

**République Algérienne Démocratique et Populaire**  
**Ministère de l'enseignement supérieur et de la recherche scientifique**  
**Université de 8 Mai 1945 – Guelma -**  
**Faculté des Mathématiques, d'Informatique et des Sciences de la**  
**matière**  
**Département d'Informatique**



**Mémoire de Fin d'études Master**

**Filière : Informatique**

**Option : SIQ**

**Thème :**

---

**Un algorithme pour la sélection de réseau dans**  
**IoV**

---

**Membres du jury:**

|                        |           |
|------------------------|-----------|
| Dr. Zedadra Warda      | président |
| Dr. Benhamida Nadjette | Encadreur |
| Dr. Gouasmi Nouredine  | Examineur |

**Présenté par :**  
**Saaidia Abderrahim**

**Septembre 2024**

## **Remerciement**

Je tiens à exprimer ma profonde gratitude à toutes les personnes qui ont contribué à la réalisation de ce mémoire.

Tout d'abord, je remercie sincèrement madame Benhamida Nadjette pour son encadrement, ses conseils avisés et sa patience tout au long la phase de réalisation de ce projet. Son expertise et son soutien constant ont été essentiels à l'aboutissement de ce travail.

Je souhaite également remercier les membres du jury pour l'honneur qu'ils me font en acceptant d'évaluer ce mémoire et pour leurs précieuses observations et suggestions.

Je suis reconnaissant envers mes collègues et amis pour leur soutien moral, leurs discussions enrichissantes et leur aide précieuse lors des moments difficiles.

Un grand merci à ma famille, pour leur amour, leur encouragement et leur compréhension tout au long de mes études. Leur soutien indéfectible m'a permis de surmonter les nombreux défis rencontrés durant ce parcours.

Enfin, je remercie toutes les personnes qui ont apporté, directement ou indirectement, leur contribution à ce travail.

## Dédicace

Je dédie ce mémoire à toutes les personnes qui ont cru en moi et m'ont soutenu tout au long de ce parcours académique.

À mes parents, pour leur amour inconditionnel, leur soutien indéfectible et leurs sacrifices. Vous m'avez toujours encouragé à poursuivre mes rêves et à ne jamais abandonner. Ce travail est le fruit de votre confiance en moi.

À Madame Benhamida Nadjette, pour ton soutien constant, ta patience et ta compréhension. Ta présence à mes côtés m'a été d'une grande aide.

À mes amis proches pour votre amitié, vos encouragements et les moments de détente qui m'ont permis de garder l'équilibre tout au long de ces années d'études.

À mes amis Menasria Chams Eddine et Aidaoui Fakher Eddine, que Dieu vous libère.

À toutes le membre de clane H2H de pubg mobile.

À tous mes professeurs, pour avoir partagé leur savoir et pour leurs conseils précieux. Vous avez tous contribué à mon épanouissement intellectuel et professionnel.

Enfin, à tous ceux qui m'ont inspiré et encouragé de près ou de loin, je dédie ce mémoire.

Tables des matières :

|                                                                  |            |
|------------------------------------------------------------------|------------|
| <b>Remerciement.....</b>                                         | <b>i</b>   |
| <b>Didicase .....</b>                                            | <b>ii</b>  |
| <b>Tables des matières .....</b>                                 | <b>iii</b> |
| <b>Liste des figures .....</b>                                   | <b>v</b>   |
| <b>Liste des tableau.....</b>                                    | <b>vi</b>  |
| <b>Liste des abréviations .....</b>                              | <b>vii</b> |
| <b>Résumé .....</b>                                              | <b>iix</b> |
| <b>Abstract:.....</b>                                            | <b>x</b>   |
| <b>المخلص:.....</b>                                              | <b>xi</b>  |
| <b>Introduction générale.....</b>                                | <b>1</b>   |
| <b>1- Introduction .....</b>                                     | <b>3</b>   |
| <b>2- Définition.....</b>                                        | <b>3</b>   |
| <b>3- Les types de communications de l’IoV.....</b>              | <b>4</b>   |
| <b>4- Les domaines d’application de l’IoV.....</b>               | <b>6</b>   |
| ➤ <b>Les applications de sécurité routière : .....</b>           | <b>6</b>   |
| ➤ <b>Les applications de confort :.....</b>                      | <b>7</b>   |
| ➤ <b>Les applications commerciaux:.....</b>                      | <b>7</b>   |
| <b>5- Les architectures de L’IOV .....</b>                       | <b>8</b>   |
| <b>5.1- L’architecture en 03 couches : .....</b>                 | <b>8</b>   |
| <b>5.2- L’architecture en 04 couches : .....</b>                 | <b>9</b>   |
| <b>5.3- L’architecture en 05 couches : .....</b>                 | <b>11</b>  |
| <b>5.4- L’architecture en 07 couches : .....</b>                 | <b>13</b>  |
| <b>6- Les technologies de communication de l’IOV .....</b>       | <b>16</b>  |
| <b>I. Bluetooth : .....</b>                                      | <b>16</b>  |
| <b>II. Wifi : .....</b>                                          | <b>16</b>  |
| <b>III. DSRC : .....</b>                                         | <b>16</b>  |
| <b>IV. ZigBee : .....</b>                                        | <b>16</b>  |
| <b>V. WIMAX : .....</b>                                          | <b>16</b>  |
| <b>VI. MBWA : .....</b>                                          | <b>16</b>  |
| <b>VII. LTE (4G/5G) : .....</b>                                  | <b>17</b>  |
| <b>VIII. Microwave : .....</b>                                   | <b>17</b>  |
| <b>Chapitre 02 : les algorithmes de sélection de réseau.....</b> | <b>19</b>  |
| <b>1- Introduction .....</b>                                     | <b>19</b>  |

|                                                                                 |           |
|---------------------------------------------------------------------------------|-----------|
| 2- Les algorithmes de sélection de réseau : .....                               | 19        |
| 2.1- Algorithmes basés sur la force du signal reçu (RSS) : .....                | 19        |
| 2.2- Les algorithmes basés sur la théorie de la logique floue (FL) : .....      | 20        |
| 2.3- Les algorithmes basés sur la fonction d'utilité (UF) : .....               | 20        |
| 2.4- Les algorithmes basés sur la théorie des jeux (GT) : .....                 | 21        |
| 2.5- Les algorithmes basés sur la prise de décision multicritère (MADM) : ..... | 21        |
| 2.6- Algorithme de sélection de réseaux basée sur la QoS : .....                | 22        |
| 3- Comparaison entre les algorithmes.....                                       | 23        |
| <b>Chapitre 03 : Conception et Implémentation .....</b>                         | <b>26</b> |
| 1- Introduction .....                                                           | 26        |
| 2- Conception et modélisation.....                                              | 26        |
| 2.1 Algorithme proposée : .....                                                 | 26        |
| 2.2- Modèle et système : .....                                                  | 35        |
| 2.3- Organigramme d'exécution : .....                                           | 37        |
| 2.4- Diagramme de séquence .....                                                | 38        |
| 3- Implémentation.....                                                          | 39        |
| 3-1 Omnet++ : .....                                                             | 39        |
| 3.1.1Présentation de la plateforme OMNet++.....                                 | 39        |
| 3.1.2Architecture de OMNET++ : .....                                            | 39        |
| 3.1.3Les principaux fichiers d'OMNET++ : .....                                  | 40        |
| 3.1.4Modèles.....                                                               | 40        |
| 3.1.4.1 INET Framework.....                                                     | 41        |
| 3.2- Paramètre de simulation : .....                                            | 41        |
| 3.4- Scénario de simulation : .....                                             | 42        |
| 3.4.1- Interface graphique de simulation : .....                                | 42        |
| 3.5- Exécution de simulation : .....                                            | 43        |
| 4- Conclusion : .....                                                           | 48        |
| <b>Conclusion générale .....</b>                                                | <b>49</b> |
| Références : .....                                                              | 51        |

## Liste des figures

|                                                                                                |    |
|------------------------------------------------------------------------------------------------|----|
| Figure 1: Les types de communication d'IOV .....                                               | 06 |
| Figure 2: l'architecture de l'IOV sur 03 couches .....                                         | 09 |
| Figure 3 : l'architecture de l'IOV sur 04 couches .....                                        | 11 |
| Figure 4 : architecture de l'IOV sur 5 couches .....                                           | 13 |
| Figure 5 : l'architecture de l'IOV sur 07 couches .....                                        | 15 |
| Figure 6 : Le modèle de simulation.....                                                        | 36 |
| Figure 7 : organigramme de l'algorithme .....                                                  | 37 |
| Figure 8 : diagramme de séquence.....                                                          | 38 |
| Figure 9 : interface graphique de simulation.....                                              | 43 |
| Figure 10 : envoi de message par véhicule aux les nœuds.....                                   | 43 |
| Figure 11 : le signal du message envoi par le véhicule à les nœuds .....                       | 44 |
| Figure 12 : confirmation de recevoir de message de véhicule pour envoi l'information .....     | 44 |
| Figure 13 : envoi les informations des nœuds au véhicule.....                                  | 44 |
| Figure 14 : Drone envoi information au véhicule et est active au les nœuds.....                | 45 |
| Figure 15 : Car envoi information au véhicule et est active au les nœuds .....                 | 45 |
| Figure 16 : Antenne envoi information au véhicule et est active au les nœuds.....              | 46 |
| Figure 17 : Point d'accès envoi information au véhicule et est active au les nœuds.....        | 46 |
| Figure 18 : Téléphone personnel envoi information au véhicule et est active au les nœuds ..... | 47 |
| Figure 19 : la réception des informations de chaque nœuds .....                                | 47 |
| Figure 20 : Calcule la distance entre véhicule et les autres nœuds .....                       | 47 |
| Figure 21 : Calcule la note best de chaque nœud.....                                           | 48 |
| Figure 22 : choisir le meilleur réseau.....                                                    | 48 |

## Liste des tableaux

|                                                                                |    |
|--------------------------------------------------------------------------------|----|
| Tableau 1 : Les avantages et les inconvénients de différents algorithmes ..... | 24 |
| Tableau 2: avantages de la solution proposée .....                             | 35 |
| Tableau 3: paramètres de simulation .....                                      | 42 |

## Liste des abréviations

BS: Base station

DSRC: Dedicated Short Range Communication.

FL: Fuzzy Logic.

GPS: Global Positioning System.

GSM: Global System for Mobile communication.

GT: Game Theory.

IoT: Internet Of Things.

IoV: Internet Of vehicle.

IPv4: Internet Protocol Version 4.

IPv6: Internet Protocol Version 6.

ITS : Intelligents Transportation Systems

LTE: long Term Evolution.

MAMD: Multi-Attribute Decision Making.

OBU: On Bord Unit.

OMNeT++: Objective Modular Network Testbed in C++.

OSI: Open Systems Interconnection.

PAN: Personal Area Network.

PPP: Point-to-Point Protocol.

QoS: Quality of Service.

RFID: Radio Frequency Identification.

RSS: Received Signal Strings.

RSU: Road Station Unit.



SCTP: Stream Control Transmission Protocol.

TCP: Transmission Control Protocol.

UDP: User Datagram Protocol.

UF: Utility Function.

UML: Unified Modeling Language.

V2I: Vehicle To Infrastructure.

V2N: Vehicle To Network.

V2P: Vehicle To pedestrian.

V2R: Vehicle To Road.

V2S: Vehicle To sensor.

V2V: Vehicle To Vehicle.

VANET: Vehicular Ad hoc Network.

## Résumé

L'Internet des véhicules (IoV) est un système de communication avancé permettant l'échange d'informations entre les véhicules, les infrastructures routières et tous les composants qui en sont connectés. Pour garantir des communications efficaces et fiables, un algorithme de sélection du meilleur réseau disponible pour les véhicules en mouvement est indispensable.

L'objectif principal de ces algorithmes est de sélectionner le réseau le plus adapté en tenant compte de plusieurs critères. Ces critères permettent d'assurer une connectivité stable et performante, essentielle pour la gestion intelligente du trafic, les services d'information en temps réel et le contrôle des véhicules.

Dans ce travail, nous proposons un algorithme pour la sélection du meilleur réseau disponible et nous l'implémentons et évaluons sous OMNET++.

**Mots clés :** IoV, sélection de réseau, OMNET++.

**Abstract:**

The Internet of Vehicles (IoV) is an advanced communication system that facilitates the exchange of information between vehicles, road infrastructures, and various other connected components. Ensuring effective and reliable communications necessitates selection algorithms of the best available network for moving vehicles.

The primary objective of these algorithms is to select the most suitable network by considering multiple criteria. These criteria ensure stable and high-performance connectivity, which is essential for intelligent traffic management, real-time information services, and vehicle control.

In this work, we propose an algorithm for the best network selection and implement this algorithm on OMNET++.

**Keywords:** IoV, best network selection, OMNET++.

## الملخص:

إنّ الإنترنت للمركبات (IoV) هو نظام اتصال متقدم يُمكن تبادل المعلومات بين المركبات وبنى التحتية الطريقية ومكونات متصلة أخرى متعددة. يتطلب ضمان التواصل الفعال والموثوق اختيار الشبكة الأفضل المتاحة للمركبات أثناء التنقل.

الهدف الرئيسي لهذه الخوارزميات هو اختيار الشبكة الأكثر ملاءمة بناءً على معايير متعددة. تلك المعايير تضمن استقرار التواصل وأدائه العالي، الأمر الضروري لإدارة حركة المرور بذكاء وتقديم خدمات المعلومات في الوقت الحقيقي والتحكم في المركبات.

في هذا العمل، نقترح خوارزمية لاختيار أفضل شبكة ونقوم بتنفيذ هذه الخوارزمية باستخدام OMNET++ .

الكلمات المفتاحية: IoV، اختيار أفضل شبكة، OMNET++.

## **Introduction générale**

L'Internet des véhicules (IoV) est un système distribué à grande échelle permettant la communication sans fil et l'échange d'informations entre les véhicules, les infrastructures routières et les usagers via Internet, en utilisant des protocoles de communication et des normes d'interaction de données convenues. L'IoV forme un réseau intégré qui prend en charge la gestion intelligente du trafic, les services d'information dynamique intelligents et le contrôle intelligent des véhicules, constituant ainsi une application typique de l'Internet des Objets (IoT) dans les systèmes de transport intelligents (ITS).

La convergence des technologies impliquées dans l'IoV englobe la communication d'informations, la protection de l'environnement, les économies d'énergie et la sécurité. Pour réussir sur ce marché émergent, il est essentiel de maîtriser les technologies et les normes de base afin d'obtenir un avantage stratégique. Toutefois, l'intégration de l'IoV avec d'autres infrastructures existantes est tout aussi importante que le développement des technologies IoV elles-mêmes. Ainsi, l'IoV s'inscrira naturellement dans la plus vaste infrastructure de l'IoT à mesure que celle-ci se développera. Il est également essentiel de souligner que la collaboration entre le secteur des transports et d'autres industries, telles que l'énergie, la santé, l'environnement, l'industrie manufacturière et l'agriculture, jouera un rôle déterminant dans les futures évolutions de l'IoV.

La sélection du réseau dans l'IoV constitue une composante clé pour garantir des communications fluides et efficaces entre les véhicules, les infrastructures routières et les autres éléments connectés. Les algorithmes de sélection de réseau doivent tenir compte de plusieurs critères, tels que le débit, la latence, la fiabilité et l'utilisation des ressources disponibles, afin de choisir le meilleur réseau pour chaque véhicule.

L'objectif principal de cette sélection est d'assurer une connexion stable et performante pour les véhicules en mouvement, tout en optimisant l'utilisation des différentes technologies de communication, telles que la norme IEEE 802.11p WAVE et les réseaux cellulaires. Ces algorithmes doivent également s'adapter aux conditions changeantes des réseaux, comme les variations de charge ou les interférences.

Dans ce mémoire, nous proposons un algorithme de sélection du meilleur réseau, qui intègre non seulement des critères classiques tels que le débit, la latence et la fiabilité, mais prend également en considération le facteur de sécurité des communications. L'inclusion de ce paramètre est important dans un contexte où les véhicules échangent des données sensibles, comme des informations de géolocalisation ou des instructions de conduite automatisée. En garantissant un niveau de sécurité optimal, notre algorithme vise à protéger ces échanges contre d'éventuelles attaques ou intrusions, tout en assurant une communication stable et efficace. Cette approche renforce la confiance dans les systèmes IoV, où la sécurité est un enjeu majeur pour le bon fonctionnement des infrastructures intelligentes et la protection des usagers.

- Le premier chapitre sera consacré à l'Internet des Véhicules (IoV). Nous débuterons par une définition du concept, suivie d'une présentation des différents types de communication dans l'IoV. Nous aborderons ensuite les domaines d'application de l'IoV, ses architectures et, pour conclure, les technologies de communication utilisées.
- Le deuxième chapitre traitera des divers algorithmes de sélection de réseaux, avec une comparaison des principales approches avant de présenter notre propre algorithme.
- Enfin, le troisième chapitre portera sur l'implémentation de notre algorithme au sein de l'environnement de simulation OMNET++.

