République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Abderrahmane Mira
Faculté des Sciences Exactes
Département d'Informatique

Mémoire de Master Recherche en Informatique

Option :
Réseaux et Sécurité

Thème

Vers une approche innovante pour renforcer la confiance dans les systèmes ferroviaires intelligents

Préparé par :

Mlle Kessouri Doua
Mlle Mahmoudi Zohra

Président	Dr. M. SADI	Maître de conf. B	U. A/Mira Béjaia.
Encadrante	Dr. N. Yessad	Maître de conf. B	U. A/Mira Béjaia.
Co-encadrante	Dr. D. Zamouche	Maître de conf. B	U. A/Mira Béjaia.
Examinatrice	Pr. L. Bouallouche	Professeur	U. A/Mira Béjaia.
Examinatrice	Dr. N. Bouadem	Maître de conf. B	U. A/Mira Béjaia.
Examinatrice	Dr. S. Ouyahia	Maître de conf. B	U. A/Mira Béjaia.

Année universitaire : 2024/2025

Remerciements

À l'issue de ce travail , nous exprimons notre profonde gratitude et adressons nos plus sincères remerciements à toutes les personnes qui ont contribué à la réalisation de ce mémoire.

Nous remercions Dieu le Tout-Puissant pour nous avoir accordé la force et la patience nécessaires à l'accomplissement de ce travail.

Nous exprimons notre sincère reconnaissance à **Madame Yessad Nawal**, notre encadrante, pour son accompagnement exemplaire, sa disponibilité et la qualité de ses conseils tout au long de ce travail. Sa rigueur scientifique, sa patience et sa bienveillance ont été déterminantes pour la réussite de ce mémoire.

Nous tenons remercier tout particulièrement **Madame Zamouche Djamila**, notre co-encadrante, pour son écoute attentive, ses orientations précieuses et ses encouragements continus. Sa disponibilité, son professionnalisme et ses remarques pertinentes ont grandement enrichi la qualité de notre travail et nous ont permis de progresser avec confiance à chaque étape de ce mémoire.

Nous adressons nos remerciements aux membres du jury pour le temps qu'ils ont consacré à l'évaluation de notre travail et pour leur attention.

Enfin, Nous tenons à remercier tous nos enseignants et le département d'informatique de l'Université de Béjaïa pour leur enseignement de qualité et leur accompagnement précieux durant toutes nos années d'études.

À tous, nous disons merci du fond du cœur.

Dedicace

À ceux qui ont rempli ma vie d'amour, de lumière et de force,
Ce mémoire est une fleur née de vos racines.

À celle que je suis devenue,
Pour avoir avancé avec courage, portée par l'amour des miens et ma propre volonté.
Ce mémoire est l'aboutissement d'un voyage riche d'apprentissages et de résilience.

À mon cher Papa, pilier silencieux de ma vie, Kessouri Messouad,
Tu es ce regard plein de fierté qui dit tout sans un mot.
Ton amour, discret mais immense, m'a portée dans les moments de doute.
Tu es ma force tranquille, mon exemple de droiture.

À ma douce Maman, lumière de mon chemin, Dalila Sissaoui,
Tu es la première voix qui m'a bercée, la première main qui m'a guidée.
Ton amour m'a appris la tendresse, ta force m'a enseigné le courage.
Dans chacun de mes pas, il y a un peu de ton cœur,
Et dans chacune de mes victoires, il y a ton âme qui m'élève.

À mes précieuses sœurs, Rania et Malek, mes éclats de vie,
Vous êtes mes alliées, mes rires d'enfance devenus les bras de l'avenir.
Je vous aime d'un amour qui ne se mesure pas.

À mon oncle adoré Adelan et son épouse bienveillante,
Merci pour votre tendresse, vos encouragements silencieux et votre présence fidèle.

À mes tendres tantes Fadila, Fatiha et Dounia,
Votre amour m'a entourée comme un manteau de douceur.
Merci pour chaque prière, chaque mot rassurant, chaque regard bienveillant.

À mes chers grands-parents, étoiles toujours présentes dans mon cœur,
Vous avez laissé des empreintes dans mon cœur que le temps ne pourra jamais effacer.
Je vous dédie cette réussite, avec tout l'amour que je n'ai pas eu assez de temps pour vous dire.

À toi, Zohra, mon binôme de cœur, mon soutien indéfectible, mon amie,
Nous avons tout traversé ensemble : les hauts, les bas, les doutes et les réussites.
Merci d'avoir été à mes côtés avec ton cœur grand ouvert.

À mes amis fidèles, Razane, Ibtissem, Laetitia et Ahmed,
Merci d'avoir coloré mon quotidien, allégé mes pensées, et cru en moi quand j'en avais le plus besoin.

Mlle KESSOURI Doua

Dedicace

Je dédie ce mémoire

À mes parents adorés , pour leur amour inconditionnel, leurs encouragements continus,et leur confiance en moi. Je ne saurais assez les remercier pour leur soutien. Que Dieu les protège et les récompense pour tout ce qu'ils m'ont offert.

À ma sœur Ilyna, et mes frères Samir et Mourad , pour tout l'amour qu'ils m'ont donné, leur présence et leur encouragement tout au long de mon parcours .Votre amour m'a portée plus que vous ne pouvez l'imaginer.

À ma meilleure amie d'enfance, Ouardia ,pour tous les beaux souvenirs partagés, pour son amitié sincère, sa présence et son soutien .

À ma chère binôme Doua , pour sa gentillesse, son soutien , sa douceur, sa patience et son engagement tout au long de ce travail. Merci d'avoir été là à chaque étape, avec le cœur, avec le sourire, et avec tant de bienveillance.

Et enfin, à tous ceux que j'aime et qui m'aiment d'un amour sincère.

Merci pour votre soutien et vos encouragements, qui ont été une source constante de motivation pour moi.

Mlle MAHMOUDI Zohra

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

ABAC	Attribute-Based Access Control
AI	Intelligence Artificielle
ANFIS	Adaptive Neuro-Fuzzy Inference System
AP	Access Point
ATO	Automatic Train Operation
ATP	Automatic Train Protection
ATS	Automatic Train Supervision
AVISPA	Automated Validation of Internet Security Protocols and Applications
CBTC	Communications-Based Train Control
CI	Computer Interlocking
CKC	Cyber Kill Chain
CNN	Convolutional Neural Network
GRU	Gated Recurrent Unit
HSS	Home Subscriber Server
IBC	Identity-Based Cryptography
IMSI	International Mobile Subscriber Identity
IOWA	Induced Ordered Weighted Averaging
IT	Technologie de l'Information
IoT	Internet des Objets
LFSR	Linear Feedback Shift Register
LSTM	Long Short-Term Memory
LTE-R	Long-Term Evolution for Railways
MA	Movement Authority
MLP	Multilayer Perceptron
MME	Mobility Management Entity
OCU	Onboard Control Unit
OT	Operational Technology
PKI	Public Key Infrastructure
PRD	Progressive Residual Detection
RBAC	Role-Based Access Control

RDKC	Railway Defender Kill Chain
RNN	Recurrent Neural Network
SCADA	Supervisory Control and Data Acquisition
SRP	Secure Remote Password
SVD	Singular Value Decomposition
SVM	Support-Vector Machine
TC-CBTC	Train Control - Communications-Based Train Control
TBAC	Trust-Based Access Control
UE	User Equipment
VOBC	Vehicle Onboard Controller
ZC	Zone Controller

Introduction générale

L'avenir du secteur ferroviaire repose sur des systèmes de transport intelligents exploitant les technologies au sein d'un vaste réseau ferroviaire, visant à réduire son coût de cycle de vie. De nouveaux services, tels que la sécurité intégrée, la gestion d'actifs et la maintenance prédictive, contribuent à améliorer l'information et la prise de décision en temps opportun pour les aspects de sécurité opérationnelle, de programmation et de capacité du système.
Les infrastructures ferroviaires intelligentes regroupent un ensemble de solutions technologiques, parmi lesquelles le TC-CBTC (Transmission-based Communication and Control), conçu pour assurer un fonctionnement optimisé et sécurisé du matériel grâce à des communications continues et fiables entre les trains et les centres de contrôle.

Toutefois, malgré les nombreux avantages offerts par ces systèmes intelligents, la complexité croissante et l'interconnexion des systèmes ferroviaires rendent la sécurité des communications un enjeu majeur. Dans un environnement aussi critique que celui des systèmes TC-CBTC, où les trains échangent continuellement des données pour calculer leur propre autorité de mouvement, la moindre défaillance ou donnée non fiable peut compromettre la sécurité globale du réseau. Dans ce contexte, plusieurs approches ont été proposées dans la littérature pour renforcer cette sécurité. Néanmoins, un aspect reste encore peu exploré : la gestion de la confiance entre les composants du réseau pour garantir la fiabilité et la sécurité du trafic. La problématique centrale de ce mémoire est de sécuriser la communication entre les trains dans un environnement TC-CBTC, en assurant une gestion efficace et dynamique de la confiance dans les données échangées, afin de renforcer l'efficacité opérationnelle et la fiabilité des services ferroviaires .

Dans ce travail, notre objectif est de concevoir une approche innovante pour renforcer la confiance dans les systèmes ferroviaires intelligents, en particulier dans les systèmes TC-CBTC. Pour y parvenir, nous nous appuyons sur une combinaison de modèles avancés d'apprentissage automatique. Ces modèles incluent les embeddings, qui transforment les données en vecteurs numériques, les réseaux de neurones convolutifs (CNN) pour l'extraction des caractéristiques, et les réseaux à mémoire long terme (LSTM) pour capturer les dépendances temporelles. Enfin, une distribution bêta est utilisée pour mettre à jour dynamiquement les scores de confiance, permettant aux trains de prendre des décisions sécurisées. La solution proposée permet de détecter rapidement les comportements anormaux dans la communication grâce à une gestion efficace de la confiance, ce qui améliore considérablement la sécurité des systèmes TC-CBTC.

Ce mémoire est structuré en quatre parties principales :

Le chapitre 1 introduit les systèmes ferroviaires intelligents, leur évolution, les systèmes de contrôle modernes comme le TC-CBTC, et l'importance de la confiance dans les communications. Ce chapitre aborde également les risques d'attaques et l'apport de l'intelligence artificielle, en particulier l'apprentissage profond, pour renforcer la fiabilité.

Le chapitre 2 approfondit notre étude en offrant une revue complète des approches existantes visant à améliorer la sécurité et la fiabilité des réseaux ferroviaires.

Le chapitre 3 présente notre approche batisée "RailTrust" intégrant les techniques d'apprentissage automatique (Embeddings, CNN, LSTM, Distribution bêta), avec une description détaillée des étapes de construction du modèle.

Enfin, le chapitre 4 évalue la performance de notre modèle à travers les métriques de précision, rappel, F1-mesure, afin de démontrer son efficacité dans des scénarios réalistes.

1

Généralités sur les systèmes ferroviaires intelligents

1.1 Introduction

Ces dernières années, les systèmes ferroviaires intelligents ont suscité un intérêt professionnel grandissant parmi les chercheurs universitaires, les entreprises du secteur industriel et les autorités, étant perçus comme la prochaine grande révolution technologique

Dans ce premier chapitre, nous présenterons les systèmes ferroviaires intelligents pour établir le contexte de notre travail, en mettant l'accent sur les systèmes Communication-Based Train Control (CBTC) et Train-Centric Communication-Based Train Control (TC-CBTC). Nous aborderons également la notion de confiance en détaillant sa définition, sa gestion, et les menaces potentielles, tout en soulignant l'impact de l'Intelligence Artificielle (IA) dans ce domaine.

1.2 Les systèmes ferroviaires intelligents

1.2.1 Définition

Les systèmes ferroviaires désignent l'ensemble des infrastructures, équipements et technologies utilisés pour le transport de passagers et de marchandises par voie ferrée. Ils englobent les voies, les trains, les gares et les systèmes de contrôle, tout en étant soumis à des défis de sécurité, notamment face à des menaces physiques et cybernétiques. Leur efficacité et leur résilience sont essentielles pour garantir la ponctualité et la sécurité du transport [1].

1.2.2 Évolution des systèmes ferroviaires intelligents

Les systèmes ferroviaires intelligents ont évolué grâce à plusieurs étapes clés, chacune d'elles étant le résultat de progrès technologiques et améliorations en la gestion des opérations ferroviaires [2, 3]. Voici un survol de cette évolution :

- **Infrastructures ferroviaires numériques** : Cette étape a marqué le début de l'informatisation des systèmes ferroviaires. Les ressources ferroviaires et l'environnement d'exploitation ont été transformés en ressources de calcul numérique.
- **Infrastructures ferroviaires intelligentes 1.0 :** Cette étape a été caractérisée par l'intégration des données éclatées de multiples spécialités et entreprises en informations unifiées dans l'espace et le temps. Il en a résulté une optimisation collaborative des services de transport.
- **Infrastructures ferroviaires intelligentes 2.0 :** Cette étape est la plus avancée de l'évolution des systèmes ferroviaires intelligents. Elle utilise les technologies comme l'IoT, le big data, l'intelligence artificielle et la robotique pour des opérations autonomes et intelligentes.

1.3 Le Contrôle de Train Basé sur la Communication (CBTC)

1.3.1 Définition

Le Contrôle de Train Basé sur la Communication (CBTC) est un système moderne de signalisation ferroviaire qui agit comme le véritable « cerveau » des réseaux urbains. Il repose sur des communications bidirectionnelles et sans fil en temps réel entre les trains et les équipements au sol, permettant ainsi un contrôle dynamique, précis et sécurisé de la circulation ferroviaire. Contrairement aux systèmes traditionnels fondés sur des signaux fixes, le CBTC optimise la gestion du trafic, améliore la capacité des lignes et renforce la sécurité des opérations en milieu urbain [4, 5].

1.3.2 Composition du Système CBTC

Le système CBTC repose sur une combinaison de technologies et d'équipements organisés en trois catégories principales : les infrastructures au sol, les systèmes de communication et les équipements embarqués. [6]

1.3.2.1 Infrastructures au Sol

Les éléments au sol sont la base du système et comprennent :

- **Réseau de base au sol (Ground backbone network)** : Il sert de lien central, reliant les composants. Ce réseau intègre l'Interverrouillage Informatique (CI) pour gérer les signaux, le Contrôleur de Zone (ZC) pour superviser les sections des voies, et la Supervision Automatique des Trains (ATS) pour coordonner le trafic.

- **Éléments de signalisation** : Incluant des points, signaux, détecteurs d'essieux, balises et autres dispositifs, ils fournissent des données essentielles en temps réel.

1.3.2.2 Systèmes de Communication

Les systèmes de communication assurent une liaison sans fil entre les trains et les infrastructures au sol. Ils permettent une transmission rapide et fiable des données critiques, telles que la position et la vitesse des trains, grâce à des technologies avancées comme le LTE et des réseaux dédiés. Ces systèmes intègrent des points d'accès (AP) qui servent de nœuds clés pour faciliter une communication bidirectionnelle en temps réel, garantissant ainsi la sécurité et l'efficacité des opérations ferroviaires.

1.3.2.3 Équipements Embarqués

Les trains sont équipés de technologies clés pour un contrôle automatisé :

- **Système de Protection Automatique des Trains (ATP)** : Garantit la sécurité en surveillant les mouvements pour prévenir les incidents.
- **Système d'Opération Automatique des Trains (ATO)** : Optimise la conduite en automatisant les opérations.

L'architecture complète du système CBTC, illustrant l'interaction de ces composants, est présentée dans la Figure 1.1.

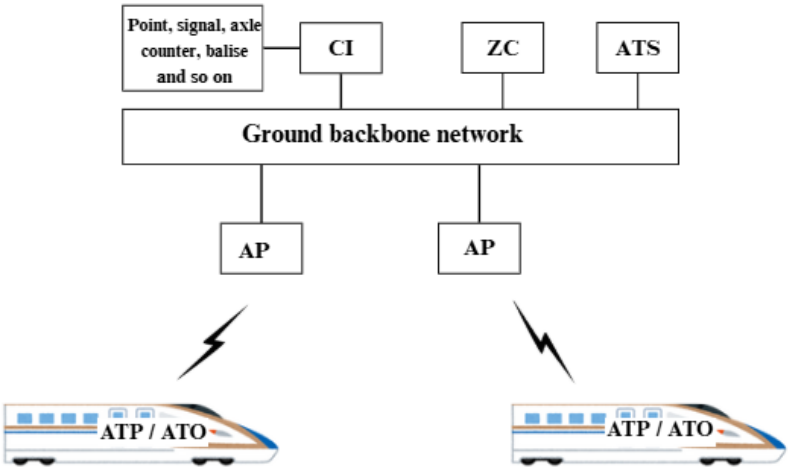

FIGURE 1.1 – L'architecture d'un système CBTC [6].

