الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
المدرسة الوطنية العليا للتكنولوجيا
Ecole Nationale Supérieure de Technologie

Département : Génie électrique Et Informatique Industrielle

Mémoire de projet de fin d'études

pour l'obtention du diplôme d'ingénieur d'état en Télécommunication

Spécialité
Systèmes de Télécommunication et Réseaux

Approche pour l'amélioration de la qualité de service du système de tracking véhiculaire Mc-Track

Réalisé par

Massinissa AHMAN
Aziz RECHACHE

Présent(e) et soutenue publiquement le : 06 Juillet 2022

Composition du Jury :

Président	M. Islem BOUCHACHI,	MCB	ENST
Promoteur	M. Abdellah KACI,	MCB	ENST
Examinateur	M. Tarek CHERIFI,	MCB	ENST
Examinateur	M. Sami BEGHAMI,	MCB	ENST
Invité	Mme / M. ……...,	……..	……..

Année universitaire 2021 –2022

Remerciements

Tout d'abord, nous remercions Dieu le tout-puissant, clément et miséricordieux qui nous a donné le courage, la force et la volonté pour accomplir ce présent travail.

Un grand merci pour nos familles, nos parents et nos amis pour leur soutien inconditionnel et leur présence continue.

Nous aimerions exprimer toute notre gratitude auprès de Monsieur A. KACI, pour sa présence, bienveillance, ses remarques, son encadrement de qualité et ses conseils pertinents au long de la rédaction de ce mémoire.

Nos vifs remerciements au corps professoral et administratif de l'École Nationale Supérieure de Technologie pour la qualité d'enseignement et la richesse de leur formation.

Enfin, nous tenons aussi à remercier également tous les membres du jury pour avoir accepté d'évaluer notre travail.

- Massinissa & Aziz

Dédicaces

Je dédie ce présent travail:

A mes parents bien aimés, qui ont toujours veillé sur le bon déroulement de mes études dans les meilleurs conditions, ans oublier mes chères soeurs Dyhia et Mélissa.

A tous mes amis et collègues avec qui j'ai partagés les hauts et les bas.

- Massinissa

Dédicaces

Je dédie ce présent travail:

À mes chers parents , qui m'ont donné la vie, aucune dédicace n'exprimera ma sincère gratitude à leurs sacrifices pour que je puisse arriver là où je suis.

À mes chers deux frères et ma petite soeur qui m'ont aidé et encouragé durant toutes mes études.

Sans oublier mon cher binôme Ahman Massinissa avec qui j'ai partagé le bien et le pire.

À mon meilleur ami Laacisse Abderahmane pour tout leur soutien.

Às tous mes amis, collègues de la promotion 2017 avec lesquels j'ai partagés mes meilleurs souvenirs. Et à toutes les personnes qui me sont chères.

- Aziz

Table des matières

LISTE DES TABLES vi

LISTE DES FIGURES vii

LISTE DES ABRÉVIATIONS viii

INTRODUCTION GÉNÉRALE 1

CHAPTER I : ÉTUDE DE L'EXISTANT 4

I.1 Introduction 4

I.2 Généralités sur les réseaux VANETs 5

I.3 Travaux Connexes 17

I.4 Conclusion 25

CHAPTER II : CONCEPTION 26

II.1 Introduction 26

II.2 *Présentation de Mc-Track* 27

II.3 Formulation du problème 33

II.4 Modélisation du problème 33

II.5 Conclusion 41

CHAPTER III : ÉTUDE EXPÉRIMENTAL 42

III.1 Introduction 42

III.2 Environnement de simulation 42

III.3 Processus de simulation 46

III.4 Les paramètres et métriques étudiés 49

III.5 Analyse des résultats 50

III.6 Conclusion 65

CONCLUSION GÉNÉRALE 66

Références bibliographique . . . . . .

Liste des tables

TABLE I.1 Comparaison entre WAVE et C-V2X 15

TABLE II.1 Tableaux des Variables 34

TABLE III.1 Paramètres de simulation 48
TABLE III.2 Paramètres de simulation 50
TABLE III.3 Paramètres de simulation 54

Liste des figures

Figure I.1 Modes de communication dans l'IoV 7
Figure I.2 Communication V2V 8
Figure I.3 Communication V2S 8
Figure I.4 Communication V2I 9
Figure I.5 GPSR Greedy Forwarding 18
Figure I.6 Maximum local au noeud A 19
Figure I.7 Choix des voisins selon WAGPSR 20
Figure I.8 Découverte de route par le protocole AODV 22

Figure II.1 Architecture de Mc-Track 28
Figure II.2 Abonnements des véhicules 30
Figure II.3 Abonnements des véhicules 31
Figure II.4 Chiffrement sélectif et sécurité adaptative 32
Figure II.5 la sélection des noeuds voisins 38

Figure III.1 Site de Open Street Map 44
Figure III.2 Architecture de simulateur MHR 46
Figure III.3 Processus de simulation de réseau 47
Figure III.4 Nombre de noeuds utilisés: Scénario 1 51
Figure III.5 Temps d'exécution: Scénario 1 52
Figure III.6 délai de bout en bout: scénario1 53
Figure III.7 Nombre de noeuds utilisés: Scénario 2 55
Figure III.8 Temps d'exécution 56
Figure III.9 Délai de bout en bout 57
Figure III.10nombre de noeuds utilisé 58
Figure III.11Délai de bout en bout 59
Figure III.12Section de réseau à t_0 60
Figure III.13Distribution de trafic à l'instant t_0 61
Figure III.14Distribution de trafic à l'instant t_1 62
Figure III.15Distribution de trafic à l'instant t_2 63
Figure III.16Distribution de trafic à l'instant t_3 64

LISTE DES ABRÉVIATIONS

ABE	*attribute-based encryption*
AODV	*Ad hoc On Demand Distance Vector*
CA	*Certification Authority*
C-V2X	*Cellular Vehicle to Everything*
DoS	*Denial of Service*
DSDV	*Destination Sequence-Distance Vector*
DSRC	*Dedicated Short Range Communication*
FBAODV	*Fitness Based Ad hoc On Demand Distance Vector*
IoV	*Internet of vehicles*
GPSR	*Greedy Perimeter Stateless Routing*
MANET	*Mobile AdHoc Network*
MHR	*Minimum Hops Routing*
MMGPSR	*Maxduration-Minangle GPSR*

MVT *Mobile Verification Terminal*

OBU *On Board Unit*

OSM *Open Street Map*

Q *surface de communication efficace*

QoS *Quality of Service*

RSU *Road Side Unit*

SDN *Software Defined Network*

STI *Système de Transport Intelligent*

SDVN *Software Defined Vehicular Network*

TA *Tracking Authority*

VANET *Vehicular Ad hoc Network*

V2H *vehicle to human*

V2I *vehicle to infrastructure*

V2N *Vehicle-to-Network*

V2S *vehicle to sensor*

V2V *vehicle to vehicle*

V2X *vehicle to everything*

WAVE *Wireless Access in Vehicular Environment*

WLAN *Wireless Local Area Network*

INTRODUCTION GÉNÉRALE

L'Internet des véhicules (IoV) est un réseau distribué d'objets communicants sans fil, notamment des voitures, son objectif principal est d'accroître la sécurité des usagers de la route et de réduire le nombre d'accidents en permettant aux véhicules une communication bidirectionnelle en temps réel avec leurs conducteurs, piétons, autres véhicules, infrastructures routières et systèmes de gestion de flotte.

Il existe des différents types de communication dans l'IoV, à savoir, véhicule à humain (V2H) dans lequel les données sont partagées entre le véhicule et les personnes, véhicule à capteur (Vehicle to Sensor V2S), car la voiture est considérée comme un objet multisensoriel, véhicule à l'infrastructure (V2I Vehicle to Infrastructure) où la voiture communique avec les unités routières principalement en utilisant le WiFi et la 4G/5G, véhicule à véhicule (Vehicle V2V) où les données sont partagées entre les véhicules connectés à l'aide de l'accès sans fil IEEE dans les environnements de véhicules (Wireless Access in Vehicular Environment WAVE), véhicule à cloud dans laquelle les Data Centers et les véhicules sont les principaux acteurs [1]. L'internet des véhicules est un système de réseau complexe avec une topologie dynamique qui fait face à de nombreux problèmes de sécurité, qui pourraient constituer une menace majeure pour l'industrie de l'IoV, la vie des consommateurs et leurs intimité, d'où un besoin urgent d'éliminer les menaces de sécurité existantes et de trouver des solutions qui peuvent garantir la sécurité du partage de données dans le réseau IoV.

Outre la sécurité, la qualité de service est également un facteur important dans les VANETs où une grande quantité de capteurs et d'appareils sont connectés et communiquent entre eux.

La QoS est définie comme la qualité de service de la liaison de données, elle représente les caractéristiques de transmission entre les bords de la liaison de données. Les paramètres QoS sont appliqués aux modes sans connexion et orientés connexion. Les réseaux IoV génèrent une énorme quantité de données qui peuvent être critiques et ne tolèrent pas les retards, doivent donc être transmises de manière sécurisée et efficace, ce qui nécessite l'optimisation des paramètres de QoS qui ont des implications élevées telles que le retard, la gigue, la bande passante et la latence[2].

Dans les VANETs, la QoS et la sécurité sont deux services à rôle critique. Les mécanismes de sécurité gèrent la protection des utilisateurs du réseau et de leurs données, tandis que la QoS permet le bon fonctionnement des services multimédias et autres en temps réel. Les mécanismes de QoS et de sécurité ne sont pas indépendants, puisque les choix du mécanisme de sécurité peuvent avoir un impact sur l'efficacité de la QoS et vice versa. La sécurité est nécessaire pour protéger le réseau des attaques qui pourraient réduire la QoS ou compromettre la stabilité du réseau.

Parmi les systèmes qui ont fait face aux problèmes de la sécurité, on trouve *Mc-Track*, qui est un nouveau système de suivi de véhicules sécurisé, orienté données et basé sur le Cloud, proposé par Monsieur Abdellah KACI. Le système *Mc-Track* est une approche adaptative qui consiste à prédire la sensibilité des données et le niveau de sécurité à l'aide de l'apprentissage automatique (Machine Learning).*Mc-Track* fourni un cryptage sélectif et une sécurité adaptative via une autorité de suivi (Tracking Authority TA), à l'aide du classificateur d'apprentissage automatique *k-Nearest Neighbours (k-NN).*

Lors de la conception du système Mc-Track, on n'a pas pris en compte la qualité du service. C'est alors dans ce cadre que s'inscrit notre projet de fin d'études, qui consiste à enrichir l'architecture de Mc-Track pour prendre en compte la qualité du service, la gestion du trafic et à mettre en place un mécanisme d'optimisation de la QoS. Notre solution proposée nommé Minimum Hops Routing (MHR) a été simulé dans un simulateur que nous avons développé en

langage Python afin d'étudier ses performances.

Le présent mémoire a été organisé en trois chapitres, selon la structure suivante : Le premier chapitre est consacré d'une part aux notions générales sur les réseaux véhiculaires VANETs. D'une autre part nous citerons quelques travaux connexes relatives à l'optimisation de la QoS dans les VANETs. Le deuxième chapitre est consacré à la présentation de l'architecture globale de système de suivi véhiculaires MC-Track, la formulation de la problématique ainsi que sa modélisation. Le dernier chapitre est dédié à l'étude expérimentales où nous présenterons l'environnement de simulation et les résultats obtenus.

Finalement, nous terminerons ce présent travail par une conclusion générale qui résume les principaux résultats obtenus et nos futurs travaux ou nous importerons des améliorations de quelques perspectives relative à notre solution.

CHAPITRE I

ÉTUDE DE L'EXISTANT

I.1. Introduction

Les réseaux VANET ont une topologie spéciale qui change à chaque instant à cause de la mobilité des noeuds. Ces réseaux forment le coeur d'un Système de Transport Intelligent (STI), mais leurs topologie dynamique crée plusieurs défis qui pénalisent la fiabilité de la communications vu que la connectivité entre les noeuds de réseau véhiculaire n'est pas toujours maintenue, d'où la nécessité d'avoir un standards de communication fiable qui répond aux exigences d'un environnement pareil. Pour cela les protocoles de routage ont un rôle important qui est d'assurer l'échange d'information entre les véhicules et puisque le routage dans les réseaux VANET basé sur des communications multi-saut donc ces protocole facilite la communication entre plusieurs véhicules même si ils ne sont pas dans la même porté de transmission.

Dans ce chapitres on vas présenter les généralités sur les réseaux VANET et les travaux connexes relative à l'optimisation de la qualité de service. Ce chapitre est subdivisé comme suit: La première section donne une définition des réseaux véhiculaires, une description de leurs composition et architecture globale, mode de communication,standards et normes utilisés, une présentation des caractéristiques des VANETs, finalement, une vue sur la sécurité dans les réseaux véhiculaires ainsi que les protocoles de routages qu'ils utilisent. Dans la deuxième section nous allons présenté le principe de fonctionnement de certaines protocoles de routage dans les VANETs.

I.2. Généralités sur les réseaux VANETs

Les réseaux VANET

Un réseau *VANET (Vehicular AdH hoc Network)* est un réseau de communication formé par des noeuds qui peuvent être des véhicules intelligents où des infrastructures situées aux bords de routes[3], ces noeuds sont équipés d'appareils qui leur permettent de communiquer entre eux.

Les réseaux VANET font parti de la famille des réseaux MANET (Mobile AdHoc Network) qui se composent d'un ensemble de nœuds mobiles connectés en point à point sans infrastructure ou chaque neoud est un point d'accés.

L'objectif principale des VANETs est d'assurer une communication entre les véhicules et l'environnement qui les entours afin de réduire en premier lieu le nombre d'accidents et assurer la sécurité routière en offrant au conducteur une vision au delà des obstacles et un accès à plusieurs services.

Composition d'un réseau VANET:

Un réseau VANET est composé de plusieurs entités et équipements qu'on peut différencier en quatre types : unité embarquée (On Board Unit OBU), les véhicules, unités bord de route (Road Side Unit RSU) et l'équipement central (Central Authority CA).

- **On board Unit (OBU):** ce sont des équipements installés à l'intérieur de véhicule par l'utilisateur, ils effectuent plusieurs tâches comme le calcule et partage de la position ainsi que l'émission/réception de messages dans le réseau.
- **Les véhicules:** ce sont les noeuds mobiles qui forment le réseau VANET, ils sont équipés avec des OBUs qui leur permet d'échanger des informations entre eux, ainsi que des technologies avancées comme les caméras, capteurs intelligent, Global Positioning System GPS,...

- **Road Side Units:** sont des équipements au bord de la route, leur rôle est de communiquer avec les véhicules à proximité en diffusant des informations utiles comme les conditions de trafic, elles sont connectées à Internet par câble et peuvent également être interconnectées les unes avec les autres via un réseau maillé à haute capacité, le réseau câblé et sans fil formé par les RSU peut être utilisé pour ponter les différentes partitions de VANET. [4].

- **Central Authority CA:** cette équipement fournit des services et applications pour les VANETs, il pourra être un serveur de stockage,un point d'entrée au réseau internet. Il est transparent pour l'utilisateur.

Les types de communication dans les VANET

Dans les réseaux VANET on peut définir six types de communication: les communications Véhicule-à-Véhicule(V2V), Véhicule-à-Capteurs (V2S), Véhicule à-Infrastructure(V2I), Véhicule-à-Humain (V2H) et hybride.

- **Communications Véhicule-à-Véhicule(V2V)** Dans ce type de communication inter-véhicules aucune infrastructure n'est nécessaire, il est composé uniquement d'OBU, chaque véhicule peut communiquer alors directement avec une autre véhicule sans besoin d'un élément centralisé. Les communications V2V sont très utilisés car elles permettent de transférer des informations liées aux services de sécurité routière, mais elles ne garantissent pas une connectivité permanente ce qui est dû à la mobilité.

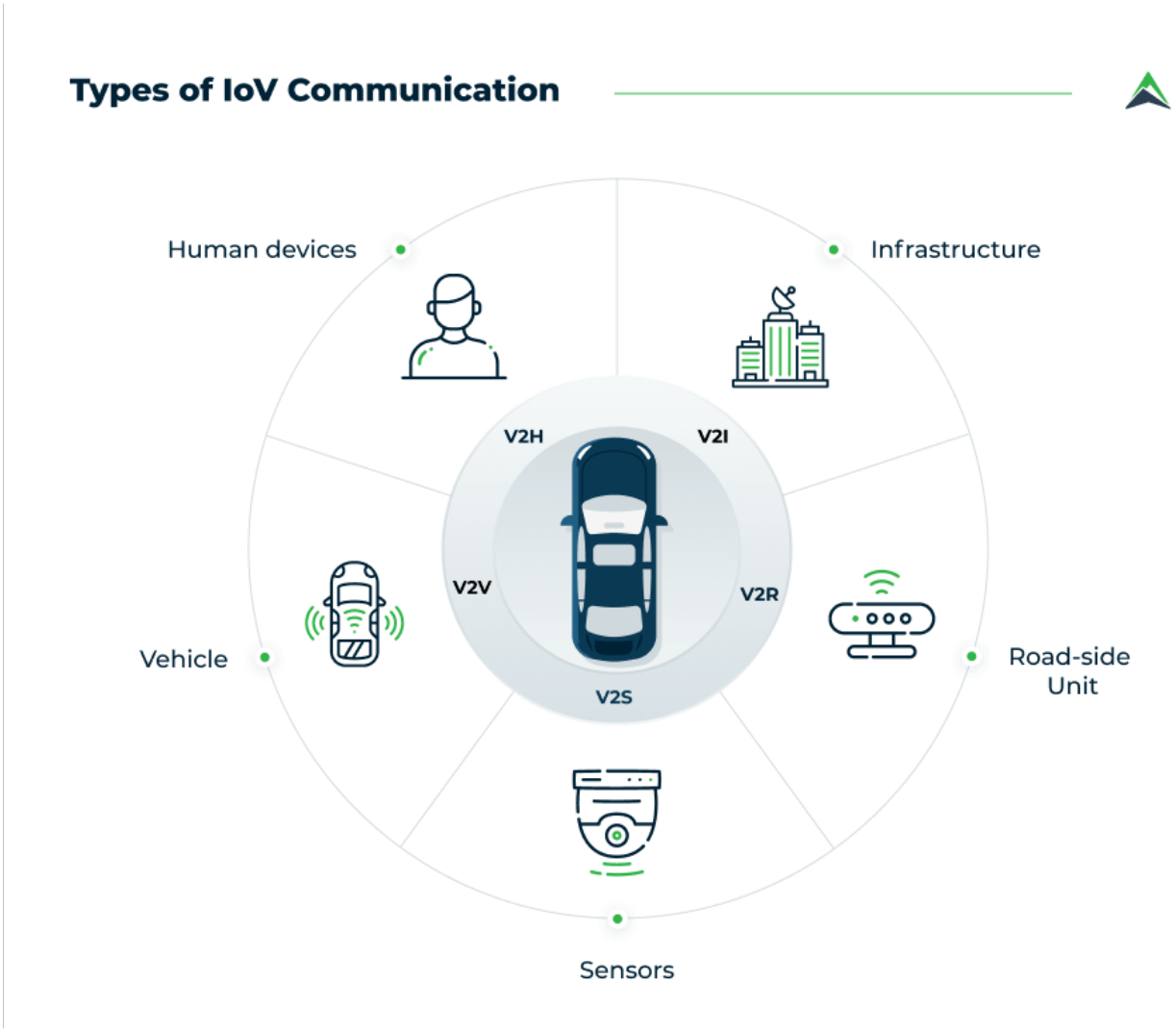


Figure I.1: Modes de communication dans l'IoV



Figure I.2: Communication V2V

- **Communication véhicules à capteurs V2S:** Un véhicule possède plusieurs capteurs qui aident à collecter des informations comme la température, la distance, position, etc cette communication est entre le véhicule et ses capteurs ou bien d'autres qui sont à proximité.

