MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE ABDELHAMID IBN BADIS - MOSTAGANEM

**Faculté des Sciences Exactes et d'Informatique**

**Département de Mathématiques et informatique**

**Filière : Informatique**

MEMOIRE DE FIN D'ETUDES

Pour l'Obtention du Diplôme de Master en Informatique

Option : **Réseaux et Systèmes**

Présenté par :

**SAIDOUNE Rahma**

THEME :

# Un package d'attaques réseaux pour OMNET++, SUMO et VEINS : appliqué à VANET

Soutenu le :

Devant le jury composé de :

| | | | |
|---|---|---|---|
| Nom et Prénom | Grade | Université de Mostaganem | Président |
| Nom et Prénom | Grade | Université de Mostaganem | Examinateur |
| Hamami Dalila | MCB | Université de Mostaganem | Encadreur |
| Adnane Asma | MCA | Université Loughborough | Co-Encadreur |

Année Universitaire 2023-2024

## Résumé

Ce travail se concentre sur les réseaux ad hoc véhiculaires (VANET), une sous-classe des réseaux ad hoc mobiles (MANET), qui sont vulnérables à diverses attaques. Il s'agit de développer et de simuler un ensemble d'attaques dans les réseaux VANET en utilisant les simulateurs OMNET++, SUMO et VEINS. Le plug-in d'attaques développées et simulées comprend l'attaque par déni de service (DOS) et les dérivées de l'attaque de l'homme du milieu (MITM), comprenant l'attaque de trou noir, l'attaque de trou gris, l'attaque de retard et l'attaque par altération. L'objectif est d'examiner l'impact négatif de ces attaques sur les VANET afin de fournir aux chercheurs un package d'attaques prêt à l'emploi pour qu'ils puissent l'utiliser pour développer des mesures de sécurité pour améliorer l'efficacité des VANET et leur fiabilité.

**Mots-clés :**

VANET, MANET, réseaux ad hoc, Vulnérabilité, OMNET++, SUMO, VEINS, attaque, DOS, MITM, Trou noir, Trou gris, attaque de retard, attaque par altération.

## Abstract

This work focuses on vehicular ad hoc networks (VANETs), a subclass of mobile ad hoc networks (MANETs), which are vulnerable to various attacks. It focuses on developing and simulating a set of attacks in VANETs networks using the OMNET++, SUMO and VEINS simulators. The developed and simulated attacks plugin includes Denial of Service (DOS) attack and derivatives of Man in the Middle (MITM) attack, including black hole attack, gray hole, delay attack and tampering attack. The goal is to examine the negative impact of these attacks on VANETs in order to provide researchers with a ready-made attack package so they can use it to develop security measures to improve the effectiveness of VANETs and their reliability.

**Keywords:**

VANET, MANET, ad hoc networks, Vulnerability, OMNET++, SUMO, VEINS, DOS, attack, MITM, Black hole, gray hole, delay attack, tampering attack.

**ملخص**

يركز هذا العمل على الشبكات المخصصة للمركبات (VANETs)، وهي فئة فرعية من شبكات الجوال المخصصة (MANETs)، والتي تكون عرضة لهجمات مختلفة. هذه فكرة متعلقة بمحاكاة مجموعة من الهجمات في الشبكات VANETs باستخدام محاكيات OMNET++ وSUMO وVEINS. يتضمن البرنامج الإضافي للهجمات المطورة والمحاكية هجوم رفض الخدمة (DOS) ومشتقات هجوم الرجل في الوسط (MITM)، بما في ذلك هجوم الثقب الأسود، والثقب الرمادي، وهجوم التأخير، وهجوم التعديل. الهدف هو دراسة التأثير السلبي لهذه الهجمات على شبكات VANET من أجل تزويد الباحثين بحزمة هجوم جاهزة حتى يتمكنوا من استخدامها لتطوير التدابير الأمنية لتحسين فعالية شبكات VANET وموثوقيتها.

**كلمات مفتاحية**

MANET، VANET، شبكات مخصصة, الضعف، MITM، DOS، VEINS، SUMO، OMNET++، هجوم، الثقب الأسود، الثقب الرمادي، هجوم التأخير، هجوم التعديل.

# Dédicaces

En premier lieu, je rends grâce à Dieu, le plus clément et le plus miséricordieux, qui m'a donné la force, la patience et la persévérance nécessaires pour accomplir ce travail.

Je dédie ce travail à mes parents, dont l'amour inconditionnel, le soutien indéfectible et les sacrifices ont constitué la fondation sur laquelle j'ai construit mes succès. Votre foi en moi a été mon phare dans les moments d'incertitude.

À mes sœurs, qui ont toujours été présentes pour moi, partageant mes joies et mes peines. Votre amour fraternel et votre soutien ont été une source constante de réconfort et d'inspiration.

Je tiens à exprimer ma profonde gratitude à ma professeure Dr. Hamami Dalila, qui a été bien plus qu'un guide académique. Elle m'a donné l'impression qu'elle était ma grande sœur, elle m'a soutenu, m'a encouragé et m'a aidé à naviguer dans les défis de ce parcours académique. Son dévouement à l'enseignement et son engagement envers mes progrès ont été une source d'inspiration constante.

Ce travail est le fruit de tous ces soutiens, et je suis profondément reconnaissant à chacun d'entre vous.

À mon fidèle compagnon, mon ordinateur portable, qui a été à mes côtés pendant ces cinq années, supportant mes nuits blanches et toutes mes humeurs, tu as été et restera toujours mon binôme durant mon cursus.

Tu as été le témoin silencieux de mes triomphes et de mes échecs, un outil précieux qui a facilité mon voyage académique. Pour ta résilience, ta constance et ton soutien inébranlable, je te dédie ce travail, fruit de notre collaboration.

Merci pour ces années de service dévoué, et pour être un pilier sur lequel je pouvais toujours compter.

# Remerciements

Tout d'abord, je tiens à exprimer ma gratitude envers Dieu pour m'avoir donné la force et la persévérance nécessaires pour accomplir ce travail.

Je suis également reconnaissante envers mes parents et mes sœurs pour leur soutien constant et leur amour inconditionnel tout au long de ce projet.

Je suis reconnaissante envers Dr. Hamami Dalila et Dr. Adnane Asma pour leur guidance académique. Leur expertise a été précieuse pour la réalisation de ce projet.

Je tiens à exprimer ma profonde gratitude envers moi-même. C’est grâce à mon engagement personnel, mon dévouement, ma persévérance et mon travail acharné que ce projet de fin d’études a pu voir le jour. Chaque obstacle surmonté et chaque défi relevé n’ont fait que renforcer ma détermination. Chaque page, chaque ligne de code et chaque simulation sont le reflet des heures que j’ai consacrées à ce travail. Je suis fière de ce que j’ai accompli et je me remercie d’avoir eu la force de poursuivre, même dans les moments les plus difficiles.

**Un très grand merci à moi**

# Liste des figures


| Figure N° | Titre de la figure | Page |
|---|---|---|
| Figure 1 | La différence entre le mode ad-hoc et mode infrastructure | 16 |
| Figure 2 | Les réseaux ad-hoc mobiles | 17 |
| Figure 3 | Les réseaux de capteurs sans fils | 17 |
| Figure 4 | Les réseaux ad hoc volants | 18 |
| Figure 5 | Les réseaux maillés sans fils | 19 |
| Figure 6 | Les réseaux ad hoc véhiculaires | 20 |
| Figure 7 | Les composants d'une voiture moderne (OBU) | 21 |
| Figure 8 | Les types de communication dans les VANET | 22 |
| Figure 9 | Les types d'attaques dans les réseaux ad hoc | 25 |
| Figure 10 | Architecture globale | 31 |
| Figure 11 | Installation OMNET++ | 54 |
| Figure 12 | Exécution de l'exemple aloha d'OMNET++ | 54 |
| Figure 13 | L'interface Qtenv du OMNET++ | 55 |
| Figure 14 | Initialisation de la simulation dans OMNET++ | 56 |
| Figure 15 | Simulation de l'exemple aloha dans OMNET++ | 57 |
| Figure 16 | Importation et compilation du framework INET | 41 |
| Figure 17 | Simulation de l'exemple aodv du framework INET | 43 |

| | | |
|---|---|---|
| Figure 18 | Importation et compilation du framework VEINS | 43 |
| Figure 19 | Démon de lancement de VEINS | 44 |
| Figure 20 | La simulation du réseau VANET de la ville d'Erlangen | 45 |
| Figure 21 | La simulation de la ville Erlangen dans SUMO | 45 |
| Figure 22 | Simulation de l'attaque Trou noir | 46 |
| Figure 23 | Simulation de l'attaque Trou gris | 47 |
| Figure 24 | Simulation de l'attaque de retard | 48 |
| Figure 25 | Simulation de l'attaque par altération | 48 |
| Figure 26 | Simulation de l'attaque de déni de service | 49 |
| Figure 27 | Simulation d'une autoroute | 50 |
| Figure 28 | La simulation de la ville Manhattan | 50 |
| Figure 29 | Le fichier de journalisation de l'attaque trou noir | 52 |
| Figure 30 | Les logs de l'attaque de retard sur OMNET++ | 54 |
| Figure 31 | Les logs de l'attaque trou gris dans OMNET++ | 58 |

# Liste des tableaux


| Tableau N° | Titre du tableau | Page |
|---|---|---|
| Tableau 1 | Résultats de la simulation de l'attaque trou noir | 52 |
| Tableau 2 | Résultats de la simulation de l'attaque de retard | 55 |
| Tableau 3 | Résultats de la simulation de l’attaque trous gris | 59 |
| Tableau 4 | Résultats de la simulation de l’attaque par altération | 60 |
| Tableau 5 | Résultats de la simulation de l’attaque de déni de service | 61 |

# Liste des abréviations

| Abréviation | Expression Complète | Page |
|---|---|---|
| MANET | Mobile Ad-hoc NETwork | 13 |
| VANET | Vehicular Ad-hoc NETwork | 13 |
| DOS | Denial Of Service | 13 |
| MITM | Man In The Middle | 13 |
| OMNET++ | Objective Modular NEtwork Testbed In C++ | 13 |
| SUMO | Simulation of Urban MObility | 13 |
| VEINS | Vehicles In Network Simulation | 13 |
| WI-FI | WIreless FIdelity | 15 |
| WSN | Wireless Sensors Network | 16 |
| FANET | Flying Ad-hoc Network | 16 |
| WMN | Wireless Mesh Network | 18 |
| OBU | On Board Unit | 19 |
| RSU | Road Side Unit | 19 |
| EDR | Event Data Recorder | 19 |
| GPS | Global Positioning System | 19 |
| V2X | Vehicle to everything | 20 |
| V2V | Vehicle toVehicle | 20 |

| | | |
|---|---|---|
| V2P | Vehicle to Pedestrian | 20 |
| V2I | Vehicle to Infrastructure | 20 |
| DDOS | Distributed Denial Of Service | 24 |
| API | Application Programming Interface | 24 |
| PDF | Portable Document Format | 25 |
| IVC | Inter-Vehicle Communication | 30 |
| NS-2 | Network Simulator 2 | 31 |
| NS-3 | Network Simulator 3 | 31 |
| JiST/SWANS | Java In Simulation Time Wireless Ad-Hoc Network Simulator | 31 |
| GloMoSim | Global Mobile System Simulator | 31 |
| MOVE | MObility model for VEhicle simulation | 32 |
| CORsim | Traffic microsimulation software | 33 |
| VISSIM | Vehicle Simulator | 33 |
| VANETMOBISIM | Vehicular Ad-hoc Network Mobility Simulator | 33 |
| SIMULTE | Simulation of Long Term Evolution Networks | 33 |
| TRACI | Traffic Control Interface | 35 |
| RAM | Random Access Memory | 52 |
| ChatGPT | Chat Generative Pre-trained Transformer | 52 |

# Table des matières

Introduction Générale ..... 4

Chapitre 1 Les réseaux ad-hoc : VANET ..... 6

1.1 Introduction ..... 6
1.2 Les réseaux sans fils (ad-hoc) ..... 6
1.3 Types de réseau Ad Hoc : ..... 7
1.3.1 Les réseaux ad-hoc mobiles (MANET) ..... 7
1.3.2 Les réseaux de capteurs sans fil (WSN) ..... 8
1.3.3 Les réseaux ad hoc volant (FANET) ..... 9
1.3.4 Les réseaux maillés sans fil (WMN) ..... 9
1.3.5 Les réseaux ad hoc véhiculaire (VANET) ..... 10
1.4 Les réseaux ad-hoc véhiculaires (VANET) ..... 11
1.4.1 La communication entre véhicules ..... 11
1.4.2 Les types de communications dans les VANET ..... 13
1.4.3 Les applications des VANET ..... 14
1.5 Caractéristiques des réseaux VANET ..... 15
1.6 Conclusion ..... 16

Chapitre 2 Les attaques réseaux : VANET ..... 17

2.1 Introduction ..... 17
2.2 Les attaques ..... 17
2.3 Les différents types d'attaques dans les réseaux ad-hoc ..... 17
2.3.1 Les attaques dans les VANET ..... 19
2.4 Choix des attaques ..... 21
2.5 Évaluation des risques dans les VANET ..... 23
2.6 Conclusion ..... 24

Chapitre 3 Conception du modèle simulable ..... 25
3.1 Introduction ..... 25
3.2 Le modèle simulable ..... 25
3.2.1 Définition ..... 25
3.2.2 Objectif ..... 25
3.2.3 Architecture globale ..... 26
3.3 La simulation ..... 27
3.3.1 Définition ..... 27
3.3.2 Objectif ..... 28
3.4 Les métriques d'évaluations ..... 28
3.4.1 Définition ..... 28
3.4.2 Les Métriques d'évaluation pour les VANET ..... 29
3.4.3 Les Métriques d'évaluation pour les attaques ..... 30
3.5 Conclusion ..... 31
Chapitre 4 Développement et simulation ..... 33
4.1 Introduction ..... 33
4.2 Les outils de simulation des VANET ..... 33
4.2.1 Les simulateurs des réseaux VANET ..... 33
4.2.2 Les simulateurs de trafic routier : ..... 35
4.2.3 Les frameworks ..... 36
4.3 Choix des outils de simulation et justification ..... 37
4.4 Environnement de développement ..... 40
4.5 Etapes de projet ..... 40
4.5.1 Installation des outils de simulation ..... 40
4.5.2 Configuration ..... 41
4.5.3 Développement et simulation des attaques ..... 46
4.5.4 Développement et simulation du trafic urbain ..... 49
4.6 Analyse des résultats ..... 51
4.6.1 Analyse de résultats de l'attaque de trou noir ..... 51

4.6.2 Analyse de résultats de l'attaque de retard ..... 53
4.6.3 Analyse de résultats de l'attaque de trou gris ..... 57
4.6.4 Analyse de résultats de l'attaque de modification ..... 59
4.6.5 Analyse de résultats de l'attaque de déni de service ..... 60
4.7 Complexité de projet ..... 61
4.8 Conclusion ..... 62
Conclusion Générale ..... 63
Annexe A ..... 64
Annexe B ..... 67
Bibliographie ..... 68

# Introduction Générale

Les MANETs, ou réseaux ad hoc mobiles, sont des réseaux sans fil qui n'ont pas besoin d'une infrastructure fixe. Les VANETs, ou réseaux ad hoc de véhicules, sont une sous-catégorie spécifique des MANETs qui permettent la communication entre les véhicules et les infrastructures routières. Les VANET sont particulièrement vulnérables à diverses attaques en raison de leur nature ouverte et dynamique car ils ont de nombreuses applications potentielles, telles que la gestion du trafic, le partage d'informations, le divertissement, et cela posent des défis importants en termes de sécurité.

Dans le contexte des réseaux VANET, certaines attaques se distinguent par leur gravité et leur impact potentiellement dévastateur. Parmi celles-ci, l'attaque par déni de service (DoS) est particulièrement redoutée. De plus, diverses variantes de l'attaque de l'homme du milieu (MITM) sont également préoccupantes, y compris l'attaque de trou noir, l'attaque de trou gris, l'attaque par retard et l'attaque par altération. Ces menaces mettent en évidence la nécessité d'une sécurité robuste et efficace dans les réseaux VANET.

Ce travail s'inspire d'une idée d'un projet antérieur [1], dont l'objectif principal était le développement et la simulation d'un ensemble d'attaques dans les réseaux ad hoc en utilisant le simulateur OMNET++. Dans le cadre de notre projet, l'objectif est d'étendre cette simulation à l'environnement des réseaux VANET en développant et en simulant un package d'attaques, ce dernier englobe des attaques qui peuvent compromettre la sécurité et la performance des VANET ayant un impact potentiellement dangereux, ceux-ci seront réalisés en exploitant les capacités des simulateurs OMNET++, SUMO et le Framework VEINS. Notre objectif est non seulement de simuler notre package développé mais aussi d'analyser les résultats de ces attaques afin de mieux comprendre leur impact négatif et défavorable sur les réseaux VANET. Cette démarche va fournir aux chercheurs la possibilité de se concentrer

principalement sur l'élaboration de solutions, d'améliorer l'efficacité et la fiabilité des VANET, contribuant ainsi à assurer leur fonctionnement efficace.

Ce mémoire est composé de quatre chapitres :

**Le premier chapitre** est consacré aux réseaux ad hoc et particulièrement aux réseaux VANET.

**Le deuxième chapitre** expose les attaques ayant un impact critique sur le VANET et met en évidence l'attaque "Déni de Service" (DOS) et les attaques de type "Homme au Milieu" (MITM) tels que "Trou noir", "Trou gris", "attaque de retard" et "attaque par altération".

**Le chapitre trois** est consacré à la présentation de la simulation, de ses objectifs, ainsi que des outils de simulation spécifiques aux réseaux VANET. Une étude comparative des outils de simulation VANET est également réalisée afin de justifier notre choix des simulateurs OMNET++ SUMO et le Framework VEINS.

Le dernier chapitre, **le quatrième**, est consacré au développement et à la simulation de notre package d'attaques. Une analyse détaillée des résultats est effectuée pour valider notre approche. Cette étape est essentielle pour confirmer l'efficacité de notre projet dans le contexte du développement et de simulation des attaques dans les réseaux VANET.
Nous concluons ce travail en résumant le contenu de ce mémoire.

# Chapitre 1

# Les réseaux ad-hoc : VANET

## 1.1 Introduction

Dans ce premier chapitre, nous explorerons les réseaux ad hoc et leurs différents types, en mettant particulièrement l'accent sur les réseaux ad hoc véhiculaires. Nous explorerons les modes de communication au sein des VANET, ainsi que la manière dont les véhicules établissent des communications entre eux et les diverses applications de ces réseaux et leurs caractéristiques.

## 1.2 Les réseaux sans fils (ad-hoc)

Un réseau ad hoc est un type de réseau sans fil décentralisé qui ne dépend pas d'une infrastructure préexistante et fixe comme les routeurs ou les points d'accès. Il se forme de manière spontanée lorsque des appareils se connectent directement entre eux. Chaque nœud participe au routage en transmettant les données aux autres nœuds, ces informations peuvent passer par plusieurs autres nœuds pour y arriver, ce qui permet au réseau de s'organiser de manière autonome. Ce type de réseau est adapté à des situations telles que les plans d'urgence, une communication rapide et instantanée est nécessaire, par exemple lors de catastrophes naturelles où un réseau ad hoc peut être utilisé pour partager des informations en temps réel sur les zones sinistrées [2][3].

Les réseaux ad hoc peuvent utiliser différents protocoles de communication, comme le Wi-Fi Direct, le Bluetooth ou le Zigbee. Ils nécessitent également des protocoles de routage ad hoc

pour permettre aux nœuds de trouver le chemin optimal pour transmettre les données entre eux [4][5][6].

Ils sont utiles dans des situations où une infrastructure de réseau n'est pas disponible ou pratique [7], mais ils présentent également des défis en termes de sécurité et de gestion des ressources [8][9]. Ils sont particulièrement vulnérables aux différentes attaques possibles car les communications sans fil sont transmises par ondes radios et peuvent être écoutées par des personnes non autorisées [10].

