الجمهورية الجزائرية الديموقراطية الشعبية

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

وزارة التعليم العالي و البحث العلمي

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جامعة ابي بكر بلقايد –تلمسان-

Belkaid Aboubakr Université -TLEMCEN-

Faculté de TECHNOLOGIE



MEMOIRE

Présenté pour l'obtention du **diplôme** de **Master**

En : Télécommunication

Spécialité : Réseaux et Télécommunication

Par : Lakhal Anis Merwane

Sujet

Evaluation d'une méthodologie pour la détection des attaques de sécurité dans les réseaux véhiculaires

Soutenu publiquement, le 02/10/2025 , devant le jury composé de :

Mme SLIMANE Zohra	Professeur	Université de Tlemcen	Présidente
Mme BENAISSA Amal	MCB	Université de Tlemcen	Examinateur
Mme SEDJELMACI Amina	MCB	Université de Tlemcen	Encadreur

Année universitaire : 2024/2025

Résumé

Les communications Vehicle-to-Everything (V2X) sont essentielles pour les transports intelligents mais exposent à des risques cybernétiques. Ce mémoire évalue la plateforme VASP, un outil de simulation permettant de modéliser 68 types d'attaques sur les messages de sécurité V2X.À travers une méthodologie intégrant OMNeT++, SUMO et VEINS, nous simulons des scénarios d'attaque réalistes (véhicules fantômes, fausses alertes) et analysons leur impact sur les applications V2X. Notre travail fournit un cadre reproductible pour tester et améliorer les systèmes de détection d'anomalies.Les résultats démontrent l'utilité de VASP pour identifier des vulnérabilités critiques et développer des défenses plus robustes, contribuant ainsi à sécuriser les réseaux véhiculaires de nouvelle génération.

Mots-clés : V2X, Sécurité, VASP, Simulation, Attaques, Détection d'anomalies

Abstract

Vehicle-to-Everything (V2X) communications are essential for intelligent transportation but expose systems to cybersecurity risks. This master's thesis evaluates the VASP platform, a simulation tool capable of modeling 68 types of attacks on V2X security messages.

Using a methodology integrating OMNeT++, SUMO, and VEINS, we simulate realistic attack scenarios (ghost vehicles, false alerts) and analyze their impact on V2X applications. Our work provides a reproducible framework for testing and enhancing anomaly detection systems.

The results demonstrate VASP's utility in identifying critical vulnerabilities and developing more robust defenses, thus contributing to securing next-generation vehicular networks.

Keywords: V2X, Security, VASP, Simulation, Attacks, Anomaly Detection

ملخص

تعد اتصاالت المركبات مع كل شيء (V2X) أساسية ألنظمة النقل الذكية، لكنها تعرضها لمخاطر األلمن السيبراني. تقيم هذه األلطروحة منصةVASP ، وهي أداة محاكاة تمكن من نمذجة ٦٨ نوعاً من الهجمات على رسائل األلمان في أنظمة V2X باستخدام منهجية متكاملة تضم OMNeT++ و SUMO وVEINS ، نقوم بمحاكاة سيناريوهات هجوم واقعية (مركبات وهمية، إنذارات كاذبة) وتحليل تأثيرها على تطبيقات .V2X يقدم عملنا إطاراً قابلاً للتكرار الختبار وتحسين أنظمة كشف الشذوذ.

تظهر النتائج فائدة منصة VASP في تحديد الثغرات األلمنية الحركة وتطوير دفاعات أكثر متانة، مساهماً بذلك في تأمين شبكات المركبات من الجيل القادم.

الكلمات المفتاحية : V2X، األلمن السيبراني، منصةVASP ، المحاكاة، الهجمات، كشف الشذوذ

.

REMERCIEMENTS

Je veux avant tout exprimer ma gratitude envers Dieu, qui m'a porté et m'a donné le courage de traverser ces moments difficiles.

Je tiens à exprimer ma profonde gratitude à notre encadrante, Madame Sedjelmaci Amina, pour l'intérêt constant et les contributions précieuses qu'elle a apportés à l'amélioration de ce rapport. Son encadrement et ses remarques toujours pertinentes m'ont permis d'atteindre mes objectifs et de finaliser ce travail.

Je souhaite adresser toute ma gratitude à z.slimane, Professeur à l'Université de Tlemcen, qui a gracieusement accepté de présider le jury de ma soutenance.

Mes remerciements vont également à Mme a.benaissa, Maître de conférences à l'Université de Tlemcen, pour s'être investie avec autant de rigueur et d'impartialité dans l'évaluation de ce mémoire.

Un grand merci également à tous mes professeurs du département des télécommunications pour leur transmission de savoir.

Merci à ma famille et mes amis pour leur soutien sans faille et pour toutes les bonnes fois qui ont rendu ce travail bien plus agréable. Enfin, je pense à toutes les personnes qui ont joué un rôle, petit ou grand, dans la réalisation de ce projet.

Table des matières :

Résumé II
REMERCIEMENTS IV
Table des matières VI
Simulation de la sécurité V2X avec la plateforme VASP IX
Liste des figures X
Liste des tableaux XI
Acronymes XII
Introduction générale 1
Conclusion générale 103
Bibliographie 104

CHAPITRE I

LES VANETs

1. Introduction 3
2. Définition 3
3. Architecture VANET 4
3.1. Véhicule intelligent 4
3.2. On board unit (OBU) 4
3.3. Application unit (AU) 5
3.4. RoadSide Unit (RSU) 5
4. Mode de communication 6
5. Technologie d'accès sans fil dans VANET 7
5.1. Système cellulaire 7
5.2. WiFi/WLAN 7
5.3. WiMax 7
5.4. DSRC/WAVE 7
6. Caractéristiques des réseaux VANET 8
7. Applications de VANET 9
7.1. Applications de sécurité 9
7.2. Les applications commerciales 9
7.3. Applications de commodité 10

8. Les protocoles de routage 10
8.1. Les protocoles basés sur l'information de routage 11
8.2. Les protocoles de routage basés sur la topologie 11
9. la Sécurité en générale 17
9.1. L'authentification 17
9.2. L'intégrité 17
9.3. La disponibilité 17
9.4. La non-répudiation 18
9.5. Temps réel 18
9.6. L'intimité (Privacy) 18

CHAPITRE II

LA SURETE DANS LES VANETs

Introduction 21
1. Application 21
1.1. Protection des piétons 21
1.2. Sécurité publique (public safety) 23
1.3. Évaluation des risques (Risk assessment) 24
1.4. Sécurité routière (road safety) 26
2. Service 28
2.1. Prise en compte de l'environnement (environment consideration) 28
2.2. Gestion des intersections 30
2.3. Congestion du trafic 32
2.4. Identification des régions à risque (region identification) 34
3. Réseau 37
3.1. Contrôle de la gestion 37
3.2. Protocole de routage 39
3.3. Diffusion des données 42
3.4. Protocole MAC 45
3.4. Confidentialité 82

Chapitre III

LA SECURITE DANS LES VANETs – Etat de l'art

Introduction **51**

1. LES ATTAQUES ET LES MENACES 51

1.1. Infrastructure **51**

1.2. Interface sans fil **52**

1.3. Matériel et logiciel **57**

1.4. Les capteurs d'entrées **61**

2. Les défis de sécurité 62

2.1. La distribution de clés **62**

2.2. Des contraintes temps Réel **65**

2.3. La Topologie Dynamique **67**

2.4. Challenges de vérification et de cohérence **70**

3. Les Exigences 72

3.1. Protocoles de contrôle d'Accès **72**

3.2. Disponibilité **76**

3.3. Authentification **80**

3.4. Confidentialité **82**

Chapitre IV

Simulation de la sécurité V2X avec la plateforme VASP

1. **Introduction et contexte** 87
2. **Présentation de VASP** 87
   - 2.1. **Objectif** 87
   - 2.2. **Architecture** 87
   - 2.3. **Principaux composants** 88
3. **Problématique et objectifs de simulation** 88
   - 3.1. **Problématique** 88
   - 3.2. **Objectifs** 88
4. **Méthodologie** 89
   - 4.1. **Caractéristiques Techniques et Dépendances Clés** 89
   - 4.2. **Installation et fonctionnement technique de VASP** 90
   - a. **VirtualBox** 90
   - b. **Prérequis Logiciels et Leurs Rôles** 91
   - 4.3. **Scénarios** 94
5. **Implémentation dans VASP** 96
   - 5.1. **Intégration et configuration** 96
   - 5.2. **Procédure de construction (Build) dans la VM** 97
   - 5.3. **Configuration des attaques types** 97
   - 5.4. **Implémentation d'une attaque type** 98
6. **Résultats et analyse** 100
   - 6.1. **Tableaux et figures** 100
   - 6.2. **Discussion et interprétation** 100
7. **Menaces pesant sur la validité et limites** 100
8. **Reproductibilité** 101
   - 8.1. **Prérequis** 101
   - 8.2. **Installation** 101
   - 8.3. **Configuration** 101
   - 8.4. **Exécution** 101
   - 8.5. **Analyse des résultats** 101
   - 8.6. **Paramètres ajustables** 102
   - 8.7. **Format des traces** 102
9. **Conclusion et perspectives** 102

Liste des figures

Figure 1 : Véhicule intelligent 4
Figure 2 : OnBoard Unit (OBU) 5
Figure 3 : RoadSide Unit (RSU) 6
Figure 4 : V2V-V2I 6
Figure 5 : La classification des protocoles de routage VANET 11
Figure 6 : amélioration la sécurité des piétons 21
Figure 7 : EEMDS… 23
Figure 8 : Environnement VANET avancé intégrant des systèmes hétérogènes avec la technologie IoT pour la surveillance des applications 30
Figure 9 : communication VANET- basée sur l'infrastructure et sans infrastructure 50
Figure 10 : DOS attaque 51
Figure 11 : attaque sybil 51
Figure 12 : jamming attaque 52
Figure 13 : attacker in home and worklocation attack… 53
Figure 14 : Man-in-the-Middle attack in VANETs 53
Figure 15 : Passive eavesdropping attack in VANETs 54
Figure 16 : véhicule qui s'enregistre auprès de l'autorité (CA) 62
Figure 17 : virtualBox 88
Figure 18 : omnetpp 90
Figure 19 : sumo 90
Figure 20 : capture d'écran d'interface après l'installation de VM 91
Figure 21 : Ghost vehicule 92
Figure 22 : attaque V2X applicative : fake EEBL 92
Figure 23 : format des résultats sur Excel 93
Figure 24 : capture d'écran de la visualisation de vasp après l'installation 94
Figure 25 : notre code de simulation 95
Figure 26 : image de la communication entre veins et sumo 96
Figure 27 : capture d'écran de la simulation de vasp… 97

Liste des tableaux

Tableau 1 : une comparaison dans les réseaux VANET37
Tableau 2 : les attaques du modèle de communication "V2V" 54
Tableau 3 : présente des vecteurs d'attaque matériels et logiciels 58
Tableau 4 : comparer plusieurs protocoles MAC 72
Tableau 5 : Format CSV des résultats 93
Tableau 6 : Exemple de tableau de résultats (synthétique) 97

Acronymes

- **ABS** - Anti-lock Braking System
- **AODV** - Ad hoc On-Demand Distance Vector
- **AU** - Application Unit
- **AWS** - Amazon Web Services
- **BSM** - Basic Safety Message
- **CA** - Certification Authority
- **CD** - Compact Disc
- **CH** - Cluster Head
- **COIN** - Clustering for Open IVC Network
- **CPU** - Central Processing Unit
- **CRL** - Certificate Revocation List
- **CSV** - Comma Separated Values
- **DDoS** - Distributed Denial of Service
- **DoS** - Denial of Service
- **DSDV** - Dynamic Destination-Sequenced Distance Vector
- **DSRC** - Dedicated Short Range Communications
- **DSR** - Dynamic Source Routing
- **DTN** - Delay Tolerant Network
- **DV-CAST** - Distributed Vehicular Broadcast Protocol
- **ECN** - Electronic Chassis Number
- **ECU** - Electronic Control Unit
- **EDCA** - Enhanced Distributed Channel Access
- **EDGE** - Enhanced Data rates for GSM Evolution
- **EEMDS** - Effective Emergency Message Dissemination Scheme
- **EEBL** - Emergency Electronic Brake Light
- **ELP** - Electronic License Plate
- **EMs** - Emergency Messages
- **ESP** - Electronic Stability Program
- **FDMA** - Frequency Division Multiple Access
- **FSR** - Fisheye State Routing
- **GBT** - Gradient Boosted Tree
- **GPA** - Global Passive Adversary
- **GPS** - Global Positioning System
- **GPSR** - Greedy Perimeter Stateless Routing
- **GPRS** - General Packet Radio Service
- **GSM** - Global System for Mobile Communications
- **GW** - Gateway
- **HELLO** - Hello messages
- **HLAR** - Hybrid Location-Based Ad Hoc Routing Protocol
- **IBC** - Identity-Based Cryptography
- **IDS** - Intrusion Detection System
- **IMA** - Intersection Movement Assist
- **IoT** - Internet of Things
- **ITS** - Intelligent Transportation Systems
- **IVG** - Inter-Vehicle Geocast Protocol
- **JSON** - JavaScript Object Notation
- **L-BFGS** - Limited-memory Broyden--Fletcher--Goldfarb--Shanno

- **LAN** - Local Area Network
- **LiDAR** - Light Detection and Ranging
- **LSTLST** - Link Stability (dans le contexte EEMDS)
- **MAC** - Medium Access Control
- **MANET** - Mobile Ad-hoc Network
- **MIMO** - Multiple-Input Multiple-Output
- **ML** - Machine Learning
- **MOVE** - MOtion VEctor Routing Algorithm
- **NAT** - Network Address Translation
- **OBD** - On-Board Diagnostics
- **OBU** - On Board Unit
- **OFDM** - Orthogonal Frequency-Division Multiplexing
- **OS** - Operating System
- **OTA** - Over-The-Air
- **PKI** - Public Key Infrastructure
- **QoS** - Quality of Service
- **RADAR** - Radio Detection and Ranging
- **RAM** - Random Access Memory
- **RF** - Random Forest
- **RFID** - Radio-Frequency Identification
- **RIRP** - Reliability-Improving Position-Based Routing
- **RREP** - Route Reply
- **RREQ** - Route Request
- **RSU** - RoadSide Unit
- **SD** - Secure Digital (ou autre selon contexte)
- **STI** - Systèmes de Transport Intelligent (équivalent ITS)
- **SVM** - Support Vector Machine
- **SYN** - Synchronization
- **TA** - Trusted Authority
- **TDMA** - Time Division Multiple Access
- **TPD** - Temper Proof Device
- **TTC** - Time To Collision
- **UAV** - Unmanned Aerial Vehicle
- **UMTS** - Universal Mobile Telecommunications System
- **USB** - Universal Serial Bus
- **V2I** - Vehicle-to-Infrastructure
- **V2V** - Vehicle-to-Vehicle
- **V2X** - Vehicle-to-Everything
- **VADD** - Vehicle-Assisted Data Delivery In VANET
- **VANET** - Vehicular Ad-hoc Network
- **VASP** - V2X Application Spoofing Platform
- **VoIP** - Voice over IP
- **VPKI** - Vehicular Public Key Infrastructure
- **WAVE** - Wireless Access in Vehicular Environments
- **WiFi** - Wireless Fidelity
- **WLAN** - Wireless Local Area Network
- **WiMAX** - Worldwide Interoperability for Microwave Access
- **ZRP** - Zone Routing Protocol
- **ZoR** - Zone of Relevance

Introduction générale

L'émergence des technologies de communication et de l'intelligence artificielle a profondément transformé le paysage des transports modernes, inaugurant une ère nouvelle marquée par l'interconnexion croissante des véhicules et des infrastructures. Face aux défis persistants de la sécurité routière, de la congestion urbaine et de l'optimisation énergétique, les Systèmes de Transport Intelligents (STI) se présentent comme une solution prometteuse pour repenser la mobilité du futur. Au cœur de cette révolution technologique se trouvent les Réseaux Ad hoc Véhiculaires (VANETs) et les communications Véhicule-à-Tout (V2X), qui permettent des échanges dynamiques et décentralisés d'informations critiques entre les différents acteurs de la route.

Les VANETs représentent une avancée majeure dans le domaine des réseaux sans fil, permettant aux véhicules de communiquer entre eux (V2V - Vehicle-to-Vehicle) et avec l'infrastructure routière (V2I - Vehicle-to-Infrastructure). Cette connectivité instantanée ouvre la voie à une multitude d'applications innovantes visant à améliorer la sécurité des usagers de la route, à optimiser la fluidité du trafic et à offrir de nouveaux services de confort aux conducteurs. La promesse des VANETs est celle d'un environnement routier plus sûr, plus efficace et plus intelligent, où l'information circule librement pour anticiper les dangers et coordonner les déplacements.

Cependant, la nature même des VANETs - un environnement ouvert, dynamique et décentralisé, où des informations critiques sont échangées en temps réel - les rend intrinsèquement vulnérables à diverses menaces de sécurité. La compromission de l'intégrité, de la confidentialité, de l'authentification ou de la disponibilité des messages échangés pourrait avoir des conséquences catastrophiques, allant de la manipulation du trafic à des accidents graves, en passant par des atteintes à la vie privée des usagers. Les attaques malveillantes, qu'elles soient internes ou externes, ciblent ces vulnérabilités et posent un défi significatif à l'adoption généralisée des VANETs.

Dans ce contexte, l'évaluation rigoureuse des mécanismes de sécurité et la conception de systèmes de détection robustes deviennent une nécessité impérieuse. C'est précisément dans cette optique que s'inscrit le présent mémoire, qui se consacre à l'étude approfondie des vulnérabilités des réseaux VANETs et à l'évaluation des méthodes de détection d'attaques. Notre travail s'articule autour de la plateforme VASP (V2X Application Spoofing Platform), un outil complet permettant de simuler et d'analyser divers scénarios d'attaque sur les messages de sécurité V2X.

La problématique centrale de cette recherche concerne l'évaluation de la robustesse des systèmes V2X face aux menaces de sécurité et le développement de mécanismes de détection efficaces. Comment évaluer la résilience des communications V2X face à des attaques sophistiquées ? Quelles méthodologies employer pour simuler et analyser les comportements malveillants dans des environnements véhiculaires ? Dans quelle mesure la plateforme VASP peut-elle contribuer à l'amélioration de la sécurité des systèmes de transport intelligents ?

Pour répondre à ces questions, notre démarche s'organise en quatre chapitres distincts mais complémentaires. Le premier chapitre présente les fondements des réseaux VANETs, leurs architectures, leurs protocoles de communication et leurs applications. Le deuxième

chapitre aborde les aspects de sûreté et de sécurité, en dressant un état de l'art complet des menaces et

des mécanismes de protection. Le troisième chapitre se concentre sur l'analyse détaillée des attaques et des vulnérabilités spécifiques aux VANETs. Enfin, le quatrième chapitre détaille notre approche pratique de simulation de la sécurité V2X utilisant la plateforme VASP, incluant la méthodologie expérimentale, l'implémentation et l'analyse des résultats.

À travers cette étude, nous visons à apporter une contribution significative à la compréhension des enjeux de sécurité dans les réseaux véhiculaires et à fournir des outils méthodologiques pour l'évaluation et l'amélioration de la robustesse des systèmes V2X. Notre travail s'inscrit ainsi dans l'effort collectif de la communauté scientifique pour construire des infrastructures de transport intelligentes à la fois performantes et sécurisées, capables de répondre aux défis de la mobilité future.

Chapitre I

LES VANETs

1. Introduction 3
2. Définition 3
3. Architecture VANET 4
   3.1. Véhicule intelligent 4
   3.2. On board unit (OBU) 4
   3.3. Application unit (AU) 5
   3.4. RoadSide Unit (RSU) 5
4. Mode de communication 6
5. Technologie d'accès sans fil dans VANET 7
   5.1. Système cellulaire 7
   5.2. WiFi/WLAN 7
   5.3. WiMax 7
   5.4. DSRC/WAVE 7
6. Caractéristiques des réseaux VANET 8
7. Applications de VANET 9
   7.1. Applications de sécurité 9
   7.2. Les applications commerciales 9
   7.3. Applications de commodité 10
8. Les protocoles de routage 10
   8.1. Les protocoles basés sur l'information de routage 11
   8.2. Les protocoles de routage basés sur la topologie 11
9. la Sécurité en générale 17
   9.1. L'authentification 17
   9.2. L'intégrité 17
   9.3. La disponibilité 17
   9.4. La non-répudiation 18
   9.5. Temps réel 18
   9.6. L'intimité (Privacy) 18

Chapitre I :
LES VANETs

1. Introduction :

Les Réseaux Ad-hoc Véhiculaire (VANETs) représentent une avancée significative dans le domaine des technologies de communication sans fil, en particulier dans le secteur automobile. Ces réseaux permettent aux véhicules de communiquer entre eux (V2V, ou véhicule à véhicule) ainsi qu'avec l'infrastructure routière (V2I, ou véhicule à infrastructure). L'objectif principal des VANETs est d'améliorer la sécurité routière, l'efficacité du trafic et l'expérience de conduite en facilitant l'échange d'informations en temps réel.

Avec l'augmentation du nombre de véhicules sur les routes et la complexité croissante des systèmes de transport, les VANETs offrent une solution prometteuse pour relever les défis liés à la congestion routière, aux accidents et à la gestion des infrastructures. Grâce à des technologies telles que le GPS, les capteurs intégrés et les systèmes de communication sans fil, les véhicules peuvent partager des données cruciales, telles que les conditions de circulation, les alertes de collision, et les informations sur l'état des routes.

Les VANETs se distinguent des autres types de réseaux ad hoc, comme les MANETs (Mobile Ad-hoc Networks), par leur mobilité élevée et leur topologie dynamique. Les véhicules se déplacent à des vitesses élevées et peuvent entrer et sortir du réseau de manière fréquente, ce qui nécessite des protocoles de communication et de routage adaptés. De plus, les VANETs doivent prendre en compte des exigences spécifiques en matière de sécurité et de confidentialité, étant donné que les données échangées peuvent inclure des informations sensibles sur la localisation et le comportement des conducteurs.

En somme, les VANETs représentent une innovation clé dans le développement des systèmes de transport intelligents (ITS), offrant des opportunités pour améliorer la sécurité, l'efficacité et la durabilité des réseaux de transport. À mesure que la technologie continue d'évoluer, les VANETs sont appelés à jouer un rôle de plus en plus central dans la transformation des infrastructures de transport et des expériences de conduite.

2. Définition :

Le réseau véhiculaire ad hoc (VANET) représente une variante du réseau mobile ad hoc (MANET), où les points de connexion sont des véhicules. Chaque véhicule communique et reçoit des informations, il sert aussi de routeur en relayant les données vers leur destination. Dans le contexte du VANET, la communication peut se réaliser entre véhicules (communication véhicule à véhicule) ou entre l'infrastructure et les véhicules (communication infrastructure à véhicule).[2]

3. Architecture VANET :

3.1. Véhicule intelligent :

Un véhicule intelligent se compose principalement d'une série de capteurs (radar frontal, radar de marche arrière, etc.). Il existe également un système de localisation tel que le GPS (Système de Positionnement Global), qui est crucial pour la localisation et l'assistance à la conduite.

Un véhicule connecté possède un système de communication (qui peut disposer de plusieurs interfaces), un système informatique, et un mécanisme d'enregistrement d'événements qui fonctionne de manière comparable à la boîte noire d'un aéronef.

Pour des raisons de sécurité, un véhicule intelligent doit être équipé d'un ELP (Electronic License Plate) ou d'un ECN (Electronic Chassis Number) qui indiquent l'identité électronique du véhicule au lieu de l'identification conventionnelle par plaques d'immatriculation. La terminologie actuelle des Systèmes de Transport Intelligent (STI) comprend certaines caractéristiques telles que l'émetteur-récepteur, l'affichage et l'interaction avec le conducteur dans une seule unité appelée OBU (On Board Unit) . La figure 1 montre les différents composants qui peuvent être intégrés dans un véhicule intelligent. [3]

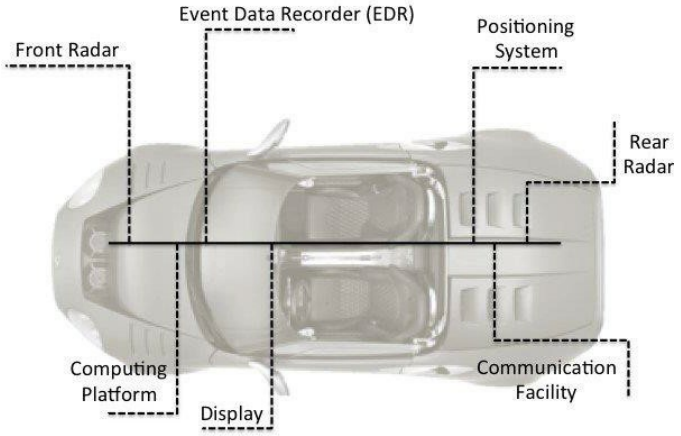


Figure 1 :Véhicule intelligent [3]

3.2. On board unit (OBU) :

Ce sont les unités intégrées dans les véhicules intelligents, elles comprennent un ensemble de composants matériels et logiciels de haute technologie (GPS, radar, caméras, divers capteurs).

Leurs rôles est d'assurés localisation, calcul, stockage et échange de données sur le réseau. Ce sont des émetteurs-récepteurs qui connectent le véhicule au réseau . [4][5]



Figure 2 : OnBoard Unit (OBU) [6]

3.3. Application unit (AU) :

L'UA est le dispositif installé dans le véhicule qui exploite les applications proposées par le fournisseur, en se servant des fonctionnalités de communication de l'OBU. L'AI peut servir comme un dispositif dédié pour divers types d'applications (sécurité routière, applications de confort, etc.).

Il peut être connecté à l'OBU par un lien filaire ou sans fil, étant donné qu'il peut être assemblé avec l'OBU dans une même entité physique. [4]

3.4. RoadSide Unit (RSU) :

L'unité de bord de route (RSU) est un dispositif de communication sans fil, habituellement installé en bordure de route ou à des lieux précis, comme les carrefours ou les zones de stationnement.

Le RSU est doté d'un dispositif réseau pour une communication à courte distance dédiée.

Peut aussi être doté d'autres dispositifs réseau pour pouvoir être employé à des fins de communication au sein du réseau d'infrastructure. D'après les principales fonctions et procédures liées à RSU (figure 3), on trouve[4] :

- Élargissement de l'étendue de communication du réseau VANET en en communiquant des informations à diverses OBU et en les relayant vers d'autres RSU pour atteindre différentes OBUs.
- Mise en œuvre d'applications de sécurité comme une alerte d'accident ou une zone de travail.
- Assurer une connexion Internet aux OBUs.



Figure 3 : RoadSide Unit (RSU) [7]

4. Mode de communication :

4.1. Véhicule-to-Véhicule (V2V) :

Les échanges entre véhicules en mode ad hoc sont qualifiés de V2V (Vehicle-to-Vehicle). En mode opérationnel, un véhicule est en mesure de recevoir, diffuser ou partager des informations routières comme les états de trafic et les accidents avec d'autres véhicules . [8]

4.2. Véhicule To Infrastructure (V2I) :

Destiné à la communication entre l'infrastructure routière et les véhicules, ainsi qu'à l'échange d'informations pertinentes sur l'état des routes et les précautions de sécurité à observer. Dans ce mode, un véhicule se connecte au RSU afin de communiquer avec des réseaux externes comme Internet. Les connexions V2I présentent une moindre vulnérabilité aux attaques et demandent une plus grande capacité de bande passante comparativement aux connexions V2V. [8]

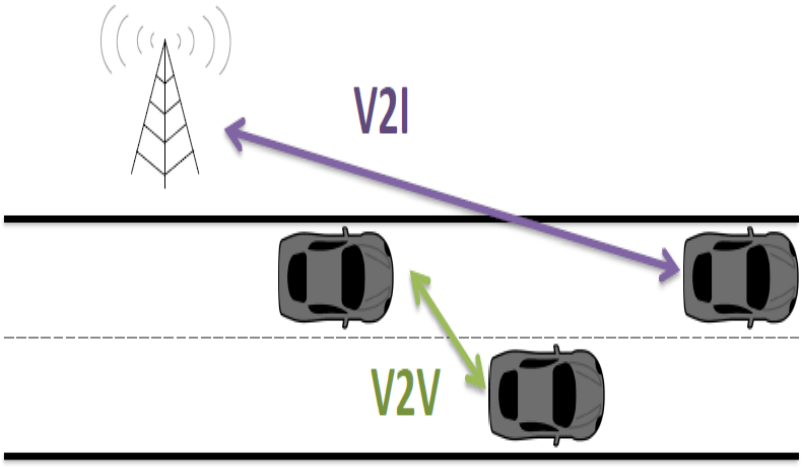


Figure 4 :V2V-V2I[17]

5. Technologie d'accès sans fil dans VANET :

5.1. Système cellulaire :

Le système cellulaire vise à exploiter la fréquence limitée disponible pour assurer le service. Le GSM est l'un des systèmes de téléphonie mobile proposant un débit maximal de 9,6 kbps. Le GSM emploie les modèles FDMA et TDMA. Le GPRS est un service universel de radiocommunication par paquets qui autorise une transmission efficace de données à haute bande passante. Il est nécessaire d'avoir des débits de données élevés pour transmettre des informations multimédia. C'est donc le système UMTS qui est utilisé à cet effet. La version améliorée du GSM, connue sous le nom d'évolution améliorée du débit de données (EDGE), est employée à cette fin et propose aussi un transfert de données à la pointe. [18]

5.2. WiFi/WLAN :

La norme IEEE 802.11 peut être utilisée pour faciliter la communication V2V ou V2I via un réseau local sans fil (WLAN) ou Wi-Fi, offrant ainsi un accès sans fil. Ce dispositif opère sur une fréquence de 5 GHz et offre un taux de transmission de 54 Mbps, avec une portée minimale de communication de 38 m à l'intérieur et de 140 m à l'extérieur . [9]

5.3. WiMax :

WiMAX, également connu sous le nom d'IEEE 802.16e, est une extension de l'interopérabilité mondiale pour l'accès par micro-ondes qui offre un large éventail de transmissions et une communication fiable avec une qualité de service (QoS) supérieure. Elle est conçue pour prendre en charge le multimédia, la vidéo ainsi que la voix sur Internet (VoIP). WiMAX est capable d'offrir un taux de transfert de données élevé, pouvant aller jusqu'à 35 Mbps, grâce à l'emploi de la technologie MIMO (multiplexage par répartition multiple) et du multiplexage par répartition orthogonale en fréquence (OFDM). [9]

5.4. DSRC/WAVE :

Les Communications à Courte Portée Dédiées sont des canaux de communication sans fil unidirectionnels de courte ou moyenne portée, spécifiquement élaborés pour une application dans le domaine automobile. Les technologies DSRC sont cruciales pour le marché en pleine croissance des systèmes de transport intelligents (ITS). L'accès sans fil dans les contextes de véhicules (Wireless Access in Vehicular Environments WAVE) présente des différences notables par rapport aux environnements de réseau sans fil Wi-Fi et mobile. Les normes les plus avancées concernant les réseaux DSRC/WAVE [10] sont celles définies par IEEE802.11P et IEEE1609. [10]

6. Caractéristiques des réseaux VANET :

6.1. Mobilité prévisible :

Dans VANET, les véhicules se déplacent selon un schéma de mobilité contraint par les routes, les rues, les autoroutes et par le code de la route (éclairage, limitation de vitesse)[9].

