République Algérienne Démocratique et Populaire
Université Abderrahmane MIRA de Béjaia
Faculté des Sciences Exactes

Département de Recherche Opérationnelle

Mémoire Présenté pour L'obtention du Diplôme de Master
en Mathématiques Appliquées

Spécialité : Sciences de Données et Aide à la Décision

Traitement des données intrusives dans le contexte des réseaux VANETs

Présenté par :
BRAHMI Mokrane
DJABALLI Reda Nassim

Sous la direction de : Mme HAMZA Lamia

Défendu le 29/06/2024, devant le jury composé de :

M M. Soufit	Président de jury	UAMB - Bejaia.
M L. Asli	Examinateur	UAMB - Bejaia
M R. Djabri	Examinateur	UAMB - Bejaia.
M^{elle} Z. Chibane	Examinateur	UAMB - Bejaia.

Année Universitaire 2024 – 2025

Remerciments

On souhaite exprimer notre profonde gratitude à notre encadrante, ***Madame HAMZA Lamia****, pour sa bienveillance, sa rigueur scientifique et son accompagnement tout au long de ce travail. Sa disponibilité, ses conseils précieux et son exigence méthodologique ont constitué un appui fondamental dans la réalisation de ce mémoire.*

Nos remerciements vont également à l'ensemble des membres du jury pour l'intérêt porté à notre travail et pour les remarques constructives qui enrichissent cette recherche.

On remercie très sincèrement l'ensemble du corps enseignant du Master Sciences de Données et Aide à la Décision pour la qualité des enseignements, leur dévouement et leur engagement à transmettre des compétences solides, aussi bien théoriques que pratiques, qui nous seront précieuses dans la suite de notre parcours.

On adresse également nos remerciements à tous nos camarades, en particulier ceux de notre spécialité, pour leur entraide, leurs échanges enrichissants et leur esprit de collaboration, qui ont rendu cette expérience académique encore plus humaine et stimulante.

Dédicaces

Je dédie ce travail, fruit de plusieurs années d'efforts, d'apprentissage et de persévérance :
À mes parents,

Pour votre amour incommensurable, votre soutien indéfectible et vos sacrifices innombrables que les mots ne pourront jamais pleinement traduire.

Vous avez été mes piliers dans les moments d'incertitude, mes repères dans les tempêtes, mes sources d'inspiration dans chaque pas franchi.

Votre patience, votre foi en moi, et votre courage silencieux m'ont porté bien au-delà de ce que je croyais possible.

Chaque ligne de ce mémoire, chaque réussite, vous appartient autant qu'à moi. C'est à vous que je dois cette force intérieure, cette ténacité à poursuivre mes rêves, même dans les instants les plus sombres.

Je vous dédie ce travail avec une reconnaissance infinie, du plus profond de mon cœur.

À mes frères et sœurs, pour leur tendresse, leur écoute et leurs encouragements constants. Vous êtes ma force discrète.

À mes meilleurs amis : ***Abdallah, Abderraouf, Ahmad Ghilas, Samy.R , Samy.S, Helena et Meriem*** *et à toute ma famille en particulier ma cousine* ***Ikram*** *, pour leur présence réconfortante, leurs mots bienveillants et leurs encouragements dans les moments de doute.*

À mes camarades de spécialité et aux autres, pour les échanges d'idées, l'entraide mutuelle et les instants de complicité qui ont marqué ce parcours académique.

Ce mémoire vous est dédié avec tout mon cœur et ma reconnaissance.

Mokrane. B

Dédicaces

Je dédie ce travail, fruit de plusieurs années d'efforts, d'apprentissage et de persévérance :

À mes parents,

Pour votre amour inconditionnel, votre soutien indéfectible et vos innombrables sacrifices, que les mots ne suffiront jamais à exprimer. Vous avez été mes piliers dans les moments d'incertitude, mes repères dans les tempêtes, et ma source d'inspiration à chaque étape. Votre patience, votre foi en moi, et votre force silencieuse m'ont porté bien au-delà de ce que je pensais possible. Ce mémoire est autant le vôtre que le mien. Je vous l'offre avec une gratitude infinie.

À mon frère et ma sœur,

Pour votre affection, vos encouragements sincères et votre présence rassurante tout au long de ce parcours. Vous avez été des soutiens précieux dans les moments de doute.

À ma tante et son époux,

Pour leur générosité, leur attention constante et leurs conseils bienveillants qui ont grandement contribué à m'apaiser et à me motiver.

À mes amis proches et à toute ma famille,

Pour vos paroles réconfortantes, votre présence chaleureuse et vos encouragements, même à distance.

À mes camarades de spécialité et à tous ceux qui ont partagé ce chemin avec moi,

Pour l'entraide, les échanges constructifs et les instants de complicité.

Ce mémoire vous est dédié avec tout mon cœur et ma reconnaissance.

Nassim

Table des matières

Table des figures

Liste des tableaux

Liste d'abriviations et notations

3G	Third Generation (Mobile Telecommunications Technology)
4G	Fourth Generation (Mobile Telecommunications Technology)
5G	Fifth Generation (Mobile Telecommunications Technology)
AGA-POCG	Adaptive Genetic Algorithm–Proof of Concept Graph
ANN	Artificial Neural Network
ASKD	Adaptive Secure Key Distribution
AU	Application Unit
AES	Advanced Encryption Standard
CH	Cluster Head
CIDS	Collaborative Intrusion Detection System
CNN	Convolutional Neural Network
C-V2X	Cellular Vehicle-to-Everything
DL	Deep Learning
DoS	Denial of Service
DDoS	Distributed Denial of Service
DRL	Deep Reinforcement Learning
DSRC	Dedicated Short-Range Communications
EGBAD	Enhanced Graph-Based Anomaly Detection
FN	False Negative
FP	False Positive
GAN	Generative Adversarial Network
GPS	Global Positioning System
IA	Intelligence Artificielle
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IoT	Internet of Things
IoV	Internet of Vehicles
ITS	Intelligent Transportation Systems
ITS-G5	Intelligent Transport Systems–G5 (IEEE 802.11p-based standard)
KDD99	Knowledge Discovery in Databases 1999 Dataset
LSTM	Long Short-Term Memory
MD-GAN	Multi-Discriminator Generative Adversarial Network
ML	Machine Learning
MLP	Multi-Layer Perceptron
NS-2	Network Simulator 2
NSL-KDD	New Subset of KDD (Improved version of KDD99)
OBU	On-Board Unit
OSI	Open Systems Interconnection
PDR	Packet Delivery Ratio
PKI	Public Key Infrastructure
PPO	Proximal Policy Optimization
PPOTR	Privacy-Preserving Optimal Trust Routing
PQC	Post-Quantum Cryptography
QGAN	Quantum Generative Adversarial Network

QKD	Quantum Key Distribution
RNN	Recurrent Neural Network
RTA	Real-Time Analysis
RSU	Road Side Unit
SAC	Soft Actor-Critic
SQL	Structured Query Language
STI	Systèmes de Transport Intelligents
SVM	Support Vector Machine
TA	Trusted Authority
TP	True Positive
TPD	Trusted Platform Module
TN	True Negative
V2I	Vehicle-to-Infrastructure
V2P	Vehicle-to-Pedestrian
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
VANET	Vehicular Ad Hoc Network
VCG	Vickrey-Clarke-Groves
WAVE	Wireless Access in Vehicular Environments
WiFi	Wireless Fidelity

Introduction générale

À l'ère du numérique, où l'automatisation et la connectivité redéfinissent nos modes de vie, les villes intelligentes (Smart Cities) émergent comme un modèle de société intégrant les technologies avancées pour améliorer la qualité de vie des citoyens. Au cœur de cette transformation, les Systèmes de Transport Intelligents (STI) jouent un rôle crucial en s'appuyant sur les réseaux véhiculaires ad hoc (VANETs), qui permettent aux véhicules de communiquer entre eux (V2V), avec les infrastructures (V2I), et même avec les piétons (V2P). Ces échanges ont pour objectifs d'améliorer la sécurité routière, la fluidité du trafic et l'efficacité du transport urbain. Cependant, la nature dynamique, distribuée et sans fil des VANETs les rend particulièrement vulnérables à un large éventail d'attaques informatiques, comme les attaques de type Blackhole, les faux paquets, ou encore les déni de service (DoS). Ces menaces peuvent non seulement compromettre l'intégrité des données échangées, mais aussi mettre en péril la sécurité physique des usagers. Ainsi, détecter de manière fiable ces intrusions devient un défi critique, notamment face à des comportements malveillants sophistiqués et adaptatifs.

Pour répondre à ces enjeux, la recherche en cybersécurité explore de plus en plus les techniques d'intelligence artificielle, et en particulier le Machine Learning (ML) et le Deep Learning (DL). Ces approches ont montré leur capacité à identifier des schémas complexes, à apprendre de grandes quantités de données et à détecter les anomalies en temps réel. Toutefois, elles atteignent leurs limites dans certains cas, notamment lorsque les classes d'attaques sont très déséquilibrées, rendant difficile l'apprentissage efficace d'un système de détection.

Dans ce contexte, la théorie des jeux apparaît comme un outil théorique pertinent pour modéliser l'interaction stratégique entre un attaquant et un défenseur. Elle permet de représenter leurs décisions respectives comme des stratégies en compétition ou en adaptation. Associée à des approches d'apprentissage, cette modélisation ouvre la voie à des systèmes de détection plus dynamiques et plus résilients.

C'est dans cette perspective que s'inscrit ce travail, qui propose une approche hybride combinant la théorie des jeux pour la modélisation stratégique, les réseaux génératifs adversariaux (GANs) pour le rééquilibrage de données synthétiques, et un réseau de neurones MLP pour la classification du trafic réseau.
Ce mémoire est structuré en trois chapitres :

Chapitre 1 : "Réseaux VANETs : Fondements et Enjeux de Sécurité" : Ce premier chapitre pose les bases théoriques nécessaires à la compréhension de notre travail. Il présente les caractéristiques fondamentales des réseaux véhiculaires ad hoc (VANETs), leur rôle au sein des Systèmes de Transport Intelligents (STI), ainsi que les principaux enjeux

de sécurité auxquels ces réseaux sont confrontés. Les différentes menaces et attaques connues dans ce contexte sont décrites.

Chapitre 2 : ”État de l’art” : Ce chapitre dresse un panorama des recherches récentes dans les domaines du Machine Learning, du Deep Learning et de la théorie des jeux appliqués à la détection d’intrusions dans les VANETs. Nous y présentons les approches classiques et avancées, notamment les GANs, les QGANs et les MLP, tout en mettant en évidence leurs avantages et limites. Une discussion sur les contributions existantes permet de positionner notre travail dans le paysage scientifique actuel..

Chapitre 3 : ”Proposition” : Dans ce dernier chapitre, nous présentons notre contribution, qui repose sur une approche hybride de détection d’intrusion appliquée aux réseaux VANETs. Celle-ci s’appuie à la fois sur la modélisation stratégique par la théorie des jeux et sur l’utilisation de techniques d’intelligence artificielle avancées. Deux variantes sont explorées : une première basée sur un générateur conditionnel classique (cGAN) et une seconde exploitant les potentialités de l’informatique quantique à travers un Quantum GAN (QGAN). Pour chaque approche, nous détaillons l’architecture du système, les étapes d’implémentation, la génération de données synthétiques visant à corriger le déséquilibre des classes, ainsi que l’apprentissage supervisé effectué à l’aide d’un perceptron multicouche (MLP). Une évaluation expérimentale comparative est ensuite menée afin de valider l’efficacité des deux méthodes proposées.

Ce mémoire se conclut par une synthèse générale accompagnée de perspectives pour des travaux futurs.

1

Réseaux VANETs : Fondements et Enjeux de Sécurité

Introduction

Le chapitre 1 introduit les réseaux VANET (Vehicular Ad Hoc Networks) en tant que fondation des Systèmes de Transport Intelligents (STI). Ces réseaux permettent une communication directe entre les véhicules et les unités routières, améliorant ainsi la sécurité et l'efficacité du trafic. Cependant, leur architecture ouverte et mobile les expose à des risques croissants en matière de cybersécurité. Cette introduction met l'accent sur la nécessité de solutions intelligentes et adaptatives pour garantir l'intégrité et la fiabilité de ces systèmes connectés.

Sommaire

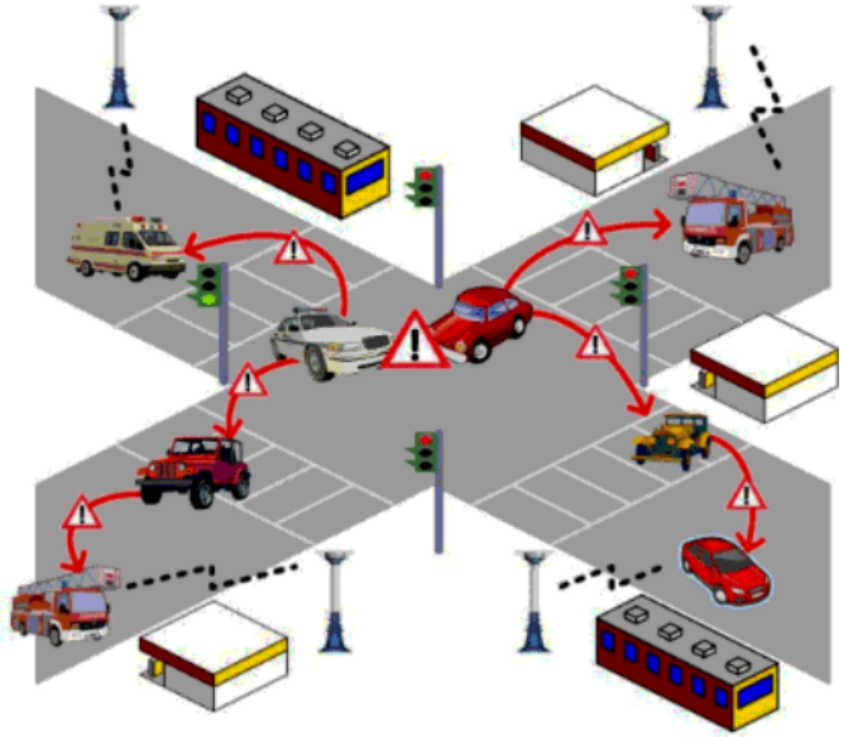


FIGURE 1.1 – Exemple d'un réseau VANET[1]

1.1 Définition des VANETs

Les Vehicular Ad Hoc Networks (VANETs) sont des réseaux sans fil spécifiques aux véhicules en mouvement, dans lesquels chaque véhicule agit comme un nœud mobile équipé pour communiquer à la fois avec d'autres véhicules (Vehicle to Vehicle, V2V) et avec des unités fixes en bordure de route (Vehicle to Infrastructure, V2I), tel que indiqué dans la figure 1.1. Ces réseaux constituent un pilier des Systèmes de Transport Intelligents (STI), visant à améliorer la sécurité routière, la gestion du trafic et le confort des passagers. Ce qui distingue les VANETs des réseaux sans fil classiques comme le Wi Fi est leur environnement extrêmement dynamique : la mobilité rapide des véhicules entraîne des changements fréquents de topologie, rendant la connectivité instable et affectant la latence ainsi que la qualité de service[2].

1.2 Composants principaux de l'architecture des VANETs

L'architecture des réseaux VANETs repose sur une organisation modulaire intégrant à la fois des composants embarqués dans les véhicules et des entités fixes au sein de l'infrastructure routière. Ces éléments assurent collectivement la communication, la sécurité, le traitement des données et la mise en œuvre des services intelligents dans un environnement caractérisé par une forte mobilité, une connectivité intermittente et des exigences de temps réel élevées.

1.2.1 Composants embarqués

Unité embarquée (OBU – On-Board Unit) L'unité embarquée est installée dans chaque véhicule. Elle intègre des dispositifs de communication sans fil (comme DSRC ou IEEE 802.11p), un processeur, de la mémoire, et parfois un module sécurisé (TPD). Sa fonction principale est d'émettre et de recevoir des messages vers d'autres véhicules (communication V2V) ou vers les infrastructures fixes (V2I), notamment pour transmettre des alertes de sécurité, des coordonnées GPS, des informations de vitesse ou tout autre événement critique. L'OBU peut également faire office de relais pour d'autres véhicules se trouvant hors de portée directe[3].

Unité d'application (AU – Application Unit) L'AU est un composant logiciel ou matériel intégré au véhicule, chargé d'exécuter les applications utilisateurs, telles que la navigation, les alertes de circulation, les services de divertissement ou de paiement. Elle est reliée à l'OBU, soit par un lien filaire soit via une interface sans fil. Dans certaines configurations, l'AU et l'OBU peuvent être fusionnées en une seule unité fonctionnelle. Elle rend les services connectés accessibles au conducteur et aux passagers[4].

1.2.2 Composants d'infrastructure

Unités en bord de route (RSU – Road Side Unit) Les RSUs sont des stations fixes déployées à des emplacements stratégiques tels que les carrefours, les axes routiers majeurs ou les parkings. Elles permettent la communication entre les OBUs et l'infrastructure réseau. Elles assurent la réception, le traitement et la transmission des messages vers d'autres RSUs ou des serveurs distants. Les RSUs jouent également un rôle crucial dans la gestion des certificats d'authentification et la diffusion de listes de révocation, contribuant ainsi à renforcer la sécurité globale du réseau VANET[5].

Autorité de confiance (TA – Trusted Authority) L'autorité de confiance est une entité centrale chargée de la gestion des identités numériques des véhicules et des unités RSU. Elle délivre et révoque les certificats d'authentification, orchestre les politiques de sécurité et garantit l'intégrité du réseau. Fonctionnant généralement selon un modèle hiérarchique avec des autorités régionales (RTA), la TA est responsable de l'exclusion des entités malveillantes du réseau et assure la traçabilité des comportements suspects[6].

1.2.3 Modèle en couches de l'architecture VANET

Les réseaux VANET sont structurés selon un modèle en couches inspiré de l'OSI, mais optimisé pour les Systèmes de Transport Intelligents (STI). Les couches physique et liaison utilisent principalement le protocole IEEE 802.11p / ITS-G5 (WAVE), offrant une communication fiable à faible latence dans la bande des 5,9 GHz, adaptée à la mobilité élevée des véhicules. Les couches réseau et transport exploitent des protocoles tels que GeoNetworking, conçus pour le routage géographique dynamique. La couche application prend en charge les services STI, comme la signalisation d'alerte routière et la gestion adaptative du trafic. Cette architecture en couches permet de répondre efficacement aux exigences de latence faible, de fiabilité et de sécurité dans un environnement très dynamique[7].

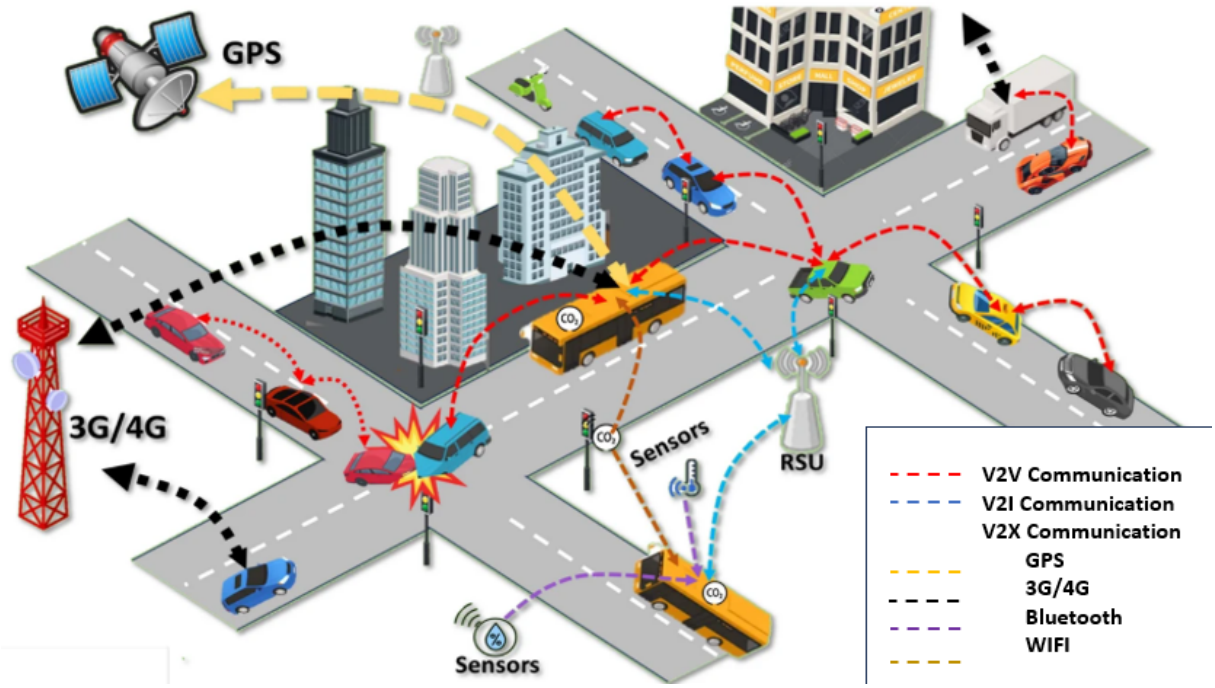


FIGURE 1.2 – Types de communication dans les VANETs[8]

1.3 Types de Communication dans les VANETs

Les réseaux VANETs reposent sur plusieurs modes de communication sans fil, essentiels pour permettre l'échange de données entre véhicules et leur environnement. Ces échanges assurent la sécurité, la fluidité du trafic et l'accès à des services connectés. Trois types principaux de communication se distinguent selon les interlocuteurs : V2V (Vehicle-to-Vehicle), V2I (Vehicle-to-Infrastructure) et V2X (Vehicle-to-Everything), chacun remplissant des missions spécifiques au sein de l'écosystème véhiculaire.

1.3.1 Communication V2V (Vehicle-to-Vehicle)

La communication V2V permet aux véhicules d'échanger des informations en temps réel entre eux, sans passer par une infrastructure fixe. Grâce à cette communication directe, les véhicules peuvent détecter et anticiper les risques afin d'améliorer la sécurité et la fluidité du trafic[9].

— **Exemple** L'une des applications majeures du V2V est le système d'alerte de collision. Lorsqu'un véhicule freine brusquement sur l'autoroute, il peut envoyer un signal aux véhicules qui le suivent pour leur permettre d'adapter leur vitesse et ainsi éviter un accident. Cette technologie est particulièrement utile pour prévenir les carambolages sur routes rapides.

FIGURE 1.3 – Exemple de communication V2V[10]

1.3.2 Communication V2I (Vehicle-to-Infrastructure)

La communication V2I établit un lien entre les véhicules et les infrastructures routières fixes, telles que les feux de circulation, les panneaux de signalisation intelligents, les unités de bord de route (RSU) et les centres de gestion du trafic. L'objectif principal est d'améliorer la gestion du trafic et la sécurité routière en fournissant aux véhicules des informations en temps réel sur l'état des routes et les conditions de circulation[11].

— **Exemple** le contrôle adaptatif des feux de signalisation. Dans une ville intelligente, les feux de circulation peuvent communiquer avec les véhicules en approche et ajuster leur durée en fonction du flux de trafic détecté. Cela permet de réduire la congestion et d'optimiser la circulation urbaine.

FIGURE 1.4 – Exemple de communication V2I[10]

1.3.3 Communication V2X (Vehicle-to-Everything)

Le V2X est une communication plus avancée qui englobe tous les types d'interactions possibles entre un véhicule et son environnement. Il regroupe le V2V, le V2I, mais aussi la communication avec d'autres entités comme les piétons (V2P - Vehicle-to-Pedestrian), les deux-roues, ou encore les serveurs cloud chargés de traiter les informations collectées[12].

— **Exemple** le système d'alerte de passage piéton intelligent. Lorsqu'un piéton traverse une rue dans une zone à visibilité réduite, son téléphone portable peut émettre un signal V2P, qui est reçu par un véhicule en approche. Ce dernier peut alors ralentir automatiquement ou alerter le conducteur via un signal sonore.

1.3.4 Technologies de communication sous-jacentes

Les VANETs s'appuient principalement sur deux technologies radio :

— **IEEE 802.11p / DSRC (ITS-G5)** pour les communications V2V et V2I à courte portée. Adapté aux environnements urbains, il offre une latence réduite essentielle aux applications critiques pour la sécurité.

— **C-V2X (LTE-V / 5G-V2X)** pour une communication à plus longue portée et des performances réseau améliorées, notamment grâce aux capacités d'edge computing intégrées dans l'architecture cellulaire[13].

L'utilisation de ces technologies en combinaison permet de couvrir différents besoins selon la portée, la mobilité et les objectifs applicatifs.

1.4 Applications des VANETs

Les réseaux VANETs permettent une large gamme d'applications visant à améliorer la sécurité routière, la gestion du trafic, le confort des usagers et les services commerciaux.

1.4.1 Applications de sécurité routière

L'une des principales motivations des VANETs est l'amélioration de la sécurité routière grâce à une communication instantanée entre les véhicules et l'infrastructure. Ces applications permettent de réduire le nombre d'accidents en anticipant les risques et en fournissant des alertes en temps réel aux conducteurs. L'avertissement de collision est une des applications les plus critiques. Lorsqu'un véhicule détecte une collision imminente, il peut envoyer un message d'alerte aux autres véhicules à proximité, leur permettant de réagir à temps pour éviter un accident. Ce système est particulièrement utile sur les autoroutes et aux intersections où les risques de collisions sont élevés. L'avertissement d'urgence informe les conducteurs de la présence de véhicules prioritaires, tels que les ambulances, pompiers ou voitures de police, afin qu'ils puissent libérer la voie rapidement. Cette fonctionnalité est essentielle pour réduire le temps d'intervention des secours et améliorer la gestion des urgences. Les systèmes d'alerte aux intersections visent à réduire les accidents en informant les conducteurs des véhicules approchant d'une intersection. Grâce aux feux de circulation intelligents et aux capteurs, ces systèmes préviennent les collisions en ajustant les priorités et en diffusant des recommandations de trajectoire. Enfin, les alertes de conditions routières dangereuses permettent aux véhicules d'échanger des informations sur l'état de la route. Par exemple, un véhicule traversant une zone verglacée ou un brouillard dense peut partager ces informations avec les autres conducteurs, leur permettant d'adapter leur vitesse et leur conduite en conséquence[14].

1.4.2 Applications d'efficacité et de gestion du trafic

Les VANETs permettent également d'optimiser la gestion du trafic urbain et interurbain en facilitant l'échange d'informations sur la circulation. Ces applications aident à réduire les embouteillages, optimiser la consommation de carburant et améliorer la fluidité du trafic. La gestion du trafic aux intersections repose sur l'utilisation de feux de circulation intelligents capables de s'adapter à la densité de véhicules en temps réel. En ajustant les temps de feu vert et rouge en fonction du trafic, ces systèmes permettent d'éviter les congestions inutiles et d'améliorer la fluidité du réseau routier. La régulation de la vitesse adaptative est un autre mécanisme qui vise à harmoniser les flux de circulation. En fonction des conditions routières et des véhicules environnants, les systèmes VANETs peuvent recommander une vitesse optimale aux conducteurs afin de réduire le nombre d'arrêts et d'améliorer la consommation énergétique[14].

1.4.3 Applications de confort et de divertissement

Les applications de confort dans les VANETs sont conçues pour améliorer l'expérience des conducteurs et des passagers en offrant une connectivité avancée et des services numériques embarqués. L'accès à Internet est une des fonctionnalités les plus appréciées. Grâce aux réseaux 5G et aux hotspots Wi-Fi, les véhicules peuvent offrir une connexion stable aux passagers, leur permettant de naviguer sur le web, d'accéder aux réseaux sociaux ou de travailler en déplacement.

Les services de localisation sont également très utilisés. Les systèmes VANETs peuvent recommander les stations-service, restaurants ou hôtels les plus proches, facilitant ainsi la planification des trajets et des arrêts. Le streaming multimédia embarqué est une autre application importante. Les passagers peuvent regarder des films, écouter de la musique ou jouer à des jeux en ligne directement depuis le système de divertissement du véhicule. Cette fonctionnalité est particulièrement utile pour les longs trajets et améliore l'expérience des passagers. Enfin, l'échange d'informations entre conducteurs permet d'améliorer la communication sur la route. Les véhicules peuvent partager des alertes sur le trafic, les conditions météorologiques ou les contrôles de police, offrant ainsi une expérience de conduite plus fluide et collaborative[15].

1.4.4 Applications commerciales

Les VANETs offrent également des opportunités commerciales et publicitaires en permettant aux entreprises de proposer des services personnalisés aux conducteurs et passagers. La publicité contextuelle est l'une des applications les plus développées. En analysant la position et les préférences des utilisateurs, les systèmes VANETs peuvent afficher des publicités ciblées sur l'écran de bord du véhicule, proposant par exemple des promotions dans un restaurant à proximité. Le paiement automatique est une autre avancée majeure. Grâce aux technologies de communication sans fil, les conducteurs peuvent payer automatiquement aux péages, stations-service et parkings, sans avoir besoin d'effectuer un paiement manuel. Cette solution accélère les transactions et améliore l'expérience utilisateur[16].

1.5 Enjeux et défis des réseaux VANETs

Malgré leur potentiel considérable dans le cadre des systèmes de transport intelligents, les réseaux VANETs sont confrontés à plusieurs défis techniques, sécuritaires et opérationnels qui freinent leur adoption à grande échelle. Ces obstacles doivent être maîtrisés pour garantir une communication fiable, sécurisée et universellement interopérable.

1.5.1 Contraintes techniques et communicationnelles

L'environnement des VANETs est marqué par une forte mobilité des véhicules, ce qui engendre des variations rapides de la topologie du réseau et compromet la stabilité des connexions. De plus, la latence faible est une exigence cruciale, notamment pour les applications critiques comme les alertes de collision ou les feux de signalisation adaptatifs. À cela s'ajoute le problème de l'interopérabilité, qui suppose une parfaite compatibilité entre équipements issus de différents fabricants pour assurer une communication fluide et homogène sur l'ensemble du réseau[17].

1.5.2 Sécurité et confidentialité

La sécurité représente un enjeu central dans les VANETs, en raison de leur exposition à une variété d'attaques potentielles (Sybil, DoS, DDoS, interception de données, etc.). Ces menaces peuvent gravement perturber la transmission d'informations critiques. Il est également nécessaire d'assurer une authentification robuste des véhicules tout en préservant l'anonymat

et la vie privée des conducteurs. Cela exige des mécanismes cryptographiques à la fois efficaces et légers, capables de fonctionner dans un environnement à connectivité intermittente et à ressources limitées[18].

1.5.3 Infrastructure et coûts de déploiement

Le déploiement à grande échelle des VANETs repose sur une infrastructure dense en unités de bord de route (RSU), ce qui représente un investissement conséquent en termes de matériel, d'installation et de maintenance. Par ailleurs, la scalabilité constitue un autre défi majeur : plus le nombre de véhicules connectés augmente, plus la gestion du réseau devient complexe, nécessitant des solutions dynamiques et évolutives pour équilibrer charge et ressources[19].

1.5.4 Perspectives d'évolution

Les perspectives d'évolution des VANETs sont encouragées par plusieurs avancées technologiques. L'intégration des réseaux 5G et des architectures V2X promet une amélioration significative de la bande passante, de la fiabilité et de la couverture. Par ailleurs, l'usage de l'intelligence artificielle et du machine learning ouvre la voie à des systèmes auto-adaptatifs pour la gestion du trafic, la détection des anomalies et la cybersécurité. Le recours à la blockchain est également envisagé pour garantir l'intégrité des échanges et la résilience des communications. Enfin, la standardisation internationale et l'optimisation énergétique, notamment en lien avec l'essor des véhicules électriques, constituent des leviers essentiels pour une adoption durable et cohérente à l'échelle mondiale[20][21].

1.6 Sécurité dans les réseaux VANETs

La sécurité dans les réseaux VANETs désigne l'ensemble des mesures visant à protéger les communications et les données échangées entre les véhicules et les infrastructures. Elle est essentielle pour assurer l'intégrité, la confidentialité et l'authenticité des informations transmises. Dans un environnement où les véhicules échangent en temps réel des données critiques (alertes d'accidents, conditions de circulation, etc.), toute faille de sécurité peut avoir des conséquences graves sur la sécurité routière et la vie privée des usagers[22].

1.6.1 Types d'attaques dans les réseaux VANETs

Les attaques dans les réseaux VANETs peuvent être classifiées en quatre catégories principales : passives, actives, internes et externes. Chaque type d'attaque présente des caractéristiques spécifiques et des exemples concrets qui illustrent leur fonctionnement[23].

1.6.1.1 Attaques passives

Les attaques passives consistent en une interception ou une analyse du trafic sans modification des données. Elles sont souvent difficiles à détecter car elles n'altèrent pas directement le réseau, ces attaques menacent principalement la confidentialité des données échangées. Nous citons à titre d'exemple :

Écoute clandestine (Eavesdropping) : L'attaquant capture les communications entre les véhicules ou entre un véhicule et une infrastructure pour collecter des informations sensibles, telles que des identifiants ou des positions GPS.

Analyse de trafic : En observant les motifs de communication, l'attaquant peut déduire des informations sur les habitudes de conduite ou les itinéraires fréquemment empruntés par un véhicule.

1.6.1.2 Attaques actives

Les attaques actives impliquent une manipulation ou une altération des communications. Elles sont plus destructrices que les attaques passives car elles perturbent directement le fonctionnement du réseau.Nous citons à titre d'exemple :

l'usurpation d'identité (Spoofing) : L'attaquant se fait passer pour un véhicule légitime afin de diffuser des messages malveillants ou trompeurs, tels que de fausses alertes d'accidents.

Injection de faux messages : Des messages incorrects sont insérés dans le réseau pour induire en erreur les autres véhicules, par exemple en signalant un embouteillage fictif.

Attaques DoS/DDoS (Denial of Service/Distributed Denial of Service) : L'attaquant submerge le réseau ou une infrastructure spécifique (comme une RSU) avec un grand volume de requêtes, rendant les services indisponibles pour les utilisateurs légitimes.

Ces attaques peuvent causer des accidents graves ou des perturbations majeures dans le trafic.

1.6.1.3 Attaques internes

Les attaques internes sont menées par des nœuds légitimes compromis, c'est-à-dire des véhicules ou des infrastructures qui ont été piratés ou infectés par un logiciel malveillant.Nous citons à titre d'exemple :

Compromission d'un véhicule : Un véhicule infecté peut diffuser des messages malveillants ou participer à des attaques coordonnées contre le réseau.

Attaque Sybil : Un seul véhicule malveillant crée plusieurs identités fictives pour manipuler le réseau, par exemple en simulant une congestion artificielle.

Ces attaques sont particulièrement dangereuses car elles exploitent la confiance accordée aux nœuds

1.6.1.4 Attaques externes

Les attaques externes proviennent d'entités extérieures au réseau VANET, telles que des pirates informatiques ou des dispositifs malveillants situés en dehors du réseau.Nous citons à titre d'exemple :

Brouillage (Jamming) : L'attaquant utilise un dispositif pour perturber les signaux de communication, rendant impossible l'échange de données entre les véhicules.

Attaque de falsification GPS : L'attaquant manipule les signaux GPS pour fournir des informations de position erronées aux véhicules.

Ces attaques exploitent les vulnérabilités des technologies sans fil utilisées dans les VANETs.