1.3.3 Fonctionnalités du CBTC

Le CBTC intègre un ensemble de fonctionnalités clés qui permettent une gestion intelligente, sûre et optimisée du trafic ferroviaire [7, 8] .

- **Protection de la vitesse :** Le système est chargé d'assurer en permanence la vitesse des trains afin de s'assurer qu'elle reste bien dans les limites autorisées.

Lorsque la vitesse libre est atteinte, un dispositif de freinage d'urgence est engagé automatiquement pour rendre la vitesse à une valeur considérée comme sûre. Le CBTC fait pour cela appel à des courbes de protection qui permettent de déterminer la distance à parcourir pour l'arrêt à partir de la vitesse du train, de la décélération maximale et de l'état de la voie.

- **Communication bidirectionnelle :** Le CBTC est un système qui repose sur la communication permanente entre les ordinateurs de bord des trains et les systèmes de commande fixés en ligne. Ce système autorise également des échanges directs entre trains, réduisant ainsi les délais de transmission d'informations, donc de coordination de leur mouvement. Grâce à cette communication bilatérale, chaque train transmet à l'autre sa position et sa vitesse, garantissant ainsi un mouvement fluide et sûr des trains..

- **Contrôle automatique des opérations :** La régulation de la performance des trains se fait en temps réel pour respecter les horaires et limiter les aléas. Elle assure un pilotage centralisé du trafic routier, rendant obsolètes les signaux lumineux traditionnels. Les trains peuvent désormais être entièrement gérés à distance ce qui améliore globalement efficacité et réactivité des systèmes.

- **Simplification des équipements en voie :** Le CBTC contribue à une réduction des équipements en voie puisque les systèmes d'interlocking traditionnels et les signaux lumineux y sont absents, et que le système repose sur des balises et des transpondeurs pour localiser les trains de manière plus précise et fiable, tout en réduisant les coûts de maintenance. Cela a pour effet de faciliter la gestion des infrastructures ferroviaires de façon plus efficace et plus économique

- **Sécurité et fiabilité :** Ce système repose sur des méthodes formelles, principalement topologiques, pour garantir la sécurité des opérations. Il s'accompagne de protections contre les pannes, permettant un arrêt sécurisé du train en cas de défaillance, et confie à des équipements embarqués et à des systèmes de contrôle en voie redondants la fiabilité et la disponibilité du système.

1.4 Le Contrôle de Train Basé sur la Communication Centré sur le Train (TC-CBTC)

1.4.1 Définition

Le TC-CBTC est un système de contrôle ferroviaire moderne qui simplifie les équipements le long des voies et intègre les calculs d'interverrouillage et de génération d'autorité de mouvement directement à bord des trains. Il utilise la communication sans fil pour permettre aux trains de communiquer entre eux, réduisant ainsi les intervalles entre les trains et améliorant l'efficacité. Ce système est conçu pour gérer les incertitudes comme les pannes de communication et les retards, en utilisant des méthodes formelles pour assurer la sécurité des opérations [9].

1.4.2 Architecture du TC-CBTC

L'architecture du système TC-CBTC est présentée dans la Figure 1.2 Comme la plupart des fonctions de contrôle des trains sont prises en charge par les équipements embarqués, les équipements en voie du système sont grandement simplifiés. Le système comprend principalement le système de supervision automatique des trains (ATS), l'unité de contrôle des objets en voie (OCU) et le contrôleur embarqué du véhicule (VOBC) [4] . Les communications associées aux équipements sont connectées aux trains et aux dispositifs associés via des points d'accès sans fil (AP), permettant une communication continue et fiable. Cette architecture réduit la complexité du système, améliore la performance et la sécurité des opérations ferroviaires, et répond mieux aux exigences futures des transports urbains.

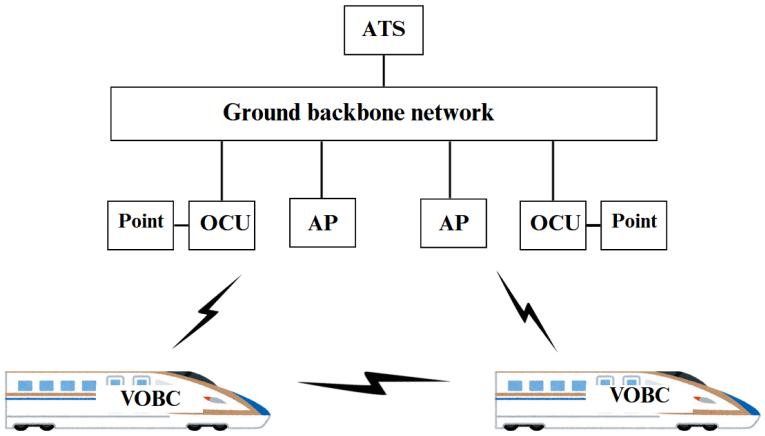

FIGURE 1.2 – L'architecture d'un système TC-CBTC [6].

1.4.3 Caractéristiques du TC-CBTC

Les principales caractéristiques du TC-CBTC englobent [9, 10] :

- **Architecture centrée sur le train** : Contrairement aux systèmes CBTC traditionnels qui sont centrés sur le sol, le TC-CBTC déplace une grande partie des responsabilités et des fonctionnalités vers les équipements embarqués à bord des trains. Cela rend le système plus simple et plus facile à entretenir.
- **Communication train-train** : Les trains échangent des informations entre eux grâce à une connexion sans fil. Cette communication en temps réel leur permet de s'adapter rapidement à la situation, de se coordonner et d'optimiser la circulation.
- **Calcul de l'autorité de mouvement (MA)** : Chaque train est capable de faire ses propres calculs concernant l'autorité de mouvement, comme savoir jusqu'où il peut aller et à quelle vitesse, sans attendre des instructions d'un système central, ce qui permet une prise de décision plus rapide.
- **Réduction des infrastructures au sol** : Le TC-CBTC réduit la nécessité de poser autant de matériel au sol, ce qui diminue les coûts et la complexité de la gestion des infrastructures, tout en augmentant l'efficacité du système.

- **Sécurité fonctionnelle renforcée** : Le TC-CBTC utilise des méthodes mathématiques avancées, comme les réseaux de Petri colorés, pour modéliser et vérifier les procédures de contrôle des trains, assurant ainsi la sécurité dans toutes les situations possibles.

1.4.4 Autorité de Mouvement (MA)

L'Autorité de Mouvement (MA) est un concept central dans les systèmes de contrôle de train basés sur les communications, comme le système TC-CBTC. Elle représente l'autorisation pour un train d'entrer et de circuler sur une section spécifique de la voie dans une direction donnée, tout en maintenant des séparations sûres entre les trains. Le calcul de la MA est réalisé par le Vehicle On-Board Controller (VOBC) en fonction des données transmises en continu entre les équipements embarqués des trains et les sous-systèmes de contrôle en voie, tels que l'ATS (Automatic Train Supervision) et l'OCU (Object Control Unit) [7].

1.5 Sécurité dans les systèmes ferroviaires

Dans les systèmes ferroviaires intelligents, la protection des données et la sécurisation des communications représentent des enjeux cruciaux. La numérisation croissante et l'interconnexion des sous-systèmes exposent les échanges d'informations sensibles à divers risques, pouvant compromettre la disponibilité, l'intégrité , la confidentialité et la confiance des données échangées entre les trains, les infrastructures au sol et les centres de contrôle [11, 12]. La cybersécurité vise ainsi à assurer la fiabilité des transmissions en prévenant les perturbations susceptibles d'affecter la continuité des opérations ferroviaires. L'analyse des risques constitue un levier essentiel pour identifier les vulnérabilités potentielles, évaluer les niveaux de menace et mettre en œuvre des mécanismes de protection adaptés, incluant notamment des protocoles de communication sécurisés, des systèmes de détection d'intrusion et des dispositifs de surveillance continue [13].

1.5.1 La Confiance

La confiance est un concept intervenant dans différentes disciplines, parmi lesquelles la philosophie, les sciences sociales et les technologies de l'information. Dans les systèmes ferroviaires intelligents, elle se rapporte à un lien établi entre deux entités : l'une déposant sa confiance, l'autre en étant le bénéficiaire, et ce dans un contexte donné. Dans les systèmes ferroviaires intelligents, la confiance revêt une importance particulière en raison de la nature mobile et dynamique des réseaux. Elle repose principalement sur l'exactitude des informations échangées entre les trains et les systèmes de commande, garantissant ainsi la sûreté et l'efficacité des opérations [14, 15].

1.5.2 Gestion de la confiance

La Gestion de la confiance [16, 17] est un élément clé dans les systèmes ferroviaires intelligents. Elle a pour but de sécuriser l'exactitude des échanges entre les différentes entités et de légitimité des informations qui sont échangées. La confiance repose sur deux principaux concepts : la confiance accordée aux entités et la confiance accordée aux données.

Confiance dans l'entité : Elle concerne la crédibilité des acteurs du système, comme les trains ou les capteurs. Pour exemple, un train doit pouvoir compter sur un autre train ou un capteur pour disposer des informations réelles et précises.

Confiance dans les données : Elle concerne l'estimation de la crédibilité des informations, sans tenir compte de leur émetteur. Un message reçu peut donc être jugé crédible ou non en fonction de sa cohésion avec d'autres informations en sa possession ou en fonction de sa provenance.

1.5.3 Attaques potentielles contre les mécanismes de gestion de la confiance

La gestion de la confiance dans les systèmes ferroviaires intelligents est confrontée à plusieurs défis et menaces [16]. Parmi celles-ci, on peut citer les attaques potentielles suivantes :

- **Injection de fausses données :** Une entité malveillante diffuse de fausses informations intentionnellement pour compromettre le bon fonctionnement du système.
- **Attaques par intermittence :** Une entité malveillante se met en alternance entre des comportements légitimes et malveillants pour ne pas être détecté.
- **Attaques de type Sybil :** Une entité malveillante crée et utilise plusieurs identités fictives pour tromper le système
- **Attaques par collusion :** Plusieurs entités malveillantes agissent de concert pour manipuler ou influencer le système à leur avantage.

1.6 L'Intelligence artificielle (IA)

L'intelligence artificielle (IA) regroupe un ensemble de techniques et de théories visant à développer des modèles capables de simuler le comportement humain [18]. À la base de cette discipline se trouvent l'apprentissage automatique (Machine Learning (ML)).

1.6.1 Apprentissage automatique

L'apprentissage automatique est une branche de l'intelligence artificielle. Il s'agit de la recherche des ordinateurs qui peuvent apprendre et se corriger sans pour autant être dotés d'instructions claires pour chaque élément détaillé. L'apprentissage automatique comprend différentes formes d'apprentissage [19] :

Apprentissage supervisé : Utilise un ensemble de données étiquetées pour faire des prédictions. Il comprend deux types principaux de problèmes :

- Classification : Prédiction de l'appartenance à une catégorie ou une classe.
- Régression : Prédiction de valeurs continues.

Apprentissage non supervisé : Détecte des motifs sans étiquettes ou spécifications préexistantes.

Apprentissage par renforcement : Le système apprend à atteindre un objectif par lui-même en utilisant le principe de l'essai et de l'erreur pour maximiser une récompense.

1.6.2 Apprentissage profond

L'apprentissage profond (deep learning) est un sous-ensemble du machine learning basé sur des réseaux de neurones profonds (DNN) dans lesquels les données sont analysées à travers plusieurs couches de neurones artificiels interconnectés [20]. La profondeur de ces réseaux permet de capturer des caractéristiques hiérarchiques et abstraites, rendant le deep learning particulièrement puissant pour des tâches complexes comme la reconnaissance d'images et la compréhension du langage naturel.

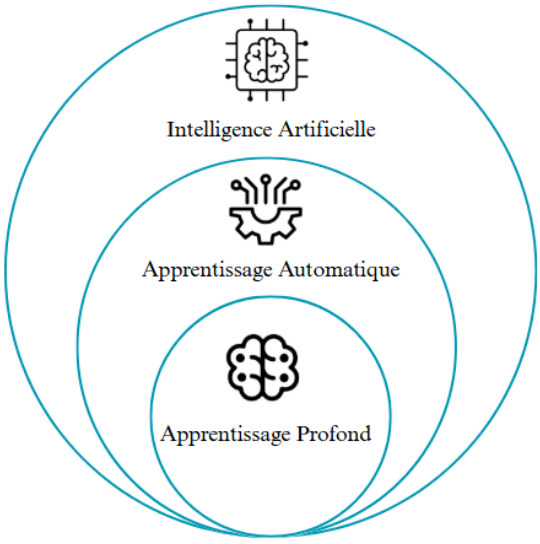

FIGURE 1.3 – Hiérarchie de l'IA,Apprentissage Automatique et Apprentissage Profond.

1.6.3 Convolutional Neural Networks(CNN)

Le réseau de neurones convolutif (CNN) est l'un des sous-types de réseaux de neurones profonds, qui excelle dans l'extraction de caractéristiques pertinentes à partir d'images. Le CNN [21] utilise une opération mathématique sous la forme de convolution, utilisée à la place de la multiplication matricielle normale, afin de calculer les caractéristiques à

partir des données d'entrée dans ses couches entièrement connectées. Le CNN [22] convolue les données d'image à travers un grand nombre de filtres et finit par produire une carte de caractéristiques. Ensuite, la carte de caractéristiques obtenue est combinée avec des couches entièrement connectées de neurones, et finalement, la classification consiste à attribuer une classe particulière en fonction de la sortie [23]. En dehors de cela, le CNN peut être utilisé pour plusieurs autres applications liées aux images/vidéos, telles que l'analyse basée sur les images médicales, le domaine agricole (détection de maladies des plantes), la détection d'objets, la reconnaissance faciale, la détection de visages, etc.

Avantages des CNN :

Extraction de Caractéristiques Locales : Les CNN sont très efficaces pour extraire des caractéristiques locales des données, ce qui est utile pour capturer des motifs locaux dans les séries temporelles financières.

Réduction de la Dimensionnalité : En réduisant la dimensionnalité des données, les CNN aident à améliorer l'efficacité du modèle et à réduire le risque de surajustement.

Invariance aux Translations : Les CNN sont capables de reconnaître des motifs indépendamment de leur position dans l'image, ce qui est crucial pour la reconnaissance d'objets dans des images.

Partage des Poids :Les filtres convolutifs sont appliqués à travers toute l'image, ce qui signifie que le même ensemble de poids est utilisé pour différentes parties de l'image. Cela réduit le nombre total de paramètres dans le modèle, le rendant plus efficace [24].

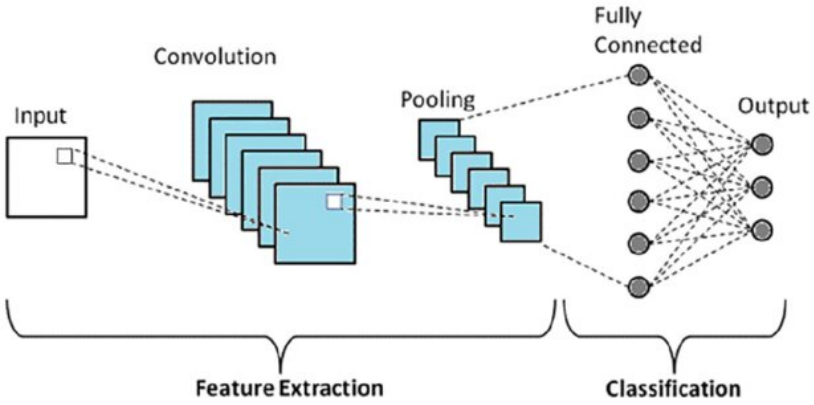

FIGURE 1.4 – L'Architecture des Reseaux de Neurones Convolutifs [25].

