UNIVERSITÉ DU QUÉBEC

MÉMOIRE PRÉSENTÉ À
L'UNIVERSITÉ DU QUÉBEC À TROIS-RIVIÈRES

COMME EXIGENCE PARTIELLE
DE LA MAÎTRISE EN MATHÉMATIQUE ET INFORMATION APPLIQUÉES

PAR
DIPA DIALLO

# DÉVELOPPEMENT D'UN MODÈLE DE PRÉDICTION DES ATTAQUES DOS SUR LES RÉSEAUX VÉHICULAIRES ÉLECTRIQUES V2G

Avril 2023

# Remerciement

Je rends grâce au tout-puissant Allah, qui m'a permis d'être là où je suis aujourd'hui.

Je remercie ma famille qui s'est sacrifiée pour que j'aie un lendemain meilleur.

Je remercie également mon directeur de recherche, le Professeur Amar Bensaber, Boucif, qui n'a ménagé aucun effort durant tout mon parcours universitaire. Il a su répondre à mes attentes grâce à son expertise et son professionnalisme.

Je tiens également à exprimer ma gratitude envers les évaluateurs de mon mémoire, pour leur temps, leur expertise et leur feedback constructif. Leurs commentaires ont grandement contribué à améliorer mon travail et à rendre mon mémoire encore plus solide.

Cette maîtrise a été pour moi une expérience enrichissante et valorisée par la rencontre de toutes ces personnes qui ont ajouté une corde à mon arc, tant sur le plan éducatif que social.

# Résumé

Les Stations de Recharge de Véhicules Électriques (EVCS) sont nécessaires pour assurer le déploiement fiable des véhicules électriques. Cependant, la communication bidirectionnelle et les flux d'alimentation qui facilitent la fonctionnalité du réseau V2G peuvent également faciliter les attaques des cybercriminels. La protection de la confidentialité est donc devenue un défi majeur pour le développement des réseaux V2G.

Pour faire face à ce défi, nous avons proposé un nouveau système de Détection d'Intrusion (IDS) basé sur l'apprentissage automatique pour détecter les attaques de Deni de Service (DoS) dans les EVCS. Nous avons analysé les techniques existantes pour traiter les problèmes d'attaque DoS et de protection de la vie privée dans le réseau V2G. Les algorithmes de classification ont été implémentés en python avec la distribution Anaconda.

Les résultats montrent que notre IDS a atteint une précision de détection de 98%. Cela permet d'améliorer la fiabilité du réseau V2G pour les utilisateurs et de mieux protéger les EVCS contre les attaques de Deni de Service.

DIPA DIALLO BOUCIF AMAR BENSABER

# Abstract

Electric Vehicle Charging Stations (EVCS) are necessary to ensure the reliable deployment of electric vehicles. However, the bidirectional communication and power flows that enhance the functionality of the V2G network can also make it easier for cybercriminals to attack. Therefore, privacy protection has become a major challenge for the development of V2G networks.

To tackle this challenge, we have proposed a new Intrusion Detection System (IDS) based on machine learning to detect Denial of Service (DoS) attacks in EVCS. We analyzed existing techniques to address DoS attack and privacy protection problems in the V2G network. The classification algorithms were implemented in python using the Anaconda distribution.

The results show that our IDS has achieved a detection accuracy of 98%.
This improves the reliability of the V2G network for users and better protects the EVCS against Denial of Service attacks.

# Table des matières

# Liste des tableaux

# Table des figures

# Liste des acronymes

**ANFIS** Adaptive Neuro-Fuzzy Inference System

**ANN** Réseau de neurone artificiel

**ATT** Variable Attaque

**CICIDS2017** Canadian Institute for Cybersecurity Intrusion Detection Set 2017

**DDoS** Attaque de déni de service distribué

**DNN** Réseau de neurones profonds

**DoS** Deni de Service

**ECU** Electronic Control Unit

**EVCS** Stations de Recharge de Véhicules Électriques

**EVSE** Équipements de recharge pour véhicules électriques

**IDS** Intrusion System Detection

**IEC** International Electrotechnical Commission

**IoT** Sécurité de l'internet des objets

**IPS** Système de prévention d'intrusion

**KDD Cup 99** Knowledge Discovery in Database

**MiM** Man-in-the-Middle

**NB** Naive Bayes

**NB ISCX 2012** éseau de données publiques pour l'évaluation de la détection d'intrusion (ISCX) de l'Université du Nouveau-Brunswick (UNB) en 2012

**NSL-KDD** Network Security Lab-KDD Cup 99 dataset

**SDN** Software-Defined Networking

**SG** Smart Gird

**SVM** Support Vector Machine

**V2G** Vehicule-to-Grid

**VE** Véhicule Électrique Rechargeable

# Liste des symboles

$alpha$ poids associé au classificateur faible

$f(x_i)$ classe prédite pour l'échantillon $i$

$h_m$ poids de l'échantillon $i$

$i$ index utilisé pour parcourir les échantillons de donnés

$log_e$ ajuste les poids des échantillons à chaque étape de l'entraînement

$m$ poids pour un classificateur

$N$ nombre total d'échantillons

$w_i$ poids de l'échantillon $i$

$x_i$ représente une observation ou un échantillon du jeu de données $i$

$y_i$ poids de l'échantillon $i$

# Chapitre 1

# Introduction

Les enjeux climatiques ont incité les gouvernements, les entreprises et les chercheurs à agir pour réduire les émissions de gaz à effet de serre. Pour répondre à cette inquiétude croissante, les chercheurs travaillent sur de nouvelles options pour un avenir vert et durable. La transition des véhicules à essence vers des véhicules électriques au cours de la dernière décennie a suscité un grand intérêt en ce qui concerne les défis et les problèmes liés à la réduction de la pollution. Les réseaux électriques évoluent également, passant de systèmes de distribution unidirectionnelle vers des systèmes de distribution intelligents bidirectionnels connectant de nombreux périphériques en continu. Les véhicules électriques (VE) ont besoin d'énergie pour fonctionner, ils doivent donc se connecter au réseau électrique pour charger et décharger leur énergie, ce qui est appelé Vehicle-to-Grid (V2G). Les véhicules électriques peuvent être connectés à des bornes de recharge publiques ou résidentielles. La sécurité, la confidentialité, l'authentification et les protocoles de communication doivent être pris en compte dans le réseau V2G. Les véhicules électriques et les bornes de recharge intelligentes échangent de nombreuses informations, ce qui a suscité des questions de sécurité. Pour cela, le réseau V2G doit être fiable et sécuritaire pour les utilisateurs. Plusieurs travaux ont été proposés pour améliorer la sécurité du V2G en détectant

les attaques ([5], [6], [7]). La plupart des attaques mentionnées sont théoriques et ne sont jamais mises en pratique en raison de la difficulté à trouver des bancs d'essai. Cependant, les menaces sont réelles, il est donc important d'étudier et de développer de nouvelles stratégies de sécurité pour protéger le réseau V2G. Les réseaux véhiculaires électriques (V2G pour Vehicle-to-Grid) sont des systèmes qui permettent aux véhicules électriques de communiquer avec le réseau électrique et de fournir de l'énergie à celui-ci lorsque cela est nécessaire. Les V2G peuvent être utilisés pour aider à stabiliser le réseau électrique en répondant aux fluctuations de la demande en énergie et pour stocker de l'énergie excédentaire produite par les sources d'énergie renouvelable. Les réseaux V2G font face à plusieurs menaces qui peuvent compromettre leur fonctionnement et leur sécurité. Parmi les menaces on peut citer : la menace de cybersécurité, la menace de la sécurité physique, la menace de la sécurité énergétique, etc. Dans ce travail, nous avons traité les problèmes de cybersécurité. En effet les attaques informatiques peuvent compromettre la communication entre les véhicules électriques et le réseau électrique et altérer les données de charge et de décharge de l'énergie.

Pour remédier à ces menaces, plusieurs mesures de sécurité sont mises en place pour protéger les réseaux V2G :

— Mise en place de protocoles de communication sécurisés pour protéger les données de charge et de décharge de l'énergie contre les attaques informatiques.

— Mise en place de mécanismes de sécurité physique pour protéger les véhicules électriques contre le vol et les dommages.

— Mise en place de procédures de surveillance et de gestion des perturbations pour garantir la fiabilité et la sécurité de la fourniture d'énergie.

— Mise en place de procédures de maintenance et de vérification régulière pour garantir la sécurité électrique des véhicules électriques.

Il est important de noter que la sécurité des réseaux V2G est un domaine en constante évolution et de nouvelles mesures de sécurité peuvent être développées et mises en place pour répondre à de nouvelles menaces. Les systèmes de détection d'intrusion

(IDS) sont des outils utilisés pour détecter et signaler les activités malveillantes sur un réseau ou un système informatique. Pour cela, l'apprentissage automatique peut être utilisé pour détecter les anomalies dans les réseaux en utilisant des algorithmes de détection d'anomalies. L'idée est de former un modèle sur des données normales de réseau, puis d'utiliser ce modèle pour détecter des comportements anormaux dans les données en temps réel. Les algorithmes d'apprentissage automatique populaires pour la détection d'anomalies incluent les réseaux de neurones profonds, les arbres de décision, les algorithmes de clustering, etc. L'apprentissage automatique peut être utilisé pour détecter les anomalies dans les réseaux en utilisant des algorithmes de détection d'anomalies. Dans [8] les auteurs ont proposé un système de détection d'anomalies basé sur l'apprentissage en profondeur. Ce système utilise un réseau neuronal profond pour analyser les données de trafic réseau en temps réel, ce qui lui permet de détecter avec précision les comportements inhabituels et les anomalies dans les réseaux Software-Defined Networking (SDN). Grâce à cette détection précoce, il est possible de prévenir les attaques et les menaces potentielles. L'utilisation de l'apprentissage automatique pour détecter les anomalies dans les réseaux est une approche prometteuse pour renforcer la sécurité des réseaux véhiculaires électriques V2G. Les algorithmes de détection d'anomalies basés sur l'apprentissage automatique, tels que les réseaux de neurones profonds, peuvent offrir des performances supérieures à celles des méthodes traditionnelles basées sur des règles ou des seuils fixes.

## 1.1 Généralités sur les réseaux électriques V2G

Les réseaux électriques V2G (Vehicle to Grid) sont une application de la technologie de stockage d'énergie qui utilise les batteries des véhicules électriques pour fournir de l'énergie au réseau électrique. Cela permet non seulement de stocker l'excès d'énergie produit par les sources renouvelables, mais aussi de réduire les coûts d'énergie en utilisant les batteries des véhicules pour compenser les pics de demande

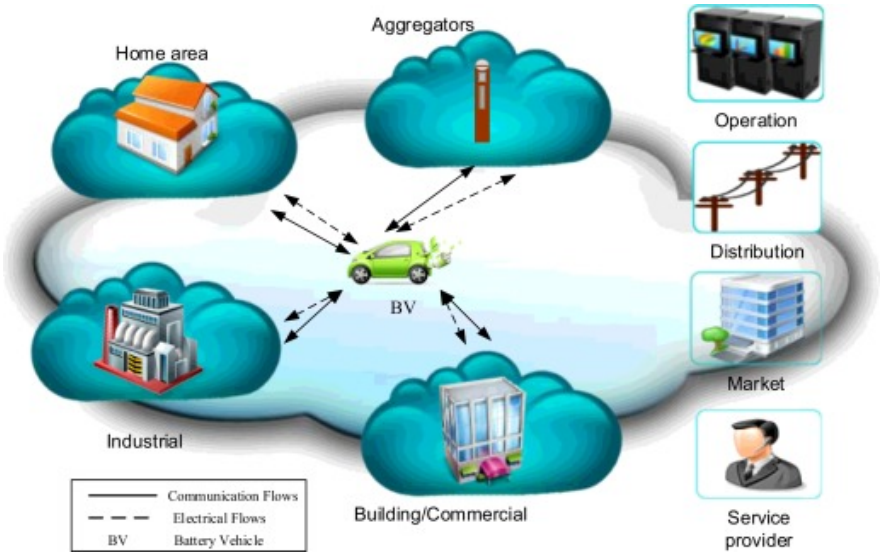


FIGURE 1.1 – V2G[1]

sur le réseau. Les réseaux V2G sont également considérés comme une solution pour améliorer la flexibilité et la fiabilité du système électrique en permettant aux batteries des véhicules de fournir de l'énergie en cas de besoin. Cependant, la technologie V2G n'est encore qu'au stade de la mise en œuvre pilote et il reste encore beaucoup de défis à relever, notamment en ce qui concerne la compatibilité des véhicules et des infrastructures électriques, la tarification et les questions de sécurité. La Figure 1.1 présente l'environnement V2G.

Les défis de sécurité auxquels le réseau véhiculaire électrique V2G fait face sont nombreux et comprennent l'intégrité des données, la sécurité du système électrique, la sécurité des véhicules électriques, la sécurité physique des systèmes de recharge, la confidentialité des données et l'interopérabilité des systèmes. Au cours de ce travail de recherche, nous avons mis l'accent sur l'intégrité des données, la confidentialité et l'interopérabilité des systèmes pour garantir la sécurité du réseau véhiculaire électrique V2G. Il existe plusieurs acteurs impliqués dans le développement et la mise en œuvre du réseau V2G, comme indiqué dans la Figure 1.2. Parmi ces acteurs, on peut citer :

— Les constructeurs de véhicules électriques : Ils développent des véhicules équi-

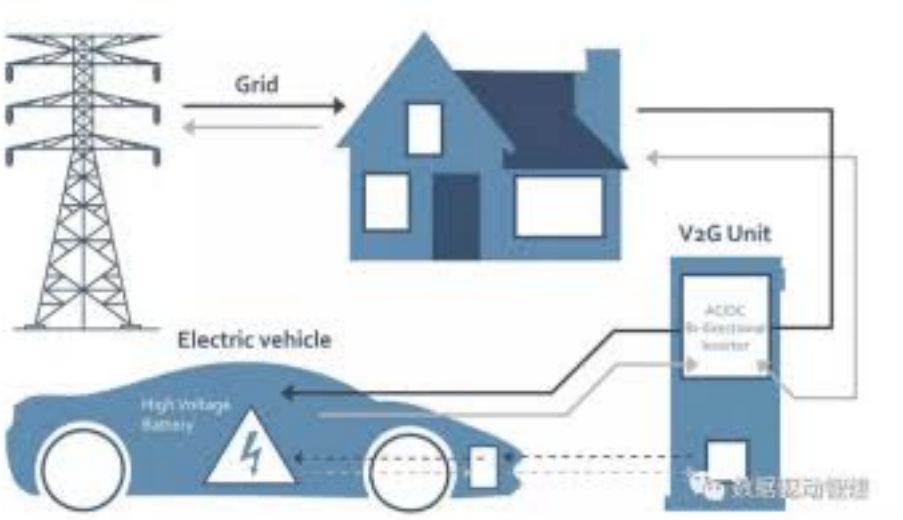


FIGURE 1.2 – Acteurs du V2G [2]

pés de la technologie V2G et sont responsables de la production de véhicules compatibles V2G.

— Les fournisseurs de réseau d'alimentation électrique : Ils fournissent l'infrastructure nécessaire pour connecter les véhicules électriques à leur réseau électrique.

— Les fournisseurs de solutions V2G : Ils développent des solutions logicielles et matérielles pour faciliter la communication entre les véhicules électriques et les réseaux électriques.

— Les entreprises d'énergie : Elles utilisent le V2G pour gérer la demande et l'offre d'énergie sur le réseau électrique.

— Les utilisateurs finaux : Ce sont les propriétaires de véhicules électriques qui peuvent être rémunérés pour la participation au V2G en fournissant de l'énergie stockée dans leur véhicule.

— Les bornes de recharge : Ce sont des équipements destinés à recharger les véhicules électriques, elles peuvent être publiques ou privées. Il est important de s'assurer que les bornes de recharge soient sécurisées et fiables pour garantir une expérience de recharge agréable pour les utilisateurs de véhicules électriques.

Ce travail nous a permis d'examiner en profondeur le réseau V2G, en mettant

en lumière les différents acteurs impliqués ainsi que les défis de sécurité auxquels il est confronté. La communication entre ces différents acteurs, en particulier entre le véhicule et la borne de recharge, est assurée grâce au protocole ISO/IEC 15118.

Les normes IEC 61850 et ISO/IEC 15118 sont les principales normes utilisées pour garantir une communication fiable dans les réseaux véhiculaires électriques V2G. Pour ce travail, la norme ISO 15118 a été privilégiée, car elle est largement adoptée et spécifique aux réseaux V2G, et elle permet les échanges de données bidirectionnels entre les différents acteurs du réseau.

## 1.2 La norme ISO 15118

La norme ISO 15118 [4] définit les protocoles de communication pour la recharge électrique bidirectionnelle (V2G) des véhicules électriques. Elle définit les interactions entre le véhicule électrique, la borne de recharge et les infrastructures réseau nécessaires pour un processus de recharge efficace et sécurisé. La norme couvre les aspects techniques de la communication, tels que les protocoles de communication, la gestion de la sécurité, la gestion des données et la compatibilité entre différents systèmes. Elle est un outil clé pour garantir l'interopérabilité des systèmes V2G pour une utilisation efficace et sécurisée de l'électricité à partir des véhicules électriques.

Créée par l'Organisation internationale de normalisation (ISO) pour spécifier les exigences de communication et de sécurité pour les systèmes de recharge de véhicules électriques (V2G). La première partie est publiée en 2012 et a pour objectif de standardiser les interactions entre les véhicules électriques et les bornes de recharge. La norme ISO 15118-1 est divisée en trois parties pour définir le protocole de communication dans les réseaux de recharge de véhicules électriques :

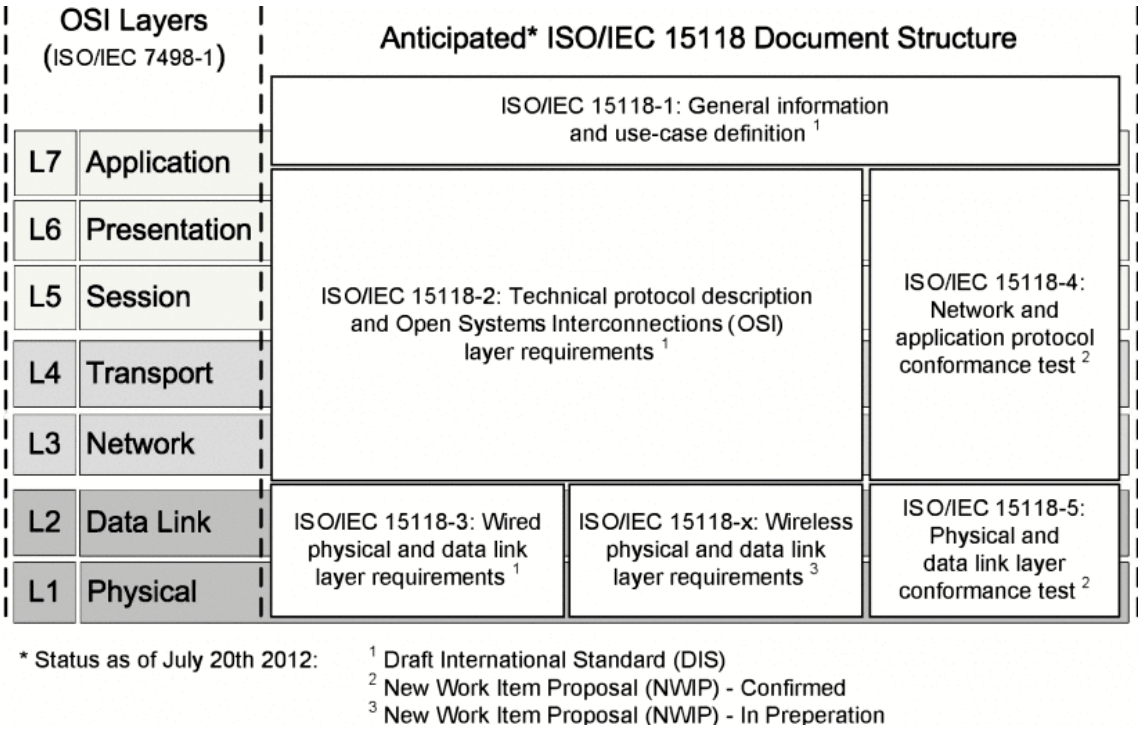


FIGURE 1.3 – ISO/IEC 15118

— La première partie définit les fonctionnalités et les échanges de données entre les véhicules électriques et les bornes de recharge.