1.6.2 Mécanismes de sécurité pour les VANETs

Pour contrer ces menaces, plusieurs mécanismes de sécurité ont été développés, chacun répondant à des besoins spécifiques[24] :

- **Authentification et cryptographie :** Les certificats numériques permettent de valider l'identité des véhicules et garantissent que les messages échangés proviennent de sources fiables. Par exemple, le standard IEEE 1609.2 propose des mécanismes de signature numérique pour sécuriser les communications.
- **Détection d'intrusion (IDS) :** Les systèmes IDS basés sur le machine learning analysent le comportement du réseau pour identifier les anomalies, comme une augmentation soudaine du trafic ou des messages incohérents. Ces systèmes peuvent être entraînés pour détecter des attaques spécifiques, telles que les attaques DDoS ou Sybil.
- **Confidentialité des communications :** Le chiffrement des échanges empêche l'interception des données sensibles. Par exemple, les algorithmes AES (Advanced Encryption Standard) sont couramment utilisés pour protéger les messages V2V et V2I.
- **Protocoles sécurisés :** Des protocoles robustes comme IEEE 1609.2 et PKI (Public Key Infrastructure) assurent une gestion efficace des clés cryptographiques et des certificats numériques.

1.6.3 Défis et limites des solutions de sécurité existantes

Malgré les avancées réalisées, plusieurs défis persistent dans la sécurisation des réseaux VANETs[25] :

- **Latence et ressources limitées :** Les véhicules disposent souvent de ressources matérielles limitées (processeur, mémoire), ce qui rend difficile l'implémentation de mécanismes de sécurité complexes sans affecter les performances du réseau.
- **Anonymat vs traçabilité :** Il est essentiel de protéger la vie privée des conducteurs tout en permettant l'identification des véhicules malveillants. Trouver un équilibre entre ces deux exigences reste un défi majeur.
- **Scalabilité :** Avec l'augmentation du nombre de véhicules connectés, les mécanismes de sécurité doivent être capables de gérer efficacement des volumes croissants de données et d'utilisateurs.

1.6.4 Approches émergentes pour renforcer la sécurité des VANETs

De nouvelles approches innovantes émergent pour répondre aux défis de sécurité des réseaux VANETs :

- **Utilisation de la blockchain :** La blockchain peut être utilisée pour sécuriser les transactions et les échanges de données, offrant une solution décentralisée et transparente pour la gestion des certificats et des messages[26].
- **Intelligence artificielle et machine learning :** Ces technologies permettent une détection proactive des menaces et une adaptation en temps réel aux nouvelles attaques. Par exemple, des algorithmes d'apprentissage supervisé peuvent être utilisés pour classifier les comportements anormaux dans le réseau[27] .
- **Sécurité adaptative :** Des mécanismes dynamiques capables d'évoluer en fonction des menaces et du contexte du réseau sont développés. Par exemple, des systèmes basés sur

la théorie des jeux peuvent optimiser les stratégies de défense en fonction des actions des attaquants[32].

— **Quantum Key Distribution (QKD) :** Cette technologie émergente utilise les principes de la physique quantique pour distribuer des clés cryptographiques de manière sécurisée, offrant une protection infaillible contre les attaques futures[28].

Les approches classiques de sécurité dans les réseaux VANETs, bien qu'efficaces dans certains scénarios, montrent leurs limites face à des menaces sophistiquées et à la complexité croissante des environnements connectés. De ce fait, de nouvelles approches dites émergentes combinant intelligence artificielle, technologies quantiques ou distribuées, sont aujourd'hui explorées pour anticiper, détecter et répondre de manière plus dynamique aux attaques.

Critère	**Approches traditionnelles**	**Approches émergentes**
Méthode principale	Filtrage, cryptographie, PKI	IA, Deep Learning, Blockchain, Théorie des jeux, QKD
Réactivité	Réactive (basée sur des règles prédéfinies)	Proactive (apprentissage, détection comportementale)
Adaptabilité	Faible (règles fixes, non contextuelles)	Élevée (capacité à évoluer face à de nouveaux types d'attaques)
Type d'analyse	Signature ou heuristique	Comportementale, prédiction, génération synthétique
Exemples d'outils	IDS basé sur règles, AES, PKI	GAN, QKD, IDS par Deep Learning, Réseaux bayésiens
Protection contre attaques avancées	Limitée (DoS, spoofing simples)	Élevée (Sybil, internes, DDoS complexes)
Interopérabilité	Moyenne	Intégrée avec smart cities, IoT, 5G

Table 1.1 – Comparaison entre approches traditionnelles et émergentes dans les VANETs

Conclusion

La conclusion du chapitre réaffirme la nature critique des défis sécuritaires dans les VANETs. Elle souligne que, face à la sophistication croissante des cybermenaces, les approches classiques doivent être renforcées par des techniques avancées comme le Machine Learning, le Deep Learning et, plus récemment, l'informatique quantique. Cette transition vers des systèmes intelligents ouvre de nouvelles perspectives pour une cybersécurité proactive et efficace dans les environnements de mobilité intelligente.

2
État de l'Art

Introduction

Ce chapitre présente un état de l'art des approches d'intelligence artificielle appliquées à la cybersécurité des réseaux VANETs. Il met en lumière l'apport du Machine Learning et du Deep Learning dans la détection d'intrusions, en détaillant leurs principes, algorithmes courants, ainsi que leurs avantages et limites dans un environnement dynamique et distribué. Nous abordons également le rôle croissant de la théorie des jeux, qui permet de modéliser les interactions stratégiques entre attaquant et défenseur. Cette revue fournit ainsi le cadre conceptuel nécessaire à la compréhension de notre méthodologie développée dans le chapitre suivant.

Sommaire

2.1 Théorie des jeux appliquée dans les VANETs

La théorie des jeux est un domaine des mathématiques et de l'économie qui étudie les interactions stratégiques entre des agents rationnels appelés joueurs. Chaque joueur choisit une stratégie pour maximiser son propre gain ou minimiser ses pertes, en tenant compte du comportement potentiel des autres joueurs.[29]

Les jeux peuvent être classés selon plusieurs dimensions : à somme nulle ou non, coopératifs ou non coopératifs, statiques ou dynamiques. Dans les jeux à somme nulle, le gain d'un joueur est exactement la perte de l'autre, tandis que dans les jeux à somme non nulle, les deux joueurs peuvent être simultanément gagnants ou perdants.

Dans un contexte de cybersécurité comme celui des réseaux VANETs, la théorie des jeux permet de modéliser les interactions entre un attaquant et un défenseur comme un jeu à deux joueurs. Chaque partie agit de manière non coopérative, adaptant ses choix pour tirer avantage des failles du système (pour l'attaquant) ou pour maximiser la protection du réseau (pour le défenseur).[32]

Cette approche offre un cadre analytique puissant pour anticiper les actions adverses, évaluer les conséquences des décisions de défense, et concevoir des systèmes de détection d'intrusion plus robustes.

Un concept central de la théorie des jeux est celui de l'équilibre de Nash. Il correspond à une situation où aucun joueur n'a intérêt à changer sa stratégie de manière unilatérale. Dans un cadre de cybersécurité, cet équilibre représente l'état où les deux parties – l'attaquant et le défenseur – ont optimisé leurs tactiques respectives, rendant toute tentative d'adaptation marginalement inefficace.

2.1.1 Types de jeux utilisés dans la modélisation des attaques en cybersécurité

La théorie des jeux propose plusieurs types de modèles pour analyser les comportements stratégiques entre entités opposées, comme les attaquants et les défenseurs dans un système informatique. Selon le niveau d'information, la temporalité des décisions et la nature des gains, différents types de jeux peuvent être utilisés pour modéliser des scénarios de cybersécurité. Dans le contexte des réseaux VANETs, ces classifications permettent d'adapter la stratégie de défense à la nature évolutive des attaques.

Les jeux à somme nulle représentent une situation purement conflictuelle dans laquelle le gain de l'un correspond exactement à la perte de l'autre. En cybersécurité, ce type de jeu peut modéliser des scénarios où l'intérêt d'un attaquant s'oppose strictement à celui du défenseur. Cependant, les jeux à somme non nulle sont plus représentatifs de la réalité : par exemple, un faux positif peut nuire au défenseur sans pour autant améliorer significativement la situation de l'attaquant. Ces jeux permettent de prendre en compte des interactions aux conséquences asymétriques. Par ailleurs, les jeux statiques, où les joueurs choisissent leurs stratégies simultanément sans connaître les choix adverses, conviennent aux attaques ponctuelles ou aux décisions discrètes. À l'inverse, les jeux dynamiques introduisent une dimension temporelle : les décisions s'enchaînent, et chaque joueur ajuste sa stratégie selon l'historique des interactions, ce qui reflète mieux la co-adaptation entre un attaquant et un système de défense intelligent. Enfin, dans un jeu complet, les deux parties disposent d'une connaissance parfaite de l'état du système et des stratégies disponibles, hypothèse souvent irréaliste dans des environnements complexes comme les VANETs. C'est pourquoi les jeux partiellement observables sont

privilégiés : ils modélisent l'incertitude du défenseur, qui ne peut pas toujours détecter clairement l'intention de l'attaquant ou anticiper ses mouvements, notamment dans les systèmes de détection d'anomalies.

2.1.2 Réseaux Antagonistes Génératifs (GANs)

Les GANs (Generative Adversarial Networks) sont une classe de modèles de Deep Learning introduits par Ian Goodfellow en 2014. Leur principe repose sur un apprentissage compétitif entre deux réseaux de neurones : un générateur et un discriminateur.
Le générateur a pour rôle de produire des données artificielles qui imitent les données réelles. En parallèle, le discriminateur tente de distinguer les données synthétiques des données authentiques. Ces deux réseaux s'affrontent dans un jeu à somme nulle, où chacun cherche à optimiser sa fonction objectif : le générateur tente de « tromper » le discriminateur, tandis que celui-ci s'efforce de ne pas se faire berner.
Cette architecture de type minimax s'apparente naturellement à une modélisation par la théorie des jeux. Le GAN atteint son objectif lorsque le générateur produit des échantillons suffisamment réalistes pour que le discriminateur ne puisse plus faire la distinction – un point d'équilibre analogue à un équilibre de Nash.
Afin d'illustrer le fonctionnement interactif entre les deux composants principaux d'un GAN, la figure suivante 2.1 met en évidence le processus d'apprentissage adversarial. On y voit comment le générateur propose des données synthétiques à partir d'une source d'entraînement, tandis que le discriminateur les évalue en les comparant à des exemples réels issus d'une cible d'entraînement.Dans ce mécanisme compétitif, seul le discriminateur sait si un exemple est réel ou généré. Il fournit alors une rétroaction (feedback) sous forme d'un score d'évaluation. Cette évaluation détermine ensuite quelles parties du réseau sont mises à jour. Le symbole "v" dans la figure indique que le discriminateur reçoit le bon label (réel ou généré) et ajuste ses paramètres en conséquence. En revanche, le symbole "x" montre que le générateur ne reçoit pas directement cette vérité mais s'améliore indirectement, en cherchant à maximiser la confusion du discriminateur. Ce jeu d'interactions permet aux deux réseaux de s'améliorer mutuellement : le générateur affine sa capacité à produire des données réalistes, tandis que le discriminateur renforce sa faculté de différenciation. L'objectif ultime est d'atteindre un équilibre, où les données synthétiques deviennent indiscernables des données réelles.

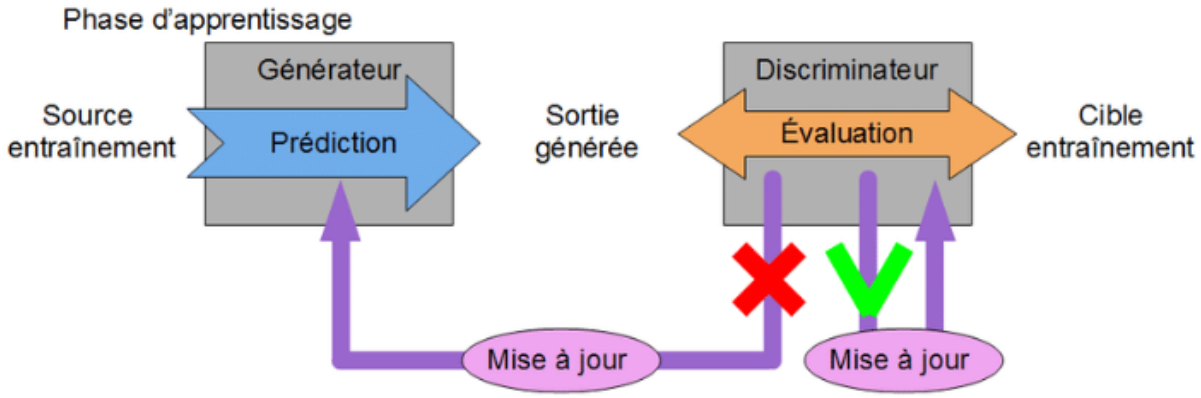


FIGURE 2.1 – Figure explicative des GANs[31]

2.2 Machine Learning dans les réseaux VANETs

Machine Learning (ML), ou apprentissage automatique, désigne un ensemble de techniques permettant à un système informatique d'apprendre à partir de données, sans être explicitement programmé. L'objectif est de reconnaître des modèles et de faire des prédictions ou des décisions en se basant sur des données d'entrée. Dans le cadre des réseaux VANETs, le ML est principalement utilisé pour détecter des comportements anormaux, classer le trafic réseau (normal vs malicieux) et anticiper des menaces avant qu'elles ne compromettent la sécurité du réseau.[30]

Le ML repose sur différents paradigmes d'apprentissage, chacun adapté à un contexte spécifique de traitement des données. Dans les réseaux VANETs, la sélection du type d'apprentissage dépend du degré de connaissance préalable sur les comportements malveillants, de la structure des données disponibles, et des objectifs de détection. On distingue principalement trois grandes catégories(Apprentissage supervisé, Apprentissage non supervisé, Apprentissage par renforcement).L'apprentissage supervisé repose sur un jeu de données annoté, c'est-à-dire contenant des exemples d'entrée associés à des étiquettes de sortie connues. L'algorithme apprend à généraliser ces correspondances pour traiter de nouveaux cas. Dans les VANETs, on distingue des paquets normaux de paquets malveillants (blackhole, faux paquet), en s'appuyant sur des données déjà étiquetées.L'apprentissage non supervisé l'algorithme n'a pas d'étiquettes en entrée. Il doit découvrir des structures sous-jacentes, comme des regroupements ou des anomalies. Dans les VANETs, cela consiste à repérer des comportements inhabituels dans le trafic réseau sans savoir à l'avance s'ils sont malveillants. Quant à l'apprentissage par renforcement,il est fondé sur l'idée de récompense ; un agent apprend à interagir avec un environnement pour maximiser un gain au fil du temps. Dans le context des VANETs, adapter dynamiquement les règles d'un IDS pour répondre à des attaques changeantes dans un réseau VANET.

L'adoption du Machine Learning dans les systèmes VANETs présente des atouts majeurs, mais également des limitations qui peuvent compromettre son efficacité s'ils ne sont pas bien gérés. Il est donc essentiel d'en évaluer les points forts et les contraintes pour concevoir une architecture adaptée et fiable. Le tableau 2.1 présente ses avantages et ses limites.

Avantages	Limites
Détection automatisée d'attaques en temps réel	Performance fortement dépendante de la qualité des données
Adaptabilité à différents types de comportements malveillants	Problème de déséquilibre de classes (ex. : très peu d'exemples d'attaques)
Possibilité de détection précoce (apprentissage sur historiques)	Difficulté à interpréter les décisions des modèles complexes (boîtes noires)
Intégration facile dans des systèmes embarqués ou distribués	Nécessité d'un entraînement et d'une validation rigoureuses

TABLE 2.1 – Avantages et limites du Machine Learning

2.3 Deep Learning dans les réseaux VANETs

Le Deep Learning est une branche du Machine Learning qui repose sur l'utilisation de réseaux de neurones profonds, composés de multiples couches de traitement. Ces modèles ont la capacité d'apprendre automatiquement des représentations complexes à partir de grandes quantités de données, ce qui les rend particulièrement adaptés à des problèmes comme la détection d'anomalies, la reconnaissance de schémas ou encore la génération de données. Dans le contexte des réseaux VANETs, le Deep Learning permet d'analyser des données multidimensionnelles (vitesse, signal, latence, comportement réseau,etc.) pour détecter des comportements malicieux, même lorsqu'ils sont très subtils ou déguisés.[30]

Le DL est de plus en plus utilisé dans le domaine de la sécurité des réseaux VANETs pour sa capacité à détecter des attaques complexes, même dans des contextes dynamiques et non linéaires. Contrairement aux approches classiques fondées sur des règles ou des signatures, les architectures neuronales profondes permettent une détection plus proactive et contextuelle. Parmi les contributions majeures dans le domaine de la détection d'intrusions dans les réseaux, on retrouve l'utilisation des perceptrons multicouches (MLP) pour la classification binaire ou multiclasses du trafic réseau, l'application des réseaux de neurones convolutifs (CNN) pour extraire des schémas spatiaux à partir de représentations matricielles du trafic, ainsi que l'intégration de réseaux récurrents tels que les RNN ou les LSTM pour l'analyse des séquences temporelles des paquets. Par ailleurs, les réseaux antagonistes génératifs (GANs) ont été employés pour simuler des attaques et générer des jeux de données équilibrés, permettant d'améliorer la robustesse des classifieurs. Enfin, des approches plus récentes s'orientent vers des modèles hybrides ou même quantiques, dans le but d'accroître la diversité, la résilience et l'adaptabilité des systèmes de détection face à des menaces évolutives.

