République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

ECOLE SUPERIEURE EN INFORMATIQUE 08 MAI 1945 SIDI BEL ABBES

Mémoire

En vue de l'obtention du diplôme d' **ingenieur d'état**

Filière : **Informatique**

Spécialité : **Ingénierie des Systèmes Informatiques (ISI**)

Thème

Integration of Metaheuristic Optimization and AI for Cyber Threat Mitigation in Smart Vehicular Networks

Présenté par :
M^r KAMRAOUI Ibrahim
Soutenu le : 08/07/2025

Devant le jury composé de:

Président:	M^r AZZA Mohammed	Maître de conférences A
Examinatrice:	M^{me} BELMEKKI Ghizlene Amira	Maître de conférences B
Encadrante:	M^{me} Baba-Ahmed Manel	Maître de conférences B
Co-Encadrant:	M^r MAHAMMED Nadir	Maître de conférences A

Année universitaire 2024/2025

Abstract

Modern intelligent transportation systems depend on smart vehicular networks to enable seamless vehicle-to-vehicle and vehicle-to-infrastructure communication, enhancing both road safety and traffic efficiency. However, this increased connectivity introduces a broad spectrum of cyber threats, posing significant risks to public safety and data integrity.

To address these challenges, this work presents a comprehensive cyber threat detection framework for smart vehicular networks, centered on a robust XGBoost-based architecture. The proposed system employs a multi-stage optimization pipeline: metaheuristic feature selection (using Battle Royale Optimization), advanced feature engineering, and global hyperparameter tuning via Differential Evolution. This approach systematically reduces feature dimensionality, improves model interpretability, and maximizes detection performance.

A sender-aware validation protocol is implemented to ensure true generalization to unseen vehicular entities, effectively preventing data leakage and overfitting. The optimized XGBoost model demonstrates strong and realistic accuracy and macro-averaged F1-score on the VeReMi Extension dataset. The system also uses class weighting strategies to address severe class imbalance and is designed for real-time deployment, supporting integration with existing vehicular security infrastructures.

This dissertation briefly presents the technologies, methodology, and optimization strategies used, along with an evaluation of results and their implications for intelligent transportation security. The findings confirm that combining metaheuristic optimization with advanced machine learning provides a scalable and effective solution for cyber threat detection in smart vehicular networks.

Key words: Smart Vehicular Networks, Cyber Threat Detection, Machine Learning, Metaheuristic Optimization, Sender-Aware Validation, