Table des matières

Introduction générale 1
Chapitre I Généralités sur les réseaux VANETs 3
I.1 Introduction 3
I.2 Généralités sur les réseaux sans fil 4
I.2.1 Les réseaux sans fil "Wirless Network" 4
a) Réseaux sans fil avec infrastructure 4
b) Réseaux sans fil sans infrastructure 4
I.2.2 Les réseaux mobiles sans fil MANETs 4
I.2.3 Les réseaux Ad-hoc véhiculaire (VANETs) 5
I.3 Présentation détaillée sur les VANETs 5
I.3.1 Nœud d'un réseau VANET 5
I.3.2 Composants d'un réseau VANET 6
I.3.3 Les modes de communication dans les réseaux VANETs 6
a) Le mode de communication de véhicule à véhicule (V2V) 7
b) Le mode de communication de véhicule à infrastructure (V2I) 8
c) Le mode de communication hybride 8
I.3.4 Les caractéristiques des réseaux VANET 8
a) Topologie hautement dynamique 9
b) Réseau déconnecté fréquemment 9
c) Mobilité de la modélisation et de la prévention 9
d) Environnement de communication 9
e) Contrainte de délai difficile 9
f) Interaction avec les capteurs embarqués 9
g) Batterie et stockage illimités 9
I.3.5 Domaines d'application des réseaux VANETs 9
a) Application de sécurité 10
b) Application commerciales 11
c) Applications de commodité 11
d) Applications productives 12
I.3.6 La sécurité dans les réseaux VANETs 12
a) Caractéristique de la sécurité 12
b) Menaces sur la sécurité 13

c) Mécanismes de base de la sécurité 13
I.4 Norme et standard de communication 14
I.4.1 DSRC 14
I.4.2 IEEE 802.11 p 15
I.4.3 WAVE 15
a) La couche physique du WAVE 15
b) La couche MAC du WAVE 16
I.5 Les avantages et les inconvénients des réseaux VANETs 16
I.5.1 Les avantages 16
a) Topologie dynamique 16
b) Echange entre des nœuds hétérogène 16
c) Propagation par trajet multiple 16
d) Relais d'information 17
I.5.2 Les inconvénients 17
a) Canal radio partagé et limité 17
b) Les interférences 17
I.6 Conclusion 17
Chapitre II Le routage dans les réseaux VANETs 19
II.1 Introduction 19
II. 2 Objectifs du routage dans les réseaux sans fil 19
II.3 Routage dans les MANETs 19
II.4 Routage dans les réseaux VANETs 20
II.5 La différence entre les MANETs et les VANETs 20
II.6 Classification des protocoles de routage dans les réseaux VANETs 21
II.6.1 Les protocoles de routage basé sur la topologie 22
a) Les protocoles réactifs 22
b) Les protocoles proactifs 22
c) Les protocoles hybrides 22
II.6.2 Les protocoles de routage géographiques 22
II.7 Les principaux protocoles de routage dans les réseaux VANETs 23
II.7.1 AODV (Ad-hoc On Demand Distance Vector) 23
a) Les avantages 23
b) Les inconvénients 23
II.7.2 GSR (Global State Routing) 23
a) Les avantages 24

b) Les inconvénients 24
II.7.3 A-STAR (Anchor-based Street and Traffic Aware Routing) 24
a) Les avantages 24
b) Les inconvénients 24
II.7.4 GPSR (Greedy Perimeter Stateess Routing) 24
a) Les avantages 24
b) Les inconvénients 25
II.7.5 GyTAR (Greedy Traffic Aware Routing) 25
a) Les avantages 25
b) Les inconvénients 25
II.8 Conclusion 25
Chapitre III Version améliorée du protocole EGyTAR 27
III.1 Introduction 27
III.2 Environnement de simulation de notre application 27
III.2.1 Simulateur : OMNET++ 27
a) Présentation du simulateur 27
b) Architecture d'OMNET++ 28
c) Comparaison entre OMNET++ et d'autres simulateurs 28
d) BonnMotion 29
e) ManhattanGrid 30
III.2.2 Outils d'implémentation et d'évaluation 30
a) Environnement matériel 30
b) Environnement logiciel 30
III.2.3 Implémentation et évaluation 30
a) Fonctionnement GyTAR 30
b) Amélioration proposé : CDP périodique 32
d) Métriques d'évaluation 36
III.2.4 Résultats et discussion 37
a) Taux de paquets délivrés 37
b) Taux d'utilisation du trafic véhiculaire 38
c) Délai de bout en bout 39
III.3 Conclusion 39
Conclusion générale et perspectives 39
Références 40
Liste des figures 42

Liste des tableaux 42
Glossaire 43
Annexe A : Comment installer les outils de simulation ? 46
Annexe B : Composants d'un projet OMNET++ 47

Introduction générale

Introduction générale

Ces dernières années, 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 l'augmentation des coûts de carburants, la pollution causée par la combustion des carburants et la haute densité automobiles en particulier dans les grandes villes.

Par ailleurs, les systèmes de transport actuels fournissent très peu d'informations sur les conditions routières. Ils sont l'une des causes des difficultés de circulation entraînant des dégâts environnementaux ainsi qu'une piètre qualité de vie. Selon le rapport réalisé par l'OMS[1] sur la sécurité routière dans le monde en 2013, les traumatismes dus aux accidents de circulation représentent la huitième cause de décès dans le monde et la première cause de décès de la population dans la tranche d'âge est comprise entre 15 et 29 ans. En effet, ces systèmes de transport sont à la base des embouteillages qui coûtent près de 266 milliards de dollars par an et ralentissent de façon considérable les usagers dans leurs trajets.

La circulation en voiture est devenue dans les grandes villes, telles Moscou, Pékin ou encore Mexico, une souffrance quotidienne aux automobilistes à cause des embouteillages. Par exemple, à Moscou il y a en moyenne plus de deux heures d'embouteillage par jour. Un problème encore plus important est celui de la sécurité routière. A cet effet, plusieurs démarches ont été prises pour améliorer la sécurité routière et résoudre les problèmes de la circulation. Parmi ces démarches, les compagnes de sensibilisation et de prévention routière, les sanctions aux violations du code de la route qui deviennent plus en plus sévères, l'intégration des moyens de protection à bord de véhicules, l'amélioration des infrastructures routières ainsi que l'augmentation et l'amélioration des services à bord des moyens de transport en commun. En outre, une autre solution a vu le jour dans les années 90. Cette solution est appelée "Systèmes de Transport Intelligent (STI) ou ITS[2]".

Les systèmes de transport intelligent sont considérés comme un ensemble de véhicules interconnectés directement entre eux ou via une infrastructure. Dans ces systèmes, un véhicule est doté d'un certain nombre de capteurs et d'un système de géolocalisation lui permettant la mesure de la vitesse et de la distance entre les autres véhicules, etc. Ils peuvent être aussi dotés, des microcontrôleurs ou même des microprocesseurs capables de traiter les informations issues des capteurs et ainsi permettre au véhicule de réagir aux évènements inattendus. Ces équipements sont embarqués dans un véhicule et doivent communiquer et échanger des données

[1] OMS : Organisation Mondiale de la Santé
[2] ITS : Intelligent Tranportation System

entre les véhicules afin de garantir la sécurité routière ainsi que la fluidité du trafic routier d'où on parle de réseaux Ad-hoc véhiculaires (VANETs).

Les VANETs (Vehicular Ad Hoc Networks) sont des réseaux constitués d'un ensemble d'objets mobiles qui communiquent entre eux à l'aide de réseau sans fil de type IEEE Bluetooth, Wi-Fi, WiMax, 4G, etc. Avec de tels mécanismes de communication, un véhicule peut recevoir des informations de ses voisins proches ou d'autre plus distants, grâce à un schéma de routage multi-sauts qui exploite dans ce cas des objets intermédiaires comme relais. Dans ce type de réseaux, un véhicule pourra être soit un nœud ou un routeur.

L'objectif de ce projet est de proposer une amélioration du protocole de routage EGyTAR en termes de délai de bout en bout, de taux de paquets délivrés et de taux de paquets délivrés avec succès.

Ce mémoire s'articule autour de trois chapitres encadrés par une introduction générale et une conclusion générale :

Le premier chapitre fait l'objet d'une présentation de quelques généralités sur les réseaux VANETs.

Le deuxième chapitre présente le routage dans les réseaux VANETs tout en mettant l'accent sur les protocoles de routage les plus répandus pour ce type de réseaux.

Le troisième chapitre est une implémentation de la version améliorée du protocole EGyTAR suivie d'une évaluation des performances des deux protocoles : la version originale et la version améliorée.

Rapport-Gratuit.com

Chapitre I
Généralités sur les réseaux VANETs

Chapitre I
Généralités sur les réseaux VANETs

I.1 Introduction

Les communications qui peuvent être établies par un véhicule joueront un rôle important dans les années à venir. Ces communications peuvent être entre véhicules ou entre un véhicule (V2V) et une infrastructure existante au bord de la route (V2I). En effet, les véhicules de demain ne se contenteront plus de détecter les dangers grâce à des radars ou des caméras, ils seront capables de recevoir des messages d'alertes envoyés par les autres véhicules ou par l'infrastructure (panneaux, portiques, etc.) et de transmettre ces informations à d'autres véhicules.

Le nombre de véhicules en circulation est de plus en plus important. En 2010, nous avons dépassé le milliard de voitures sur les routes, et l'augmentation est en moyenne de 35 millions par an. Liés à cette croissance constante, les accidents de la route font partie de dix principales causes de la mortalité dans le monde. Afin de réagir à cette situation, l'amélioration de la sécurité routière est devenue une préoccupation de tous les gouvernements dans le monde. C'est dans cet esprit que sont apparues un certain nombre de recherches qui visent non seulement à réduire le nombre de mort sur les routes et à améliorer les conditions de la circulation, mais aussi à diminuer les embouteillages et la pollution en particulier dans les grandes villes [3]. Cette pollution a aussi un impact négatif sur la santé des citoyens.

Dans cette optique, un nouveau type de réseaux est apparu, qui sont connus sous le nom "Réseaux Véhiculaires (VANETs[3])". Ces réseaux est un type particulier des réseaux ad-hoc mobiles (MANETs). Ils constituent le noyau des Systèmes de Transport Intelligents (STI) qui ont objectif principal l'amélioration de la sécurité routière en tirant profit de l'émergence de la technologie de communication et la baisse du coût des dispositifs sans fil. En effet, grâce à des capteurs installés à bord des véhicules, ou bien situés au bord des routes et des centres de contrôle, les communications véhiculaires permettront aux conducteurs d'être avertis suffisamment tôt de dangers éventuels. De plus, ces réseaux ne se contenteront plus d'améliorer la sécurité routière seulement, mais ils permettront aussi d'offrir de nouveaux services aux usagers des routes rendant la conduite plus agréable.

Dans ce chapitre, nous présentons d'abord les réseaux ad-hoc de manière général, puis nous se focalisons sur les réseaux VANETs, les différents types de services offerts par ces réseaux et les modes de communication existants. Enfin, nous décrivons les différentes caractéristiques, contraintes et défis qui affronteront les concepteurs lors de la conception des protocoles de routage dédiés à ce type de réseaux.

[3] VANETs : Vehicular Ad-hoc NETworks

Rapport-gratuit.com
LE NUMERO 1 MONDIAL DU MÉMOIRES

I.2 Généralités sur les réseaux sans fil

Dans cette section, nous présentons tout d'abord les réseaux sans fil puis nous mettons le point sur les réseaux VANETs, leurs caractéristiques, objectifs, avantages et inconvénients. Enfin, nous présentons la spécificité de routage dans les réseaux VANETs.

I.2.1 Les réseaux sans fil "Wirless Network"

Ce sont des réseaux qui ne nécessitent pas une connexion filaire entre les nœuds, la communication se fait par voie hertzienne. Les réseaux sans fil peuvent être organisés en deux classes :

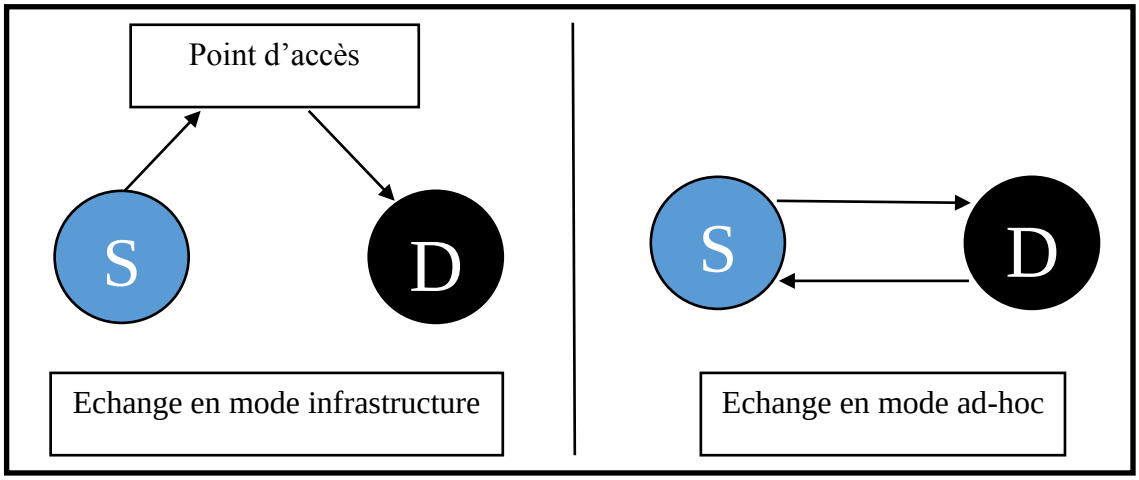


Figure 1: Exemple de réseaux avec infrastructure et sans infrastructure

a) Réseaux sans fil avec infrastructure

Dans cette architecture de ce type, le réseau est obligatoirement composé par au moins un point d'accès appelé aussi station de base, muni d'une interface de communication sans fil pour permettre une communication directe avec les nœuds mobiles se trouvant dans sa proximité. Un point d'accès couvre une zone géographique limitée. Un nœud mobile rattachée à un moment donné qu'à un point d'accès lui offrant tous les services tant que le nœud mobile est à l'intérieure de la zone de couverture du point d'accès.

b) Réseaux sans fil sans infrastructure

Il s'agit d'un mode point à point, nécessitant pas de points d'accès. Il permet de connecter les stations quand aucun point d'accès n'est disponible. L'absence d'infrastructure oblige les stations mobiles à jouer le rôle à la fois station et routeur.

I.2.2 Les réseaux mobiles sans fil MANETs

Ce sont des systèmes autonomes composés des nœuds mobiles dynamiques interconnectés par des liens sans fil sans l'utilisation d'une infrastructure fixe. Dans ces

systèmes, les nœuds sont libres de se déplacer de façon aléatoire, par conséquence, la structure du réseau change fréquemment et d'une manière imprévisible.

I.2.3 Les réseaux Ad-hoc véhiculaire (VANETs)

Un réseau VANET est un réseau de communication entre véhicules intelligents équipés de calculateurs, de périphériques réseau et de différents types de capteurs.

Les VANETs fonts partie de la famille des réseaux mobiles MANET qui fonctionnent dans des réseaux à liaison pair à pair sans infrastructure, c'est-à-dire que tout nœud appartenant au réseau pourra être considéré comme un point d'accès. Dans un réseau véhiculaire, les nœuds sont des véhicules intelligents appartenant au réseau et qui peuvent communiquer entre eux directement s'ils sont à portée ou via des véhicules intermédiaires s'ils sont éloignés.