2.4 Travaux antérieurs

Nabil et al.[32] explorent de manière approfondie le rôle de la théorie des jeux comme outil stratégique pour améliorer la détection et la prédiction des comportements malveillants dans les réseaux véhiculaires ad hoc (VANET). Face à l'augmentation de la complexité des attaques

et à l'environnement dynamique des VANETs, les approches classiques basées uniquement sur l'analyse statistique ou les règles prédéfinies montrent leurs limites. La théorie des jeux permet de modéliser les interactions entre les attaquants et les systèmes de défense (IDS) comme des confrontations stratégiques, où chaque acteur ajuste ses décisions en fonction des actions adverses. L'article passe en revue quatre catégories majeures de jeux : les jeux non coopératifs, où attaquant et défenseur sont en opposition directe, reflétant bien le modèle GAN/discriminateur, mais pouvant entraîner des erreurs de classification importantes ; les jeux coopératifs, qui encouragent les véhicules à collaborer pour améliorer la détection via des échanges d'informations de confiance, au détriment d'une plus grande consommation de bande passante ; les jeux bayésiens, permettant de prendre en compte l'incertitude des observations à travers des distributions de croyance, particulièrement utiles pour détecter des attaques cachées ou sophistiquées, bien que nécessitant une puissance de calcul plus élevée ; et enfin les jeux de Stackelberg, où l'un des joueurs (souvent le défenseur) prend l'initiative, ce qui permet une meilleure anticipation des comportements malveillants, mais demeure sensible à l'imprévisibilité des attaques adaptatives. Les auteurs soulignent que l'utilisation de ces modèles permet non seulement d'augmenter la précision de détection et de réduire les taux de faux positifs, mais aussi d'optimiser la consommation de ressources réseau. Toutefois, ils relèvent également que la prédiction proactive des attaques reste un défi majeur, notamment en raison du manque de données fiables, de la variabilité du comportement des attaquants et de l'évolution rapide des protocoles VANET. L'article conclut que les perspectives les plus prometteuses résident dans le développement de systèmes IDS hybrides, combinant théorie des jeux, techniques de machine learning et deep learning, dans le but de créer des systèmes intelligents, adaptatifs et capables d'évoluer face à de nouvelles formes d'attaques dans les environnements intelligents et connectés.

Subba et al. [33] proposent un cadre de détection d'intrusion multi-niveaux spécifiquement conçu pour les réseaux véhiculaires ad hoc (VANET), en combinant les avantages de la théorie des jeux et du machine learning. L'objectif principal est de pallier les limites des systèmes IDS classiques dans un environnement VANET marqué par une grande mobilité, des contraintes de ressources, et la nécessité d'une détection rapide et précise des comportements malveillants. La contribution majeure de ce travail repose sur une architecture de détection à trois niveaux. Le premier niveau repose sur un mécanisme de détection basé sur des règles simples (surveillance de la vitesse, distance, densité), destiné à filtrer rapidement les nœuds clairement non suspects. Le deuxième niveau, plus sophistiqué, intègre un modèle d'apprentissage automatique (machine learning) léger, capable de distinguer les comportements suspects des comportements normaux à partir d'attributs dynamiques (vitesse, direction, fréquence des messages, etc.). Ce modèle, entraîné offline et déployé dans les chefs de clusters, permet une classification rapide et efficace en environnement réel. Enfin, le troisième niveau est un module de confirmation, activé uniquement si un nœud est jugé suspect par les deux premières couches, évitant ainsi les faux positifs. Ce dispositif est renforcé par l'intégration d'un modèle de jeu non coopératif à somme nulle entre l'IDS (le défenseur) et l'attaquant. Dans cette modélisation, chaque joueur cherche à maximiser ses gains : l'IDS veut maximiser la détection avec un minimum de ressources, tandis que l'attaquant tente de contourner la surveillance. La stratégie optimale est obtenue via un équilibre de Nash, permettant à l'IDS de choisir de manière probabiliste les nœuds à surveiller. Cela réduit considérablement la surcharge du réseau tout en maximisant les chances de détection. En parallèle, un mécanisme d'incitation de type Vickrey-Clarke-Groves (VCG) est

utilisé pour sélectionner les chefs de clusters de manière honnête et efficace, selon des critères comme la position, l'énergie restante et la mobilité. Les résultats expérimentaux issus de simulations NS-2 démontrent une amélioration significative des performances du système par rapport à des approches IDS classiques. Le taux de détection atteint plus de 90 % pour différentes attaques telles que Sybil, Blackhole ou Denial-of-Service, tout en maintenant un faible taux de faux positifs. La combinaison du machine learning pour la détection comportementale et de la théorie des jeux pour l'optimisation de la stratégie de surveillance s'avère particulièrement pertinente dans le contexte dynamique des VANET. Ce travail illustre concrètement l'intérêt d'approches hybrides pour améliorer l'efficacité des systèmes de sécurité dans les réseaux intelligents. Il ouvre également la voie à des perspectives prometteuses, notamment l'intégration de réseaux de neurones profonds (deep learning) pour une détection temps réel plus robuste, ou encore l'extension du modèle de jeu à un cadre multi-agent avec apprentissage adaptatif.

Wang et al. [34] s'attaquent à la problématique critique du délestage optimal des tâches computationnelles dans les environnements IoV (Internet of Vehicles), où les véhicules doivent traiter rapidement de grandes quantités de données tout en faisant face à des contraintes de ressources (bande passante, énergie, puissance de calcul). Le défi consiste à minimiser simultanément la latence et la consommation énergétique tout en adaptant dynamiquement les décisions de délestage aux conditions changeantes du réseau. Pour cela, les auteurs modélisent le problème comme un jeu coopératif multi-agent basé sur un processus décisionnel de type jeu de Markov, dans lequel chaque véhicule, considéré comme un agent intelligent, apprend à choisir la meilleure stratégie de délestage. La méthodologie repose sur l'intégration de la théorie des jeux coopératifs et de l'apprentissage par renforcement profond (Deep Reinforcement Learning – DRL). Deux algorithmes sont mis en œuvre : le PPOTR (Proximal Policy Optimization with Trust Region), une amélioration de l'algorithme PPO qui introduit une région de confiance pour stabiliser l'apprentissage, et le SAC (Soft Actor-Critic), réputé pour sa rapidité de convergence grâce à l'optimisation de l'entropie et la normalisation des entrées. Le modèle est entraîné à minimiser une fonction de coût composée du délai total de traitement des tâches et de la consommation d'énergie associée. La fonction de récompense est conçue comme une combinaison pondérée de ces deux objectifs. PPOTR adopte une stratégie d'apprentissage par lot (batch learning) avec une mise à jour toutes les 2048 étapes, ce qui permet une convergence plus lente mais plus précise. SAC, de son côté, tire parti d'une exploration plus efficace et d'un apprentissage hors-ligne, lui conférant une convergence rapide. Les résultats de simulation démontrent une nette supériorité de l'algorithme PPOTR par rapport aux stratégies classiques de traitement local, de traitement edge fixe, de délestage aléatoire et même par rapport à l'algorithme SAC. Sur des tâches de 25 Mo, PPOTR permet de réduire la latence de traitement jusqu'à 56,63 %, la consommation énergétique jusqu'à 77,53 %, et d'améliorer la valeur de la fonction de récompense jusqu'à 44 %. Les courbes de convergence indiquent que PPOTR atteint une solution stable à long terme, malgré une phase d'apprentissage initialement plus lente que SAC. Ce dernier conserve l'avantage d'une convergence rapide, ce qui peut être utile dans des environnements très dynamiques ou instables. Toutefois, la capacité de PPOTR à intégrer des données dynamiques et à ajuster finement les politiques en fait un candidat de choix pour une exécution optimisée et fiable dans des environnements réels. Ce travail démontre l'intérêt de combiner DRL et théorie des jeux dans des systèmes distribués comme les VANET. L'approche proposée favorise une prise de décision autonome, coopérative et économe en ressources, tout

en étant capable de s'adapter à l'évolution du contexte réseau. Des perspectives intéressantes d'amélioration incluent l'ajout de modules de détection d'intrusions dans la boucle de décision DRL, l'incorporation de modèles de confiance entre véhicules pour mieux gérer les comportements malveillants, ou encore l'intégration d'alertes de sécurité comme signaux d'entrée pour ajuster dynamiquement la stratégie de délestage. L'extension vers d'autre modèles ou la prise en compte d'un environnement incertain du point de vue sécurité ouvrirait également la voie à une défense proactive et adaptative dans les réseaux Iov.

Hamza et al.[35] proposent une approche innovante de modélisation des attaques complexes dans les réseaux IoT en combinant la théorie des jeux et les processus de décision partiellement observables. Leur objectif est de fournir un outil d'aide à la décision permettant à l'administrateur réseau d'anticiper, de détecter et de contrer les attaques tout en intégrant les contraintes d'incertitude et de coût propres aux environnements connectés. L'approche développée, baptisée AGA-POSG (Attack Graph Analysis - Partially Observable Stochastic Game), repose sur une modélisation du problème sous la forme d'un jeu stochastique à deux joueurs non coopératif, où l'administrateur et l'attaquant s'affrontent selon des stratégies évolutives dans un environnement à visibilité partielle. L'attaquant dispose d'un ensemble d'actions lui permettant de progresser vers un objectif final, tandis que le défenseur cherche à perturber ces trajectoires d'attaque au moindre coût. Pour résoudre ce jeu, les auteurs adoptent une approche méthodologique combinant une représentation matricielle du jeu (forme normale) et un algorithme d'élimination des stratégies dominées, permettant d'identifier les stratégies optimales de défense à chaque étape. Cette méthode est appliquée à un graphe d'attaque construit à partir de scénarios réalistes, incluant des attaques telles que le buffer overflow, l'injection SQL ou encore l'élévation de privilèges. Chaque nœud du graphe représente un état du système compromis, et les transitions sont pondérées en fonction de leur coût et de leur niveau de vulnérabilité. L'analyse repose alors sur l'évaluation de différents chemins d'attaque menant à un terminal critique, en identifiant les vulnérabilités les plus fréquemment exploitées et les plus coûteuses à corriger. Les résultats expérimentaux, obtenus à travers une étude de cas simulant un environnement IoT domestique comportant divers dispositifs connectés (caméras IP, capteurs, imprimantes), démontrent l'efficacité de cette approche pour prioriser les mesures de protection. En supprimant les vulnérabilités les plus critiques identifiées par l'analyse du graphe, il est possible de réduire significativement le nombre de chemins exploitables par l'attaquant et, par conséquent, le risque global du réseau. Ainsi, la stratégie optimale consiste non pas à éliminer toutes les failles, mais à cibler celles dont la présence affecte plusieurs trajectoires d'attaque. En conclusion, cette étude contribue à l'enrichissement des méthodes de modélisation des attaques dans les réseaux IoT en introduisant un cadre théorique rigoureux combinant jeu stochastique partiellement observable et analyse de graphes d'attaque. Les auteurs envisagent, dans les perspectives futures, d'étendre leur approche à des jeux dynamiques répétitifs intégrant des techniques d'apprentissage automatique. Cela permettrait de rendre le système encore plus adaptatif face aux menaces émergentes dans les réseaux intelligents et fortement interconnectés, tels que les VANETs ou les environnements industriels de type IIoT.

Phull et al. [36] proposent dans cet article propose une approche combinant la théorie des jeux et le machine learning pour améliorer la stabilité et la fiabilité du routage dans les réseaux VANETs (Vehicular Ad Hoc Networks). Les réseaux VANETs permettent la communication

inter-véhicule et avec l'infrastructure, mais souffrent d'instabilité due à la mobilité élevée des véhicules et aux changements dynamiques de topologie. L'une des principales difficultés réside dans la sélection des Cluster Heads (CH), qui doit être optimisée pour assurer un fonctionnement efficace du réseau. L'objectif de cette étude est d'automatiser la formation des clusters et d'optimiser la sélection des Cluster Heads afin de minimiser la fréquence des reconfigurations du réseau et d'améliorer la qualité des communications. Pour ce faire, l'approche proposée repose sur deux techniques principales : la théorie des jeux et le machine learning. D'un côté, la théorie des jeux est utilisée pour modéliser l'interaction entre les véhicules comme un processus décisionnel où chaque véhicule est un joueur tentant d'optimiser sa connectivité et sa fiabilité. D'un autre côté, un algorithme de clustering, K-Means, est employé pour regrouper les véhicules en fonction de leur proximité et de leur comportement social. Les performances de cette méthode ont été évaluées selon plusieurs critères, notamment le taux de livraison des paquets (PDR), le délai de transmission, le nombre de réaffiliations et la durée de vie des Cluster Heads. Les résultats montrent que le modèle proposé améliore le taux de livraison des paquets, qui se situe entre 0.97 et 0.99, réduit le délai de transmission et minimise les interruptions de communication dues aux changements de clusters. L'analyse comparative avec d'autres techniques, telles que la théorie des graphes, la logique floue et les réseaux de neurones artificiels (ANNs), met en évidence les avantages de l'approche hybride. Contrairement aux méthodes classiques qui souffrent d'une stabilité réduite ou d'un temps de calcul élevé, l'intégration de la théorie des jeux et du machine learning permet d'obtenir une meilleure adaptabilité du réseau face aux variations dynamiques des VANETs. Toutefois, bien que les résultats obtenus soient prometteurs, ils soulèvent certaines interrogations sur le risque de surapprentissage, étant donné la précision élevée des simulations. L'article recommande de valider ces résultats à travers des tests en conditions réelles et d'explorer des solutions complémentaires telles que l'intégration de modèles de deep learning plus avancés ou l'application de nouvelles stratégies de gestion des ressources réseau. En conclusion, cette étude démontre que l'approche hybride basée sur la théorie des jeux et le machine learning constitue une solution efficace pour améliorer la gestion des clusters et le routage dans les VANETs. Elle permet une communication plus fiable et stable, une meilleure optimisation des ressources, ainsi qu'une réduction des pertes de données et des délais de transmission. Toutefois, des travaux futurs sont nécessaires pour tester cette approche dans des environnements réels et explorer de nouvelles optimisations, notamment en intégrant des technologies émergentes telles que la blockchain ou les transformers en deep learning.

Asadi [37] propose une approche combinant la théorie des jeux coopératifs avec des techniques avancées d'apprentissage automatique (Machine Learning) et d'apprentissage profond (Deep Learning) pour détecter les botnets IoT (Internet des Objets). Les botnets IoT représentent une menace croissante pour la cybersécurité, car ils exploitent des vulnérabilités dans les appareils connectés pour lancer des attaques à grande échelle, telles que les DDoS (attaques par Déni de Service Distribué). Une des principales difficultés dans la détection de ces menaces réside dans la sélection des caractéristiques (features) pertinentes à partir de grands ensembles de données réseau. L'approche proposée utilise un algorithme basé sur la théorie des jeux coopératifs pour sélectionner les caractéristiques les plus significatives. Cette méthode repose sur deux critères principaux : la valeur de Shapley et le critère de victoire (Victory Criterion), qui permettent d'évaluer l'importance relative de chaque caractéristique dans la classification des données. Les dix meilleures caractéristiques ont été identifiées, offrant ainsi une

meilleure précision tout en réduisant la complexité computationnelle. Pour tester l'efficacité de cette approche, plusieurs algorithmes de classification ont été utilisés, notamment les machines à vecteurs de support (SVM), les réseaux LSTM (Long Short-Term Memory) et les autoencodeurs. Les résultats montrent que l'utilisation des caractéristiques sélectionnées améliore significativement les performances des modèles en termes de précision , rappel , et temps d'entraînement . Par exemple, le modèle SVM atteint une précision de 99,996 % avec seulement 10 caractéristiques sélectionnées, surpassant largement les approches précédentes. Toutefois, bien que les résultats obtenus soient très prometteurs, ils soulèvent certaines interrogations concernant leur applicabilité dans des environnements réels. L'étude a été réalisée à l'aide d'un ensemble de données simulées (Bot-IoT), ce qui pourrait limiter la généralisation des conclusions. L'article recommande de valider ces résultats dans des conditions réelles et d'explorer des solutions complémentaires, comme l'intégration de modèles d'apprentissage profond plus avancés ou l'utilisation de nouvelles stratégies pour la gestion des ressources réseau. En conclusion, cette recherche met en lumière le potentiel de la combinaison de la théorie des jeux coopératifs et des techniques d'apprentissage automatique pour détecter efficacement les botnets IoT. Elle ouvre ainsi de nouvelles perspectives pour le développement de systèmes de sécurité capables de protéger les infrastructures IoT contre des cyberattaques de plus en plus sophistiquées.

Zebboudj et al.[38] présentent une avancée majeure en cryptographie quantique en proposant un nouveau protocole de distribution semi-quantique de clés authentifiée (ASQKD) qui se distingue par son approche innovante et ses garanties de sécurité renforcées. Les auteurs, Sofia Zebboudj et ses collaborateurs, partent du constat que les protocoles existants, bien que prometteurs, présentent des vulnérabilités critiques pouvant être exploitées par des attaques quantiques sophistiquées. Leur solution repose sur une architecture novatrice éliminant le recours à l'intrication quantique (états de Bell), simplifiant ainsi considérablement les exigences matérielles tout en maintenant un niveau de sécurité élevé. Le protocole proposé se décline en deux variantes complémentaires : une approche basée sur la randomisation des particules de vérification et une autre utilisant le principe mesure-renvoi. Ces deux méthodes s'appuient sur un système ingénieux de clés pré-partagées et de fonctions de hachage cryptographiques (H_auth) pour garantir à la fois l'authenticité des parties et l'intégrité des échanges. Un mécanisme dynamique de mise à jour des clés, combiné à des particules de contrôle spécialement conçues, permet de détecter et de neutraliser les tentatives d'intrusion avec une grande efficacité. L'analyse de sécurité approfondie menée par les auteurs démontre la supériorité de leur approche face aux principales classes d'attaques quantiques. Le protocole résiste particulièrement bien aux attaques d'impersonation, aux attaques par interception-renvoi, ainsi qu'aux scénarios de type "man-in-the-middle". Contrairement aux solutions précédentes, il préserve la confidentialité des clés pré-partagées même en cas d'attaque partiellement réussie, grâce à un système sophistiqué d'amplification de la confidentialité. D'un point de vue pratique, cette recherche ouvre des perspectives intéressantes pour le déploiement à grande échelle de systèmes cryptographiques quantiques. L'élimination des états intriqués réduit considérablement la complexité technique et le coût d'implémentation, tout en maintenant une sécurité inconditionnelle. Les auteurs soulignent que leur protocole est particulièrement adapté aux architectures client-serveur et pourrait trouver des applications dans les systèmes de communication critiques nécessitant une authentification forte. Cette contribution s'inscrit dans la lignée des travaux visant à rendre la cryptographie quantique accessible tout en maintenant des garanties de sécurité absolues. Elle combine

judicieusement les avantages des systèmes quantiques (détection d'intrusion naturelle, sécurité prouvée) avec la praticité des approches semi-quantiques (réduction des exigences matérielles). Les résultats présentés dans cet article représentent une avancée notable vers la réalisation concrète de réseaux de communication quantiques sécurisés et économiquement viables.