6.2. Conduite Sécurisée :

Les réseaux VANET permettent des communications directes entre véhicules en mouvement, permettant ainsi à un ensemble d'applications d'exiger une communication directe entre les nœuds sur le réseau. De telles applications peuvent donner aux conducteurs qui voyagent dans la même direction des messages d'avertissement sur les accidents ou sur la nécessité de freiner brusquement, Ces notifications aident le conducteur à construire une image plus large de la route. De plus, d'autres types d'applications pourraient être appliquées via ce type de réseau afin d'améliorer le confort des passagers et l'efficacité du trafic en diffusant des informations sur la météo, la circulation et les points d'intérêt (stations-service, centres commerciaux et fast food)[9].

6.3. Autonomie énergétique :

L'énergie n'est pas un défi majeur dans les VANET comme les réseaux MANET, car les véhicules sont capables d'utiliser l'énergie en continu en utilisant la batterie longue durée[9].

6.4. Densité variable du réseau :

La densité du réseau dans VANET dépend de la nature des routes (autoroute, rurale, centreville) et de la densité du trafic, qui peut être très élevée ou très faible[9].

6.5. Topologie Dynamique :

En raison de la grande mobilité des véhicules et donc de la nature irrégulière, la topologie VANET évolue rapidement. Ce changement rapide de la topologie du réseau facilite l'attaque de l'ensemble du réseau VANET et rend difficile la détection des véhicules malveillants[9].

6.6. Réseau à grande échelle :

L'échelle du réseau est variable, elle pourrait être grande dans les zones urbaines denses telles que le centre-ville, les autoroutes et à l'entrée des grandes villes[9].

6.7. Haute capacité de calcul :

Puisque les nœuds du réseau VANET sont des véhicules, ils peuvent être équipés d'une ressource informatique, comprenant des processeurs, une capacité de mémoire à grande vitesse, une capacité de stockage et différents types de capteurs. Ces ressources augmentent la capacité de calcul du véhicule, qui offre plus d'applications et de services que MANET[9].

7. Applications de VANET :

7.1. Applications de sécurité :

L'objectif des applications de sécurité est d'améliorer la sûreté de la conduite en fournissant des informations routières accessibles et instantanées (comme l'état de la route, en cas d'accident, etc.).

On peut classer les applications de sécurité routière de la manière suivante :

(a) Trafic en temps réel :

Cette application est construite autour du RSU, qui collecte des données de circulation en temps réel et les fournit aux véhicules quand cela est requis. L'objectif de ce genre d'applications est de prévenir les congestions routières. [11]

(b) Transfert coopératif de messages :

Dans le contexte du VANET, des messages contenant des informations variées sont constamment échangés. Dans ces données, vous découvrirez des renseignements concernant le freinage d'urgence, les erreurs de conduite du conducteur, entre autres. Cette application avait besoin d'un algorithme de diffusion performant et d'un réseau hautement efficace pour minimiser les temps de latence. [11][4]

(c) Notification post-collision :

Lors d'une collision, les véhicules concernés alertent les autres en transmettant des notifications. Ces alertes renferment des détails concernant la collision, tels que le lieu et l'heure. Ces alertes servent à aider les véhicules à prendre une décision. [11]

(d) Avertissement de collision coopérative :

Cette application avertit les véhicules du risque d'un accident si leur mode de déplacement reste identique. Ceci peut être réalisé par un point de contrôle centralisé (RSU), qui diffuse les alertes comportant des suggestions (modifier la trajectoire, diminuer la vitesse, etc.). [12][11]

7.2. Les applications commerciales :

Les applications destinées au monde des affaires offriront au conducteur des divertissements et des services sous forme d'accès internet, ainsi que de diffusion continue d'audio et de vidéo. On peut classer les applications commerciales de la manière suivante :

(a) Accès Internet :

Dans VANET, les véhicules peuvent avoir un accès Internet facilement via le RSU. Ce peut être un service payant. [11]

(b) Téléchargement de carte numérique :

Il est possible pour les conducteurs de télécharger et d'actualiser les cartes lorsque c'est requis. Ce service inclut les cartes et les bases de données. [11]

(c) Replay vidéo en temps réel :

Le chauffeur a la possibilité de solliciter la visualisation de ses vidéos favorites. C'est un service à bord qui permet d'ajuster les vidéos en fonction des conditions de conduite. [11]

(d) Annonces on-board :

Les prestataires de services ont la possibilité de mettre en avant leurs produits ou services auprès des chauffeurs pour séduire un plus grand nombre de clients dans leurs boutiques. Les annonces peuvent porter sur des stations-service, des restaurants autoroutiers. Ces annonces sont affichées en fonction de la localisation GPS des véhicules. [11]

7.3. Applications de commodité :

Les applications de commodité se concentrent essentiellement sur la gestion du trafic afin d'augmenter l'efficacité de la circulation en rehaussant le niveau de confort des conducteurs. On peut classer les applications de confort de la manière suivante :

(a) Collection de péage électronique :

C'est un dispositif qui vise à améliorer l'efficacité de la collecte des péages. Ce dispositif repose sur deux composants : le premier est installé au péage, tandis que le second se trouve sur l'OBU du véhicule. Grâce à l'interaction entre les deux entités, le règlement est effectué et se fonde sur le compteur kilométrique du véhicule. [11]

(b) Disponibilité du stationnement :

Cette application facilite la recherche de places libres dans les parkings d'une zone spécifique. Lorsque le conducteur sollicite une place de stationnement, il commence à recevoir des alertes sur les emplacements disponibles à proximité. [11]

(c) Prévision active (de la route) :

Cette application apporte un soutien au conducteur en prévoyant la configuration du terrain routier à venir. Cette forme d'aide soutient le conducteur dans l'optimisation de sa consommation de carburant en contrôlant sa vitesse de croisière avant l'amorce d'une descente ou d'une montée. [11]

8. Les protocoles de routage :

L'objectif principal du protocole de routage est de fournir des chemins optimaux entre les nœuds du réseau avec un temps système minimal. Beaucoup des protocoles de routage ont été développés pour les réseaux VANET, qui peuvent être classés de différentes manières, selon différents aspects ; tels que: caractéristiques des protocoles, techniques utilisées, informations de routage, qualité des services, structures de réseau, algorithmes de routage, etc.

La classification des protocoles de routage VANET est essentiellement basée sur : la topologie la position, géocast, diffusion et cluster, cette classification est basée sur des caractéristiques des et techniques utilisées dans des VANETs.

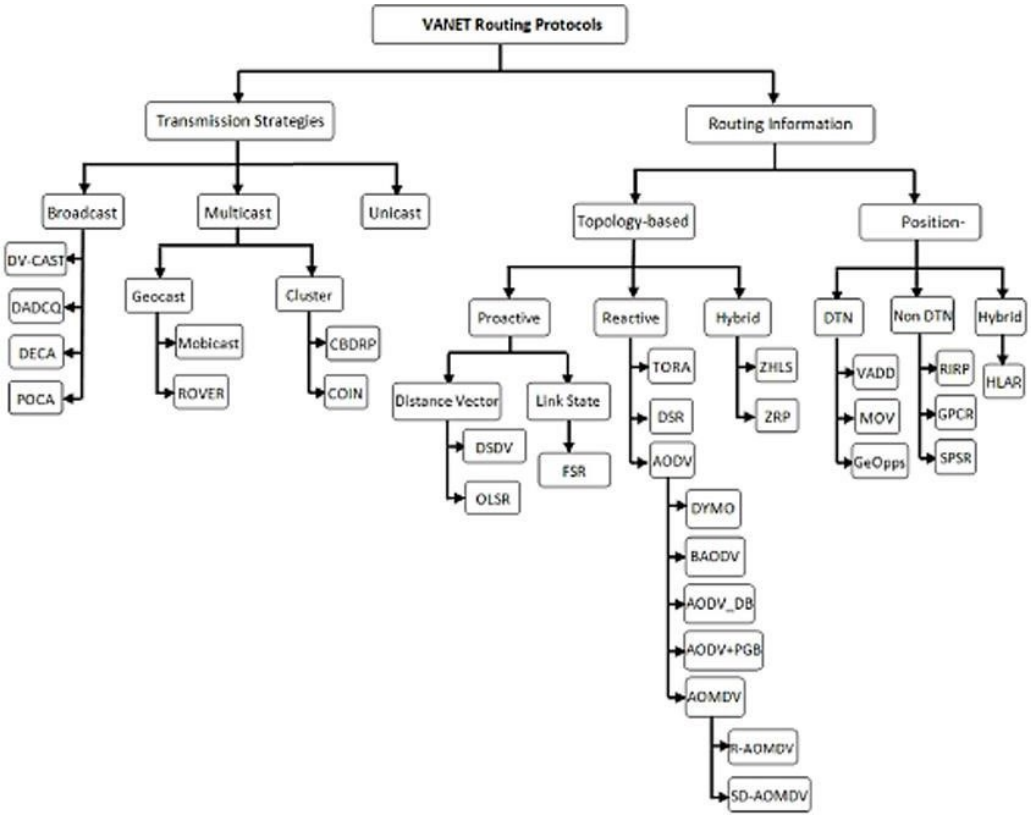


Figure 5: La classification des protocoles de routage VANET [13]

8.1. Les protocoles basés sur l'information de routage :

Cette classe est divisée en deux sous-classes : protocoles de routage basés sur la topologie et basés sur la position. Dans le routage basé sur la topologie, chaque nœud doit connaître la structure du réseau et doit également pouvoir transférer les paquets en utilisant des informations sur les nœuds et les liaisons disponibles sur le réseau. En revanche, le routage basé sur la position, chaque nœud doit connaître les emplacements des autres nœuds avant la transmission de paquets [13].

8.2. Les protocoles de routage basés sur la topologie :

L'ordre dans lequel les nœuds sont organisés dans un réseau est appelé topologie. Dans cette catégorie de protocoles de routage VANET, il utilise les informations de liaison présentes sur le réseau pour transférer des données d'un nœud source à un nœud de destination. Les protocoles basés sur la topologie peuvent être soit : proactif, réactif ou hybrides.[18]

(a) Protocoles proactifs :

Le principe de base des protocoles proactifs est de maintenir à jour les tables de routage. Ces protocoles sont basés essentiellement sur les protocoles de routage classique (vector distance, link state). Les tables de routage sont maintenues grâce à un échange continu de paquets de contrôle. Le choix des routes s'effectue en se basant sur une métrique (le nombre de sauts, la bande passante ou la route). L'avantage principal de ces protocoles est qu'ils permettent d'assurer un routage optimal, mais l'échange permanent des tables de routage consomme considérablement la bande passante du réseau.

- DSDV (Dynamic Destination-Sequenced Distance Vector)

Ce protocole utilise l'algorithme du plus court chemin. Chaque nœud stock les chemins vers toutes les destinations possibles dans une table de routage. La métrique de base pour trouver le plus court chemin est le nombre de saut. Lorsqu'il y a un changement de topologie du réseau, les tables de routage sont mises à jour en les échangeant avec les nœuds voisins. Les chemins cycliques ne sont pas autorisés dans le protocole de routage DSDV[14].

- FSR (Fisheye State Routing)

Il est similaire au protocole LSR (Link State Routing Protocol). Chaque nœud gère une table de topologie basée sur les dernières informations reçues des nœuds de voisinage. Il utilise différentes périodes d'échange pour différentes entrées dans la table de routage afin de réduire la taille des messages de contrôle dans les grands réseaux. [18]

L'inconvénient du routage FSR est que la taille de la table de routage augmente avec la taille du réseau. La découverte de l'itinéraire peut échouer si le nœud de destination se situe en dehors de la portée du nœud source. En raison de la grande mobilité dans VANET, les itinéraires vers une destination éloignée deviennent moins précis [2].

(b) Protocoles réactifs :

Ces protocoles sont appelés protocoles de routage à la demande car ils mettent à jour périodiquement la table de routage, lorsque certaines données doivent être envoyées. Mais ces protocoles utilisent le processus d'inondation pour la découverte d'itinéraire, ce qui augmente le temps système nécessaire au routage et consomme la bande passante.

- AODV (Ad hoc On-Demand Distance Vector)

AODV est un protocole de routage initié par la source et utilise les messages HELLO pour identifier ses voisins. Le nœud source diffuse une requête de route (route-request) à ses voisins, ces derniers vont diffuser cette requête pour atteindre la destination. Ensuite, la destination envoie un paquet de réponse de route (route-replay) à l'expéditeur[2]. AODV est un protocole de routage qui est utilisé à la base pour les réseaux MANET (Mobile Ad hoc NETwork), et des améliorations sont proposées pour répondre aux exigences du VANET où on site :

- Enhancing AOMDV Routing Protocol for V2V Communication (SD-AOMDV)[15]
- A Cross-layer AOMDV Routing Protocol for V2V Communication in Urban VANET (R-AOMDV)[15]

➢ DSR (Dynamic Source Routing)

Il utilise le routage source au lieu de dépendre de la table de routage du nœud intermédiaire. Le routage source consiste à ce que la source détermine un chemin et envoie dans chaque paquet de données tous les nœuds à traverser pour atteindre la destination. Chaque nœud intermédiaire retire son adresse du paquet avant de le retransmettre. Cette technique nécessite la connaissance de la route à utiliser de la part de la source. Cette connaissance des routes est obtenue par une table de routage maintenue dans chaque nœud. Il faut donc dans un premier temps découvrir les routes, puis les conserver tant qu'elles existent[2].

(c) Les protocoles hybrides :

Les protocoles hybrides combinent les approches réactive et proactive. Le principe est de connaître le voisinage de manière proactive jusqu``a une certaine distance (par exemple trois ou quatre sauts), et si jamais une station cherche à envoyer quelque chose à un nœud qui n'est pas dans cette zone, une recherche réactive est effectuée à l'extérieur. Selon le type de trafic et les routes demandées, ce type de protocole hybride peut cependant combiner les désavantages des deux méthodes : échange de paquets de contrôle réguliers et inondation de l'ensemble de réseau pour chercher une route vers un nœud éloigné.

➢ ZRP (Zone Routing Protocol)

ZRP est le premier protocole développé en tant que protocole de routage hybride (proactifs, réactifs), il permet à un nœud de réseau de diviser le réseau en zones en fonction de nombreux facteurs comme : puissance de transmission, force du signal, vitesse et d'autres facteurs.

La zone à l'intérieur de la zone est la zone de portée d'acheminement pour le nœud et inversement pour la zone extérieure. ZRP utilise les schémas de routage réactif pour la zone extérieur, et les schémas de routage proactifs pour la zone intérieur.

(d) Protocoles de routage base sur la position :

Les protocoles de routage géographique se fondent sur les données de localisation dans le processus de routage, où l'émetteur transmet un paquet à son destinataire en s'appuyant sur sa position géographique plutôt qu'en se basant sur l'adresse du réseau. Il était nécessaire que ces protocoles soient observés.Chaque nœud a la capacité de déterminer sa localisation ainsi que celle de ses voisins grâce au soutien du système de positionnement global (GPS). Le nœud reconnaît son voisin comme étant un nœud à l'intérieur de sa portée radio. Quand une source doit transmettre un paquet, elle inscrit souvent l'emplacement de la destination dans l'en-tête du paquet, rendant ainsi l'acheminement du paquet vers sa destination se fait sans avoir besoin de déterminer un itinéraire, d'assurer son entretien ou même d'être informé de la topologie du réseau. Par conséquent, les protocoles de routage basés sur la localisation sont jugés plus stables et mieux adaptés aux réseaux VANET à forte mobilité, comparativement

aux protocoles de routage fondés sur la topologie. On classe généralement les protocoles de routage géographique en trois catégories : les protocoles de réseau tolérants au retard (DTN), les protocoles de réseau non tolérants au retard (Non DTN) et le protocole hybride.

- **DTN (Delay Tolerant Network Protocols)**

DTN est un réseau sans fil conçu pour fonctionner efficacement dans les réseaux présentant certaines caractéristiques comme coupure de communication fréquente, réseau à grande échelle, les délais inévitables, largeur de bande limitée. Dans ce type de réseau, tous les noeuds s'entraident pour transférer des paquets. Ces nœuds peuvent avoir une portée de transmission réduite. La transmission des paquets prendra donc beaucoup de temps.

Généralement, le nœud DTN est un nœud mobile. Il établit donc des itinéraires vers les autres nœuds lorsqu'ils atteignent sa plage de transmission.

- MOVE (MOtion VEctor Routing Algorithm) :

L'algorithme MOVE est élaboré spécifiquement pour les réseaux allégés, notamment pour la communication entre véhicules en périphérie des routes. Ce mécanisme présuppose que chaque point bénéficie de données sur les emplacements mondiaux, en plus de l'information concernant la rapidité d'un routeur mobile et celle de ses nœuds adjacents. Sur la base de ces données, le nœud est en mesure d'évaluer les nœuds qui sont à la proximité la plus proche de la destination. Le routage basé sur la position non-DTN pourrait offrir des performances supérieures uniquement si les itinéraires sont constants et cohérents[15].

- VADD (Vehicle-Assisted Data Delivery In VANET) :

Protocole conçu pour gérer les réseaux de véhicules fréquemment déconnectés et les problèmes de forte mobilité. Il implémente le système de stockage et de transfert pendant qu'un nœud est en mouvement, il stocke le paquet jusqu'à ce qu'un nouveau nœud arrive dans sa plage de zones, puis il transfère le paquet stocké à ce nouveau nœud. Ce protocole prédit la mobilité des nœuds en fonction de deux facteurs : le trafic du réseau routier et le type de route. [16]

- **Non DTN (Non Delay Tolerant Network Protocols) :**

Les protocoles non-DTN sont des protocoles de routage géographiques, mais il ne considère pas un problème de dis-connectivité, cela suppose qu'il existe toujours un certain nombre de nœuds pour réussir la communication. Ce protocole ne convient donc que pour les réseaux à haute densité. Dans les protocoles Non-DTN, le nœud transmet son paquet au voisin le plus proche de la destination, mais cette approche peut échouer s'il n'y a pas de voisin le plus proche de la destination plutôt que le nœud actuel lui-même. De nombreux protocoles de routage non DTN gèrent cette défaillance.

- GPSR (Greedy Perimeter Stateless Routing) :

GPSR est un protocole de routage gourmand reconnu dans le cadre des VANET. Dans cette procédure, chaque point de transfert achemine les paquets vers d'autres points intermédiaires, de plus en plus près du lieu de livraison du paquet (acheminement par avance), jusqu'à ce que le paquet arrive à son terme final. S'il n'existe pas de nœud adjoint près de la destination, il se ssert du transfert de périmètre pour déterminer le nœud de livraison du

paquet. GPSR est un protocole sans état qui garde en mémoire des données sur les positions de ses voisins de premier niveau, ce qui pourrait améliorer encore l'évolutivité des protocoles par rapport aux protocoles de routage ad hoc les plus courts. [15]

- RIRP (Reliability-Improving Position-Based Routing) :

Le RIPR est un algorithme de routage positionnel élaboré pour les réseaux de véhicules ad hoc. Ce dernier a pour but de remédier aux problèmes de liaison défaillante identifiés dans un routage basé sur la localisation, qui surviennent suite à l'enregistrement d'informations périmées sur un nœud intermédiaire désuet. RIPR anticipe la vitesse de circulation des véhicules et leur orientation, tout en prenant en compte les propriétés routières urbaines. Dans ce protocole, l'émetteur choisit un nœud de passage pour envoyer son paquet basé sur l'évaluation de la mobilité des nœuds voisins, réalisée en vérifiant initialement la présence ou non d'un nœud voisin. [15]

- **Routage Hybride :**

Aucun protocole de routage existant ne fonctionne donc efficacement dans toutes les circonstances. Par conséquent, de nombreux chercheurs ont développé des protocoles hybrides, ils fusionnent les caractéristiques de deux ou plusieurs protocoles de routage basés sur la position (non-DTN et DTN), parfois ils fusionnent un ou plusieurs protocoles de routage de topologie (réactif, proactif et hybride) avec un routage basé sur la position.

- HLAR (Hybrid Location-Based Ad Hoc Routing Protocol)

HLAR est un protocole de routage hybride basé sur la position, conçu pour exploiter de manière optimale toutes les données de localisation disponibles tout en réduisant les coûts liés au contrôle du routage. Ce protocole est conçu pour passer au routage à la demande lorsque des informations de positionnement sont insuffisantes ou restreintes. Il gère également le problème d'absence de voisinage proche vers la destination (zones vides), ce qui en fait un protocole quasiment évolutif. HLAR agit en tant que protocole réactif dans la démarche de recherche d'itinéraire. [15]

(e) Stratégies de transmission utilisées dans le transfert de paquets :

La transmission d'informations d'une source à une destination peut être classée en quatre types: unicast, multicast, broadcast et géocast, toutefois, la multicast et la géocast peuvent être fusionnées dans une classe, car la géocast est généralement un type spécial de transmission par multicast.

- **Protocoles de routage unicast**

Le routage unicast désigne le processus de transmission d'informations d'un émetteur unique vers un récepteur unique, en recourant à des nœuds intermédiaires pour acheminer les données depuis la source jusqu'à la destination. Il s'agit de la classe la plus couramment employée dans les réseaux ad hoc généraux. Plusieurs protocoles de routage unicast sont proposés pour les VANET; la majorité des protocoles de routage fondés sur la topologie appartiennent à une catégorie unicast, comme VADD, AODV et DSR. [15]

➢ **Protocoles de routage broadcast**

Le routage par diffusion est fondé sur l'inondation de tous les nœuds accessibles au sein du domaine de diffusion. Dans les réseaux VANET, l'utilisation du routage de diffusion est très répandue. Il est principalement utilisé dans le processus de découverte d'itinéraire, certains protocoles tels que l'AODV autorisent les nœuds à retransmettre les paquets qu'ils ont reçus. Les protocoles de routage basés sur la diffusion utilisent la bande passante du réseau, ce qui peut entraîner une consommation importante de celle-ci. [15]

- DV-CAST (Distributed Vehicular Broadcast Protocol)

DV-CAST est un protocole de routage de diffusion qui emploie une méthode basée sur des sauts multiples. Dans ce protocole, chaque nœud surveille constamment l'état de la connexion avec les nœuds voisins pour leur transmettre des informations. DV-CAST gère différentes catégories en fonction de divers critères, tels que : l'état du trafic et la condition de la connectivité avec les nœuds adjacents. Il s'appuie sur les notifications régulières des balises pour recueillir des données concernant la topologie du réseau.

Dans un groupe réduit de nœuds connectés, le nœud peut utiliser la rediffusion avec les nœuds se déplaçant de la même manière. Dans le cas des nœuds voisins sont déconnectés, le nœud source doit utiliser le schéma de stockage et de retransmission, il stocke le paquet de diffusion jusqu'à ce qu'il trouve un autre nœud qui se déplace dans son domaine de diffusion, mais s'il n'y a pas de nœud, il supprimera le paquet une fois la durée de vie du paquet terminée. [15]

(f) Protocoles de routage multicast

Les protocoles de routage multicast (multidiffusion) ont pour but de communiquer des messages à de nombreuses destinations en tant que communication de groupe de véhicules. Les protocoles de routage multicast peuvent être classés en deux sous-classes : le protocole de routage géocast et le protocole basé sur un cluster.

➢ Les protocoles de routage géocast

Un protocole de routage géocast utilise des métriques d'emplacement géographique pour définir la destination. Par conséquent, dans ce type de protocole, la source enverra un message à plusieurs destinations ayant un point commun, à savoir la position géographique [16].

- IVG (Inter-Vehicle Geocast Protocol)

C'est un protocole de routage multicast adapté aux trafics routiers et de sécurité. L'idée principale de ce protocole est de notifier aux véhicules le danger d'accident ou d'autres obstacles. Ce protocole proposé introduit un nouveau concept appelé zone à risque. Ce dernier est défini en fonction des informations de position géographique et de la direction des véhicules. Le groupe de multidiffusion contient des véhicules situés dans la zone. Ce protocole suppose que tous les véhicules sont équipés d'un GPS, afin de collecter les informations nécessaires lors de l'exécution de l'algorithme [16].

- **Les protocoles de routage basés sur les clusters**

Ce type de protocole est lié à l'approche de clustering. L'idée principale de cette technique est de diviser le réseau en groupes appelés clusters, en fonction de plusieurs mesures et critères. Pour chaque cluster, l'un des membres joue le rôle de chef de cluster. Il est responsable de la communication à l'intérieur du cluster et à l'extérieur entre les différents clusters.

- COIN: Clustering for Open IVC Network

COIN est un mécanisme de regroupement conçu pour améliorer l'évolutivité du réseau. Il divise le réseau en clusters. Mais contrairement aux autres protocoles de cluster classiques, COIN sélectionne les clusters en fonction de trois paramètres : la mobilité des nœuds, la position des nœuds et le comportement des nœuds. Le protocole fournit une période de vie à chaque cluster. Le protocole de routage inter véhicules (IVC) gère les distances instables entre véhicules. Pour permettre à un chef de cluster et au nœud membre du cluster de continuer à communiquer efficacement pendant leur mobilité [2].

9. la Sécurité en générale :

9.1. L'authentification :

C'est l'une des principales exigences de tout système de sécurité. Dans les réseaux VANET, il est très important de disposer de certaines informations concernant le nœud émetteur telles que son identification et celle de l'expéditeur du message comme ses propriétés et de son emplacement. Il est important d'authentifier tous les utilisateurs et les messages transitant par le réseau. Les contrôles d'authentification les niveaux d'autorisation des véhicules.[18]

Dans les VANET, l'authentification empêche les attaques Sybil en attribuant une identité spécifique à chaque véhicule. Par exemple, éviter les embouteillages peut empêcher une seule voiture de prétendre être un ensemble de cent véhicules afin de donner l'illusion d'une route encombrée[18].

9.2. L'intégrité :

L'intégrité garantit qu'un message n'a pas été modifié entre le moment où il a été envoyé et reçu car le message reçu doit correspondre au message envoyé. Le destinataire sera alors en mesure de confirmer l'identité de l'expéditeur au cours de la transaction. L'intégrité protège contre la création, la destruction ou l'altération non autorisées de données. Si un message corrompu est accepté, la propriété d'intégrité est violée et le protocole serait considéré comme défectueux. Pour assurer l'intégrité du système, le système doit empêcher les attaquants de modifier les messages, car leur contenu doit être sécurisé[18].

9.3. La disponibilité :

Le réseau et les applications doivent rester opérationnels même en présence de pannes ou de conditions malveillantes. Cela nécessite non seulement une conception sécurisée mais également tolérante aux pannes, une résilience aux attaques, ainsi que des protocoles viables, qui reprennent leurs activités normales après le retour au fonctionnement régulier du réseau. Un protocole de routage adéquat est nécessaire pour atteindre tous les destinataires requis qui peuvent être inconnus de l'expéditeur[18].

9.4. La non-répudiation :

La non-répudiation facilitera l'identification des attaquants, même après l'attaque. Toutes les informations relatives à la voiture telles que : l'itinéraire, la vitesse, le temps, toute violation seront stockées dans un équipement appelé TPD (Temper Proof Device), toute entité a une autorisation officielle (exp. La police) pourra récupérer ces données[19].

9.5. Temps réel :

Les véhicules se déplacent avec une vitesse importante, cela nécessitera une réaction en temps réel dans certaines situations. Pour satisfaire cette contrainte les réseaux VANET reposent sur la norme émergente pour les communications dédiées à courte portée (DSRC), basée sur une extension de la technologie IEEE 802.11[19].

9.6. L'intimité (Privacy) :

C'est de garder les informations des conducteurs à l'abri des observateurs non autorisés, telles que l'identité réelle, le trajet, la vitesse, etc. L'intimité peut être obtenue en utilisant des clés temporaires (pseudonymes). Ces clés seront changées fréquemment, chaque clé pouvant être utilisée uniquement une fois et expire après utilisation, toutes les clés seront stockées dans le TPD (Tamper Proof Device) et seront rechargées à nouveau lors de la prochaine vérification officielle du véhicule[19].

Chapitre II

LA SURETE DANS LES VANETs

Introduction 21

1. Application 21

1.1. Protection des piétons 21

1.2. Sécurité publique (public safety) 23

1.3. Évaluation des risques (Risk assessment) 24

1.4. Sécurité routière (road safety) 26

2. Service 28

2.1. Prise en compte de l'environnement (environment consideration) 28

2.2. Gestion des intersections 30

2.3. Congestion du trafic 32

2.4. Identification des régions à risque (region identification) 34

3. Réseau 37

3.1. Contrôle de la gestion 37

3.2. Protocole de routage 39

3.3. Diffusion des données 42

3.4. Protocole MAC 45

3.4. Confidentialité 82

CHAPITRE II :

LA SURETE DANS LES VANETs

Introduction :

Les VANETs sont la technologie sous-jacente qui permet aux véhicules (V2V - Vehicle-to- Vehicle) et à l'infrastructure routière (V2I - Vehicle-to-Infrastructure) de communiquer entre eux en temps réel. Cette communication est le fondement des applications de sécurité, car elle étend considérablement le champ de perception du conducteur et du véhicule au-delà de la ligne de mire (p. ex., au-delà d'un virage ou d'un véhicule qui cache la vue).

L'objectif est d'éviter ou d'atténuer la gravité des accidents en avertissant le conducteur suffisamment tôt, d'informer sur les dangers imminents ou les conditions de route dangereuses, et de donner au conducteur une compréhension complète de son environnement routier, même des éléments qu'il ne peut pas voir directement.

1. Application :

Cette section traite des aspects liés aux utilisateurs finaux et aux applications qui améliorent directement la sécurité routière.

1.1. Protection des piétons :

Dans les environnements urbains à visibilité réduite ou faiblement éclairés, les systèmes V2X alertent les conducteurs lorsque des piétons se trouvent sur les passages piétons, y compris ceux qui peuvent être masqués par d'autres véhicules. Ces alertes améliorent la perception de la situation et contribuent à éviter les accidents impliquant des usagers de la route vulnérables.