# Chapitre 01 : L'internet des véhicules

## 1- Introduction

L'Internet des Véhicules (IoV) représente une avancée majeure dans les technologies de transport intelligentes. En intégrant les concepts de l'Internet des Objets (IoT) aux infrastructures et systèmes automobiles, l'IoV vise à créer un réseau de véhicules connectés capables de communiquer entre eux ainsi qu'avec leur environnement. Cette interconnexion permet de développer des applications innovantes et variées, promettant de transformer la mobilité, la gestion du trafic, la sécurité routière et l'efficacité énergétique [45].

Dans ce chapitre, nous abordons les concepts clés de l'Internet des Véhicules. Nous commencerons par une définition de l'IoV, suivie d'une présentation des principaux types de communication utilisés dans ces réseaux. Ensuite, nous discuterons de certains domaines d'application de l'IoV, ainsi que de ses architectures et technologies de communication.

## 2- Définition

L'Internet des véhicules (IoV) est un terme général désignant l'interconnexion des véhicules et leur interaction avec leur environnement. Il s'agit d'un réseau de véhicules connectés qui communiquent entre eux pour partager des informations, analyser les conditions de circulation et fournir des services aux conducteurs [1].

L'Internet des Véhicules représente un autre jalon vers la ville intelligente, après l'avènement de l'Internet et de l'Internet des Objets. Par rapport aux services de communication mobile traditionnels, le domaine d'application de l'Internet des Véhicules se distingue par sa portée commerciale plus vaste, sa chaîne de valeur étendue et ses exigences professionnelles accrues. Sur le plan technique, les réseaux automobiles doivent d'abord collecter diverses informations à travers une gamme de capteurs, tels que l'identification par radiofréquence, les capteurs infrarouges, le système de positionnement

global (GPS), et d'autres dispositifs. Ce processus permet d'obtenir une compréhension approfondie de l'environnement routier, des conditions de conduite et des interactions entre les véhicules, ouvrant ainsi la voie à une nouvelle ère de mobilité intelligente et sécurisée. Les dispositifs de détection, tels que les scanners laser, jouent un rôle important dans la collecte d'informations pour permettre l'échange de données entre les véhicules. Ils facilitent l'identification intelligente, le positionnement, le suivi, la surveillance et la gestion. Ces dernières années, en Chine, le développement du réseau de capteurs basé sur la technologie RFID (Radio Frequency Identification) s'est accéléré. Ce réseau constitue un pilier essentiel pour l'essor de la mise en réseau des véhicules. En exploitant ces technologies de manière stratégique, les réseaux de véhicules peuvent bénéficier d'une communication plus fluide, d'une gestion du trafic améliorée, et d'une sécurité renforcée sur les routes. Ce progrès est fondamental pour façonner l'avenir des transports intelligents et la connectivité des véhicules [2].

### **3- Les types de communications de l'IoV**

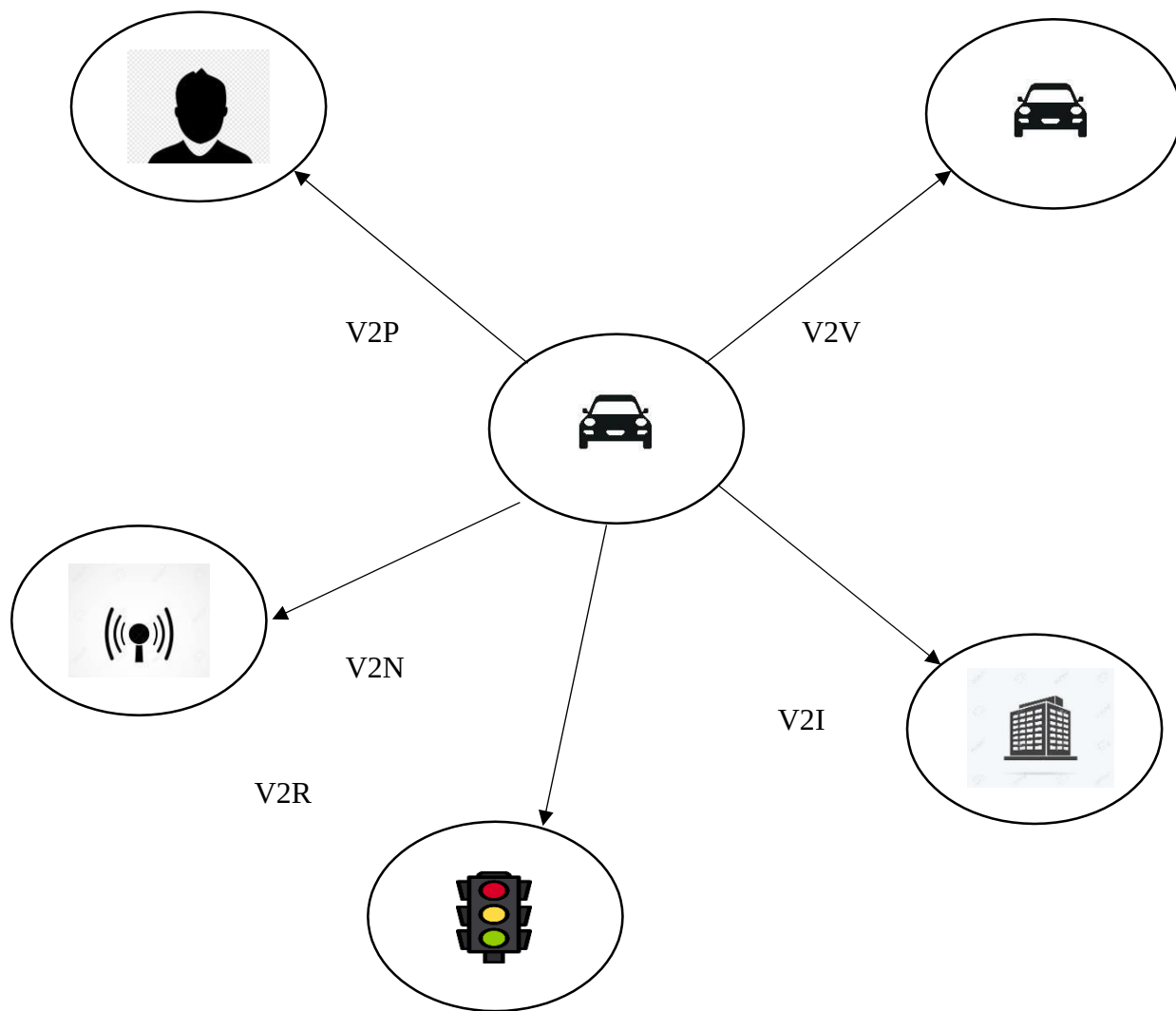
Les réseaux de véhicules peuvent être classés en plusieurs types de structures, en fonction de la capacité des usagers de la route à accéder aux données et à les partager.

- **Les communications de Véhicule à Véhicule (V2V) :** permettant à un véhicule de recevoir, transmettre ou échanger des informations routières avec d'autres véhicules inclut des données sur les conditions de circulation et les incidents sur la route [5].
- **Les communications de Véhicule à Infrastructure (V2I) :** utilisés pour diffuser des informations entre l'infrastructure du réseau et les véhicules, ainsi que pour échanger des données nécessaires sur les conditions routières et les mesures de sécurité à prendre. Dans ce mode, un véhicule se connecte aux Unités de Station Routière (RSU) ou aux Stations de Base (SB) pour communiquer avec des réseaux externes comme l'internet. Les liaisons V2I sont moins vulnérables aux attaques et nécessitent une bande passante plus importante que les liaisons V2V [6].
- **Les communications de Véhicule à Pedestrian (V2P)** Les communications entre un véhicule et un usager de la route non motorisé, comme un piéton ou un cycliste, visent à réduire les risques de collisions. Pour ce faire, les communications V2P



utilisent des technologies telles que le Bluetooth Low Energy, l'Ultra Wide Band et les réseaux cellulaires. Ces communications peuvent être unilatérales, où seule l'une des entités (usager de la route ou véhicule) est avertie de l'approche de l'autre, ou bilatérales, où les deux entités sont informées du risque de collision. [7].

- **Les communications de véhicule à réseau (V2N) :** Les communications entre un véhicule et un équipement du réseau de communication cellulaire, comme les stations de base (BS), offrent les mêmes fonctionnalités que les communications V2I dans les zones sans équipements de bord de route (RSU). Les BS peuvent transmettre des informations entre véhicules, telles que l'état de la chaussée et les accidents. De plus, les communications V2N assurent un accès à Internet, permettant aux véhicules de se connecter à des services distants [8].
- **Les communications de Véhicule à Route (V2R) :** Les véhicules peuvent interagir avec une infrastructure fixe le long des routes pour fournir des services de communication et d'information aux utilisateurs. Lorsque les véhicules échangent des informations, ceux à proximité utilisent la technique V2V, tandis que pour les véhicules plus éloignés, la communication se fait via V2R, d'où le nom de cette technologie. La connectivité Véhicule-Route (V2R) est indispensable pour améliorer les performances des réseaux dédiés aux véhicules (VANET) [9].



*Figure 1: Les types de communication d'IOV*

#### **4- Les domaines d'application de l'IoV**

##### **➤ Les applications de sécurité routière :**

Les applications de sécurité routière des réseaux véhiculaires ad hoc (VANET) sont conçues pour prévenir ou réduire les accidents de la route. Ces applications, sensibles au temps, fournissent des informations essentielles pour une gestion efficace du trafic. Par exemple, en cas d'accident, les véhicules proches du danger reçoivent des alertes

d'urgence. Ces notifications sont envoyées à un centre d'appels, qui les transmet ensuite aux services d'urgence. Chaque fois qu'un accident se produit, un système de notification envoie des messages d'urgence aux intervenants concernés, incluant la localisation estimée du véhicule grâce à un GPS compatible [10].

Les applications de sécurité routière des réseaux véhiculaires ad hoc (VANET) peuvent être classées en cinq catégories :

- ❖ Évitement des collisions aux intersections : Par exemple, un assistant de mouvement pour la signalisation d'arrêt.
- ❖ Sécurité publique : Comme la préemption de la signalisation pour les véhicules d'urgence.
- ❖ Extension de la signalisation : Par exemple, des avertissements sur les comportements dangereux pour les conducteurs.
- ❖ Diagnostic et maintenance des véhicules : Par exemple, des avis de rappel de sécurité.
- ❖ Informations provenant d'autres véhicules : Telles que des alertes sur l'état de la route [11].

➤ **Les applications de confort :**

Dans cette catégorie, les conducteurs peuvent profiter de services véhiculaires qui améliorent leur confort et leur expérience de conduite. Ces applications visent à fournir des informations fiables et disponibles au bon moment, répondant aux besoins des conducteurs. Elles incluent notamment :

- Applications d'accès à Internet en voiture.
- Partage de fichiers et de données avec d'autres conducteurs.
- Applications de localisation des stations de service, des restaurants, des hôtels et des stations d'essence [13].

➤ **Les applications commerciales:**

Aujourd'hui, les véhicules intelligents équipés de technologies avancées créent une forte concurrence entre les constructeurs automobiles dans les domaines du commerce et de la publicité. Ces applications commerciales offrent aux conducteurs des services de

divertissement adaptés à la dynamique et à la mobilité des véhicules et des individus au sein des réseaux véhiculaires ad hoc (VANET). Cela inclut :

- **Accès à Internet** pour effectuer des achats ou des ventes en ligne
- **Contrôle domestique** à distance
- **Services de divertissement synchronisés** avec la mobilité des véhicules

Ces innovations visent à améliorer l'expérience de conduite en offrant des services pratiques et connectés [14].

## **5- Les architectures de L'IOV**

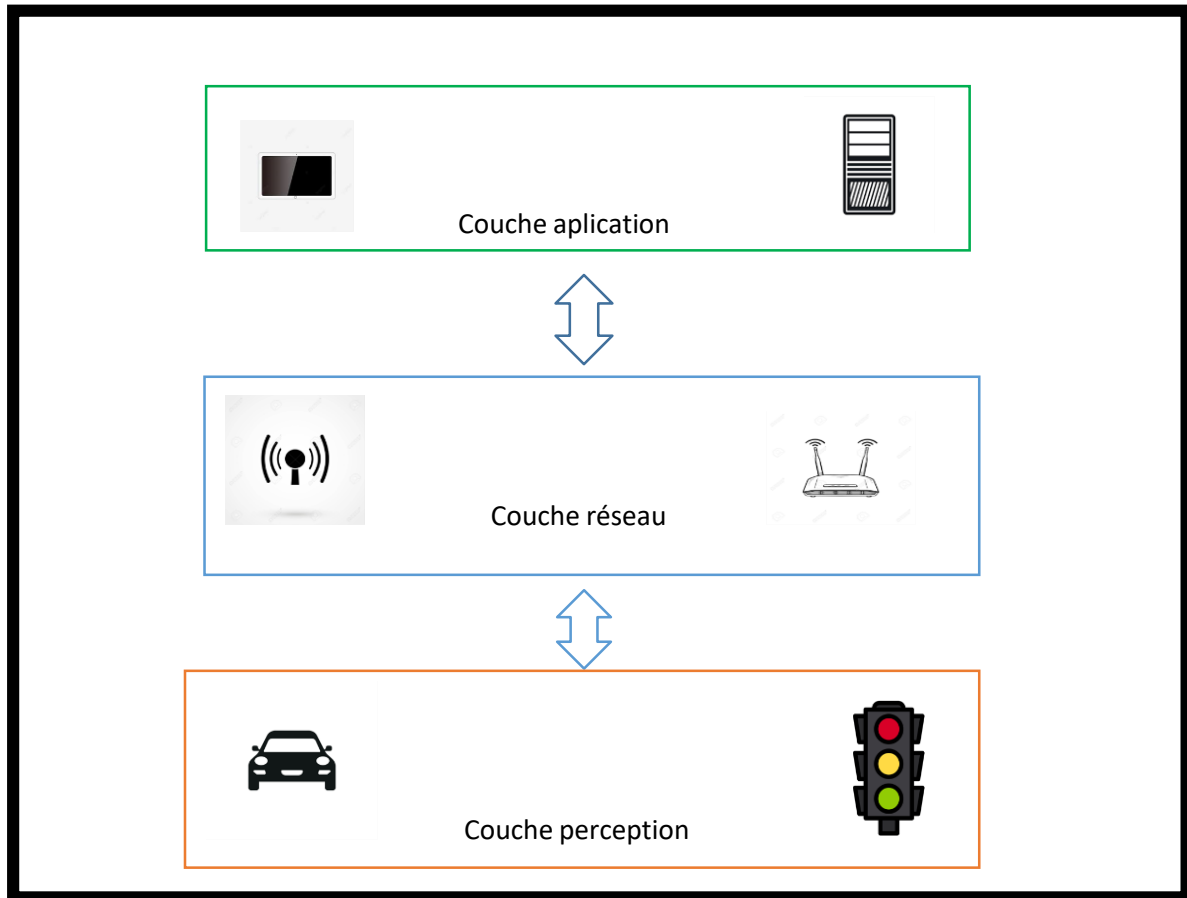
En raison des différentes compréhensions de l'Internet des Véhicules (IoV), il n'existe actuellement aucune architecture spécifique pour l'IoV. Certains chercheurs proposent une architecture basée sur l'Internet des Objets (IoT), similaire à l'IoV, composée d'une couche de détection, d'une couche réseau et d'une couche d'application. Cependant, l'IoV ne se limite pas à un réseau de services pour la communication entre véhicules ou terminaux de véhicules. C'est un système complexe caractérisé par une interaction étroitement coordonnée entre l'homme, le véhicule et l'environnement, ainsi qu'une évolution extrêmement dynamique [15].

### **5.1- L'architecture en 03 couches :**

L'architecture à trois couches de l'Internet des véhicules (IoV) se décompose sur les couches suivantes :

1. **Couche de perception** : Les capteurs du véhicule collectent des données sur l'environnement et détectent des événements comme la position des véhicules, les modèles de conduite et les conditions environnementales.
2. **Couche de réseau** : Elle prend en charge divers types de communication sans fil, notamment véhicule à piéton (V2P), véhicule à infrastructure (V2I), véhicule à véhicule (V2V) et véhicule à capteur (V2S). Cette couche assure une connectivité fluide entre plusieurs réseaux tels que IEEE 802.15.4, IEEE 802.11p, GSM, LTE, Wi-Fi et Bluetooth.

3. **Couche d'application** : Elle utilise des ressources d'intelligence IoV pour prendre des décisions dans des situations à risque, comme les conditions routières dangereuses et les accidents. Cette couche s'appuie sur des outils statistiques ainsi que sur des ressources de stockage et de traitement de données massives (big data) [16].