Shu et al.[39] présentent dans cet article un système innovant de détection collaborative d'intrusions (CIDS) pour les réseaux ad hoc véhiculaires (VANETs), combinant les avantages des architectures SDN distribuées et des techniques avancées d'apprentissage profond. Leur approche repose sur une adaptation des réseaux antagonistes génératifs (GANs) avec plusieurs discriminateurs (MD-GAN) et un cadre inspiré de EGBAD (Efficient GAN-Based Anomaly Detection). Le système proposé permet à plusieurs contrôleurs SDN répartis géographiquement de collaborer pour entraîner un modèle global de détection d'intrusions, sans nécessiter d'échange direct des flux réseau sensibles entre eux. Cette architecture évite ainsi les problèmes de biais liés aux données locales (problème du biased flow) tout en réduisant la surcharge de calcul et de communication associée aux approches centralisées. Les auteurs démontrent théoriquement la convergence du modèle dans des scénarios où les données sont indépendamment et identiquement distribuées (IID) ou non-IID, grâce à un mécanisme d'échange périodique (swapping) des paramètres entre contrôleurs. Les évaluations expérimentales, menées sur des jeux de données réels (KDD99 et NSL-KDD), confirment l'efficacité de CIDS en termes de précision, rappel et F1-score, surpassant les méthodes individuelles de détection tout en approchant les performances des systèmes centralisés. De plus, l'analyse des coûts en calcul, mémoire et communication montre que CIDS offre un bon compromis entre efficacité et scalabilité, essentiel pour les VANETs dynamiques où la mobilité des véhicules et la diversité des attaques (DoS, spoofing, etc.) posent des défis majeurs. Enfin, les auteurs discutent des limitations, notamment face aux attaques zero-day, et suggèrent des améliorations possibles via des mécanismes d'apprentissage en ligne (online learning). Cette contribution ouvre des perspectives prometteuses pour la sécurisation des réseaux véhiculaires tout en préservant la confidentialité et l'efficacité opérationnelle.

2.5 Discussion

L'analyse des approches existantes appliquées à la cybersécurité des réseaux VANETs montre une progression significative dans l'intégration de l'intelligence artificielle, en particulier du Machine Learning (ML) et du Deep Learning (DL). Le ML a permis de concevoir des systèmes capables de détecter des comportements anormaux dans les flux de données en s'appuyant sur des modèles d'apprentissage supervisés ou non. Cependant, ces méthodes sont souvent limitées par la qualité et la quantité des données disponibles, ainsi que par le déséquilibre des classes entre trafic normal et attaques.

L'introduction du Deep Learning, notamment par le biais des réseaux de neurones multicouches (MLP), des CNN et des RNN/LSTM, a permis de surmonter certaines de ces limites en automatisant la détection de caractéristiques pertinentes et en renforçant la capacité à identifier des patterns complexes.

La théorie des jeux, quant à elle, offre un cadre rigoureux pour modéliser les interactions stratégiques entre attaquants et défenseurs. Elle permet de mieux comprendre les dynamiques d'adaptation entre générateurs d'attaques et systèmes de détection, ce qui est essentiel pour

développer des IDS (Intrusion Detection Systems) intelligents, résilients et dynamiques. Cette modélisation est particulièrement pertinente lorsqu'on considère les GANs comme une mise en œuvre implicite d'un jeu adversarial, alignée avec le concept d'équilibre de Nash.

Enfin, l'essor de l'informatique quantique ouvre de nouvelles perspectives. L'intégration des circuits quantiques dans les architectures génératives (QGANs) pourrait offrir des avantages substantiels en matière de diversité des données synthétiques et d'optimisation des performances, tout en explorant des espaces de probabilité difficilement accessibles par les modèles classiques. Cela renforce l'idée que la convergence entre IA, théorie des jeux et technologies quantiques représente un axe stratégique pour la cybersécurité des VANETs et des systèmes de transport intelligents de demain.

Conclusion

Ces apports montrent que le Deep Learning constitue un levier stratégique pour faire face aux nouvelles générations d'attaques dans les réseaux véhiculaires. Ce constat justifie l'intérêt croissant pour des solutions basées sur des architectures génératives et discriminatives, qui seront explorées dans le chapitre suivant.

3
Proposition

Introduction

Ce chapitre présente la démarche méthodologique adoptée pour la détection d'intrusions dans les réseaux VANETs. Après une modélisation stratégique de l'interaction entre l'attaquant et le défenseur, fondée sur la théorie des jeux, nous introduisons plusieurs approches basées sur l'intelligence artificielle, avec pour objectif d'améliorer la détection d'attaques dans des environnements hautement dynamiques et distribués.

Notre étude se concentre principalement sur l'attaque Blackhole, une menace critique dans les réseaux VANETs. Dans ce type d'attaque, un nœud malveillant attire les messages de routage en prétendant avoir la meilleure route vers la destination, avant d'intercepter ou de supprimer les paquets de données, provoquant ainsi un déni de service comme illustrer dans cette figure 3.1.

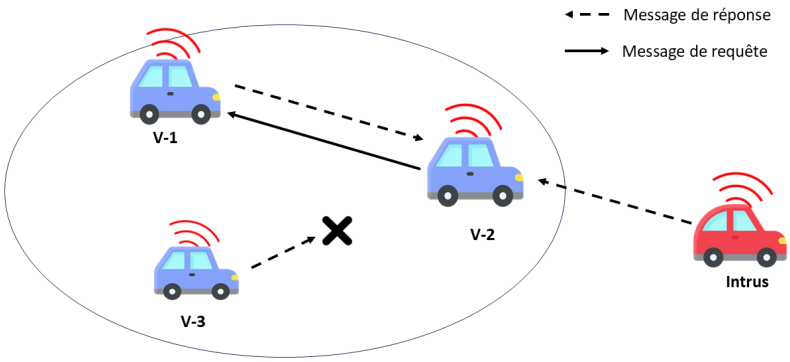


FIGURE 3.1 – Représentation de l'attaque Blackhole

Pour répondre à ce défi, nous proposons deux approches basées sur des réseaux génératifs adversariaux : une architecture classique conditionnelle (cGAN) et une version hybride intégrant des circuits quantiques paramétrés (QGAN). Ces modèles permettent de générer des données synthétiques pour enrichir les classes d'intrusions et renforcer la capacité de détection d'un classifieur supervisé.

Ce chapitre détaille le cadre théorique sous-jacent, l'implémentation des différentes architectures, ainsi qu'une analyse comparative des performances obtenues.

Sommaire

3.1 Cadre conceptuel : modélisation stratégique via la théorie des jeux

Les attaques malveillantes comme le Blackhole représentent une menace sérieuse. La lutte contre ces attaques peut être interprétée comme un conflit stratégique entre deux entités : un attaquant qui tente de perturber le réseau, et un défenseur qui cherche à détecter et bloquer cette perturbation. Cette dynamique est particulièrement bien illustrée dans les systèmes d'apprentissage adversarial tels que les Generative Adversarial Networks (GAN), où deux modèles le générateur et le discriminateur s'affrontent dans un cadre compétitif. Cette confrontation est analogue à celle entre un attaquant et un défenseur dans un Système de Détection d'Intrusion (IDS). Afin de formaliser cette interaction, nous avons recours à la théorie des jeux, un outil mathématique puissant permettant de modéliser les situations de conflit entre acteurs rationnels

3.1.1 Définition du jeu

La situation étudiée est modélisée comme un jeu statique à deux joueurs, non coopératif et à somme non nulle. Dans ce cadre, les décisions des joueurs sont prises simultanément, sans que l'un ait connaissance préalable des choix de l'autre. Ce type de jeu permet de représenter fidèlement les interactions conflictuelles entre un attaquant et un défenseur dans un réseau VANET, où les actions sont menées de manière indépendante et souvent sans communication directe.

Les deux joueurs du jeu sont définis comme suit :

— **Attaquant (A)** : son objectif est d'injecter une attaque de type Blackhole et de maximiser l'effet de cette perturbation sur le réseau.

— **Défenseur (D)** : il vise à minimiser l'impact de l'attaque en adoptant des stratégies de détection reposant sur des techniques d'intelligence artificielle.

Le jeu est dit non coopératif car chaque joueur agit de manière autonome, sans coordination ni collaboration avec l'autre. De plus, il s'agit d'un jeu à somme non nulle, ce qui signifie que les gains de l'un ne correspondent pas nécessairement à une perte équivalente de l'autre ; autrement dit, les intérêts des deux joueurs ne sont pas strictement opposés et les résultats ne s'annulent pas automatiquement.

3.1.2 Stratégies des joueurs

Dans ce jeu stratégique, chaque joueur dispose d'un ensemble restreint mais pertinent de stratégies, représentant les comportements réalistes observables dans notre système de détection d'intrusion appliqué aux réseaux VANETs.

Stratégies de l'attaquant (S_a) :

— **no_attack** : l'attaquant adopte un comportement neutre, sans lancer d'attaque ni tenter de perturber le réseau.

— **blackhole** : l'attaquant exécute une attaque de type Blackhole, consistant à s'insérer dans le réseau pour intercepter et supprimer les paquets de données qu'il reçoit.

Stratégies du défenseur (S_d) :

1. **discriminator_only** : le défenseur utilise uniquement le discriminateur d'un réseau antagoniste génératif (GAN) comme outil de détection, sans recours à un classifieur externe.

2. **mlp_cgan** : un perceptron multicouche (MLP) est entraîné sur un ensemble de données enrichi par un GAN conditionnel (cGAN), dans le but d'améliorer la capacité de détection.
3. **mlp_qgan** : le défenseur exploite un MLP formé sur des données générées par un QGAN (GAN quantique), permettant de capturer des structures de données plus complexes et subtiles, souvent inaccessibles aux méthodes classiques.

3.1.3 Matrice des gains

La matrice suivante illustre les gains respectifs des deux joueurs, l'attaquant et le défenseur, pour chaque combinaison possible de stratégies. Les cellules de la matrice sont représentées sous forme de paires (a, d), où a correspond au gain de l'attaquant et d à celui du défenseur. Cette modélisation permet de visualiser les dynamiques conflictuelles et les équilibres potentiels entre les différentes approches de détection et d'attaque le tableau 3.1 montre la matrice de gain.

Attaquant / Défenseur	discriminator_only	mlp_cgan	mlp_qgan
no_attack	(0, -1)	(0, -2)	(0, -3)
blackhole	(1, -1)	(-1, 1)	(-2, 1)

TABLE 3.1 – Matrice de gain

3.1.4 Analyse de la matrice

L'analyse de cette matrice met en évidence l'efficacité relative de chaque stratégie défensive face à une attaque de type Blackhole :

— **Cas 1 : *no_attack***
Lorsque l'attaquant choisit de ne pas lancer d'attaque, l'attaquant n'obtient aucun gain (0) mais le défenseur subit malgré tout un coût dû à la complexité des mécanismes défensifs. Ce coût augmente selon la défense choisie : discriminator_only : -1, mlp_cgan : -2, mlp_qgan : -3. Ceci traduit le fait que maintenir des défenses coûte en ressources même en l'absence d'attaque, et que des défenses plus sophistiquées peuvent être plus onéreuses à exploiter ou maintenir.

— **Cas 2 : *blackhole* vs *discriminator_only***
Le seul discriminateur du GAN reste peu performant face à l'attaque Blackhole : l'attaquant tire un petit bénéfice (+1) tandis que le défenseur subit une perte légère (-1). La vulnérabilité existe mais elle est moins catastrophique qu'avec la matrice initiale — ici l'impact est modéré.

— **Cas 3 : *blackhole* vs *mlp_cgan***
L'entraînement du MLP sur des exemples synthétiques fournis par un cGAN améliore sensiblement la détection. Dans cette configuration l'attaquant perd légèrement (–1) — l'attaque est en grande partie contrée — et le défenseur en tire un petit bénéfice (+1). Cela montre l'intérêt d'un apprentissage supervisé alimenté par des synthèses réalistes pour limiter l'efficacité de l'attaquant.

— **Cas 4 : *blackhole* vs *mlp_qgan***
L'usage d'un QGAN pour générer des exemples d'attaque encore plus représentatifs rend le MLP plus robuste : l'attaquant subit une perte plus marquée (–2) tandis que le

défenseur obtient un gain modéré (+1). Cette combinaison apparaît comme la meilleure défense contre le Blackhole dans la matrice proposée.

Remarque sur l'équilibre stratégique : avec ces valeurs la matrice admet un équilibre de Nash mixte : l'attaquant joue Pr(no_attack) = $\frac{2}{3}$ et Pr(blackhole) = $\frac{1}{3}$, tandis que le défenseur mélange entre discriminator_only et mlp_cgan avec des probabilités $\frac{1}{2}$ chacune (la stratégie mlp_qgan a probabilité 0 à l'équilibre). Ainsi, aucune stratégie pure n'est dominante et les deux joueurs doivent randomiser pour rester optimaux.

3.2 Méthodologie générale

Dans cette partie, nous présentons la démarche méthodologique adoptée pour la conception et l'évaluation de notre système de détection d'intrusions dans les réseaux VANETs. Elle repose sur un enchaînement structuré de modules comprenant l'élaboration et le prétraitement d'un jeu de données simulé, l'utilisation de modèles génératifs pour rééquilibrer les classes, l'entraînement d'un classifieur supervisé de type MLP, et enfin l'évaluation des performances à l'aide de métriques standardisées. Ce cadre expérimental nous permet de comparer objectivement plusieurs variantes d'architectures, notamment celles intégrant des composants quantiques, dans un contexte de détection d'attaques Blackhole.

3.2.1 Présentation du jeu de données et prétraitement

L'expérimentation proposée s'appuie sur un jeu de données simulé, représentatif d'un réseau VANET soumis à des conditions normales ainsi qu'à des attaques de type Blackhole. Ce dataset, structuré au format CSV, regroupe les caractéristiques de plusieurs milliers de nœuds simulés, en prenant en compte à la fois leurs paramètres de mobilité, leurs interactions réseau et leurs comportements suspects. Dans le cadre de cette étude, seules deux classes ont été retenues : les nœuds bénins et ceux impliqués dans des attaques Blackhole. Un processus rigoureux de prétraitement a été appliqué : suppression des colonnes non pertinentes, encodage des classes en format binaire, normalisation des variables quantitatives, et stratification du jeu de données en ensembles d'apprentissage (80 %) et de test (20 %). Ce pipeline assure la cohérence, la qualité et l'adéquation du jeu de données aux différents modèles d'apprentissage supervisé et génératif proposés dans ce travail, tout en tenant compte du déséquilibre significatif entre les classes, justifiant le recours à des techniques de génération de données synthétiques.

3.2.2 Méthodes génératives pour le rééquilibrage des données

Le déséquilibre de classes constitue un enjeu critique dans les systèmes de détection d'intrusion, notamment dans le contexte des VANETs où les attaques réelles sont beaucoup moins fréquentes que les comportements normaux. Pour pallier ce problème, les méthodes de génération de données synthétiques se sont imposées comme une solution efficace. Parmi elles, les autoencodeurs et les réseaux antagonistes génératifs (GANs) sont largement utilisés.

Les GANs sont constitués de deux réseaux en compétition : un générateur, chargé de produire des données artificielles à partir d'un bruit aléatoire, et un discriminateur, dont le rôle est de différencier les données réelles de celles générées. Cette dynamique compétitive pousse le

générateur à améliorer la qualité de ses échantillons jusqu'à ce que ceux-ci deviennent indiscernables pour le discriminateur.

Dans notre approche, nous utilisons une variante appelée *Conditional GAN* (cGAN), où les deux réseaux sont conditionnés par une étiquette de classe. Cette spécificité permet de diriger la génération vers des exemples appartenant à une classe précise, en l'occurrence ici, la classe minoritaire correspondant aux attaques de type Blackhole. Le cGAN permet ainsi de produire des instances synthétiques réalistes de comportements malveillants, contribuant à rééquilibrer le jeu de données et à améliorer la performance du classifieur MLP utilisé en aval.

3.2.3 Présentation du réseau MLP (Multi-Layer Perceptron)

Le MLP (Multi-Layer Perceptron) est l'une des architectures les plus fondamentales du Deep Learning. Il s'agit d'un réseau de neurones entièrement connecté, où chaque couche de neurones est connectée à la suivante. Dans notre projet, le MLP est utilisé comme classifieur final, chargé de distinguer les types de paquets (bénins ou malicieux) à partir de caractéristiques extraites. Grâce à des techniques de régularisation comme le Dropout et la normalisation par lot (Batch Normalization), le MLP est capable d'apprendre efficacement même à partir de données enrichies de manière synthétique par des GANs[43].

3.2.4 Métriques d'évaluation

L'évaluation des performances constitue une étape essentielle dans tout système de détection d'intrusions, en particulier dans les réseaux VANETs, où les conséquences d'une mauvaise détection peuvent compromettre la sécurité du système. Pour évaluer la capacité de nos modèles à distinguer efficacement les paquets malveillants des paquets bénins, nous nous appuyons sur quatre métriques classiques mais robustes : l'accuracy, la précision, le rappel et le F1-score. Ces indicateurs sont dérivés des valeurs de la matrice de confusion, qui regroupe les vrais positifs (TP), vrais négatifs (TN), faux positifs (FP) et faux négatifs (FN)[44].