— La deuxième partie définit les procédures pour la communication sécurisée entre les deux parties, ce qui inclut l'authentification, la signature numérique et l'encryptage.

— La troisième partie définit les spécifications pour la mise en œuvre et les tests de conformité à la norme.

Les trois parties collaborent ensemble afin de garantir un protocole de communication normalisé et fiable pour les réseaux de recharge V2G, comme expliqué dans la Figure 1.3. La norme ISO 15118-2 définit le protocole de communication pour le transfert de données entre un véhicule électrique et une station de charge dans un système de recharge pour véhicules électriques. Cela inclut les messages pour la demande de charge, la négociation de la puissance de charge et la conclusion de la transaction de charge. La norme ISO 15118-2 qui est une amélioration de la norme ISO 15118-1

définit également les sécurités nécessaires pour garantir la confidentialité et l'intégrité des données durant la communication entre le véhicule et la station de charge. Enfin, elle décrit les mécanismes pour les mises à jour logicielles des systèmes impliqués dans le processus de charge.

La norme ISO 15118 est un standard mondial pour les systèmes de recharge de véhicules électriques, qui facilite la coopération entre les différents acteurs du secteur automobile et énergétique pour développer des solutions de recharge sûres, fiables et interopérables.

## 1.3 Contexte général et problématique de recherche

### 1.3.1 Contexte général

Le V2G (Vehicle-to-Grid) est un système qui permet à un véhicule électrique de se connecter au réseau électrique et d'échanger de l'énergie électrique avec celui-ci. Ce système fait partie du smart-grid (grille électrique intelligente), qui est un réseau électrique intelligent offrant une communication bidirectionnelle et une meilleure protection de l'environnement. Différents acteurs sont impliqués dans le V2G, tels que les véhicules électriques, les fabricants de véhicules, les fournisseurs d'énergie et les opérateurs de réseau. Toutefois, le réseau V2G doit faire face à plusieurs défis en matière de sécurité, tels que l'intégrité des données, la sécurité du système électrique, la sécurité physique des systèmes de recharge, la confidentialité des données et l'interopérabilité des systèmes.

Pour gérer les communications entre les différents acteurs, la norme ISO 15118 est utilisée. Cette norme est spécifique au V2G et prend en charge les principes des échanges bidirectionnels dans le réseau V2G. Le protocole de communication de la

norme 15118 est divisé en deux parties, ISO 15118-1 et ISO 15118-2.

Dans ce contexte, ce travail de recherche a été mené pour proposer un système de détection d'intrusion visant à prédire les attaques dans le réseau V2G. L'objectif principal est d'améliorer la sécurité des réseaux informatiques en fournissant des solutions à un large éventail de problèmes liés à la sécurité du réseau.

### 1.3.2 Problématique de recherche

Le réseau électrique V2G (Vehicle to Grid) doit faire face à plusieurs défis liés à sa communication et à son architecture réseau, qui peuvent potentiellement compromettre la sécurité du système. Il est donc crucial d'identifier ces vulnérabilités afin de proposer des solutions adéquates et efficaces pour renforcer la sécurité du réseau V2G. Ainsi, la problématique de cette étude consiste à déterminer un système de détection d'intrusions pour prédire les attaques dans le réseau V2G, ainsi qu'à élaborer des stratégies de sécurité appropriées pour prévenir et contrer ces attaques.

## 1.4 Objectif du travail de recherche

L'objectif principal de ce travail est de développer un modèle de prédiction d'intrusion dans le réseau V2G (Vehicle to Grid) afin de renforcer sa sécurité en prévenant les menaces potentielles. Ce système de détection devra être capable de détecter les activités anormales et suspectes dans le réseau V2G en utilisant des algorithmes et des modèles appropriés. Enfin, l'évaluation de ce modèle permettra de mesurer son efficacité pour résoudre les problèmes de sécurité rencontrés dans le réseau V2G et de proposer des solutions pour renforcer sa sécurité.

La structure du mémoire est organisée en six chapitres principaux :

— Le chapitre 1 présente l'introduction, la problématique, les objectifs et la structure du mémoire.

— Le chapitre 2 décrit la revue de littérature du réseau électrique V2G en présentant les avantages et les défis liés à la sécurité.

— Le chapitre 3 examine les différents systèmes de détection d'intrusion et la démarche méthodologique mise en place pour atteindre l'objectif du travail.

— Le chapitre 4 porte sur la collecte de la base de données, les démarches, les simulations et les travaux effectués pour obtenir ces données.

— Le chapitre 5 examine les expériences menées pour évaluer les modèles proposés dans le chapitre 3 et compare les résultats finaux.

— Le chapitre 6 présente la conclusion en synthétisant les travaux effectués et les résultats obtenus, en identifiant également les perspectives potentielles pour l'avenir.

## 1.5 Conclusion

Ce chapitre offre une vue d'ensemble du réseau véhiculaire électrique, qui connaît une importance croissante dans le domaine de la mobilité électrique, tout en mettant en lumière les défis de sécurité auxquels il est confronté. Nous avons également abordé la norme ISO 15118, qui définit les exigences de communication pour les véhicules électriques, les véhicules hybrides rechargeables et les bornes de recharge. Dans ce travail, l'objectif principal est de proposer un système de détection d'intrusion pour renforcer la sécurité du réseau V2G. La méthodologie utilisée pour atteindre cet objectif consiste en une revue de la littérature sur le sujet, une modélisation et la mise en place d'algorithmes pour la détection d'intrusion. Des expériences ont été menées pour évaluer les modèles proposés et les résultats ont été comparés pour déterminer

leur efficacité. Enfin, ce mémoire souligne l'importance de la sécurité dans le réseau V2G et met en évidence les avantages d'un système de détection d'intrusion efficace pour prévenir les attaques potentielles et garantir la fiabilité du réseau.

# Chapitre 2

# État de l'art

Ce chapitre se consacre à la présentation de l'état de l'art en matière de modélisation de systèmes de détection d'intrusion. Pour atteindre les objectifs de ce travail de recherche, nous allons examiner les différentes approches utilisées pour la modélisation d'un système de détection d'intrusion. Nous allons également présenter une analyse des systèmes de détection d'intrusion existants et des méthodes proposées dans la littérature pour les améliorer. Cette analyse permettra de déterminer les tendances actuelles et les opportunités pour l'amélioration continue des systèmes de détection d'intrusion.

## 2.1 Revue de littérature

Cet état de l'art a pour objectif de présenter les différentes approches proposées dans la littérature pour renforcer la sécurité et la confidentialité des réseaux véhiculaires électriques V2G. Nous discuterons des différents problèmes de sécurité et de confidentialité associés aux réseaux V2G, ainsi que des enjeux et des défis à relever

pour garantir une utilisation sécurisée et fiable de ces réseaux. Enfin, nous passerons en revue les différentes approches proposées pour renforcer la sécurité et la confidentialité des réseaux V2G, en évaluant leurs avantages, leurs limites et leurs performances.

[4] La norme ISO 15118 est un ensemble de normes qui définit les exigences pour la communication entre les véhicules électriques (VE) et l'équipement d'alimentation en électricité (EVSE) pour les véhicules électriques (VE). Elle définit les protocoles de communication utilisés pour établir une connexion entre un VE et une borne de recharge, ainsi que les données échangées entre eux. Les normes ISO 15118 incluent des exigences pour les protocoles de sécurité pour protéger les données échangées lors de la charge, ainsi que pour la gestion de l'identité et de l'autorisation d'accès. La norme ISO 15118 est divisée en plusieurs parties qui couvrent différents aspects de la communication V2G, comme la communication entre véhicules et bornes de charge, la communication entre les différents acteurs d'un système V2G, et les protocoles utilisés pour établir une connexion sécurisée entre les équipements de charge et les véhicules. Elle couvre également les exigences pour les protocoles de communication pour l'échange de données entre les véhicules et les équipements de charge, et les protocoles pour l'autorisation d'accès à la charge et la facturation pour les services de charge. Il est important de noter que cette norme est en constante évolution pour prendre en compte les nouveaux développements et les nouvelles fonctionnalités liées à l'écosystème V2G.

La norme ISO 15118 a plusieurs avantages :

— • Elle permet une communication standardisée et sécurisée entre les véhicules électriques (VE) et les équipements de recharge pour véhicules électriques (EVSE), permettant ainsi une interopérabilité accrue entre les différents fabricants et les opérateurs de réseau.

— • Elle définit les protocoles de communication pour les interactions entre les véhicules et les bornes de charge, les données échangées et les fonctions de sécurité, ce qui contribue à protéger la vie privée et la sécurité des utilisateurs.

— • Elle inclut des exigences pour la gestion de la charge pour les systèmes de recharge bidirectionnelle, ce qui permet une meilleure utilisation de l'énergie stockée dans les batteries des véhicules électriques pour soutenir le réseau électrique.

— • Elle facilite l'expansion de la technologie des véhicules électriques en permettant une communication standardisée entre les véhicules et les bornes de charge, contribuant ainsi à favoriser la transition vers les véhicules propres.

En ce qui concerne les points faibles, la norme ISO 15118 est encore en cours de développement, et certains aspects pourraient être améliorés dans les prochaines révisions.

— La mise en œuvre peut être coûteuse et complexe pour les fabricants et les opérateurs de réseau.

— Il peut y avoir des défis pour garantir la sécurité des communications dans un système interconnecté, avec une vulnérabilité accrue aux cyberattaques.

Depuis la publication de la norme ISO 15118 part 2, d'autres avancées ont été faites pour tenir compte des nouvelles fonctionnalités et des développements liés à l'écosystème V2G. Cela inclut notamment des exigences pour les protocoles de communication pour l'échange de données entre les véhicules et les équipements de charge, et les protocoles pour l'autorisation d'accès à la charge et la facturation pour les services de charge.La norme ISO 15118 est en constante évolution pour s'adapter aux nouveaux développements et aux nouvelles fonctionnalités liées au réseau véhiculaire électrique V2G. La dernière mise à jour de la norme ISO 15118 est la version 2.0, publiée en 2020 pour remplacer la version précédente publiée en 2014. Cette mise à jour inclut des améliorations significatives en termes de sécurité, de fiabilité et de convivialité de l'interface de communication entre les véhicules électriques et les réseaux de recharge intelligents. Les principales améliorations comprennent :

— Amélioration de la sécurité de la communication, en ajoutant des protocoles de sécurité supplémentaires pour les communications de bout en bout et pour les certificats numériques.

— Renforcement de la protection de la vie privée, en incluant des exigences pour

la protection des données personnelles et des informations de localisation.

— Simplification des procédures de connexion, en permettant une identification automatique de l'EVSE et une négociation automatique des paramètres de charge.

— Ajout de nouvelles fonctionnalités pour la gestion de la charge, notamment la gestion de la charge bidirectionnelle et la gestion de la charge par priorité.

Ces améliorations visent à renforcer la sécurité, l'interopérabilité et la flexibilité des systèmes de communication V2G, tout en offrant de nouvelles fonctionnalités pour répondre aux besoins émergents du réseau V2G.

[9] Ce travail propose une analyse des menaces potentielles associées au protocole de charge Vehicle-to-Grid (V2G) ISO 15118, qui permet aux véhicules électriques de se connecter aux réseaux électriques intelligents pour échanger de l'énergie. Bao et al passent en revue les différentes étapes de la négociation de charge ISO 15118 et évaluent les menaces potentielles pour chaque étape, y compris la collecte et le stockage de données d'identification, l'échange de certificats numériques, la communication de données de charge et les attaques liées à la qualité de service. Ils proposent également des mesures de sécurité pour réduire les risques de ces menaces, notamment l'utilisation de mécanismes de chiffrement, de certificats numériques, de signatures numériques, de pare-feu et de restrictions d'accès. Cette étude est importante, car elle fournit une analyse détaillée des menaces liées aux protocoles de la norme ISO 15118 pour la recharge des véhicules électriques, en se concentrant sur les aspects de disponibilité, d'intégrité, d'authenticité et de confidentialité de la communication. Elle identifie les vulnérabilités potentielles de la norme, ce qui permet aux développeurs de prendre des mesures de sécurité pour les atténuer ou les éliminer. Elle met en évidence les hypothèses implicites dans la norme, qui peuvent ne pas être bien documentées, et souligne la nécessité de clarifier ces hypothèses pour améliorer la sécurité de la norme. En conclusion pour une amélioration potentielle que ce travail pourrait inclure :

— Une évaluation plus détaillée des risques associés aux vulnérabilités identifiées, afin de hiérarchiser les mesures de sécurité à prendre.

— Une évaluation de la faisabilité technique et économique des mesures de sécurité proposées pour atténuer les vulnérabilités identifiées.

— Une évaluation de l'impact des attaques potentielles sur les utilisateurs, les opérateurs de réseaux et les fournisseurs de services de recharge.

[10] Ce travail est une revue de la littérature qui explore les systèmes de détection d'intrusion de réseaux (IDS) basés sur les réseaux définis par logiciel (SDN) et les approches d'apprentissage automatique (machine learning). Sultana et al, examinent les avantages et les limites des différentes approches et techniques utilisées pour détecter les attaques sur les réseaux. Les avantages de l'approche SDN pour les IDS comprennent la possibilité de surveiller et de contrôler le trafic réseau à partir d'un point centralisé, facilitant ainsi la détection des anomalies et des intrusions. Les techniques d'apprentissage automatique, quant à elles, offrent la possibilité de détecter des attaques complexes et nouvelles, qui peuvent échapper aux méthodes traditionnelles de détection d'intrusion. Les auteurs soulignent également l'importance de la sélection de bonnes fonctionnalités pour l'apprentissage automatique, afin de garantir la qualité de la détection. Cependant, les limites des systèmes d'IDS basés sur SDN et l'apprentissage automatique comprennent des défis tels que la gestion de grands volumes de données, la sélection des paramètres optimaux pour les algorithmes de machine learning et la complexité de l'infrastructure requise pour déployer ces systèmes. Les auteurs soulignent également la nécessité de garantir la sécurité du contrôleur SDN, qui peut être une cible d'attaque pour les pirates informatiques. En résumé, cette étude montre que l'approche SDN et l'apprentissage automatique peuvent fournir des outils puissants pour la détection d'intrusions sur les réseaux, mais il est important de prendre en compte les limites et les défis de ces techniques pour garantir l'efficacité et la sécurité des systèmes de détection d'intrusions.

[11] Fouda et all, propose un schéma d'authentification pour assurer l'intégrité des messages dans le Vehicle-To-Gird. Le schéma proposé est adapté aux exigences des communications Smart Gird (SG) basées sur le protocole d'échange de clé Diffie-Hellman et le code d'authentification basé sur le hachage. Une analyse de sécurité du

schéma d'authentification de message a été proposée pour vérifier si les propriétés de sécurité requises peuvent être satisfaites.

— Le schéma proposé peut fournir une authentification mutuelle

— Le schéma proposé peut établir une clé partagée sémantique sécurisée dans l'environnement d'authentification mutuelle

— Le schéma proposé peut fournir un canal authentifié et crypté pour la transmission successive tardive

Les réseaux de communication existants basés sur IP, tels qu'Internet et le Smart Grid basé sur IP, sont confrontés à un énorme volume de données, tels que les attaques malveillantes, la relecture, l'analyse du trafic et les attaques DoS. Le schéma proposé ne protège pas le SG contre les attaques DoS.

[7] Dudek et all, présentent une nouvelle approche de communication entre véhicules électriques (VE) et bornes de recharge dans les réseaux de vehicle-to-gird (V2G). Cette approche, baptisée "V2G Injector", permet de transmettre des données à travers la ligne électrique qui alimente les VE et les bornes de recharge. Les auteurs décrivent en détail le fonctionnement de cette approche et présentent une évaluation de ses performances en termes de débit de transmission et de fiabilité de la communication. Ils montrent que V2G Injector permet d'établir une communication fiable entre les VE et les bornes de recharge, tout en offrant un débit de transmission satisfaisant. Leur travail apporte une contribution à la communication entre VE et bornes de recharge dans le réseau V2G en proposant une nouvelle approche basée sur l'utilisation de la ligne électrique. La démarche originale et les résultats encourageants pourraient inspirer d'autres travaux de recherche dans ce domaine.

[12] Dans ce travail, Roman et al. apportent une solution innovante pour les défis de sécurité rencontrés dans les réseaux V2G en proposant un protocole d'authentification basé sur l'appariement. Le protocole vise à résoudre les problèmes de complexité, de faible sécurité et de consommation de ressources des protocoles d'authentification existants en utilisant des techniques d'appariement sécurisées pour établir une com-

munication sécurisée entre le véhicule et le réseau. Les résultats des travaux expérimentaux montrent que le protocole présente des avantages en termes de coûts de calcul et de communication, tout en garantissant une authentification réussie. Cependant, il reste encore des défis à relever pour la mise en œuvre pratique de ce protocole et pour la résolution de certains problèmes liés à la sécurité des systèmes cyber-physiques. Il serait donc judicieux de continuer à explorer d'autres pistes pour améliorer la sécurité dans les réseaux V2G, notamment en explorant de nouvelles technologies et méthodes pour renforcer la sécurité des communications et pour protéger les identités des utilisateurs d'EV. En résumé, ce travail est un pas important dans la direction de la sécurisation des réseaux V2G en proposant un protocole d'authentification sécurisé avec des améliorations en termes de coûts computationnels et de communication. Les travaux futurs devraient se concentrer sur la mise en œuvre pratique de ce protocole et sur la résolution des défis restants liés à la sécurité des systèmes cyber-physiques.

[13] Dans cet article, Youssef Lahrouni et all s'intéressent aux attaques de type "denial of service" (DoS) dans les réseaux de véhicules autonomes (VANET). Ils proposent une approche basée sur l'utilisation de méthodes mathématiques pour mitiger ces attaques, qui visent à rendre indisponibles les services proposés par le réseau en saturant les canaux de communication. Les auteurs présentent une étude de cas portant sur l'application de la théorie des graphes pour détecter et contrer ces attaques de manière efficace. Ils montrent que cette approche permet de réduire significativement le risque d'interruptions de service dans le VANET. Leur travail apporte une contribution intéressante à la sécurisation des réseaux de véhicules autonomes en proposant une solution innovante pour lutter contre les attaques de type DoS. La démarche basée sur l'utilisation de méthodes mathématiques pourrait être étendue à d'autres contextes de sécurisation de réseaux de communication.

[14] Hyunsung Lee et al ont mis en place un système de détection d'intrusion appelé OTIDS (Offset Ratio and Time Interval based Intrusion Detection System, ou système de détection d'intrusion basé sur le ratio de décalage et l'intervalle de temps).

Ce modèle utilise des ratios de décalage et des intervalles de temps pour détecter les intrusions dans le réseau CAN (Controller Area Network, ou Réseau de contrôleur de zone). OTIDS envoie périodiquement des trames à distance et reçoit les messages de réponse des nœuds expéditeurs. En l'absence d'attaque, le rapport de décalage entre les demandes et les réponses a un temps fixe, mais en cas d'attaque, il varie. Ainsi, OTIDS peut détecter les intrusions et protéger le système contre les attaques potentielles. Cette approche a l'avantage d'être efficace dans la détection des attaques dans le réseau CAN, ce qui permet de garantir un niveau de sécurité supplémentaire. Cependant, l'inconvénient de cette méthode est que le temps de réponse peut être affecté par la charge du réseau, ce qui peut entraîner des fausses alertes ou des détections manquées. En outre, cette approche nécessite une période de formation pour identifier le rapport de décalage de référence, ce qui peut prendre du temps et des ressources supplémentaires.