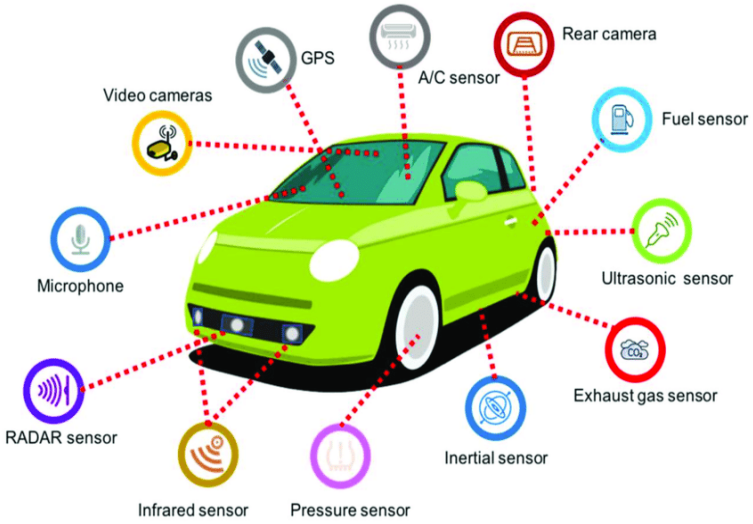


Figure I.3: Communication V2S

- **Communications Véhicule à-Infrastructure(V2I)** L'utilisation des RSUs dans ce type de communication est nécessaire, elles sont utilisées par les véhicules pour accèder à

des applications de sécurité, de gestion et de confort, ce qui assure une mielleure utilisation des ressources partagées et offre un accés à quelques services comme Internet, échange de données de voiture-à-domicile, voiture-à-parking, etc.

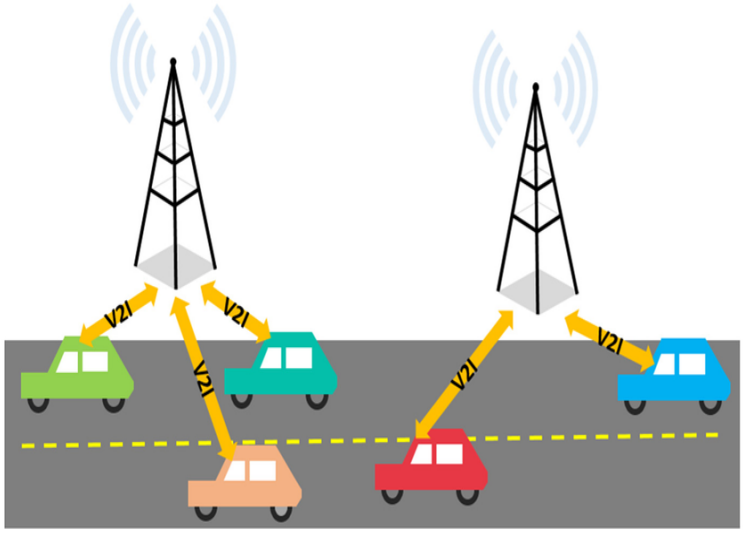


Figure I.4: Communication V2I

- **Véhicule-à-Humain (V2H):** Le modèle V2H facilite la communication entre le conducteur et le véhicule, il prend aussi en charge la mobilité et la sensibilisation des utilisateurs les plus proches, tels que les piétons, cyclistes et automobilistes [5].

- **communications Hybride:** C'est une combinaison d'un ou plusieurs modes de communication cités précédemment. Vu que la portée des infrastructures est limitée, ce mode offre la possibilité d'augmenter cette dernière en utilisant les véhicules comme relais. L'accès à l'infrastructure réduit aussi les problèmes de routage V2V et améliore les performances globales de réseau. Une communication hybride est nécessaire pour assurer un partage efficace d'information .

Caractéristiques des réseaux VANET

les réseaux VANET font partie de réseau MANET, ils ont des caractéristiques spéciales qui seront présentées dans cette section :

La mobilité

La mobilité dans les VANET est liée aux décisions des conducteurs et leurs réactions face à des obstacles ou des situations différentes rencontrées (état de la route, panneaux de signalisation, obstacles, etc. . .) ou aux stations de base routières (infrastructures) que ce soit dans les autoroutes ou au sein d'une zone métropolitaine. Ces contraintes affectent énormément le modèle de mobilité et la qualité des transmissions radio [6].

Topologie dynamique

Les nœuds de réseau VANET se caractérisent par leur vitesse élevées qui varie constamment au cours de temps . Cela conduit à des changements fréquents de topologie de réseau , qui introduit des frais généraux de communication dû aux échanges de nouvelles informations de topologie.

Environnement de déploiement

On distingue l'environnement urbaine et les autoroutes:

- Urbaine: un environnement urbaine est caractérisé par un nombre élevé de véhicules qui circulent à des vitesses limitées, ce qui permet d'avoir une bonne connectivité entre les entités de réseau.

- Autoroute: l'autoroute est caractérisées par une grandes variétés de véhicule circulant à des vitesse élevées ce qui limite la connectivité entre les noeuds, d'où le besoin d'utiliser les RSUs pour remédier aux difficultés de communication.

Mode de communication

Dans les VANETs, il existe trois mode de communications qui sont en changement continu selon le besoin:

- **Mode Ad hoc:** la communication entre les noeuds est directe, chaque noeud est considéré comme un point d'accès qui communique sans intermédiaire avec un noeud voisin, c'est

le cas de V2V.

- **Mode infrastructure:** la communication entre les entités de réseau nécessite l'utilisation de l'infrastructure (RSU).

- **Mode hybride:** dans ce mode, on trouve que la communication entre les entités de réseau peut utiliser les deux modes cités, donc on trouve que les noeuds communiquent directement et aussi à travers les RSU.

Capacité de traitement et de calcul

La communication entre les noeuds nécessite un traitement rapide et efficace d'informations collectées afin de prendre des décisions relatives aux cas possibles de circulation sur la route. Généralement dans les réseaux VANET, les entités dispose une énergie suffisante afin d'effectuer les différentes opérations sans interruptions.

Applications des VANETs

On peut diviser ces applications en deux catégories, on trouve les applications de sécurité et applications de confort:

Applications de sécurité:

Les applications de sécurité sont mise en place dans le but de diminuer le nombre d'accidents sur les routes et réduire les pertes de vie que ça soit pour les conducteurs, passagers et piétons. En effet, les VANET offre au conducteur une vue de 360° sur l'environnement routier et leurs permet de voir au delà des obstacles, ces informations collectées peuvent être utilisés pour l'activation des systèmes de sécurité. Ces applications sont résumées dans les cas suivants :

- **Alerte d'accidents:** Si un accident venait à surgir, les véhicules derrières peuvent être en danger. Les applications de sécurité sont alors utilisées dans ce cas pour avertir les autres conducteur d'un accident qui s'est produit à proximité, ce qui éviterait un carambolage. Ils peuvent être utilisés pour envoyer un alerte précoce au pilote et éviter qu'un autre accident surgisse.

- **Alerte de ralentissement:** cette alerte incite le conducteur à ralentir si une anomalie de circulation est détectée par le réseau (freinage important effectué par une voiture, pluie, un véhicule qui effectue des travaux . . .etc.)[7]

- **Trafic routier:** les applications de sécurité aident les conducteurs à déterminer le meilleur chemin à prendre pour atteindre leur destination en évitant les embouteillages, cela peut déminer de manière indirecte le nombre d'accidents.

Application de confort

Ces applications aident l'utilisateur dans la vie quotidienne, parmi ces applications on trouve:

- **Smart Parking:** ce service permet d'obtenir des informations sur des parkings proches comme la disponibilité d'espace de stationnement et guider les conducteurs vers un espace libre.

- **Internet:** les VANET permet aux utilisateurs d'accéder à internet en leur leur offrant divers services comme la consultation des mails, le partage de music,etc..

- **Application P2P(Peer to Peer):** les passagers dans la voiture peuvent exploiter le réseau VANET pour un usage personnel à travers les applications P2P de partage de la musique et films, discussion instantanée entre passagers, jeux en réseau,...

Standard de communication

V2X (Vehicle to Everything) est un terme utilisé pour désigner la communication d'un véhicule avec toutes les autres entités, y compris les autres véhicules en mouvement et en stationnement, les piétons, les feux de circulation, les panneaux de signalisation, les chantiers de construction et bien d'autres. Un véhicule communique avec le monde extérieur de deux manières:

- En recevant un retour physique des capteurs lidar installés autour du véhicule.

- Par une communication sans fil qui envoie et reçoit des messages vers et depuis d'autres entités.

Par exemple, les capteurs lidar fournissent une rétroaction de l'environnement autour pour détecter toute menace immédiate, tandis que des messages concernant l'emplacement, la vitesse et la direction de chaque véhicule jusqu'à 300 mètres peuvent être obtenus via une communication sans fil afin que la voiture puisse ajuster ses comportements loin devant le temps [8].

Dans cette partie, nous examinerons plus en détail les deux différentes technologies de communication sans fil V2X actuellement utilisées par les constructeurs automobiles et les développeurs d'infrastructures à travers le monde.

- **Dedicated Short Range Communication (DSRC):** DSRC a été introduit pour la première fois en tant que technologie V2X dans la norme 802.11p de "Institute of Electrical and Electronics Engineers" (IEEE), un protocole de communication véhiculaire destiné à ajouter un accès sans fil dans les environnements véhiculaires (Wireless Access in Vehicular Environnements (WAVE)).

  En tant que première norme de communication pour V2X, WAVE utilise la technologie WLAN (Wireless Local Area Network) pour établir des canaux de communication dédiés à courte portée (DSRC) afin que les véhicules puissent communiquer directement avec d'autres entités dans des portées courtes à moyennes (généralement 300 mètres). Bien que WAVE soit le nom officiel du protocole, beaucoup se réfèrent encore à la technologie comme DSRC pour décrire le mécanisme sous-jacent.

  En fait, de nombreux experts du secteur utiliseraient indifféremment les termes DSRC, 802.11p, WAVE ou WLAN-based V2X pour désigner la même chose[8].

  DSRC est essentiellement une modification du Wi-Fi. La technologie a été considérée comme une percée majeure dans l'industrie automobile car elle permet la transmission de données entre deux appareils sans passer par aucun intermédiaire, ce qui la rend très

utile pour les zones rurales et éloignées sans aucune infrastructure de télécommunication. C'est comme envoyer un message texte à un autre téléphone à 300 mètres sans avoir besoin d'une couverture de réseau cellulaire. De plus, DSRC est connu pour avoir une latence très faible en raison de l'élimination de l'intermédiaire.

Après son approbation initiale en 2010, le DSRC a subi des années de tests avant d'être déployé pour la première fois dans certains véhicules fabriqués par Toyota au Japon en 2015, puis adopté par certains modèles Cadillac aux États-Unis en 2017. En 2019, la Volkswagen Golf 8, une des voitures les plus populaires en Europe, est devenue la voiture compatible V2X la plus vendue sur le marché [8].

- **Cellular V2X (C-V2X)** Introduit peu après le DSRC, C-V2X est un autre protocole de communication véhiculaire développé pour V2X. Défini par les projets de partenariat de "3rd Generation Partnership Project" (3GPP) [8], C-V2X utilise la radio cellulaire au lieu du WLAN, ce qui signifie qu'il utilise le même ensemble de technologie radio cellulaire que les téléphones portables. La principale différence qui distingue le C-V2X du DSRC est qu'il permet une communication directe et indirecte.

  - En C-V2X direct, les véhicules communiquent directement avec les autres véhicules (V2V) et les unités routières (V2I) de la même manière que le fonctionnement du DSRC.

  - Sous C-V2X indirect, les véhicules communiquent indirectement avec d'autres entités via le réseau cellulaire, ce que DSRC ne peut pas faire.

  Le C-V2X indirect est utile car le réseau cellulaire peut collecter des données de nombreux véhicules et peut donc être plus efficace pour gérer le trafic à large échelle. Conçu à l'origine dans la version 14 pour utiliser la norme LTE, le 3GPP a ensuite ajouté la compatibilité pour la 5G et dans les versions 15 et 16.

Comparaison WAVE / C-V2X [9]		
	DSRC	C-V2X
Standard	IEEE 802.11P	C-V2X Version. 14/15 (pour jusqu'à 4G-LTE) et version 16 (pour 5G NR)
Modulation	BPSK/QPSK/16QAM/64QAM	BPSK/QPSK/16QAM/64QAM pour 4G-LTE, OFDM (QAM+FDM) pour 5G
Sécurité	Cryptage par clé publique	Cryptage par clé publique
Débit des données	27Mbps	4-12Mbps
Latence maximale	150ms	moins de 50ms pour le test avec 4G-LTE

Table I.1: Comparaison entre WAVE et C-V2X

Sécurité dans les VANETs

Les réseaux VANETs sont des systèmes de réseau complexe avec une topologie dynamique qui fait face à de nombreux problèmes de sécurité, qui pourraient constituer une menace majeure pour l'industrie de l'IoV, la vie des consommateurs et leurs intimité, d'où un besoin urgent d'éliminer les menaces de sécurité existantes et de trouver des solutions qui peuvent garantir la sécurité du partage de données dans le réseau IoV. Et pour cela, la sécurité dans les réseaux VANET doit être considérée comme importante pour les autres réseaux informatiques sécurisés. Il y'a un certain nombre d'attaques possibles dans VANET. Le but des ces attaques est de créer un problème pour que les utilisateurs perdent l'accès au système où pour voler leurs informations. On peut citer quelque types des attaques:

- **Attaques d'authentification:** Il existe des différents types d'attaques d'authentification, l'attaque Sybil, l'attaque par tromperie GPS, la mascarade, l'attaque wormhole.
- **Attaques de routage:** Les nœuds malveillants peuvent modifier les informations de routage, ce qui entraîne de fausses informations de routage et un nombre de sauts incorrect

qui entraîneront une livraison de données incorrecte et une communication erronée. Ces attaques peuvent être contrées en utilisant les systèmes de détection d'intrusion (IDS) et le protocole de routage pour les réseaux à faible puissance et avec perte (RPL) dans IoV.

- **Attaques de disponibilité:** Ils peuvent affecter la disponibilité du système, en utilisant des méthodes qui obligent la bande passante du système et la puissance de transmission à devenir inutilisables en dépassant sa capacité de service maximale. Des exemples d'attaques de disponibilité sont l'attaque par déni de service (DoS) et l'attaque par interférence de canal.

- **Attaques de confidentialité:** Les réseaux sans fil sont les plus exposés aux écoutes clandestines ou aux attaques de confidentialité, c'est le même cas avec les VANETs car il utilise une communication sans fil. Les attaques d'écoute clandestine ne peuvent pas être facilement tracées car il s'agit d'une attaque passive qui ne perturbe aucun composant du réseau. Le cryptage est une technique courante pour contrer ce type d'attaque mais le partage sécurisé des clés avec différentes entités communicantes en toute sécurité est un problème majeur, en particulier lorsque les composants du réseau évoluent rapidement.

Visant à permettre aux véhicules de communiquer en toute sécurité et en privé, tout mécanisme de sécurité doit mettre en œuvre quatre caractéristiques de base :

1. **Intégrité:** S'assurer que les données transmises sont exactes, sans erreur et n'ont pas été modifiées par un tiers.

2. **Authenticité:** S'assurer que l'expéditeur est celui qu'il prétend être et non quelqu'un qui se fait passer pour lui.

3. **confidentialité:** consiste à s'assurer que toutes les données sensibles restent protégées et ne sont accessibles qu'aux bonnes personnes.

4. **Disponibilité:** S'assurer que le système est accessible à tout moment, fonctionne par-

faitement et comme il le doit.

I.3. Travaux Connexes

La QoS est essentiellement liée au mécanisme de routage utilisé pour la communication. Le routage dans les VANET utilise trois stratégies, basées sur la position, la topologie[10] et Software Defined Network (SDN).

Protocoles de routage basés sur la position

Les protocoles de routage basés sur la position sont considérés comme étant les plus performant dans l'environnement VANET, la table de routage n'a pas besoin d'être partagée avec d'autres véhicules, les principaux problèmes sont le maintient de la fiabilité de la liaison, l'évolutivité du réseau, une sélection appropriée d'un nœud relais pour transmettre les données et le maintient du transfert de données en taux maximal.

Il est supposé que chaque nœud a ses propre information de position disponible via GPS et/ou localisation à courte portée. Les nœuds échangent périodiquement ces informations avec leur voisin à un saut par le biais de Beacon Messages. Donc à chaque instant donné, chaque nœud a les informations de position de tous ses voisins à portée de communication ainsi que la position de la destination par les Beacon Messages et service de localisation [11]. Greedy Perimeter Stateless Routing (GPSR) GPSR est un protocole de routage basés sur la position, il offre un délai E2E (End to End) minimum et réduit la latence. GPSR utilise la stratégie de Greedy Forwarding en sélectionnant le nœud le plus proche de la destination comme prochain saut pour transmettre les données, comme montré dans la figure I.5 où S et D représentent respectivement la source et la destination, les noeuds en gris sont les voisins de S. Cependant, cela augmente les risques de défaillance de la liaison pendant le transfert de données puisque le nœud sélectionné pourrait quitter la portée de communication à tout moment.

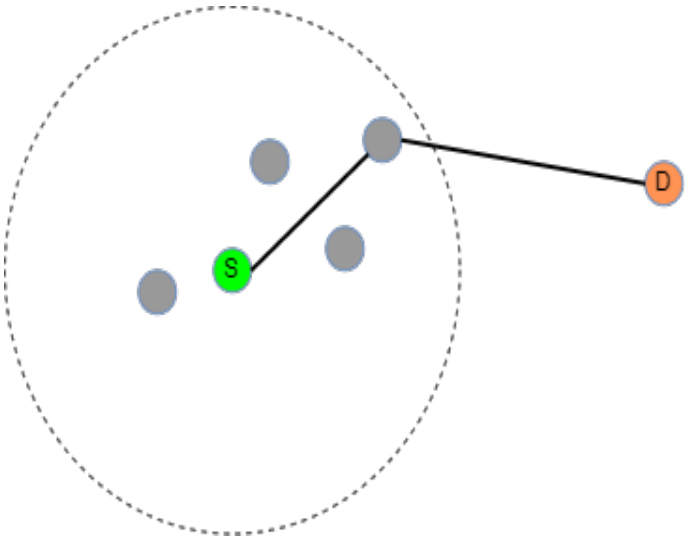


Figure I.5: GPSR Greedy Forwarding

Il existe des situations où la source est plus proche de la destination que le voisin, ce cas est appelé maximum local. Dans ce cas, GPSR ne peut plus maintenir la stratégie de Greedy Forwarding, donc il rentre dans le mode récupération (Recovery Mode) pour transmettre le paquet au nœud suivant, en utilisant la règle de la main droite pour choisir le prochain saut. Dans la figure I.6, le noeud S choisi A comme prochain saut puisqu'il est le plus proche de la destination. Cependant, il n'y a pas de nœud plus proche de la destination que le nœud A lui-même, ce qui créé le problème de maximum local. Le noeud A rentre en mode récupération et utilise la règle de la main droite pour transmettre la donnée au noeud B.

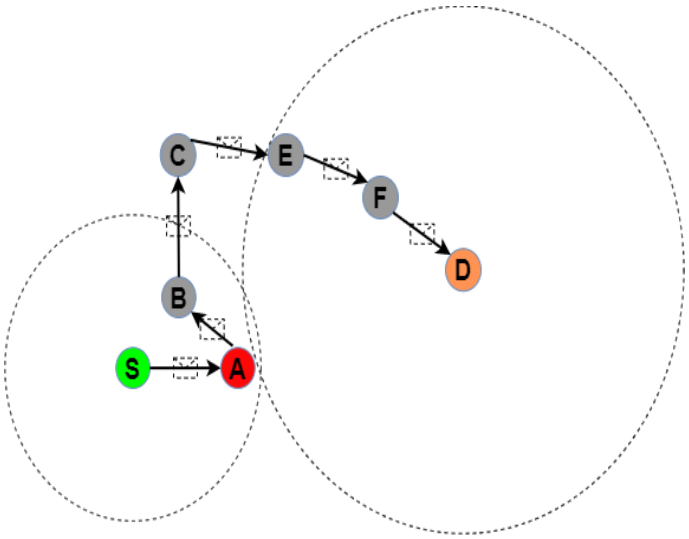


Figure I.6: Maximum local au noeud A

Maxduration-Minangle GPSR (MMGPSR)

MMGPSR est un protocole de routage amélioré basé sur GPSR, il a résolu le problème de rupture de liaison de communication en sélectionnant un véhicule voisin qui maintient la communication de données la plus longue avec le nœud source. MMGPSR élimine également le problème de maximum local en calculant l'angle minimum entre la source et les véhicules voisins, le nœud voisin avec un angle minimum sera sélectionné comme prochain saut.

Weight Aware GPSR (WAGPSR)

Contrairement au protocole GPSR qui sélectionne le nœud le plus proche de la destination comme prochain saut, WAGPSR choisit le véhicule le plus adéquat comme prochain saut en prenant en compte plusieurs mesures de routage par attribution des pondérations et calcule du poids pour chaque noeud voisin afin d'offrir une qualité de service (QoS) supérieure [12].