*Figure 2: l'architecture de l'IOV sur 03 couches*

#### **5.2- L'architecture en 04 couches :**

L'architecture en quatre couches de l'Internet des véhicules (IoV) proposée par CISCO se présente comme suit :

1. **Couche des véhicules** : Cette couche inclut les véhicules eux-mêmes et les logiciels de communication, principalement pour les communications V2V (véhicule à véhicule) utilisant le protocole 802.11p.
2. **Couche d'infrastructure** : Elle définit les technologies permettant la connectivité entre tous les participants de l'écosystème IoV, assurant que le véhicule reste connecté à tout moment.
3. **Couche d'opération** : Cette couche vérifie et assure le respect des politiques applicables à la gestion de l'information et des flux de données.
4. **Couche cloud** : Elle spécifie le type de nuage (public, privé ou commercial) en fonction d'un profil défini, et permet la réception de services à la demande, tels que la voix, la vidéo d'entreprise et les données [17].

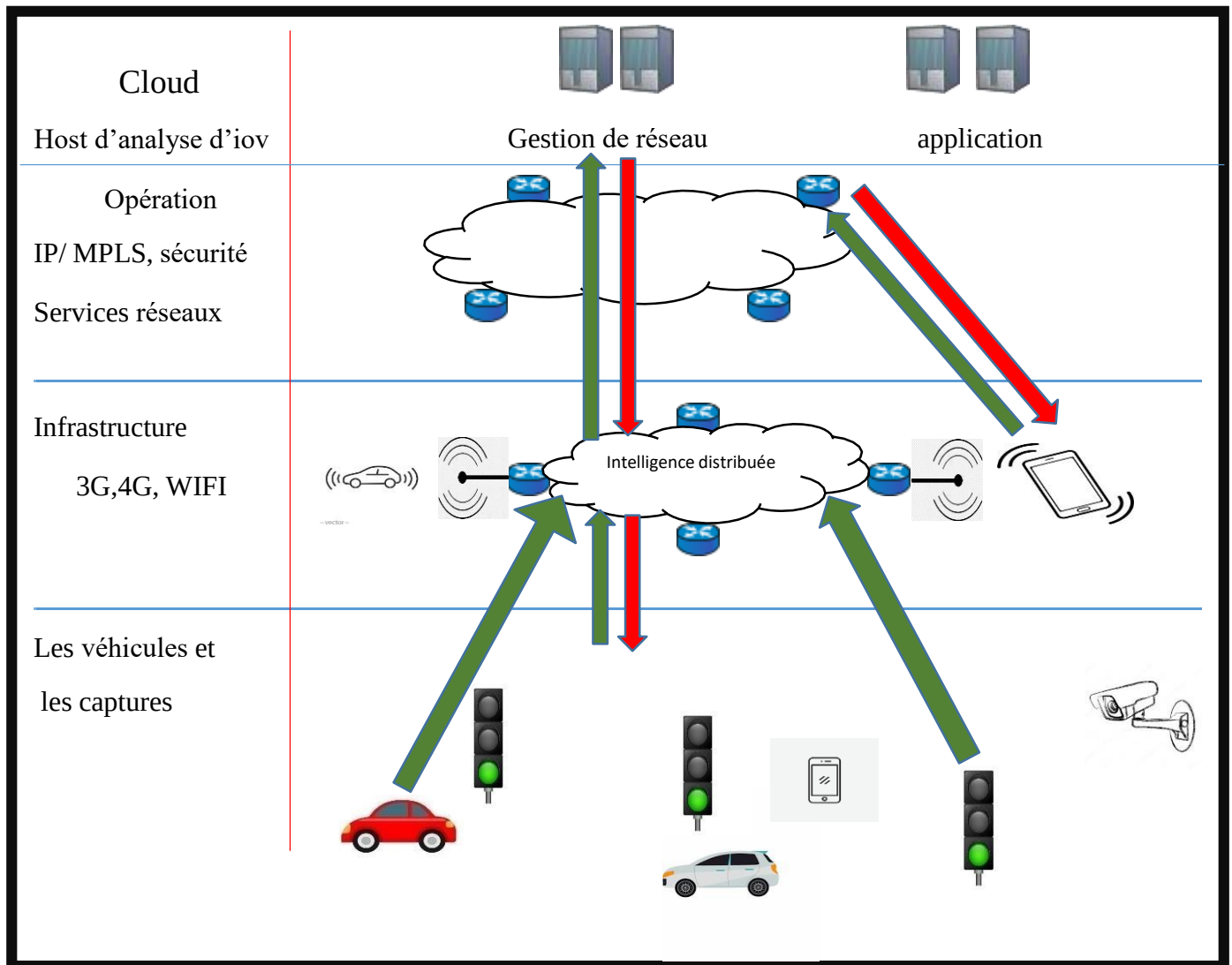


Figure 3 : l'architecture de l'IOV sur 04 couches

### 5.3- L'architecture en 05 couches :

L'architecture en cinq couches de l'Internet des véhicules (IoV) contient les couches suivantes :

1. **Couche de perception** : Gère l'interaction entre le véhicule et son environnement. Elle utilise des dispositifs tels que des capteurs, des actionneurs, et des équipements routiers

comme les RSU (Unités de Station Routière) pour collecter des informations pertinentes pour la prise de décision.

2. **Couche de coordination** : Assure l'interopérabilité, le routage et la sécurité des messages, garantissant une communication efficace entre les différents composants du système.
3. **Couche d'intelligence artificielle** : Au cœur du système, elle exécute les tâches de décision en se concentrant sur l'analyse de Big Data, l'exploration de données, le cloud computing et la prise de décision basée sur des systèmes experts.
4. **Couche d'application** : Concerne les services disponibles dans le système et répond aux exigences spécifiques des utilisateurs.
5. **Couche business** : Décrit les différents modèles d'affaires que le marché de l'IoV proposera, incluant les services et les opportunités économiques [18].



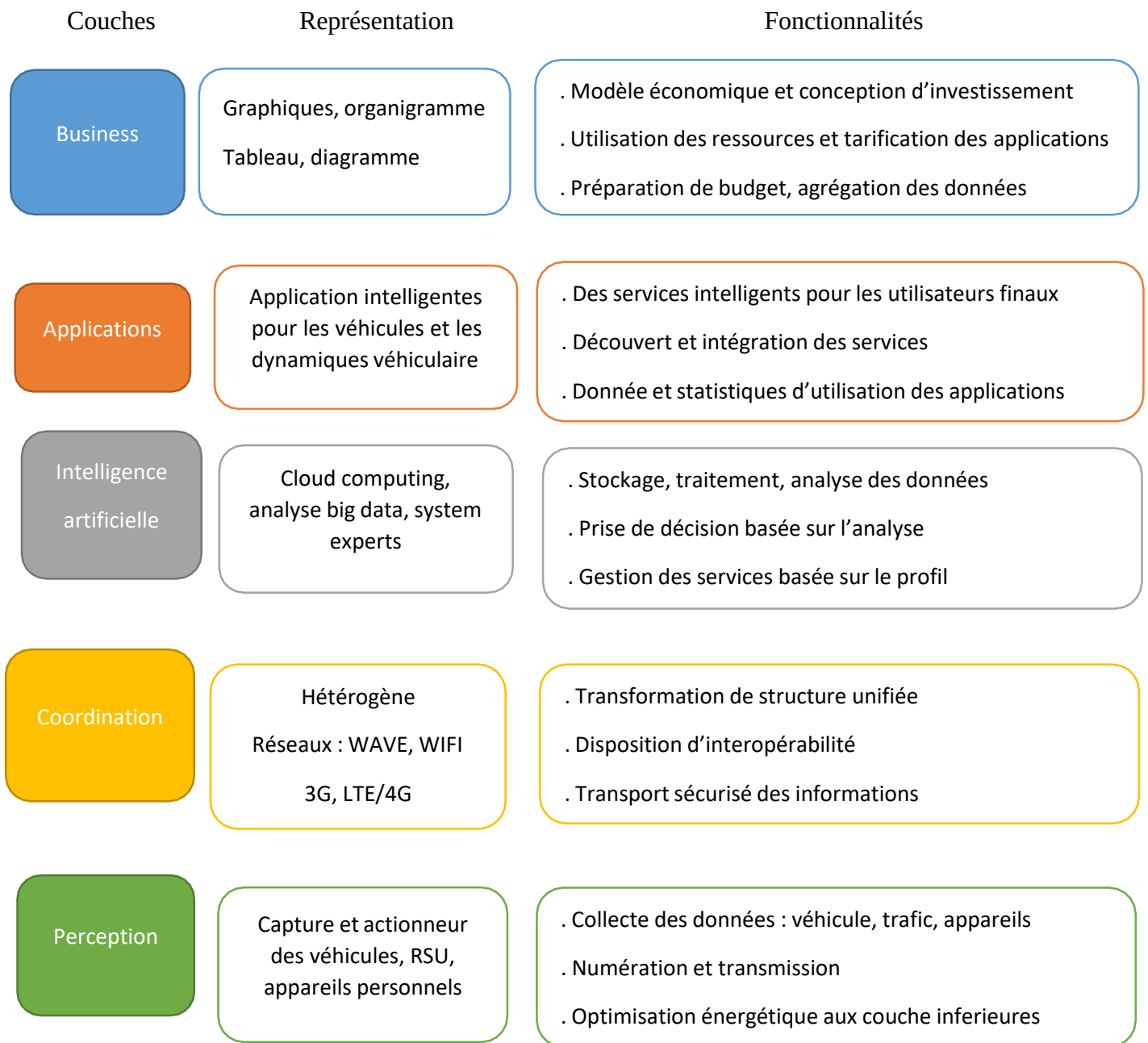


Figure 4 : architecture de l'IOV sur 5 couches

#### 5.4- L'architecture en 07 couches :

L'architecture en sept couches de l'Internet des véhicules (IoV) :

- ✓ **Interface utilisateur** : Gère les interactions entre le conducteur et le véhicule, incluant les éléments visuels et les dispositifs de commande comme le tableau de bord, les commandes vocales et les écrans tactiles.
- ✓ **Acquisition de données** : Collecte des données à partir de diverses sources à l'intérieur et autour du véhicule, telles que les capteurs embarqués, les caméras, les radars, les lidars, les GPS, et les Unités de Station Routière (RSU).
- ✓ **Filtrage et prétraitement** : Filtre et prétraite les données collectées pour éliminer le bruit, corriger les erreurs et réduire la dimensionnalité, garantissant ainsi que seules les données pertinentes et de haute qualité sont transmises aux couches supérieures.
- ✓ **Communication** : Gère la transmission des données entre les différents composants du système IoV, utilisant des technologies de communication sans fil comme le Wi-Fi, la 4G/5G et le Bluetooth.
- ✓ **Contrôle et gestion** : Assure le contrôle et la gestion des opérations du système IoV, incluant la gestion des ressources, la planification des tâches, la gestion de la qualité de service (QoS), ainsi que la supervision et la maintenance des composants.
- ✓ **Traitement** : Analyse et traite les données prétraitées pour extraire des informations significatives, utilisant des analyses statistiques, des algorithmes d'apprentissage automatique et des modèles prédictifs pour prendre des décisions intelligentes et fournir des services personnalisés.
- ✓ **Sécurité** : Comprend des mécanismes de sécurité pour protéger les données et les communications contre les menaces telles que le piratage, la falsification et le vol d'identité. Elle englobe également la gestion des accès, le chiffrement des données et l'authentification des utilisateurs [19].

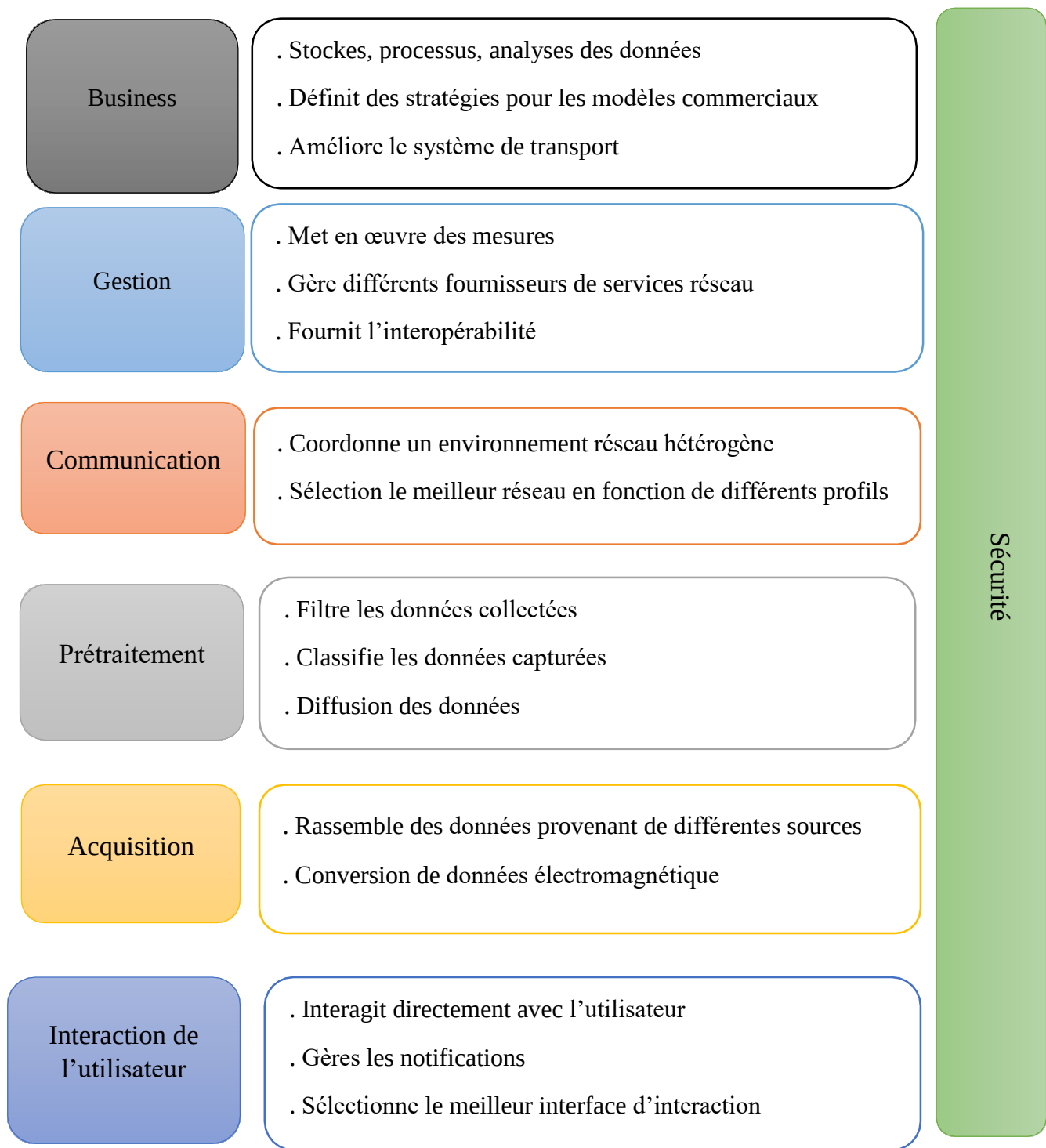


Figure 5 : l'architecture de l'IOV sur 07 couches

## **6- Les technologies de communication de l'IOV**

### **I. Bluetooth :**

Est une technologie largement employée pour établir des réseaux personnels (PAN) et peut également être exploitée pour prendre en charge les applications V2V et V2I, par rapport à d'autres applications. Cependant, ses capacités ne la rendent pas adaptée aux applications de sécurité des bâtiments en raison de sa vitesse de transmission relativement lente, de sa portée limitée et de sa sensibilité aux interférences atmosphériques [20].

### **II. Wifi :**

Est un protocole de communication sans fil utilisé pour les réseaux locaux, basé sur la norme IEEE 802.11. Il fonctionne sur une fréquence radio libre de 2,4 GHz et permet des vitesses de transmission de données élevées pouvant atteindre 150 Mbps [21].

### **III. DSRC :**

Le système de communication radio bidirectionnelle à courte portée appelé « Dedicated Short Range Communication » a été spécialement développé pour les systèmes de transport intelligents, en particulier pour la communication entre véhicules dans un réseau VANET. Les voitures munies d'une unité embarquée (OBU) font appel à la DSRC afin de communiquer des données et des informations avec d'autres voitures. Le concept de DSRC inclut également tous les protocoles et normes liés à ce genre de communication [22].

### **IV. ZigBee :**

La bande sans licence de 2,4 GHz permet de transmettre des données à une vitesse de 250 kbps, avec une portée de 70 mètres. En outre, il utilise les bandes de fréquences inférieures de 915 MHz afin de faire face à des débits de transfert de 40 kbps. De plus, cette technologie est réputée pour sa consommation d'énergie relativement faible en communication [23].

### **V. WIMAX :**

Qui signifie Interopérabilité Mondiale pour les Micro-ondes Access, est un système de communication sans fil couramment employé pour accéder à Internet à haut débit dans de vastes zones géographiques. Il est aussi vendu sous forme de label, à l'instar du Wifi, en raison de sa catégorisation parmi les technologies de nouvelle génération [24].

