Revue Internationale de la Recherche Scientifique et de l'Innovation (Revue-IRSI)
ISSN: 2960-2823
Vol. 4, No. 3, Mai 2026

Utilisation d'algorithmes intelligents pour la détection d'anomalies dans les réseaux Wi-Fi déployés en mode infrastructure

NTUNKADI MOMBO Aristote[1]
[1]*Professeur d'informatique et chercheur au Laboratoire NetSecure AI Lab, Haute École de Commerce de Kinshasa.*

Résumé : Ce travail explore l'utilisation de l'intelligence artificielle, et plus spécifiquement d'un modèle d'apprentissage non supervisé (One-Class SVM), pour détecter des comportements anormaux dans un réseau Wi-Fi à partir des mesures d'intensité de signal (RSSI). Contrairement aux systèmes de détection d'intrusion classiques reposant sur des signatures d'attaques connues, cette approche modélise le comportement normal du réseau afin d'identifier des observations atypiques, y compris potentiellement inconnues. Le résultat obtenu montre qu'une visualisation par analyse en composantes principales des données normales forment un nuage relativement compact, tandis que les anomalies se dispersent autour, voire s'en éloignent complètement.

Mots clés : IEEE 802.11, WPA2, WPA3, Wi-Fi security ; intrusion detection ; Attaques ; IDS ; RSSI-based attack detection

Digital Object Identifier (DOI): https://doi.org/10.5281/zenodo.**20367004**

1 Introduction

La conception initiale des trames dans le réseau Wi-fi ne prévoyait pas de mécanisme de sécurité robuste, avec les évolutions actuelles cette faiblesse expose de plus en plus le réseau aux vulnérabilités facilement exploitable par des personnes malveillantes. L'algorithme de sécurité WEP3 a été développé dans le but de corriger des failles constatées dans ses prédécesseurs notamment le WEP et le WEP2. Cependant, la nature dynamique des attaques menées sur le réseau révèle qu'il présente encore des limites laissant d'autres possibilités aux manipulations malveillantes (Chatzoglou E. et al., 2021).

Ces vulnérabilités donne lieu à plusieurs types de menaces telles que les attaques d'authentification, les attaques de type Man-in-the-Middle, l'usurpation de points d'accès (Rogue Access Point) ou encore l'interception du trafic réseau (Sheikh et al.,2019). Ces faiblesses relèvent d'un point de vue technique, du fait que ce type de réseau repose sur la diffusion d'ondes électromagnétiques dans le spectre hertzien, un espace physique partagé et intrinsèquement non clos. Différents mécanismes externes protègent les réseaux sans fil, notamment les systèmes de détection d'intrusion (IDS). Un système de détection d'intrusion (IDS) constitue une méthode d'observation du trafic réseau visant à déterminer la présence de menaces consécutives à des intrusions. Disponible en permanence (24h/24 et 7j/7), il remplit trois fonctions principales : la génération d'informations sur l'état du système, la surveillance des activités des utilisateurs, et la transmission de rapports à un poste de gestion (Abbas et al., 2023).

Cependant, ces dispositifs montrent parfois leurs limites face à la complexité et à l'évolution rapide des techniques d'attaque. De ce fait, les atteintes à l'intégrité des données, à la disponibilité des échanges et à la confidentialité des informations continuent de compromettre la sécurité du réseau.

L'objectif de cet article est d'étudier l'apport de l'intelligence artificielle dans la prévention et la détection des attaques sur les réseaux Wi-Fi. Nous présenterons d'abord le contexte et la problématique de cette étude. Suivra une revue de littérature dans laquelle nous aborderons les principales menaces ciblant les réseaux sans fil, puis les concepts fondamentaux de l'intelligence artificielle appliqués à la cybersécurité. Enfin, nous analyserons comment les techniques d'apprentissage automatique peuvent être utilisées pour améliorer la sécurité des réseaux Wi-Fi.

1.1 Problématique de recherche

Avec la croissance rapide de l'utilisation des réseaux Wi-Fi dans les environnements domestiques, universitaires et professionnels, les risques liés aux perturbations du signal ainsi qu'aux attaques informatiques constituent des enjeux fondamentaux sur lesquels il convient de se pencher afin d'assurer la fiabilité, la sécurité et la disponibilité des communications sans fil. Pour bien illustrer nos propos, la figure 2 présente un bâtiment multi-zones où plusieurs points d'accès Wi-Fi (AP) sont positionnés stratégiquement afin de couvrir l'ensemble des espaces, qu'il s'agisse des bureaux, des couloirs ou des salles de réunion. Chaque point d'accès diffuse un signal radio permettant aux dispositifs mobiles de se connecter au réseau.

