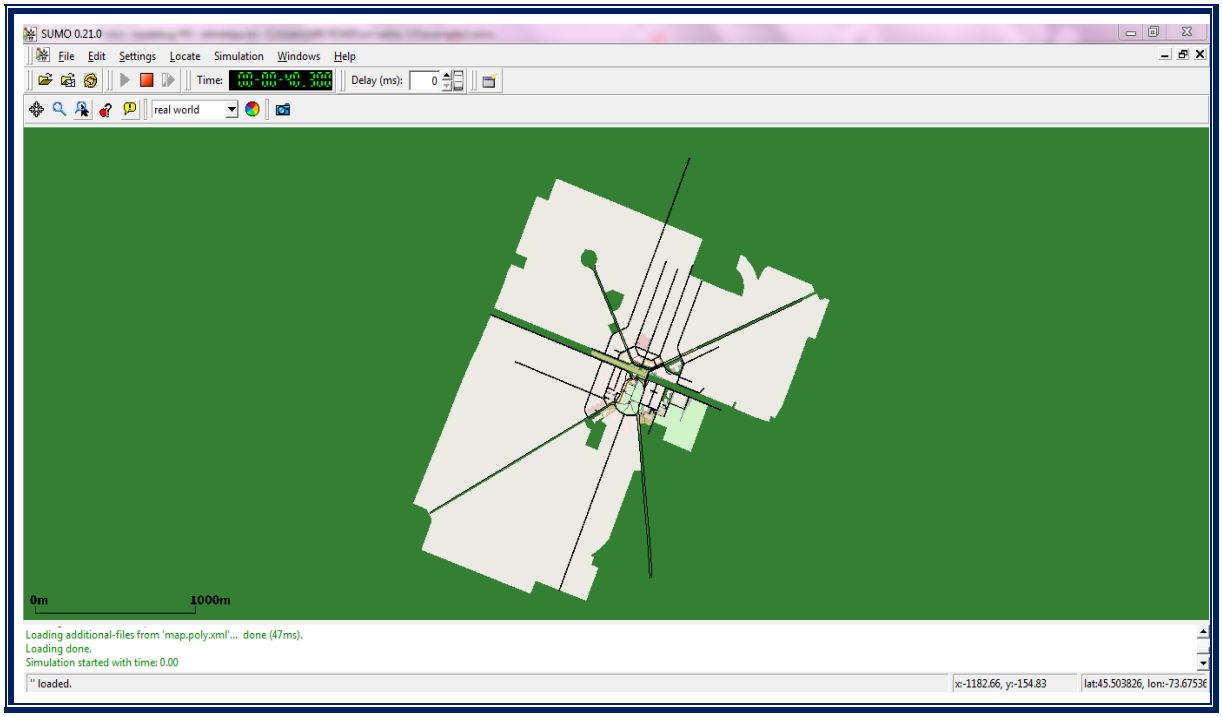


Fig. IV. 34 : *Fenêtre de simulation de SUMO.*

Enfin, les figures *Fig. IV.35* et *Fig. IV.36* montrent le déroulement de la simulation de notre réseau du trafic routier.

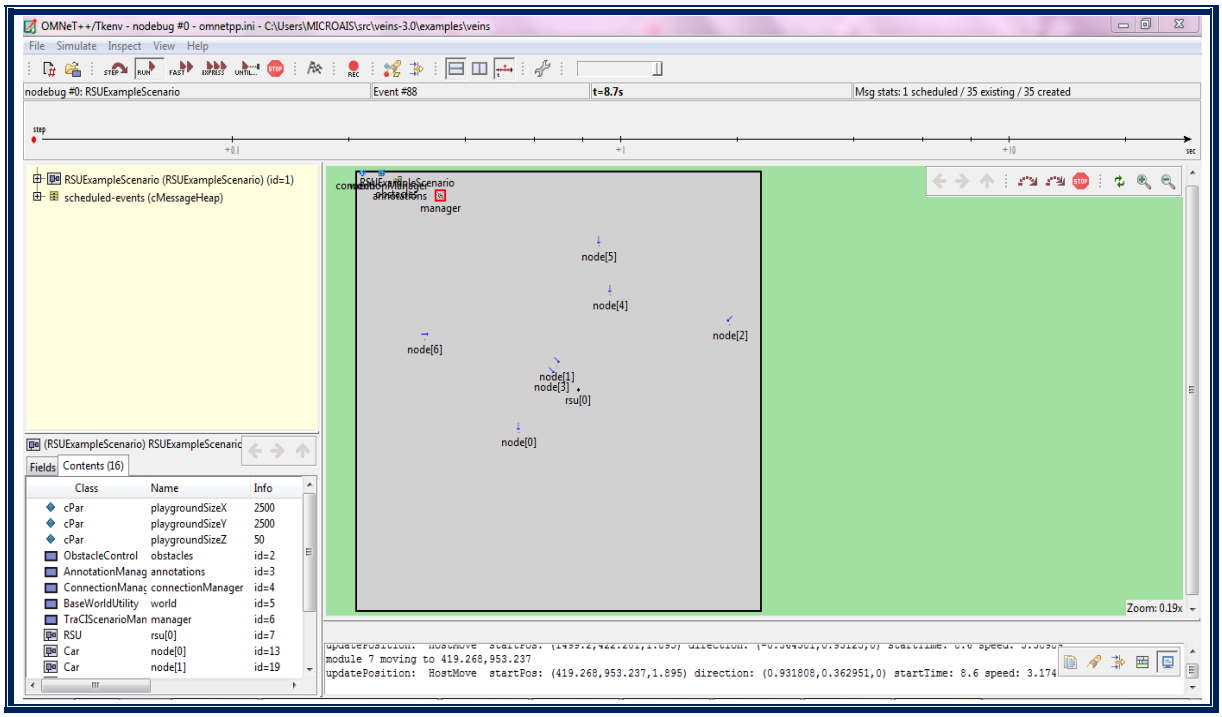


Fig. IV. 35 : *Simulation dans OMNeT++.*

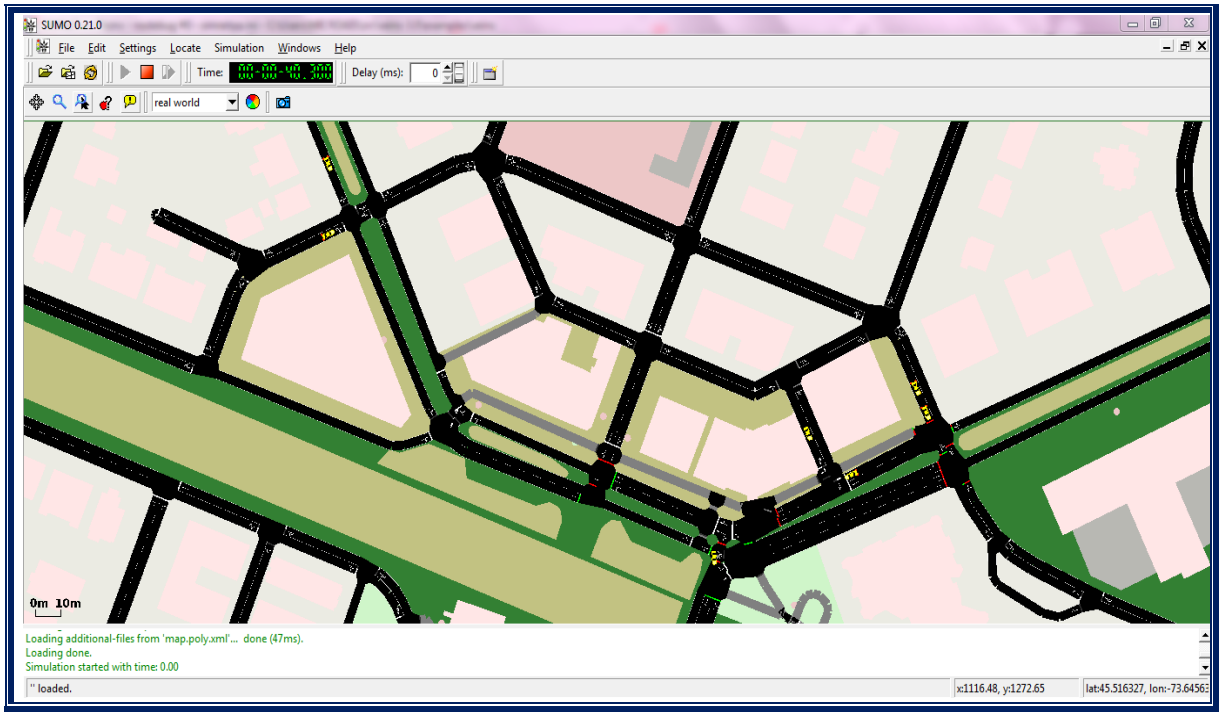


Fig. IV. 36 : *Simulation dans SUMO.*

IV.6. Conclusion :