### **VI. MBWA :**

Le Mobile Broadband Wireless Access est une norme IEEE 802.20 qui définit cela. Son objectif est de permettre l'accès à Internet sans fil aux appareils extrêmement mobiles. Cette technologie offre la possibilité de se déplacer à des vitesses de véhicule allant jusqu'à 250 km/h. En outre, elle garantit une connexion fluide et rapide grâce à des transferts manuels fluides [25].

#### **VII. LTE (4G/5G) :**

Ou Long-Term Evolution, c'est une norme de réseau sans fil avancé. La norme HSPA+ est utilisée dans les réseaux les plus récents, qu'ils soient de quatrième ou cinquième génération (4G/5G) [26].

#### **VIII. Microwave :**

Les faisceaux d'ondes radio à haute fréquence sont utilisés dans la technologie de communication sans fil pour établir des connexions sans fil à haut débit. Son utilisation facilite l'échange et la réception d'informations vocales, vidéo et de données. Cette norme fonctionne à une fréquence de 0,3 GHz à 300 GHz et peut transmettre des données à une vitesse de 16 Gbps sur de grandes distances [27].

### **7- Conclusion**

L'IoV se positionne comme une pierre angulaire des futures infrastructures de transport intelligentes. À travers ses différentes architectures et technologies de communication, l'IoV favorise l'émergence d'un écosystème interconnecté, permettant aux véhicules de s'adapter en temps réel à leur environnement et d'échanger des données de manière fluide et sécurisée. Les domaines d'application, tels que la gestion du trafic, la sécurité routière et l'efficacité énergétique, illustrent le potentiel de transformation qu'apporte cette innovation technologique. Toutefois, pour exploiter pleinement ses avantages, des défis subsistent, notamment en termes de sécurité des données, de confidentialité, et d'interopérabilité des systèmes. Le développement et l'adoption croissante de l'IoV ouvriront la voie à une mobilité plus sûre, durable et efficace, tout en remodelant le paysage des transports urbains et interurbains.

Dans le chapitre suivant, nous aborderons les algorithmes de sélection de réseau, essentiels pour optimiser les communications au sein de l'IoV. Ces algorithmes jouent un rôle clé dans le choix du réseau le plus adapté à chaque situation, garantissant ainsi des

performances optimales en matière de transmission de données et de connectivité entre véhicules.

## **Chapitre 02 : les algorithmes de sélection de réseau**

### **1- Introduction**

Dans le cadre de l'Internet des Véhicules (IoV), plusieurs types d'algorithmes sont utilisés pour sélectionner le réseau le plus adapté, chacun présentant des avantages et des limitations spécifiques. Le choix optimal de l'algorithme dépend des caractéristiques du réseau en question, ainsi que des objectifs de performance recherchés, tels que la qualité de service, la latence ou la fiabilité des communications.

Ce chapitre propose d'examiner les algorithmes de sélection de réseau dans le contexte de l'IoV. Nous commencerons par une présentation des principaux algorithmes existants, suivie d'une comparaison de leurs forces et faiblesses. Ensuite, nous introduirons l'algorithme que nous avons développé, en mettant en avant ses spécificités et avantages. Enfin, le chapitre se terminera par une conclusion.

### **2- Les algorithmes de sélection de réseau :**

L'apparition des réseaux hétérogènes a donné lieu à la conception de divers algorithmes de choix de réseaux. Ces algorithmes ont été développés en prenant en compte différents points de départ et objectifs d'optimisation, tels que maximiser le débit des utilisateurs, équilibrer la charge entre les réseaux, améliorer l'utilisation des ressources et réduire le taux de blocage, les coûts de communication et la consommation de ressources. Globalement, les algorithmes de sélection de réseau peuvent être répartis dans les catégories suivantes :

#### **2.1- Algorithmes basés sur la force du signal reçu (RSS) :**

Dans une certaine mesure, le RSS peut caractériser la qualité du signal sans fil, jetant ainsi les bases de la sélection du réseau. Ensuite, le terminal collecte les RSS des réseaux sans fil, compare les qualités de liaison entre eux et choisit celui ayant la meilleure qualité de liaison. Tucker et Alizadeh fixent un seuil minimal pour le RSS de chaque réseau sans fil,

de sorte que le terminal mobile puisse choisir le réseau optimal en comparant le RSS de chaque réseau avec ce seuil [29]. Lee et Kim. et Haider, Gondal et Kamruzzaman. ont amélioré les algorithmes basés sur le RSS pour résoudre l'effet ping-pong induit par les fluctuations du RSS [30], [31].

Les algorithmes basés sur le RSS prédisent principalement la tendance du RSS actuel, afin que le terminal connaisse à l'avance le réseau auquel il doit se connecter. Malgré leurs alternatives des réseaux simples, les algorithmes basés sur le RSS échouent souvent à faire le bon choix dans des conditions de couverture réseau complexes, car le RSS ne peut pas pleinement refléter la qualité des liaisons sans fil ni démontrer les performances globales du réseau.

### **2.2- Les algorithmes basés sur la théorie de la logique floue (FL) :**

L'intégration entre la théorie de la logique floue et les attributs de réseau pourrait améliorer efficacement la précision et l'efficacité de la sélection du réseau. Hou et O'Brien ont établi un ensemble flou pour chaque attribut de décision du réseau, défini une base de règles d'inférence floue pour le raisonnement, et évalué la performance du réseau par défuzzification [32]. Grâce à l'évaluation floue globale (FCE), Radhika et Reddy [33] et Wang et al. [34] ont déterminé l'appartenance relative de chaque attribut de décision, évalué la performance de chaque réseau candidat par sommation pondérée, et choisi le réseau idéal en se basant sur les résultats de l'évaluation.

La cartographie linéaire est utilisée par les algorithmes de sélection de réseau basés sur la FL pour mesurer les attributs et créer des ensembles flous, ce qui ne permet pas de décrire de manière objective les informations floues de l'utilisateur ou l'état du réseau. En outre, la grande charge de calcul empêche l'utilisation de ces algorithmes dans la sélection entre différents réseaux sans fil.

### **2.3- Les algorithmes basés sur la fonction d'utilité (UF) :**

Inspirés par la théorie de l'utilité en microéconomie, les algorithmes basés sur l'UF paramètrent chaque alternative avec une fonction d'utilité, construisent un modèle mathématique pour évaluer la performance de la sélection de réseau, et dérivent l'alternative d'allocation de ressources efficace en maximisant l'utilité de chaque réseau d'accès (le bénéfice de l'utilisateur après l'accès à chaque réseau). Chan et al. ont adopté la



fonction d'utilité logarithmique basée uniquement sur le RSS [35]. Stevens-Navarro et Wong ont conçu un algorithme basé sur l'UF en tenant compte de multiples attributs : bande passante, sécurité, prix et perte de puissance [36]. Wang et Binet ont développé un algorithme basé sur l'UF en prenant en compte la bande passante, le prix, le trafic, la tolérance aux pannes et la gigue [37]. Zhu et McNair ont présenté un algorithme basé sur l'UF, en considération de la bande passante, du délai et de la consommation d'énergie [38]. L'algorithme de sélection de réseau basé sur l'UF doit clarifier les attributs à considérer dans la prise de décision de réseau et décrire raisonnablement le bénéfice et le coût de chaque attribut. Il est à noter que la courbe d'utilité d'un attribut peut varier en fonction des types de service.

#### **2.4- Les algorithmes basés sur la théorie des jeux (GT) :**

La théorie des jeux est appropriée pour résoudre les problèmes de sélection de réseau dans les réseaux sans fil hétérogènes, car les utilisateurs de ces réseaux partagent les ressources sans fil, et différents réseaux sont en compétition pour les intérêts. Cesana et al, ont modélisé le problème de la sélection de réseau comme un jeu non coopératif, dans lequel chaque utilisateur formulait une stratégie de tarification en fonction du degré de congestion dans le réseau candidat, et sélectionnait l'accès réseau au moindre coût [39]. Niyato et Hossain et Chan et al ont modélisé le jeu entre utilisateurs comme un jeu évolutif, et ont réalisé le contrôle d'accès aux réseaux sans fil hétérogènes [40], [35].

Les algorithmes basés sur la théorie des jeux sont trop complexes pour contrôler efficacement l'accès aux réseaux sans fil hétérogènes. De plus, ces algorithmes nécessitent de définir clairement le modèle de jeu et la méthode d'équilibre avant de contrôler l'accès au réseau.

#### **2.5- Les algorithmes basés sur la prise de décision multicritère (MADM) :**

La prise de décision multicritère (MADM) est une méthode de prise de décision qui prépare un nombre limité d'alternatives à l'avance pour plusieurs attributs qui ne peuvent pas être partagés ou substitués les uns aux autres, et choisit la meilleure alternative parmi celles préparées [41]. Lors du MADM, le décideur fait une évaluation globale de chaque

alternative par une certaine méthode, selon la matrice de jugement et les poids des attributs [42].

Dans les réseaux hétérogènes, il existe certaines différences en termes de bande passante, taux de perte de paquets et délai. Ces facteurs doivent être considérés de manière globale lors de la sélection de l'accès réseau. Il est évident que le MADM est applicable à la sélection de réseau dans les réseaux hétérogènes.

## **2.6- Algorithme de sélection de réseaux basée sur la QoS :**

Un algorithme de sélection de réseaux basé sur la QoS (Qualité de Service) évalue différents réseaux disponibles en fonction de critères tels que la bande passante, le taux de perte de paquets, le délai et la fiabilité. Voici un aperçu des étapes typiques de cet algorithme :

1. **Collecte des données** : Rassembler des informations sur les performances des réseaux disponibles.
2. **Évaluation des critères QoS** : Analyser chaque réseau en fonction des critères QoS définis.
3. **Pondération des critères** : Attribuer des poids aux différents critères en fonction de leur importance relative.
4. **Calcul des scores** : Utiliser une méthode de décision multicritère pour calculer un score global pour chaque réseau.
5. **Sélection du réseau optimal** : Choisir le réseau avec le score le plus élevé [43].

### 3- Comparaison entre les algorithmes

| Algo.        | Avantages                                                                                                                                                                                                                                                                                                                                          | Inconvénients                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Basé sur RSS | <ul style="list-style-type: none"> <li>• <b>Simplicité</b> : Facile à implémenter et à comprendre.</li> <li>• <b>Paramètre Unique</b> : Utilise une mesure directe du signal pour évaluer la qualité du réseau, ce qui rend l'évaluation immédiate et simple.</li> </ul>                                                                           | <ul style="list-style-type: none"> <li>• <b>Paramètre Unilatéral</b> : Ne prend en compte que la puissance du signal reçus sans considérer d'autres aspects importants du réseau comme la bande passante ou la latence.</li> <li>• <b>Sensibilité aux Interférences</b> : Peut être affecté par les interférences et les obstacles physiques, ce qui peut entraîner des évaluations incorrectes de la qualité du réseau.</li> </ul> |
| Basé sur FL  | <ul style="list-style-type: none"> <li>• <b>Flexibilité</b> : Ne nécessite pas de modèle mathématique exact et peut traiter des informations imprécises ou vagues.</li> <li>• <b>Adaptabilité</b> : Peut s'ajuster aux variations du réseau et aux incertitudes en utilisant des règles floues.</li> </ul>                                         | <ul style="list-style-type: none"> <li>• <b>Précision Limitée</b> : Les états du réseau peuvent être mal décrits après traitement flou, ce qui peut entraîner des décisions moins précises.</li> <li>• <b>Complexité de la Modélisation</b> : La création de règles floues et la définition des fonctions d'appartenance peuvent être complexes.</li> </ul>                                                                         |
| Basé sur UF  | <ul style="list-style-type: none"> <li>• <b>Optimisation de l'Utilité</b> : Maximise l'utilité globale du réseau en prenant en compte différents attributs pour une évaluation complète.</li> <li>• <b>Approche Quantitative</b> : Permet de comparer de manière quantitative les différents réseaux en fonction de plusieurs critères.</li> </ul> | <ul style="list-style-type: none"> <li>• <b>Incertitude des Attributs</b> : Les valeurs d'utilité et les coûts des attributs peuvent être incertains ou subjectifs, ce qui peut affecter la précision des décisions.</li> <li>• <b>Complexité d'Évaluation</b> : Peut nécessiter des ajustements fréquents des fonctions d'utilité pour refléter correctement les conditions du réseau.</li> </ul>                                  |

|               |                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Basé sur GT   | <ul style="list-style-type: none"> <li>• <b>Performance Améliorée</b> : Utilise des concepts de la théorie des graphes pour évaluer les réseaux, ce qui peut améliorer la performance globale en tenant compte des connexions et des chemins.</li> <li>• <b>Analyse Structurée</b> : Permet une analyse structurée des réseaux en modélisant les relations entre les nœuds.</li> </ul> | <ul style="list-style-type: none"> <li>• <b>Complexité Élevée</b> : La modélisation et l'analyse basées sur la théorie des graphes peuvent être très complexes et exigeantes en termes de calcul.</li> <li>• <b>Efficacité</b> : Peut souffrir d'une faible efficacité en raison du temps de calcul élevé nécessaire pour résoudre les problèmes complexes de graphes.</li> </ul>                 |
| Basé sur MADM | <ul style="list-style-type: none"> <li>• <b>Évaluation Globale</b> : Prend en compte plusieurs attributs du réseau de manière globale, offrant une évaluation complète.</li> <li>• <b>Flexibilité</b> : Permet d'intégrer divers critères et de pondérer leur importance selon les besoins spécifiques.</li> </ul>                                                                     | <ul style="list-style-type: none"> <li>• <b>Complexité</b> : La gestion de multiples critères et la définition des pondérations peuvent rendre l'algorithme complexe à concevoir et à implémenter.</li> <li>• <b>Difficulté d'Interprétation</b> : Les résultats peuvent être difficiles à interpréter en raison de la combinaison de nombreux critères.</li> </ul>                               |
| Basé sur QoS  | <ul style="list-style-type: none"> <li>• <b>Expérience Utilisateur</b> : Assure une qualité de service élevée en évaluant des aspects comme la bande passante, la latence et la fiabilité du réseau.</li> <li>• <b>Adaptation Dynamique</b> : Permet des ajustements en temps réel pour maintenir une bonne qualité de service.</li> </ul>                                             | <ul style="list-style-type: none"> <li>• <b>Ressources</b> : Peut nécessiter une grande quantité de ressources de calcul et de stockage pour surveiller et évaluer en continu les paramètres de qualité.</li> <li>• <b>Complexité de Mise en Œuvre</b> : La mise en œuvre peut être complexe en raison de la nécessité de mesurer et de gérer divers aspects de la qualité du service.</li> </ul> |

Tableau 1 : Les avantages et les inconvénients de différents algorithmes.

#### **4- Conclusion :**

La sélection de réseau dans l'Internet des Véhicules (IoV) repose sur une diversité d'algorithmes, chacun adapté à des contextes et objectifs spécifiques. Après avoir exploré et comparé les différentes approches, nous avons mis en avant notre algorithme proposé, qui présente des avantages en termes de performance et de pertinence dans certaines situations. Cette analyse nous permet de mieux comprendre les critères à considérer pour une sélection de réseau optimale dans l'IoV.

Dans le chapitre suivant, nous détaillerons les différentes étapes de conception et d'implémentation de cet algorithme proposé, en exposant les choix techniques et méthodologiques qui ont guidé son développement.

## Chapitre 03 : Conception et Implémentation

### 1- Introduction

Dans ce chapitre, nous commencerons par présenter le modèle de simulation utilisé pour notre étude. Nous analyserons ensuite l'organigramme d'exécution ainsi que le diagramme de séquence de l'algorithme proposé. Par la suite, nous décrirons la mise en œuvre, en commençant par une exploration de l'environnement OMNeT++, qui a servi de base pour nos simulations. Nous passerons ensuite en revue les principaux paramètres de simulation à travers un tableau détaillé. Enfin, nous illustrerons nos résultats à l'aide de captures d'écran et d'interfaces graphiques issues de la simulation. Le chapitre se terminera par une conclusion synthétisant les points clés abordés.

### 2- Conception et modélisation

#### 2.1 Algorithme proposée :

Notre algorithme proposé est basé sur QoS pour la sélection du meilleur réseau

##### i. Définition des informations de chaque nœud :

- **Capacité réseau** : représente le nombre maximal de nœuds connectés simultanément.
- **Nombre de nœuds connectés** : le nombre de nœuds connectés à chaque point d'accès.
- **Sécurité** : représente le niveau de sécurité de chaque nœud.
- **Énergie** : représente le niveau d'énergie de chaque nœud.
- **Distance** : représente la distance entre le nœud principal et les autres nœuds.