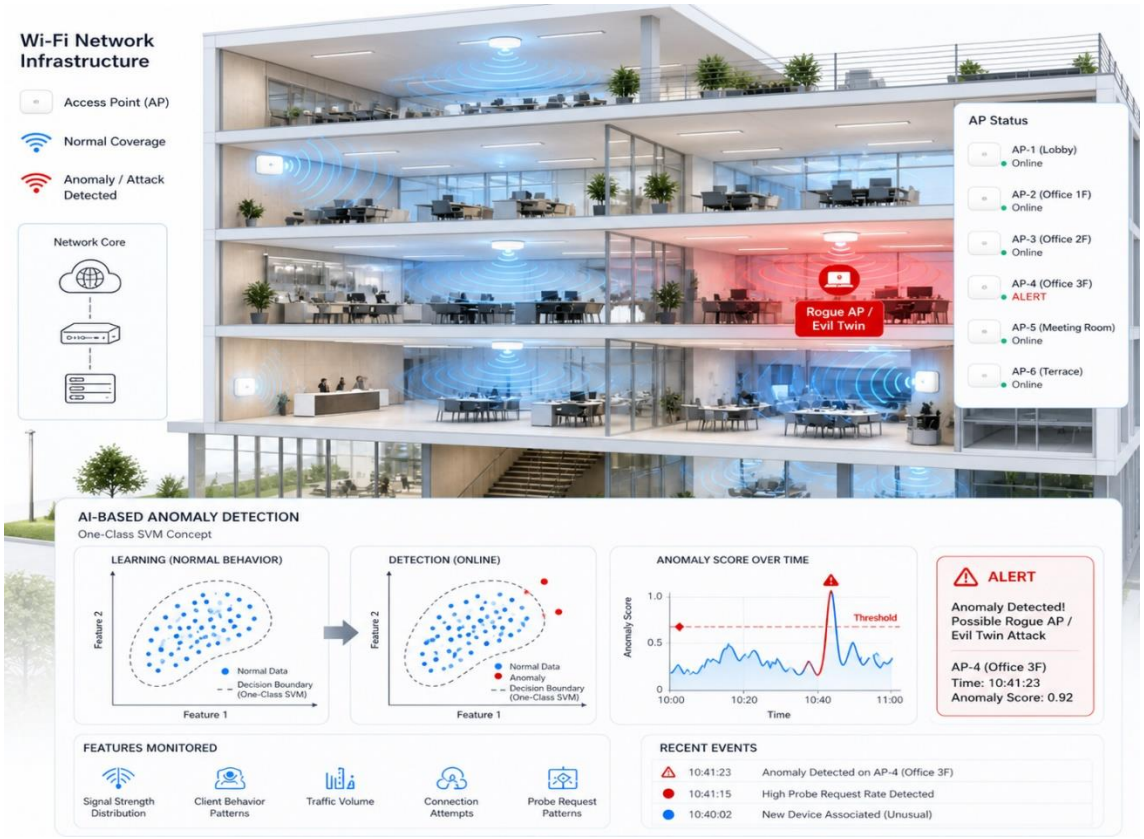

Figure 1. Réseaux Wi-Fi basés sur l'infrastructure

Dans un fonctionnement normal, les signaux RSSI observés dans les différentes zones présentent une certaine cohérence spatiale. Cette cohérence se traduit par des niveaux de signal relativement stables et homogènes autour de chaque point d'accès, formant des zones de couverture bien définies.

Cependant, certaines zones du bâtiment peuvent présenter des comportements anormaux. Ces anomalies peuvent être représentées par des régions où les signaux diffèrent fortement des valeurs attendues. Elles peuvent correspondre à des situations réelles telles qu'une interférence locale, une forte proximité inhabituelle avec un point d'accès, un brouillage du signal ou encore une tentative de perturbation du réseau.

Ces anomalies locales (interférences, brouillage) peuvent parfois résulter d'actions malveillantes. En effet, en raison de leur nature ouverte et de la transmission des données par ondes radio, les réseaux sans fil sont particulièrement vulnérables à différentes formes d'attaques telles que l'interception du trafic, l'usurpation de points d'accès, les attaques d'authentification ou encore les attaques de type Man-in-the-Middle.

Cette distinction est d'autant plus difficile que, dans les réseaux Wi-Fi en mode infrastructure, la nature dynamique et bruitée du canal radio entraîne des variations importantes du signal RSSI dues à des interférences locales, des effets de propagation ou des changements environnementaux. Ces fluctuations compliquent la distinction entre un comportement normal du réseau et une activité réellement anormale.

Dans ce contexte, les approches classiques de détection d'intrusion basées sur des signatures ou des seuils fixes sont insuffisantes, car elles ne modélisent pas correctement la variabilité naturelle du signal et peuvent conduire à des faux positifs ou à des attaques non détectées.

Ainsi, dans un environnement multi-étages où les zones normales présentent des distributions homogènes de RSSI et où certaines régions peuvent contenir des anomalies spatiales, la question se pose de savoir comment apprendre le comportement normal du réseau afin d'identifier automatiquement les écarts significatifs, sans disposer de données d'attaque étiquetées.

Dans un environnement Wi-Fi multi-zones, comment détecter automatiquement les anomalies spatiales du signal RSSI en les distinguant des variations naturelles du canal radio, sans disposer de données d'attaques étiquetées, et avec des contraintes de détection en temps réel ? Comment déterminer dynamiquement un seuil de détection (ou un taux de rejet dans un One-Class SVM) qui minimise les faux positifs tout en détectant des anomalies réelles ? Comment vérifier que les anomalies détectées correspondent effectivement à des comportements anormaux (interférence, brouillage, attaque) et non à des variations environnementales normales (affluence, réaménagement) ?

Cette problématique s'inscrit dans une approche de détection d'anomalies non supervisée, où l'intelligence artificielle permet d'apprendre le comportement normal du réseau pour signaler les écarts significatifs. Parmi les approches non supervisées, le One-Class SVM est particulièrement adapté car il apprend une frontière compacte autour des données normales, sans nécessiter d'exemples d'attaques. Une fois entraîné, il est capable de détecter les écarts significatifs par rapport à ce comportement. Les zones normales sont alors considérées comme

des régions de forte densité de données, tandis que les anomalies apparaissent comme des points isolés ou des clusters atypiques.