1.6.4 Recurrent Reural Network (RNN)

Les Réseaux de Neurones Récurrents (RNN) sont un ensemble de modèles d'apprentissage profond avec mémoire interne, qui leur permettent de capturer des dépendances séquentielles. Les réseaux de neurones traditionnels traitent les entrées comme des entités indépendantes, tandis que les RNN sont sensibles à l'ordre temporel des entrées, les rendant appropriés pour les tâches impliquant des informations séquentielles [26]. En utilisant une boucle, les RNN appliquent la même opération à chaque élément d'une sé-

rie, la computation actuelle dépendant à la fois de l'entrée actuelle et des computations précédentes [27].

La capacité des RNN à faire usage de données contextuelles est particulièrement valable dans des domaines tels que le traitement du langage naturel, la classification vidéo et la reconnaissance de parole. Par exemple, lors du modèle du langage, le savoir comprendre les mots qui viennent précédemment dans une phrase est crucial pour prédire le mot suivant. Les RNN sont très bons pour enregistrer de telles relations en raison de leur aspect récurrent [28].

Néanmoins, les RNN simples ont une limitation sous la forme d'une mémoire à court terme, ce qui restreint leur capacité à conserver des informations concernant de longues séquences. Pour remédier à cela, des versions plus avancées de RNN ont été créées, telles que la Mémoire à Long et Court Terme (LSTM) [29].

1.6.5 Long short-term memory (LSTM)

Un réseau récurrent à mémoire court [30] est un type spécial de réseau de neurones récurrents (RNN), capables d'apprendre les dépendances à long terme. Ils ont été introduits par Hochreiter et Schmidhuber en 1997 . Le LSTM (Long Short-Term Memory) est une solution efficace pour gérer l'explosion ou la disparition du gradient, grâce à sa structure de portes et de transitions de cellules. La figures 1.5 illustre cette structure tandis que les équations fondamentales décrivant son fonctionnement sont présentées ci-après.

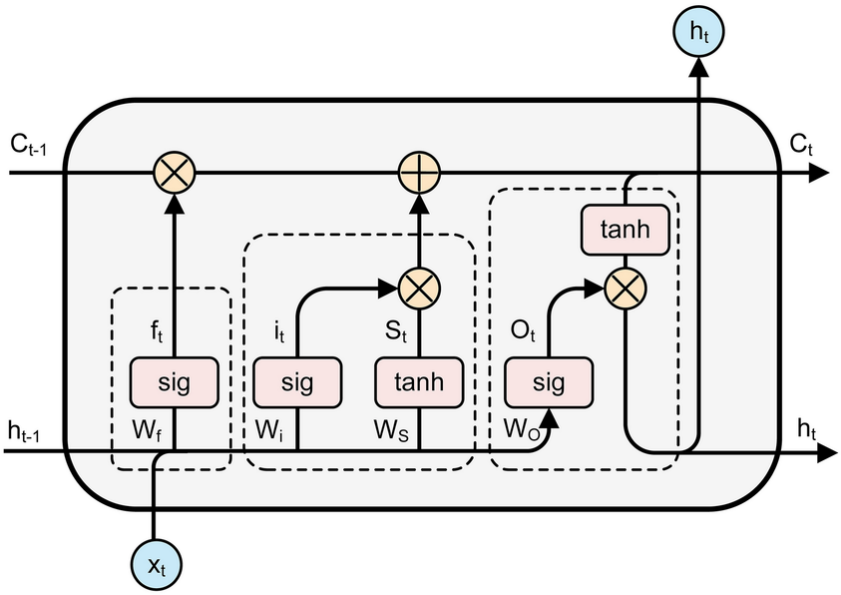

FIGURE 1.5 – Structure d'une cellule LSTM [31].

Porte d'oubli

La porte d'oubli est définie par :

$$f_t = \sigma(W_f[h_{t-1}, x_t] + b_f) \tag{1.1}$$

où σ est la fonction d'activation sigmoïde, X_t représente le vecteur des entrées, h_{t-1} désigne le vecteur caché de la couche précédente, et W_f et b_f désignent respectivement les poids et les valeurs de biais des entrées.

Porte d'entrée

La porte d'entrée est définie par :

$$i_t = \sigma(W_i[h_{t-1}, x_t] + b_i) \tag{1.2}$$

Porte de sortie

La porte de sortie contrôle la sortie des valeurs de l'état de la cellule et est définie par :

$$o_t = \sigma(W_o[h_{t-1}, x_t] + b_o) \tag{1.3}$$

Cellule de mémoire candidate

Une cellule de mémoire candidate est représentée par :

$$\tilde{C}_t = \tanh(W_c[h_{t-1}, x_t] + b_c) \tag{1.4}$$

Mise à jour de l'état de la cellule

L'état actuel de la cellule est mis à jour comme suit :

$$C_t = f_t \times C_{t-1} + i_t \times \tilde{C}_t \tag{1.5}$$

Sortie de l'état caché

La sortie finale de l'état caché actuel, qui sera utilisée comme entrée pour la couche suivante du LSTM, est donnée par :

$$h_t = O_t \times \tanh(C_t) \tag{1.6}$$

1.6.6 Les modèles d'embeddings

Un modèle d'embedding est un modèle d'apprentissage automatique conçu pour transformer des données (comme du texte, des images ou des sons) en représentations numériques appelées vecteurs d'embedding [32]. Comme le montre la figure 1.5. Ces vecteurs peuvent ensuite être utilisés dans des tâches en aval telles que la classification, le clustering et la recommandation.

Les modèles embeddings offrent de nombreux avantages : ils saisissent automatiquement les caractéristiques sémantiques et syntaxiques à partir de corpus bruts, réduisent la dimensionnalité des données, et permettent une généralisation efficace sur différentes tâches sans nécessiter de réentraînement. Leur capacité à modéliser des relations complexes, alliée à leur adaptabilité à divers domaines via un apprentissage spécifique.

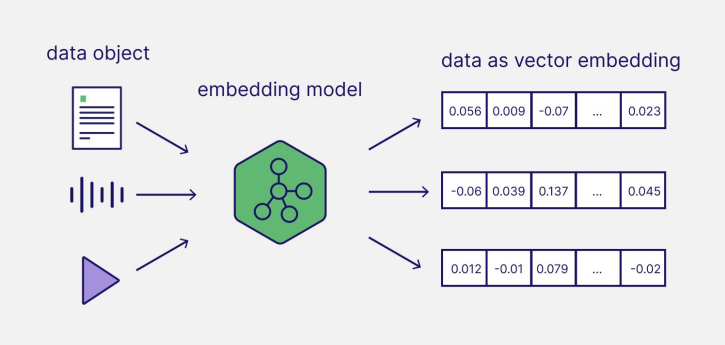

FIGURE 1.6 – Processus de Modèle d'Embedding [32].

1.7 La distribution Bêta

La distribution bêta est une famille de lois de probabilité continues définies sur l'intervalle $[0, 1]$. Elle est couramment utilisée pour modéliser des variables aléatoires représentant des proportions ou des probabilités. Sa grande flexibilité provient de ses deux paramètres de forme, notés α (alpha) et β (bêta), qui déterminent la forme de la distribution. Ces paramètres influencent notamment la moyenne et la variance, données respectivement par les formules suivantes [33] :

$$\text{Moyenne :} \quad \mu = \frac{\alpha}{\alpha + \beta} \tag{1.7}$$

$$\text{Variance :} \quad \sigma^2 = \frac{\alpha\beta}{(\alpha + \beta)^2(\alpha + \beta + 1)} \tag{1.8}$$

La distribution bêta est couramment utilisée dans des domaines tels que l'écologie, la finance, et la modélisation de données de proportion comme les taux de couverture végétale, les taux de réussite, etc. Elle est également appliquée dans des tâches liées au web, comme la modélisation du taux de clic sur des publicités, ce qui permet d'analyser l'efficacité des campagnes publicitaires en ligne.

1.8 Conclusion

En conclusion, Ce premier chapitre a permis de présenter les systèmes ferroviaires intelligents, leur évolution, ainsi que les technologies qui les composent, comme le CBTC et le TC-CBTC. Nous avons également expliqué la gestion de la confiance dans ces systèmes, en soulignant les risques liés aux attaques . Enfin, nous avons introduit le rôle de l'intelligence artificielle, notamment l'apprentissage automatique , les embeddings et la distribution bêta, comme outils prometteurs pour renforcer la confiance dans les communications.

Le chapitre suivant, nous passerons en revue les travaux existants qui ont été proposés pour améliorer la sécurité dans les systèmes ferroviaires.

2

Revue de la littérature

2.1 Introduction

Les systèmes ferroviaires intelligents, bien que performants, sont exposés aux cyberattaques en raison de l'intégration accrue des technologies de l'information. Ce chapitre passe en revue les récentes avancées et innovations technologiques conçues pour améliorer la sécurité de ces systèmes.

2.2 Revue des études précédentes

Différentes méthodes sont mises en œuvre pour renforcer la sécurité des systèmes ferroviaires intelligents. Chaque recherche offre des stratégies particulières pour lutter contre les cyberattaques et améliorer la sécurité des communications. À cette fin, nous examinons les méthodes mises en œuvre pour détecter les activités suspectes et anticiper les incidents.

2.2.1 Improve Safety and Security of Intelligent Railway Transportation System Based on Balise Using Machine Learning Algorithm and Fuzzy System

Wang, Y. et al. [34] ont concentré leurs efforts sur la conception une méthode innovante pour détecter et contrer les attaques cybernétiques ciblant les balises ferroviaires, tout en évitant des modifications substantielles de l'infrastructure ferroviaire existante. Les auteurs identifient et classifient les différentes catégories d'attaques possibles, notamment les attaques par écoute, brouillage, falsification, clonage et transmission de faux télégrammes.

Afin de répondre à ces menaces, les auteurs suggèrent la mise en place d'un module de détection fondé sur des techniques d'apprentissage automatique. Ce module analyse les données issues des capteurs embarqués dans le train afin de repérer les comportements anormaux. Les algorithmes proposés incluent les réseaux neuronaux multicouches (MLP), les machines à vecteurs de support (SVM) et les systèmes adaptatifs d'inférence neuro-floue (ANFIS), permettant une détection précise et rapide des anomalies avec un taux d'exactitude de 92% et une précision de 91%.

Par ailleurs, un contrôleur flou est proposé pour atténuer les conséquences des attaques détectées. Ce contrôleur est conçu pour mettre en œuvre des mesures de mitigation, telles que le rejet des télégrammes suspects, la réduction contrôlée de la vitesse ou l'exécution d'un arrêt d'urgence du train. Ces mécanismes visent à renforcer la sécurité globale des systèmes ferroviaires tout en garantissant leur résilience face aux menaces émergentes.

Analyse Critique :

L'idée de recourir à l'apprentissage automatique pour renforcer la sécurité des trains intelligents est prometteuse et ouvre la voie à des solutions innovantes. Les algorithmes utilisés, tels que ANFIS et MLP, se montrent performants pour la détection d'anomalies dans les environnements simulés. Toutefois, l'étude ne fournit que peu d'éléments sur leur efficacité en conditions réelles, où des facteurs imprévus comme les interférences ou les fluctuations du signal peuvent altérer les performances.

Par ailleurs, la portée de cette approche semble limitée à un cadre spécifique, sans réelle évaluation de sa capacité à s'adapter à d'autres types de réseaux ou à des scénarios d'attaque variés. Un autre point critique concerne la sécurité des données traitées par le système : l'absence de précisions sur les mécanismes de protection des informations échangées soulève des interrogations quant à la robustesse globale de la solution.

Enfin, bien que les résultats obtenus soient encourageants, l'absence de tests en environnement opérationnel rend difficile l'évaluation de la fiabilité du modèle une fois déployé.

2.2.2 A Novel Hierarchical Situation Awareness Model for CBTC Using SVD Entropy and GRU With PRD Algorithms

Li, Q. et al. [35] proposent dans cet article un modèle hiérarchique innovant de conscience situationnelle pour les systèmes de Contrôle Basé sur la Communication (CBTC). Ce modèle a pour but d'améliorer la sécurité et la réactivité des systèmes CBTC en utilisant des algorithmes d'entropie de Décomposition en Valeurs Singulières (SVD) et des réseaux de neurones à Unité Récurrente à Porte (GRU) avec des algorithmes de Détection Progressive des Résidus (PRD).

Le modèle est structuré en trois couches principales : la couche physique, la couche réseau et la couche application. Chaque couche utilise des techniques spécifiques pour traiter et analyser les données. La couche physique et la couche réseau utilisent l'algorithme d'entropie SVD pour réduire la dimensionnalité des données hétérogènes multi-sources, permettant ainsi une classification rapide et précise des différentes catégories de données, y compris les données normales et les données d'attaque. La couche application, quant à elle, utilise un réseau de neurones GRU pour apprendre et prédire les valeurs d'Autorité de Mouvement (MA) en temps réel, et l'algorithme PRD pour détecter les anomalies.

Pour évaluer la performance et la sécurité du modèle, des tests ont été réalisés avec des attaques par déni de service (Dos), des attaques par sondage et des attaques par fal-

sification de données. Les résultats montrent que le modèle peut réaliser une conscience situationnelle et une alerte précises et en temps réel du système. Lorsque le seuil d'entropie des valeurs singulières est fixé à 0,85, l'algorithme d'entropie SVD peut compresser le temps de formation et de classification d'environ 80 % tout en maintenant la précision de classification stable. De plus, l'algorithme GRU avec PRD a démontré une capacité à détecter les attaques de falsification de données avec une précision de 100 % dans les cas où une collision ou un freinage d'urgence est provoqué.

Analyse Critique :

Le modèle hiérarchique pour la conscience situationnelle dans les systèmes CBTC, bien que prometteur, présente des défis liés à sa complexité et à son implémentation. L'utilisation de données d'un seul train limite sa portée, et sa dépendance à des paramètres précis comme le seuil d'entropie peut affecter sa performance. Bien qu'efficace contre certaines attaques, sa robustesse face à de nouvelles menaces reste incertaine. Enfin, l'interprétabilité limitée des réseaux de neurones et la nécessité d'une faible latence en temps réel posent des défis supplémentaires pour une utilisation pratique.

2.2.3 Blockchain enabled zero trust based authentication scheme for railway communication networks

Feng, Y. et al. [36] proposent un schéma d'authentification basé sur la blockchain et le modèle de sécurité zéro confiance pour les réseaux de communication ferroviaires. La problématique réside dans la complexité et la vulnérabilité des réseaux ferroviaires modernes, qui utilisent des services cloud tiers difficiles à superviser et un trafic réseau non fiable. Pour résoudre ces défis, les auteurs introduisent la blockchain et l'arbre de Merkle pour stocker de manière distribuée les informations d'identité des utilisateurs, des dispositifs et des services cloud, améliorant ainsi l'efficacité et la sécurité des mises à jour de données.

Le modèle inclut également un mécanisme d'authentification bidirectionnelle entre les proxys réseau et les serveurs cloud pour contrer les menaces internes et externes. Un système d'évaluation de la réputation est mis en place pour évaluer la fiabilité des services cloud publics, réduisant ainsi les risques d'accès à des services malveillants. Les auteurs utilisent AVISPA pour valider la sécurité du modèle.

Les analyses de performance montrent que ce modèle améliore la sécurité, l'efficacité et la stabilité des réseaux ferroviaires. Les résultats démontrent une réduction significative des risques de sécurité et une amélioration de l'efficacité des processus d'authentification, garantissant ainsi une interaction sécurisée et fiable dans les systèmes ferroviaires modernes.

Analyse Critique :

L'approche de sécurité zéro confiance avec la blockchain pour les réseaux ferroviaires vise à améliorer la sécurité en utilisant des technologies comme l'arbre de Merkle pour vérifier les identités. Cependant, cette méthode est complexe et coûteuse, nécessitant beaucoup de ressources informatiques et de temps de développement. Elle peut aussi ralentir les communications importantes et demande une gestion continue des informations d'identification.