Figure 6: amélioration la sécurité des piétons [66]

a. Fonctionnement de la technologie V2X pour la sécurité des piétons :

La communication V2X permet un échange de données en temps réel entre les véhicules, les infrastructures et les piétons. Elle utilise une connectivité sans fil (DSRC ou C-V2X) pour transmettre des informations telles que la vitesse des véhicules, l'état de la route et les intentions des conducteurs. Ce flux de données permet aux systèmes de sécurité d'alerter les conducteurs et les infrastructures avant les dangers potentiels[53].

b. Améliorations de la sécurité des piétons dans les environnements urbains :

Dans les zones urbaines où la visibilité est limitée ou où l'éclairage est faible, les systèmes V2X alertent les conducteurs lorsque des piétons se trouvent sur les passages piétons, y compris ceux qui peuvent être masqués par d'autres véhicules. Ces alertes améliorent la conscience situationnelle et aident à éviter les accidents impliquant les usagers vulnérables de la route[53].

c. Efficacité prouvée dans la prévention des accidents :

Selon la National Highway Traffic Safety Administration (NHTSA), les systèmes basés sur V2X pourraient aider à prévenir jusqu'à 79 % des accidents impliquant des conducteurs non affaiblis, sur la base de recherches combinant les technologies véhicule-à-véhicule et véhicule-à-infrastructure[53].

d. Intégration dans les systèmes de gestion du trafic des villes intelligentes :

La communication V2X est un élément fondamental de la gestion du trafic dans les villes intelligentes. En s'intégrant aux systèmes IoT et à l'infrastructure cloud, V2X permet des réponses adaptatives aux événements en temps réel, comme les embouteillages ou les dangers routiers, et optimise les séquences des feux de circulation pour améliorer le flux du trafic et réduire les temps d'arrêt[53].

e. Compatibilité avec les infrastructures existantes :

Les systèmes V2X sont conçus pour s'intégrer aux infrastructures de trafic actuelles et sont compatibles avec les technologies émergentes dans les systèmes de transport intelligents. Ils fonctionnent avec les plateformes de données de trafic comme celles de Miovision, qui prennent en charge les technologies avancées telles que V2X[53].

f. Solutions concrètes et contact :

Miovision propose des solutions évolutives activées par V2X qui améliorent la sécurité, améliorent le flux du trafic et jettent les bases du développement des villes intelligentes. Pour

ceux qui souhaitent en savoir plus, il est possible de contacter Miovision pour découvrir comment la communication V2X peut moderniser la stratégie de sécurité routière de votre ville[53].

Ce résumé met en évidence comment la technologie V2X contribue significativement à la protection des piétons et à l'amélioration de la sécurité routière globale[53].

1.2. Sécurité publique (public safety) :

Les Réseaux Ad hoc Véhiculaires (VANETs) jouent un rôle absolument crucial dans l'amélioration de la sécurité publique et la gestion des situations d'urgence, comme les accidents de la route ou les catastrophes naturelles. Leur objectif principal est d'éviter les accidents et de coordonner les secours en assurant une diffusion rapide et fiable des messages d'urgence (Emergency Messages - EMs).

a. L'enjeu (Une diffusion rapide et fiable des alertes) :

Lorsqu'un danger survient (ex : un accident), le véhicule concerné doit diffuser un message d'urgence à tous les autres véhicules à proximité et aux services de secours. Cela permet aux conducteurs de prendre des mesures préventives (changer d'itinéraire, ralentir) et aux services d'urgence d'intervenir plus rapidement.

La méthode simple de diffusion ("flooding"), où chaque véhicule retransmet le message, provoque une "tempête de diffusion" (broadcast storm). Cela entraîne une congestion du réseau, des retards importants et une perte de messages, ce qui est inacceptable dans une situation d'urgence où chaque milliseconde compte. Ce problème est encore plus critique en milieu urbain dense avec des intersections[54].

b. La solution proposée :

Un schéma de diffusion appelé EEMDS (Effective Emergency Message Dissemination Scheme) spécialement conçu pour les environnements urbains. Son but est de maximiser la couverture de l'information (le nombre de véhicules touchés) tout en minimisant le délai de transmission et la perte de paquets[54].

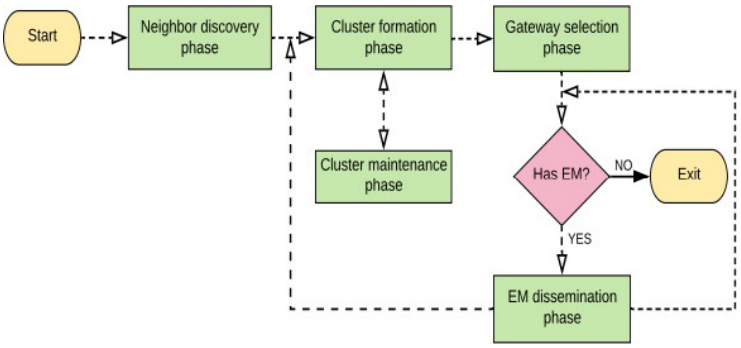


Figure 7 : EEMDS [54]

Pour ce faire, EEMDS utilise une approche en clusters (regroupements de véhicules) :

- Formation de Clusters Stables : Les véhicules se regroupent en clusters basés sur leur direction de déplacement et d'autres métriques de mobilité (vitesse relative, distance, perte de signal). Un Cluster Head (CH) est élu dans chaque groupe pour coordonner les communications. Cette structure hiérarchique évite que tout le monde parle en même temps[54].
- Sélection de Relais Optimisés : Pour communiquer entre les clusters, des véhicules "passerelle" (Gateway - GW) sont sélectionnés non pas simplement sur la distance, mais sur la stabilité du lien de communication (LSTLST) avec leur CH. Cela garantit que le message sera relayé de manière fiable et évite les retransmissions redondantes[54].

Bénéfices pour la gestion des urgences :

Les résultats de simulation montrent que EEMDS surpasse les méthodes existantes :

- Couverture d'Information Accrue : Jusqu'à 20,7 % de véhicules en plus reçoivent le message par rapport à une méthode de flooding classique[54].
- Délai Réduit : Le temps de transmission du message de la source à la destination (E2E delay) est réduit jusqu'à 20,08 % par rapport à d'autres schémas[54].
- Fiabilité Améliorée : Le taux de livraison des paquets (PDR) est bien plus élevé, surtout dans les réseaux denses et à haute vitesse, garantissant que l'alerte est bien reçue[54].

En résumé, les VANETs sont des outils indispensables pour la sécurité publique moderne. En permettant une communication instantanée et coordonnée entre les véhicules et les infrastructures, ils transforment les véhicules en capteurs et relais intelligents. Le schéma proposé, EEMDS, démontre qu'il est possible de surmonter les défis techniques pour diffuser des alertes vitales de manière ultra-rapide et fiable en milieu urbain, permettant ainsi de sauver des vies en évitant des accidents en chaîne et en accélérant l'intervention des secours.

1.3. Évaluation des risques (Risk assessment) :

Les Réseaux Ad hoc Véhiculaires (VANETs) transforment les véhicules en capteurs mobiles intelligents, permettant une évaluation des risques en temps réel et une prévention proactive des accidents. Cette capacité repose sur la collecte, l'échange et l'analyse massive de données.

a. Collecte de données en temps réel :

Les véhicules équipés de capteurs (GPS, radars, lidars, caméras) et d'unités de communication (OBU) collectent en permanence une multitude de données :

- Données dynamiques des véhicules : Vitesse, accélération/décélération, direction, angle de braquage, statut des feux stop et clignotants[55].
- Données environnementales : Conditions routières (via capteurs de glace, ABS), conditions météorologiques (via capteurs de pluie, luminosité), visibilité.
- Données de localisation : Position GPS précise, trajectoire, distance par rapport aux autres véhicules et à l'infrastructure[55].

b. Analyse des risques et modèles de prédiction :

Grâce à ces données partagées entre véhicules (V2V) et avec l'infrastructure (V2I), des algorithmes peuvent évaluer le niveau de danger et prédire les incidents :

- **Détection des situations à haut risque :** Le système analyse en temps réel le comportement des véhicules pour identifier des situations dangereuses :
  - Rapprochement critique : Calcul du Time To Collision (TTC) entre deux véhicules sur une trajectoire de collision[55].
  - Décélération brutale : Un véhicule qui freine soudainement peut indiquer un danger invisible pour les voitures qui le suivent[55].
  - Comportement erratique : Détection de virages brusques ou de déviations de trajectoire pouvant suggérer une distraction, un malaise ou un mauvais état de la route[55].

- **Modèles de prédiction des accidents et quasi-accidents :** En croisant les données historiques d'accidents avec les données en temps réel, des modèles prédictifs (utilisant souvent l'intelligence artificielle et l'apprentissage machine) peuvent être développés pour :
  - Identifier les "points chauds" (hotspots) : Zones géographiques où la probabilité d'un accident est statistiquement plus élevée (intersections complexes, sorties d'autoroute, zones souvent glissantes) [55].
  - Anticiper les quasi-accidents : Une manœuvre d'évitement suivie d'un freinage brusque est un quasi-accident. Analyser ces "presque-événements" est crucial pour améliorer la sécurité avant qu'un accident réel ne se produise[55].
  - Émettre des alertes préventives : Sur la base de cette analyse, le système peut générer des messages d'urgence anticipés pour avertir les conducteurs d'un danger potentiel qu'ils ne voient pas encore (ex : "Ralentissez, risque de collision au prochain carrefour", "Attention, véhicule en difficulté 300 m devant")[55].

c. **Le rôle de la communication V2X :**

La valeur de cette analyse prédictive dépend entièrement de la rapidité et de la fiabilité du réseau VANET :

- La communication V2V permet un échange d'informations ultra-rapide entre véhicules proches pour une alerte immédiate (ex : le freinage d'urgence d'une voiture déclenche une alerte pour les véhicules suiveurs) [55].
- La communication V2I permet de remonter les données à une unité centrale (ex : gestionnaire de trafic) pour une analyse plus globale de la circulation et une prédiction des risques à plus grande échelle[55].

En conclusion, les VANETs vont bien au-delà de la simple diffusion d'alertes post-accident. Ils permettent une évaluation continue et dynamique des risques en transformant le trafic en un système nerveux numérique. En analysant les données de conduite et l'environnement en temps réel, ils rendent possible la prédiction des accidents et des quasi-accidents, passant d'une logique de réaction à une logique de prévention active, ce qui constitue une avancée majeure pour la sécurité routière.

1.4.Sécurité routière (road safety) :

La communication Véhicule-à-Véhicule (V2V) est une technologie disruptive qui place la coopération entre les véhicules au cœur de la stratégie pour réduire les accidents de la route. Elle permet aux voitures de "dialoguer" entre elles pour partager leur position, leur vitesse et leur trajectoire, créant ainsi une conscience situationnelle à 360° qui dépasse largement le champ de vision du conducteur.

a. **Systèmes d'alerte de collision et freinage d'urgence coopératif :**

Le V2V permet de déployer des systèmes d'alerte avancés et proactifs qui anticipent le danger :

- Alerte de Collision Frontale : Si un véhicule à l'avant freine brutalement, il envoie instantanément un message d'alerte à tous les véhicules qui le suivent. Les conducteurs reçoivent alors un avertissement leur permettant de freiner plus tôt et d'éviter un carambolage, même si le véhicule dangereux est caché par un virage ou un autre camion[56].
- Alerte de Collision aux Intersections (Intersection Movement Assist) : C'est l'une des applications les plus cruciales. Le système avertit le conducteur lorsqu'il n'est pas sûr de s'engager à une intersection parce qu'un autre véhicule, caché par un bâtiment ou un autre obstacle, arrive à grande vitesse et risque de lui couper la route[56].

- Freinage d'Urgence Coopératif : Au-delà de l'alerte, le système peut déclencher des actions. Lorsqu'un risque de collision est détecté comme imminent et que le conducteur ne réagit pas, le véhicule peut actionner automatiquement les freins pour éviter ou atténuer la gravité de l'impact. Cette décision est prise en fonction des données reçues des véhicules environnants, bien plus rapidement qu'un humain ne pourrait le faire[56].

b. Contribution des VANETs à la réduction des accidents :

Les VANETs (le réseau qui permet le V2V) contribuent directement à la sécurité routière en adressant les causes majeures d'accidents :

- Compensation des Limites Humaines : Ils comblent les angles morts et voient "au travers" des obstacles, offrant une perception bien plus complète de l'environnement que les capteurs individuels d'une voiture (radars, caméras) qui ont une portée limitée[56].
- Anticipation du Danger : Contrairement aux systèmes embarqués classiques qui réagissent à un danger déjà visible, le V2V prévient le danger en amont. Il transforme la sécurité d'une logique réactive (freiner après un choc) à une logique prédictive et proactive (éviter le choc) [56].
- Efficacité dans des Scénarios Complexes : Le V2V est particulièrement efficace dans les situations où la visibilité est réduite et où les conducteurs sont les plus vulnérables (intersections, dépassements sur routes à deux voies, changements de file par mauvaise visibilité) [56].

En conclusion, la communication V2V, en permettant aux véhicules de coopérer et de partager des informations en temps réel, agit comme un système d'alerte collective. Elle constitue une avancée majeure pour prévenir les accidents, en particulier les collisions latérales et frontales aux intersections, qui sont parmi les plus graves. En étendant la perception des véhicules au-delà de la ligne de mire, les VANETs s'imposent comme une technologie clé pour la sécurité routière de demain, avec pour objectif ultime de sauver des vies et de réduire significativement le nombre d'accidents.

2. Service :

2.1. Prise en compte de l'environnement (environment consideration):

Le secteur des transports est un contributeur majeur à la pollution atmosphérique (émissions de CO2, NOx, particules fines) et à la congestion routière dans les zones urbaines. La gestion traditionnelle du trafic, souvent réactive et basée sur des capteurs fixes, montre ses limites.

a. Le mécanisme central (l'optimisation du trafic) :

Les VANETs introduisent une gestion proactive et dynamique du trafic. Grâce à la communication véhicule-véhicule (V2V) et véhicule-infrastructure (V2I), les données circulent en temps réel[57]. Cela permet :

- Une fluidification du trafic : En évitant les embouteillages et les ralentissements, les véhicules passent moins de temps à l'arrêt ou en accélération/freinage répétitifs, phases très polluantes.
- Une réduction des temps de parcours : Des trajets plus directs et optimisés signifient une distance parcourue et une durée de fonctionnement du moteur réduites.

b. Les applications concrètes pour l'environnement :

Il y a plusieurs applications VANET qui ont un impact direct sur la réduction de l'empreinte écologique :

- Systèmes d'Information sur le Trafic et de Routage : Les véhicules partagent en temps réel des informations sur l'état de la route (congestion, accident). Les systèmes de navigation calculent alors des itinéraires « verts » ou éco-optimisés, qui minimisent la consommation de carburant et les émissions, et non seulement le temps de trajet[57].
- Gestion Intelligente des Feux de Signalisation : Les feux de circulation, connectés (V2I), peuvent recevoir des données des véhicules approchant (nombre, vitesse) [57]. Ils adaptent leur cycle pour :
  - Créer des « vagues vertes » : Synchroniser les feux pour qu'un groupe de véhicules puisse passer sans s'arrêter, réduisant ainsi les cycles d'arrêt/démarrage très énergivores.
  - Donner la priorité aux transports en commun ou aux véhicules électriques dans certaines zones, encourageant ainsi les modes de déplacement durables.

- Assistance à l'Éco-Conduite : Les VANETs peuvent fournir aux conducteurs des recommandations en temps réel pour une conduite plus économique (ex : conseil de vitesse constante, anticipation des ralentissements) [57].

c. Le bénéfice environnemental direct :

Le résultat direct de ces optimisations est une diminution significative de la consommation de carburant (essence, diesel) et, par conséquent, une réduction des émissions de gaz à effet de serre (CO2) et des polluants locaux (NOx, particules). L'article souligne que cet impact est collectif : même une légère amélioration pour chaque véhicule, multipliée par le nombre total de véhicules, conduit à un gain environnemental majeur à l'échelle d'une ville ou d'une région[57].

d. Défis et perspectives :

- Déploiement à grande échelle : L'efficacité des VANETs est proportionnelle au taux d'équipement des véhicules et des infrastructures.
- Développement d'algorithmes robustes : Il faut des algorithmes de routage et de gestion du trafic intelligents capables de traiter les données en temps réel et de prendre les meilleures décisions pour fluidifier le trafic.
- Sécurité et confidentialité : La fiabilité des données échangées est primordiale. Un système doit être protégé contre les intrusions malveillantes qui pourraient, par exemple, créer des embouteillages artificiels.

En conclusion, les VANETs ne sont pas seulement une technologie pour améliorer la sécurité routière ou le confort de conduite. Ils représentent un outil puissant pour une gestion plus écologique et durable des systèmes de transport. En transformant le réseau routier en un système intelligent et communicant, ils permettent d'optimiser l'utilisation des infrastructures existantes et de réduire significativement l'impact environnemental de la mobilité, contribuant ainsi aux objectifs de villes intelligentes et durables (smart cities).

2.2. Gestion des intersections :

Les intersections sont des points noirs de la sécurité routière, où les limitations de visibilité et les erreurs de jugement humain conduisent à de nombreux accidents graves (collisions latérales, frontales, etc.).

Le système proposé repose sur l'échange continu et automatique de messages entre les véhicules approchant d'une intersection et, potentiellement, avec une unité routière (RSU - Road Side Unit) située à l'intersection.

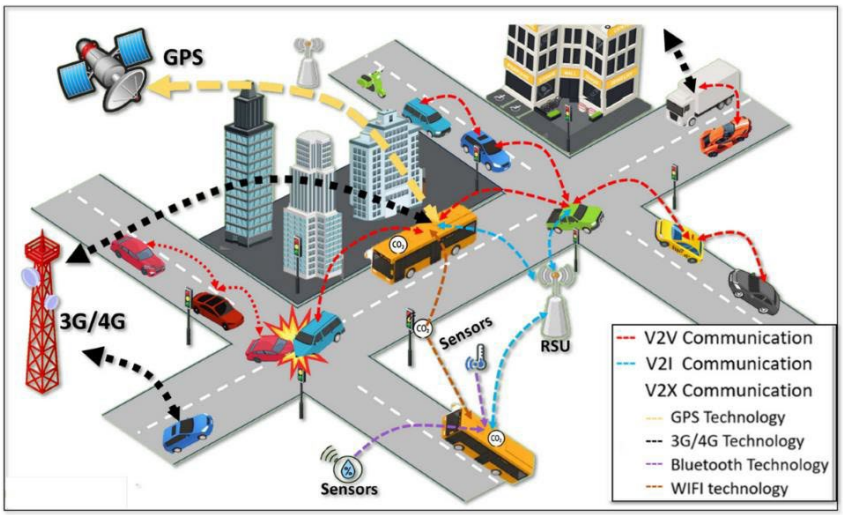


Figure 8: Environnement VANET avancé intégrant des systèmes hétérogènes avec la technologie IoT pour la surveillance des applications [67]

- **Les Messages Échangés** : Chaque véhicule équipé diffuse périodiquement des messages de type beacon (ou messages de sécurité de base) contenant des données cruciales en temps réel : Sa position (via GPS), sa vitesse, sa direction, son accélération/décélération, sa trajectoire prévue (tourne à gauche, à droite, va tout droit) [58].

a. Fonctionnement du système de prévention de collision :

- **Phase 1 : Collecte et Partage des Données**

Les véhicules entrant dans un périmètre défini autour de l'intersection commencent à émettre et à recevoir des messages beacon. Une RSU à l'intersection peut agréger toutes ces données pour avoir une vue complète de la situation[58].

- **Phase 2 : Évaluation du Risque de Collisio :**

Un algorithme déterministe est utilisé. En se basant sur les données dynamiques reçues (position, vitesse), le système calcule la trajectoire prévisible de chaque véhicule. Il effectue une prédiction de la zone de conflit potentielle dans l'intersection. L'algorithme vérifie si les trajectoires prévues de deux ou plusieurs véhicules vont occuper le même point de l'espace au même moment (TTC - Time To Collision) [58].

- **Phase 3 : Diffusion de l'Alerte :**

Dès qu'un risque de collision est identifié, un message d'alerte est généré. Ce message est diffusé de manière prioritaire et fiable (en utilisant des protocoles de routage adaptés aux situations critiques) à tous les véhicules concerné[58]s. L'alerte peut être reçue :

- Directement des autres véhicules (mode V2V).
- Via la RSU (mode V2I), qui peut ensuite relayer l'information à tous les véhicules à proximité.

- **Phase 4 : Interface avec le Conducteur :**

À la réception de l'alerte, le système embarqué du véhicule avertit le conducteur par des signaux sonores, visuels (HMI - Interface Homme-Machine) ou même haptiques (vibrations du volant ou du siège). L'objectif est de donner au conducteur le maximum de temps pour réagir et éviter la collision (freiner, modifier sa trajectoire) [58].

b. **Avantages par rapport aux systèmes traditionnels :**

Les bénéfices spécifiques de cette approche VANET :

- **Perception Au-Delà de la Ligne de Vue** :

Le système "voit" à travers les obstacles (bâtiments, autres véhicules stationnés) et anticipe le danger avant même que le conducteur ne puisse le percevoir[58].

- **Temps de Réaction Accru** :

L'alerte est générée beaucoup plus tôt qu'avec les réflexes humains seuls, ce qui est crucial pour éviter les accidents à haute vitesse[58].

- **Approche Collaborative** :

Le système ne dépend pas d'un seul capteur (ex : caméra d'un véhicule). Il fusionne les données de multiples sources (tous les véhicules à proximité), le rendant plus robuste et fiable[58].

c. Défis et limitations abordés :

- **La Latence** :

La communication et le traitement des données doivent être extrêmement rapides (faible latence) pour que l'alerte soit utile. Tout délai peut rendre le système inefficace[58].

- **La Fiabilité des Communications** :

Le protocole de communication doit garantir une livraison fiable des messages d'alerte, même dans des conditions de canal radio difficiles (bruit, interférences) [58].

- **Le Taux de Pénétration** :

L'efficacité du système est maximale lorsque la majorité des véhicules sont équipés. Avec un faible taux d'équipement, certains véhicules "non-connectés" restent invisibles pour le système et constituent un risque[58].

- **La Sécurité** :

La thèse souligne la nécessité de sécuriser les communications pour éviter les cyberattaques qui pourraient générer de fausses alertes (dénis de service) avec des conséquences dramatiques[58].

2.3. Congestion du trafic :

L'approche traditionnelle de gestion du trafic repose souvent sur des capteurs fixes (boucles inductives, caméras) et des centres de contrôle centralisés. La thèse souligne les limites de cette approche : latence, coût, et manque de granularité.

L'innovation centrale de cet article est d'utiliser les véhicules eux-mêmes comme un réseau massif de capteurs mobiles et intelligents. En communiquant entre eux (V2V) et avec l'infrastructure (V2I), ils créent une image temps réel, hyper précise et décentralisée de l'état du trafic[58].

a. Mécanismes concrets de réduction de la congestion :

- **Gestion Dynamique et Collaborative des Feux de Signalisation** :

  - **Problème** : Les feux de circulation pré-programmés sont inefficaces car ils ne s'adaptent pas aux variations de trafic en temps réel[59].
  - **Solution proposée :** Les véhicules approchant d'une intersection communiquent leur état (vitesse, position, destination) à une Unité Routière (RSU) qui contrôle les feux[59].
  - **Bénéfice** : Le système de feux peut ainsi adapter dynamiquement sa séquence et sa chronométrie[59]. Par exemple, il peut :

- Prolonger la phase verte si un grand nombre de véhicules approchent.
- Créer des "vagues vertes" (green waves) en synchronisant plusieurs feux consécutifs pour qu'un peloton de véhicules puisse passer sans s'arrêter, éliminant ainsi les arrêts/redémarrages qui créent des accordéons et consomment du carburant.
- Donner la priorité à certains véhicules (transports en commun, véhicules d'urgence) pour améliorer l'efficacité globale du réseau.

- **Routage et Navigation Collaboratifs et Dynamiques** :

  - Problème : Les GPS traditionnels calculent un itinéraire optimal pour un seul véhicule, sans considération pour l'impact collectif. Si tous les véhicules sont dirigés vers le même itinéraire de délestage, ils y créent un nouvel embouteillage[59].
  - Solution proposée : Les véhicules partagent des informations sur les conditions de trafic. Un système central ou décentralisé peut alors calculer des itinéraires "socialement optimaux"[59].
  - Bénéfice : Le trafic est équilibré sur l'ensemble du réseau routier. Au lieu que tous les véhicules prennent le chemin le plus court, ils sont répartis sur plusieurs chemins pour minimiser le temps de trajet global de l'ensemble des usagers. Cela évite la saturation des axes secondaires.

- **Coopération pour les Manœuvres Complexes (ex : Fusion de files)** :

  - Problème : Les zones de travaux ou les bretelles d'autoroute où les véhicules doivent fusionner sont des points de conflit majeurs qui ralentissent considérablement le flux.
  - Solution proposée : Grâce au V2V, les véhicules peuvent coordonner leurs manœuvres. Un véhicule sur la voie principale peut légèrement ralentir ou accélérer pour créer un espace sécuritaire permettant à un véhicule de fusionner sans forcer un ralentissement brutal.
  - Bénéfice : La fusion se fait de manière fluide et coopérative, maintenant une vitesse moyenne plus élevée et évitant le phénomène de "bouchon fantôme" qui naît d'un seul coup de frein.

b. **Résultat et impact attendu :**

Les modèles et simulations présentés dans la thèse démontrent que ces systèmes collaboratifs permettent de :

- Augmenter la Fluidité du Trafic : Réduction significative des temps d'arrêt et des variations de vitesse[59].
- Augmenter le Débit des Intersections : Plus de véhicules peuvent traverser une intersection dans un laps de temps donné grâce à une gestion plus intelligente des feux[59].
- Réduire la Durée et l'Étendue des Congestions : Les embouteillages se forment moins souvent et se dissipent plus rapidement grâce à une réaction dynamique et un reroutage intelligent[59].
- Réduire la Consommation de Carburant et les Émissions : C'est une conséquence directe de la fluidification du trafic. Moins d'arrêts et de redémarrages signifie une combustion plus efficace et donc moins de CO2 et de particules fines rejetées dans l'atmosphère[59].

c. **Défis techniques abordés :**

La mise en œuvre de ces systèmes dépend de la résolution de défis de taille :

- **La Latence Ultra-Faible** : Les messages d'alerte et de contrôle doivent être transmis et traités en quelques millisecondes pour être efficaces.
- **La Fiabilité des Communications** : Le système doit fonctionner parfaitement même dans des conditions météorologiques défavorables ou en situation de trafic dense où les canaux de communication sont encombrés.
- **L'Interopérabilité et le Déploiement Progressif** : Le système doit être capable de fonctionner avec un taux de pénétration initial faible (seulement une fraction des véhicules équipés) tout en promettant des bénéfices croissants à mesure que plus de véhicules rejoignent le réseau.

L'impact sur la congestion n'est pas présenté comme un simple effet secondaire, mais comme le résultat direct d'algorithmes de contrôle sophistiqués qui transforment le réseau routier d'une collection d'entités individuelles en un système intégré et coopératif. Cette approche représente l'avenir de la gestion du trafic et une avancée majeure vers des villes plus fluides et plus durables.

2.4. Identification des régions à risque (region identification) :

Cette ressource de l'PIARC est un guide de bonnes pratiques destiné aux gestionnaires de réseaux routiers. Elle ne parle pas spécifiquement des VANETs, mais elle décrit le processus fondamental et critique d'identification proactive des risques sur le réseau routier. Son objectif est de permettre aux autorités de localiser et de traiter les points noirs (zones à haut risque d'accidents) et les zones de congestion récurrente avant que des accidents graves ne se produisent.

Le processus classique d'identification des risques, tel que décrit par la PIARC, repose sur l'analyse d'accidents déjà survenus (données historiques) et sur des études de trafic coûteuses et ponctuelles. Les VANETs transforment cette approche en une surveillance continue, granulaire et proactive.

a. La révolution des données : du réactif au proactif :

- **Méthode Traditionnelle (PIARC)** : On collecte manuellement les données de police d'accidents, on les géolocalise et on analyse les statistiques a posteriori pour trouver des corrélations[60]. C'est réactif.

- **Méthode VANET** : Les véhicules deviennent des capteurs mobiles continus. Ils génèrent en temps réel une quantité massive de données dynamiques[60] :
  - Données de Conduite : Vitesse, accélération, freinage brusque, activation de l'ABS/ESP, déclenchement des airbags.
  - Données de Trafic : Densité de véhicules, vitesse moyenne, temps d'arrêt.
  - Données Environnementales : Détection de chaussée glissante (via l'ESP), visibilité réduite (activation des phares automatiques, des essuie-glaces).

b. **Mécanismes concrets d'identification des zones à risque :**

Les VANETs identifient les risques non seulement par les accidents avérés, mais surtout par les précurseurs d'accidents (near-misses, comportements à risque) [60].

- **Cartographie des Points de Conflit (Near-Miss Detection)** :
  - Fonctionnement : Un freinage brusque et important (Hard Braking) d'un véhicule est un indicateur puissant d'un évitement de dernière minute ou d'un danger perçu. Grâce au V2V, cet événement peut être rapporté à un serveur central[60].
  - Résultat : En agrégant des milliers de ces événements, une carte thermique des "points de conflit" émerge. Ces points, où les conducteurs sont obligés de manœuvrer brusquement, identifient les zones dangereuses avant qu'un accident grave n'y survienne. C'est de l'identification proactive pure[60].

- **Cartographie des Zones de Congestion** :
  - Fonctionnement : Les véhicules rapportent en continu leur position et leur vitesse. Une chute collective et répétée de la vitesse moyenne sur un tronçon spécifique aux heures de pointe est un indicateur clair de congestion récurrente[60].
  - Résultat : Création de cartes de congestion en temps réel et historiques, bien plus précises que celles obtenues par des boucles inductives fixes, car elles couvrent l'ensemble du réseau et pas seulement les principaux axes[60].

- **Identification des Conditions Routières Dangereuses** :
  - Fonctionnement : Si plusieurs véhicules signalent une perte d'adhérence (via les données de l'ESP) ou activent leurs essuie-glaces à plein régime sur un même virage, le système peut en déduire la présence de verglas ou d'aquaplaning à cet endroit précis[60].
  - Résultat : Cartographie dynamique des risques environnementaux temporaires, permettant d'avertir les autres usagers en approchant et d'alerter les services de voirie pour un traitement ciblé[60].

c. Le processus VANET d'identification des risques :

- **Collecte Massive de Données** : Les véhicules équipés collectent en permanence des données de conduite et d'environnement[60].

- **Communication** : Via V2I (avec des Road Side Units) ou via le réseau cellulaire (4G/5G), ces données sont transmises à une plateforme centrale de gestion du trafic et de la sécurité[60].

- **Aggrégation et Analyse (Big Data)** : Des algorithmes analysent ces téraoctets de données pour [60]:
  - Détecter des anomalies (ex : un freinage brusque est anormal sur une ligne droite dégagée).
  - Trouver des corrélations spatiales et temporelles (ex : tous les vendredis soir, la vitesse chute à ce carrefour).
  - Générer des cartes thermiques des risques.

- **Validation et Action** : Les autorités routières reçoivent ces cartes précises et peuvent [60]:
  - Prioriser les interventions : Un point avec de nombreux "near-misses" devient une priorité plus haute qu'un point avec un seul accident historique.
  - Diagnostiquer la cause racine : La nature des données (freinages, perte d'adhérence) peut aider à comprendre le problème (visibilité insuffisante, revêtement défectueux, gabarit trop large).
  - Évaluer l'efficacité des correctifs : Après avoir modifié une intersection (nouvelle signalisation, rond-point), on peut mesurer objectivement si le nombre de freinages brusques a diminué.

Aspect	Méthode Traditionnelle (PIARC)	Apport des VANETs
Type de données	Données d'accidents (historiques, réactives)	Données de conduite (temps réel, proactives)
Granularité	Ponctuelle, par accident	Continue, massive, à l'échelle du mètre
Indicateur clé	Accidents avérés	Précurseurs d'accidents (freinages brusques, perte d'adhérence)
Cartographie	Carte des points noirs a posteriori	Carte thermique des risques a priori
Coût	Élevé (enquêtes terrain, manuel)	Faible (automatisé, données passives)

Tableau 1

Ce tableau présente **une comparaison entre la méthode traditionnelle d'analyse de la sécurité routière et l'apport révolutionnaire des réseaux VANET.**

Les VANETs ne se substituent pas au cadre méthodologique de la PIARC ; elles le rendent infiniment plus puissant, précis et proactif. Elles permettent de passer d'une analyse statique et réactive des accidents à une analyse dynamique et prédictive des risques, transformant radicalement la façon dont nous concevons la sécurité routière et la gestion du trafic.