Un système de supervision en temps réel peut exploiter ces résultats pour générer des alertes lorsqu'un comportement inhabituel est détecté. Ces alertes peuvent ensuite être visualisées sous forme de carte du bâtiment, avec une distinction claire entre les zones normales (par exemple en bleu) et les zones suspectes ou anomalies (par exemple en rouge).

L'hypothèse sous-jacente est que les données normales forment un motif spatial et temporel relativement stable, et que la plupart des comportements anormaux d'intérêt (attaques, interférences malveillantes) s'écartent significativement de ce motif. Toutefois, la distinction reste délicate en présence de variations environnementales brutales ou d'attaques furtives.

2 Revue de la littérature

Le grand défi des réseaux Wi-Fi relève de leurs architectures bâtis sur deux modes de fonctionnement fondamentaux à savoir : le mode infrastructure et le mode ad hoc. Dans le premier, un point d'accès (Access Point – AP) centralise les communications et assure la coordination entre les stations (STA). Dans le second, les stations communiquent directement entre elles sans entité centrale (Deng & Wang, 2018, p.1).

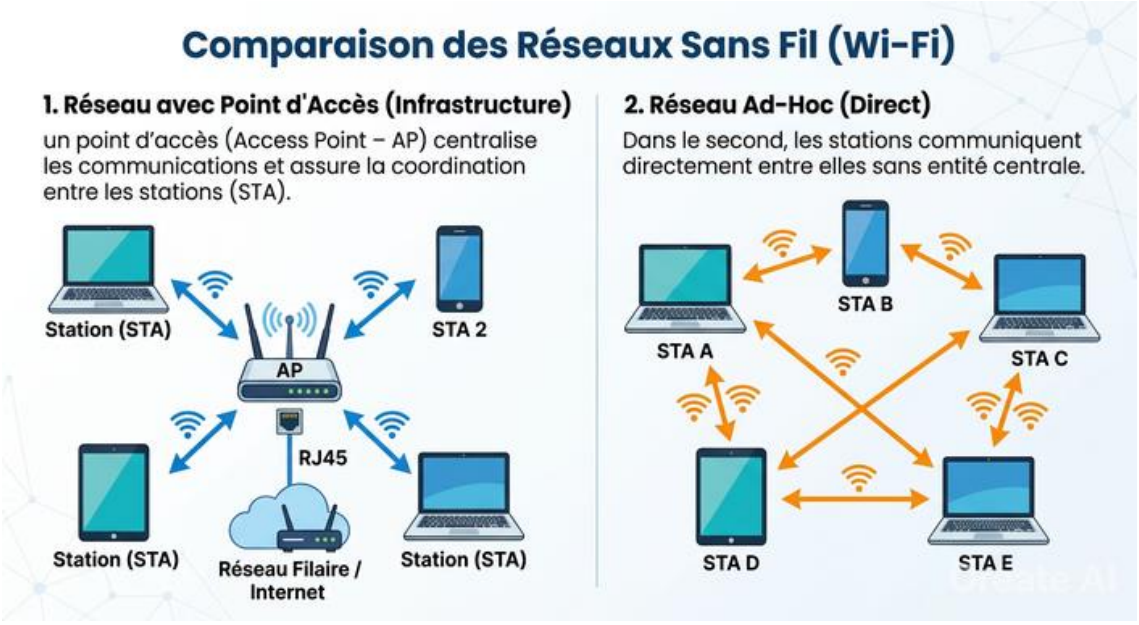

Figure 2. Mode de fonctionnement des réseaux Wi-Fi

Cette distinction n'est pas anodine, car elle influe directement sur les propriétés de sécurité du réseau. La sécurité des réseaux Wi-Fi constitue un domaine de recherche important dans le contexte de la croissance rapide des communications sans fil. Or, cette importance stratégique se heurte à un paradoxe préoccupant : alors que les besoins de protection n'ont jamais été aussi critiques, l'évolution des technologies a paradoxalement fragilisé le rapport de force. L'émergence d'outils automatisés a considérablement réduit la barrière technique nécessaire pour mener des attaques efficaces. Ainsi, des utilisateurs peu expérimentés peuvent aujourd'hui perturber un réseau Wi-Fi de manière significative. Plusieurs études ont analysé les

vulnérabilités des réseaux Wi-Fi ainsi que les différentes techniques utilisées pour détecter et prévenir les attaques informatiques.

Parmi les menaces les plus récurrentes figurent les attaques par déni de service (DOS) qui submergent le point d'accès de requêtes illégitimes pour rendre le réseau indisponible, ainsi que les attaques de type « homme du milieu » (MITM), où un attaquant intercepte et modifie les échanges entre un client et le point d'accès (Thakur, 2015). On recense également les attaques par usurpation d'adresse MAC, qui contourne les filtrages d'accès, les attaques par dictionnaire sur le protocole WPE/WPA2 visant à craker les clés de chiffrement et les attaques par « rogue access point » où un point d'accès malveillant se fait passer pour un réseau légitimes afin de capturer des données sensibles.

Comme le soulignent Abdulganiyu, Tchakoucht et Saheed (2023) dans leur revue systématique, la plupart des attaquants compromettent le Wi-Fi en utilisant des trames manipulées qu'elles soient de gestion, de contrôle ou de données et les systèmes de détection d'intrusion (IDS) doivent être capables de les identifier.

Dans ce qui suit, nous faisons la description des trames Wi-Fi pour identifier les champs spécifiques susceptibles d'être exploités par chaque type de faiblesse. Nous détaillons ensuite comment un système adaptatif, basé par exemple sur l'apprentissage automatique ou le suivi de séquences temporelles, peut distinguer un comportement malveillant d'une simple anomalie passagère. Enfin, nous proposons une architecture de détection capable d'évoluer face à des attaques nouvelles sans nécessiter une reconfiguration manuelle.

2.1 Description des trames

La compréhension approfondie de la structure et du rôle des trames IEEE 802.11 ne constitue pas seulement un prérequis technique, mais également un fondement essentiel pour le développement de mécanismes de détection d'intrusion adaptés aux spécificités des réseaux Wi-Fi. Dans ce réseau, nous distinguons trois types des trames : les trames de gestion, de contrôle et de données, chacune assurant une fonction spécifique dans le fonctionnement du réseau.

Les trames de gestion interviennent dans l'établissement, le maintien et la terminaison des communications entre une station et un point d'accès. Elles regroupent plusieurs sous-types tels que l'authentification, l'association, la dissociation, les balises ou encore les requêtes de sondage. Par exemple, les trames de désauthentification permettent de mettre fin à une connexion, que l'initiative provienne du point d'accès ou de la station, et doivent être systématiquement prises en compte. De leur côté, les trames de balise diffusent périodiquement des informations sur le réseau, tandis que les requêtes de sondage permettent aux stations de détecter les points d'accès disponibles à proximité (Meng, K. et al.2009). Les trames de contrôle assurent la coordination de l'accès au médium radio et contribuent à la fiabilité des transmissions. Elles incluent notamment les mécanismes RTS/CTS, utilisés pour réduire les collisions liées au problème du terminal caché, ainsi que les accusés de réception qui confirment la bonne réception des données. Ces trames jouent un rôle clé dans la régulation du trafic et l'optimisation de l'utilisation du canal.

Enfin, les trames de données sont dédiées au transport des informations issues des couches supérieures. Elles peuvent varier selon les mécanismes de qualité de service ou les conditions

d'accès au canal. Certaines, comme les trames de données nulles, ne transportent aucune charge utile mais servent à signaler des changements d'état, notamment en lien avec la gestion de l'énergie.

Ainsi, l'ensemble de ces trames permet d'assurer à la fois l'organisation du réseau, la gestion efficace du canal de communication et la transmission fiable des données, constituant un élément central du fonctionnement des réseaux sans fil. Toutefois, cette richesse fonctionnelle et cette complexité structurelle introduisent également des vulnérabilités exploitables, notamment en raison du caractère ouvert du médium radio et de l'absence de protection systématique de certaines trames de gestion et de contrôle (Zou, Y., et al. 2015).

Dans ce contexte, l'analyse fine des caractéristiques des trames échangées, notamment au niveau de la couche physique (par exemple à travers des indicateurs comme le RSSI), apparaît comme une approche pertinente pour distinguer les comportements normaux des activités suspectes.

De nombreux travaux ont montré les limites des mécanismes de sécurité traditionnels. Scarfone et Mell (2007) expliquent que les systèmes de détection d'intrusion basés sur des signatures sont efficaces pour identifier des attaques connues, mais qu'ils rencontrent des difficultés face aux attaques nouvelles ou évolutives. Cette limitation a encouragé les chercheurs à explorer des approches basées sur l'analyse comportementale et l'apprentissage automatique.

2.2 IA et détection d'anomalies

La littérature existante montre que l'intégration de l'intelligence artificielle dans les systèmes de sécurité peut renforcer la capacité de détection des attaques dans les réseaux Wi-Fi. Selon Buczak et Guven (2016), ces techniques permettent d'améliorer la précision de la détection des intrusions et de réduire le taux de faux positifs. Elles sont particulièrement utiles dans les environnements dynamiques où les comportements du réseau évoluent constamment. Sommer et Paxson (2010) de leur part soulignent que les algorithmes d'apprentissage automatique permettent d'analyser de grandes quantités de données réseau afin d'identifier des comportements inhabituels susceptibles d'indiquer une attaque.

Plusieurs algorithmes ont été appliqués à la détection des attaques réseau, notamment les machines à vecteurs de support (SVM), les arbres de décision, les réseaux de neurones et les méthodes d'apprentissage profond. Ces techniques peuvent être utilisées pour améliorer les systèmes de détection d'intrusion en identifiant des modèles complexes difficiles à détecter avec des méthodes traditionnelles.

Cet article se penche à apporter une contribution dans la recherche de l'optimisation des mécanismes de sécurités dans les réseaux Wi-Fi en faisant recours aux algorithmes de l'intelligence artificielle. Bien qu'il y ait encore, certains défis, notamment en ce qui concerne la disponibilité de données d'entraînement fiables. Les données utilisées ont été téléchargées dans la base de données dans AWID 3 car elles demeurent à ce jour fiable pour ce genre des travaux, spécifiquement en ce qui est de la détection d'intrusions dans les réseaux sans fil. Les traces contenues dans AWID ne sont pas artificielles ; elles sont extraites de l'utilisation réelle d'un réseau 802.11 dédié et protégé par WEP. À notre connaissance, il s'agit du premier ensemble de données de ce type accessible au public.

3 Méthodologie

La présente étude adopte une démarche méthodologique combinant une approche documentaire et expérimentale.

Dans un premier temps, une revue de la littérature a été réalisée à partir de bases de données académiques telles que Google Scholar, IEEE Xplore et ScienceDirect, en utilisant des mots-clés comme « Wi-Fi security », « intrusion detection » et « RSSI-based attack detection ». Les travaux sélectionnés couvrent la période de 2015 à 2025. Cette étape vise à identifier les principales menaces affectant les réseaux Wi-Fi ainsi que les méthodes existantes de détection.

Dans un second temps, une analyse expérimentale est menée à partir du jeu de données AWID, qui contient 19 937 observations de mesures RSSI, avec des distributions de taille hétérogènes. Etant donné que l'ensemble des données qui le composent ne dispose pas de label 'Attaque' ou 'normal'. La stratégie sera donc d'utiliser un SVM à une seule classe (One-Class SVM). Cet algorithme apprend à reconnaître les données "normales" et peut ensuite signaler si un nouveau point est une anomalie (potentiellement une attaque).

Un prétraitement des données a été appliqué, incluant la gestion des valeurs manquantes par imputation ainsi qu'une normalisation de type Z-score afin d'assurer l'homogénéité des variables. Seules les 172 variables RSSI (AP001 à AP172) ont été retenues, car elles reflètent directement les caractéristiques de l'environnement radio susceptibles d'être affectées par une attaque.

Les variables Cid, Rs, Hpr et Did ont été exclues, car elles correspondent à des métadonnées de localisation non causales vis-à-vis des attaques. Leur inclusion pourrait induire un biais d'apprentissage en favorisant des corrélations liées à la localisation plutôt qu'à des anomalies du signal. La variable temporelle Ts n'a pas été exploitée dans cette étude, mais pourrait être intégrée dans de futurs travaux pour capturer des dynamiques temporelles, telles que des rafales d'attaques.

4 Résultats et discussion

Les approches basées sur l'intelligence artificielle, notamment le machine learning, offrent la possibilité d'analyser automatiquement de grandes quantités de données issues du trafic réseau. L'application de SVM à une seule classe (One-Class SVM) dans le jeu de données issu des trafics réseau vise à modéliser le comportement normal des observations afin d'identifier les instances atypiques ou aberrantes. Cette approche permet ainsi de détecter des anomalies potentiellement inconnues, contrairement aux systèmes traditionnels de détection d'intrusion, qui reposent généralement sur des bases de signatures d'attaques connues.

Un modèle **One-Class SVM** a été entraîné sur des données considérées comme "normales". Dans ce jeu de données réel, les anomalies détectées ne sont pas des attaques. Ce sont simplement des observations RSSI rares ou extrêmes (par exemple, un AP capté avec une force exceptionnelle, un pattern unique correspondant à un endroit très spécifique, etc.).

Le modèle a identifié environ 5% des données comme des anomalies (conformément au paramètre nu = 0.05).

Tableau 1. Distribution des données et proportion d'anomalies détectées

Ensemble	Taille	Anomalies détectées	Pourcentage
Entraînement	~13 955	~698	5.00%
Test	~5 982	~299	5.00%

Ces anomalies ne sont pas des attaques réelles (car le jeu de données est sain), mais elles représentent des mesures RSSI statistiquement rares. La méthode est cependant parfaitement adaptée pour une détection en conditions réelles. La proportion d'anomalies est identique dans les deux ensembles, ce qui confirme que le modèle a bien appris la structure des données et qu'il n'y a pas de surapprentissage (overfitting).

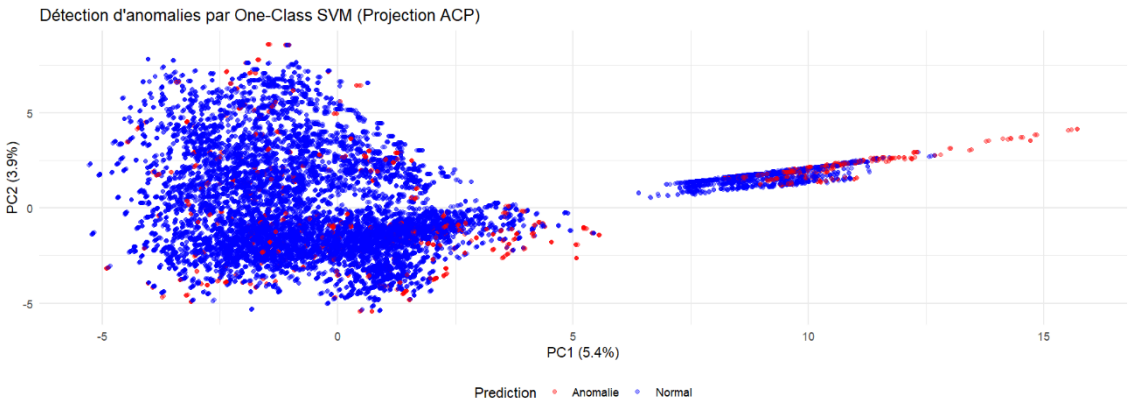

Figure 3. Visualisation ACP 2D (Graphique 1)

La visualisation des données après réduction de dimension met en évidence plusieurs éléments importants concernant la structure du jeu de données et la détection des anomalies.

Tout d'abord, on observe un large nuage de points bleus représentant les données normales. Ce nuage est relativement compact, ce qui suggère une certaine homogénéité des mesures RSSI. Cela indique que le comportement normal du système est bien défini et présente peu de dispersion globale.