2.2.4 A Novel Intrusion Detection Method in Train-Ground Communication System

Bing Gao et Bing Bu [37] ont proposé une méthode pour améliorer la détection des intrusions dans les systèmes de communication train-sol, qui sont essentiels pour les systèmes CBTC utilisés dans les réseaux ferroviaires urbains. Leur approche commence par l'utilisation du modèle n-gram pour modéliser les transitions d'état du protocole IEEE 802.11, permettant ainsi de capturer les séquences de caractères dans les données de communication et d'identifier les comportements normaux et anormaux. Par la suite, un algorithme AdaBoost amélioré est utilisé pour la classification binaire et multi-classes, s'appuyant sur des classificateurs faibles qui, une fois combinés, génèrent un classificateur puissant et robuste pour détecter différents types d'attaques. De plus, cette méthode intègre les résultats de détection issus des réseaux sans fil et filaires et prend en compte des informations telles que la position et la vitesse du train, renforçant ainsi l'efficacité de la détection. Enfin, une approche mixte combinant la détection d'anomalies et la détection de mauvais usage permet d'identifier à la fois les comportements normaux et les attaques. En somme, cette méthode se révèle plus efficace que les techniques traditionnelles, avec des taux de détection plus élevés et une réduction significative des faux positifs et faux négatifs.

Analyse Critique :

La méthode envisagée est à la fois innovante et prometteuse, mais elle soulève plusieurs défis. L'utilisation du modèle n-gram pour analyser les comportements normaux et anormaux s'avère efficace, mais la gestion des ensembles de données peut devenir complexe, surtout avec l'apparition de nouvelles formes d'attaques. La précision de la détection dépend également de la qualité des données d'apprentissage, ce qui peut poser problème en cas de biais ou d'informations incomplètes.

Bien que cette approche cherche à limiter l'impact du bruit, elle reste sensible aux interférences et aux pertes de paquets, des phénomènes fréquents dans les environnements ferroviaires. Sa mise en œuvre pourrait aussi exiger des investissements conséquents, que ce soit pour le développement logiciel ou la formation du personnel. Par ailleurs, adapter cette solution à des réseaux ferroviaires plus vastes et complexes représente un autre défi à relever.

2.2.5 Improved SRP algorithm and bidirectional heterogeneous LTE-R authentication key

Chen, Y. et al. [38] abordent les défis de sécurité dans les systèmes de communication sans fil ferroviaire à grande vitesse (LTE-R). Ils identifient des vulnérabilités critiques telles que la transmission non chiffrée de l'identité internationale des abonnés mobiles (IMSI), la divulgation des clés à long terme, et les vecteurs d'authentification non protégés. Pour résoudre ces problèmes, ils proposent une solution en deux parties : un algorithme SRP (Secure Remote Password) amélioré pour chiffrer les messages entre l'équipement utilisateur (UE) et l'entité de gestion de la mobilité (MME), et une méthode de signature numérique hétérogène bidirectionnelle utilisant l'infrastructure à clé publique (PKI) et le système de chiffrement basé sur l'identité (IBC) pour sécuriser les communications entre

MME et le serveur d'abonnés domestique (HSS). Cette approche améliore la sécurité en empêchant la transmission en texte clair des informations sensibles et en résistant aux attaques courantes. Les résultats expérimentaux montrent que cette méthode est supérieure aux approches existantes en termes de sécurité et de coût d'authentification, tout en répondant aux exigences de communication LTE-R.

Analyse Critique :

L'approche proposée améliore significativement la sécurité des systèmes LTE-R en utilisant un algorithme SRP amélioré et des signatures numériques hétérogènes. Cependant, cette méthode nécessite des ressources computationnelles importantes, ce qui peut compliquer son intégration dans les infrastructures existantes. De plus, la robustesse de cette approche face à des attaques sophistiquées et émergentes, telles que les attaques par injection de données ou les attaques de l'homme du milieu, n'est pas entièrement validée, ce qui pourrait la rendre vulnérable à des menaces avancées.

2.2.6 Data Integrity Threats and Countermeasures in Railway Spot Transmission Systems

Hoon Wei Lim et al. [39] ont proposé une approche visant à renforcer la sécurité des systèmes de transmission des balises ferroviaires, particulièrement ceux conformes à la norme Eurobalise. Bien que ces balises soient initialement conçues pour être fiables, elles ne disposent pas des mécanismes nécessaires pour résister aux cyberattaques sophistiquées, telles que l'injection de fausses données ou les attaques par rejeu, qui menacent l'intégrité et l'authenticité des informations transmises. Afin d'y remédier, les auteurs présentent une solution en deux volets, combinant des techniques cryptographiques avancées et des mécanismes de contrôle intelligent.

Dans un premier temps, au niveau des balises, une solution cryptographique légère et optimisée est intégrée directement dans les télégrammes. Cette approche repose sur des bits de brouillage et une clé générée par un registre à décalage à rétroaction linéaire (LFSR), dérivée de clés cryptographiques secrètes, et ne nécessite aucune modification matérielle, garantissant ainsi une compatibilité totale avec les équipements existants. Dans un second temps, au niveau système, un contrôleur de vitesse hybride sécurisé est développé. Celui-ci exploite des modèles théoriques de contrôle pour détecter les anomalies dans les données transmises par les balises et ajuste de manière proactive la vitesse des trains en cas de détection d'une menace, minimisant ainsi les risques potentiels.

Les simulations effectuées valident l'efficacité de cette méthode en démontrant sa capacité à préserver l'intégrité des données tout en atténuant les impacts des attaques, avec un surcoût computationnel négligeable. De plus, cette solution reste pleinement compatible avec les infrastructures existantes. En conclusion, les auteurs suggèrent une exploration future de l'intégration de technologies émergentes, comme la blockchain, afin d'améliorer davantage la sécurité des systèmes ferroviaires face aux menaces évolutives.

Analyse Critique :

L'approche suggérée pour la sécurisation des systèmes de transmission point à point dans le domaine ferroviaire se démarque par son innovation et son potentiel prometteur. Cependant, plusieurs éléments nécessitent une considération spécifique. Premièrement, la gestion des clés cryptographiques représente un défi majeur. Si la clé principale venait à être compromise, l'ensemble du dispositif de sécurité pourrait être mis en danger. Ensuite, bien que la structure fixe du réseau ferroviaire facilite la validation des informations, elle pourrait devenir un frein en cas de modifications de l'infrastructure, limitant ainsi la flexibilité du système.

Par ailleurs, même si la solution a été conçue pour être légère et compatible avec les systèmes existants, son déploiement nécessiterait des ajustements significatifs, que ce soit en matière de développement logiciel ou de formation du personnel, ce qui pourrait engendrer des coûts non négligeables. Enfin, bien que cette approche renforce la protection contre les attaques de falsification et de clonage, elle pourrait néanmoins rester vulnérable à des attaques sophistiquées combinant plusieurs vecteurs d'attaque.

Ainsi, bien que cette solution constitue une avancée importante pour la sécurisation des infrastructures ferroviaires, des tests approfondis et des améliorations restent nécessaires pour garantir son efficacité dans des conditions réelles.

2.2.7 Real-Time Reliability Access Control Based on Rail Traffic Data Platform

Yu, W. et al. [40] ont proposé une approche basée sur le concept de "confiance zéro" pour renforcer la sécurité des systèmes de données, en particulier dans les plateformes de transport ferroviaire. Cette méthode repose sur une combinaison de trois modèles de contrôle d'accès : RBAC (Role-Based Access Control), ABAC (Attribute-Based Access Control) et TBAC (Trust-Based Access Control), permettant une évaluation continue et dynamique de la confiance des utilisateurs.

Pour affiner cette évaluation, ils ont utilisé l'opérateur IOWA, qui permet de calculer la confiance en temps réel en accordant une importance plus grande aux comportements récents. Le processus débute par une authentification initiale, suivie d'une évaluation de la confiance lors de chaque demande d'accès, et se poursuit par une surveillance continue qui ajuste les permissions en fonction des comportements observés.

Grâce à cette approche, les droits d'accès peuvent être adaptés en temps réel, réduisant ainsi les risques d'intrusion et de comportements malveillants, tout en offrant une sécurité plus robuste et flexible.

Analyse Critique :

Malgré la promesse d'améliorer la sécurité des systèmes de données par une évaluation continue de la confiance des utilisateurs, l'approche soulève plusieurs défis significatifs. L'application de cette structure requiert des modifications importantes de l'infrastructure actuelle, ce qui peut s'avérer onéreux et compliqué, comme le suggère le besoin d'une mise en œuvre intelligente pour l'optimisation organisationnelle. Par ailleurs, l'observation constante des actions des utilisateurs suscite d'importantes inquiétudes en termes de confidentialité et de protection des données personnelles, particulièrement avec le recours à un moteur d'évaluation de confiance qui gère en permanence des informations provenant

de journaux et des caractéristiques des utilisateurs. Le système s'appuie également massivement sur des technologies de pointe et des algorithmes complexes, ce qui peut soulever des questions de fiabilité et d'entretien sur le long terme. Par ailleurs, il y a le danger de faux positifs ou négatifs, où des actions légitimes pourraient être erronément considérées comme suspectes, ou à l'inverse, des actions malintentionnées pourraient demeurer invisibles. En définitive, les contrôles incessants peuvent provoquer des pauses ou des délais pour les utilisateurs autorisés, nuisant ainsi à leur productivité et à leur contentement.

2.2.8 Railway Defender Kill Chain to Predict and Detect Cyber-Attacks

Kour, R. et al. [41] aborde la vulnérabilité croissante des systèmes ferroviaires face aux cyberattaques, en raison de l'intégration accrue des technologies de l'information (IT) et des technologies opérationnelles (OT). Cette convergence, bien qu'elle améliore l'efficacité opérationnelle, expose les systèmes à des risques de cybersécurité, notamment des attaques sur les systèmes SCADA, essentiels pour le contrôle centralisé. Pour répondre à cette problématique, l'article propose le modèle "Railway Defender Kill Chain" (RDKC), une approche structurée pour prédire, prévenir, détecter et répondre aux cyberattaques. Ce modèle s'appuie sur une version étendue de la chaîne de cyber-attaque (CKC) et intègre des technologies prédictives pour renforcer la sécurité des systèmes ferroviaires. La RDKC utilise une matrice de cours d'action pour déterminer comment prédire, prévenir, détecter et répondre aux événements adverses le long des phases de la chaîne de destruction. Les outils incluent des technologies de détection d'intrusion et des analyses comportementales, offrant une préparation proactive aux cybermenaces et une réduction des risques grâce à des contrôles de sécurité multiples. La validation de cette approche repose sur des simulations et des études de cas, démontrant son efficacité à améliorer la résilience opérationnelle des systèmes ferroviaires face aux cyberattaques.

Analyse Critique :

L'approche "Railway Defender Kill Chain" (RDKC) offre une méthode structurée pour renforcer la cybersécurité ferroviaire en intégrant des technologies avancées pour la détection et la prévention des cyberattaques. Elle permet une identification précoce des menaces grâce à des analyses comportementales et des simulations, réduisant ainsi les risques de compromission. Cependant, cette approche nécessite des ressources importantes et une expertise technique, ce qui peut compliquer son intégration, notamment pour les petites organisations. De plus, sa robustesse face à des attaques sophistiquées et émergentes n'est pas entièrement validée, et un attaquant pourrait utiliser une nouvelle technique non encore incluse dans la matrice de défense, rendant le système vulnérable à des attaques inédites.

Le tableau 2.1 synthétise les méthodes examinées :

Référence	**Objectif Principal**	**Méthodes Utilisées**	**Approche**
Wang, Y. et al .[34]	Détecter et contrer les attaques sur les balises ferroviaires	Apprentissage automatique (MLP, SVM, ANFIS), contrôleur flou	Utilisation de l'apprentissage automatique pour détecter les anomalies et un contrôleur flou pour atténuer les conséquences des attaques.
Li, Q. et al. [35]	Améliorer la sécurité et la réactivité des systèmes CBTC	Entropie SVD, réseaux de neurones GRU, algorithmes PRD	Modèle hiérarchique utilisant l'entropie SVD pour la réduction de dimensionnalité et les réseaux GRU pour la prédiction des valeurs d'Autorité de Mouvement.
Feng, Y. et al. [36]	Sécuriser les réseaux de communication ferroviaires	Blockchain, arbre de Merkle, authentification bidirectionnelle	Utilisation de la blockchain pour stocker les informations d'identité et un mécanisme d'authentification bidirectionnelle pour sécuriser les communications.
Bing Gao et Bing Bu.[37]	Améliorer la détection des intrusions dans les systèmes de communication train-sol	Modèle n-gram, algorithme AdaBoost, détection d'anomalies	Modélisation des transitions d'état avec n-gram et classification avec AdaBoost pour détecter les intrusions.
Chen, Y. et al. [38]	Sécuriser les communications LTE-R	Algorithme SRP amélioré, signatures numériques hétérogènes	Chiffrement des messages avec SRP et utilisation de signatures numériques pour sécuriser les communications entre les entités du réseau.
Hoon Wei Lim et al.[39]	Renforcer la sécurité des systèmes de transmission des balises ferroviaires	Techniques cryptographiques, contrôleur de vitesse hybride	Intégration de techniques cryptographiques dans les télégrammes et utilisation d'un contrôleur de vitesse hybride pour détecter les anomalies.
Yu, W. et al. [40]	Renforcer la sécurité des systèmes de données ferroviaires	Modèles de contrôle d'accès (RBAC, ABAC, TBAC), opérateur IOWA	Évaluation continue de la confiance des utilisateurs avec des modèles de contrôle d'accès combinés.
Kour, R. et al.[41]	Prédire et détecter les cyberattaques dans les systèmes ferroviaires	Chaîne de cyber-attaque étendue, technologies de détection d'intrusion	Utilisation d'une chaîne de cyber-attaque étendue pour prédire, prévenir, détecter et répondre aux cyberattaques.

TABLE 2.1 – Récapitulatif des Approches

2.3 Classification des travaux passés en revus

Pour mieux comprendre les avancées actuelles et repérer les lacunes ou les opportunités pour des travaux futurs, la classification de l'état de l'art consiste à organiser et à analyser les recherches et découvertes en rapport avec un domaine donné. Dans cette section, nous nous proposons d'utiliser trois critères afin de distinguer les travaux examinés : **la détection, la prédiction, et la combinaison de prédiction et détection.**

La première catégorie regroupe les approches qui cherchent à détecter les intrusions ou les anomalies sur le réseau ferroviaire, généralement en temps réel. La deuxième catégorie concerne les méthodes qui visent à prédire une éventuelle attaque avant qu'elle ne se produise, en se basant sur des comportements suspects. Enfin, la troisième catégorie combine détection et prédiction. Ces techniques permettent à la fois de repérer les anomalies au moment où elles apparaissent et de prévoir les risques à venir, en utilisant des outils avancés.

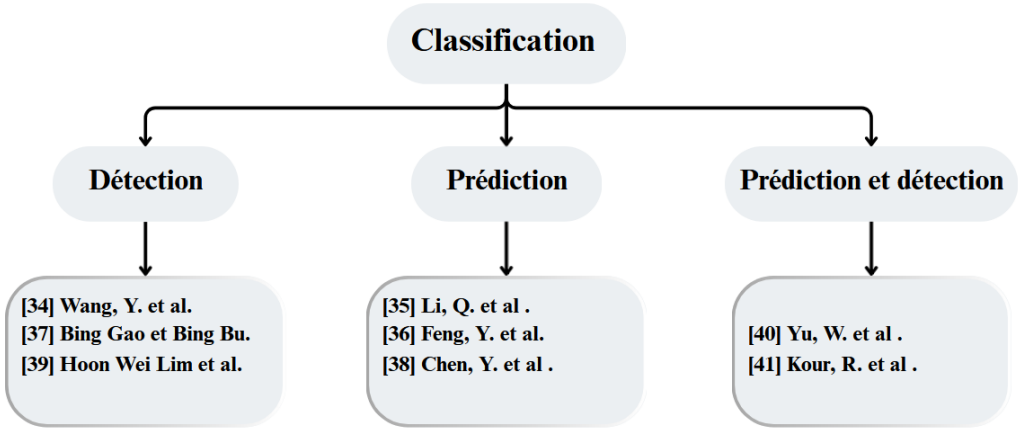

FIGURE 2.1 – Classification des Approches

2.4 Conclusion

Pour résumer, nous avons examiné diverses techniques et stratégies en rapport avec notre sujet. Cette analyse nous a aidé à souligner les points forts et les restrictions de chaque technique, tout en tenant compte de leur adéquation selon le cadre d'utilisation.