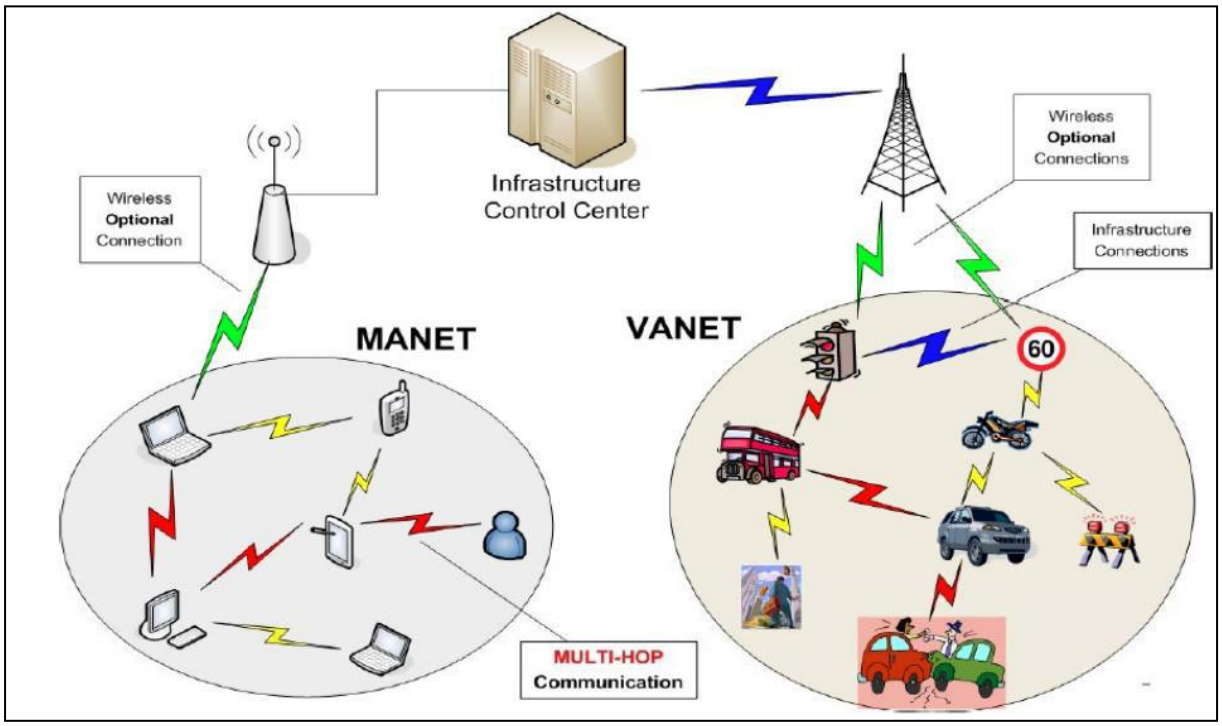


Figure 2: Exemple de réseaux VANETs [4]

I.3 Présentation détaillée sur les VANETs

I.3.1 Nœud d'un réseau VANET

Un nœud dans un réseau de véhicules est un véhicule intelligent équipé de terminaux tels que :

- Les calculateurs
- Les interfaces réseaux
- Les capteurs capables de collecter et traiter les informations

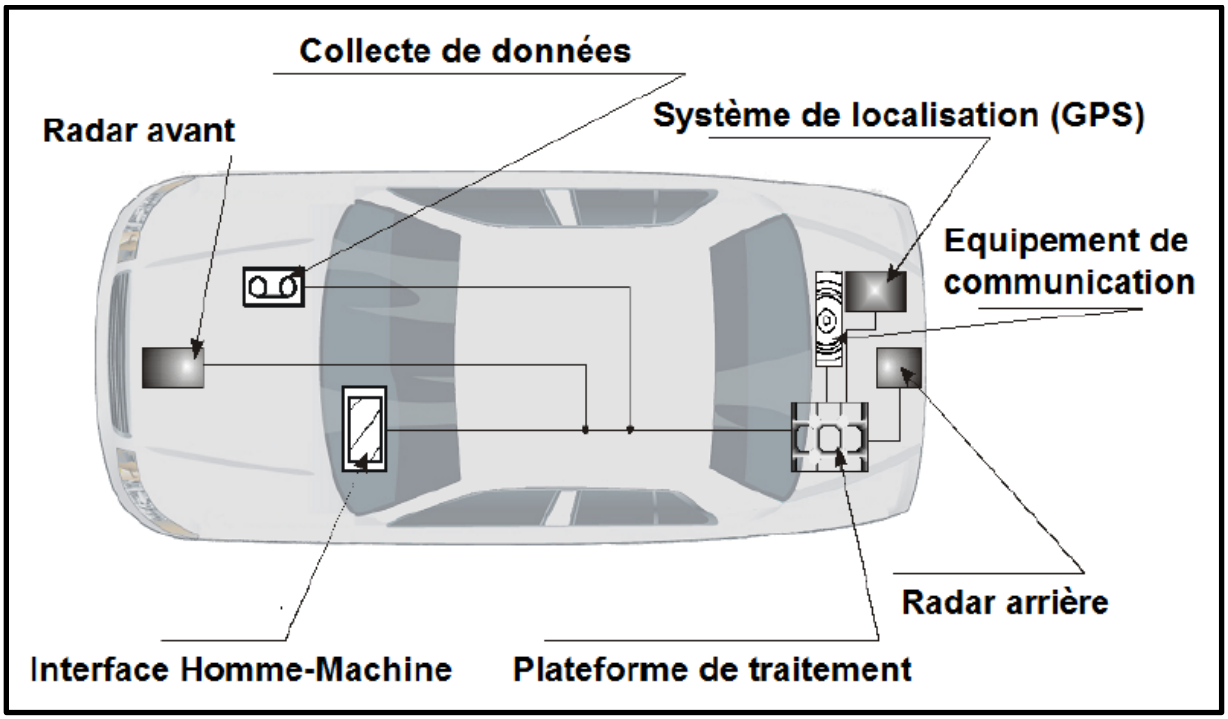


Figure 3: Eléments constituant un véhicule intelligent [5]

I.3.2 Composants d'un réseau VANET

Un réseau VANET est constitué principalement de trois entités [6]:

- TA (Trusted Authority) : C'est une source d'authenticité de l'information. Elle assure la gestion et l'enregistrement de toutes les entités sur le réseau : RSU (Road Side Unit) et OBU (On Board Unit). TA est sensée connaitre toutes les vraies identités des véhicules et au besoin les divulguer pour les forces de l'ordre.
- RSU (Road Side Unit) : Elles sont installées au bord des routes. Leur principale responsabilité est de soutenir la TA dans la gestion du trafic et des véhicules. Elles représentent des points d'accès au réseau et peuvent fournir les différentes informations sur la circulation aux véhicules sur un certain tronçon de route.
- OBU (On-Bord Unit) : Ce sont des entités embarquées dans les véhicules intelligents. Elles regroupent un ensemble de composants matériels et logiciels de hautes technologies (GPS, radar, caméras, différents capteurs et autres). Leurs rôles sont d'assurer la localisation.

I.3.3 Les modes de communication dans les réseaux VANETs

On distingue trois types de communication :

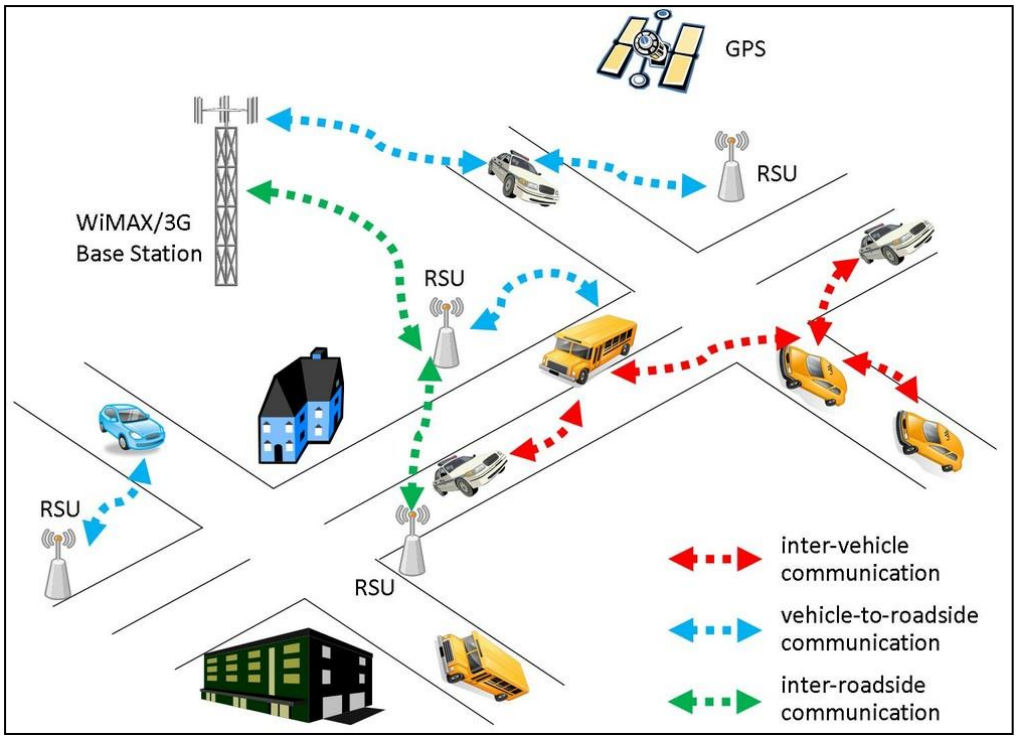


Figure 4: Modes de communications dans les réseaux VANETs [7]

a) Le mode de communication de véhicule à véhicule (V2V)

Dans ce mode, un réseau de véhicules est vu comme un cas particulier de réseaux mobiles ad-hoc MANET où les contraintes d'énergie, de mémoire et de capacité de calcul sont relaxées et où le modèle de mobilité n'est pas aléatoire, mais prévisible avec une très forte mobilité. Cette architecture peut 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 des applications de la sécurité routière, les réseaux à infrastructure montrent leurs limites, surtout en termes de délais. Et il est clair qu'une communication ad-hoc multi-sauts est plus performante qu'une communication passant par un réseau d'opérateur ou une infrastructure. La figure 5 illustre ce mode de communication entre véhicules.

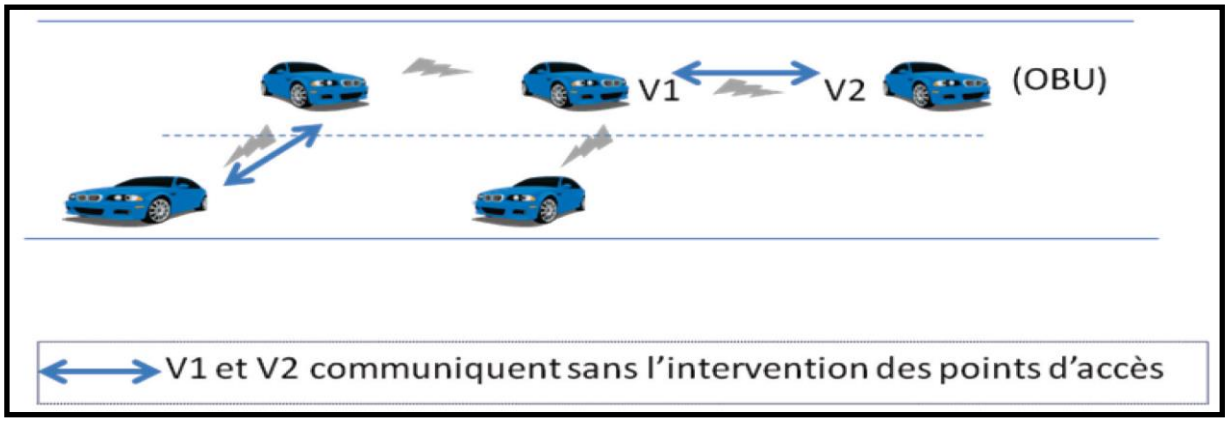


Figure 5: Communication véhicule à véhicule (V2V)

b) Le mode de communication de véhicule à infrastructure (V2I)

Ce mode de communication permet une meilleure utilisation des ressources partagées et démultiplie les services fournis (exemple d'échange de données de voiture à domicile, accès Internet, diagnostique distant pour réparer un véhicule, etc.) grâce à des point d'accès RSU déployés aux bords des routes. Ce mode est inadéquat pour les applications liées à la sécurité routière car les réseaux à infrastructure ne sont pas performants quant aux délais d'acheminement [8].

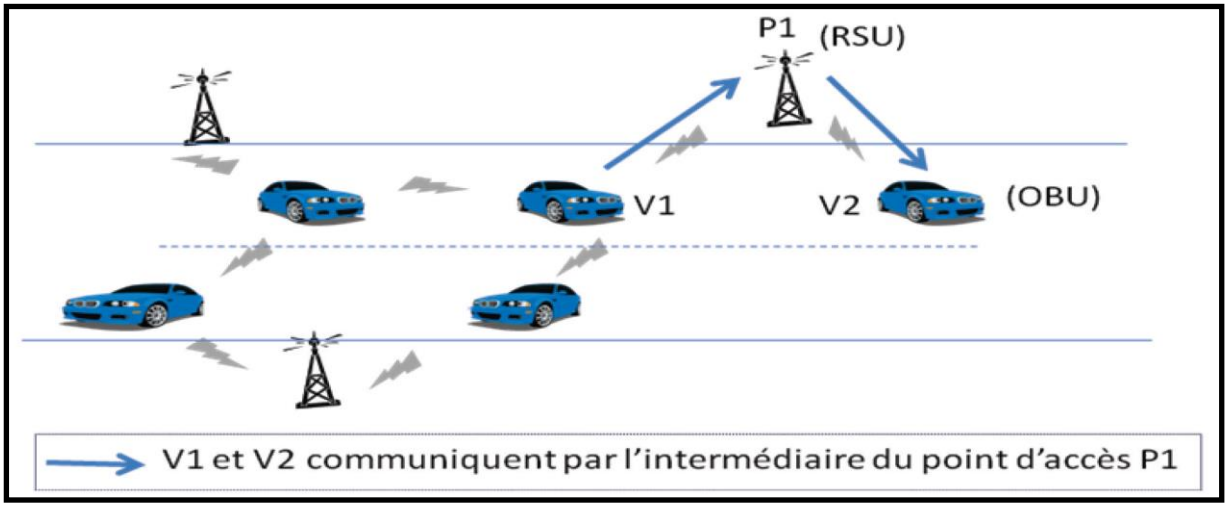


Figure 6 - Mode de communication Véhicule à Infrastructure

c) Le mode de communication hybride

Ce type de communication est une combinaison des deux modes de communications précédentes V2V et V2I, et comme les portées des infrastructures étant limitées alors que l'utilisation des véhicules comme relais permet d'étendre cette distance et d'éviter la multiplication des stations de base à chaque coin de la route et cela conduit à une communication hybride très intéressante et économique.

I.3.4 Les caractéristiques des réseaux VANET

De nombreux objectifs de conceptions différentes et parfois concurrentes doivent être pris en compte pour les VANETs pour assurer leur succès commercial. Lorsqu'un véhicule est équipé de la technologie IEEE82.11p (Wireless Access for Vehicular Environment : WAVE), il forme un réseau hautement dynamique puisque cette technologie permet d'utiliser le concept de multicanaux afin d'assurer les communications pour des applications de sécurité et pour d'autres services.