##### ii. Calcule le Best pour chaque réseau :

$$\text{Score} = (w_{\text{capacité}} * (\text{capacité} - \text{nb\_noeuds\_connectés})) + (w_{\text{sécurité}} * \text{sécurité}) + (w_{\text{énergie}} * \text{énergie}) - (w_{\text{distance}} * \text{distance})$$

**iii. Sélection le meilleur réseau :**

Meilleur\_réseau = max(Score) ;

**iv. L'algorithme proposé :**

```
/* Fonction principale */
```

```
Début
```

```
nœud_initiateur = collecter_informations_noeuds() ; Si nœud_initiateur est
```

```
vrai alors {
```

```
liste_PA = liste_points_accès_disponibles() ;  $\forall PA_i \in$  liste_PA faire {
```

```
envoyer_demande_info(nœud_initiateur,  $PA_i$ ) ; réponse[ $PA_i$ ] =
```

```
recevoir_réponse( $PA_i$ );}
```

```
Meilleur_réseau = sélectionner_meilleur_reseau(réponse) ;
```

```
}
```

```
/* Fonction pour calculer la valeur de chaque réseau */
```

```
fonction calculer_score( $PA_i$ ) {
```

```
capacité =  $PA_i$ .capacité_reseau ;
```

```
nb_noeuds_connectés =  $PA_i$ .nb_noeuds_connectés ;
```

```
sécurité =  $PA_i$ .sécurité ;
```

```
énergie =  $PA_i$ .énergie ;
```

```
distance =  $PA_i$ .distance ;
```

```
/* Pondération des paramètres pour le calcul du score */
```

```
w_capacité = p1 ;
```

```
w_sécurité = p2 ;
```

```
w_énergie = p3 ;
```

```
w_distance = p4 ;
```

```
Score = (w_capacité * (capacité - nb_noeuds_connectés)) +
```

```
(w_sécurité * sécurité) + (w_énergie * énergie) - (w_distance * distance) ;
```

```
Retourner Score ;
```

```
}
```

```
/* Fonction pour sélectionner le meilleur réseau */
```

```
fonction sélectionner_meilleur_reseau(réponses) {
```

```
meilleurs_scores = {}
```

```
∀ PAi ∈ réponses faire{
```

```
score = calculer_score(PAi) ;
```

```
meilleurs_scores[PAi] = score
```

```
}
```

```
}
```

```
Meilleur_reseau = max(meilleurs_scores) ;
```

```
Retourner Meilleur_reseau ;
```



Dans l'algorithme que nous proposons ci-dessus, la sécurité est l'un des critères importants à prendre en compte pour évaluer un point d'accès (PA). Calculer la valeur de la sécurité peut se faire en fonction de plusieurs paramètres liés à la sécurité du réseau.

Le calcul de la valeur de la sécurité dans cet algorithme est basé sur :

1. **Utilisation de niveaux de chiffrement** : Un point d'accès pourrait utiliser différents types de protocoles de sécurité, tels que WPA3, WPA2, WPA, ou être non sécurisé (Open Network). *Dans ce cas, on peut attribuer une note de sécurité basée sur le type de chiffrement du réseau comme suit :*

- WPA3 : 5 (meilleure sécurité)
- WPA2 : 4 (bonne sécurité)
- WPA : 3 (sécurité moyenne)
- WEP : 2 (sécurité faible)
- Open : 1 (aucune sécurité)

Par exemple : Si un réseau utilise WPA3, la valeur de sécurité pour ce réseau sera 5.

2. **Certificats et authentification** : Certains réseaux sécurisés utilisent des certificats numériques pour authentifier les utilisateurs ou les appareils. Si un point d'accès utilise une authentification basée sur des certificats, il peut recevoir une note de sécurité élevée, comme suit :

- Authentification par certificats (EAP-TLS, etc.) : 5
- Authentification par mot de passe (WPA2-PSK) : 3

- Authentification simple ou nulle : 1

Par exemple : Si un réseau utilise des certificats pour l'authentification, il peut obtenir une valeur de 5 pour la sécurité.

3. **Détection d'intrusions et systèmes de surveillance** : points d'accès peuvent avoir des systèmes de détection d'intrusions ou des mécanismes pour surveiller et bloquer les attaques potentielles (comme le firewall, IDS, IPS). Si un PA dispose de tels mécanismes de sécurité, on peut attribuer des points supplémentaires :

- PA avec IDS/IPS activé : +2.
- PA sans système de détection d'intrusion : +0.

Par exemple : Un réseau avec un IDS et un pare-feu activé pourrait obtenir 2 points supplémentaires sur l'échelle de sécurité.

4. **Historique de vulnérabilité** : Si le réseau ou l'infrastructure associée a un historique de vulnérabilités ou de failles de sécurité, cela devrait être pris en compte pour réduire la valeur de sécurité. On pourrait soustraire des points si des vulnérabilités connues sont présentes :

- Aucune vulnérabilité détectée : +0
- Une vulnérabilité connue : -2

Par exemple : Si un PA utilise un équipement ou un protocole avec des failles de sécurité connues, sa note de sécurité pourrait être réduite de 2 points.

5. **Mise à jour des systèmes** : La fréquence des mises à jour de sécurité est cruciale pour déterminer la robustesse d'un point d'accès. Si un PA est régulièrement mis à jour (dernier patch appliqué récemment), il peut obtenir une meilleure note.

- Dernière mise à jour < 1 mois : +2
- Dernière mise à jour < 6 mois : +1
- Pas de mise à jour depuis > 6 mois : 0

Par exemple : Si un réseau a été mis à jour récemment (dans le mois dernier), il obtiendrait un bonus de 2 points pour la sécurité.

En combinant ces critères, la valeur de sécurité pour chaque point d'accès peut être calculée en utilisant une somme pondérée des différents aspects de sécurité (eq1).

$$\begin{aligned} \text{Sécurité} = & (\text{Poids\_chiffrement} * \text{Valeur\_chiffrement}) + \\ & (\text{Poids\_authentification} * \text{Valeur\_authentification}) + (\text{Poids\_surveillance} * \\ & \text{Valeur\_surveillance}) + (\text{Poids\_mise\_à\_jour} * \text{Valeur\_mise\_à\_jour}) - \\ & (\text{Poids\_vulnérabilité} * \text{Valeur\_vulnérabilité}) \quad (\text{eq1}) \end{aligned}$$

**Note:** Les poids peuvent être ajustés en fonction des priorités du système :

- Si la sécurité est cruciale (ex. dans des zones sensibles), les poids des paramètres comme le chiffrement et l'authentification peuvent être augmentés.
- Dans d'autres contextes, les systèmes de surveillance ou la gestion des mises à jour peuvent être prioritaires.

Exemple de calcul : soit un point d'accès avec les caractéristiques suivantes :

- Chiffrement WPA3 : Valeur = 5
- Authentification par certificats : Valeur = 5
- Surveillance IDS activé : Valeur = 2
- Dernière mise à jour il y a 2 mois : Valeur = 1
- Aucune vulnérabilité connue : Valeur = 0

Avec des poids égaux pour chaque critère (par exemple, tous à 1 pour simplifier), le calcul serait :

$$\text{Sécurité} = (1 * 5) + (1 * 5) + (1 * 2) + (1 * 1) - (1 * 0) \text{ Sécurité} = 13.$$

Ainsi, la valeur de sécurité dans l'algorithme reflétera une combinaison de plusieurs paramètres de sécurité critiques, assurant que les points d'accès les plus sécurisés soient privilégiés dans la sélection du meilleur réseau

#### **Les avantages de la solution proposée :**

L'intégration de la sécurité dans l'algorithme de sélection du meilleur réseau dans un environnement d'Internet des véhicules (IoV) offre plusieurs avantages importants. Ces avantages se traduisent par une meilleure protection des données, une fiabilité accrue du système, et une meilleure expérience utilisateur globale. Voici les principaux avantages :

| Concept | Avantage | Impact |
|---------|----------|--------|
|---------|----------|--------|

|                                          |                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                           |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Protection contre les attaques réseau    | En tenant compte de la sécurité dans la sélection des réseaux, les véhicules peuvent éviter de se connecter à des points d'accès vulnérables ou compromis. Cela réduit le risque de cyberattaques comme les attaques de type homme-du-milieu, le piratage, ou l'écoute clandestine. | Cela protège les données sensibles échangées entre le véhicule et l'infrastructure (V2I), ou entre véhicules (V2V), comme les informations de localisation, les messages d'alerte ou de navigation, et autres informations critiques pour la conduite autonome.                                           |
| Prévention des fuites de données         | Un réseau sécurisé est crucial pour prévenir la fuite de données personnelles, comme les informations de localisation des utilisateurs, les données des capteurs embarqués, ou d'autres informations sensibles.                                                                     | En sélectionnant des réseaux avec des protocoles de chiffrement robustes (WPA3, par exemple) et des méthodes d'authentification fiables, on garantit que les données échangées sont protégées contre les interceptions non autorisées.                                                                    |
| Amélioration de la confiance utilisateur | Les utilisateurs auront davantage confiance dans le système IoV s'ils savent que les réseaux sélectionnés pour la connexion sont sécurisés. Cela favorise une adoption plus rapide des technologies IoV et des véhicules connectés.                                                 | La sécurité intégrée permet de renforcer la réputation du système, ce qui est particulièrement important pour les systèmes de transport publics, les services de livraison automatisés et les systèmes de véhicules autonomes, où la sécurité des données et des connexions est un facteur clé de succès. |

|                                                                   |                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                |
|-------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Protection des systèmes critiques des véhicules                   | Les véhicules modernes et autonomes sont équipés de systèmes critiques, comme les systèmes de freinage, de direction et de gestion des capteurs. Une connexion réseau non sécurisée pourrait potentiellement permettre à un attaquant de prendre le contrôle de certaines fonctionnalités critiques du véhicule.                               | En s'assurant que le réseau choisi est suffisamment sécurisé, on protège les systèmes vitaux du véhicule contre toute tentative de prise de contrôle malveillante, augmentant ainsi la sûreté des passagers et des autres usagers de la route. |
| Meilleure résilience face aux cybermenaces                        | En évaluant la sécurité avant la connexion, les véhicules peuvent adapter leur comportement pour éviter les réseaux potentiellement dangereux. Cela renforce la résilience du système global contre les cybermenaces émergentes et les attaques sur le réseau.                                                                                 | Cela assure que, même en cas de menaces ou de vulnérabilités découvertes dans certains réseaux, les véhicules peuvent éviter ces réseaux automatiquement et opérer en toute sécurité.                                                          |
| Réduction des coûts de maintenance liés aux incidents de sécurité | Les cyberattaques et les incidents de sécurité peuvent entraîner des coûts importants pour réparer les dommages, restaurer les données, ou corriger les failles. En intégrant la sécurité dès la phase de sélection du réseau, il est possible de réduire le nombre d'incidents de sécurité, et par conséquent de diminuer les coûts associés. | Moins de failles de sécurité se traduisent par des coûts de maintenance réduits et moins de temps d'arrêt pour réparer ou remettre à jour les systèmes.                                                                                        |

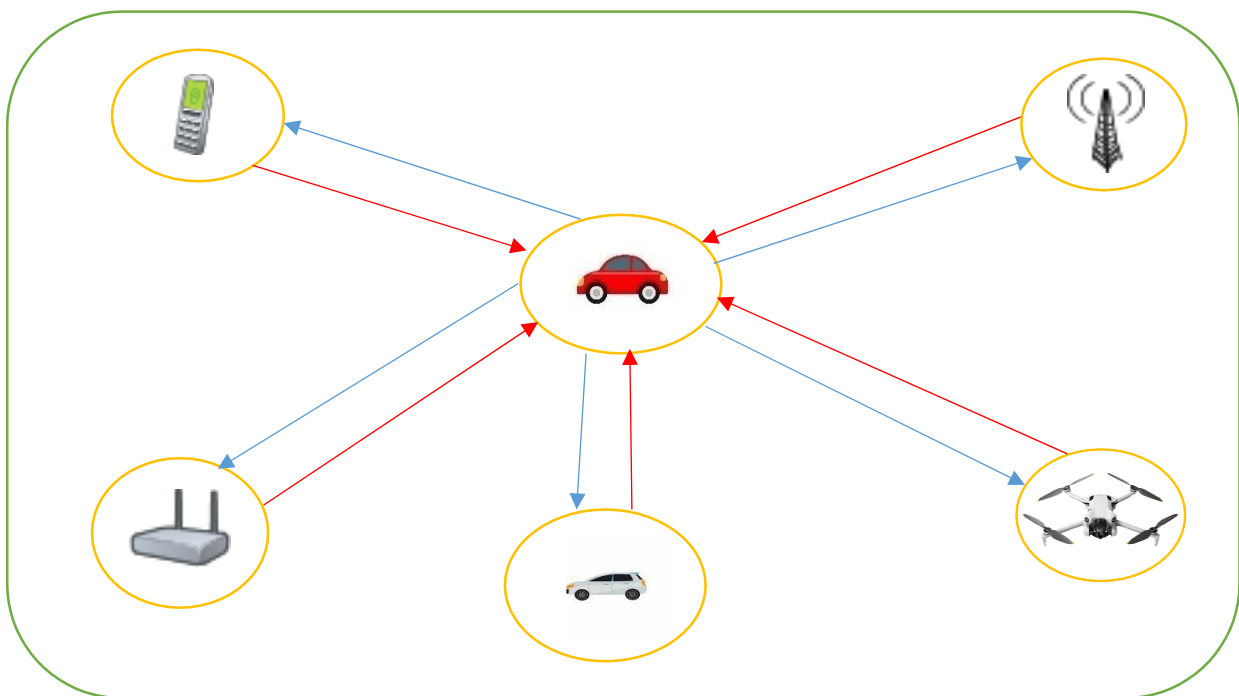
|                                      |                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                              |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Conformité aux réglementations       | De nombreux pays et industries imposent des normes de sécurité pour les véhicules connectés et autonomes. Intégrer la sécurité dans la sélection des réseaux aide à respecter ces réglementations, en garantissant que les véhicules se connectent uniquement à des réseaux conformes.                                       | En intégrant ces considérations de sécurité, les constructeurs et opérateurs IoV peuvent éviter des sanctions légales ou des pénalités pour non-respect des règles en matière de protection des données et de cybersécurité. |
| Stabilité et qualité de la connexion | Les réseaux sécurisés tendent à être mieux gérés et plus fiables. En privilégiant les points d'accès sécurisés, on peut s'attendre à des connexions plus stables et de meilleure qualité. Les réseaux non sécurisés sont plus susceptibles d'être perturbés ou compromis, ce qui pourrait affecter la qualité de service.    | Cela améliore la continuité du service dans les systèmes IoV, ce qui est crucial pour la gestion du trafic, les services d'urgence, et les communications critiques entre véhicules.                                         |
| Prévention des accès non autorisés   | En prenant en compte des mécanismes d'authentification robustes (par exemple, EAP-TLS avec certificats numériques), les véhicules se connectent uniquement à des réseaux où ils sont correctement authentifiés. Cela empêche les entités non autorisées de se connecter au réseau et de s'infiltrer dans les communications. | Les véhicules IoV pourront donc éviter les réseaux non sécurisés où un attaquant pourrait se faire passer pour un utilisateur légitime, limitant les risques d'infiltration.                                                 |

|                                         |                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                            |
|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Préparation pour des menaces émergentes | En intégrant un processus de sélection du réseau qui évalue la sécurité de manière dynamique (ex. : en prenant en compte les mises à jour régulières des réseaux et les vulnérabilités connues), le système est mieux préparé à s'adapter aux menaces émergentes. | Le véhicule peut continuellement éviter les points d'accès présentant des failles de sécurité ou des vulnérabilités récemment découvertes, garantissant ainsi un environnement plus sécurisé à long terme. |
|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

*Tableau 2: avantages de la solution proposée*

## 2.2- Modèle et système :

La simulation est représentée dans la figure ci-dessous : elle compose de deux véhicules, un point d'accès, une antenne, un phone personnel et drone. Lorsque le mouvement du véhicule envoie un message pour le recevoir des informations des nœuds et lorsque la réception des informations de chaque nœud, calcule le Score de chaque nœud et choisit le meilleur réseau.



 Demande information  
 Réception information



Véhicule



Véhicule2



Point d'accès



Drone



Antenne



Téléphone personnel

*Figure 6 : Le modèle de simulation*



### 2.3- Organigramme d'exécution :

Un organigramme est une représentation visuelle d'un algorithme, parmi les premières méthodes utilisées pour illustrer le flux des données dans un programme. Ce diagramme met en évidence non seulement les différentes étapes du traitement des données, mais aussi les opérations effectuées à chaque étape. Les étapes pour sa création incluent : définir l'objectif de l'organigramme, identifier les postes et fonctions, structurer les relations hiérarchiques.

Le diagramme ci-dessous illustre l'ensemble du processus d'exécution de notre algorithme.