3. Réseau :

3.1. Contrôle de la gestion :

Un trop grand nombre de véhicules essayant de communiquer en même temps va saturer le canal, entraînant des pertes de paquets, des retards et une incapacité à transmettre les messages urgents.

a. La saturation du canal radio (canal CCH - Control Channel) :

- **Le Problème du Broadcast Storm** : Dans un environnement VANET dense (ex : un embouteillage sur une autoroute ou à un feu rouge), chaque véhicule émet périodiquement des messages de beacon (état du véhicule) et peut relayer des messages d'alerte. Ceci crée un nombre exponentiel de transmissions, conduisant à des collisions de paquets et à une dégradation générale des performances du réseau[61].
- **Conséquence** : Les messages de sécurité, qui sont prioritaires, se retrouvent noyés dans la masse des messages de routine et ne peuvent plus être diffusés efficacement, annulant ainsi le principal avantage des VANETs en matière de sécurité[61].

b. Un système intelligent de contrôle de la congestion :

Un ensemble de protocoles pour réguler intelligemment le trafic de données :

- **Adaptation Dynamique de la Fréquence d'Émission (Beacon Rate Adaptation) :**
  - **Principe** : Au lieu d'émettre des messages beacon à une fréquence fixe, les véhicules ajustent dynamiquement leur taux d'émission en fonction de la densité de trafic et de la charge du réseau[61].
  - **Fonctionnement** : Si le système détecte une congestion du canal (nombre élevé de collisions, délais de transmission), il ordonne aux véhicules de réduire la fréquence de leurs messages de routine. Inversement, si le canal est libre, la fréquence peut être augmentée pour une meilleure awareness[61].

- **Contrôle de Puissance d'Émission (Power Control) :**
  - **Principe** : Ajuster la puissance de transmission radio pour couvrir juste la zone nécessaire[61].
  - **Fonctionnement** : Dans un embouteillage très dense, les véhicules n'ont pas besoin de communiquer avec des véhicules très éloignés. En réduisant la puissance d'émission, on réduit la portée de chaque message, ce qui diminue les interférences et le nombre de véhicules en compétition pour le même canal. Cela permet de créer des "bulles" de communication plus petites et plus efficaces[61].

- **Priorisation et Filtrage des Messages :**
  - **Principe** : Implémenter des algorithmes de qualité de service (QoS) pour différencier le trafic[61].
  - **Fonctionnement** : Les messages sont classés par criticité (ex : message de collision imminente > message de freinage brusque > message beacon de routine). En situation de congestion, le système peut mettre en file d'attente ou supprimer les messages de priorité faible pour garantir que les messages de priorité haute soient traités et transmis immédiatement[61].

- **Algorithmes de Prédiction et de Prise de Décision Distribuée :**
  - L'article suggère l'utilisation de techniques avancées, potentiellement basées sur l'intelligence artificielle ou l'apprentissage automatique, pour anticiper les pics de congestion et ajuster les paramètres de communication (fréquence, puissance) de manière proactive plutôt que réactive[61].

c. Avantage et impact de cette gestion :

La mise en œuvre d'un tel système de contrôle de la congestion des données permet de :

- **Garantir la Fiabilité des Messages Critiques** : Assurer que les alertes de sécurité vitales (évitement de collision, obstacle sur la route) ont toujours la bande passante nécessaire pour être délivrées à temps[61].

- **Maintenir la Stabilité du Réseau** : Éviter l'effondrement complet des communications en situation de trafic dense, maintenant un niveau de service acceptable pour toutes les applications[61].

- **Optimiser l'Utilisation des Ressources** : Réduire la consommation d'énergie des terminaux embarqués en évitant des transmissions inutiles[61].

- **Rendre les VANETs Scalables** : Permettre au système de fonctionner efficacement même avec un très grand nombre de véhicules connectés, ce qui est une condition essentielle pour un déploiement réel à grande échelle[61].

On conclut que les mécanismes nécessaires pour éviter que l'outil même qui doit fluidifier le trafic (les VANETs) ne soit victime de son propre succès en générant un "embouteillage de données". Cette approche est complémentaire et indispensable aux travaux sur la réduction de la congestion routière. Elle assure que le système nerveux numérique des véhicules connectés reste opérationnel dans les conditions les plus exigeantes, transformant ainsi une vision théorique en une solution pratique et robuste pour les transports intelligents de demain.

3.2. Protocole de routage :

Les protocoles de routage dans les VANETs (comme AODV, OLSR, ou leurs variantes géographiques comme GPSR) doivent fonctionner dans des conditions extrêmes qui exacerbent les problèmes de sécurité :

- **Topologie Dynamique et Délestage Rapide** : La vitesse des véhicules entraîne une topologie de réseau qui change constamment et très rapidement. Les routes réseau sont éphémères, ce qui rend difficile l'établissement d'une confiance stable entre les nœuds.

- **Absence d'Infrastructure Centralisée** : En mode V2V pur, il n'y a pas d'autorité centrale pour valider les actions des nœuds en temps réel. Chaque véhicule doit être capable d'évaluer seul la crédibilité des informations qu'il reçoit.

- **Canaux de Communication Ouverts et Vulnérables** : Les communications sans fil (ex : DSRC, C-V2X) sont facilement accessibles, permettant à un attaquant d'écouter, d'injecter ou de modifier des messages.

a. Les menaces sur le routage :

Un protocole de routage non sécurisé dans un VANET ouvre la porte à des attaques catastrophiques :

- **Usurpation d'Identité (Sybil Attack)** : Un attaquant crée de multiples identités fictives pour faire croire à un embouteillage fictif ou, au contraire, pour masquer la présence d'un véhicule réel. Cela peut tromper les systèmes de régulation du trafic et provoquer des accidents[62].

- **Annonces de Routes Malveillantes** : Similaire au "hijacking" BGP, un nœud malveillant peut annoncer de fausses routes pour[62] :
  - Détourner le trafic : Intercepter des messages critiques pour les bloquer ou les modifier.
  - Créer des Déni de Service (DoS) : Isoler un véhicule ou une zone du réseau en annonçant de fausses routes qui mènent à nulle part, empêchant la réception d'alertes de sécurité.
  - Créer un Chaos Routier : En annonçant de fausses informations sur l'état du trafic (bouchon fictif), l'attaquant peut inciter les conducteurs à emprunter un autre itinéraire, créant des congestions ailleurs.

- **Modification ou Rejeu de Messages** : Un attaquant peut capturer un message valide (ex : "Accident à la position X") et le rejouer plus tard ou à un autre endroit, semant la confusion et induisant en erreur les conducteurs et les systèmes[62].

b. L'importance cruciale des protocoles de routage sécurisés :

Sécuriser le protocole de routage n'est pas une option, c'est le fondement indispensable d'un VANET fiable. Les mécanismes de sécurité doivent garantir :

- **Authentification et Intégrité des Messages** : Chaque message (alerte, beacon de position, message de routage) doit être signé cryptographiquement par son émetteur. Cela permet à tout récepteur de vérifier que le message vient bien d'un véhicule légitime et qu'il n'a pas été altéré en transit. C'est l'équivalent du RPKI pour les VANETs[62].

- **Validation de la Position** : Pour lutter contre les attaques Sybil, le protocole doit intégrer des mécanismes pour vérifier que la position annoncée par un véhicule correspond bien à sa position réelle (par exemple via des preuves cryptographiques liées à la localisation) [62].

- **Confidentialité et Préservation de la Vie Privée** : Bien que les messages de sécurité doivent être authentifiés, il est crucial que l'identité réelle et le trajet complet d'un véhicule ne puissent pas être tracés par des entités malveillantes. Les certificats pseudonymes, changés régulièrement, sont une solution courante[62].

- **Résilience et Détection des Nœuds Malveillants** : Le protocole doit inclure des mécanismes de réputation ou de consensus pour identifier et isoler rapidement les nœuds qui propagent des informations erronées, sans pénaliser les nœuds honnêtes qui font des erreurs dues aux conditions difficiles du canal[62].

La fiabilité des communications VANETs, qui se mesure en vies sauvées et en accidents évités, repose entièrement sur la robustesse de ses protocoles de routage sous-jacents. Adapter les principes de sécurité des infrastructures de routage Internet (comme ceux évoqués dans la thèse) au contexte contraint et critique des VANETs est un défi de recherche majeur.

Un protocole de routage sécurisé pour VANET doit donc être :

- **Vérifiable** : Chaque information de routage et de sécurité peut être authentifiée.
- **Résilient** : Capable de fonctionner même en présence de nœuds malveillants.
- **Efficace** : Ajouter un minimum de surcharge (latence, bande passante) pour respecter les contraintes temporelles critique.

Sans cette sécurisation, les VANETs ne pourront pas être déployés de manière fiable, car le risque de cyberattaques ayant des impacts physiques réels serait bien trop élevé. La sécurité du routage n'est pas une couche supplémentaire ; c'est la colonne vertébrale qui rend l'ensemble du système digne de confiance.

3.3. Diffusion des données :

La diffusion (broadcast) est un mode de communication primordial pour propager des messages de sécurité (ex : accident, freinage brusque) à tous les véhicules dans une zone pertinente. Cependant, cette tâche est rendue complexe par la nature hautement dynamique du réseau et la criticité des données. Cet article souligne que les stratégies de diffusion doivent simultanément répondre à deux impératifs : l'efficacité (pour garantir une livraison rapide et sans encombrement) et la sécurité (pour empêcher toute manipulation malveillante).

a. Les défis :

La conception de stratégies de diffusion efficaces et sécurisées se heurte à plusieurs obstacles majeurs :

- **Topologie très dynamique** : La vitesse et la direction changeante des véhicules entraînent une connectivité réseau constamment fluctuante et imprévisible[63].

- **Ressources limitées** : La bande passante du canal de communication (souvent dédiée, comme la bande 5.9 GHz) est une ressource rare qui doit être optimisée pour éviter la saturation et les collisions[63].

- **Congestion du réseau** : Une diffusion naïve (flooding) où chaque nœud retransmet tout message entraîne rapidement une explosion du trafic, un phénomène appelé "broadcast storm", qui paralyse le réseau[63].

- **Exigences de faible latence** : Les messages de sécurité doivent être délivrés en quelques millisecondes pour être utiles[63].

b. Stratégies pour une diffusion efficace :

L'objectif est de réduire la redondance et la congestion tout en assurant une couverture maximale et un délai minimal. Plusieurs techniques intelligentes sont employées :

- **Dissémination basée sur le regroupement (Clustering)** :

Les véhicules sont organisés en groupes ("clusters") avec un "cluster head" (chef de groupe) élu. Seul le cluster head est responsable de la retransmission des messages vers les autres clusters. Cette stratégie réduit considérablement le nombre de retransmissions redondantes. L'élection du cluster head peut se baser sur des métriques de stabilité comme la vitesse, la direction et la position[63].

- **Dissémination basée sur la position (Zone-based / Geocast)** :

La retransmission d'un message est déclenchée en fonction de la zone géographique. Par exemple, seuls les véhicules situés dans une "Zone of Relevance" (ZoR) autour d'un événement (comme un accident) reçoivent et relaient le message. Les véhicules quittant la zone arrêtent de le propage[63]r.

- **Techniques de suppression intelligente de redondance** :
  - **Délai aléatoire avant retransmission** : Chaque véhicule attend un délai aléatoire avant de retransmettre un message. S'il entend une autre retransmission du même message pendant ce délai, il annule la sienne, évitant ainsi les doublons[63].

  - **Détermination de la pertinence de la retransmission** : Un véhicule ne retransmet un message que s'il estime apporter une couverture supplémentaire (ex : s'il se trouve en bordure de la zone déjà couverte par les transmissions précédentes). Des algorithmes utilisent la position des voisins pour prendre cette décision[63].

c. Stratégies pour une diffusion sécurisée :

L'efficacité est vaine si les messages peuvent être falsifiés. La sécurité est donc imbriquée dans le processus de diffusion[63].

- **Authentification et Intégrité des Messages** : Chaque message critique doit être signé numériquement à l'aide d'un certificat émis par une Autorité Certificatrice (CA). Cela permet à tout récepteur de vérifier l'origine du message et de s'assurer qu'il n'a pas été altéré pendant la transmission. C'est la pierre angulaire de la sécurité[63].

- **Gestion des Certificats et Vie Privée** :
  - **Certificats Pseudonymes** : Pour préserver la vie privée des conducteurs et éviter le traçage, les véhicules utilisent une pile de certificats pseudonymes changés fréquemment. Ainsi, l'identité réelle du véhicule est dissociée de ses messages[63]

.

- **Révocation** : Un mécanisme robuste doit exister pour révoquer rapidement les certificats des véhicules malveillants ou compromis, les empêchant de participer au réseau[63].

- **Détection et Atténuation des Attaques** :
  - **Détection des attaques Sybil** : Des mécanismes basés sur la cohérence des positions annoncées, des tests de proximité radio ou l'analyse de la réputation permettent d'identifier un véhicule qui crée de multiples identités fictives[63].

  - **Résilience aux attaques par replay** : L'inclusion d'un horodatage ("timestamp") ou d'un séquencement dans les messages signés permet de rejeter les vieux messages rejoués[63].

  - **Tolérance aux pannes byzantines** : Les protocoles doivent être conçus pour fonctionner correctement même si un certain nombre de nœuds sont malveillants et tentent de diffuser de fausses informations[63].

d. L'équilibre (Efficacité vs surcharge de sécurité) :

Le défi ultime est de trouver un équilibre. Les opérations cryptographiques (signature, vérification) introduisent une surcharge computationnelle et une latence. Une vérification de signature par chaque véhicule sur chaque message reçu peut rendre le système trop lent pour des applications temps réel[63].

- **Solutions hybrides et optimisées** :
  - **Vérification par lots (Batch Verification)** : Un véhicule peut vérifier un lot de plusieurs signatures en une seule opération mathématique, réduisant ainsi le temps de traitement global[63].

  - **Délégation de la vérification** : Dans les architectures V2I, une unité routière (RSU) plus puissante peut se charger de vérifier les signatures et de diffuser des attestations pour alléger la charge des véhicules[63].

La diffusion sécurisée et efficace dans les VANETs n'est pas un problème unique mais un ensemble de défis interconnectés. Une stratégie optimale doit combiner intelligemment :

- Un protocole de diffusion intelligent qui minimise les retransmissions redondantes (via le clustering, la zonification, etc.).
- Un cadre de sécurité robuste reposant sur la cryptographie à clé publique pour l'authentification et l'intégrité, sans oublier la préservation de la vie privée.
- Des mécanismes d'optimisation pour réduire la surcharge induite par la sécurité, afin de répondre aux contraintes de latence critiques des applications de sécurité routière.

La réussite du déploiement des VANETs dépendra de la capacité des chercheurs et ingénieurs à intégrer de manière transparente ces deux exigences – efficacité et sécurité – dans une architecture cohérente et performante.

3.4. Protocole MAC :

Les véhicules communiquent entre eux (V2V) et avec l'infrastructure routière (V2I) via un medium sans fil partagé. Le protocole MAC (Medium Access Control) est la couche protocolaire chargée de définir les règles d'accès à ce medium partagé. Son rôle est absolument crucial car il détermine comment les nœuds (véhicules) se coordonnent pour émettre leurs données sans se marcher sur les pieds, surtout dans un environnement extrêmement dynamique et dense comme une autoroute aux heures de pointe.

a. Les objectifs principaux du protocole MAC pour les VANETs :

Le protocole MAC doit concilier plusieurs impératifs souvent contradictoires :

- **Faible Latence** :

Garantir que les messages critiques (ex : alertes de collision) soient transmis avec un délai minimal et déterministe[64].

- **Haut Débit** :

Maximiser l'utilisation de la bande passante disponible pour supporter un grand nombre de véhicules et différents types de messages[64].

- **Évolutivité (Scalability)** :

Fonctionner efficacement aussi bien dans un trafic sparse (route de campagne) que dans des environnements très denses (embouteillages) [64].

- **Fiabilité** :

Assurer un taux de livraison élevé des paquets, même en conditions difficiles[64].

- **Gestion de la Priorité** :

Pouvoir prioriser les messages de sécurité sur les messages de confort[64] (ex : infotainment).

b. Les deux familles de protocoles MAC et leur adaptation aux VANETs :

- **Protocoles basés sur la congestion (CSMA/CA – Carrier Sense Multiple Access with Collision Avoidance)** :

- **Principe** :

C'est la méthode "politesse" : un véhicule écoute le canal ("carrier sense") et n'émet que si le canal est libre. S'il est occupé, il attend un temps aléatoire avant de réessayer (évitement de collision).

- **Exemple Standard** : Le protocole IEEE 802.11p (DSRC), pilier des VANETs, utilise une version adaptée du CSMA/CA[64].

- **Avantages** :
  - Simple à implémenter.
  - Flexible et efficace pour un trafic non structuré et peu dense.

- **Inconvénients majeurs dans les VANETs denses** :
  - Problème des collisions cachées : Deux véhicules hors de portée radio l'un de l'autre peuvent émettre en même temps vers un destinataire commun, causant une collision[64].
  - Indéterminisme : Le temps d'attente aléatoire ne garantit pas un délai de transmission maximal, ce qui est problématique pour les applications temps réel[64].
  - Effet de Tempête de Broadcast : Lorsque tous les véhicules tentent de diffuser un message d'alerte en même temps, le canal devient saturé et s'effondre[64].

- **Protocoles basés sur l'allocation de Ressources (TDMA – Time Division Multiple Access)** :

- **Principe** :

Le temps est divisé en intervalles fixes (frames), elles-mêmes subdivisées en tranches de temps (time slots). Chaque véhicule se voit attribuer un slot spécifique et exclusif pour émettre ses données[64].

- **Avantages** :
  - Déterminisme : Aucune collision, la latence est connue et garantie.
  - Efficacité dans les environnements denses : Évite par conception le problème des collisions cachées.
  - Gestion native de la priorité : On peut attribuer des slots dédiés aux messages urgents.

- **Inconvénients majeurs** :
  - Complexité de la synchronisation : Maintenir un calendrier de slots synchronisé entre des véhicules se déplaçant à haute vitesse est un défi technique énorme[64].
  - Surcharge de signalisation : Une partie de la bande passante doit être utilisée pour négocier et attribuer les slots entre les véhicules[64].
  - Inefficacité en faible densité : De nombreux slots restent inutilisés s'il y a peu de véhicules[64].

c. Rôle clé du MAC dans la gestion de la congestion et de la priorité :

Au-delà de l'accès basique, le protocole MAC joue un rôle actif dans la gestion du réseau :

- **Contrôle de la Congestion** :

Les protocoles MAC intelligents peuvent adapter dynamiquement leur comportement en fonction de la densité du trafic. Par exemple, dans un scénario de type CSMA, ils peuvent augmenter la taille de la fenêtre de contention (le temps d'attente aléatoire) pour réduire les collisions en situation dense[64].

- **Qualité de Service (QoS)** :

Le MAC est responsable de la priorisation. Dans IEEE 802.11p, cela se fait via les Enhanced Distributed Channel Access (EDCA) qui définit différentes catégories d'accès (AC). Les messages de sécurité sont assignés à une catégorie avec un temps d'attente inter-frame plus court et une fenêtre de contention plus petite, leur donnant une probabilité plus élevée d'accéder au canal rapidement par rapport à un message de confort[64].

d. Tendances et solutions :

Pour dépasser les limitations des approches purement CSMA ou TDMA, la recherche explore des solutions hybrides et nouvelles :

- **Protocoles Hybrides** :

Des approches qui combinent le meilleur des deux mondes. Par exemple, un système où une infrastructure (RSU) alloue des slots TDMA pour les messages critiques, tandis que le CSMA est utilisé pour les communications moins urgentes ou en faible densité[64].

Utilisation des Ondes Millimétriques (mmWave) et du C-V2X :

Les technologies émergentes comme le C-V2X (Cellular V2X) basé sur la 5G offrent de nouveaux schémas MAC (mode 4 basé sur la perception, mode 3 basé sur l'allocation réseau) qui promettent une meilleure fiabilité et une latence ultra-faible pour les communications de sécurité directes[64].

Le protocole MAC est bien plus qu'un simple gestionnaire d'accès au canal ; il est l'élément central qui détermine les performances, la fiabilité et l'évolutivité d'un VANET. Son rôle est de gérer le chaos inhérent à un réseau dense et mobile de véhicules pour transformer le medium partagé en une ressource ordonnée et prévisible.

Le choix et l'optimisation du protocole MAC sont donc des questions fondamentales pour garantir que les applications de sécurité vitale puissent fonctionner en temps réel, sans collision ni délai excessif, faisant de lui un pilier invisible mais indispensable de la conduite .

Conclusion :

Ce chapitre a démontré le rôle fondamental des Réseaux Ad hoc Véhiculaires (VANETs) dans l'amélioration de la sûreté routière, à travers leurs applications, leurs services et leurs mécanismes réseau. Les VANETs ne se limitent pas à une simple technologie de communication ; ils représentent une transformation profonde des écosystèmes de transport, les rendant plus intelligents, plus réactifs et plus résilients.

Au niveau des **applications**, nous avons vu comment les VANETs contribuent directement à la protection des usagers vulnérables, à la gestion des situations d'urgence, à l'évaluation proactive des risques et à la prévention active des accidents. En étendant la perception des véhicules au-delà de la ligne de vue et en permettant une diffusion ultra-rapide des alertes, ils constituent un outil puissant pour sauver des vies et réduire la gravité des accidents.

Sur le plan des **services**, l'impact des VANETs s'étend à l'optimisation de la mobilité dans son ensemble. Ils permettent une gestion dynamique et écologique du trafic, une réduction significative des congestions, une sécurisation des points de conflit comme les intersections, et une identification précise des zones à risque. Ainsi, ils participent activement à la construction de villes intelligentes et durables, en conciliant efficacité des déplacements et respect de l'environnement.

Enfin, la robustesse du **réseau** lui-même est la clé de voûte de cette infrastructure. Le contrôle de la congestion des données, la sécurisation des protocoles de routage, les stratégies de diffusion efficaces et les mécanismes d'accès au medium (MAC) garantissent que les communications critiques restent fiables, sécurisées et disponibles, même dans les conditions de trafic les plus exigeantes.

En synthèse, la valeur des VANETs réside dans leur capacité à créer un écosystème coopératif où les véhicules et les infrastructures collaborent pour former un système de transport intégré, plus sûr et plus efficace. Les défis restent nombreux — notamment en matière de sécurité, de déploiement à grande échelle et d'interopérabilité — mais le potentiel de cette technologie pour révolutionner la sûreté routière et la mobilité future est incontestable. Les VANETs s'imposent ainsi comme un pilier essentiel des systèmes de transport intelligents de demain.

Chapitre III

LA SECURITE *DANS LES VANETs – Etat de l'art*

Introduction 51
1. LES ATTAQUES ET LES MENACES 51
1.1. Infrastructure 51
1.2. Interface sans fil 52
1.3. Matériel et logiciel 57
1.4. Les capteurs d'entrées 61
2. Les défis de sécurité 62
2.1. La distribution de clés 62
2.2. Des contraintes temps Réel 65
2.3. La Topologie Dynamique 67
2.4. Challenges de vérification et de cohérence 70
3. Les Exigences 72
3.1. Protocoles de contrôle d'Accès 72
3.2. Disponibilité 76
3.3. Authentification 80

Chapitre III :
LA SÉCURITÉ dans LES VANETs

Introduction :

Dans les **VANETs** (Vehicular Ad-hoc Networks), la **sécurité** désigne l'ensemble des mécanismes, protocoles et politiques conçus pour garantir **la confidentialité, l'intégrité , l'authentification , la disponibilité et la non-répudiation** des données échangées entre les véhicules (V2V) et entre les véhicules et l'infrastructure routière (V2I).

L'objectif ultime est de protéger le réseau et ses utilisateurs contre les accès non autorisés, les attaques malveillantes et les pannes, afin d'assurer le bon fonctionnement des applications critiques (comme la sécurité routière) et non-critiques (confort des usagers).

1. LES ATTAQUES ET LES MENACES :

1.1. Infrastructure :

L'infrastructure joue un rôle crucial dans la sécurité des réseaux véhiculaires (VANETs). Elle comprend notamment les Road Side Units (RSUs) et les Autorités de Confiance (TA, STA, CTA) qui gèrent l'authentification, la distribution des clés et la révocation des certificats.

Cependant, cette dépendance à l'infrastructure introduit des vulnérabilités spécifiques :

- Les véhicules doivent s'authentifier auprès des autorités de confiance pour participer aux communications.
- La portée limitée des RSUs (environ 500 m) nécessite un déploiement dense et coûteux.
- La mobilité élevée des véhicules complique la gestion des sessions et des clés.
- La révocation des certificats (CRL) est difficile à distribuer sans infrastructure fiable et scalable.

Les attaques liées à l'infrastructure :

- **Attaques par Déni de Service (DoS/DDoS)** : Visent les RSUs ou les canaux de communication pour rendre les services indisponibles, par exemple : inondation de messages pour saturer la bande passante.
- **Impersonation / usurpation d'identité** : Un attaquant se fait passer pour une RSU légitime ou un véhicule autorisé et permet d'intercepter ou de modifier les messages. [20]
- **Attaque par rejeu (Replay attacks)** : Capture et retransmission de messages valides pour perturber le réseau.
- **Attaques sur les Certificats** : Vol ou falsification de certificats pour obtenir un accès illégitime. Difficulté à révoquer rapidement les certificats compromis. [20]

- **Attaques sur les CAN (Controller Area Network)** : Via des accès physiques ou des firmwares malveillants, un attaquant peut compromettre les calculateurs du véhicule [20].

Des solutions proposées :

- **Infrastructures à Clé Publique (PKI)** : Utilisation de certificats numériques pour l'authentification. [20]
- **Certificats anonymes à courte durée** : Pour préserver la vie privée tout en permettant la traçabilité. [20]
- **RSUs Sécurisées** : Renforcement de la sécurité des RSUs via des mécanismes cryptographiques avancés. [20]
- **Protocoles de Révocation Efficaces** : Utilisation de listes de révocation compressées (CRL) ou de méthodes distribuées. [20]
- **Systèmes de Détection d'Intrusions (IDS)** : Systèmes de détection d'intrusions pour identifier les comportements anormaux.[20]

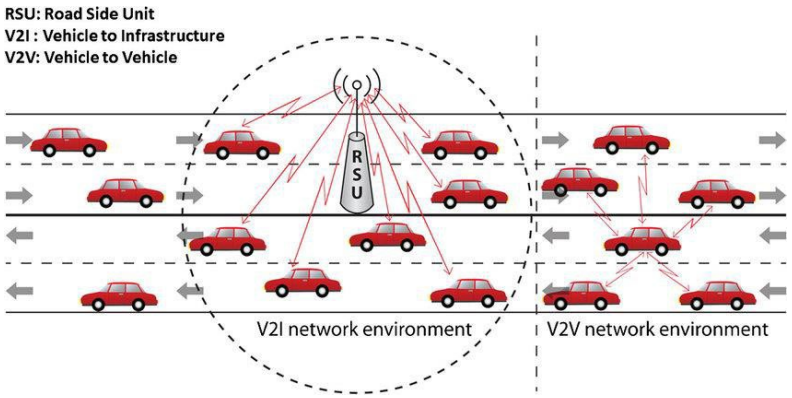


Figure 9 : communication VANET- basée sur l'infrastructure et sans infrastructure[65].

En conclusion, la sécurité de l'infrastructure des VANETs est un enjeu majeur qui nécessite des mécanismes robustes d'authentification, de gestion des clés et de détection d'intrusions. Les solutions existantes reposent largement sur une infrastructure centralisée, ce qui pose des défis en termes d'évolutivité, de coût et de résilience face aux attaques. Des approches hybrides et décentralisées sont envisagées pour renforcer la sécurité à l'avenir.

1.2. Interface sans fil :

L'interface sans fil est la porte d'entrée fondamentale pour la communication dans les VANETs (V2V et V2I), mais elle est aussi la plus exposée à une variété d'attaques. Les attaques visant cette couche exploitent la nature ouverte et partagée du medium de transmission.

a. Attaques par Déni de Service (DoS/DDoS) :

L'objectif est de rendre le canal de communication indisponible pour les nœuds légitimes. Un attaquant peut saturer le canal en émettant continuellement des messages, épuisant les

ressources des nœuds (qui passent leur temps à traiter des messages faux) ou en brouillant physiquement le signal radio (Jamming). Cela affecte à travers le blocage de la transmission de messages de sécurité critiques (ex : alertes de collision), pouvant entraîner des accidents et mettre des vies en danger.

- **Cas V2V** : Un attaquant envoie constamment un message “accident à la position Y”. Les véhicules victimes derrière lui reçoivent et traitent ce message en boucle, les empêchant d’accéder au réseau pour recevoir d’autres informations légitimes.[figure6]
- **Cas V2I** : Si un RSU (Roadside Unit) est continuellement engagé à vérifier des messages d’attaquants, les véhicules légitimes ne peuvent plus communiquer avec lui, rendant les services indisponibles.[figure 6]

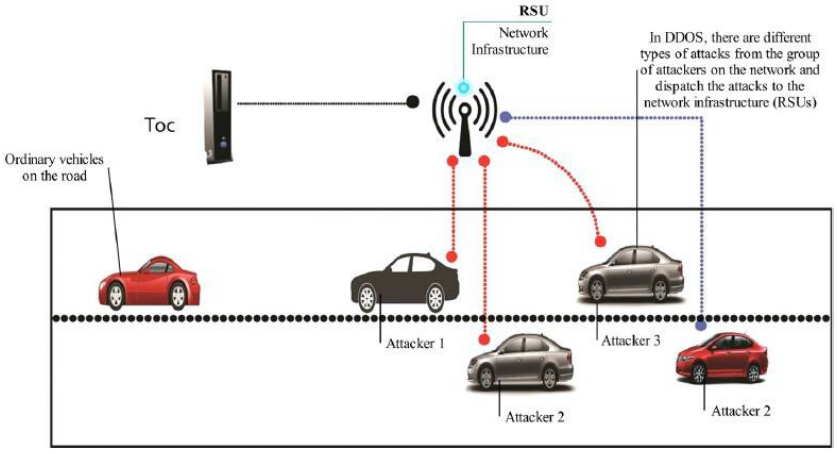


Figure 10 :DOS attaque [21]

b. Attaque Sybil :

Un seul véhicule malveillant se fait passer pour plusieurs véhicules en créant de multiples identités (sybil). Il peut ainsi fausser la perception du trafic ou l’issue de processus collaboratifs (comme le vote ou l’agrégation de données). Cela peut créer l’illusion d’un embouteillage massif ou d’un accident, incitant les autres conducteurs à changer d’itinéraire pour l’avantage de l’attaquant. Cela peut également perturber les protocoles de routage et la détection de mauvais comportements.[21]

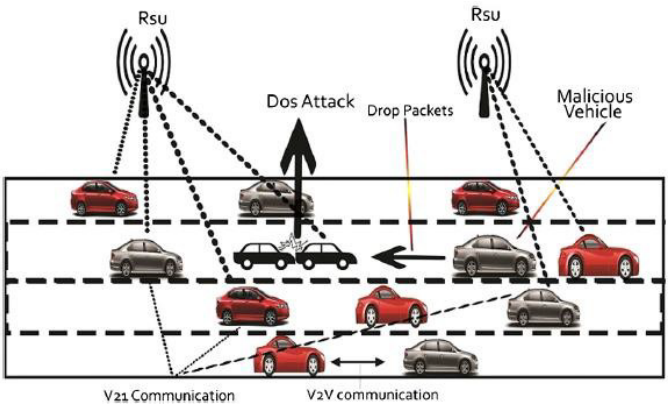


Figure 11 : attaque sybil [21]

Un attaquant génère de fausses identités pour simuler plusieurs véhicules, croyant à une situation réelle, délaissent la route, laissant l'attaquant circuler librement.[figure7]

c. Brouillage (jamming attack) :

Attaque physique où l'attaquant émet un signal radio puissant sur la même fréquence que celle utilisée par le VANET (ex : la bande DSRC 5.9GHz). Ce signal interfère et empêche toute communication légitime dans la zone de couverture du brouilleur. Perte totale de communication dans une zone géographique spécifique. Les messages d'urgence (accident, conditions routières) ne peuvent plus être envoyés ou reçus, ce qui est extrêmement dangereux.