Bien que certaines des caractéristiques des VANETs ressemblent aux caractéristiques des MANETs [9] [10], mais il existe des caractéristiques spécifiques pour les VANETs qui peuvent être classées comme suit :

a) Topologie hautement dynamique

La vitesse élevée des véhicules ainsi que la disponibilité de choix de chemins multiples caractérisent la topologie dynamique des VANETs.

b) Réseau déconnecté fréquemment

La vitesse élevée des véhicules définit d'une part la topologie dynamique alors que d'autre part elle provoque des déconnexions fréquentes.

c) Mobilité de la modélisation et de la prévention

La prédiction de la position du véhicule et de ses mouvements est très difficile. Par ailleurs, la modélisation de la mobilité et la prédiction dans les VANETs sont basées sur la disponibilité des modèles de feuille de route déjà prédéfinis. La vitesse des véhicules est considérée comme une métrique importante pour une conception d'un réseau efficace.

d) Environnement de communication

Le modèle de mobilité peut avoir différentes caractéristiques selon l'architecture routière, les autoroutes ou les environnements urbains. A cet effet, la communication dans ces situations doit être prise avec soin.

e) Contrainte de délai difficile

Au moment de l'urgence, la remise des messages en fonction du temps devient un problème critique. Par conséquent, gérer de telles situations devient primordial que se contenter au taux de données élevés.

f) Interaction avec les capteurs embarqués

Les capteurs peuvent lire les données relatives à la vitesse du véhicule, direction et peuvent communiquer avec le centre de données. Ainsi, les capteurs peuvent être aussi utilisés dans la formation de liens et dans les protocoles de routage.

g) Batterie et stockage illimités

Les nœuds dans les VANET ne souffrent pas d'alimentation et de limitation de stockage comme dans les réseaux de capteurs, ainsi le cycle de service n'est pas aussi pertinent que dans les réseaux de capteurs.

I.3.5 Domaines d'application des réseaux VANETs

Les unités de bord de routes (RSU : Road Side Unit) peuvent être considérées comme des points d'accès ou des routeurs ou même des points tampons qui peuvent stocker des données et les fournir au besoin aux véhicules demandeurs [11]. Toutes les données stockées sur les RSU peuvent être téléchargées par les véhicules. En tant qu'applications de voiture vers le trafic

automobile, les applications vers l'infrastructure, les applications de la voiture vers la maison et les applications au profit du routage.

Par ailleurs, une classification des applications pourra être effectuée selon les modes de communication soit V2V ou V2I. Nous organisons les applications liées aux réseaux VANETs dans les classes suivantes :

- Orientée vers la sécurité
- Orientée commercialement
- Orientée vers la commodité
- Applications productives

a) Application de sécurité

Les applications de sécurité peuvent être classées comme suite :

- Traffic en temps réel : Les données de trafic en temps réel peuvent être stockées dans les RSUs pour qu'elles soient disponibles aux véhicules. Cela peut jouer un rôle important dans la résolution des problèmes tels que les embouteillages, les alertes d'urgence telles que les accidents.
- Transfert de messages coopératifs : Un véhicule échangera des messages avec les RSUs et coopérera pour aider d'autres véhicules. Bien que la fiabilité et la latence soient très préoccupantes, cela peut automatiser des problèmes comme le freinage d'urgence pour éviter d'éventuels accidents.
- Notification post-crash : Un véhicule impliqué dans un accident diffusera des messages d'avertissement concernant sa position pour les véhicules en aval afin que ces derniers puissent prendre des décisions ainsi que pour la patrouille d'autoroute pour le soutien de remorquage, comme le montre la figure 7.

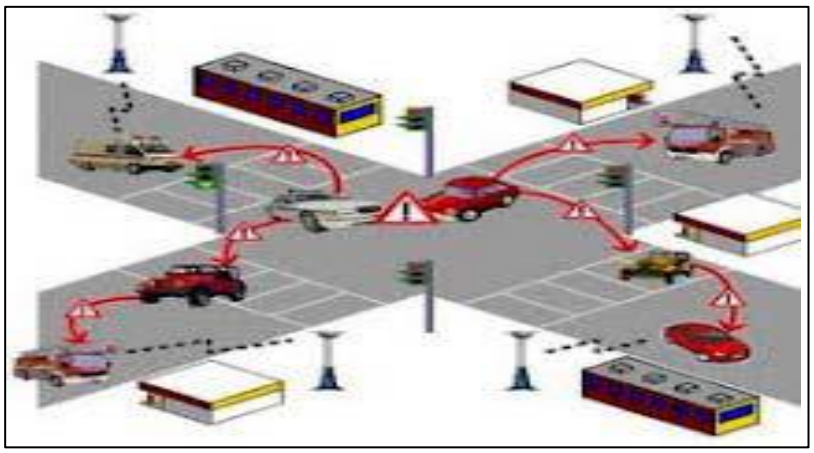


Figure 7 - Emergency situation notification

Rapport-gratuit.com
LE NUMERO 1 MONDIAL DU MÉMOIRES

- Notification de contrôle des dangers de la route : Les véhicules déclarent à d'autres véhicules des informations concernant l'état des routes telles que le glissement de terrain, l'existence d'un virage dangereux, la descente soudaine, etc.
- Avertissement de collision coopérative : Alerte aux conducteurs de l'existence d'un accident sur la route.

b) Application commerciales

Les applications commerciales fourniront aux conducteurs le divertissement et les services en tant qu'administrateur sur le web, en streaming audio et vidéo. Les applications commerciales peuvent être classées comme suit :

- Personnalisation/diagnostic de véhicule à distance : Il permet de télécharger des paramètres de véhicule personnalisés ou de télécharger des diagnostics de véhicules à partir d'une infrastructure.
- Accès à Internet : Les véhicules peuvent accéder à Internet via les RSUs si ces dernières fonctionnent comme routeurs.
- Téléchargement de la carte numérique : Les cartes routières des régions peuvent être téléchargées par les conducteurs selon l'exigence avant d'entrer dans une nouvelle zone pour le guidage des conducteurs. En outre, "Content Map Database Download" agit comme un portail pour obtenir des informations actualisées sur l'état des routes des régions en question.
- Publicité à valeur ajoutée : Spécialement pour les fournisseurs de services, qui souhaitent attirer les clients dans leurs magasins. Les annonces comme les pompes à essence, les restaurants routiers pour annoncer leurs services aux conducteurs dans la gamme de communication. Cette application peut être disponible même en absence d'Internet.

c) Applications de commodité

La solution de commodité concerne principalement la gestion du trafic dans le but d'améliorer l'efficacité du trafic en augmentant le degré de commodité des conducteurs. Les applications de commodité peuvent être classées comme suit :

- Routes : La planification de l'itinéraire et du voyage peut être faite en cas de congestion routière.
- Systèmes de collecte de péage électronique : Le paiement du péage peut se faire par voie électronique au moyen d'un point de collecte de péage. Un point de collecte de péage doit en mesure de lire l'OBU du véhicule. Les OBU fonctionnent en utilisant un GPS et l'odomètre et permettent aux techniciens à bord des routes de déterminer dans quelle mesure les véhicules ont voyagé en référence à une carte numérique et à un GSM pour autoriser le paiement du péage via un lien sans fil.

Rapport-Gratuit.com

- Disponibilité du stationnement : Les notifications concernant la disponibilité du stationnement dans les villes métropolitaines permettent de trouver la disponibilité des créneaux horaires dans les parkings dans une certaine zone géographique.
- Prévision active : Elle anticipe la prochaine publication de la route, qui devait optimiser l'utilisation du carburant en ajustant la vitesse de croisière avant de commencer une descente ou une montée.

d) Applications productives

Nous l'appelons intentionnellement comme productif, car ces applications sont additionnelles aux applications susmentionnées. Les applications productives peuvent être classées comme suit :

- Avantages environnementaux : Le programme de recherche AERIS consiste à générer et à acquérir des données de transport en temps réel pertinentes sur le plan environnemental et à utiliser ces données pour créer des informations pouvant être mises en évidence pour soutenir et faciliter les choix de transport par les utilisateurs et les opérateurs du système de transport. Dans le cadre d'une approche multimodale, le programme AERIS fonctionnera en collaboration avec l'effort de recherche de communication en mode V2V pour mieux définir la manière dont les données et les applications des véhicules connectés pourraient contribuer à atténuer certains impacts environnementaux négatifs.
- Le temps d'utilisation : Si un voyageur télécharge son courrier électronique, il peut transformer le trafic de bourrage en une tâche productive en consultant les informations retournées par le système embarqué implanté sur son véhicule et connaitre aussi si le trafic est bloqué en aval. On peut naviguer sur Internet quand quelqu'un attend en véhicule un parent ou un ami.

I.3.6 La sécurité dans les réseaux VANETs

La sécurité des réseaux sans fil, comme les réseaux filaires, vise à garantir essentiellement la confidentialité, l'intégrité et la disponibilité des services. C'est une tâche difficile, tout particulièrement dans un contexte de connectivité croissante, ce qui est le cas des réseaux ad hoc mobiles. Pour améliorer la sécurité des réseaux en général, il faut mettre en place des mécanismes de sécurité spécifiques à chaque réseau.

a) Caractéristique de la sécurité

Lors de l'analyse de la nature des communications dans les réseaux ad hoc, des propriétés spécifiques liées à la sécurité et la confidentialité doivent être prises en compte pour la conception des protocoles de communications, à savoir :

- Un support de transmission partagé : Comme avec tout système de communication sans fil, l'utilisation des ondes radio permet aux attaquants d'intercepter facilement les messages échangés ou bien d'injecter de faux messages dans le réseau.

- Les communications multi-sauts : Dans les réseaux sans fil mobiles en général et spécialement dans les réseaux VANETs, il faut avoir des communications sans fil sur une très grande portée, afin de pouvoir communiquer avec certaines entités du réseau éloignées. Pour cette raison, il est nécessaire d'utiliser des communications multi-sauts. Cependant, cela a toujours des conséquences négatives sur le bon fonctionnement des réseaux car certaines entités malveillantes exploitent cette caractéristique pour mettre en péril le réseau, soit en altérant les communications ou bien en refusant la retransmission des messages.
- Diffusion de l'information sur la position géographique : Avec certains protocoles dans les réseaux ad-hoc mobiles, les nœuds envoient périodiquement des messages indiquant leurs positions courantes ou d'autres données. Par conséquent, les attaquants peuvent créer un profil sur les trajectoires des nœuds.
- Les opérations autonomes : Les entités sont autonomes pour envoyer des messages dans les réseaux VANETs, ce qui donne la possibilité aux entités malveillantes d'envoyer à leur tour, des informations erronées ou falsifiées, pour nuire considérablement les autre entités ou causer le dysfonctionnement du réseau.

b) Menaces sur la sécurité

Lorsqu'on aborde le problème de la sécurité dans les réseaux VANETs particulièrement on vise certains objectifs [12]. En effet, dans les réseaux VANETs, une application ou un protocole de sécurité selon ses fonctionnalités, devrait assurer une ou plusieurs des exigences suivantes :

- L'authentification : Cet objectif de sécurité permet aux membres du réseau de s'assurer de la bonne identité des membres avec lesquels il communiquent.
- La non-répudiation : Cet objectif permet d'assurer qu'aucun émetteur ne peut nier d'être l'origine du message. La non-répudiation est indispensable dans toutes communications sensibles.
- La confidentialité : Ce troisième objectif garantit que seules les parties autorisées peuvent accéder aux données transmises à travers le réseau.
- L'intégrité : Cet objectif de sécurité permet d'assurer que les données échangées n'ont pas subi une altération volontaire ou accidentelle. Donc, il permet aux destinataires de détecter les manipulations de données effectuées par les entités non autorisées et rejeter les paquets correspondants.
- La disponibilité : Ce dernier objectif vise à garantir aux entités autorisées d'accéder aux ressources du réseau avec une qualité de service adéquate.

c) Mécanismes de base de la sécurité

Il existe des mécanismes importants qui permettent un certain niveau de sécurité dans les réseaux. On va citer quelques-uns :

Rapport-gratuit.com
LE NUMERO 1 MONDIAL DU MÉMOIRES

- La cryptographie : C'est une technique utilisée pour protéger les données transmises. Elle utilise des clés, des codes pour crypter le contenu à l'aide d'un algorithme de chiffrement. Il existe la cryptographie symétrique et asymétrique.
- Le hachage : Une fonction de hachage cryptographique est une fonction qui permet d'associer à une donnée de taille arbitraire une image de taille fixe et dont une propriété essentielle est qu'elle est pratiquement impossible à inverser. Pour cette raison, on dit qu'elle est à sens unique.
- La signature numérique : Parfois appelée signature électronique est un mécanisme permettant de garantir l'intégrité d'un document électronique et d'en authentifier l'auteur, par analogie avec la signature manuscrite d'un document papier.
- Les certificats : Parmi les résultats des algorithmes de la cryptographie, on trouve les certificats, qui permettent d'augmenter le degré de la sécurité dans les réseaux VANETs. Chaque véhicule possède un seul certificat à long terme [13], qui contient l'identité et les caractéristiques du véhicule. Il se charge principalement de renouveler les certificats à court terme. Ainsi, le véhicule possède donc plusieurs certificats à court terme, qui contiennent un identifiant virtuel et des pseudonymes de communication.
- Les certificats doivent permettre la préservation de la vie privée et l'anonymat du véhicule.

I.4 Norme et standard de communication

Pour mettre en place la communication entre les différentes entités dans les réseaux véhiculaires sans fil, ASTM (American Society for Testing and Materials) a adopté en 2002 une norme de communication DSRC (Dedicated Short Range Communication) [8] dont la couche physique est basée sur la norme IEEE802.11a.

En 2003, l'IEEE s'inspirant des travaux de l'ASTM, a étendu sa famille de standard 802.11 en y ajoutant le 802.11p [14] [8].

Dans cette section, nous allons décrire brièvement la norme et le standard de communication utilisé dans les réseaux véhiculaires.

I.4.1 DSRC

Les réseaux véhiculaires permette d'établir des communications entre véhicules dites IVC (Inter-Vehicule Communication) d'une part et entre véhicules et infrastructure dite RVC (Rode to Vehicule Communication) d'autre part. DSRC regroupe un ensemble de technologies dédiées aux communications véhiculaires. Dans le système DSRC, chaque véhicule embarque un terminal de communication appelé OBU (On Bord Unit) tandis que les terminaux fixes disposés le long des routes et constituant l'infrastructure sont appelés RSU (Road Side Unit). Ainsi, au lieu de recourir à un dispositif spécifique pour chaque type d'application, on utilise

les OBU et les RSU qui constituent le point d'entrée pour tout type d'application déployée dans les réseaux véhiculaires.

Le standard DSRC sous-tend une technologie de communication radio plus connue sous la norme IEEE 802.11p ou WAVE (Wireless Access for Vehicular Environment). Cette technologie radio offre des portées de transmission pouvant aller jusqu'à 1000 mètres. Elle en outre est définie dans la bande de fréquence des 5.9 GHz sur une largeur de bande totale de 75 MHz (5.850 GHz – 5.925 GHz).

I.4.2 IEEE 802.11 p

Le standard IEEE 802.11p utilise le concept de multicanaux dans le but d'assurer les communications liées aux applications de sécurité et autres services de transport intelligent [8] [15]. Ce standard dérive de la couche physique du standard 802.11a, et est adapté au fonctionnement à faible charge de spectre DSRC.

IEEE 802.11p offre un débit compris entre 6 et 27 Mb/s sur une distance de 1000 m et avec une modulation de type OFDM (Orthogonal Frequency Division Multiplexing). Aussi, la couche MAC du 802.11p reprend le principe du CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) développé dans le protocole MAC d'IEEE 802.11 afin de gérer la qualité de service et le support du protocole de marquage de priorité d'accès [8] [15].

