République Algérienne Démocratique Populaire
Ministère de l'enseignement supérieur et de la recherche scientifique
Université Echahid Cheikh Larbi Tebessi- Tébessa
Faculté des Sciences Exactes et des Sciences de la Nature et de la Vie
Département: Mathématiques et Informatique

Mémoire de fin d'étude
Pour l'obtention du diplôme de MASTER
Domaine: MI
Filière: Informatique
Option: Réseaux et Sécurité Informatique

Thème

Une architecture Edge Computing basée sur les réseaux 5G pour améliorer l'internet des véhicules (IOV)

Réalisé par:
Hamaidia Dhia Errahmene

Devant le jury :

Mr G. Tahar	MAB	Université Echahid Cheikh Larbi Tebessi	Président
Mr K. Abderrazak	MCA	Université Echahid Cheikh Larbi Tebessi	Examinateur
Mr S. Abdelatif	MCA	Université Echahid Cheikh Larbi Tebessi	Encadreur

Date soutenance: 07/06/2023

Résumé

L'Internet des Véhicules (IoV) représente une évolution des réseaux de véhicules ad hoc traditionnels (VANET) grâce à l'intégration des technologies de l'Internet des Objets (IdO) dans les véhicules. Cette convergence crée des véhicules connectés intelligents qui bénéficient de nouvelles fonctionnalités. L'architecture IoV associée au paradigme de contrôle par logiciel (SDN) se distingue des réseaux VANET traditionnels en offrant une flexibilité, une vitesse, une fiabilité et une évolutivité améliorées. Dans ce contexte, notre travail propose une architecture Edge Computing pour exploiter les fonctionnalités avancées des réseaux de nouvelle génération dans le domaine de l'Internet des Véhicules. En adoptant des stratégies de routage dynamique IoV basées sur SDN, notre conception vise à optimiser le transfert de données via le protocole OpenFlow, ce qui améliore la vitesse et la stabilité globales des systèmes IoV. Cette approche favorise une gestion plus efficace du trafic routier et une meilleure utilisation des ressources du réseau. Les résultats de notre recherche contribueront à améliorer les performances et l'efficacité des systèmes IoV, en particulier dans la gestion du trafic et l'optimisation des ressources. Notre travail offre ainsi de nouvelles perspectives pour répondre aux besoins croissants des véhicules connectés en termes de connectivité, de sécurité et de services avancés.

Mots clés : IoV, SDN , stratégie de routage , OpenFlow

Abstract

The Internet of Vehicles (IoV) represents an evolution of traditional Vehicular Ad Hoc Networks (VANET) through the integration of Internet of Things (IoT) technologies in vehicles. This convergence creates intelligent connected vehicles that benefit from new functionalities. The IoV architecture combined with Software Defined Network (SDN) paradigm sets itself apart from traditional VANET networks by providing improved flexibility, speed, reliability, and scalability. In this context, our work proposes an edge computing architecture to exploit the advanced features of next-generation networks in the field of the Internet of Vehicles (IoV). By adopting dynamic SDN-based IoV routing strategies, our design aims to optimize data transfer through the OpenFlow protocol, which improves the overall speed and stability of IoV systems. This approach promotes more efficient road traffic management and better use of network resources. The results of our research will help improve the performance and efficiency of IoV systems, especially in traffic management and resource optimization. Our work thus offers new perspectives to meet the growing needs of connected vehicles in terms of connectivity, security and advanced services.

Keyworks: IoV , SDN, routing strategy , OpenFlow.

الملخص

يمثل إنترنت المركبات (IoV) تطورًا لشبكات المركبات المخصصة التقليدية (VANET) من خلال دمج تقنيات إنترنت الأشياء (IoT) في المركبات. يخلق هذا التقارب مركبات متصلة ذكية تستفيد من وظائف جديدة. تميز بنية IoV جنبًا إلى جنب مع نموذج التحكم المستند إلى البرامج (SDN) نفسها بعيدًا عن شبكات VANET التقليدية من خلال توفير مرونة وسرعة وموثوقية وقابلية تطوير محسّنة. في هذا السياق ، يقترح عملنا بنية حوسبة متطورة لاستغلال الميزات المتقدمة لشبكات الجيل الحديث في مجال إنترنت المركبات. من خلال اعتماد استراتيجيات توجيه IoV الديناميكية القائمة على SDN ، يهدف تصميمنا إلى تحسين نقل البيانات من خلال بروتوكول OpenFlow ، مما يحسن السرعة الإجمالية واستقرار أنظمة IoV. يعزز هذا النهج إدارة أكثر كفاءة لحركة المرور على الطرق واستخدام أفضل لموارد الشبكة. ستساعد نتائج بحثنا في تحسين أداء وكفاءة أنظمة IoV ، لا سيما في إدارة حركة المرور وتحسين الموارد. وبالتالي فإن عملنا يقدم وجهات نظر جديدة لتلبية الاحتياجات المتزايدة للمركبات المتصلة من حيث الاتصال والأمن والخدمات المتقدمة.

الكلمات المفتاحية: IoV انترنيت مركبات ، SDN ، استراتيجية التوجيه ، OpenFlow

Dédicace

To My Dear Parents

To My Sister, To My Brothers

To My Supervisor Dr. Sahraoui Abdelatif

Appréciation

First of all, I thank Allah for giving me courage and patience needed to complete this work.

I appreciate my family. They've always loved, supported, and strengthened me. Their constant support has shaped me.

My family has supported me through thick and thin. They've cheered me on, shared my pleasures, and comforted me. I cherish their affection and acceptance.

I appreciate my family's generosity, respect, tenacity, and understanding. They taught me to value connections, honesty, and togetherness.

My family has supported me in times of need and offered advice. Their advice and life experiences helped me navigate life's problems and make good judgments.

I'm lucky to have such a wonderful family. They provide warmth and delight to every moment, giving an invaluable feeling of belonging.

To my father, who can be proud and find here the result of many years of sacrifices and hardships to help me progress in life, may God make this work fruitful. Thank you for the noble values, education, and constant support that you have provided.

To my mother, who has worked for my success through her love, support, all the sacrifices made, and her precious advice. For all her assistance and presence in my life, receive through this humble work the expression of my feelings and eternal gratitude.

To my sister Nour Houda Hanine and my brothers Saif El Islam, Fadel Allah, my wishes for happiness and success.

To my uncles, aunt, cousins, whether near or far, you have contributed to my upbringing, and I express my heartfelt gratitude.

To all my friends and my lovely CAR. I dedicate this work to you and wish you a future that matches your ambitions. May our friendship endure.

Table Des Matieres

LISTE DE FIGURES

Liste Des Tableaux

Introduction Générale

L'avènement de l'Internet des Objets (IdO) a considérablement renforcé la connectivité sans fil dans notre vie quotidienne. L'application de cette technologie au secteur automobile a donné naissance à l'Internet des Véhicules (IoV). Les véhicules connectés représentent une avancée majeure dans l'industrie automobile, en introduisant une technologie qui est à la fois inévitable et prometteuse pour l'avenir. L'objectif des véhicules connectés est d'améliorer et d'optimiser la sécurité, la commodité et le divertissement à bord, tant pour les passagers que pour les conducteurs.

La connectivité des véhicules permet de créer un environnement de conduite plus sûr en facilitant l'échange d'informations en temps réel entre les véhicules, les infrastructures routières et les autres acteurs du système de transport. Grâce à cette interconnexion, les véhicules peuvent partager des données sur les conditions de la route, les dangers potentiels et les informations de circulation, permettant ainsi aux conducteurs d'anticiper les situations et de prendre des décisions éclairées.

En plus d'améliorer la sécurité, les véhicules connectés offrent une plus grande commodité de déplacement. Grâce à la connectivité Internet, les passagers et les conducteurs peuvent accéder à une multitude de services et d'applications à bord du véhicule. Cela inclut la navigation en temps réel avec des mises à jour de trafic en direct, la réservation de stationnement, l'accès à des services de divertissement en streaming, ainsi que la possibilité de contrôler à distance les systèmes de climatisation, de verrouillage et d'autres fonctionnalités du véhicule. L'info-divertissement à bord constitue également un aspect essentiel des véhicules connectés. Les passagers peuvent accéder à Internet, consulter leurs e-mails, utiliser des applications de médias sociaux et profiter de divertissements multimédias en streaming pendant leurs trajets. Cela transforme l'expérience de conduite en offrant une connectivité permanente et une gamme étendue de services.

Les environnements Edge Computing ont émergé afin de rendre réalisables les fonctionnalités d'info-divertissement à bord en exploitant la proximité et la puissance de traitement des ressources informatiques présentes au niveau du réseau périphérique. Ces ressources permettent de traiter et de stocker localement les données et les services

nécessaires à l'info-divertissement, notamment au sein des points d'accès Edge, ce qui réduit la latence et améliore la réactivité de ces applications. En particulier, l'adoption des architectures Edge Computing dans ce domaine peut offrir une expérience d'info-divertissement plus fluide, interactive et personnalisée pour les passagers, en tirant parti des capacités de traitement local des ressources Edge.

Objective :

Dans le cadre de ce travail, nous approfondirons l'intégration du paradigme de l'Edge Computing dans le domaine de l'info-divertissement à bord des véhicules connectés. Notre étude se concentrera sur l'exploration des défis techniques et des opportunités inhérents à cette intégration, dans le but de proposer des solutions innovantes visant à améliorer de manière efficace la qualité de l'expérience offerte aux utilisateurs. Plus précisément, nous examinerons en détail les différentes applications et les technologies sous-jacentes qui permettent de concrétiser la vision des véhicules connectés. Nous analyserons les avantages potentiels et les impacts de l'Internet des Véhicules (IoV) afin de mieux comprendre les implications de cette technologie en termes de sécurité, de commodité et d'expérience pour les passagers et les conducteurs.

Dans ce travail, nous présentons une architecture Edge Computing qui vise à mettre en œuvre les fonctionnalités avancées des réseaux de nouvelle génération pour améliorer les capacités de l'Internet des Véhicules (IoV). Notre approche se concentre particulièrement sur deux stratégies de routage IoV dynamique avancé basées sur le paradigme de contrôle par logiciel (SDN). Ces stratégies sont spécifiquement conçues pour gérer les problèmes de congestion routière. En mettant l'accent sur la conception de ces stratégies, notre objectif principal est d'améliorer le flux du trafic réseau en déplaçant les opérations de calcul et de traitement des données vers la périphérie du réseau. En exploitant des capacités de calcul avancées au niveau des points d'accès Edge, notre proposition vise à réduire de manière significative la quantité de données qui doivent transiter par le réseau central, ce qui se traduit par des délais réduits et des prises de décision en temps réel plus fluides.

Dans la phase d'expérimentation, Nous mettrons en œuvre notre architecture Edge Computing dans l'environnement de simulation Omnet++ pour évalues ses performances en utilisant des mesures de performances. Les résultats obtenus nous permettront de valider

l'efficacité de notre proposition et d'identifier les avantages concrets qu'elle peut offrir en termes de gestion du trafic routier et d'amélioration des performances du système IoV.

Structure de mémoire :

Notre travail est structuré en quatre chapitres, chacun abordant des aspects spécifiques de notre recherche :

Chapitre 1 : Introduction aux réseaux véhiculaires dans les contextes 5G

Dans ce chapitre introductif, nous présenterons les concepts clés des réseaux véhiculaires, en mettant l'accent sur leur intégration dans les réseaux 5G. Nous explorerons les architectures, les protocoles et les normes de communication utilisés dans les réseaux véhiculaires, en mettant en évidence les défis et les opportunités liés à cette technologie émergente.

Chapitre 2 : État de l'art des techniques de diffusion de l'information dans l'environnement IoV

Le deuxième chapitre consistera en une revue approfondie des travaux et des techniques existants concernant la diffusion de l'information dans l'environnement de l'Internet des Véhicules (IoV). Nous examinerons les approches et les stratégies adoptées pour améliorer la transmission, la distribution et la gestion des données dans les réseaux véhiculaires. Cette revue de littérature nous permettra de mieux comprendre les avancées récentes, les lacunes existantes et les pistes de recherche prometteuses dans ce domaine.

Chapitre 3 : Proposition d'une architecture IoV basé SDN et stratégies de routage dynamique

Le troisième chapitre sera dédié à notre proposition d'architecture et aux stratégies de routage dynamique que nous avons développées. Nous présenterons en détail notre architecture proposée, mettant en évidence les composants clés et leur fonctionnement. Nous décrirons également les stratégies de routage dynamique conçues pour optimiser la diffusion de l'information dans l'environnement IoV. Enfin, nous présenterons un modèle de simulation d'un cas d'étude pour évaluer l'efficacité de notre proposition, en comparant les résultats de simulation avec nos objectifs de performance.

CHAPTER 1 : Introduction Aux Réseaux Véhiculaires Dans Les Contextes 5G

1. Introduction

L'Internet des véhicules (IoV) est actuellement une technologie prometteuse et innovante pour les systèmes de conduite intelligents. Cette technologie combine l'Internet des objets (IdO) avec les systèmes des véhicules pour permettre la connectivité entre les véhicules, l'infrastructure et les personnes. Le développement rapide de cette technologie a changé l'ensemble du secteur des transports en améliorant la mobilité, en réduisant le trafic et en améliorant la sécurité routière. L'une des technologies clés qui rendent possible l'Internet des objets (IoV) est le réseau cellulaire de cinquième génération (5G), qui fournit une connectivité rapide, fiable et à faible latence qui facilite la communication en temps réel entre les composants IoV.

L'Internet des véhicules (IoV) utilise les capacités de l'Internet des objets pour répondre aux besoins de connexion de l'environnement intelligent. Des réseaux de capteurs sans fil (WSN), des ressources, de nombreuses interfaces de communication et des applications peuvent être utilisés pour assurer une communication fiable et transparente entre l'environnement du véhicule. Les véhicules et les usagers de la route bénéficient de cette combinaison de services et d'équipements. Ces services intelligents collectent des données de trafic en temps réel et analysent le Big data de son infrastructure (feux rouges, trafic, etc.) pour améliorer la fluidité du trafic et la sécurité routière.

Dans ce chapitre, nous présenterons les concepts clés d'un environnement IoV, ses architectures IoV, ses protocoles, ses normes de communication et leurs performances. Nous explorerons également les principaux défis entourant un environnement IOV.

2. L'internet des véhicules

L'avènement de l'Internet des véhicules (IoV) a fondamentalement changé les systèmes de transport modernes [1]. Il fait référence à l'intégration des véhicules avec les réseaux de communication et les systèmes de transport intelligents pour créer un réseau de véhicules interconnectés. L'objectif principal d'IoV environnent est d'améliorer la sécurité routière, d'augmenter l'efficacité et la commodité des transports en permettant aux véhicules de communiquer entre eux et avec les infrastructures environnantes.

La technologie derrière IoV implique l'utilisation de divers protocoles de communication sans fil tels que Bluetooth, Wi-Fi et les réseaux cellulaires. Le réseau de capteurs est installé

dans les véhicules pour détecter et collecter des données telles que des informations sur le trafic, la prévision des conditions routières et d'autres informations pertinentes pour le conducteur. Ces données peuvent ensuite être transmises à d'autres véhicules et systèmes de gestion du trafic pour optimiser les itinéraires, réduire les embouteillages et améliorer la sécurité globale sur la route. Comme la technologie présente un grand potentiel, nous résumons ce qui suit :

- Les IoV ont la capacité de transformer la vie des gens en adoptant des schémas de mouvement intelligents et en interagissant avec tout ce qui les entoure [2]. Il peut accroître l'efficacité, la durabilité et la sécurité des transports. La technologie IoV permet au personnel d'urgence de réagir rapidement aux incidents. Il peut également tirer parti des voitures autonomes et d'autres technologies d'assistance pour améliorer les services de transport pour les personnes handicapées.
- Les entreprises peuvent également profiter de cette technologie et l'utiliser pour suivre et gérer à distance leur flotte de véhicules [2]. De meilleures routes et une meilleure utilisation du carburant peuvent également aider à réduire les dépenses d'exploitation. De plus, comme il encourage l'adoption d'options de transport plus respectueuses de l'environnement, il peut aider à réduire les émissions de carbone.
- L'utilisation généralisée de la technologie IoV soulève également des inquiétudes concernant la confidentialité et la sécurité des données [3]. Étant donné que les véhicules transmettent de grandes quantités de données sur des réseaux sans fil, il existe un risque d'accès non autorisé et d'utilisation abusive des données. Par conséquent, des mesures de confidentialité et de sécurité des données doivent être en place pour protéger les informations sensibles. De plus, il est nécessaire de réglementer l'utilisation de la technologie IoV. Des normes doivent être élaborées pour assurer l'interopérabilité entre les différents systèmes IoV et pour garantir que la technologie est utilisée de manière sûre et responsable.

2.1 Composants IoV

L'environnement Internet des véhicules (IoV) se développe rapidement car il espère transformer l'industrie du transport en construisant un réseau de voitures, de structures et d'autres équipements interconnectés qui peuvent interagir les uns avec les autres sur Internet. L'Internet des objets (IoT), un réseau d'objets physiques, de capteurs et de systèmes liés qui

interagissent et échangent des données sur Internet, sert de base à partir de laquelle l'environnement de l'Internet des objets (IoT) est développé.

L'environnement IoV a été créé pour permettre aux voitures de communiquer entre elles, avec l'infrastructure le long de la route et avec des appareils électroniques supplémentaires dans les environs afin de donner aux conducteurs des informations en temps réel sur les conditions de la route, la vitesse de la circulation et les dangers potentiels. En anticipant la fluidité du trafic, en réduisant les embouteillages et en réduisant le nombre d'accidents, l'objectif est d'accroître la sécurité routière, l'efficacité du trafic et de réduire l'impact environnemental.

L'environnement IoV se compose de quatre composants principaux : les véhicules, l'infrastructure, les technologies de communication et les plates-formes de données basées sur le cloud. Chacun de ces composants joue un rôle essentiel pour permettre à l'environnement IoV de fonctionner de manière efficace et efficiente.

- **Les véhicules** sont le composant principal de l'environnement IoV. Les véhicules modernes sont équipés d'une gamme de capteurs et de technologies de communication, telles que le GPS, le Wi-Fi, le cellulaire et le Bluetooth, qui leur permettent de communiquer avec d'autres véhicules, infrastructures et appareils. Les véhicules peuvent collecter et transmettre des données en temps réel, telles que la vitesse, l'emplacement et les diagnostics du véhicule, à d'autres véhicules ou à des plates-formes de données basées sur le Cloud.
- **Le composant d'infrastructure** de l'environnement IoV fait référence aux équipements et capteurs routiers intégrés, tels que les feux de signalisation, les capteurs et les caméras, qui sont utilisés pour collecter et transmettre des données sur les conditions routières et le flux de trafic. Le composant d'infrastructure est essentiel au fonctionnement de l'environnement IoV car il fournit des données en temps réel qui peuvent être utilisées pour optimiser le flux de trafic, réduire la congestion et prévenir les accidents.
- **Les technologies de communication** sont l'épine dorsale de l'environnement IoV. Les technologies de communication utilisées dans l'environnement IoV comprennent les réseaux cellulaires, le Wi-Fi, le Bluetooth et les communications dédiées à courte portée (DSRC). Ces technologies de communication permettent

aux véhicules de communiquer entre eux, avec l'infrastructure et avec d'autres appareils dans l'environnement.

- **Les plates-formes de données** basées sur le Cloud sont les plates-formes centralisées qui stockent et gèrent les énormes quantités de données générées par l'environnement IoV. Ces plates-formes utilisent des outils de méga données pour analyser les méga données du trafic et fournir des informations en temps réel qui peuvent être utilisées pour optimiser le flux de trafic, réduire les embouteillages et prévenir les accidents.

2.2 Technologies de communication dans l'environnement IoV

Les technologies de communication utilisées dans l'environnement IoV sont essentielles à son succès. Ces technologies permettent aux véhicules de communiquer entre eux, avec l'infrastructure et avec d'autres appareils dans l'environnement. Il existe plusieurs technologies de communication utilisées dans l'environnement IoV [4], notamment :

- **Le réseau cellulaire** est la technologie de communication largement utilisée dans l'environnement IoV. Les véhicules utilisent des réseaux cellulaires pour communiquer avec des plates-formes de données basées sur le Cloud et d'autres appareils dans l'environnement. L'avantage d'utiliser des réseaux cellulaires est qu'ils offrent une large couverture et peuvent prendre en charge des applications à large bande passante.
- **Le Wi-Fi** est une autre technologie de communication utilisée dans l'environnement IoV. Le Wi-Fi est principalement utilisé pour la communication à courte portée entre les véhicules et l'infrastructure. L'avantage d'utiliser le Wi-Fi est qu'il permet un transfert de données à haute vitesse et qu'il est rentable.
- **Le Bluetooth** est une autre technologie de communication à courte portée utilisée dans l'environnement IoV. Bluetooth est principalement utilisé pour la communication entre les appareils dans le véhicule, comme entre le système de divertissement du véhicule et le Smartphone du conducteur.