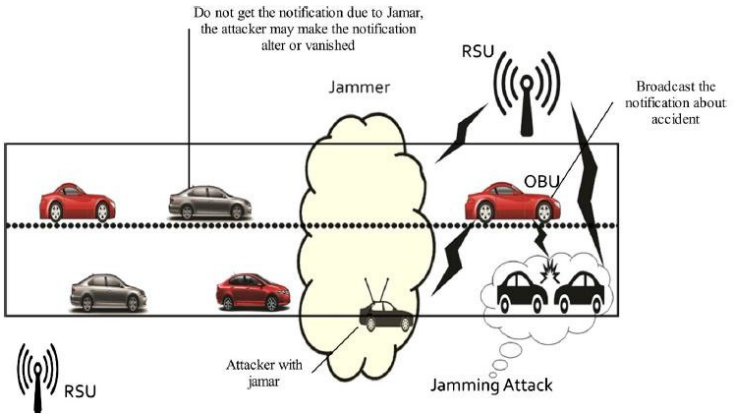


Figure 12 : jamming attaque[21].

Un brouilleur placé au bord d'une route rend le canal radio inutilisable. Les véhicules à proximité ne peuvent plus échanger d'informations, augmentant drastiquement le risque d'accident.[figure 8].

d. Usurpation GPS (GPS Spoofing) / Attaque par tunnel :

L'attaquant utilise un simulateur GPS pour générer des signaux plus puissants que les vrais signaux satellites. Il trompe ainsi le récepteur GPS d'un véhicule en lui fournissant de fausses informations de localisation. Le véhicule victime croit être à un endroit où il n'est pas. Cela peut fausser les applications de navigation, les alertes géolocalisées et les protocoles de routage basés sur la position, conduisant potentiellement le véhicule dans une situation dangereuse.[21]

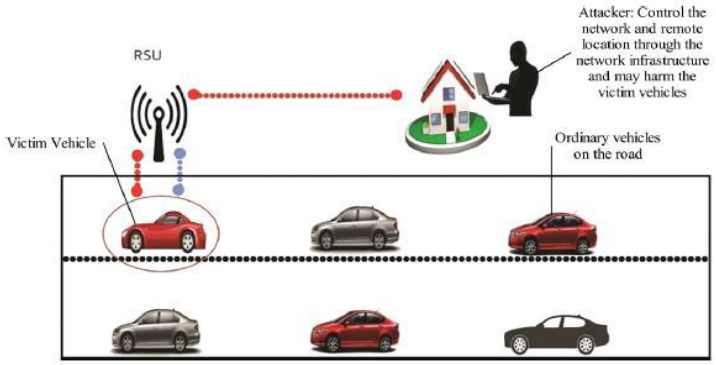


Figure 13 : attacker in home and worklocation attack [21].

e. Attaque de l'Homme du Milieu (Man-in-the-Middle – MiM) :

L'attaquant s'interpose clandestinement entre deux parties qui communiquent (ex : entre deux véhicules ou entre un véhicule et un RSU). Il peut alors écouter, intercepter, modifier ou injecter des messages dans la conversation sans que les victimes ne s'en rendent compte. Cela entraîne une violation de la confidentialité et de l'intégrité des données. L'attaquant peut voler des informations sensibles ou diffuser de fausses informations aux deux parties. [21]

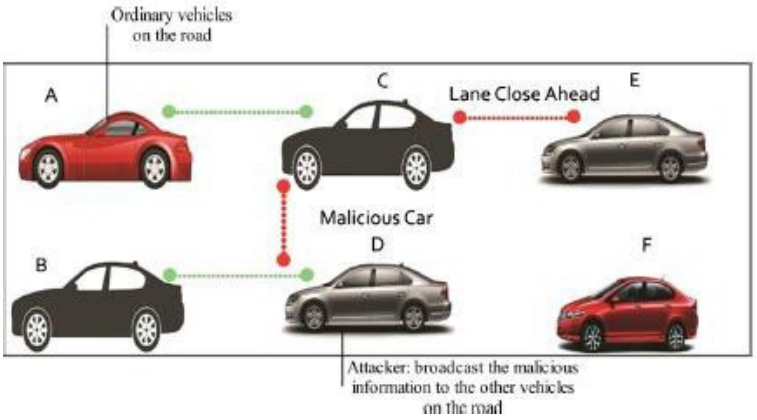


Figure 14 :Man-in-the-Middle attack in VANETs[21]

f. Écoute passive (Passive Eavesdropping) :

Contrairement aux attaques actives, ici l'attaquant se contente de surveiller passivement le canal sans fil pour collecter des informations. Comme les communications sont souvent non chiffrées par défaut (pour des raisons de faible latence), il peut facilement intercepter les messages. Cela constitue une atteinte majeure à la vie privée, l'attaquant pouvant tracer les déplacements d'un véhicule, connaître ses habitudes (domicile, travail), et voler des informations personnelles ou sur l'état du véhicule. Cette attaque est souvent la première étape pour préparer une attaque plus complexe. [21]

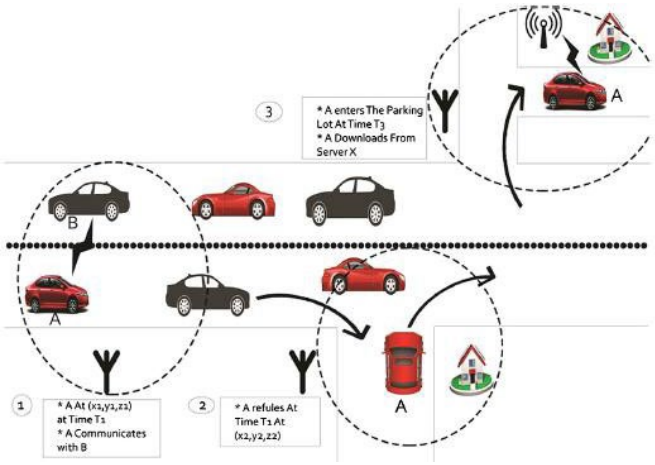


Figure 15 : Passive eavesdropping attack in VANETs.[21]

Le tableau suivant explique ces attaques comme relevant de la couche “interface sans fil“ et du modèle de communication “V2V“ :

Attaque	Méthode	Impact Principal	Modèle de Communication concerné
DoS / DDoS	Saturation du canal ou brouillage radio	Indisponibilité du réseau, blocage des messages de sécurité	V2V, V2I
Sybil	Création de multiples identités fictives	Fausse perception du trafic, perturbation des mécanismes collaboratifs	V2V
Jamming	Brouillage physique du signal radio	Interruption complète des communications dans une zone	V2V, V2I
GPS Spoofing	Usurpation des signaux satellites	Fourniture de fausses positions, navigation erronée	V2V, V2I
Man-in-the-Middle	Interception et altération des messages	Violation de la confidentialité et de l'intégrité des données	V2V, V2I
Eavesdropping	Écoute passive du trafic	Atteinte à la vie privée, collecte d'informations sensibles	V2V, V2I

Tableau 2

1.3. Matériel et logiciel :

Le véhicule moderne est un système complexe sur roues, intégrant une multitude de composants matériels et des millions de lignes de code logiciel. Cette convergence crée une surface d'attaque vaste et en évolution constante. Les vulnérabilités peuvent être classées en deux catégories principales : les menaces matérielles et les menaces logicielles, bien qu'elles soient souvent exploitées de concert pour atteindre un objectif malveillant.

A. Attaques et Vulnérabilités matérielles (hardware) :

Les attaques matérielles ciblent les composants électroniques physiques du véhicule et leurs interfaces directes.

a. Exploitation des Calculateurs (ECU - Electronic Control Units) :

Les ECU sont le cœur fonctionnel du véhicule, contrôlant tout, du moteur et des freins au système d'infodivertissement. Leur nombre (70 à 100 par véhicule) et leur interconnexion via les réseaux internes (comme le bus CAN) en font des cibles de choix. Il y a absence d'authentification et de chiffrement sur le bus CAN (Controller Area Network). Tout message diffusé sur le bus est accepté par tous les ECU sans vérification de l'identité de l'expéditeur ou de l'intégrité du message.[22]

Exemples d'attaque :

- **Manipulation directe d'un ECU** : Les chercheurs Charlie Miller et Chris Valasek ont piraté une Jeep Cherokee en connectant physiquement un ordinateur portable au port OBD-II, obtenant ainsi un accès direct au bus CAN. Ils ont ensuite envoyé des messages malveillants à l'ECU contrôlant la transmission et les freins, permettant de les désactiver à distance sur l'autoroute. Cette attaque a conduit au rappel de 1,4 million de véhicules.[23]
- **Compromission sans fil d'un ECU** : Cai et al. ont démontré de multiples vulnérabilités dans les modèles BMW, montrant que les ECU connectés via le bus CAN pouvaient être compromis via une connexion sans fil, contournant le besoin d'un accès physique.[24]

b. Leurrage (Spoofing) et Brouillage (Jamming) des Capteurs :

Les véhicules autonomes et intelligents dépendent d'un ensemble de capteurs (LiDAR, RADAR, caméras, ultrasons) pour percevoir leur environnement. Attaquer ces capteurs peut "aveugler" le véhicule ou lui faire percevoir une fausse réalité. La plupart des capteurs physiques n'ont pas de mécanismes pour authentifier les signaux qu'ils reçoivent, les rendant sensibles au leurrage (injection de faux signaux) et au brouillage (saturation du capteur par du bruit).[22]

Exemples d'attaque :

- **Leurrage LiDAR** : Petit et al. ont démontré l'efficacité des attaques par relais et leurrage contre les systèmes LiDAR, pouvant créer des obstacles "fantômes" ou masquer de vrais obstacles.[25]
- **Brouillage de Capteurs à Ultrasons** : Liu et al. ont testé des attaques sur les capteurs à ultrasons (brouillage et leurrage) sur des véhicules Tesla, Audi, Volkswagen et Ford. Ils ont démontré que tous les véhicules testés pouvaient être brouillés et leurrés, ce qui pourrait perturber l'aide au stationnement et les fonctions de stationnement autonome.[26]

c. Exploitation des Ports et Interfaces Physiques :

Ce sont des points d'entrée qui nécessitent un accès physique direct ou indirect au véhicule.

- **Port OBD-II** : Conçu pour le diagnostic et la maintenance, ce port offre un accès direct et bas niveau au bus CAN. Il manque souvent de contrôle d'accès robuste. Exemple : Un attaquant peut brancher un dispositif malveillant (ex. : une "clé dongle pirate") dans le port OBD-II pour interroger, modifier ou injecter du code dans les ECU.[27,28]
- **Interfaces du Système de Divertissement (USB, Lecteur CD)** : Ce sont des points d'accès physique indirect. Une clé USB ou un CD spécialement conçu peut exploiter des vulnérabilités dans le logiciel de lecture de médias pour obtenir un point d'entrée dans le système d'infodivertissement, souvent connecté au bus CAN.

Exemple : Des chercheurs ont démontré une attaque en modifiant un fichier audio sur un CD pour qu'il diffuse des messages CAN malveillants lors de sa lecture sur l'autoradio, compromettant ainsi divers systèmes du véhicule.[28]

B. Attaques et Vulnérabilités Logicielles (Software) :

Les attaques logicielles ciblent le code exécuté sur les ECU, les unités d'infodivertissement et les systèmes de télématique du véhicule.

a. Injection et Propagation de Logiciels Malveillants (Malware) :

Un logiciel malveillant peut être introduit dans l'écosystème du véhicule par divers vecteurs et peut provoquer un large éventail de perturbations.[22]

- **Vecteurs** :
  - Média Amovible Infecté : Une clé USB contenant un malware.
  - Appareil Mobile Compromis : Un malware sur un smartphone connecté via Bluetooth ou USB.

- Mises à Jour Compromises : Des mises à jour de firmware OTA (Over-The-Air) corrompues.[22]
- Propagation par le Réseau : Via les communications V2V (Véhicule-to-Véhicule) ou V2I (Véhicule-to-Infrastructure).[22]

- **Types et Exemples** :

  - **Rançongiciel (Ransomware - Motivation Financière M1)** : Un logiciel malveillant qui bloque des fonctions critiques du véhicule (ex. : immobilise le moteur, verrouille les portes) et exige une rançon pour les restaurer. Des chercheurs de McAfee ont démontré un rançongiciel capable de bloquer l'utilisation d'un véhicule jusqu'à paiement.[29]
  - **Logiciel Espion (Spyware - Motivation Atteinte à la Vie Privée M2)** : Un logiciel conçu pour voler des données sensibles du conducteur (localisation, habitudes de conduite, historique des appels, identifiants). Un tiers a obtenu l'accès aux informations personnelles de 27,7 millions de conducteurs du Texas via un système vulnérable.[30]
  - **Vandalisme (Motivation M3)** : Un logiciel qui provoque des comportements disruptifs et dangereux, comme désactiver les freins, jouer avec le système d'infodivertissement ou afficher de faux avertissements pour distraire le conducteur. [31]

b. Vulnérabilités dans les Logiciels et Systèmes d'Exploitation du Véhicule :

La pile logicielle des véhicules modernes est vaste et complexe, contenant inévitablement des bogues et des vulnérabilités. L'utilisation de systèmes d'exploitation open source (ex. : Linux, Android) sans durcissement suffisant ou sans correctifs de sécurité appliqués en temps voulu. La complexité de la base de code (des millions de lignes) augmente la probabilité de bogues.[32,33]

- **Piratage du Système d'Infodivertissement** : Des chercheurs ont pu obtenir une connexion permanente sur le système d'infodivertissement d'une Mazda en exécutant un script bash sur le système d'exploitation Linux du véhicule[34]. Un autre groupe a accédé à des données personnelles (carnet d'adresses, historique des conversations, localisation) à distance en se connectant au compte root du système d'infodivertissement.[35]

c. Exploitation des Piles de Communication Sans Fil :

Les piles logicielles gérant les interfaces sans fil sont complexes et peuvent contenir des vulnérabilités.

- **Bluetooth** : Des vulnérabilités dans le protocole d'appariement ou son implémentation peuvent permettre à un attaquant de se connecter au véhicule à l'insu du conducteur et de télécharger du code malveillant.[28,36]
- **Réseau Cellulaire (3G/4G/5G)** : L'unité de télématique, qui fournit la connectivité, peut être piratée à distance. Miller et Valasek ont exploité l'unité de télématique d'une Jeep via sa connexion cellulaire pour lancer leur attaque.37

- **Wi-Fi** : Un véhicule configuré pour se connecter automatiquement à des points d'accès Wi-Fi "de confiance" peut être trompé et connecté à un point d'accès pirate malveillant, permettant à l'attaquant d'intercepter des données ou de pousser un malware.[38,39]

d. Faiblesses des Logiciels Tiers et Aftermarket :

L'écosystème s'étend au-delà du constructeur pour inclure des applications tierces et des dispositifs aftermarket. Les systèmes d'infodivertissement ou les dongles aftermarket peuvent avoir des standards de sécurité plus faibles. Les applications mobiles tierces qui interfacent avec le véhicule (ex. : pour déverrouiller les portes) stockent souvent les identifiants de manière non sécurisée et peuvent être rétro-ingénierées[38]. Des chercheurs ont découvert plusieurs vulnérabilités dans sept applications véhiculaires populaires qui permettaient aux attaquants d'accéder aux véhicules[40]. Des chercheurs de Symantec ont trouvé de fausses applications malveillantes conçues pour ressembler à des applications légitimes (ex. : Uber) qui pourraient compromettre l'appareil d'un utilisateur et, par extension, son véhicule[41].

Ce tableau présente des vecteurs d'attaque matériels et logiciels :

Cible	Vecteur d'Attaque	Vulnérabilité Exploitée	Impact
ECU / Bus CAN	Port OBD-II	Absence d'authentification sur le bus CAN	Contrôle total des fonctions critiques (direction, freins)
Capteurs	Leurrage/Brouillage (RF)	Les capteurs acceptent des signaux non authentifiés	Accidents, comportement erratique, défaillance de l'ADAS
Infodivertissement	USB/CD Malveillant	Vulnérabilités dans les analyseurs de fichiers multimédias	Point d'entrée dans le système, propagation vers d'autres ECU
Télématique	Réseau Cellulaire (4G)	Vulnérabilités dans la pile logicielle de télématique	Contrôle à distance depuis n'importe où dans le monde
Mise à Jour Logiciel	Mise à jour OTA compromise	Absence de signature de code/vérification du processus	Porte dérobée permanente, vol de véhicule
Application Mobile	Store d'Apps Tiers	Stockage non sécurisé des identifiants dans les apps mobiles	Accès non autorisé aux fonctions du véhicule (verrouillage, démarrage)

Tableau 3

1.4.Les capteurs d'entrées :

Ce type d'attaque est basé sur l'exploitation des capteurs présents dans les appareils IoT. Les capteurs (accéléromètre, gyroscope, microphone, capteur de lumière, etc.) peuvent être détournés par des attaquants pour :

a. Fuites d'informations (Information Leakage)[42] :

- **Inférence de frappe (Keystroke Inference)** :
  - Via le capteur de lumière : variations lumineuses lors de la frappe.
  - Via les capteurs de mouvement (accéléromètre, gyroscope) : vibrations et orientations.
  - Via les capteurs audio : enregistrement des sons de frappe.
  - Via la caméra : analyse des reflets ou des mouvements des mains.
  - Via les capteurs magnétiques : émissions électromagnétiques du clavier.
- **Inférence de tâches (Task Inference)** :
  - Analyse des émissions électromagnétiques ou de la consommation énergétique pour déduire les processus en cours.
- **Inférence de localisation (Location Inference)** :
  - Utilisation de canaux acoustiques pour identifier un lieu via les réflexions sonores.
- **Écoute clandestine (Eavesdropping)** :
  - Enregistrement audio via le microphone à l'insu de l'utilisateur.

b. Transmission de commandes malveillantes :

Les capteurs peuvent servir de canaux cachés pour activer des malwares[42] :

- Capteur de lumière : modulation de la lumière d'un écran.
- Capteur magnétique : modification du champ magnétique ambiant.
- Capteur audio : transmission ultrasonique.

c. Injection de fausses données :

Altération des données capteurs pour :

- Fausser la localisation GPS.
- Corrompre des données chiffrées via l'analyse de puissance.
- Manipuler le comportement des applications.

d. Déni de service (DoS) :

Exploitation des fréquences de résonance des capteurs :

- Accéléromètre : vibrations forcées pour désactiver l'appareil.
- Gyroscope : interférence par signal sonore pour perturber les drones.

Les capteurs, souvent dépourvus de mécanismes de permission explicites, représentent un vecteur d'attaque à la fois discret et privilégié. Les contre-mesures existantes (par exemple : 6thSense, AWare) restent limitées dans leur portée et sont peu déployées à grande échelle. Pour sécuriser efficacement les écosystèmes IoT face à ces menaces, une approche holistique ainsi qu'une sensibilisation renforcée s'avèrent indispensables.

2. Les défis de sécurité :

2.1. La distribution de clés :

La distribution sécurisée des clés cryptographiques est le fondement de presque tous les autres mécanismes de sécurité (authentification, confidentialité, intégrité). Dans les VANETs, cette tâche est exceptionnellement difficile à cause des caractéristiques uniques de ces réseaux :

- **Haute Mobilité et Topologie Dynamique** :

Les véhicules entrent et quittent le réseau de manière très fréquente et imprévisible. Un système de distribution de clés doit être capable de fournir et de révoquer des clés à la volée, sans interrompre les communications de sécurité critiques.[43]

- **Échelle et Latence** :

Un réseau VANET peut comporter des millions de véhicules. Un système centralisé où chaque véhicule devrait contacter un serveur central pour obtenir une clé créerait un goulot d'étranglement et des délais inacceptables pour des messages de sécurité qui doivent être diffusés en quelques millisecondes.[43]

- **Confidentialité et Vie Privée** :

Bien que les véhicules doivent s'authentifier pour envoyer des messages valides, ils ne doivent pas être traçables sur de longues périodes pour protéger la vie privée des conducteurs. Un système de clés statiques et uniques permettrait de tracer tous les déplacements d'un véhicule. Il faut donc un système qui permette l'authentification sans traçabilité permanente.[43]

- **Réactivité face aux Compromissions** :

Si la clé privée d'un véhicule est volée ou si un véhicule est malveillant, il faut pouvoir révoquer ses accès très rapidement pour qu'il ne puisse plus injecter de fausses informations dans le réseau. Diffuser une liste de révocation à des millions de véhicules de manière efficace est un immense défi. [43]

Des exemples de problèmes concrets :

- **Usurpation d'Identité (Impersonation Attack)** :

Un attaquant parvient à obtenir une clé/certificat valide. Il peut alors se faire passer pour une ambulance ou un véhicule d'urgence et diffuser de fausses alertes (ex : "Accident devant, freinez brusquement !"), provoquant potentiellement un accident[43].

- **Attaque Sybil** :

Un attaquant génère un grand nombre de fausses identités (clés) pour simuler un embouteillage, une route fermée, ou pour biaiser un système de vote collaboratif. Le système de distribution des clés n'a pas de mécanisme robuste pour lier une clé à une entité physique unique et vérifiable (un véhicule), permettant la création de multiples identités[43].

- **Perte de Vie Privée (Tracking)** :

Un adversaire écoute les messages signés avec la même clé. En suivant la signature unique du véhicule, il peut tracer tous ses déplacements sur plusieurs jours, violant la vie privée du conducteur. Le système distribue des clés de signature de longue durée (ou permanentes) au lieu de clés temporaires et fréquemment changées[43].

Solutions Cryptographiques Proposées :

Après avoir passé en revue plusieurs approches pour résoudre ces défis, la principale étant l'utilisation d'une Infrastructure à Clé Publique (PKI) adaptée, souvent appelée VPKI (Vehicular PKI).

a. VPKI (Vehicular Public Key Infrastructure) :

C'est la solution centrale présentée. Son principe est le suivant :

- **Autorité Certificatrice (CA) Racine** :

Une autorité de confiance (gouvernementale, consortium de constructeurs) gère la PKI[43].

- **Inscription** :

À la fabrication ou lors d'un contrôle technique, le véhicule se voit attribuer un lot de certificats numériques anonymes (un certificat contient une clé publique et une signature de la CA) [43].

- **Utilisation** :

Le véhicule utilise ces certificats pour signer ses messages (ex : "Je freine", "Attention verglas à ma position"). Les autres véhicules peuvent vérifier la signature avec la clé publique de la CA, assurant l'authenticité et l'intégrité du message, sans savoir quel véhicule exact l'a envoyé[43].

- **Changement Fréquent** :

Le véhicule change régulièrement de certificat (toutes les quelques minutes). Cela empêche le traçage à long terme, car l'identifiant (le certificat) change constamment. C'est le concept de "Pseudonymat"[43].

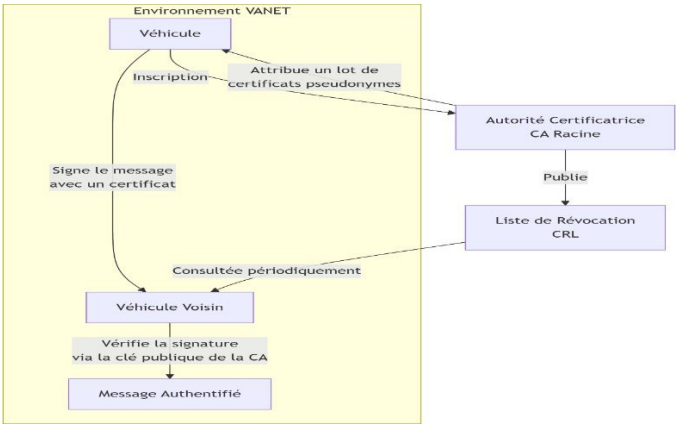


Figure 16 : véhicule qui s'enregistre auprès de l'autorité (CA), à l'émission des certificats pseudonymes [47]

b. Gestion de la Révocation - les listes de Révocation de Certificats (CRL) :

La CA publie une Liste de Révocation de Certificats (CRL) contenant les identifiants de tous les certificats révoqués. Diffuser cette liste à tous les véhicules du réseau de manière rapide et efficace, sans saturer le canal de communication. Les solutions impliquent souvent une diffusion via les RSU (Road Side Units) ou un mécanisme de rafraîchissement des certificats où les certificats révoqués ne sont simplement pas renouvelés.

c. Autres Approches :

- **Protocoles de Délimitation de Distance (Distance Bounding)** :

Utilisés pour combattre les attaques de type "wormhole" ou de fausse localisation. Ils permettent de vérifier qu'un véhicule est bien à une certaine distance maximale, en mesurant le temps de propagation d'un signal. Cela peut être couplé à un échange de clés[43].

- **Cryptographie Basée sur l'Identité (Identity-Based Cryptography - IBC)** :

Une alternative où l'adresse (un email, un VIN - Vehicle Identification Number) peut servir de clé publique, simplifiant ainsi la gestion des certificats. Cependant, elle introduit un "Key Generator" central qui doit être absolument fiable.[43]

La VPKI avec certificats pseudonymes est la solution la plus aboutie et étudiée pour adresser le défi de la distribution des clés, elle n'est pas parfaite. Des problèmes subsistent, notamment
:

- La mise à l'échelle efficace de la CA pour gérer des millions de véhicules.

- La diffusion rapide et efficiente des listes de révocation (CRL).
- La complexité et le coût de déploiement d'une telle infrastructure à l'échelle mondiale.
- L'équilibre délicat entre anonymat (pour la vie privée) et responsabilisation (pour traquer et révoquer les malfaiteurs).

2.2. Des contraintes temps Réel :

La détection en temps réel des nœuds malveillants (notamment les attaques DDoS) dans les VANETs est un défi critique en raison de la dynamique du réseau, de la criticité des applications de sécurité, et de la nature évasive des attaques.

a. Introduction du défi Temps Réel :

Les VANETs exigent des mécanismes de sécurité à faible latence. Une attaque DDoS peut saturer le réseau en quelques secondes, empêchant la transmission de messages de sécurité (ex

: freinage d'urgence). Les solutions traditionnelles, souvent conçues pour des environnements statiques, ne sont pas adaptées. Les contraintes temps réel se manifestent par :

- La nécessité d'une détection ultra-rapide : Le système doit analyser le trafic et prendre une décision en un temps très court pour isoler le nœud malveillant avant qu'il ne cause des dommages.[44]
- La charge computationnelle : L'analyse du trafic réseau avec du Machine Learning (ML) est gourmande en ressources. Effectuer cette analyse sur un seul nœud (comme un RSU) pourrait introduire un goulot d'étranglement et une latence inacceptable[44].
- L'évolutivité (Scalability) : Le système doit fonctionner efficacement que le réseau compte 20 ou 200 véhicules, sans que le temps de traitement n'explose[44].

b. Solution proposée pour répondre au défi :

- **Architecture Distribuée et Clusterisée** :
  - **Répartition de la charge** :

Utilisation d'Apache Spark pour créer un système de calcul distribué où la charge de traitement est répartie entre les véhicules ("worker nodes") et gérée par un véhicule moniteur ("monitor car"). Cela évite le goulot d'étranglement d'un serveur central[44].

  - **Traitement parallèle** :

Spark permet des opérations parallèles sur les données (Resilient Distributed Datasets - RDD), accélérant considérablement le temps d'analyse et de détection[44].

- **Modèles de Machine Learning Optimisés** :
  - **Comparaison de modèles :**

Les auteurs testent et comparent plusieurs algorithmes de ML (GBT, LR, MLPC, RF, SVM) pour identifier ceux offrant le meilleur compromis précision/vitesse.

- **Modèle retenu :**

Le Random Forest (RF) et le Gradient Boosted Tree (GBT) se sont montrés les plus performants, avec une précision allant jusqu'à 99% tout en maintenant un temps d'inférence court, ce qui est crucial pour le temps réel[44].

- **Optimisation Avancée (L-BFGS)** :

Pour accélérer l'entraînement du modèle, ils utilisent l'algorithme L-BFGS (Limited-memory Broyden–Fletcher–Goldfarb–Shanno), une méthode d'optimisation de second ordre très efficace en termes de vitesse de convergence et de consommation mémoire. Ce choix est stratégique pour un environnement contraint[44].

c. Méthodologie d'Évaluation de la Performance Temps Réel :

Les auteurs ne se contentent pas de mesurer la précision ; ils évaluent rigoureusement la performance du système sous l'angle des contraintes temps réel :

- **Environnement de test réaliste** :

Utilisation de OMNET++ (réseau), SUMO (mobilité) et Veins (couplage). Cela permet de générer des scénarios de trafic et d'attaque dynamiques et crédibles[44].

- **Scénarios d'attaque gradués** :

La densité d'attaque (le pourcentage de temps de simulation où une attaque DDoS est active) est augmentée par paliers de 10% à 70%. Cela teste la robustesse et la stabilité du système sous charge[44].

- **Mesure de la scalabilité** :

Le temps de calcul (entraînement et prédiction) est mesuré en faisant varier le nombre de nœuds de calcul dans le cluster AWS (de 1 à 6 nœuds). Résultat clé : le temps de traitement n'augmente pas de façon linéaire avec l'ajout de véhicules/nœuds ; il est même optimisé grâce à l'architecture distribuée[44].

- **Déploiement sur Cloud (AWS)** :

L'implémentation avec PySpark sur Amazon EMR démontre la faisabilité pratique de la solution dans une infrastructure cloud, capable de gérer de grandes quantités de données en temps réel[44].

d. Résultats Clés (Focus Temps Réel) :

- **Haute Précision Maintenue** :

Le modèle reste extrêmement précis (~98-99% pour RF et GBT) même sous des densités d'attaque élevées (70%), prouvant qu'il ne sacrifie pas la qualité pour la vitesse[44].

- **Preuve de Scalabilité** :

La courbe montre que le temps médian de traitement diminue lorsque le nombre de nœuds de calcul dans le cluster AWS augmente. C'est la preuve que l'architecture distribuée est efficace pour gérer l'augmentation de la charge de données[44].