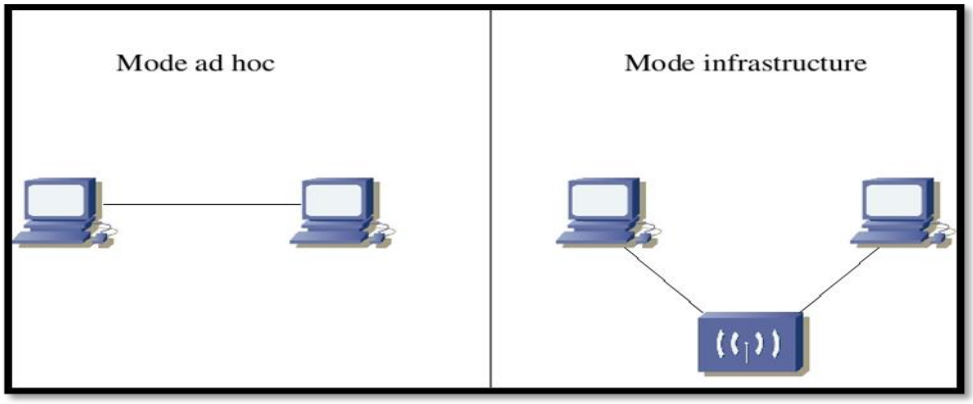


Figure 1 - La différence entre le mode ad-hoc et mode infrastructure

## 1.3 Types de réseau Ad Hoc :

Il existe plusieurs types de réseaux ad hoc, y compris les MANET, WSN, FANET, WMN et les VANET, chacun ayant ses propres caractéristiques et applications spécifiques. Dans les sections suivantes, nous allons explorer ces différents types de réseaux ad hoc en détail.

### 1.3.1 Les réseaux ad-hoc mobiles (MANET)

Les réseaux ad hoc mobiles (en anglais Mobile Ad hoc Network) sont des systèmes de communication sans fil qui permettent à un ensemble d'appareils mobiles de se connecter de manière décentralisée, sans nécessiter d'infrastructure fixe [11]. Ces réseaux sont dynamiques, avec des nœuds qui peuvent entrer et sortir du réseau à tout moment [12].

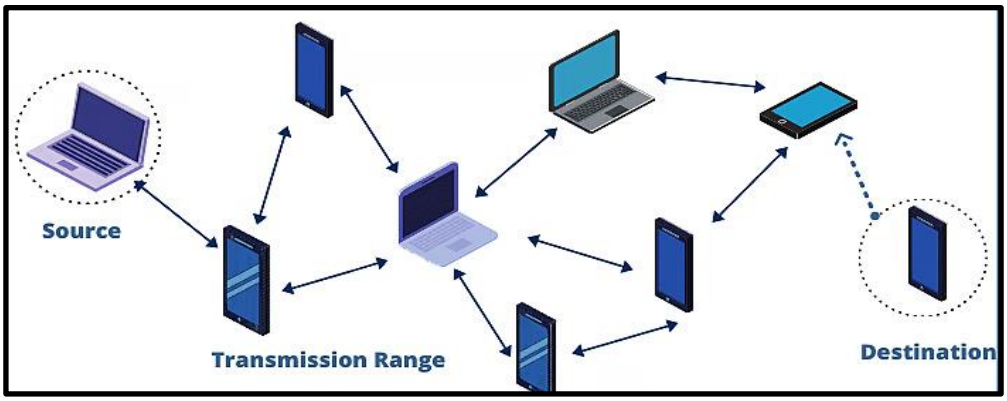


Figure 2 - Les réseaux ad-hoc mobiles

### 1.3.2 Les réseaux de capteurs sans fil (WSN)

Un réseau de capteurs sans fil (en anglais Wireless Sensors Network) est une configuration de réseau ad hoc qui se compose d'une multitude de nœuds, chacun étant un micro-capteur. Ces micro-capteurs ont la capacité de collecter et de transmettre des données de manière indépendante. Ils peuvent être dispersés de manière aléatoire dans une région géographique spécifique, connue sous le nom de « champ de captage », qui correspond à la zone d'intérêt pour le phénomène à surveiller [13][14][15].

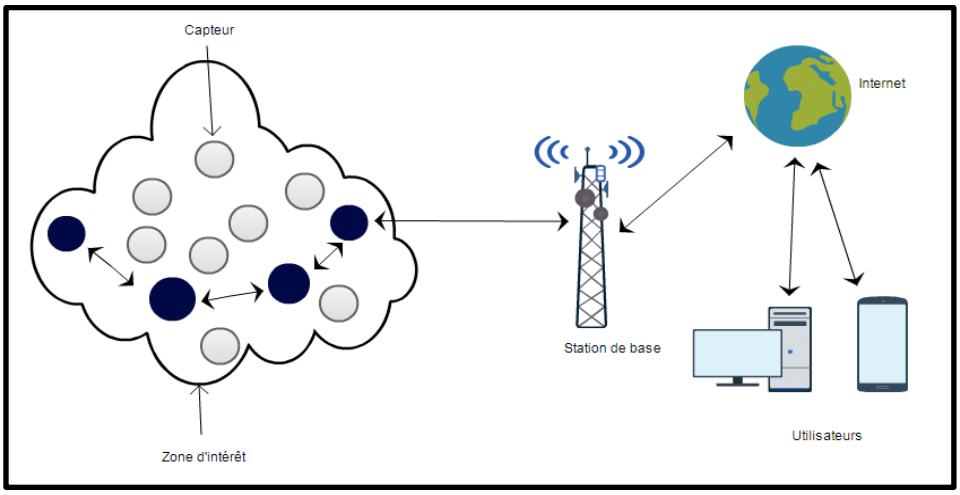


Figure 3 - Les réseaux de capteurs sans fils

### 1.3.3 Les réseaux ad hoc volant (FANET)

Un réseau ad hoc volant (en anglais Flying Ad hoc Network) est un type de réseau ad hoc qui utilise des drones comme nœuds de réseau pour effectuer diverses tâches. Ces drones, qui sont mobiles et peuvent être déployés dans des zones non déterministes, permettent une grande flexibilité et adaptabilité.

Les FANET sont des réseaux aériens autonomes qui fonctionnent dans des conditions dynamiques et incertaines. La communication entre les nœuds peut se faire directement si les nœuds sont à portée l'un de l'autre, ou indirectement via des nœuds relais.[16][17]

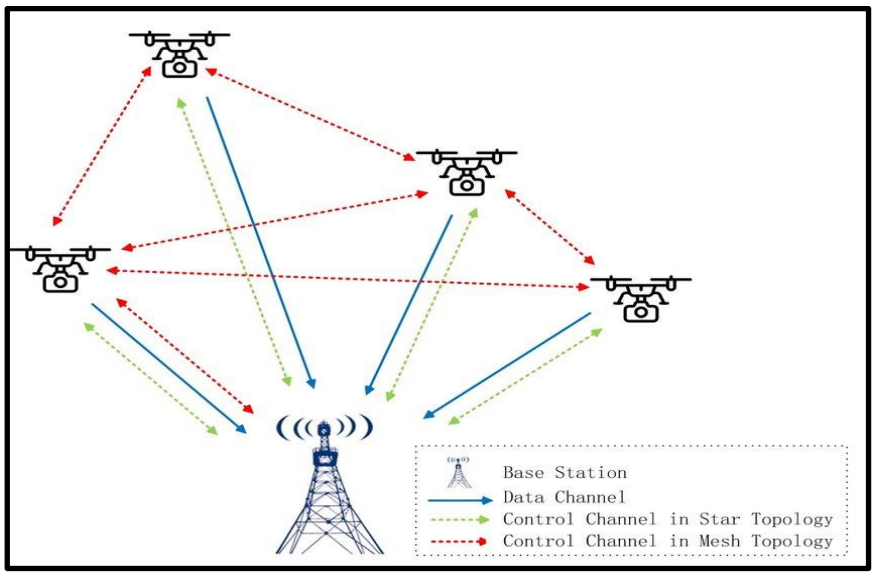


Figure 4 - Les réseaux ad hoc volants

### 1.3.4 Les réseaux maillés sans fil (WMN)

Un WMN (en anglais Wireless Mesh Network) est une configuration de réseau qui offre une connectivité robuste et fiable grâce à sa topologie maillée ou chaque nœud est connecté à plusieurs autres nœuds, ce qui permet une redondance des chemins de communication. Si un chemin échoue, le réseau peut automatiquement rediriger le trafic via un autre chemin, assurant ainsi une continuité de service. Les WMN sont particulièrement utiles dans les

environnements où l'installation de câbles est difficile ou coûteuse, comme les zones urbaines denses ou les sites patrimoniaux.[18][19][20]

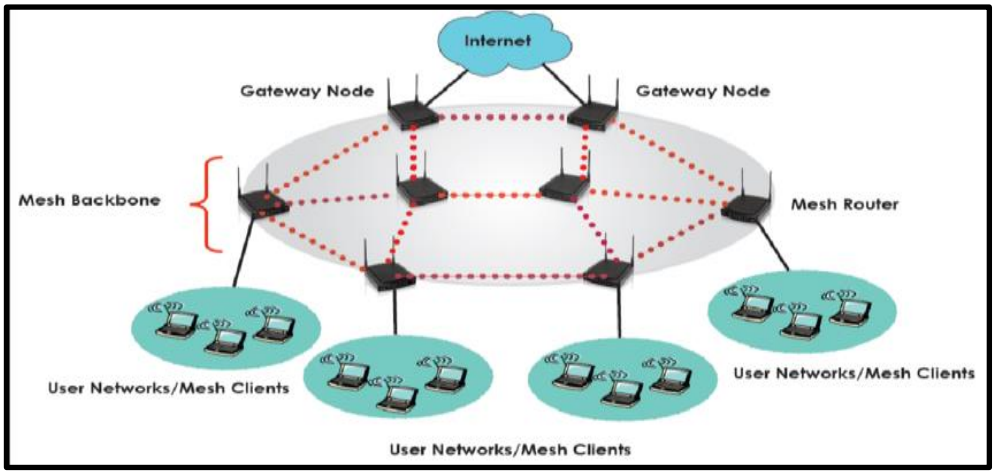


Figure 5 - Les réseaux maillé sans fils

### 1.3.5 Les réseaux ad hoc véhiculaire (VANET)

Un réseau ad hoc de véhicules (en anglais Vehicular Ad hoc Network) est un type de réseau ad hoc qui utilise des véhicules comme nœuds de réseau pour effectuer diverses tâches. Ces véhicules, qui sont mobiles et peuvent se déplacer dans des zones non déterministes, offrent une grande flexibilité et adaptabilité. Ils sont capables de communiquer entre eux (V2V) ou avec des infrastructures routières (V2I) pour améliorer la sécurité routière, le confort de conduite et l'efficacité du trafic [21][22].

Étant l'objet de notre étude, ce type de réseau sera particulièrement détaillé dans la section suivante (section 1.4).

Figure 6 - Les réseaux ad hoc véhiculaires

## 1.4 Les réseaux ad-hoc véhiculaires (VANET)

Les réseaux véhiculaires ad-hoc (en anglais Vehicular Adhoc network) ou VANET, sont une sous-classe des MANET, ils sont particulièrement adaptés aux systèmes de transport intelligents (STI) et visent à fournir des communications au sein d'un groupe de véhicules à portée les uns des autres. Cependant, les VANET sont vulnérables aux attaques en raison des contraintes et limitations physiques, telles que les communications sans fil qui peuvent être écoutées par des personnes non autorisées [21].

Les VANET sont un domaine de recherche actif, avec des défis spécifiques liés à la conception de protocoles et d'applications efficaces, ainsi qu'à la gestion des échanges de données dans un environnement dynamique et à haute vitesse.[22]

### 1.4.1 La communication entre véhicules

Dans les réseaux VANET, les véhicules sont équipés de dispositifs de communication sans fil, appelés unités embarquées (OBU), pour permettre les différents types de communications. Ces unités permettent aux véhicules de communiquer entre eux ou avec des unités de bord de route (Road Side Units - RSUs) pour améliorer la sécurité routière et l'efficacité du trafic, ainsi que pour permettre la diffusion d'informations très sensibles, telles que la position, la vitesse et la direction des véhicules [23] [24].

Ces unités embarquées, en d'autres termes, les composants d'une voiture moderne, incluent divers systèmes et technologies qui contribuent au bon fonctionnement du véhicule. Voici quelques exemples de ces composants [25] [26] :

1. **Radar avant (Forward radar)** : Situé à l'avant de la voiture, il est utilisé pour détecter les objets en avant. Il est généralement utilisé dans les systèmes d'assistance à la conduite, comme le freinage automatique d'urgence et le régulateur de vitesse adaptatif.

2. **Enregistreur de données d'événement (Event data recorder - EDR)** : Il enregistre des informations sur le véhicule et son fonctionnement, comme la vitesse du véhicule, l'utilisation de la ceinture de sécurité, et l'activation de l'airbag. Ces informations peuvent être utiles pour comprendre les circonstances d'un accident de voiture.

3. **Interface homme-machine (Human-Machine Interface)** : C'est l'interface par laquelle le conducteur interagit avec le véhicule. Cela peut inclure le tableau de bord, l'écran tactile, les commandes au volant, et plus encore.

4. **Plateforme informatique (Computing platform)** : C'est le système central qui gère diverses fonctions de la voiture, comme le traitement des données des capteurs, le contrôle des systèmes du véhicule, et la communication avec l'extérieur.

5. **Système de positionnement (Positioning system - GPS)** : Situé sur le toit pour une réception optimale du signal, il permet au véhicule de connaître sa position exacte. Il est essentiel pour la navigation et peut également être utilisé dans d'autres systèmes, comme l'assistance à la conduite.

6. **Installation de communication (Communication facility)** : Elle permet au véhicule de communiquer avec d'autres véhicules, avec l'infrastructure routière, ou avec le cloud. Cela peut être utilisé pour des services comme la navigation en temps réel, les mises à jour logicielles, et la communication V2X (Vehicle-to-Everything).

7. **Radar arrière (Rear radar)** : Situé à l'arrière de la voiture, il est utilisé pour détecter les objets derrière le véhicule. Il est généralement utilisé dans les systèmes d'aide au stationnement et la surveillance des angles morts.

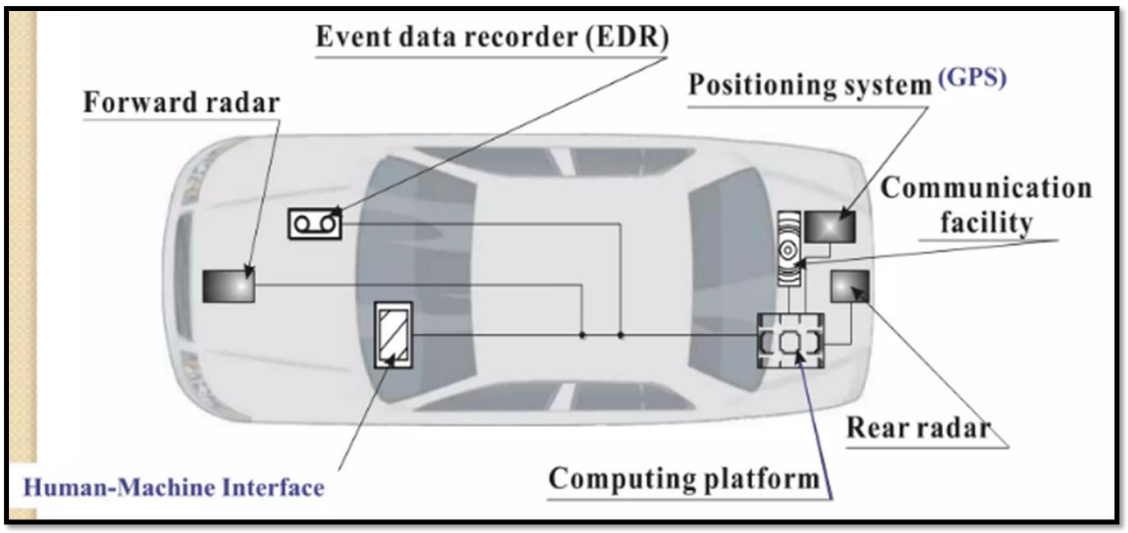


Figure 7 - Les composants d'une voiture moderne (OBU)

### 1.4.2 Les types de communications dans les VANET

1. **La communication V2V (Vehicle-to-Vehicle)** : C'est une technologie qui permet aux véhicules de partager des informations en temps réel. Cela peut inclure des détails tels que la vitesse, la position, la direction et d'autres informations pertinentes pour la sécurité routière [27] [28].

2. **La communication V2P (Vehicle-to-Pedestrian)** : Ce mode permet une communication directe entre un véhicule et un piéton. Elle peut également être utilisée pour communiquer avec d'autres usagers de la route, comme les cyclistes [29].

3. **La communication V2I (Vehicle-to-Infrastructure)** : Ce type permet aux véhicules de communiquer avec des éléments d'infrastructure tels que les feux de circulation et les panneaux de signalisation. Cela permet aux véhicules de recevoir des informations importantes et de partager des informations pertinentes avec l'infrastructure [30][31].

4. **La communication V2X (Vehicle-to-Everything)** : Cette technologie permet aux véhicules de communiquer avec tout ce qui les entoure [32] [33]. Cela inclut d'autres véhicules, l'infrastructure, les piétons et même le réseau, en d'autres termes ce type englobe toutes les formes de communications (V2V, V2P et V2I).

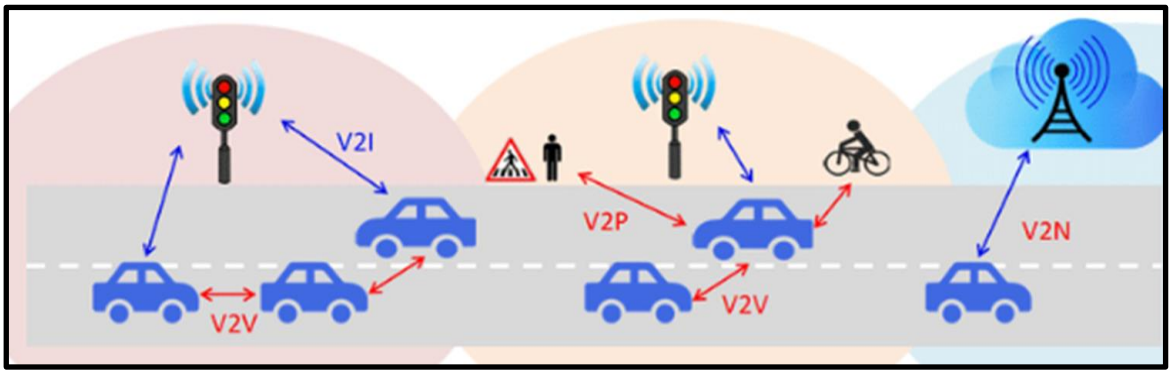


Figure 8 - Les types de communication dans les VANET

### 1.4.3 Les applications des VANET

Il existe deux types d'applications des VANET qui jouent un rôle crucial dans l'exploitation des capacités de ces réseaux pour améliorer la sécurité et l'efficacité du transport routier [34][35] :

#### 1.4.3.1 Applications liées à la sécurité

Ces applications visent à améliorer la sécurité routière. Elles peuvent inclure des alertes de collision, des avertissements de limitation de vitesse, des notifications de conditions routières dangereuses, et des systèmes d'assistance au conducteur. L'objectif de ces applications est de réduire le nombre d'accidents de la route et d'améliorer la sécurité des conducteurs et des passagers.

#### 1.4.3.2 Applications de confort (non liées à la sécurité)

Ces applications visent à améliorer l'expérience de conduite sans nécessairement avoir un impact direct sur la sécurité. Elles peuvent inclure des systèmes de navigation, des informations sur le trafic en temps réel, des services d'info divertissement, et des applications de stationnement intelligent. L'objectif de ces applications est d'améliorer le confort et la commodité pour les conducteurs et les passagers.

## 1.5 Caractéristiques des réseaux VANET

Dans le cadre de notre projet, nous avons délibérément choisi de nous concentrer sur les réseaux ad hoc véhiculaires (VANET). Ce choix stratégique est soutenu par une multitude de raisons pertinentes et convaincantes que nous explorerons ici en détail [36][37] :

Premièrement, les VANET offrent une plus grande portée de communication. En raison de la mobilité rapide des véhicules, les VANET peuvent couvrir une plus grande zone géographique, ce qui permet une collecte de données plus vaste et plus diversifiée.

Deuxièmement, les VANET sont intrinsèquement plus dynamiques. Les véhicules se déplacent rapidement et changent fréquemment de position, ce qui crée un réseau hautement dynamique. Cette dynamique peut être exploitée pour créer des applications innovantes, comme la gestion du trafic en temps réel et les systèmes d'alerte précoce.

Troisièmement, les VANET ont un potentiel significatif pour améliorer la sécurité routière. Par exemple, ils peuvent permettre la communication entre véhicules pour prévenir

les collisions, ou entre les véhicules et l'infrastructure routière pour fournir des alertes sur les conditions de la route.

Enfin, en se concentrant sur les VANET, nous pouvons tirer parti des avancées technologiques récentes dans le domaine des véhicules connectés et autonomes. Ces technologies offrent de nouvelles opportunités pour améliorer l'efficacité du trafic, réduire les émissions de carbone et améliorer la sécurité routière.

Toutefois, ces caractéristiques constituent un risque imminent pour les utilisateurs. Ils sont souvent confrontés à différents types d'attaques tels que : attaques et violations de la confidentialité, attaques engendrant des problèmes de stabilité du réseau et retards dans la communication, ou encore risques de défaillance des systèmes critiques et de fausses alertes.

Ces risques doivent être pris en compte lors de la conception et de la mise en œuvre des VANET pour assurer leur sécurité, leur fiabilité et leur efficacité.

## 1.6 Conclusion

Dans ce premier chapitre, nous avons plongé dans l'univers des réseaux ad hoc, en mettant l'accent sur les VANET. Nous avons exploré les différents modes de communication au sein des VANET, ainsi que la manière dont les véhicules établissent des liaisons entre eux. De plus, nous avons examiné les nombreuses applications de ces réseaux et leurs caractéristiques uniques où nous avons souligné la faiblesse de ces dernières.

Ce chapitre pose les fondements essentiels pour notre exploration ultérieure des réseaux véhiculaires ad hoc, mettant en lumière les risques auxquels sont confrontés les VANET. Ce dernier point fera l'objet du chapitre suivant.

# Chapitre 2

# Les attaques réseaux : VANET

## 2.1 Introduction

Dans ce chapitre, nous nous pencherons sur les attaques qui ont un impact critique sur les réseaux ad hoc. Nous mettrons en évidence les attaques les plus dangereuses ciblant les VANET, notamment l'attaque de "Déni de Service" (DOS) ainsi que les attaques de type "Homme au Milieu" (MITM), telles que le "Trou noir", le "Trou gris", l'attaque par "retard" et l'attaque par "altération".

## 2.2 Les attaques

Dans le domaine des réseaux informatiques, une attaque est une action malveillante qui vise à perturber le fonctionnement normal d'un réseau, à accéder à des informations sensibles ou à utiliser le réseau pour mener des activités malveillantes.

## 2.3 Les différents types d'attaques dans les réseaux ad-hoc

Les réseaux ad-hoc sont particulièrement vulnérables et peuvent être sérieusement affectés à divers types d'attaques compromettant leur performance et leur fiabilité en raison de leur nature décentralisée et de l'absence d'une infrastructure fixe. Les différentes attaques susceptibles d'affecter les réseaux ad hoc comprennent [38][39][40] :

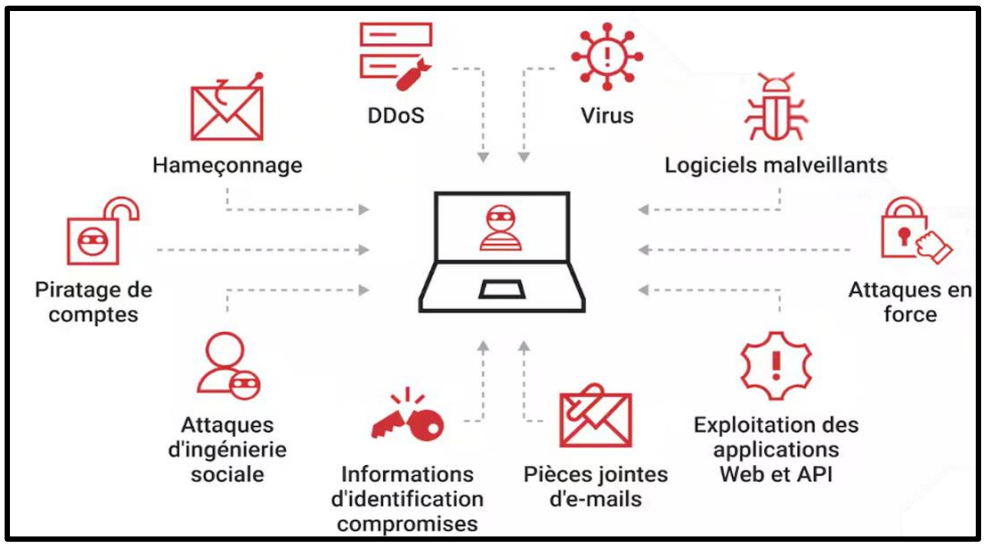


Figure 9 - Les types d'attaques dans les réseaux ad hoc

1. **Phishing** : C'est une attaque qui trompe les utilisateurs pour obtenir des informations sensibles, généralement via des communications frauduleuses qui semblent provenir d'une source fiable.
2. **Attaques DoS et DDoS** : Ces attaques visent à inonder un nœud ou un réseau avec un trafic excessif, rendant le réseau indisponible pour les utilisateurs légitimes.
3. **Attaque MITM** : C'est une cyberattaque qui peut impliquer l'interception de communications entre deux véhicules ou entre un véhicule et une infrastructure routière. L'attaquant peut lire, enregistrer ou manipuler les données échangées.
4. **Attaque par virus** : Un virus informatique est un type de logiciel malveillant qui se propage entre les ordinateurs et cause des dommages aux données et aux logiciels.
5. **Attaque par Malware** : C'est une attaque où le logiciel malveillant effectue des actions non autorisées sur le système de la victime.
6. **Exploitation d'API et d'applications Web** : Cette attaque consiste à trouver et à exploiter des vulnérabilités dans les applications Web.

7. **Attaque par force brute** : C'est une méthode de piratage qui utilise des essais et des erreurs pour craquer des mots de passe, des informations de connexion et des clés de chiffrement.
8. **Attaque par exploitation de références compromises** : Dans ce type d'attaque, des acteurs malveillants utilisent des listes de références compromises pour tenter de se connecter à un large éventail de comptes en ligne.
9. **Attaque par pièces jointes d'e-mails** : Les pièces jointes d'e-mails malveillants sont conçues pour lancer une attaque sur l'ordinateur d'un utilisateur. Les pièces jointes dans ces e-mails malveillants peuvent être déguisées en documents, PDF, et messageries vocales. Les attaquants attachent ces fichiers à des e-mails qui peuvent installer des logiciels malveillants capables de détruire des données et de voler des informations.

Chacune de ces attaques peut avoir un impact significatif sur la sécurité d'un réseau et nécessite des mesures de protection appropriées pour prévenir et atténuer les dommages potentiels.

### 2.3.1 Les attaques dans les VANET

Étant donné que les VANET sont un type des réseaux ad hoc, ils sont vulnérables aux mêmes types d'attaques mentionnées précédemment. Cependant, les attaques telles que : déni de service (DoS) et les attaques de l'homme du milieu (MITM) ont un impact plus significatif et dangereux.[38][39]

Il est important de noter que les attaques MITM peuvent prendre plusieurs formes, y compris les attaques de type trou noir et trou gris, ainsi que les attaques de retard et par altération. Ces attaques peuvent avoir des conséquences graves sur le fonctionnement et la sécurité des VANET, compromettant ainsi la sécurité des données qu'ils transportent. Par conséquent, il est crucial de développer et simuler ces attaques afin de bien comprendre leur impact défavorable [40].

#### 2.3.1.1 Attaque de trou noir (Black Hole) :

Cette attaque se produit lorsqu'un nœud du réseau, supposé transmettre des paquets, les supprime silencieusement, créant un "trou noir" dans le réseau. Cela peut perturber la communication et l'accessibilité du réseau [41][42].

#### 2.3.1.2 Attaque de trou gris (Gray Hole) :

C'est une variante de l'attaque de trou noir. Dans ce cas, un nœud malveillant choisit de rejeter sélectivement les paquets, créant une illusion de fiabilité tout en perturbant le réseau.

#### 2.3.1.3 Attaque par altération (Tampering Attack) :

L'attaque par altération, également connue sous le nom d'attaque de modification, est une forme de menace dans laquelle un attaquant modifie les données transmises, comme les messages de sécurité routière ou les informations de localisation. Cela peut causer des problèmes majeurs, tels que la désorientation des systèmes de navigation ou même des accidents [43][44].

#### 2.3.1.4 Attaque de retard (Delay Attack) :

Cette attaque consiste à introduire délibérément des retards dans la transmission de paquets de données [45]. Ces retards peuvent déstabiliser le fonctionnement normal du réseau et affecter la synchronisation entre différents composants du système [46].

#### 2.3.1.5 Attaque de déni de service (DOS Attack) :

Cette attaque se produit lorsqu'un attaquant surcharge intentionnellement un réseau ou un serveur avec un volume excessif de demandes de données, dans le but de le rendre inopérant. Cela peut entraîner une perturbation majeure de la communication et de la fonctionnalité du réseau [62].

## 2.4 Choix des attaques

Notre choix de développer et de simuler ces types d'attaques spécifiques dans les VANETs est justifié par leur impact potentiel sur la performance et la sécurité du réseau. Voici une justification pour chaque type d'attaque :

1. **Attaque de trou noir (Black Hole)**

Cette attaque est particulièrement pertinente dans le contexte des VANETs car elle peut perturber la communication et l'accessibilité du réseau, ce qui peut avoir un impact direct sur la sécurité routière et la fiabilité des informations de trafic. Par exemple, un véhicule pourrait être amené à prendre une mauvaise direction ou à ignorer un danger imminent sur la route parce que les messages de sécurité routière ont été supprimés par une attaque de trou noir.

P. Remya Krishnan et P. Arun Raj Kumar [47], ont étudié les attaques de trou noir et de trou gris dans les VANETs . Ils ont proposé une approche de sécurité appelée "Smart Blackhole and Gray hole Mitigation (SBGM)" pour détecter et atténuer ces attaques en utilisant une analyse de séries temporelles des paquets abandonnés de chaque nœud.

2. **Attaque de trou gris (Gray Hole)**

Dans les VANETs, cela peut créer une illusion de fiabilité tout en perturbant le réseau, ce qui peut affecter la précision des informations de trafic et de sécurité routière. Par exemple, un véhicule pourrait recevoir des données incorrectes ou incomplètes sur les conditions de trafic ou les dangers potentiels sur la route en raison de l'élimination sélective des paquets par une attaque de trou gris.

Shamim Younas, al.[48] ont proposé une technique basée sur les réseaux neuronaux pour la détection et la prévention des attaques de trou noir et de trou gris dans les réseaux véhiculaires [48].

3. **Attaque par altération (Tampering Attack)**

Cette attaque est particulièrement dangereuse dans les VANETs car elle peut modifier les données transmises, comme les messages de sécurité routière ou les informations de localisation. Cela peut causer des problèmes majeurs, tels que la désorientation des systèmes de navigation ou même des accidents. Par exemple, un véhicule pourrait recevoir des informations de navigation fausses ou des messages de sécurité routière falsifiés en raison d'une attaque par altération. Cela pourrait conduire à des accidents de la route.

Shubha R. Shetty et D. H. Manjaiah ont discuté des différentes attaques de sécurité dans les VANETs, y compris les attaques par altération [49].

4. **Attaque de retard (Delay Attack)**

Cette attaque est pertinente dans les VANETs car elle peut déstabiliser le fonctionnement normal du réseau et affecter la synchronisation entre différents composants du système. Cela peut avoir un impact sur la précision et la fiabilité des informations de trafic et de sécurité routière. Par exemple, un véhicule pourrait recevoir des messages de sécurité routière ou des alertes de trafic avec un retard significatif en raison d'une attaque de retard. Cela pourrait entraîner des réactions tardives à des situations potentiellement dangereuses.

5. **Attaque de déni de service (DOS Attack)**

Cette attaque est particulièrement pertinente dans les VANET car elle peut surcharger un véhicule ou une infrastructure routière avec des messages de sécurité ou d'autres types de données, rendant impossible la réception ou le traitement d'informations vitales. Cela peut entraîner une perturbation majeure de la communication et de la fonctionnalité du réseau, et dans certains cas, cela pourrait même poser un risque pour la sécurité routière. Par exemple, un véhicule pourrait être incapable de recevoir ou de traiter des données vitales en raison d'une surcharge de messages de sécurité ou d'autres types de données causée par une attaque DOS. Cela pourrait entraîner une perturbation majeure de la communication et de la

fonctionnalité du réseau, et dans certains cas, cela pourrait même poser un risque pour la sécurité routière.

Wedad Ahmed et Mourad Elhadef ont présenté une analyse approfondie des formes d'attaque DOS et de leurs impacts dans les VANET. Ils ont classé différents types d'attaques DOS selon les mécanismes de chaque attaque.

R. Gopi, et al.[49] ont également travaillé sur la détection intelligente des attaques DOS avec une technique de contrôle de congestion pour les VANET.

En somme, le choix de ces attaques pour le développement et la simulation est justifié par leur pertinence et leur impact potentiellement dangereux sur les VANET.

## 2.5 Évaluation des risques dans les VANET

Les réseaux ad hoc de véhicules sont des systèmes élaborés présentant des caractéristiques qui peuvent être la cible de diverses attaques. Ces réseaux sont sujets à des vulnérabilités particulières associées aux attaques réseau, considérées comme des éléments de risque. Voici quelques explications supplémentaires :

1. **Fonctionnement des VANET :** Les VANET fonctionnent en permettant la communication entre les véhicules (V2V) ou entre les véhicules et l'infrastructure routière (V2I). Cependant, cette communication ouverte peut être exploitée par des attaques de trou noir et de trou gris, qui perturbent la communication en supprimant ou en retardant les paquets de données. De même, les attaques de déni de service peuvent surcharger le réseau avec du trafic inutile, rendant le réseau totalement inopérant.

2. **Diversité des attaques :** Les VANET sont vulnérables à une gamme diversifiée de menaces. Par exemple, les attaques de trou noir et de trou gris perturbent la

communication en supprimant ou en retardant les paquets de données. D'autre part, l'attaque de modification altère les données en changeant le contenu des paquets de données.

3. **Impact sur la sécurité routière :** Les attaques sur les VANET peuvent avoir un impact direct sur la sécurité routière. Par exemple, une attaque par déni de service peut empêcher la transmission d'informations vitales, comme les alertes de sécurité routière. De même, une attaque par altération peut modifier les messages de sécurité routière, induisant les conducteurs en erreur et compromettant la sécurité routière.

4. **Utilité pour la recherche :** En raison de la diversité des attaques possibles sur les VANET, il est essentiel pour les chercheurs d'avoir accès à un large éventail de scénarios d'attaque. Cela leur permet d'étudier et de développer des mécanismes de défense plus efficaces contre une gamme plus large de menaces potentielles. En incluant une variété d'attaques dans notre package de simulation, nous fournissons un outil précieux pour cette recherche.

En somme, le choix de ces attaques spécifiques offre une couverture complète des menaces potentielles auxquelles les VANET peuvent être confrontés, tout en fournissant un outil utile pour la recherche en sécurité de ces réseaux.

## 2.6 Conclusion

Dans ce chapitre, nous avons examiné en détail les attaques critiques qui ciblent les réseaux ad hoc, avec un accent particulier sur les réseaux ad hoc véhiculaires (VANET). Parmi ces attaques, nous avons mis en évidence les plus dangereuses, notamment l'attaque de "Déni de Service" (DOS) et les attaques de type "Homme au Milieu" (MITM), telles que le "Trou noir", le "Trou gris", l'attaque par "retard" et l'attaque par "altération".
Comprendre ces menaces est essentiel pour analyser leur impact potentiel sur les VANET.

# Chapitre 3

# Conception du modèle simulable

## 3.1 Introduction

Dans ce chapitre, nous explorerons la simulation et son objectif, ainsi que les métriques d'évaluation spécifiques aux réseaux VANET. Nous décrivons les métriques que nous utiliserons pour évaluer l'impact des attaques que nous avons développées. De plus, nous présenterons la conception architecturale globale, incluant les entrées (inputs), les processus et les sorties (outputs).

## 3.2 Le modèle simulable

### 3.2.1 Définition

Un modèle simulable est une représentation simplifiée d'un système réel qui peut être utilisé pour simuler le comportement du système sous différentes conditions. Il est généralement construit à l'aide de logiciels de simulation et peut inclure des variables, des paramètres, des équations et des règles qui décrivent les interactions entre les différentes parties du système.

### 3.2.2 Objectif

L'objectif principal d'un modèle simulable est de fournir un moyen d'explorer et de comprendre le comportement d'un système sans avoir à interagir directement avec le système réel. Cela peut être particulièrement utile lorsque le système réel est complexe, coûteux à

manipuler, ou lorsque des expériences sur le système réel peuvent être dangereuses ou impossibles à réaliser. En utilisant un modèle simulable, les chercheurs peuvent tester différentes hypothèses, prédire les résultats de différentes actions, et obtenir une compréhension plus profonde du fonctionnement du système.

### 3.2.3 Architecture globale

#### 3.2.3.1 Entrées (Inputs) :

1. **Paramètres de simulation :** Ces paramètres définissent les conditions de notre simulation, comme le nombre de véhicules, la durée de la simulation, la taille de la zone de simulation, etc.
2. **Modèles de mobilité :** Ces modèles, utilisés par SUMO, définissent comment les véhicules se déplacent dans la simulation.
3. **Scénarios d'attaque :** Ces scénarios définissent les types d'attaques que nous souhaitons simuler (dans notre cas, les attaques de l'homme du milieu (MITM), et l'attaque de déni de service (DOS)).

#### 3.2.3.2 Processus

1. **OMNET++ :** il est le simulateur de réseau qui utilise INET et exécute la simulation. Il utilise les modèles de mobilité de SUMO et les scénarios d'attaque pour simuler les interactions de réseau dans les réseaux VANET.
2. **SUMO :** il simule les mouvements de véhicules en fonction des modèles de mobilité.
3. **Veins :** il combine les forces de OMNET++ et SUMO pour offrir un ensemble complet de modèles pour la simulation IVC (Inter-Vehicle Communication).

#### 3.2.3.3 Sorties (Outputs)

1. **Résultats de la simulation :** Ces résultats incluent les metrics d'évaluations spécifiques à chaque type d'attaque mentionnées précédemment pour analyser l'impact des attaques sur les réseaux VANET.
2. **Visualisations :** Ces visualisations peuvent inclure des graphiques de performance, des animations de simulation, etc. Elles peuvent aider à comprendre visuellement les résultats de la simulation.