2.3 Normes IoV

L'Internet des véhicules (IoV) est un système complexe qui nécessite une normalisation pour assurer l'interopérabilité, la sécurité et la fiabilité des communications entre les différents appareils et systèmes. Voici quelques-unes des principales normes liées à l'IoV :

- **Les normes de communication** telles que Dedicated Short-Range Communications (*DSRC-IEEE 802.11p*) [5] et Cellular Vehicle-to-Everything (*C-V2X*) [6] sont essentielles pour permettre la communication entre les véhicules, l'infrastructure routière périphérique et d'autres dispositifs dans l'IoV. Ces normes garantissent que les appareils peuvent communiquer efficacement entre eux, fournissant des données en temps réel sur les conditions de circulation, la météo et d'autres informations importantes.
- **Les normes de sécurité** telles que ISO/SAE 21434 [7], ISO 27001 [8] et Security Credential Management System (*SCMS*)[9] sont nécessaires pour garantir un environnement IoV sécurisé. Ces normes fournissent des lignes directrices pour une communication et un échange de données sécurisés, ainsi que pour la protection des informations sensibles telles que les données personnelles et les informations financières.
- **Les normes de données** telles que l'Open Automotive Alliance (*OAA*) [10], GENIVI [11] et l'Open Connectivity Foundation (*OCF*) [12] garantissent que les données générées par les appareils IoV sont compatibles et facilement traitées sur différents systèmes. Ces normes fournissent des directives pour le formatage des données, les protocoles d'échange de données et la gestion des données, garantissant que les appareils IoV peuvent communiquer et fonctionner de manière transparente les uns avec les autres.
- **Les normes d'interopérabilité** telles que ISO 15118 [13], SAE J2735 [14] et Open ADR [15] sont nécessaires pour garantir que différents appareils et systèmes peuvent fonctionner ensemble de manière transparente dans l'environnement IoV. Ces normes fournissent des directives pour la communication des appareils et des systèmes, permettant l'interopérabilité et l'échange de données entre différents appareils et systèmes IoV.
- **Les normes de qualité** telles que ISO 26262 [16], Automotive SPICE [17] et la norme de sécurité fonctionnelle (ISO 26262) [18] garantissent que les appareils et systèmes IoV répondent à des exigences de qualité et de sécurité spécifiques. Ces normes fournissent des lignes directrices pour la conception, le développement et les tests des appareils et systèmes IoV, garantissant qu'ils répondent à des exigences de qualité et de sécurité spécifiques.

2.4 Applications IOV

Les applications ITS et smart city sont des applications IoV [19]. Les études des auteurs sur l'IoV en tant que service se sont concentrées sur les applications STI telles que la sécurité des conducteurs, l'efficacité du trafic et le divertissement. Le potentiel de l'IoV pour la détection, la collecte, le traitement et le stockage de données à grande échelle dans les villes intelligentes n'a pas été exploré. Les solutions IoV basées sur les STI donnent la priorité aux objets du véhicule et aux demandes de réseau. Cependant, les objets véhicules IoV répondent aux besoins de milliers d'objets de ville intelligente pour la collecte, la transmission, le traitement et le stockage de données opportunistes.

L'étude des systèmes de transport intelligents (*STI*) [19] intègre des technologies de pointe pour améliorer l'efficacité et la sécurité des systèmes de transport. Les applications IoV basées sur les STI [19] utilisent la technologie IoV pour améliorer les systèmes STI. Ces applications utilisent des véhicules, des infrastructures et d'autres données en temps réel pour optimiser le flux de trafic, prévenir les collisions, gérer le stationnement, améliorer les transports publics, surveiller les conditions routières et optimiser le fret et la logistique. Ces applications fournissent aux conducteurs, aux passagers et aux fournisseurs de transport des informations en temps réel pour les aider à prendre des décisions et à améliorer l'efficacité et la sécurité du système de transport. Les sous-applications de ce domaine incluent :

- Systèmes intelligents de gestion du trafic.
- Systèmes d'évitement de collision.
- Systèmes coopératifs véhicule-infrastructure.
- Systèmes avancés d'information des voyageurs.
- Systèmes de stationnement intelligents.
- Systèmes d'optimisation du fret et de la logistique.
- Systèmes de gestion des transports publics.
- Systèmes d'information météo routière.
- Systèmes de notification des véhicules d'urgence.
- Systèmes de surveillance de l'état des routes.

2.5 IoV dans les villes intelligentes

L'IoV peut être utilisé comme une alternative rentable pour répondre aux exigences des villes intelligentes en matière de collecte, de transmission et de traitement de données à grande échelle à partir d'objets intelligents dans un environnement de ville intelligente. Par rapport aux réseaux de capteurs sans fil traditionnels (WSN), les nœuds de véhicule au sein d'un IoV ne souffrent pas des contraintes de ressources liées à la puissance limitée de la batterie et aux limitations du traitement de l'information. Au sein de l'IoV, les véhicules agissent comme des nœuds mobiles ou des objets intelligents au sein du réseau de capteurs. Chaque objet véhicule dans un environnement de ville intelligente peut jouer quatre rôles :

1. L'objet véhicule fonctionne comme un nœud de réseau (homologue) pour établir et maintenir la connectivité réseau au sein de l'IoV lui-même.
2. L'objet véhicule fonctionne comme des clients pour consommer des services IoV et Internet.
3. L'objet véhicule fonctionne comme des collecteurs de données ou des "mules de données" pour collecter et transporter des données d'autres objets intelligents vers des centres de données au sein de la ville intelligente.
4. L'objet véhicule fonctionne comme une ressource informatique distribuée pour compléter les ressources limitées de traitement de l'information dans les objets intelligents (plus petits).

Actuellement, de nombreux travaux de recherche se sont concentrés sur l'IoV uniquement pour les rôles de (1) et (2). Cette section présente une discussion sur les rôles étendus de (3) et (4) pour les applications IoV dans les villes intelligentes. Voici quelques exemples d'applications IoV liées aux Smart-Cities :

- Systèmes intelligents de gestion du trafic.
- Systèmes de stationnement intelligents.
- Systèmes intelligents de gestion des déchets.
- Systèmes de gestion de la charge des véhicules électriques (VE).
- Systèmes de transport public intelligents.
- Passages piétons intelligents.
- Systèmes d'éclairage intelligents.
- Systèmes de surveillance environnementale.

- Systèmes intelligents de sécurité publique.
- Systèmes intelligents de gestion de l'eau.
- Systèmes de distribution autonomes.
- Systèmes intelligents de gestion de l'énergie.
- Systèmes d'agriculture urbaine.
- Systèmes de gestion de bâtiment intelligents.

2.6 Caractéristiques IOV

L'Internet des véhicules (IoV) se caractérise par plusieurs caractéristiques clés qui distinguent les systèmes de véhicules traditionnels et modernes [20]. Ces caractéristiques comprennent :

Connectivité : les systèmes IoV sont hautement connectés et s'appuient sur diverses technologies de communication, telles que la 5G, le Wi-Fi et le Bluetooth, pour permettre une communication en temps réel entre les véhicules, l'infrastructure et d'autres systèmes.

Collecte de données : les systèmes IoV collectent et traitent de grandes quantités de données provenant de diverses sources, telles que des capteurs, des caméras et des systèmes GPS. Ces données sont utilisées pour fournir des informations qui permettent une prise de décision intelligente et une optimisation des opérations.

Communication en temps réel : les systèmes IoV permettent une communication en temps réel entre les véhicules, l'infrastructure et d'autres systèmes. Cela permet un échange d'informations rapide et efficace, essentiel pour améliorer la sécurité routière et optimiser la fluidité du trafic.

Automatisation : les systèmes IoV permettent l'automatisation de diverses opérations, telles que la conduite autonome et le stationnement intelligent. Cela améliore l'efficacité, réduit le risque d'accidents et améliore la mobilité globale.

Sécurité : les systèmes IoV s'appuient sur une communication sécurisée et la protection des données pour garantir la sécurité et la confidentialité des utilisateurs. Ceci est essentiel pour prévenir les cyberattaques et maintenir l'intégrité des systèmes IoV.

La standardisation : les systèmes IoV nécessitent une standardisation des protocoles de communication et des formats de données pour assurer l'interopérabilité entre les différents

systèmes et appareils. Cela permet une intégration transparente et un fonctionnement efficace des systèmes IoV.

3. Réseaux 5G

La prochaine génération de réseaux est la technologie sans fil de cinquième génération (5G), qui promet d'offrir des vitesses Internet plus rapides, une latence plus faible et une plus grande capacité. Les réseaux 5G devraient permettre une large gamme de nouvelles applications et de nouveaux services qui étaient auparavant impossibles, tels que la réalité virtuelle et augmentée, les véhicules autonomes et la chirurgie à distance. Certaines des principales caractéristiques des réseaux 5G incluent [21] :

Des vitesses plus élevées : les réseaux 5G sont capables de fournir des vitesses de téléchargement maximales allant jusqu'à 20 Gbit/s, ce qui est nettement plus rapide que les réseaux 4G actuels.

Latence plus faible : la latence fait référence au temps nécessaire pour que les données se déplacent d'un point à un autre. Les réseaux 5G ont une latence plus faible que les réseaux 4G, ce qui signifie qu'ils peuvent fournir des services plus réactifs, tels que les jeux en temps réel et les vidéoconférences.

Une plus grande capacité : les réseaux 5G peuvent prendre en charge beaucoup plus d'appareils par unité de surface que les réseaux 4G, ce qui est particulièrement important dans les zones densément peuplées.

Network slicing : il s'agit d'une fonctionnalité des réseaux 5G qui permet aux opérateurs de créer plusieurs réseaux virtuels sur un seul réseau physique. Chaque réseau virtuel peut être personnalisé pour répondre aux exigences spécifiques des différents types de services.

Edge Computing : les réseaux 5G permettront également l'edge computing, ce qui implique de traiter les données au plus près de l'utilisateur final. Cela contribuera à réduire la latence et à améliorer les performances des applications nécessitant un traitement en temps réel.

Dans l'ensemble, les réseaux 5G sont sur le point de révolutionner la façon dont nous utilisons la technologie sans fil, ouvrant de nouvelles opportunités pour les entreprises et les consommateurs.

3.1 Génération de réseaux mobiles

L'évolution des réseaux mobiles a été marquée par des avancées technologiques importantes, apportant des vitesses plus rapides, une plus grande capacité et des fonctionnalités plus avancées. Dans ce qui suit, nous présenterons un aperçu des différentes générations de réseaux mobiles, de la première génération (1G) à la cinquième génération (5G).

1) La première génération (1G)

La 1G était la première génération de réseaux mobiles, lancée dans les années 1980. Cette génération était basée sur l'analogique et autorisait les appels vocaux, mais ne prenait pas en charge le transfert de données. La technologie utilisée dans le réseau 1G n'était pas très efficace et la qualité des appels était souvent médiocre.

2) La deuxième génération (2G)

La 2G a été lancée dans les années 1990 et constituait une amélioration significative par rapport à la 1G. Les réseaux 2G étaient basés sur le numérique, ce qui signifiait qu'ils étaient plus efficaces et pouvaient prendre en charge le transfert de données. Les réseaux 2G offraient des services tels que la messagerie texte et un accès Internet de base. Les technologies 2G les plus courantes étaient le GSM (*Global System for Mobile Communications*) [22] et le CDMA (*Code Division Multiple Access*) [23].

3) La troisième génération (3G)

La 3G a été lancée au début des années 2000 et a marqué une amélioration significative par rapport aux réseaux 2G. Les réseaux 3G offraient des taux de transfert de données plus rapides et des services plus avancés, tels que les appels vidéo et l'accès Internet mobile. Les technologies 3G les plus courantes étaient l'UMTS (*Universal Mobile Telecommunications System*) [24] et le CDMA2000 (*Code Division Multiple Access 2000*) [24].

4) La troisième génération et demie (3.5G)

La 3.5G était une autre phase de transition entre les réseaux 3G et 4G. Les réseaux 3.5G ont fourni des taux de transfert de données plus rapides que la 3G, mais pas aussi rapides que la 4G. L'amélioration la plus significative par rapport à la 3G a été l'introduction du HSPA

(*High-Speed Packet Access*) [24], qui a permis des taux de transfert de données encore plus rapides.

5) La quatrième génération (4G)

La 4G a été lancée dans les années 2010 et a marqué une amélioration significative par rapport aux réseaux 3G. Les réseaux 4G offraient des vitesses plus rapides et une plus grande capacité, permettant un streaming vidéo et des jeux mobiles de haute qualité. Les technologies 4G les plus courantes étaient LTE (*Long-Term Evolution*) [24] et WiMAX (*Worldwide Interoperability for Microwave Access*) [24].

6) La quatrième génération et demie (4.5G)

La 4.5G était une phase de transition entre les réseaux 4G et 5G. Les réseaux 4.5G ont fourni des taux de transfert de données plus rapides que la 4G, mais pas aussi rapides que la 5G. L'amélioration la plus significative par rapport à la 4G a été l'introduction de LTE Advanced Pro [24], qui a permis des taux de transfert de données encore plus rapides.

7) La cinquième génération (5G)

La 5G est la dernière génération de réseaux mobiles et est actuellement déployée dans de nombreux pays du monde. Les réseaux 5G promettent des vitesses encore plus rapides, une latence plus faible et une plus grande capacité, permettant une large gamme de nouvelles applications et services. Les réseaux 5G devraient prendre en charge diverses nouvelles technologies, telles que les véhicules autonomes, la chirurgie à distance et la réalité virtuelle et augmentée [25].

3.2 Le 5G technologies

La cinquième génération de réseaux mobiles promet d'apporter des améliorations significatives en termes de vitesse, de capacité et de fonctionnalité par rapport à ses prédécesseurs. La technologie derrière la 5G est complexe et implique plusieurs technologies et normes différentes. Dans ce qui suit, nous aborderons certaines des technologies clés de la 5G :

3.2.1 RAN (Radio Access Networks)

Le système de réseau d'accès radio (*RAN*) [26] de nouvelle génération est considéré comme un véritable réseau mondial sans fil. En effet, un tel système connectera tout de manière transparente et omniprésente et prendra en charge au moins 1 000 volumes de trafic, 100 milliards d'appareils sans fil connectés et divers cas d'utilisation ainsi que des exigences de qualité de service (*QoS*) (*par exemple, fiabilité, latence, débit de données, couverture, sécurité et confidentialité*) des applications multimédias d'ici 2020 [26]. Récemment, un certain nombre de défis de recherche, notamment une croissance explosive des volumes de trafic mobile, des appareils connectés sans précédent et divers cas d'utilisation, ont été identifiés pour les systèmes 5G-RAN. De plus, des technologies spécifiques telles que la communication multi niveaux, le MIMO massif [26], le *Backhauling mmWave* [26], les densifications extrêmes de nœuds (*UDN*) [26], les communications en duplex intégral (*FDC*) [26] et les techniques de récupération d'énergie ont émergé dans le littérature, pour résoudre certains de ces défis 5G-RAN. Cependant, les activités de recherche définissant des avancées techniques spécifiques pour les systèmes 5G-RAN doivent encore se poursuivre au cours de la prochaine demi-décennie avant que les spécifications de normalisation et de commercialisation ne soient conclues. Dans ce cas, ces recherches sont motivées par le nombre limité d'études existantes sur ces avancées techniques dans une perspective plus large (c'est-à-dire la gestion des interférences, l'efficacité du spectre et les schémas d'économie d'énergie).

Le RAN comprend un certain nombre de composants, notamment des stations de base (*également appelées sites cellulaires*), des antennes et d'autres équipements qui transmettent et reçoivent des signaux sans fil. Ces composants sont généralement installés sur des tours cellulaires ou d'autres structures hautes, et sont utilisés pour créer des cellules, qui sont les éléments de base d'un réseau mobile.

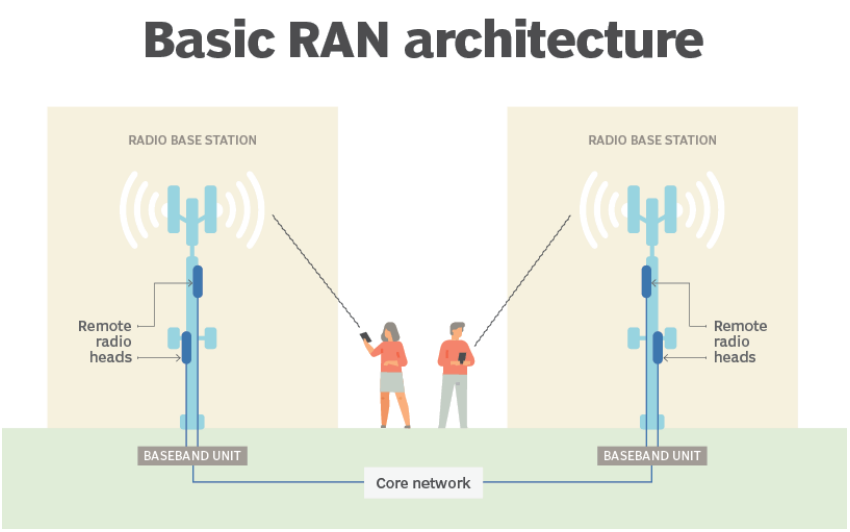

Figure 1 Architecteure RAN basic [27]

Chaque cellule couvre une zone géographique spécifique, et lorsque les utilisateurs se déplacent entre les cellules, leurs appareils sont transférés d'une station de base à une autre. Ce processus de transfert est géré par le RAN, qui garantit que la connexion de l'utilisateur reste ininterrompue lors de ses déplacements.

Le RAN est un élément essentiel des réseaux mobiles modernes et évolue constamment pour prendre en charge de nouvelles technologies et de nouveaux services. Par exemple, les derniers réseaux 5G utilisent des techniques avancées telles que la formation de faisceaux [26] et le MIMO massif [26] pour améliorer la capacité et les performances du réseau, et le RAN joue un rôle clé dans la mise en œuvre de ces technologies.

3.2.2 Cloud Computing

Le Cloud Computing (CC) est un modèle de fourniture de ressources informatiques [28] (telles que des serveurs, du stockage, des bases de données, des réseaux, des logiciels et des analyses) sur Internet. Il permet aux utilisateurs d'accéder aux ressources informatiques et de les utiliser sans avoir à se soucier de l'infrastructure sous-jacente, de la maintenance ou de la gestion. Le CC est généralement fourni par des fournisseurs tiers et est accessible via un navigateur Web ou une interface de programmation d'application (*API*).

En bref, le CC est un terme large qui englobe un large éventail de technologies et de services liés à la fourniture de ressources informatiques sur Internet. Dans ce qui suit, nous donnerons un aperçu de la technologie du CC y compris sa définition, son histoire, ses

avantages, ses défis et ses tendances futures. En quoi, il offre de nombreux avantages [28], notamment :

Évolutivité : les ressources de CC peuvent être augmentées ou réduites rapidement et facilement, en fonction des besoins de l'utilisateur. Cela permet aux utilisateurs de s'adapter facilement aux changements de la demande, sans avoir à se soucier de l'infrastructure sous-jacente.

Flexibilité : les ressources de CC sont accessibles de n'importe où avec une connexion Internet, ce qui permet aux utilisateurs de travailler facilement de n'importe où et sur n'importe quel appareil.

Rentabilité : les fournisseurs de CCfacturent généralement leurs services en fonction de l'utilisation, ce qui signifie que les utilisateurs ne paient que ce dont ils ont besoin. Cela permet aux utilisateurs d'éviter les coûts associés à la possession et à la maintenance de leur propre infrastructure.

Fiabilité : les fournisseurs de CC offrent généralement des niveaux élevés de fiabilité et de disponibilité, ce qui signifie que les utilisateurs peuvent accéder à leurs ressources quand ils en ont besoin.

Sécurité : les fournisseurs de CC proposent généralement des mesures de sécurité robustes pour protéger les données et les ressources de leurs utilisateurs, notamment le cryptage, les pare-feu et les contrôles d'accès.

3.2.3 FoG Computing

Le Fog Computing (FC), également connu sous le nom de Edge Computing (EC), est une architecture informatique distribuée qui étend les capacités de CC à la périphérie du réseau [28]. Le FC est conçu pour répondre aux limites du CC en permettant aux ressources informatiques d'être situées plus près de l'endroit où les données sont générées et consommées, généralement à la périphérie du réseau [28].

De plus, le FC est un type d'informatique décentralisée qui implique le déploiement de ressources informatiques, telles que des serveurs, des périphériques de stockage et des équipements réseau, à proximité de l'endroit où les données sont générées et consommées. Cela permet un traitement à faible latence et des temps de réponse plus rapides [28], ce qui est

particulièrement important pour les applications en temps réel telles que les appareils de l'Internet des objets (IoT), les véhicules autonomes et d'autres applications sensibles au facteur temps.

Le principal avantage du FC est qu'il permet des temps de traitement et de réponse plus rapides en réduisant la distance entre la source de données et la ressource informatique [28]. Cela réduit la latence associée à l'envoi de données à un serveur Cloud distant pour traitement et permet une prise de décision et une action plus rapides [28].

Un autre avantage du FC est qu'il réduit la quantité de données qui doit être envoyée sur le réseau à un serveur Cloud distant, ce qui peut être particulièrement important pour les applications avec une bande passante limitée ou des volumes de données élevés. En traitant les données localement, à la périphérie du réseau, seules les données pertinentes doivent être envoyées au Cloud pour stockage ou traitement ultérieur, réduisant la bande passante réseau requise [28].

Le FC permet une utilisation plus efficace des ressources de CC en déchargeant une partie du traitement du Cloud vers la périphérie du réseau. Cela peut aider à réduire la charge sur les serveurs Cloud et à améliorer l'évolutivité des systèmes de CC.