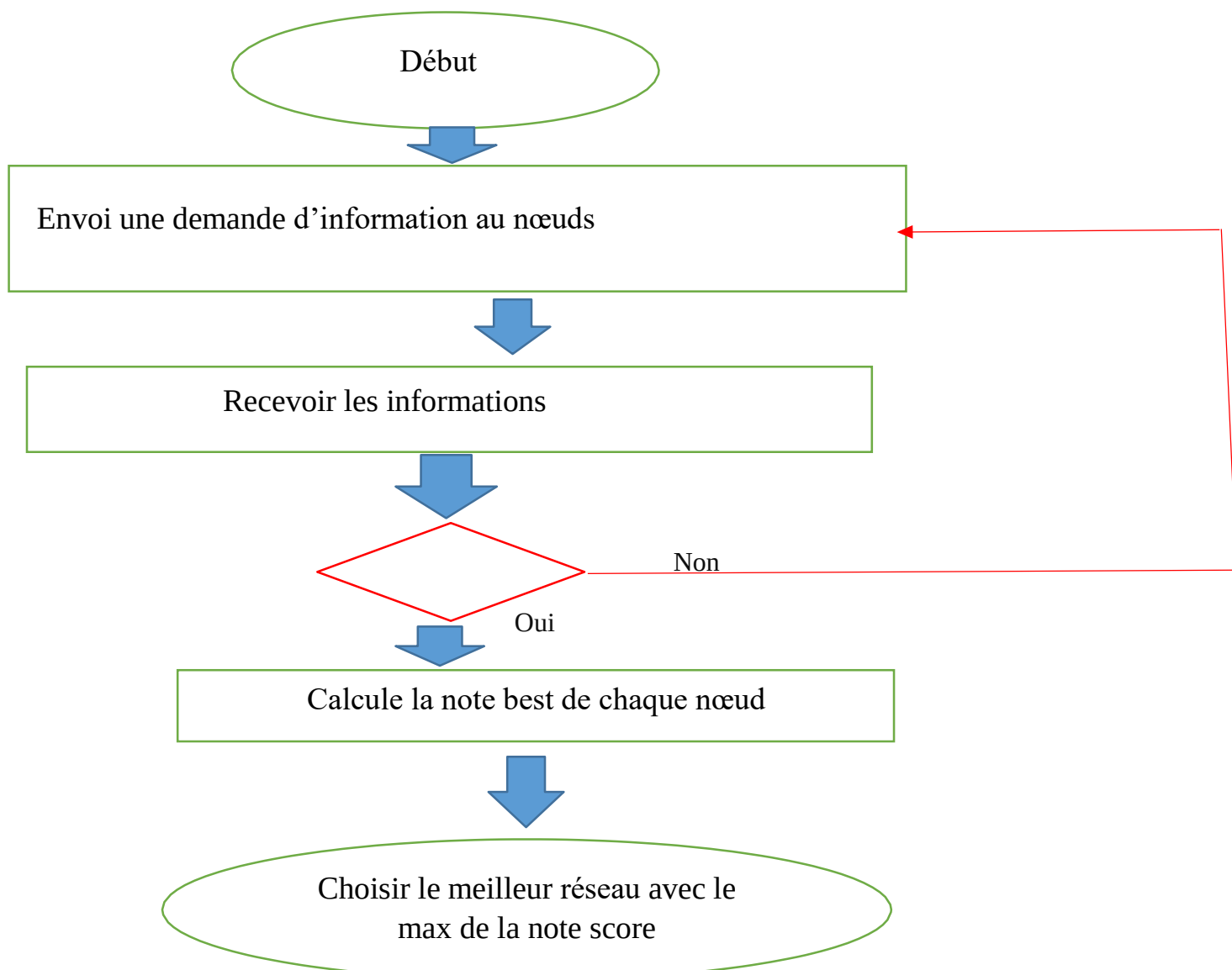


Figure 7 : organigramme de l'algorithme.

## 2.4- Diagramme de séquence

Un diagramme de séquence est un type de diagramme UML (Unified Modeling Language) qui illustre l'interaction des objets dans un processus en fonction de la chronologie. Il décrit l'ordre des interactions entre les différents composants d'un système pour accomplir une tâche donnée. Dans le cadre de mon algorithme de sélection de réseaux, ce diagramme de séquence permettrait de visualiser comment chaque élément du système collabore pour réaliser le processus de sélection, basé sur plusieurs critères.

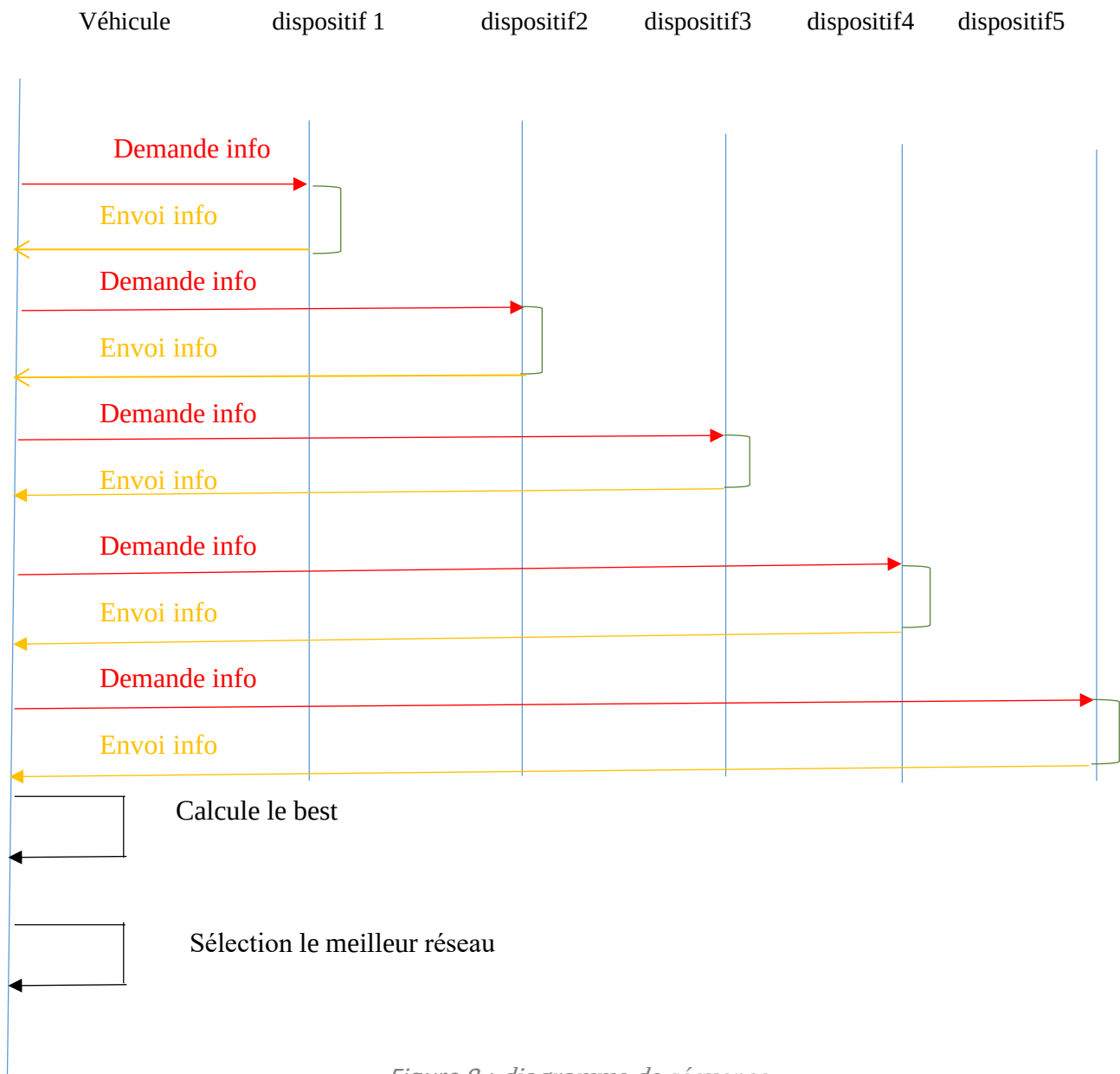


Figure 8 : diagramme de séquence

### **3- Implémentation**

#### **3-1 Omnet++ :**

##### **3.1.1 Présentation de la plateforme OMNet++**

OMNeT++ est un logiciel de simulation basé sur C++, orienté objet et à événements discrets. Il se caractérise par son caractère open source, avec un projet entamé en 1992. On utilise principalement cet environnement pour simuler des réseaux de communication, des systèmes multiprocesseurs et d'autres systèmes distribués.

OMNeT++ est largement utilisé dans différents domaines d'application grâce à son architecture modulaire, notamment dans la modélisation des protocoles de communication, la simulation de réseaux filaires et sans fil, la modélisation des systèmes distribués et la conception des architectures matérielles.

En général, OMNeT++ peut être utilisé pour modéliser tout système à événements discrets, où les entités communiquent par l'envoi de messages. Cet environnement offre des outils pour créer et configurer des modèles de réseaux à l'aide des fichiers NED et INI, exécuter les simulations, et analyser les résultats [44].

##### **3.1.2 Architecture de OMNET++ :**

L'architecture d'OMNeT++ repose sur un système modulaire, où les modules (ou composants) sont organisés de manière hiérarchique. Un module simple constitue l'unité de base, tandis qu'un module composé est un regroupement de modules simples, formant ainsi des structures plus complexes appelées modules composés. Cette hiérarchie peut être approfondie sans limitation, permettant la création de systèmes de simulation complexes, où les modules interagissent entre eux par l'échange de messages.

Les modules simples, qui constituent les feuilles de cette architecture, sont directement liés à des classes C++. Pour chaque module simple, il existe un fichier .cc et un fichier.h. La structure interne d'un module, incluant ses paramètres, sous-modules, et ports, est définie dans un fichier.ned.

Dans cette architecture, les modules simples agissent à la fois comme émetteurs et récepteurs de messages, tandis que les modules composés se chargent de relayer ces

messages de manière transparente. Les connexions entre modules peuvent être configurées avec différents paramètres tels que les délais de propagation, les débits de données, et les taux d'erreur.

La communication entre les modules s'effectue via des messages, qui peuvent représenter divers éléments, tels que des paquets ou des trames dans un réseau, des clients en file d'attente, ou toute autre entité nécessitant un service. Ces messages transitent à travers des ports, qui sont les interfaces d'entrée et de sortie de chaque module.

La conception d'un réseau s'effectue dans un fichier.ned, tandis que les paramètres spécifiques de chaque module sont définis dans un fichier.ini [44].

### 3.1.3 Les principaux fichiers d'OMNET++ :

**Fichier .Ned** : Dans OMNeT++, le fichier de description réseau (Network Descriptor File) utilise le langage NED (Network Description) pour définir la topologie d'un modèle. Ce langage permet de déclarer des modules simples, de les interconnecter, et de les organiser en modules composés. Le module composé à simuler est spécifié par le mot-clé network, qui indique au simulateur quel ensemble de modules doit être exécuté [44].

**Fichier .ini** : En étroite relation avec le fichier NED, ce fichier permet à l'utilisateur d'initialiser les paramètres des différents modules et de définir la topologie du réseau [28].

**Fichier .msg** : Les modules échangent des messages pour communiquer, et ceux-ci peuvent être définis dans un fichier .msg, où il est possible d'ajouter des champs de données[28].

**Fichier .ccp** : Fichier de code source en C++.

**Fichier .h** : Fichier d'en-tête, utilisé pour déclarer les classes et les fonctions.

### 3.1.4 Modèles

Au fil des ans, OMNeT++ a été enrichi par de nombreux modèles de simulation et cadres de modélisation créés par des chercheurs dans divers domaines. La plupart de ces cadres de modélisation sont open source et développés en tant que projets indépendants avec leurs propres cycles de publication [12].

### **3.1.4.1 INET Framework**

INET est une bibliothèque de modèles open source pour l'environnement de simulation OMNeT++. Elle offre une gamme variée de protocoles, d'agents et d'autres modèles, destinés aux chercheurs et étudiants travaillant sur les réseaux de communication. INET est particulièrement utile pour concevoir et valider de nouveaux protocoles, ainsi que pour explorer des scénarios innovants ou complexes.

INET comprend des modèles pour la pile de protocoles Internet (TCP, UDP, IPv4, IPv6, OSPF, BGP, etc.), des protocoles de couche de liaison pour réseaux filaires et sans fil (Ethernet, PPP, IEEE 802.11, etc.), la prise en charge de la mobilité, des protocoles MANET, DiffServ, MPLS avec signalisation LDP et RSVP-TE, ainsi que plusieurs modèles d'application et autres protocoles et composants.

De plus, plusieurs autres cadres de simulation utilisent INET comme base et l'étendent pour des applications spécifiques, telles que les réseaux véhiculaires, les réseaux superposés/peer-to-peer, ou encore LTE [44].

#### **3.1.4.1.1 Conçu pour l'expérimentation**

INET est basé sur un concept modulaire où les modules communiquent par l'envoi de messages. Les agents et les protocoles réseau sont représentés par des composants qui peuvent être librement combinés pour former des hôtes, des routeurs, des commutateurs, et autres dispositifs réseau. Les utilisateurs peuvent programmer de nouveaux composants, et les composants existants sont conçus pour être facilement compréhensibles et modifiables.

INET exploite pleinement l'infrastructure fournie par OMNeT++. En plus des services offerts par le noyau et la bibliothèque de simulation d'OMNeT++ (modèle de composants, paramétrisation, enregistrement des résultats, etc.), les modèles peuvent être développés, assemblés, paramétrés, exécutés, et leurs résultats évalués directement depuis l'IDE de simulation OMNeT++ ou via la ligne de commande [44].

### **3.2- Paramètre de simulation :**

Les paramètres de notre simulation sont présentés dans le tableau suivant :

| Paramètres         | Valeur           |
|--------------------|------------------|
| Position           | Aléatoire        |
| Nombre des nœuds   | 6                |
| Taille de réseau   | 640m*420m        |
| Modèle de mobilité | Vehicle Mobility |
| Vitesse            | 100 m/s          |

*Tableau 3: paramètres de simulation*

### 3.4- Scenario de simulation :

Dans cette section nous présentons l'exécution de notre application.

#### 3.4.1- Interface graphique de simulation :

Dans notre simulation a les composants suivants :

**Visualizer** : il permet de visualiser graphiquement les résultats de la simulation.

**RadioMeduim** : permet la modélisation des communications sans fil dans le réseau simulé.

**Véhicule** : le nœud principal qui recherche le meilleur réseau.

**Nœuds (drone, Point accès, Antenne, Car, telephone personal)** : les nœuds qui permetde communiqué avec ils sans fil.

**Cercle bleu** : la zone de couverture de chaque nœud

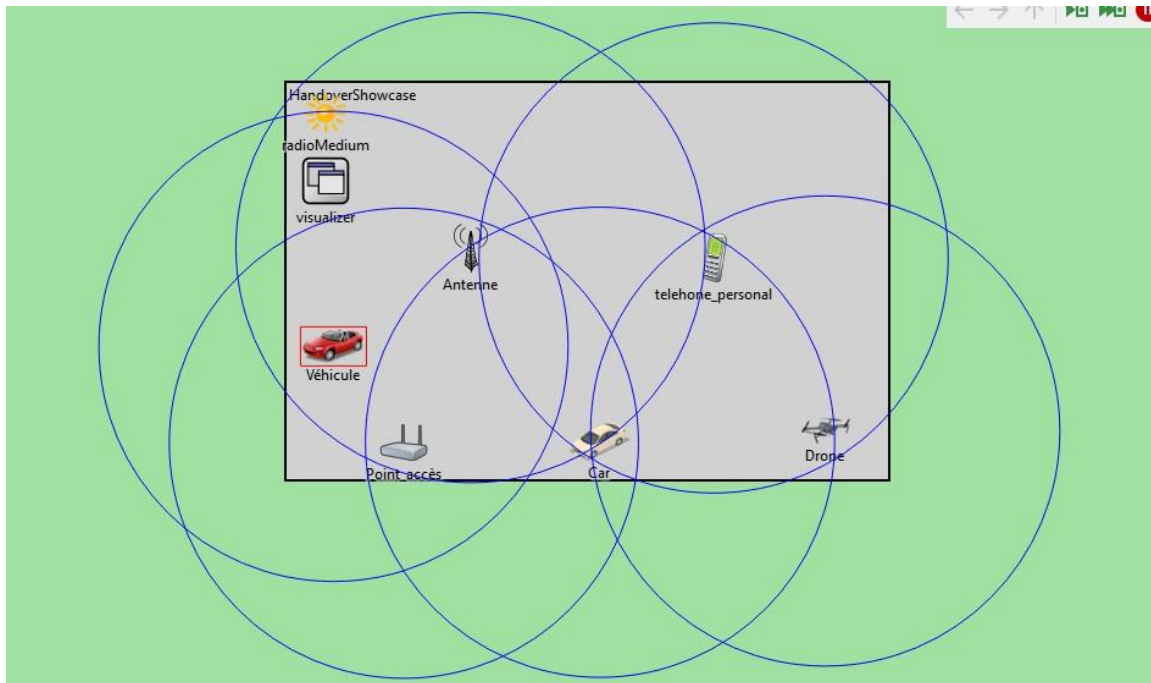


Figure 9 : interface graphique de simulation

### 3.5- Exécution de simulation :

L'exécution de simulation compose les étapes suivantes :