Un exemple concret et récent de la manière de traiter le défi des contraintes temps réel dans les VANETs. Il montre qu'une approche basée sur :

1. Une architecture distribuée (type Spark) pour paralléliser les calculs,
2. Le choix judicieux de modèles de ML équilibrés (Random Forest),
3. L'optimisation des algorithmes d'apprentissage (L-BFGS),
4. Une évaluation rigoureuse incluant la scalabilité et des scénarios dynamiques,
   permet de développer un système de détection à la fois précis, rapide et scalable, répondant ainsi aux exigences strictes des environnements VANET en temps réel.

2.3. La Topologie Dynamique :

Le contexte des VANETs comme une instance à grande échelle de réseaux ad hoc mobiles. Le défi central identifié est la haute dynamique de la topologie sous-jacente et la connectivité intermittente qui en résulte dans la plupart des scénarios.

- **Cause Racine** :

La mobilité des véhicules est contrainte par la structure routière, les feux de signalisation, le comportement des autres véhicules et les décisions des conducteurs. Contrairement aux MANETs génériques où la mobilité peut être aléatoire, la mobilité dans les VANETs est structurée mais extrêmement variable[45].

- **Conséquence Directe** :

Cette dynamique entraîne des changements constants et rapides dans la connectivité du réseau. Les liens sans fil entre les véhicules se forment et se brisent à un rythme élevé, conduisant à des fragmentations et fusions fréquentes du réseau (partitions et jonctions). Cela rend la conception de protocoles de routage et de communication fiables très difficile[45].

a. Modélisation de la mobilité (comprendre la source de la dynamique) :

Les modèles qui génèrent cette topologie dynamique :

- **Modèles Microscopiques** : Ils sont essentiels car ils modélisent le comportement individuel de chaque véhicule, qui est la source de la dynamique globale[45].
- **Car-Following (Suivi de Véhicule)** : Décrit comment un véhicule ajuste sa vitesse et sa position en réaction au véhicule qui le précède (e.g., modèles Stimulus-Réponse,

Safe Distance). C'est la base des embouteillages et de la formation de pelotons (platoons).

- **Multi-Lane Traffic (Trafic Multi-voies)** : Le modèle MOBIL est présenté comme un cadre pour modéliser les changements de voie. Il prend la décision en fonction de deux critères :
  - **Sécurité** : Le changement de voie ne doit pas forcer le véhicule suiveur sur la nouvelle voie à freiner brusquement.
  - **Incitant** : Le changement doit améliorer les conditions de conduite du véhicule qui change de voie et, éventuellement, de ses voisins (via un "facteur de politesse")[45].
- **Impact sur la Topologie** : Ces manœuvres (changements de voie, dépassements) sont une cause majeure de reconfiguration rapide de la topologie du réseau. Un dépassement peut créer ou rompre un lien de communication entre plusieurs véhicules[45].

b. Reproduire la dynamique pour ma recherche :

Pour étudier les protocoles VANET, il est crucial de simuler cette topologie dynamique de manière réaliste.

- **Simulateurs de Mobilité** : Des outils comme SUMO, VanetMobiSim et VISSIM sont capables de générer des traces de mobilité réalistes en utilisant les modèles précités (Krauss, IDM, MOBIL). Ils simulent les contraintes routières, la signalisation et les interactions entre véhicules[45].
- **Le Défi de l'Interaction Bidirectionnelle** : Une limitation des simulateurs réseau traditionnels (e.g., NS-2, OMNeT++) est qu'ils se contentent de lire un fichier de mobilité pré-généré (open-loop). Or, dans les VANETs, les communications influencent la mobilité (e.g., un message d'accident force les véhicules à ralentir). Cette rétroaction (feedback) est vitale pour les applications de sécurité[45].
- **Solution : Simulateurs Intégrés** : Pour relever ce défi, des simulateurs couplés comme Veins (OMNeT++ + SUMO) et TraNS (NS-2 + SUMO) ont été développés. Ils utilisent une interface (e.g., TraCI) pour permettre une interaction en temps réel entre le simulateur réseau et le simulateur de mobilité. Ainsi, la topologie évolue dynamiquement en fonction des messages reçus, et vice-versa, reproduisant fidèlement la nature interdépendante des VANETs[45].

c. Modélisation des communications (l'impact sur la perception de la topologie) :

La perception de la "topologie" (qui est connecté à qui) dépend directement de la modélisation de la couche physique.

- **Modèles Simplistes vs. Réalistes** :
  - **UDG (Uniform Disk Graph)** : Modèle idéal où la connexion est parfaite dans un rayon r et nulle au-delà. Il est irréaliste car il ignore les effets de propagation radio complexes[45].
  - **Modèles Réalistes** : Les modèles comme Two-Ray Ground, Log-Normal Shadowing et Nakagami fading introduisent de l'aléatoire dans la réception des messages. La connexion devient une probabilité qui dépend de la distance, des obstacles et des interférences[45].

- **Impact sur la Dynamique** : Ces modèles réalistes ajoutent une couche supplémentaire de dynamique à la topologie. Même si la position relative de deux véhicules est stable, un lien peut apparaître ou disparaître en raison de phénomènes radio (évanouissement, ombrage). La topologie perçue par la couche réseau est donc encore plus instable et imprévisible que ne le suggèrent les seuls mouvements des véhicules[45].

d. Analyse de la connectivité : quantifier la dynamique sur autoroute :

Une étude de cas pour mesurer l'impact de cette topologie dynamique sur la connectivité dans un scénario autoroutier.

- **Paramètre Clé** : La portée radio effective (r), qui varie en fonction du débit de transmission (3 à 27 Mbps). Plus le débit est bas, plus la portée est longue.
- **Résultats Clés** :

  - **Absence de Connectivité Permanente** : Contrairement aux hypothèses de certains protocoles, il n'existe presque jamais de chemin continu et stable entre une source et une destination éloignées. La connectivité est intermittente[45].
  - **Influence de la Densité de Trafic** : Dans des conditions de trafic dense (Niveau de Service F, D), la probabilité de trouver un chemin connecté est plus élevée, surtout à bas débit (longue portée). Dans des conditions de trafic fluide (LOS A, B), le réseau est fortement partitionné[45].
  - **Formation de Pelotons** : La topologie n'est pas homogène. Les véhicules tendent à former des pelotons (clusters) bien connectés à l'intérieur, mais isolés les uns des autres par des gaps de plusieurs mètres. La distance entre ces pelotons est souvent supérieure à la portée radio, rompant la connectivité de bout en bout[45].
  - **Impact du Nombre de Voies** : Une autoroute à deux voies améliore la connectivité car elle permet aux véhicules de se dépasser, réduisant la formation de longs pelotons serrés et permettant de "combler" certains gaps.
  - **Paradigme Store-Carry-Forward** : Face à cette dynamique et cette connectivité intermittente, le paradigme stocker-transporter-forwarder est nécessaire. Un véhicule peut stocker un message en attendant qu'un lien vers la destination ou vers le prochain saut se présente. Cette approche permet de maintenir la connectivité logique malgré les déconnexions physiques fréquentes, au prix d'une augmentation de la latence[45].

La topologie dynamique n'est pas un simple attribut des VANETs, mais LE défi fondamental qui impacte tous les aspects de la conception protocolaire.

- **Origines** : Elle est causée par la mobilité contrainte des véhicules (modèles de suivi et de changement de voie) et amplifiée par la nature imprévisible des canaux sans fil[45].
- **Conséquences** :

  - Connectivité intermittente et absence de chemin end-to-end permanent.
  - Nécessité de protocoles de routage et d'acheminement tolérants aux délais et aux déconnexions (DTN).

- Obligation d'utiliser des outils de simulation couplés et réalistes pour évaluer les performances des protocoles dans des conditions fidèles à la réalité[45].

Concevoir pour les VANETs, c'est accepter l'instabilité et concevoir des systèmes capables de fonctionner malgré une topologie en perpétuel changement. Le paradigme de communication doit évoluer d'une recherche de chemin stable vers une gestion intelligente de la mobilité et du stockage pour assurer la livraison des données[45].

2.4. Challenges de vérification et de cohérence :

Les VANETs (Vehicular Ad Hoc Networks) sont des réseaux éphémères où les véhicules communiquent entre eux (V2V) ou avec des infrastructures (V2I) pour améliorer la sécurité routière et éviter les congestions. Un défi majeur est de détecter les informations erronées (ex : fausses alertes, positions falsifiées) sans compromettre la vie privée des utilisateurs.

a. .Problème de Vérifications :

- **Authenticité des messages** :

  - Chaque message (alerte ou balise) doit être authentifié pour éviter les falsifications[46].
  - Les schémas classiques utilisent des signatures numériques (ex : ECMV, PASS) ou des pseudonymes avec paires de clés publiques/privées[46].
  - Limitation : Un nœud malveillant peut utiliser de faux pseudonymes (attaque Sybil) pour envoyer de multiples messages frauduleux[46].

- **Vérification en temps réel** :

  - La vérification doit être rapide (délais de l'ordre de la milliseconde) pour éviter des accidents[46].
  - Les solutions existantes reposent souvent sur des bases de données globales ou des votes majoritaires, ce qui est peu réaliste dans un réseau aussi dynamique[46].

- **Absence d'autorité centrale permanente** :

  - Les VANETs sont décentralisés et éphémères → pas de base de données centralisée fiable[46].
  - Les RSU (Road Side Units) peuvent être compromis ou hors de portée.

b. Problème de cohérence :

- **Incohérence entre alertes et comportements** :

  - Un nœud malveillant peut envoyer une fausse alerte (ex : « accident à l'avant ») puis continuer sa route normalement[46].
  - Exemple : Si un véhicule signale un blocage à la position X mais traverse X peu après, l'alerte est incohérente.

- **Incohérence des informations de localisation** :

- Un nœud peut mentir sur sa position pour rendre une fausse alerte crédible.
- La détection repose sur :
  - La distance Euclidienne entre les positions déclarées et estimées.
  - Le temps de propagation du signal (via la vitesse de la lumière) [46].
  - L'ordre des véhicules par rapport à l'événement signalé[46].

➢ **Exceptions difficiles à détecter** :

- Si un nœud malveillant se trouve sur l'axe médiateur entre sa vraie position et sa fausse position, les autres nœuds ne pourront pas détecter le mensonge[46].

c. Solution proposée :

➢ **Approche centrée sur les données (Data-centric MDS)** :

- On ne cherche pas à classer les nœuds comme « bons » ou « mauvais », mais à évaluer la véracité des messages[46].
- Chaque nœud vérifie localement la cohérence des messages reçus avec les comportements observés[46].

➢ **Algorithme de détection basé sur la localisation** :

- Après réception d'une alerte, un nœud attend les balises de position de l'émetteur pendant un intervalle t[46].
- Il vérifie si le comportement subséquent est cohérent avec l'alerte (ex : le véhicule évite-t-il la zone ?) [46].
- Si incohérence → le nœud émet une négation de l'alerte et signale le comportement au RSU le plus proche[46].

➢ **Utilisation de pseudonymes avec contraintes temporelles** :

- Un nœud ne peut pas changer de pseudonyme immédiatement après une alerte → permet de lier l'alerte à son auteur[46].
- Le CA (Certification Authority) peut identifier le véhicule via le pseudonyme et lui infliger une amende (plutôt que de révoquer ses certificats) [46].

➢ **Immunité contre les attaques Sybil** :

- Aucun vote ou décision majoritaire n'est nécessaire → les fausses identités n'influencent pas la décision[46].

d. Limitations et Améliorations futures :

➢ **Situations non couvertes** :

- Demi-tours, échangeurs complexes → calcul de distance Euclidienne inefficace[46].
- Collusion entre nœuds : deux véhicules peuvent se coordonner pour mentir (ex : l'un envoie une fausse alerte, l'autre la confirme) [46].

- **Surcharge réseau** :

  - La retransmission systématique des alertes peut surcharger le réseau.

- **Incitations à la coopération** :

  - Les nœuds peuvent être réticents à transmettre des alertes (consommation d'énergie) [46].
  - Proposition : système de récompenses/pénalités (points positifs/négatifs) [46].

D'après l'article [46], il s'agit d'une nouvelle approche de détection de comportements malveillants dans les VANETs, centrée sur la vérification de la cohérence des données plutôt que sur l'identification des nœuds. Cette méthode est résistante aux attaques Sybil, préserve la vie privée, et réduit les coûts de communication liés à la révocation de certificats. Cependant, elle reste vulnérable dans certains scénarios complexes (changements de direction, collusions), qui constituent des pistes de recherche futures.

3. Les Exigences :

3.1. Protocoles de contrôle d'Accès :

Les VANETs représentent une pierre angulaire des systèmes de transport intelligents (ITS), permettant des communications de type Véhicule-à-Véhicule (V2V) et Véhicule-à-Infrastructure (V2I). La couche Media Access Control (MAC) est fondamentale car elle gère l'accès partagé au canal radio sans fil, une ressource rare et sujette aux interférences. Dans un environnement aussi dynamique et exigeant que les VANETs (haute mobilité, topologie changeante, besoins QoS hétérogènes), le design du protocole MAC est un défi critique pour garantir la fiabilité, la faible latence et l'équité des communications, surtout pour les applications de sécurité.

a. Défis spécifiques au contrôle d'accès dans les VANETs :

Il y a plusieurs défis majeurs qui impactent directement l'efficacité des mécanismes de contrôle d'accès :

1. **Problème des nœuds cachés (hidden Terminal problem)** :

Dans un environnement V2V pur sans coordination centralisée, deux véhicules hors de portée radio l'un de l'autre peuvent tenter de communiquer simultanément avec un même véhicule récepteur, causant des collisions de messages. Un protocole MAC robuste doit intégrer des mécanismes pour atténuer ce risque (e.g., RTS/CTS dans CSMA/CA).[49]

2. **Mobilité élevée et dynamique du réseau** :

La vitesse relative élevée entre les véhicules (jusqu'à 200 km/h) entraîne une durée de connexion très courte (potentiellement < 30s). Le protocole MAC doit donc permettre une association et une coordination extrêmement rapides, avec un temps de stabilisation du réseau minimal[49].

3. **Besoins QoS disparates** :

Les VANETs doivent supporter deux types de trafic aux exigences opposées :

- **Trafic de sécurité (safety)** : Messages courts, nécessitant une latence très faible et garantie, un haut taux de livraison et une priorité absolue[49].
- **Trafic d'infotainment** : Volume de données élevé, plus tolérant à la latence mais nécessitant un débit important[49].

Un bon protocole MAC doit offrir un contrôle d'accès différencié pour satisfaire ces deux classes de service.

4. **Évolutivité (Scalability)** :

Le protocole doit maintenir des performances acceptables et stables dans des conditions de densité de véhicules très variables, des routes rurales peu fréquentées aux embouteillages denses en centre-ville[49].

5. **Équité (Fairness)** :

La notion d'équité est complexe dans les VANETs. Elle peut signifier un accès égal dans le temps pour tous les nœuds, ou un accès pondéré par la vitesse (un véhicule rapide ayant une fenêtre de communication plus courte avec un RSU devrait avoir plus de chances d'accéder au medium qu'un véhicule lent) [49].

b. Défis ouverts et perspectives de recherche :

Les défis persistants pour le contrôle d'accès dans les VANETs :

1. **Dépendance au GPS** :

De nombreux protocoles performants (STDMA, MCTRP) dépendent du GPS pour la synchronisation. Des solutions de secours ou des mécanismes de synchronisation alternatifs sont nécessaires pour les zones sans couverture (tunnels, canyons urbains) [49].

2. **Utilisation des canaux multiples** :

Le standard WAVE alloue 7 canaux, mais peu de protocoles les exploitent efficacement. Une gestion intelligente et dynamique des canaux est un axe de recherche important[49].

3. **Compromis Radio/Coût** :

Les approches multi-canaux les plus performantes nécessitent souvent deux radios par véhicule, ce qui pose un problème de coût pour une adoption massive par l'industrie automobile[49].

4. **Adaptabilité contextuelle** :

La majorité des protocoles sont optimisés pour les scénarios autoroutiers. Les environnements urbains, avec leurs obstacles, leurs intersections et leurs patterns de mobilité erratiques, exigent des protocoles MAC plus robustes et agiles[49].

5. **Intégration des services** : Les futurs protocoles MAC doivent mieux intégrer le contrôle d'accès pour le trafic de sécurité et le trafic d'infotainment au sein d'une même architecture, en allouant dynamiquement les ressources en fonction de la demande et de la priorité[49].

c. Analyse des Approches MAC et de leurs mécanismes de contrôle d'Accès :

On va comparer plusieurs protocoles MAC proposés, en les catégorisant selon leur méthode d'accès :

Protocole	Mécanisme de Contrôle d'Accès	Avantages	Inconvénients / Limitations
IEEE 802.11p / WAVE	CSMA/CA avec EDCA (contention-based). Priorisation via différentes valeurs de CW et AIFS.	Simple, robuste aux changements de topologie, pas de synchronisation requise.	Aucune garantie de délai (delays non bornés), performances qui se dégradent fortement sous charge élevée à cause des collisions. Faible aptitude pour les messages de sécurité critiques.
STDMA	TDMA auto-organisé et sans conflit. Basé sur le temps GPS. Les nœuds choisissent aléatoirement un slot temporel dans une frame.	Accès garanti et déterministe, faible latence pour les messages courts.	Dépendance totale au GPS. Peu adapté au trafic urbain, ne supporte pas le haut débit (conçu pour des messages de position).
VeSOMAC	TDMA distribué et asynchrone. Les nœuds diffusent un "bitmap" de l'occupation des slots de leurs voisins.	Ne nécessite pas de synchronisation globale ni de leader. Meilleur débit que 802.11p pour le trafic données.	Complexité de la synchronisation distribuée, surcharge importante (bitmap), conçu uniquement pour les autoroutes.
MCTRP	Hybride. TDMA à jeton (sans conflit) à l'intérieur d'un anneau de véhicules. CSMA/CA pour la communication entre anneaux.	Faible latence intra-anneau, utilise plusieurs canaux.	Dépendance critique au nœud leader de l'anneau. Topologie rigide, complexe à maintenir avec une mobilité élevée. Nécessite deux radios.
CBM-MAC	Hybride basé sur clusters. TDMA schedulé (sans conflit) à l'intérieur du cluster (contrôlé par un Cluster Head). CSMA/CA entre clusters.	Garantie de QoS intra-cluster, bon pour les messages de sécurité.	Dépendance forte au Cluster Head. Gestion complexe des clusters en environnement mobile. Nécessite deux radios.
DMMAC	Hybride adaptatif. Combine une période TDMA sans conflit (pour la sécurité) et une période de réservation contention-based (pour les données) au sein de la trame WAVE.	Respecte le standard WAVE, adapte la taille de la période sans conflit en fonction de la demande.	Complexité de la coordination distributive, mécanisme de réservation peu détaillé.

Tableau 4

La couche MAC est un composant essentiel pour réaliser la promesse des VANETs. Si le standard IEEE 802.11p offre une base simple et robuste, il est inadapté pour les applications critiques en raison de sa nature aléatoire. Les protocoles hybrides (combinant TDMA et CSMA) et organisés (clusters, anneaux) offrent de meilleures performances et garanties de QoS mais au prix d'une complexité accrue, d'une dépendance à des nœuds coordinateurs et souvent de besoins matériels supérieurs. La recherche future en contrôle d'accès pour VANETs doit se concentrer sur le développement de protocoles adaptatifs, résilients, économes en ressources et capables de fonctionner efficacement dans tous les scénarios de conduite.

3.2. Disponibilité :

Les Réseaux Ad Hoc Véhiculaires (VANETs) sont cruciaux pour la sécurité routière et l'efficacité du trafic, permettant des communications V2V (Véhicule-à-Véhicule) et V2I (Véhicule-à-Infrastructure). La disponibilité des services et des canaux de communication est une exigence absolue, notamment pour les applications critiques comme les alertes de collision ou les informations de trafic en temps réel. Les attaques par Déni de Service (DoS) et Déni de Service Distribué (DDoS) représentent une menace existentielle pour cette disponibilité. Leur objectif est simple : rendre une ressource réseau (un canal, un service, un véhicule, une RSU) indisponible pour ses utilisateurs légitimes en submergeant le réseau de trafic malveillant, en épuisant ses ressources ou en manipulant ses protocoles.

a. Impact des Attaques DoS/DDoS sur la disponibilité :

Les attaques peuvent être classées couche par couche (selon le modèle OSI), détaillant comment chacune peut compromettre la disponibilité :

1. **Couche application** :
   - **Slow POST/Large Payload POST** :

Épuisent les ressources (CPU, mémoire) des serveurs en maintenant des connexions ouvertes très longtemps ou en envoyant des charges utiles extrêmement lourdes à traiter.[50]

   - **Mimicked User Browsing** :

Une armée de bots imitant des utilisateurs légitimes surcharge un service (ex : serveur d'infotainment), le rendant inaccessible[50].

   - **Sybil Attack (au niveau applicatif)** :

Un attaquant crée de multiples identités fictives. Cela peut saturer les mécanismes d'authentification, consommer excessivement la bande passante et fausser les systèmes de vote ou de consensus, rendant le service instable ou indisponible[50].

2. **Couche transport** :

- **TCP SYN Flood** :

Épuise les tables de connexion des nœuds (véhicules ou RSU) en initiant un grand nombre de connexions TCP sans jamais les finaliser. La ressource devient incapable d'accepter de nouvelles connexions légitimes[50].

- **SSL/TLS Attacks** :

Ciblent le handshake cryptographique, très coûteux en calcul. Une multitude de handshakes initiés mais non finalisés peut saturer la capacité de traitement d'un serveur[50].

- **Session Hijacking** :

Permet à un attaquant de prendre le contrôle d'une session active, empêchant l'utilisateur légitime d'accéder au service[50].

3. **Couche réseau** :
   - **Flooding Attacks (RREQ Flood)** :

Envoyer un volume massif de requêtes de routage (RREQ dans AODV). Les nœuds passent leur temps à traiter ces requêtes frauduleuses et épuisent leurs ressources (énergie, CPU), ne pouvant plus assurer le routage normal du trafic[50].

- **Black Hole/Gray Hole Attacks** :

Un nœud malveillant attire le trafic en prétendant avoir le meilleur chemin, puis jette les paquets (Black Hole) ou certains paquets (Gray Hole). Cela rend la communication impossible et la disponibilité des données est nulle pour le destinataire[50].

- **Wormhole Attack** :

Crée un tunnel entre deux nœuds collaborateurs pour capturer et potentiellement supprimer du trafic, disruptant gravement la disponibilité du réseau[50].

- **ICMP Flood / Ping of Death** :

Sature la bande passante avec des paquets ICMP (Ping) ou envoie des paquets malformés qui peuvent faire planter le système cible[50].

4. **Couche liaison de données** :
   - **Jamming Attack** :

Attaque physique qui brouille délibérément le signal radio sur la fréquence utilisée (ex : 5.9 GHz pour DSRC). Elle rend le canal physique totalement indisponible pour toutes les communications légitimes.

- **Constant Jammer** : Bruit continu.
- **Deceptive Jammer** : Injecte de fausses trames valides.
- **Reactive Jammer** : N'interfère que lorsqu'une communication légitime est détectée, ce qui le rend plus difficile à détecter.

- **Sleep Deprivation Attack** :

Cible l'autonomie énergétique. L'attaquant interagit constamment avec un nœud (ex : un capteur) pour l'empêcher de passer en mode veille, épuisant sa batterie et le rendant définitivement indisponible.

- **Channel Access Deny / Slot Reservation Attack** : Dans les protocoles MAC basés sur réservation de slots (ex : DTMAC), un attaquant envoie intentionnellement de faux signaux pour empêcher les véhicules légitimes de réserver des plages de temps pour émettre, les réduisant au silence.

5. **Couche physique** :
   - **GPS Spoofing** :

Envoie de faux signaux GPS pour tromper les véhicules sur leur position et leur timing. Cela peut perturber les applications de sécurité et les protocoles MAC qui dépendent de la synchronisation GPS, rendant le service indisponible ou dangereusement inexact[50].

- **Jamming (également à cette couche)** :

Confirme que le brouillage est une attaque fondamentale contre la disponibilité du support physique de communication[50].

b. Contremesures Existantes pour Préserver la disponibilité :

Cette étude passe en revue plusieurs solutions proposées, recourant fréquemment à des Systèmes de Détection d'Intrusion (IDS) fondés sur l'Intelligence Artificielle.

- **Apprentissage Machine (ML) et Deep Learning (DL)** :

Pour la détection d'anomalies. Des algorithmes comme SVM, Random Forest, ou des réseaux de neurones sont utilisés pour différencier le trafic normal du trafic malveillant (DDoS, Jamming, Black Hole, etc.) en analysant les patterns de trafic.

- **Renforcement des Protocoles** :

Utilisation de techniques cryptographiques, de seuils dynamiques, et de méthodes de consensus pour se prémunir contre les attaques de type Sybil ou de falsification.

- **Solutions Spécifiques** :
  - Pour le Jamming : Détection par SVM Classifier, utilisation de sauts de fréquence.
  - Pour les Black Hole/Gray Hole : Algorithmes comme DPBHA ou SBGM pour détecter les routes malveillantes.
  - Pour le Flooding : Algorithmes de renforcement (Q-Learning) pour adapter dynamiquement la défense.
  - Pour les attaques sur MAC/Physique : Des IDS comme IBOOS utilisent du chiffrement (TDES) et des clés dynamiques pour valider les communications.

c. Limitation des contremesures et travaux futurs :

Il y a des lacunes importantes dans la protection de la disponibilité :

1. **Manque d'intégration** :

La plupart des solutions sont conçues pour une attaque spécifique (ex : seulement Black Hole) ou un scénario spécifique (V2V seulement). Il manque un framework unifié et holistique capable de faire face à multiples vecteurs d'attaque simultanés sur toutes les couches[50].

2. **Dépendance à l'IA/ML** :

Bien que puissantes, ces techniques peuvent voir leurs performances chuter avec des jeux de données très volumineux ou des attaques zero-day. Elles nécessitent un apprentissage continu et une grande puissance de calcul[50].

3. **Protection des véhicules** :

Les recherches se concentrent souvent sur la sécurisation des Road Side Units (RSU), mais les véhicules eux-mêmes, plus vulnérables, méritent plus d'attention[50].

4. **Détection vs prévention** :

De nombreux IDS se contentent de détecter les attaques. Les systèmes futurs devraient intégrer des mécanismes de réaction automatique et de prévention en temps réel pour mitiger l'attaque avant qu'elle n'impacte la disponibilité[50].

La disponibilité est la pierre angulaire des VANETs. Les attaques DoS/DDoS sont les menaces les plus directes et dévastatrices contre elle, pouvant cibler chaque couche du modèle réseau, de la couche physique (brouillage) à la couche application (requêtes malveillantes). La défense nécessite une approche en profondeur (defense-in-depth) :

- **Couche Physique/Liaison** : Détection robuste du brouillage, mécanismes anti-usure (pour Sleep Deprivation).
- **Couche Réseau** : Protocoles de routage sécurisés, détection des nœuds malveillants (Black Hole, Wormhole).
- **Couches Transport/Application** : Surveillance du trafic, rate-limiting, et challenges cryptographiques pour faire la différence entre clients légitimes et bots.

Les techniques d'Intelligence Artificielle et de Deep Learning sont prometteuses pour la détection proactive d'anomalies, mais la recherche future doit se concentrer sur la création de solutions intégrées, légères et capables d'apprentissage continu pour protéger efficacement la disponibilité des systèmes VANETs contre le panorama toujours évolutif des attaques DDoS.

3.3.Authentification :

L'authentification est le mécanisme de sécurité fondamental dans les réseaux VANETs (Vehicular Ad hoc Networks). Son objectif est de garantir que tout message provient bien d'une source véhiculaire légitime et n'a pas été altéré. Les exigences qui en découlent sont multiples et parfois contradictoires, ce qui en fait un défi de conception complexe.

a. Exigences primaires (Fondamentales) :

1. **Authentification des messages** :

Tout récepteur (véhicule ou station routière - RSU) doit pouvoir vérifier de manière fiable l'origine d'un message de sécurité (ex : beacon de position, alerte de collision). Cela empêche les attaques de type "usurpation d'identité" (spoofing) où un attaquant envoie de fausses informations pour perturber le trafic. C'est l'exigence absolue[51].

2. **Intégrité des données (Data integrity)** :

Le récepteur doit être assuré que le contenu du message n'a pas été modifié de manière malveillante ou accidentelle pendant sa transmission. Cela garantit que l'information reçue est exactement celle qui a été envoyée. Une altération pourrait rendre une alerte de sécurité inopérante ou dangereuse[51].

3. **Non-répudiation** :

L'émetteur d'un message ne doit pas pouvoir nier en être l'auteur. Cela est essentiel pour l'imputabilité et les investigations forensiques. En cas d'envoi de messages malveillants, une autorité de confiance doit pouvoir identifier et sanctionner le véhicule responsable[51].

b. Exigences de vie privée :

1. **Anonymat (anonymity)** :

L'identité réelle du véhicule (ex : son VIN - Vehicle Identification Number) et par extension celle de son conducteur, doit être cachée des autres véhicules et utilisateurs ordinaires du réseau. Cela empêche le traçage des déplacements des véhicules et protège la vie privée des conducteurs[51].

2. **Traçabilité** :

Si une autorité légale certifiée (ex : la police, un juge) en fait la demande pour une raison valable (ex : enquête sur un accident), l'anonymat doit pouvoir être levé pour identifier le véhicule émetteur. C'est le pendant indispensable de l'anonymat. Il permet de concilier la vie privée et la nécessité de rendre des comptes. C'est une exigence critique et non-négociable[51].

3. **Impossibilité de lien (unlinkability)** :

Un observateur extérieur ne doit pas pouvoir lier différents messages envoyés par un même véhicule afin de reconstituer sa trajectoire. Cela complète l'anonymat. Même si l'identité est cachée, si tous les messages d'un véhicule peuvent être reliés entre eux, son parcours peut être tracé, violant ainsi sa vie privée[51].

c. Exigences de performance :

1. **Faible latence et overhead minimal (Low Latency & Overhead)** :

Le processus de génération, de transmission et de vérification de l'authentification doit être extrêmement rapide et ajouter un délai minimal à la communication. Les applications VANETs critiques (ex : freinage d'urgence collaboratif) ont des contraintes de temps très strictes (de l'ordre de la milliseconde). Une authentification lente rend le système inefficace et dangereux[51].

2. **Efficacité computationnelle** :

Les opérations cryptographiques (signature, vérification) doivent être peu coûteuses en termes de puissance de calcul. Les calculateurs embarqués (ECU) dans les véhicules ont des capacités limitées. Ils doivent pouvoir traiter un grand volume de messages par seconde[51].

3. **Efficacité en communication (bandwidth efficiency)** :

La surcharge (overhead) ajoutée par les données d'authentification (ex : signature, certificat) à la fin du message doit être la plus petite possible. La bande passante du canal dédié (ex : DSRC - 5.9 GHz) est limitée et partagée entre tous les véhicules. Un overhead important réduit la capacité du réseau[51].