Dans l'ensemble, le FC est un développement important dans l'évolution des architectures informatiques distribuées, offrant un moyen plus efficace et évolutif de traiter et de gérer les données à la périphérie du réseau. À mesure que de plus en plus d'appareils se connectent à Internet et génèrent de gros volumes de données, le FC devrait devenir de plus en plus important pour permettre des applications et des services plus rapides et plus réactifs.

3.2.4 Edge Computing

L'informatique de périphérie est un paradigme informatique distribué qui rapproche les ressources informatiques de la périphérie du réseau, là où les données sont générées et consommées, plutôt que dans des centres de données centralisés [29]. Dans l'informatique de périphérie, les services de traitement, de stockage et de mise en réseau des données sont fournis par des nœuds situés à la périphérie du réseau, tels que des routeurs, des passerelles et des appareils IoT, plutôt que par des serveurs centralisés.

L'objectif de l'EC est de réduire les exigences de latence et de bande passante associées à l'envoi de données vers des centres de données centralisés pour traitement, ce qui peut être

particulièrement important dans les applications qui nécessitent un traitement en temps réel, telles que l'automatisation industrielle, les véhicules autonomes et les soins de santé.

L'EC peut être vu comme un complément au CC, qui se concentre sur la centralisation des ressources informatiques dans les centres de données. Dans l'informatique de pointe, les ressources informatiques sont réparties sur un réseau de nœuds, qui peut inclure des appareils tels que des capteurs, des caméras et des appareils mobiles, ainsi que des serveurs locaux et des passerelles. Ces nœuds peuvent être situés dans divers environnements, tels que des installations industrielles, des magasins de détail et des habitations.

L'EC offre plusieurs avantages par rapport aux modèles informatiques centralisés traditionnels [29], notamment :

- Latence réduite : en traitant les données plus près de la périphérie du réseau, l'informatique de périphérie peut réduire la latence associée à l'envoi de données vers des centres de données centralisés.
- Fiabilité améliorée : l'informatique de périphérie peut améliorer la fiabilité des applications en réduisant la dépendance vis-à-vis des centres de données centralisés et des connexions réseau qui les relient.
- Besoins réduits en bande passante : en traitant les données à la périphérie du réseau, l'informatique de périphérie peut réduire la quantité de données qui doit être envoyée aux centres de données centralisés pour le traitement, ce qui peut réduire les besoins en bande passante.
- Améliorer la sécurité des données : L'EC permet d'améliorer la sécurité des applications en réduisant la surface d'attaque associée aux centres de données centralisés et aux connexions réseau qui les relient.

L'Edge Computing en 5G peut avoir les rôles suivants [29] :

- Stockage local.
- Calcul local.
- Prise de décision locale.
- Opération locale.
- Amélioration de la sécurité locale.

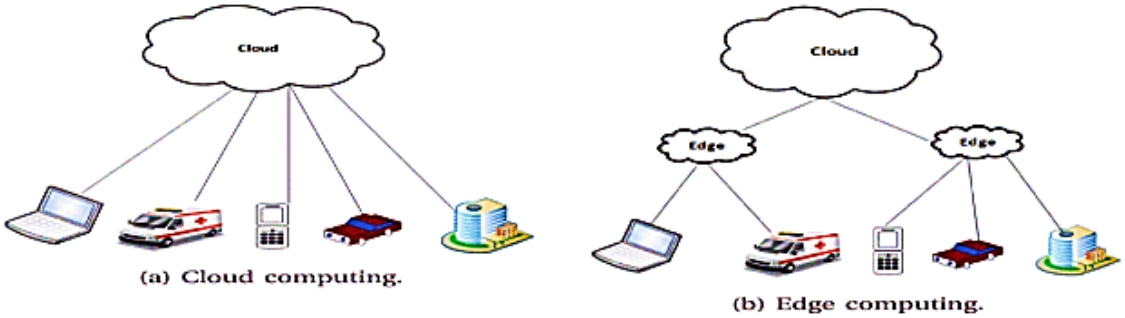

Figure 2 Difference between cloud with edge and fog [29]

3.2.5 5G Network function virtualization (NFV)

Dans le contexte des réseaux 5G, la virtualisation des fonctions réseau (*NFV*) [30] joue un rôle essentiel en permettant le déploiement et la gestion des différentes fonctions réseau nécessaires pour prendre en charge les services 5G. L'objectif de NFV dans les réseaux 5G est de créer une infrastructure flexible, agile et rentable qui peut prendre en charge un large éventail de cas d'utilisation et d'applications.

L'une des fonctions clés activées par NFV dans les réseaux 5G est la virtualisation du réseau d'accès radio (*RAN*). En virtualisant le RAN, les opérateurs de réseau peuvent déployer et gérer le RAN de manière plus efficace et flexible, tout en réduisant les coûts. Cela se fait en utilisant la virtualisation logicielle pour créer des fonctions RAN virtuelles qui peuvent être allouées, mises à l'échelle et gérées de manière dynamique [30].

Une autre fonction importante que NFV active dans les réseaux 5G est Mobile EC (*MEC*). Le MEC implique le déploiement de ressources informatiques à la périphérie du réseau, plus près de l'endroit où se trouvent les utilisateurs et les appareils. En virtualisant les fonctions MEC, les opérateurs peuvent fournir des services à faible latence et à large bande passante qui nécessitent un traitement plus proche de la périphérie, tels que les applications de réalité augmentée et de réalité virtuelle.

NFV permet également la virtualisation d'autres fonctions réseau importantes, telles que le réseau central, la gestion du trafic et les fonctions de sécurité. En virtualisant ces fonctions, les opérateurs peuvent plus facilement faire évoluer et gérer leur infrastructure réseau, tout en réduisant les coûts.

En plus de virtualiser les fonctions réseau individuelles, NFV permet également la création de tranches de réseau. Le découpage de réseau implique la création de réseaux virtuels adaptés aux exigences spécifiques de différents cas d'utilisation et applications. En utilisant NFV pour créer des fonctions réseau virtualisées, les opérateurs peuvent plus facilement créer et gérer des tranches de réseau, offrant une plus grande flexibilité et agilité.

Dans l'ensemble, la fonction NFV est un catalyseur essentiel des réseaux 5G, offrant la flexibilité, l'évolutivité et les économies de coûts nécessaires pour prendre en charge le large éventail de cas d'utilisation et d'applications que la 5G promet de fournir. En virtualisant les fonctions réseau clés, les opérateurs peuvent créer une infrastructure plus agile et plus réactive, capable de s'adapter à l'évolution des besoins des utilisateurs et à l'évolution de la dynamique du marché.

3.2.6 Software-Defined Networking (SDN)

La mise en réseau définie par logiciel, ou SDN, est un moyen de créer des réseaux où le plan de contrôle et le plan de données sont séparés. Dans la conception de réseau standard, les plans de contrôle et de données sont intégrés dans les mêmes périphériques physiques, tels que les routeurs et les commutateurs.

Dans SDN, le plan de contrôle est déplacé vers un gestionnaire unique, ce qui facilite la gestion et l'automatisation des tâches réseau. Le contrôleur gère le réseau en communiquant avec les commutateurs et les routeurs. Les commutateurs et les routeurs envoient ensuite des paquets de données là où le contrôleur leur dit d'aller. Le routeur peut être configuré pour faire différentes choses pour le réseau, comme la planification, la protection et l'équilibrage de charge [31], comme la figure 3 :

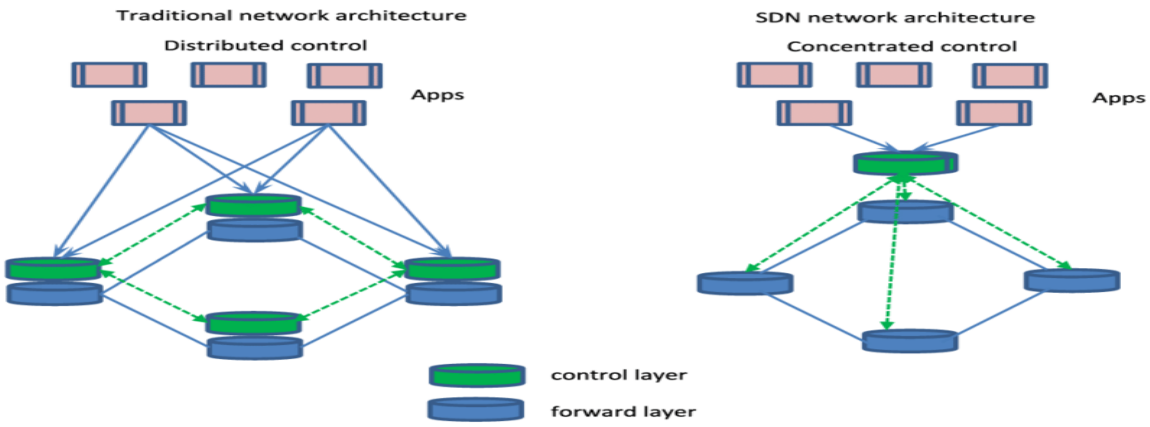

Figure 3 Réseau traditionnel et SDN [32]

La couche de base, la couche de contrôle et la couche d'application sont les trois parties de la conception SDN.

- La couche d'infrastructure.
- La couche de contrôle.
- La couche d'application.

3.3 Architectures réseaux 5G

Les réseaux 5G sont conçus pour fournir des débits de données plus élevés, une latence plus faible et une meilleure connectivité par rapport aux générations précédentes de réseaux sans fil. L'architecture des réseaux 5G repose sur plusieurs composants clés, notamment le réseau d'accès radio (RAN), le réseau central et l'infrastructure informatique de pointe.

3.3.1 Radio Access Network (RAN)

Le RAN est chargé de connecter les appareils au réseau sans fil et de donner aux utilisateurs l'accès aux services du réseau. Dans les réseaux 5G [33], le RAN est construit sur une nouvelle conception appelée 5G New Radio (*5G NR*) et utilise une gamme de bandes de fréquences, y compris des fréquences inférieures à 6 GHz et à ondes millimétriques (*mmWave*). Le RAN comprend deux parties principales : la station de base (également appelée gNB ou nouvelle station de base radio) et l'équipement utilisateur (*UE*), qui comprend des appareils tels que les Smartphones et d'autres appareils cellulaires.

3.3.2 Core Network

Le réseau central gère et contrôle la façon dont les données se déplacent entre le RAN et d'autres réseaux, comme Internet et les réseaux privés. Le réseau principal des réseaux 5G est construit sur une nouvelle conception appelée 5G principal (*5GC*), qui se veut plus flexible, évolutive et efficace que les réseaux mobiles du passé. Le 5GC comprend plusieurs parties importantes, telles que les fonctions réseau (*NF)* qui fournissent des services réseau, les tranches de réseau qui permettent de fournir différents types de services sur la même infrastructure réseau et l'architecture basée sur les services (*SBA*) qui la rend plus facile à déployer et à faire évoluer les fonctions réseau.

3.3.3 Infrastructure de Edge Computing

L'infrastructure informatique Edge est conçue pour traiter et stocker les données à proximité de l'endroit où elles sont créées et utilisées. Cela peut réduire la latence et améliorer

les performances des applications qui doivent traiter des données en temps réel, comme les véhicules autonomes et les applications de réalité augmentée. Le matériel informatique Edge est généralement installé à la périphérie des réseaux 5G, à proximité du RAN et des réseaux principaux. L'infrastructure informatique Edge peut comprendre de nombreuses parties différentes, telles que des serveurs Edge, des ports et des réseaux de diffusion de contenu (*CDN*). Ces composants sont destinés à fournir aux applications nécessitant une gestion des données en temps réel des ressources de calcul et de stockage hautes performances avec un faible délai.

L'architecture des réseaux 5G est conçue pour être plus flexible, évolutive et efficace que l'architecture des réseaux sans fil des versions antérieures. En utilisant de nouvelles technologies telles que la 5G New Radio, la 5G Core et l'infrastructure informatique de pointe, les réseaux 5G devraient être en mesure de prendre en charge une large gamme de nouveaux services et applications, tels que les véhicules autonomes, les villes intelligentes et la réalité augmentée, qui nécessitent une haute- vitesse, connexions à faible latence et capacité à traiter les données en temps réel.

5. Conclusion

En conclusion, l'Internet des véhicules (IoV) et les réseaux 5G sont deux technologies qui changent notre façon de penser le mouvement, la communication et la connexion. L'IoV prévoit de relier les voitures, les chauffeurs et les équipements de transport à Internet et à d'autres réseaux numériques. Cela rendra les systèmes de transport plus sûrs, plus efficaces et plus intelligents. Pendant ce temps, les réseaux 5G sont plus rapides, ont moins de retard et peuvent gérer plus de données que les versions antérieures des réseaux sans fil. Cela donne à l'IoV et aux autres technologies liées de nouvelles façons de travailler.

Bien que les réseaux IoV et 5G présentent de nombreux avantages potentiels, il existe également des défis importants qui doivent être relevés afin de réaliser pleinement leur potentiel. Il s'agit notamment d'assurer la sécurité et la confidentialité des données, de promouvoir l'interopérabilité et la normalisation, de gérer de grandes quantités de données et de garantir l'accessibilité et l'abordabilité pour tous.

L'avenir du transport et de la connectivité évolue rapidement, avec les réseaux IoV et 5G à la pointe de cette transformation. En relevant les défis et en tirant parti des opportunités

présentées par ces technologies, nous pouvons construire des systèmes de transport plus sûrs, plus efficaces et plus intelligents qui améliorent la vie des personnes dans le monde entier.

CHAPTER 2 : État de l'art des techniques de diffusion de l'information dans l'environnement IoV

1. Introduction

L'Internet des véhicules (IoV) est un nouveau concept qui vise à intégrer les réseaux de véhicules dans l'environnement de l'Internet des objets (IdO). L'objectif principal de l'IoV est d'améliorer la sécurité, l'efficacité et la commodité de la conduite en interconnectant les véhicules entre eux ainsi qu'avec l'infrastructure et d'autres appareils. Pour cela, les véhicules sont équipés de capteurs et d'outils de communication qui leur permettent de partager des données avec d'autres véhicules et infrastructures.

Ces données comprennent des informations telles que la localisation, la vitesse, la direction du véhicule, ainsi que des données provenant de caméras et de radars. Pour faciliter cette interconnexion, différentes technologies avancées sont utilisées, notamment la connectivité radio, le CC et le Big Data. Les données collectées sont ensuite transmises à des unités centrales ou à des services Cloud, où elles sont analysées et traitées en temps réel. Ce traitement des informations est essentiel pour la prise de décision, ce qui permet d'améliorer la gestion du trafic, d'optimiser les itinéraires et d'offrir un confort accru aux conducteurs.

Par exemple, une communication fiable entre les véhicules permet une détection précoce des accidents potentiels et d'autres dangers sur la route, avec une alerte immédiate des conducteurs. Les systèmes avancés d'aide à la conduite peuvent également contribuer à identifier et à éviter certains types d'accidents, améliorant ainsi la sécurité routière. De plus, les systèmes de stationnement intelligents facilitent la recherche de places de stationnement disponibles.

Dans ce chapitre, nous examinons en détail les architectures de l'Internet des véhicules (IoV), en abordant sa classification et ses protocoles. Nous explorons également le cadre et les composants nécessaires à la connectivité IoV, à l'échange de données et à la communication entre les véhicules et l'infrastructure.

2. La Classification De l'internet Des Véhicules

L'Internet des véhicules (IoV) peut être classé en différents groupes en fonction de facteurs tels que la technologie de communication utilisée, le degré d'automatisation et le domaine d'application [35]. Il existe deux types de modèles de communication d'interaction dans l'écosystème IoV : les modèles d'interaction intra-véhicule et les modèles d'interaction inter-véhicule, comme illustré dans la figure suivante.

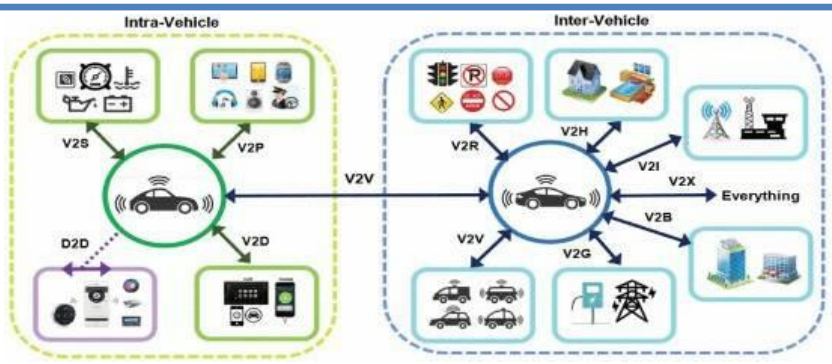

Figure 4 Les modèles de communication d'interaction IoV [35]

2.1 Modèles d'interaction intra-véhicule

La communication intra-véhicule fait référence à l'échange d'informations entre différents systèmes électriques à l'intérieur d'un véhicule. Cette communication interne joue un rôle crucial dans l'amélioration des fonctionnalités et de l'expérience client. En effet, il constitue la base du contact véhicule à véhicule au sein de l'Internet des Véhicules (IoV), et sa pertinence est donc primordiale pour le succès global du système [34], ce modèle comprend les sous-modèles suivants :

2.1.1-Vehicle-to-Cloud (V2C): avec ce modèle, les véhicules peuvent communiquer avec des services Cloud (*par exemple, contrôle du trafic, navigation, divertissement, etc*.). La connectivité V2C peut fournir aux conducteurs et aux passagers des services personnalisés et des informations de localisation en temps réel [36].

2.1.2-Vehicle-to-Infrastructure (V2I): Les véhicules utilisent ce modèle pour communiquer avec les infrastructures routières telles que les panneaux de signalisation et les horodateurs. L'interaction V2I donne aux conducteurs des informations sur le trafic en temps réel telles que la météo, le stationnement et l'amélioration de la fluidité du trafic [37].

2.1.3-Vehicle-to-Sensors (V2S): ce type de communication connecte les équipements de bas niveau (*capteurs, moteurs, etc*.) à l'infrastructure et à d'autres appareils utilisant plusieurs technologies pour mettre en œuvre l'IoV. il peut détecter certains problèmes tels que des dysfonctionnements d'équipements, des pertes de connectivité, des capacités de traitement et de stockage limitées [38].

2.1.4-Vehicle-to-Driver (V2D): ce modèle de communication convient aux motos équipées d'un système d'interaction innovant qui permet la communication avec le pilote, lui-même et l'environnement. Ce système utilise un Smartphone comme composant central,

profitant à la fois de ses fonctionnalités de base et de la technologie sans fil Bluetooth. La moto est équipée d'un adaptateur CAN-Bluetooth qui se connecte de manière transparente au Smartphone. Agissant comme un pont, le Smartphone facilite la communication entre la moto et divers périphériques, comme un casque audio et un serveur web [39].

2.2 Modèles de communication d'interaction inter-véhicule IoV

La communication inter-véhicules (IVC) met en œuvre des modes de communication entre les véhicules et le système IoV en partageant des informations. Cela rendrait le déplacement de ces systèmes plus rapide, plus facile et plus sûr. Les systèmes IoV utilisent souvent un certain nombre de schémas de transmission entre véhicules, à savoir [35] :

2.2.1 Vehicle-to-Vehicle (V2V): ce type de contact se produit entre deux voitures ou plus pour partager des informations sur leur emplacement, leur vitesse et leur direction. Le contact de véhicule à véhicule (V2V) permet aux voitures de se parler et de travailler ensemble, ce qui peut rendre les routes plus sûres et réduire le trafic [40].

2.2.2 Vehicle-to-Pedestrian (V2P): par des pas ou d'autres éléments non véhiculaires, tels que des vélos ou des scooters, et les voitures se parlent en utilisant ce modèle de communication pour partager des informations. Le contact V2P peut aider à rendre les rues plus sûres et à réduire les accidents en permettant aux voitures de savoir quand et où se trouvent les gens [41].

2.2.3 Vehicle-to-Roadside (V2R): ce type de communication permet aux automobiles et aux infrastructures publiques telles que les feux de circulation, les caméras et les capteurs de communiquer dans l'Internet des automobiles (IoV). V2R donne aux automobiles des informations en temps réel sur le trafic, les dangers de la route et la météo. Ces données peuvent améliorer la sécurité routière, le trafic et l'itinéraire [42].

- Gestion du trafic : les feux de circulation et les caméras donnent aux voitures des informations sur le trafic afin qu'elles puissent éviter de rester coincées dans la circulation.
- Services d'urgence : La communication V2R aide les véhicules d'urgence à se rendre rapidement et en toute sécurité sur les lieux des accidents en communiquant avec l'infrastructure routière.

- Avertissements de danger routier : les capteurs routiers sur la route peuvent détecter les dangers tels que la glace, les nids-de-poule ou les débris et avertir les véhicules à proximité de les éviter.
- Informations de stationnement : la communication V2R aide les conducteurs à trouver rapidement une place de stationnement et réduit les embouteillages en partageant les informations de stationnement disponibles.

2.2.4 Vehicle-to-Barrier (V2B): Le véhicule communique avec la porte/barrière (*péage, parking, poste frontière*). La communication V2B permet aux véhicules de communiquer avec des barrières ou des portails d'accès ou de paiement sans interaction humaine [43].