[15] Attia et al, proposent une approche de détection d'intrusion pour les attaques sur les réseaux électriques intelligents. Les auteurs proposent un modèle d'architecture distribuée pour les systèmes de détection d'intrusion qui surveillent les consommateurs, les dispositifs de construction et les compteurs intelligents. Cette approche utilise une politique de détection basée sur des règles combinant des règles de détection temporelles et spatiales. Les auteurs ont testé cette approche sur un ensemble de données de réseau électrique intelligent pour évaluer son efficacité dans la détection des attaques. Les avantages de cette approche incluent une détection améliorée des attaques et une réduction des taux de faux positifs, grâce à l'utilisation de règles de détection temporelles et spatiales combinées. La méthode proposée est également distribuée, ce qui permet une surveillance plus efficace des différents composants du réseau. Cependant, l'approche nécessite une surveillance en temps réel, ce qui peut nécessiter des ressources supplémentaires pour les opérations de surveillance, et les résultats de la simulation doivent être validés par des tests sur le terrain pour confirmer son efficacité dans les conditions réelles.

[16] Sajjad Abedi et al, ont exploré les problèmes de sécurité auxquels les véhicules électriques sont confrontés dans le contexte des réseaux intelligents. Ils ont examiné certaines des méthodes de détection d'intrusion les plus récentes pour détecter les attaques, car la sécurité est un défi majeur pour la fiabilité et la disponibilité du système de recharge V2G (Vehicle-to-Grid). Parmi les défis de sécurité, les auteurs ont évoqué les problèmes de communication qui doivent être sécurisés de manière bidirectionnelle. Pour répondre à ces enjeux, ils ont classé les problèmes de sécurité dans le contexte de la communication V2G, qui relèvent notamment des protocoles de communication. La sécurité des communications est en effet essentielle pour garantir la confidentialité des données, l'authenticité des messages et la disponibilité du système. En somme, la sécurité est un enjeu clé pour la fiabilité et l'efficacité des systèmes de recharge V2G. Ils ont donc examiné les dernières méthodes de détection d'intrusion pour prévenir les attaques malveillantes, en se concentrant sur les problèmes de communication sécurisée. Leur étude contribue ainsi à mieux comprendre les défis liés à la sécurité des véhicules électriques et à identifier les domaines qui nécessitent une attention particulière.

[5] Angelos et al ont décrit une méthode pour détecter et identifier les anomalies dans la consommation d'énergie des clients dans les systèmes de distribution d'énergie. Les auteurs utilisent des techniques statistiques et d'apprentissage automatique sur les données de consommation d'énergie pour mettre en place cette méthode. Ils montrent que cette méthode est efficace pour détecter les anomalies avec une bonne fiabilité et pour les identifier avec une certaine précision. Ils utilisent un indicateur appelé taux d'assertivité pour mesurer l'exactitude de leur méthode. Les résultats obtenus montrent que cette méthode est prometteuse et pourrait être utilisée pour améliorer la fiabilité et l'efficacité des systèmes de distribution d'énergie. [17] J Autoun et all, ont effectué une étude théorique mettant en évidence les cybermenaces dans un système de tarification des différents acteurs ciblés. Ils ont catégorisé ces menaces et présenté une analyse des lacunes ainsi que des directives pour les futurs travaux de recherche dans les systèmes de recharge des véhicules électriques. Avec l'intérêt croissant pour

les véhicules électriques, il est crucial de concevoir des bornes de recharge fiables. Cela nécessite une compréhension plus approfondie des interactions entre les aspects cybernétiques et physiques au sein de la borne de recharge. Dans [18], Gottumukkala et al présentent une approche d'un système cyber-physique pour comprendre l'interaction de divers composants au sein d'un équipement de charge intelligent. Ils expliquent également les différents types de vulnérabilités et d'attaques possibles, ainsi que les approches pour améliorer la sécurité de ces équipements. Cependant, il est important de noter que les approches proposées par les auteurs pour améliorer la sécurité des bornes de recharge intelligentes peuvent ne pas être suffisantes pour faire face à toutes les formes d'attaques. De plus, il est crucial de continuer à surveiller et à améliorer la sécurité des équipements de recharge pour assurer une utilisation sûre et fiable des véhicules électriques.

[19] Cette étude présente un protocole de sécurité pour l'accord de clés légères et préservant la vie privée pour la communication entre les véhicules électriques et les infrastructures de recharge dans les réseaux V2G dans le contexte de l'Internet social des objets (SIoT). Shen et al, proposent un protocole se concentrant sur la préservation de la vie privée et la légèreté du processus de négociation de clé entre le VE et l'infrastructure de recharge, en utilisant des méthodes de chiffrement légères et des fonctions de hachage. Le protocole fournit également une sécurité contre les attaques de rejeu et de modification. Les avantages de cette étude sont la légèreté du protocole proposé et sa capacité à préserver la vie privée des utilisateurs. Il offre également une protection contre les attaques de rejeu et de modification. Cependant, certaines limites peuvent inclure le manque d'analyse de sécurité formelle du protocole proposé et le manque de comparaison avec d'autres protocoles existants. De plus, l'efficacité et la sécurité du protocole peuvent être affectées par les conditions du réseau et les capacités des dispositifs utilisés.

[20] Dans leur étude, Prak et al, ont démontré que le protocole proposé par Shen et al. en 2017 pour prévenir l'usurpation d'identité, la relecture et les attaques de

l'homme du milieu, tout en assurant une confidentialité de transmission parfaite et une authentification mutuelle sécurisée, n'était pas efficace contre les différentes attaques qu'ils ont proposées. Cependant, ils ont élaboré un protocole de gestion de clés basé sur des identités de groupe et des fonctions de hachage pour fournir une sécurité robuste et une gestion efficace des clés dans les réseaux V2G. Le nouveau protocole proposé offre plusieurs avantages. Tout d'abord, il est plus résistant aux attaques que le protocole précédent, car il utilise une clé dynamique et des algorithmes de hachage pour améliorer la sécurité. De plus, il assure une confidentialité de transmission et une authentification mutuelle sécurisée, ce qui garantit que seuls les utilisateurs autorisés peuvent accéder aux informations et contrôler les véhicules. Cependant, malgré ses avantages, le nouveau protocole présente également certaines limites. Par exemple, il peut nécessiter une plus grande quantité de ressources, telles que de la bande passante ou de la puissance de calcul, pour fonctionner correctement. De plus, il est possible que de nouvelles attaques puissent être développées à l'avenir qui pourraient compromettre la sécurité du protocole.

[21] Étant donné que les véhicules électriques (VE) doivent fournir leurs informations privées aux agrégateurs/serveurs lors de la charge/décharge à différentes stations de charge, la confidentialité des propriétaires de véhicules peut être compromise si les informations sont mal utilisées, tracées ou révélées. Le déplacement des véhicules électriques d'un réseau à un autre rend plus complexes la sécurité et la confidentialité en raison des entités non fiables dans les réseaux visiteurs. Sexana et all proposent un schéma d'authentification basé sur des certificats numériques pour garantir la sécurité des transactions de charge et de décharge entre les véhicules et les réseaux. Les auteurs abordent également les problèmes de sécurité dans les réseaux V2G et les défis liés à la mise en œuvre de systèmes d'authentification efficaces. Leur schéma améliore l'efficacité du système, contrecarre diverses attaques de sécurité et maintient l'intraçabilité, la confidentialité et l'anonymat de l'identité.

[22] Les auteurs de cette étude analysent les caractéristiques des informations confi-

dentielles dans les systèmes V2G afin de déterminer leur vulnérabilité aux attaques et de vérifier si ces informations sont exposées à des risques de divulgation. Pour cela, ils ont utilisé une technique de classification floue permettant de développer un système flou. Afin de démontrer l'efficacité et la performance de leur approche de classification floue, ils ont comparé les résultats obtenus avec ceux des techniques de classification Support Vector Machine (SVM) et Naive Bayes (NB). Cette étude présente ainsi une méthodologie innovante pour analyser la sécurité des informations confidentielles dans les systèmes V2G, en utilisant une approche de classification floue qui peut s'avérer très utile pour les experts en sécurité. Toutefois, les limites de cette étude résident dans le fait que les tests ont été effectués sur un seul ensemble de données, ce qui pourrait limiter la généralisation des résultats obtenus. [23] Su et al, proposent un schéma d'authentification pour les réseaux V2G qui garantit la confidentialité des informations sensibles telles que l'identité des utilisateurs et les données de charge des véhicules électriques. Le schéma d'authentification proposé utilise une combinaison de techniques de chiffrement et de hachage pour assurer la confidentialité et l'authenticité des données. Cette étude présente également une évaluation de la sécurité du schéma proposé en utilisant des outils formels de vérification et de simulation. Les avantages de cette étude sont la présentation d'un schéma d'authentification innovant qui garantit la confidentialité des informations sensibles et la sécurité des communications V2G. Ce schéma peut aider à renforcer la confiance des utilisateurs dans les réseaux V2G et à encourager l'adoption de véhicules électriques. Cependant, les limites de cette approche peuvent inclure la complexité de la mise en œuvre du schéma et la nécessité d'une infrastructure de clé publique pour la gestion des clés de chiffrement. En outre, l'article ne fournit pas d'analyse de la performance ou de l'efficacité du schéma proposé par rapport à d'autres approches existantes.

[24]Cette étude porte sur l'utilisation de la corrélation des événements pour réduire les faux positifs dans les systèmes de détection d'intrusion. Moughit et al. proposent une méthode qui consiste à analyser et corréler plusieurs événements pour identifier plus précisément les attaques réelles et ainsi réduire le nombre de faux positifs. Cette

méthode est importante, car elle permet de réduire la charge de travail des analystes de sécurité, d'améliorer la précision de la détection d'intrusion et de réduire les risques de fausses alarmes. Cependant, cette méthode peut être complexe, car elle nécessite une analyse approfondie pour identifier les relations causales entre les événements. De plus, elle peut entraîner des retards dans la détection d'attaques réelles, car elle nécessite une analyse plus approfondie des événements avant de déclencher une alerte.

[25] La sécurité de l'internet des objets (IoT) suscite un intérêt croissant dans plusieurs domaines tels que la médecine, la logistique, les villes intelligentes et l'automobile. Cependant, les menaces d'intrusion sur les réseaux IoT sont de plus en plus nombreuses et doivent être prises en considération. Dans cette optique, Hodo et al, ont proposé l'utilisation d'un réseau de neurones artificiels pour analyser les menaces pesant sur l'IoT et trouver des solutions à ces risques. Leur travail consiste à classifier les données normales et les menaces sur un réseau IoT à l'aide d'un algorithme de réseau de neurones artificiels. Les résultats expérimentaux ont montré que cet algorithme est capable de détecter avec succès diverses attaques DDoS/DoS. Les avantages de ce travail sont notamment la proposition d'une solution pour détecter les menaces sur les réseaux IoT à l'aide d'un réseau de neurones artificiels, ainsi que la capacité de l'algorithme ANN à détecter divers types d'attaques DDoS/DoS. Cependant, les limites de ce travail résident dans le fait que seules certaines attaques ont été prises en compte et que les performances de l'algorithme de réseau de neurones artificiels pourraient varier en fonction des types d'attaques ou des environnements spécifiques. En outre, la mise en œuvre d'un tel système nécessite une analyse approfondie des données et un ajustement régulier des paramètres pour garantir des résultats précis.

[26] Cet article présente une approche d'IDS (Système de Détection d'Intrusion) basée sur une ontologie pour surveiller les attaques définies. Shukla et al, proposent un modèle ontologique qui permet de représenter les informations des événements d'IDS et des données des attaques, pour aider à la prise de décision rapide et précise. Ils présentent également un algorithme de classification basé sur une ontologie pour la

détection d'intrusion, qui utilise une combinaison de techniques de classification telles que l'arbre de décision, le réseau bayésien, la régression logistique et les arbres de décision C4.5. Les avantages de cette approche sont notamment la capacité à représenter de manière formelle et structurée les connaissances relatives aux événements d'IDS et aux attaques, ce qui peut faciliter la détection d'intrusion. L'utilisation de l'algorithme de classification basé sur une ontologie permet également une prise de décision rapide et précise. Cependant, les limites de cette approche incluent la nécessité de développer et de maintenir l'ontologie, ainsi que le coût potentiellement élevé de sa mise en place. En outre, l'efficacité de l'algorithme de classification basé sur une ontologie dépend de la qualité de l'ontologie et de l'exactitude des données d'entraînement.

Cette étude propose une classification et une étude de différents systèmes de détection d'intrusion (IDS) utilisant des réseaux de neurones peu profonds et profonds. [27] Elike et al. commencent par présenter les définitions et les différentes catégories de réseaux de neurones, puis analysent les caractéristiques et les avantages de chaque type de réseau de neurones pour la détection d'intrusions. Ensuite, ils passent en revue différentes IDS qui ont utilisé des réseaux de neurones pour la détection d'intrusions et classent ces IDS en fonction de leur type de réseau de neurones. Les avantages de cette étude sont la présentation d'une classification claire et complètent des différents types de réseaux de neurones utilisés dans les IDS. Cette étude peut aider les chercheurs et les professionnels de la sécurité à mieux comprendre les différentes approches de détection d'intrusions basées sur des réseaux de neurones peu profonds et profonds. Cependant, cette étude présente des limitations et des défis qui n'ont pas été suffisamment discutés, tels que la nécessité de prendre en compte d'autres facteurs importants tels que le type de données d'entrée ou les algorithmes de formation utilisés dans la classification des IDS. De plus, la classification des différentes IDS est basée uniquement sur le type de réseau de neurones utilisé, ce qui peut limiter la pertinence de l'étude pour des applications spécifiques de détection d'intrusions. [28] Ce travail décrit un système de détection d'intrusion basé sur l'apprentissage profond pour les stations de recharge de véhicules électriques. Basnet et al, soulignent

la nécessité de protéger les stations de recharge contre les cyberattaques, qui peuvent potentiellement compromettre la sécurité du réseau électrique. Ils proposent une méthode basée sur l'apprentissage profond pour détecter les attaques à l'aide de données de trafic réseau capturées sur les stations de recharge. Le système utilise un réseau de neurones convolutifs (CNN) pour extraire les caractéristiques des données de trafic et un réseau de neurones entièrement connecté (FNN) pour classifier les données en attaque ou non-attaque. Les résultats expérimentaux montrent que le système proposé est efficace pour détecter les attaques et peut être utilisé pour protéger les stations de recharge de véhicules électriques contre les cyberattaques. Dans ce travail, ils ont testé leur système de détection d'intrusion (IDS) basé sur l'apprentissage en profondeur (deep learning) sur un ensemble de données réelles provenant d'une station de recharge de véhicules électriques en Chine. Les résultats ont montré que leur système est capable de détecter les intrusions avec une précision de $99,9\%$ et un taux de fausses alarmes inférieur à $0,1\%$. Le temps de détection moyen des intrusions était d'environ 2,2 secondes, ce qui est considéré comme rapide. Les auteurs ont également comparé les performances de leur IDS avec d'autres méthodes de détection d'intrusion basées sur des règles et des techniques d'apprentissage automatique, et ont montré que leur système d'apprentissage en profondeur surpassait ces autres méthodes en termes de précision et de taux de fausses alarmes.

[29] Le travail de Sainis et al, portent sur la classification de divers ensembles de données pour les IDS. Ils ont étudié plusieurs ensembles de données tels que KDD Cup 99 (Knowledge Discovery in Databases), NSL-KDD (Network Security Lab - KDD Cup 99 dataset), NB ISCX 2012 (réseau de données publiques pour l'évaluation de la détection d'intrusion (ISCX) de l'Université du Nouveau-Brunswick (UNB) en 2012), CICIDS2017 (Canadian Institute for Cybersecurity Intrusion Detection Set 2017) et ont utilisé différentes techniques de classification pour évaluer leur performance. Les techniques de classification utilisées comprennent l'arbre de décision, la régression logistique, le SVM, le KNN et le réseau de neurones artificiels. Les avantages de cette étude sont qu'elle fournit une évaluation comparative des performances

des différentes techniques de classification pour différents ensembles de données, ce qui peut aider à choisir la meilleure technique pour un IDS particulier. Il peut également être utile pour les chercheurs travaillant dans le domaine de la détection d'intrusions en leur fournissant un point de départ pour leurs travaux de recherche. En conclusion, les techniques de classification utilisées ne représentent pas toutes les méthodes disponibles pour la détection d'intrusions. De plus, l'étude ne fournit pas une analyse en profondeur des ensembles de données étudiés, limitant ainsi sa portée pour la recherche future. [30] Dans Höfer et al, proposent un protocole de recharge qui permet aux utilisateurs de recharger leur véhicule tout en protégeant leur identité et leurs informations de localisation. Le protocole utilise des clés publiques et privées pour chiffrer les informations de localisation de l'utilisateur et empêcher toute divulgation d'informations sensibles. Les auteurs ont également effectué des tests pour évaluer les performances de leur protocole de recharge et ont constaté qu'il était efficace et sécurisé. Ce travail présente plusieurs avantages :

— Protection de la vie privée : le travail propose des extensions modulaires du protocole ISO/IEC 15118 pour garantir une protection maximale de la confidentialité des utilisateurs lors de la recharge de leurs véhicules électriques.

— Sécurité : le protocole Popcorn utilise des techniques de chiffrement et de signatures numériques pour garantir la sécurité de la communication entre les véhicules et les infrastructures de recharge.

— Efficacité : le protocole Popcorn permet d'optimiser les coûts de facturation en minimisant les données échangées entre les véhicules et les infrastructures de recharge, tout en garantissant la fiabilité des transactions.

— Modularité : le protocole Popcorn est conçu pour être facilement intégrable dans les infrastructures de recharge existantes et peut être étendu pour prendre en compte de nouveaux besoins de sécurité et de confidentialité.

Le travail propose une solution innovante et efficace pour assurer la confidentialité et la sécurité de la recharge des véhicules électriques, tout en garantissant l'efficacité et la modularité du système.

[31] Ce travail traite de la détection d'intrusion dans les réseaux de véhicules automobiles en utilisant des réseaux de neurones profonds (DNN). Kang et al, proposent une architecture DNN capable de détecter les attaques sur le bus CAN (Controlled Area Network) qui est largement utilisé dans les systèmes de véhicules automobiles pour les communications inter-ECU (Electronic Control Unit). Les performances du système proposé ont été évaluées en utilisant un jeu de données CAN-intrusion comprenant des attaques sur le bus CAN.

Les résultats expérimentaux montrent que l'architecture DNN proposée atteint des performances élevées pour la détection d'attaques sur le bus CAN. Par contre les auteurs n'ont pas abordé la question de la généralisation de l'architecture DNN proposée à d'autres types d'attaques ou à d'autres types de réseaux de véhicules automobiles. La performance du système proposé peut être affectée par des facteurs tels que le taux de fausses alertes, la latence, le coût de calcul et la consommation d'énergie, qui doivent être pris en compte dans les applications pratiques.