I.4.3 WAVE

Le groupe de travail IEEE a repris ces travaux pour définir un nouveau standard dédié aux communications inter-véhicules, nommé WAVE et aussi connu sous le nom de IEEE 802.11p [1]. Cette norme utilise le concept de multicanaux afin d'assurer les communications pour les applications de sécurité et les autres services des STI.

a) La couche physique du WAVE

La couche physique de WAVE est dérivée d'IEEE 802.11a. Elle est capable d'offrir un débit compris entre 6 et 27 Mb/s sur une distance de 1000 m et avec une modulation de type OFDM. Cette couche physique s'appuie sur 7 canaux de communication d'une longueur de 10 MHz, chacun se trouvant dans la zone des 5.9 GHz comme montre [8].

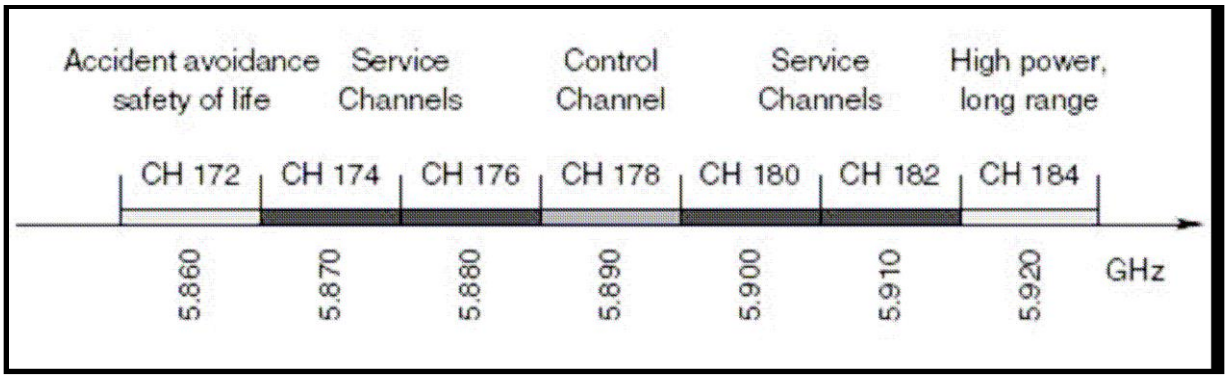


Figure 8 - Les canaux disponibles pour l'IEEE 802.11p [8]

b) La couche MAC du WAVE

La couche MAC du protocole WAVE est identique à celle dans le protocole 802.11e dont l'extension concerne la qualité de service.

Les messages sont rangés en 4 classes d'accès différentes (AC : Access Classes) et chacune de ces classes a sa propre priorité : AC_0 ayant la priorité la plus basse et AC_3 la plus élevée. De plus chacune de ces classes disposent d'une file d'attente. Ainsi, un paquet arrivant dans l'une de ses files d'attente ne sera pas envoyé immédiatement, il devra quoi qu'il arrive attendre un temps minimum dans cette file. Ce temps étant fixe selon les paramètres de contention.

I.5 Les avantages et les inconvénients des réseaux VANETs

I.5.1 Les avantages

a) Topologie dynamique

Vue le nombre important des nœuds qui augmente d'une façon exponentielle et qui se déplace avec une grande vitesse ceci va influencer sur la topologie du réseau. Cette caractéristique permet de garantir et d'assurer l'activité du réseau.

b) Echange entre des nœuds hétérogène

Bien que les nœuds sont de nature différente (marque, capacité de traitement, composants, etc.) les concepteurs ont conçu un protocole qui assure le bon échange des informations

c) Propagation par trajet multiple

Les messages échangés par un véhicule sont reçus par tous les autres véhicules qui se trouvent dans la zone de couverture de l'émetteur.

d) Relais d'information

Deux véhicules distants peuvent partager des informations à l'aide des nœuds intermédiaires.

I.5.2 Les inconvénients

a) Canal radio partagé et limité

Un canal radio à fréquence statique est partagé entre tous les nœuds du réseau ce qui limitera le flux de données et la bande passante surtout dans les endroits denses.

b) Les interférences

Un réseau véhiculaire utilise les transmissions radio pour l'échange d'information ce qui rend les communications exposées aux interférences. Ces interférence font augmenter le taux d'erreurs de transmission, et rendent les messages incompréhensibles par le récepteur.

I.6 Conclusion

Dans ce chapitre, nous avons présenté les réseaux véhiculaires VANETs qui sont des réseaux de communication entre véhicules intelligents, ensuite nous avons exposé quelques caractéristiques de ce type de réseaux, leurs domaines d'applications et les mécanismes de sécurité pour garantir la confidentialité, l'intégrité et la disponibilité des services par ces derniers. Par la suite, nous avons cité les modes de communications V2I et V2V qui permettent d'améliorer d'une part la sécurité routière grâce aux messages échangés entre les véhicules et de rendre d'autre part les routes plus agréables grâce à la diversité des services offerts. Enfin nous avons conclu par les avantages et les contraintes des VANETs.

Toutes les illustrations présentées dans ce chapitre nous permettent de tirer profit des avantages des réseaux VANETs pour un routage efficace dans ce type de réseaux.

Dans le chapitre suivant nous allons étudier le routage dans les réseaux véhiculaires (VANETs) et nous présentons les protocoles de routage les plus répandus.

Chapitre II

Le routage dans les réseaux VANETs

Chapitre II
Le routage dans les réseaux VANETs

II.1 Introduction

Le routage joue un rôle très important dans les réseaux VANETs puisque tous les services supportés, unicast ou multicast, se basent sur des communications multi-sauts pour l'acheminement des données. Les communications unicast sont généralement utilisées dans les applications de confort telles que le transfert de fichiers et les jeux alors que Les communications multicast sont utilisées dans les applications de sécurité et de gestion de trafic telles que l'avertissement de collision et les alertes. Pour réaliser les échanges, les protocoles de routage utilisent des informations locales, sur le voisinage immédiat, ou globales, concernant tout le réseau, afin de déterminer les nœuds relais qui participent à l'acheminement des données. Ces informations sont obtenues par des échanges de paquets de contrôle entre les nœuds. La fréquence des échanges et les informations spécifiées dans les paquets diffèrent d'un protocole à l'autre tout comme les mécanismes utilisés pour déterminer les nœuds relais.

Dans les réseaux VANETs, le routage pose des défis pour de nombreux chercheurs. Alors pour que les véhicules puissent communiquer entre eux, nous devons définir un protocole de routage efficace et fiable qui est à la mesure de remonter une information d'un véhicule à un autre.

Dans ce chapitre, nous présentons les différents protocoles de routage utilisés dans les réseaux véhiculaires, leurs objectifs ainsi que leurs principes. Finalement, nous terminons par une conclusion dans laquelle nous récapitulons le résultat de cette étude.

II. 2 Objectifs du routage dans les réseaux sans fil

L'objectif du routage dans les réseaux VANETs est d'améliorer la sécurité routière, les conditions de circulation et d'apporter aux conducteurs et aux passagers quelques applications publicitaires ou de divertissements. Pour cela, il est important de faire circuler l'information de la manière la plus efficace possible entre les différents véhicules et de déterminer une route respectant certaines contraintes, pour établir une connexion entre l'émetteur et le récepteur. Le but d'un algorithme de routage est de permettre le calcul de route entre la source et la destination au sens de certains critères, et la diffusion des informations nécessaires à ce calcul.

II.3 Routage dans les MANETs

Les réseaux ad-hoc mobiles (MANETs) sont des réseaux sans infrastructure fixe, composés d'entités mobiles, appelées nœuds. Ces nœuds communiquent entre eux directement

sans l'intervention de points d'accès stationnaires si ils sont au voisinage et via un schéma de routage multi-saut si ils sont éloignés. Dans les années 2000, les réseaux ad-hoc mobiles ont été déployés en particulier dans les environnements fortement dynamiques tels que les réseaux inter-véhicules.

Dans les réseaux MANETs, tous les nœuds coopèrent pour assurer le service du routage. L'approche la plus intuitive dans la conception des protocoles de routage consiste en l'adaptation des protocoles de routage traditionnels (vecteur de distance ou à état de lien) au contexte des MANETs, ce qui a donné naissance à la classe des protocoles de routage dits "proactifs". D'autres protocoles de routage reposent sur des approches complètement novatrices. Elles consistent, par exemple à calculer les chemins à la demande, à exploiter les informations de géolocalisation ou à définir une topologie logique au-dessus de celle physique, etc, ces protocoles sont dits "réactifs". Évidemment, des combinaisons de différentes approches sont aussi envisageables, ce que génèrent des protocoles dits "hybrides"

II.4 Routage dans les réseaux VANETs

Un réseau ad-hoc de véhicules (VANET), est une sous-classe de réseaux mobiles ad-hoc (MANETs). Il est considéré comme une approche prometteuse pour le système de transport intelligent (STI). La conception des protocoles de routage dans les VANETs est un problème important et nécessaire pour supporter les STI. La principale différence entre les VANETs et les MANETs est le modèle de mobilités spéciales et la topologie rapidement modifiable. Il n'est pas effectivement pratique d'appliquer les protocoles de routage existants des MANET pour les réseaux VANETs.

Le routage est basé sur des communications multi-sauts, cela rend la communication entre deux nœuds ou plusieurs possible même s'ils ne sont pas dans la même portée de transmission radio. La stratégie de routage doit prendre en considération les différentes caractéristiques des réseaux VANETs (changements de topologie, la mobilité forte, la capacité limitée des liaisons radio …) pour assurer une stratégie permettant de garantir une connectivité du réseau permanente.

II.5 La différence entre les MANETs et les VANETs

Le tableau 1 illustre la différence entre les réseaux MANETs et les réseaux VANETs en mettant le point sur des caractéristiques essentielles.

Tableau 1 : Comparaison entre les MANETs et les VANETs [2]

MANETs	VANETs
1. Réseau sans fil multi-sauts qui manque d'infrastructure, décentralisé et auto-organisé.	1. Un cas particulier des réseaux MANETs qui satisfait toutes ses caractéristiques et exigences.
2. Applications identiques que celles permises par internet.	2. Des applications en relation avec la sécurité routière, l'efficacité du transport et les applications d'information ou de divertissement.
3. Les nœuds sont supposés avoir une mobilité modérée.	3. Un grand degré de mobilité des nœuds.
4. Le modèle de mobilité le plus utilisé est le RWP (Random Way Point).	4. Des simulations détaillées du trafic véhiculaires sont utilisées.
5. Plusieurs protocoles pour l'efficacité énergétique.	5. Pas de problème concernant l'efficacité énergétique.

II.6 Classification des protocoles de routage dans les réseaux VANETs

Afin de présenter les principaux protocoles de routage dans les VANETs, nous avons choisi de commencer par faire une classification des différents protocoles existants dans la littérature. Généralement, les protocoles de routage peuvent être classés en deux grandes familles [16] : les protocoles géographiques basés sur la position et les protocoles basés sur la topologie qui sont divisés en protocoles proactifs, réactifs et hybrides. La figure 9 illustre cette classification.

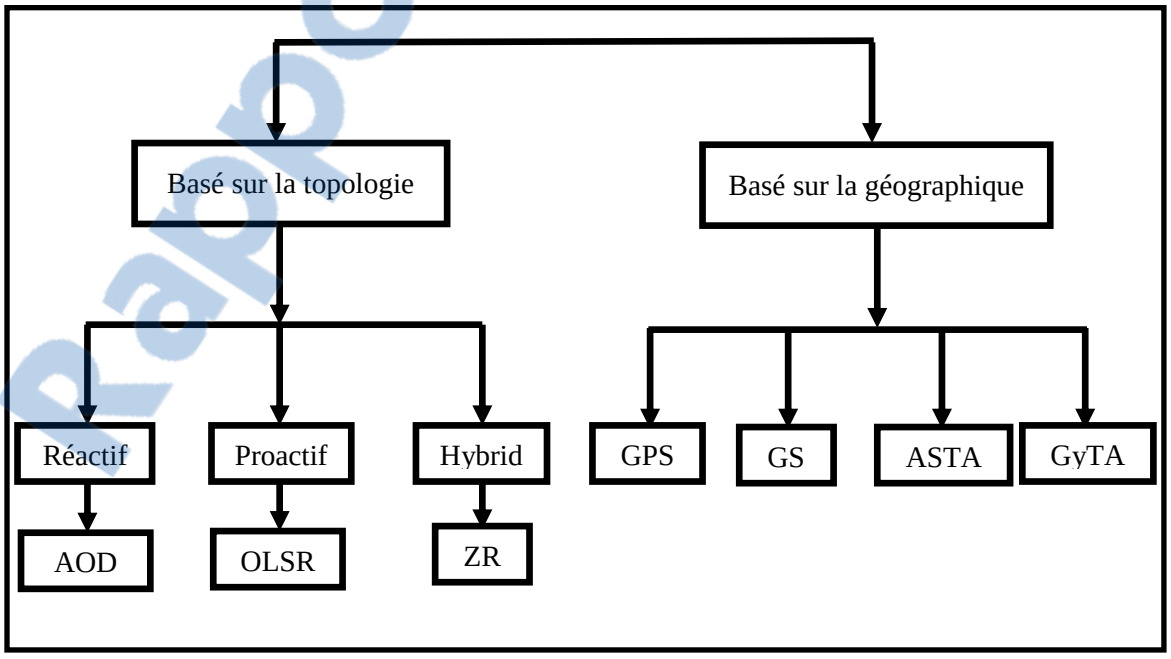


Figure 9 - Famille des protocoles de routage dans les VANET

II.6.1 Les protocoles de routage basé sur la topologie

a) Les protocoles réactifs

Dans les réseaux VANETs, les protocoles réactifs adoptent des algorithmes classiques tels que le routage par vecteur de distance. Les routes sont établies uniquement sur demande et seules les routes en cours d'utilisation sont maintenues. Dans ce cas, un délai supplémentaire est nécessaire au début de chaque session pour la recherche d'un chemin. Parmi les protocoles réactifs les plus répandus, nous citons AODV (Ad hoc On Demand Distance Vector), DSR (Dynamic Source Routing) et TORA (Temporally Ordered Routing Algorithm).

b) Les protocoles proactifs

Dans les protocoles proactifs [17], chaque nœud garde une image de la topologie de tout le réseau. Cette image est mise à jour, périodiquement ou à chaque modification de la topologie, par un échange de messages de contrôle. Les routes sont déterminées sur la base de cette image. Il existe plusieurs protocoles proactifs parmi lesquels nous citons OLSR (*Optimized Link State Routing),* et DSDV (*Destination-Sequenced Distance-Vector)*.

c) Les protocoles hybrides

Les protocoles hybrides combinent les deux idées, celle des protocoles proactifs et celle des protocoles réactifs. Ils utilisent un protocole proactif, pour connaitre le prochain voisin (par exemple le voisinage à deux ou trois sauts), ainsi ils disposent des routes immédiatement dans le voisinage. Au-delà de cette zone prédéfinie, le protocole hybride fait appel aux techniques réactives pour rechercher des routes. Avec ce découpage, le réseau est partagé en plusieurs zones et la recherche de routes en mode réactif peut être améliorée. A la réception d'une requête de recherche réactive, un nœud peut indiquer immédiatement si la destination est dans le voisinage ou non et par conséquent savoir s'il faut aiguiller la requête vers les autres zones sans déranger le reste de sa zone. Parmi les protocoles de routage hybride nous citons ZRP (*Zone Routing Protocol*).

II.6.2 Les protocoles de routage géographiques

Les protocoles de routage géographiques (ou basés sur la position) utilisent des coordonnées géographiques par exemple fournies par le GPS afin de trouver un chemin vers la destination [18]. Pour atteindre cet objectif, les coordonnées géographiques des nœuds sont incluses dans les tables de routage.