- Toll Collection : la communication V2B permet aux véhicules de payer automatiquement les péages sans s'arrêter.
- Parking Access : la communication V2B permet aux voitures d'entrer et de sortir des aires de stationnement sans que le conducteur ait besoin de prendre un ticket ou de payer à une borne.
- Contrôle aux frontières : la communication V2B aide les véhicules à franchir les frontières plus rapidement sans interaction du conducteur avec un agent de contrôle aux frontières humain.
- Portillons de sécurité : la communication V2B permet aux véhicules de franchir les portillons de sécurité sans que le conducteur n'ouvre et ne ferme le portillon.

2.2.5 Vehicle-to-Home (V2H): les véhicules communiquent avec la maison intelligente, contrôlent les appareils et les systèmes. La communication V2H permet aux véhicules de stocker et de gérer l'énergie pour la maison ; cela aide le propriétaire à économiser sur les coûts énergétiques [44].

- Stockage d'énergie : les véhicules peuvent stocker de l'énergie supplémentaire provenant de l'énergie solaire ou éolienne et la restituer plus tard à la maison.
- Alimentation de secours d'urgence : lors d'une panne de courant, le V2H peut utiliser la voiture pour alimenter la maison, fournissant une alimentation de secours pour les appareils et systèmes importants.
- Intégration de la maison intelligente : la communication V2H aide les véhicules à communiquer avec les appareils de la maison intelligente comme les thermostats et les lumières. Cela économise de l'énergie et rend la vie plus efficace.

2.2.6 Vehicle-to-Grid: Le V2G et la communication avec le réseau permettent aux véhicules électriques d'économiser de l'énergie lorsqu'ils ne sont pas utilisés, ce qui en fait des batteries mobiles pour le réseau [45]. De plus, l'intégration des énergies renouvelables permet aux véhicules électriques d'économiser de l'énergie supplémentaire provenant de l'énergie éolienne et solaire et de la restituer au réseau en cas de besoin.

3. Les Protocoles IoV

Comme mentionné précédemment, l'IoV (*Internet Vehicle Integration*) fait référence à l'interopérabilité des véhicules avec Internet et d'autres réseaux de communication. Les protocoles IOV permettent aux véhicules, à l'infrastructure et aux services Cloud de se connecter et d'échanger des données. Ces protocoles jouent un rôle crucial dans la communication entre les véhicules, l'infrastructure routière et les services basés sur le Cloud.

Les protocoles IOV sont d'une grande importance pour les applications et services de transport et automobiles. Ils facilitent la communication en temps réel entre les véhicules, leur permettant de partager des informations entre eux. De plus, ces protocoles garantissent la sécurité, la fiabilité et l'interopérabilité du système IOV avec d'autres systèmes [46].

L'IoT utilise divers protocoles de communication V2X pour diverses communications, c'est-à-dire des actions IoV qui se produisent pour sécuriser l'IoV. Ces protocoles aident un système à interagir sans fil dans l'environnement IoV et fournissent des informations sur le trafic, les stations-service et les services routiers.

Il existe plusieurs protocoles et normes différents utilisés dans IoV, notamment :

3.1 Dedicated Short-Range Communication (*DSRC*): le DSRC est un protocole permettant aux véhicules de communiquer à l'aide d'une communication sans fil à courte portée. Il utilise la fréquence de 5,9 GHz à des fins de sécurité, comme éviter les collisions et avertir les urgences. Si une voiture s'arrête soudainement devant vous, le système DSRC de votre voiture peut envoyer un avertissement à votre tableau de bord [46].

3.2C-V2X (*Cellular Vehicle-to-Everything*): C-V2X est un protocole mobile qui connecte les véhicules, les infrastructures et les appareils à l'aide de réseaux cellulaires. Il fonctionne sur les réseaux LTE et 5G et est utilisé pour la gestion du trafic, les diagnostics à distance et le divertissement en voiture. Si votre voiture est équipée du C-V2X, elle peut

obtenir des mises à jour sur le trafic et suggérer de nouveaux itinéraires pour éviter le trafic [47].

3.3Vehicular Ad Hoc Network (*VANET*): VANET connecte les voitures pour construire un réseau sans unité centrale. Il est utilisé pour les pelotons, où les voitures roulent à proximité pour économiser du carburant [48]. Les camions dotés de la technologie VANET peuvent rouler en groupe appelé peloton, chaque camion gardant une distance de sécurité par rapport à celui qui le précède, ce qui améliore l'utilisation du gaz et améliore la fluidité du trafic.

3.4 Message Queuing Telemetry Transport (*MQTT*): MQTT est un protocole IoT pour la communication des appareils. Les appareils peuvent envoyer des messages à un courtier central et d'autres appareils peuvent les recevoir. Le MQTT peut partager des données de trafic et météorologiques pour améliorer la sécurité et l'efficacité dans IoV. Si les véhicules détectent une route glissante, ils peuvent envoyer un avertissement aux autres voitures en utilisant MQTT [49].

3.5 Extensible Messaging and Presence Protocol (*XMPP*): le XMPP [50] est un protocole de communication d'appareils en temps réel. Il est utilisé dans les chats et peut aider les véhicules et les appareils à communiquer dans IoV. Un client XMPP peut recevoir des messages en temps réel d'un système de trafic sur les fermetures de routes ou les accidents, afin que le conducteur puisse modifier son itinéraire.

3.6 ITS-G5 (*Intelligent Transport Systems - Global System for Mobile Communications*): Ce protocole aide les véhicules et l'infrastructure routière à communiquer sans fil; il utilise 5,9 GHz et dispose d'une communication rapide et fiable [51].

3.7 OBD-II (*On-Board Diagnostics*): Ce protocole aide l'ordinateur de bord à communiquer avec des appareils extérieurs pour les diagnostics. Il montre les performances du moteur, l'efficacité énergétique et les niveaux d'émission [52].

3.8 CAN (*Controller Area Network*): Ce protocole aide les composants électroniques d'un véhicule à communiquer entre eux, par exemple le module de commande du moteur, le module de commande de transmission et les affichages du tableau de bord. C'est un moyen de communication bon marché et fiable [53].

3.9 J1939 (*Society of Automotive Engineers J1939*): Ce protocole est destiné à la communication entre les gros véhicules utilitaires tels que les camions et les bus, est un

système de surveillance des performances des moteurs, de la transmission et d'autres parties du véhicule [54].

3.10 ISO 15118 (*Vehicle to Grid*): Ce protocole relie les véhicules électriques et le réseau électrique. Il aide la voiture à communiquer avec le réseau pour la charge, la gestion de l'alimentation et les services réseau [55].

4. Modèles de Communication pour IoV

Les approches de communication dans IoV sont classées en modèles centralisés et modèles distribués. Les modèles centralisés ont une autorité centrale qui gère la communication entre les véhicules, l'infrastructure et le Cloud [56]. Les voitures envoient des données à un serveur qui partage des informations. Les modèles distribués permettent aux véhicules et aux infrastructures de communiquer directement sans autorité centrale. Les voitures communiquent et prennent des décisions ensemble dans un réseau [59].

Les modèles de contrôle IoV sont les règles de prise de décision et de coordination au sein du système. Les modèles de contrôle centralisés ont une autorité centrale qui prend des décisions, gère les données et émet des instructions. Les modèles de contrôle distribué permettent aux véhicules et à l'infrastructure de prendre ensemble des décisions locales à l'aide d'informations partagées. Les modèles de contrôle façonnent le fonctionnement de l'écosystème IoV et affectent la gestion du trafic, l'évitement des collisions et l'efficacité du système.

4.1 Modèles centralisés

Dans les modèles de communication IoV centralisés, un serveur central contrôle la communication entre les véhicules, l'infrastructure et le Cloud. Les voitures envoient des données à un serveur. Ensuite, le serveur partage les données avec d'autres voitures ou infrastructures. L'autorité décide sur la base des données [57].

4.2 Modèles distribués

Les modèles de communication IoV se concentrent sur la communication directe entre les véhicules et les infrastructures à proximité, sans autorité centrale. Les véhicules communiquent et prennent des décisions ensemble dans un réseau. Il permet aux usagers de la route de prendre des décisions ensemble rapidement, comme changer de vitesse ou d'itinéraire, sans qu'une seule personne soit responsable.

Les modèles centralisés ont une autorité centrale qui gère la communication, tandis que les modèles distribués ont une communication Peer-to-Peer et décentralisée.

4.2.1 Architectures Cloud IoV

Une architecture Cloud distribuée proposée dans [58] fournit un ensemble d'outils sur de nombreux centres de données ou "nœuds périphériques". Le traitement des données plus près de leur source réduit la latence. Les conceptions de cloud distribué peuvent être particulièrement utiles pour les applications en temps réel dans l'Internet des voitures (IoV) car elles rapprochent le traitement des voitures ou des éléments d'infrastructure, ce qui entraîne des temps de réaction plus rapides [58].

4.2.2 Architectures IoV basé sur Fog Computing

Le paradigme Fog computing [59] utilise une architecture informatique de pointe pour traiter les données rapidement et prendre des décisions plus rapidement. Le Fog Computing dans IoV rapproche l'ordinateur des véhicules de la périphérie du réseau, comme dans les véhicules, les serveurs de périphérie ou les infrastructures en bordure de route. La proximité réduit les délais, accélère les choses et réduit la quantité de données envoyées à des serveurs éloignés [59].

4.2.3 Architectures IoV Base sur Edge Computing

L'Edge computing place les ressources et les services informatiques à la périphérie du réseau, comme dans les véhicules, les serveurs de périphérie ou les infrastructures routières. L'IoV utilise l'informatique de pointe pour résoudre les problèmes liés aux temps de réponse lents, à la capacité de transfert de données limitée et à la nécessité d'un traitement immédiat des données [59].

4.3 Modèle de controle

Dans l'Internet des véhicules (IoV), les modèles de contrôle sont chargés de prendre des décisions, de coordonner les activités, de gérer l'environnement IoV. Voici quelques méthodes de contrôle IoV souvent utilisées :

4.3.1 Architectures Base - SDN

Le SDN (*Software Defined Networking*) comme nouvelle façon de mettre en place un réseau où les plans de contrôle et de données sont séparés (comme illustré dans la figure suivante).

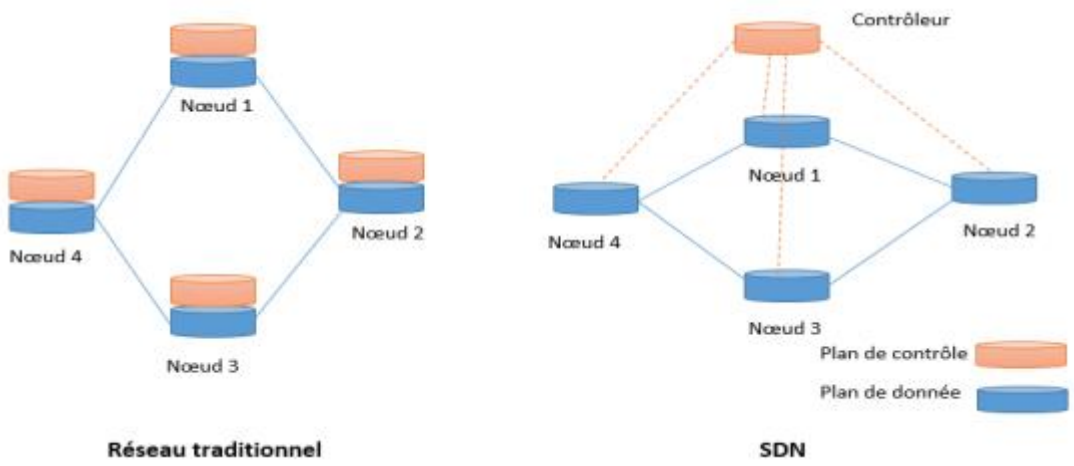

Figure 5 Réseau traditionnel et SDN [60]

L'architecture SDN sépare le contrôle et les données et utilise un seul contrôleur logiciel pour gérer plusieurs appareils via des API. Ce contrôleur aide les applications à communiquer avec le réseau en faisant abstraction de la couche physique et en permettant la programmation. Un réseau suit une architecture SDN s'il répond à ces critères :

- Séparez les plans de données et de contrôle.
- Périphériques simplifiés.
- Le contrôle est centralisé.
- Automatisation et virtualisation du réseau.
- Open source.

L'architecture SDN permet de découpler complètement le plan de contrôle des données comme le montre la figure suivante :

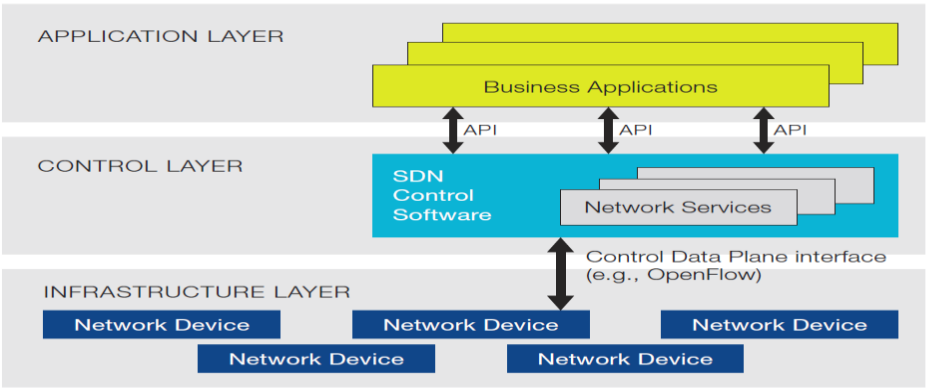

Figure 6 L'architecture SDN [61]

La couche infrastructure, la couche contrôle et la couche application constituent les trois niveaux de l'architecture SDN [62] :

- La couche d'infrastructure : cette couche est composée de dispositifs réseau réels tels que des commutateurs, des routeurs et d'autres parties du réseau qui déplacent les paquets en fonction des ordres du gestionnaire.
- La couche de contrôle : le gestionnaire principal qui gère le réseau se trouve dans cette couche. Le gestionnaire interagit avec la couche d'infrastructure pour comprendre comment les bits de données seront envoyés et traités.
- La Couche Application : les applications pouvant interagir avec le gestionnaire avec des API (*Application Programming Interfaces*) se trouvent dans cette couche. La conception SDN permet aux applications de gérer des tâches réseau telles que la gestion des données, la sécurisation du réseau et la bonne qualité de service.

4.3.2 Le protocole Openflow

L'OpenFlow [63] est important pour le SDN car il permet au contrôleur de communiquer avec les périphériques réseau. Il aide à programmer les commutateurs et les routeurs du réseau pour contrôler les flux de trafic de manière dynamique.

Le protocole sépare les plans de contrôle et de données des périphériques réseau, où les périphériques réseau ont une logique de contrôle qui décide de la manière dont les paquets de données sont envoyés. Le réseau OpenFlow dispose d'un contrôleur séparé pour le plan de contrôle et les périphériques réseau fonctionnent dans le plan de données. Le contrôleur donne des instructions pour transférer les paquets.

Le protocole OpenFlow fournit au contrôleur un ensemble de règles permettant aux périphériques de gérer les paquets entrants. Les règles déterminent ce qu'il faut faire des paquets en fonction de facteurs tels que leur provenance, leur destination, leur type et leur importance. Le contrôleur peut modifier les règles en temps réel pour des configurations de réseau flexibles et une gestion du trafic.

Les messages entre le gestionnaire et les périphériques réseau sont envoyés via un chemin sécurisé dans le protocole the OpenFlow. Le contrôleur envoie des instructions aux appareils et reçoit des notifications de leur part. Les instructions peuvent inclure des actions de transfert, des modifications de paquets ou des décisions de routage. Les notifications peuvent inclure des statistiques de trafic ou des déclencheurs d'événements.

4.3.3 Contrôleurs

Le contrôleur SDN modifie le réseau en traduisant une requête en opérations sur les équipements. De plus, le contrôleur vérifie l'état du protocole Openflow et le configure à l'aide de la CLI. L'application utilise une API appelée "*Northbound*" pour donner des ordres au contrôleur. Le contrôleur utilise des API appelées "*Southbound*" pour communiquer avec l'équipement. L'Openflow est une API sud qui fonctionne sur le plan de données [30]. Il existe de nombreux contrôleurs SDN disponibles, on peut citer

- **NOX** [64] NOX est le premier contrôleur OpenFlow développé à Nicira. Il est écrit en C++ et open-source. Il diminue et n'a pas beaucoup changé depuis la mi-2012.
- **POX** [64] est comme le petit frère de NOX. POX est un contrôleur open source basé sur Python pour OpenFlow. Il est similaire à NOX et peut être utilisé pour développer et tester des contrôleurs. Cependant, ses performances sont inférieures à celles des autres contrôleurs, il n'est donc pas recommandé pour une utilisation en entreprise.
- **Beacons** [64] est un contrôleur Java stable. Créé en 2010, toujours utilisé pour la recherche. Il fonctionne bien dans des conditions difficiles réel. Ce contrôleur a été utilisé dans d'autres projets comme Floodlight ou OpenDaylight.
- **Floodlight** [64] est un contrôleur OpenFlow gratuit qui utilise Java et est soutenu par les réseaux BigSwitch. C'est sous licence Apache. Facile à installer

et fonctionne bien. Floodlight est une solution complète avec de nombreuses fonctionnalités.

- **Open Daylight** est un projet de la Fondation Linux soutenu par l'industrie. Il s'agit d'un cadre permettant d'accéder à un logiciel SDN open source. C'est comme Floodlight et peut être une solution complète [64].

4.4 Communications de Machine-to-Machine

L'IOV a besoin d'une communication M2M pour connecter les véhicules, les infrastructures et les gadgets pour la mobilité intelligente, les capteurs, les systèmes de trafic et les nuages échangent des données par connectivité M2M. Les communications M2M améliorent l'IOV comme suit :

- Le M2M permet aux automobiles de communiquer sur la route. Le V2V permet aux automobiles de transmettre la position, la vitesse, la direction et les conditions routières. Ces données augmentent la sécurité routière, la fluidité du trafic et la formation de pelotons, ce qui permet d'économiser du carburant.
- Le M2M connecte les automobiles aux feux de circulation, aux panneaux, aux postes de péage et aux systèmes de stationnement. Le V2I informe les automobiles de la circulation, des feux verts et du stationnement. La réduction du trafic et des flux améliore les transports [65].
- Le M2M avec connectivité V2C permet aux véhicules d'interagir avec les systèmes Cloud. La connexion V2C permet aux voitures de stocker et d'analyser les données des capteurs dans le Cloud. L'environnement, les diagnostics de voiture et les habitudes de conduite sont inclus, la maintenance prédictive, la personnalisation et les informations basées sur l'analyse augmentent les performances du véhicule et l'expérience utilisateur sur les systèmes Cloud [65].
- La communication V2D permet aux voitures de communiquer avec les téléphones, les appareils portables et les maisons intelligentes. Le V2D permet le contrôle à distance du véhicule. Verrouillez/déverrouillez les portes, démarrez le moteur et modifiez les réglages de température. Il relie la maison intelligente et les assistants numériques [65].

4.5 Applications IoV SDN

Le SDN et l'IoV peuvent améliorer les systèmes de transport ; les applications IoV SDN incluent [66] :

- **La gestion et l'optimisation du trafic :** le SDN peut aider à gérer et à améliorer le trafic [66] dans IoV. Le SDN contrôle les ressources du réseau pour acheminer le trafic, détecter la congestion et équilibrer les charges. Il aide les gestionnaires de trafic à prendre des décisions rapides en fonction des conditions de circulation pour réduire les embouteillages, améliorer l'efficacité des routes et raccourcir les temps de trajet.
- **Routage et navigation intelligents :** le SDN permet un routage et une navigation intelligents dans IoV. Les contrôleurs SDN utilisent les données de trafic pour guider les véhicules sur les meilleurs itinéraires, en tenant compte du trafic, des conditions routières et des préférences des utilisateurs. Cela permet d'économiser du temps, du carburant et de réduire les émissions, ce qui améliore la conduite [66].
- **Communication (V2V) (V2I) :** le SDN peut améliorer la communication en IoV via V2V et V2I [66]. Le SDN aide les véhicules et l'infrastructure à mieux communiquer en contrôlant tout depuis un seul endroit. Il permet de partager des informations routières telles que des alertes de trafic et de sécurité pour une conduite plus sûre.
- **Sécurité et confidentialité du réseau :** le SDN peut aider à sécuriser et à protéger les réseaux IoV. Le SDN permet des mesures de sécurité solides pour protéger la communication véhicule-réseau, telles que la détection d'intrusion et le cryptage, grâce à un contrôle centralisé. Il protège la communication IoV contre les accès non autorisés, les attaques et protège les données sensibles [67].
- **Gestion de flotte et surveillance des performances des véhicules :** le SDN peut aider à gérer les flottes et à surveiller les performances des véhicules. Les contrôleurs SDN collectent des données sur les performances du véhicule, la consommation de carburant, les besoins de maintenance et le comportement du conducteur en se connectant aux capteurs du véhicule et aux systèmes embarqués. Il utilise ces données pour améliorer l'efficacité de la flotte et planifier les tâches de maintenance [67].