"Adaptive Neuro-Fuzzy Inference System" ou " Système d'inférence neuro-floue adaptatif en français" (ANFIS), est un modèle d'apprentissage automatique qui combine des réseaux de neurones artificiels et des systèmes d'inférence flous, créé par Jang en 1993. Le principe de base de ANFIS est d'utiliser les règles de la logique floue pour définir les paramètres d'un réseau de neurones. En utilisant ces règles floues, ANFIS est capable de résoudre des problèmes complexes en prenant en compte les données d'entrée, en les pré-traitant via une approche floue, puis en les utilisant pour entraîner un réseau de neurones. Dans [32] Caroly et al, ont proposé un système d'inférence neuro-floue adaptatif (ANFIS) pour évaluer l'indice de sécurité dans un réseau vehiculaire ad-hoc (VANET). Leur travail constitue l'une des premières propositions pour la détection d'attaques dans ce type de réseau. Après l'entraînement du modèle sur les données, le système proposé par les auteurs a montré une bonne performance dans la prédiction des véhicules qui ne subissent pas d'attaques, ainsi qu'une petite marge d'erreur dans la détection des véhicules qui sont sous attaque. Cependant, les auteurs

précisent que la marge d'erreur reste acceptable pour garantir l'efficacité du système dans la prédiction d'attaques en utilisant l'indice de sécurité comme mesure de protection. En conclusion, le modèle proposé par les auteurs montre que l'utilisation de réseaux de neurones et de logique floue peut être utilisée pour obtenir un indice de sécurité comme mesure de protection et de prédiction d'éventuelles attaques. L'un des principaux avantages d'ANFIS, et cela s'applique également à ce travail, est sa capacité à combiner la logique floue pour le raisonnement avec la puissance de modélisation des réseaux de neurones. Le travail de Caroly et al sur l'utilisation d'un système d'inférence neuro-floue adaptatif (ANFIS) est l'une des premières propositions pour la prédiction d'attaques dans le réseau VANET. Les résultats obtenus dans cette étude montrent que l'utilisation de réseaux de neurones et de logique floue peut fournir un indice de sécurité précis pour la protection et la prédiction d'éventuelles attaques. Cependant, la conception d'un modèle ANFIS peut être complexe et nécessite une bonne compréhension des principes de la logique floue et des réseaux de neurones. De plus, l'ajustement des paramètres du modèle peut être difficile pour obtenir des résultats optimaux, ce qui peut nécessiter un temps d'entraînement plus long. Malgré ces défis, ANFIS reste un outil puissant pour la prédiction de la sécurité dans les réseaux VANET.

[1] Han et al, ont réalisé une étude exhaustive de la littérature de recherche sur les techniques de préservation de la confidentialité dans le réseau véhiculaire électrique V2G. Leurs travaux ont permis de recenser les problèmes déjà résolus dans la littérature, mais aussi de proposer des solutions novatrices pour les problèmes non résolus. Cette étude fournit donc une base solide pour la mise en place de solutions de préservation de la confidentialité dans le réseau véhiculaire électrique V2G, contribuant ainsi à améliorer la sécurité de ces réseaux.

[33] "The Basics of Hacking and Penetration Testing" est un livre qui explique de manière simple les concepts de base du piratage éthique et des tests de pénétration. L'auteur présente les outils et les techniques utilisés dans ce domaine, ainsi que les

méthodes pour protéger les systèmes contre les attaques. L'objectif de l'auteur est d'aider les professionnels de la sécurité informatique, les étudiants et les passionnés à acquérir les compétences nécessaires pour identifier et corriger les vulnérabilités de sécurité dans les systèmes informatiques. Ce travail a plusieurs avantages pour les professionnels de la sécurité informatique, notamment : une approche pratique pour enseigner les concepts d'hacking éthique et de test de pénétration. Il fournit des instructions étape par étape pour mener des tests de pénétration sur des systèmes et des réseaux. La planification et la configuration des tests de pénétration à l'exploitation de vulnérabilités et à la récupération de données. L'éthique et l'aspect légal de la sécurité informatique. Il insiste sur l'importance de suivre les lois et les réglementations en vigueur lors de la réalisation de tests de pénétration.

## 2.2 Défis de sécurité dans le V2G

Les défis de sécurité dans les réseaux V2G sont nombreux et complexes, car ils incluent des aspects tels que la confidentialité, l'intégrité, la disponibilité et l'authenticité des données, ainsi que la sécurité physique des dispositifs connectés. Les défis de sécurité peuvent également provenir des interactions entre les différents composants du réseau, tels que les véhicules électriques (VE), les bornes de recharge, les réseaux électriques et les systèmes de gestion des énergies renouvelables.

Parmi les défis de sécurité les plus importants, on peut citer :

— Attaques de type DoS (Denial of Service) et DDoS (Distributed Denial of Service), qui visent à rendre les systèmes indisponibles en surchargeant les ressources du système.

— Attaques Man-in-the-middle, où un attaquant intercepte et modifie les données transmises entre deux parties.

— Attaques liées à la sécurité physique, telles que le vol de batteries et les sabo-

tages.

— Problèmes de confidentialité des données sensibles, telles que les informations personnelles des utilisateurs, les données de localisation et les informations sur l'état de la batterie.

— Problèmes de fiabilité et d'intégrité des données, tels que les erreurs de transmission, les erreurs de mesure et les manipulations malveillantes.

Il est important de noter que les réseaux V2G peuvent également être vulnérables à d'autres types d'attaques, telles que les attaques de type phishing, les attaques de type malware et les attaques de type réseau. Pour faire face à ces défis de sécurité, il est important de mettre en place des solutions de sécurité appropriées, telles que des protocoles d'authentification sécurisés, des mécanismes de cryptage des données, des systèmes de détection d'intrusion, ainsi que des politiques de gestion de la sécurité. Les équipes de recherche et les développeurs travaillent constamment sur de nouvelles solutions pour améliorer la sécurité des réseaux V2G, mais il est important de poursuivre les efforts pour faire face aux défis en constante évolution de la sécurité.

## 2.3 Conclusion

La sécurité du réseau V2G est un enjeu majeur qui a suscité de nombreuses recherches et propositions de solutions ces dernières années. Les principales menaces auxquelles le réseau V2G est exposé incluent des problèmes de confidentialité, d'authentification, d'autorisation et de facturation pour la recharge des véhicules électriques. Plusieurs méthodologies, telles que les algorithmes de machine learning et de deep learning, ont été utilisées pour développer des systèmes de détection d'intrusion. Les résultats montrent que les IDS basées sur ces méthodologies ont tendance à fournir des résultats plus précis que les autres méthodologies. Cependant, il reste encore des défis à relever pour parvenir à une sécurité optimale du réseau V2G.

En conclusion, la revue de la littérature a montré que la sécurité dans les réseaux V2G est un enjeu important, car des types d'attaques potentielles, tels que les attaques DoS et Man-in-the-Middle, peuvent affecter les performances du réseau et menacer la confidentialité des communications. Il est donc nécessaire de mettre en place des mesures de sécurité efficaces pour protéger les réseaux V2G contre ces types d'attaques. Cela peut inclure l'utilisation de protocoles d'authentification sécurisés, l'analyse de sécurité et la détection des attaques, ainsi que la mise en place de mécanismes de défense pour atténuer les attaques en cas de détection. Pour conclure, on peut dire que la sécurité dans les réseaux V2G est un domaine en constante évolution, et des études supplémentaires sont nécessaires pour développer des solutions plus efficaces pour garantir la sécurité des communications dans ces réseaux.

# Chapitre 3

# Systèmes de détection d'intrusion et démarche méthodologique

Dans ce chapitre, nous présentons les concepts de base des systèmes de détection d'intrusion (IDS) et détaillons la méthodologie utilisée pour développer ces systèmes. Nous décrivons également le modèle de comportement du réseau V2G étudié dans ce travail et discutons des méthodes utilisées pour détecter les attaques potentielles et proposer des solutions pour y faire face.

Ainsi nous pourrons développer un système de détection d'intrusion efficace et adapté aux besoins du réseau V2G.

## 3.1 Généralité sur les systèmes de détection d'intrusion

Au cours de la dernière décennie, Internet et les systèmes informatiques ont connu une croissance exponentielle des problèmes de sécurité. Plusieurs études citées dans la revue de littérature de ce travail ont montré que le nombre d'intrusions et d'attaques avait augmenté de manière significative chaque année. Dans ce contexte, le réseau électrique véhiculaire (V2G) n'échappe pas aux menaces de sécurité, et différents types d'attaques peuvent être menés contre lui. Parmi ces attaques, on peut citer :

— Déni de service (DoS) : il s'agit d'une attaque qui vise à rendre un site Web ou un service inaccessible en envoyant un grand nombre de requêtes au serveur. Cela peut causer des problèmes pour les utilisateurs qui essaient d'accéder au site ou au service.

— Malware : il s'agit de logiciels malveillants qui peuvent endommager le V2G ou voler des données. Les types de malware comprennent les virus et les logiciels espions.

— L'attaque homme du milieu, également connu sous le nom de "man-in-the-middle", est une technique de piratage dans laquelle un intrus s'insère dans une communication entre deux parties et intercepte les données qui y sont transmises. L'intrus peut alors lire, modifier ou même remplacer ces données sans que les parties impliquées ne s'en rendent compte. Il existe de nombreuses variantes de cette attaque, mais elles ont toutes pour objectif d'intercepter les communications et d'y injecter du contenu malveillant ou trompeur. Il est important de prendre des mesures de sécurité pour protéger les communications contre les attaques homme du milieu, comme l'utilisation de chiffrement fort et de protocoles de sécurité fiables.

Une telle violation de la sécurité informatique, c'est-à-dire la confidentialité, l'intégrité et la disponibilité, peut avoir des conséquences graves, telles que des pertes

financières importantes ou la fuite de données sensibles. La sécurité du réseau est l'une des préoccupations majeures de l'ère moderne, et c'est pourquoi il est essentiel de mettre en place des mesures de sécurité efficaces, comme la mise en place de protocoles de sécurité rigoureuses. En effectuant plusieurs travaux de recherche, nous pouvons protéger nos réseaux et nos systèmes d'information contre les menaces en constante évolution.

Dans ce travail, nous avons entrepris une étude approfondie des techniques d'apprentissage automatique utilisées pour détecter les intrusions sur les réseaux informatiques. Pour cela, nous avons examiné plusieurs documents pertinents, tels que des articles de recherche et des rapports sur le sujet. Notre méthodologie consiste à sélectionner attentivement ces sources et à les analyser de manière critique afin de mieux comprendre les approches couramment utilisées dans ce domaine. Nous avons ainsi pu comparer les différentes approches et en tirer des conclusions sur leur efficacité pour la détection d'intrusions.

### 3.1.1 Systèmes de détection d'intrusion - IDS

Les systèmes de détection d'intrusion (IDS) sont des outils de sécurité conçus pour surveiller les activités des réseaux et des systèmes informatiques et détecter les comportements anormaux ou suspects qui pourraient indiquer une intrusion ou une tentative d'attaque. Ces systèmes peuvent être installés sur un ordinateur ou un réseau pour surveiller en temps réel les activités et envoyer une alerte en cas d'anomalie détectée.

Le réseau V2G (vehicle-to-grid) est un réseau de communication qui permet aux véhicules électriques de se connecter au réseau électrique et de fournir ou de recevoir de l'électricité. Le système de détection d'intrusion du réseau V2G est conçu pour surveiller les activités sur ce réseau et détecter les comportements anormaux ou suspects

qui pourraient indiquer une intrusion ou une tentative d'attaque. Les systèmes de détection d'intrusion du réseau V2G peuvent être installés sur les véhicules électriques et sur les infrastructures du réseau V2G (comme les stations de charge et les centres de contrôle du réseau). Ils surveillent les activités sur le réseau en temps réel et peuvent envoyer une alerte en cas d'anomalie détectée. Les systèmes de détection d'intrusion du réseau V2G sont généralement utilisés en conjonction avec d'autres mesures de sécurité, comme les pare-feux et les logiciels antivirus, pour protéger le réseau V2G contre les intrusions et les attaques. Ils jouent un rôle important dans la sécurité du réseau V2G et peuvent aider à prévenir les pertes financières et les dommages causés par les intrusions et les attaques.

La sécurité des réseaux est un sujet de recherche important de nos jours, face aux menaces croissantes qui pèsent sur cette sécurité. Bien que de nombreux travaux aient été réalisés sur les systèmes de détection d'intrusion (IDS), il reste encore des domaines importants à explorer. Dans le cadre de ce travail, nous avons fait une distinction claire entre les concepts d'intrusion, de détection d'intrusion, de système de détection d'intrusion et de système de prévention d'intrusion, en nous appuyant sur les travaux [6] de Bace et Mell (2001). Pour cela, nous allons définir ces distinctions en nous appuyant sur des sources de la littérature dans le chapitre 2 et en donnant des exemples concrets pour illustrer chaque concept.

— Intrusion : il s'agit de toute action visant à pénétrer de manière non autorisée dans un système informatique ou un réseau. L'intrusion peut être motivée par différents objectifs, comme le vol de données, la perturbation du fonctionnement du système ou la destruction de données.

— Détection d'intrusion : il s'agit de la détection de tentatives ou de réussites d'intrusion dans un système informatique ou un réseau. La détection d'intrusion peut être réalisée de manière passive (en surveillant les activités du système pour repérer les anomalies) ou active (en envoyant des requêtes spécifiques au système pour tester sa vulnérabilité).

— Système de détection d'intrusion (IDS) : il s'agit d'un outil de sécurité conçu

pour surveiller les activités des réseaux et des systèmes informatiques et détecter les comportements anormaux ou suspects qui pourraient indiquer une intrusion ou une tentative d'attaque. Les IDS peuvent être installés sur un ordinateur ou un réseau et surveillent les activités en temps réel.

— Système de prévention d'intrusion (IPS) : il s'agit d'un outil de sécurité conçu pour bloquer ou éliminer les intrusions dans un système informatique ou un réseau. Les IPS sont généralement installés sur les pare-feux et surveillent les activités du réseau en temps réel, bloquant ou éliminant les comportements anormaux ou suspects.

La cybersécurité est un domaine de plus en plus important qui vise à protéger les ordinateurs, les réseaux, les applications et les données contre les attaques et les accès non autorisés. Elle se compose de différentes technologies et processus, comme les pare-feux, les antivirus et les systèmes de détection d'intrusion (IDS). Ces derniers aident à identifier les utilisations non autorisées du réseau et à maintenir la disponibilité des services. Malheureusement, les menaces sur la sécurité des réseaux restent un sujet de recherche important de nos jours, ce qui rend la cybersécurité encore plus cruciale.

Les failles de sécurité peuvent être internes ou externes et compromettre la sécurité des systèmes informatiques et des réseaux. Pour lutter contre ces menaces, les analystes en sécurité informatique ont recours à différentes techniques de machine learning et de deep learning au cours des dernières années.

## 3.2 Définition du modèle et méthodologie

Dans ce travail, nous proposons un modèle d'IDS (Intrusion Detection System) qui sera utilisé pour classifier les données du réseau V2G afin de détecter les anomalies et maintenir la disponibilité, l'intégrité et la confidentialité des services. Notre modèle sera divisé en deux parties :

La première partie consiste à étudier l'interface de communication des véhicules électriques avec les bornes de recharge intelligente selon la norme ISO-15118.

La seconde partie vise à améliorer la première en permettant de classifier les données normales et les données potentiellement anormales. Cette partie nous permettra d'identifier plus efficacement les anomalies sur n'importe quel point du réseau et de trouver des solutions pour y faire face.

Il est important de prendre en compte un large éventail de types d'attaques lors de la mise en place d'un système de détection d'intrusion pour le réseau V2G, afin de garantir une couverture maximale contre les menaces potentielles. Notre étude abordera certaines attaques courantes qui peuvent être visées par un IDS dans le réseau V2G :

— Les attaques de type "homme du milieu" (man-in-the-middle), qui visent à intercepter les communications entre deux parties et à les modifier ou à les diffuser de manière non autorisée.

— Les attaques de type "déni de service" (DoS), qui visent à rendre indisponibles les services du réseau en envoyant un grand nombre de requêtes ou de paquets de données à un serveur ou à un réseau.

— Les attaques de type "injection de code" (code injection), qui visent à insérer du code malveillant dans un programme ou un système, afin de prendre le contrôle de ce dernier.

— Les attaques de type "phishing", qui visent à tromper les utilisateurs en leur faisant croire qu'ils sont en train de communiquer avec une personne ou une entreprise de confiance, alors qu'en réalité ils sont en train de donner des informations sensibles à des tiers malveillants.

— Les attaques de type "piratage de compte", qui visent à accéder à des comptes d'utilisateur sans autorisation en utilisant des techniques de devinette de mot de passe ou de "brute force.

## 3.3 Méthodologie

Un système de détection d'intrusion (IDS) est un outil de cybersécurité qui permet de surveiller et d'analyser en temps réel les activités du réseau V2G, afin de détecter les comportements anormaux et les attaques potentielles. Un IDS peut être configuré pour envoyer des alertes en cas de comportement suspect, permettant ainsi aux responsables de la sécurité de réagir rapidement pour protéger le réseau.

Les objectifs généraux et spécifiques d'un IDS pour le réseau V2G :

Objectif général :

— Améliorer la sécurité du réseau V2G en détectant et en prévenant les attaques et les accès non autorisés.

Objectifs spécifiques :

— Surveiller en temps réel les activités du réseau V2G.

— Analyser les comportements anormaux et les attaques potentielles.

— Envoyer des alertes en cas de comportement suspect.

— Protéger le réseau V2G contre les attaques de type "homme du milieu".

— Prévenir les fuites de données sensibles.

— Assurer la disponibilité et l'intégrité des services du réseau V2G.

— Protéger la confidentialité des données du réseau V2G.

Dans le cadre de ce travail, nous avons étudié les comportements de différents algorithmes de machine learning afin d'améliorer la sécurité des systèmes de détection d'intrusion (IDS). Cette étude avait pour objectif d'améliorer les capacités de détection et de prévention des intrusions.

1- Le support vector machine (SVM) est un algorithme de classification qui peut être représenté sous forme de schéma. Voici un exemple de schéma simplifié qui illustre

le fonctionnement d'un SVM :

- Les données d'entraînement sont chargées et préparées.
- Un hyperplan est sélectionné comme frontière de décision.
- Les données sont classées en fonction de leur position par rapport à l'hyperplan.
- Les données de test sont chargées et préparées.
- Les données de test sont classées en fonction de leur position par rapport à l'hyperplan.
- Les résultats sont évalués et le modèle est ajusté en fonction de la performance.

Ce schéma donne une vue d'ensemble du fonctionnement d'un SVM, mais il existe de nombreux autres aspects et détails techniques qui peuvent être inclus dans un schéma plus détaillé.

2- Le réseau de neurones artificiels (ANN) est un type de modèle de machine learning inspiré du fonctionnement du cerveau humain. Il est composé de plusieurs couches de "neurones" reliés entre eux, qui permettent de traiter et de classifier les données. Voici un exemple de schéma simplifié qui illustre le fonctionnement d'un ANN :

- Les données d'entraînement sont chargées et préparées.
- Les données sont envoyées dans la première couche de neurones, appelée couche d'entrée.
- Les données sont transmises de couche en couche jusqu'à la couche de sortie en passant par une ou plusieurs couches cachées.
- Chaque neurone de chaque couche effectue des calculs sur les données et transmet les résultats à la couche suivante.
- Les données sont classées en fonction des résultats de la couche de sortie.
- Les résultats sont évalués et le modèle est ajusté en fonction de la performance.

3- AdaBoost (Adaptive Boosting) est un algorithme de machine learning utilisé pour résoudre des problèmes de classification. Il fonctionne en combinant plu-

sieurs classificateurs "faibles" pour obtenir un classificateur "fort" plus précis. Voici un exemple de schéma simplifié qui illustre le fonctionnement d'AdaBoost :

— Les données d'entraînement sont chargées et préparées.

— Un premier classificateur "faible" est entraîné sur les données.

— Les données qui ont été mal classées par le premier classificateur sont passées avec plus de poids pour le prochain classificateur.

— Un deuxième classificateur "faible" est entraîné sur les données, en prenant en compte les poids des données.

— Les données qui ont été mal classées par le deuxième classificateur sont passées avec plus de poids pour le prochain classificateur.

— Ce processus est répété jusqu'à ce qu'un nombre prédéterminé de classificateurs "faibles" ait été entraîné.

— Les résultats des différents classificateurs "faibles" sont combinés pour obtenir un classificateur "fort" final.

Pour mettre en place notre système de détection d'intrusion (IDS), nous avons utilisé les algorithmes de classification Adaboost et SVM. Ces deux algorithmes seront expliqués en détail dans notre travail afin de démontrer comment ils peuvent être utilisés pour améliorer la précision de la détection des intrusions dans le réseau V2G.

### 3.3.1 Contexte de recherche

Le réseau V2G (Vehicle-to-Grid) est un réseau qui permet la communication entre les véhicules électriques (VE) et les infrastructures de recharge. Ce réseau est essentiel pour la gestion de l'énergie électrique, en particulier pour les VE qui sont de plus en plus présents sur les routes. Le réseau V2G permet de gérer la recharge des VE de manière efficace, en utilisant l'électricité produite par les VE lorsqu'ils ne sont pas utilisés.