#### 3.5.1- Etape 01 :

Le nœud véhicule envoie un message de demande des informations aux autres nœuds.

```
void Vehicle::initialize(int stage) {
    ApplicationBase::initialize(stage);
    if (stage == inet::INITSTAGE_APPLICATION_LAYER) {
        scheduleAt(simTime(), &sendMsgEvent);
    }
}

void Vehicle::demandinfo() {
    // envoi un msg pour obtenir les information de chaque noeuds
    auto packet = new inet::Packet("Donné vous information");
    send(packet, "udpOut");
    scheduleAt(simTime() + 1, &sendMsgEvent);
}
```

Figure 10 : envoi de message par véhicule aux nœuds

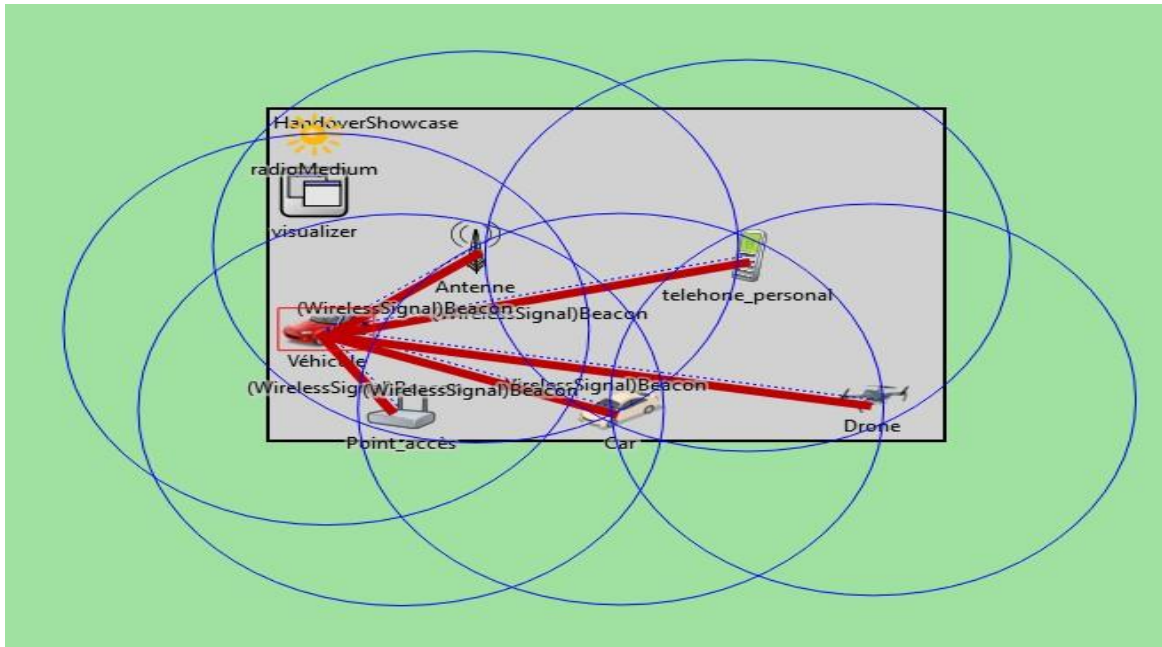


Figure 11 : le signal du message envoi par le véhicule à les nœuds

### 3.5.2- Etape 02 :

Les nœuds envois leur information au véhicule et signal d'active aux autres nœuds

```
void Nodes::handleMessageWhenUp(cMessage *msg) {
    if (msg->arrivedOn("udpIn")) {
        sendResponse();
    }
}
```

Figure 12 : confirmation de recevoir de message de véhicule pour envoi les informations

```
void Nodes::envoiiinformation() {
    // Envoi les information
    auto packet = new inet::Packet("Les information");
    auto payload = inet::makeShared<inet::FieldsChunk>();
    payload->addField("name", inet::Chunk::FieldInfo::TYPE_STRING)->setValue(inet::makeShared<inet::ByteCountChunk>(name));
    payload->addField("capacite_reseau", inet::Chunk::FieldInfo::TYPE_INTEGER)->setValue(inet::makeShared<inet::ByteCountChunk>(capacite_reseau));
    payload->addField("nb_noeuds_connecte", inet::Chunk::FieldInfo::TYPE_INTEGER)->setValue(inet::makeShared<inet::ByteCountChunk>(nb_noeuds_connecte));
    payload->addField("securite", inet::Chunk::FieldInfo::TYPE_INTEGER)->setValue(inet::makeShared<inet::ByteCountChunk>(securite));
    payload->addField("energie", inet::Chunk::FieldInfo::TYPE_INTEGER)->setValue(inet::makeShared<inet::ByteCountChunk>(energie));
    payload->addField("x", inet::Chunk::FieldInfo::TYPE_DOUBLE)->setValue(inet::makeShared<inet::ByteCountChunk>(getX()));
    payload->addField("y", inet::Chunk::FieldInfo::TYPE_DOUBLE)->setValue(inet::makeShared<inet::ByteCountChunk>(getY()));
    packet->insertAtBack(payload);

    send(packet, "udpOut");
}
```

Figure 13 : envoi les informations des nœuds au véhicule



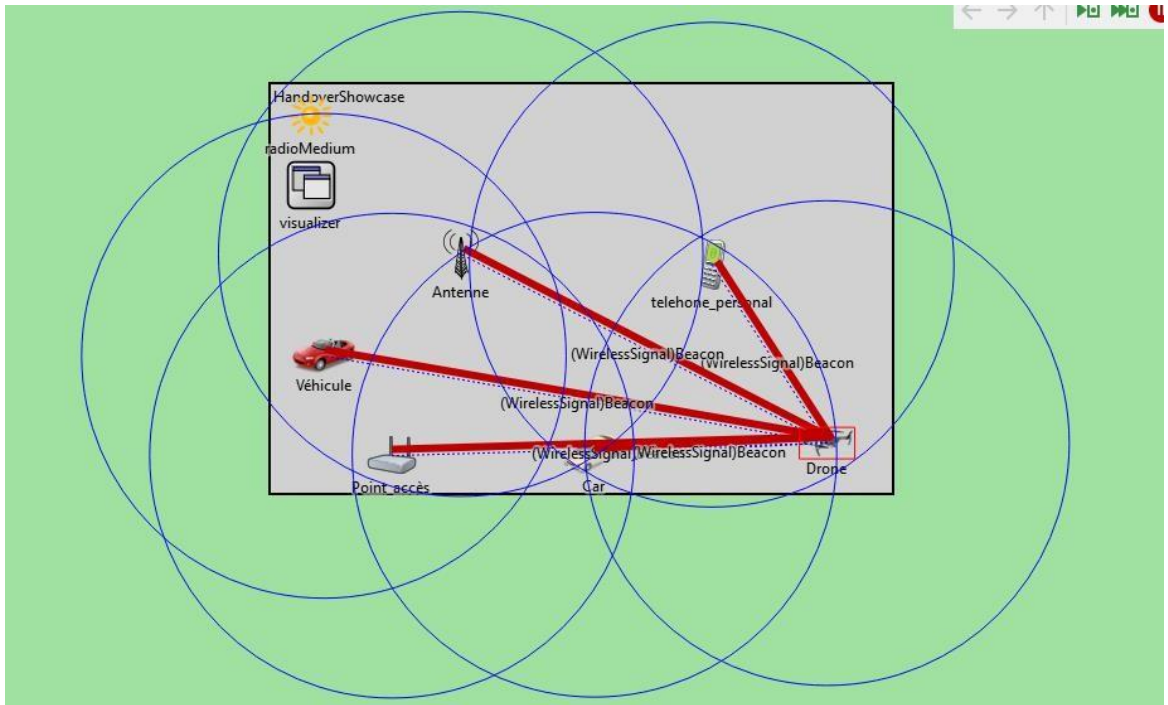


Figure 14 : Drone envoi information au véhicule et est active aux nœuds

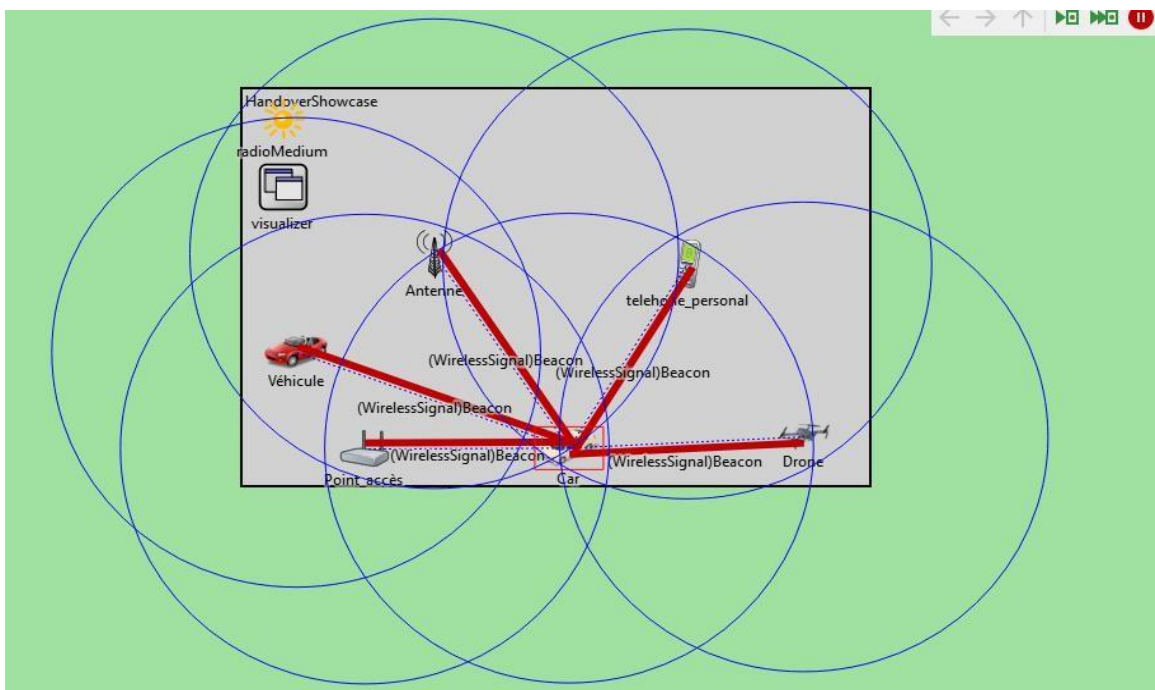


Figure 15 : Car envoi information au véhicule et est active aux nœuds

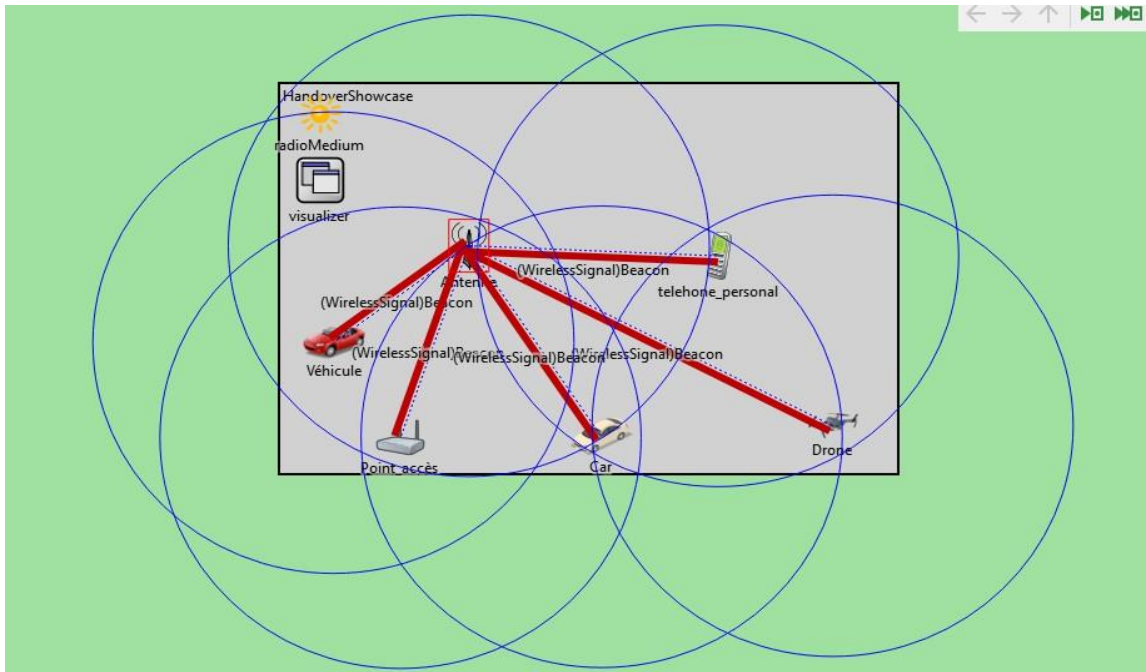


Figure 16 : Antenne envoi information au véhicule et est active aux nœuds

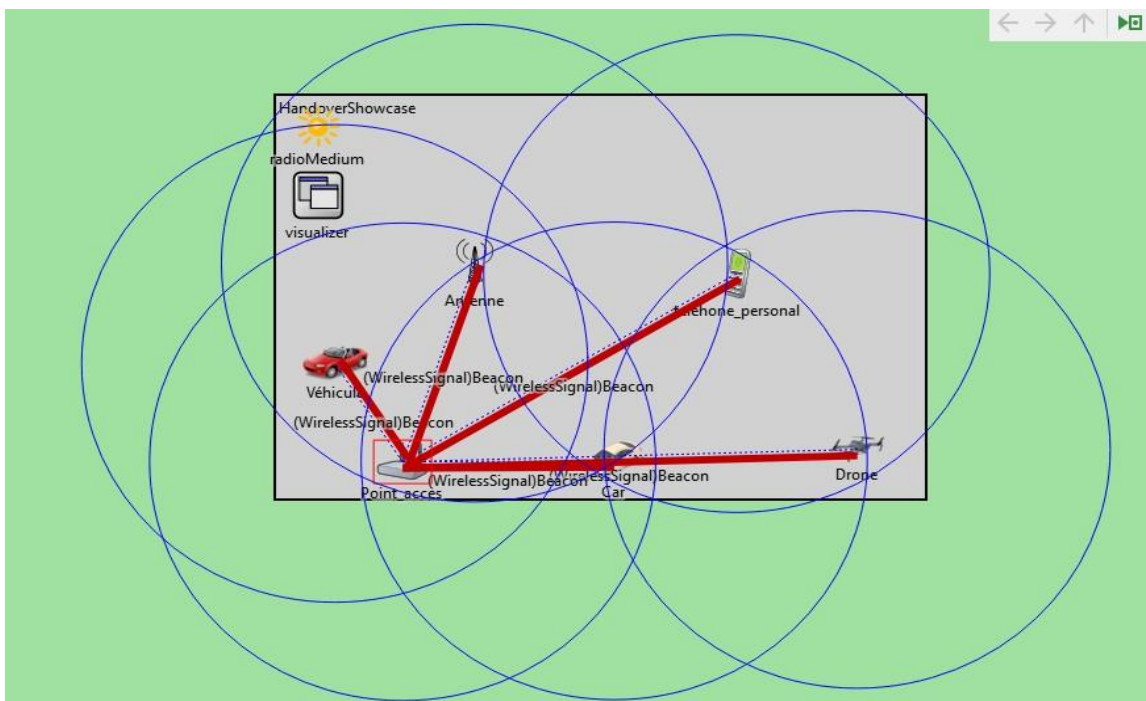


Figure 17 : Point d'accès envoi information au véhicule et est active aux nœuds

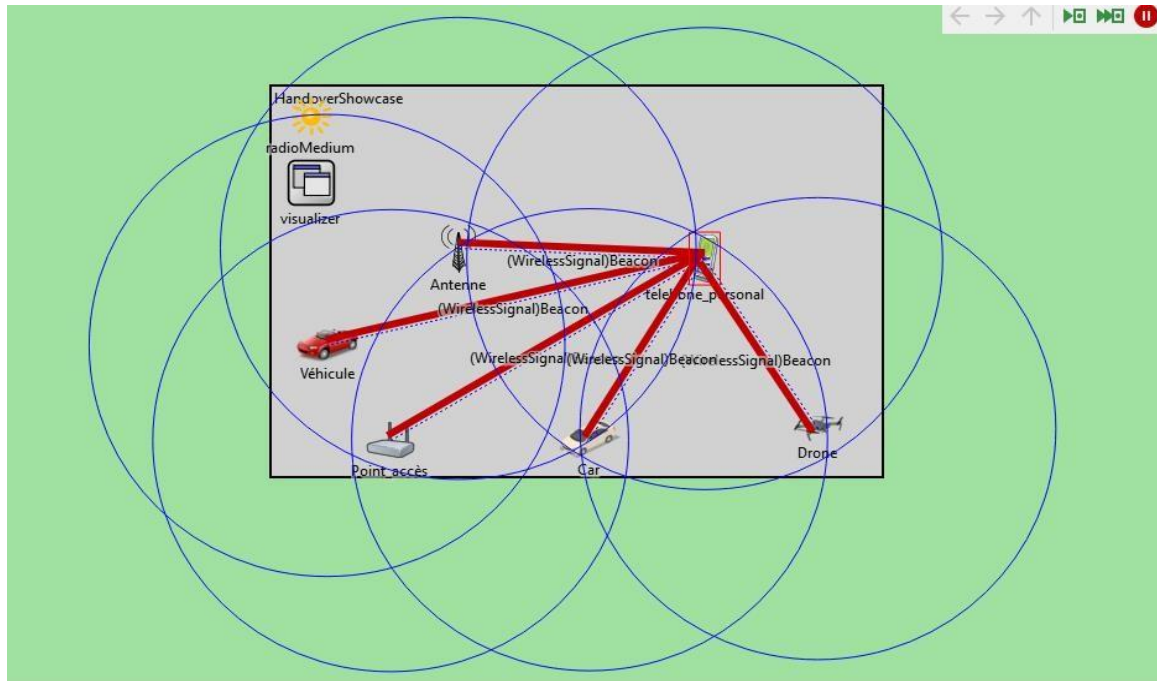


Figure 18 : Téléphone personnel envoi information au véhicule et est active aux nœuds

```

41 void Vehicle::recevoiinfo(inet::Packet *packet) {
42     // recevoir les information de chaque nœud puis calcule la distance et le best de chaque nœud
43     const auto& payload = packet->peekData()->peekAtFront<inet::FieldsChunk>();
44     auto name = payload->getField("name").str();
45     auto capacite_reseau = payload->getField("capacite_reseau").intValue();
46     auto nb_noeuds_connecte = payload->getField("nb_noeuds_connecte").intValue();
47     auto securite = payload->getField("securite").intValue();
48     auto energie = payload->getField("energie").intValue();
49     auto x = payload->getField("x").doubleValue();
50     auto y = payload->getField("y").doubleValue();