L'avantage majeur de ces protocoles par rapport aux protocoles précédents est qu'ils réduisent considérablement la signalisation (les paquets de contrôle), notamment dans les réseaux larges et dynamiques. Ils permettent aussi d'économiser l'énergie des nœuds, gagner la bande passante et le passage à l'échelle du réseau. En effet, ces protocoles n'ont pas besoin de tables de routage ce qui limite les paquets de contrôle pour la maintenance de la table. Ce

qu'ils ont besoin, c'est uniquement la localisation de la destination outre la possibilité que chaque nœud connaît sa propre localisation à tout moment. La localisation d'un nœud peut être obtenue en utilisant le système de positionnement global appelé GPS, attaché au nœud mobile ou un algorithme de localisation.

Il existe plusieurs protocoles de routage géographiques. Les plus connus sont: LAR (*Location Aided Routing)* [19], DREAM (*Distance Routing Effect Algorithm Mobility)* [20], GPSR (*Greedy Perimeter Stateless Routing)* [21].

II.7 Les principaux protocoles de routage dans les réseaux VANETs

II.7.1 AODV (Ad-hoc On Demand Distance Vector)

AODV est un protocole [22] de routage réactif qui établit une route lorsqu'un nœud nécessite l'envoi de paquet de données. Il a la capacité d'unicast et routage multicast. Il utilise un numéro de séquence de destination (Destination Sequence Number) qui le distingue des autres protocoles de routage à la demande.

a) Les avantages

- Un chemin à jour vers la destination en raison de l'utilisation du numéro de séquence de destination.
- Il réduit les exigences de mémoire excessives et l'itinéraire redondant.
- Réponses AODV à l'échec de la liaison dans le réseau.
- Il peut être appliqué aux réseaux ad-hoc à grand échelle.

b) Les inconvénients

- Plus de temps est nécessaire pour la configuration de la connexion et l'initiale communication pour établir une route par rapport à d'autres approches.
- Pour un seul paquet de réponse d'itinéraire s'il y a une réponse d'itinéraire multiple les paquets entraîneront de lourds coûts de contrôle.
- En raison du balisage périodique, il consomme de la bande passante supplémentaire.

II.7.2 GSR (Global State Routing)

GSR [23] a été proposé pour les réseaux ad-hoc de véhicules dans les environnements urbains qui constituent la combinaison de routage avec connaissance topologique. GSR utilise gourmand transmettant le chemin le plus court présélectionné et ce chemin est calculé en utilisant l'algorithme de Dijkstra.

Rapport-gratuit.com
LE NUMERO 1 MONDIAL DU MÉMOIRES

a) Les avantages

- Le taux de livraison des paquets de GSR est meilleur qu'AODV.
- GSR est évolutif comparativement à AODV.

b) Les inconvénients

- Ce protocole néglige la situation comme un réseau restreint où il n'y a pas assez de nœuds pour le transfert de paquets.
- GSR affiche un overhead plus élevé que GyTAR (Greedy Traffic Aware Routing) [24,25] en raison d'utiliser les messages hello comme messages de contrôle

II.7.3 A-STAR (Anchor-based Street and Traffic Aware Routing)

A-STAR [26] est un protocole de routage basé sur la position qui est spécialement conçu pour les scénarios de veille pour les systèmes de communication entre véhicules. Il assure une connectivité élevée dans la livraison de paquets en utilisant la circulation des véhicules. Les informations des bus de la ville pour une connexion de bout en bout.

a) Les avantages

- Dans une densité de trafic faible, A-STAR assure une recherche de connexion.
- Par rapport à l'approche gourmande de GSR et le mode périmétrique du GPSR, A-STAR utilise une nouvelle reprise locale, une stratégie qui convient mieux à l'environnement de la ville.
- La sélection de l'option A-STAR assure une connectivité élevée, bien que le taux de livraison des paquets soit inférieur à GSR et GPSR.

b) Les inconvénients

- Le taux de livraison des paquets d'A-STAR est inférieur à ceux de GSR et GPSR
- Pour trouver un chemin de la source vers la destination, il utilise des paramètres statiques basés sur les itinéraires de bus de la ville qui causent un problème sur une partie des rues.

II.7.4 GPSR (Greedy Perimeter Stateess Routing)

GPSR [21] sélectionne un nœud qui est le plus proche à la destination finale en utilisant la balise. Il utilise un algorithme glouton de transfert en cas d'échec et utilise aussi un renvoi périmétrique pour sélectionner un nœud par lequel un paquet transite.

a) Les avantages

- Pour transférer le paquet, un nœud doit se souvenir d'un seul saut voisinage.
- Les décisions sur les paquets sont effectuées dynamiquement.

b) Les inconvénients

- Pour les caractéristiques de mobilité élevée du nœud, des informations de la position des voisins sont souvent contenues dans la table voisine des nœuds d'envoi.
- Bien que le nœud de destination transfère ses informations dans l'en-tête des paquets au nœud intermédiaire ces informations ne sont jamais mises à jour.

II.7.5 GyTAR (Greedy Traffic Aware Routing)

GyTAR [24,25] donne un nouveau concept de protocole de routage basé sur l'intersection qui vise à réduire les retards de bout en bout des messages de contrôle.

a) Les avantages

- Pour la topologie à haute mobilité, qui change rapidement souvent une fragmentation du réseau est effectuée par GyTAR.
- Performance montre que le débit, le retard et l'acheminement de l'overhead sont meilleurs que ceux de GSR.

b) Les inconvénients

- GyTAR dépend des unités routières (RSUs) parce qu'il suppose que le nombre de véhicules dans la route sera donné à partir des unités à bord de route.
- GyTAR ne peut pas éviter son vide.

II.8 Conclusion

Dans les réseaux ad-hoc, tout équipement peut être impliqué pour acheminer des données qui ne le concerne pas et chaque nœud participe à une stratégie de routage afin que tous les nœuds puissent ensemble créer un réseau efficace. C'est pour cela que les protocoles de routage mis en œuvre dans les réseaux ad-hoc ont une importance cruciale et il est impensable de vouloir créer un routage statique dans un environnement mobile. A cet effet, les protocoles de routage doivent être très réactifs à la dynamique du réseau.

Ce chapitre a montré les différentes techniques utilisées par les protocoles de routage pour les rendre plus réactifs en consommant un minimum de bande passante. Ces protocoles sont divisés en deux catégories, les protocoles de routage proactifs qui tentent de maintenir à jour la représentation actuelle du réseau et les protocoles de routage réactifs qui déterminent une route uniquement en cas de besoin. Il existe aussi des protocoles de routage mélangeant les deux protocoles précédents, ce sont les protocoles de routage hybrides.

Ce chapitre a montré aussi qu'il existe de nombreux protocoles de routage pour les réseaux ad-hoc ayant chacun des avantages et des inconvénients, il n'existe pas de protocole meilleur que les autres mais certains sont adaptés que d'autre suivant les situations.

Dans le chapitre suivant, nous présentons les outils nécessaires qu'on a utilisés afin de préparer notre environnement de travail pour faire une amélioration et une évaluation du protocole de routage EGyTAR [27]. Et nous concluons par une discussion sur les résultats obtenus.

Chapitre III
Version améliorée du protocole EGyTAR

Chapitre III
Version améliorée du protocole EGyTAR

III.1 Introduction

La mise en œuvre dans des environnements réels et avec une topologie complexe est très difficile à réaliser. Pour cela des simulateurs réseaux ont été conçus pour faire des évaluations et des validations.

La simulation est l'implantation d'un modèle simplifié du système à l'aide d'un programme de simulation adéquat dans un environnement qui imite l'environnement réel. Cette démarche traduit le comportement du système à évaluer d'une manière réaliste. La simulation permet de tester et visualiser à moindre coût les résultats sous forme de graphe facile à analyser et à interpréter.

L'étude des performances d'un protocole de routage dédié aux réseaux véhiculaires sans fil, fait appel à deux types de simulateurs : le simulateur de trafic routier et le simulateur réseau. Le premier permet de générer la mobilité des véhicules sur une carte alors que le deuxième modélise le comportement de différentes entités du réseau.

Il y a plusieurs simulateurs réseau parmi lesquels nous citons NS-2 (Network Simulator 2) et son successeur NS3 (Network Simulator 3), COOJA (Contiki OS Java Simulator), SUMO (Simulation of Urban Mobility), OMNET++ (Operation and Maintenance New Equipment Training++) [28], etc.

Dans ce chapitre nous allons commencer tout d'abord par la description de quelques simulateurs et faire une comparaison entre eux, par la suite nous présentons notre environnement de travail et nous concluons par l'implémentation et l'évaluation du protocole de routage EGyTAR [27] et la version améliorée que nous avons proposée.

III.2 Environnement de simulation de notre application

Dans cette section, nous présentons les outils logiciels nécessaires pour implémenter et évaluer le protocole de routage EGyTAR et la version améliorée proposée.

III.2.1 Simulateur : OMNET++

a) Présentation du simulateur

OMNET++ est un simulateur d'évènements basé sur le langage C++, destiné principalement à simuler les protocoles conçus pour les réseaux et les systèmes distribués. Il est totalement

programmable, paramétrable et modulaire. C'est une application open-source et sous licence GNU.

OMNET++ est destiné avant tout à un usage académique et il est l'intermédiaire entre des logiciels de simulation comme NS, destiné principalement à la recherche et Opnet qui est une alternative commerciale d'OMNET++.

b) Architecture d'OMNET++

Le fonctionnement d'OMNET++ repose entièrement sur l'utilisation de modules structurés sous forme hiérarchique qui communiquent entre eux par le biais de messages. 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 composé 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 ».

Les messages sont transmis par le biais de portes (gates). Les portes sont les interfaces d'émission et de réception des modules et une connexion peut relier une porte d'entrée à une porte de sortie. 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 figure ci-dessous montre l'architecture d'OMNET++.

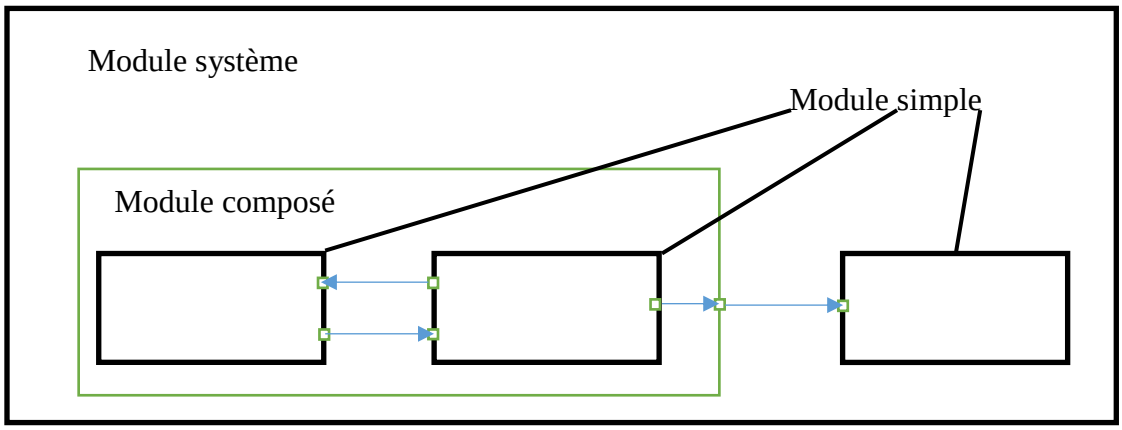


Figure 10 - Architecture OMNET++

c) Comparaison entre OMNET++ et d'autres simulateurs

Actuellement, il y a de nombreuses plateformes de simulation de réseaux disponibles sur le marché, qu'elles soient commerciales ou non. Nous faisons dans cette section une comparaison entre OMNET++ et les plus importantes solutions concurrentes.

Les outils de simulation réseaux considèrent qu'un réseau est un ensemble de nœuds connectés entre eux. Quelques outils, comme PARSEC (PARallel Simulation Environnement for Complex Systems) et C++Sim, ne fournissent pas de moyens explicites pour décrire des

topologies. Dans PARSEC, il faut programmer "entité pilote" qui initialisera le réseau en créant les nœuds nécessaires et en les interconnectant. Cette solution n'encourage pas la séparation entre topologies et fonctionnement. En outre, les possibilités de réutiliser des modèles existants sont peu nombreuses dans PARSEC. D'autres outils comme NS et CLASS ne gèrent pas la hiérarchie dans les réseaux, ce qui entraine moins de flexibilité dans l'architecture du modèle. Opnet, comme OMNET++, permet la gestion de la hiérarchie dans les modèles, mais il a tout de même quelques restrictions. La principale différence entre OMNET++ et Opnet est que les modèles Opnet utilisent uniquement des topologies fixes alors qu'OMNET++, avec l'éditeur graphique NED, permet de créer des topologies entièrement paramétrables. L'éditeur d'Opnet propose une librairie de modèles sous forme de fichiers binaires au format propriétaire.

Les logiciels de simulation sont souvent la source de longues phases de débogages. Il est souvent compliqué de s'assurer que la simulation lancée fonctionne correctement. Offrir des méthodes efficaces de débogage et de traçabilité et donc primordial. La traçabilité via des logs est disponible sur tous les logiciels. Un autre outil très utile est proposé par Opnet. Il s'agit du debugger en line de commande.

OMNET++ propose trois outils de débogage différents : une fenêtre "module output", un inspecteur et l'animation automatique. La fenêtre "module output" et l'inspecteur n'existent pas dans les autres outils de simulation. Cette absence s'explique souvent par le manque d'environnement d'exécution graphique. Malgré tout, l'aspect animation automatique est présent dans la plus part des outils. Certains d'entre eux, comme Opnet, propose même des animations personnalisables, ce qu'OMNET++ ne propose pas.

Le facteur déterminant le temps d'exécution de la simulation et le langage de programmation utilisé représentent les points forts du simulateur OMNET++. Les simulations sous OMNET++ peuvent être programmées en C ou en C++. C'est également le cas pour NS, Opnet. Ce sont ces langages qui fournissent les meilleurs temps d'exécution.

OMNET++ est totalement open-source mais certains logiciels commerciaux comme PARSEC ne mettent pas leurs sources à disposition des développeurs. L'accès au code source ne permet pas uniquement de modifier le moteur de simulation mais aide également au débogage des modèles de simulation.

d) BonnMotion

BonnMotion est un logiciel développé en Java qui permet de créer et analyser des scénarios de mobilité. Il est plus souvent utilisé comme outil pour l'étude de caractéristiques des réseaux ad hoc mobiles. Les scénarios peuvent également être exportés pour plusieurs simulateurs de réseau, tels que NS-2, NS-3, COOJA.

BonnMotion génère plusieurs types de scénarios parmi lesquels : ColumnMobility Model, Chain Model "ChainScenario", the Manhattan Grid model "ManhattanGrid", the Random Waypoint model "RandomWaypoint". Dans notre projet nous avons utilisé le type de scénario ManhattanGrid.

e) ManhattanGrid

Le modèle de mobilité de Manhattan émule la mobilité dans le secteur de ville avec les grilles reliées. Dans ce modèle, les nœuds ne se déplacent que sur les chemins précédents et les arguments -u et -v définissent le nombre de blocs entre les chemins.