Le domaine d'étude de notre travail est la sécurité des réseaux V2G. La sécurité des réseaux V2G est un enjeu majeur, car plusieurs infrastructures sont impliquées dans ce réseau, comme la garantie du fournisseur de service, la confidentialité, l'authentification des VE, et les moyens de paiement. La sécurité du réseau V2G est essentielle pour assurer la disponibilité, l'intégrité et la confidentialité des services proposés.

Les éléments clés du réseau V2G sont les VE, les infrastructures de recharge, et les systèmes de gestion de l'énergie électrique. Les VE sont connectés aux infrastructures de recharge via des bornes de recharge intelligentes, qui permettent de gérer la recharge des VE de manière efficace. Les systèmes de gestion de l'énergie électrique sont utilisés pour gérer l'électricité produite par les VE lorsqu'ils ne sont pas utilisés, afin de maximiser l'utilisation de l'énergie électrique disponible.

Dans le cadre de notre travail, nous avons développé un modèle conceptuel basé sur l'analyse des comportements du réseau V2G afin de détecter les éventuelles attaques et de trouver des solutions adaptées pour y faire face. Nous avons fait l'hypothèse que le comportement anormal du réseau peut être utilisé comme indicateur de la présence d'une intrusion ou d'une attaque.

Les variables clés de notre modèle sont le comportement du réseau, les données normales et les données anormales, ainsi que les différents types d'attaques auxquels le réseau peut être exposé. Nous avons également pris en compte les différentes mesures de sécurité mises en place pour protéger le réseau et les différentes méthodes de détection d'intrusion disponibles.

Notre objectif est de développer un système de détection d'intrusion efficace pour le réseau V2G, qui puisse être utilisé pour identifier les comportements anormaux et prévenir les attaques avant qu'elles ne causent des dommages ou des perturbations dans le fonctionnement du réseau.

Le développement d'un système de détection d'intrusion (IDS) est un moyen pour la sécurisation des services du V2G. Dans la littérature plusieurs travaux ont été réalisés notamment sur la sécurité du V2G, cependant la plupart des attaques sont possibles mais n'ont pas encore été démontrées dans la pratique. En exploitant les renseignements recueillis lors de la lecture scientifique, ceci nous a permis d'acquérir une maîtrise approfondie des notions relatives au domaine d'étude (V2G).

Ceci nous a permis d'avoir une idée sur les méthodes existantes, les améliorations pour les futurs travaux et les solutions proposées. Pour la suite du travail, nous avons proposé de scinder notre travail en deux étapes :

La première partie propose d'étudier l'interface de communications des véhicules électriques aux bornes de recharge intelligente selon la norme ISO-15118. La seconde partie serait une amélioration de la première partie, qui va classifier les données normales, aux potentielles données anomales. Cette seconde partie va nous permettre de mieux organiser notre travail afin de pouvoir identifier toute anomalie, de pouvoir corriger pour maintenir la disponibilité, l'intégrité et la confidentialité des services.

Cette démarche a permis d'identifier les méthodes existantes dans l'état de l'art, ainsi que leurs limitations, contraintes et difficultés. Puis, des améliorations, des ajustements et de nouvelles méthodes sont proposés afin de répondre aux critères, aux exigences et aux particularités du problème abordé.

## 3.4 Conclusion

Il est important de préciser que pour mener à bien notre étude, plusieurs échantillons de données ont été collectés et utilisés. Ces échantillons ont été choisis de manière à couvrir un large éventail de situations possibles dans le réseau V2G, afin

de pouvoir valider le modèle proposé.

En outre, différents outils et techniques ont été utilisés pour analyser les données et mettre en place le modèle de prédiction d'intrusion. Parmi ces outils et techniques, on peut citer l'analyse de données statistiques, l'apprentissage automatique et les réseaux de neurones.

Enfin, il est important de préciser que cette méthode de recherche a été choisie car elle permet de prendre en compte les spécificités du réseau V2G et de développer un modèle de prédiction d'intrusion efficace et adapté à ce type de réseau.

# Chapitre 4

# Conception d'une base de données pour le réseau V2G

Dans le cadre de notre projet de recherche, nous avons mis en place un processus détaillé pour la création de notre base de données. Comme il existe de nombreux modèles de détection d'intrusion (IDS) décrits dans la littérature (voir les références [3], [7] et [14]), nous avons jugé essentiel d'expliquer clairement comment nous avons obtenu notre base de données, afin de faciliter sa compréhension et sa manipulation pour notre travail.

Ainsi, nous avons suivi une méthode rigoureuse pour collecter les données pertinentes. Nous avons commencé par identifier les sources fiables de données de trafic V2G et avons extrait les données brutes à partir des simulations effectuées sur les bornes de recharge de véhicules électriques. Nous avons ensuite nettoyé les données pour éliminer les anomalies et les valeurs aberrantes. Enfin, nous avons appliqué des techniques de traitement de données pour les préparer à l'utilisation dans notre modèle IDS. En résumé, notre approche méthodique pour la création de notre base de données nous a permis d'obtenir des données de qualité pour notre travail de détection

d'intrusion. Cela nous permettra d'obtenir des résultats précis et fiables dans notre modèle.

## 4.1 Modélisation de la base de données

Le travail de Attanasio et al dans [3] a mis à disposition des chercheurs un banc d'essai rentable appelé Miniv2g. Nous avons utilisé Miniv2g pour simuler notre réseau V2G en effectuant plusieurs scénarios de test. Nous avons créé deux réseaux différents, l'un sans attaque et l'autre avec des attaques de type man-in-the-middle et de type Dos. Cela nous a permis de tester la performance de notre système de détection d'intrusion et d'identifier les besoins en matière de sécurité pour notre base de données. L'utilisation de Miniv2g a été cruciale pour la réalisation de notre projet de recherche.

Pour mettre en œuvre les attaques dans MiniV2G, nous avons utilisé deux types d'attaques qui exploitent les vulnérabilités de la norme ISO 15118. Ces vulnérabilités peuvent être utilisées par des utilisateurs malveillants pour simuler des attaques dans des scénarios de charge réelle. Ces attaques ont été utilisées pour tester la performance de notre système de détection d'intrusion et pour identifier les besoins en matière de sécurité pour notre base de données. Les résultats de ces expériences ont permis de définir les exigences spécifiques de notre base de données pour garantir une détection efficace des attaques dans les réseaux électriques V2G.

Tous les travaux pour obtenir la base de données ont été réalisés au Laboratoire de mathématique et d'informatique appliquées (LAMIA). Les expériences de simulation de réseau V2G et d'attaques ont été menées sur des machines virtuelles créées à l'aide de VirtualBox. Cette approche nous a permis de créer et de configurer facilement plusieurs machines virtuelles pour simuler différents scénarios de réseau V2G et d'attaques, avec un haut niveau de contrôle et de flexibilité. Cela nous a permis d'obtenir

des résultats précis et fiables pour notre étude de faisabilité et pour la mise en place de notre base de données pour la détection d'intrusion dans les réseaux électriques V2G.

### 4.1.1 Présentation de MiniV2G

MiniV2G est un outil de simulation de réseaux de véhicules électriques connectés (V2G). Il permet de simuler des réseaux V2G en utilisant des modèles de véhicules, de chargeurs et de réseaux électriques. MiniV2G est principalement utilisé pour étudier la communication entre les véhicules et les chargeurs dans un réseau V2G, et pour évaluer les impacts de la recharge des véhicules sur le réseau électrique.

Avec MiniV2G, il est possible de simuler différents scénarios de charge et de décharge des véhicules, ainsi que d'ajouter des charges supplémentaires sur le réseau (par exemple, des appareils électroménagers). MiniV2G permet également de simuler des attaques sur le réseau V2G, comme des attaques de type homme du milieu ou de type DoS (Denial of Service), afin d'étudier la sécurité de ces réseaux. Enfin, MiniV2G offre une interface graphique pour visualiser les résultats de la simulation et pour paramétrer les différents éléments du réseau. Il peut être utilisé en combinaison avec d'autres outils d'analyse de données pour effectuer des études de performance ou de sécurité des réseaux V2G.

## 4.2 Obtention d'une base de données à partir de MiniV2G

Pour générer une base de données avec MiniV2G, il faut d'abord définir les paramètres de la simulation (par exemple, le nombre de véhicules, les caractéristiques des véhicules et des chargeurs, etc.). Ensuite, MiniV2G exécute la simulation en utilisant ces paramètres et génère des résultats sur les échanges de données entre les véhicules et les bornes, les temps de charge, les taux de charge, etc. Ces données peuvent être enregistrées dans un fichier de sortie, généralement sous forme de fichier CSV (Comma-Separated Values) ou de fichier PCAP (Packet Capture).

Il est possible de paramétrer MiniV2G pour qu'il simule également des attaques sur le réseau V2G, comme des attaques de type homme du milieu ou de type DoS (Denial of Service). Dans ce cas, MiniV2G génère des données sur les comportements anormaux détectés sur le réseau et sur les effets de ces attaques sur les performances du réseau.

En résumé, MiniV2G génère une base de données en simulant des réseaux V2G et en collectant les données produites par la simulation. Ces données peuvent être enregistrées et analysées pour étudier les performances et la sécurité des réseaux V2G.

— Les chargeurs sont des appareils qui permettent de recharger les batteries des véhicules électriques. Ils peuvent être de différents types, selon la puissance de chargement et la technologie utilisée (par exemple, chargeurs rapides ou chargeurs à induction).

— Les bornes, quant à elles, sont des points de recharge pour les véhicules électriques. Elles peuvent être installées chez les particuliers, dans les parkings ou sur le bord de la route. Les bornes sont équipées de chargeurs et permettent aux véhicules de se recharger en se connectant à elles.

Dans notre étude sur les réseaux V2G, les chargeurs sont utilisés pour recharger les véhicules électriques, tandis que les bornes permettent de communiquer avec les véhicules et de gérer la recharge de manière centralisée.

### 4.2.1 Processus de création de la base de données

Nous avons utilisé MiniV2G pour générer notre base de données. Nous avons créé trois scénarios de simulation avec MiniV2G : un scénario sans attaque, et deux scénarios avec des attaques de type homme du milieu et de type DoS (Denial of Service). Pour chaque scénario, nous avons enregistré les données collectées par Wireshark (un logiciel de surveillance de réseau) sous forme de fichiers PCAP.

Ensuite, nous avons utilisé CICFlowmeter pour traiter ces fichiers PCAP et générer trois bases de données partielles, une par scénario. Nous avons nettoyé ces bases de données en supprimant les variables identiques entre les trois bases et en ajoutant une colonne "Attaque" indiquant si l'enregistrement correspond à une attaque (1) ou non (0). Enfin, nous avons fusionné les trois bases de données partielles pour obtenir la base de données finale.

CICFlowmeter est un outil open source utilisé pour extraire des caractéristiques (ou "fonctionnalités") de données de trafic réseau à partir de fichiers PCAP (Packet Capture). Il est principalement utilisé dans le domaine de la cybersécurité pour analyser et classifier les données de trafic afin de détecter des anomalies ou des comportements suspects.

Pour fonctionner, CICFlowmeter prend en entrée un ou plusieurs fichiers PCAP et les analyse pour extraire des informations sur les paquets de données qui y sont contenus. Il peut extraire un grand nombre de caractéristiques différentes, telles que l'adresse IP source et destination, le port source et destination, le protocole utilisé,

la taille des paquets, etc. CICFlowmeter peut également fusionner plusieurs fichiers PCAP en un seul fichier de sortie, ce qui est utile lorsqu'on travaille avec de grandes quantités de données.

Enfin, CICFlowmeter peut être utilisé pour générer des statistiques sur les données de trafic et pour visualiser ces données sous forme de graphiques ou de tableaux. Il est souvent utilisé en combinaison avec d'autres outils d'analyse de données pour effectuer des études de sécurité ou pour évaluer les performances d'un réseau.

## 4.3 Norme ISO 15118

La norme ISO 15118 définit les exigences pour la communication entre un véhicule électrique (VE) et une station de charge (SC) ou tout autre point de charge (AC) pour la recharge de la batterie du véhicule. Cette norme couvre les aspects de sécurité, de fonctionnement et de performance de la communication entre le VE et la SC/AC, ainsi que les aspects de gestion de l'énergie et de l'information associés à la recharge du véhicule.

La norme ISO 15118 est divisée en deux parties : la partie 1 définit les exigences de communication entre le VE et la SC/AC, tandis que la partie 2 définit les exigences pour la communication entre la SC/AC et le réseau électrique auquel elle est connectée.

La norme ISO 15118 vise à assurer une communication sécurisée et fiable entre le VE et la SC/AC, ainsi qu'une gestion efficace de l'énergie et de l'information durant le processus de recharge. Elle est utilisée pour garantir une recharge rapide, sûre et fiable des véhicules électriques, ainsi que pour faciliter l'intégration des véhicules électriques dans les réseaux électriques existants. En résumé, la norme ISO 15118 définit les exigences pour la communication entre un véhicule électrique et une station de charge

ou tout autre point de charge pour la recharge de la batterie du véhicule.

### 4.3.1 Avantage et amélioration

Les avantages de la norme ISO 15118 sont définis comme suit :

— Sécurité : La norme ISO 15118 prévoit des mesures de sécurité pour protéger les données et l'énergie échangées entre le VE et la SC/AC.

— Fiabilité : La norme ISO 15118 garantit une communication fiable entre le VE et la SC/AC, ce qui permet de minimiser les erreurs de transmission et les temps d'arrêt.

— Efficacité énergétique : La norme ISO 15118 permet une gestion efficace de l'énergie durant le processus de recharge, en optimisant l'utilisation de l'énergie disponible et en réduisant les pertes d'énergie.

— Interopérabilité : La norme ISO 15118 garantit l'interopérabilité entre les VE et les SC/AC de différents fabricants, ce qui facilite l'utilisation de bornes de recharge par les propriétaires de véhicules électriques.

— Intégration au réseau électrique : La norme ISO 15118 permet l'intégration des VE au réseau électrique existant, en garantissant une communication sécurisée et fiable entre les VE et le réseau.

## 4.4 Simulation

MiniV2G est un émulateur pour les chercheurs et les étudiants qui travaillent sur des scénarios V2G, il permet d'expérimenter l'environnement V2G. Comme dans le travail de [3] et al, MiniV2G est présenté dans cette section avec ses principales fonctions :

— L'architecture de l'émulateur,

— Les détails de sa mise en oeuvre,

— L'interface graphique,

— Les limitations actuelles de l'émulateur

Pour notre étude, nous avons suivi les étapes suivantes pour simuler MiniV2G et obtenir notre base de données :

— Préparation de l'environnement : Nous avons configuré l'environnement de simulation en utilisant des outils tels que VirtualBox pour créer des machines virtuelles. Nous avons également configuré les paramètres des réseaux V2G simulés, tels que les configurations de charge et de décharge des véhicules électriques.

— Simulation de scénarios de réseau V2G : Nous avons lancé des simulations de réseau V2G pour simuler des scénarios de charge et de décharge des véhicules électriques. Nous avons simulé différents types de réseaux V2G avec des configurations différentes.

— Simulation d'attaques : Nous avons également simulé des attaques sur les réseaux V2G pour récupérer des données sur les vulnérabilités de la norme ISO 15118.

— Récupération des données : Nous avons récupéré les données des attaques simulées pour les utiliser comme base de données pour notre étude.

### 4.4.1 Analyse de l'architecture

MiniV2G est un banc d'essai pour la simulation de réseaux électriques V2G qui utilise Mininet pour créer un réseau connecté de véhicules électriques et de colonnes de charge. Il utilise également la suite de dispositifs Mininet-WiFi pour fournir des fonctionnalités sans fil aux utilisateurs finaux. Le processus de charge est simulé avec RiseV2G [34], en utilisant les fonctionnalités de base fournies par les fichiers jar de RiseV2G. Pour simuler des attaques man-in-the-middle, MiniV2G utilise les outils

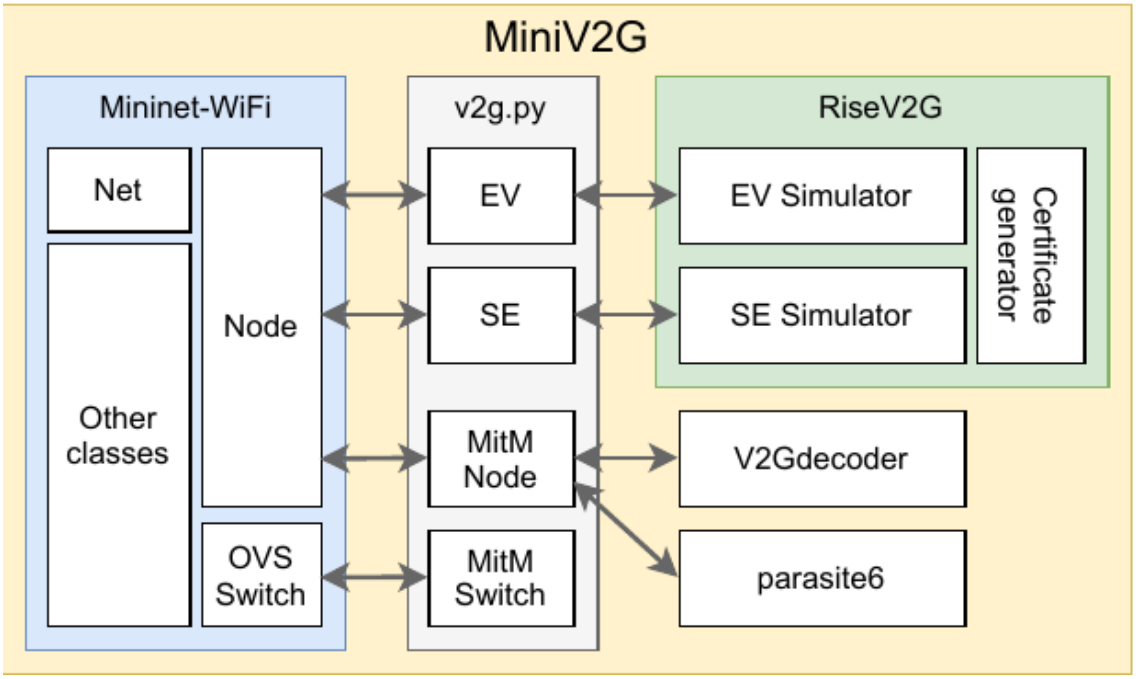


FIGURE 4.1 – MiniV2G [3]

parasite et V2Gdecoder, qui sont intégrés dans un nouveau noeud nommé MitM Node. Il utilise également les fonctions d'OVSSwitch dans Mininet en introduisant le noeud MitM Switch, qui redirige les flux de communication vers le MitM Node.

Mininet-Wifi permet de fournir des fonctionnalités sans fil à l'utilisateur final.

RiseV2G est une partie intégrante de MiniV2G qui permet de simuler le processus de charge. La 4.1 illustre de manière graphique le fonctionnement de l'architecture MiniV2G.

### 4.4.2 Implémentation

MiniV2G est un simulateur de réseau V2G basé sur l'émulateur Mininet-WiFi et intégrant RiseV2G pour simuler le processus de charge des véhicules électriques. Le code source du simulateur est disponible sur le dépôt GitHub et est entièrement

open-source [34]. L'architecture du simulateur repose sur Mininet-WiFi, mais deux nouvelles entités ont été ajoutées pour implémenter les communications V2G. Ces deux nouvelles classes permettent les communications V2G via le simulateur RiseV2G. En résumé, MiniV2G est un outil de simulation open-source permettant de modéliser et de tester des scénarios de recharge de véhicules électriques basés sur la technologie V2G. Il utilise l'émulateur Mininet-WiFi comme base et intègre RiseV2G pour simuler le processus de charge. Le simulateur est facilement accessible via GitHub, ce qui permet à la communauté de l'utiliser et de le développer. Les deux nouvelles classes ajoutées pour les communications V2G sont un ajout essentiel pour la simulation réussie des scénarios V2G.