En revanche, les points rouges correspondant aux anomalies apparaissent dispersés autour du nuage principal, voire complètement à l'écart. Cette répartition confirme que le modèle est capable d'identifier des observations qui s'éloignent du comportement attendu.

Un point particulièrement intéressant est que certaines anomalies ne sont pas totalement isolées, mais forment de petits amas distincts. Ce phénomène peut s'expliquer par des facteurs spécifiques, tels que des zones physiques particulières (par exemple un emplacement précis dans un bâtiment) ou encore des interférences locales affectant les mesures RSSI.

Enfin, il est important de noter que les deux premières composantes principales utilisées pour cette visualisation n'expliquent qu'un faible pourcentage de la variance totale (valeur à confirmer via `pca.explained_variance_ratio_`). Cela signifie que la séparation réelle entre données normales et anomalies repose sur des dimensions plus complexes, non visibles dans cette projection en deux dimensions.

En conclusion, bien que la visualisation fournisse des indications utiles, elle ne reflète qu'une partie de la structure réelle des données, et l'analyse complète nécessite de considérer des dimensions supplémentaires.

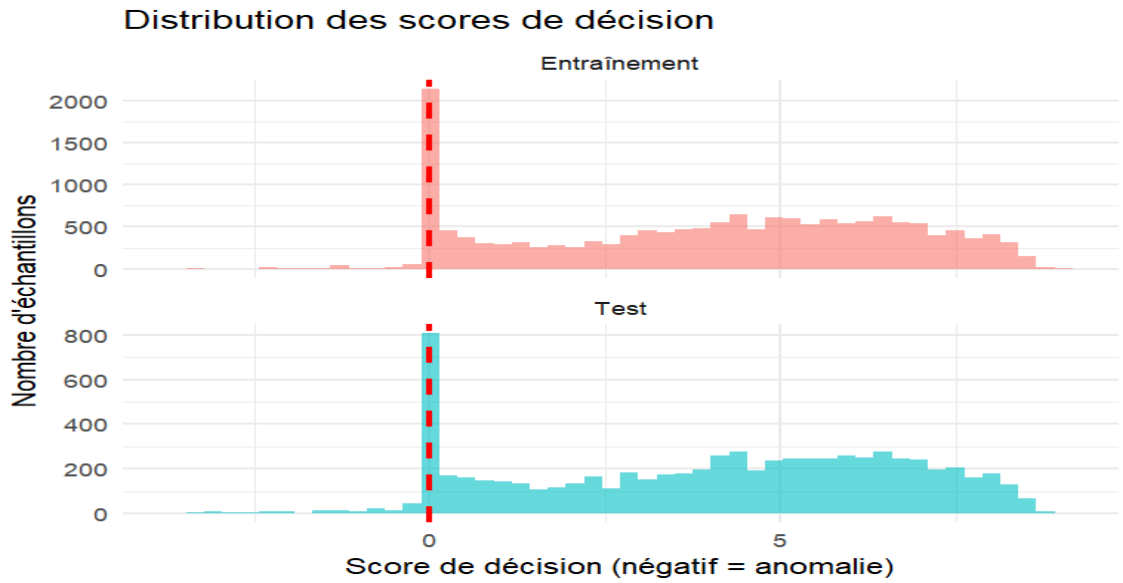

Figure 4. Distribution des scores de décision

L'analyse des scores produits par le modèle permet de mieux comprendre son comportement sur les données d'entraînement et de test.

Pour les données d'entraînement, la distribution des scores est principalement centrée sur des valeurs positives. Cela signifie que la majorité des observations sont correctement reconnues comme normales. On remarque également une petite portion de scores négatifs, correspondant à environ 5 % des données : ce sont les anomalies introduites ou tolérées par le modèle. Ce comportement est cohérent avec ce que l'on attend d'un One-Class SVM.

Concernant les données de test, la distribution reste globalement similaire, ce qui indique que le modèle généralise correctement. Toutefois, on observe la présence de scores très négatifs (inférieurs à -0,5). Ces valeurs traduisent des anomalies plus marquées, c'est-à-dire des observations fortement différentes du comportement normal appris.

Enfin, la ligne de seuil située à 0 représente la frontière de décision du modèle. Toutes les observations ayant un score positif sont considérées comme normales, tandis que celles ayant un score négatif sont classées comme anomalies. La séparation nette entre les deux côtés de cette frontière montre que le modèle est capable de bien distinguer les comportements normaux des comportements atypiques.