Tout d'abord, il détermine la zone de communication efficace dans laquelle il sélectionne le prochain saut parmi les voisins qui se trouvent dans cette zone, comme le montre la figure I.7. Cette zone est l'intersection de cercle centré en S de rayon équivalent à la portée de transmission et le cercle centré en D de rayon D_{max}. On note que $D_{max} = D_a + \lambda D_b$, tel que D_a et D_b représente respectivement la distance entre D et le voisin de S le plus proche de D appelé R,

et entre S et R. Tant que pour λ , il prend des valeurs entre 0 et 1, généralement pris égale à 0.3.

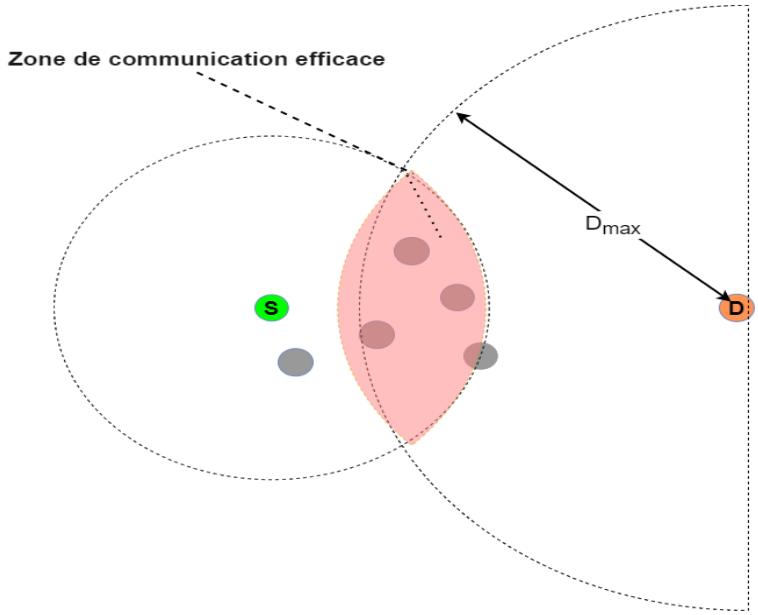


Figure I.7: Choix des voisins selon WAGPSR

Ensuite, un poids W est calculé pour chaque voisin selon la formule suivante :

$$weight_v = w_1 \times LLT_s + w_2 \times T_i + w_3 \times Density_v + w_4 \times \frac{1}{Mob_v}$$

où:

- **LLTs:** est la durée de vie du lien, qui représente le temps restant jusqu'à ce que l'un des nœuds quitte la portée de communication.
- **Ti:** représente le temps de communication cumulé, il construit un chemin stable et évite les reconstructions fréquentes du routage dues aux changements de position des nœuds en Greedy Forwarding.
- $Density_v$**:** indique la densité de nœuds autour de la source. Le nœud direct ayant la densité de trafic la plus élevée est choisi et calculé comme suit :

$$Density_v = \frac{Nombredevoisins}{RangdeTransmission}$$

- Mob_v**:** indique la différence de vitesse entre deux nœuds, moins elle est grande, plus ils restent dans la zone de communication l'un de l'autre. La mobilité des nœuds v et s est calculée comme suit :

$$Mob_v == |vitesse_s - vitesse_v|$$

- w1,w2,w3 et w3 sont des constantes de pondération, leur somme est égale à 1.

Finalement, le voisin avec le poids le plus élevé est sélectionné comme prochain saut.

Protocoles basés sur la topologie

Dans le routage basé sur la topologie, chaque nœud du réseau partage sa table de routage avec d'autres nœuds. Cela augmente la surcharge des paquets ainsi que le délai de bout en bout (E2E). Par conséquent, il a de bonnes performances dans un petit réseau. Cependant, le protocole de routage basé sur la position est approprié pour un réseau dynamique et mobile comme VANET[10].

Ad hoc On Demand Distance Vector (AODV)

Le protocole de routage AODV a été originalement développé pour les MANETs. Lorsqu'un noeud veut débuter une transmission, AODV diffuse un paquet de découverte en mode broadcast, ensuite la destination utilisera le chemin suivi par le paquet de découverte qui l'a atteint pour envoyer un paquet réponse afin d'annoncer ce chemin à la source. L'envoi de données peut alors commencer. En cas de disparition d'un lien sur le chemin choisi, un paquet d'erreur est généré. Le routage à l'aide d'AODV est effectué principalement par deux processus :

- **La découverte de routes:** Le processus de découverte de route commence lorsqu'un nœud source ne dispose pas d'informations de routage concernant le noeud destinataire. La découverte de route est initiée par la diffusion d'un message (Route Request RREQ). Si un voisin a une route vers la destination, il répond à la requête avec un paquet de réponse (Route Reply RREP); sinon, les voisins rediffusent le paquet RREQ. Enfin, certains

paquets de requête atteignent la destination. La route est établie lorsqu'un message RREP est reçu. Un nœud source peut recevoir plusieurs messages RREP avec différentes routes [13].

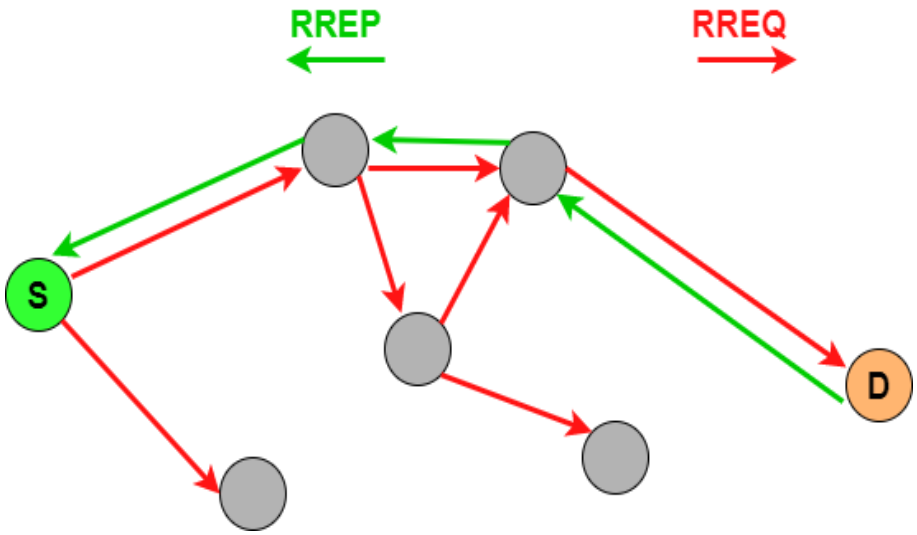


Figure I.8: Découverte de route par le protocole AODV

- **La maintenance de routes:** Le processus de maintenance de route est effectué en cas de rupture de lien. Comme les nœuds du réseau sont en mouvement, le lien peut se rompre. Si un nœud ne reçoit pas de message HELLO de l'un de ses voisins pendant une durée spécifique appelée intervalle HELLO, le nœud détectera une rupture de lien et retire ce dernier de sa table de routage. Le message (Route Error Message RERR) sera générés pour informer les autres nœuds de cette rupture de lien [13].

Fitness Based Ad hoc On Demand Distance Vector (FBAODV)

FBAODV est un protocole basé sur AODV, il a été proposé avec le nouveau calcul de l'indication de la force du signal reçu ainsi que les étapes normales trouvées dans l'AODV. La raison de l'utilisation de ce protocole est qu'il ne collecte qu'une quantité limitée d'informations, il est divisé en quatre étapes : formation du réseau, découverte du voisin, estimation de la fonction de fitness, processus de routage.

- Formation du réseau : le nombre variable de nœuds sans fil (véhicules) forment le réseau,

les points d'accès et les passerelles fixes autour du bord de la route assurent l'établissement de la connectivité entre les nœuds mobiles, le mouvement des véhicules peut modifier la topologie du réseau.

- Découverte de voisin : pour initier la découverte de route, le nœud source n diffuse la requête de route (RREQ) sur les nœuds voisins. Le nœud qui reçoit la demande est classé en deux types : nœuds de destination ou nœud intermédiaire. Lorsque le nœud intermédiaire reçoit la demande, il transmet la réponse de route (RREP) au nœud source. S'il ne reçoit pas de message d'accueil pendant une certaine période, la rupture de lien impliquée ci-dessus peut être détectée.

- Estimation de la fonction de fitness : FBAODV calcule la meilleure route en se basant sur les métriques de la QoS.

- Processus de routage : le processus de routage peut être activé après évaluation de la QoS. Sur la base des mesures de QoS, les meilleurs chemins de routage disponibles dans le réseau sont estimés, la QoS maximale établit la transmission de données.

Destination Sequence-Distance Vector (DSDV)

Il utilise un algorithme basé sur le vecteur de distance afin de trouver le meilleur chemin du noeud source vers le noeud destinataire. La mise à jour des tables se fait en fonction du temps (de façon périodique grâce à des timers), ou en fonction d'événement (mauvais débit de connexion, délais trop élevés,..) Chaque nœud possède en permanence dans sa table de routage le chemin le plus récent découvert vers chaque nœud du réseau. Parmi plusieurs chemins possibles, DSDV privilégie le chemin le plus court.

Protocoles de routage basé SDN

Récemment, avec l'évolution exponentielle du SDN (Software Defined Network), les méthodes de routage basées sur le SDN ont suscité une grande attention pour concevoir un protocole de routage basé sur l'infrastructure dans VANET [14] nommé Software Defined Vehicular Net-

work (SDVN). Ces méthodes fonctionnent très bien dans les réseaux à grande topologie et aident à basculer le flux de données entre les réseaux filaires et sans fil.

Les véhicules mettent à jour en permanence leurs informations comme l'emplacements et la vitesse au niveau d'un contrôleur SDN, ainsi, ce dernier aura une vue globale sur l'ensemble du réseau. Lorsque un noeud veut emmètre un trafic, il consulte le contrôleur au sujet de trouver une route disponible pour la transmission. Le contrôleur utilise une application de routage pour calculer l'itinéraire et insérer des règles de transfert dans son tableau des flux [15].

Dans [16], ils ont proposé une approche méta-heuristique améliorée : une variante de Jaya, cette approche présente un modèle de coût comme solution au problème de routage, en considérant les métriques de qualité du réseau, y compris la congestion, les déplacements, les collisions et le coût de la QoS. La fuzzification du facteur QoS est également incluse dans ce coût total de routage. De plus, l'objectif principal de cette approche se concentre sur la minimisation du modèle de coût de routage en trouvant la route optimale à l'aide de Mean Computing Jaya Algorithm.

Dans [17], chahal et al ont proposé une méthode de routage basée sur le SDN qui minimise la défaillance de la liaison en utilisant les unités routières (RSU), qui sont connectées au réseau basé sur le SDN. Le RSU agit comme un contrôleur avec certains commutateurs spéciaux sélectionnés, ce qui a en fait minimisé la latence.

Dans [18], l'auteur a proposé une nouvelle architecture VANET hiérarchique 5G de nouvelle génération qui intègre la centralisation et la flexibilité de SDN et Cloud-RAN (CRAN), avec les technologies de communication 5G, pour allouer efficacement les ressources avec une vue globale du réseau. De plus, un cadre de calcul de brouillard de bord a été proposé afin d'éviter les transferts fréquents entre les RSU et les véhicules.

Les SDN se sont avérés être l'une des meilleures solutions de gestion des réseaux filaires, ce succès a commencé à s'étendre vers les réseaux sans fil et plusieurs applications sur les VANET

ont montré d'excellentes performances et résolu de nombreux problèmes.

I.4. Conclusion

Dans ce chapitre nous avons donné une vue global sur les réseaux VANET, leurs caractéristiques et application, ensuite on a présenté les modes et les standards de communication ainsi que les différents types d'attaques dans les réseaux VANET, finalement, une vue sur quelques protocoles de routage utilisé dans les réseaux véhiculaires.

Dans le prochain chapitre, nous allons discuter le concept de système de suivi des véhicules Mc-track, après nous introduiront la problématique traitée par ce présent mémoire.

CHAPITRE II

CONCEPTION

II.1. Introduction

Les réseaux véhiculaires sont confrontés à des failles de sécurité, plusieurs systèmes ont été proposé afin d'assurer la sécurisation des données, parmi ces systèmes, on trouve *Mc-Track*, un nouveau système de suivi des véhicules basé sur le cloud et orienté données sécurisées. *Mc-Track* est une approche adaptative qui consiste à prédire la sensibilité des données et le niveau de sécurité à l'aide de l'apprentissage automatique.*Mc-Track* fourni un cryptage sélectif et une sécurité adaptative via l'autorité de suivi (Tracking Authority TA), à l'aide du classificateur d'apprentissage automatique *k-Nearest Neighbours (k-NN)*. Pour assurer la sécurité des informations véhiculaires, ce système fournit une architecture à trois niveaux composée de : service Cloud, les nœuds véhiculaires et des proxys appelés Tracking Authorities, chargées d'effectuer le chiffrement basé sur les attributs (ABE)[19]. Cette approche proposé décrive que la partie sécurité mais elle n'a pas pris en considération la QoS, hors que cette dernière joue un rôle important pour assurer plus de fiabilité.

Dans ce chapitre nous présenterons l'architecture de système de suivi véhiculaire *Mc-Track* et détaillerons son fonctionnement, par la suite, nous allons introduire et traiter la problématique relative à ce dernier. Finalement, nous exposerons notre contribution en proposant une formulation algébrique à cette problématique qui mènera à l'obtention d'une solution optimale.

II.2. *Présentation de Mc-Track*

MC track est un nouveau système de suivi des véhicules orienté données sécurisées basé sur le cloud, qui consiste à prédire la sensibilité des données et le niveau de sécurité à l'aide de l'apprentissage automatique, dans le but d'assurer la sécurité des informations transmises dans le réseau VANET [19].

Architecture de *Mc-Track*

Le système *Mc-Track* fournit un système à trois niveaux de sécurisation des informations véhiculaires, composé de :

1. **Service Cloud:** il stocke en toute sécurité les informations des véhicules. Ces informations sont composées de deux types : les informations de suivi en temps réel et l'abonnement des véhicules.

2. **Les proxys:** ils sont appelés *Tracking Authorities (TA*), leur rôle est de transmettre les informations de suivi collectées à partir des véhicules vers le service cloud sous une forme cryptée à l'aide du cryptage basé sur les attributs (Attribute-based encryption ABE), selon le niveau de sécurité de l'information. En outre, la TA autorise aux véhicules mobiles de s'abonner au service de suivi et sauvegarde un index d'abonnement au service. Cet index est utilisé par la TA pour répondre à une demande de vérification depuis un terminal mobile de vérification (Mobile Verification Terminal MVT). *Mc-Track* utilise une autorité de certification (CA) pour fournir des certificats aux entités de système.

3. **Les Véhicules Mobiles (MV):** ils représentent les clients de service *Mc-Track*, ils envoient des informations de suivi vers le cloud à travers le réseau VANET.

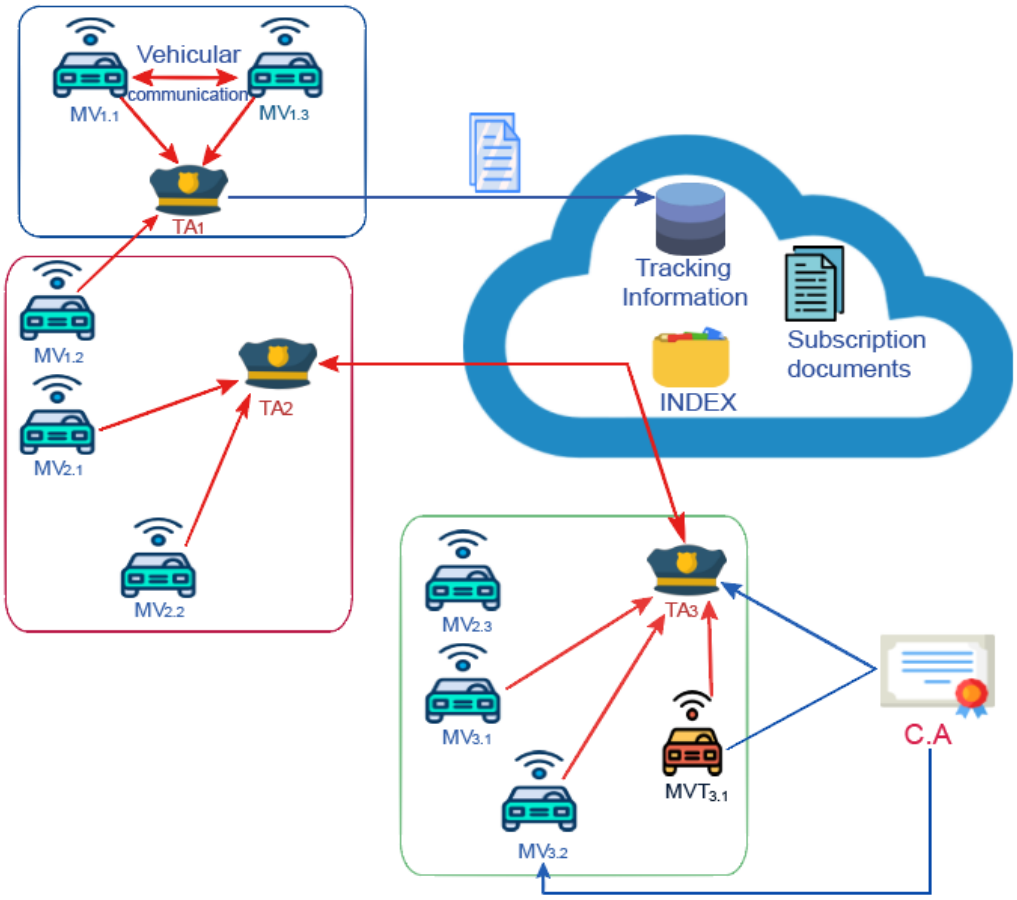


Figure II.1: Architecture de Mc-Track

Collection des informations de suivi

Les informations de suivi des véhicules sont transmises depuis les véhicules vers l'autorité de suivi(TA), pour assurer la sécurité d'une telle transmission dans le réseau véhiculaire, le système *Mc-Track* propose un protocole de sécurité en préservant la confidentialité et l'intégrité des informations de suivi. Dans une telle transmission, un paquet est construit contenant : la signature, le message et l'identifiant du véhicule. Les informations et les message de données sont cryptés à l'aide de la clé publique de TA[19].

Filtrage des informations de suivi: Pour filtrer les informations de suivi reçues, la TA vérifie leur intégrité. Lorsque les données atteignent l'autorité de suivi Ta, elle vérifie leur signature associée. Si la signature correspond aux données reçues, les informations sont déchiffrées à

l'aide de la clé privée de TA, sinon les données reçues sont ignorées. En utilisant le chiffrement ABE, l'autorité de suivi crypte les informations de suivi pour stocker les données dans le service cloud[19].

Suivi de la récupération des informations avec contrôle d'accès: Le service cloud stocke les informations de suivi reçues de plusieurs autorités de suivi. Ces informations sont cryptées selon une politique de contrôle d'accès spécifique, en utilisant le cryptage ABE des autorités de suivi. Un utilisateur doit s'inscrire auprès de l'autorité de suivi correspondante pour pouvoir lui accéder. Quand l'utilisateur se connecte au TA, cette dernière lui générera une clé ABE ku. Afin d'effectuer une recherche sur les informations de suivi, un utilisateur envoie une requête de suivi au service cloud, contenant ses clés ABE. Le service cloud utilise ces clés pour déchiffrer les informations de suivi conformes aux politiques d'accès définies par Autorités de suivi. Chaque autorité de suivi du système souscrit au service cloud en lui envoyant les paramètres ABE nécessaires pour effectuer des opérations de déchiffrement. Pour effectuer une requête de suivi, l'utilisateur associera ses clés ABE à sa requête. Le service cloud renverra aux utilisateurs, uniquement les informations de suivi qui respecte les politiques de contrôle d'accès définies par les autorités de suivi [19]

Abonnements des véhicules: Les Véhicules Mobiles peuvent souscrire au service de suivi via les autorités de suivi(TA). La TA génère le document d'abonnement des véhicules mobiles crypté à l'aide des paramètres globaux ABE obtenus auprès de l'Autorité de Certification CA. Le service cloud met à jour l'index des abonnements en indiquant pour chaque abonnement l'identifiant de son document d'abonnement. L'autorité de suivi crypte l'identifiant du document (emplacement) à l'aide du cryptage basé sur les attributs (ABE) et invoque l'autorité de certification (CA) pour obtenir un code HMAC correspondant à l'identifiant du véhicule. L'autorité de suivi joint l'entrée d'index sécurisé au document d'abonnement, de sorte que le service Cloud mettra à jour l'index des abonnements lors de la réception de chaque document d'abonnement. Ces mises à jour sont transmises, de sorte que les autorités de suivi détiennent

la même copie de l'index. Un QR code (Quick Response code) de l'abonnement est envoyé au Véhicule Mobile[19].