Les problématiques propres aux réseaux de véhicules doivent être étudiées et évaluées par simulation. Ce chapitre s'est focalisé sur la modélisation et la simulation du réseau VANET de l'approche proposée.

Nous avons commencé par présenter un bref aperçu sur la simulation dans les VANET, après ça, on a abordé l'étude des logiciels nécessaires à la simulation. Ensuite, nous avons mis l'accent sur les étapes de la réalisation des clusters ainsi que l'implémentation des algorithmes de détection de la vitesse et de la distance dans l'environnement de développement OMNeT++.

A la fin de ce chapitre, nous avons simulé un scénario réel, extrait de la ville de Montréal (Canada), et cela s'est fait grâce à une simulation du réseau dans OMNeT++ et du trafic routier dans SUMO en parallèle, et ça, après avoir établi une connexion TCP Proxy en utilisant le Framework VEINS.

Conclusion Générale

Conclusion Générale et perspectives :

L'évolution des réseaux véhiculaires vise à rendre les réseaux plus sûrs, plus efficaces, plus fiables et plus écologiques aussi bien du point de vue de l'industrie automobile que des opérateurs de réseaux et services. Les réseaux ad hoc de véhicules (VANET) forment un nouveau type de réseaux issu des réseaux ad hoc mobiles (MANET). Ils se composent d'un nombre de véhicules circulant sur des routes, capables de communiquer entre eux. Cette communication peut être réalisée autant dans une topologie à infrastructure avec des stations de base et des RSU que dans une topologie ad-hoc dans laquelle les nœuds communiquent les uns avec les autres sans besoin de tiers d'aide à la communication.

Une technique de dissémination efficace pour les VANET doit absolument prendre en considération les caractéristiques de ces dernières, comme la taille du réseau, la vitesse des véhicules, ainsi que les différents besoins des services offerts par les réseaux VANET.

Notre mémoire s'est investi dans un domaine de recherche d'actualité, à savoir les réseaux véhiculaires et leur apport à l'amélioration de la sécurité routière. Les infractions routières et leur prévention dans ce type de réseaux est une problématique très intéressante par sa dimension humaine et économique. De ce fait nous avons apporté un système pour prévenir ce type d'événements durant le trafic routier.

L'objectif principal était de proposer une nouvelle approche de détection, basée sur un protocole de signature et de vérification des alertes frauduleuses en utilisant la cryptographie à seuil et un système de facturation automatique des contraventions routières, et l'adapter aux caractéristiques d'un réseau véhiculaire VANET organisé hiérarchiquement.

Dans un premier temps, nous avons présenté des généralités sur les réseaux sans fil ensuite nous avons abordé les réseaux ad hoc véhiculaires VANET : architecture des VANET et leurs composants ainsi que leurs caractéristiques et applications qui peuvent être déployées sur ce type de réseau.

Ensuite, nous avons abordé les principaux concepts des systèmes de transports intelligents (STI) : le contexte, le principe de fonctionnement, les objectifs, les types des STI et leurs enjeux. De ce fait, on a conclu que les STI peuvent contribuer directement ou indirectement dans l'amélioration de la sécurité, de l'efficacité et de la convivialité dans les transports routiers. Cependant ils sont déficients, ils ne procurent pas une circulation routière sûre à 100 %.

C'est pourquoi dans le troisième chapitre nous avons proposé une approche, qui permet d'éviter, ou du moins minimiser, le nombre d'accidents routiers, en détectant à l'avance les infractions (dépassement de la vitesse limite et le non-respect de la distance autorisée) commises par les conducteurs des véhicules tout au long de leur trajet, et les signaler auprès du serveur de police. Après vérification, ce dernier facture son propriétaire en calculant une amende en fonction de l'infraction commise. Cette approche, fonctionne sous un système de contrôle à seuil qui permet aux véhicules de coopérer pour produire la signature des preuves contre toute infraction commise.