Le prochain chapitre se focalisera sur une présentation approfondie de notre méthode pour instaurer la confiance dans les systèmes ferroviaires intelligents.

3

RailTrust : An Efficient Trust Approach for Secure TC-CBTC Communications

3.1 Introduction

La sécurité des systèmes ferroviaires intelligents (SFI) a fait l'objet de nombreuses recherches. Toutefois, comme vu dans le chapitre précédent, la question de la confiance dynamique entre les trains reste encore peu explorée. Dans les systèmes TC-CBTC, où les trains communiquent directement pour échanger des informations critiques, la fiabilité des messages échangés devient essentielle pour garantir la sécurité opérationnelle.

Dans ce chapitre, nous présenterons notre approche innovante RailTrust visant à renforcer la confiance dans les communications inter-trains au sein des systèmes TC-CBTC (Train-Centric Communication-Based Train Control), en reposant sur des techniques d'apprentissage automatique avancées.

3.2 Motivations

Dans les systèmes TC-CBTC , l'Autorité de Mouvement (MA) joue un rôle clé en assurant une gestion sécurisée et efficace de la circulation des trains. Cependant, la fiabilité de la MA dépend entièrement de la qualité des données échangées entre les trains et les systèmes de contrôle. Dans ce contexte, la notion de confiance devient primordiale : les trains doivent être en mesure de s'appuyer sur l'exactitude des informations reçues afin d'adapter leur comportement en temps réel, qu'il s'agisse de ralentir, de s'arrêter ou de corriger leur trajectoire.

Malgré son importance, la confiance est rarement abordée dans les recherches actuelles. La plupart des travaux se concentrent sur l'amélioration des algorithmes de contrôle et de communication, mais peu traitent de la confiance dans les données échangées. C'est ce manque qui a inspiré notre recherche : introduire une nouvelle approche qui place la confiance au centre des communications dans les systèmes ferroviaires intelligents.

Notre proposition est une solution innovante qui intègre des techniques d'apprentissage automatique avancées, notamment les embedding , les réseaux de neurones convolutifs (CNN) et les réseaux de neurones à long terme (LSTM). Ces outils permettent de détecter en temps réel les anomalies et incohérences dans les messages échangés, assurant que seules des données fiables sont utilisées pour calculer l'Autorité de Mouvement. En actualisant dynamiquement les scores de confiance attribués à chaque train, RailTrust facilite des décisions sécurisées et éclairées, réduisant ainsi les risques d'incidents et d'accidents.

En adoptant cette approche, nous visons non seulement à renforcer la sécurité, mais aussi à améliorer l'efficacité opérationnelle des systèmes TC-CBTC. L'intégration de la confiance comme élément central des communications permet de mieux gérer les incertitudes et les risques potentiels, créant ainsi un environnement ferroviaire plus sûr et plus résilient.

3.3 Notre proposition

Cette section présente notre proposition RailTrust, un module embarqué dans chaque train du système. Ce module est conçu pour renforcer la confiance et la sécurité dans les systèmes de communication entre trains. L'objectif principal de RailTrust est d'assurer la confiance dans les données reçues ainsi que dans l'identité du train émetteur, avant d'autoriser un train à calculer l'autorité de mouvement. Comme illustré dans la Figure 3.1, notre approche se compose de trois phases essentielles : l'évaluation de la qualité des données, la mise à jour des scores de confiance, et la prise de décision. Dans ce qui suit, nous détaillons chacune des phases constituant notre proposition.

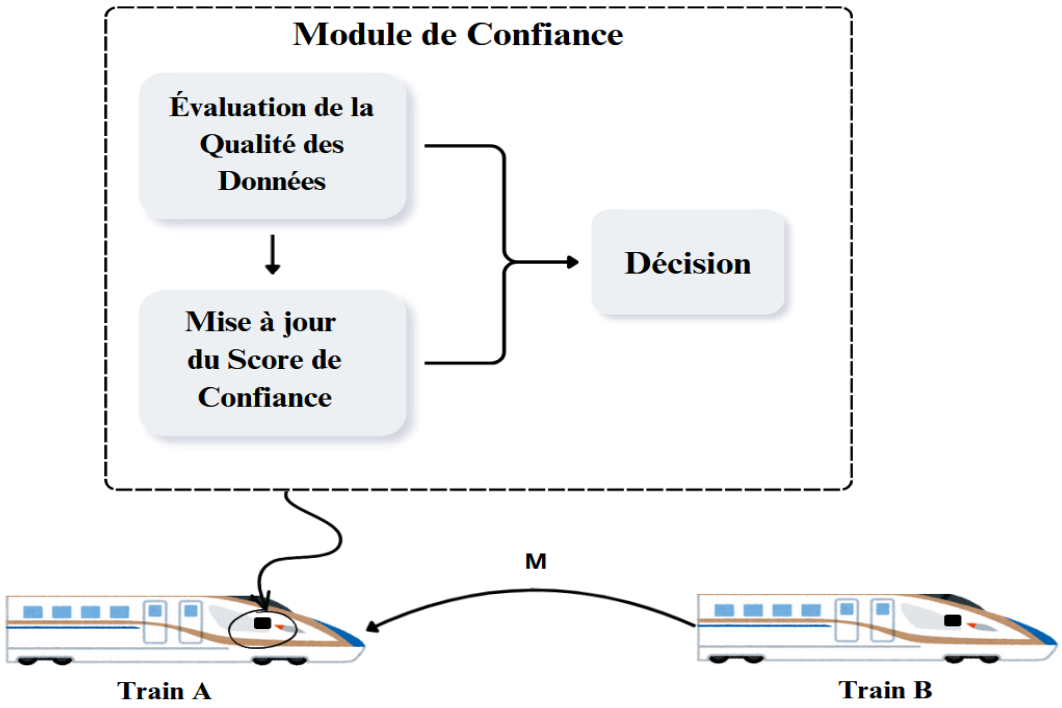

FIGURE 3.1 – Solution proposée.

Le tableau 3.1 présente les différentes notations utilisées dans cette étude.

Notations	Description
M	Message échangé entre les trains
Train A	Le train récepteur
Train B	Le train émetteur
α	Nombre d'observations positives (Message fiable)
β	Nombre d'observations négatives (Message non fiable)
$S_{Confiance}(B)$	Score de confiance calculé pour le train B

TABLE 3.1 – Table des notations utilisées.

3.3.1 Évaluation de la Qualité des Données

La première phase de notre approche consiste à évaluer la qualité des données reçues par le train dans un système TC-CBTC. Notre modèle de l'évaluation repose sur des techniques d'apprentissage automatiques (ML pour Machine Learning), combinant un modèle d'embedding (Embedding Model), des réseaux de neurones convolutifs (CNN) et des couches LSTM. Ce modèle est composé d'une couche CNN pour extraire les caractéristiques des données d'entrée, suivie de trois couches LSTM permettant de capturer les dépendances temporelles sur plusieurs niveaux. La structure du ce modèle illustrée dans la Figure 3.2.

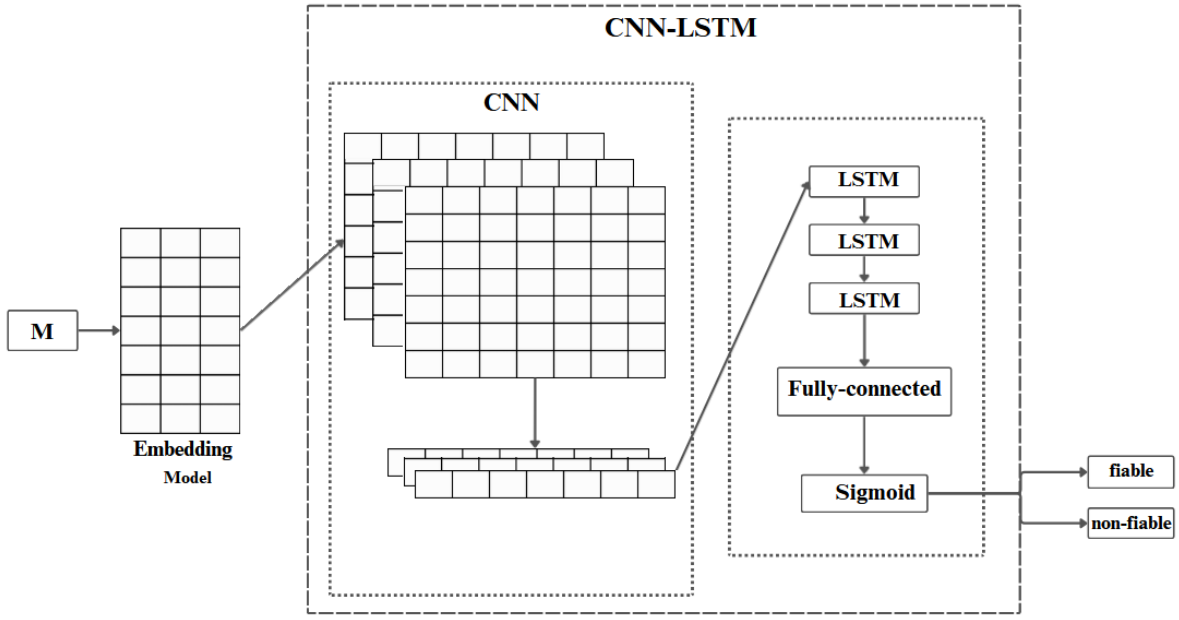

FIGURE 3.2 – Diagramme de Structure du notre modèle d'évaluation .

Lorsque le Train A reçoit un message **M** (ID_MSG, ID_TRAIN, horodatage,V_train, D_train, P_train , gare_D , gare_A), il déclenche le processus d'évaluation de la qualité des données .

Composant	**Description**
ID_MSG	Identifiant unique du message.
ID_TRAIN	Identifiant unique du train émetteur.
Horodatage	Horodatage du message (timestamp).
V_train	Vitesse actuelle du train.
D_train	Direction actuelle du train (avant/arrière).
P_train	Position actuelle du train (coordonnées GPS ou distance par rapport à un point de référence).
gare_D	La gare de départ du train .
gare_A	La gare d'arrivée du train .

TABLE 3.2 – Description des composants du message **M**.

3.3.1.1 Embedding Model

Le processus commence par le modèle d'embedding, qui transforme les données brutes du message en une représentation dense sous forme de vecteurs de dimension fixe. Cette étape convertit les informations textuelles, comme l'état ou la direction, et les données numériques, comme la vitesse ou la position, en un format exploitable. L'embedding capture les relations sémantiques et structurelles entre les éléments du message, telles que la cohérence entre la vitesse et les coordonnées de position ou les relations temporelles implicites. Cette transformation est essentielle pour standardiser les données hétérogènes et les rendre compatibles avec les réseaux neuronaux.

3.3.1.2 Modèle CNN-LSTM

Ces embeddings servent d'entrée au CNN, qui possède deux couches : une couche de convolution et une couche de pooling.

La couche de convolution, c'est un peu comme un détecteur de motifs, elle est utilisée pour extraire des caractéristiques locales des séquences de représentations numériques des données d'entrée. . Elle fonctionne en appliquant des filtres (kernels) sur les embeddings, qui sont des représentations numériques des données d'entrée. Chaque filtre glisse sur les données d'entrée avec un pas (stride) . À chaque position, le filtre effectue une opération de convolution, qui consiste en une multiplication élément par élément suivie d'une somme.

Le résultat de cette opération est une carte de caractéristiques (feature map) qui met en évidence les motifs détectés. Par exemple, un filtre de taille 3x3 peut détecter une relation entre la vitesse, la position et l'état du train. Si le filtre détecte une incohérence, comme une vitesse anormale pour une position donnée, cela peut indiquer une anomalie dans les données. Cette capacité à détecter des motifs spécifiques permet au réseau de neurones convolutif de capturer des informations importantes et de les utiliser pour des tâches ultérieures, comme la classification ou la détection d'anomalies.

Ensuite, on applique une couche de pooling (ou sous-échantillonnage). Là, on utilise une petite fenêtre qu'on déplace elle aussi sur la carte de caractéristiques. Cette fenêtre va résumer les valeurs qu'elle contient, souvent en gardant la plus grande (c'est ce qu'on appelle le max pooling). Ça permet de réduire la taille des données, d'enlever un peu de bruit et de garder l'essentiel des informations détectées auparavant.

Les trois couches LSTM sont utilisées pour modéliser les dépendances temporelles dans les données séquentielles. L'entrée de la première couche LSTM est l'ensemble des caractéristiques extraites par le CNN, et la sortie finale est une représentation codée de ces séquences, capturant les relations temporelles entre les différents points de données. Cette étape permet de comprendre comment les informations évoluent au fil du temps, ce qui est essentiel pour détecter des anomalies ou des comportements inhabituels dans les communications.

La couche fully-connected (dense) intègre les dépendances temporelles capturées par les couches LSTM. Elle utilise une fonction d'activation sigmoïde pour classer les messages en deux catégories : "fiable" ou "non fiable". La sortie de la couche sigmoïde fournit une probabilité de classes, sur la base de laquelle les messages sont catégorisés selon un seuil de fiabilité fixé à 0,6.

3.3.2 Mise à Jour des Scores de Confiance

La mise à jour des scores de confiance permet de modéliser et d'ajuster dynamiquement la confiance entre les trains en utilisant la distribution bêta. Cette méthode probabiliste repose sur deux paramètres fondamentaux, α (alpha) et β (bêta), qui représentent respectivement le nombre d'observations positives (fiables) et négatives (non fiables).

À chaque réception d'un nouveau message M par le train récepteur ($TrainA$) du train émetteur ($TrainB$), et après avoir évalué la qualité de ce message, les paramètres α et β associés à $TrainB$ dans la base de données de confiance de $TrainA$ sont mis à jour comme suit :

$$\text{Si le message est jugé fiable,} \quad \alpha_{\text{nouveau}} = \alpha_{\text{ancien}} + 1,$$

$$\text{Si le message est jugé non fiable,} \quad \beta_{\text{nouveau}} = \beta_{\text{ancien}} + 1.$$

Une fois les paramètres α et β mis à jour, le score de confiance est calculé comme la moyenne de la distribution bêta, comme le montre la formule 3.1 :

$$S_{\text{Confiance}}(B) = \frac{\alpha}{\alpha + \beta} \tag{3.1}$$

Ce score, compris entre 0 et 1, représente la confiance actuelle de $TrainA$ dans la fiabilité des messages envoyés par $TrainB$, basée sur l'ensemble des observations passées.

3.3.3 Prise de Décision

La prise de décision dans notre modèle est basée sur la fiabilité du message et le score de confiance associé. Le processus de la prise de décision est illustré dans la Fig 3.3, et sa logique peut être résumée dans ce qui suit.

- Si le message est fiable et le score de confiance est supérieur à un seuil $\theta = \mathbf{0,5}$: autoriser le train à calculer l'autorité de mouvement.
  Dans ce cas, le train a confiance dans le message reçu. Cela signifie que les informations fournies sont considérées comme fiables et peuvent être utilisées pour le calcul de l'autorité de mouvement, permettant au train de poursuivre ses opérations en toute sécurité.
- Sinon : alerter.
  En cas d'alerte déclenchée par le module de confiance, par exemple lorsque le score de confiance d'un train émetteur passe en dessous de 0.5 , plusieurs types de messages peuvent être transmis afin de garantir une réaction rapide et adaptée. Tout d'abord, un avertissement est envoyé localement au train récepteur pour lui indiquer de ralentir ou de passer en mode de sécurité. En parallèle, une alerte est transmise au centre de supervision (ATS) afin d'enregistrer l'incident et de permettre une analyse ultérieure. Si le niveau de risque est jugé élevé, une notification peut également être diffusée aux trains à proximité pour les informer d'éventuelles communications compromises.