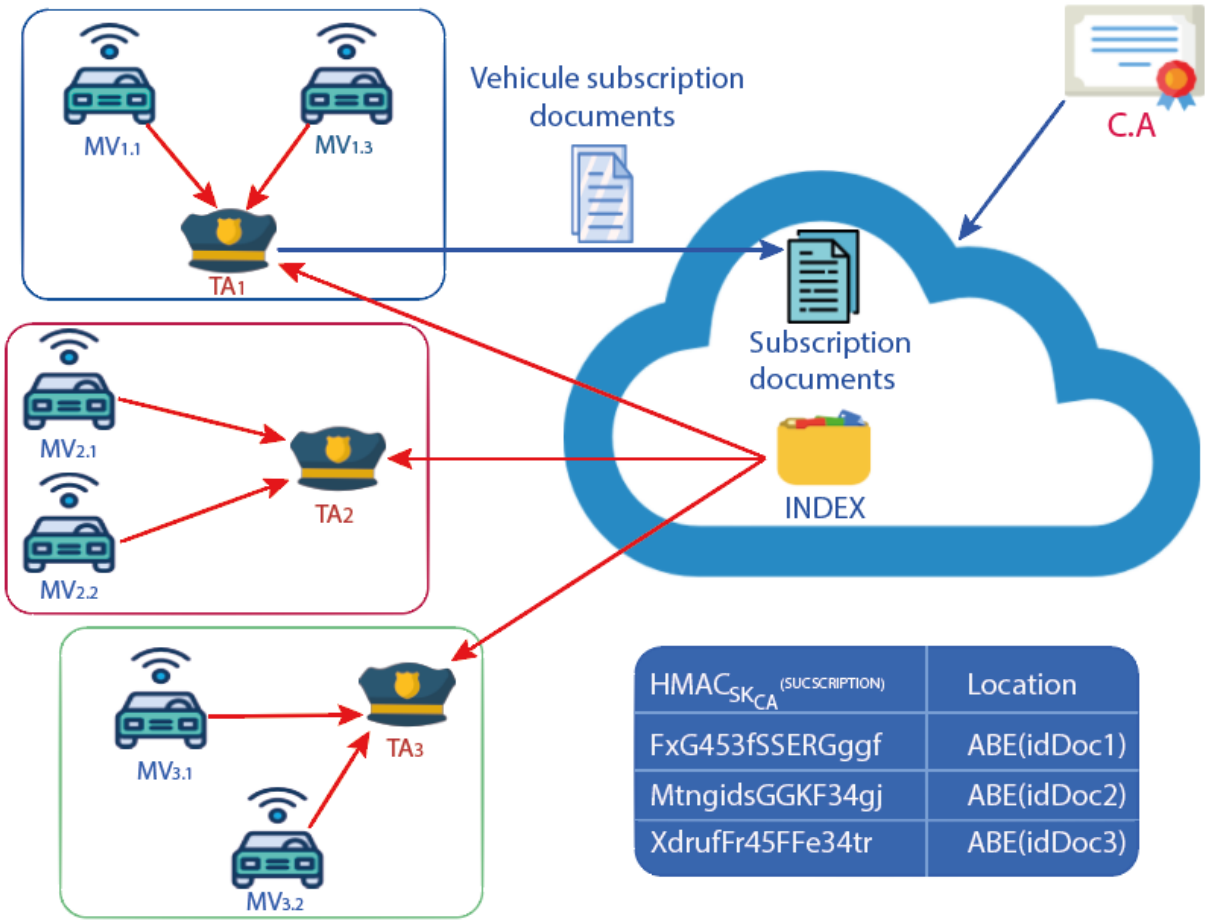


Figure II.2: Abonnements des véhicules

Vérification des véhicules: Le système *Mc-Track* fournit un mécanisme de vérification pour les terminaux mobiles de vérification (MVT). Les MVT extraient le code HMAC de l'abonnement, puis utilisent ce code pour aller chercher l'identifiant du document d'abonnement auprès de l'autorité de suivi, enfin les MVT déchiffrent le document stocké dans le cloud à l'aide de clé ABE[19].

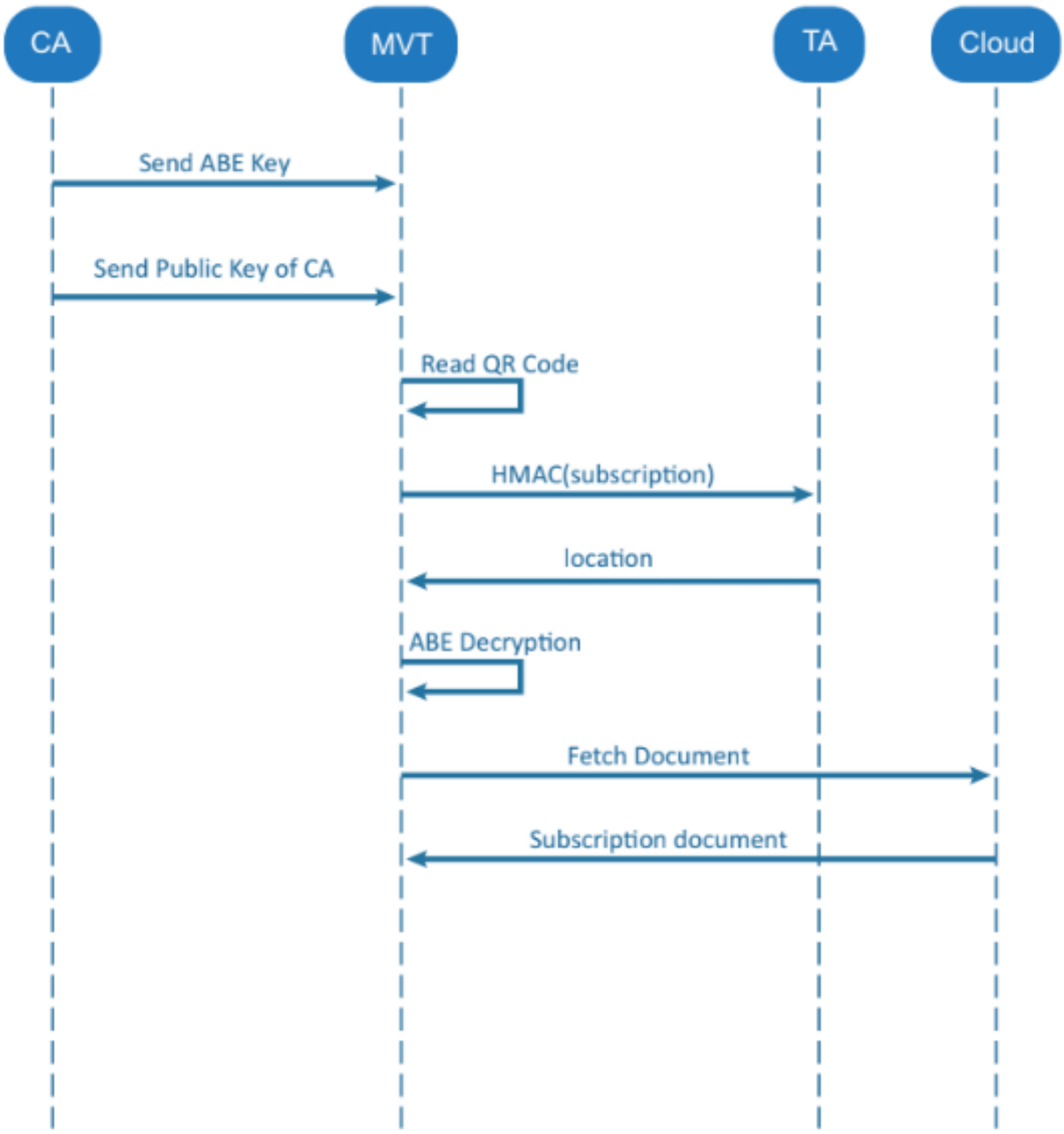


Figure II.3: Abonnements des véhicules

Chiffrement sélectif et sécurité adaptative

Le chiffrement sélectif dans le système *Mc-Track* consiste à utiliser un classificateur d'apprentissage automatique, de sorte que seules les données classées comme sensibles sont chiffrées. L'autorité de Suivi(TA) utilise une classification binaire afin de déterminer la classe des données reçues

: données sensibles ou non sensibles. À l'aide de la classification d'apprentissage automatique Tracking Authority, extrayez le niveau de sécurité, en utilisant les caractéristiques du message (Temps de réception: Trecep, Taille de message: sizemsg, Identifiant de l'expéditeur: numsendr). L'Autorité de suivi choisira la politique de chiffrement appropriée en fonction du niveau de sensibilité[19].

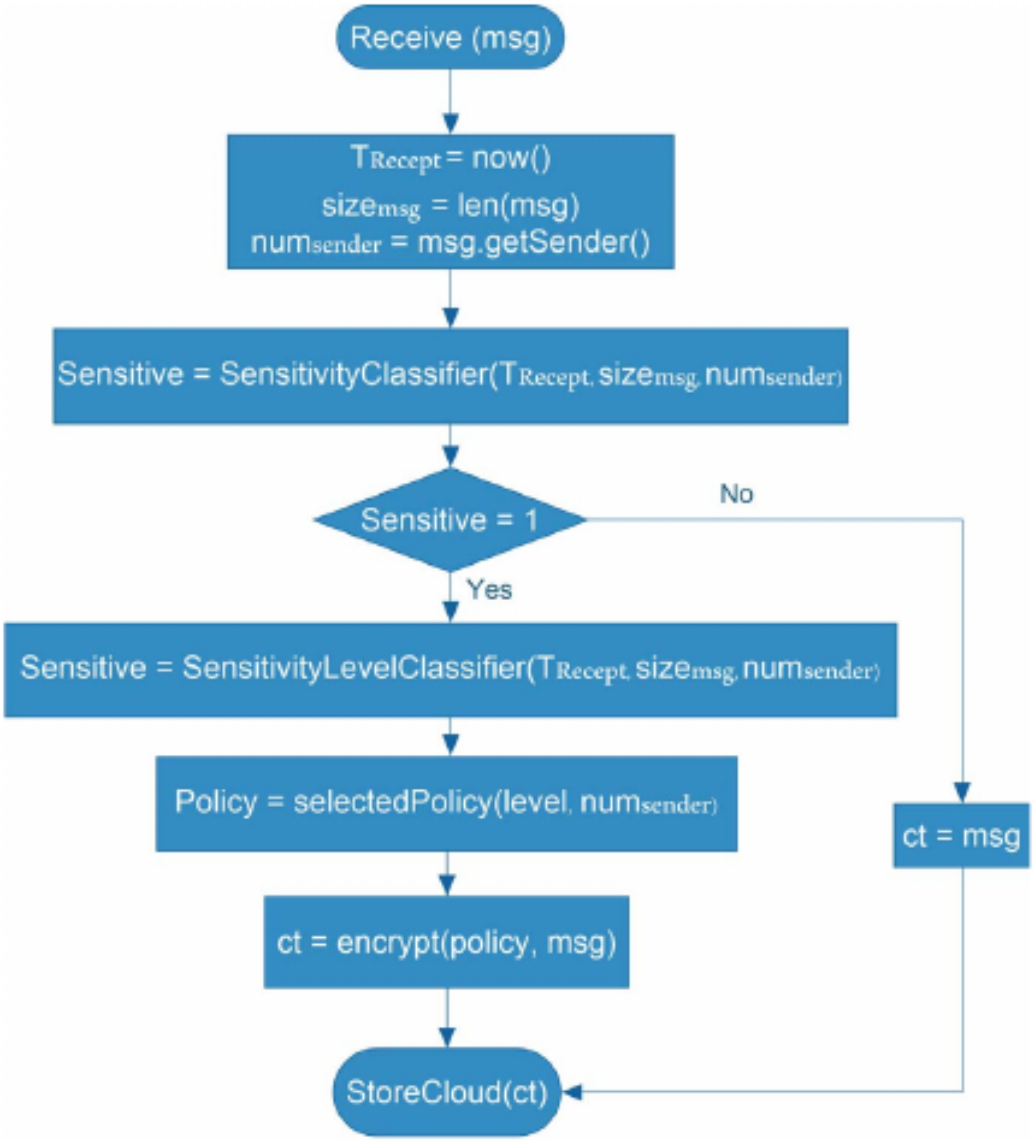


Figure II.4: Chiffrement sélectif et sécurité adaptative

II.3. Formulation du problème

Le système Mc-Track n'as pas pris en considération la qualité de service qui est d'une grande importance pour les systèmes assurant la sécurité des données. La QoS est essentiellement liée au mécanisme de routage utilisé pour la communication. Lors de la transmission des paquets à partir des sources vers les destinations dans un réseau véhiculaire, les protocoles de routage communs calculent la route ou bien le prochain saut séparément pour chaque paquet ou ensemble de paquets selon des algorithmes propre à chaque protocole. Cela peut créé plusieurs problèmes, par exemple dans un réseau à faible mobilité, les même noeuds seront réutilisés à chaque fois pour l'acheminement de trafic, donc cela consommera la bande passante disponible des liens formés entre ces noeuds, en revanche augmenter la perte de paquets. Ce choix indépendant des routes pour chaque paquets augmente considérablement le nombre de noeuds utilisés. Une régulation sur le transfert de trafic entre les noeuds de réseau est aussi nécessaire pour une exploitation meilleure de la bande passante et éviter les congestions. cela augmente considérablement le nombre de noeud utilisés, mais aussi le retard, et la perte de paquet qui est du sois à la rupture de lien de communication ou la saturation de la bande passante.

II.4. Modélisation du problème

Dans ce qui suit, nous décrivons la solution d'optimisation basée sur l'algorithme MHR. Pour tout u $\in S \cup O$ et v $\in O \cup T$, nous définissons les variables suivantes. Pour chaque Autorité de suivi t $\in$ T, on définit une matrice F^s de variables entières qui représente le trafic généré et transmis à cette T. Chaque élément $F^s_{i,j}$ représente le nombre de flux qui doivent être transmis de i à j, où i $\in S \cup O$ et j $\in O \cup T$.

variable	**Description**
S	l'ensemble des véhicules sources envoyant des données aux autorités de suivi T.
O	l'ensemble des nœuds du réseau à l'exclusion des sources et autorités de suivi.
T	l'ensemble des autorités de suivi dans le réseau
O_r	Le noeud voisin le plus proche de la destination
S_t	une variable contenant pour chaque autorité de suivi t (t ∈ T), l'ensemble des sources communiquant avec t.
$\|S_t\|$	la cardinalité de S_t
G(V,E,W)	Le graphe qui montre la topologie du réseau, où $V = S \cup O \cup T$, E désigne l'ensemble des arêtes, W désigne la bande passante de communication entre les différents nœuds de V et $w_{i,j}$∈ W désigne la capacité de bande passante entre i, j ∈ V.
Q	C'est une surface qui est définie comme la zone de communication efficace contenant les voisins optimaux
$X_{i,j}$	Une variable booléenne de décision qui indique si un nœud i sélectionne j comme parent pour transférer le trafic de S à T. $X_{i,j} = \begin{cases} 1 : \text{si i sélectionnez j comme parent pour lui envoyer du trafic} \\ 0 : \text{si non} \end{cases}$
$P_{i,j}$	Une variable booléenne de décision qui indique si un nœud j se trouve dans la zone de communication efficace Q. $P_{i,j} = \begin{cases} 1 : \text{si j appartient à Q} \\ 0 : \text{si non} \end{cases}$
$T_{i,j}$	Une variable réel représentant la quantité de trafic qui sera transmise de i vers j.
$\eta(u)$	Une fonction qui renvoie les voisins du nœud u dans le graphe G.
$\eta'(u)$	Une fonction qui renvoie les voisins du nœud u qui se trouve dans Q. $\forall u \in S \cup O \cup T, \forall j \in \eta(u) : \eta'(u) = P_{u,j} \times \eta(u)$
$F^t_{i,j}$	Une variable entière positive, représentant le nombre de flux qui doivent être transmis de i à j, elle imite le flux de paquets généré à partir de différentes sources vers les autorités de suivi T.
Y_i	Variable booléenne de décision qui indique si un noeud $o \in O$ est sélectionné ou non pour transférer le trafic: $y_i = \begin{cases} 1 : \text{si le noeud i est choisi pour transférer le trafic} \\ 0 : \text{sinon} \end{cases}$
R_s	La portée de transmission du véhicule source
D_1	Distance entre le noeud O_r et la destination
D_2	Distance entre le noeud O_r et la source
$D_{i,j}$	distance entre le noeud i et j.

Table II.1: Tableaux des Variables

- **La fonction Objective :**

$$\min \sum_{\forall i \in O} y_i \tag{II.1}$$

- **Contraintes:**

$$\forall i \in S \sum_{\forall j \in \eta'(i)} X_{i,j} = 1 \tag{II.2}$$

$$\forall i \in O, \forall j \in \eta(i) \cap (O \cup T) : X_{i,j} \leq y_i \tag{II.3}$$

$$\forall i \in O, \forall j \in \eta(i) \cap (O \cup S) : X_{j,i} \leq y_i \tag{II.4}$$

$$\forall i \in S, \forall j \in \eta'(i) : T_{i,j} = \sum_{\forall t \in T} d_i^t \times X_{i,j} \tag{II.5}$$

$$\forall i \in O : \sum_{j \in \eta'(i) \cap (S \cup O)} T_{j,i} = \sum_{j \in \eta'(i) \cap (O \cup T)} T_{i,j} \tag{II.6}$$

$$\forall i \in S \cup O, \forall j \in \eta'(i) \cap (O \cup T) : T_{i,j} \leq W_{i,j} \times X_{i,j} \tag{II.7}$$

$$\forall i \in T \sum_{\forall j \in \eta'(i)} F_{i,j}^i = |S_i| \tag{II.8}$$

$$\forall t \in T, \forall i \in S_t : \sum_{\forall j \in \eta'(i)} F_{i,j}^t = 1 \tag{II.9}$$

$$\forall i \in O, \forall t \in T : \sum_{j \in \eta(i) \cap (S \cup O)} F_{j,i}^t = \sum_{j \in \eta(i) \cap (O \cup T)} F_{i,j}^t \tag{II.10}$$

$$\forall i \in S \cup O, \forall j \in O \cup T : F_{i,j}^{t} \leq |S_t| \times X_{i,j} \tag{II.11}$$

$$\forall j \in \eta'(i) : D_{i,j} < R_s \tag{II.12}$$

- Dans la fonction objective II.1, nous visons à minimiser le nombre de nœuds utilisés pour le transfert de trafic, c'est à dire minimiser la longueur de tous les chemins de routage entre les sources et les *TAs*.

- Contrainte II.2 garantit que chaque nœud source se connecte à un seul nœud relais.

- Les contraintes II.3 et II.4 garantissent que seuls les noeuds actifs c'est à dire les véhicules équipés d'un dispositif de transmission sans fil en état de marche participent au routage du trafic.

- La contrainte II.5 représente le trafic généré par les sources S qui doit être router vers les Autorités de Suivi T.

- Contrainte II.6 garantit que tout le trafic reçu par un nœud, provenant de ses voisins $\eta(i)$ ou source doit être égal au trafic de sortie émis par ce nœud.

- Contrainte II.7 garantit que le trafic acheminé d'un nœud (nœud source ou relais) vers un autre nœud (nœud relais ou T) ne doit pas dépasser la capacité du lien qui inter-connecte ces deux nœuds. Pour i ∈ S, le trafic généré par le client i ne doit pas dépasser la capacité de liaison entre cette source et le nœud relais. De même, pour i ∈ O, le trafic agrégé transmis d'un nœud relais i à son le successeur j ne doit pas dépasser la capacité de ce lien.

- Les contraintes II.8, II.9 et II.10 garantissent que la connectivité entre les sources et leurs autorités de trafic respectives est établie sans aucune boucle de routage.

- La contrainte II.8 garantit que le nombre de flux arrivant à une autorité de suivi t est

égal au nombre de requêtes des sources.

- La contrainte II.9 garantit qu'un seul flux doit être créé entre une source et son autorité de suivi choisi t.

- La contrainte II.10 garantit que le nombre de flux entrants vers un nœud est exactement égal au nombre de flux sortants. Cette contrainte permet d'assurer la connectivité et d'empêcher la création de boucles de routage.

- La contrainte II.11 force le flux généré d'un véhicule source à être acheminé uniquement dans les chemins configurés tout en évitant les boucles.

- La contrainte II.12 garantit que la distance entre le nœud i et j est inférieure à la portée de communication R_s.