Notons également que dans cette approche, les véhicules sont organisés sous forme de clusters, où chaque cluster est doté d'un chef appelé Cluster-Head (CH) qui joue le rôle d'un coordinateur local et d'une passerelle pour communiquer avec la RSU (Road Side Unit) et avec les membres de son cluster dits Cluster-Membre (CM).

Enfin, dans le quatrième chapitre, nous avons commencé d'abord par présenter les logiciels utilisés dans notre travail. Ensuite nous avons simulé notre algorithme de clustering accompagné de nos algorithmes de calcul de la vitesse limite et de la distance de sécurité minimale dans le simulateur de réseau OMNeT++. Enfin nous avons clôturé par la simulation de notre réseau routier créé dans le simulateur de trafic SUMO, par la suite nous avons présenté les différentes étapes nécessaires pour intégrer le simulateur SUMO dans OMNeT++ en utilisant Veins

Pour conclure, nous espérons que notre travail soit à la hauteur de vos expectations malgré le fait de ne pas pouvoir terminer entièrement l'approche proposée à cause de certaines circonstances qui ont fait retarder le déroulement de notre mémoire, et ainsi nous empêcher d'avoir le temps nécessaire pour terminer.

Perspectives :

Dans la continuité du travail de recherche présenté, nous pourrions approfondir notre étude afin d'améliorer les résultats obtenus. Plusieurs perspectives futures peuvent être proposées à la suite de ce travail :

- Réussir à implémenter l'approche au complet pour visionner et discuter les résultats, et la réaliser également sur le terrain.
- Extension de l'approche proposée afin de pouvoir détecter d'autres infractions routières.
- Concevoir un protocole d'échange de messages plus sécurisé en utilisant les pseudonymes.

Bibliographie

[1] « Organisation Mondiale de la Santé », 7 avril 1948. [En ligne]. Adresse URL : https://www.who.int/fr [Accès le 20 Mars 2020].

[2] A. AOUES, M. HAMMOUDI, Y. BENAISSA et N. BENSAIDANE. « Gestion de l'anonymat des communications dans les réseaux véhiculaires Adhoc sans fil (VANETs) ». Mémoire de licence en Informatique, présenté à l'université des sciences et de la technologie HOUARI BOUMEDIENE (USTHB), 2015. [En ligne]. Adresse URL : https://www.academia.edu [Accès le 23 mars 2020].

[3] M. Kahina. « Gestion de l'anonymat des communications dans les réseaux véhiculaires Adhoc sans fil (VANETs) ». Mémoire de fin d'études en vue de l'obtention du diplôme de MASTER, présenté à l'université du Québec à Trois-Rivières, juillet 2015. [En ligne]. Adresse URL : https://oraprdnt.uqtr.uquebec.ca/pls/public/docs/FWG/GSC/Publication/1645/34/1918/1/75448/8/F1689012680_M_moire_FINAL__K._Moghraoui.pdf [Accès le 23 Mars 2020].

[4] A. M. Nada. « L'intelligence ambiante et les systèmes de transport intelligents ». Mémoire en vue de l'obtention du diplôme MAGISTER en Informatique, présenté à l'université BADJI MOKHTAR de Annaba, 2014. [En ligne]. Adresse URL : http://biblio.univ-annaba.dz/wp-content/uploads/2015/10/Ahmed-Malek-Nada-.pdf [Accès le 10 Avril 2020].

[5] PIARC. « Amélioration de la sécurité routière par l'utilisation de systèmes de transport intelligents » 2011.

[6] J. Petit. « Surcoût de l'authentification et du consensus dans la sécurité des réseaux sans fil véhiculaires ». Thèse en vue de l'obtention du DOCTORAT, présentée à l'université Toulouse III - Paul Sabatier, Juillet 2018.

[7] J.-F. Pillou. « CommentCaMarche.net » [En ligne]. Adresse URL : https://www.commentcamarche.net [Accès le 15 juin 2020].

[8] L. Thing. « TechTarget », 1999. [En ligne]. Adresse URL : https://whatis.techtarget.com. [Accès le 15 juin 2020].