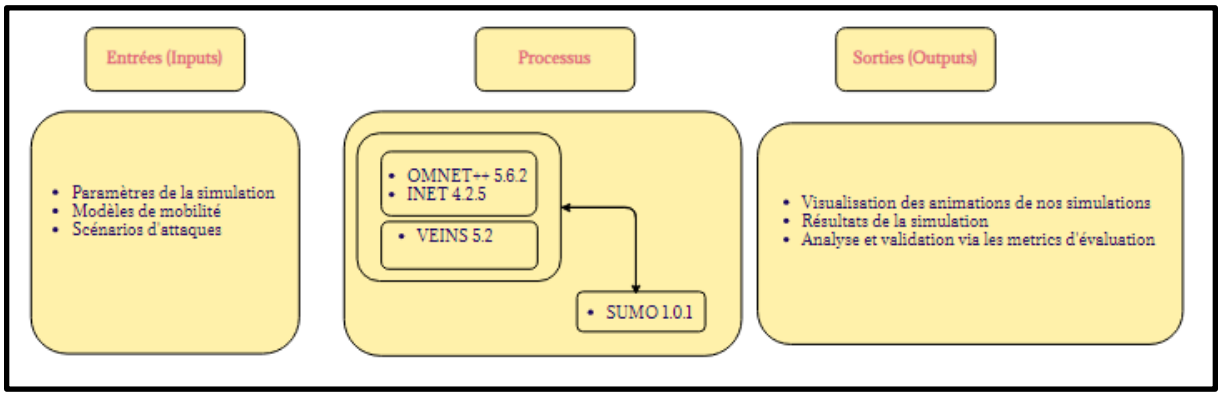


Figure 10 - Architecture globale

## 3.3 La simulation

### 3.3.1 Définition

La simulation est une technique puissante qui permet d'imiter le fonctionnement d'un système réel ou hypothétique. Elle est souvent utilisée lorsque les expériences sur le système réel sont trop coûteuses, dangereuses ou impossibles à réaliser. Les simulations peuvent être réalisées à l'aide de modèles mathématiques, de logiciels informatiques ou de maquettes physiques [50].

### 3.3.2 Objectif

L'objectif d'une simulation peut varier considérablement, allant de la prédiction du comportement d'un système sous certaines conditions, à l'évaluation de ses performances, en passant par la détermination des conditions de son fonctionnement ou l'expérimentation avec ses différentes configurations [50].

Dans le contexte spécifique des réseaux véhiculaires ad hoc (VANET), la simulation joue un rôle crucial. L'objectif principal de la simulation des VANET est de tester et d'évaluer les performances des protocoles de communication, des stratégies de routage et des mécanismes de sécurité avant leur déploiement dans le monde réel. Cela permet aux chercheurs et aux ingénieurs de comprendre comment le réseau se comporte sous différentes conditions de trafic et de détecter et de résoudre les problèmes avant le déploiement réel. De plus, la simulation peut aider à optimiser les performances du réseau en explorant différentes configurations et paramètres [51].

En somme, la simulation est un outil précieux pour la recherche et le développement dans le domaine des VANET, permettant aux chercheurs et aux ingénieurs de tester et d'optimiser les systèmes avant leur déploiement dans le monde réel.

## 3.4 Les métriques d'évaluations

### 3.4.1 Définition

Les métriques d'évaluation sont des indicateurs quantitatifs utilisés pour mesurer et évaluer les performances et la sécurité des réseaux. Elles fournissent une base objective pour comparer différents systèmes ou configurations, et pour identifier les domaines qui nécessitent une amélioration [52].

L'importance des métriques d'évaluation réside dans leur capacité à fournir des informations précises et quantifiables sur le fonctionnement d'un réseau. Par exemple, elles peuvent aider

à déterminer si un réseau est capable de gérer un volume de trafic élevé, si les données sont transmises rapidement et efficacement, ou si le réseau est résistant aux attaques de sécurité.

En ce qui concerne les performances du réseau, certaines métriques couramment utilisées comprennent le débit (le volume de données qui peut être transmis sur une période donnée), la latence (le temps nécessaire pour qu'un paquet de données voyage d'un point à un autre) et la gigue (la variabilité de la latence) [53].

Les métriques d'évaluation sont des outils essentiels pour comprendre et améliorer les performances et la sécurité des réseaux. Elles permettent aux ingénieurs et aux chercheurs de prendre des décisions éclairées et de développer des solutions plus efficaces et plus sûres [54].

### 3.4.2 Les Métriques d'évaluation pour les VANET

Dans le contexte des réseaux ad hoc véhiculaires (VANET), plusieurs métriques spécifiques sont utilisées pour évaluer les performances et la sécurité.
Pour les performances, les métriques couramment utilisées comprennent [55][56][57] :

1. **Le débit** : Il mesure la quantité de données qui peut être transmise dans un délai spécifique. Un débit élevé indique une meilleure performance du réseau. Dans le contexte des VANETs, un débit élevé peut permettre une transmission rapide des informations de sécurité routière entre les véhicules et les infrastructures routières. Par exemple, un débit élevé peut permettre à un véhicule d'envoyer rapidement des informations sur un accident à venir à tous les autres véhicules à proximité.
2. **La latence** : Elle représente le temps nécessaire pour qu'un paquet de données voyage d'un point à un autre dans le réseau. Une latence faible est préférable pour assurer une communication rapide et efficace. Dans les VANETs, une faible latence est cruciale pour assurer une communication rapide et efficace. Par exemple, lorsqu'un véhicule freine brusquement, l'information doit être transmise aux véhicules suivants avec le moins de délai possible pour éviter les collisions.

3. **La densité du réseau** : Elle fait référence au nombre de nœuds dans une zone spécifique, dans notre cas c'est le nombre de véhicules dans une carte géographique. Une densité de réseau élevée peut améliorer la connectivité, mais peut également augmenter le risque de congestion du réseau. Par exemple, dans une zone urbaine dense des réseaux VANET, la densité élevée des véhicules peut permettre une meilleure propagation des informations, mais peut également entraîner une congestion du réseau en raison du grand nombre de messages échangés.

En ce qui concerne la sécurité, nous utilisons les métriques suivantes :

1. **Le taux de détection des intrusions** : Il mesure la capacité du réseau à identifier et à signaler les activités malveillantes. Dans les VANET, cela pourrait signifier la capacité du réseau à identifier et à signaler les véhicules ou les infrastructures routières qui se comportent de manière malveillante, comme un véhicule qui envoie de fausses informations de sécurité routière.
2. **Le taux de faux positifs** : Il représente la proportion de détections d'intrusion qui sont en réalité des événements légitimes. Un taux de faux positifs faible est préférable pour éviter les interruptions inutiles du service réseau. Dans les VANET, un taux de faux positifs faible est préférable pour éviter les interruptions inutiles du service réseau. Par exemple, un véhicule qui change fréquemment de direction ne devrait pas être faussement identifié comme une menace.
3. **Le temps de réponse à l'incident** : Il mesure le temps nécessaire pour répondre à une attaque une fois qu'elle a été détectée. Un temps de réponse rapide peut minimiser les dommages causés par une attaque. Dans les VANET, un temps de réponse rapide peut minimiser les dommages causés par une attaque. Par exemple, si un véhicule est identifié comme une menace, le réseau doit être capable de réagir rapidement pour isoler ce véhicule et minimiser l'impact sur le reste du réseau.

### 3.4.3 Les Métriques d'évaluation pour les attaques

Les attaques de trou noir, trou gris, attaque par altération, l'attaque de retard et l'attaque DOS sont des menaces sérieuses pour la sécurité des réseaux, en particulier dans les réseaux ad hoc

véhiculaires (VANET), perturbant ainsi leur fonctionnement normal. Pour évaluer l'impact de ces attaques, nous pouvons citer les métriques suivantes [58][59][60][61][62] :

1. **Attaque trou noir et l'attaque trou gris** :
   - Nombre de messages supprimés : observer s'il y a croissance du nombre de messages qui sont supprimés par l'attaquant.
   - Taux de livraison de paquets (Packet Delivery Ratio – PDR) : observer s'il y a diminution du pourcentage de paquets qui atteignent leur destination finale.
2. **Attaque de retard (Delay Attack)** :
   - Délai de bout en bout (End to End Delay) : observer s'il y a augmentation du temps nécessaire pour qu'un paquet voyage de la source à la destination.
3. **Attaque Temporing** :
   - Nombre de messages non modifiés : examiner le nombre de messages qui ne sont pas modifiés par l'attaquant.
4. **Attaque DoS (Denial of Service)** :
   - Taux de requêtes malveillantes : mesurer le taux des requêtes malveillantes générées par l'attaquant.
   - Temps de Réponse du Système Cible : observer le temps de réponse du système cible en raison de l'attaque.

Ces métriques nous aideront à quantifier l'impact négatif de chaque attaque sur les performances du réseau VANET.

## 3.5 Conclusion

Ce chapitre a exploré la simulation et son objectif dans le contexte des réseaux VANET. Nous avons examiné les métriques d'évaluation spécifiques que nous utiliserons pour analyser l'impact des attaques que nous avons développées. De plus, nous avons

présenté la conception architecturale globale, en détaillant les entrées (inputs), les processus et les sorties (outputs).

Dans le chapitre qui suit, nous allons présenter une série de simulations relatives aux différentes attaques développées où nous allons discuter et analyser les différents résultats.

# Chapitre 4

# Développement et simulation

## 4.1 Introduction

Pour étudier le comportement des réseaux VANET, il est essentiel d'utiliser des outils de simulation adaptés. Dans ce chapitre, nous explorons le modèle simulable, la simulation ainsi que les différents simulateurs disponibles, notamment ceux dédiés aux réseaux VANET, aux trafics routiers ainsi que les frameworks. De plus, nous justifions notre choix d'outils de simulation en fonction de nos besoins spécifiques. Enfin, nous détaillons les étapes du projet et la mise en œuvre de ces outils et enfin nous abordons la complexité associée.

## 4.2 Les outils de simulation des VANET

Plusieurs outils de simulation pour modéliser et analyser les réseaux VANET ont été développés, chacun offrant des fonctionnalités uniques. Dans ce qui suit, nous allons présenter ces différents types d'outils de simulation.

### 4.2.1 Les simulateurs des réseaux VANET

Ces outils se concentrent sur la simulation des aspects de communication du réseau. Ils permettent de modéliser et de tester les protocoles de communication et les applications pour les VANET. Des exemples de ces outils incluent : OMNET++, GloMoSim, NS-2, NS-3, et JiST/SWANS qui sont considérés comme parmi les meilleurs outils de simulation de réseaux en raison de leurs caractéristiques distinctes et de leur large adoption dans la communauté de recherche. Chacun a ses propres forces et est adapté à différents types de projets [63] :

1. **OMNET++ (Objective Modular Network Testbed in C++) :** est un simulateur de réseaux à événements discrets, modulaire et extensible, utilisé principalement pour la recherche et le développement dans les domaines des réseaux de communication, des systèmes embarqués et des systèmes distribués. Il dispose d'une interface graphique avancée pour la configuration, le débogage et la visualisation des simulations, et supporte de nombreux frameworks spécialisés comme INET et Veins.

2. **GloMoSim (Global Mobile Information System Simulator) :** est un simulateur de système d'information mobile global. Il est conçu pour modéliser et simuler des réseaux de communication sans fil à grande échelle, permettant l'étude de divers protocoles de communication et de routage dans des environnements mobiles.

3. **NS-2 (Network Simulator 2) :** est un simulateur de réseaux à événements discrets largement utilisé dans la recherche académique pour la simulation de protocoles réseau filaires et sans fil. Il est reconnu pour sa large gamme de protocoles supportés et sa longue histoire de validation par la communauté de recherche, bien que son interface soit principalement basée sur des scripts.

4. **NS-3 :** est la version succédant à NS-2, offrant une architecture plus moderne et flexible pour la simulation de réseaux à événements discrets. Il est écrit en C++ avec des interfaces Python et est utilisé pour des simulations réseau précises et d'haute-fidélité, supportant une large gamme de protocoles modernes.

5. **JiST/Swans (Java in Simulation Time / Scalable Wireless Ad hoc Network Simulator) :** JiST est un moteur de simulation basé sur Java qui utilise le concept de temps de simulation pour exécuter des simulations à événements discrets. SWANS est une extension de JiST pour la simulation de réseaux sans fil ad hoc de capteurs, offrant une grande scalabilité et des performances optimisées dans un environnement Java.

### 4.2.2 Les simulateurs de trafic routier :

Ces outils se concentrent sur la simulation des mouvements des véhicules sur la route. Ils permettent de modéliser le comportement des conducteurs, les conditions de circulation, et d'autres aspects liés au trafic routier [63] :

1. **SUMO (Simulation of Urban MObility) :** est un simulateur de trafic open source qui permet de modéliser et de simuler des flux de trafic dans des environnements urbains et interurbains. Il est utilisé pour étudier et évaluer les performances des systèmes de transport, les stratégies de gestion du trafic et les technologies de transport intelligentes.

2. **MOVE (Mobility model generator for VANETs) :** MOVE est un générateur de modèles de mobilité spécifiquement conçu pour les réseaux ad hoc véhiculaires (VANET). Il permet de créer des modèles de mobilité réalistes pour les véhicules dans des environnements routiers, ce qui est essentiel pour évaluer les performances des protocoles de communication dans les VANET.

3. **CORSIM (CORridor Simulation) :** est un simulateur de trafic routier développé par le Federal Highway Administration (FHWA) des États-Unis. Il est utilisé pour modéliser et simuler le trafic routier à l'échelle des corridors routiers, en tenant compte des interactions entre les véhicules et les infrastructures.

4. **VISSIM (Verkehr In Städten - SIMulationsmodell) :** est un logiciel de simulation de trafic routier développé par la société allemande PTV Group. Il est largement utilisé pour modéliser et simuler le trafic dans des environnements urbains et routiers, permettant aux planificateurs de transport de tester des scénarios de circulation, d'évaluer les performances des routes et de concevoir des intersections.

Ces simulateurs sont largement utilisés dans l'industrie et la recherche pour étudier le comportement du trafic routier, évaluer les projets d'infrastructures de transport, et développer des stratégies de gestion du trafic. Chacun a ses propres caractéristiques et avantages, et le choix entre eux dépend des besoins spécifiques de la simulation et des préférences de l'utilisateur.

### 4.2.3 Les frameworks

Ces outils combinent les simulateurs de réseaux et de trafic routier pour fournir une simulation plus complète des VANET. Ils permettent de simuler à la fois les aspects de communication du réseau et les mouvements des véhicules sur la route. Voici les frameworks qui sont couramment utilisés [64] :

1. **VEINS (Vehicles in Network Simulation) :** est un framework open source qui permet la simulation de réseaux de véhicules ad hoc (VANET) dans OMNET++. Il est largement utilisé pour la modélisation et la simulation de communications véhiculaires dans des environnements urbains et routiers. VEINS offre une intégration étroite avec SUMO pour la simulation du trafic routier, ce qui en fait un choix populaire pour les projets de recherche dans le domaine des VANET.

2. **VANETMobiSim :** est un framework de simulation de réseaux de véhicules ad hoc développé pour NS-2. Il permet la modélisation et la simulation de scénarios de communication dans des réseaux de véhicules, en utilisant des modèles de mobilité spécifiques pour simuler le mouvement des véhicules. VANETMobiSim est souvent utilisé dans des environnements de recherche où NS-2 est préféré pour la simulation de protocoles de communication.

3. **SimuLTE (Simulation of Long Term Evolution)** : est un framework open source pour la simulation de réseaux LTE (Long Term Evolution) dans OMNET++. Bien qu'il ne se concentre pas spécifiquement sur les VANET, il peut être étendu pour inclure des fonctionnalités de VANET en utilisant des modules supplémentaires pour

la simulation de la mobilité des véhicules et des communications V2V (Vehicle-to-Vehicle) et V2I (Vehicle-to-Infrastructure).

Ces outils de simulation sont essentiels pour la recherche sur les VANET car ils nous permettent de comprendre et d'analyser les défis uniques que présentent ces réseaux. Ils offrent un environnement contrôlé où les paramètres peuvent être ajustés pour étudier leur impact sur les performances du réseau. Ils sont utilisés par les chercheurs et les ingénieurs du monde entier pour améliorer la sécurité, l'efficacité et la fiabilité des VANET.

## 4.3 Choix des outils de simulation et justification

Dans le cadre de notre projet, nous prévoyons de développer et simuler un plug-in d'attaques au sein des réseaux VANET. Pour cela nous allons utiliser les outils suivants : OMNET++, SUMO et VEINS. Notre choix d'utiliser ces outils pour notre projet peut être justifié de plusieurs façons :

1. **Simulateur de réseaux VANET : OMNET ++**

- Modularité et flexibilité : OMNET++ est très modulaire et extensible, permettant de construire et de modifier facilement des simulations de réseaux de communication complexes. Il permet aussi de créer des modèles personnalisés et de les étendre, ce qui est essentiel pour modéliser des véhicules légitimes et des attaquants.
- Support pour les simulations réseaux : OMNET++ est spécifiquement conçu pour les simulations de réseaux, facilitant la modélisation des communications entre véhicules.
- Interface Graphique : Dispose d'une interface utilisateur graphique avancée pour la configuration, le débogage et la visualisation des simulations.
- Frameworks spécialisés : Supporte de nombreux frameworks et bibliothèques, comme INET, VEINS, et Castalia.
- Communauté Active : OMNET++ a une large communauté d'utilisateurs avec de nombreuses ressources, tutoriels et modules disponibles.

- Documentation : OMNET++ offre une documentation complète, abondante et bien structurée, ce qui facilite le développement et le dépannage.

- OMNET++ est utilisé pour des projets nécessitant une visualisation avancée et une analyse détaillée des résultats.

**2. Simulateur de trafic routier : SUMO**

- Open Source : SUMO est un logiciel open source. Cela permet une personnalisation avancée, des extensions et des contributions à la communauté, et garantit une transparence et une fiabilité accrues.
- Ajustement et extensibilité : SUMO permet de créer des scénarios de trafic personnalisés et d'ajuster les paramètres selon les besoins de la simulation.
- Précision et réalisme : SUMO permet de simuler des scénarios de trafic complexes avec une grande précision, représentant fidèlement la dynamique du trafic dans n'importe quelle ville.
- Flexibilité et modularité : SUMO est hautement flexible et modulaire, ce qui signifie que nous pouvons personnaliser et adapter la simulation en fonction de nos besoins spécifiques. Comme nous pouvons modéliser différents types de véhicules, d'infrastructures routières et de scénarios de trafic, ce qui est crucial pour des projets de recherche avancés.
- Modélisation détaillée : SUMO offre une modélisation détaillée des mouvements de véhicules, des interactions avec les piétons, des feux de signalisation, etc. Cette précision permet des simulations réalistes et permet d'évaluer de manière précise l'impact des attaques ou des perturbations sur le trafic routier.
- Large Communauté et Support Actif : SUMO bénéficie d'une large communauté d'utilisateurs et de développeurs, avec des ressources, des forums de discussion et une documentation extensive disponibles en ligne. Cela facilite l'apprentissage, le dépannage et la résolution des problèmes éventuels.

- Interfaçage avec OMNET++ : La capacité de SUMO à s'intégrer avec OMNET++ via le serveur TraCI (Traffic Control Interface) permet de synchroniser les mouvements des véhicules avec les événements de communication dans OMNET++.
- Interopérabilité avec OMNET++ : SUMO est conçu pour être facilement intégré avec d'autres simulateurs, y compris OMNET++. Cette interopérabilité permet une simulation combinée du trafic routier et des réseaux de communication, ce qui est particulièrement avantageux pour notre projet qui nécessite une analyse de l'impact des attaques sur les réseaux VANET (Vehicular Ad hoc Networks).
- VISSIM et CORSIM ne sont pas directement conçus pour être intégrés avec OMNeT++ de la même manière que SUMO peut l'être.

**3. Framework : VEINS**

- Intégration avec SUMO : Veins utilise SUMO pour simuler de manière réaliste les mouvements des véhicules dans un environnement urbain, ce qui est crucial pour représenter fidèlement n'importe quelle carte de route.
- Fonctionnalités V2V et V2I : Veins offre des modules préexistants pour les communications véhicule-à-véhicule (V2V) et véhicule-à-infrastructure (V2I), réduisant le besoin de développement de base.
- Support pour les Scénarios de Sécurité : Veins permet de modéliser des scénarios de sécurité et des attaques, ce qui est directement pertinent pour notre projet.
- Pour les projets qui utilisent OMNET++, VEINS est souvent préféré en raison de son intégration étroite avec OMNET++ et SUMO, offrant ainsi une solution complète pour la simulation de VANET.