Sélection des noeuds voisins:

Un noeud donné est le voisin d'un autre si ce dernier se trouve dans sa portée de transmission, mais dans notre cas nous les avons divisé en deux type :

1. **Voisin non-optimal:** est un nœud qui se trouve dans la portée de communication de la source, mais son choix comme noeud relais ou bien comme prochain saut peut augmenter le nombre de saut et la longueur de la route pendant le transfert des paquets vers la destination (TA).

2. **Voisin optimal:** est un noeud qui se trouve dans la surface de communication efficace Q, son choix comme prochain saut diminuera la longueur de chemin de routage.

Soit D_1 la distance entre le voisin le plus proche de la destination noté O_r (avec les coordonnées (x_{O_r}, y_{O_r})) et l'autorité de suivi noté TA (avec les coordonnées (x_T, y_T)), D_2 la

distance entre le nœud source S (x_S , y_S) et le nœud O_r.

$$D_1 = \sqrt{(x_D - x_{O_r})^2 + (y_D - y_{O_r})^2} \tag{II.13}$$

$$D_2 = \sqrt{(x_S - x_{O_r})^2 + (y_S - y_{O_r})^2} \tag{II.14}$$

Nous définissons *dmax* par la formule suivante :

$$d_{max} = D_1 + \lambda \times D_2 \tag{II.15}$$

où $\lambda \in [0, 1]$

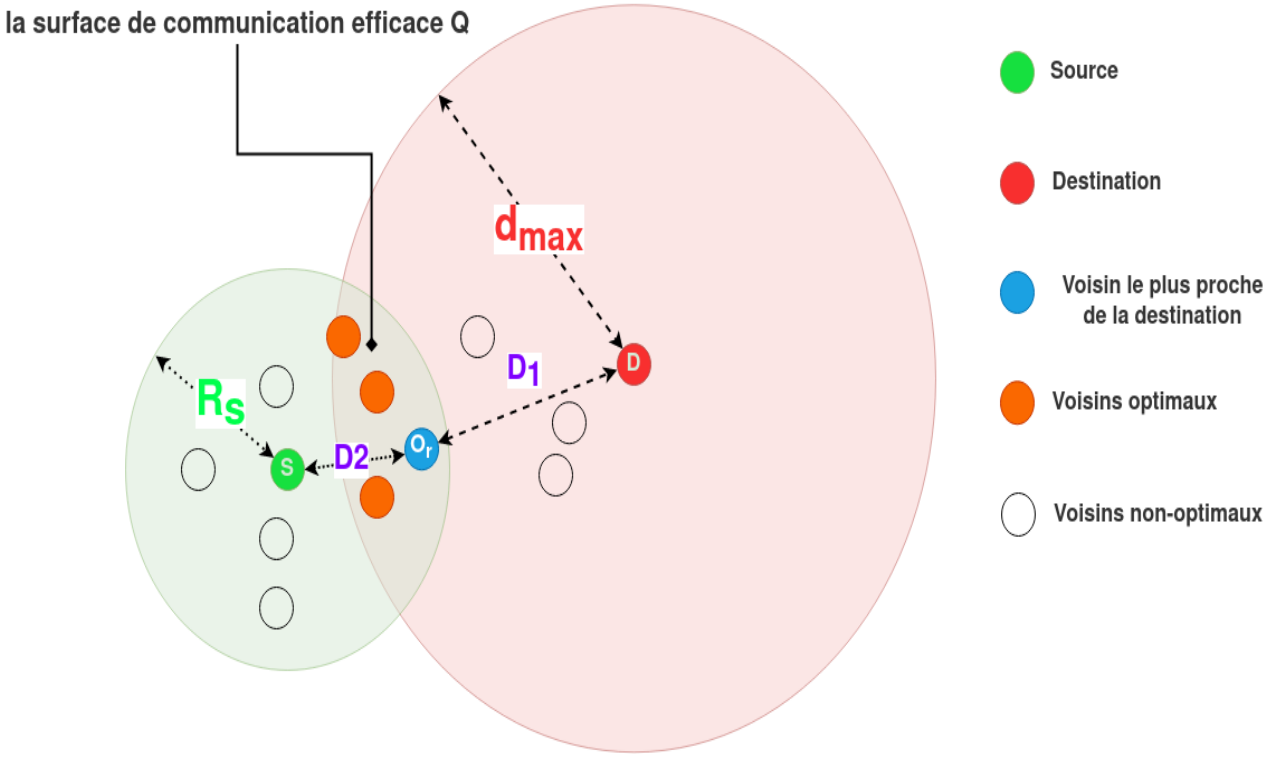


Figure II.5: la sélection des noeuds voisins

- **Surface de communication efficace:** est défini comme la zone où deux cercles se chevauchent, ayant la source S comme centre, R_s comme rayon et D comme centre, d_{max} comme rayon. Cette zone est définie comme la zone de communication effective Q où se trouve les voisins optimaux.

  Dans l'équation ci-dessus II.15, λ contrôle la taille de Q, lorsque λ est plus proche de 1, Q devient plus grand, donc le nœud relais sera plus proche de la source, cela peut augmenter le Délai E2E.

  Lorsque λ est plus proche de 0, cela réduit la taille de Q, par conséquence, le nœud relais sera plus proche de la destination, cela réduit le délai E2E, mais d'un autre côté augmente la perte de paquets car le nœud relais pourrait quitter la portée de communication de la source.

  λ peut être choisi dans la plage [0,2, 0,6] en fonction de la densité du trafic routier, la portée de transmission, la sensibilité des données et si elles tolèrent ou ne tolèrent pas le retard.

  Choix des voisins : les voisins d'un noeud donné sont tout les noeuds qui sont dans sa portée de transmission. Chaque nœud a plusieurs voisins, mais seuls les voisins optimaux (en tenant compte de toutes les sources et TA) sont choisis pour être utilisés dans le calcule de chemin optimal, la figure II.5 montre la méthode de choix des voisins optimaux.

  Choix du prochain saut : le prochain saut est choisi parmi les voisins optimaux appartenant à la surface de communication efficace par considération de toute les sources et Autorités de suivis qui communiquent dans le réseaux, car par cela les sources proches peuvent partager un noeud entre eux, ce qui va minimiser le nombre de noeud utilisé.

Dans le cas ou les voisins optimaux ne sont pas suffisant pour trouver une route, la totalité des voisins seront utilisés.

Calcul du la route:

Après avoir obtenu l'ensemble des voisins de chaque nœud, des informations supplémentaires telles que la bande passante disponible entre les noeuds communiquants sont utilisées par l'algorithme MHR pour calculer le meilleur chemin et allouer une bande passante pour chaque flux de trafic entre les sources et les TA.

Durée de vie de chemin de routage (LLT)

Vu la mobilité des noeuds formant le chemin de routage, le transfert des données peut s'interrompre à tout moment. La durée de vie d'un chemin de routage notée *LLT* (Link Life Time) peut être estimée en utilisant les informations relatives à la position et vitesse des noeuds formant la route.

Vitesse relative V_r: la vitesse relative des nœuds i et j donne une estimation de la durée de connectivité du lien, elle peut être calculée comme suit :

$$|\overrightarrow{\mathrm{V_{r_{i,j}}}}| = \sqrt{V_i^2 + V_j^2 - 2V_iV_j\cos\theta} \tag{II.16}$$

Où V_i et V_j est respectivement la vitesse de noeud i et j, θ est l'angle entre $\overrightarrow{\mathrm{V_i}}$ et $\overrightarrow{\mathrm{V_j}}$.

Connectivité de lien : est la fenêtre temporelle pour laquelle la transmission de données entre deux nœuds est maintenue, elle dépend de la vitesse relative et de la direction des nœuds en mouvement.

Elle représente le temps restant avant que la communication entre deux nœuds soit interrompue par le fait que l'un d'eux ou les deux quittent la portée de communication. La connectivité de lien entre les noeuds i et j est donnée par :

$$T_{L(i,j)} = \frac{R_s - D_L}{V_r} \tag{II.17}$$

Durée de vie de chemin de routage (LLT): Soit les noeuds S, B, C et D, on suppose que S envoie un flux de trafic vers D selon l'itinéraire $S \to B \to C \to D$. Soit $T_{L_{(S,B)}}$, $T_{L_{(B,C)}}$ et

$T_{L_{(C,D)}}$ la connectivité de lien respectivement entre S et B, B et C et entre C et D. La durée de vie de ce chemin de routage est la plus petite connectivité :

$$LLT = min(T_{L_{(S,B)}}, T_{L_{(B,C)}}, T_{L_{(C,D)}}) \tag{II.18}$$

II.5. Conclusion

Dans ce chapitre nous avons exposé l'architecture et le fonctionnement de système de suivi Mc-Track, qui est basé sur l'amélioration de la sécurité dans les réseaux VANET, mais n'a pas pris en considération la qualité de service pour assurer une communication fiable entre ses entités. Cette problématique a été modélisée par un modèle algébrique qui a aussi traité quelques problèmes rencontrés par les protocoles de routages dans les VANETs.

Enfin, La résolution de ce modèle proposé emmènera à trouver un chemin de routage optimal respectant plusieurs contraintes pour assurer une meilleure QoS. Dans le prochain chapitre, nous présenterons les résultats de ce modèle et étudierons ses performances.

CHAPITRE III

ÉTUDE EXPÉRIMENTAL

III.1. Introduction

Afin d'évaluer et valider toute solution proposée pour l'optimisation de la QoS dans les réseaux véhiculaires, la simulation est le moyen le plus idéal pour réaliser cette tâche, puisque elle permet d'effectuer des testes dans des conditions réelles tout en ayant un contrôle total sur les variables environnementales. Elle est largement utilisé non seulement pour son coût réduit et sa facilité d'utilisation, mais aussi parce qu'elle offre la possibilité d'analyser la performance des solutions sous différents scénarios. Pour le déploiement de notre solution, nous avons eu besoin d'utiliser des outils pour simuler la mobilité des noeuds et les interconnexions entre eux dans le réseau.

Dans ce chapitre nous allons présenté l'environnement et le processus de simulation avec ses différentes étapes, ainsi que les résultats et les métriques étudiées, enfin nous allons interpréter les résultats obtenus, suivi d'une étude comparative en terme de performance entre notre solution proposé MHR avec deux autres protocoles de routage basés sur la position: GPSR et MMGPSR.

III.2. Environnement de simulation

Dans les réseaux VANETs, nous distinguons deux types de simulateurs: les simulateurs du trafic routier et les simulateurs réseau. Afin de réaliser la simulation d'un réseau VANET, il est nécessaire d'avoir un modèle de mobilité proche de la réalité d'où le besoin d'utiliser un

simulateur de trafic routier, puis pour évaluer les performances des protocoles de communication on utilisera un simulateur réseau que nous avons développé vu que les simulateurs réseaux existants n'offrent pas la possibilité d'implémenter notre solution d'optimisation proposée , d'où le besoin de développer un nouveau programme qui répond à nos exigences, ce qui a permet d'obtenir et d'estimer certaines paramètres qui décrivent les caractéristiques de notre solution. Pour cela, plusieurs outils ont été utilisé :

- **Open Street Map OSM :** OpenStreetMap est une carte gratuite modifiable du monde entier, construite par des bénévoles en grande partie, publiée avec une licence open source qui permet un accès gratuit aux images cartographiques et à toutes les données cartographiques sous-jacentes. La carte récupérée à partir d'OSM sera utilisée par le module de mobilité pour la génération de trafic routier[20].

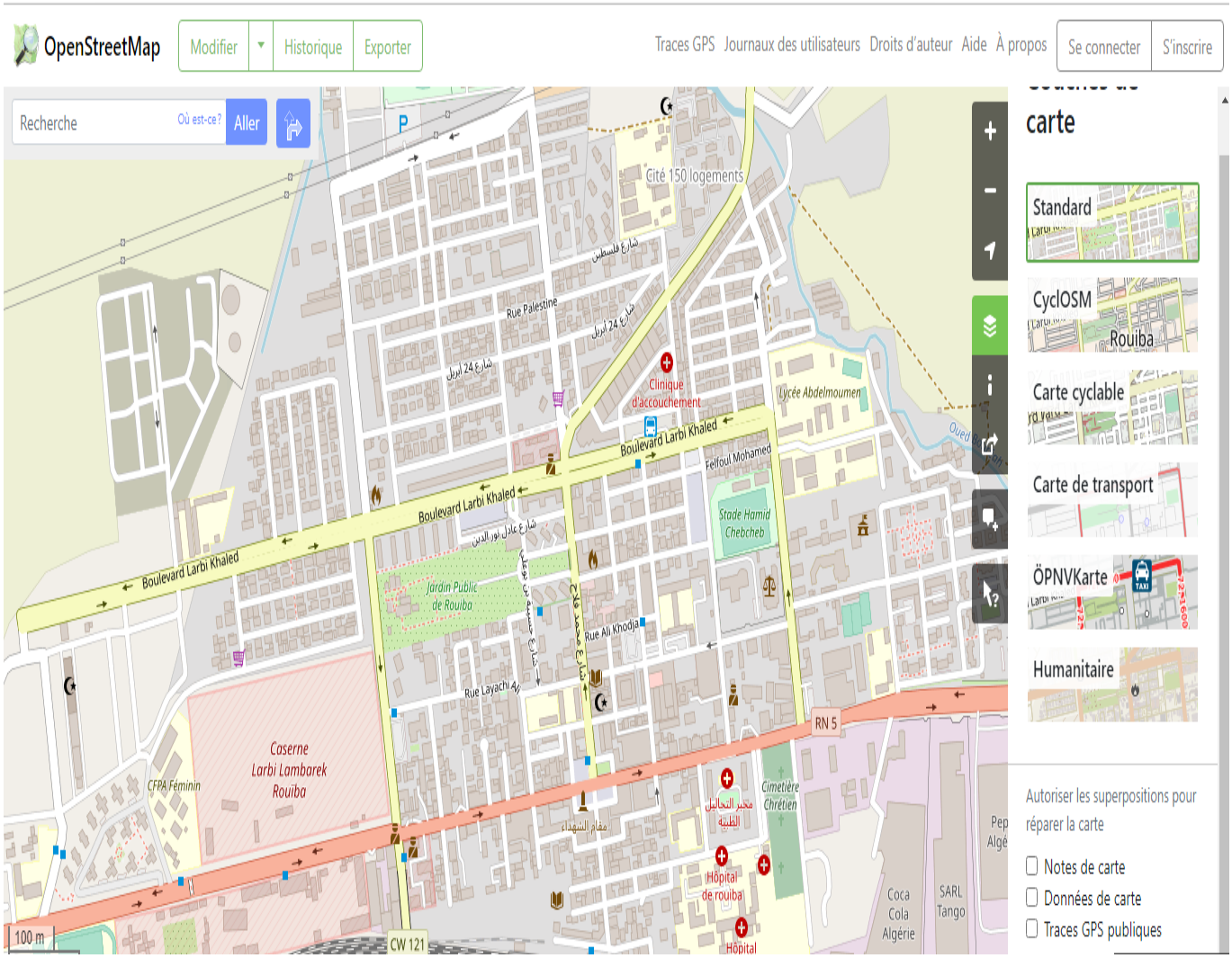


Figure III.1: Site de Open Street Map

- **Simulateur MHR :** est un simulateur à événements discrets que nous avons développé en langage *Python* dans le but d'obtenir les données qui seront utilisées pour le calcule de la solution optimale, l'architecture de simulateur MHR a été développé afin que nous puissions implémenter et tester l'efficacité de notre solution proposée, et la comparer avec d'autres protocoles de routage basés sur la position.

  On peut décomposer l'architecture de ce simulateur en trois partie :

  1. **Module de mobilité:** il offre la possibilité de simuler le trafic routier urbaine dans les villes et autoroutes. Il peut simuler le trafic routier dans n'importe quel endroit en lui donnant comme entrée une carte géographique provenant de Google Earth, Open Street Map,...etc. Les routes sont présentées sous forme de plusieurs voies. Il permet à la fin de récupérer les informations de chaque véhicule tel que la position, la vitesse et les données décrivant la mobilité des noeuds à chaque instant.

  2. **Module réseau:** il est basé sur les évènements discrets, il permet de simuler la transmission des paquets de données dans le réseau selon l'algorithme ou bien le protocole de routage choisi.

  3. **Module d'optimisation:** il représente la partie la plus importante, son rôle est de récupérer les données de simulation comme entrée, les traiter et enfin calculer la solution optimale qui est représentée par les chemins de routage des paquets, les noeuds disponibles qui peuvent être utilisés pour transmettre le trafic et une distribution balancée de ce dernier. A l'aide d'un solveur de pointe pour la programmation mathématique, Le module d'optimisation nous a permis d'énoncer le problème relatif à la QoS sous forme de modèles mathématiques, puis de trouver la meilleure solution parmi plusieurs possibilités en un temps d'exécution très rapide.

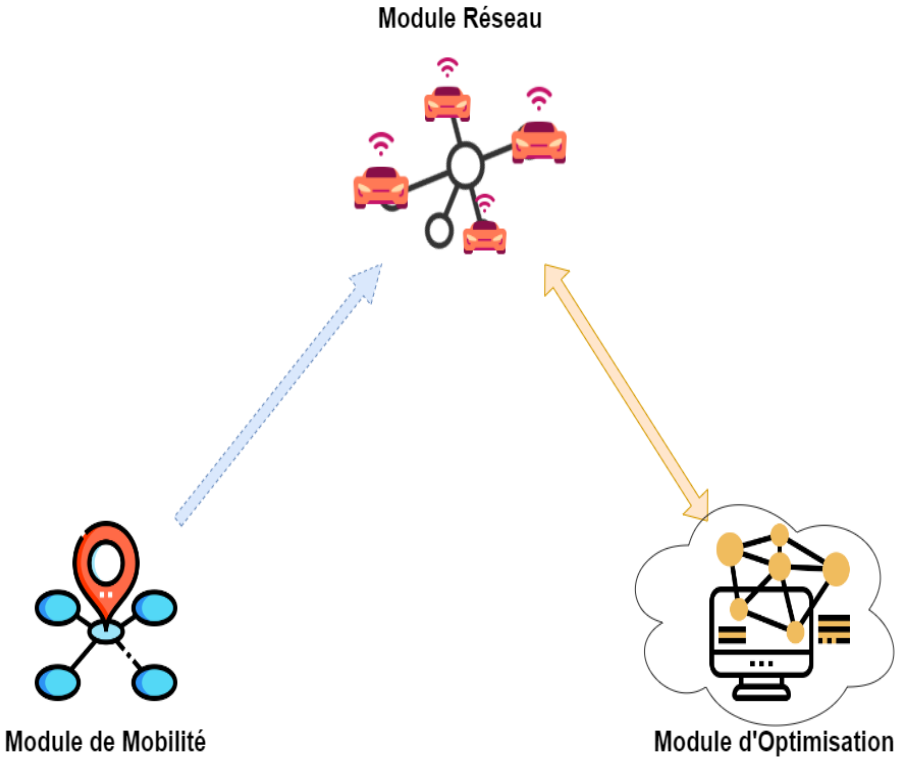


Figure III.2: Architecture de simulateur MHR

III.3. Processus de simulation

Dans cette section nous allons introduire le processus de simulation qui peut se résumer en quatre étapes :

1. Création des noeuds par le module réseau en se basant sur les données de module de mobilité.

2. Configuration des paramètres de simulation, comme les paires sources/destinations, trafic généré par les sources,...

3. Calcule de solution optimale par le module d'optimisation.

4. Extraction des résultats à partir de la solution produite par le module d'optimisation.

la figure suivante III.3 résume les différentes étapes de la simulation:

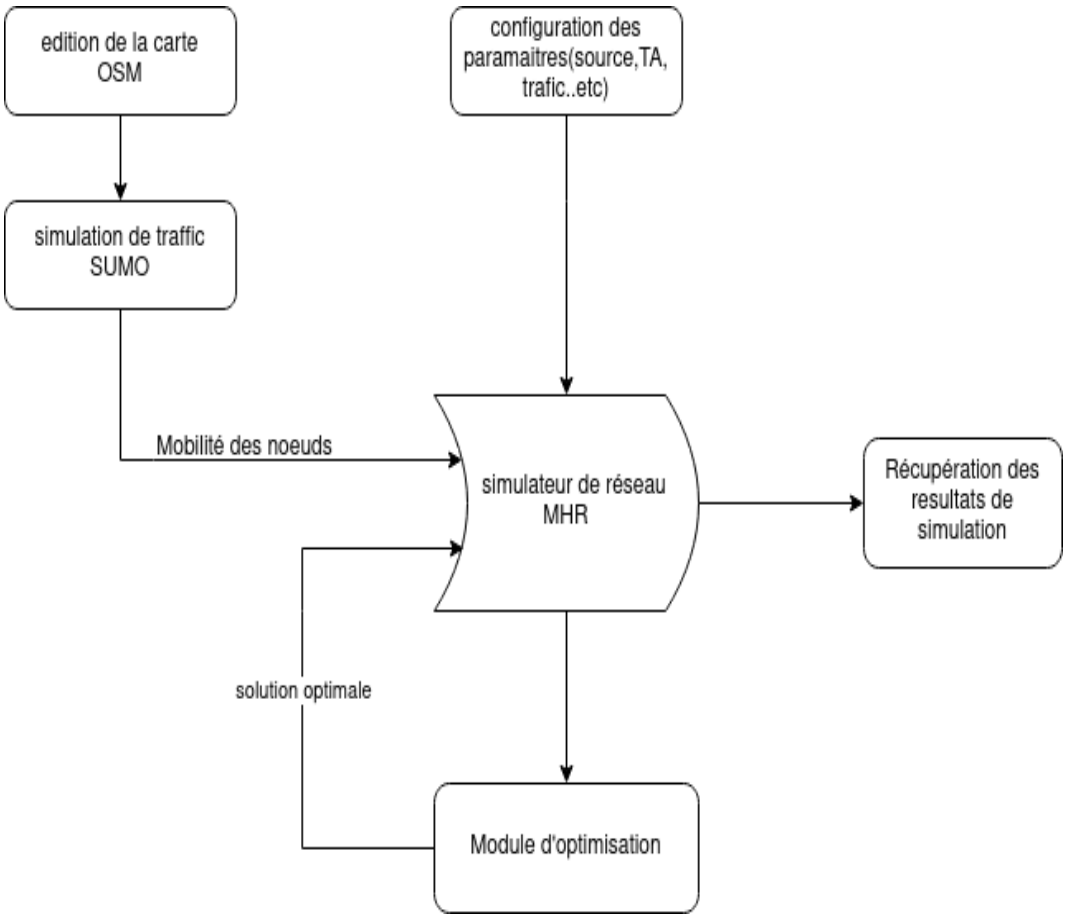


Figure III.3: Processus de simulation de réseau

Génération de la mobilité

Une carte de la ville de Rouiba a été téléchargé à partir de site Open Street Map, les dimensions de la zone choisie sont 2500x2500m^2. Cette carte contient toutes les informations concernant les routes, chemins et autoroutes de cette ville, ces données seront converties en réseau routier.