[9] « Automobile Club Association » [En ligne]. Adresse URL : https://www.automobile-club.org [Accès le 01 Avril 2020].

[10] « La sécurité routière de A à Z », 2015. [En ligne]. Adresse URL : http://m.securite-routiere-az.fr/a/adas/ [Accès le 01 Avril 2020].

[11] O. Publishing. « Sécurité routière, l'impact des nouvelles technologies », 16 Octobre 2003. [En ligne]. Adresse URL : https://books.google.dz/books?id=SANWlGrLoCUC&printsec=frontcover&hl=fr#v=onepage&q&f=false [Accès le 02 Avril 2020].

[12] « Squarell » [En ligne]. Adresse URL : https://squarell.com. [Accès le 02 Avril 2020].

[13] R. P. Nayak, S. Sethi et S. K. Bhoi. « PHVA : A Position Based High Speed Vehicle Detection Algorithm for Detecting High Speed Vehicles using Vehicular Cloud », 2018.

[14] C. Olaverri-Monreal, G. C. Krizek, F. Michaeler, R. Lorenz et M. Pichler. « Collaborative approach for a safe driving distance using stereoscopic image processing » Université des sciences appliquées Technikum Wien .

[15] « CommentCalculer.fr » [En ligne]. Adresse URL : https://commentcalculer.fr/calcul/calculateur-de-distance-3d [Accès le 02 Août 2020].

[16] « Bibm@th.net » [En ligne]. Adresse URL : http://www.bibmath.net [Accès le 21 juin 2020].

[17] « Britannica » [En ligne]. Adresse URL : https://www.britannica.com/ [Accès le 21 juin 2020].

[18] P. Changgen et L. Xiang. « Threshold Signcryption Scheme Based on Elliptic Curve Cryptosystem and Verifiable Secret Sharing ». Université Guizhou en Chine, 2005.

[19] S. BOUCHELAGHEM et O. MAWLOUD. « Reliable and Secure Distributed Smart Road Pricing System for Smart Cities », 2018.

[20] A. Ayadi. « Extensions du simulateur Omnet++ pour la validation de mécanismes de transmission multimédia dans les réseaux sans fils IEEE 802.11 ». Université de la Manouba, [En ligne]. Adresse URL : https://www.memoireonline.com/07/08/1359/extensions-simulateur-omnet-tramsmission-multimedia-reseaux-ieee-802-11.html. [Accès le 07 Août 2020].

[21] « VEINS : vehicles in network simulation ». [En ligne]. Adresse URL : http://veins.car2x.org/ [Accès le 07 Août 2020].

La cryptographie :

Définition :

De manière générale, Le mot cryptographie est un terme générique désignant l'ensemble des techniques permettant de chiffrer des messages, c'est-à-dire permettant de les rendre inintelligibles sans une action spécifique.

La cryptographie est traditionnellement utilisée pour dissimuler des messages aux yeux de certains utilisateurs. Cette utilisation a aujourd'hui un intérêt d'autant plus grand que les communications via internet circulent dans des infrastructures dont on ne peut garantir la fiabilité et la confidentialité. Désormais, la cryptographie sert non seulement à préserver la confidentialité des données mais aussi à garantir leur intégrité et leur authenticité. On l'emploie dans des domaines très divers, y compris les VANET.

Dans cette section, nous présentons quelques notions utiles sur la signature numérique, la cryptographie à seuil, la signature à seuil et la cryptographie à courbe elliptique.

Types de cryptographie :

- **La signature numérique :**

La signature numérique, est une technique de validation mathématique de l'authenticité et de l'intégrité d'un message, d'un logiciel ou d'un document électronique. Equivalent électronique, par essence plus sécurisé, d'une signature manuscrite ou de l'apposition d'un sceau, la signature numérique est une solution à la falsification et l'usurpation d'identité dans les communications électroniques. Elle constitue un élément supplémentaire prouvant l'origine, l'identité et l'état d'un document électronique, d'une transaction ou d'un message et démontre le consentement éclairé du signataire.

Étant donné un message m et une clé privée $\widehat{K}$, la fonction $S(m, \hat{k})$ affiche σ_m, qui est la signature du message m par la clé privée $\widehat{K}$. Une signature numérique est valide si pour la signature σm produite par $S(m, \hat{k})$, la vérification avec la fonction $V(m, \sigma m, K)$ est correct, où K est la clé publique correspondante de $\hat{k}$.