- **Contrôle et gestion autonomes des véhicules :** SDN peut contrôler les voitures autonomes dans IoV. Les contrôleurs SDN peuvent aider les véhicules autonomes à se comporter de manière optimale, à respecter les règles de circulation et à interagir en toute sécurité avec d'autres véhicules et infrastructures en centralisant la prise de décision et la coordination [67].

5. IoV Challenges

La mise en œuvre des systèmes IoV est confrontée à plusieurs défis qui doivent être relevés afin d'assurer leur adoption et leur fonctionnement réussis. Voici quelques-uns des principaux défis associés à l'IoV :

1) Sécurité : avec l'augmentation de la connectivité et de l'échange de données dans IoV, la sécurité devient une préoccupation essentielle. La sécurisation des canaux de communication, la protection de la confidentialité des données, la prévention des cyberattaques et la garantie de l'intégrité du système sont des enjeux majeurs. Des protocoles de sécurité, des méthodes de cryptage et des mécanismes d'authentification robustes doivent être en place pour atténuer ces risques [68].
2) Normalisation : l'IoV implique de multiples parties prenantes, notamment des constructeurs de véhicules, des fournisseurs d'infrastructures et des fournisseurs de services. Le manque de protocoles et d'interfaces standardisés peut entraver l'interopérabilité et la communication transparente entre les différents composants IoV. L'établissement de normes et de protocoles à l'échelle de l'industrie est essentiel pour permettre une collaboration et une intégration efficaces entre les différents systèmes [68].
3) Coût : la mise en œuvre de systèmes IoV peut impliquer des coûts importants, notamment l'installation d'une infrastructure de communication, la modernisation des véhicules avec des fonctionnalités de connectivité et la garantie de la compatibilité avec les technologies existantes. Ces dépenses peuvent limiter l'adoption généralisée de l'IoV, en particulier dans les régions aux ressources limitées ou aux infrastructures obsolètes. Il est important de trouver des solutions rentables et d'encourager les investissements pour surmonter ce défi [68].
4) Adoption : Encourager les individus et les organisations à adopter les technologies IoV peut être difficile. Des facteurs tels que le manque de sensibilisation, la résistance au changement et les préoccupations concernant la confidentialité et la

sécurité des données peuvent ralentir le processus d'adoption. Sensibiliser le public, fournir une éducation sur les avantages de l'IoV et répondre aux préoccupations par le biais de politiques et de réglementations transparentes sont essentiels pour favoriser une plus grande acceptation et adoption [69].

5) Évolutivité : à mesure que le nombre de véhicules et d'appareils connectés augmente, l'évolutivité devient un défi important. Les systèmes IoV doivent être capables de gérer le grand volume de données générées par les véhicules, de les traiter et de les analyser en temps réel et de fournir des réponses en temps opportun. Le développement d'architectures évolutives et l'utilisation de techniques avancées de traitement des données, telles que l'informatique de pointe, peuvent aider à relever ce défi [69].

Relever ces défis nécessite des efforts de collaboration de la part de diverses parties prenantes, notamment des acteurs de l'industrie, des décideurs et des chercheurs. Investir dans la recherche et le développement, promouvoir le partage d'informations et favoriser les partenariats sont essentiels pour surmonter les obstacles et libérer tout le potentiel des systèmes IoV.

6. Conclusion

L'intégration des véhicules dans l'Internet des véhicules (IoV) a le potentiel d'améliorer la sécurité, l'efficacité et la durabilité des transports. En connectant les véhicules, les infrastructures et les appareils, les systèmes IoV permettent l'échange de données en temps réel sur les conditions de circulation, les mises à jour météorologiques et les informations routières. Cette richesse d'informations permet aux conducteurs de prendre des décisions éclairées, contribuant ainsi à améliorer la sécurité et l'efficacité routières globales.

Les architectures IoV se composent généralement de trois composants clés : la communication de véhicule à véhicule, la communication de véhicule à infrastructure et la communication de véhicule à tout. Chaque composant joue un rôle essentiel pour assurer le bon fonctionnement des systèmes IoV et la fourniture de données qui améliorent et sécurisent les conditions de trafic.

Cependant, les implémentations IoV sont également confrontées à certains défis qui doivent être résolus. Ces défis incluent les problèmes de sécurité, le besoin de normalisation, les considérations de coût et l'adoption généralisée. Pour surmonter ces défis, il est crucial

d'investir dans des efforts de recherche et développement axés sur l'amélioration des protocoles de sécurité, l'établissement de normes à l'échelle de l'industrie et la mise en œuvre de méthodes de cryptage de données robustes. La collaboration et l'accord entre les différents systèmes IoV sont essentiels pour assurer l'interopérabilité et encourager une plus grande utilisation parmi le public.

En tirant parti des avantages de l'IoV, les systèmes de transport peuvent connaître des améliorations significatives. Investir dans les systèmes IoV permet des options de transport plus durables, efficaces et plus sûres, ce qui a finalement un impact positif sur l'ensemble des réseaux de transport et l'état des routes.

CHAPTER 3: Proposition d'une architecture IoV basé SDN et stratégies de routage dynamique

1. Introduction

Dans le chapitre précédent, nous avons souligné l'importance des architectures dans le contexte de l'Internet des véhicules (IoV) pour faciliter l'échange de données efficace. Nous avons exploré les différentes techniques et stratégies utilisées dans l'IoV, notamment les modèles centralisés, distribués et de contrôle, ainsi que les diverses approches de communication spécifiquement conçues pour l'IoV. Nous avons également examiné les conceptions basées sur le Software-Defined Networking (*SDN*) et le protocole OpenFlow, en mettant en évidence les contrôleurs associés à ces approches.

Dans ce chapitre, notre objectif est de présenter une stratégie de routage IoV dynamique avancée, adoptée dans un environnement SDN. Cette solution est spécifiquement conçue pour gérer les embouteillages du réseau dans un système IoV. En mettant l'accent sur la conception de cette stratégie, notre objectif est d'améliorer le flux du trafic réseau en déplaçant les calculs et le traitement des données vers la périphérie du réseau. En utilisant des capacités de calcul avancées, notre proposition vise à réduire considérablement la quantité de données qui doivent transiter par le réseau, ce qui se traduit par des délais réduits et des prises de décision en temps réel plus fluides. En conséquence, notre conception permet d'optimiser le transfert de données, améliorant ainsi la vitesse et la stabilité globales des systèmes IoV.

2. Architecture de périphérie pour IoV

Comme nous avons vus dans les chapitres précédents, l'internet des objets véhiculaires (IoV) émerge comme une technologie révolutionnaire qui permet la connectivité entre les véhicules, les infrastructures routières et d'autres entités infrastructures distantes via des réseaux cellulaires. Cependant, l'IoV présente des défis uniques en termes de gestion du trafic réseau, surtout dans les heures de pointes ou le trafic véhiculaire est dense.

Pour relever ces défis, nous proposons une architecture EC basé SDN de gestion du trafic réseau (*SDIoV*), pour surmonter les problèmes de la surcharge réseau confronté par les protocoles de routage dynamique comme AODV. Cette architecture fournie une approche novatrice et un routage adaptative dans les pires conditions du trafic. Le contrôleur permet de séparer le plan de contrôle du plan de données, ce qui permet une gestion centralisée et dynamique du réseau. Cela offre une flexibilité sans précédent pour gérer et contrôler les communications dans l'IoV.

La figure 7 montre l'architecture SDN adaptée à l'IoV que nous proposons, les véhicules sont équipés de commutateurs SDN qui agissent comme des points de contrôle intelligents. Ces commutateurs SDN sont interconnectés avec des contrôleurs SDN centralisés qui prennent des décisions de routage, de gestion de la mobilité des véhicules et de la sécurité du réseau. Grâce à cette architecture, les opérateurs de réseau peuvent configurer, contrôler et optimiser les flux de données en fonction des exigences spécifiques de l'IoV.

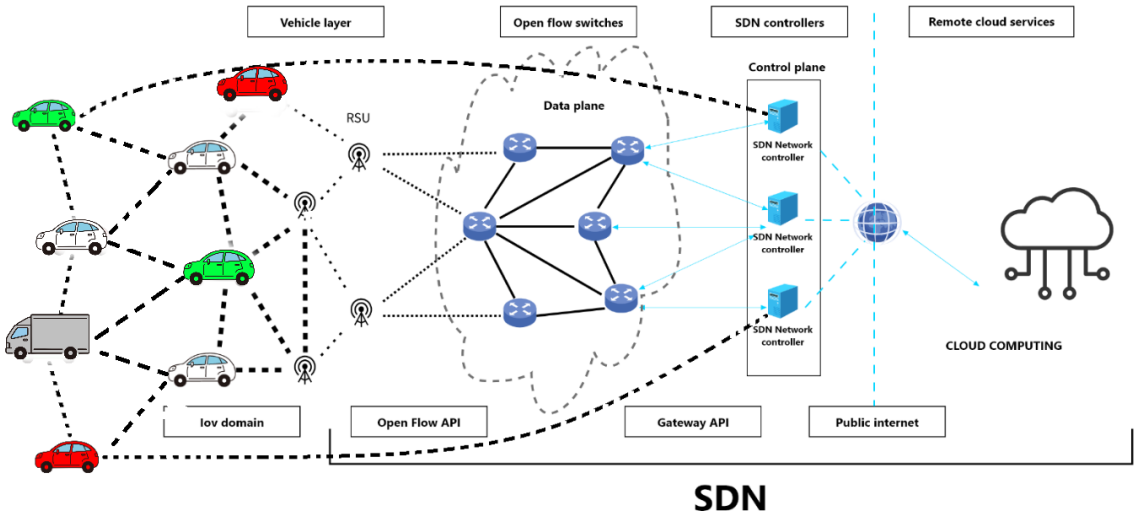

Figure 7 Architecture routage IoV dynamique dans un environnement Edge Computing

En effet, l'architecture de périphérie de l'Internet des véhicules (*IoV*) comprend généralement trois couches principales : la couche de domaine IoV, la couche de réseau défini par logiciel (*SDN*) et la couche Cloud. Chacune de ces couches joue un rôle spécifique dans la connectivité et le fonctionnement des véhicules connectés. Regardons de plus près chaque couche :

1. **La couche de domaine IoV**

La couche de domaine IoV constitue l'interface la plus proche des véhicules dans IoV, englobe également les éléments physiques et les entités essentielles à son fonctionnement. Cette couche comprend des véhicules, des infrastructures, des capteurs, des actionneurs et des appareils. Son rôle principal est de collecter des données sur la dynamique du véhicule, l'environnement, le trafic et d'autres paramètres pertinents. Les données sont recueillies par le biais de capteurs présents à la fois dans les véhicules et dans l'infrastructure de la couche de domaine IoV. Une fois collectées, ces données sont transmises à la couche SDN afin d'être analysées et traités.

2. Couche Cloud

L'objectif de l'infrastructure Cloud dans une architecture IoV contrôlée par SDN est de fournir une infrastructure distante pour le stockage et le traitement des données. Dans cette architecture, le contrôleur prend des décisions de traitement en fonction de la sensibilité de la situation. Si les données nécessitent un traitement urgent, le contrôleur effectue un traitement à court terme en traitant les données localement. Sinon, les données sont traitées à long terme par le Cloud. Ce mécanisme présente l'avantage de réduire les calculs complexes qui exigent une grande quantité de ressources. La couche Cloud est généralement située dans des centres de données distants et peut être accessible via le réseau. À long terme, le Cloud récupère les données de la couche SDN et effectue des analyses complexes ainsi que des traitements des données en utilisant des techniques avancées d'IA. Cela vise à améliorer les performances des systèmes IoV existants.

3. La couche SDN

La couche SDN joue un rôle crucial en connectant la couche de domaine IoV et la couche Cloud au sein de l'architecture IoV. Elle utilise un réseau de contrôle pour gérer le flux de données au sein d'un réseau IoV. La couche SDN est composée de contrôleurs, de commutateurs et d'une infrastructure réseau SDN. Les contrôleurs SDN sont responsables de la gestion et de la configuration des périphériques réseau. Ils collectent les données provenant du domaine IoV et utilisent des politiques ou des algorithmes préalablement définis pour prendre des décisions intelligentes. Ces décisions englobent des tâches telles que la gestion du trafic, l'optimisation des réseaux, la mise en œuvre de mesures de sécurité et la gestion de la qualité de service. Grâce à la flexibilité offerte par le SDN, les réseaux peuvent s'adapter en fonction des besoins spécifiques d'un réseau IoV. Le SDN facilite le routage des données, réduisant ainsi les problèmes de congestion et permettant une prise de décision rapide à la périphérie du réseau.

Dans ce travail, nous nous intéressons par le rôle crucial du contrôleur dans la gestion du trafic de données dans les environnements IoV. Contrairement au routage traditionnel, l'approche d'adaptation de routage dans l'IoV aide à prendre des décisions de routage optimales en fonction des conditions du réseau et des métriques de routage telles que la disponibilité de la bande passante et la latence. Cela permet d'optimiser la qualité de service (*QoS*) en choisissant les meilleures routes en termes de performances. Ainsi, la couche SDN

permet de gérer de manière plus efficace le trafic de données dans les environnements IoV, en optimisant les décisions de routage en fonction des conditions du réseau et des exigences de qualité de service.

3. Les Applications SDIoV

3.1 La gestion du trafic véhiculaire

Les systèmes de communication dans l'environnement IoV nécessitent des améliorations pour soutenir les applications et les systèmes de transport avancés. Les protocoles de routage actuels sont rigides et ont des limitations en termes d'évolutivité. Cependant, l'introduction de l'architecture SDN peut contribuer à améliorer l'infrastructure et le routage dans IoV [70]. Avec une augmentation des tâches de communication IoV, il y a également une augmentation du trafic dans les grandes villes, ce qui devient difficile à gérer avec une approche distribuée. Le SDN permet une gestion centralisée de l'IoV en utilisant divers réseaux, tels que les réseaux cellulaires.

Le contrôle est initialement utilisé pour la gestion des réseaux fixes tels que les réseaux d'accès et les centres de données, offre des opportunités d'amélioration de la communication dans les villes intelligentes pour la gestion du trafic en IoV. En appliquant les principes du SDN, il est possible d'améliorer la communication au sein des réseaux de véhicules. Cette approche novatrice présente un potentiel considérable pour améliorer l'efficacité et les performances des systèmes de communication dans l'IoV.

Un exemple concret d'application des contrôleurs SDN pour améliorer la communication dans l'IoV serait la gestion du trafic dans une grande ville (voir la figure 8). Soit une situation où plusieurs véhicules connectés circulent dans une ville densément peuplée, créant ainsi un trafic intense. Les contrôleurs SDN peuvent jouer un rôle clé dans l'amélioration de cette situation. Tout d'abord, les contrôleurs SDN collectent en temps réel des données sur les conditions de circulation, la densité du trafic et d'autres paramètres pertinents à partir des véhicules connectés et des infrastructures de la ville. Ensuite, en utilisant ces informations, les contrôleurs SDN analysent les données pour prendre des décisions intelligentes concernant la gestion du trafic. Ils peuvent identifier les zones de congestion, les itinéraires alternatifs possibles, et même ajuster les feux de signalisation pour optimiser le flux de circulation.

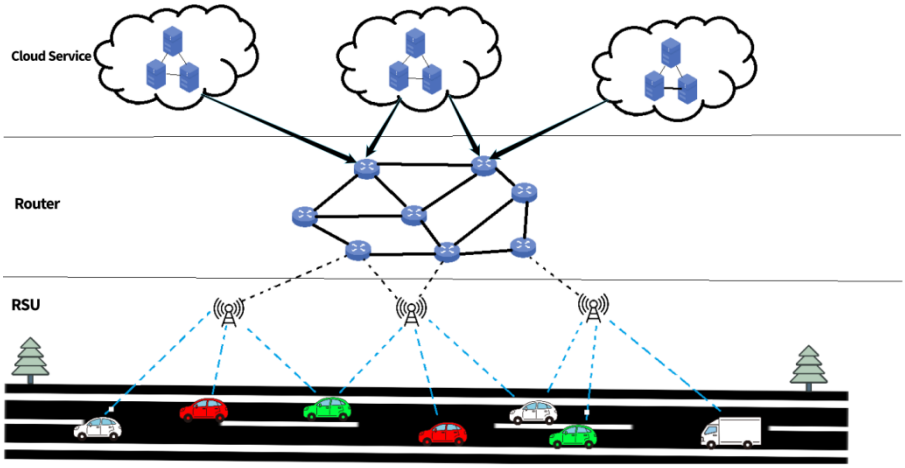

Figure 8 Architecture SDN pour la gestion du trafic.

Grâce à la gestion centralisée des contrôleurs SDN, les décisions de routage et de gestion du trafic peuvent être prises de manière rapide et efficace. De plus, les contrôleurs SDN peuvent également gérer les priorités de circulation en fonction des besoins spécifiques, tels que les véhicules d'urgence, les transports en commun ou les véhicules électriques nécessitant une recharge. L'application des contrôleurs SDN dans l'IoV permet une gestion intelligente et centralisée du trafic, en utilisant les données en temps réel pour prendre des décisions de routage optimales, réduire les embouteillages et améliorer l'efficacité de la circulation dans une ville.

3.2 La stockage des données IoV

Le contrôle SDN peuvent jouer un rôle important dans l'optimisation du stockage et de la gestion des données dans l'IoV. En centralisant le stockage des données dans le Cloud ou les centres de données, le SDN facilite l'organisation, la mise à l'échelle et l'accès aux données dans le système IoV. En outre, le SDN facilite la localisation rapide et efficace des données en utilisant des méthodes intelligentes d'accès aux données stockées. Les contrôleurs SDN peuvent gérer efficacement les demandes de données en adoptant une approche centralisée, ce qui permet de fournir rapidement les données pertinentes aux véhicules ou aux applications IoV. Cela se traduit par une récupération de données plus rapide et plus réactive dans l'IoV.

La figure 9 ci-dessous présente un exemple concrète de configuration d'un cluster de serveurs pour le stockage de différents types de données véhiculaire. Dans cet exemple, le contrôleur peut configurer un cluster de serveurs dédié au stockage des annuaires pour résoudre le problème de routage, tandis qu'un autre cluster est configuré en mode bloc pour le

stockage des contenus multimédias. Cette approche permet d'optimiser le stockage en fonction des types de données circulé dans le réseau véhiculaire, en utilisant des clusters spécialisés pour différents besoins de stockage.

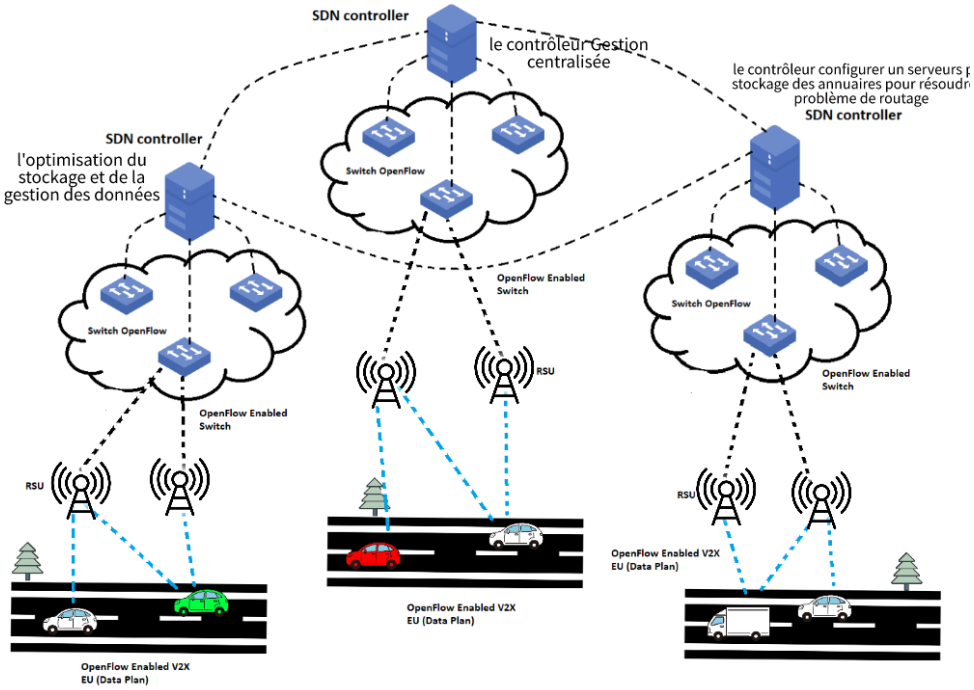

Figure 9 Architecture SDVN de gestion stockage.

Néanmoins, il convient de noter que l'application spécifique du stockage dans un réseau véhiculaire dépendra des besoins et des caractéristiques propres à l'environnement et aux cas d'utilisation envisagés.

4. Processus de routage véhiculaire avec SDN

Dans cette section, nous présenterons brièvement le processus de contrôle SDN appliquée au routage dans réseaux de véhicules. Nous expliquerons le rôle central du contrôleur SDN, qui agit en tant qu'entité de contrôle intelligente pour la gestion du réseau.

4.1 Collecte des informations des véhicules

Le processus de routage véhiculaire avec SDN repose sur la collecte d'informations en temps réel à partir des véhicules eux-mêmes. Nous décrirons les différents types de données qui peuvent être collectées, tels que la localisation, la vitesse, la direction et les conditions environnementales. Nous expliquerons les moyens de collecte de ces informations,

notamment les capteurs embarqués dans les véhicules et les dispositifs de communication utilisés pour les transmettre au contrôleur SDN.