— La SE (Supply Equipment) qui est une classe d'expansion d'hôte fournissant des fonctionnalités EVSE telles que l'écoute pour les véhicules électriques qui ont besoin d'une charge et de changer ou de récupérer les paramètres de la station initialisée.

— Et la classe EV (Electric Vehicle) qui est conçue pour étendre un hôte en fournissant une fonction pour charger le véhicule électrique et pour définir/récupérer les paramètres du véhicule.

RiseV2G est une implémentation open-source de la norme de communication V2G, qui permet aux véhicules électriques de communiquer avec les réseaux électriques intelligents et de fournir des services de stockage d'énergie à la grille. RiseV2G fournit une implémentation de la couche de communication du protocole V2G, qui permet aux véhicules électriques de communiquer avec les stations de recharge et les réseaux électriques. En utilisant RiseV2G en conjonction avec MiniV2G, nous avons pu simuler et tester des scénarios V2G complexes.

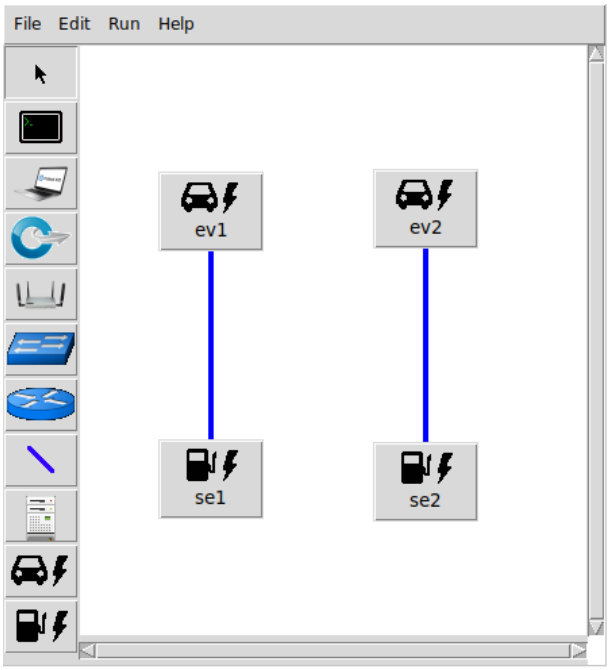


FIGURE 4.2 – Création d'une topologie de base pour les réseaux V2G avec l'outil d'interface graphique MiniEdit

### 4.4.3 Interface graphique

MiniEdit est un outil pratique pour Mininet et Mininet-WiFi, qui permet de concevoir, configurer et tester des topologies de base à l'aide d'une interface graphique intuitive en glisser-déposer. Cela en fait un excellent choix pour les utilisateurs débutants de l'émulateur. En utilisant MiniV2G avec MiniEdit, les utilisateurs peuvent également créer des topologies de réseau qui intègrent des véhicules électriques et des stations de recharge en utilisant l'interface utilisateur étendue de MiniV2G. La Figure 4.2 permet de visualiser de manière graphique la création de ces topologies à l'aide de MiniEdit. De plus, MiniV2G offre une fenêtre dédiée pour configurer les propriétés des nœuds RiseV2G, qui sont introduites dans [3]. Si les utilisateurs préfèrent une approche en ligne de commande, MiniV2G fournit également des exemples de commandes dans le dossier "exemples". En utilisant MiniV2G, les utilisateurs peuvent créer des topologies de réseau personnalisées et simuler des scénarios complexes de gestion de la charge de véhicules électriques en utilisant la norme V2G.

Actuellement, MiniV2G permet uniquement de simuler le processus de communication lié à la charge de véhicules électriques, mais ne fournit pas d'informations sur les paramètres physiques tels que la tension réelle délivrée par un EVSE (Electric Vehicle Supply Equipment) ou la durée de charge.

Cependant, selon [3], il n'existe actuellement aucun autre logiciel capable de fournir une simulation complète de la norme ISO 15118, qui est utilisée pour la communication entre les véhicules électriques et les stations de recharge intelligentes. Par conséquent, MiniV2G reste un outil précieux pour simuler le processus de communication dans le cadre de la gestion de la charge de véhicules électriques, même s'il ne fournit pas de données physiques détaillées. Il est important de noter que MiniV2G reste un outil de simulation en constante évolution, et il est possible que les futures versions offrent davantage de fonctionnalités pour la simulation de la charge de véhicules électriques.

### 4.4.4 Simulation des attaques

MiniV2G est un outil qui permet de simuler des attaques de type déni de service (DoS) et Man-in-the-Middle (MiM) sur les réseaux électriques V2G. Il est construit sur Mininet-WiFi et intègre RiseV2G [34] pour simuler le processus de charge. Pour faciliter la mise en place d'attaques, MiniV2G implémente un nœud MitM qui peut être placé entre un véhicule électrique (VE) et un point de charge (SE) pour interrompre, modifier, fabriquer ou intercepter les messages échangés entre les deux parties. En utilisant le nœud MitM, un attaquant peut également remplacer la réponse de découverte de service pour ajouter ou supprimer les services de charge pris en charge par le SE ou refuser le support d'une méthode d'authentification et d'autorisation. De plus, en modifiant les messages de livraison de puissance et de fin de session, l'attaquant peut mettre en pause, arrêter ou réorganiser la charge du VE.

Un nœud MitM (Man-in-the-Middle) est un type d'attaque informatique dans

laquelle un attaquant interpose sur la communication entre deux parties, en prenant le contrôle de leur communication pour lire, modifier ou intercepter les messages échangés.

Dans le contexte de MiniV2G, il s'agit d'un élément logiciel qui permet de simuler ces types d'attaques dans les réseaux électriques V2G en se plaçant entre un véhicule électrique (EV) et une station d'alimentation (SE) pour interrompre, modifier ou intercepter les messages échangés entre les deux parties.

## 4.5 Conclusion

En somme, ce chapitre a décrit les différentes étapes que nous avons suivies pour obtenir la base de données nécessaire à notre étude. Nous avons commencé par identifier les sources de données pertinentes, puis nous avons procédé à la collecte des données et à leur nettoyage pour éliminer les erreurs et les incohérences. Ensuite, nous avons effectué une analyse exploratoire des données pour mieux comprendre leur structure et leur contenu. Enfin, nous avons effectué une sélection de variables et une transformation des données pour les rendre utilisables dans nos analyses ultérieures.

Cette procédure rigoureuse nous a permis d'obtenir une base de données de qualité qui nous permettra de répondre à nos questions de recherche de manière fiable et précise. Dans le chapitre suivant, nous allons décrire les méthodes d'analyse que nous avons utilisées pour explorer et interpréter les données obtenues.

# Chapitre 5

# Chapitre V - Application du modèle et expérimentation

Dans ce chapitre, nous allons détailler le développement de notre modèle de prédiction d'attaques sur le réseau V2G basé sur l'algorithme AdaBoost. Nous présenterons ensuite les résultats obtenus au cours de nos expérimentations sur des données réelles, en utilisant des graphiques et des tableaux pour aider à visualiser les données. Nous discuterons également des implications pratiques de ces résultats et de la façon dont notre modèle peut être utilisé pour améliorer la sécurité du réseau V2G. La documentation détaillée des étapes du processus, des résultats obtenus et des conclusions tirées sera fournie pour permettre aux lecteurs de comprendre et de vérifier les résultats.

Les expérimentations effectuées dans le cadre de ce travail ont été menées en utilisant le langage de programmation Python dans le cadre d'un environnement Jupyter Notebook au sein du laboratoire de mathématiques et d'informatique appliquées (LAMIA). Pour faciliter le développement et la gestion des paquets, nous avons utilisé la distribution open-source et gratuite Anaconda. Anaconda est spécialement conçue pour les applications de science des données et d'apprentissage automatique,

en supportant les langages de programmation Python et R pour le traitement de grandes quantités de données, l'analyse prédictive et les calculs scientifiques. L'utilisation d'Anaconda nous a permis de simplifier considérablement la gestion des paquets et le déploiement de notre modèle. La création d'un modèle de détection d'intrusion est une étape cruciale dans le développement de systèmes de sécurité. Dans ce travail, nous proposons un IDS (système de détection d'intrusion) basé sur l'apprentissage automatique pour détecter les attaques DoS dans le système de recharge pour véhicules électriques (EVCS). Nous allons implémenter des algorithmes pour détecter et classifier les attaques DoS et les attaques de type homme du milieu dans l'EVCS.

## 5.1 Modélisation

La modélisation se concentre sur la création d'un modèle pour représenter les comportements du réseau V2G en termes de données, processus et fonctionnalités. Cette étape est cruciale pour la compréhension et la prévention des attaques potentielles sur le réseau V2G. En utilisant des algorithmes d'apprentissage automatique, les modèles peuvent être formés sur des données réelles pour prédire et détecter les anomalies de sécurité dans le système V2G.

La norme ISO 15118 est un protocole de communication clé utilisé pour l'authentification, l'autorisation et la facturation de la recharge des véhicules électriques. Outre la coordination du processus de charge, cette norme aborde également des aspects tels que la facturation, l'authentification et les services à valeur ajoutée qui peuvent être fournis en connectant le véhicule électrique à Internet via la borne de recharge. La Figure 5.1 explique de manière graphique les différents aspects couverts par la norme ISO 15118."

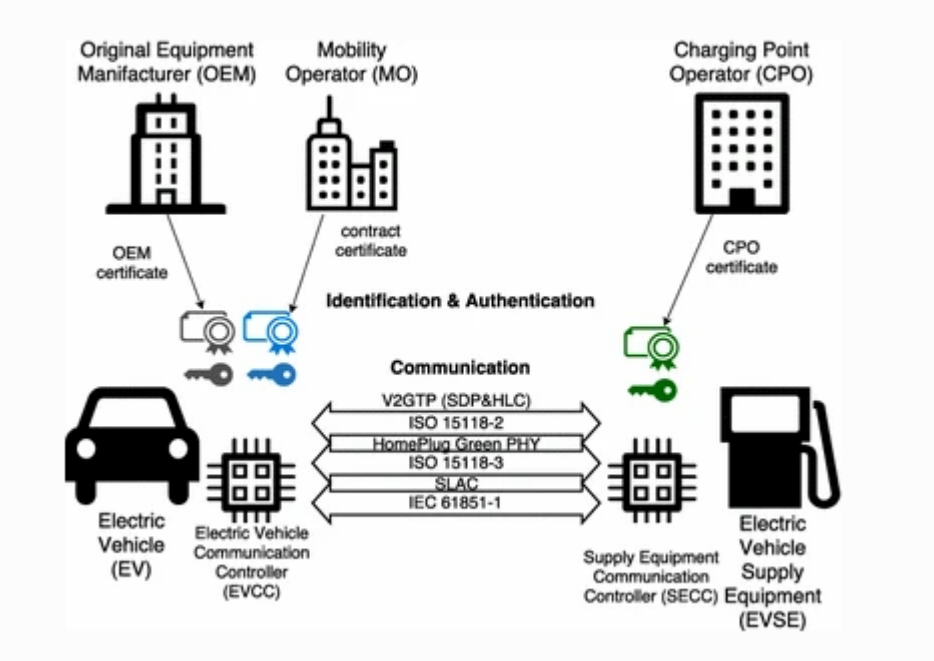


FIGURE 5.1 – ISO 15118 [4]

Le développement d'un modèle prédictif pour les attaques dans les réseaux V2G est crucial pour assurer la sécurité des systèmes de recharge pour les véhicules électriques. Cela peut être accompli en utilisant des techniques de machine Learning telles que l'apprentissage supervisé pour former un modèle en utilisant des données historiques d'attaques. Les données peuvent être préparées en utilisant des techniques telles que l'acquisition, la normalisation et la segmentation. La sélection des caractéristiques les plus significatives pour la classification peut également être effectuée. Le modèle peut être formé en utilisant une fonction coût pour évaluer les erreurs, puis en utilisant des algorithmes tels que la descente de gradient pour minimiser la fonction coût et mettre à jour les paramètres W (poids) et B (biais) du modèle. Ce modèle formé peut être utilisé pour détecter les attaques potentielles et prévenir les dommages au réseau V2G.

Dans une régression linéaire simple, W (poids) est le vecteur de coefficients qui affecte la contribution de chaque caractéristique (variable indépendante) à la valeur de sortie prédite. B (biais) est un terme de constante ajouté à la somme pondérée des

entrées, permettant au modèle de décaler le plan de régression pour mieux s'ajuster aux données. En somme, W et B sont les paramètres que le modèle ajuste durant la phase d'entraînement pour minimiser la fonction de coût et prédire les valeurs cibles le plus précisément possible.

Pour développer notre système de détection d'intrusion pour la prédiction des attaques dans le réseau V2G, nous avons utilisé l'algorithme AdaBoost. AdaBoost (Adaptive Boosting) est un algorithme d'apprentissage ensembliste qui combine plusieurs classificateurs faibles pour former un classificateur fort. Il utilise une méthode de pondération pour adapter les poids des observations en fonction de leur difficulté à être classées correctement par les classificateurs faibles. Les classificateurs faibles sont formés successivement sur les données pondérées, et leur performance est évaluée en termes d'erreur de classification. Les classificateurs qui obtiennent de bons résultats leurs sont attribués un poids plus élevé dans la combinaison finale, tandis que ceux qui sont moins performants leurs sont attribués un poid plus faible. Les paramètres clés d'AdaBoost comprennent le nombre de classificateurs faibles à utiliser, la méthode de pondération des données, et la méthode de formation des classificateurs faibles.

Out[8]:

| kts/s | Flow IAT Min | Flow IAT Mean | Flow Pkts/s | Flow IAT Max | Tot Fwd Pkts | Flow IAT Std | Fwd IAT Tot | ... | Subflow Fwd Pkts | Active Mean | Active Std | Active Max | Active Min | Idle Mean | Idle Std | Idle Max | Idle Min | ATT |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3659 | 817221.0 | 817221.000000 | 2.447318 | 817221.0 | 1 | 0.000000e+00 | 0.0 | ... | 1 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0 |
| 1442 | 213942.0 | 248667.000000 | 6.032163 | 283392.0 | 2 | 4.910857e+04 | 213942.0 | ... | 2 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0 |
| 0599 | 194909.0 | 194909.000000 | 10.261199 | 194909.0 | 1 | 0.000000e+00 | 0.0 | ... | 1 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0 |
| 2628 | 3026.0 | 4709.370000 | 214.466054 | 21201.0 | 100 | 2.850551e+03 | 465516.0 | ... | 100 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0 |
| 6072 | 223913.0 | 272771.500000 | 5.499108 | 321630.0 | 2 | 6.909635e+04 | 223913.0 | ... | 2 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0 |
| ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... |
| 2923 | -113521.0 | 283051.739130 | 3.686528 | 4958153.0 | 23 | 1.032388e+06 | 6474674.0 | ... | 23 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 1 |
| 8972 | -218763.0 | 313580.680000 | 3.316531 | 4964013.0 | 25 | 1.009609e+06 | 7701631.0 | ... | 25 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 1 |
| 4655 | -5.0 | 269204.000000 | 4.952873 | 807599.0 | 3 | 4.662637e+05 | 807594.0 | ... | 3 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 1 |
| 2671 | 3.0 | 267904.666667 | 4.976895 | 803704.0 | 3 | 4.640158e+05 | 803711.0 | ... | 3 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 1 |
| 2151 | -78283.0 | 308437.238095 | 3.396539 | 4950577.0 | 21 | 1.077235e+06 | 6398901.0 | ... | 21 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 1 |

FIGURE 5.2 – Capture d'écran d'une partie du jeu de données utilisé (avant pré traitement)

La Figure 5.2 ci-dessus montre une représentation visuelle de notre ensemble de données. Étant donné que la colonne cible (ATT) est binaire, nous sommes face à un problème de classification. Pour commencer, nous allons affecter des poids à chaque point de données. Au départ, tous les poids seront égaux. La formule utilisée pour déterminer les poids des échantillons est la suivante :

$$w\left(x_i, y_i\right) = \frac{1}{N}, i = 1, 2, \ldots n \tag{5.1}$$

Où $N$ est le nombre total de points de données. Ici, puisque nous avons plusieurs points de données, les poids d'échantillon attribués seront de $1/N$.

$x_i$ représente une observation ou un échantillon du jeu de données.

$y_i$ représente la cible ou la variable à prédire pour cette observation $x_i$.

Et le $i$ est l'index utilisé pour parcourir les échantillons de données. Il peut être considéré comme un compteur, qui permet de parcourir tous les échantillons de données, un par un.

La fonction de coût pour l'algorithme AdaBoost est définie comme la somme des poids de tous les échantillons mal classés :

$$\Sigma i = 1 \text{ to } N \left(w_i^* I(y_i \neq f(x_i))\right) \tag{5.2}$$

— où $N$ est le nombre total d'échantillons,

— $w_i$ est le poids de l'échantillon $i$,

— $y_i$ est la classe réelle de l'échantillon $i$,

— $f(x_i)$ est la classe prédite pour l'échantillon $i$ et I(condition) est une fonction indicatrice qui retourne 1 si la condition est vraie et 0 sinon.

Nous allons maintenant calculer l'« Amount of Say », ou « Importance », ou « Influence » de ce classificateur dans la classification des points de données à l'aide de la formule suivante :

$$\frac{1}{2} \log \frac{1 - \text{ Total Error}}{\text{Total Error}} \tag{5.3}$$

La somme des poids des échantillons mal classés constitue l'erreur totale.

"Amount of Say" ou "Importance" ou "Influence" sont des termes qui font référence à une mesure de l'importance d'un classificateur pour la classification de points de données. Cette mesure est généralement utilisée dans les ensembles de classificateurs, où plusieurs classificateurs sont utilisés pour classer des points de données.

L'Amount of Say est généralement calculé en utilisant une formule qui prend en compte la performance de chaque classificateur dans l'ensemble, ainsi que la corrélation entre les prédictions des différents classificateurs. Cette mesure permet de déterminer la contribution de chaque classificateur à la décision finale de classification et peut être utilisée pour optimiser la combinaison de plusieurs classificateurs dans un ensemble.

Supposons qu'il y ait une sortie erronée dans notre ensemble de données, alors l'erreur totale sera de 1/N, où N représente le nombre total de points de données dans l'ensemble. En outre, la performance du classificateur, alpha, sera également déterminée.

$$\text{Performance du Classifieur } = \frac{1}{2}\log_e\left(\frac{1 - \text{ Total Error}}{\text{Total Error}}\right) \tag{5.4}$$

La performance du classifieur fait référence à l'exactitude et à l'efficacité d'un algorithme de classification dans la tâche de prédiction d'étiquettes pour les données d'entrée. Plus précisément, la performance du classifieur est mesurée par sa capacité à classer correctement les exemples dans l'ensemble de données de test, en comparant les prédictions faites par le modèle avec les étiquettes réelles des exemples de test. Les mesures courantes de la performance du classifieur incluent l'exactitude, la précision, le rappel, le F1-score, l'aire sous la courbe ROC, entre autres.

$$\alpha = \frac{1}{2}\log_e\left(\frac{1 - \frac{1}{9}}{\frac{1}{9}}\right) \tag{5.5}$$

$$\alpha = \frac{1}{2}\log_e(8) \tag{5.6}$$

$$\begin{aligned} \alpha &= \frac{1}{2}\log_e(8) \\ \alpha &= 0.96 \end{aligned} \tag{5.7}$$

*alpha*, $log_e$

Dans le processus de modélisation d'un algorithme de machine learning, une étape

cruciale consiste en l'Initialisation, la Propagation vers l'avant, la Propagation arrière et la Mise à jour. Cette séquence d'actions permet de former le modèle, de prédire les données et de mettre à jour les paramètres pour améliorer la précision. Il est donc important de comprendre comment ces étapes fonctionnent ensemble pour atteindre les meilleurs résultats. Le tableau ci-dessous permet de mieux visualiser les étapes suivies par notre algorithme.