N'importe quel message, chiffré ou non, peut contenir une signature numérique pour assurer le destinataire de l'identité de l'expéditeur et de l'intégrité du message. Le recours aux signatures numériques empêchera le signataire de nier avoir signé (non-répudiation), à moins que sa clé privée n'ait été compromise.

- **La cryptographie à seuil :**

L'idée de la cryptographie à seuil basée sur $< t, n >$ a été introduite par « Shamir ». La cryptographie à seuil est une technique de partage d'un secret (un fichier, un texte...) en le distribuant par *n* participants.

Le secret est divisé en plusieurs morceaux, appelés « parties ». Ces morceaux, sont utilisés pour reconstituer le secret original. Pour déverrouiller l'accès au secret via le principe de

Shamir, un nombre minimum de parties doit être réunies. C'est ce qu'on appelle « le seuil *t* », qui est utilisé pour indiquer le nombre minimum de parties nécessaires pour déverrouiller l'accès au secret.

Plus formellement, on parle de partage de secret à *n* participants avec seuil *t* si on partage un secret entre n personnes de sorte que :

- ✓ t personnes prises parmi ces n participants peuvent toujours reconstituer l'information secrète;
- ✓ (t-1) personnes prises parmi ces '*n*' participants ne peuvent jamais reconstituer l'information secrète.

La cryptographie à seuil a trouvé applications dans de nombreux domaines, y compris les signatures numériques.

- **La signature numérique à seuil :**

Dans une signature numérique à seuil $< t, n >$, une clé privée est divisée en *n* parties, chacune appartenant à un participant. Une signature numérique à seuil valide peut être produite si *t* participants combinent leurs parts. Cependant, aucune signature valide ne peut être générée par moins de *t* participants. Chaque participant utilise son partage de clé privée pour générer une signature partielle sur un message, et ces signatures partielles peuvent être combinées en une signature de seuil sur le message. La signature de seuil peut être vérifiée à l'aide de la clé publique correspondant à la clé privée divisée. La taille de la signature de groupe et le temps de vérification de la signature de groupe sont équivalents à ceux d'une signature numérique individuelle. En d'autres termes, la signature de seuil $< t, n >$ a les cinq propriétés suivantes :

- ✓ Toute signature de groupe est générée mutuellement par au moins *t* membres du groupe.
- ✓ La taille de la signature de groupe est équivalente à la taille d'une signature individuelle.
- ✓ Le processus de vérification de signature est simplifié car il n'y a qu'une seule clé publique de groupe requise.
- ✓ La signature du groupe peut être vérifiée par tout étranger.
- ✓ Le groupe est responsable du message signé.

Chaque membre du groupe signe un message séparément et envoie la signature individuelle à un commis désigné. Le commis valide chaque signature individuelle (partielle) puis combine toutes les signatures individuelles en une signature de groupe. Le schéma de signature de seuil $< t, n >$ peut être facilement étendu pour devenir un schéma multi signature numérique. Le schéma de cette opération est illustré dans la figure Fig. 1.