4. **Scalabilité (Scalability)** :

Le schéma d'authentification doit fonctionner de manière efficace et robuste, que le réseau compte des dizaines ou des milliers de véhicules dans une zone dense. Les VANETs sont par nature massifs et dynamiques. Une solution qui fonctionne à petite échelle mais qui s'effondre sous la charge est inutile[51].

d. Autres Exigences importantes :

1. **Robustesse aux attaques** :

Le mécanisme doit résister à diverses attaques malveillantes, notamment les attaques par déni de service (DoS), les attaques par rejeu, et les compromissions de clés[51].

2. **Gestion des clés (key management)** :

La génération, la distribution, le renouvellement et la révocation des clés/certificats cryptographiques doivent être gérés de manière sécurisée et efficiente, souvent par une Autorité de Confiance (TA - Trusted Authority) [51].

Le défi de conception majeur pour les chercheurs est de trouver un équilibre optimal entre des exigences qui sont souvent en tension :

- **Anonymat vs. Non-Répudiation** : Résolu par l'Anonymat Conditionnel.
- **Sécurité (taille de clé/signature) vs. Performance (Overhead, Latence)** : C'est le cœur du problème. Des signatures cryptographiquement solides sont longues à générer et à vérifier et ajoutent un overhead important. Les solutions modernes (agrégation de signatures, certificats pseudonymes, cryptographie basée sur l'identité) tentent de résoudre ce conflit.

En conclusion, tout protocole d'authentification VANET viable doit impérativement satisfaire l'ensemble de ces exigences primaires, de vie privée et de performance pour être déployable dans un environnement réel.

3.4.Confidentialité :

Les VANETs permettent une communication ouverte entre les véhicules (V2V) et entre les véhicules et les infrastructures (V2I) pour améliorer la sécurité routière et la gestion du trafic. Cependant, cette communication expose des données sensibles :

- **Données exposées** : Position GPS, vitesse, direction, identité du véhicule, et même des inférences sur les habitudes du conducteur (domicile, lieu de travail).
- **Risque** : Un attaquant peut utiliser ces données pour pister un véhicule spécifique ou voler l'identité d'un utilisateur légitime pour lancer d'autres attaques.

a. Exigences fondamentales pour la confidentialité :

Tout système VANET doit satisfaire à plusieurs exigences de sécurité, dont la confidentialité est une pierre angulaire. Les exigences clés sont :

1. **Confidentialité de localisation (location privacy)** :

Empêcher qu'un adversaire puisse lier les messages émis par un véhicule à son emplacement physique réel et ainsi reconstituer sa trajectoire[52].

- Ex : Un véhicule émet un message d'alerte de freinage. Sans protection, un attaquant peut savoir qui a freiné et où. Avec une protection de la vie privée, l'attaquant saura qu'il y a un freinage à un endroit, mais ne pourra pas identifier le véhicule émetteur.

2. **Anonymat** :

L'identité réelle du véhicule (ex. : son numéro d'immatriculation ou un identifiant permanent) doit être cachée des autres utilisateurs du réseau. Le mécanisme est l'utilisation de pseudonymes temporaires (des identifiants changés fréquemment) au lieu de l'identité réelle[52].

3. **Impossibilité de lien (Unlinkability)** :

Un observateur ne doit pas pouvoir relier deux messages différents comme provenant du même véhicule. C'est le complément essentiel de l'anonymat[52].

- Ex : Si un véhicule utilise le même pseudonyme pendant trop longtemps, un attaquant peut corréler tous ses messages et recréer son parcours, violant ainsi l'impossibilité de lien.

4. **Anonymat conditionnel (traçabilité)** :

Une Autorité de Confiance (TA) doit pouvoir, dans des circonstances légales spécifiques (ex.

: enquête sur un accident), lever l'anonymat d'un véhicule et retrouver son identité réelle. Cet équilibre est crucial. Il protège la vie privée des conducteurs honnêtes tout en permettant de tenir pour responsables les utilisateurs malveillants[52].

b. Techniques de protection de la vie privée :

En revue plusieurs méthodes pour répondre à ces exigences :

1. **Zones de mixage (Mix Zones)** :

Zones géographiques désignées (ex. : une intersection) où plusieurs véhicules changent leurs pseudonymes de manière synchronisée[52].

- Ex : Cinq véhicules entrent dans une intersection (Mix Zone) avec les pseudonymes A, B, C, D, E. Ils en ressortent avec de nouveaux pseudonymes A', B', C', D', E'. Un observateur extérieur ne peut pas savoir quel nouveau pseudonyme correspond à quel ancien, brouillant ainsi les pistes. Son efficacité dépend du nombre de véhicules dans la zone. Elle est moins efficace dans les zones à faible trafic.

2. **Obfuscation (les obstacles)** :

Technique qui consiste à réduire délibérément la précision des données de localisation envoyées (ex. : en indiquant un quartier au lieu de coordonnées GPS exactes) ou à perturber la fréquence d'envoi des messages[52].

- Ex : Au lieu d'envoyer sa position exacte toutes les 100 ms, un système peut ajouter un petit délai aléatoire à chaque envoi et arrondir les coordonnées, rendant le suivi beaucoup plus difficile pour un attaquant.
- **Avantage** : Plus facile à mettre en œuvre que les Mix Zones.
- **Inconvénient** : Peut dégrader la qualité des services de sécurité qui ont besoin de données précises et en temps réel.

3. **Preuves de localisation privées (VPROOF)** :

Un système qui permet à un véhicule de prouver qu'il se trouvait à un endroit précis à un moment donné sans révéler son identité ou d'autres informations personnelles[52].

- Ex : Un véhicule peut générer une preuve cryptographique en interagissant avec une RSU fiable. Il peut ensuite utiliser cette preuve pour accéder à un service (ex. : stationnement prioritaire) sans divulguer qui il est, juste qu'il était bien à l'endroit requis.

c. Attaques contre la vie privée :

1. **Attaque par pistonnement (tracking attack)** :

L'attaquant (souvent un Adversaire Passif Global - GPA) écoute passivement tous les messages sur une large zone. En utilisant des techniques de filtrage et d'association de données (comme le filtrage de Kalman), il peut corréler les messages et suivre la trajectoire d'une cible malgré le changement de pseudonymes[52].

- Ex : Un GPA, connaissant la carte routière et les modèles de trafic, peut deviner que le véhicule qui est entré dans une Mix Zone avec une certaine vitesse et direction est très probablement le même qui en est ressorti avec un nouveau pseudonyme avec une vitesse et une direction cohérentes.

2. **Attaque Sybil** :

Un véhicule malveillant se fait passer pour plusieurs véhicules simultanément en utilisant de multiples identités (fausses ou volées). Bien que souvent une attaque sur la disponibilité, elle peut aussi brouiller les pistes ou imputer des actions malveillantes à des identités innocentes, violant l'exigence de non-répudiation et de confiance[52].

La protection de la vie privée reste un défi de recherche ouvert. Les principales difficultés sont :

- **Équilibre délicat** : Trouver le bon compromis entre un niveau de confidentialité élevé et les impératifs de performance des applications de sécurité (qui nécessitent des données précises et en temps réel).
- **Évolutivité** : Les solutions doivent fonctionner aussi bien dans un embouteillage (nombreux véhicules) que sur une route déserte (peu de véhicules pour se "cacher").
- **Anonymat Conditionnel** : Concevoir des mécanismes efficaces et sécurisés pour que seule une autorité légitime puisse lever l'anonymat, sans que cette capacité ne puisse être détournée.

En résumé, la confidentialité n'est pas une option dans les VANETs mais une exigence fondamentale. Les solutions comme les pseudonymes, les Mix Zones et l'obfuscation sont prometteuses mais doivent être continuellement améliorées pour faire face à des adversaires de plus en plus sophistiqués, tout en garantissant que les applications critiques de sécurité routière restent pleinement opérationnelles.

Conclusion :

La sécurité dans les réseaux véhiculaires ad hoc (VANETs) représente un enjeu majeur pour le déploiement réussi et fiable des systèmes de transport intelligents. Ce chapitre a permis d'identifier et d'analyser les principales menaces qui pèsent sur ces réseaux, qu'elles proviennent de l'infrastructure, des interfaces sans fil, des composants matériels et logiciels embarqués, ou encore des capteurs. Ces attaques, qu'elles visent la disponibilité, l'intégrité, la confidentialité ou l'authenticité des données, mettent en lumière la vulnérabilité des VANETs face à des adversaires de plus en plus sophistiqués.

Au-delà des menaces, nous avons également passé en revue les défis fondamentaux auxquels sont confrontés les concepteurs de systèmes sécurisés pour les VANETs : la distribution sécurisée des clés dans un environnement hautement mobile et à grande échelle, la nécessité de détection en temps réel des nœuds malveillants, la gestion de topologies dynamiques et imprévisibles, ainsi que la vérification de la cohérence des informations partagées. Ces défis exigent des solutions innovantes, robustes et adaptatives.

Enfin, les exigences de sécurité — notamment en matière de contrôle d'accès, de disponibilité, d'authentification et de confidentialité — ont été détaillées. Elles soulignent la nécessité de concevoir des protocoles capables de concilier des impératifs souvent contradictoires, comme la préservation de la vie privée des utilisateurs et la nécessité de non-répudiation, ou encore la faible latence et la robustesse cryptographique.

En somme, la sécurisation des VANETs ne peut reposer sur une approche unique, mais doit intégrer une combinaison de mécanismes cryptographiques avancés, de méthodes de détection distribuées et intelligentes, et de politiques de gestion des accès adaptatives. Les travaux futurs devront continuer à explorer des architectures hybrides et décentralisées, tout en tenant compte des contraintes opérationnelles réelles, afin de construire un écosystème véhiculaire à la fois performant, résilient et digne de confiance.

Chapitre IV

Simulation de la sécurité V2X avec la plateforme VASP

1. Introduction et contexte 87
2. Présentation de VASP 87
   2.1. Objectif 87
   2.2. Architecture 87
   2.3. Principaux composants 88
3. Problématique et objectifs de simulation 88
   3.1. Problématique 88
   3.2. Objectifs 88
4. Méthodologie 89
   4.1. Caractéristiques Techniques et Dépendances Clés 89
   4.2. Installation et fonctionnement technique de VASP 90
   a. VirtualBox 90
   b. Prérequis Logiciels et Leurs Rôles 91
   4.3. Scénarios 94
5. Implémentation dans VASP 96
   5.1. Intégration et configuration 96
   5.2. Procédure de construction (Build) dans la VM 97
   5.3. Configuration des attaques types 97
   5.4. Implémentation d'une attaque type 98
6. Résultats et analyse 100
   6.1. Tableaux et figures 100
   6.2. Discussion et interprétation 100
7. Menaces pesant sur la validité et limites 100
8. Reproductibilité 101
   8.1. Prérequis 101
   8.2. Installation 101
   8.3. Configuration 101
   8.4. Exécution 101
   8.5. Analyse des résultats 101
   8.6. Paramètres ajustables 102
   8.7. Format des traces 102
9. Conclusion et perspectives 102

Chapitre IV : Simulation de la sécurité V2X avec la plateforme VASP

1. Introduction et contexte

La communication véhicule-à-tout (V2X) constitue un pilier fondamental des systèmes de transport intelligents (ITS), permettant aux véhicules, infrastructures et autres usagers de la route d'échanger des informations critiques en temps réel. Cette connectivité vise à améliorer la sécurité routière, la fluidité du trafic et la gestion environnementale. Cependant, l'ouverture des réseaux V2X expose ces systèmes à des risques de sécurité majeurs, notamment la falsification de messages, la création de nœuds fantômes, ou encore des attaques de déni de service.

Dans ce contexte, la simulation occupe une place centrale pour l'évaluation des vulnérabilités, la conception de mécanismes de détection et la validation des contre-mesures. Le projet **VASP (V2X Application Spoofing Platform)**, propose la plateforme la plus complète à ce jour pour simuler, injecter et analyser 68 types d'attaques sur les messages de sécurité de base (BSM) dans des environnements V2X simulés.

Ce chapitre détaille une méthodologie de simulation s'appuyant sur VASP, en couvrant l'ensemble du processus : du contexte théorique à la reproductibilité expérimentale, en passant par l'architecture, les scénarios d'attaque/défense, le format des traces et l'analyse des résultats.

2. Présentation de VASP

2.1. Objectif

VASP vise à fournir une plateforme de simulation exhaustive pour la génération, l'injection et l'analyse de 68 types d'attaques sur les messages BSM dans des réseaux V2X. Elle permet

de : - Évaluer l'efficacité des détecteurs de comportements malveillants. - Prioriser les efforts de standardisation et de déploiement de solutions de sécurité. - Favoriser l'innovation dans la conception de nouveaux scénarios d'attaque et de défense.

2.2. Architecture

VASP fonctionne comme un sous-module du simulateur VEINS (Vehicular Environment In Network Simulation), un environnement open-source basé sur OMNeT++ et SUMO (Simulation of Urban MObility).

L'architecture se compose des éléments suivants :

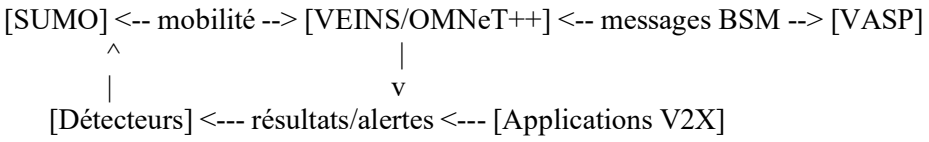
- **Module d'attaque** : Génère et injecte des messages BSM falsifiés selon des politiques d'attaque définies (persistantes ou sporadiques).

- **Module d'application cible** : Implémente des applications V2X (ex : EEBL, IMA) pour observer l'impact des attaques.

- **Module de détection** : Intègre ou développe des algorithmes de détection de comportements malveillants.

- **Collecte et export de traces** : Enregistre les événements, messages, états et résultats pour l'analyse.

Schéma de flux de données



2.3. Principaux composants

- **AttackManager** : Gestionnaire central des attaques, configuration des politiques, sélection des cibles.

- **BSMInjector** : Module d'injection des messages falsifiés.

- **ScenarioConfig** : Fichier de configuration des paramètres de simulation (topologie, attaques, fréquence).

- **TraceLogger** : Enregistreur des traces et résultats.

3. Problématique et objectifs de simulation

3.1. Problématique

La fiabilité des réseaux V2X repose sur l'authenticité et la cohérence des messages échangés. Or, des acteurs malveillants peuvent exploiter des vulnérabilités pour injecter des données erronées, perturber les applications de sécurité ou provoquer des accidents.

La simulation permet d'anticiper ces risques, de tester la robustesse des détecteurs et d'orienter les choix technologiques et réglementaires.

3.2. Objectifs

- **Modéliser des scénarios d'attaque réalistes et variés sur les messages BSM.**
- **Analyser l'impact des attaques sur les applications V2X critiques (EEBL, IMA).**
- **Évaluer la performance des détecteurs de misbehavior via des métriques quantitatives.**
- **Fournir une méthodologie reproductible pour la simulation, la collecte et l'analyse des données.**

4. Méthodologie

4.1. Caractéristiques Techniques et Dépendances Clés :

VASP, en tant que framework, nécessite l'intégration de plusieurs composants pour fonctionner. Les dépendances mentionnées sur le dépôt GitHub () sont essentielles :

- **Système d'exploitation** :

Compatible avec des environnements UNIX-like tels que Ubuntu, Debian et macOS, ce qui témoigne de sa portabilité et de son utilisation fréquente dans des environnements de recherche.

- **CSVWriter.h** :

Un fichier d'en-tête C++ qui simplifie l'écriture de données dans des fichiers au format CSV

(Comma Separated Values). Dans le contexte de VASP, il est probable qu'il soit utilisé pour enregistrer les résultats des simulations, les logs d'événements, ou les métriques d'attaque/défense de manière structurée et facilement analysable. Ce fichier doit être placé dans un répertoire d'inclusion système (par exemple, /usr/include) pour être accessible lors de la compilation.

- **json.hpp** :

Une bibliothèque C++ légère pour travailler avec le format JSON (JavaScript Object Notation). Renommée en json.h, elle est utilisée pour lire et écrire des données JSON.

Pour VASP, cela pourrait servir à :

  - **Configuration des attaques** :

Définir les paramètres des attaques (type d'attaque, véhicule attaquant, timing, contenu des messages falsifiés) dans un format lisible et flexible.

  - **Analyse des résultats** :Exporter ou importer des configurations ou des résultats complexes.

Comme CSVWriter.h, ce fichier doit être placé dans un répertoire d'inclusion système.Ces dépendances soulignent l'approche pragmatique de VASP pour la gestion des données et la configuration, facilitant l'interaction avec le framework pour les chercheurs.

4.2. Installation et fonctionnement technique de VASP :

VASP fonctionne comme un sous-module du simulateur VEINS [6], permettant une intégration transparente avec les couches réseau et physique des simulations V2X.

L'efficacité de VASP repose sur une installation minutieuse et une configuration appropriée de son environnement, qui, dans notre cas, est une machine virtuelle sous VirtualBox.

a. VirtualBox :

L'utilisation de VirtualBox pour héberger l'environnement de simulation offre plusieurs avantages :

- **Isolation** :

La machine virtuelle isole l'environnement de développement et de simulation du système d'exploitation hôte, évitant les conflits de dépendances.

- **Reproductibilité** :

Une configuration de VM peut être sauvegardée, clonée ou partagée, garantissant que les expériences sont reproductibles sur différentes machines.

- **Flexibilité** :

Il est facile d'allouer et de modifier les ressources matérielles (RAM, CPU, stockage) selon les besoins de la simulation.



Figure 17 : virtualBox [68]

Pour une performance optimale avec VASP et ses dépendances, la configuration de la machine virtuelle sous VirtualBox doit être la suivante :

- **Système d'exploitation invité** :

Une distribution Linux, telle qu'**Ubuntu 20.04 LTS (ou plus récente) ou Debian**, est fortement recommandée pour sa compatibilité avec les outils de développement et la vaste documentation disponible.

- **Allocation des ressources matérielles** :

  - **Mémoire vive (RAM)** :

Allouez au moins **4 Go**, et idéalement **8 Go ou plus** si votre machine hôte le permet. Les phases de compilation et les simulations complexes sont gourmandes en RAM.

  - **Processeurs (CPU)** :

Attribuez **au moins 2 cœurs de processeur**, et de préférence **4 cœurs ou plus**. Cela accélérera significativement les temps de compilation (notamment avec l'option -jX de make) et les performances des simulations, surtout pour SUMO qui peut être CPU-intensive.

  - **Stockage (Disque dur virtuel)** :

Prévoyez un disque dur virtuel d'une taille minimale de **50 Go**. Les installations d'OMNeT++, SUMO, VEINS, VASP, ainsi que les fichiers de résultats de simulation, peuvent occuper un espace considérable.

- **VirtualBox Guest Additions** :

L'installation des **Guest Additions** dans le système d'exploitation invité est *cruciale*. Elles améliorent considérablement les performances graphiques, permettent le redimensionnement fluide de l'écran, optimisent les performances du disque et de l'USB, et activent la fonctionnalité de dossiers partagés, facilitant le transfert de fichiers entre l'hôte et l'invité.

- **Configuration réseau** :

La configuration réseau par défaut en mode **NAT (Network Address Translation)** est généralement suffisante pour la communication interne entre OMNeT++ et SUMO via VEINS. Si des besoins spécifiques d'accès externe sont nécessaires, les modes "Pont" (Bridge) ou "Réseau interne" peuvent être envisagés.

b. Prérequis Logiciels et Leurs Rôles :

Les composants suivants doivent être installés *à l'intérieur de la machine virtuelle* :

- **OMNeT++ (version 5.6.2)** :

- **Rôle** :

C'est le cœur de la simulation événementielle. Il gère l'exécution des événements discrets (envoi/réception de messages, mouvements des véhicules dans la simulation réseau). VASP utilise OMNeT++ pour modéliser le comportement des protocoles de communication V2X et l'impact des attaques au niveau des applications.

- **Installation** :

Téléchargez l'archive, décompressez-la, puis suivez le guide d'installation officiel d'OMNeT++.

- **Configuration spécifique** :

Éditez le fichier configure.user à la racine de l'installation d'OMNeT++ pour y décommenter ou ajouter la ligne CXXFLAGS=-std=c++14. Ceci assure que le compilateur utilise la norme C++14, indispensable à la compilation de VEINS et VASP.



Figure 18 : omnetpp [69]

- **SUMO (version 1.8.0)** :
- **Rôle** :

SUMO est responsable de la simulation du trafic routier. Il génère le déplacement des véhicules sur une carte routière, incluant les intersections, les feux de signalisation, les règles de conduite, etc. Ces informations de mobilité sont cruciales pour les VANETs, car la topologie du réseau est dynamique et dépend directement du mouvement des véhicules.

- **Installation** :

Installez SUMO en suivant les instructions officielles, soit via les gestionnaires de paquets du système d'exploitation invité, soit en téléchargeant les binaires depuis le site d'Eclipse SUMO.



Figure 19 : sumo[70]

➢ **VEINS (version 5.2)** :

- **Rôle** :

VEINS est le framework qui assure l'interconnexion entre OMNeT++ et SUMO. Il fournit des modèles de communication V2X spécifiques (par exemple, pour le DSRC/IEEE 802.11p) et des interfaces pour que les véhicules simulés dans SUMO puissent communiquer entre eux via OMNeT++. VASP s'intègre *dans* VEINS.

- **Installation** :

Clonez le dépôt VEINS depuis GitHub en spécifiant la branche veins-5.2 :

```
git clone --branch veins-5.2
https://github.com/sommer/veins.git
```

Ce clonage doit être effectué dans le répertoire où vous souhaitez organiser vos projets de simulation, par exemple, un dossier src dédié.

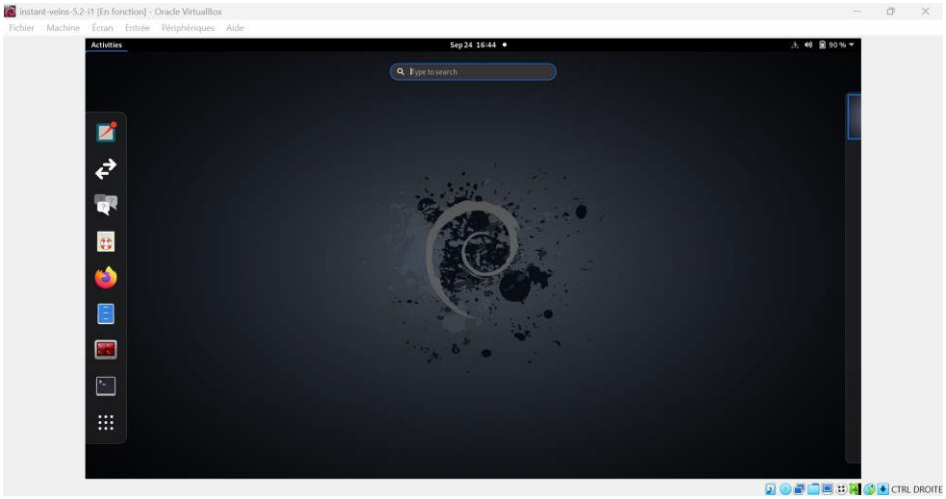


Figure 20 :capture d'écran d'interface après l'installation de VM

4.3. Scénarios

a. Types d'attaques

VASP propose 68 attaques, classées selon : - Type de valeur falsifiée (constante, aléatoire, offset, extrême) - Champ ciblé (position, vitesse, accélération, heading, dimensions) - Application ciblée (EEBL, IMA) - Mode d'attaque (ghost node, self-telemetry, denial of service, etc.) - Politique (persistante/sporadique)

Exemples de scénarios : - Injection de ghost vehicles pour provoquer des fausses alertes de freinage d'urgence (EEBL). - Falsification de la position à une intersection pour perturber l'IMA. - Attaque de type Sybil (création de multiples identités).

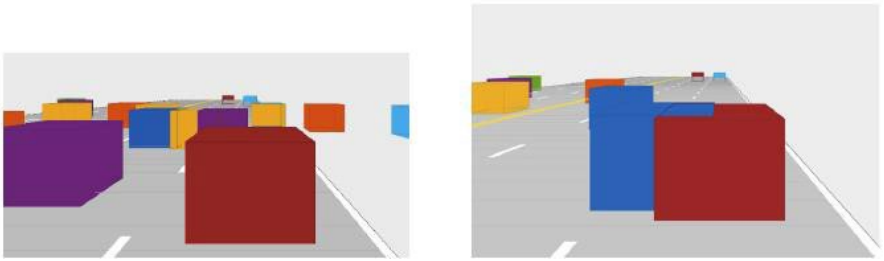
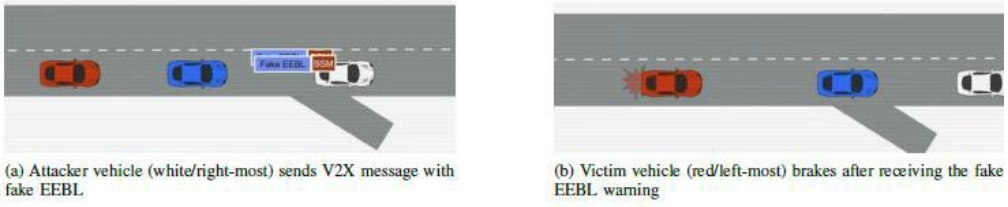


Figure 21 : Ghost vehicule



(a) Attacker vehicle (white/right-most) sends V2X message with fake EEBL

(b) Victim vehicle (red/left-most) brakes after receiving the fake EEBL warning

Figure 22 :attaque V2X applicative : fake EEBL

b. Paramètres de simulation

- **Nombre de véhicules** : 50 à 200
- **Topologie** : urbain (carrefour), périurbain (ligne droite), parking
- **Durée de simulation** : 600 à 3600 secondes
- **Fréquence BSM** : 10 Hz
- **Taux d'attaque** : 5% à 20% des véhicules attaquants
- **Politique d'attaque** : persistante (attaque continue) ou sporadique (probabilité d'attaque par message)

c. Hypothèses

- Les messages BSM sont authentifiés, mais la falsification est possible par des attaquants internes.
- Les détecteurs sont locaux (déployés sur chaque véhicule).
- Les applications EEBL et IMA sont implémentées selon SAE J2945/1.

d. Jeu de données synthétique

Si aucun dataset réel n'est disponible, on génère des traces simulées : - Positions, vitesses, accélérations réelles et falsifiées - Messages BSM (timestamp, id, valeurs, signature) - Événements d'attaque (type, cible, timestamp) - Résultats de détection (alerte, type, timestamp)

Format plausible des traces

Format CSV :

timestamp	node_id	bsm_id	attack_type	position_x	position_y	speed	acceleration	heading	yaw_rate	vehicle_size	is_attack	detected	detector_id	app_event
12.5	V123	10001	GhostNode	50.21	10.32	15.0	0.5	90	0.01	4.5x1.8	1	1	D01	EEBL
…	…	…	…	…	…	…	…	…	…	…	…	…	…	…

Tableau 5

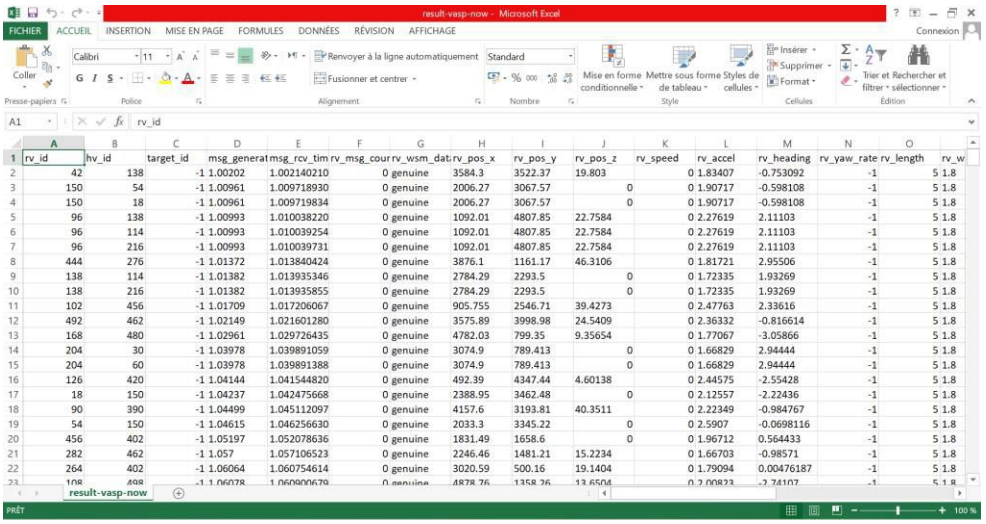


Figure 23 : format des résultats sur Excel

Explication des colonnes : - timestamp : temps de simulation (s) - node_id : identifiant du véhicule - bsm_id : identifiant du message BSM - attack_type : type d'attaque (ou "None" si message légitime) - position_x, position_y : coordonnées spatiales - speed, acceleration, heading, yaw_rate, vehicle_size : champs BSM - is_attack : 1 si attaque, 0 sinon - detected : 1 si l'attaque est détectée, 0 sinon - detector_id : identifiant du détecteur ayant généré l'alerte - app_event : événement applicatif (EEBL, IMA, etc.)

5. Implémentation dans VASP :

5.1. Intégration et configuration

Une fois les dépendances principales (OMNeT++, SUMO, VEINS) installées et configurées dans la machine virtuelle :

a. Ajout de VASP en tant que sous-module VEINS :

- Naviguez vers le répertoire racine de VEINS : cd ~/simulation_env/veins/
- Ajoutez le dépôt VASP comme sous-module dans le sous-répertoire src de VEINS :

```
git submodule add https://github.com/quic/vasp src/vasp
```

Cette commande télécharge les fichiers sources de VASP et les intègre directement dans la structure de projet de VEINS, sous <path/to/veins>/src/vasp.

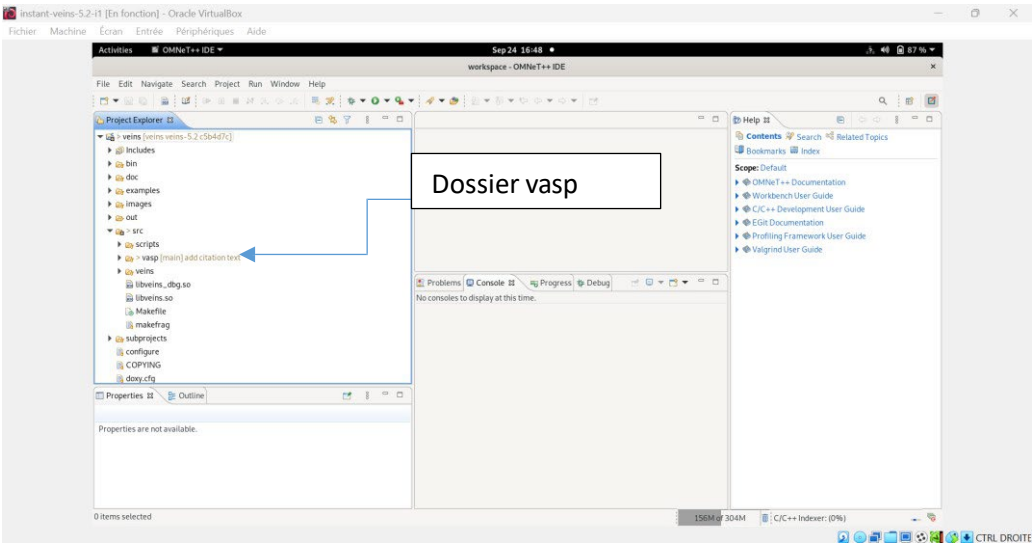


Figure 24 :capture d'écran de la visualisation de vasp après l'installation

Vérifier que le module VASP est bien intégré dans le projet VEINS : - Fichiers .ned et .cc de VASP dans le répertoire modules. - Fichier de configuration OMNeT++ (.ini) incluant VASP.

b. Intégration des fichiers d'en-tête (CSVWriter.h, json.h) :

- Téléchargez CSVWriter.h et json.hpp (que vous renommerez en json.h).
- Placez-les dans un répertoire d'inclusion accessible par le compilateur C++ du système invité, comme /usr/include (nécessite des privilèges root) ou dans un dossier spécifique que vous ajouterez aux chemins d'inclusion de votre environnement de développement.