1. Initialisation : c'est la première étape de l'apprentissage automatique, consistant à définir les paramètres de modèle tels que les poids, les biais et autres variables.
2. Propagation vers l'avant : aussi appelée la phase de propagation avant, elle consiste à faire une prédiction en utilisant les données d'entrée pour les comparer aux valeurs réelles attendues.
3. Propagation arrière : aussi appelée la phase de rétropropagation, elle consiste à mesurer l'erreur du modèle et à utiliser cette erreur pour ajuster les poids et les biais du modèle.
4. Mise à jour : cette étape consiste à mettre à jour les paramètres du modèle en utilisant les informations obtenues lors de la propagation arrière. Les méthodes telles que la descente de gradient sont utilisées pour effectuer cette mise à jour.

Notre algorithme fonctionne en itérant sur notre jeu de données en plusieurs cycles, en ajustant les poids des échantillons à chaque cycle pour minimiser l'erreur de classification. Chaque cycle ajoute un modèle de base au modèle final et les poids des échantillons sont mis à jour en fonction de leur performance antérieure.

$$_m = (1/2) * ln((1 - e_m)/e_m)$$

Lors du premier cycle, tous les échantillons ont le même poids (voir formule 5.1). Le modèle de base est alors formé sur ces échantillons et utilisé pour classer de nouvelles données. Les échantillons qui ont été classés incorrectement ont leur poids augmenté,

tandis que les échantillons classés correctement ont leur poids diminué. Le deuxième cycle utilise ces poids modifiés pour former un nouveau modèle de base, qui est ensuite utilisé pour classer les données. Ce processus se poursuit jusqu'à ce que la précision souhaitée soit atteinte ou que le nombre maximum de cycles soit atteint.

Le modèle final est la combinaison linéaire de tous les modèles de base formés au cours de chaque cycle, avec des coefficients déterminés en fonction de la performance des modèles de base. Le modèle final peut être utilisé pour classer de nouvelles données en utilisant les poids des échantillons ajustés et les modèles de base formés au cours de chaque cycle.

$$f(x) = sign(_m * hm(x)) \tag{5.8}$$

où $m$ est le poids pour un classifieur et $h_m$ est le classifieur correspondant.

## 5.2 Résultats et Discussion

Dans cette partie de notre travail, nous présentons les résultats de nos expérimentations. Lors de la construction d'un modèle de machine learning, la préparation et le nettoyage des données sont des étapes fondamentales pour garantir une performance optimale. Nous allons décrire comment ces étapes se sont déroulées dans notre travail.

— Import des données

— Analyses exploratoires

— Gestion des valeurs manquantes

— Gestion des données dupliquées

— Conversion des types de données

— Transformation des données

— Séparation en jeux d'entraînement et de test

Out[8]:

| kts/s | Flow IAT Min | Flow IAT Mean | Flow Pkts/s | Flow IAT Max | Tot Fwd Pkts | Flow IAT Std | Fwd IAT Tot | ... | Subflow Fwd Pkts | Active Mean | Active Std | Active Max | Active Min | Idle Mean | Idle Std | Idle Max | Idle Min | ATT |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3659 | 817221.0 | 817221.000000 | 2.447318 | 817221.0 | 1 | 0.000000e+00 | 0.0 | ... | 1 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0 |
| 1442 | 213942.0 | 248667.000000 | 6.032163 | 283392.0 | 2 | 4.910857e+04 | 213942.0 | ... | 2 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0 |
| 0599 | 194909.0 | 194909.000000 | 10.261199 | 194909.0 | 1 | 0.000000e+00 | 0.0 | ... | 1 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0 |
| 2628 | 3026.0 | 4709.370000 | 214.466054 | 21201.0 | 100 | 2.850551e+03 | 465516.0 | ... | 100 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0 |
| 6072 | 223913.0 | 272771.500000 | 5.499108 | 321630.0 | 2 | 6.909635e+04 | 223913.0 | ... | 2 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0 |
| ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... |
| 2923 | -113521.0 | 283051.739130 | 3.686528 | 4958153.0 | 23 | 1.032388e+06 | 6474674.0 | ... | 23 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 1 |
| 8972 | -218763.0 | 313580.680000 | 3.316531 | 4964013.0 | 25 | 1.009609e+06 | 7701631.0 | ... | 25 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 1 |
| 4655 | -5.0 | 269204.000000 | 4.952873 | 807599.0 | 3 | 4.662637e+05 | 807594.0 | ... | 3 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 1 |
| 2671 | 3.0 | 267904.666667 | 4.976895 | 803704.0 | 3 | 4.640158e+05 | 803711.0 | ... | 3 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 1 |
| 2151 | -78283.0 | 308437.238095 | 3.396539 | 4950577.0 | 21 | 1.077235e+06 | 6398901.0 | ... | 21 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 1 |

FIGURE 5.3 – Dataset

La Figure 5.3 représente notre jeu de données avant d'avoir été prétraité.

1. Import des données : Cette étape consiste à importer nos données dans un format approprié pour notre analyse. Ce format est utile pour stocker des données en tableaux avec des colonnes et des lignes, et offre de nombreuses fonctionnalités pour travailler avec des données.
2. Analyses exploratoires : Cette étape consiste analyser les données pour comprendre leur structure, leurs caractéristiques et leur distribution. Cela peut inclure des visualisations de données, des statistiques descriptives et d'autres techniques d'analyse exploratoire. Le but de cette étape est de comprendre les données avant de les utiliser pour former notre modèle.
3. Gestion des valeurs manquantes : Les valeurs manquantes peuvent avoir un impact négatif sur les résultats du modèle d'apprentissage automatique. Il est donc important de les traiter. Il existe plusieurs techniques pour gérer les valeurs manquantes, telles que la suppression de lignes ou de colonnes contenant des valeurs manquantes, ou la substitution des valeurs manquantes par la moyenne ou la médiane.
4. Gestion des données dupliquées : Il est possible que certaines données se soient dupliquées dans les données d'origine. Il est important de les supprimer pour éviter les erreurs dans les résultats du modèle.
5. Conversion des types de données : Certaines colonnes peuvent avoir des types de

| | Flow Duration | Bwd Pkts/s | Fwd Pkts/s | Flow IAT Min | Flow IAT Mean | Flow Pkts/s | Flow IAT Max | Tot Fwd Pkts | ATT |
|---|---|---|---|---|---|---|---|---|---|
| **0** | 817221 | 1.223659 | 1.223659 | 817221 | 817221.000000 | 2.447318 | 817221 | 1 | 0 |
| **1** | 497334 | 2.010721 | 4.021442 | 213942 | 248667.000000 | 6.032163 | 283392 | 2 | 0 |
| **2** | 194909 | 5.130599 | 5.130599 | 194909 | 194909.000000 | 10.261199 | 194909 | 1 | 0 |
| **3** | 470937 | 2.123426 | 212.342628 | 3026 | 4709.370000 | 214.466054 | 21201 | 100 | 0 |
| **4** | 545543 | 1.833036 | 3.666072 | 223913 | 272771.500000 | 5.499108 | 321630 | 2 | 0 |
| **...** | ... | ... | ... | ... | ... | ... | ... | ... | ... |
| **240** | 869716 | 1.149801 | 231.109926 | -248151 | 4326.945274 | 232.259726 | 168251 | 201 | 1 |
| **241** | 519 | 1926.782274 | 9633.911368 | -468 | 103.800000 | 11560.693642 | 382 | 5 | 1 |
| **242** | 1392459 | 0.718154 | 147.221570 | -241369 | 6792.482927 | 147.939724 | 465562 | 205 | 1 |
| **243** | 7867097 | 0.127112 | 1.652452 | -139057 | 605161.307692 | 1.779564 | 4994049 | 13 | 1 |
| **244** | 902733 | 1.107747 | 3.323242 | 7 | 300911.000000 | 4.430989 | 902715 | 3 | 1 |

FIGURE 5.4 – Dataset après prétraiment

données inappropriés pour la modélisation. Il est donc important de les convertir en types plus appropriés, comme les nombres réels ou les variables catégoriques. Les étapes de gestion des données dupliquées et de conversion des types de données ne sont pas nécessaires dans notre travail, car nous avons déjà supprimé toutes les données dupliquées dans la phase précédente lors de l'acquisition de la base de données. De plus, toutes nos données sont des données numériques telles que des nombres décimaux, entiers ou continues. Cependant, cette étape est cruciale si nous avions des données catégorielles ou textuelles, car nous devrions les convertir en variables binaires (en utilisant par exemple la technique de codage "one hot") ou en données numériques (en utilisant par exemple la technique d'encodage d'entier) avant de les utiliser pour la classification. Il est important de s'assurer que les types de données sont appropriés pour la tâche de classification afin d'optimiser les performances du modèle. La Figure 5.4 représente notre jeu de données après prétraitement. Les données ont été nettoyées, transformées et réduites en dimensions afin d'éliminer les valeurs aberrantes et les corrélations, ce qui permet une analyse plus précise et efficace. La Figure 5.4 offre ainsi une visualisation claire de la structure de notre jeu de données optimisé.

6. Transformation des données : Certaines données peuvent avoir des distributions non-normales ou des valeurs extrêmes qui peuvent affecter les résultats du modèle. Il peut être nécessaire de les normaliser ou de les transformer pour qu'elles soient plus adaptés à l'analyse.

```
# Réduction de dimension avec l'ACP
pca = PCA(n_components=2)
X_pca = pca.fit_transform(data.drop('ATT', axis=1))

# Séparation des données en variables explicatives (X) et variable cible (y)
X = X_pca
y = data['ATT']

# Séparation des données en ensemble d'entraînement et ensemble de test
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.2, random_state=21)

# Initialisation et entraînement du classifieur AdaBoost
clf = AdaBoostClassifier()
clf.fit(X_train, y_train)

# Prédiction sur les données de test
y_pred = clf.predict(X_test)

# Evaluation de la performance du modèle
acc = accuracy_score(y_test, y_pred)
print("Accuracy: {:.2f}%".format(acc * 100))
```

FIGURE 5.5 – Traitement de la méthode ACP sur le dataset

7. Séparation en jeux d'entraînement et de test : Pour évaluer la performance de notre modèle, il est important de séparer les données en deux parties. Le premier ensemble de données est utilisé pour entraîner le modèle, tandis que le second est utilisé pour évaluer la performance du modèle en utilisant des métriques telles que la précision ou la courbe ROC. La Figure 5.5 explique visuellement les étapes impliquées dans le traitement de la méthode ACP sur notre jeu de données.

La Figure 5.6 ci-dessous résume les étapes que nous venons de développer et offre un aperçu de la progression de notre modèle. Les deux phénomènes de sur-ajustement (overfitting) et de sous-ajustement (underfitting) peuvent survenir dans un modèle de machine learning. L'overfitting se produit lorsque le modèle est trop complexe par rapport à la quantité de données d'entraînement qu'il reçoit, ce qui peut entraîner des performances inférieures sur des données nouvelles ou non vues. D'un autre côté, le sous-ajustement se produit lorsque le modèle est insuffisamment complexe pour capturer les relations complexes présentes dans les données d'entraînement, ce qui peut également entraîner des performances inférieures. Il est important de trouver un bon équilibre entre la complexité du modèle et la quantité de données d'entraînement pour

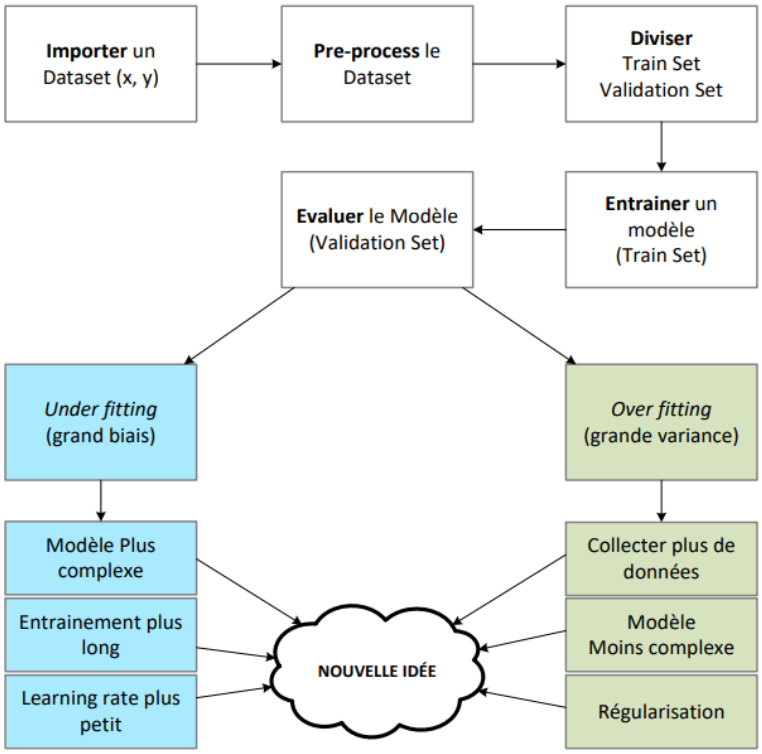


FIGURE 5.6 – Développement du modèle

éviter ces deux phénomènes. La figure 5.6 récapitule le cycle complet de développement d'un modèle d'apprentissage automatique en incluant toutes les étapes.

Dans le chapitre 4 de notre travail, nous avons exposé avec précision la manière dont nous avons collecté nos données ainsi que les étapes de traitement que nous avons réalisées. Dans le but d'améliorer nos résultats, nous avons procédé à une comparaison entre les données que nous avons collectées et celles présentées dans [35]. Bien que nous n'ayons pas utilisé les données de [35] dans notre propre travail, cette comparaison nous a permis d'optimiser notre expérimentation en identifiant les différences et les similitudes avec notre base de données initiale. De plus, une analyse exploratoire des données a été menée pour mieux comprendre les caractéristiques de notre base de données et les visualiser de manière plus claire.

## 5.3 Résultats

Dans cette section, nous présentons les résultats obtenus lors de nos expériences. Les performances de notre modèle sont évaluées grâce à ces résultats. Nous avons préalablement effectué des étapes préparatoires, telles que le pré-traitement et la division de la base de données en ensemble d'entraînement 80% et ensemble de validation 20% pour permettre une évaluation adéquate de notre modèle, (voir figure 5.5).

Pour ce travail, nous avons utilisé Anaconda sur notre ordinateur Windows, équipé d'un processeur Intel Core i9 de 3.60 GHz et 16 Go de RAM. Cette installation nous a permis de bénéficier de l'environnement Python sur notre machine. Tous les travaux de codage ont été effectués dans Jupyter Notebook.

### 5.3.1 Analyses descriptives

Avant de construire notre modèle, nous avons mené une analyse des données pour nous assurer que le modèle de prédiction choisi pour la détection des attaques dans le réseau V2G est approprié. Cette analyse s'est basée sur la description des variables et nous a permis de déterminer que les variables sont quantitatives. La Figure 5.3 nous permet de mieux visualiser les variables. La Figure 5.7 quant à elle, fournit une description détaillée de chacune des variables.

| No | Attribut | Description | Type |
|---|---|---|---|
| 1 | Flow Duration | Durée d'écoulement | Quantitative |
| 2 | Tot Fwd Pkts | Total des paquets dans le sens direct | Quantitative |
| 3 | Flow Pkts/s | Débit des paquets qui est le nombre de paquets transférés par seconde | Quantitative |
| 4 | Flow IAT Mean | Temps moyen entre deux flux | Quantitative |
| 5 | Flow IAT Std | Temps d'écart type deux flux | Quantitative |
| 6 | Flow IAT Max | Temps maximum entre deux flux | Quantitative |
| 7 | Flow IAT Min | Temps minimum entre deux flux | Quantitative |
| 8 | Fwd IAT Tot | Temps total entre deux paquets envoyés dans le sens direct | Quantitative |
| 9 | Fwd IAT Mean | Temps moyen entre deux paquets envoyés dans le sens direct | Quantitative |
| 10 | Fwd IAT Std | Temps d'écart type entre deux paquets envoyés dans le sens direct | Quantitative |
| 11 | Fwd IAT Max | Temps maximum entre deux paquets envoyés dans le sens direct | Quantitative |
| 12 | Fwd IAT Min | Temps minimum entre deux paquets envoyés dans le sens direct | Quantitative |
| 13 | Fwd Pkts/s | Taille de l'écart type du paquet dans le sens direct | Quantitative |
| 14 | Bwd Pkts/s | Taille de l'écart type du paquet vers l'arrière | Quantitative |
| 15 | Subflow Fwd Pkts | Le nombre moyen de paquets dans un sous-flux dans le sens direct | Quantitative |
| 16 | Active Mean | Temps moyen pendant lequel un flux était actif avant de devenir inactif | Quantitative |
| 17 | Active Std | Écart type temps pendant lequel un flux était actif avant de devenir inactif | Quantitative |
| 18 | Active Max | Durée maximale pendant laquelle un flux était actif avant de devenir inactif | Quantitative |
| 19 | Active Min | Temps minimum pendant lequel un flux était actif avant de devenir inactif | Quantitative |
| 20 | Idle Mean | Temps moyen pendant lequel un flux était inactif avant de devenir actif | Quantitative |
| 21 | Idle Std | Écart type temps pendant lequel un flux était inactif avant de devenir actif | Quantitative |
| 22 | Idle Max | Temps maximum pendant lequel un flux était inactif avant de devenir actif | Quantitative |
| 23 | Idle Min | Temps minimum pendant lequel un flux était inactif avant de devenir actif | Quantitative |
| 24 | ATT | Attaque | Quantitative |

FIGURE 5.7 – Description des variables

### 5.3.2 Application du modèle

Nous avons utilisé l'algorithme Support Vector Machine (SVM) pour obtenir les premiers résultats. Ensuite, nous avons considéré AdaBoost comme un bon modèle de classification étant donné que nos variables sont quantitatives. Au préalable, nous avons effectué un pré-traitement sur les données pour les organiser et les préparer à l'expérimentation en utilisant des techniques telles que la normalisation, la réduction de dimensions, etc. Afin de maximiser les performances de notre analyse de données et de permettre au modèle de faire des prédictions plus précises, nous avons effectué un pré-traitement pour nettoyer notre base de données et la préparer pour l'application de l'apprentissage automatique.

En examinant la colonne cible, c'est-à-dire la variable à prédire, nous pouvons constater, comme l'indique la Figure 5.8 ci-dessous, que 70% des véhicules n'ont pas subi d'attaques, tandis que 30% ont été attaqués.

```
0    0.696296
1    0.303704
Name: ATT, dtype: float64
```

FIGURE 5.8 – Analyse de la variable target

La précision (Precision) est le nombre de vrais positifs divisé par le nombre total de prédictions positives. Elle mesure la capacité du modèle à ne pas faire de faux positifs.

Le rappel (Recall) est le nombre de vrais positifs divisé par le nombre total de vrais échantillons positifs. Il mesure la capacité du modèle à trouver tous les échantillons positifs.

La F1-mesure (F1-score) est un score qui équilibre la précision et le rappel en les moyennant. Il donne une indication globale de la performance d'un modèle.

Le support est le nombre total d'observations dans chaque classe. En utilisant la matrice de confusion, le support désigne le nombre d'observations réelles pour chaque classe. Il peut être utilisé pour mesurer la qualité des prédictions effectuées par le modèle de machine learning, en comparant le nombre de prédictions correctes et incorrectes pour chaque classe.

```
AdaBoost
[[33  1]
 [ 0 23]]
              precision    recall  f1-score   support

           0       1.00      0.97      0.99        34
           1       0.96      1.00      0.98        23

    accuracy                           0.98        57
   macro avg       0.98      0.99      0.98        57
weighted avg       0.98      0.98      0.98        57
```

FIGURE 5.9 – Résultats AdaBoost

```
SVM
[[34  0]
 [20  3]]
              precision    recall  f1-score   support

           0       0.63      1.00      0.77        34
           1       1.00      0.13      0.23        23

    accuracy                           0.65        57
   macro avg       0.81      0.57      0.50        57
weighted avg       0.78      0.65      0.55        57
```

FIGURE 5.10 – Résultats SVM

Les deux Figure 5.9 Figure 5.10 (AdaBoost, SVM) représentent les scores de performance pour une classification binaire (2 classes). Pour AdaBoost, les chiffres dans la matrice de confusion (33, 1, 0 et 23) décrivent le nombre de vrais positifs, de faux positifs, de faux négatifs et de vrais négatifs respectivement. Dans le tableau SVM, les chiffres dans la matrice de confusion (34, 0, 20 et 3) décrivent le nombre de vrais positifs, de faux positifs, de faux négatifs et de vrais négatifs respectivement.