4.2 Prise de décision du routage

Une fois les informations des véhicules collectées, le contrôleur SDN est en mesure de prendre des décisions de routage éclairées. Nous présenterons les principaux critères pris en compte dans le processus de prise de décision, tels que l'optimisation de la durée du trajet, la minimisation de la congestion, la priorisation des véhicules d'urgence, etc. Nous pouvons également utiliser les algorithmes de routage couramment utilisés dans le contexte du routage véhiculaire, en mettant l'accent sur leur adaptabilité aux changements dynamiques du réseau.

4.3 Diffusion des décisions de routage via le protocole OpenFlow

Une fois que le contrôleur SDN a pris des décisions de routage, il est essentiel d'adapter ces décisions avec le réseau IoV concerné. Nous discuterons dans ce qui suit les différentes stratégies de diffusion de ces décisions. Une telle décision de routage sont est liée à l'ensemble des canaux de communication dédiés, tels que les connexions cellulaires, les modes de communications véhiculaire (V2V ou V2I) et la portée de couverture du RSU. Nous soulignerons l'importance de la réactivité du protocole OpenFlow pour garantir la fiabilité de la communication et de la dissémination des sans faille entre le contrôleur SDN et les véhicules. Pour cela, nous proposons une adaptation de routage via protocole OpenFlow en deux stratégies principales: une stratégie de contrôle et une stratégie de transfert de données IoV.

La stratégie de contrôle OpenFlow

La stratégie de contrôle SDN via le protocole OpenFlow utilise l'en-tête OpenFlow pour structurer les messages échangés entre un réseau IoV et le contrôleur. Une technique de virtualisation est adoptée dans ce contexte pour gérer logiquement les différents types de services (voir la figure 10 ci-dessous). Par défaut, une connexion sécurisée basée sur TLS sur TCP est établie pour protéger les échanges de données, comme montre dans la stratégie proposée dans [71].

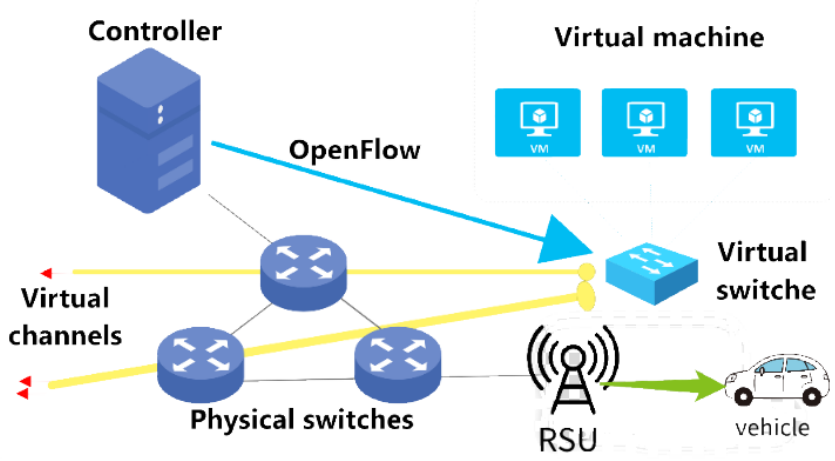

Figure 10 Couche de contrôle virtuel via le protocole OpenFlow.

La stratégie de contrôle utilise trois types de messages: les requêtes, les réponses et les événements, dont la classification des messages est illustrée dans la figure 11 ci-dessous. Ces messages permettant au Switch OpenFlow et au contrôleur de communiquer efficacement et de prendre des décisions en fonction des besoins de l'IoV.

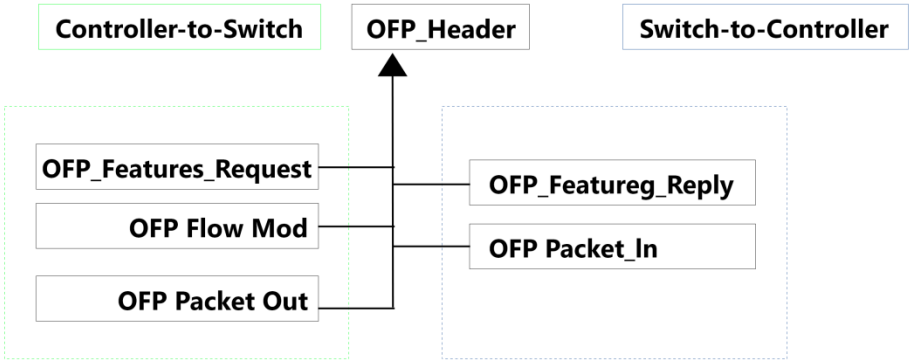

Figure 11 La classification des messages OpenFlow.

Chaque message commence par un en-tête OpenFlow qui contient des informations telles que la longueur du message, le numéro de transaction et le type de message. Cela permet d'identifier et de structurer les échanges entre le commutateur et le contrôleur. Le tableau 1 suivant illustre les instanciations des messages échangés :

Message	Définition OpenFlow	Description
Hello	OFPT_HELLO	C'est le premier mot que le contrôleur et le commutateur s'envoient lorsqu'ils se connectent. Il est utilisé pour communiquer la version de l'OpenFlow que les deux parties peuvent utiliser.
Service	OFPT_FEATURES_REQUEST	Le contrôleur envoie ce message pour demander les fonctionnalités appliqué du réseau IoV, tels que le nombre de ports connecté, les protocoles qu'il prend en charge et les versions de l'OpenFlow avec lesquelles il fonctionne
Réponse	OFPT_FEATURES_REPLY	le commutateur envoie ce message en réponse à une demande de fonctionnalités. Il indique les décisions de routage, le nombre de ports dont il dispose et d'autres détails sur le commutateur.
Paquet entrant	OFPT_PACKET_IN	Le commutateur envoie un message au contrôleur lorsqu'il reçoit un paquet véhiculaire sans entrée de flux correspondante. Il contient des détails sur les paquets tels que l'en-tête et la charge utile. Cela aide le contrôleur à décider comment gérer le paquet
Flow Mod	OFPT_FLOW_MOD	le contrôleur utilise ce message pour ajouter, modifier ou supprimer des entrées de flux dans la table du commutateur. Il fixe les règles du flux.
Flux supprimé	OFPT_FLOW_REMOVED	Le commutateur envoie un message au contrôleur lorsqu'un flux est supprimé de sa table. Cela peut arriver parce qu'il a expiré ou a été supprimé.
État du port	OFPT_PORT_STATUS	Le commutateur informe le contrôleur des changements d'état du port à l'aide de ce message. Il peut concerner l'ajout, la modification ou la suppression de ports
Erreur	OFPT_ERROR	Est un message d'erreur pour signaler les problèmes rencontrés par le commutateur ou le contrôleur. Il a des codes d'erreur et spécifiques erreur détails.

Tableau 1 Les descriptions des messages échangés.

La stratégie de transfert OpenFlow

Cette stratégie permet aux switchers OpenFlow d'assurer la gestion efficace du trafic et des données circulant entre les véhicules et les RSUs. Les règles de correspondance dans les

tables de flux peuvent être configurées pour prendre en compte des critères spécifiques, tels que les informations de localisation du véhicule, le type de service demandé ou les politiques de priorité (voir la figure 12) .Grâce à cette approche, les switchers OpenFlow facilitent la prise de décisions intelligentes et dynamiques pour le transfert des paquets de données dans le réseau IoV. Ils contribuent ainsi à optimiser les performances du réseau, à garantir une communication fiable et à offrir des services adaptés aux besoins des véhicules connectés, comme montre la figure suivante :

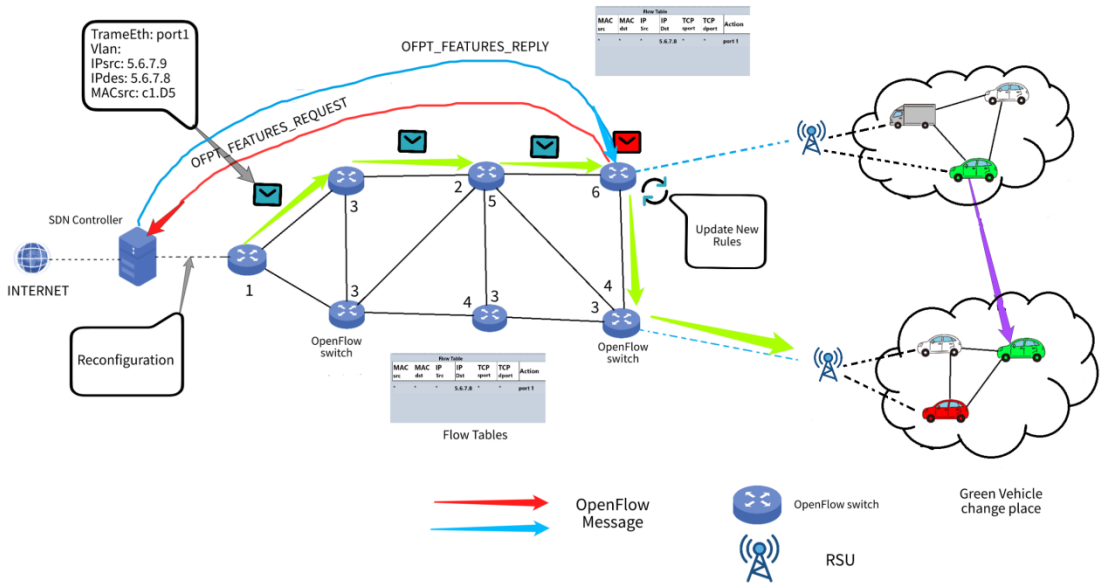

Figure 12 La stratégie de transfert de routage via le protocole OpenFlow.

5. Implémentation et Evaluation

5.1 Scenario d'étude

Pour évaluer notre proposition, nous mettrons en place un modèle de simulation sous Omnet++ d'un un cas d'étude spécifique (Voir figure 13 ci-dessous). Les résultats obtenus nous permettront de démontrer l'efficacité de notre approche et sa correspondance avec les objectifs de simulation. L'objective de notre scénario est de simulé une architecture Edge Computing mobile composé d'un contrôleur, un ensemble des switchers OpenFlowet un réseau véhiculaire. Le scénario proposé inclut les fonctionnalités suivantes :

- La couche de contrôleur qui gère les stratégies de communication dans le réseau véhiculaire en fonction des données collecté de l'IoV, les routeurs et les RSU. Ensuite, il peut prendre des décisions de redirection du trafic et de configurer réseau.

- La couche des switchers connecte un réseau IoV au contrôleur en appliquant les instructions du contrôle et aident les véhicules à communiquer entre eux et avec le réseau.
- L'ensemble des véhicules connectés, dont chaque véhicule est doter de capacités de communication rejoignent le système IOV. Les véhicules peuvent partager des informations importantes telles que leur position, leur vitesse, leur direction et les conditions routières avec les voitures à proximité en utilisant la communication V2V. La communication V2V améliore la sécurité routière, la fluidité du trafic et permet une conduite en peloton économe en carburant et une conduite collaborative.

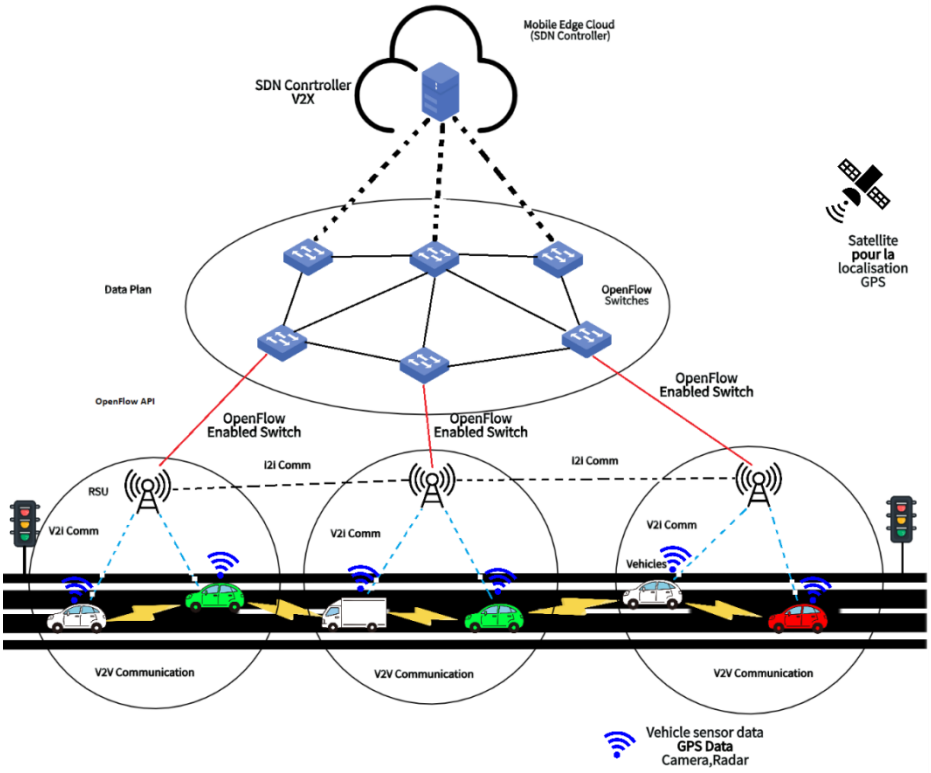

Figure 13 Scenario d'étude.

5.2 Outils de simulation

- **Ubuntu**

Un système d'exploitation Ubuntu open source populaire basé sur Linux (voir figure14). Il a une interface conviviale, est stable et sécurisé, et dispose de nombreux logiciels de support. Canonical Ltd. crée Ubuntu, un logiciel gratuit. Ubuntu convient à différents types d'ordinateurs, tels que les ordinateurs personnels, les serveurs et le Cloud. De nombreuses

applications sont déjà installées pour le travail, la navigation, les médias et le développement, afin que les utilisateurs puissent faire beaucoup de choses immédiatement.

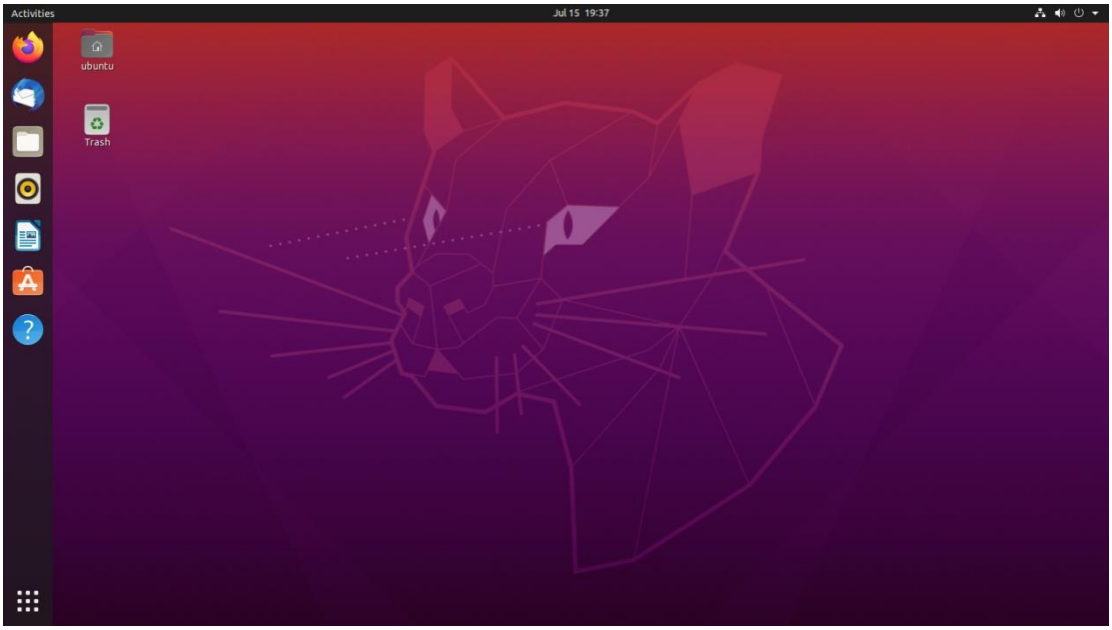

Figure 14 Ubuntu

- **OMNeT ++**

Objective Modular Network Test est un outil de simulation d'événements discrets largement utilisé pour décrire et tester différents types de réseaux (voir figure15), tels que les réseaux de données, les réseaux radio et les systèmes distribués. Il est conçu pour fournir un cadre flexible et extensible pour modéliser des situations de réseau complexes et tester les performances des protocoles, des algorithmes et des systèmes.

OMNeT ++ est écrit en C++ et a une conception basée sur les composants. Cela permet aux utilisateurs de décrire et de tester des modèles de réseau à l'aide de composants réutilisés. Il dispose d'une grande bibliothèque de modules et de modèles de réseau déjà créés, et vous pouvez également créer vos propres modules.

Le langage NED (*Network Description*) est utilisé pour créer les modèles de modélisation dans OMNeT ++. Ce langage permet aux utilisateurs de décrire la structure, le comportement et les relations des composants du réseau. OMNeT ++ fonctionne également avec différentes méthodes de simulation, comme la simulation d'événements discrets et la modélisation basée sur les événements, pour enregistrer le comportement des systèmes de réseau aussi précisément que possible.

OMNeT ++ a beaucoup d'options pour contrôler les simulations, analyser les résultats et montrer ce qu'ils signifient. Il dispose d'une interface utilisateur graphique (*IDE*) appelée OMNeT ++ Simulation IDE, qui dispose d'outils pour créer des structures de réseau, configurer des paramètres de simulation, exécuter des modèles et examiner les résultats de simulation.

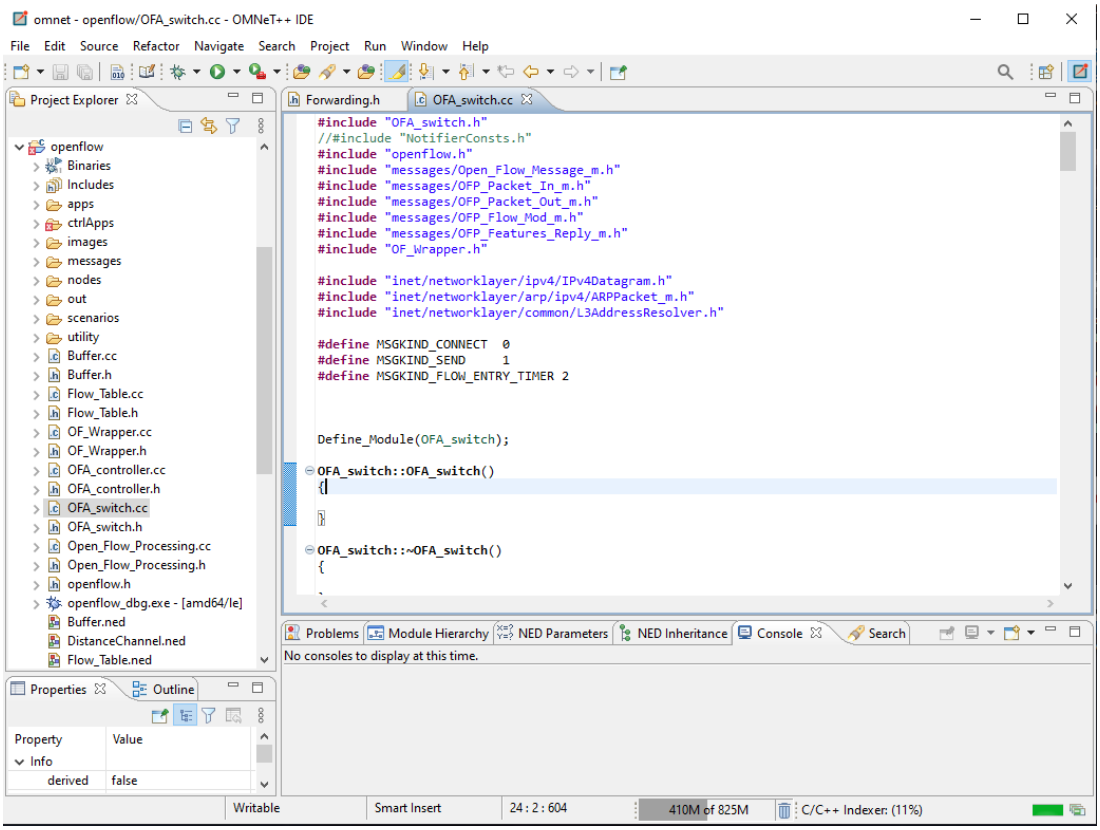

Figure 15 interface Omnet ++

- **INET**

INET est un système et un outil pour construire et créer des réseaux de communication. Il a été fait dans ce but. Il est construit sur le système de modélisation OMNeT ++ et comprend un ensemble de modèles de réseau, de protocoles et de composants qui peuvent être utilisés pour simuler différents événements de réseau.

INET signifie "Internet" et est utilisé pour modéliser et simuler les réseaux IP (*Internet Protocol*). Il couvre un large éventail de protocoles et de technologies réseau, tels que TCP, UDP, IP, Ethernet, WiFi , MPLS, etc. INET utilise des modules de réutilisation pour implémenter ces protocoles et technologies. Cela permet aux utilisateurs de créer facilement des modèles de réseau en assemblant et en configurant ces modules.