III.2.2 Outils d'implémentation et d'évaluation

Dans ce qui suit nous présentons les outils matériels et logiciels nécessaire à la mise en place de l'application.

a) Environnement matériel

Notre projet a été réalisé en utilisant un ordinateur "HP Probook 450 G2" dont la configuration est décrite dans le tableau suivant :

Tableau 2: Environnement matériel

Processeur	Intel® Core™ i5-4210U CPU @ 1.70GHz
Mémoire vive	6 GB
Disque dure	1 To
Carte graphique	AMB Radéon R5 M255 (Lié) 2048 MB

b) Environnement logiciel

Dans le cadre de notre projet de fin d'étude nous avons opté pour le simulateur OMNET++ 5.0, ce choix est basé sur ces nombreux avantages et ces limitations minimes par rapport aux autres simulateurs.

L'avantage d'OMNET++ est sa facilité d'apprentissage, d'intégration de nouveaux modules et la modification de ceux déjà implémentés. Nous introduisons dans la suite l'architecture du simulateur OMNET++.

Le tableau ci-dessous montre l'environnement logiciel utilisé dans notre projet.

Tableau 3: Environnement logiciel

Système d'exploitation	Ubuntu 16.04 LTS
Type de système d'exploitation	64 bits
Librairie	INET 3.4.0

III.2.3 Implémentation et évaluation

a) Fonctionnement GyTAR

C'est un protocole de routage géographique basé sur la densité de trafic véhiculaire, conçu spécifiquement pour le routage dans les environnements urbains. L'idée principale de GyTAR est d'acheminer les paquets des données dans le réseau en prenant en considération la variation en

Rapport-Gratuit.com

temps réel du trafic véhiculaire. Pour faire simple, on peut diviser le module de routage de GyTAR en 3 modules principaux :

- **Mécanisme de sélection des intersections :**

Dans GyTAR [27], les intersections où les paquets doivent passer pour atteindre la destination sont choisies dynamiquement un par un afin de prendre en compte la variation en temps réel du trafic véhiculaire. Dans le cas de la sélection de l'intersection suivante, le nœud identifie les intersections candidates (les intersections de voisinage) par l'utilisation de la carte digitale, en suite il affect un coût à chaque intersection candidate. L'intersection qui a un coût maximal est choisie comme l'intersection suivante, la figure suivante montre un exemple de sélection des intersections.

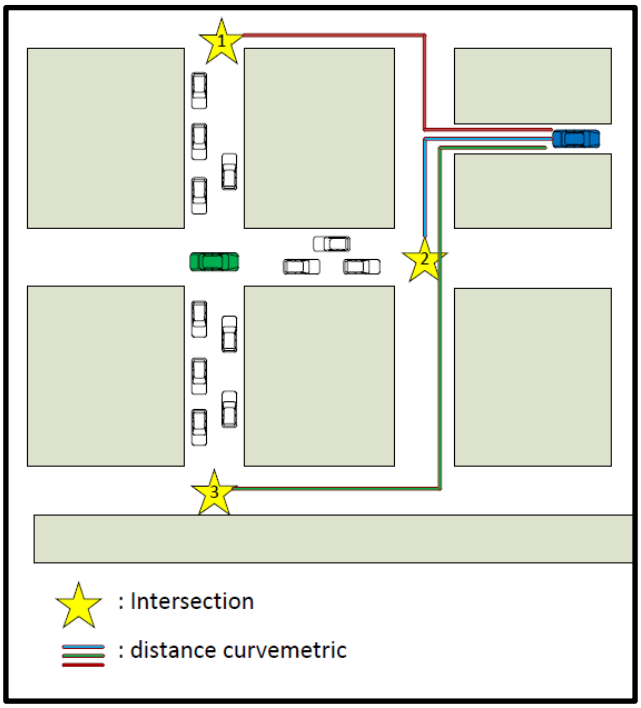


Figure 11 - Mécanisme de sélection des intersections

Le coût d'une intersection "j" est calculé par la formule suivante :

$$S(j) = \alpha f(T_j) + \beta g(D_i)$$

α, β: *facteurs de pondération, les poids associé à la distance et à la densité du trafic routier pour le calcul du score avec* $\alpha + \beta = 1$

$$f(T_j) = \frac{D_j}{D_i}$$

D_i : *distance curvemetric de l'intersection courante*

D_j : *distance curvemetric de l'intersection 'j'*

Rapport-gratuit.com
LE NUMERO 1 MONDIAL DU MÉMOIRES

$$g(D_j) = \min(\frac{N_{avg}}{N_{con}}, 1)$$

$$N_{avg} = \frac{N_v}{N_c}$$

N_v: *densité de trafic*, N_c: *nom*bre de cellules physiques

N_{con} : *nombre minimal de véhicules pour garantir la connectivité dans une cellule*

Le nœud relai a besoin des informations de trafic pour chaque intersection candidate pour calculer les coûts. Ces informations sont maintenues par les messages Cell Density Packet (CDP).

- **Cell Density Packet**

Dans GyTAR, chaque route est divisée par des cellules physiques de diamètre fixe (250m). Le véhicule le plus proche au centre de cellule est élu comme Group Leader GL, à la réception d'un message CDP, le GL compte le nombre de véhicules dans sa cellule et met à jour les informations de CDP et transmet ce message CDP vers le GL de la cellule suivante.

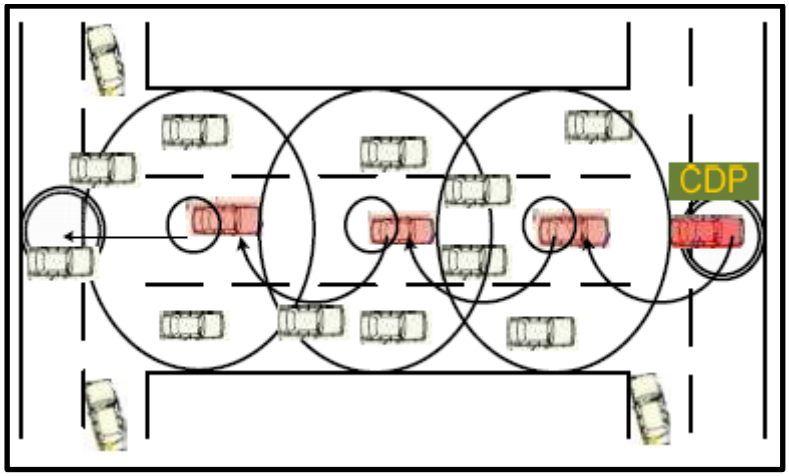


Figure 12 - Mécanisme de diffusion de message CDP

- **Le Routage entre deux intersections**

Une fois l'intersection suivante est fixée, GyTAR emploie la stratégie Improved Greedy Forwarding. Cette stratégie consiste de trouver un voisin plus proche à l'intersection suivante en utilisant les positions prédit à la base de la vitesse des nœuds.

b) Amélioration proposé : CDP périodique

Le protocole GyTAR est basé sur les sélections dynamiques des intersections en fonction de la densité de trafic véhiculaire. Ce mécanisme de sélection a besoin à chaque sélection les informations de trafic pour chaque intersection (fournies par les messages CDP). Par ailleurs, selon le fonctionnement de GyTAR, la diffusion des messages CDP se fait si et seulement si un véhicule entre dans une nouvelle route, si ce n'est pas le cas, on a aucune information sur l'intersection candidate donc le routage dans ce cas se fait sans en prendre en considération le trafic véhiculaire.

Rapport-gratuit.com
LE NUMERO 1 MONDIAL DU MÉMOIRES

Pour pallier cet inconvénient, Nous avons proposé un mécanisme de diffusion des messages CDP périodiquement.

- **CDP périodiques :**

Dans notre proposition on a gardé la même structure de division des routes en cellules physiques qui est utilisé dans GyTAR alors que le principe de diffusion des messages CDP se fait comme suite :

1) Chaque véhicule a un timer,
2) A chaque changement de cellule ou à la réception d'un message CDP le véhicule initialise son timer,
3) Une fois le timer dépasse une seconde, le véhicule qui se trouve au centre de cellule initialise un message CDP, calcule le nombre des véhicules, envoie le message CDP vers le GL de la cellule suivante et initialise le timer de son groupe.
4) A la réception d'un message CDP, le véhicule qui se trouve au voisinage de l'intersection garde ce message pendant une seconde.

a) <u>Structure de message CDP</u>

Cell Density Packet	
Road id	Destination Junction
connectivity	last_node

Figure 13 – Structure des messages CDP

b) Pseudo code de CDP périodique

```
v : véhicule
t :  timer
Cp : la première cellule
Cd : la dernière cellule
Début :
        Si ‘v’ est un membre de Cp ou Cd
           alors
              Si t>1 seconde et ‘v’ est le plus proche au centre de cellule
                 alors
                        -   Créer un nouveau message CDP
                        -   Compter le nombre de véhicules
                        -   last_node := la dernier véhicule dans la cellule
                        -   Calculer la connectivité moyenne de cellule par la formule.1
                        -   t :=0 /* initialisation de timer */
                        -   Mettre à jour les champs connectivité et last_node du message CDP par
                            les valeurs calculées
                        -   Transférer le message CDP vers le GL de la cellule suivante
               Fsi
        Fsi
Fin
```

c) La connectivité d'une cellule

1) La liaison entre deux nœuds

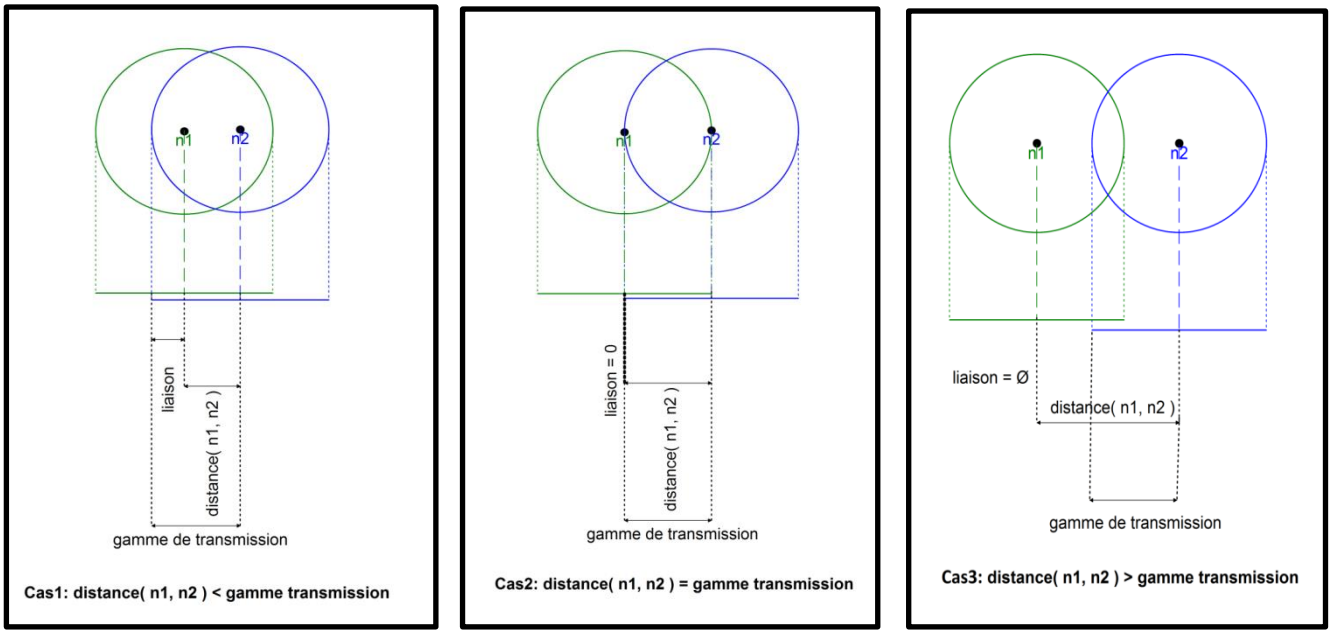


Figure 14: Evaluation de la liaison entre deux nœuds

$$Liaison(n_i, n_j) = \begin{cases} Range - Distance(n_i, n_j) & si\ Distance(n_i, n_j) < Range \\ 0 & si\ \ Distance(n_i, n_j)\ \geq Range \end{cases}$$

2) Moyenne **liaison**

$$Moyenne_{liaison} = \frac{\sum_{i=1}^{N-1}(\ liaison\ (n_i\ , n_{i+1}\ ))}{N-1}$$

N : nombre des nœuds (y a compris les deux extrémités de la route)

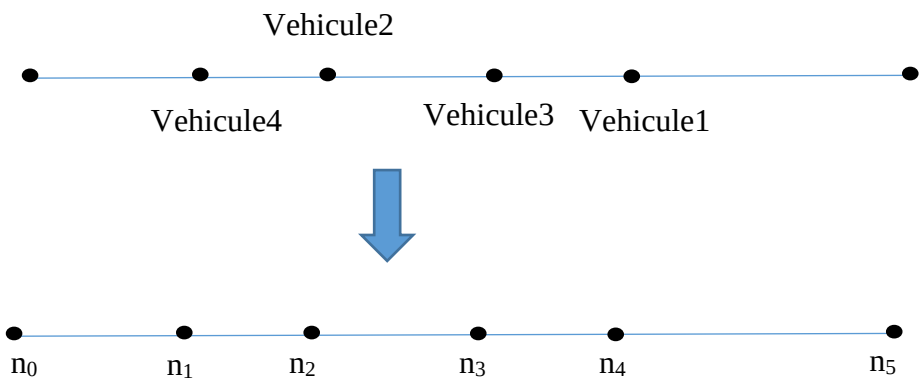
3) Connectivité

Pour calculer la connectivité d'une cellule :

n : est un tableau des positions de tous les véhicules dans la cellule.

Ordonner les nœuds par ordre croissant selon la distance entre n_i et la 1er extrémité de la cellule

Exemple :



$\boldsymbol{si}$ $\exists i \; tel \; que \; liaison(n_i, n_{i+1}) = 0$ alors connectivité = 0

$\boldsymbol{sinon}$ **Connectivité** $= \frac{\boldsymbol{Moyenne_{liaison}}}{\boldsymbol{range\ of\ transmission}}$

$$Moyenne_{liaison} = \frac{\sum_{i=1}^{N-1}\left(liaison\left(n_i, n_{i+1}\right)\right)}{N-1} = \frac{\sum_{i=1}^{N-1}\left(range - distance\left(n_i, n_{i+1}\right)\right)}{N-1}$$

$$= \frac{(N-1)range - \sum_{i=1}^{N-1}\left(distane\left(n_i, n_{i+1}\right)\right)}{N-1} = \frac{(N-1)range - L}{N-1}$$

$$= range - \frac{L}{N-1}$$

(La somme des distances (n_i, n_{i+1}) égale la longueur de la route 'L')

Donc $Moyenne_{liaison} = range - \frac{L}{N-1}$

d) Métriques d'évaluation

Nous donnons dans ce qui suit des définitions brèves à ces métriques :

- **Le taux d'utilisation CDP** : C'est le rapport entre le nombre d'utilisation de la densité du trafic dans la sélection de l'intersection suivante et le nombre total de sélection des intersections.
- **Le taux de paquets délivrés** : C'est le rapport entre le nombre de paquets émis par la source (les sources) et le nombre de paquets reçus par la destination (les destinations).
- **Le délai de bout en bout** : Représente l'intervalle de temps qui s'écoule entre la date d'envoi du paquet, par la source, et la date de réception de ce paquet par la destination.

III.2.4 Résultats et discussion

Nous présentons les résultats obtenus lors de la simulation en termes de taux de paquets délivrés, de délai de bout en bout et le taux d'utilisation CDP. Pour ces simulations les paramètres utilisés sont présentés dans le tableau suivant :

Tableau 4: Paramètres de simulation

Critères	Valeurs
Nombre des nœuds	100, 120, 140, 160, 180, 200
Modèle de mobilité	BonnMotion
Type de mouvement	ManhathanGrid
Topologie réseau	1500 m * 1500 m (16 intersections, 24 routes)
Temps de simulation	100 s
Taille des paquets	128 Ko
Taux de transmission	1 paquet/seconde
Temps de transmission	De 10 s jusqu'à 100 s
Vitesse	35 Km/h – 80 Km/h
Couche MAC	802.11p
Gamme de transmission	250 m

a) Taux de paquets délivrés

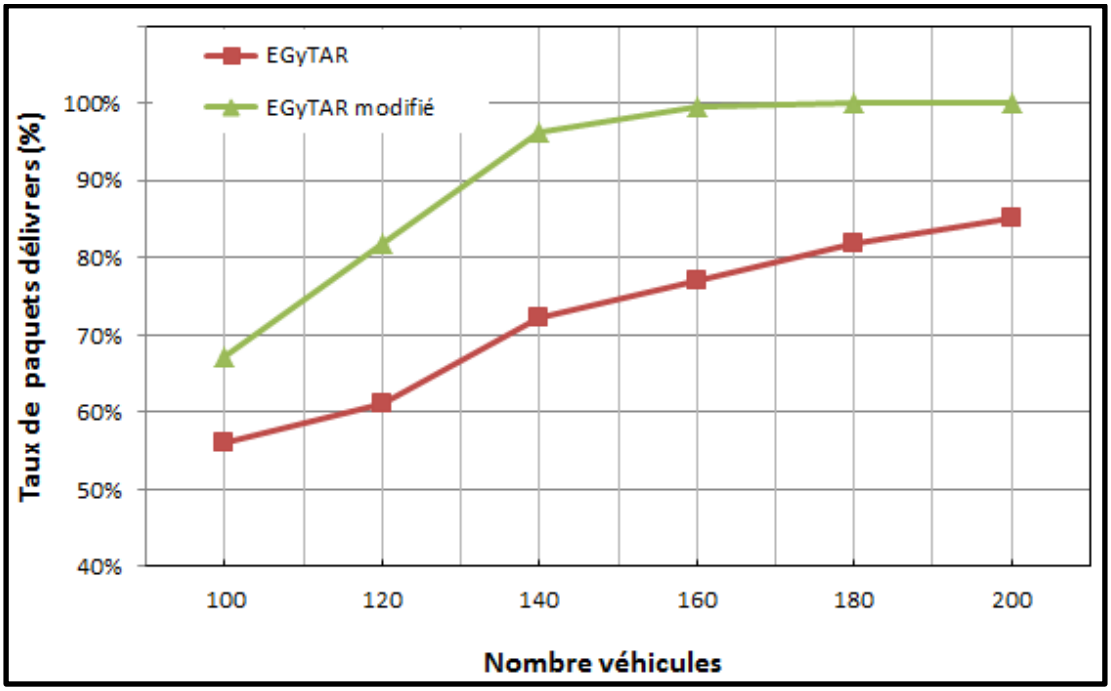


Figure 15 – Taux de paquets délivrés

La figure 15 illustre le taux de paquets délivrés en fonction de la densité des véhicules. On observe que le taux de délivrance de paquets pour EGyTAR et EGyTAR modifié augmente de manière continue en fonction de nombre de véhicules. D'après les deux courbes de la figure 15 on observe que le taux de succès d'EGyTAR modifié est meilleur par rapport à EGyTAR original, cela peut

s'expliquer par le fait que EGyTAR modifié utilise les informations de trafic véhiculaire mieux que EGyTAR original. Par l'utilisation de l'information du trafic véhiculaire, les nœuds relais ont plus de chance de trouver le saut suivant ce qui conduit d'augmenter la probabilité d'atteindre la destination finale.

On peut dire que le taux de succès est relativement lié avec le taux d'utilisation du trafic véhiculaire ce qui est montré par la suite.

b) Taux d'utilisation du trafic véhiculaire

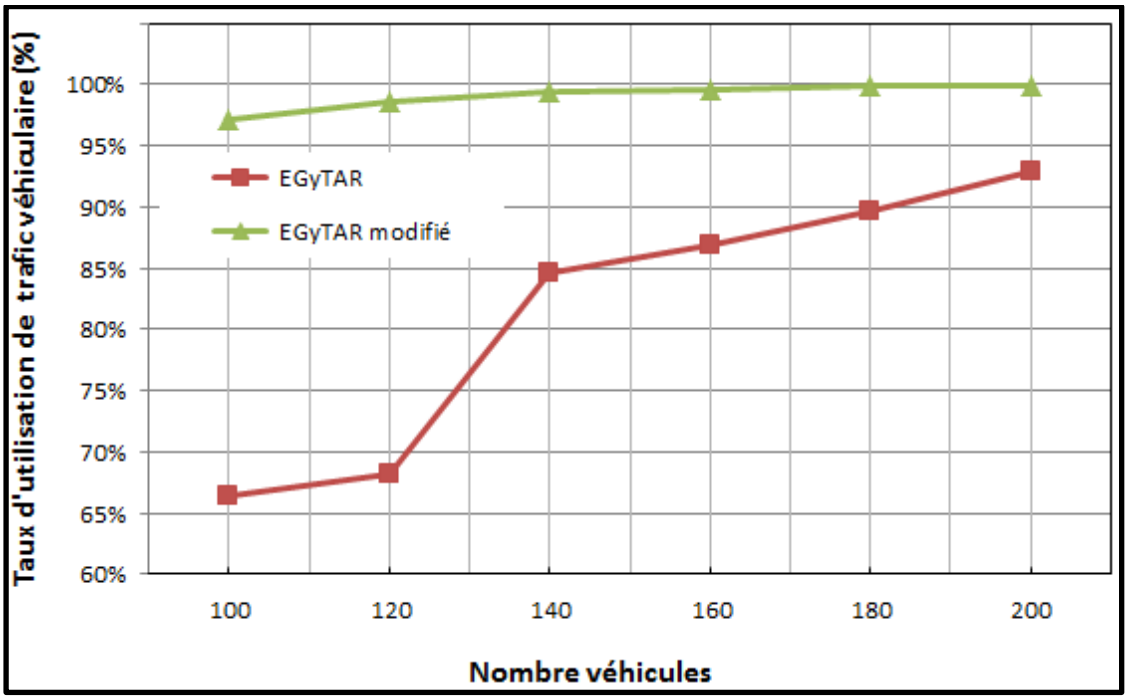


Figure 16 - Taux d'utilisation du trafic véhiculaire

La figure ci-dessous présente le taux d'utilisation du trafic véhiculaire en fonction du nombre de véhicules. La version modifiée d'EGyTAR montre un taux élevé de trafic véhiculaire par rapport à celui de la version originale d'EGyTAR, il peut atteindre 97 % avec une densité de 100 véhicules pour la version améliorée d'EGyTAR par contre dans la version originale il atteint seulement 66 %. Ceci est dû à la diffusion périodique des messages CDP ce qui augmente l'utilisation de l'information du trafic véhiculaire par contre dans la version originale la diffusion des messages CDP est limitée par l'évènement de changement de la route.

c) Délai de bout en bout

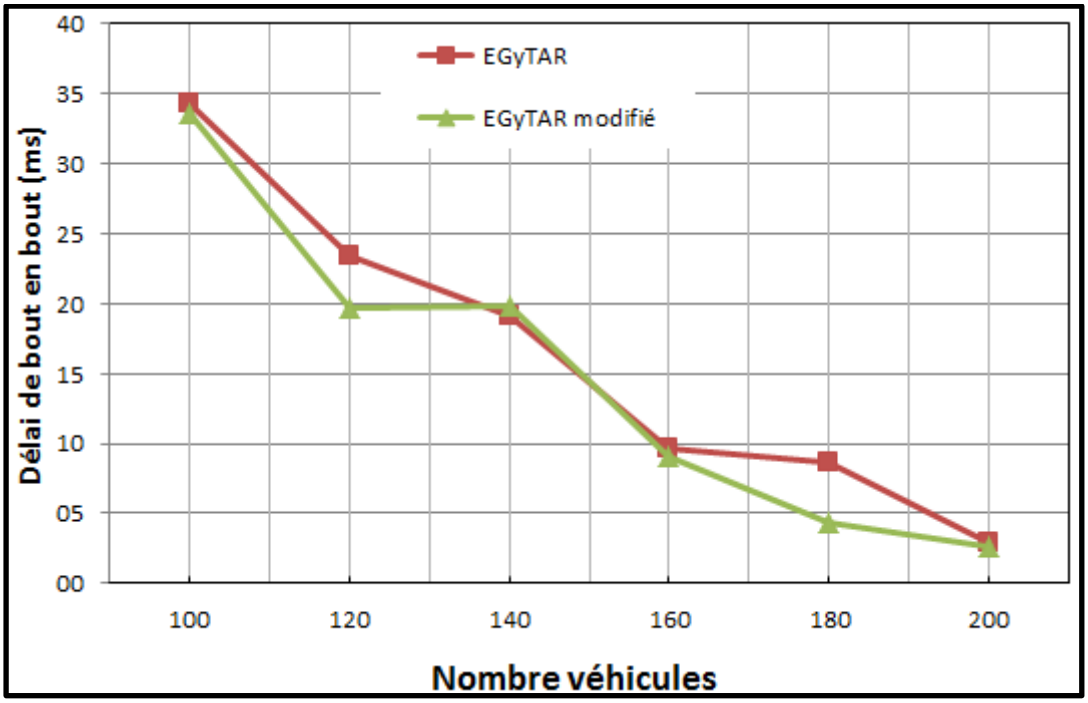


Figure 17 - Délai de bout en bout

D'après le graphe présenté dans la figure ci-dessus, il est clair que le délai de bout en bout d'EGyTAR modifié est minimisé d'une manière continue par rapport à celui d'EGyTAR original.

III.3 Conclusion

Dans ce chapitre, nous avons proposé une contribution concernant le protocole de routage pour les réseaux de véhicules appelé EGyTAR. Ce protocole adopte une approche progressive de choix des intersections intermédiaires. Une approche qui prend en compte aussi bien la distance vers la destination finale que le trafic routier et sa constante évolution dans le temps. Ainsi, EGyTAR est capable de sélectionner des routes robustes ayant une connectivité élevée, afin d'y injecter les paquets de données. Par la suite nous avons évalué ce protocole en fonction de quelques métriques. Ce qui nous a permis de conclure qu'EGyTAR amélioré nous a donné des résultats plus satisfaisants par rapport à EGyTAR original.

Conclusion générale et Perspectives

Rapport-Gratuit.com

Conclusion générale et perspectives

Les VANETs sont une particularité des réseaux MANETs. Ils permettent de faire une communication entre véhicules intelligents équipés de calculateurs, de périphériques réseau et de différents types de capteurs.

Les réseaux véhiculaires sont une projection des systèmes de transports intelligents (Intelligent Transportation System – ITS). Leur objectif principal est d'améliorer la sécurité routière par l'utilisation de la technologie des communications et de l'émergence de dispositif sans fil à faible coût.

Les systèmes de transport intelligents ne sont qu'à leurs balbutiements. A termes, le développement des technologies a favorisé une évolution remarquable des réseaux véhiculaires. Cette évolution a rendu les réseaux plus efficaces, plus fiables, plus sûrs et plus écologiques aussi bien du point de vue de l'industrie automobile que des opérateurs de réseaux et de services.

Par ailleurs, les VANETs commencent à être appréciés et reconnus par les usagers des véhicules et sont de plus en plus utilisés dans différents pays. Ils aident les utilisateurs dans leur conduite et minimisent les risques d'accident et offrent un plus de confort aux usagers et la possibilité d'accès à des loisirs. Pour assurer la communication entre véhicules, des protocoles de routage ont été conçus spécialement pour les VANETs. Mais le problème de routage consiste à déterminer un acheminement optimal des paquets à travers le réseau au sens d'un certain critère de performance.

Dans ce projet de fin d'études, notre domaine d'étude est concentré à l'étude des performances de protocole de routage dans un réseau VANET. Pour atteindre notre objectif et obtenir des résultats de simulation proches de la réalité, nous avons implémenté un modèle de mobilité pour un réseau véhiculaire et nous avons testé dans ce réseau le protocole « GyTAR » de la classe géographique.

D'après la contribution qu'on a faite, on a déduit que le routage dans les environnements urbains nécessite une bonne utilisation de l'information du trafic véhiculaire pour un routage efficace. Les résultats obtenus étaient très prometteurs ce qui justifie la valeur de notre contribution.

Références

[1] IEEE 802.11p Amendment, « Wirless Access in Vehicular Environments, » v. D3.0, 2007, work in progress.

[2] Chen, Y.S., Chapitre 1 : Vehicular Ad Hoc Networks : Applications and Challenges. Departement of Computer Science and Information Engineering National Taipei University

[3] Xin Wang, editor. Mobile Ad-Hoc Networks: Applications. INTECH, January 2011.

[4] https://www.academia.edu/24446527/Projet_VANET_20142015_1

[5] J. P. Hubaux, S. Capkun and Jun Luo, “The security and privacy of smart vehicles”, in IEEE Security & Privacy, vol. 2, no. 3, pp. 49-55, May-June 2004.

[6] Y. Park, K. H. Rhee and C. Sur, “A Secure and Location Assurance Protocol for Location-Aware Services in VANETs”, 5th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, Seoul, 2011, pp. 456-461.

[7] http://www.cs.nthu.edu.tw/-jungchuk/research.html (Accédé 20/02/2017)

[8] Jerbi Moez, "Protocoles pour les communications dans les réseaux de véhicules en environnement urbain : Routage et GéoCast bases sur les intersections", Thèse de doctorat de L'université d’Evry-Val d'Essonne, 2008.

[9] K. C. Lee, U. Lee and M. Gerla, “Survey of Routing Pro-tocols in Vehicular Ad Hoc Networks,” in Advances in Vehicular Ad-Hoc Networks : Developments and Challenges, IGI Global, 2009.

[10] V. Kumar, K. S. Vaisla, S. D. Sudarshan, “Priority Based Data Scheduling in VANETs”, in third IEEE International Conference on Advances in Computing, Communication and Engineering (ICACCE-2016), Durban, South Africa, Nov 2016.

[11] A. Aijaz et al. “Attacks on Inter Vehicle Communication Systems – an Analysis”, In Proceedings WIT, pp.189-194, 2006.

[12] C. TCHEPNDA, "Authentification dans les Réseaux Véhiculaires Opérés," Thèse de doctorat, Ecole Nationale Supérieure des Télécommunications, 2008.

[13] S. Busanelli, G. Ferrari and L. Veltri, "Short-lived key management for secure communications in VANETs," 11th International Conference on ITS Telecommunications, St. Petersburg, 2011, pp.613-618.

[14] Jonathan Petit, "Surcoût de l'authentification et du consensus dans la sécurité des réseaux sans fil véhiculaires", Thèse de Doctorat, Université de Toulouse, 2011.

[15] Ahizoune Ahmed, " Un protocole de diffusion des messages dans les réseaux véhiculaires", Mémoire, Université de Montréal, Département d'informatique et de recherche opérationnelle, Faculté des arts et sciences, avril 2011.

[16] L. K. Qabajeh, L. M. Kiah, and M. M. Qabajeh, "A qualitative comparison of position-based routing protocols for ad-Hoc networks," International Journal of Computer Science and Network Security, vol. 9, no. 2, pp. 131-140, Feb. 2009.

[17] Ait Ali Kahina. (2012). Modélisation Et Etude De Performances Dans Les Réseaux VANET. Thèse de doctorat de l’Université de Technologie de Belfort-Montbéliard. Octobre 2012.