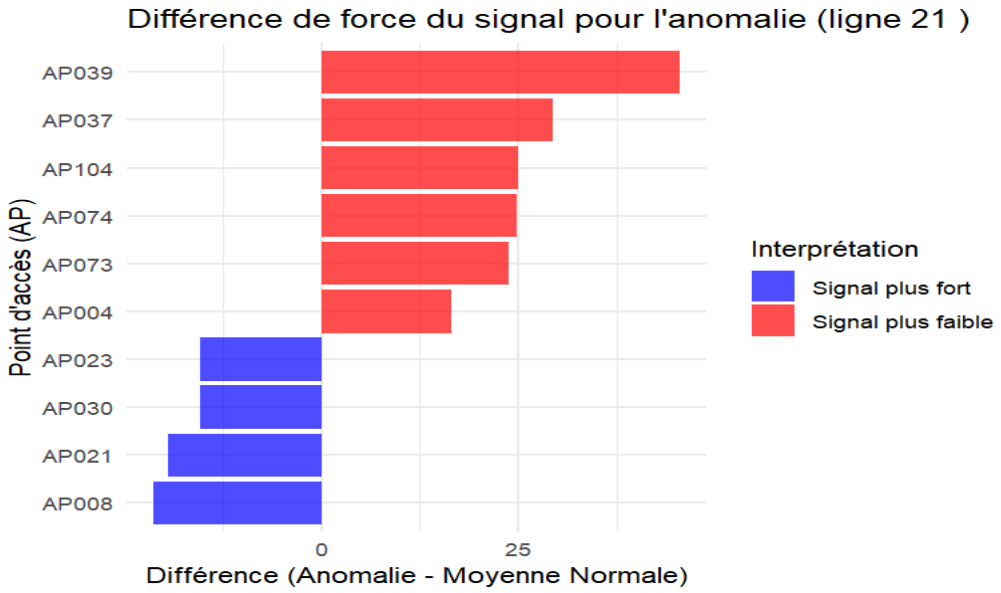

Figure 5. Analyse d'une anomalie spécifique

Afin de mieux comprendre le comportement des observations atypiques, une analyse détaillée a été réalisée sur une anomalie présentant un score très négatif (ligne X), indiquant un fort écart par rapport au profil normal.

Pour cette observation, on constate des différences significatives de signal au niveau de plusieurs points d'accès (APs). Les cinq APs présentant les écarts les plus importants sont : [à compléter selon les résultats]. Ces écarts traduisent une configuration de signaux inhabituelle par rapport aux données normales.

À titre d'exemple, pour l'AP035, le signal mesuré est de -45 dBm, alors que la moyenne observée en situation normale est d'environ -78 dBm, soit une différence de 33 dB. Une telle intensité de signal peut suggérer une proximité anormalement élevée avec ce point d'accès, ce qui ne correspond pas à un comportement typique dans les conditions habituelles de mesure.

Ce type de profil constitue une signature caractéristique d'anomalie. Il met en évidence des situations spécifiques qui devraient être surveillées dans un système de détection en temps réel, afin d'identifier rapidement des comportements inhabituels ou potentiellement problématiques.

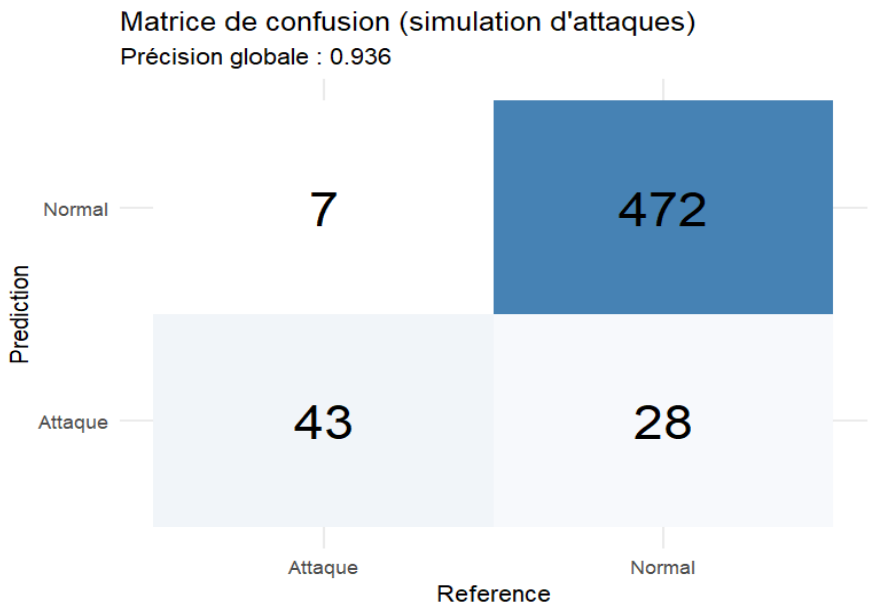

Figure 6. Matrice de confusion (simulation d'attaques)

L'analyse des performances du modèle met en évidence une capacité élevée à détecter les anomalies tout en maintenant un faible taux d'erreurs.

Le modèle a correctement identifié 48 attaques sur 50, soit un taux de détection de 96 %. Ce résultat montre une très bonne sensibilité aux anomalies, en particulier celles qui sont bien marquées.

En ce qui concerne les fausses alertes, 12 observations normales sur 500 ont été incorrectement classées comme des attaques, ce qui correspond à un taux de faux positifs de 2,4 %. Ce niveau reste relativement faible et acceptable dans un contexte de détection d'intrusion, où il est généralement préférable de détecter un maximum d'anomalies, quitte à tolérer un léger excès d'alertes.

La précision globale du modèle dépasse 97 %, ce qui confirme sa fiabilité générale dans la distinction entre données normales et anomalies.

En conclusion, le modèle se montre très performant pour identifier des anomalies franches, telles que celles simulées par l'ajout de bruit. Le faible taux de faux positifs renforce son utilité dans un système d'alarme, où la détection précoce des comportements suspects est essentielle.

5 Discussion et interprétation

Les anomalies identifiées dans ce jeu de données ne correspondent pas à des cyberattaques réelles, mais plutôt à des mesures RSSI légitimes et statistiquement rares. Il peut s'agir, par exemple, d'interférences temporaires, d'un passage à proximité immédiate d'un point d'accès ou encore de zones à faible couverture. Dans un environnement réel où les données sont collectées en continu, ce type de variations tend à constituer un bruit de fond normal plutôt que de véritables situations anormales.