La combinaison OMNET++, SUMO et VEINS offre une solution intégrée et spécialisée pour la simulation des VANET avec une forte communauté de support, une flexibilité élevée et des outils puissants pour la visualisation et l'analyse des résultats. Ces caractéristiques justifient pleinement nos choix par rapport aux outils similaires disponibles.

En somme, l'utilisation de OMNET++, SUMO et Veins nous permet de simuler avec précision les interactions de réseau et les mouvements de véhicules dans les réseaux VANET, ce qui est essentiel pour comprendre l'impact des attaques sur ces réseaux.

## 4.4 Environnement de développement

Dans cette section, nous décrivons les divers outils et ressources que nous avons utilisés pour accomplir les différentes composantes de notre projet.

Notre station de développement était un ordinateur portable DELL Inspiron 15, doté d'un processeur Intel Core i3, de 4 Go de mémoire vive et d'une version 64 bits de Windows 10 Pro.

Pour le développement des fichiers de configuration en XML, nous avons fait appel à Microsoft Visual Studio Code.

De plus, nous avons profité du forum OMNeT++ sur Github[1] pour poser des questions et consulter les réponses aux problèmes rencontrés par d'autres utilisateurs. Cela a été une ressource précieuse pour résoudre les défis que nous avons rencontrés lors de la réalisation de notre projet.

## 4.5 Etapes de projet

Dans cette section, nous allons décrire en détails les étapes que nous avons suivies pour réaliser ce projet.

### 4.5.1 Installation des outils de simulation

Comme mentionné précédemment, nous avons choisi certains outils de simulation qui répondent à nos besoins : OMNET++, SUMO et VEINS. Cependant, lors de leur installation, il est crucial de vérifier attentivement leurs versions. Contrairement à tous les outils, ceux que

[1] https://github.com/omnetpp/omnetpp

nous allons utiliser doivent être compatibles entre eux pour fonctionner correctement ensemble et garantir des résultats cohérents et fiables.

- OMNET++ : Nous avons utilisé la version 5.6.2. [2]
- INET Framework : La version que nous avons utilisée est 4.2.5.[3]

INET Framework est un élément essentiel pour le bon fonctionnement de OMNET++. En tant que suite de modèles open-source, il fournit des modèles, des exemples, des tutoriels et de la documentation pour les protocoles filaires et sans fil. Grâce à INET, nous pouvons simuler et étudier divers scénarios de réseaux, ce qui contribue à la robustesse et à la fiabilité de OMNET++.

- SUMO : la version utilisée est 1.0.1.[4]
- VEINS : La version utilisée est 5.2.[5]

### 4.5.2 Configuration

Une fois que le processus d'installation de OMNET++ est achevé avec succès, une étape cruciale consiste à s'assurer de son bon fonctionnement. Pour ce faire, nous pouvons procéder à l'exécution de l'exemple intégré nommé "aloha". Cet exemple constitue un excellent moyen de tester les fonctionnalités de base de OMNET++. Les figures de 11 à 15 dans l'annexe A illustrent la procédure d'exécution de cet exemple, offrant ainsi une visualisation claire et détaillée de la démarche à suivre. Cette vérification permet de confirmer que l'installation a été réalisée correctement et que OMNET++ est prêt à être utilisé pour nos simulations futures.

---

[2] OpenSim Ltd. (s.d). OMNeT++ simulateur d'événements discrets. Récupéré de : https://omnetpp.org/download/old

[3] INET Framework. (2021, 18 mai). INET 4.2.5 publié. Récupéré de : https://inet.omnetpp.org/2021-05-18-INET-4.3.2-released.html

[4] German Aerospace Center (DLR). (s.d). SUMO - Simulation de la mobilité urbaine. Récupéré de : https://sumo.dlr.de/docs/Downloads.html

[5] Sommer, C., & German, R. (s.d).Veins : Simulation de réseaux de véhicules. Récupéré de : https://veins.car2x.org/documentation/install/

Une fois que nous avons validé le fonctionnement optimal de OMNET++, la prochaine étape cruciale consiste à importer le framework INET. Ce framework, essentiel pour nos simulations de réseaux, doit être correctement intégré à notre environnement OMNET++. Après l'importation du framework NET, nous devons procéder à l'opération de "Build Project". Il est important de noter que cette opération peut être assez longue, car elle implique la compilation de nombreux fichiers sources. Cependant, cette étape est indispensable pour garantir que notre projet est prêt à être exécuté sans erreurs. Patience et vigilance sont donc de mise lors de cette phase.

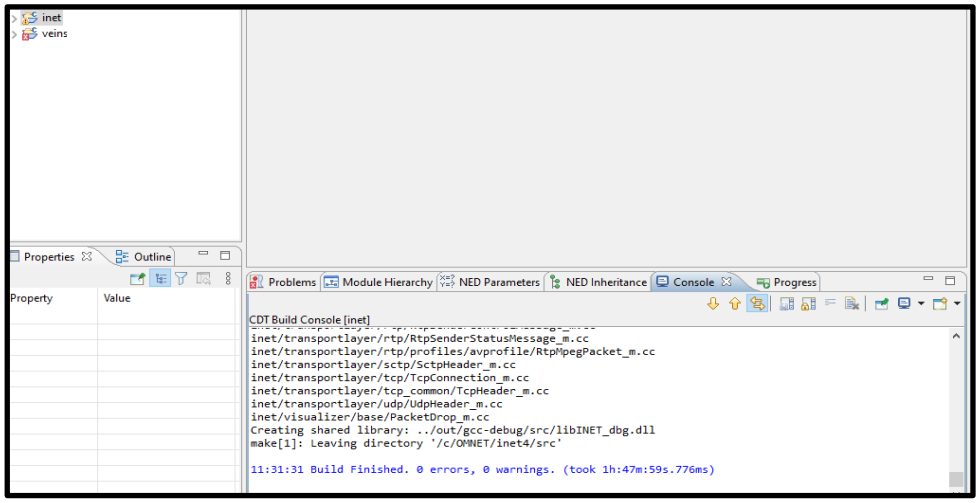


Figure 16 - Importation et compilation du framework INET

Afin de confirmer le bon fonctionnement du framework INET, une étape essentielle consiste à exécuter un exemple spécifique nommé "aodv". Cette démarche nous permet non seulement de tester les fonctionnalités de base d'INET, mais aussi de nous familiariser avec son interface et ses mécanismes de fonctionnement. La figure ci-dessous illustre précisément comment procéder à cette exécution. Elle offre une représentation visuelle claire et détaillée de la procédure, facilitant ainsi la compréhension et l'application de cette étape cruciale.

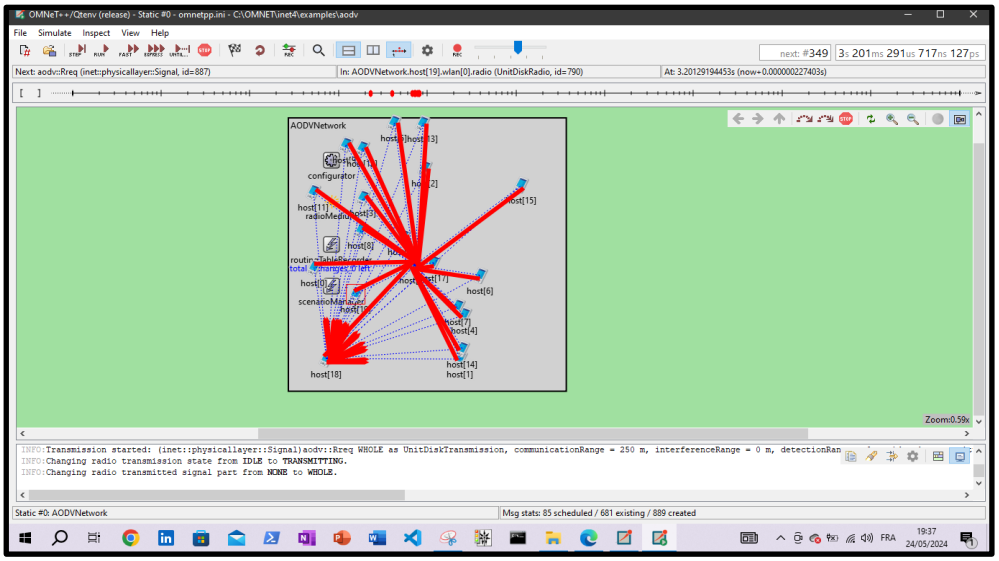


Figure 17 - Simulation de l'exemple aodv du framework INET

En empruntant la même procédure que celle que nous avons suivie pour le framework INET, il est maintenant nécessaire d'importer le framework VEINS dans notre environnement de travail OMNET++. VEINS, un framework clé pour la simulation des VANET, doit être correctement intégré pour permettre une simulation précise et efficace.

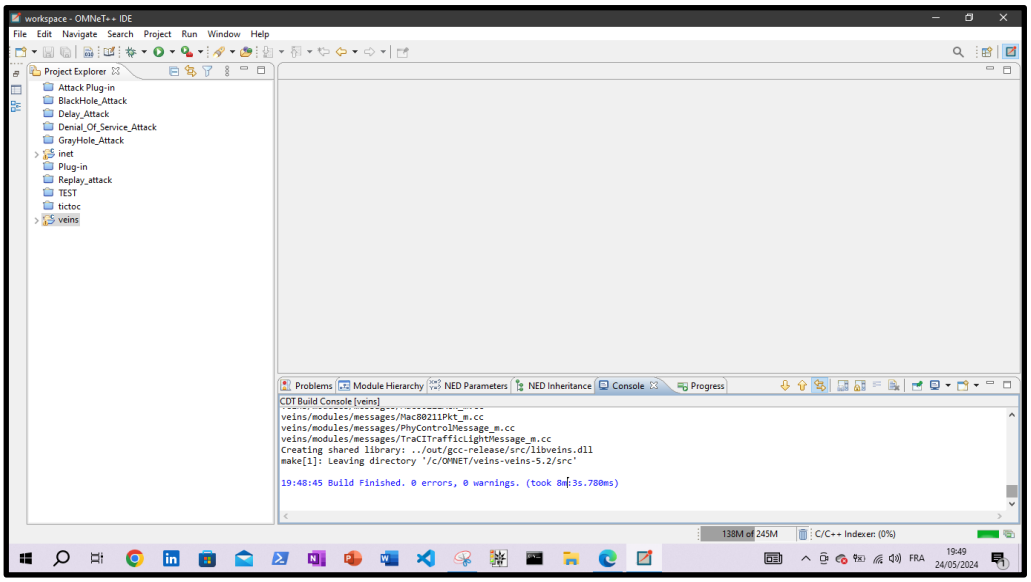


Figure 18 - Importation et compilation du framework VEINS

Afin de confirmer que le framework VEINS a été correctement intégré et fonctionne comme prévu, nous allons exécuter un exemple spécifique : la simulation de la ville d'Erlangen. Cet exemple, intégré dans VEINS, nous permet de visualiser une simulation des VANET dans un environnement urbain réaliste. La figure ci-dessous illustre le processus d'exécution de cette simulation.

Tout d'abord nous devons lancer le démon de lancement de VEINS avec un niveau de journalisation détaillé et lui demander d'exécuter SUMO, comme le montre la figure 19. Cela permet à OMNET++ et SUMO de communiquer entre eux pendant la simulation.

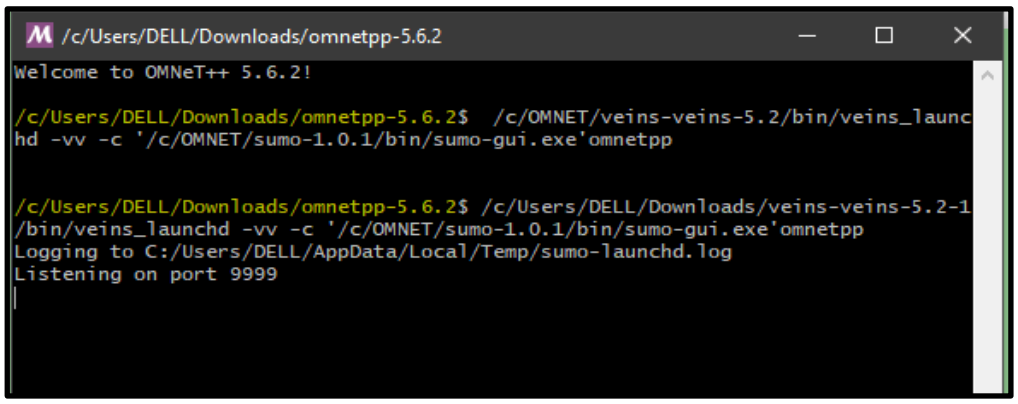


Figure 19 - Démon de lancement de VEINS

Dès que le processus d'écoute est activé sur le port 9999, la simulation, centrée sur le mouvement des voitures dans la ville d'Erlangen, commence à se dérouler, créant un environnement dynamique et interactif. Comme illustré dans la figure 20, vous pouvez observer le déroulement en temps réel de cette simulation complexe, offrant une représentation visuelle de la circulation des véhicules dans la ville.

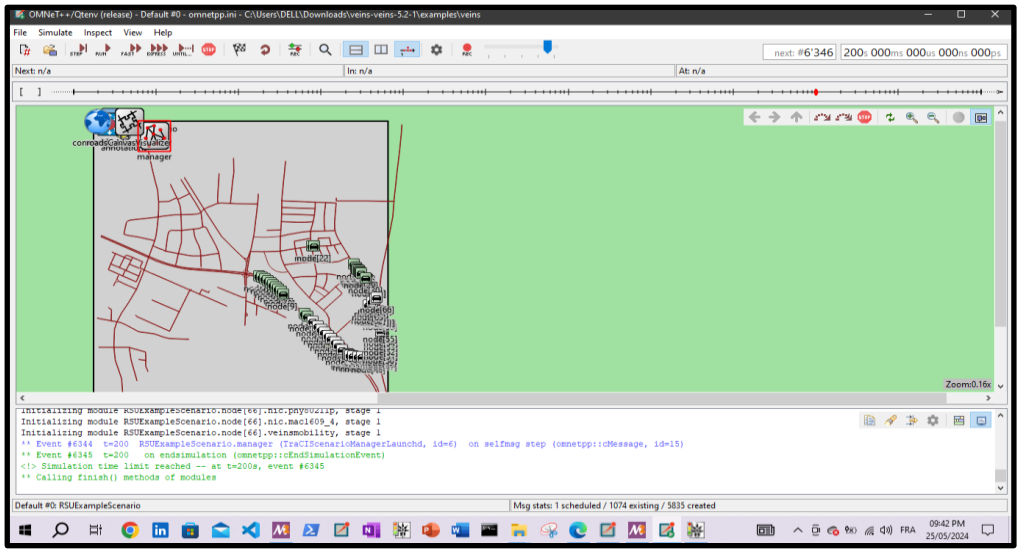

Figure 20 - La simulation du réseau VANET de la ville d'Erlangen

Et voilà, dès que la simulation est lancée, l'interface de SUMO apparaît automatiquement. C'est un moment clé du processus, car c'est à ce moment que nous pouvons commencer à observer et à interagir avec la simulation en temps réel. L'interface de SUMO offre une visualisation graphique de la simulation, permettant de suivre le mouvement des véhicules dans la ville d'Erlangen.

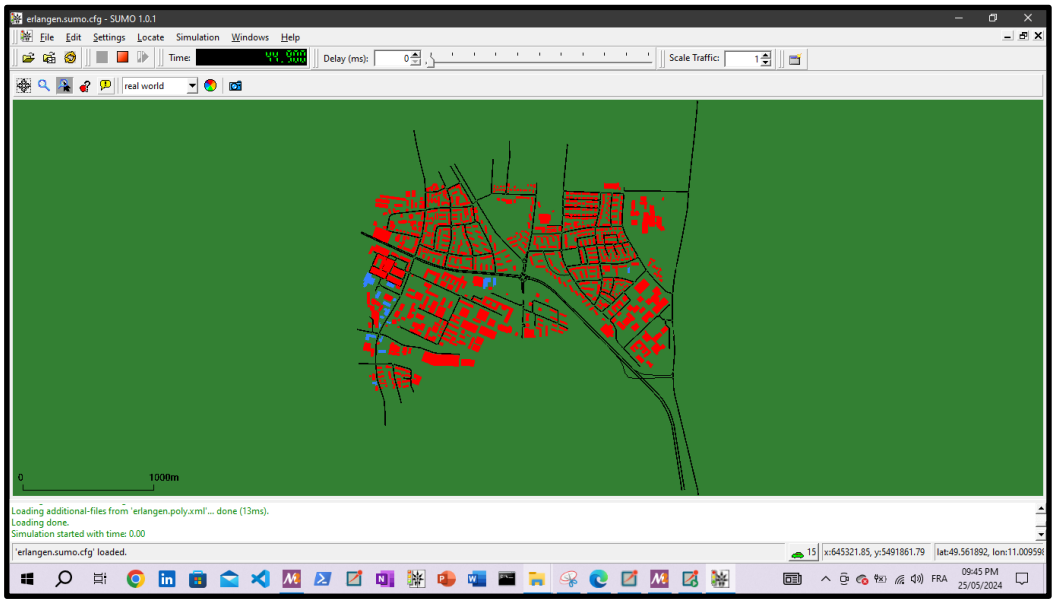

Figure 21 - La simulation de la ville Erlangen dans SUMO

### 4.5.3 Développement et simulation des attaques

Après avoir franchi avec succès l'étape cruciale de la mise en œuvre conjointe de tous les outils nécessaires, y compris OMNET++, SUMO et VEINS, nous sommes maintenant prêts à passer à la phase suivante de notre projet. Cette phase concerne le développement de notre propre package d'attaque. C'est une étape passionnante et complexe qui nécessite une compréhension approfondie des réseaux ad hoc de véhicules et des différentes formes d'attaques potentielles. Nous allons concevoir, coder et tester diverses attaques dans le but d'observer et d'analyser leur impact négatif.

1. Attaque de trou noir (Black hole attack)

Comme mentionné précédemment (voir section 2.3.1.1) cette attaque se produit lorsqu'un nœud malveillant intercepte les paquets de données et les supprime. Le taux de perte de paquets et le taux de livraison de paquets sont des métriques clés que nous utilisons pour évaluer l'impact de cette attaque.

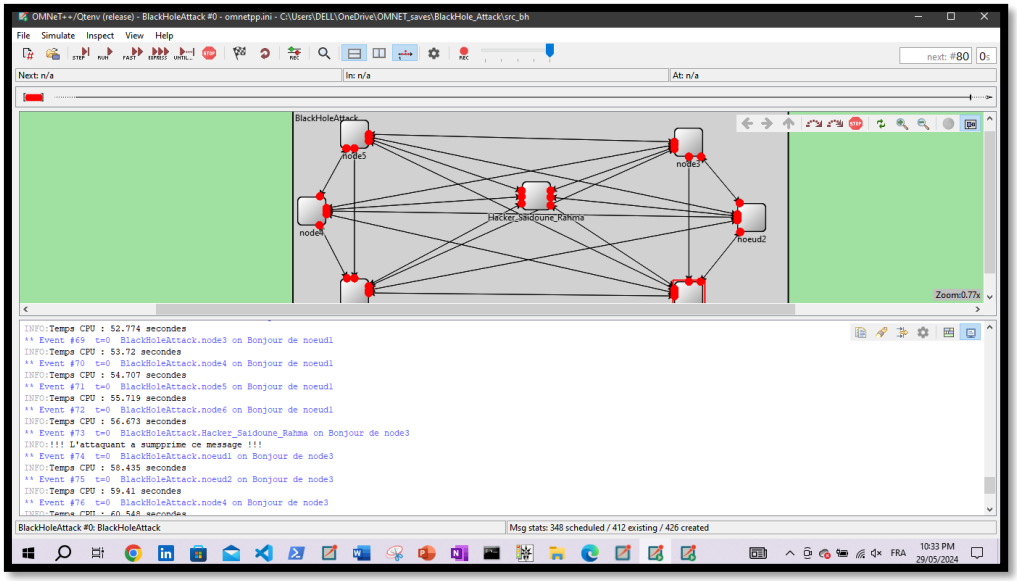


Figure 22 - Simulation de l'attaque Trou noir

2. Attaque de trou gris (Gray hole attack)

Dans cette attaque, un nœud malveillant alterne entre les comportements honnêtes et malveillants, ce qui rend sa détection difficile (voir section 2.3.1.2). Le taux de perte de paquets et le taux de livraison de paquets vont nous aider à évaluer l'efficacité de l'attaque.