— **Accuracy (Exactitude)** : elle mesure la proportion d'exemples correctement classés parmi l'ensemble des données. Bien qu'intuitive, cette mesure peut être trompeuse dans des contextes où les classes sont déséquilibrées, comme c'est souvent le cas en cybersécurité.

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

— **Recall (Rappel ou sensibilité)** : il indique la capacité du modèle à identifier correctement les paquets réellement malveillants. Une valeur élevée de rappel montre que peu d'attaques sont ignorées.

$$\text{Recall} = \frac{TP}{TP + FN}$$

— **Precision (Précision)** : elle évalue la proportion de paquets prédits comme malveillants qui le sont réellement. Une faible précision suggère que de nombreux paquets bénins sont classés à tort comme malveillants, ce qui peut générer des faux positifs coûteux.

$$\text{Precision} = \frac{TP}{TP + FP}$$

— **F1-score** : il s'agit de la moyenne harmonique entre la précision et le rappel. Il offre un bon compromis dans les situations de déséquilibre de classes, en pénalisant à la fois les faux positifs et les faux négatifs.

$$\text{F1-score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$$

Ces métriques sont utilisées pour évaluer les performances des différentes approches proposées dans ce travail, notamment celles fondées sur le cGAN, le QGAN et les classifieurs MLP. Elles permettent d'assurer une comparaison objective entre les modèles, en tenant compte à la fois de leur capacité de détection et de leur fiabilité.

3.3 Proposition 1 : Méthode hybride basée sur GAN et théorie des jeux

3.3.1 Approche 1 : Utilisation du discriminateur comme classifieur

Dans une première approche exploratoire, nous avons étudié la possibilité de réutiliser directement le discriminateur du réseau antagoniste génératif (GAN) comme un classifieur binaire. Cette démarche repose sur une intuition fondamentale du fonctionnement des GANs : le rôle du discriminateur est d'apprendre à distinguer des données « réelles » (provenant du jeu d'apprentissage) de celles générées artificiellement par le générateur. En théorie, cette capacité de discrimination peut être exploitée comme une première forme rudimentaire de classification.

3.3.2 Architecture et fonctionnement

Le discriminateur utilisé dans cette approche est un réseau de neurones simple, prenant en entrée des vecteurs de caractéristiques issus du dataset VANET. Ce réseau est composé de plusieurs couches denses avec fonctions d'activation de type LeakyReLU, suivies de couches de régularisation par Dropout. En sortie, une unique unité avec une fonction d'activation sigmoïde fournit une probabilité comprise entre 0 et 1, interprétée comme la probabilité que l'entrée soit malicieuse (attaque) ou bénigne. Plutôt que de l'utiliser uniquement dans un cadre adversarial (où il fournit un feedback au générateur), le discriminateur est ici exploité en mode évaluation directe, c'est-à-dire appliqué sur des échantillons réels du jeu de test, sans régénération. Sa sortie est ensuite comparée à l'étiquette réelle (benign ou blackhole) afin d'évaluer ses performances.

3.3.3 Principe de classification

Pour effectuer cette classification, un seuil de décision est défini, généralement fixé à 0.5. Si la sortie du discriminateur dépasse ce seuil (valeur supérieure à 0.5), l'exemple est alors classé comme une attaque de type blackhole. Dans le cas contraire, c'est-à-dire si la sortie est inférieure ou égale à 0.5, l'exemple est considéré comme bénin.

3.3.4 Évaluation et résultats

Une fois le discriminateur entraîné dans le cadre d'un CGAN conditionnel, il est évalué indépendamment à l'aide des métriques classiques de classification : l'accuracy, le rappel (recall), la précision (precision) et le F1-score. Le tableau 3.3.4 présente les résultats obtenus :

Classe	Précision	Rappel	F1-score
Benign	0,86	0,82	0,84
Blackhole	0,41	0,48	0,45
Accuracy globale	0,75		

TABLE 3.2 – Performances du discriminateur utilisé comme classifieur

Cette approche minimaliste consiste à détourner le rôle initial du discriminateur, non pas uniquement comme adversaire du générateur, mais comme classifieur binaire. Malgré l'absence d'un apprentissage supervisé spécifique, cette méthode a permis d'atteindre une accuracy globale de 75 %, avec des performances acceptables sur la classe benign (précision de 0.86, rappel de 0.82). Toutefois, la capacité à détecter les attaques blackhole reste limitée (précision 0.41, rappel 0.48), ce qui s'explique par le fait que le discriminateur n'a pas été entraîné à distinguer spécifiquement les catégories de comportement mais seulement à différencier le "vrai" du "faux". Cette expérience met cependant en lumière une capacité d'apprentissage implicite du discriminateur à capter des régularités structurelles utiles. Il s'agit là d'un premier jalon vers des systèmes de détection d'intrusion légers, dans lesquels des composants adversariaux pourraient jouer un double rôle : produire des données synthétiques et servir de détecteur de comportement anormal.

3.3.5 Approche 2 : Détection par génération classique avec conditional GAN (cGAN)

La détection d'intrusion est confrontée à un défi majeur : l'extrême déséquilibre des classes entre les comportements bénins, largement majoritaires, et les attaques, qui sont rares mais critiques. Cette disproportion statistique complique l'apprentissage supervisé, car les modèles ont tendance à être biaisés vers la classe majoritaire. Afin de renforcer la détection des attaques de type Blackhole, nous avons mis en œuvre une approche de génération de données synthétiques ciblées à l'aide d'un conditional Generative Adversarial Network (cGAN).

3.3.6 Motivation d'utilisation cGAN

L'objectif principal est de générer artificiellement des exemples supplémentaires représentant des attaques Blackhole, afin d'équilibrer les données d'apprentissage. Contrairement aux GANs classiques, le cGAN permet de conditionner la génération sur une étiquette de classe explicite, ce qui facilite la production de données ciblées. Cette capacité est exploitée ici pour synthétiser uniquement des attaques Blackhole réalistes

3.3.7 Architecture du cGAN

Le cGAN repose sur une architecture à deux composantes : un générateur et un discriminateur, tous deux conditionnés par une information de classe. Dans notre contexte, le cGAN est utilisé pour générer artificiellement des exemples d'attaques de type Blackhole, afin de rééquilibrer un jeu de données initialement déséquilibré. Le générateur apprend à produire des vecteurs de caractéristiques réalistes à partir d'un bruit aléatoire et d'un label conditionnel fourni (ici, "Blackhole"). Parallèlement, le discriminateur reçoit à la fois des exemples réels ou générés et leur étiquette de classe correspondante, et apprend à distinguer les données synthétiques des authentiques. L'information conditionnelle est injectée dans les deux réseaux : elle est transformée par une couche d'embedding dans le générateur et concaténée aux entrées du discriminateur. Cette structuration permet au générateur de se focaliser sur la génération ciblée d'un type d'attaque précis, tout en contraignant le discriminateur à apprendre une distinction plus fine, spécifique à cette catégorie. Ce mécanisme est représenté dans la figure 3.2 suivante.

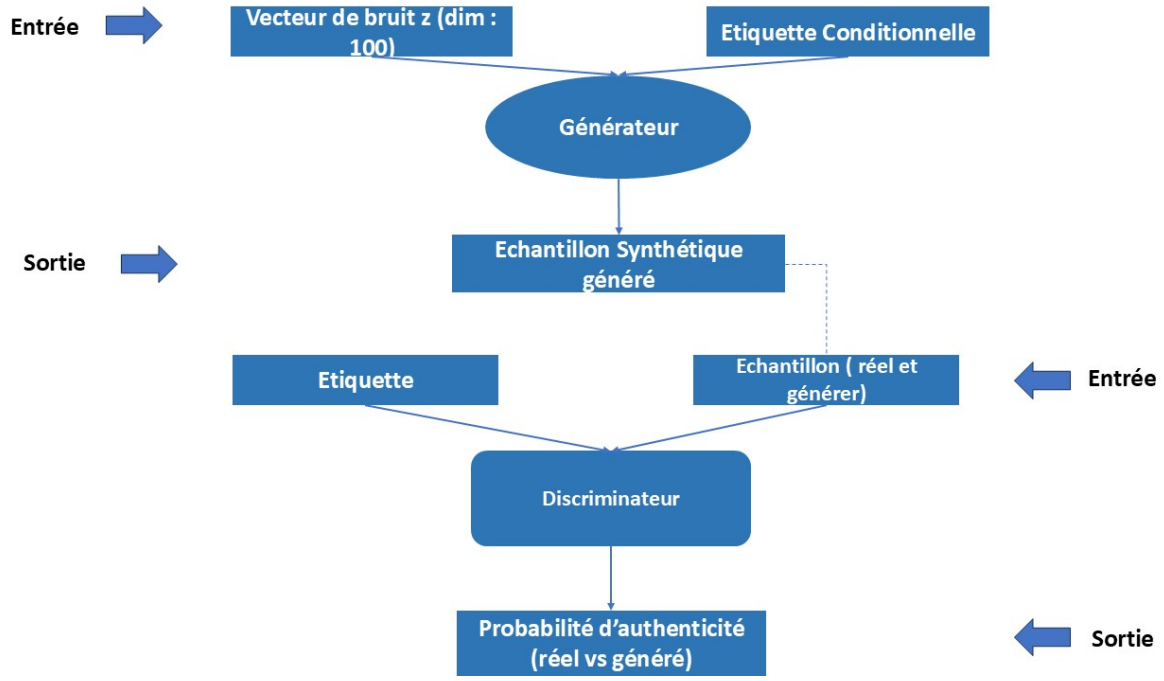
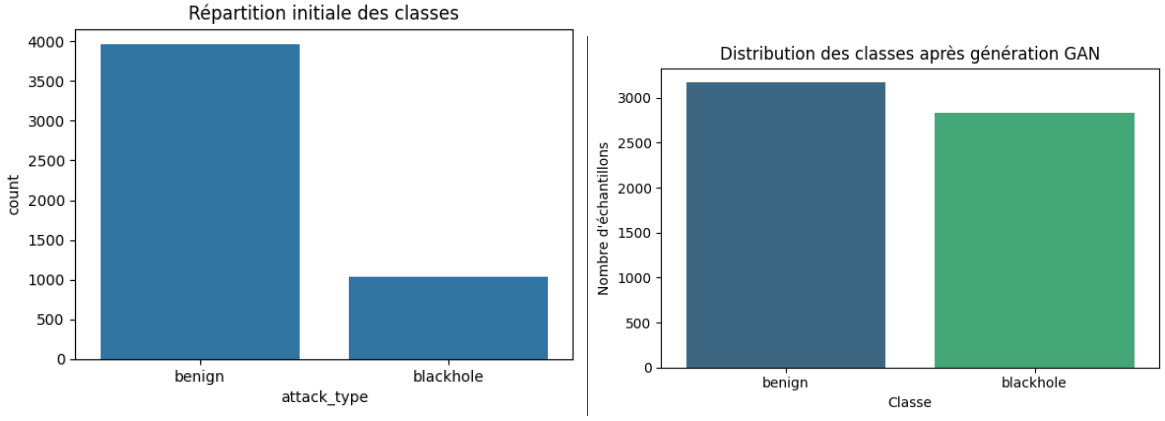


FIGURE 3.2 – Architecture du cGAN conditionné sur le label *Blackhole*

3.3.8 Génération d'échantillons synthétiques

Une fois le modèle entraîné, le générateur est utilisé pour produire plusieurs milliers d'exemples synthétiques. La figure 3.3 illustre la distribution des classes avant et après génération, mettant en évidence l'effet de rééquilibrage. Afin de garantir la qualité des données générées, un filtrage est appliqué : seules les instances obtenant un score de crédibilité supérieur à un seuil (par exemple 0.6) selon le discriminateur sont conservées. Cela permet d'éliminer les échantillons peu réalistes ou bruités.



(a) ***Avant génération.*** **(b)** ***Après génération.***

FIGURE 3.3 – Effet de la génération d'échantillons synthétiques sur la distribution des classes.

3.3.9 Entraînement du classifieur MLP

Après la génération des échantillons synthétiques d'attaques Blackhole à l'aide des modèles cGAN, ces données sont fusionnées avec les données réelles issues du jeu d'origine pour constituer un ensemble d'entraînement enrichi et mieux équilibré. Ce nouvel ensemble est ensuite utilisé pour entraîner un classifieur supervisé de type Perceptron Multi-Couches (MLP). L'architecture du MLP comprend une couche d'entrée dense, suivie de deux couches cachées activées par la fonction ReLU. Ces couches sont régularisées par des techniques de Dropout et de Batch Normalization, afin de prévenir l'overfitting et de stabiliser l'apprentissage. La couche de sortie, quant à elle, comporte deux neurones activés par une fonction softmax, correspondant aux deux classes : « benign » et « blackhole », comme le montre la figure 3.4.

L'apprentissage du MLP repose sur plusieurs stratégies visant à optimiser la robustesse du modèle. D'abord, le jeu de données est équilibré grâce à l'ajout d'exemples synthétiques, ce qui améliore la représentativité de la classe minoritaire. Ensuite, une pondération dynamique des classes est appliquée via l'argument `class_weight`, pour compenser le déséquilibre résiduel entre les classes. Enfin, une validation croisée est intégrée à travers la méthode d'*EarlyStopping*, qui permet de stopper l'entraînement dès que la performance en validation cesse de progresser, évitant ainsi le surapprentissage.

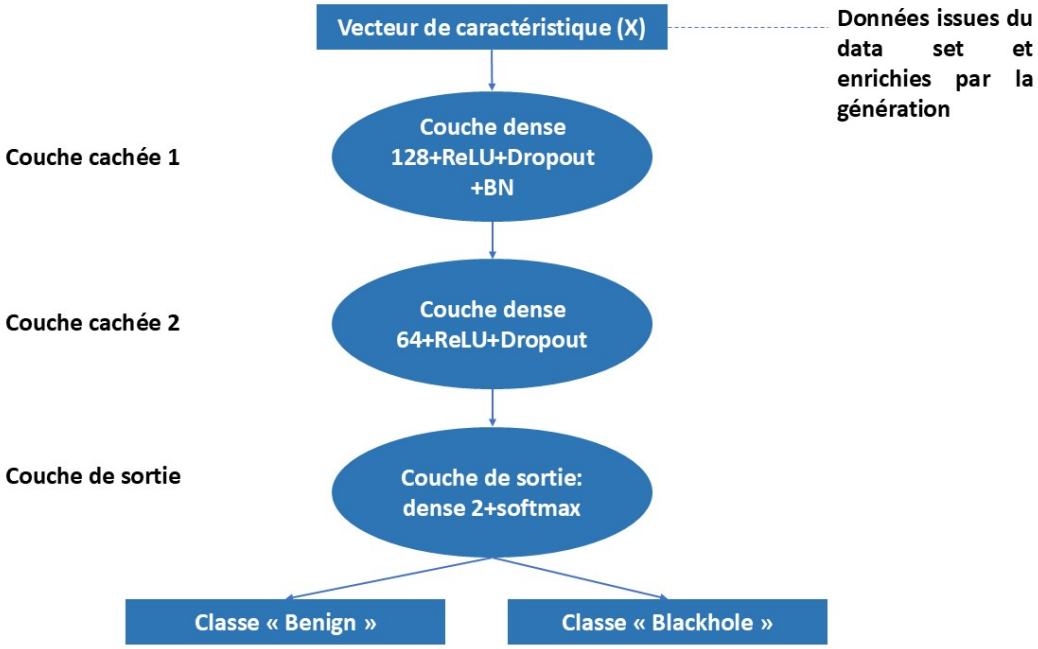


FIGURE 3.4 – Architecture du classifieur MLP utilisé pour la détection des attaques Blackhole.

3.3.10 Évaluation et résultats

Dans cette approche, les performances du classifieur MLP, entraîné avec un jeu de données enrichi à l'aide du cGAN, ont été évaluées sur un ensemble de test stratifié. Les indicateurs de classification permettent de quantifier l'impact de la génération synthétique ciblée sur l'amélioration de la détection des attaques de type *Blackhole*.

Les résultats obtenus sont résumés dans le tableau 3.3, qui présente les valeurs des principales métriques d'évaluation : l'accuracy, la précision, le rappel et le F1-score, pour chaque classe (benign, blackhole) ainsi qu'une moyenne générale.

Classe	Accuracy	Précision	Rappel	F1-score
Benign	0.96	0.96	0.96	0.96
Blackhole	0.87	0.87	0.87	0.87
Général	0.9460	0.8738	0.8654	0.8696

TABLE 3.3 – Résultats de classification du MLP entraîné avec données enrichies par cGAN

cette approche introduit un cGAN pour générer spécifiquement des échantillons synthétiques représentant des attaques blackhole, ce qui permet de pallier le déséquilibre marqué du jeu de données initial. Une fois les données augmentées, un classifieur MLP est entraîné sur ce jeu enrichi. Cette méthode a permis d'obtenir les meilleurs résultats de l'étude, avec une accuracy globale de 94.6 %, un rappel de 87.38 %, et un score F1 de 86.54 %. Ces chiffres traduisent non seulement une excellente capacité à reconnaître les comportements bénins, mais également une forte aptitude à détecter les attaques blackhole, avec un équilibre remarquable entre précision

et rappel (0.87 pour les deux). Le succès de cette approche repose en grande partie sur deux éléments la capacité du cGAN à apprendre une distribution conditionnelle sur les étiquettes, et le fait que le générateur a été entraîné pendant 2000 époques, soit une durée suffisante pour affiner la qualité des exemples synthétiques produits. Cette profondeur d'entraînement permet de mieux capturer les caractéristiques propres aux comportements malveillants, en particulier ceux, rares, liés à l'attaque Blackhole.

3.4 Proposition 2 : Détection d'intrusion par QGAN (GAN quantique)

Dans cette section, nous présentons notre seconde proposition de détection d'intrusion dans les réseaux VANETs, fondée sur l'utilisation des réseaux antagonistes génératifs quantiques (QGAN). Nous commençons par un cadre théorique qui expose les motivations du recours à l'informatique quantique, avant de décrire l'implémentation concrète de notre approche et d'en analyser les résultats.