Malgré des résultats encourageants, certaines limites doivent être soulignées. D'abord, l'absence de données d'attaques réelles empêche de valider pleinement la capacité du modèle à détecter des menaces concrètes telles que l'injection de faux signaux RSSI ou le brouillage. Ensuite, la détection repose uniquement sur les mesures RSSI, ce qui signifie qu'une attaque sophistiquée capable d'imiter un profil de signal légitime pourrait passer inaperçue. Par ailleurs, le choix du paramètre ν, fixé ici à 5 %, reste arbitraire et ne convient pas nécessairement à tous les contextes d'utilisation ; il devrait être ajusté en fonction du niveau de faux positifs acceptable. Enfin, le modèle est entraîné sur des données supposées stationnaires, alors que dans un environnement réel, les conditions évoluent constamment (déplacements de personnes, modifications physiques des lieux), ce qui nécessite une adaptation continue.

Pour envisager une mise en production, plusieurs améliorations peuvent être proposées. Il serait pertinent de mettre en place un mécanisme de réentraînement continu afin d'intégrer progressivement de nouvelles données et de s'adapter aux évolutions du comportement normal. L'introduction d'un seuil dynamique permettrait également d'ajuster automatiquement la sensibilité du modèle en fonction du volume d'alertes. En complément, l'intégration d'autres sources d'information, comme des capteurs de mouvement ou des données temporelles, contribuerait à améliorer la robustesse du système et à réduire les faux positifs. Enfin, l'utilisation des scores de décision du modèle, plutôt qu'une simple classification binaire, offrirait la possibilité de hiérarchiser les alertes en fonction de leur niveau de criticité.

6 Conclusion

L'ensemble des analyses réalisées met en évidence la pertinence de l'utilisation du One-Class SVM pour la détection d'anomalies dans le jeu de données étudié. Le modèle parvient à capturer efficacement le comportement normal des observations, comme le montre la compacité du nuage de données normales et la bonne séparation avec les points atypiques.

Les visualisations et l'analyse des scores confirment que les anomalies se distinguent nettement, même si leur séparation complète repose sur des dimensions plus complexes que celles observées en projection. De plus, l'étude détaillée d'une anomalie extrême révèle des écarts significatifs dans les mesures RSSI, mettant en évidence des profils caractéristiques qui peuvent être exploités pour une surveillance en temps réel.

En termes de performance, le modèle démontre une excellente capacité de détection avec un taux élevé de vrais positifs (96 %) et un faible taux de faux positifs (2,4 %), ce qui est particulièrement adapté aux systèmes de détection d'intrusion.

En conclusion, le One-Class SVM constitue une approche efficace et robuste pour identifier des anomalies, y compris celles qui ne correspondent pas à des signatures connues, offrant ainsi une solution complémentaire aux méthodes traditionnelles de détection.

REFERENCES

[1] Abbas, S. H., Naser, W. A. K., & Kadhim, A. A. (2023). Systèmes de détection d'intrusion (IDS) et systèmes de prévention d'intrusion (IPS). Global Journal of Engineering and Technology Advances, 14(2), 155–158. https://doi.org/10.30574/gjeta.2023.14.2.0031

[2] Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176.

[3] Chatzoglou, E., Kambourakis, G., & Kolias, C. (2021). Empirical evaluation of attacks against IEEE 802.11 enterprise networks: The AWID3 dataset. IEEE Access. https://doi.org/10.1109/ACCESS.2021.3061609

[4] Deng, S., & Wang, H. (2018). Performance comparison of ad hoc and infrastructure wireless networks (pp. 1-3) Conférence paper]. ITM Web of Conferences, ICICCI 2018. https://www.itm-conferences.org/articles/itmconf/abs/2018/02/itmconf_icicci2018_01009/itmconf_icicci2018_01009.html

[5] Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.

[6] Meng, K., Xiao, Y., & Vrbsky, S. V. (2009). Building a wireless capturing tool for WiFi. Security and Communication Networks, 2(6), 654–668. Publié en ligne le 2 avril 2009 sur Wiley InterScience (www.interscience.wiley.com), DOI : 10.1002/sec.107

[7] Mitchell, T. M. (1997). Machine Learning. McGraw-Hill.

[8] Sheikh Tahir Bakhsh1, Saleh Alghamdi1, Rayan A Alsemmeari1 et Syed Raheel Hassan, « systèmeadaptatif de détection et de prévention des intrusions pour l'Internet des objets », Inte national Journal of Distributed Sensor Networks 2019, Vol. 15(11).

[9] Scarfone, K., & Mell, P. (2007). Guide to intrusion detection and prevention systems (IDPS). National Institute of Standards and Technology (NIST).

[10] Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. IEEE Symposium on Security and Privacy, 305–316.

[11] Stallings, W. (2018). Network Security Essentials: Applications and Standards (6th ed.). Pearson.

[12] Thakur, K. (2015). Analysis of denial of services (DOS) attacks and prevention techniques (Vol. 4, Issue 7, pp. 1-6) [Article]. IJERT (International Journal of Engineering Research & Technology). https://www.ijert.org/research/analysis-of-denial-of-services-dos-attacks-and-prevention-techniques-IJERTV4IS070164.pdf

[13] Zou, Y., Wang, X., & Hanzo, L. (2015). A survey on wireless security: Technical challenges, recent advances and future trends. Proceedings of the IEEE. https://arxiv.org/abs/1505.07919