Le système INET dispose d'un grand nombre de fonctionnalités et d'outils pour simuler des réseaux (voir figure 16). Par exemple, il prend en charge la simulation au niveau des paquets, les modèles pilotés par les événements et la visualisation des résultats de simulation. Il propose une large gamme de conceptions et de paramètres de réseau, ce qui permet aux utilisateurs de créer des modèles qui ressemblent à de vrais environnements de réseau.

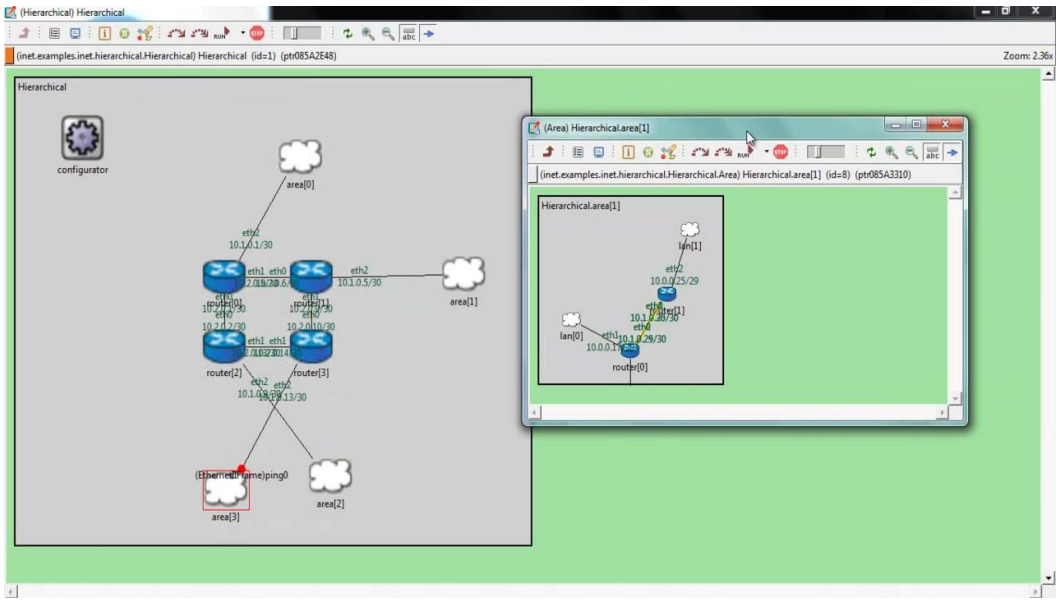

Figure 16 Cadre OMNeT ++ INET

- **Le projet OpenFlow**

Le projet OpenFlow est modèle de simulation sous Omnet++ Il a été utilisé pour simuler le comportement des commutateurs réseau dans OMNeT++. Le modèle de simulation des commutateurs permet de reproduire le comportement des commutateurs réels dans un réseau simulé (voir figure 17).

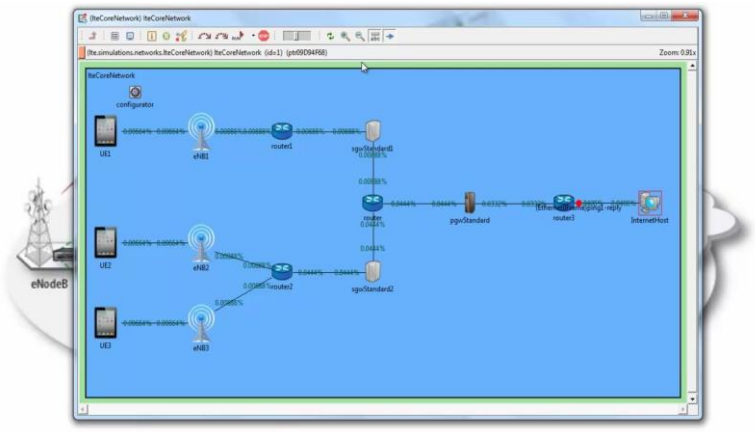

Figure 17 Flux ouvert

- **Le projet Veins**

Le projet *Veins* (voir figure 18) est un outil de simulation open-source de réseaux de communication de véhicules dans *OMNeT* ++. Il contient des modèles de simulation de la communication entre les véhicules et les RSU, il fournit également de modèles de protocoles et d'outils pour rendre la simulation plus précise.

Un projet *Veins* est lancer dans l'environnement OMNeT en fonction de la plateforme INET et SUMO. Il possède de nombreuses fonctionnalités telles que la modélisation de véhicules, la modélisation de canaux de communication, les protocoles sans fil (*comme IEEE 802.11p/WAVE*) et la modélisation de communication V2V et V2I. Simuler et à tester les réseaux de communication véhiculaire pour des éléments tels que la sécurité routière, la gestion, la conduite coopérative et le transport intelligent.

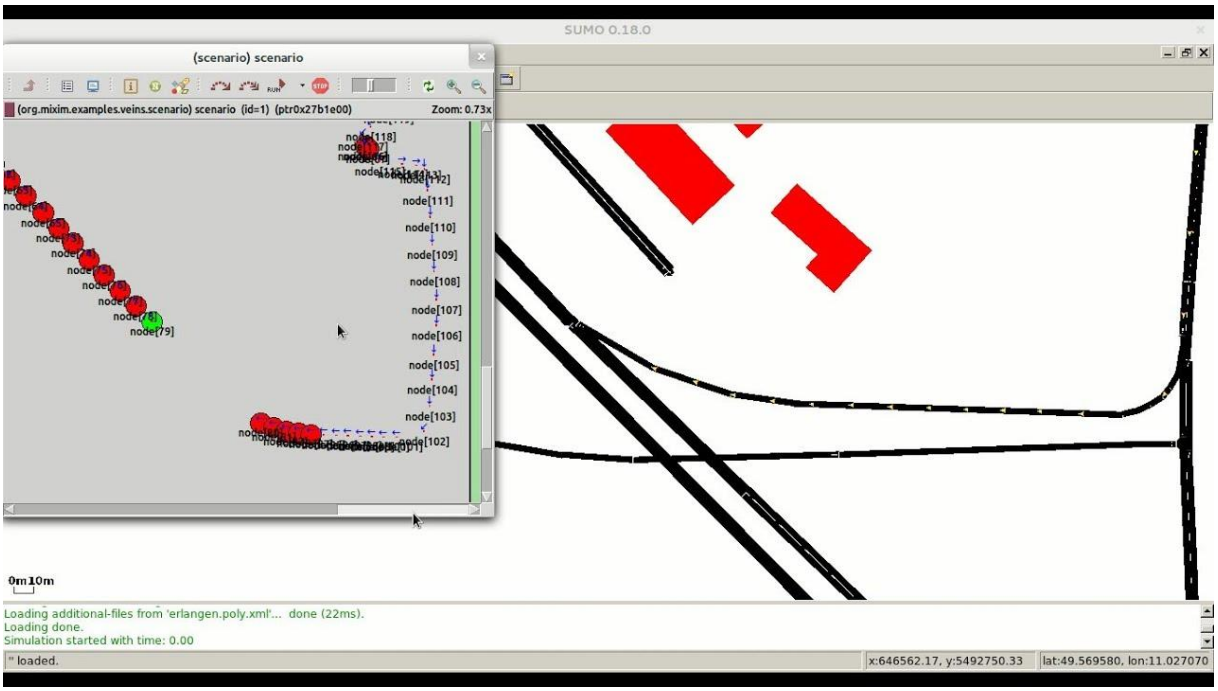

Figure 18 Interface veines

5.3 Le projet de simulation :

Sur la base des modèles de simulation précédemment mentionnés, nous proposons un projet de simulation pour développer des modèles de routage pour l'Internet des véhicules (IoV) basés SDN sous OMNeT++.Dans ce projet, nous utiliserons les interfaces utilisateur d'OMNeT++ pour faciliter l'exécution de la simulation, le débogage et la démonstration du routage IoV basé sur SDN. Les bibliothèques de simulation d'OMNeT++ seront utilisées pour

construire les programmes de simulation nécessaires. Le tableau suivant montre les paramètres de simulation du protocole proposé :

Modèle	Paramètre	Valeur
Contrôleur	App	*LLDPForwarding*
	Service Time	*5.556*10^{-6}*
	ControllerAdresse	*« sdn_IoV_ contoller »*
	Connexion Interval	*0s- 1s*
	promiscuous	*true*
	Buffer size	*3712Mb*
IoV	Configuration	*IPv4Config.xml*
	Zone	*600m*400m*
	Mobility	*« MassMobility»*
	Speed	*10mps*

Tableau 2 tableau de simulation

- **Le projet de simulation sous Omnet++ :**

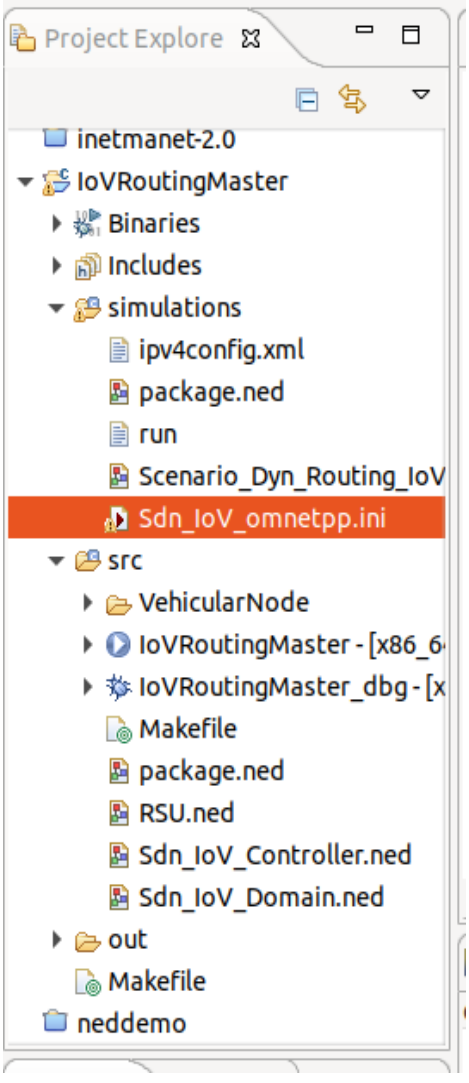

Figure 19 Le projet IoVRoutingMaster

- **Modèle du contrôle :**

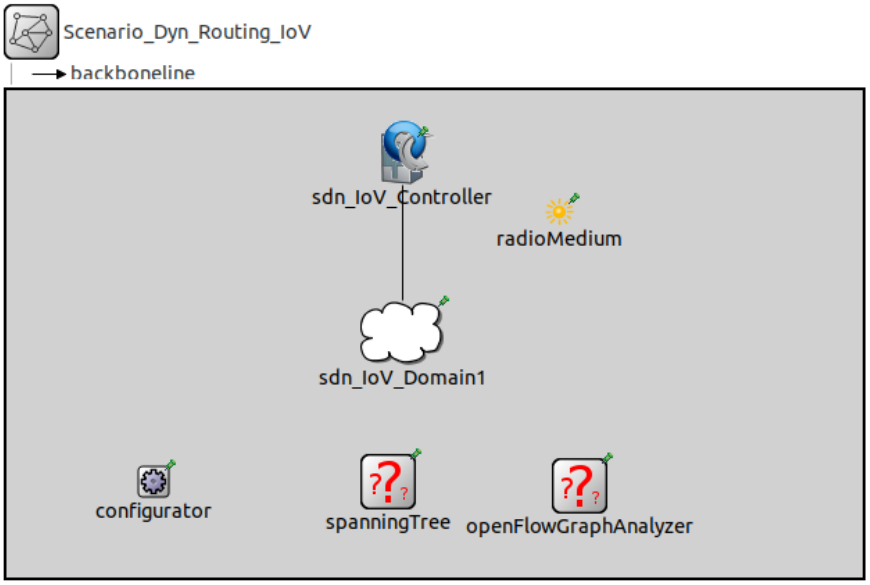

Figure 20 Le contrôle OpenFlow

- **Modèle IoV :**

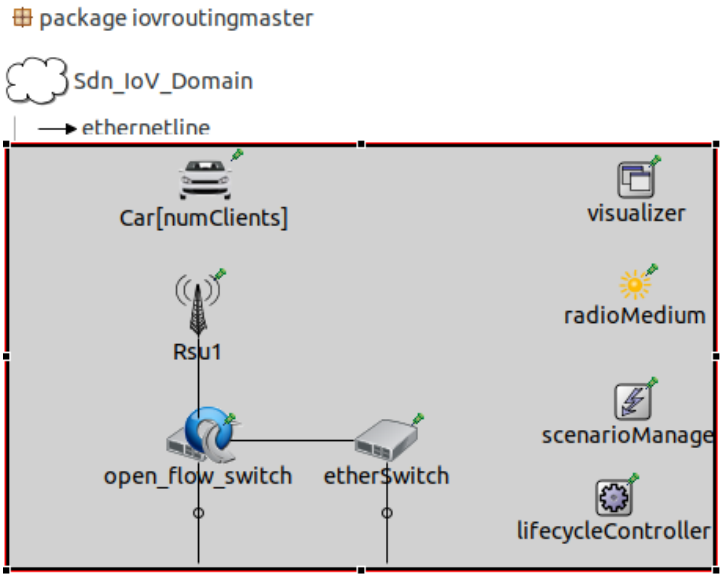

Figure 21 Domaine IoV

6. Métriques du schéma de contrôle du trafic réseau

Le SDN contrôle le trafic réseau en surveillant, analysant et gérant le flux de données à l'aide de différentes techniques et métriques. Ces mesures montrent à quel point le réseau

fonctionne et aident à gérer le trafic. Voici les métriques courantes utilisées dans le contrôle du trafic SDN :

- **Bande passante :** c'est le plus de données qui peuvent être envoyées sur un réseau en un certain temps. La surveillance de l'utilisation de la bande passante aide à identifier les points de congestion et permet des mesures de contrôle du trafic, telles que la hiérarchisation de certains types de trafic ou la mise en œuvre de politiques d'allocation de bande passante.
- **Latence :** c'est le retard des paquets de données dans un réseau. Une latence élevée peut avoir un impact négatif sur les applications en temps réel et l'expérience utilisateur. Les administrateurs réseau peuvent réduire les retards en mesurant et en surveillant la latence et en corrigeant les goulots d'étranglement grâce au contrôle du trafic.
- **Perte de paquets :** la perte de paquets se produit lorsque des paquets de données sont abandonnés ou n'atteignent pas leur destination. Cela peut arriver en raison de problèmes de réseau ou de connexions défectueuses. La vérification de la perte de paquets peut aider à détecter les problèmes de réseau et à réduire les taux de perte à l'aide de techniques telles que la mise en forme du trafic ou l'évitement de la congestion.
- **Trafic réseau :** se produit lorsqu'il y a trop de demande de ressources réseau. Le SDN surveille la congestion du réseau en temps réel en analysant la perte de paquets, la latence et la longueur des files d'attente. La détection précoce des embouteillages peut aider à améliorer les performances du réseau en utilisant l'ingénierie du trafic et l'équilibrage de charge.
- **Statistiques de flux :** le SDN fournit des données de flux, notamment la taille, la durée et la source/destination. Les statistiques de flux aident à découvrir les modèles de trafic, les anomalies et les méthodes de gestion.

Ces métriques aident le contrôleur SDN à faire des choix intelligents de contrôle du trafic. Le SDN utilise des métriques pour gérer et contrôler le trafic réseau, en l'adaptant et en l'optimisant pour atteindre les objectifs de performances.