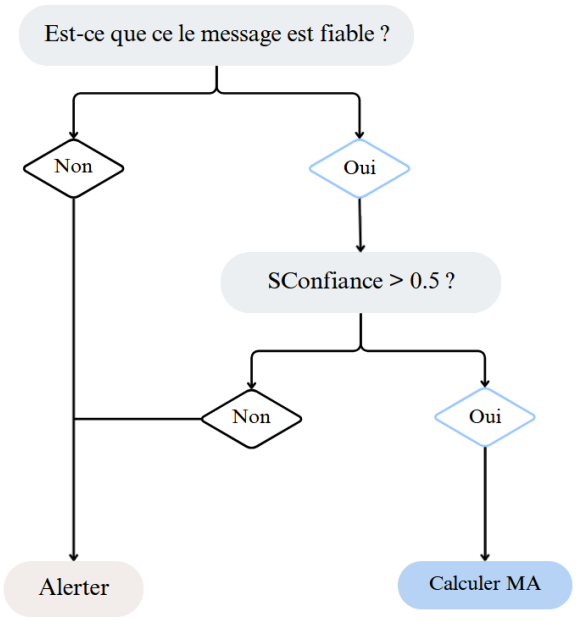

FIGURE 3.3 – Processus de prise de décision.

L'algorithme 1 récapitule les différentes étapes de notre approche RailTrust. Il décrit, de manière structurée, le processus complet d'évaluation de la qualité des données, de mise à jour des scores de confiance et de prise de décision.

Algorithm 1 Algorithme RailTrust

Input: M : Message reçu
α : Paramètre alpha de la distribution bêta
β : Paramètre bêta de la distribution bêta
$SeuilC$: Seuil de confiance

Initialisation : $\alpha > 0$, $\beta > 0$, $SeuilC = 0.5$
$E \leftarrow Embedding(M)$
$C \leftarrow CNN(E)$
$L \leftarrow LSTM(C)$
$MessageFiable \leftarrow PrédireFiabilité(L)$
if $MessageFiable = Vrai$ **then**
  $\alpha \leftarrow \alpha + 1$
else
  $\beta \leftarrow \beta + 1$
$SConfiance \leftarrow \frac{\alpha}{\alpha+\beta}$
  if $SConfiance > SeuilC$ ***et*** $MessageFiable = Vrai$ **then**
    Autoriser le calcul de l'autorité de mouvement (MA)
    return *"Autorité de Mouvement accordée"*
  else
    Envoyer une alerte
    return *"Alerte"*

3.4 Analyse sécurité

Examiner la résilience de RailTrust face aux différentes formes d'attaques courantes dans les systèmes ferroviaires intelligents est essentiel pour évaluer son efficacité et sa robustesse. Le tableau 3.2 montre quelques attaques que l'approche RailTrust peut contrer.

Type d'Attaque	**Description**	**Contre-mesure avec RailTrust**
Injection de faux messages	Un attaquant tente de perturber les opérations ferroviaires en injectant de fausses données dans les communications entre les trains.	L'utilisation de techniques d'apprentissage automatique (un modèle d'embedding, CNN, LSTM) permet de détecter les anomalies dans les données reçues. Si les données injectées ne correspondent pas aux modèles appris, elles seront identifiées comme non fiables. Les messages non fiables réduiront le score de confiance, limitant ainsi l'impact des fausses données sur les décisions du système.
Rejeu (Replay Attack)	Un attaquant intercepte et rejoue des messages légitimes précédemment envoyés pour tromper les trains.	L'algorithme RailTrust utilise des horodatages et étudie les séquences temporelles des messages. Les messages rejoués avec des horodatages dépassés seront détectés comme non fiables. De plus, le modèle LSTM permet de détecter des anomalies dans la succession chronologique des messages, ce qui contribue à déceler des attaques par rejeu .
Brouillage (Jamming)	Un attaquant submerge le canal de communication avec du bruit pour perturber les échanges de données entre les trains.	L'algorithme RailTrust peut détecter les anomalies dans les communications. Si les données reçues sont incomplètes ou corrompues en raison du brouillage, elles seront identifiées comme non fiables.
Attaque par clonage de train (Train Cloning)	Un attaquant fabrique un train virtuel ou matériel ayant un identifiant similaire à un train légitime pour envoyer des messages de tromperie.	En analysant les séquences temporelles et les features des messages, RailTrust peut détecter des incohérences, comme deux trains avec l'identifiant identique mais position ou vitesse différentes. Il permet d'éliminer les messages émis par le train cloné.

TABLE 3.3 – Analyse critique des attaques contrées par l'approche RailTrust.

3.5 Conclusion

Dans ce chapitre, nous avons proposé une approche visant à renforcer la confiance entre les trains au sein d'un système ferroviaire intelligent. En combinant des techniques avancées : Embedding, CNN, LSTM et la distribution bêta, notre solution permet l'analyse des messages, l'ajustement dynamique de la confiance et la prise de décision sécurisée.

Dans le chapitre suivant, nous procéderons à l'évaluation des performances de cette approche en analysant sa fiabilité et son efficacité.

4

Évaluation de Performances

4.1 Introduction

Ce chapitre décrit notre environnement de travail, les outils et bibliothèques utilisés, ainsi que le jeu de données employé pour évaluer notre modèle. Nous détaillons les étapes de prétraitement des données, les paramètres de simulation, et les résultats obtenus, en mettant l'accent sur des métriques clés comme la précision et le score F1. Enfin, nous analysons l'impact des scores de confiance sur la prise de décision.

4.2 Outils et bibliothèques utilisés

- **Visual Studio Code :** Visual Studio Code (VSCode) est un éditeur de code open-source et multiplateforme de Microsoft. Il supporte de nombreux langages de programmation et offre des fonctionnalités comme la coloration syntaxique, l'auto-complétion, le débogage et l'intégration avec Git. Il est personnalisable grâce à des extensions [42].
- **Python :** Python est un langage de programmation forte et facile d'utilisation, célèbre pour sa syntaxe esthétique et sa typologie dynamique. Il est excellent pour la création des scripts et pour le développement rapide des applications à l'aide de ses haut niveau données structures et sa programmation orientée objet approche simple [43].
- **Numpy :** NumPy est une bibliothèque Python bien connue utilisée pour faire des calculs mathématiques et scientifiques. Elle a beaucoup d'outils et de fonctionnalités qui peuvent être utilisés dans un projet de Data Science. Il est nécessaire de se faire connaître NumPy dans un projet de Data Science [44].
- **Pandas :** Pandas est une bibliothèque Python open-source conçue pour le traitement et l'analyse de données. Elle permet de charger, aligner, manipuler et unir des

données à la fois efficacement et flexiblement [44]. Pandas s'adapte très bien aux données structurées comme les tableaux et les séries temporelles.

- **Matplotlib :** Matplotlib [44] est une bibliothèque Python open-source pour la génération de graphiques et de visualisations de données haute qualité. Écrit initialement par John Hunter en 2002, il offre des fonctionnalités similaires à MATLAB pour la génération de tracés, histogrammes, diagrammes en barres et bien plus encore, avec seulement quelques lignes de code. Matplotlib est très largement utilisée à la fois par la communauté scientifique ainsi que pour l'intégration de graphiques dans les applications web et interfaces graphiques.
- **Tensorflow :** L'outil de calcul normalisé TensorFlow, développé par Google, est devenu la seconde génération du système Google Brain. Il sert de boîte à outils pour construire et exécuter des applications d'apprentissage automatique et/ou d'apprentissage profond (ou machine learning et deep learning). En effet, il permet de résoudre des problèmes mathématiques extrêmes, mais aussi d'effectuer des calculs numériques de haute performance avec une certaine aisance. Grâce à son architecture modulaire, ses calculs peuvent être effectués sur des CPU, des GPU ou des TPU [45].
- **Scikit-learn (Sklearn) :** Scikit-Learn est une bibliothèque Python qui fournit des algorithmes de machine learning efficaces et une API uniformisée. Elle propose un très large ensemble d'algorithmes d'apprentissage automatique supervisé et non supervisé, ainsi que d'outils pour la préparation et la transformation des données, la sélection des modèles et l'évaluation des performances. Scikit-learn est généralement appliquée à la construction de modèles prédictifs et au traitement de tâches de classification, régression, regroupement (clustering) et réduction de dimension. Préciée pour sa facilite d'emploi, son documentation complète et sa base de utilisateurs actifs, elle est le choix préférentiel de développeurs et chercheurs en apprentissage automatique [44].

- **Keras :** Keras est une bibliothèque Python qui rend le développement de réseaux de neurones beaucoup plus simple. Elle s'utilise avec TensorFlow en arrière-plan, et permet de créer des modèles profonds sans avoir à gérer toute la complexité technique. Ce qui est pratique, c'est qu'on peut facilement tester différentes architectures en modifiant juste quelques lignes. Keras est surtout appréciée pour sa clarté et sa souplesse, ce qui la rend accessible même quand on débute en deep learning [44].

4.3 Dataset

Afin d'obtenir un ensemble de données pertinent pour l'évaluation de performances de l'approche proposée, nous avons fusionné trois jeux de données, chacun apportant des éléments essentiels à l'analyse de la fiabilité des communications ferroviaires.

Le premier jeu de données fournit des informations sur la vitesse maximale nominale autorisée sur les lignes du réseau [46]. Il indique, en km/h, la vitesse théorique maximale que peuvent atteindre les trains les plus rapides, sans prendre en compte les limitations temporaires. De ce jeu, les attributs retenus sont l'identifiant de train, la vitesse maximale autorisée, ainsi que les coordonnées géographiques . Le deuxième jeu de données concerne la classification de l'armement des voies [47], permettant de caractériser l'infrastructure ferroviaire. Les attributs pertinents extraits sont le nom de la voie , les coordonnées géographiques. Enfin, le troisième jeu de données traite de la régularité mensuelle des TGV [48], en précisant si un train est arrivé à l'heure à son terminus. Les attributs sélectionnés dans ce cas incluent l'horodatage ainsi que la gare de départ, la gare d'arrivée.

Le tableau 4.1 présente les principaux attributs de notre base de données, caractérisant les messages échangés entre les trains.

Nous avons étiqueté ces messages en fonction de la vitesse et de la géolocalisation du train, en utilisant ces paramètres comme indicateurs clés de la fiabilité des communications.

Attribut	**Type**	**Description**
Message_ID	float64	Identifiant du message.
ID_Train	object	Identifiant du train.
NOM_VOIE	object	Nom de la voie.
V_MAX	float64	Vitesse maximale du train.
Geo_Train	float64	la géolocalisation du train.
Horodatage	object	Horodatage du message .
Gare_depart	object	Nom de la gare de départ.
Gare_arrivee	object	Nom de la gare d'arrivée.
Fiabilite (la classe)	bool	1 pour fiable, 0 pour non fiable.

TABLE 4.1 – Description des Attributs du Dataset.

4.4 Simulation

Dans cette section, nous allons détailler le processus d'évaluation des performances de notre modèle. Nous présentons les différentes étapes de prétraitement qui sont mises en œuvre.

La Figure 4.1 illustre les étapes clés de notre processus d'expérimentation, depuis le prétraitement des données jusqu'à l'évaluation finale des performances du modèle.

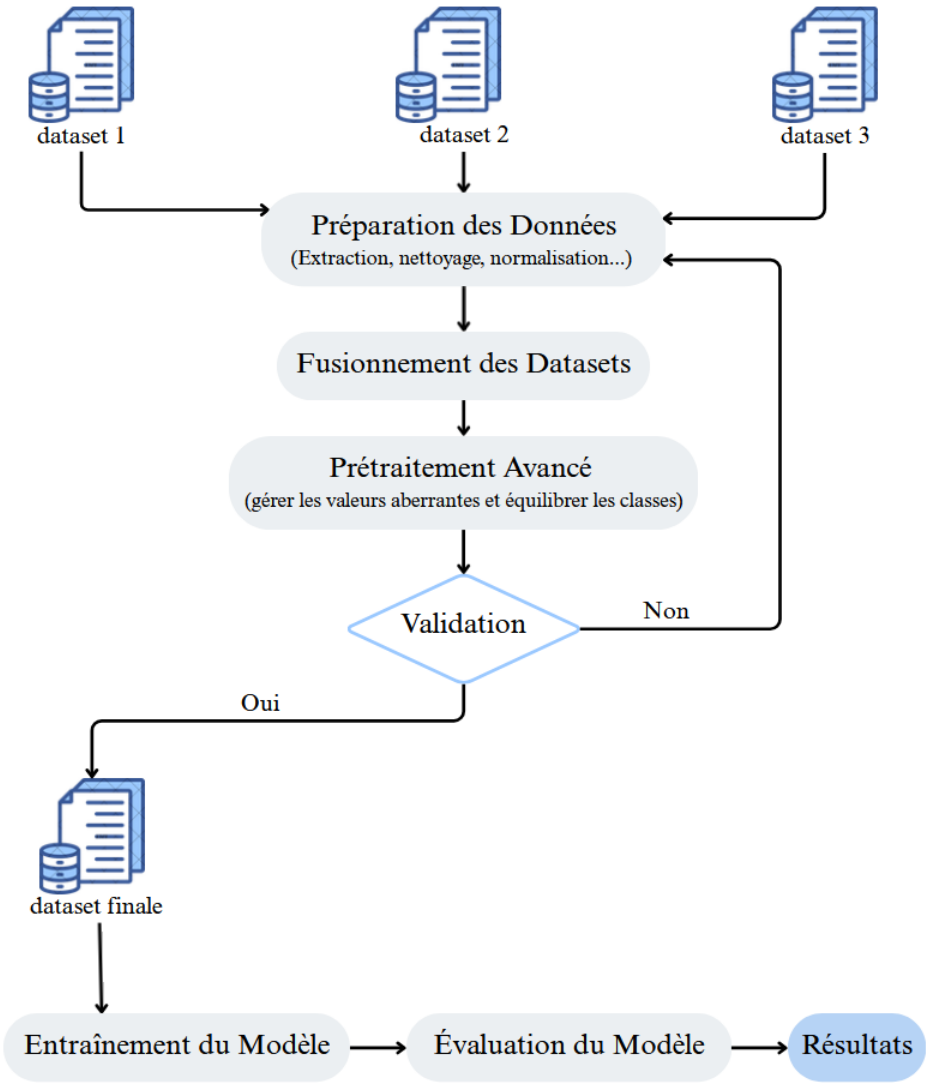

FIGURE 4.1 – Processus global d'expérimentation.

4.4.1 Prétraitement des données

Le prétraitement des données est une étape essentielle dans l'analyse des données de communication, visant à préparer les données brutes pour une analyse et une modélisation efficaces. Cette étape comprend plusieurs phases clés : le nettoyage des données, la normalisation.

4.4.1.1 Nettoyage des données

Le nettoyage des données consiste à corriger les erreurs, éliminer les valeurs aberrantes, traiter les valeurs manquantes. Les erreurs peuvent provenir de capteurs défectueux ou d'interférences environnementales, tandis que les valeurs aberrantes peuvent être dues à des événements imprévus. Le traitement des valeurs manquantes est crucial pour éviter

les erreurs d'analyse, et la réduction du bruit améliore la qualité des données.

- **Suppression des valeurs manquantes** : Les lignes contenant des valeurs manquantes sont éliminées pour garantir la complétude des données.
- **Élimination des doublons** : Les lignes dupliquées sont supprimées pour éviter les redondances.
- **Traitement des valeurs aberrantes** : Les valeurs qui s'écartent significativement de la moyenne sont identifiées et supprimées pour améliorer la qualité des données.
- **Prétraitement des données textuelles** : Les colonnes textuelles sont nettoyées en convertissant le texte en minuscules, en supprimant les mots dupliqués consécutifs.