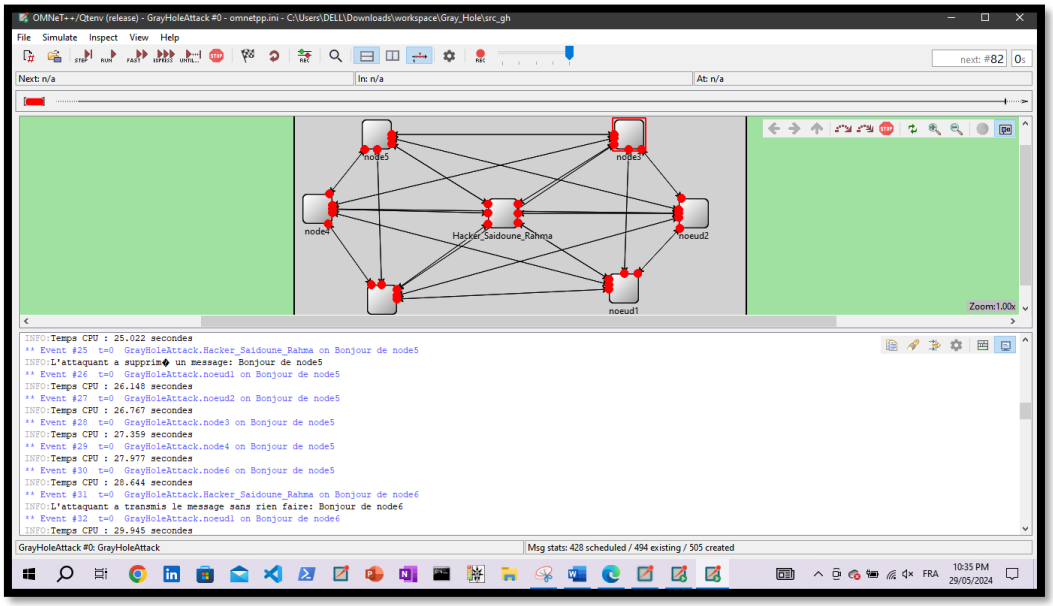


Figure 23 - Simulation de l'attaque Trou gris

3. Attaque de retard (Delay attack)

Cette attaque (voir section 2.3.1.4) se produit lorsqu'un attaquant retarde intentionnellement la transmission de paquets. Le délai de bout en bout (End to end delay), fait référence au temps qu'il faut pour qu'un paquet de données arrive à sa destination, est une métrique pertinente pour évaluer cette attaque.

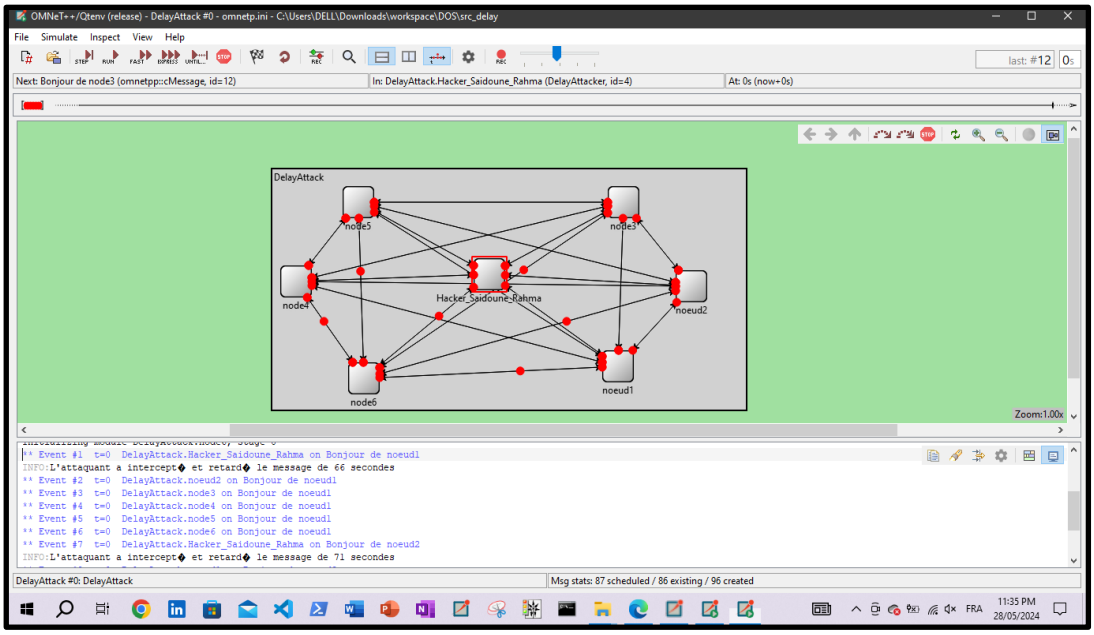


Figure 24 - Simulation de l'attaque de retard

4. Attaque par altération (Tampering attack)

Dans cette attaque (voir section 2.3.1.3), un attaquant modifie les paquets de données et les transmet. Le nombre de messages non modifiés est une métrique clé pour évaluer cette attaque.

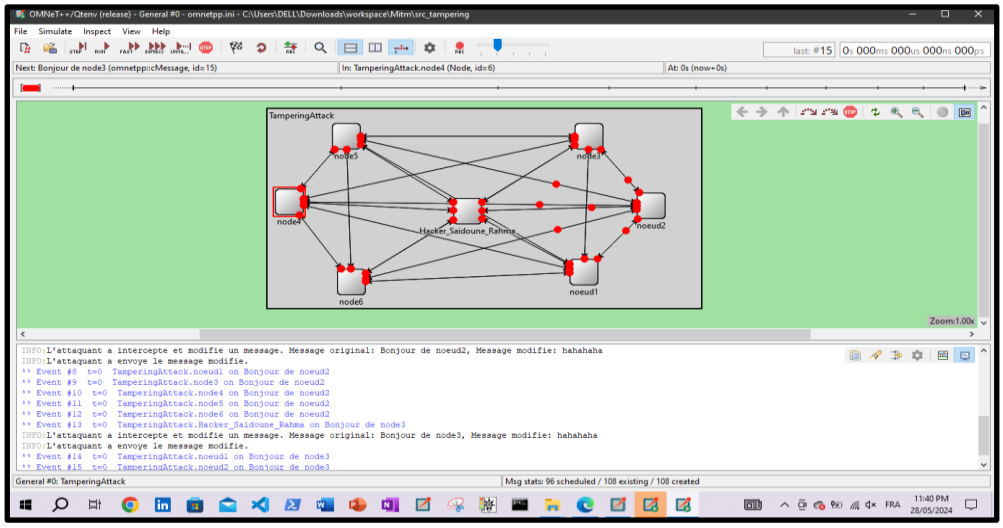


Figure 25 - Simulation de l'attaque par altération

5. Attaque de déni de service (DOS attack)

Dans cette attaque (voir section 2.3.1.5), l'attaquant envoie plusieurs messages dans le but de submerger la cible et de perturber son fonctionnement normal. Il est important de noter que l'exécution de cette attaque peut être très exigeante en termes de ressources. En effet, si l'ordinateur utilisé pour la simulation n'est pas suffisamment performant, l'environnement peut ralentir et parfois, le Qtenv d'OMNET++ peut cesser de répondre. Le nombre de messages envoyés par l'attaquant et le temps de réponse de la cible sont des métriques que nous allons utiliser pour analyser l'impact de cette attaque. Cela souligne l'importance d'avoir un système informatique capable de gérer la charge de travail associée à la simulation de ces attaques.

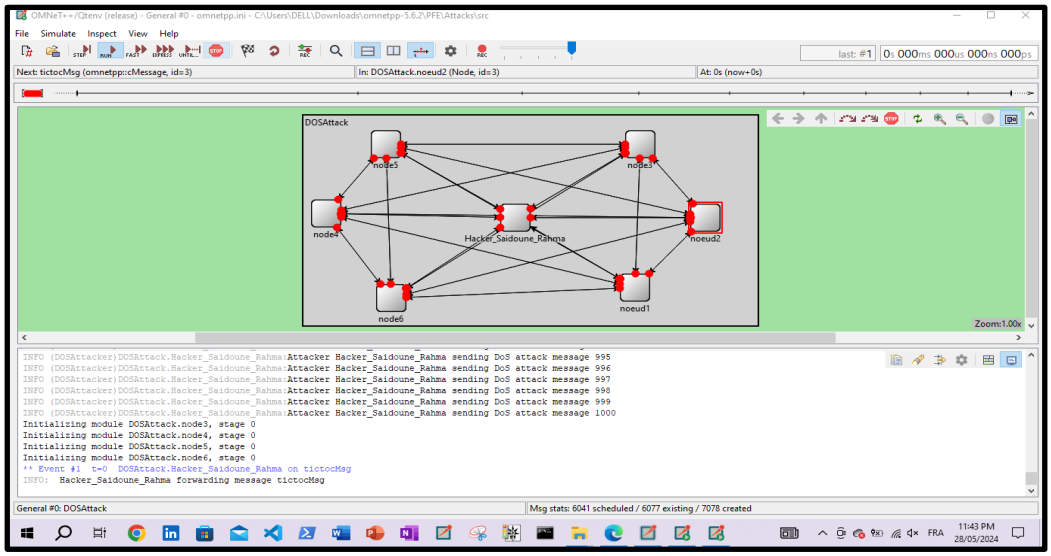


Figure 26 - Simulation de l'attaque de déni de service

### 4.5.4 Développement et simulation du trafic urbain

Dans le cadre de notre projet de recherche sur les réseaux ad hoc de véhicules (VANET), nous avons mis en œuvre une simulation de trafic sur une autoroute à double sens, comme le montre la figure suivante :

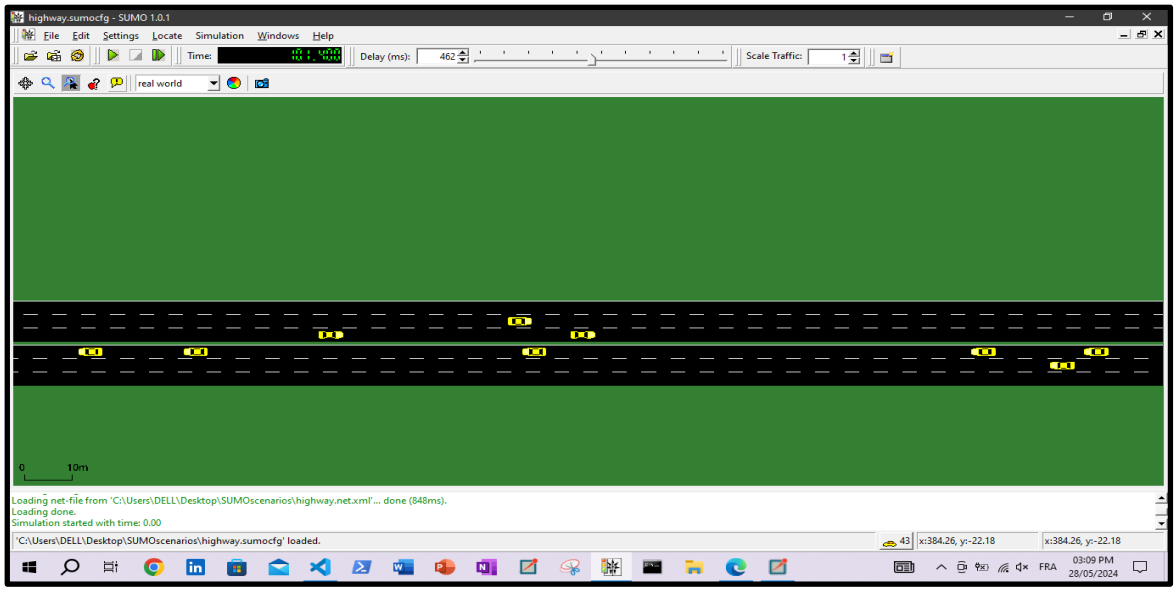


Figure 27 - Simulation d'une autoroute

De plus, nous avons également effectué une simulation complexe de la ville Manhattan avec SUMO et VEINS en utilisant l'outil OSM Wizard pour générer la carte géographique. Cet outil a permis de générer un modèle détaillé de la ville, comprenant un grand nombre d'intersections et une densité de trafic élevée.

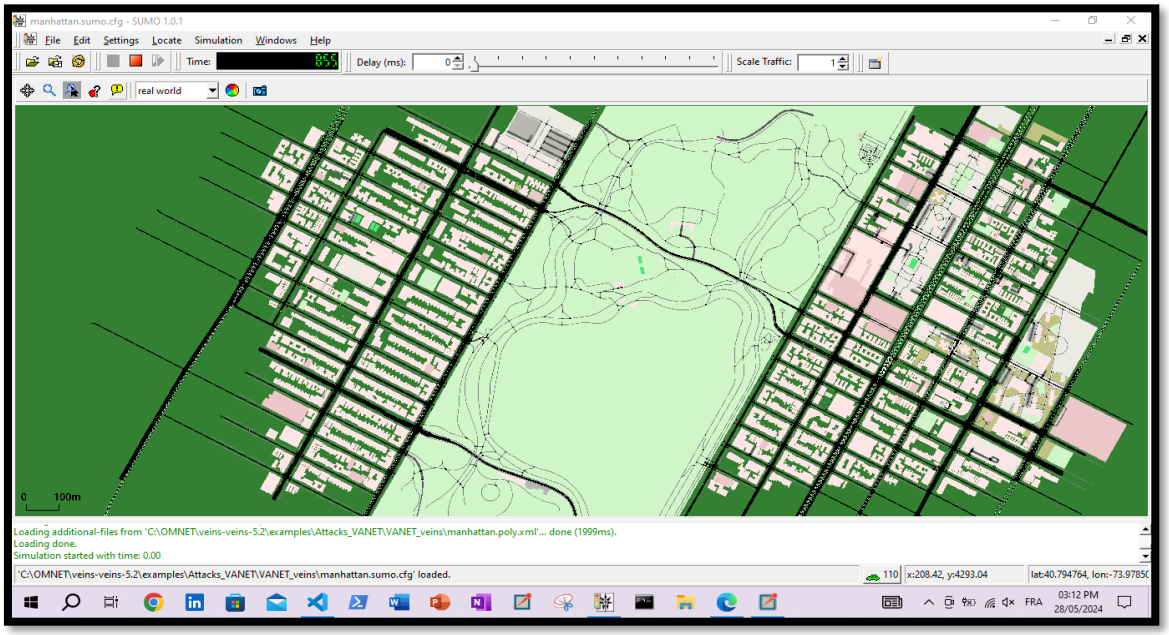


Figure 28 - la simulation de la ville Manhattan

Ces simulations ont été essentielles pour évaluer les performances de notre système VANET dans divers scénarios de trafic et conditions environnementales. Les résultats obtenus ont fourni des informations précieuses pour l'amélioration continue de notre système.

## 4.6 Analyse des résultats

### 4.6.1 Analyse de résultats de l'attaque de trou noir

Voici un tableau qui présente nos résultats :

| Numéro de l'événement | Action de l'attaquant | Message Supprimé |
|---|---|---|
| 1 | Message supprimé | Bonjour de noeud1 |
| 7 | Message supprimé | Bonjour de noeud2 |
| 13 | Message supprimé | Bonjour de node3 |
| 19 | Message supprimé | Bonjour de node4 |
| 25 | Message supprimé | Bonjour de node5 |
| 31 | Message supprimé | Bonjour de node6 |
| 37 | Message supprimé | Bonjour de noeud2 |
| 43 | Message supprimé | Bonjour de node3 |

Tableau 1 - Résultats de la simulation de l'attaque trou noir

Le PDR (voir section 3.4.3) est un indicateur clé de la performance du réseau, car il mesure le pourcentage de paquets qui sont effectivement livrés à leur destination par rapport au nombre total de paquets envoyés. Le nombre de paquets supprimés donne une indication de l'efficacité de l'attaque du trou noir. Une augmentation significative de ce nombre indique une attaque réussie.

En comptant le nombre total d'événements impliquant des messages envoyés (sans tenir compte des suppressions) : 79 événements.

Les messages supprimés par l'attaquant En total, 14 messages ont été supprimés.

Dans notre réseaux chaque nœud (il y en a 7 : noeud1, noeud2, node3, node4, node5, node6, et Hacker_Saidoune_Rahma) envoie un message de "Bonjour" à chaque autre nœud une fois. Donc, pour chaque nœud, il y a 6 messages envoyés à ces voisins.

- Nombre total de messages envoyés : $7 \times 6 = 427 \times 6 = 42$
- Nombre de messages supprimés : 14

Le nombre de messages reçus serait alors :

- Messages reçus = Message envoyés – Messages supprimés
- Messages reçus = 42 – 14 = 28

Le PDR peut être calculé comme suit :

- PDR = ( Messages reçus / Messages envoyés ) * 100 = ( 28 / 42 ) *100
- PDR = 66.67 %

Le PDR de 66.67% indique qu'environ un tiers des messages ont été perdus à cause de l'attaque trou noir. Cela montre que cette attaque a eu un impact significatif sur la communication dans le réseau, réduisant la fiabilité du réseau en termes de livraison de paquets.

En comprenant ces résultats, les chercheurs peuvent développer des stratégies pour renforcer la sécurité et la résilience des VANET face à de telles attaques.

### 4.6.2 Analyse de résultats de l'attaque de retard

Pour analyser l'impact de l'attaque de retard (Delay Attack), nous avons examiné les logs générés par OMNET++ ainsi que les logs que nous avons enregistrés sous forme de fichier texte.

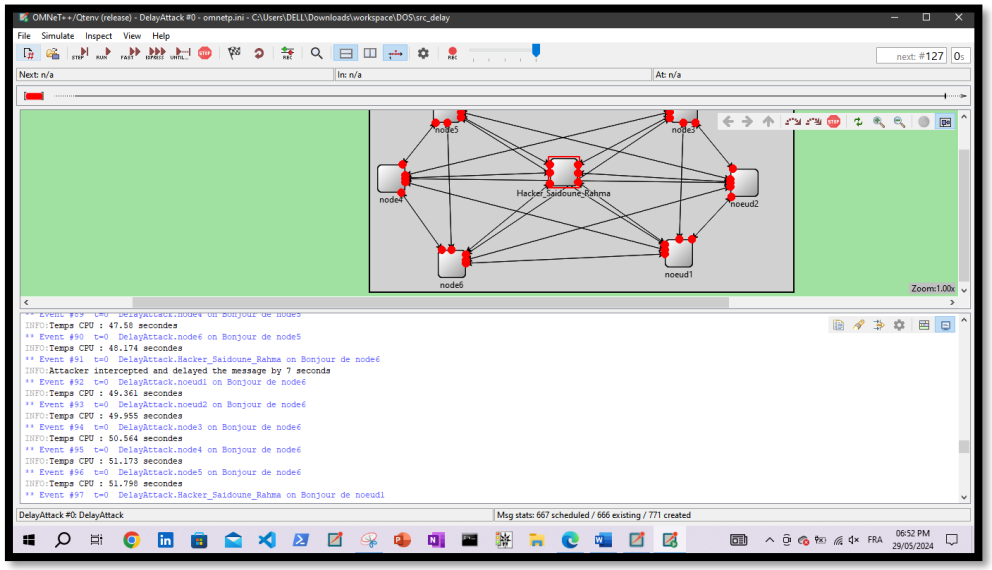


Figure 30 - Les logs de l'attaque de retard sur OMNET++

Les métriques importantes ici sont le temps de retard introduit par l'attaquant, les temps de CPU des différents nœuds au moment de la réception des messages, ainsi que les sources et destinations des messages.