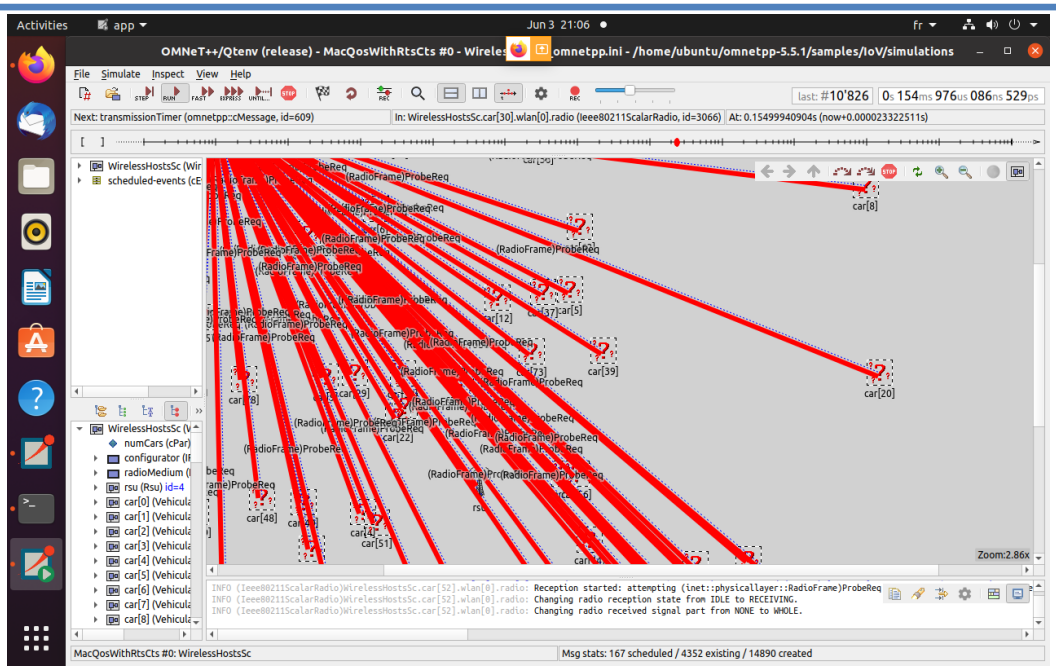

Figure 22 Routage d'information via le model V2V

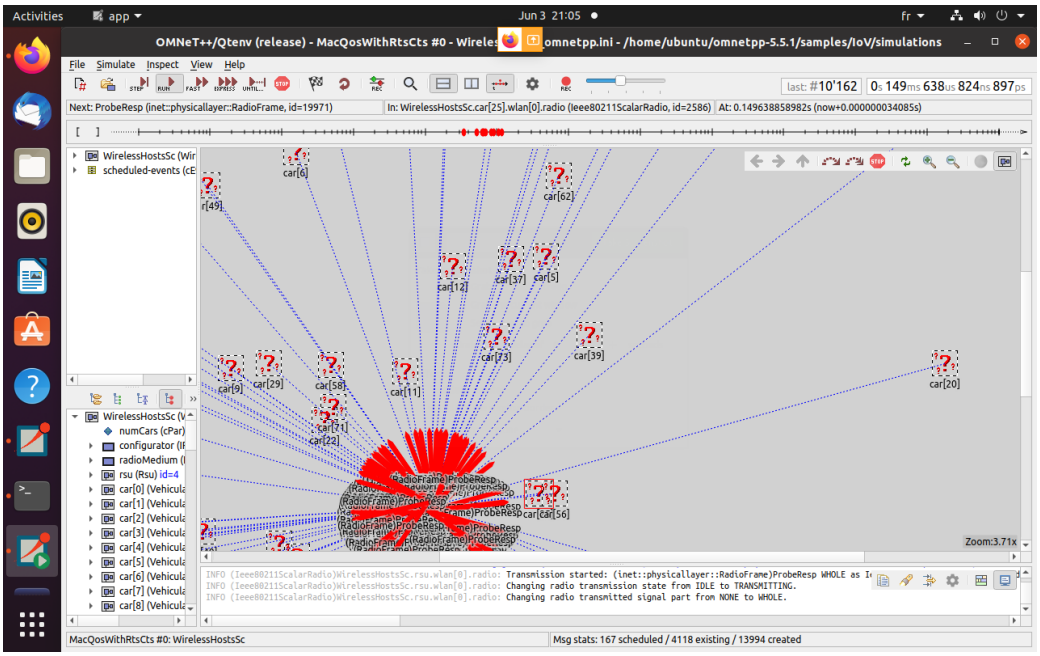

Figure 23 Routage d'information via V2I

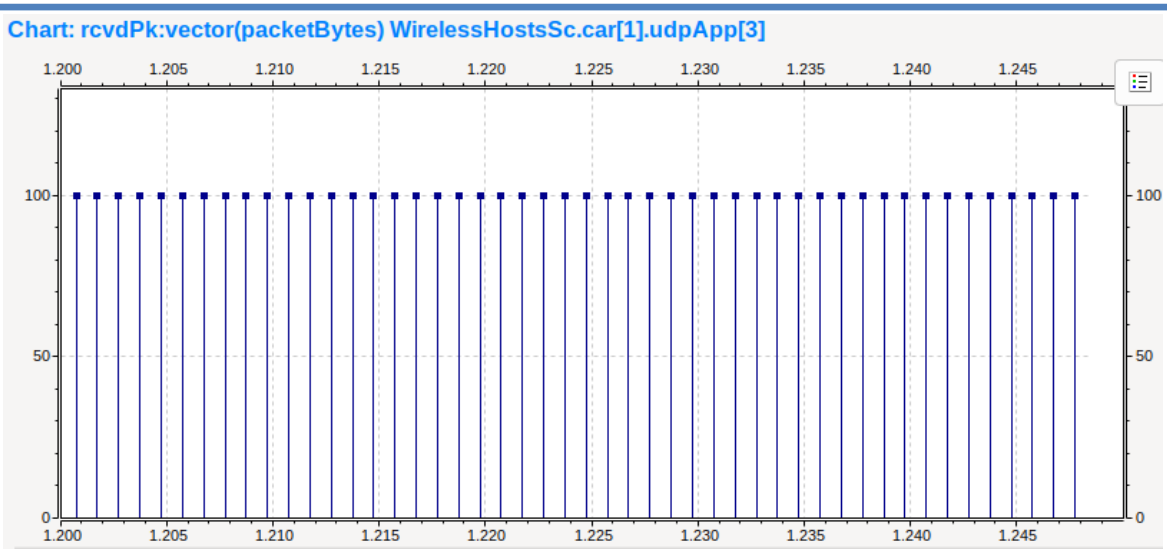

Figure 24 Nombre des paquets reçu par une application via le protocole UDP

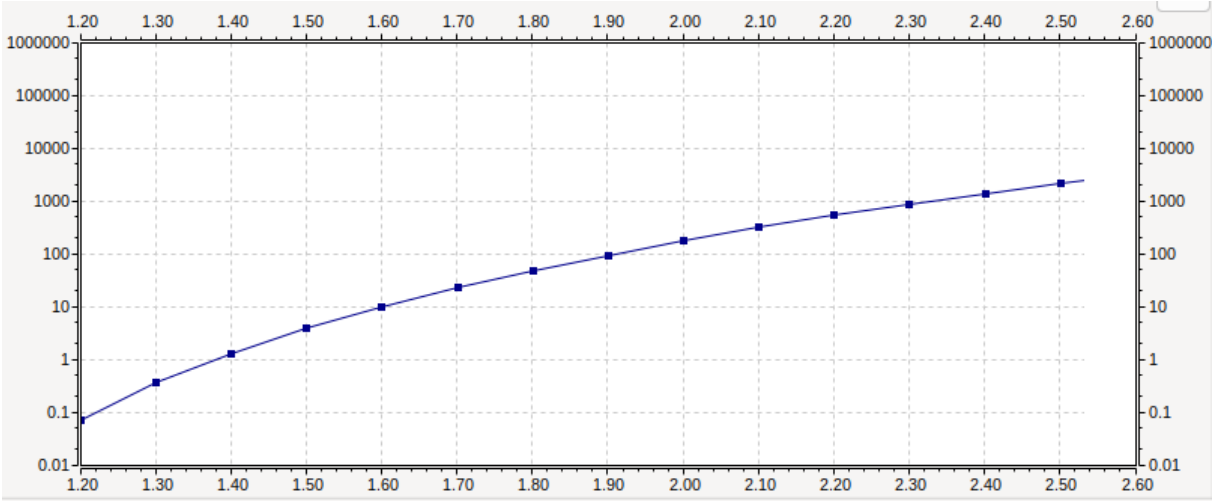

Figure 25 La bande passante consommée

7. Conclusion

Enfin, notre recherche an examiné les modèles de communication entre les véhicules et les protocoles utilisés dans le domaine de l'Internet des véhicules (IoV). En utilisant un environnement de réseau défini par le SDN, notre objectif principal était de présenter une stratégie de routage avancée et dynamique pour l'IoV.

Nous avons pu centraliser le contrôle du réseau et utiliser des contrôleurs intelligents pour gérer le routage des communications en adoptant un environnement SDN. Cela nous a permis

de mettre en place une stratégie de routage avancée et dynamique qui utilise les conditions du réseau et les besoins des véhicules pour prendre des décisions de routage en temps réel.

Plusieurs avantages ont été démontrés par notre méthode. En premier lieu, elle augmente la flexibilité en permettant une adaptation rapide aux modifications de l'environnement routier. Deuxièmement, en optimisant les chemins de communication en fonction des conditions de trafic et des contraintes du réseau, l'efficacité du routage est améliorée. Troisièmement, en permettant l'ajout ou la suppression dynamique de noeuds et de ressources réseau, elle facilite l'évolutivité.

Pour résumer, notre méthode de routage avancée et dynamique basée sur l'environnement SDN représente une avancée significative dans le domaine de l'IoV. Elle bénéficie de la flexibilité, de l'efficacité de routage et de l'évolutivité. Cependant, des efforts supplémentaires sont nécessaires pour résoudre les problèmes de sécurité, de confidentialité et de gestion du réseau.

Conclusion Générale

Pour conclure, l'objectif principal de cette thèse est de développer une architecture de Edge Computing basée sur les réseaux 5G pour améliorer l'Internet des véhicules (IoV) et de réaliser des simulations IoV dans l'environnement OMNeT++ en utilisant le protocole OpenFlow afin de réduire le trafic réseau.

Au cours de ce travail, nous avons présenté de manière générale l'Internet des véhicules et les réseaux 5G, en mettant en évidence les composants, les caractéristiques et les différentes applications dans le domaine des véhicules. Nous avons également abordé les architectures réseau et les principaux défis rencontrés par l'IoV.

Ensuite, nous avons examiné les modèles de communication entre les véhicules et les protocoles utilisés dans le domaine de l'IoV. Dans la contribution, notre objectif était de présenter une stratégie de routage avancée et dynamique pour l'IoV, en adoptant un environnement SDN.

Pour les perspectives et les travaux futurs, nous identifions plusieurs domaines d'amélioration potentiels :

1. Amélioration de la connectivité : Une connectivité améliorée dans l'IoV permettra aux véhicules de communiquer avec l'infrastructure routière, d'autres dispositifs intelligents et entre eux.
2. Sécurité de l'IoV : Des efforts supplémentaires seront consacrés à la prévention des cyberattaques pour garantir la sécurité de l'IoV.
3. Développement d'infrastructures routières intelligentes : L'IoV facilitera le développement d'infrastructures routières intelligentes, favorisant ainsi une meilleure gestion du trafic et des systèmes de transport plus efficaces.
4. Électrification des véhicules : L'IoV jouera un rôle important dans l'électrification des véhicules en permettant une gestion intelligente des stations de recharge, une planification efficace des trajets et une optimisation de la consommation d'énergie.

Ces perspectives et travaux futurs témoignent de l'importance croissante de l'IoV et de l'utilisation de l'OMNeT++ avec le protocole OpenFlow pour améliorer les fonctionnalités et les performances des réseaux IoV. Ils offrent également des opportunités de recherche et de

développement pour répondre aux défis et aux besoins émergents dans ce domaine en constante évolution.

Bibliography

[1] Li, K., Zhang, Z., Li, L., & Li, Y. (2017). The internet of vehicles: A review on technologies, challenges and opportunities. IEEE Access, 5, 3617-3634.

[2] Wu, D., Wu, C., & Sun, J. (2016). The internet of vehicles: Opportunities and challenges. IEEE Intelligent Transportation Systems Magazine, 8(1), 9-21.

[3] Chen, X., Xu, X., Zhu, H., & Wang, Y. (2017). Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds. IEEE Communications Magazine, 55(2), 84-91.

[4] Li, Z., Zhao, Y., Li, D., Liu, J., & Chen, Y. (2018). A Survey on Communication Technologies for Internet of Vehicles. Mobile Information Systems, 2018, 1-15. https://doi.org/10.1155/2018/3028936

[5] Ramanathan, R. (2018). An Empirical study on MAC layer in IEEE 802.11 p/WAVE based Vehicular Ad hoc Networks. Procedia computer science, 143, 720-727.

[6] Chen, S., Hu, J., Zhao, L., Zhao, R., Fang, J., Shi, Y., & Xu, H. (2023). Cellular Vehicle-to-Everything (C-V2X). Springer Nature.

[7] Ponsard, C., Ramon, V., & Deprez, J. C. (2021). Goal and Threat Modelling for Driving Automotive Cybersecurity Risk Analysis Conforming to ISO/SAE 21434. In SECRYPT (pp. 833-838).

[8] Al-Mayahi, I., & Sa'ad, P. M. (2012). Iso 27001 gap analysis-case study. In Proceedings of the International Conference on Security and Management (SAM) (p. 1). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

[9] Brecht, B., Therriault, D., Weimerskirch, A., Whyte, W., Kumar, V., Hehn, T., & Goudy, R. (2018). A security credential management system for V2X communications. IEEE Transactions on Intelligent Transportation Systems, 19(12), 3850-3871.

[10] Cazenave, F. (2014). Stop Google: Relever les nouveaux défis du géant du web. Pearson Education France.

[11] Kim, M., Nam, J. H., & Jang, J. W. (2014). Implementation of smart car infotainment system including black box and self-diagnosis function. International Journal of Software Engineering and Its Applications, 8(1), 267-274.

[12] Velliet, M. (2022). “Open” Telecom Networks (Open RAN): Towards a Reconfiguration of International Competition in 5G?. Notes de l’Ifri.

[13] Mültin, M. (2018, July). ISO 15118 as the Enabler of Vehicle-to-Grid Applications. In 2018 International Conference of Electrical and Electronic Technologies for Automotive (pp. 1-6). IEEE.

[14] Park, H., Miloslavov, A., Lee, J., Veeraraghavan, M., Park, B., & Smith, B. L. (2011). Integrated traffic–communication simulation evaluation environment for intellidrive applications using SAE J2735 message sets. Transportation research record, 2243(1), 117-126.

[15] Ghatikar, G. (2014). Analysis of open automated demand response deployments in california and guidelines to transition to industry standards.

[16] Kafka, P. (2012). The automotive standard ISO 26262, the innovative driver for enhanced safety assessment & technology for motor cars. Procedia Engineering, 45, 2-10.

[17] Sassenburg, H., & Kitson, D. (2006). A comparative analysis of CMMI and automotive SPICE. European SEPG, Amsterdam/Netherlands (June 2006).

[18] Birch, J., Rivett, R., Habli, I., Bradshaw, B., Botham, J., Higham, D., ... & Palin, R. (2013). Safety cases and their role in ISO 26262 functional safety assessment. In Computer Safety, Reliability, and Security: 32nd International Conference, SAFECOMP 2013, Toulouse, France, September 24-27, 2013. Proceedings 32 (pp. 154-165). Springer Berlin Heidelberg.

[19] L. -M. Ang, K. P. Seng, G. K. Ijemaru and A. M. Zungeru, "Deployment of IoV for Smart Cities: Applications, Architecture, and Challenges," in IEEE Access, vol. 7, pp. 6473-6492, 2019, doi: 10.1109/ACCESS.2018.2887076.

[20] Chowdhary, N., & Kaur, P. D. (2016, April). Addressing the characteristics of mobility models in IoV for smart city. In 2016 International Conference on Computing, Communication and Automation (ICCCA) (pp. 1298-1303). IEEE.

[21] Al-Falahy, N., & Alani, O. Y. (2017). Technologies for 5G networks: Challenges and opportunities. It Professional, 19(1), 12-20.

[22] Brisson, P., & Kropf, P. (1998). Global system for mobile communication (GSM). Université de Montréal.

[23] Prucnal, P. R. (Ed.). (2018). Optical code division multiple access: fundamentals and applications. CRC press.

[24] Mshvidobadze, T. (2012, October). Evolution mobile wireless communication and LTE networks. In 2012 6th international conference on Application of information and communication technologies (AICT) (pp. 1-7). IEEE.

[25] Kumar, S., Dixit, A. S., Malekar, R. R., Raut, H. D., & Shevada, L. K. (2020). Fifth generation antennas: A comprehensive review of design and performance enhancement techniques. IEEE Access, 8, 163568-163593.

[26] T. O. Olwal, K. Djouani and A. M. Kurien, "A Survey of Resource Management Toward 5G Radio Access Networks," in IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 1656-1686, thirdquarter 2016, doi: 10.1109/COMST.2016.2550765.

[27] Johnson, C. (2011). Radio Access Networks for UMTS: Principles and Practice. John Wiley & Sons.

[28] Mijuskovic, A., Chiumento, A., Bemthuis, R., Aldea, A., & Havinga, P. (2021). Resource management techniques for cloud/fog and edge computing: An evaluation framework and classification. Sensors, 21(5), 1832.

[29] N. Hassan, K. -L. A. Yau and C. Wu, "Edge Computing in 5G: A Review," in IEEE Access, vol. 7, pp. 127276-127289, 2019, doi: 10.1109/ACCESS.2019.2938534.

[30] N. Hassan, S. Gillani, E. Ahmed, I. Ibrar and M. Imran, "The role of edge computing in Internet of Things", IEEE Commun. Mag., vol. 56, pp. 110-115, Nov. 2018.

[31] Thirupathi, V., Sandeep, C. H., Kumar, N., & Kumar, P. P. (2019). A comprehensive review on sdn architecture, applications and major benifits of SDN. International Journal of Advanced Science and Technology, 28(20), 607-614.

[32] Liang, Geng & Li, Wen. (2018). A novel industrial control architecture based on Software-Defined Network. Measurement and Control. 51. 002029401878431. 10.1177/0020294018784310.

[33] Chaouch, S. (2017). Gestion Des Ressources Des Réseaux Cloud RAN Dans Un Contexte 5G (Doctoral dissertation, Thèse de doctorat, Télécom SudParis).

[34] Thirupathi, V., Sandeep, C. H., Kumar, N., & Kumar, P. P. (2019). A comprehensive review on sdn architecture, applications and major benifits of SDN. International Journal of Advanced Science and Technology, 28(20), 607-614.

[35] Tigadi, A., Gujanatti, R., Gonchi, A., & Klemsscet, B. (2016). Advanced driver assistance systems. International Journal of Engineering Research and General Science, 4(3), 151-158.

[36] Ang, L. M., Seng, K. P., Ijemaru, G. K., &Zungeru, A. M. (2018). Deployment of IoV for smart cities: Applications, architecture, and challenges. IEEE access, 7, 6473-6492.

[37] Hussain, M. M., Alam, M. S., & Beg, M. S. (2017). Plug-in electric vehicle to cloud data analytics for charging management. IJET, 9(3), 361-370.

[38] Dey, K. C., Rayamajhi, A., Chowdhury, M., Bhavsar, P., & Martin, J. (2016). Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication in a heterogeneous wireless network–Performance evaluation. Transportation Research Part C: Emerging Technologies, 68, 168-184.

[39] Kaiwartya, O., Abdullah, A. H., Cao, Y., Altameem, A., Prasad, M., Lin, C. T., & Liu, X. (2016). Internet of vehicles: Motivation, layered architecture, network model, challenges, and future aspects. IEEE access, 4, 5356-5373.

[40] Liu, Z., Liu, Z., Meng, Z., Yang, X., Pu, L., & Zhang, L. (2016). Implementation and performance measurement of a V2X communication system for vehicle and pedestrian safety.International Journal of Distributed Sensor Networks, 12(9), 1550147716671267.

[41] El Zorkany, M., Yasser, A., &Galal, A. I. (2020). Vehicle to vehicle "V2V" communication: scope, importance, challenges, research directions and future. The Open Transportation Journal, 14(1).

[42] Sewalkar, P., & Seitz, J. (2019). Vehicle-to-pedestrian communication for vulnerable road users: hSurvey, design considerations, and challenges. Sensors, 19(2), 358.

[43] Campolo, C., Cozzetti, H. A., Molinaro, A., &Scopigno, R. (2013). Augmenting vehicle-to-roadside connectivity in multi-channel vehicular ad hoc networks. Journal of Network and Computer Applications, 36(5), 1275-1286.

[44] Temel, S., Vuran, M. C., Lunar, M. M., Zhao, Z., Salam, A., Faller, R. K., &Stolle, C. (2018). Vehicle-to-barrier communication during real-world vehicle crash tests. Computer Communications, 127, 172-186.

[45] Borge-Diez, D., Icaza, D., Açıkkalp, E., &Amaris, H. (2021). Combined vehicle to building (V2B) and vehicle to home (V2H) strategy to increase electric vehicle market share.Energy, 237, 121608.

[46] Tan, K. M., Ramachandaramurthy, V. K., & Yong, J. Y. (2016). Integration of electric vehicles in smart grid: A review on vehicle to grid technologies and optimization techniques. Renewable and Sustainable Energy Reviews, 53, 720-732.

[47] Bagga, P., Das, A. K., Wazid, M., Rodrigues, J. J., & Park, Y. (2020). Authentication protocols in internet of vehicles: Taxonomy, analysis, and challenges. Ieee Access, 8, 54314-54344.

[48] Chen, S., Hu, J., Zhao, L., Zhao, R., Fang, J., Shi, Y., &Xu, H. (2023). Cellular Vehicle-to-Everything (C-V2X).Springer Nature.

[49] Abdelatif, S., Derdour, M., Ghoualmi-Zine, N., &Marzak, B. (2020). VANET: A novel service for predicting and disseminating vehicle traffic information. International Journal of Communication Systems, 33(6), e4288.

[50] Sanjuan, E. B., Cardiel, I. A., Cerrada, J. A., &Cerrada, C. (2020). Message queuing telemetry transport (MQTT) security: A cryptographic smart card approach. IEEE Access, 8, 115051-115062.

[51] Saint-Andre, P. (2011). Extensible messaging and presence protocol (XMPP): Core (No. rfc6120).

[52] Jutila, M., Scholliers, J., Valta, M., &Kujanpää, K. (2017). ITS-G5 performance improvement and evaluation for vulnerable road user safety services. IET Intelligent Transport Systems, 11(3), 126-133.

[53] Pazul, K. (1999). Controller area network (can) basics. Microchip Technology Inc, 1.

[54] Marx, S. E., Luck, J. D., Hoy, R. M., Pitla, S. K., Blankenship, E. E., &Darr, M. J. (2015). Validation of machine CAN bus J1939 fuel rate accuracy using Nebraska Tractor Test Laboratory fuel rate data. Computers and Electronics in Agriculture, 118, 179-185.

[55] Wellisch, D., Lenz, J., Faschingbauer, A., Pöschl, R., &Kunze, S. (2015). Vehicle-to-grid AC charging station: an approach for smart charging development. IFAC-PapersOnLine, 48(4), 55-60.

[56] Ang, L. M., Seng, K. P., Ijemaru, G. K., & Zungeru, A. M. (2018). Deployment of IoV for smart cities: Applications, architecture, and challenges. IEEE access, 7, 6473-6492.

[57] Wu, Z., Lu, Z., Hung, P. C., Huang, S. C., Tong, Y., & Wang, Z. (2019). QaMeC: A QoS-driven IoVs application optimizing deployment scheme in multimedia edge clouds. Future Generation Computer Systems, 92, 17-28.

[58] Nahri, M., Boulmakoul, A., Karim, L., &Lbath, A. (2018). IoV distributed architecture for real-time traffic data analytics. Procedia computer science, 130, 480-487.

[59] Alouache, L., Nguyen, N., Aliouat, M., & Chelouah, R. (2017). Nouveau protocole robuste pour les communications dans l'IoV. Internet des objets, 1.

[60] Mecheri, T. Une architecteurs SDN pour les réseaux locaux Étude de cas réseau ERSI_SUD/AlgerieTélécom Ouargla (Doctoral dissertation, UNIVERSITY OF KASDI MERBAH OUARGLA).

[61] Durand, J. (2015). Le SDN pour les nuls. JRES 2015-Montpellier, 1-12.

[62]Thirupathi, V., Sandeep, C. H., Kumar, N., & Kumar, P. P. (2019). A comprehensive review on sdn architecture, applications and major benifits of SDN. International Journal of Advanced Science and Technology, 28(20), 607-614.

[63] Braun, W., &Menth, M. (2014). Software-defined networking using OpenFlow: Protocols, applications and architectural design choices. Future Internet, 6(2), 302-336.

[64] Durand, J. (2015). Le SDN pour les nuls. Cisco Systems JRES.

[65] Paradis, T. (2014). Software-Defined Networking.

[66] Hakimi, A., Yusof, K. M., Azizan, M. A., Azman, M. A. A., &Hussain, S. M. (2021). A Survey on Internet of Vehicle (IoV): A pplications& Comparison of VANETs, IoV and SDN-IoV. ELEKTRIKA-Journal of Electrical Engineering, 20(3), 26-31.

[67] Chen, C., & Quan, S. (2022). A Summary of Security Techniques-Based Blockchain in IoV. Security and Communication Networks, 2022.

[68] Ang, L. M., Seng, K. P., Ijemaru, G. K., & Zungeru, A. M. (2018). Deployment of IoV for smart cities: Applications, architecture, and challenges. IEEE access, 7, 6473-6492.

[69] Kaiwartya, O., Abdullah, A. H., Cao, Y., Altameem, A., Prasad, M., Lin, C. T., & Liu, X. (2016). Internet of vehicles: Motivation, layered architecture, network model, challenges, and future aspects. IEEE access, 4, 5356-5373.

[70] Abbas, MT, Muhammad, A. & Song, WC. SD- IoV : Routage activé par SDN pour l'Internet des véhicules dans une approche consciente de la route. J Ambient Intell Human Comput 11, 1265-1280 (2020). https://doi.org/10.1007/s12652-019-01319-w

[71] MBAYE, M. (2020). Un plan de contrôle intelligent pour le déploiement de services de sécurité dans les réseaux SDN. Gestion et contrôle intelligents des réseaux: Sécurité intelligente, optimisation multicritères, Cloud Computing, Internet of Vehicles, radio intelligente, 29.