4.4.1.2 Normalisation des données

La normalisation des données transforme les données pour les mettre à une échelle commune, ce qui est crucial pour optimiser les performances des algorithmes de machine learning en réduisant les biais liés aux différentes échelles de mesure et en garantissant une contribution équitable de chaque variable à l'analyse. Dans ce contexte, nous avons utilisé la méthode Min-Max pour normaliser les colonnes numériques, en les transformant pour qu'elles soient comprises dans une plage commune, généralement [0, 1], afin d'uniformiser leur échelle. La formule utilisée pour la normalisation des données est la suivante :

$$x' = \frac{x - x_{\min}}{x_{\max} - x_{\min}} \tag{4.1}$$

où :

- x est la valeur d'une caractéristique avant normalisation,
- $x_{\min}$ est la valeur minimale de cette caractéristique dans les données d'entraînement,
- $x_{\max}$ est la valeur maximale de cette caractéristique dans les données d'entraînement,
- x' est la valeur normalisée de la caractéristique.

4.4.1.3 Division du dataset

Notre dataset comprend un total de 9847 données, dont 5028 données fiables (classe 1) et 4819 données non fiables (classe 0), ce qui traduit une distribution équilibrée entre les deux classes. Les données ont été divisées en trois ensembles : 72 % des données ont été utilisées pour l'entraînement du modèle, 8 % pour la validation, et 20 % ont été réservées pour les tests.

Cette division a été réalisée en deux étapes : d'abord, une séparation initiale du jeu de données en 80 % pour l'entraînementet 20 % pour le test, puis une subdivision d'ensemble d'entraînement complet en 90 % pour l'entraînement et 10 % pour la validation.

4.4.2 Paramètres

Dans les simulations, nous avons utilisé un modèle Embedding et une dimension vectorielle de 100. Puis, nous avons inséré une couche de type CNN avec plusieurs couplages, tant pour les filtres que pour les tailles des noyaux. L'ajout d'une couche convolutionnelle n'avait pas produit de meilleurs résultats en termes de convergence. Les premiers résultats unidimensionnels s'étaient stabilisés avec une unique couche CNN de 32 filtres avec un noyau de forme (3×3).

La sortie du CNN ayant été traitée avec un LSTM, plusieurs tailles pour cette couche ont été essayées. Avec une première configuration à 16 unités. En doublant la taille à 32, les résultats se sont vus considérablement améliorés. L'introduction d'une troisième couche LSTM a amélioré les performances.
Les paramètres sont illustré dans le tableau 4.1 .

Paramètre	**Valeurs utilisées**
Taille du lot	128
Nombre d'époques	10
Dimension des embeddings	100
Longueur maximale des séquences	187
Nombre de filtres (Conv1D)	32
Taille du noyau (Conv1D)	3
Taille du pooling (MaxPooling1D)	2
Unités LSTM	32 , 32 , 32
Dropout LSTM	0.3, 0.4
Unités Dense	32
Dropout Dense	0.5
Taux d'apprentissage	1×10^{-4}

TABLE 4.2 – Paramètres du modèle.

4.4.3 Résultats obtenus

Pour évaluer de manière plus approfondie les performances de notre modèle, nous avons utilisé plusieurs métriques d'évaluation. Le tableau 4.2 présente les résultats obtenus.

Métrique	**Valeur**
Précision	0.969
Exactitude	0.981
Rappel	0.995
F1-Score	0.987
Perte	0.16

TABLE 4.3 – Résultats de l'évaluation.

4.4.3.1 Précision

La précision est définie comme la proportion de prédictions positives correctes parmi l'ensemble des prédictions positives effectuées par le modèle. Notre modèle présente une performance extrêmement élevée avec une précision de 97%.
La formule pour calculer la précision est la suivante :

$$\text{Précision} = \frac{TP}{TP + FP} \times 100\% \tag{4.2}$$

4.4.3.2 Exactitude (Accuracy)

L'exactitude est définie comme la proportion des prédictions correctes (vrais positifs et vrais négatifs) parmi le nombre total de prédictions effectuées, Avec une exactitude de 0.981 , cela signifie que 98% des prédictions faites par le modèle sont correctes.La formule pour calculer l'exactitude est la suivante :

$$\text{Exactitude} = \frac{VP + VN}{VP + FN + FP + VN} \times 100\% \tag{4.3}$$

4.4.3.3 Rappel

Le rappel, ou sensibilité, mesure la capacité du modèle à identifier tous les échantillons positifs. Un rappel de 0,995 indique que le modèle détecte environ 99,5% des vrais positifs. La formule pour calculer le rappel est la suivante :

$$\text{Rappel} = \frac{TP}{TP + FN} \times 100\% \tag{4.4}$$

4.4.3.4 F1-Score

Un F1-score de 98% , qui est la moyenne harmonique de la précision et du rappel, montre que le modèle maintient un bon équilibre entre ces deux métriques, ce qui est important pour obtenir une performance robuste en pratique. La formule pour calculer le F1 –score est la suivante :

$$\text{F1-Score} = 2 \times \frac{\text{Précision} \times \text{Rappel}}{\text{Précision} + \text{Rappel}} \tag{4.5}$$

4.4.3.5 Perte (Loss)

La fonction de perte mesure l'erreur totale entre les prédictions de modèle et les valeurs réelles des données d'entraînement ou de validation. Une perte de 0,16 indique que les prédictions sont très proches des vraies valeurs, prouvant la précision élevée du modèle.

4.4.3.6 Matrice de confusion

La matrice de confusion constitue une technique d'évaluation qui permet de présenter les résultats d'un algorithme de classification. En d'autres termes, il s'agit d'un tableau exposant les nombres d'instances d'une classe de vérité terrain par rapport au nombre d'instances des classes prédites. La matrice de confusion est un des indicateurs de nombreuses métriques de performance des modèles de classification [49]. La Matrice de confusion de notre modèle est représentée sur la Figure 4.2.

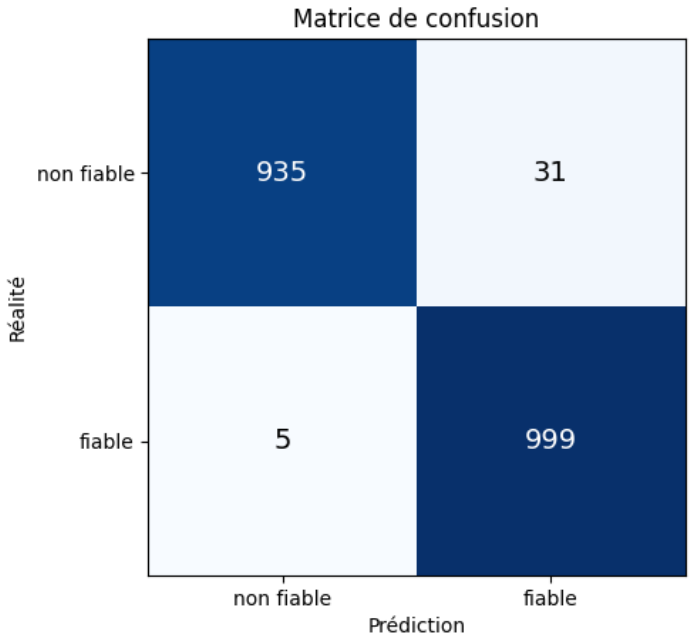

FIGURE 4.2 – Matrice de confusion de notre modèle.

Cette matrice de confusion montre que notre modèle, qui classe les messages en fiables ou non fiables, est performant. Il identifie correctement 999 messages fiables (vrais positifs (VP)) sur 1004 (sensibilité de 99,5 %) et 935 messages non fiables(vrais négatifs) sur 966 (spécificité de 96,8 %). Cependant, les 31 faux positifs montrent des erreurs où le modèle a incorrectement prédit qu'un message était fiable, tandis que les 5 faux négatifs (FN) indiquent de rares cas où le modèle a manqué de reconnaître des messages réellement fiables.

4.4.3.7 La courbe ROC :

La Figure 4.3 présente la courbe ROC (Receiver Operating Characteristic) obtenue pour notre modèle. Elle illustre l'évolution du taux de vrais positifs (sensibilité) en fonction du taux de faux positifs (1 - spécificité) pour différents seuils de classification.

Avec une aire sous la courbe (AUC) de 0,99, notre modèle démontre une excellente capacité à bien distinguer les messages fiables des messages non fiables . Cela signifie que le modèle présente de très bonnes performances globales, avec un risque très faible de mauvaise classification des messages.

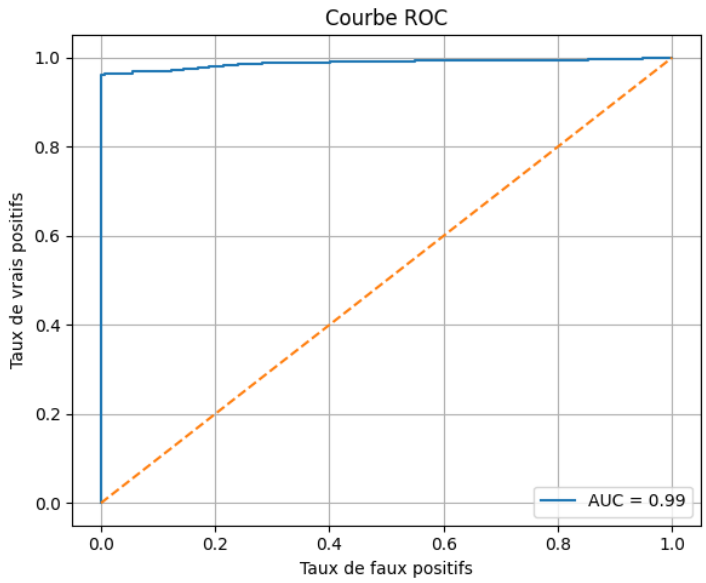

FIGURE 4.3 – La courbe ROC de notre modèle.

4.4.3.8 Performances du Modèle durant l'Apprentissage

Au cours de l'apprentissage, notre modèle a démontré une amélioration progressive de la précision et une diminution constante de la perte. Les courbes illustrent une bonne convergence, confirmant la capacité de notre modèle à apprendre efficacement et à généraliser sur les données de validation.

- **Courbes de perte et de précision d'entraînement**

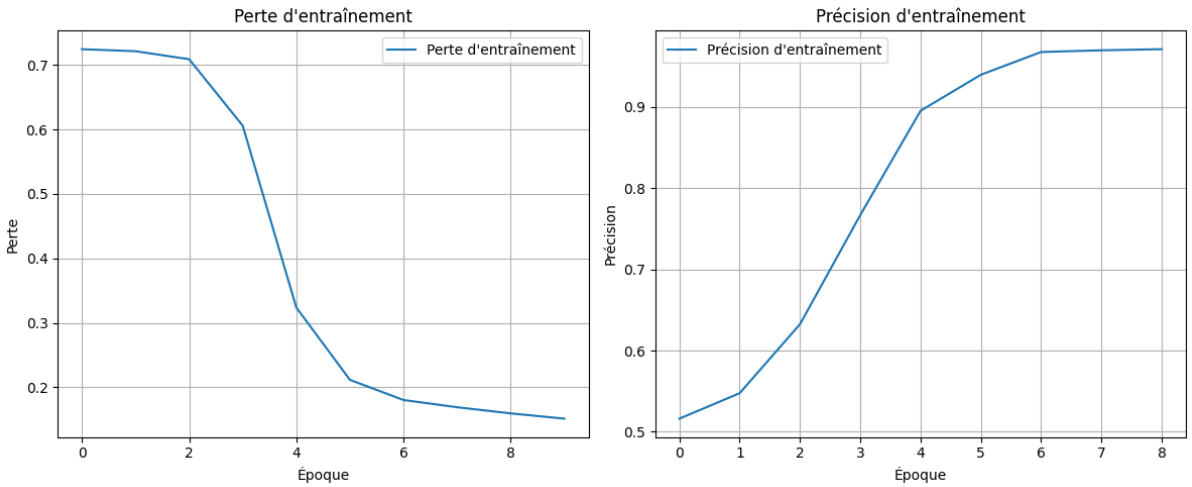

FIGURE 4.4 – Courbes de perte et de précision d'entraînement .

La figure 4.4 présente deux graphiques. À gauche, on observe la fonction de perte de d'entraînement en fonction des époques, tandis qu'à droite, il y a la précision de d'entraînement sur le même intervalle.
La courbe de perte diminue régulièrement au fur et à mesure que le nombre d'époques augmente. Cela indique que le modèle apprend et s'améliore progressivement, réduisant l'erreur sur les données d'entraînement. La perte passe d'environ 0,7 à environ

0,25 après 8 époques, ce qui montre une amélioration significative de la précision du modèle.

La précision augmente avec le nombre d'époques, atteignant près de 0,98 après environ 8 époques, puis se stabilise avec quelques variations mineures autour de cette valeur. Cela montre que le modèle devient de plus en plus capable de faire des prédictions correctes sur les données d'entraînement et maintient une haute précision tout au long de l'entraînement. Cependant, il est essentiel de comparer ces résultats avec ceux de la validation Figure (4.5). Pour s'assurer qu'il n'y a pas de surapprentissage (overfitting).

- **Courbes de perte et de précision de validation :**

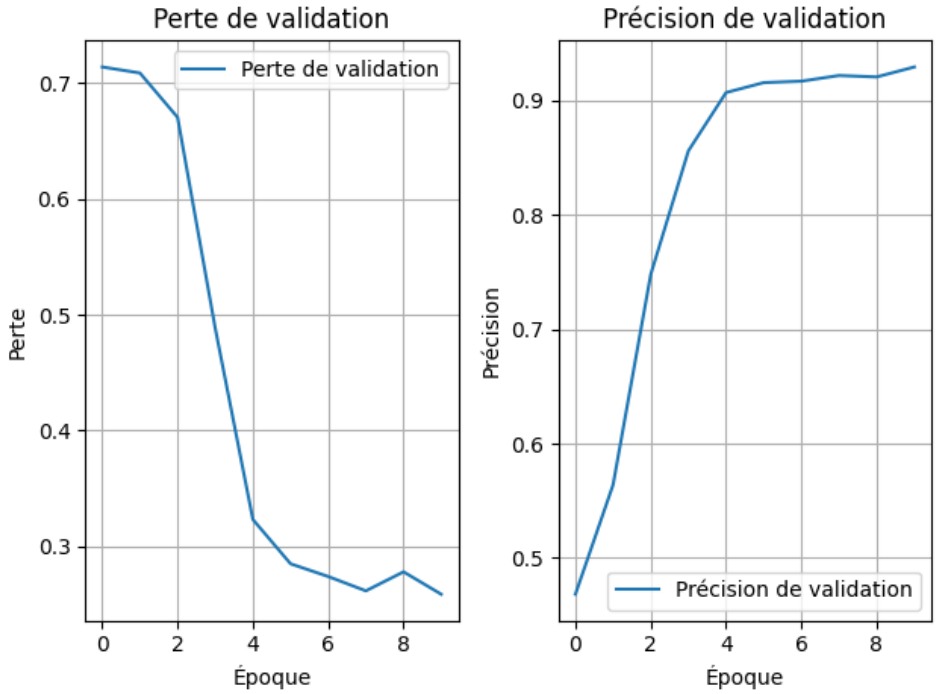

FIGURE 4.5 – Courbes de perte et de précision de validation .

La figure 4.5 montre présente deux graphiques similaires à ceux de la première figure, mais cette fois pour les données validation.
La perte de validation diminue également et atteint environ 0,1 après 8 époques. Cela indique que le modèle devient de plus en plus précis sur les données de validation, avec une erreur très faible.
La précision de validation montre une augmentation régulière et atteint environ 0,94 au fil des époques. Cela indique que le modèle généralise bien aux données de validation et devient de plus en plus précis pour classer correctement les échantillons de validation.

Le fait que les courbes de validation et d'entraînement suivent des tendances similaires et atteignent des valeurs proches en termes de précision et de perte suggère que le modèle généralise bien et ne se contente pas de mémoriser les données d'entraînement.

4.5 Analyse des scores de confiance et de la prise de décision

Dans cette section, nous analysons l'impact des scores de confiance, calculés de manière dynamique, sur les décisions prises par le système. Les informations utilisées ont été extraites à partir de notre jeu de données expérimental, dans lequel plusieurs messages ont été émis par différents trains.

Un seuil de confiance $\theta = 0{,}5$ a été défini afin d'orienter la prise de décision, en particulier pour déterminer si le calcul de l'autorité de mouvement du train doit être autorisé ou non.
Pour illustrer ce processus, nous avons sélectionné le train B avec l'ID 825bf272 (Table 4.3).