En observant le tableau AdaBoost, nous remarquons que notre modèle a de bons scores de précision, de rappel et de F1-score pour les deux classes, ce qui signifie qu'il a bien fonctionné pour la classification. L'algorithme AdaBoost semble offrir des résultats supérieurs à ceux obtenus avec l'algorithme SVM dans cette comparaison.

### 5.3.3 Observation des courbes

Une courbe de train score et de validation score est utilisée pour visualiser et évaluer la performance d'un modèle de machine learning. La courbe montre comment les scores de performance (en général la précision) évoluent en fonction du nombre d'itérations (par exemple, lors de l'entraînement d'un modèle). Le score de formation représente la performance du modèle sur les données d'entraînement, tandis que le score de validation représente sa performance sur des données de validation indépendantes.

L'objectif est de trouver un modèle qui a un bon score sur les données de validation, ce qui signifie que le modèle est capable de généraliser sur des données nouvelles et non vues auparavant. Si le score de formation est très élevé et que le score de validation est faible, cela signifie que le modèle est sur-entraîné et a tendance à sur-apprendre les données d'entraînement, ce qui peut entraîner de mauvaises performances sur des données nouvelles. Inversement, si le score de validation est supérieur au score de formation, cela peut signifier que le modèle n'a pas été formé suffisamment et qu'il y a une opportunité d'améliorer les performances en continuant à entraîner le modèle.

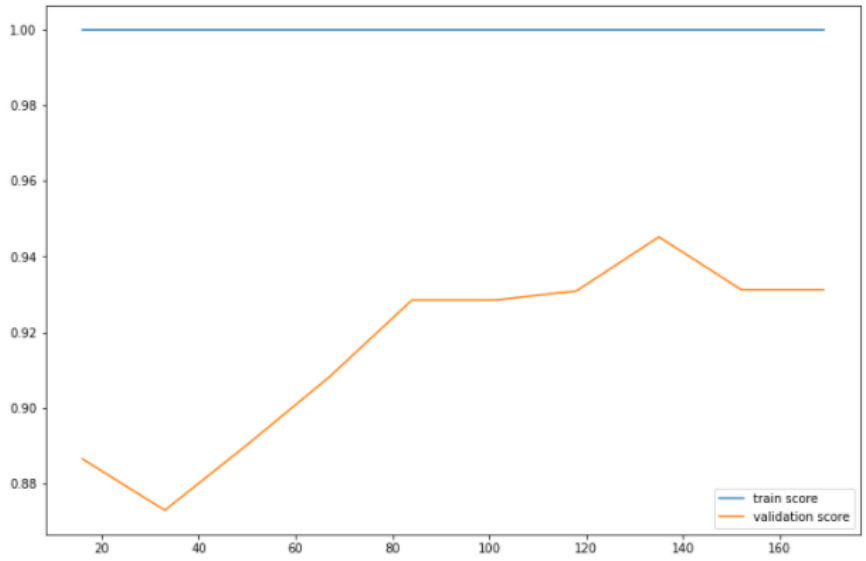


FIGURE 5.11 – Validation score AdaBoost

Dans la Figure 5.11, le train score reste constant à la valeur maximale de 1, ce qui indique que le modèle a réussi à bien s'ajuster aux données d'entraînement, mais qu'il peut avoir mémorisé les données plutôt que de les comprendre. En effet, cela peut conduire à une suradaptation du modèle aux données d'entraînement et à une mauvaise performance sur les données de test ou sur de nouvelles données en général.

Cependant, la courbe de validation score montre que le modèle est capable d'apprendre efficacement et d'améliorer sa performance, tout en conservant sa capacité à prédire avec précision sur de nouvelles données. La courbe de validation score atteint son maximum à 0.94, ce qui correspond au point optimal de la performance du modèle sur les données de validation. Cette valeur indique que le modèle est performant pour la prédiction et qu'il conserve cette performance par la suite. Il n'est donc pas nécessaire de régulariser le modèle pour améliorer ses performances.

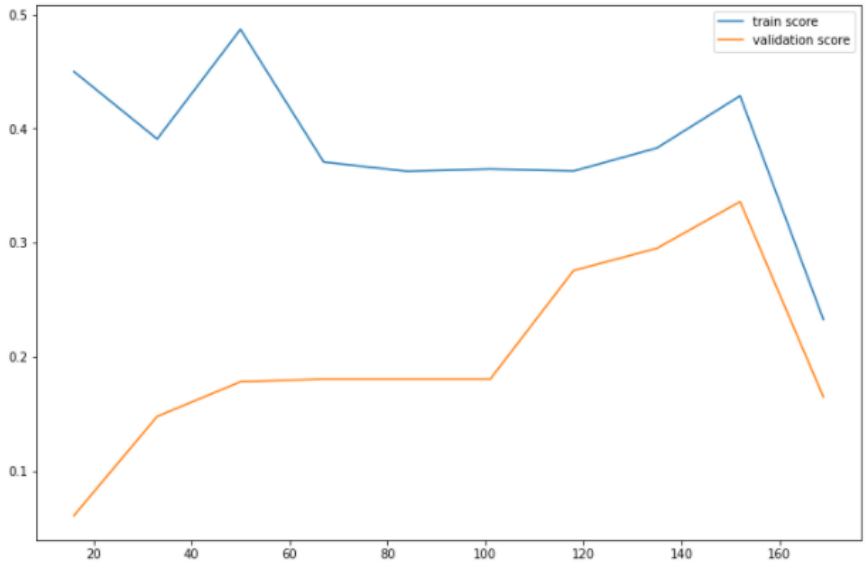


FIGURE 5.12 – Validation score SVM

En observant la Figure 5.12, la courbe du train score explique que le modèle a appris de nouvelles informations à un certain point et a amélioré sa performance sur les données d'entraînement. En revanche, la courbe de validation score indique que le modèle peut parfois trop s'adapter aux données d'apprentissage, ce qui se traduit par une amélioration temporaire de sa performance sur les données de validation. Cependant, cette amélioration n'est pas durable, car le modèle finit par perdre sa capacité à généraliser et à prédire avec précision sur de nouvelles données, ce qui explique sa chute.

| Precision | Recall | F1-Score | Support |
|---|---|---|---|
| 0.96 | 1.00 | 0.98 | 23 |

TABLE 5.1 – Classification AdaBoost

| Precision | Recall | F1-Score | Support |
|---|---|---|---|
| 1.00 | 0.13 | 0.23 | 23 |

TABLE 5.2 – Classification SVM

Les Tableaux 5.1 et 5.2 représentent les mesures de performance détaillées de nos classificateurs. Comme le montrent les tableaux 5.1 et 5.2 l'IDS basé sur AdaBoost est supérieur en termes de classification et donne de meilleur performance par rapport à l'IDS basé sur SVM.

Le support dans le tableau 5.1 et 5.2 représentent le nombre d'échantillon de vraie réponse qui se trouve dans cette classe. L'analyse des tableaux peuvent être faite de différente manière, mais nous nous sommes basés sur le recall ou le F1-score de notre classe 1, c'est-à-dire la classe des véhicules attaqués.

## 5.4 Conclusion

Au cours de nos expérimentations, nous avons comparé les résultats obtenus à partir de notre propre base de données avec ceux issus de l'étude présentée dans [35]. Bien que nous n'ayons pas utilisé les données de l'étude dans [35] dans notre travail, cette comparaison nous a permis d'obtenir un taux de prédiction supérieur, en particulier pour les attaques DoS récentes incluses dans l'ensemble de données d'attaque de CICID 2018. Grâce à notre modèle fiable, nous avons pu renforcer la sécurité du réseau contre ces types d'attaques, ainsi que contre les attaques DDoS et l'homme du milieu récentes. En conclusion, les résultats obtenus dans cette étude ont montré que notre approche de prédiction basée sur AdaBoost a été efficace pour prédire les attaques dans le réseau V2G. Le taux de prédiction atteint de 98%

a démontré la robustesse de notre modèle et sa capacité à généraliser sur des données inconnues. Ces résultats sont encourageants pour la sécurité du réseau V2G. Cependant, certaines limites ont été identifiées et doivent être prises en compte pour améliorer les performances du modèle. Parmi les points forts, nous pouvons citer la précision du modèle, sa capacité à traiter des données complexes et à fournir des résultats en temps réel. Ces résultats ont des implications importantes pour la sécurité du réseau V2G et pour la mise en place de mesures de prévention contre les attaques. Cette étude a permis de mettre en évidence l'efficacité de notre modèle AdaBoost pour la prédiction des attaques dans le réseau V2G, ainsi que son potentiel pour améliorer la sécurité des réseaux intelligents.

# Chapitre 6

# Conclusion générale

Ce travail de recherche a examiné le développement d'un modèle pour prédire les attaques dans le réseau V2G. Nous avons commencé par une étude des différents types de systèmes de détection d'intrusion, y compris ceux basés sur l'intelligence artificielle qui sont largement utilisés dans divers domaines tels que la reconnaissance vocale, l'estimation de la consommation d'énergie et la sécurité informatique. La modélisation d'un système de détection d'intrusion est cruciale pour garantir la sécurité du réseau V2G. Nous avons examiné les modèles IDS actuels, en analysant leurs avantages et inconvénients.

La performance du modèle dans la détection des attaques a été évaluée et les résultats montrent qu'il peut faire des estimations précises dans la détection des attaques. Cependant, il y a encore de la place pour l'amélioration en fournissant plus d'informations et en prenant en compte différents types d'attaques.

En raison de la croissance exponentielle de la demande de véhicules électriques et des changements climatiques, il est important de s'assurer de la sécurité du réseau V2G. Bien que ce travail ait fourni une évaluation des IDS actuels, il y a encore des

défis non résolus, tels que l'amélioration de la performance de prédiction, la gestion des alertes et la coordination des systèmes de détection d'intrusion. Dans l'avenir, nous continuerons à explorer des méthodes pour améliorer les systèmes de détection d'intrusion, notamment en utilisant des techniques de classification en apprentissage automatique et d'intelligence artificielle.

En conclusion, ce travail fournit une vision raisonnable de l'évolution des IDS au cours de la dernière décennie et montre la direction future de la recherche en la matière.

## 6.1 Travaux futurs

Dans les futurs travaux, nous prévoyons la conception et la mise en place d'une base de données plus grande pour la détection d'intrusion dans les réseaux véhiculaires électriques V2G. Plusieurs perspectives de travaux futurs sont possibles pour améliorer encore la détection d'intrusion dans les réseaux véhiculaires électriques V2G :

— Amélioration de la base de données : La base de données de détection d'intrusion pourrait être améliorée en incluant des données provenant de sources supplémentaires et en augmentant la quantité de données dans la base de données. Cela permettrait de créer des modèles plus complets et plus précis pour détecter les intrusions.

— Étudier les vulnérabilités du protocole de communication : Il serait donc intéressant de mener une étude sur les vulnérabilités de ce protocole afin de mieux comprendre les points faibles et de proposer des solutions pour les sécuriser.

— Élargir la portée de la recherche : Bien que notre travail se soit concentré sur la prédiction des attaques, il existe d'autres types d'attaques potentielles sur le réseau V2G, tels que les attaques de déni de service distribué (DDoS) et les attaques par débordement de mémoire tampon. Par conséquent, nous envisageons

d'étendre notre recherche pour inclure ces types d'attaques et explorer comment notre modèle de prédiction pourrait être adapté pour les détecter.

— Exploration de techniques de détection d'intrusion plus avancées : bien que notre modèle actuel ait montré des résultats prometteurs, il existe des techniques plus avancées en matière de détection d'intrusion que nous pourrions explorer. Par exemple, l'utilisation de techniques de deep learning ou de techniques basées sur le comportement pourraient améliorer considérablement la précision de la détection des attaques.

Pour les travaux futurs, les points cités ci-dessus pourront aider à mieux sécuriser le réseau V2G. Pour évaluer de manière plus approfondie la performance des IDS, nous proposons de réaliser des tests en temps réel sur des bancs d'essai. Cela permettra de simuler des conditions réelles d'utilisation du réseau V2G et de mesurer l'efficacité des IDS sur la prédiction des attaques.

# Bibliographie


[1] W. Han et Y. Xiao, « Privacy preservation for v2g networks in smart grid : A survey », *Computer Communications*, vol. 91, p. 17–28, 2016.

[2] « Will v2g take off in 2022 ? investment is likely – top charger », `https://topcharger.co.uk/will-v2g-take-off-in-2022/`.

[3] L. Attanasio, M. Conti, D. Donadel et F. Turrin, « Miniv2g : An electric vehicle charging emulator », *in Proceedings of the 7th ACM on Cyber-Physical System Security Workshop*, p. 65–73, 2021.

[4] A. Observations, L. Des *et al.*, « Road vehicles–vehicle-to-grid communication interface–part 2 : network and application protocol requirements », 2014.

[5] E. W. S. Angelos, O. R. Saavedra, O. A. C. Cortés et A. N. de Souza, « Detection and identification of abnormalities in customer consumptions in power distribution systems », *IEEE Transactions on Power Delivery*, vol. 26, no. 4, p. 2436–2442, 2011.

[6] R. Bace et P. Mell, « Intrusion detection systems, national institute of standards and technology (nist) », *Technical Report 800-31*, 2001.

[7] S. Dudek, J.-C. Delaunay et V. Fargues, « V2g injector : Whispering to cars and charging units through the power-line », 2019.

[8] Y. Qin, J. Wei et W. Yang, « Deep learning based anomaly detection scheme in software-defined networking », *in 2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS)*, p. 1–4, IEEE, 2019.

[9] K. Bao, H. Valev, M. Wagner et H. Schmeck, « A threat analysis of the vehicle-to-grid charging protocol iso 15118 », *Computer Science-Research and Development*, vol. 33, no. 1, p. 3–12, 2018.

[10] N. Sultana, N. Chilamkurti, W. Peng et R. Alhadad, « Survey on sdn based network intrusion detection system using machine learning approaches », *Peer-to-Peer Networking and Applications*, vol. 12, no. 2, p. 493–501, 2019.

[11] M. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu et X. S. Shen, « A lightweight message authentication scheme for smart grid communications », *IEEE Transactions on Smart grid*, vol. 2, no. 4, p. 675–685, 2011.

[12] L. F. Roman, P. R. Gondim et J. Lloret, « Pairing-based authentication protocol for v2g networks in smart grid », *Ad Hoc Networks*, vol. 90, p. 101745, 2019.

[13] Y. Lahrouni, C. Pereira, B. A. Bensaber et I. Biskri, « Using mathematical methods against denial of service (dos) attacks in vanet », *in Proceedings of the 15th ACM International Symposium on Mobility Management and Wireless Access*, p. 17–22, 2017.

[14] H. Lee, S. H. Jeong et H. K. Kim, « Otids : A novel intrusion detection system for in-vehicle network by using remote frame », *in 2017 15th Annual Conference on Privacy, Security and Trust (PST)*, p. 57–5709, IEEE, 2017.

[15] M. Attia, H. Sedjelmaci, S. M. Senouci et E.-H. Aglzim, « A new intrusion detection approach against lethal attacks in the smart grid : temporal and spatial based detections », *in 2015 Global Information Infrastructure and Networking Symposium (GIIS)*, p. 1–3, IEEE, 2015.

[16] S. Abedi, A. Arvani et R. Jamalzadeh, « Cyber security of plug-in electric vehicles in smart grids : application of intrusion detection methods », *in Plug In Electric Vehicles in Smart Grids*, p. 129–147, Springer, 2015.

[17] J. Antoun, M. E. Kabir, B. Moussa, R. Atallah et C. Assi, « A detailed security assessment of the ev charging ecosystem », *IEEE Network*, vol. 34, no. 3, p. 200–207, 2020.

[18] R. Gottumukkala, R. Merchant, A. Tauzin, K. Leon, A. Roche et P. Darby, « Cyber-physical system security of vehicle charging stations », *in 2019 IEEE Green Technologies Conference (GreenTech)*, p. 1–5, IEEE, 2019.

[19] J. Shen, T. Zhou, F. Wei, X. Sun et Y. Xiang, « Privacy-preserving and lightweight key agreement protocol for v2g in the social internet of things », *IEEE Internet of things Journal*, vol. 5, no. 4, p. 2526–2536, 2017.

[20] K. Park, Y. Park, A. K. Das, S. Yu, J. Lee et Y. Park, « A dynamic privacy-preserving key management protocol for v2g in social internet of things », *IEEE Access*, vol. 7, p. 76812–76832, 2019.

[21] N. Saxena et B. J. Choi, « Authentication scheme for flexible charging and discharging of mobile vehicles in the v2g networks », *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 7, p. 1438–1452, 2016.

[22] G. A. Kaya et A. Badwan, « Fuzzy rule based classification system from vehicle-to-grid data », *in 2021 9th International Symposium on Digital Forensics and Security (ISDFS)*, p. 1–7, IEEE, 2021.

[23] Y. Su, G. Shen et M. Zhang, « A novel privacy-preserving authentication scheme for v2g networks », *IEEE Systems Journal*, vol. 14, no. 2, p. 1963–1971, 2019.

[24] M. MOUGHIT, « Systèmes de détection d'intrusion : Réduction des faux positifs à l'aide de la corrélation des événements »,

[25] E. Hodo, X. Bellekens, A. Hamilton, P.-L. Dubouilh, E. Iorkyase, C. Tachtatzis et R. Atkinson, « Threat analysis of iot networks using artificial neural network intrusion detection system », *in 2016 International Symposium on Networks, Computers and Communications (ISNCC)*, p. 1–6, IEEE, 2016.

[26] V. K. Shukla et D. Ojha, « Ontological ids monitoring on defined attack », *Int J Sci Res*, vol. 3, p. 665–670, 2014.

[27] E. Hodo, X. Bellekens, A. Hamilton, C. Tachtatzis et R. Atkinson, « Shallow and deep networks intrusion detection system : A taxonomy and survey », *arXiv preprint arXiv :1701.02145*, 2017.

[28] M. Basnet et M. H. Ali, « Deep learning-based intrusion detection system for electric vehicle charging station », *in 2020 2nd International Conference on Smart Power & Internet Energy Systems (SPIES)*, p. 408–413, IEEE, 2020.

[29] N. Sainis, D. Srivastava et R. Singh, « Classification of various dataset for intrusion detection system », *International Journal of Computer Applications*, vol. 161, no. 2, p. 6–9, 2017.

[30] C. Höfer, J. Petit, R. Schmidt et F. Kargl, « Popcorn : privacy-preserving charging for emobility », *in Proceedings of the 2013 ACM workshop on Security, privacy & dependability for cyber vehicles*, p. 37–48, 2013.

[31] M.-J. Kang et J.-W. Kang, « Intrusion detection system using deep neural network for in-vehicle network security », *PloS one*, vol. 11, no. 6, p. e0155781, 2016.

[32] B. A. Bensaber, C. G. P. Diaz et Y. Lahrouni, « Design and modeling an adaptive neuro-fuzzy inference system (anfis) for the prediction of a security index in vanet », *Journal of Computational Science*, vol. 47, p. 101234, 2020.

[33] P. Engebretson, *The basics of hacking and penetration testing : ethical hacking and penetration testing made easy.* Elsevier, 2013.

[34] « The open source reference implementation of the vehicle-2-grid communication interface iso 15118 », `https://github.com/SwitchEV/RISE-V2G`.

[35] « Cicflowmeter (formerly iscxflowmeter) », `https://https://www.unb.ca/cic/research/applications.html#CICFlowMeter`.