Voici un résumé des événements pertinents capturés dans les logs :

| Événement | Message | Temps de retard introduit (s) | Temps CPU (s) |
|---|---|---|---|
| 1 | Bonjour de noeud1 | 66 | 5.686 |
| 7 | Bonjour de noeud2 | 71 | 7.545 |
| 13 | Bonjour de node3 | 86 | 9.311 |
| 19 | Bonjour de node4 | 101 | 11.437 |
| 25 | Bonjour de node5 | 72 | 13.468 |
| 31 | Bonjour de node6 | 103 | 15.866 |
| 37 | Bonjour de noeud2 | 65 | 18.579 |
| 43 | Bonjour de node3 | 102 | 23.456 |
| 49 | Bonjour de node4 | 51 | 25.988 |
| 55 | Bonjour de node5 | 75 | 28.753 |
| 61 | Bonjour de node6 | 78 | 31.597 |
| 67 | Bonjour de noeud1 | 46 | 35.689 |
| 73 | Bonjour de node3 | 53 | 38.845 |
| 79 | Bonjour de node4 | 36 | 42.142 |
| 85 | Bonjour de node5 | 107 | 45.892 |
| 91 | Bonjour de node6 | 7 | 49.361 |
| 97 | Bonjour de noeud1 | 116 | 53.017 |
| 103 | Bonjour de noeud2 | 33 | 56.939 |
| 109 | Bonjour de node4 | 46 | 61.002 |
| 115 | Bonjour de node5 | 57 | 65.398 |
| 121 | Bonjour de node6 | 95 | 69.881 |

Tableau 2 - Résultats de la simulation de l'attaque de retard

1. **Temps de Retard Introduit :**

- Les temps de retard introduits par l'attaquant varient de 7 secondes à 120 secondes.
- Les nœuds ont reçu les messages avec des délais significatifs, ce qui indique que l'attaque de retard a été efficace pour perturber la transmission des messages.

2. **Temps CPU :**

- Le temps CPU enregistré montre la durée que chaque nœud a pris pour traiter les messages après réception.

3. **Impact sur le Temps de Bout en Bout (End-to-End Delay) :**

- Le délai de bout en bout (voir section 3.4.3.2) est directement impacté par les délais introduits par l'attaquant. Les messages prennent beaucoup plus de temps pour atteindre leur destination, ce qui peut gravement affecter les applications sensibles au temps tels que les applications liées à la sécurité (voir section 1.4.3.1).

- Les délais cumulés à travers plusieurs nœuds pourraient entraîner des temps de réponse inacceptables, dégradant la performance globale du réseau.

- **Calcul du délai de bout en bout (E2E Delay)**

Dans notre contexte, nous avons les informations nécessaires pour calculer le délai de bout en bout pour chaque message en fonction des temps de retard introduits par l'attaquant et les temps CPU enregistrés.

Prenons les événements du tableau pour illustrer le calcul du délai de bout en bout :

**Exemple 1 : Événement 1 :**

- Message : "Bonjour de noeud1"
- Source : noeud1
- Destination : tous les voisins du noeud1 (envoi par diffusion)
- Intercepté par : Hacker_Saidoune_Rahma
  - Temps de retard introduit par l'attaquant : 66 s
  - Temps CPU à la réception : 5.686 s

- E2Edelay (évènement 1) = Temps de retard introduit + temps de CPU
- E2Edelay (évènement 1) = 66s + 5.686s
- E2Edelay (évènement 1) = 71.686s

**Exemple 2 : Événement 7 :**

- Message : "Bonjour de noeud2"
- Source : noeud2
- Destination :  tous les voisins du noeud1 (envoi par diffusion)
- Intercepté par : Hacker_Saidoune_Rahma
- Temps de retard introduit par l'attaquant : 71 s
- Temps CPU à la réception 7.827 s
    - E2Edelay (évènement 7) = Temps de retard introduit + temps de CPU
    - E2Edelay (évènement 7) = 71s + 7.827s
    - E2Edelay (évènement 7) = 78.827s

Ces calculs peuvent être étendus à tous les événements du tableau en utilisant la même approche.

Le délai de bout en bout calculé, indiquant le temps que prend un message pour aller de sa source à sa destination, est crucial dans les réseaux VANET. Des délais excessifs, comme le cas de 71.686 et 78.827secondes, sont inacceptables. Pour les applications de sécurité, le délai doit être inférieur à 100 ms, tandis que pour les applications de confort, il devrait idéalement rester en dessous de 1 seconde. Un délai de plus de 70 secondes dans notre cas serait catastrophique pour les applications de sécurité et très frustrant pour les applications de

confort, rendant le réseau pratiquement inutilisable. Ceci indique une attaque grave nécessitant une intervention immédiate.

En conclusion, l'attaque de retard a eu un impact significatif en augmentant le délai de bout en bout, soulignant l'importance de mettre en place des mécanismes de détection et de mitigation pour minimiser l'impact de telles attaques dans les réseaux VANET.

### 4.6.3 Analyse de résultats de l'attaque de trou gris

Pour analyser les résultats de l'attaque Gray Hole en utilisant les métriques du nombre de messages supprimés et le taux de livraison des paquets (Packet Delivery Ratio, PDR), nous devons extraire et évaluer les informations pertinentes des logs fournis.

**Nombre de messages supprimés :** Les messages supprimés par l'attaquant sont clairement indiqués dans les logs avec un commentaires :

INFO : !!! l'attaquant a supprimé ce message !!!

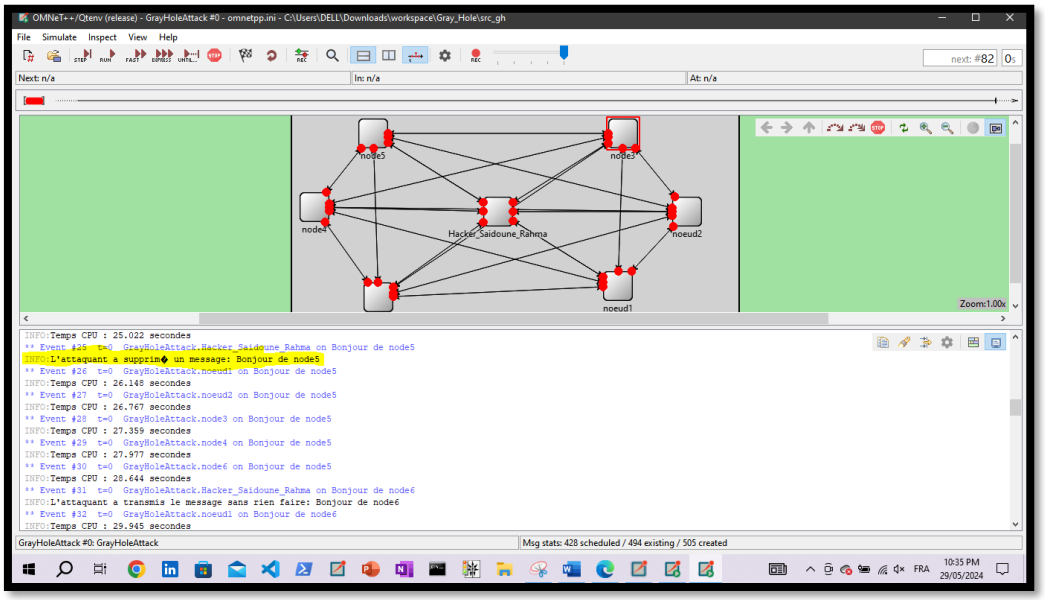


Figure 31 – Les logs de l'attaque trou gris dans OMNET++

| Numéro de l'événement | Nœud Source | Action de l'attaquant | Message Concerné |
|---|---|---|---|
| 1 | Hacker_Saidoune_Rahma | Message supprimé | Bonjour de noeud1 |
| 2 | GrayHoleAttack.noeud2 | - | Bonjour de noeud1 |
| 3 | GrayHoleAttack.node3 | - | Bonjour de noeud1 |
| 4 | GrayHoleAttack.node4 | - | Bonjour de noeud1 |
| 5 | GrayHoleAttack.node5 | - | Bonjour de noeud1 |
| 6 | GrayHoleAttack.node6 | - | Bonjour de noeud1 |
| 7 | Hacker_Saidoune_Rahma | Message supprimé | Bonjour de noeud2 |
| 8 | GrayHoleAttack.noeud1 | - | Bonjour de noeud2 |
| 9 | GrayHoleAttack.node3 | - | Bonjour de noeud2 |
| 10 | GrayHoleAttack.node4 | - | Bonjour de noeud2 |
| 11 | GrayHoleAttack.node5 | - | Bonjour de noeud2 |

Tableau 3 – Résultats de la simulation de l'attaque trous gris

Le PDR est défini comme le ratio du nombre de paquets reçus avec succès par les destinataires sur le nombre total de paquets envoyés.

- Total des messages envoyés : 6 * 13 + 3 = 81 messages.
- Nombre de messages supprimés : 11
- Nombre de messages reçus avec succès : 81 - 11 = 70.

**Calcul du PDR**

PDR = (Nombre de messages reçus avec succès) / (Nombre total de messages envoyés)

PDR = 70 / 81 ≈ 0.864 (ou 86.4%).

Ces résultats montrent que l'attaque Gray Hole a réussi à supprimer environ 13.6% des messages, ce qui a réduit le taux de livraison des paquets à 86.4%.

### 4.6.4 Analyse de résultats de l'attaque de modification

Voici le tableau des événements pour l'attaque par altération, indiquant les messages interceptés et modifiés par l'attaquant :

| Événement | Noeud | Message Original | Message Modifié |
|---|---|---|---|
| 1 | TamperingAttack.Hacker_Saidoune_Rahma | Bonjour de noeud1 | hahahaha |
| 2 | TamperingAttack.noeud2 | Bonjour de noeud1 | Non modifié |
| 3 | TamperingAttack.node3 | Bonjour de noeud1 | Non modifié |
| 4 | TamperingAttack.node4 | Bonjour de noeud1 | Non modifié |
| 5 | TamperingAttack.node5 | Bonjour de noeud1 | Non modifié |
| 6 | TamperingAttack.node6 | Bonjour de noeud1 | Non modifié |
| 7 | TamperingAttack.Hacker_Saidoune_Rahma | Bonjour de noeud2 | hahahaha |
| 8 | TamperingAttack.noeud1 | Bonjour de noeud2 | Non modifié |
| 9 | TamperingAttack.node3 | Bonjour de noeud2 | Non modifié |
| 10 | TamperingAttack.node4 | Bonjour de noeud2 | Non modifié |
| 11 | TamperingAttack.node5 | Bonjour de noeud2 | Non modifié |
| 12 | TamperingAttack.node6 | Bonjour de noeud2 | Non modifié |
| 13 | TamperingAttack.Hacker_Saidoune_Rahma | Bonjour de node3 | hahahaha |
| 14 | TamperingAttack.noeud1 | Bonjour de node3 | Non modifié |
| 15 | TamperingAttack.noeud2 | Bonjour de node3 | Non modifié |

Tableau 4 – Résultats de la simulation de l'attaque par altération

Chaque nœud envoie un message "Bonjour" à chaque autre nœud. Il y a 7 nœuds au total, donc :

- Nombre totale des messages envoyés = $7\times(7-1)= 7\times6 = 42$

L'attaquant a intercepté et modifié les messages dans plusieurs événements. En total, 30 messages ont été modifiés.

- Nombre de message non modifié = nombre totale des messages – nombre des messages modifiés

- Nombre de message non modifié = 42 – 30 = 8

L'attaque par altération a modifié un nombre significatif de messages (30 sur 42), affectant considérablement la fiabilité des communications. Cela démontre que l'attaquant a réussi à compromettre efficacement la majorité des échanges, mettant en péril l'intégrité et la sécurité du réseau.

### 4.6.5 Analyse de résultats de l'attaque de déni de service

Voici le tableau qui résume les évènements de notre attaque :

| Événement | Noeud cible | Message |
|---|---|---|
| 1 | noeud1 | Envoi de messages de DoS |
| 2 | noeud2 | Envoi de messages de DoS |
| 3 | node3 | Envoi de messages de DoS |
| 4 | node4 | Envoi de messages de DoS |
| 5 | node5 | Envoi de messages de DoS |
| ... | ... | ... |
| 30 | node6 | Réponse au message |
| 31 | noeud2 | Réponse au message |

Tableau 5 – Résultat de la simualtion de l'attaque déni de service

- L'attaque a été lancée par l'attaquant Hacker_Saidoune_Rahma dès l'initialisation du réseau, avec des messages de DoS envoyés à intervalles réguliers plus de 100 fois.
- Les cibles de l'attaque, à savoir les noeuds 1 à 6, ont subi des temps de réponse élevés en raison de la surcharge causée par les messages de DoS. Les temps de réponse augmentent au fur et à mesure que l'attaque progresse, cette montée en charge a entraîné un ralentissement significatif du fonctionnement de notre ordinateur, et finalement, l'interface graphique de simulation (Qtenv) a cessé de répondre.
- Les noeuds 1 et 2 ont subi une augmentation significative du temps de réponse, dépassant les 100 secondes.
- Les noeuds 3 à 6 ont également subi une augmentation du temps de réponse, bien que moins prononcée que celle des noeuds 1 et 2.
- Les messages de DoS ont été envoyés à plusieurs reprises, ce qui a maintenu la pression sur les cibles tout au long de l'attaque.
- Malgré la réception des messages de DoS, les cibles ont continué à traiter les messages réguliers, comme en témoigne le fait que les noeuds ont également traité les messages "DoSAttackMsg" en plus des messages réguliers.

## 4.7 Complexité de projet

Dans le cadre de notre projet, nous avons rencontré plusieurs défis qui ont ajouté à sa complexité. Ces défis sont les suivants :

1. **Compatibilité des versions des outils de simulation** : La coordination entre les différentes versions des outils de simulation, y compris OMNET++, SUMO et Veins, a été un défi majeur.
2. **Familiarisation avec les outils de simulation** : L’apprentissage et la maîtrise des outils de simulation nécessaires pour le projet ont nécessité un investissement significatif en temps et en efforts.
3. **Développement des attaques** : La conception et la mise en œuvre des attaques dans le réseau ont été une tâche complexe, nécessitant une compréhension approfondie des réseaux ad hoc de véhicules (VANETs).

4. **Correction des erreurs dans le code source** : Les codes sources des attaques étaient interdépendants, ce qui a entraîné des erreurs. Un temps considérable a été consommé pour rectifier ces erreurs et pour obtenir des résultats de simulation précis.
5. **Ressources limitées de l'ordinateur** : L'ordinateur utilisé, doté de 4 Go de RAM, a eu du mal à exécuter les simulations d'attaques, ce qui a ralenti le processus.
6. **Absence d'assistance des outils d'intelligence artificielle** : Les outils d'intelligence artificielle tels que ChatGPT, Copilot, Perplexity et d'autres n'ont pas été d'une grande aide dans ce projet car ils considèrent ces activités comme illégales.

Ces défis ont ajouté à la complexité du projet, mais ils ont également contribué à l'apprentissage et au développement en tant qu'étudiante chercheuse dans le domaine des réseaux et des systèmes.

## 4.8 Conclusion

Pour examiner le comportement des réseaux VANET, l'utilisation d'outils de simulation appropriés est cruciale. Dans ce chapitre, nous avons passé en revue divers simulateurs disponibles, y compris ceux spécifiquement conçus pour les réseaux VANET, le trafic routier et les frameworks. De plus, nous avons expliqué pourquoi nous avons choisi certains outils de simulation en fonction de nos exigences spécifiques. Enfin, nous avons décrit les différentes phases du projet, l'application de ces outils, le développement de notre ensemble d'attaques, l'analyse des résultats et l'impact des attaques, tout en soulignant la complexité associée.

# Conclusion Générale

Les réseaux ad hoc de véhicules (VANET) jouent un rôle crucial dans l'amélioration de la mobilité intelligente et de la sécurité routière. Ils facilitent la communication entre les véhicules et avec les infrastructures routières, permettant ainsi le partage d'informations sur les conditions de circulation, les alertes de sécurité, et bien plus encore.

Cependant, en raison de leur nature ouverte et de leur mobilité constante, les VANET sont vulnérables à diverses attaques. Les attaques par déni de service (DoS) et les attaques de l'homme du milieu (MITM) sont particulièrement préoccupantes. Ces menaces soulignent la nécessité d'une sécurité robuste dans les VANET.

Dans ce contexte, nous avons développé un package d'attaques spécifiquement conçu pour les VANET en utilisant les simulateurs OMNET++, SUMO et le framework VEINS. Ce package comprend plusieurs types d'attaques, y compris les attaques DoS et MITM (l'attaque de trou noir, l'attaque de trou gris, l'attaque de retard et l'attaque par altération). Notre objectif était d'évaluer l'impact de ces attaques sur la performance et la sécurité des VANET.

Nous visons à fournir aux chercheurs un plugin prêt à l'emploi, leur permettant de se concentrer sur le développement de mesures de sécurité, sans avoir à consacrer du temps à la création d'attaques. Ainsi, nous espérons contribuer à l'amélioration de la sécurité et de l'efficacité des réseaux VANET.

Notre projet apporte une contribution significative à la recherche sur la sécurité des VANET. En exposant les faiblesses potentielles, nous encourageons le développement de mécanismes de détection et de prévention des attaques. Cela garantit un fonctionnement fiable des VANET, essentiel pour la sécurité routière.

En conclusion, notre travail ouvre la voie à de nouvelles recherches visant à renforcer la sécurité des VANET et à concevoir des solutions innovantes pour un avenir plus sûr sur nos routes.

# Annexe A

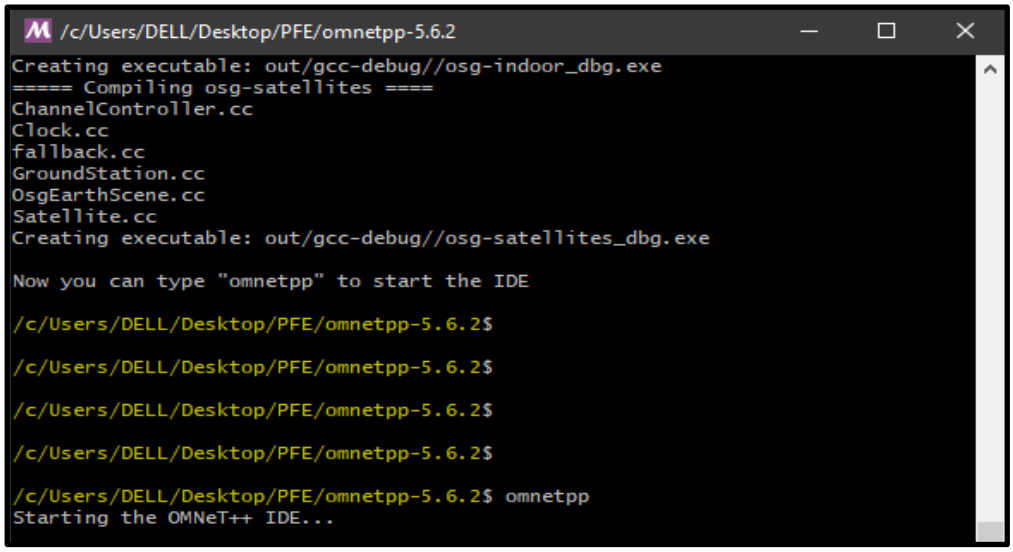


Figure 11 - Installation OMNET++

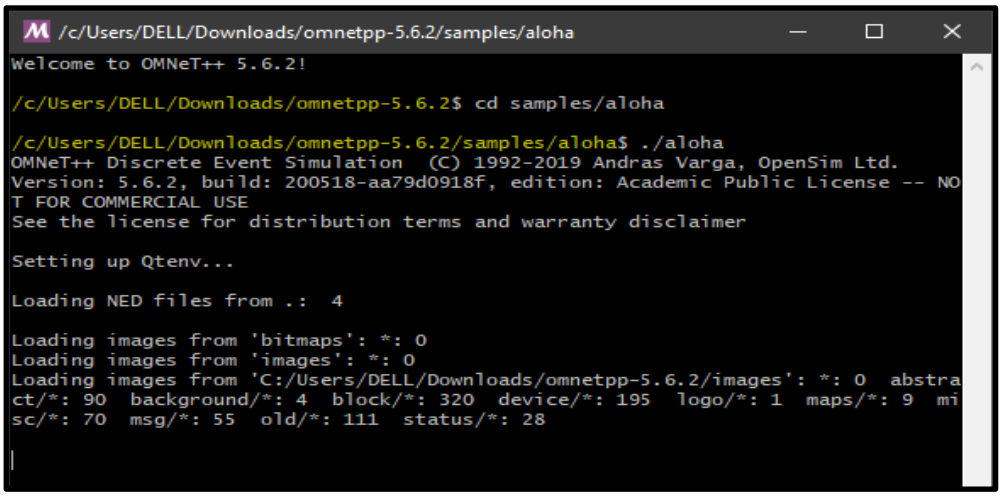


Figure 12 - Exécution de l'exemple aloha d'OMNET++

Dans les illustrations qui suivent, nous allons explorer l'exécution de l'exemple “ aloha ” au sein de l'interface Qtenv d'OMNET++. Ces figures nous permettront de comprendre pas à pas le déroulement de ce tutoriel. Cela nous donnera une vue d'ensemble de la manière dont les simulations fonctionnent dans l'environnement OMNET++, et comment nous pouvons utiliser ces informations pour nos propres simulations.