3.4.1 Cadre théorique et motivations

Cette sous-section expose les fondements théoriques de notre proposition. Nous y détaillons les limites des approches classiques de détection d'intrusion, les principes de l'informatique quantique, les apports spécifiques des QGANs, ainsi que les raisons pour lesquelles ces technologies sont adaptées au contexte dynamique et incertain des réseaux VANETs.

3.4.1.1 Contexte général et limites des approches classiques

L'émergence des réseaux intelligents, en particulier les VANETs (Vehicular Ad-hoc Networks), dans les Systèmes de Transport Intelligents (STI) s'accompagne d'une intensification des risques de cybersécurité. Ces réseaux génèrent en continu un flux de données massives, souvent déséquilibrées et sensibles au bruit, rendant la détection d'intrusions difficile.

Les approches traditionnelles, basées sur le Machine Learning ou le Deep Learning, se montrent performantes dans des contextes standardisés. Néanmoins, elles souffrent de limitations lorsqu'il s'agit d'identifier des attaques rares, subtiles ou déguisées, comme les attaques Blackhole ou Sybil. Ces méthodes peinent à généraliser à partir d'exemples peu nombreux ou à extraire des motifs faibles dans un environnement fortement dynamique.

Face à ces contraintes, l'informatique quantique s'impose comme une voie innovante pour explorer des espaces de solution plus riches, avec une expressivité accrue. L'intégration du quantique dans des modèles de détection offre des perspectives nouvelles, notamment grâce aux Quantum GANs (QGAN), qui exploitent la puissance des circuits quantiques pour affiner la génération et la discrimination d'exemples malveillants.

3.4.1.2 Fondements de l'informatique quantique

L'informatique quantique est un paradigme computationnel qui repose sur les lois de la mécanique quantique pour traiter l'information. Elle diffère profondément de l'informatique classique, en manipulant des entités appelées *qubits*, capables de représenter simultanément plusieurs états, ce qui ouvre la voie à une puissance de calcul exponentielle[40].

Qubit : Le bit quantique, ou qubit, est l'unité fondamentale d'information dans un ordinateur quantique. Contrairement au bit classique, un qubit peut se trouver dans un état de *superposition* : il est simultanément dans les états 0 et 1, représentés par une combinaison linéaire $\alpha 0 + \beta 1$, où α et β sont des amplitudes complexes satisfaisant $|\alpha|^2 + |\beta|^2 = 1$.

Superposition : Ce phénomène permet à un processeur quantique de traiter un grand nombre de configurations en parallèle, ce qui accélère significativement certains types de calculs, notamment en recherche combinatoire et en optimisation.

Intrication : Deux qubits peuvent être *intriqués*, c'est-à-dire que leur état est corrélé de manière non classique. Une mesure sur l'un affecte instantanément l'état de l'autre, même à grande distance. Cette propriété est utilisée pour sécuriser des communications ou augmenter la puissance d'un algorithme quantique.

Mesure : Lorsque l'on mesure un qubit, il "s'effondre" dans l'un des deux états classiques (0 ou 1), avec une probabilité dictée par les amplitudes α et β. C'est cette opération qui permet de lire le résultat d'un calcul quantique.

En cybersécurité, ces propriétés quantiques offrent plusieurs atouts majeurs :

— **Exploration efficace d'espaces de grande dimension** : Utile pour détecter des comportements anormaux dans des volumes massifs de données.

— **Représentation compacte et expressive des modèles** : Grâce à l'espace de Hilbert, un petit nombre de qubits permet de représenter un très grand espace de configurations.

— **Applications directes à la cryptographie et à la détection d'intrusion** : Notamment à travers des algorithmes comme Grover ou Shor, ou l'usage de circuits quantiques dans des discriminants (ex. QGANs).

3.4.1.3 Introduction aux QGANs : concept et intérêt

Les *Quantum Generative Adversarial Networks* (QGANs) représentent une extension hybride des GANs traditionnels, combinant des réseaux neuronaux classiques avec des circuits quantiques paramétrés. Dans une telle architecture, le générateur reste généralement un réseau dense classique, tandis que le discriminateur repose sur un circuit quantique capable de traiter les données dans un espace de Hilbert plus riche. Cette hybridation permet d'exploiter les avantages respectifs de l'apprentissage profond et des propriétés de la mécanique quantique. Les QGANs ont pour objectif principal de générer des données synthétiques simulant des attaques réalistes, tout en s'appuyant sur la capacité du discriminateur quantique à identifier des motifs subtils dans des jeux de données déséquilibrés. Contrairement aux modèles classiques, les circuits quantiques permettent de représenter des fonctions de décision plus complexes avec un nombre de paramètres réduit, ce qui favorise une meilleure généralisation dans le contexte de détection d'intrusions rares, notamment dans les environnements dynamiques comme les réseaux VANETs[41].

3.4.1.4 Composants fonctionnels d'un QGAN

Un Quantum Generative Adversarial Network (QGAN) repose sur une architecture hybride combinant des éléments de l'apprentissage profond et des circuits quantiques paramétrés. Cette combinaison permet de capturer des structures complexes dans les données tout en exploitant les propriétés de la mécanique quantique. Les principaux composants de cette architecture sont décrits ci-dessous[42].

Circuits quantiques paramétrés (PQC) Les circuits quantiques paramétrés sont au cœur du QGAN. Il s'agit de circuits composés de portes quantiques dont les paramètres (généralement des angles de rotation) sont ajustés pendant l'entraînement. Ces circuits jouent un rôle similaire aux couches d'un réseau de neurones classique, mais dans un espace de Hilbert beaucoup plus riche. L'optimisation de ces paramètres permet d'adapter le comportement du discriminateur ou du générateur en réponse aux données.

Encodage des données classiques (Angle Embedding) Avant de traiter des données classiques avec un circuit quantique, il faut les encoder dans un état quantique. Une méthode couramment utilisée est l'*Angle Embedding*, qui consiste à convertir chaque caractéristique en un angle, ensuite appliqué à des portes de rotation comme $R_Y(\theta)$ ou $R_Z(\theta)$ sur les qubits correspondants. Cette étape est cruciale pour assurer une bonne expressivité du modèle quantique.

Mesure et fonction de perte À la fin du circuit quantique, les qubits sont mesurés (généralement en base Z), produisant des probabilités qui représentent la sortie du discriminateur. Ces probabilités sont ensuite utilisées pour calculer une fonction de perte, comme la *Binary Cross-Entropy*, qui guide l'optimisation des paramètres. L'optimisation se fait par rétropropagation à l'aide d'algorithmes adaptés aux circuits quantiques (ex. méthode des gradients paramétriques).

Plateformes d'exécution Les QGANs peuvent être implémentés sur des *simulateurs quantiques* (comme ceux proposés par PennyLane, Qiskit, ou Cirq) ou, de manière expérimentale, sur du *hardware quantique réel* (ex. IBM Quantum, Rigetti, IonQ). Le choix dépend du niveau de précision requis et de la complexité du modèle. Les simulateurs offrent un environnement plus stable pour l'expérimentation, tandis que les processeurs quantiques permettent d'explorer la faisabilité pratique des QGANs sur des dispositifs physiques.

3.4.1.5 Vers une cybersécurité adaptative pour les VANETs

Dans le contexte dynamique et distribué des réseaux VANETs, l'utilisation des QGANs s'inscrit dans une logique de co-évolution stratégique inspirée de la théorie des jeux : un générateur classique apprend progressivement à produire des intrusions réalistes et difficiles à détecter, tandis que le discriminateur quantique renforce continuellement sa capacité à identifier ces comportements malveillants. Cette interaction adversariale conduit à l'émergence d'un système de détection (IDS) adaptatif, capable de réagir face à des attaques nouvelles ou non vues. L'approche QGAN se révèle particulièrement efficace lorsque les intrusions sont rares, les flux de données instables en raison de la mobilité des véhicules, et lorsque les modèles doivent conserver une performance élevée tout en évoluant en temps réel. Elle offre ainsi un cadre robuste pour bâtir une cybersécurité proactive et contextuelle, parfaitement adaptée aux environnements à haute variabilité comme les VANETs. Cette partie théorique constitue donc le socle de notre contribution et introduit naturellement la section suivante (3.4.2), où l'implémentation concrète de cette approche est présentée pour la détection d'attaques Blackhole dans un environnement simulé.

3.4.2 Implémentation de l'approche QGAN pour la détection d'intrusions

Après avoir posé les bases théoriques, nous entrons dans l'implémentation concrète de notre approche. Cette section décrit l'architecture du modèle, les étapes de génération de données synthétiques, leur intégration dans un classifieur MLP, et l'évaluation des performances obtenues.

3.4.2.1 Justification et objectifs

Les réseaux génératifs adversariaux (GAN) ont déjà démontré leur efficacité pour générer des données synthétiques permettant de rééquilibrer des jeux de données fortement déséquilibrés. Toutefois, lorsqu'il s'agit de modéliser des comportements malveillants rares ou subtils, comme certaines attaques dans les réseaux VANETs, les GAN classiques présentent plusieurs limitations. Ces limites tiennent notamment à la complexité des fonctions de décision apprises par les discriminateurs classiques, souvent incapables de capturer avec précision des anomalies fines dans des contextes hautement dynamiques.

Afin de pallier ces limitations, nous proposons une approche innovante basée sur les Quantum Generative Adversarial Networks (QGAN), dans laquelle seul le discriminateur est quantique, tandis que le générateur reste un réseau neuronal classique. L'intérêt de cette architecture hybride réside dans la capacité du discriminateur quantique à explorer des espaces de représentation plus riches grâce à la superposition et à l'interférence quantique. Cette expressivité renforcée permet d'améliorer la capacité de distinction entre données normales et malveillantes, en particulier pour des attaques complexes telles que l'attaque Blackhole.

L'objectif principal de cette approche est donc d'utiliser un discriminateur quantique pour mieux évaluer la qualité des exemples synthétiques générés et renforcer la détection d'intrusions dans des scénarios où les attaques sont rares ou camouflées. En produisant des distributions d'apprentissage plus équilibrées et plus représentatives, notre méthode vise à accroître les performances d'un classifieur supervisé en termes de précision, de rappel et de robustesse.

3.4.2.2 Architecture du modèle

L'architecture du QGAN se compose de deux blocs :

— **Le générateur classique** : un réseau dense alimenté par un bruit aléatoire, conçu pour produire des échantillons représentant des comportements malicieux (attaques Blackhole).

— **Le discriminateur quantique** : un circuit à 4 qubits implémenté via PennyLane et PyTorch. Les entrées sont encodées par des angles (*AngleEmbedding*), suivies de couches d'intrication (*BasicEntanglerLayers*), et mesurées pour obtenir une sortie binaire via une couche dense classique.

Cette structure hybride permet au modèle d'explorer des régions de l'espace de données difficiles à capturer avec des approches purement classiques. L'architecture globale du modèle est illustrée dans la figure 3.5, qui met en évidence les différentes étapes de traitement entre le générateur et le discriminateur.

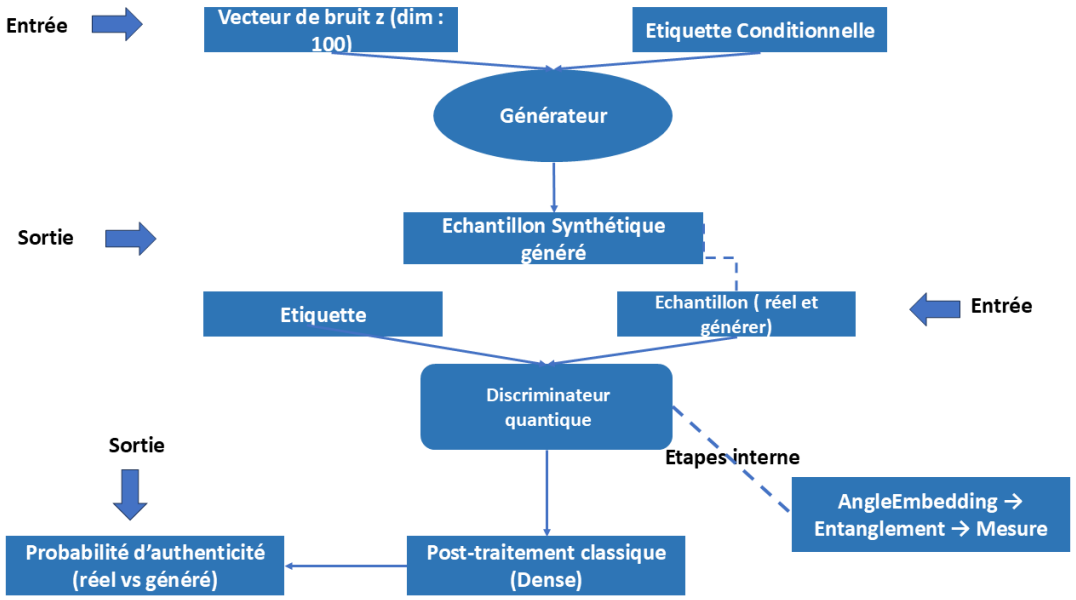


FIGURE 3.5 – Architecture du QGAN : couplage d'un générateur classique et d'un discriminateur quantique

3.4.2.3 Entraînement du modèle QGAN

L'entraînement du QGAN suit la même logique que celle des GAN traditionnels, mais avec une composante quantique dans le discriminateur. Chaque itération se déroule selon trois étapes : génération d'un batch d'échantillons synthétiques, évaluation par le discriminateur quantique, et mise à jour des paramètres du générateur selon le feedback reçu.

Le processus a été mené sur **500 époques** avec une taille de mini-lot de **32**, en utilisant la fonction de coût *Binary Cross-Entropy* et l'optimiseur *Adam*. Cette stratégie permet d'affiner progressivement la qualité des exemples générés, en exploitant les propriétés quantiques pour obtenir une distribution plus expressive des attaques.

3.4.2.4 Génération et enrichissement des données

Une fois le modèle convergé, le générateur produit **1 000 échantillons synthétiques** simulant des comportements de type Blackhole. Ces exemples sont ensuite fusionnés avec les données réelles, formant un nouveau jeu d'entraînement enrichi. Ce rééquilibrage améliore la représentativité de la classe minoritaire et prépare le classifieur MLP à des cas plus variés.

3.4.2.5 Classification avec MLP

Le jeu de données enrichi, généré à l'aide du QGAN, est ensuite utilisé pour entraîner un **perceptron multicouche (MLP)** conçu pour la détection d'intrusions. Ce classifieur est structuré autour de trois couches successives : une première couche dense composée de 128 neurones avec une fonction d'activation ReLU, suivie d'une deuxième couche dense de 64 neurones également activée par ReLU, et enfin une couche de sortie contenant 2 neurones avec une activation Softmax, adaptée à une classification binaire (normal vs attaque). Afin d'assurer

la robustesse et la capacité de généralisation du modèle, plusieurs techniques de régularisation sont mises en œuvre, notamment la validation croisée, le early stopping pour éviter le surapprentissage, ainsi qu'une pondération des classes destinée à compenser le déséquilibre du jeu de données. Ce cadre d'apprentissage permet au MLP d'apprendre efficacement à distinguer des intrusions variées, même en présence de bruit ou de variabilité dans les données simulées.

3.4.2.6 Évaluation et Résultats

L'efficacité du couple QGAN, MLP a été évaluée à l'aide d'un jeu de test stratifié. Les résultats confirment l'apport du générateur quantique dans la diversification des exemples d'attaque, ce qui améliore sensiblement la détection des comportements malicieux, tel que illustré dans le tableau 3.4.2.6.

Classe	Accuracy	Précision	Rappel	F1-score
Bénin	0.94	0.95	0.95	0.95
Blackhole	0.83	0.80	0.82	0.82
Général	0.9250	0.8342	0.7981	0.8157

TABLE 3.4 – Performances du modèle QGAN + MLP

Ces résultats montrent que le modèle hybride permet non seulement de compenser le déséquilibre des classes, mais aussi d'améliorer la précision globale du système de détection d'intrusion dans un environnement aussi critique que les VANETs. L'introduction de l'informatique quantique dans le processus de génération avec un QGAN constitue une innovation de rupture dans notre architecture. Ici, un générateur classique est combiné à un discriminateur quantique implémenté à l'aide de circuits paramétriques sur 4 qubits. Le générateur a été entraîné pendant 500 époques, ce qui, bien que moins long que pour le cGAN, était justifié par les contraintes computationnelles liées à la simulation quantique sur machine classique. Les résultats sont très prometteurs, avec une accuracy de 92.5%, un rappel de 83.42 %, et un score F1 de 81.57 %. Si ces chiffres sont légèrement inférieurs à ceux obtenus avec le cGAN, ils traduisent néanmoins une meilleure généralisation sur des exemples plus diversifiés, en particulier grâce à la capacité des circuits quantiques à explorer des distributions complexes avec un nombre réduit de paramètres. Il est important de noter que les performances légèrement inférieures au cGAN s'expliquent par une durée d'entraînement plus courte, mais aussi par la relative nouveauté des architectures quantiques hybrides, encore en phase de maturation. Toutefois, la qualité des résultats obtenus montre que l'intégration du QGAN ouvre des perspectives solides pour la détection d'intrusion dans des environnements dynamiques et incertains comme les VANETs.