Rapport-gratuit.com
LE NUMERO 1 MONDIAL DU MÉMOIRES

[18] S. C. a. A. Yasinsac, S. Carter, and A. Yasinsac, "Secure position aided ad hoc routing," in Proceedings of The IASTED International Conference on Communications and Computer Networks(CCN02), Cambridge, 2002, pp. 329-334.

[19] Ko, Young-Bae and N. H.Vaidya, "Location-Aided Routing (LAR) in mobile ad hoc networks", Wireless Networks Journal, 6(4), pp.307-321, 2000.

[20] S. Basagni et al., "A Distance routing effect algorithm for mobility (DREAM)"; In *Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking* (MobiCom '98), pp.76-84, 1998.

[21] B. Karp and H. T. Kung, "GPSR : Greedy perimeter stateless routing for wireless networks", in Proceedings of the 6th Annual international conference on Mobile computing and networking, Boston, Massachusetts, United States, 2000, pp. 243-254.

[22] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," *Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA '99. Second IEEE Workshop on*, New Orleans, LA, 1999, pp. 90-100.

[23] C. Lochert, H. Hartenstein, J. Tian, H. Fussler, D. Hermann and M. Mauve, "A routing strategy for vehicular ad hoc networks in city environments", *IEEE IV'2003 Intelligent Vehicles Symposium. Proceedings*, 2003, pp. 156-161.

[24] Jerbi M, Senouci SM, Meraihi R, Doudane YG, "An infrastructure-free traffic information system for vehicular netwroks", In: Proceedings of 66th IEEE vehicular technology conference, pp. 2086–2090, 30 Sept–03 Oct 2007.

[25] Jerb M, Senouci SM, Meraihi R, Doudane YG, "An improved vehicular ad hoc routing protocol for city environments", In: Proceedings of IEEE international conference on communications, pp. 3972–3979, 24–28 June 2007.

[26] Seet, B.-C., Liu, G., Lee, B.-S., Foh, C. H., Wong, K. J.,Lee, K.-K., "A-STAR : A Mobile Ad Hoc Routing Strategy for Metropolis Vehicular Communications", 3rd International IFIP Conference on Mobile and Wireless Communications Networking, pp.989-999, Athens, Greece, 2004.

[27] Bilal SM, Saeed U, Mustafa S. "Impact of directional density on GyTAR routing protocol for VANETs in city environments", 14th International IEEE multitopic conference (INMIC), Dec 2011.

[28] Omnet++. Http://www.omnetpp.org. Omnet++ Simulator framework, 2017.

Liste des figures

Figure 1: Exemple de réseaux avec infrastructure et sans infrastructure 4
Figure 2: Exemple de réseaux VANETs [4] 5
Figure 3: Eléments constituant un véhicule intelligent [5] 6
Figure 4: Modes de communications dans les réseaux VANETs [7] 7
Figure 5: Communication véhicule à véhicule (V2V) 7
Figure 6 - Mode de communication Véhicule à Infrastructure 8
Figure 7 - Emergency situation notification 10
Figure 8 - Les canaux disponibles pour l'IEEE 802.11p [8] 16
Figure 9 - Famille des protocoles de routage dans les VANET 21
Figure 10 - Architecture OMNET++ 28
Figure 11 - Mécanisme de sélection des intersections 31
Figure 12 - Mécanisme de diffusion de message CDP 32
Figure 13 – Structure des messages CDP 33
Figure 14: Evaluation de la liaison entre deux nœuds 35
Figure 15 – Taux de paquets délivrés 37
Figure 16 - Taux d'utilisation du trafic véhiculaire 38
Figure 17 - Délai de bout en bout 39
Figure 18 - Fichier NED en mode graphique 47
Figure 19 - Fichier NED en mode texte 48
Figure 20 - Fichier .ini 48
Figure 21 - Fichier .msg 48

Liste des tableaux

Tableau 1 : Comparaison entre les MANETs et les VANETs 21
Tableau 2: Environnement matériel 30
Tableau 3: Environnement logiciel 30
Tableau 4: Paramètres de simulation 37

Glossaire

4

4G *: 4 ème Génération*

A

AODV *: Ad hoc On Demand Distance Vector*
A-STAR *: Anchor-based Street and Traffic Aware Routing*
ASTM *: American Society for Testing and Materials*

C

CBR *: Constant Bit Rate*
CDP *: Cell Density Packet*
COOJA *: Contiki OS Java Simulator*
CSMA/CA *: Carrier Sense Multiple Access with Collision Avoidance*

D

DREAM *: Distance Routing Effect Algorithm for Mobility*
DSDV *: Destination-Sequenced Distance-Vector*
DSR *: Dynamic Source Routing*
DSRC *: Dedicated Short Range Communication*

G

GPSR *: Greedy Perimeter Stateless Routing*
GSM *: Global System for Mobile communication*
GSR *: Global State Routing*
GyTAR *: Greedy Traffic-Aware Routing*

I

IEEE *: Institute of Electrical and Electronics Engineers*
ITS *: Intelligent Transportation System*
IVC *: Inter Vehicule Communication*

L

LAR *: Location Aided Routing*

M

MAC *: Medium Access Control*
MANET *: Mobile Ad hoc Networks*

N

NAM *: Network Animator*
NS2 *: Network Simulator 2*
NS3 *: Network Simulator 3*

O

OBU *: On Board Unit*
OFDM *: Orthogonal Frequency Division Multiplexing*
OLSR *: Optimized Link State Routing*
OMNET : Operation and Maintenance New Equipment Training
Opnet *: Open Network*

P

P2P *: Peer-to-Peer*
PARSEC *: PARallel Simulation Environnement for Complex Systems, : PARallel Simulation Environnement for Complex systems*

R

RSU *: Road Side Unit*
RVC *: Rode to Vehicule Communication*
RWP *: Random Way Point*

S

STI *: Systèmes de Transport Intelligents*
SUMO *: Simulation of Urban Mobility*

T

TA *: Trusted Authority*
Tcl *: Tools Command Language*
TCP *: Transport Control Protocol*
TORA *: Temporally Ordered Routing Algorithm*

U

UDP : User Datagram Protocol, *: User Datagram Protocol*

V

V2I *: Vehicular-to-Infrastructure*
V2V *: Vehicular-to-Vehicular*
VANET *: Vehicular Ad hoc Network*

W

WAVE *: Wireless Access for Vehicular Environment*
Wi-Fi *: Wireless Fidelity*
WiMax *: Worldwide Interoperability for Microwave Access*

Z

ZRP *: Zone Routing Protocol*

Annexe A : Comment installer les outils de simulation ?

Dans cette sous-section, nous présentons les différentes étapes d'installation pour chaque outil utilisé dans notre simulation. Par hypothèse Ubuntu est installé sur le disque dur.

1. Installation OMNET++ 5.0
   - On doit accéder au site : https://omnetpp.org
   - Cliquer sur download et choisir omnet++ 5.0 (Linux) pour lancer le téléchargement.
   - Copier l'archive dans le home (où bien dans n'importe quel répertoire)
   - Décompressé le fichier télécharger, on obtient un sous-répertoire omnetpp-5.0
2. Configuration d'OMNET++ 5.0
   - Ouvrir le terminal.
   - Taper « ./configure »
   - Après la terminaison de la commande précédente on compile OMNET++ on utilisant la commande suivante « make »
3. Lancement d'OMNET++
   - Si vous souhaitez accéder à l'IDE depuis le lanceur d'application en tapant la commande suivante dans le terminal « omnetpp »
   - Ou via un raccourci de bureau, il faut exécuter les deux commandes ci-dessous :
     - Make install-menu-item
     - Make install-desktop-icon
4. Installation INET
   - Télécharger le framework INET à partir du site « https://omnetpp.org »
   - Décompressez dans un répertoire de votre choix en tapant : tar xvfz INET-<version>.tgz dans le terminal.
   - Démarrez OMNET++ IDE, et importer le projet via :
     Fichier->Importer->Projets existants à l'espace de travail. Un inet projet nommé devrait apparaître.
   - Construire avec Projet->Build, ou en appuyant sur Ctrl+B.

Annexe B : Composants d'un projet OMNET++

Les différents fichiers d'OMNET sont :

1. Fichier .ned
   Utilise le langage NED pour la description du réseau. Il est utilisable soit en mode graphique ou bien en mode texte. Ce dernier permet de décrire les paramètres et les ports du module. Les erreurs sont détectables en temps réel.
   Voici un exemple de fichier NED dans ces deux modes.

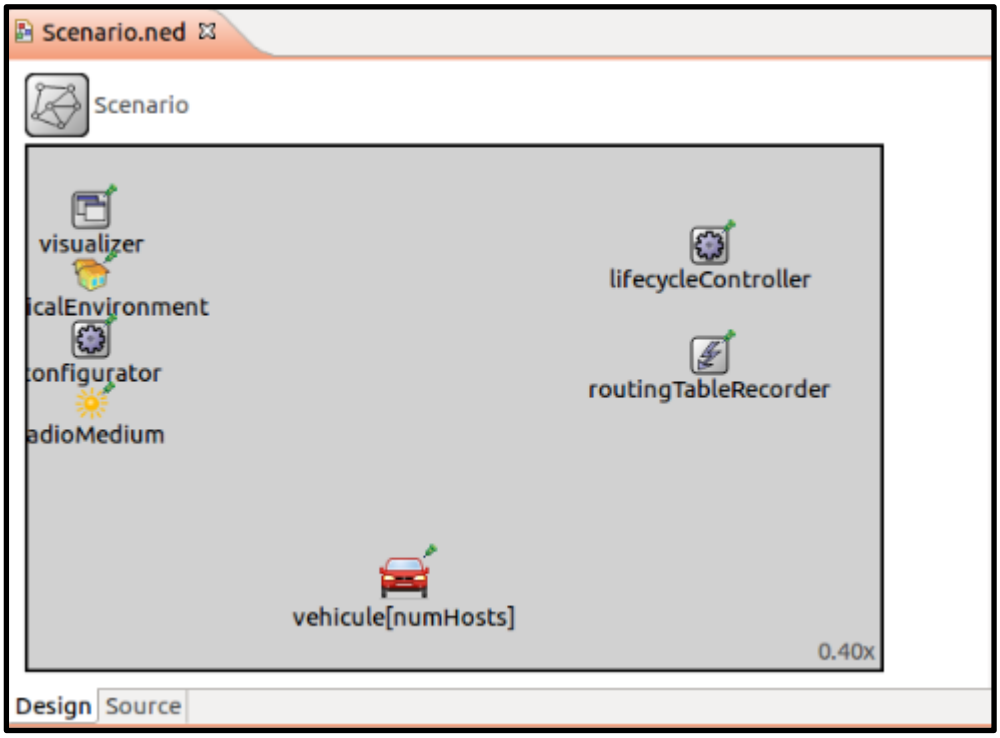


Figure 18 - Fichier NED en mode graphique

Scenario.ned

```
package EGyTARModifier.simulations;

import EGyTARModifier.nodes.Vehicule;
import inet.physicallayer.ieee80211.packetlevel.Ieee80211ScalarRadioMedium;
import inet.visualizer.integrated.IntegratedCanvasVisualizer;
import inet.node.inet.NodeBase;

import ned.DatarateChannel;
import inet.environment.common.PhysicalEnvironment;
import inet.physicallayer.ieee80211.packetlevel.Ieee80211ScalarRadioMedium;
import inet.common.lifecycle.LifecycleController;
import inet.networklayer.ipv4.RoutingTableRecorder;
import inet.networklayer.configurator.ipv4.IPv4NetworkConfigurator;
import inet.visualizer.integrated.IntegratedVisualizer;

network Scenario
{
    parameters:
        int numHosts;
        @display("bgb=1619.208,1247.688;bgl=4");
    types:
    submodules:

        visualizer: IntegratedVisualizer {
            parameters:
                @display("p=100,100");
        }
        physicalEnvironment: PhysicalEnvironment {
            parameters:
                @display("p=100,200");
        }

        configurator: IPv4NetworkConfigurator {
            parameters:
                @display("p=100,300");
        }
        radioMedium: Ieee80211ScalarRadioMedium {
            parameters:
                @display("p=100,400");
        }

        routingTableRecorder: RoutingTableRecorder {
            parameters:
                @display("p=1365.3359,297.216");
        }
        lifecycleController: LifecycleController {
            parameters:
                @display("p=1365.3359,164.088");
        }

        vehicule[numHosts]: Vehicule;

    connections:
}
```

Design Source

Figure 19 - Fichier NED en mode texte

Rapport-Gratuit.com

2. Fichier .ini

Le fichier .ini est lié étroitement avec le fichier .ned. Permet à l'utilisateur d'initialisé les paramètres des différents modules ainsi que la topologie du réseau.

La figure ci-dessous montre un exemple de ce type de fichier.

Network.ini

```
[General]
description = "EGYTAR "
network = Scenario
debug-on-errors = true
record-eventlog = false
sim-time-limit =100s
seed-0-mt = 5
num-rngs = 3
cmdenv-express-mode = true
tkenv-plugin-path = ../../../etc/plugins


**.scalar-recording = true
**.vector-recording = false

# physical environment parameters
*.physicalEnvironment.spaceMinX = 0m
*.physicalEnvironment.spaceMinY = 0m
*.physicalEnvironment.spaceMinZ = 0m
*.physicalEnvironment.spaceMaxX = 2000m
*.physicalEnvironment.spaceMaxY = 2000m
*.physicalEnvironment.spaceMaxZ = 20m
*.physicalEnvironment.config = xmldoc("obstacle.xml")

**.vehicule*.mobilityType = "BonnMotionMobility"
**.vehicule*.mobility.nodeId = -1

**.vehicule*.mobility.traceFile = "../Map/500_nodes.movements"
**.mapFile = "../Map/500_nodes.params"



######################### Test =======================
[Config Test]
description = "Test"
*.numHosts = 100
**.vehicule[8].numUdpApps=1
**.vehicule[8].udpApp[0].typename="UDPBasicApp"
**.vehicule[8].udpApp[0].destAddresses = moduleListByPath("**.vehicule[99]")

**.udpApp[0].destPort = 1234
**.udpApp[0].messageLength = 128B # Bytes

**.udpApp[0].sendInterval =1s
**.udpApp[0].startTime = 5s
**.udpApp[0].stopTime = 100s

**.vehicule[99].udpApp[0].typename = "UDPSink"
**.vehicule[99].numUdpApps = 1
**.vehicule[99].udpApp[0].localPort = 1234
```

Form Source

Figure 20 - Fichier .ini

Rapport-gratuit.com
LE NUMERO 1 MONDIAL DU MÉMOIRES

3. Fichier .msg

Les modules communiquent en échangeant des messages. Ces derniers peuvent être déclarés dans un fichier dont l'extension est « .msg » où l'on peut ajouter des champs de données. OMNET++ traduira les définitions de messages en classes C++.

EGyTAR.msg

```
cplusplus {{
#include "inet/common/geometry/common/Coord.h"
#include "inet/networklayer/common/L3Address.h"
#include "inet/common/TLVOption.h"
#include "RoutingDefs.h"
#include "CDP.h"
}}

namespace inet;
class noncobject L3Address;
class noncobject Coord;
class noncobject TLVOptionBase;
class noncobject CDP;

packet BeaconVehicule{
   L3Address adr;
   Coord position;
   Coord speed;
}
packet CDPPacket{
    Coord nextAnchor;
    L3Address nexHop;
    CDP cdp;
    bool isBroadCast=false;

}
message WaitForRep{
L3Address dst_adr;
}

class RoutingOption extends TLVOptionBase {
    Coord dst_position;
    Coord dst_junction;
}
```

Figure 21 - Fichier .msg

Rapport-gratuit.com
LE NUMERO 1 MONDIAL DU MÉMOIRES