Ensuite, ce module va générer un ensemble de trajets aléatoires pour le réseau routier en choisissant les bords source et de destination pour chaque véhicule, soit uniformément au hasard, soit avec une distribution modifiée.

Enfin, nous récupérons les informations nécessaires relatives à la mobilité des noeuds de réseau véhiculaire.

Configuration de simulateur MHR

Dans cette partie, nous supposons que chaque véhicule est équipé d'une antenne omnidirectionnelle, la portée de communication est fixée à 300 m, tandis que le débit de données du canal de transmission entre les noeuds voisins est défini à 3 Mb/s. Pour le nombre de véhicules, nous avons utilisé respectivement 50,70,90 et 110 nœuds. Le nombre de paires source/destination varie entre 2 et 20. Le protocole de couche transport utilisé est UDP, on considère que chaque paquet de donnée a une taille de 512 bits. La durée totale de chaque simulation a été fixée à 100 secondes.

Les paramètres de simulation sont résumés dans III.1.

Durée	100 seconds
Nombre de pairs source/Ta	2,6,8,10,15,20
Nombre de noeuds	50,70,90,110
Portée de transmission	300m
Vitesse maximale	30m/s
Superficie	2500x2500 m
Taille de paquet	512 bit
Trafic généré par les sources	512Kb/s
Débit de canal de transmission	3Mb/s

Table III.1: Paramètres de simulation

Le module réseau reçoit les données relatives à la mobilité et génère un ensemble de noeud, chacun porte ses propres informations comme la position, vitesse, direction,... ainsi qu'un identifiant unique. Ensuite, les paires communiquantes (source/TA) sont choisies parmi l'ensemble des noeuds. On a supposé que ces paires génèrent un trafic de 512Kb/s. Enfin, on transmet les données nécessaires au module d'optimisation qui s'occupe de calcule des chemins de routage optimaux, l'équilibrage de charge du trafic (load balancing), les noeuds à utiliser, le temps d'exécution, délai de bout en bout, distribution des flux ...

III.4. Les paramètres et métriques étudiés

Chemin de routage

Le chemin de routage est un paramètre qui définit la liste séquentielle des noeuds intermédiaires par lesquels les paquets de données doivent passer à partir d'une source pour atteindre une destination. C'est l'un des résultats important que le module d'optimisation de MHR peut calculer.

Distribution de trafic des données

L'algorithme MHR calcule non seulement le chemin optimale entre les sources et destinations mais aussi la distribution de trafic entre les noeuds qui forment ce chemin, cela en proposant des régulations sur les différents flux de données générés par les sources.

Délai de bout en bout :

Le retard de bout en bout de chaque paquet est la somme des retards rencontrés au niveau d'une séquence de nœuds intermédiaires sur le chemin de la destination. Chaque délai est la somme de deux parties, une partie fixe telle que le délai de transmission et le délai de propagation et une partie variable telle que le délai de traitement et le délai de mise en file d'attente aux nœuds. Pour un paquet p, le délai de bout en bout est :

$$D_p = Ta_p - Te_p$$

D_p,T_a et T_e représentent respectivement le délai de bout en bout de paquet p, le temps d'émission de paquet par la source et le temps d'arrivée à la destination.

Le délai moyenne est la somme des délai de chaque paquet, divisée sur le nombre de paquets envoyés.

$$D = \frac{1}{N} \sum_{p=1}^{p=N} D_p$$

Ou N représente le nombre total de paquets.

Nombre de noeuds utilisés

Ce paramètres comme son nom l'indique, représente le nombre de noeuds qui ont participé au routage des différents paquets transmis dans le réseau, sans compter les sources et les destinations.

Temps d'exécution

Il est défini comme le temps passé par le module d'optimisation pour l'exécution de l'algorithme MHR et le calcule de la solution optimale.

III.5. Analyse des résultats

Dans cette section nous allons utilisés les métriques citées précédemment pour évaluer les performances de protocole MHR . Pour cela, On applique des différents scénarios que nous allons définir par la suite, suivi des paramètres d'évaluation, puis nous avons interprétés les graphes tracés à partir des résultats collectés lors de la simulation. enfin on fait une comparaison entre notre solution proposer MHR et deux autres protocole basé sur la position: GPSR et MM-GPSR.

Premier scénario

Dans ce scénario, on a fixé le nombre de pairs source/destination pendant qu'on varie le nombre total de noeuds dans le réseau comme montré dans la table III.2.

Durée	100 seconds
Nombre de pairs source/Ta	8
Nombre de noeuds	50,70,90,110
Portée de transmission	400m
Vitesse maximale	30m/s
Superficie	2500x2500 m
Taille de paquet	512 bit

Table III.2: Paramètres de simulation

Nous avons obtenu les résultats représenté dans les figures suivantes :

- **nombre de noeuds utilisés**

  les résultats obtenus (Figure III.4) représente la variation des noeuds utilisé pour la formation des chemins de routage, par rapport à la taille de réseau:

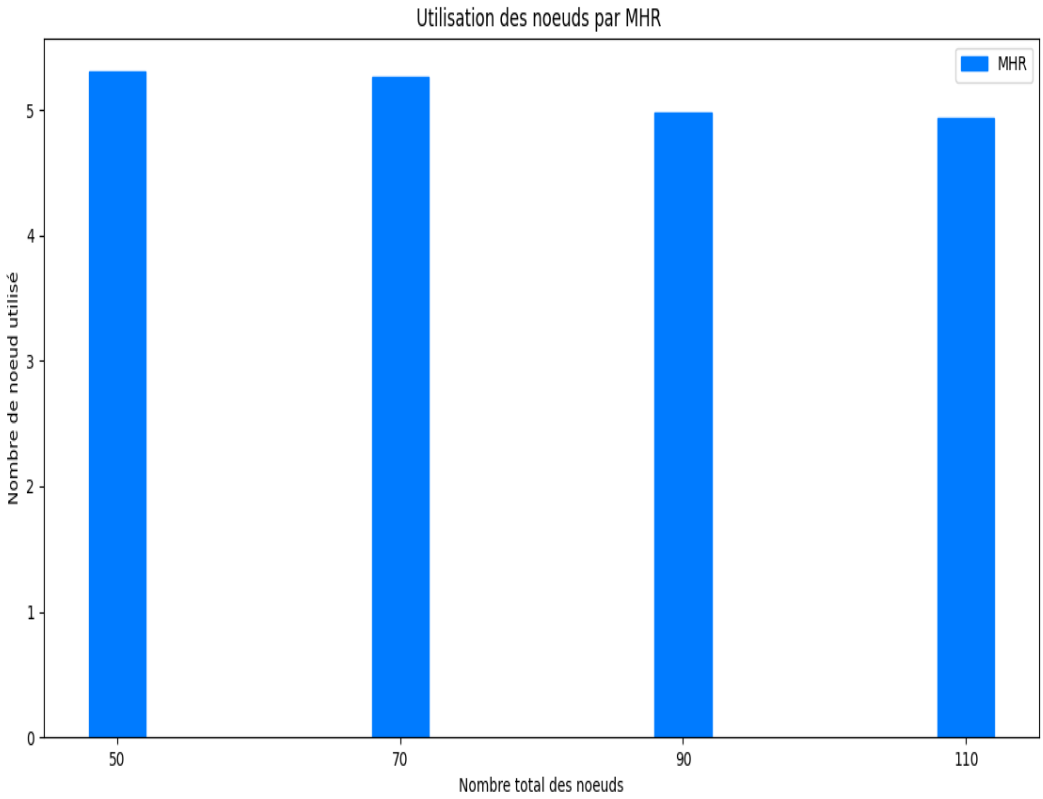


Figure III.4: Nombre de noeuds utilisés: Scénario 1

On constate que l'utilisation des noeuds diminue légèrement lors de l'augmentation de nombre total des noeuds. Cela montre que le nombre total des noeuds dans le réseaux n'a pas une grande influence sur l'usage des noeuds.

- **temps d'exécution** D'après la Figure III.5 qui représente le temps d'exécution de MHR en fonction de nombre total des noeuds de réseau en fixant le nombre de pairs source/destination à 8.

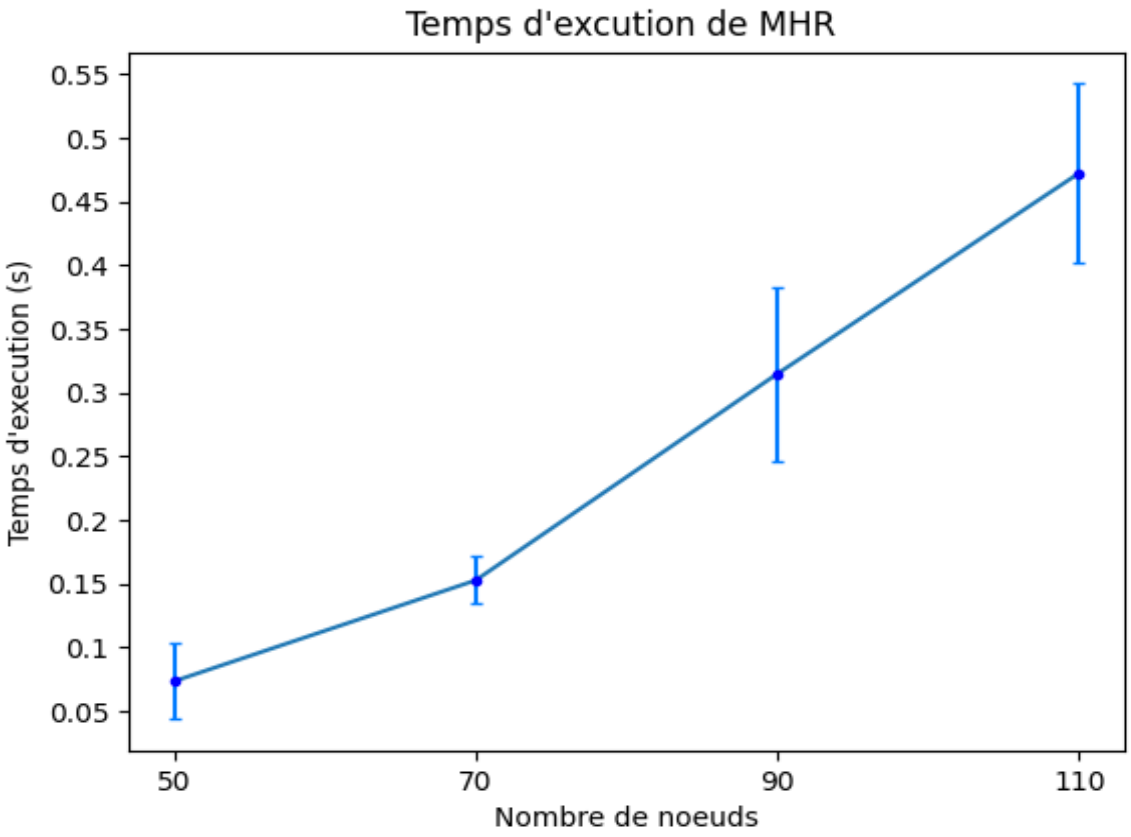


Figure III.5: Temps d'exécution: Scénario 1

On constate que le temps d'exécution augmente linéairement avec l'augmentation de la taille de réseau, ce qui confirme l'influence de nombre de noeud sur l'exécution de l'algorithme MHR, puisque cela accentue la complexité de cet algorithme et la recherche d'une solution optimale prendra plus de temps.

- **Délai de bout en bout**

La figure III.6 représente le délai de bout en bout en variant la taille de réseau. on voie qui le délai diminue légèrement en augmentant la taille de réseau, ces résultats indiquent que lors de l'augmentation de nombre de noeuds,l'algorithme MHR performe mieux en terme de délai bout en bout.

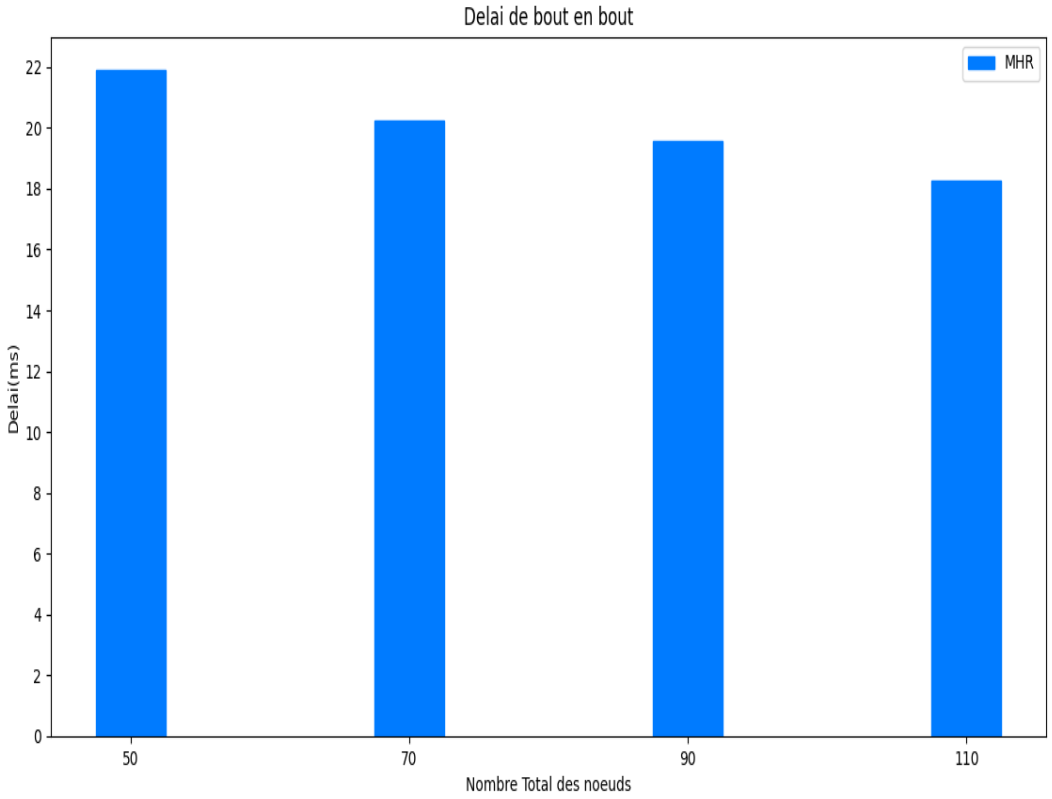


Figure III.6: délai de bout en bout: scénario1

Avec un nombre de noeud élevé, la densité de réseau augmente, et par ce fait l'algorithme MHR trouve plus de choix lors de calcule des chemins de routage, étant donné que l'objectif est de minimiser l'utilisation globale des noeuds, donc cela va aussi minimiser le nombre de sauts et ainsi le délai de bout en bout.

deuxième scénario

Dans ce scénario, nous varions le nombre de source et destination, pendant qu'on fixe le nombre total des noeuds à 110.comme les montre le tableau III.3

Durée	100 seconds
Nombre de pairs source/Ta	2,4,6,8,10,15,20
Nombre de noeud	110
Portée de transmission	300m
Vitesse maximale	30m/s
Superficie	2500x2500 m
Taille de paquet	512 bit

Table III.3: Paramètres de simulation

Nous avons obtenu les graphes suivants :

- **nombre de noeud utilisé**

  On remarque à partir de la figure III.7 qui représente l'usage des noeuds en fonction de nombre des paires(sources/TA). Lorsque le nombre des paires communiquantes augmente, cela est suivi par une augmentation de nombre de noeud utilisé dans les chemins de routage formés entre les sources et destinations, mais l'usage des noeuds reste minimale et ne dépasse pas 13 pour 20 paires.

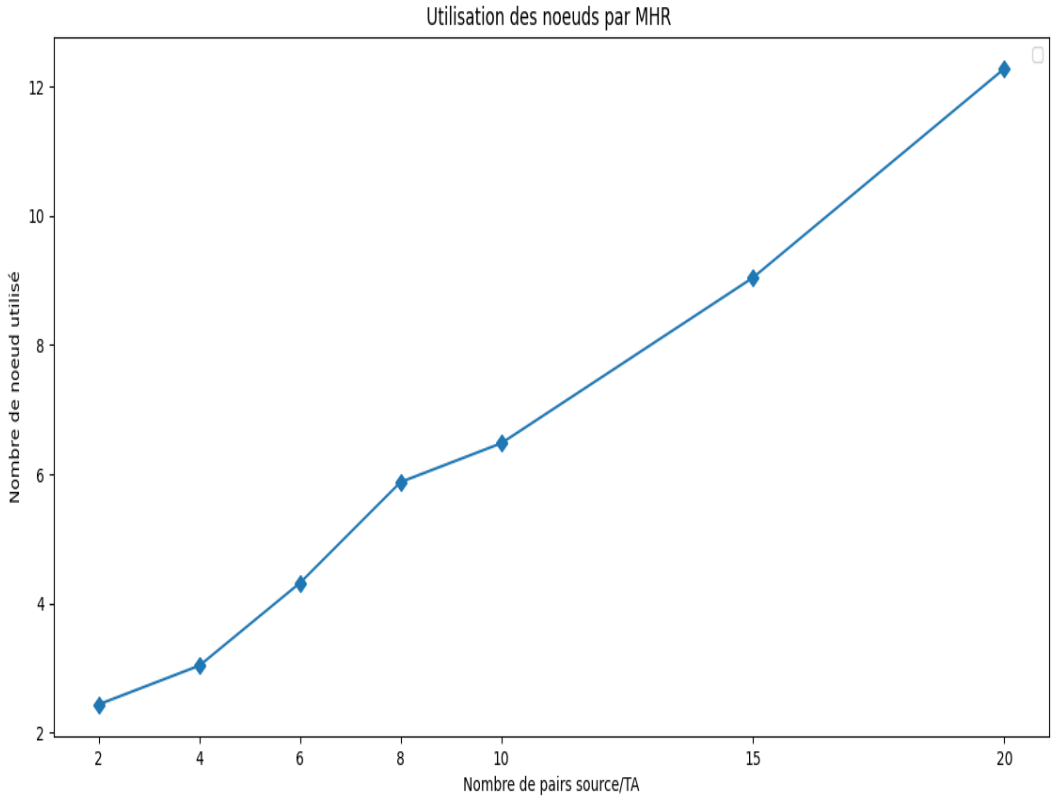


Figure III.7: Nombre de noeuds utilisés: Scénario 2

- **Temps d'exécution: Scénario 2**

  A travers la figure III.8 qui représente la variation du temps d'exécution en fonction de nombre de paires. On constate que le temps d'exécution augmente constamment en ajoutant plus de paires sources/TA, ce qui montre que le nombre de paires présente une influence sur la complexité de MHR. On constate aussi que le temps d'exécution ne dépasse pas 1.3 (s) pour 20 paires.