3.5 Discussion générale des résultats

Les résultats obtenus à travers les trois approches évaluées mettent en évidence la richesse et la complémentarité des stratégies explorées pour la détection d'intrusions dans les réseaux VANETs. L'utilisation directe du discriminateur comme classifieur constitue une solution légère et peu coûteuse en calcul, révélant une certaine capacité du modèle à capter des régularités, mais au prix d'une efficacité limitée dans la détection des attaques. À l'opposé, l'approche par

cGAN offre les meilleures performances globales, notamment grâce à une génération conditionnelle riche et un entraînement profond permettant une excellente différenciation des comportements malicieux. Enfin, l'intégration du QGAN, bien qu'encore expérimentale, s'affirme comme une solution innovante, capable d'atteindre des résultats compétitifs tout en offrant une meilleure généralisation dans des contextes de données rares ou complexes. Ainsi, si le cGAN reste pour l'instant la solution la plus performante, le QGAN représente une voie prometteuse pour les systèmes de détection de demain, en particulier dans les environnements dynamiques, distribués et soumis à de fortes incertitudes comme les VANETs. Une hybridation future entre génération conditionnelle et circuits quantiques pourrait tirer parti des forces des deux mondes pour construire des systèmes encore plus robustes et intelligents.À terme, ces modèles pourraient être combinés à des technologies embarquées sur véhicule, avec des puces quantiques miniaturisées ou des services cloud quantiques, pour une détection d'intrusion temps réel dans des environnements réels.

Conclusion

Dans ce chapitre, nous avons proposé plusieurs approches innovantes pour la détection des attaques de type Blackhole dans les réseaux VANETs. Après avoir formalisé l'interaction entre l'attaquant et le défenseur à l'aide de la théorie des jeux, nous avons exploré différentes stratégies de classification, allant de l'utilisation directe du discriminateur comme classifieur à des architectures plus avancées basées sur les GANs, notamment le cGAN et le QGAN. Les résultats expérimentaux ont démontré que l'augmentation ciblée du jeu de données, qu'elle soit classique ou quantique, améliore significativement les performances des modèles supervisés. En particulier, l'approche combinant un cGAN avec un MLP s'est révélée particulièrement efficace pour équilibrer les classes et améliorer la détection des intrusions. Ces résultats valident la pertinence de notre cadre théorique et ouvrent la voie à des mécanismes de défense plus intelligents et adaptatifs dans les environnements VANETs.

Conclusion générale et travaux futures

Ce mémoire s'est inscrit dans une démarche de recherche appliquée visant à améliorer la sécurité des réseaux véhiculaires ad hoc (VANETs) face à des attaques ciblées, notamment l'attaque Blackhole. Nous avons mobilisé des outils issus de l'intelligence artificielle, du deep learning et de la théorie des jeux pour construire un système de détection d'intrusion hybride, à la fois adaptatif, stratégique et technologiquement innovant.

À travers les différents chapitres, nous avons progressivement mis en place une architecture complète intégrant un cGAN classique, un QGAN quantique, et un classifieur MLP, permettant à la fois de résoudre le problème d'équilibrage de données et d'améliorer la robustesse de détection. La modélisation des interactions attaquant-défenseur par la théorie des jeux a permis d'introduire une dimension stratégique et réaliste à notre système, en simulant une co-adaptation continue entre les deux entités.

L'intégration des circuits quantiques à travers le discriminateur du QGAN a également constitué une avancée conceptuelle, illustrant comment les propriétés de la mécanique quantique peuvent enrichir les modèles classiques d'IA. En associant des approches computationnelles avancées avec une structure d'apprentissage compétitif, notre contribution vise à poser les bases d'un système de cybersécurité proactif, capable de s'adapter aux environnements dynamiques des VANETs.

Ce travail ouvre ainsi plusieurs pistes d'amélioration et d'approfondissement. Tout d'abord, une optimisation plus poussée des architectures GAN, notamment par des mécanismes de régularisation ou des structures plus profondes, permettrait une modélisation plus fine des comportements malveillants. Ensuite, l'exploration de modèles quantiques avancés, tels que les réseaux de neurones quantiques profonds (QDNN), représente une évolution prometteuse pour dépasser les limites actuelles des QGANs, aussi bien en diversité d'échantillons qu'en efficacité computationnelle. Une approche hybride, combinant les forces des discriminateurs classiques, des cGANs et des QGANs, pourrait également améliorer la robustesse globale, en réduisant les faux positifs et négatifs grâce à des techniques d'agrégation adaptative. Par ailleurs, l'extension de la méthodologie à d'autres types d'attaques, comme les attaques Sybil, renforcerait la polyvalence du système. Enfin, l'intégration de la théorie des jeux stochastique dans la modélisation des interactions pourrait enrichir la flexibilité stratégique de l'IDS, en tenant compte de l'incertitude et de l'évolution temporelle des comportements adverses. L'ensemble de ces perspectives s'inscrit dans une vision à long terme de conception de systèmes de détection intelligents, proactifs et adaptatifs.

En somme, ce mémoire démontre la complémentarité entre IA, quantique et théorie des jeux dans le domaine de la cybersécurité appliquée aux VANETs, et ouvre la voie à des recherches encore plus ambitieuses dans les systèmes intelligents du futur.

Bibliographie

[1] Zekri, D. (2013). Aggregation and extraction of knowledge in inter-vehicle networks. Polytechnic University of Hauts-de-France..researchgate.net

[2] Aboelnasr, M., & Abdelbaki, N. (2021). A comprehensive survey on Vehicular Ad Hoc Networks (VANET). In A.-E. Hassanien, K.-C. Chang, & M. Tang (Eds.), Advanced Machine Learning Technologies and Applications (pp. 736–749). Springer. https ://doi.org/10.1007/978-3-030-69717-4_69

[3] Li, J., Xia, W., Cui, L., & Shu, L. (2021). A hierarchical trust-based and privacy-preserving authentication scheme in VANETs. IEEE Access, 9, 130241–130253. https ://doi.org/10.1109/ACCESS.2021.3113357

[4] Kakarla, J., Azees, M., Kumar, N., & Chilamkurti, N. (2020). A secure and efficient framework for VANET with fog computing. Future Generation Computer Systems, 108, 539–548. https ://doi.org/10.1016/j.future.2020.03.024

[5] Mehboob, F., Usman, M., Khalid, S., & Alazab, M. (2021). A lightweight and efficient authentication scheme for VANETs using ECC and hash chain. PeerJ Computer Science, 7, e633. https ://doi.org/10.7717/peerj-cs.633

[6] Sharma, P. K., Park, J. H., & Wahab, A. W. A. (2021). Secure and efficient communication scheme in intelligent transportation systems. IEEE/CAA Journal of Automatica Sinica, 8(3), 547–558. https ://doi.org/10.1109/JAS.2021.1003905

[7] Arena, F., Pau, G., & Severino, A. (2020). A Review on IEEE802.11p for Intelligent Transportation Systems. Journal of Sensor and Actuator Networks, 9(2), 22. https ://doi.org/10.3390/jsan9020022

[8] Dutta, A., Samaniego Campoverde, L. M., Tropea, M., & De Rango, F. (2024). A comprehensive review of recent developments in VANET for traffic, safety & remote monitoring applications. Journal of Network and Systems Management, 32, Article 73. https ://doi.org/10.1007/s10922-024-09853-5

[9] Cao, L., Yin, H., Hu, J., & Zhang, L. (2021). Performance analysis and improvement on DSRC application for V2V communication. In IEEE 92nd Vehicular Technology Conference (VTC2020-Fall), 1–6.

[10] Sabira, Z., & Amine, A. (2021). PrOMor : A proposed prototype of V2V and V2I for crash prevention in the Moroccan case. International Journal of Innovative Science and Research Technology, 6(1), 200–207.

[11] Giovanardi, A., & Mazzini, G. (2022). Field measurements on DSRC vs 5G-V2X performance in V2I and V2V scenarios. Vehicular Communications, 38, Article 100539. https ://doi.org/10.1016/j.vehcom.2022.100539

[12] Yusuf, M., Lee, D., & Zhang, Y. (2024). Vehicle-to-Pedestrian safety systems in smart cities : A survey. Transportation Research Part C : Emerging Technologies, 157, Article 104153. https ://doi.org/10.1016/j.trc.2023.104153

[13] Molina-Masegosa, R., & Gozalvez, J. (2017). LTE-V for sidelink 5G V2X vehicular communications : A new 5G technology for short-range vehicle-to-everything communications. IEEE Vehicular Technology Magazine, 12(4), 30–39. https ://doi.org/10.1109/MVT.2017.2740335

[14] Abdel Hakeem, S., Omar, M., & Elsayed, A. (2021). Vehicular Ad-hoc Networks (VANETs) : A survey on routing protocols and applications. Alexandria Engineering Journal, 60(1), 287–305. https ://doi.org/10.1016/j.aej.2020.09.013

[15] Cunha, F., Villas, L., Boukerche, A., Maia, G., Viana, A., Mini, R. A. F., & Loureiro, A. A. F. (2016). Data Communication in VANETs : Survey, Applications, and Challenges. Ad Hoc Networks. Disponible sur Elsevier

[16] Ali, I., Daeinabi, A., & Rahbar, A. G. (2022). VANETs for smart transportation : Recent advances and future directions. Vehicular Communications, 34, Article 100453. https ://doi.org/10.1016/j.vehcom.2021.100453

[17] Talebifard, P., & Boukerche, A. (2021). Challenges of vehicular ad hoc networks in highly dynamic environments. Computer Communications, 176, 33–45. https ://doi.org/10.1016/j.comcom.2021.05.017

[18] Zhou, Z., Tang, F., & Jin, H. (2022). Security and privacy in vehicular ad hoc networks : Challenges and solutions. IEEE Communications Surveys & Tutorials, 24(1), 1–27. https ://doi.org/10.1109/COMST.2021.3119939

[19] Nguyen, T. H., Zhuang, W., & Toh, C. K. (2021). A cost-effective roadside infrastructure deployment strategy for vehicular networks. Vehicular Communications, 28, Article 100313. https ://doi.org/10.1016/j.vehcom.2020.100313

[20] Abboud, K., Omar, H. A., & Zhuang, W. (2022). Interworking of 5G and vehicular networks : A comprehensive survey. IEEE Transactions on Vehicular Technology, 71(2), 1234–1257. https ://doi.org/10.1109/TVT.2022.3145169

[21] Yuan, Y., Wang, F. Y., & Zhang, L. (2021). Blockchain-based VANETs : A survey. Future Generation Computer Systems, 128, 109–122. https ://doi.org/10.1016/j.future.2021.10.001

[22] Ali, A., Ayub, M., Iqbal, M., & Mahmood, K. (2023). A comprehensive taxonomy and survey on security threats in vehicular ad hoc networks (VANETs). Computer Science Review, 49, 100535. https ://doi.org/10.1016/j.cosrev.2023.100535

[23] Alsharif, M. H., Kim, J., & Kim, J. H. (2021). Secure and efficient communication techniques for 5G-enabled vehicular ad hoc networks (VANETs) : A survey. Vehicular Communications, 27, 100284. https ://doi.org/10.1016/j.vehcom.2020.100284

[24] Jiang, X., & Zhang, J. (2021). Cryptography and Privacy in Vehicular Communication Networks. University of Waterloo Thesis.

[25] oshizawa, T., Singelée, D., & Muehlberg, J. T. (2022). A survey of security and privacy issues in V2X communication systems. arXiv. https ://doi.org/10.48550/arXiv.2208.14674

[26] Alladi, T., Chamola, V., Sahu, N., Venkatesh, V., Goyal, A., & Guizani, M. (2022). A comprehensive survey on the applications of blockchain for securing vehicular networks. Ad Hoc Networks, 137, 102980.

[27] Billah, M., Mehedi, S. T., Anwar, A., Rahman, Z., & Islam, R. (2022). A systematic literature review on blockchain-enabled federated learning framework for Internet of Vehicles. arXiv preprint, 2022.

[28] Rahmani, Z., Barbosa, L.S., & Pinto, A.N. (2023). Quantum privacy-preserving service for secure lane change in vehicular networks. IET Quantum Communication, 4(3), 103–111.

[29] Chi, C., Wang, Y., Tong, X., Siddula, M., & Cai, Z. (2022). Game theory in Internet of Things : A survey. IEEE Internet of Things Journal, 9(14), 12125–12146. https ://doi.org/10.1109/JIOT.2021.3133669

[30] Sharifani, K., & Amini, M. (2023). Machine learning and deep learning : A review of methods and applications. World Information Technology and Engineering Journal, 10(7), 3897–3904. https ://doi.org/10.2139/ssrn.4458723

[31] Fillières-Riveau, G., Favreau, J.-M., Barra, V., & Touya, G. (2020). Génération de cartes tactiles photoréalistes pour personnes déficientes visuelles par apprentissage profond. Revue internationale de géomatique, 30(1–2), 105–126. https ://doi.org/10.3166/rig.2020.00104

[32] Mohamed Nabil, Abdelmajid Hajam, Omar Boutkhoum, Abdelkrim Haqiq, ”Game Theory Application for Misbehavior Detection and Prediction in VANET : Review and Challenges”, International Journal of Computer Networks and Applications (IJCNA), 10(3), PP : 469-482, 2023, DOI : 10.22247/ijcna/2023/221903.

[33] Subba, B., Biswas, S., & Karmakar, S. (2018). A game theory based multi layered intrusion detection framework for VANET. Future Generation Computer Systems, 82, 12–28. https ://doi.org/10.1016/j.future.2017.12.008

[34] Wang L, Zhou W, Xu H, Li L, Cai L and Zhou X (2023) Research on task offloading optimization strategies for vehicular networks based on game theory and deep reinforcement learning. Front. Phys. 11 :1292702. doi : 10.3389/fphy.2023.1292702

[35] Hamza, L., Yousfi, M., & Bounehar, L. (2024) Partially Observable Stochastic Game for Analysing Complex Attacks in IoT Networks. Journal of Cyber Security and Mobility. p. 1039-1060, 2024.

[36] Phull, N., Singh, P., Shabaz, M., & Sammy, F. (2022). Enhancing vehicular ad hoc networks' dynamic behavior by integrating game theory and machine learning techniques for reliable and stable routing. Security and Communication Networks, 2022, 1–11. https ://doi.org/10.1155/2022/4108231

[37] Asadi, M. Detecting IoT botnets based on the combination of cooperative game theory with deep and machine learning approaches. J Ambient Intell Human Comput 13, 5547–5561 (2022). https ://doi.org/10.1007/s12652-021-03185-x

[38] Zebboudj, S., Djoudi, H., Lalaoui, D. et al. Authenticated semi-quantum key distribution without entanglement. Quantum Inf Process 19, 77 (2020). https ://doi.org/10.1007/s11128-019-2573-2

[39] Shu, J., Zhou, L., Zhang, W., Du, X., & Guizani, M. (2020). Collaborative intrusion detection for VANETs : A deep learning-based distributed SDN approach. IEEE Transactions on Intelligent Transportation Systems. Advance online publication. https ://doi.org/10.1109/TITS.2020.3027390

[40] Schuld, M., & Petruccione, F. (2021). Machine learning with quantum computers (2nd ed.). Springer. https ://doi.org/10.1007/978-3-030-17801-6

[41] Lloyd, S., Schuld, M., Ijaz, A., Izaac, J., & Killoran, N. (2020). Quantum embeddings for machine learning. Nature Reviews Physics, 2(10), 538–550. https ://doi.org/10.1038/s42254-020-0190-9

[42] Benedetti, M., Lloyd, E., Sack, S., & Fiorentini, M. (2019). Parameterized quantum circuits as machine learning models. Quantum Science and Technology, 4(4), 043001. https ://doi.org/10.1088/2058-9565/ab4eb5

[43] Wei, Y., Jang-Jaccard, J., Sabrina, F., Singh, A., Xu, W., & Camtepe, S. (2021). Ae-mlp : A hybrid deep learning approach for ddos detection and classification. IEEE Access, 9, 146810-146821.

[44] Chicco, D., & Jurman, G. (2020). The advantages of the Matthews correlation coefficient (MCC) over F1 score and accuracy in binary classification evaluation. BMC genomics, 21, 1-13.

Résumé

Les réseaux véhiculaires ad hoc (VANETs) jouent un rôle central dans les Systèmes de Transport Intelligents (STI) en facilitant la communication entre véhicules (V2V) et entre véhicules et infrastructures (V2I). Toutefois, leur nature ouverte et dynamique les rend vulnérables à diverses cybermenaces, notamment les attaques de type Blackhole. Pour renforcer la détection d'intrusions (IDS) dans ces environnements, nous proposons une approche hybride combinant le Machine Learning (ML), le Deep Learning (DL) et la théorie des jeux. Cette approche repose sur l'utilisation de deux architectures génératives : un Conditional Generative Adversarial Network (cGAN) et un Quantum GAN (QGAN), ce dernier exploitant les principes de l'informatique quantique tels que la superposition et l'intrication. Les données synthétiques générées permettent d'équilibrer le jeu de données et d'entraîner un Multi-Layer Perceptron (MLP) performant. En modélisant l'interaction entre l'attaquant (générateur) et le défenseur (MLP) comme un jeu à somme non nulle, notre solution améliore la robustesse et l'adaptabilité des systèmes IDS face aux attaques évolutives dans les VANETs.

Mots-clés : VANET, cybersécurité, IDS, Deep Learning, GAN, QGAN, MLP, théorie des jeux.

Abstract

Vehicular ad hoc networks (VANETs) play a central role in Intelligent Transport Systems (ITS), facilitating communication between vehicles (V2V) and between vehicles and infrastructure (V2I). However, their open and dynamic nature makes them vulnerable to a variety of cyberthreats, including blackhole attacks. To enhance intrusion detection (IDS) in these environments, we propose a hybrid approach combining Machine Learning (ML), Deep Learning (DL) and game theory. This approach is based on the use of two generative architectures : a Conditional Generative Adversarial Network (cGAN) and a Quantum GAN (QGAN), the latter exploiting quantum computing principles such as superposition and entanglement. The synthetic data generated enables the dataset to be balanced and a high-performance Multi-Layer Perceptron (MLP) to be trained. By modeling the interaction between attacker (generator) and defender (MLP) as a non-zero-sum game, our solution improves the robustness and adaptability of IDS systems in the face of evolving attacks in VANETs.

Keywords : VANET, cybersecurity, IDS, Deep Learning, GAN, QGAN, MLP, game theory.