```

Figure 19 : la réception des informations de chaque nœuds

### 3.5.3- Etape 03 :

Calcule la distance entre véhicule et les autres nœuds

```

3 double Algorithme::calculateDistance(double x1, double y1, double x2, double y2) {
4     return std::sqrt((x2 - x1) * (x2 - x1) + (y2 - y1) * (y2 - y1));
5 }
1
2 void Algorithme::calculateDistances(double xv, double yv) {
3     for (auto& node : nodes) {
4         node.distance = calculateDistance(xv, yv, node.x, node.y);
5     }
6 }

```

Figure 20 : Calcule la distance entre véhicule et les autres nœuds

### 3.5.4- Etape 04 :

Calcule la note score de chaque nœud

```
double Algorithme::calculateBestValue(const NodeInfo& node) {  
    return (w_capacite*(node.capacite_reseau-node.nb_noeuds_connecte)+(w_securite*node.securite)+(w_energie*node.energie)-(w_distance*node.distance));  
}
```

Figure 21 : Calcule la note best de chaque nœud

Après en calcule le score de chaque nœud et en compère les score est le max de best estle meilleur réseau

```
std::string Algorithme::findBestNetwork() {  
    if (nodes.empty()) return "";  
  
    double maxBestValue = nodes[0].best;  
    std::string bestNode = nodes[0].name;  
  
    for (const auto& node : nodes) {  
        if (node.best > maxBestValue) {  
            maxBestValue = node.best;  
            bestNode = node.name;  
        }  
    }  
  
    return bestNode;  
}
```

Figure 22 : choisir le meilleur réseau

## 4- Conclusion :

Dans ce chapitre, nous avons exposé les différentes étapes d'implémentation de notre simulation. Nous avons débuté par une présentation du modèle de simulation, avant de détailler l'organigramme et le diagramme de séquence de l'algorithme proposé. Par la suite, nous avons expliqué en profondeur le processus d'implémentation de cet algorithme.

## Conclusion générale

L'Internet des Véhicules (IoV) constitue une avancée significative dans le domaine des systèmes de transport intelligents en intégrant de manière fluide les véhicules, les infrastructures routières et les technologies de communication. Cette intégration offre la possibilité d'une gestion plus intelligente du trafic, de services d'information en temps réel et d'un contrôle amélioré des véhicules. Pour tirer pleinement parti de ce domaine en pleine expansion, il est crucial de maîtriser les technologies et normes fondamentales tout en garantissant une interconnexion harmonieuse avec d'autres infrastructures IoT.

La sélection de réseau dans l'IoV est essentielle pour assurer des communications efficaces et fiables entre les véhicules et les infrastructures environnantes. Les algorithmes de sélection de réseau jouent un rôle central en permettant aux nœuds mobiles de choisir le réseau le plus adapté en fonction de divers critères.

Ainsi, la sélection de réseau représente un élément clé dans l'évolution des systèmes de transport intelligents, contribuant à un avenir où les véhicules connectés pourront fonctionner de manière plus sûre, efficace et écologique.

Dans le premier chapitre, nous avons exploré les concepts fondamentaux de l'IoV, en définissant le concept, en décrivant les types de communication, en examinant les domaines d'application, en analysant les architectures, et en présentant les technologies de communication associées. Le deuxième chapitre a porté sur les algorithmes de sélection de réseau, incluant une comparaison de ces algorithmes et la présentation de notre algorithme proposé pour le choix optimal du réseau. Enfin, le troisième chapitre a abordé les aspects pratiques de l'implémentation, en détaillant le modèle de simulation, l'organigramme de l'algorithme proposé, le diagramme de séquence, et en fournissant un aperçu de l'utilisation d'OMNeT++ pour l'implémentation de l'algorithme.

Les perspectives de ce travail se résument dans les points suivants :

1. Amélioration des Algorithmes de Sélection de Réseau :
  - Optimisation des Critères de Sélection : Explorer des critères supplémentaires pour la sélection de réseau, tels que les conditions météorologiques, la densité du trafic ou les comportements des utilisateurs, pour améliorer encore la précision et l'efficacité des algorithmes.

- Algorithmes d'Apprentissage Automatique : Intégrer des techniques d'apprentissage automatique pour adapter dynamiquement les algorithmes en fonction des variations du réseau et des conditions de conduite.
2. Intégration avec des Technologies Émergentes :
- 5G et Réseaux Avancés : Étudier l'impact des réseaux 5G et futurs réseaux avancés sur la sélection de réseau dans l'IoV, en mettant l'accent sur la latence ultra-faible et les vitesses de transmission élevées.
  - Edge Computing : Investiguer comment l'edge computing peut être utilisé pour améliorer la gestion des données et la prise de décision en temps réel dans les systèmes IoV.
3. Applications Pratiques et Scénarios Réels :
- Déploiement à Grande Échelle : Étudier les défis associés au déploiement à grande échelle des solutions IoV dans des environnements urbains complexes et proposer des stratégies pour leur mise en œuvre.

## Références :

- [1] <https://commentouvrir.com/definitions/internet-des-vehicules/>
- [2] <http://m.fr.wiringcable.com/info/what-is-the-internet-of-cars-what-is-the-use-49901504.html>
- [3] MERZOUGUI Salah Eddine, (Un schéma d'authentification sécurisé pour l'internet des véhicules), Université 8 mai 1945 Guelma, Faculté des Mathématiques, d'Informatique et des Sciences de la Matière, Département d'Informatique, Mémoire de Fin d'Études Master, 2020, page 05.
- [4] Benderradji Djihane Bouanane Isra, (Une architecture IoV hétérogène pour le transfert des données dans la communication Véhicule-Infrastructure), UNIVERSITÉ KASDI MERBAH OUARGLA, Faculté des Nouvelles Technologies de l'Information et de la communication, Département de l'Informatique et des Technologies de l'Information, Mémoire de Fin d'Études Master, 2022, pages 11 - 12 - 13.
- [5] Hafeez, K. A., Zhao, L., Ma, B., & Mark, J. W. (2013, Septembre). Performance Analysis and Enhancement of the DSRC for VANET's Safety Applications. Récupéré sur [ieeexplore.ieee.org](http://ieeexplore.ieee.org).  
URL : <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6475201>
- [6] Radja, B., & Khadidja, Z. (2019-2020). Traitement des données dans les réseaux véhiculaires à forte mobilité. Ouargla: Université Kasdi Marbah, Département d'Informatique et des Technologies de l'Informatique.
- [7] Léo Mendiboure, (Distribution géographique de données dans l'internet des véhicules : une approche logicielle et sécurisée utilisant les réseaux cellulaires), Université de Bordeaux, École doctorale de mathématique et informatique (EDMI) spécialité informatique, thèse pour obtenir le grade de docteur de l'université de Bordeaux, 2020, page 11.
- [8] Sathyanarayanan Rangarajan, Monica Verma, Anand Kannan, Ayush Sharma, and Ingmar Schoen. V2c : a secure vehicle to cloud framework

for virtualized and on-demand service provisioning. In Proceedings of the International Conference on Advances in Computing Communications and Informatics, pages 148–154, 2012.

[9] Kathiriya, H., Kathiriya, N., & Bavarva, A. (2013, février 21/23). Review on V2R Communication in VANET.

[10] Les applications de sécurité routière.

URL: <https://hal.archives-ouvertes.fr/tel-02611898/>

[11] Ait-Mlouk, A. Fouille de données et analyse de qualité des règles d'association dans les bases de données massives : Application dans le domaine de la sécurité routière. UCA - Université Cadi Ayyad [Marrakech].

URL : <https://hal.archives-ouvertes.fr/tel-02611898/>

[12] <https://omnetpp.org/intro/>

[13] Nawal, B., & Hanane, B. (2020-2021). Etude et proposition d'un model sur la dissémination des données dans les réseaux véhiculaire. Ouargla: Université Kasdi Merbah, Département de l'Informatique et Technologies de l'information.

[14] BOUKSANI, W. (s.d.). GESTION DE LA PROTECTION DE LA VIE PRIVÉE DANS LES RESEAUX VEHICULAIRES (VANET). Récupéré sur [depot-e.uqtr.ca](https://depot-e.uqtr.ca).

URL : <https://depot-e.uqtr.ca/id/eprint/8166/>

[15] YANG, Fangchun, et al. Architecture and key technologies for Internet of Vehicles: a survey.2017.

[16] K. Golestan, R. Soua, F. Karray, and M. S. Kamel, “Situation awareness within the context of connected cars: A comprehensive review and recent trends,” *Inf. Fusion*, vol. 29, pp. 68–83, May 2016

[17] Bonomi, F.: The smart and connected vehicle and the Internet of Things, WSTS 2013, San Jose.

[18] TUYISENGE, Livinus, et al. Network Architectures in Internet of Vehicles (IoV): Review, Protocols Analysis, Challenges and Issues. In: International Conference on Internet of Vehicles. Springer, Cham, 2018. p. 3-13.

[19] J. Contreras, S. Zeadally, and J. A. Guerrero-Ibanez, “Internet of vehicles: Architecture, protocols, and security,” *IEEE Internet of Things Journal*, 2017.

[20] Noé CURÉ, M. D. (s.d.). Véhicule autonome et connecté: communication V2X.



- [21] Nardini, G., Viridis, A., & Stea, G. (s.d.). Simulating device-to-device communications in OMNeT++ with SimuLTE: scenarios and configurations. Italy, Ingegneria dell'Informazione, Pisa.
- [22] A.FitahaA.BadriaM.MoughitaA.Sahela. (s.d.). Performance of DSRC and WIFI for Intelligent Transport Systems in VANET. Consulté le 05 Octobre 2021 à 17 : 13.  
URL : <https://doi.org/10.1016/j.procs.2018.01.133>
- [23] Nagpur, N. (s.d.). IRJET- VANET based wireless sensor. p. 01.  
URL : <https://www.academia.edu/download/57013700/IRJET-V5I5161.pdf>
- [24] Mojela, L. S., & Booysen, M. J. (s.d.). On the use of WiMAX and Wi-Fi to provide in-vehicle connectivity and media distribution.  
URL: [https://ieeexplore.ieee.org/abstract/document/6505869/?ca\\_bWKgAAAAA:zR-RovigPXa9obtJilONYv1Y2t9hQYFjDdP0Ils1GBWrOXMnhC5O7jcDrTrIvkjIPuGjIg6O0](https://ieeexplore.ieee.org/abstract/document/6505869/?ca_bWKgAAAAA:zR-RovigPXa9obtJilONYv1Y2t9hQYFjDdP0Ils1GBWrOXMnhC5O7jcDrTrIvkjIPuGjIg6O0)
- [25] Nampally, V., & Sharma, D. M. (2018, July). Information Sharing Standards in Communication. Récupéré sur ijsrcsams.  
URL [http://www.ijsrcsams.com/images/stories/Past\\_Issue\\_Docs/ijsrcsamsv7i4p91.pdf](http://www.ijsrcsams.com/images/stories/Past_Issue_Docs/ijsrcsamsv7i4p91.pdf)
- [26] Qu'est-ce qu'un réseau LTE? (2011, 9 28). Récupéré sur les affaires.  
URL: <https://www.lesaffaires.com/blogues/jean-francois-codere/qu-est-ce-qu-un-reseau-lte/535459>
- [27] Technologie de liaison micro-ondes. (2020, 11 16). Récupéré sur FMUSER.  
URL : <https://fr.fmuser.net/content/?7725.html>
- [28] Agred Naima Rabia khaira, (Simulation de la surveillance des réseaux de captures sans fil (RCSF) sous OMNeT++), Université Ibn Khaldoune Tiaret, Faculté Mathématique et Informatique, Département d'informatique, Mémoire de fin d'étude Master, 2019, page 44.
- [29] N. Tucker, M. Alizadeh An online admission control mechanism for electric vehicles at public parking infrastructures
- [30] H. Lee, D. Kim, B. Chung, H. Yoon Adaptive hysteresis using mobility correlation for fast handover

- [31] A. Haider, I. Gondal, J. Kamruzzaman, Dynamic dwell timer for hybrid vertical handover in 4G coupled networks, in: 2011 IEEE 73rd Vehicular Technology Conference (VTC Spring), 2011, pp. 1–5.
- [32] J. Hou, D.C. O'Brien, Vertical handover-decision-making algorithm using fuzzy logic for the integrated Radio-and-OW system.
- [33] K. Radhika, A.V.G. Reddy, Network selection in heterogeneous wireless networks based on fuzzy multiple criteria decision making, in: 2011 3rd International Conference on Electronics Computer Technology, vol. 6, 2011, pp. 136–139.
- [34] Y. Wang, J. Yuan, Y. Zhou, G. Li, P. Zhang, Vertical handover decision in an enhanced media independent handover framework, in: 2008 IEEE Wireless Communications and Networking Conference, 2008, pp. 2693–2698.
- [35] H. Chan, P. Fan, Z. Cao, A utility-based network selection scheme for multiple services in heterogeneous networks, in: 2005 International Conference on Wireless Networks, Communications and Mobile Computing, vol. 2, 2005, pp. 1175–1180.
- [36] E. Stevens-Navarro, V.W. Wong, Comparison between vertical handoff decision algorithms for heterogeneous wireless networks, in: 2006 IEEE 63rd Vehicular Technology Conference, vol. 2, 2006, pp. 947–951.
- [37] L. Wang, D. Binet, MADM-based network selection in heterogeneous wireless networks: a simulation study, in: 2009 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology, 2009, pp. 559–564.
- [38] F. Zhu, J. McNair, Optimizations for vertical handoff decision algorithms, in: 2004 IEEE Wireless Communications and Networking Conference (IEEE Cat. No. 04TH8733), vol. 2, 2004, pp. 867–872.
- [39] M. Cesana, N. Gatti, I. Malanchini Game theoretic analysis of wireless access network selection: models, inefficiency bounds, and algorithms.
- [40] D. Niyato, E. Hossain Dynamics of network selection in heterogeneous wireless networks: an evolutionary game approach.
- [41] G.S. Bauer, J.B. Greenblatt, B.F. Gerke Cost, energy, and environmental impact of automated electric taxi fleets in Manhattan.

[42] C. Huang, H.H. Juan, M.S. Lin, C.J. Chang Radio resource management of heterogeneous services in mobile WiMAX systems [Radio Resource Management and Protocol Engineering for IEEE 802.16]

[43] Wang, Y. M., & Elhag, T. M. (2006). Fuzzy TOPSIS method based on alpha level sets with an application to bridge risk assessment. Expert systems with applications, 31(2), 309-319.

[44] <https://fr.scribd.com/document/484678998/Presentation-de-la-plateforme-OMNET>

[45] Hmaidia Dhia Errahmane, (Une architecture Edge Computing basée sur les réseaux 5G pour améliorer l'internet des véhicules (IOV), Université Echahide Cheikh Larbi Tebbessi Tébbessa, Faculté des sciences Exactes et des Sciences de la nature et de la vie, Département mathématique et Informatique, Mémoire de fin d'étude Master, 2023, page 15.