Temps	**Fiables**	**Non Fiables**	$\mathbf{S_{confiance}(B)}$	**Décision**
t_0	132	130	0,504	/
t_1	132	131	0,502	Non autorisé
t_2	132	132	0,50	Non autorisé
t_3	133	132	0,502	Autorisé

TABLE 4.4 – Évolution du score de confiance du train B

- Initialement à t_0, le train B a déjà envoyé 132 messages fiables et 130 non fiables au train A (récepteur). Cela lui donne un score de confiance de 0.504.
- À t_1, le train envoie un message M1, évalué comme non fiable, ce qui fait passer le score de confiance à 0,502 . Même s'il est encore au-dessus de 0.5, le train n'est pas autorisé à cause de ce dernier message non fiable.
- À t_2, un autre message non fiable, M2, est envoyé. Le score de confiance tombe à 0.50. La décision reste "non autorisé", à cause du message non fiable et du score qui n'est pas strictement supérieur au seuil.
- À t_3, un message fiable, M3, est envoyé, et le score de confiance remonte à 0.502. Cette fois, le train A est autorisé a calculer l'autorité de mouvement.

4.6 Conclusion

Ce chapitre offre une vue d'ensemble complète de l'évaluation des performances de notre modèle RailTrust, en mettant en lumière les outils utilisés, le prétraitement des données, ainsi que les ajustements des hyperparamètres. À travers une série de simulations, nous avons analysé les résultats obtenus selon plusieurs métriques, telles que la précision, l'exactitude, le rappel et le F1-score. Une attention particulière a également été portée à l'évolution des scores de confiance et à leur influence sur le processus de prise de décision. Les résultats obtenus confirment la pertinence et l'efficacité de notre approche pour renforcer la confiance dans les systèmes ferroviaires intelligents.

Conclusion générale et perspectives

Au terme de cette étude portant sur l'approche RailTrust, visant à renforcer la confiance dans les communications des systèmes ferroviaires intelligents, plusieurs conclusions significatives peuvent être tirées, ouvrant la voie à de nouvelles perspectives pour la confiance ferroviaire intelligente.

Notre étude a débuté par une présentation détaillée des systèmes de transport ferroviaire intelligents, en exposant leurs principes de fonctionnement, leurs différentes architectures, ainsi que la sécurisation des échanges d'informations dans un environnement fortement interconnecté et dynamique. Cette première phase a permis de mettre en lumière l'importance de la confiance dans les communications inter-trains, facteur essentiel pour garantir la sécurité et la fiabilité de l'exploitation ferroviaire moderne.

Sur cette base, nous avons proposé une approche hybride intégrant des techniques avancées d'apprentissage profond pour le traitement et l'analyse des messages échangés entre les trains. Notre modèle s'appuie sur l'utilisation des embeddings pour transformer les messages textuels en représentations vectorielles exploitables par les algorithmes d'apprentissage, sur les réseaux de neurones convolutionnels (CNN) pour extraire automatiquement les caractéristiques des données traitées, et sur les réseaux de neurones à mémoire long terme (LSTM) pour modéliser les relations temporelles et séquentielles inhérentes aux communications inter-trains. Afin d'évaluer la fiabilité des messages et d'ajuster dynamiquement la confiance attribuée à chaque train, nous avons introduit l'utilisation de la distribution bêta pour modéliser les scores de confiance et alimenter le processus de prise de décision.

L'évaluation expérimentale de notre approche a été réalisée sur un jeu de données conséquent de communications ferroviaires, dans un environnement de simulation développé sous le langage Python. Les résultats obtenus démontrent des performances très satisfaisantes, avec une précision de 97 %, un rappel de 99,5%, un score F1 de 98,7% et une excellente exactitude, illustrant ainsi la capacité de RailTrust à évaluer efficacement la fiabilité des échanges d'informations dans des scénarios réalistes.

En perspective, les recherches futures pourront s'orienter vers l'enrichissement et la diversification des données d'apprentissage afin d'améliorer la robustesse et la capacité de généralisation du modèle. De plus, une comparaison approfondie avec les approches existantes dans la littérature permettra de situer objectivement les performances et les limites de l'approche RailTrust. Enfin, l'implémentation de notre approche sur une plateforme réelle constituera une étape essentielle pour valider son efficacité et sa robustesse en conditions d'exploitation opérationnelles.

Bibliographie

[1] Yu, Zujun, Hongwei Wang, and Feng Chen. "Security of Railway Control Systems : A Survey, Research Issues and Challenges." Journal of Modern Transportation, vol. 2, no. 1, 2022.

[2] Qin, Y., Cao, Z., Sun, Y., Kou, L., Zhao, X., Wu, Y., Liu, Q., Wang, M., Jia, L. (2023). Research on active safety methodologies for intelligent railway systems. Engineering, 27, 266–279.

[3] Marik, G., Dutta, A. (2023). A Sustainable Evolution of Indian Railway. Journal of Transactions in Systems Engineering, 1(3), 131-139.

[4] Chen, Tan, Yong Zhang, Haileng Wang, Tao Tang, and Kaicheng Li. "Architecture Design of a Novel Train-centric CBTC System." IEEE Access, vol. 6, 2018.

[5] Ma, J., Wang, H., Meng, L. (2017). Communication-Based Train Control (CBTC) Systems : A Comprehensive Review. IEEE Transactions on Intelligent Transportation Systems, 18(6), 1430-1449.

[6] T. Tang, Train Control System, 2nd ed., Beijing : China Railway Publishing House, 2014, pp. 195-197.

[7] Wang, W., Zhang, W., Guo, W., & Fan, P. (2018). Safety monitor for train-centric CBTC system. *IET Intelligent Transport Systems*, 12(10), 1252–1258.

[8] Schnieder, L. (2017). Communication-Based Train Control (CBTC) : Components - Functions - Operations.

[9] Lin, Y. (2022). The impact of virtual reality in physics education : A study using VR simulation to understand magnetic fields. Journal of Physics : Conference Series, 2246(1), 012077.

[10] Lin, J., Xu, Q. (2020). Functional safety verification of train control procedure in train-centric CBTC by colored petri net. Archives of Transport, 54(2), 43-58.

[11] Soderi, S., Masti, D., Lun, Y. Z. (2023). Railway Cyber-Security in the Era of Interconnected Systems : A Survey. IEEE Transactions on Intelligent Transportation Systems. DOI : 10.1109/TITS.2023.3254442

[12] Kour, R., Patwardhan, A., Thaduri, A., Karim, R. (2022). A Review on Cybersecurity in Railways. Proceedings of the Institution of Mechanical Engineers, Part F : Journal of Rail and Rapid Transit, 237(1), 3-20. DOI :10.1177/09544097221089389

[13] Voronko, I. (2020). The Security of IoT Systems in Railway Transport. Journal of Information Security and Applications.

[14] Van-Hoan Vu. Infrastructure de gestion de la confiance sur internet. PhD thesis, Ecole Nationale Supérieure des Mines de Saint-Etienne, 2010.

[15] Aït-Salem Boussad. Sécurisation des réseaux ad hoc : systèmes de confiance et de détection de répliques. PhD thesis, Université de Limoges, 2011.

[16] Shuo Ma, Ouri Wolfson, and Jie Lin. A survey on trust management for intelligent transportation system. CTS '11, page 18–23, New York, NY, USA, 2011. Association for Computing Machinery.

[17] X. Chen, J. Ding, et Z. Lu, « A Decentralized Trust Management System for Intelligent Transportation Environments », IEEE Trans. Intell. Transport. Syst., p. 1-14, 2020, doi :10.1109/TITS.2020.3013279.

[18] Woschank, M., Rauch, E., Zsifkovits, H. (2020). A review of further directions for artificial intelligence, machine learning, and deep learning in smart logistics. Sustainability, 12(9), 3760.https://doi.org/10.3390/su12093760

[19] Janiesch, C., Zschech, P., Heinrich, K. (2021). Machine learning and deep learning. Electronic Markets, 31(2), 1-15. https://doi.org/10.1007/s12525-021-00475-2

[20] Bhat, M., Rabindranath, M., Chara, B. S., Simonetto, D. A. (2023). Artificial intelligence, machine learning, and deep learning in liver transplantation. Journal of Hepatology, 78(3), 628-643.https://doi.org/10.1016/j.jhep.2023.01.006

[21] Z. Rzayeva and E. Alasgarov, "Facial Emotion Recognition using Convolutional Neural Networks," IEEE 13th International Conference on Application of Information and Communication Technologies 2019, pp. 1 - 5.

[22] S. R. Livingstone, F. A. Russo, "The Ryerson Audio-Visual Database of Emotional Speech and Song (RAVDESS) :" A dynamic, multimodal set of facial and vocal expressions in North American English. PLoS ONE Vol. 13 No. 5, 2018, e0196391

[23] S. Bursic, G. Boccignone, A. Ferrara, A. D'Amelio, R. Lanzarotti, "Improving the Accuracy of Automatic Facial Expression Recognition in Speaking Subjects with Deep Learning." Appl. Sci. Vol. 10, No. 11, 2020, 4002.

[24] Khorram, S., Jehbez, N. (2023). A Hybrid CNN-LSTM Approach for Monthly Reservoir Inflow Forecasting. Water Resources Management, 37(10), 4097–4121. https://doi.org/10.1007/s11269-023-03541-w

[25] Hochreiter, Sepp, and Jürgen Schmidhuber. 1997. "Long Short-Term Memory." Neural Computation 9 (8) : 1735–1780.doi : https://doi.org/10.1162/neco.1997.9.8.1735

[26] S. Abbaspour, F. Fotouhi, A. Sedaghatbaf, H. Fotouhi, M. Vahabi, and M. Linden, "A Comparative Analysis of Hybrid Deep Learning Models for Human Activity Recognition," Sens., vol. 20, no. 19,2020, doi : :https://doi.org/10.3390/s20195707.

[27] W. Fang, Y. Chen, and Q. Xue, "Survey on research of RNN-based spatio-temporal sequence prediction algorithms," J. Big. Data., vol. 3, no. 3, pp. 97, 2021, doi : https://doi.org/10.32604/jbd.2021.016993.

[28] J. Yue-Hei Ng, M. Hausknecht, S. Vijayanarasimhan, O. Vinyals, R. Monga, and G. Toderici, "Beyond short snippets : Deep networks for video classification," in Proc. IEEE/CVF Conf. Comput. Vis. Pattern.Recognit., 2015, pp. 4694-4702

[29] H. Apaydin, H. Feizi, M. T. Sattari, M. S. Colak, S. Shamshirband, and K.-W. Chau, "Comparative analysis of recurrent neural network architectures for reservoir inflow forecasting," Water., vol. 12, no.5, pp. 1500, 2020, doi : https://doi.org/10.3390/w12051500.

[30] Karim, Fazle, Somshubra Majumdar, Houshang Darabi, and Shun Chen. "LSTM Fully Convolutional Networks for Time Series Classification." IEEE Access, vol. 6, 2018, pp. 1662–1672.

[31] DataScientest, *Long Short-Term Memory : Tout Savoir*, https://datascientest.com/long-short-term-memory-tout-savoir, consulté le 23 Avril 2025.

[32] Weaviate. (2024). Using ML Models for Embedding - Weaviate Academy.https://weaviate.io/developers/academy/js/standalone/using-ml-models/embedding

[33] Damgaard, C. F., Irvine, K. M. (2019). Using the beta distribution to analyse plant cover data. Journal of Ecology, 107(6), 2747-2759. https://doi.org/10.1111/1365-2745.13200

[34] Wang, Y., Zhang, W., Wang, X., Guo, W., Khan, M. K., & Fan, P. (2020). Improving the security of LTE-R for high-speed railway : from the access authentication view. IEEE Transactions on Intelligent Transportation Systems, 23(2), 1332-1346.

[35] Li, Q., Bu, B., Zhao, J. (2021). A Novel Hierarchical Situation Awareness Model for CBTC Using SVD Entropy and GRU With PRD Algorithms. IEEE Access, 9, 137765-137784.

[36] Feng, Y., Zhong, Z., Sun, X., Wang, L., Lu, Y., & Zhu, Y. (2023). Blockchain enabled zero trust based authentication scheme for railway communication networks.IEEE Access, 11, 45678-45692.

[37] Gao, B., Bu, B. (2019). A novel intrusion detection method in train-ground communication system. IEEE Access, 7, 178726-178743.

[38] Chen, Y., Chang, T., & Liu, W. (2023). Improved SRP algorithm and bidirectional heterogeneous LTE-R authentication key. IET Communications, 17(12), 1300-1309. https ://doi.org/10.1049/ermi2.12624

[39] Lim, H. W., Temple, W. G., Tran, B. A. N., Chen, B., Kalbarczyk, Z., Zhou, J. (2019). Data integrity threats and countermeasures in railway spot transmission systems. ACM Transactions on Cyber-Physical Systems, 4(1), 1-26.

[40] Yu, W., Zhang, L., Xu, Q. (2023). Real-time reliability access control based on rail traffic data platform. Electronics, 12(5), 1105.

[41] Kour, R., Thaduri, A., Karim, R. (2019). Railway Defender Kill Chain to Predict and Detect Cyber-Attacks. Journal of Cybersecurity and Information Systems, 12(4), 45-67.

[42] Bility. (s.d.). Définition Visual Studio Code https://bility.fr/definition-visual-studio-code/

[43] Python Software Foundation (2025). Tutoriel Python 3.13. https://docs.python.org/fr/3.13/tutorial/index.html (visité le 22 avril 2025).

[44] DataScientest (2025). :https://datascientest.com/(visité le 22 avril 2025).

[45] Tensorflow documentation.

[46] SNCF Open Data. (2025). https://data.sncf.com/explore/dataset/vitesse-maximale-nominale-sur-ligne/ (visité le 25 avril 2025).

[47] SNCF Open Data. (2025). https://data.sncf.com/explore/dataset/classification-darmement-des-voies/(visité le 25 avril 2025).

[48] SNCF Open Data. (2025). https://ressources.data.sncf.com/explore/dataset/regularite-mensuelle-tgv-aqst/(visité le 26 avril 2025).

[49] IBM .https://www.ibm.com/fr-fr/think/topics/confusion-matrix/(visité le 30 avril 2025).

Résumé

Ce mémoire présente une approche innovante pour renforcer la confiance dans les systèmes ferroviaires intelligents, en utilisant des techniques avancées d'apprentissage automatique. L'étude se concentre sur le renforcement de la confiance dans les communications entre les trains dans un environnement TC-CBTC (Train-Centric Communication-Based Train Control). La méthodologie comprend l'évaluation de la qualité des données, la mise à jour des scores de confiance, et la prise de décision basée sur ces scores. Les techniques utilisées incluent des modèles d'embedding, des réseaux de neurones convolutifs (CNN), des réseaux à mémoire long terme (LSTM), et la distribution bêta pour modéliser la confiance. Les résultats montrent une précision de 97%, une exactitude de 98,1%, un rappel de 99,5%, et un F1-score de 98,7%, indiquant une performance élevée du modèle. Cette approche offre une solution prometteuse renforcer la confiance dans les systèmes ferroviaires intelligents, bien que des défis persistent pour son intégration et son adaptation dans des environnements réels et variés.

Mots-clés : Systèmes ferroviaires intelligents, Apprentissage automatique, TC-CBTC, Modèles d'embedding, CNN, LSTM, Distribution bêta, Confiance.

Abstract

This thesis presents a novel technique for enhancing confidence in intelligent rail systems through advanced machine learning. The study focuses on the reinforcement of trust in train-to-train communications in the context of an TC-CBTC (Train-Centric Communication-Based Train Control) environment. The process includes quality estimation of data, updating the trust values, and decision-making with trust scores. Methods utilized are embedding methods, convolutional neural networks (CNN), long short-term memory networks (LSTM), and beta distribution to model trust. The measures derived are precision of 97%, accuracy of 98.1%, recall of 99.5%, and F1-score of 98.7%, which attest that the model is working very well. This approach offers a viable answer to enhancing Trust in Smart Railway Systems, although there remain challenges for its integration and application in real and varied environments.

Keywords : Intelligent Rail Systems, Machine Learning, TC-CBTC, Embedding Models, CNN, LSTM, Beta Distribution, Trust.