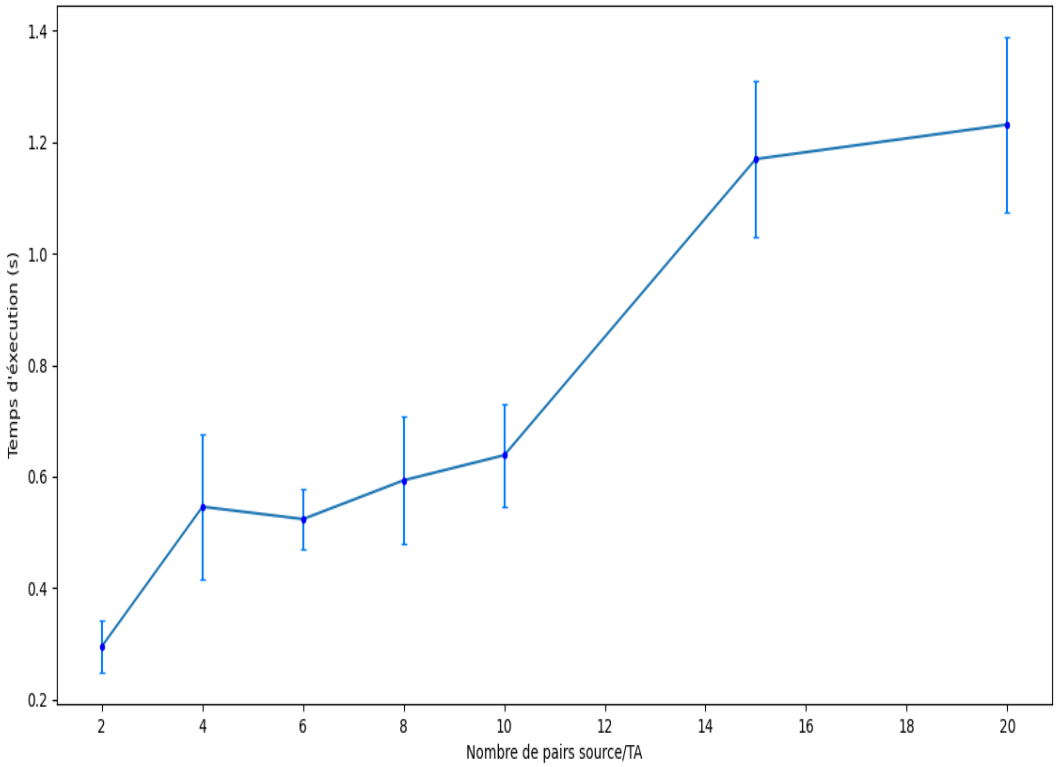


Figure III.8: Temps d'exécution

- **Délai de bout en bout**

  D'après la figure III.9 on remarque que le délai de bout en bout serait de plus en plus important avec l'augmentation de nombre de paires utilisées, mais il reste inférieur à 32(ms) pour 20 paires communiquantes.

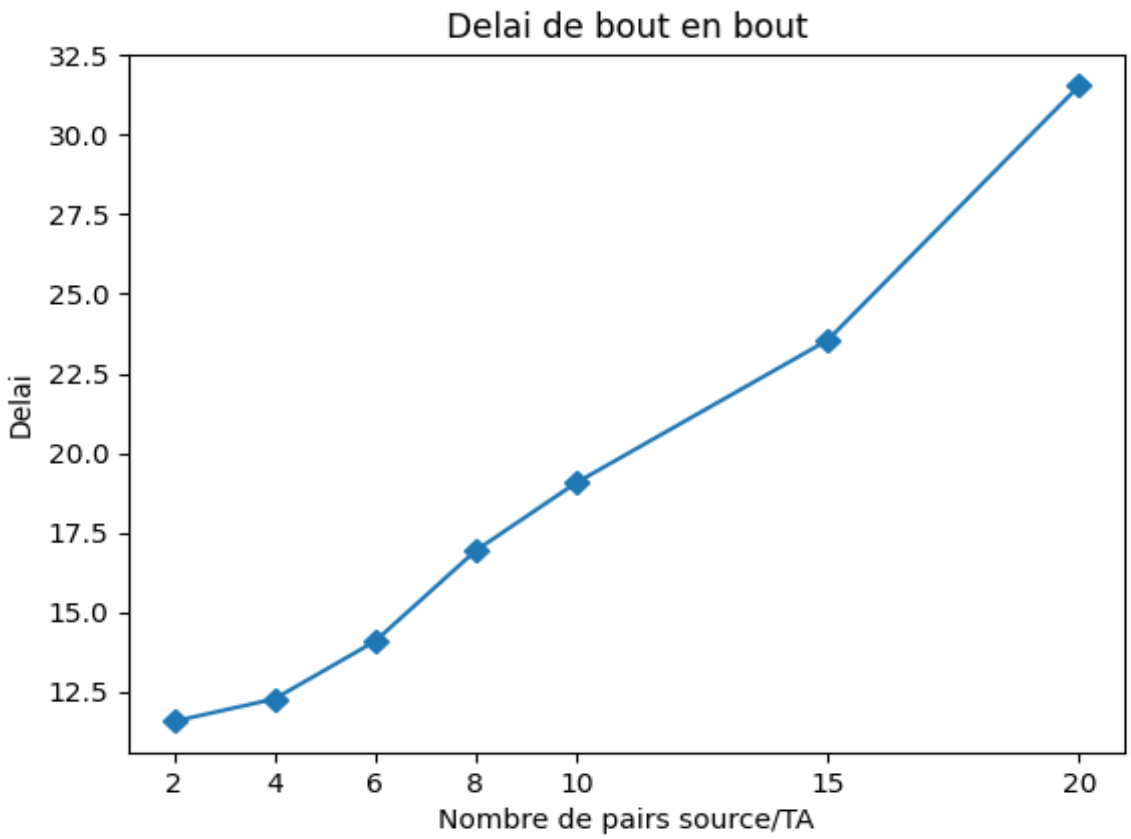


Figure III.9: Délai de bout en bout

Comparaison entre les protocoles MHR, GPSR et MM-GPSR

La simulation des trois protocoles est faite sur python. Pour atteindre une bonne comparaison on a proposer de fixé le nombre total des noeuds à 110 et on varié les paires(sources/TA), les résultats obtenues sont comme suit:

- **Nombre de noeuds utilisé**

  D'après la figure III.10 qui montre la variation de l'usage des noeuds par les trois protocoles (MHR,GPSR, MMGPSR) en fonction de nombre des paires(sources/TA), on remarque que MHR présente moins d'utilisation des noeuds par rapport aux deux autres protocoles, même si le nombre des paires augmente, les noeuds utilisé par MHR reste minimales contrairement à GPSR et MMGPSR, cela confirme que MHR performe mieux

que GPSR et MMGPSR en terme d'utilisation des noeuds.

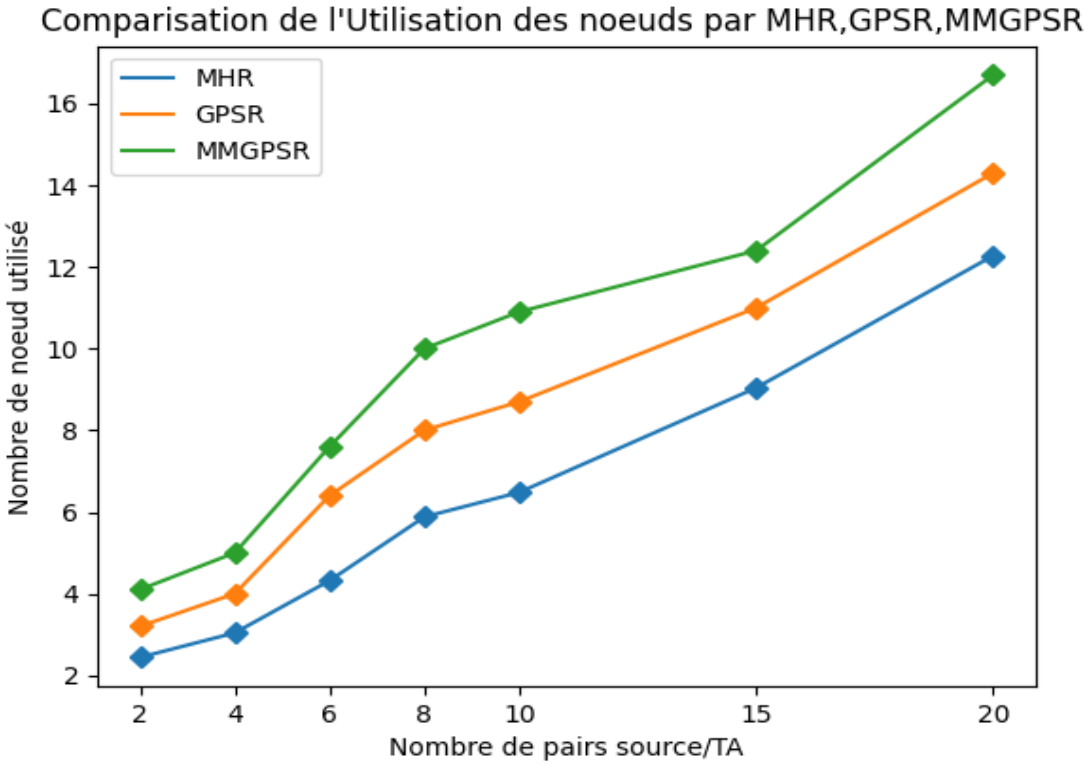


Figure III.10: nombre de noeuds utilisé

- **Délai de bout en bout** On remarque dans la figure III.11 que la variation de délai en fonction de nombre de paires utilisées par rapport aux trois protocoles(MHR, GPSR, MMGPSR) est divisé en deux parties: la première partie est lorsque le nombre de paires est entre 2 et 4, on observe que le délai dans MHR est légèrement supérieur comparant à GPSR et MMGPSR, par contre dans la deuxième partie, à chaque fois que le nombre de paires augmente, le délai augmente aussi mais celui de MHR reste inférieur aux autres protocoles.

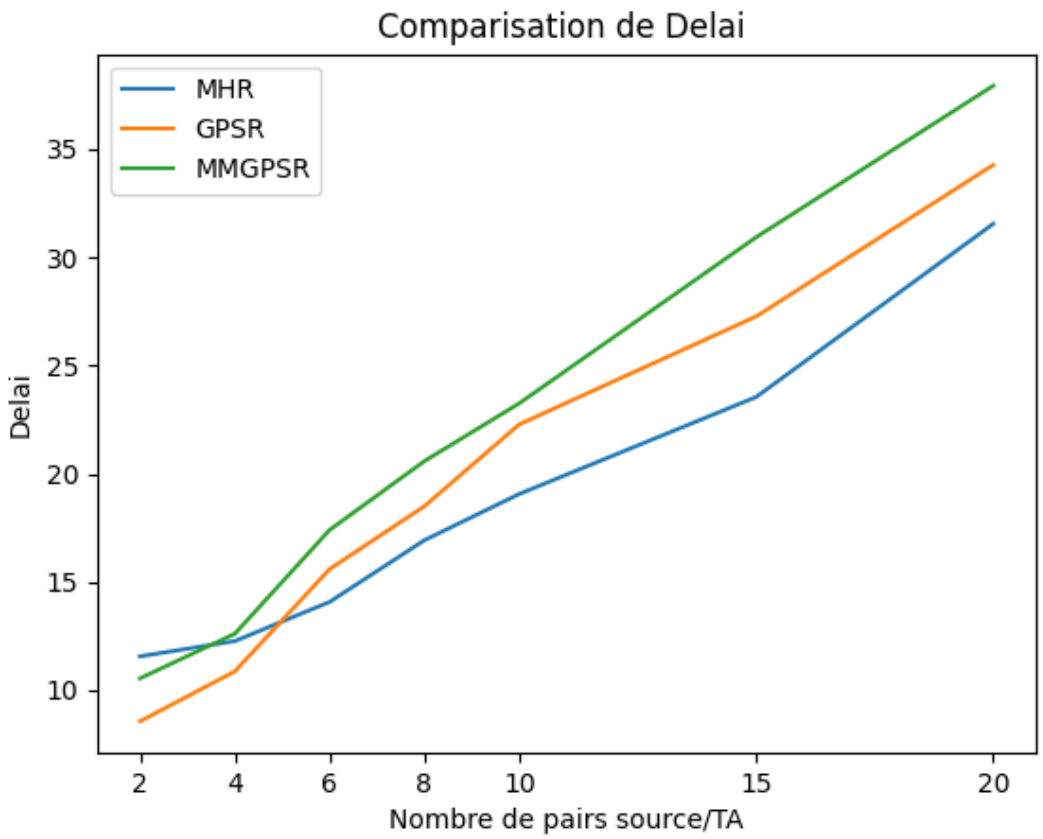


Figure III.11: Délai de bout en bout

Le protocole MHR montre plus de performance en terme de délai bout en bout pour un réseau avec plusieurs entités communiquantes.

Troisième scénario

Cette partie est consacrée pour l'étude de la distribution de trafic des données générées par les différentes sources. La figure suivante représente une partie de réseau à l'instant t_0:

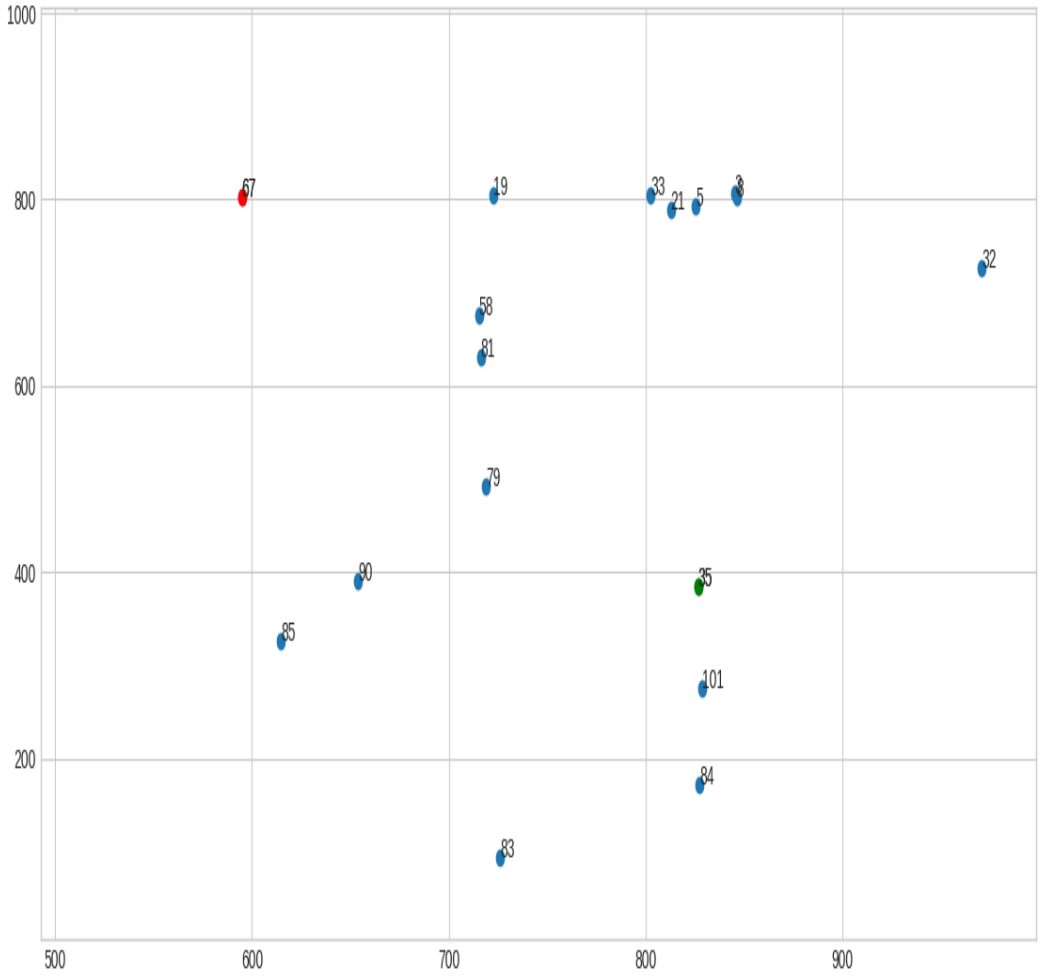


Figure III.12: Section de réseau à t_0

À l'instant t_0, le noeud 35 génère un trafic de 500kbps destiné au noeud 67 qui représente l'autorité de suivi TA. L'algorithme MHR s'occupe de trouver une route vers la destination 67 et l'allocation d'une bande passante de 500kbps dans le chemin choisi. La figureIII.13 montre le résultat donné par MHR, le noeud 81 est choisi comme prochain saut à partir de la source afin d'atteindre la destination, la distribution de trafic est indiquée ci-dessous.

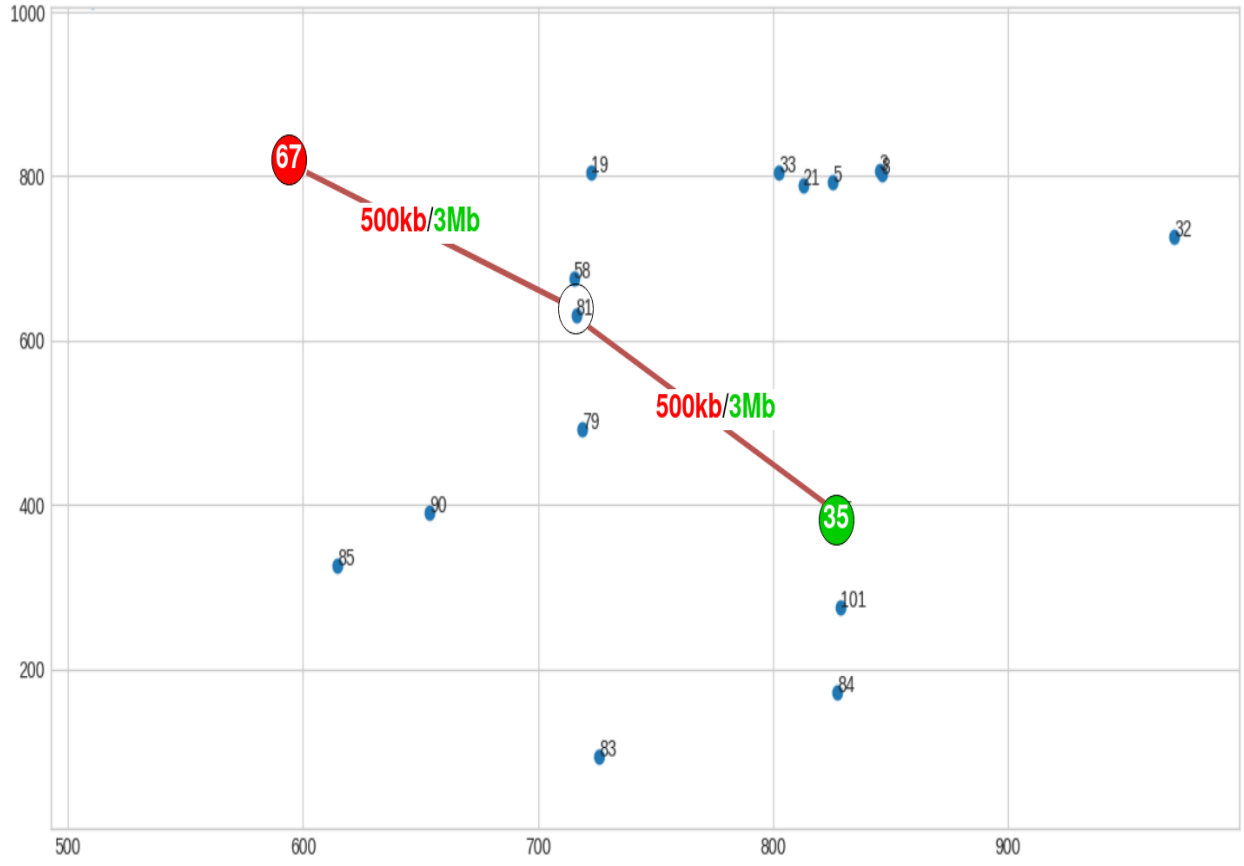


Figure III.13: Distribution de trafic à l'instant t_0

À l'instant t_1, le noeud 90 veut transmettre un trafic de 500Kbps à la même destination (noeud 67). Puisque ces deux sources sont proches et le noeud 81 est un voisin en commun, donc la deuxième source utilisera aussi ce dernier pour l'envoie de trafic vers le TA, la nouvelle solution générée par MHR est donnée dans la figure III.14:

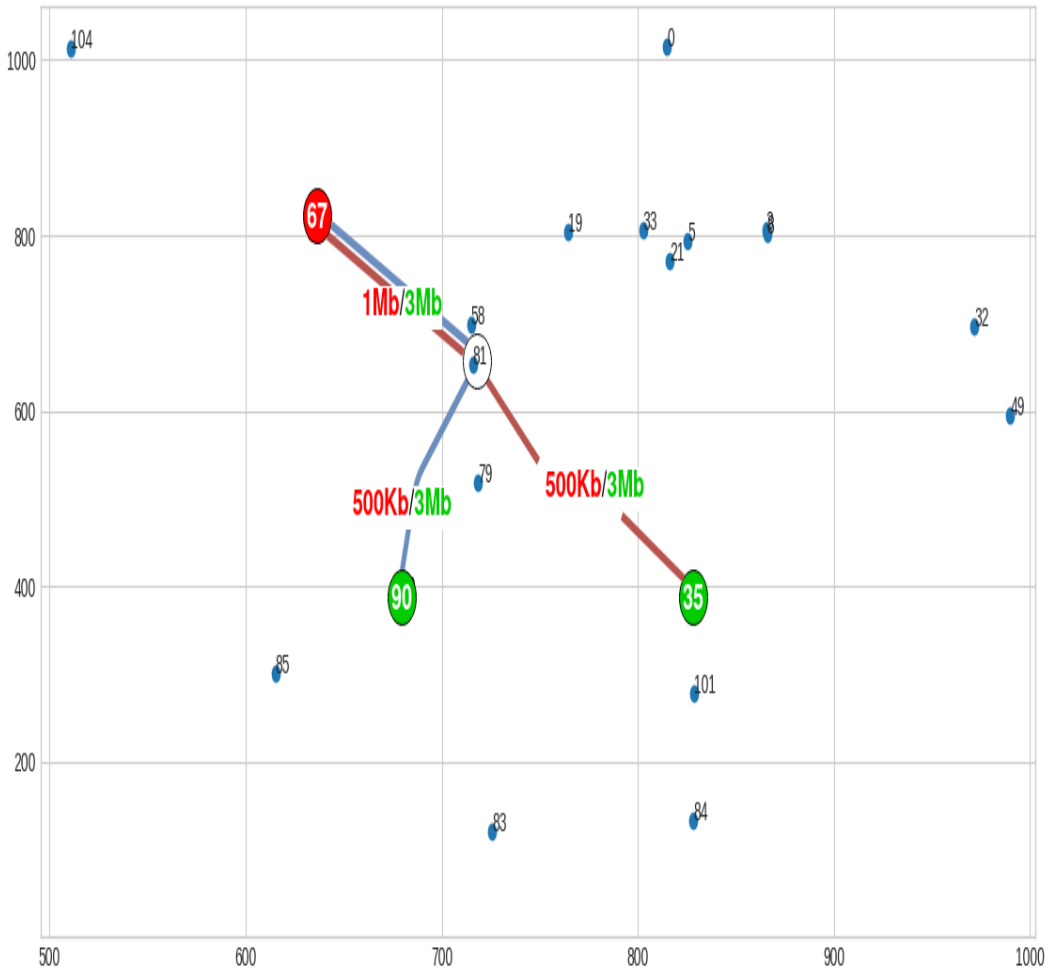


Figure III.14: Distribution de trafic à l'instant t_1

À l'instant t_2, le noeud 81 quitte la portée de communication de noeud 35, alors il sera remplacé par le noeud 79 en gardant les même distribution de trafic précédente, la figure suivante montre ce changement:

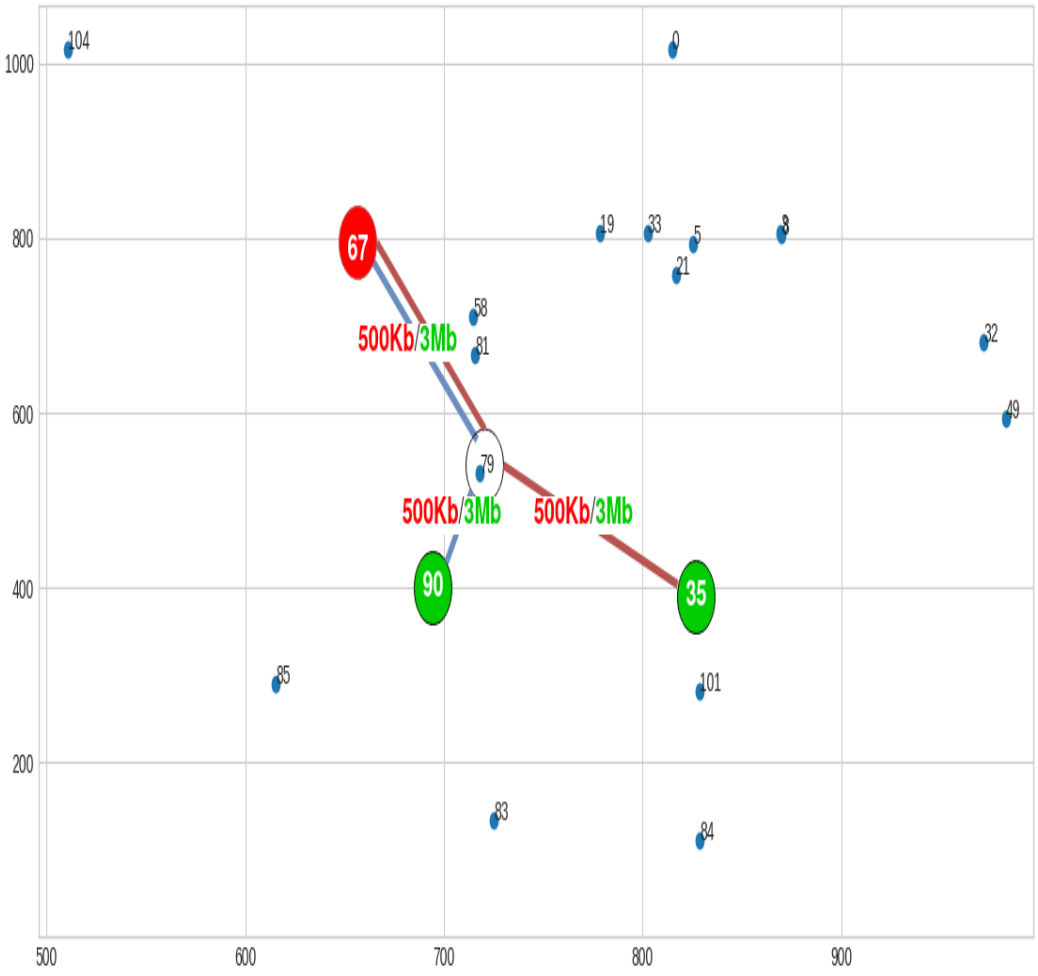


Figure III.15: Distribution de trafic à l'instant t_2

À l'instant t_3, le noeud 85 génère un trafic de 1Mpbs vers une autre Tracking Authority représentée par le noeud 0. MHR calculera une route vers cette destination, le résultat montré dans La figure III.16 indique que MHR a choisi la route 85 → 79 → 19 → 0 pour le flux de trafic généré par la troisième source.

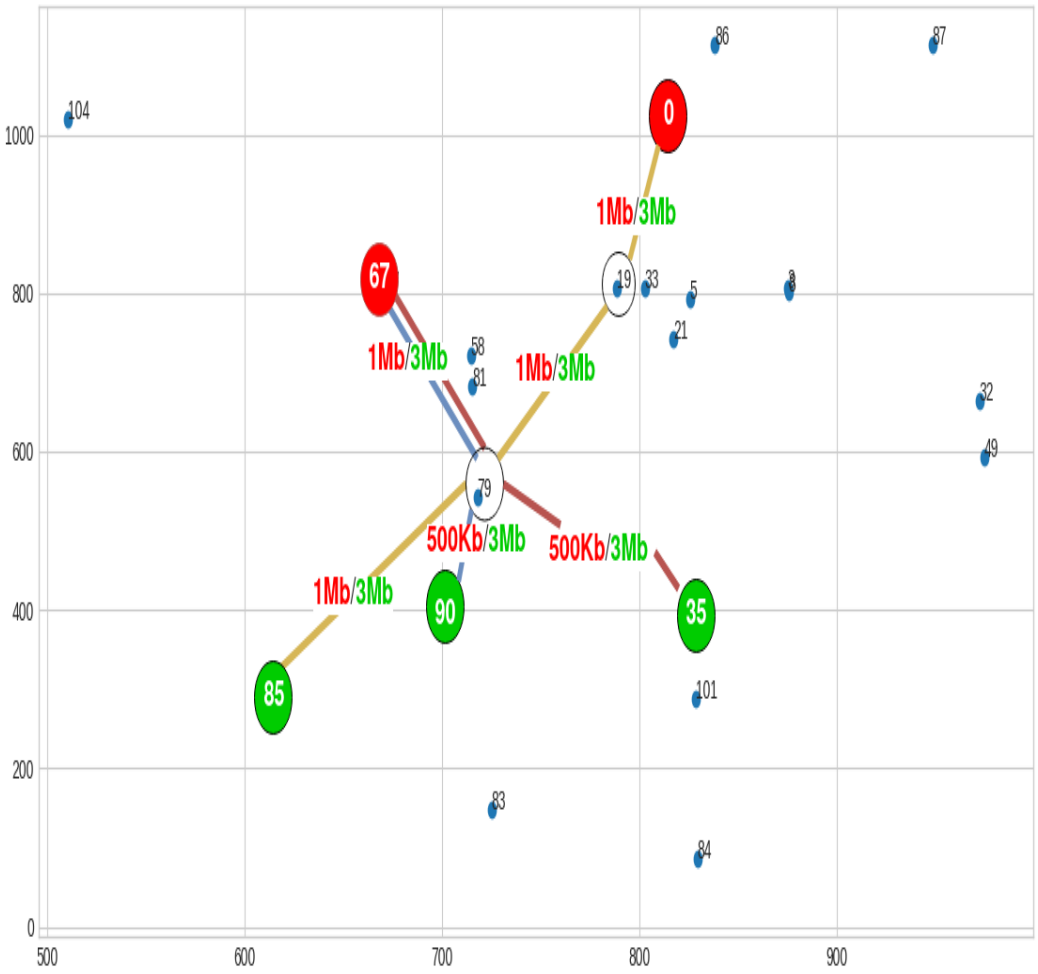


Figure III.16: Distribution de trafic à l'instant t_3

III.6. Conclusion

Dans ce dernier chapitre nous avons décrit l'aspect expérimental de notre projet, commençant par une présentation de l'environnement et processus de simulation, puis nous avons expliqué les différents métriques étudiées et interpréter les résultats obtenus, finalement on a fait une comparaison de notre solution MHR avec deux autres protocoles de routage basés sur la position GPSR et MMGPSR. Cette comparaison nous a permet de conclure que le protocole que nous avons développé présente de meilleurs performances en terme de l'usage des noeuds et délai bout en bout.

CONCLUSION GÉNÉRALE

Ce projet de fin d'études présente l'achèvement d'un travail de recherche profonde, dans lequel nous avons essayé de mettre en pratique les connaissances acquises durant notre parcours universitaire et nos lecteurs des différents travaux faites dans le domaine d'amélioration et optimisation de la qualité de service dans les réseaux véhiculaires. Nous avons fixé des objectives ambitieuses malgré la courte durée qu'on disposait, mais nous avons réussi à les atteindre en y travaillant avec patience, beaucoup d'efforts de notre part et un excellant encadrement.

Vu que le système de suivi véhiculaire MC-Track n'a pas pris en considération les problèmes relatifs à la qualité de service, nous avons fixé l'objectif de mettre en place un algorithme d'optimisation nommé MHR, son rôle est d'améliorer la qualité de service.

Il a fallu en premier temps étudier l'architecture de MC-Track afin de tirer les contraintes relatives à ce système. La problématique a été modéliser sous forme algébrique qui tient en compte les contraintes imposées non seulement par l'architecture de MC-Track mais aussi par celle de VANET. Le modèle mathématique a été implémenté dans un module d'optimisation, qui reçoit les données de réseau comme entrées et calcule les chemins de routage pour toute les sources, avec des régulations sur la distribution de trafic pour tout les flux de données générés.

En effet, dans le but de tester l'efficacité de notre solution, nous avons eu besoin de développer un nouveau simulateur, puisque les logiciels existants n'offrent pas la possibilité d'implémenter ce que nous avons proposé. Dans ce cadre, nous avons utilisé la programmation modulaire en Python et subdiviser notre simulateur en: module de mobilité, d'optimisation et

module réseau.

Ce projet nous a offert la chance d'approfondir nos connaissances, d'enrichir nos acquis et de consolider l'expérience que ce soit sur le plan théorique où nous avons appris de nouvelles notions relative à l'*internet des véhicule*, l'optimisation et modélisation des problèmes, ou sur le plan programmation où nous avons réussi dans une courte durée à développer un simulateur pour tester et implémenter notre algorithme de routage.

Références bibliographique

[1] Samira El Madani, Saad Motahhir, and Abdelaziz El Ghzizal. Internet of vehicles: concept, process, security aspects and solutions. *Multimedia Tools and Applications*, pages 1–25, 2022.

[2] Shaik Ashfaq Hussain, Kamaluddin Mohammad Yusof, Shaik Mazhar Hussain, and Ajay Vikram Singh. A review of quality of service issues in internet of vehicles (iov). In *2019 Amity International Conference on Artificial Intelligence (AICAI)*, pages 380–383. IEEE, 2019.

[3] HAMOU CHEHRI. *Étude et caractérisation d'un canal de propagation pour les réseaux VANET*. UQTR, CANADA, 2014.

[4] Khaleel Mershad, Hassan Artail, and Mario Gerla. Roamer: Roadside units as message routers in vanets. *Ad Hoc Networks*, 10(3):479–496, 2012.

[5] Muhammad Saad, Muhammad Khalid Khan, and Maaz Bin Ahmad. Blockchain-enabled vehicular ad hoc networks: A systematic literature review. *Sustainability*, 14(7):3919, 2022.

[6] KA.Ali. *Modélisation et étude de performances dans les réseaux vanets*. KA.Ali, In Université de Technologie de Belfort-Montbeliard, 2012.

[7] P. Muhlethaler Y. Toor and A. Laouiti. *Vehicle ad hoc networks : applications and related technical issues. In Communications Surveys Tutorials*. Y. Toor, 2008.

[8] autocrypt. Dsrc vs. c-v2x: A detailed comparison of the 2 types of v2x technologies. https://autocrypt.io/dsrc-vs-c-v2x-a-detailed-comparison-of-the-2-types-of-v2x-technologies/, 2021.

[9] Cellular vs. DSRC for V2X Communication: The Debate Continues. Technical report, 2021. Accessed: 2022-05-25.

[10] Arindam Debnath, Habila Basumatary, Mili Dhar, Bidyut K Bhattacharyya, and Mrinal Kanti Debbarma. A routing technique for enhancing the quality of service in vanet. *IETE Journal of Research*, pages 1–14, 2021.

[11] Andrey Silva, Niaz Reza, and Aurenice Oliveira. Improvement and performance evaluation of gpsr-based routing techniques for vehicular ad hoc networks. *IEEE Access*, 7:21722–21733, 2019.

[12] Safae Smiri, Adil Ben Abbou, Abdelali Boushaba, Azeddine Zahi, and Rachid Ben Abbou. Wa-gpsr: Weight-aware gpsr-based routing protocol for vanet. *International Journal of Interactive Mobile Technologies*, 15(17), 2021.

[13] MC Aswathy and C Tripti. A cluster based enhancement to aodv for inter-vehicular communication in vanet. *International Journal of Grid Computing & Applications*, 3(3):41, 2012.

[14] Manisha Chahal, Sandeep Harit, Krishn K Mishra, Arun Kumar Sangaiah, and Zhigao Zheng. A survey on software-defined networking in vehicular ad hoc networks: Challenges, applications and use cases. *Sustainable cities and society*, 35:830–840, 2017.

[15] Ming Zhu, Zhiping Cai, Jiannong Cao, and Ming Xu. Efficient multiple-copy routing in software-defined vehicular networks. 2015.

[16] Tony Santhosh Gnanasekar and Dhandapani Samiappan. Optimal routing in vanet using improved meta-heuristic approach: a variant of jaya. *IET Communications*, 14(16):2740–2748, 2020.

[17] Manisha Chahal and Sandeep Harit. Network selection and data dissemination in heterogeneous software-defined vehicular network. *Computer Networks*, 161:32–44, 2019.

[18] Ammara Anjum Khan, Mehran Abolhasan, and Wei Ni. 5g next generation vanets using sdn and fog computing framework. In *2018 15th IEEE Annual Consumer Communications Networking Conference (CCNC)*, pages 1–6, 2018.

[19] Abdellah Kaci and Abderrezak Rachedi. Mc-track: A cloud based data oriented vehicular tracking system with adaptive security. In *2019 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6. IEEE, 2019.

[20] Open Street Map. Technical report, 2002. Accessed: 2022-05-25.

ملخص

إن إنترنت المركبات هو حالة استخدام لإنترنت الأشياء، حيث يشكل أسطول المركبات الحضرية شبكة عالمية. يعد تحسين جودة الخدمة في مثل هذه الشباكات مهمة صعبة، لأن المركبات في حركة مستمرة، مما يجعل الشبكة غير مستقرة وفي تغير مستمر من ناحية الطوبولوجيا، وهذا يخلق بيئة معادية مع العديد من المتغيرات التي يجب أخذها في الاعتبار.

. أثبتت بروتوكولات التوجيه المعتمدة على الموقع الجغرافي أنها تعمل بشكل أفضل في مثل هذه البيئة، فهي توفر تسليم حزم عالي مع تأخير منخفض ولكنها تواجه أيضًا مشكلات مثل حلقات التوجيه والاستخدام العالي للنطاق الترددي. في هذه المقالة، سنثري بنية نظام تتبع المركبات "ماك تراك" الذي لم يأخذ في الاعتبار جودة الخدمة ثم نقترح خوارزمية معتمدة على الموقع الجغرافي لتوجيه الحزم في الشبكة بأدنى عدد من القفزات الذي يجعل من الممكن تقليل استخدام موارد الشبكة وتقليل التأخير و توزيع الضغط. فيما يخص الدراسة التجريبية قمنا بمقارنة الخوارزمية المقترحة مع أحدث الحلول الحالية. أظهرت النتائج أن الحل المقترح أكثر فعالية.

الكلمات الدالة : جودة الخدمة، التحسين، شبكة المركبات، التوجيه، ماك تراك

Résumé

L'Internet des véhicules (IoV) est un cas d'utilisation du l'Internet des objets (IoT), où la flotte de véhicules urbains constitue un réseau mondial. L'optimisation de la qualité de service (QoS) dans l'IoV est une tâche difficile, car les véhicules sont en mouvement continu, ce qui rend le réseau instable et en changement continu de topologie , cela crée un environnement hostile avec de nombreux variables à prendre en compte. Dans le présent article, nous enrichiront l'architecture de système de suivi véhiculaire Mc-Track qui n'a pas pris en compte la QoS, nous proposons alors l'algorithme de routage Minimum Hops Routing (MHR), basé sur la position qui permet de réduire l'usage des noeuds, la minimisation de délai et load balancing. Pour l'étude expérimentale, nous avons comparé l'algorithme MHR proposé avec des solutions existantes de l'état de l'art. Les résultats ont montré que la solution MHR proposée est plus efficace que les solutions existantes en termes d'usage de noeuds et délai bout en bout.
Mots clés: QoS, optimisation, VANET, routage, MC-Track.

Abstract

The Internet of Vehicles (IoV) is a use case of the the Internet of Things (IoT), where the fleet of urban vehicles constitutes a global network. Optimizing Quality of Service (QoS) in IoV is a difficult task because vehicles are in continuous motion which makes the network unstable and in a continuously changing topology, this creates a hostile environment with many variables to consider. In this article, we will enrich the Mc-Track vehicular tracking system architecture which did not take into account the QoS , we then propose the Minimum Hops Routing (MHR) algorithm, based on the position which allows to reduce node usage, delay minimization and load balancing. For experimental study, we compared the proposed MHR algorithm with existing state-of-the-art solutions. The results showed that the proposed MHR solution is more effective than the existing solutions in terms of node usage and end-to-end delay.
Keywords: QoS, optimization, VANET, routing, MC-Track.