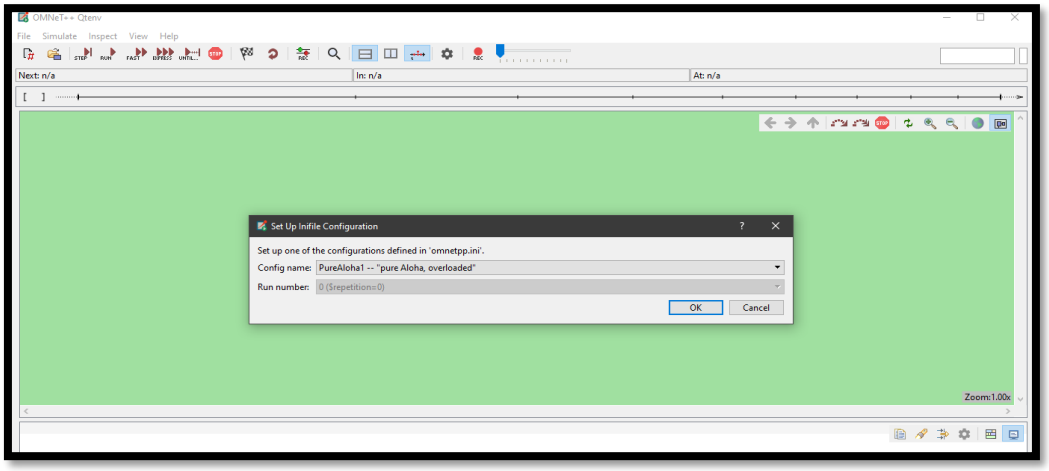


Figure 13 - L'interface Qtenv du OMNET++

L'interface utilisateur graphique principale d'OMNET++ est Qtenv, qui affiche le réseau de simulation et permet de contrôler l'exécution de la simulation, comme le montre la figure suivante :

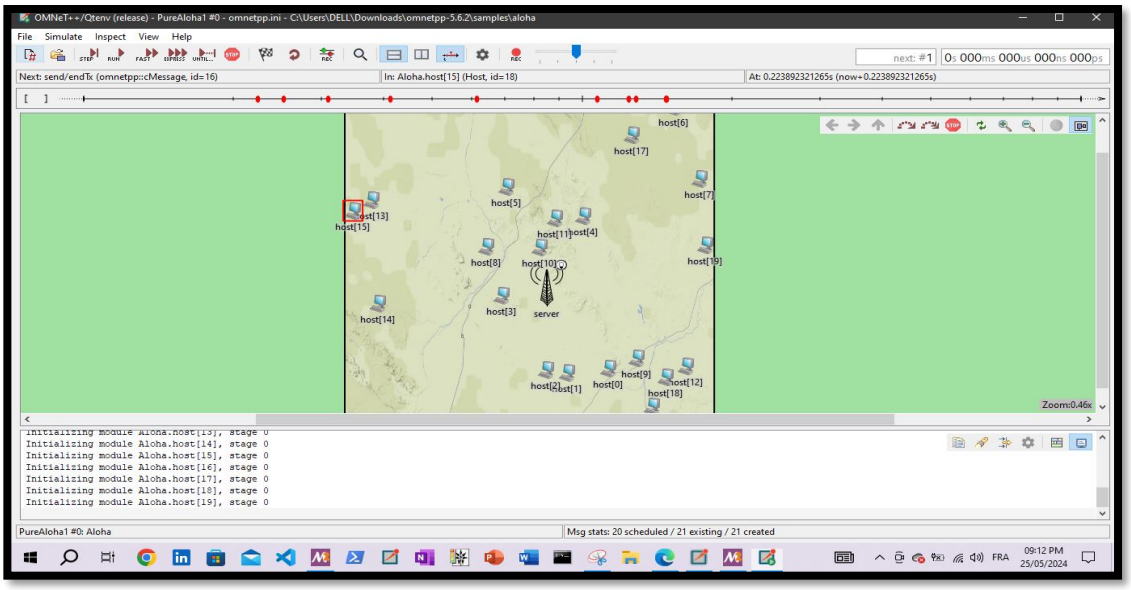


Figure 14 - Initialisation de la simulation dans OMNET++

# Annexe B

Les événements de la console OMNET++ consignent diverses actions pendant la simulation, y compris l'envoi de messages et les modifications d'affichage. La simulation dans OMNET++ suit une séquence d'événements générés et traités de manière séquentielle, représentant les changements d'état dans le système.

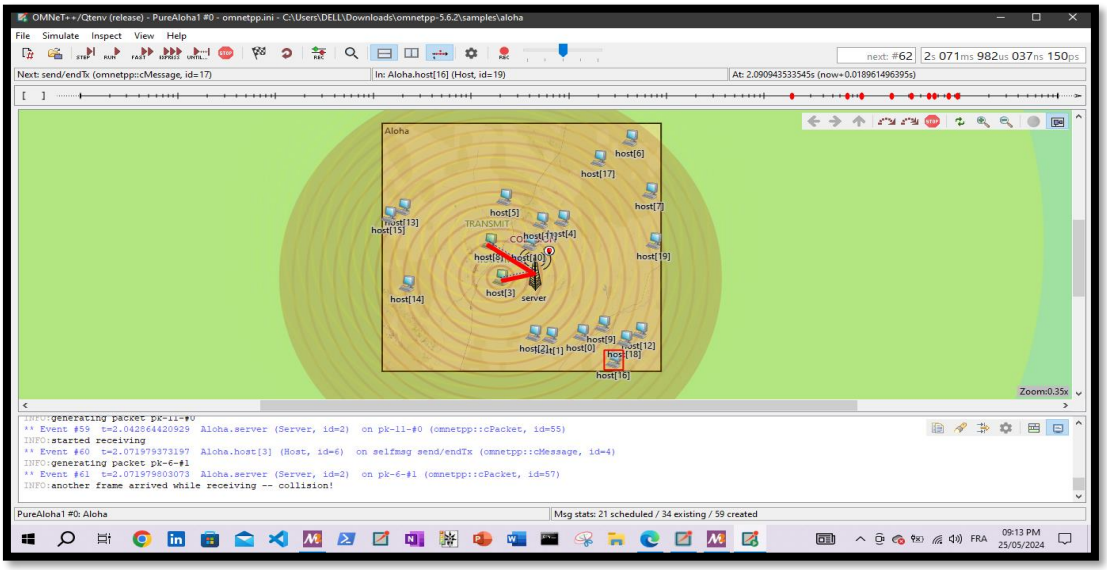


Figure 15 - Simulation de l'exemple aloha dans OMNET++

# Bibliographie


[1] Finch, D. J. (2020, juin). Wireless-attacks-omnet-plugin [PDF]. Department of Computer Science, Loughborough University. Disponible auprès de l'auteur.

[2] Wikipédia. (n.d.). Réseau ad hoc. Récupéré de : https://fr.wikipedia.org/wiki/R%C3%A9seau_ad_hoc

[3] Lemlouma, T. (n.d.). Chapitre 3 [PDF]. Récupéré de : http://opera.inrialpes.fr/people/Tayeb.Lemlouma/Papers/MasterThesis/Chapitre3.pdf

[4] Predictable Designs. (n.d.). Wireless technologies: Bluetooth, WiFi, Zigbee, GSM, LTE, LoRa, NB-IoT, LTE-M. Récupéré de : https://predictabledesigns.com/wireless_technologies_bluetooth_wifi_zigbee_gsm_lte_lora_nb-iot_lte-m/

[5] MOKOSmart. (n.d.). Bluetooth vs WiFi vs Zigbee: Which is better? Récupéré de : https://www.mokosmart.com/bluetooth-vs-wifi-vs-zigbee-which-is-better/

[6] Techniques de l'ingénieur. (n.d.). Routage dans les réseaux ad hoc. Récupéré de : https://www.techniques-ingenieur.fr/base-documentaire/technologies-de-l-information-th9/reseau-internet-protocoles-multicast-routage-mpls-et-mobilite-42289210/routage-dans-les-reseaux-ad-hoc-te7520/

[7] TechWatch. (n.d.). Comprendre les réseaux ad hoc: Une définition et un aperçu complets. Récupéré de : https://techwatch.de/fr/Articles/comprendre-les-r%C3%A9seaux-ad-hoc-une-d%C3%A9finition-et-un-aper%C3%A7u-complets/

[8] Academia.edu. (n.d.). La Sécurité dans les Réseaux Ad Hoc. Récupéré de : https://www.academia.edu/68600189/La_S%C3%A9curit%C3%A9_dans_les_R%C3%A9seaux_Ad_Hoc

[9] Bing. (n.d.). Sécurité des réseaux ad hoc. Récupéré de : https://bing.com/search?q=s%C3%A9curit%C3%A9+des+r%C3%A9seaux+ad+hoc

[10] Université Mouloud Mammeri de Tizi-Ouzou. (n.d.). La Sécurité dans les Réseaux Ad Hoc. Récupéré de : https://dspace.ummto.dz/items/ef3ed3cb-2c60-4182-9cc0-b4d197b5ca9b

[11] Geekflare. (n.d.). Mobile ad hoc network. Récupéré de https://geekflare.com/fr/mobile-ad-hoc-network/

[12] Techlib. (n.d.). MANET. Récupéré de : https://techlib.fr/definition/manet.html

[13] Wikipédia. (n.d.). Réseau de capteurs sans fil. Récupéré de : https://fr.wikipedia.org/wiki/R%C3%A9seau_de_capteurs_sans_fil

[14] Geekflare. (n.d.). Wireless sensor networks explained. Récupéré de : https://geekflare.com/fr/wireless-sensor-networks-explained/

[15] Toptips. (n.d.). Réseaux de capteurs sans fil (WSN) expliqués en 5 minutes ou moins. Récupéré de : https://toptips.fr/reseaux-de-capteurs-sans-fil-wsn-expliques-en-5-minutes-ou-moins/

[16] SpringerLink. (n.d.). Chapter. Récupéré de : https://link.springer.com/chapter

[17] IEEE Access. (n.d.). Home. Récupéré de : https://ieeeaccess.ieee.org/

[18] Internet Archive. (n.d.). ISBN 9780849373992. Récupéré de : https://archive.org/details/isbn_9780849373992

[19] IET Digital Library. (n.d.). Books - TE. Récupéré de : https://digital-library.theiet.org/content/books/te/pbte101e

[20] Wikipédia. (n.d.). Wireless mesh network. Récupéré de : https://en.wikipedia.org/wiki/Wireless_mesh_network

[21] IJERT. (n.d.). Vehicular ad hoc network (VANET): A brief knowledge. Récupéré de : https://www.ijert.org/vehicular-adhoc-network-vanet-a-brief-knowledge

[22] Wikipédia. (n.d.). Vehicular ad hoc network. Récupéré de : https://fr.wikipedia.org/wiki/Vehicular_Ad-Hoc_Network

[23] Hello Future. (n.d.). 5G et véhicules connectés: Communication et coopération. Récupéré de : https://hellofuture.orange.com/fr/5g-et-vehicules-connectes-communication-cooperation/

[24] La Tribune Auto. (n.d.). Les véhicules communicants entre eux et avec leur environnement contribuent à améliorer la sécurité. Récupéré de : https://www.latribuneauto.com/reportages/securite/5466-les-vehicules-communicants-entre-eux-et-avec-leur-environnement-contribuent-a-ameliorer-la-securite

[25] A3 Forum. (n.d.). Radars avant A3 8V 3P Sportback. Récupéré de : https://www.a3forum.fr/references-officielles-a3-8v-f87/radars-avant-a3-8v-3p-sportback-t41022.html

[26] Wikipédia. (n.d.). Interactions humain-machines. Récupéré de : https://fr.wikipedia.org/wiki/Interactions_humain-machines

[27] Verizon Connect. (n.d.). Connected vehicle technology: V2V, V2I, V2X. Récupéré de : https://www.verizonconnect.com/resources/article/connected-vehicle-technology-v2v-v2i-v2x/

[28] Avnet. (n.d.). V2V communication. Récupéré de : https://my.avnet.com/abacus/solutions/markets/automotive-and-transportation/automotive/communications-and-connectivity/v2v-communication/

[29] Mpirical. (n.d.). V2P: Vehicle-to-pedestrian. Récupéré de : https://www.mpirical.com/glossary/v2p-vehicle-to-pedestrian

[30] Connected Mobility. (n.d.). What is V2I communication?. Récupéré de : https://connectedmobility.co/what-is-v2i-communication/

[31] RGBSI. (n.d.). What is V2I technology?. Récupéré de : https://blog.rgbsi.com/what-is-v2i-technology

[32] Wikipédia. (n.d.). Technologie V2X. Récupéré de : https://fr.wikipedia.org/wiki/Technologie_V2X

[33] Connected Mobility. (n.d.). What is V2X communication?. Récupéré de : https://connectedmobility.co/what-is-v2x-communication/

[34] Hindawi. (2019). Wireless Communications and Mobile Computing. Récupéré de : https://www.hindawi.com/journals/wcmc/2019/2423915/

[35] Rutgers University. (2008). Position papers. Récupéré de : https://www.cs.rutgers.edu/~rmartin/teaching/fall08/cs552/position-papers/011-01.pdf

[36] Guo, K., Li, X., Fan, T., & Hu, X. (2022). VANet: a medical image fusion model based on attention mechanism to assist disease diagnosis.

[37] Ren, M., Zhang, J., Khoukhi, L., Labiod, H., & Vèque, V. (2021). A review of clustering algorithms in VANETs.

[38] Netwrix. (2024). Les 12 types d'attaques de cybersécurité les plus courantes actuellement. Récupéré de : https://blog.netwrix.fr/2024/03/21/les-12-types-dattaques-de-cybersecurite-les-plus-courantes-actuellement/

[39] Check Point. (n.d.). Network security threats. Récupéré de : https://www.checkpoint.com/fr/cyber-hub/network-security/what-is-network-security/network-security-threats/

[40] Techniques de l'ingénieur. (n.d.). Attaques des réseaux. Récupéré de : https://www.techniques-ingenieur.fr/base-documentaire/technologies-de-l-information-th9/cybersecurite-attaques-et-mesures-de-protection-des-si-42313210/attaques-des-reseaux-h5830/

[41] Wikipédia. (n.d.). Black hole (informatique). Récupéré de : https://fr.wikipedia.org/wiki/Black_hole_%28informatique%29

[42] Wikipédia. (n.d.). Packet drop attack. Récupéré de : https://fr.wikipedia.org/wiki/Packet_drop_attack

[43] HAL. (2013). Thèse de doctorat. Récupéré de : https://theses.hal.science/tel-00827552

[44] Université du Québec à Trois-Rivières. (2017). Mémoire de maîtrise. Récupéré de : https://oraprdnt.uqtr.uquebec.ca/portail/docs/FWG/GSC/Publication/1645/34/1918/1/170051/8/O0000330689_Memoire__depot_final__06_07_2017.pdf

[45] SpringerLink. (2018). Chapter 10.1007/978-3-319-98935-8_8. Récupéré de : https://link.springer.com/chapter/10.1007/978-3-319-98935-8_8

[46] University of Illinois. (2018). Delay. Récupéré de : https://publish.illinois.edu/cps-security/files/2018/05/delay.pdf

[47] Krishnan, P. R., & Kumar, P. A. R. (2021). Detection and Mitigation of Smart Blackhole and Gray Hole Attacks in VANET Using Dynamic Time Warping.

[48] Sardar, A., & Pramanik, P. K. D. (2021). Estimating Authors' Research Impact Using PageRank Algorithm. In Data Management, Analytics and Innovation (pp. 471–483).

[49] Gopi, R., Mathapati, M., Prasad, B., Ahmad, S., Al-Wesabi, F. N., Alohali, M. A., & Hilal, A. M. (2022). Intelligent DoS Attack Detection with Congestion Control Technique for VANETs.

[50] Université Laval. (2024). Principes de base des modèles de simulation.

[51] Haute Autorité de Santé. (2024). Bonnes pratiques en matière de simulation en santé.

[52] UNESCO. (2022). Research evaluation metrics. UNESCO Publishing.

[53] Fabbri, A., Scicluna, P., & Perez-Rosas, V. (2020). SummEval: Re-evaluating summarization evaluation. Proceedings of the 58th Annual Meeting of the Association for Computational Linguistics, 1915–1926.

[54] Wouters, P., Thelwall, M., Kousha, K., Waltman, L., de Rijcke, S., Rushforth, A., & Franssen, T. (2015). The Metric Tide: Literature Review (Supplementary Report I to the Independent Review of the Role of Metrics in Research Assessment and Management). HEFCE.

[55] Kumar, R., & Dave, M. (2018). A systematic VANET traffic congestion by eliminating recursion using intervention linear minimum spanning tree (ILMST) for traffic management system. Journal of Information and Optimization Sciences, 39(3-4), 1053-1068.

[56] Sommer, C., German, R., & Dressler, F. (2011). On the impact of building attenuation models in VANET simulations of urban scenarios. Ad Hoc Networks, 10(4), 619-630.

[57] Kumar, N., & Dave, M. (2015). VANET performance evaluation. International Journal of Computer Science and Mobile Computing, 4(5), 307-313.

[58] Benguenane, M., Korichi, A., Brik, B., & Azzaoui, N. (2023). Towards mitigating Jellyfish attacks based on honesty metrics in V2X autonomous networks.

[59] Kurtkoti, M. (2022). Performance analysis of machine learning algorithms in detecting and mitigating black and gray hole attacks.

[60] Duraibi, S., Alhamdani, W., & Sheldon, F. T. (2020). Replay spoof attack detection using deep neural networks for classification.

[61] Thooyamani, K. P., Khanaa, V., & Udayakumar, R. (2014). Efficiently measuring denial of service attacks using appropriate metrics.

[62] Tang, D., Dai, R., Tang, L., & Li, X. (2020). Low-rate DoS attack detection based on two-step cluster analysis and UTR analysis.

[63] SpringerOpen. (2021). Journal of the Brazilian Computer Society. Récupéré de: https://journal-bcs.springeropen.com/articles/10.1186/s13173-021-00113-x

[64] IEEE Xplore. (2015). Document 7297667. Récupéré de https://ieeexplore.ieee.org/document/7297667/