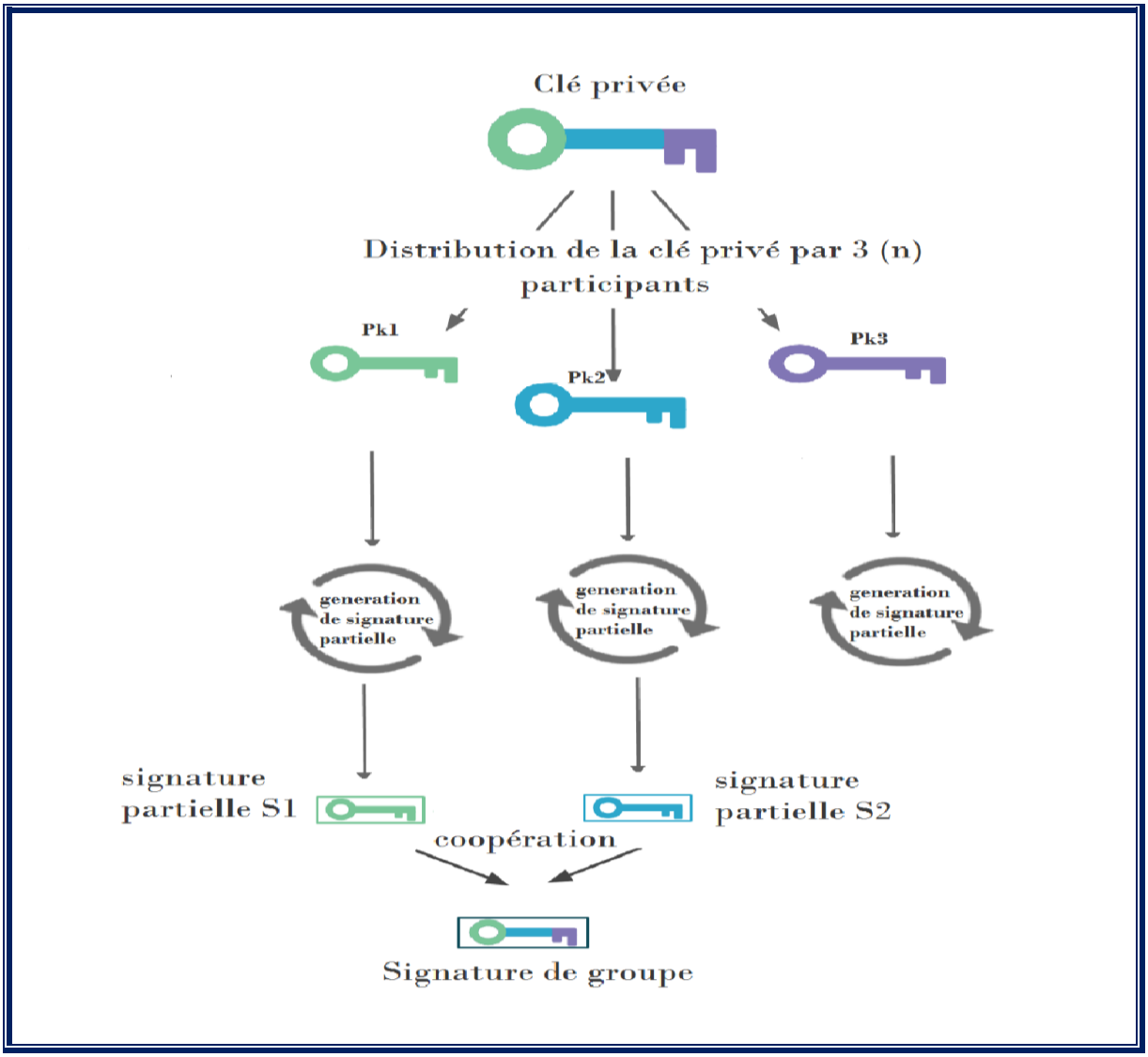


Fig. 1 : *Processus de la signature numérique à seuil.*

➢ **La cryptographie a courbe elliptique (ECC) :**

La cryptographie à courbe elliptique (en anglais, elliptic curve cryptography ou ECC) est la plus couramment utilisée pour le cryptage, l'échange de clés avec le protocole Diffie-Helman et pour les signatures numériques.

Depuis son apparition, ECC a évolué comme une alternative intéressante aux autres systèmes de clé publique tels que RSA. ECC est basé sur les mathématiques des courbes elliptiques et utilise l'emplacement des points d'une courbe elliptique pour chiffrer et déchiffrer des informations. Il offre des tailles de clés plus petites avec une force de sécurité équivalente car il repose sur la difficulté de résoudre le Problème de Logarithme Discret de la Courbe Elliptique (ECDLP).

L'utilisation de l'ECC est étendue à un large éventail d'applications modernes telles que la sécurisation des communications des véhicules dans les villes intelligentes.

La cryptographie sur les courbes elliptiques regroupe un ensemble de techniques cryptographiques qui utilisent une ou plusieurs propriétés des courbes elliptiques, ou plus généralement d'une variété abélienne.

L'utilisation de ces propriétés permet d'améliorer les primitives cryptographiques existantes, par exemple en réduisant la taille des clés cryptographiques, ou de construire de nouvelles primitives cryptographiques qui n'étaient pas connues.