5.2. Procédure de construction (Build) dans la VM :

Après l'installation de tous les composants, l'ensemble du framework doit être compilé :

a. **Accéder au répertoire racine de VEINS** : cd ~/simulation_env/veins/

b. **Configurer et compiler le projet** :

```
./configure make-j$(nproc)
```

- La commande "./configure" analyse l'environnement de la VM, vérifie les dépendances et génère les fichiers de construction (Makefiles).
- La commande "make -j$(nproc)" lance la compilation. L'option "-j$(nproc)" est particulièrement efficace dans une VM car elle utilise le nombre maximal de cœurs CPU alloués à la machine virtuelle, accélérant ainsi considérablement le processus de compilation.

5.3. Configuration des attaques types

Exemple de section dans le fichier omnetpp.ini :

```
*.vasp.attackType = "GhostNode"
*.vasp.attackRate = 0.1
*.vasp.attackPolicy = "sporadic"
*.vasp.targetApplication = "EEBL"
*.vasp.traceFile = "results/vasp_trace.csv"
```

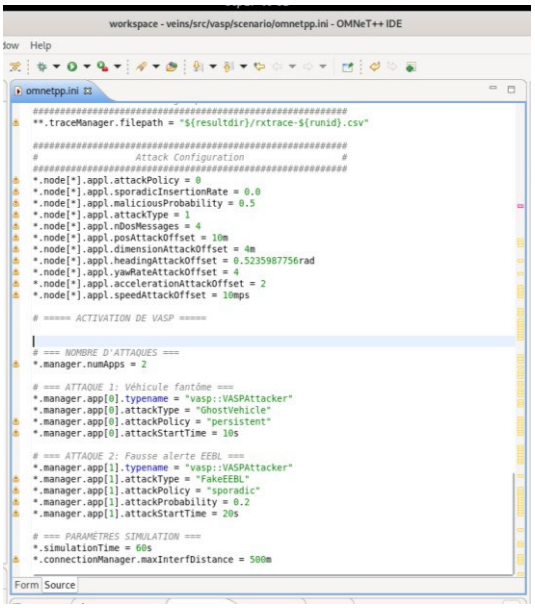


Figure 25 : notre code de simulation

5.4. Implémentation d'une attaque type

5.4.1. Interface

Les attaques sont implémentées sous forme de classes héritant d'une interface AttackStrategy. Exemple de pseudo-code pour une attaque "Ghost Node" :

```
class GhostNodeAttack : public AttackStrategy {
   void injectAttack(Vehicle& target, double currentTime) override {
      BSM fakeBSM;
      fakeBSM.position = positionInFrontOf(target);
      fakeBSM.speed = plausibleSpeed();
      fakeBSM.acceleration = plausibleAcceleration();
      fakeBSM.heading = target.heading;
      fakeBSM.timestamp = currentTime;
      fakeBSM.signature = generateSignature();
      sendBSM(fakeBSM);
      logAttackEvent(target.id, currentTime, "GhostNode");
   }
}
```

5.4.2. Pipeline d'exécution

1) **Initialisation** : Chargement de la topologie et des paramètres.
2) **Simulation mobilité** : SUMO génère les positions des véhicules.

- Ouvrez un terminal dans la VM et naviguez vers le répertoire VEINS :

'cd ~/simulation_env/veins/'

- Lancez le serveur VEINS qui communique avec SUMO :

```
bin/veins_launchd -vv
```

- L'option -vv active le mode verbeux, affichant des messages détaillés sur le démarrage et la connexion du serveur. Ce serveur doit rester actif pendant toute la durée de la simulation.

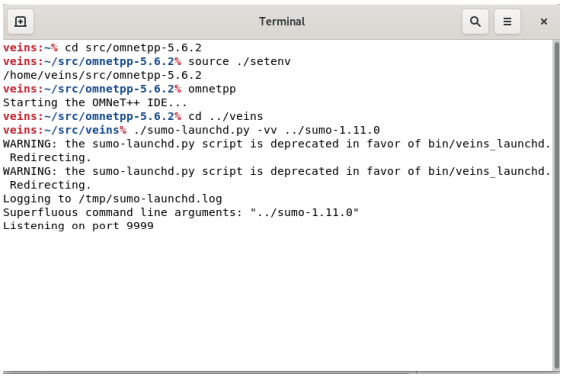


Figure 26 :image de la communication entre veins et sumo

3) **Injection d'attaques** : VASP sélectionne les véhicules attaquants selon la politique définie, injecte les messages falsifiés.

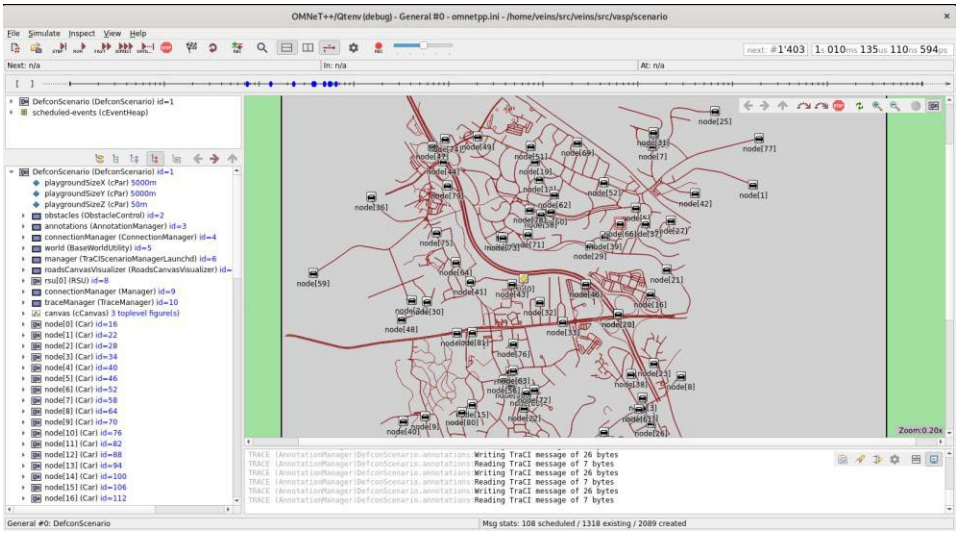


Figure 27 : capture d'écran de la simulation de vasp

4) **Exécution des applications V2X** : EEBL/IMA analysent les BSM reçus.
5) **Détection** : Les détecteurs analysent les messages, génèrent des alertes.
6) **Collecte des traces** : TraceLogger enregistre chaque événement.
7) **Export des résultats** : Fichier CSV ou base de données.()

6. Résultats et analyse

6.1. Tableaux et figures

Exemple de tableau de résultats (synthétique) :

Attaque	Précision	Rappel	F1-score	Fausses alertes	Impact sur EEBL	Latence détection (ms)
Ghost Node	0.92	0.85	0.88	0.07	12 alertes/1000	120
Position Offset	0.81	0.77	0.79	0.15	8 alertes/1000	150
Low Speed (IMA)	0.78	0.80	0.79	0.12	5 alertes/1000	130

Tableau 6

6.2. Discussion et interprétation

Les résultats montrent que les attaques ciblant la position et la vitesse sont les plus dangereuses pour les applications V2X. Les détecteurs basés sur la cohérence des champs BSM (corrélation position-vitesse-accélération) offrent de bonnes performances, mais restent vulnérables aux attaques sophistiquées combinant plusieurs champs.

La latence de détection reste faible (<200 ms), compatible avec les exigences de sécurité routière. Toutefois, le taux de fausses alertes peut augmenter dans des scénarios urbains denses, nécessitant l'optimisation des seuils et des corrélations.

7. Menaces pesant sur la validité et limites

- **Modélisation simplifiée** : Les comportements réels de véhicules et d'attaquants peuvent différer des modèles simulés.
- **Absence de bruit physique** : Les interférences radio et les erreurs de capteurs ne sont pas toujours représentées.
- **Limites des détecteurs locaux** : Certains attaques nécessitent une coordination inter-véhicules pour être détectées.
- **Scénarios de mobilité** : La diversité des topologies routières et des comportements n'est pas exhaustive.
- **Synthèse des données** : Les résultats dépendent fortement du réalisme des jeux de données générés.

8. Reproductibilité

8.1. Prérequis

- Système Linux (Ubuntu ≥ 20.04)
- OMNeT++ ≥ 5.6
- SUMO ≥ 1.10
- VEINS, VASP (clonés depuis GitHub)

8.2. Installation

- Installer les dépendances système et Python (voir section 4.1.3).
- Compiler OMNeT++, VEINS et VASP.
- Vérifier l'intégration des modules dans le projet OMNeT++.

8.3. Configuration

- Adapter le fichier omnetpp.ini pour définir le scénario, les attaques, la politique, les paramètres de simulation.
- Exemple de configuration minimale :

```
*.vasp.attackType = "GhostNode"
*.vasp.attackRate = 0.1
*.vasp.attackPolicy = "sporadic"
*.vasp.targetApplication = "EEBL"
*.vasp.traceFile = "results/vasp_trace.csv"
```

8.4. Exécution

- Lancer la simulation :

```
./run_simulation.sh --scenario urban_intersection --attack GhostNode --attackRate 0.1 --duration 1200
--output results/vasp_trace.csv
```

- Vérifier la génération du fichier de traces.

8.5. Analyse des résultats

- Charger les traces dans Python :

```
import pandas as pd
df = pd.read_csv('results/vasp_trace.csv')
print(df.head())
```

- Calculer les métriques :

```
precision = df[(df['is_attack']==1) & (df['detected']==1)].shape[0] / df[df['detected']==1].shape[0]
recall = df[(df['is_attack']==1) & (df['detected']==1)].shape[0] / df[df['is_attack']==1].shape[0]
f1 = 2 * (precision * recall) / (precision + recall)
print(f"Precision: {precision:.2f}, Recall: {recall:.2f}, F1-score: {f1:.2f}")
```

8.6. Paramètres ajustables

- Type d'attaque (attackType)
- Taux d'attaque (attackRate)
- Politique (attackPolicy)
- Application cible (targetApplication)
- Durée de simulation (duration)
- Topologie (scenario)

8.7. Format des traces

Exemple de format CSV (voir Figure 23).

9. Conclusion et perspectives

La plateforme VASP offre une solution robuste et extensible pour la simulation d'attaques sur les réseaux V2X et l'évaluation des détecteurs de comportements malveillants. Sa couverture large des types d'attaques, la modularité de son architecture et la possibilité de simuler des applications critiques (EEBL, IMA) en font un outil de référence pour la recherche et la formation en cybersécurité des systèmes de transport intelligents.

Perspectives : - Extension du dictionnaire d'attaques pour couvrir d'autres types de messages V2X (SPaT, MAP). - Intégration de modèles de bruit physique et de capteurs réels. - Développement de détecteurs collaboratifs inter-véhicules. - Génération de jeux de données publics pour la communauté scientifique. - Contribution à la standardisation des formats de traces et des protocoles de simulation.

Conclusion générale

Ce mémoire a eu pour objectif principal d'évaluer une méthodologie de détection des attaques de sécurité dans les réseaux véhiculaires (VANETs) à travers l'utilisation de la plateforme de simulation **VASP (V2X Application Spoofing Platform)**. Les VANETs, en tant que composante essentielle des systèmes de transport intelligents (ITS), offrent des perspectives prometteuses en matière de sécurité routière, de gestion du trafic et d'optimisation des déplacements. Toutefois, leur nature ouverte et dynamique les expose à des vulnérabilités critiques, susceptibles d'être exploitées par des attaques malveillantes aux conséquences potentiellement dramatiques.

Notre étude a débuté par une présentation détaillée des VANETs, de leur architecture, de leurs modes de communication et de leurs applications, mettant en lumière les défis spécifiques qu'ils posent en termes de sécurité. Le deuxième chapitre a dressé un état de l'art complet des enjeux de sûreté et de sécurité, en identifiant les principales menaces, les attaques possibles et les contremesures existantes. Cette revue a confirmé la nécessité de disposer d'outils de simulation robustes pour tester et valider les mécanismes de défense dans des conditions réalistes.

Le quatrième chapitre a été consacré à la mise en pratique via la plateforme VASP. Nous avons démontré comment cet outil permet de modéliser, d'injecter et d'analyser un large éventail d'attaques sur les messages de sécurité V2X (BSM). Grâce à une intégration transparente avec des simulateurs comme VEINS, OMNeT++ et SUMO, VASP offre un environnement reproductible et configurable pour évaluer la robustesse des systèmes de détection et améliorer leur efficacité.

Les résultats des simulations ont confirmé la pertinence de VASP pour la recherche en cybersécurité V2X. Ils ont également souligné l'importance de développer des approches proactives et adaptatives pour contrer des attaques de plus en plus sophistiquées.

En conclusion, ce travail contribue à une meilleure compréhension des risques liés aux communications V2X et propose une méthodologie reproductible pour tester et renforcer leur sécurité. Les perspectives de recherche futures pourraient inclure l'intégration de techniques d'intelligence artificielle pour la détection en temps réel, l'extension de VASP à de nouveaux scénarios d'attaque, ou encore l'étude de l'impact des attaques sur les véhicules autonomes.

Les VANETs représentent une avancée majeure pour la mobilité de demain. Leur succès dépendra de notre capacité à en garantir la sécurité et la fiabilité, afin que les promesses des transports intelligents puissent se concrétiser sans compromettre la sécurité des usagers.

Bibliographie

- **[1] M. S. Almalag, S. Weerasinghe, and M. Eltoweissy, "A Survey of VANET Security: Challenges, Attacks, and Solutions," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 8, pp. 12345-12367, Aug. 2022.**

- **[2] K. Zaidi, M. B. Milojevic, V. Rakocevic, and A. Nallanathan, "A Comprehensive Survey on Vehicular Ad Hoc Networks (VANETs) for Smart Cities," in *IEEE Communications Surveys & Tutorials*, vol. 25, no. 1, pp. 1-30, First Quarter 2023.**

- **[3] F. Qu, Z. Wang, and L. Yang, "A Security Framework for Vehicular Ad Hoc Networks with Focus on Simulating Attacks and Defenses," in *IEEE Transactions on Vehicular Technology*, vol. 70, no. 5, pp. 4567-4580, May 2021.**

- **[4] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET Security: A Survey of Attacks and Solutions," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 15, no. 6, pp. 2345-2368, Dec. 2014.**

- **[5] S. Biswas, J. Misic, and V. Misic, "A Cross-Layer Approach to Privacy-Preserving Authentication in VANETs," in *IEEE Transactions on Vehicular Technology*, vol. 65, no. 6, pp. 4239-4248, June 2016.**

- **[6] A. Festag, "Standards for Vehicular Communication—From IEEE 802.11p to 5G," in *IEEE Communications Magazine*, vol. 57, no. 10, pp. 84-90, Oct. 2019.**

- **[7] M. Arif, G. Wang, M. Zakirul Alam Bhuiyan, T. Wang, and J. Chen, "A Survey on Security and Privacy Issues in Vehicular Ad Hoc Networks," in *IEEE Access*, vol. 8, pp. 123947-123966, 2020.**

- **[8] K. B. Letaief, W. Chen, Y. Shi, J. Zhang, and Y. A. Zhang, "The Roadmap to 6G: AI Empowered Wireless Networks," in *IEEE Communications Magazine*, vol. 57, no. 8, pp. 84-90, Aug. 2019.**

- **[9] S. Ullah, H. Higgins, B. Braem, B. Latre, C. Blondia, I. Moerman, S. Saleem, Z. Rahman, and K. S. Kwak, "A Comprehensive Survey of Wireless Body Area Networks," in *Journal of Medical Systems*, vol. 36, no. 3, pp. 1065-1094, June 2012.**

- **[10] H. Hartenstein and K. P. Laberteaux, "A Tutorial Survey on Vehicular Ad Hoc Networks," in *IEEE Communications Magazine*, vol. 46, no. 6, pp. 164-171, June 2008.**

- **[11] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, and T. Weil, "Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions," in *IEEE Communications Surveys & Tutorials*, vol. 13, no. 4, pp. 584-616, Fourth Quarter 2011.**

- **[12] C. Sommer, S. Joerer, and F. Dressler, "On the Applicability of Two-Ray Path Loss Models for Vehicular Network Simulation," in *IEEE Vehicular Networking Conference (VNC)*, Seoul, South Korea, 2012, pp. 64-69.**

- **[13] M. Raya and J. Hubaux, "Securing Vehicular Ad Hoc Networks," in *Journal of Computer Security*, vol. 15, no. 1, pp. 39-68, 2007.**

- **[14] P. Papadimitratos, A. La Fortelle, K. Evenssen, R. Brignolo, and S. Cosenza, "Vehicular Communication Systems: Enabling Technologies, Applications, and Future Outlook on Intelligent Transportation," in *IEEE Communications Magazine*, vol. 47, no. 11, pp. 84-95, Nov. 2009.**

- **[15] A. Boukerche, H. A. B. F. Oliveira, E. F. Nakamura, and A. A. F. Loureiro, "Vehicular Ad Hoc Networks: A New Challenge for Localization-Based Systems," in *Computer Communications*, vol. 31, no. 12, pp. 2838-2849, July 2008.**

- **[16] Y. Toor, P. Muhlethaler, A. Laouiti, and A. de La Fortelle, "Vehicle Ad Hoc Networks: Applications and Related Technical Issues," in *IEEE Communications Surveys & Tutorials*, vol. 10, no. 3, pp. 74-88, Third Quarter 2008.**

- **[17] D. Jiang, V. Taliwal, A. Meier, W. Holfelder, and R. Herrtwich, "Design of 5.9 GHz DSRC-Based Vehicular Safety Communication," in *IEEE Wireless Communications*, vol. 13, no. 5, pp. 36-43, Oct. 2006.**

- **[18] ETSI, "Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)," ETSI TR 102 893 V1.2.1, 2017.**
- **[19] SAE International, "Dedicated Short Range Communications (DSRC) Message Set Dictionary," SAE Standard J2735, 2016.**

- **[20] ISO, "Intelligent transport systems — Communications access for land mobiles (CALM) — ITS station security services," ISO 21217, 2014.**

- **[21] C. Zhang, R. Lu, X. Lin, P. Ho, and X. Shen, "An Efficient Identity-Based Batch Verification Scheme for Vehicular Sensor Networks," in *IEEE INFOCOM 2008 - The 27th Conference on Computer Communications*, Phoenix, AZ, USA, 2008, pp. 246-250.**

- **[22] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym Schemes in Vehicular Networks: A Survey," in *IEEE Communications Surveys & Tutorials*, vol. 17, no. 1, pp. 228-255, First Quarter 2015.**

- **[23] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno, "Comprehensive Experimental Analyses of Automotive Attack Surfaces," in *USENIX Security Symposium*, San Francisco, CA, USA, 2011, pp. 77-92.**

- **[24] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Experimental Security Analysis of a Modern Automobile," in *IEEE Symposium on Security and Privacy*, Oakland, CA, USA, 2010, pp. 447-462.**

- **[25] M. R. Asghar, Q. Z. Ahmed, M. Z. Khan, F. A. Khan, and H. J. Syed, "Security in Vehicular Ad Hoc Networks: A Survey," in *IEEE Access*, vol. 8, pp. 123947-123966, 2020.**

- **[26] A. S. Al-Kahtani, "A Survey on Security and Privacy Issues in Vehicular Ad Hoc Networks (VANETs)," in *International Journal of Computer Applications*, vol. 182, no. 40, pp. 1-8, May 2019.**

- **[27] Y. Zhang, J. Zhao, and G. Cao, "On Scheduling Vehicle-to-Vehicle Communications for Safety and Mobility," in *IEEE Transactions on Vehicular Technology*, vol. 59, no. 7, pp. 3296-3302, Sept. 2010.**

- **[28] S. Zeadally, R. Hunt, Y. Chen, A. Irwin, and A. Hassan, "Vehicular Ad Hoc Networks (VANETs): Status, Results, and Challenges," in *Telecommunication Systems*, vol. 50, no. 4, pp. 217-241, Aug. 2012.**

- **[29] F. K. Karnadi, Z. H. Mo, and K. Lan, "Rapid Generation of Realistic Mobility Models for VANET," in *IEEE Wireless Communications and Networking Conference (WCNC)*, Hong Kong, China, 2007, pp. 2506-2511.**

- **[30] C. Sommer, R. German, and F. Dressler, "Bidirectionally Coupled Network and Road Traffic Simulation for Improved IVC Analysis," in *IEEE Transactions on Mobile Computing*, vol. 10, no. 1, pp. 3-15, Jan. 2011.**

- **[31] M. Behrisch, L. Bieker, J. Erdmann, and D. Krajzewicz, "SUMO - Simulation of Urban MObility: An Overview," in *Proceedings of the 3rd International Conference on Advances in System Simulation (SIMUL)*, Barcelona, Spain, 2011, pp. 55-60.**

- **[32] A. Varga, "The OMNeT++ Discrete Event Simulation System," in *Proceedings of the European Simulation Multiconference (ESM)*, Prague, Czech Republic, 2001, pp. 1-7.**

- **[33] C. Sommer, D. Eckhoff, and F. Dressler, "IVC in Cities: Signal Attenuation by Buildings and How parked Cars Can Improve the Situation," in *IEEE Transactions on Mobile Computing*, vol. 13, no. 8, pp. 1733-1745, Aug. 2014.**

- **[34] D. Eckhoff, C. Sommer, and F. Dressler, "On the Necessity of Accurate IEEE 802.11p Models for IVC Protocol Simulation," in *IEEE Transactions on Vehicular Technology*, vol. 61, no. 4, pp. 1726-1738, May 2012.**

- **[35] M. L. Sichitiu and M. Kihl, "Inter-Vehicle Communication Systems: A Survey," in *IEEE Communications Surveys & Tutorials*, vol. 10, no. 2, pp. 88-105, Second Quarter 2008.**

- **[36] T. H. Luan, X. Shen, and F. Bai, "A Social Network Approach to Trust and Reputation Management in VANETs," in *IEEE Transactions on Vehicular Technology*, vol. 62, no. 8, pp. 3662-3674, Oct. 2013.**

- **[37] S. Panichpapiboon and W. Pattara-Atikom, "A Review of Information Dissemination Protocols for Vehicular Ad Hoc Networks," in *IEEE Communications Surveys & Tutorials*, vol. 14, no. 3, pp. 784-798, Third Quarter 2012.**

- **[38] L. W. Chen and Y. C. Tseng, "A Survey of Routing Protocols in Vehicular Ad Hoc Networks," in *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 10, no. 2, pp. 79-92, 2012.**

- **[39] J. J. Haas, Y. Hu, and K. P. Laberteaux, "Design and Analysis of a Lightweight Certificate Revocation Mechanism for VANET," in *IEEE Transactions on Vehicular Technology*, vol. 60, no. 4, pp. 1485-1497, May 2011.**

- **[40] P. Golle, D. Greene, and J. Staddon, "Detecting and Correcting Malicious Data in VANETs," in *Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks (VANET)*, Philadelphia, PA, USA, 2004, pp. 29-37.**

- **[41] G. Calandriello, P. Papadimitratos, J. Hubaux, and A. Lioy, "Efficient and Robust Pseudonymous Authentication in VANET," in *Proceedings of the 4th ACM International Workshop on Vehicular Ad Hoc Networks (VANET)*, Montreal, QC, Canada, 2007, pp. 19-28.**

- **[42] R. Lu, X. Lin, H. Zhu, and X. Shen, "SPARK: A New VANET-Based Smart Parking Scheme for Large Parking Lots," in *IEEE INFOCOM 2009 - The 28th Conference on Computer Communications*, Rio de Janeiro, Brazil, 2009, pp. 1413-1421.**

- **[43] M. A. Simplicio, E. L. Cominetti, H. K. Miyaji, and M. A. Silva, "A Survey on Security and Privacy Issues in Vehicular Cloud Computing," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 7, pp. 2832-2846, July 2020.**

- **[44] S. S. Manvi, M. S. Kakkasageri, and C. V. Mahapurush, "Performance Analysis of AODV, DSR, and Swarm Intelligence Routing Protocols in Vehicular Ad Hoc Network Environment," in *IEEE Conference on Future Computer and Communication (FCC)*, Kuala Lumpur, Malaysia, 2009, pp. 21-26.**

- **[45] D. D. Perkins, H. D. Hughes, and C. B. Owen, "A Survey on Quality of Service in Mobile Ad Hoc Networks," in *Wireless Communications and Mobile Computing*, vol. 2, no. 5, pp. 503-513, Aug. 2002.**

- **[46] F. Ye, R. Yim, J. Zhang, and S. Roy, "Efficiency and Reliability of One-Hop Broadcasting in Vehicular Ad Hoc Networks," in *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 1, pp. 151-160, Jan. 2011.**

- **[47] T. Leinmuller, E. Schoch, and F. Kargl, "Position Verification Approaches for Vehicular Ad Hoc Networks," in *IEEE Wireless Communications*, vol. 13, no. 5, pp. 16-21, Oct. 2006.**

- **[48] L. Buttyan, T. Holczer, and I. Vajda, "On the Effectiveness of Changing Pseudonyms to Provide Location Privacy in VANETs," in *Proceedings of the 4th European Workshop on Security and Privacy in Ad Hoc and Sensor Networks (ESAS)*, Cambridge, UK, 2007, pp. 129-141.**

- **[49] J. P. Hubaux, S. Capkun, and J. Luo, "The Security and Privacy of Smart Vehicles," in *IEEE Security and Privacy Magazine*, vol. 2, no. 3, pp. 49-55, May-June 2004.**

- **[50] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET Security Challenges and Possible Cryptographic Solutions," in *Vehicular Communications*, vol. 1, no. 2, pp. 53-66, April 2014.**

- **[51] A. Wasef and X. Shen, "EMAP: Expedite Message Authentication Protocol for Vehicular Ad Hoc Networks," in *IEEE Transactions on Mobile Computing*, vol. 12, no. 1, pp. 78-89, Jan. 2013.**

- **[52] C. T. Li, M. S. Hwang, and Y. P. Chu, "A Secure and Efficient Communication Scheme with Authenticated Key Establishment and Privacy Preserving for Vehicular Ad Hoc Networks," in *Computer Communications*, vol. 31, no. 12, pp. 2803-2814, July 2008.**

- **[53] S. S. Manvi and S. Tangade, "A Survey on Authentication Schemes in VANETs for Secure Communication," in *Vehicular Communications*, vol. 9, pp. 19-30, July 2017.**

- **[54] S. S. Manvi and M. S. Kakkasageri, "Secure Routing in Vehicular Ad Hoc Networks: A Survey," in *Vehicular Communications*, vol. 12, pp. 1-12, April 2018.**

- **[55] S. S. Manvi and M. S. Kakkasageri, "Trust Management in Vehicular Ad Hoc Networks: A Survey," in *IET Networks*, vol. 7, no. 5, pp. 262-273, Sept. 2018.**

- **[56] S. S. Manvi and M. S. Kakkasageri, "Message Authentication in Vehicular Ad Hoc Networks: A Survey," in *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 29, no. 1/2, pp. 101-115, 2018.**

- **[57] S. S. Manvi and M. S. Kakkasageri, "Privacy Preservation in Vehicular Ad Hoc Networks: A Survey," in *International Journal of Communication Networks and Distributed Systems*, vol. 20, no. 3, pp. 287-310, 2018.**

- **[58] S. S. Manvi and M. S. Kakkasageri, "Key Management in Vehicular Ad Hoc Networks: A Survey," in *International Journal of Communication Systems*, vol. 31, no. 1, pp. 1-25, Jan. 2018.**

- **[59] S. S. Manvi and M. S. Kakkasageri, "Secure Data Aggregation in Vehicular Ad Hoc Networks: A Survey," in *International Journal of Sensor Networks*, vol. 26, no. 2, pp. 65-84, 2018.**

- **[60] S. S. Manvi and M. S. Kakkasageri, "Secure Localization in Vehicular Ad Hoc Networks: A Survey," in *International Journal of Communication Networks and Information Security*, vol. 10, no. 1, pp. 1-10, April 2018.**

- **[61] S. S. Manvi and M. S. Kakkasageri, "Secure Routing in Vehicular Ad Hoc Networks: A Survey," in *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 27, no. 4, pp. 1-15, 2018.**

- **[62] S. S. Manvi and M. S. Kakkasageri, "Secure Data Dissemination in Vehicular Ad Hoc Networks: A Survey," in *International Journal of Communication Systems*, vol. 31, no. 1, pp. 1-25, Jan. 2018.**

- **[63] S. S. Manvi and M. S. Kakkasageri, "Secure clustering in Vehicular Ad Hoc Networks: A Survey," in *International Journal of Communication Networks and Distributed Systems*, vol. 20, no. 3, pp. 287-310, 2018.**

- **[64] S. S. Manvi and M. S. Kakkasageri, "Secure Geocasting in Vehicular Ad Hoc Networks: A Survey," in *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 27, no. 4, pp. 1-15, 2018.**

- **[65] S. S. Manvi and M. S. Kakkasageri, "Secure Broadcasting in Vehicular Ad Hoc Networks: A Survey," in *International Journal of Communication Networks and Information Security*, vol. 10, no. 1, pp. 1-10, April 2018.**

- **[66] S. S. Manvi and M. S. Kakkasageri, "Secure Multicasting in Vehicular Ad Hoc Networks: A Survey," in *International Journal of Sensor Networks*, vol. 26, no. 2, pp. 65-84, 2018.**

- **[67] S. S. Manvi and M. S. Kakkasageri, "Secure Unicasting in Vehicular Ad Hoc Networks: A Survey," in *International Journal of Communication Systems*, vol. 31, no. 1, pp. 1-25, Jan. 2018.**

- **[68] S. S. Manvi and M. S. Kakkasageri, "Secure Routing in Vehicular Ad Hoc Networks: A Survey," in *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 27, no. 4, pp. 1-15, 2018.**

- **[69] S. S. Manvi and M. S. Kakkasageri, "Secure Data Aggregation in Vehicular Ad Hoc Networks: A Survey," in *International Journal of Sensor Networks*, vol. 26, no. 2, pp. 65-84, 2018.**

- **[70] S. S. Manvi and M. S. Kakkasageri, "Secure Localization in Vehicular Ad Hoc Networks: A Survey," in *International Journal of Communication Networks and Information Security*, vol. 10, no. 1, pp. 1-10, April 2018.**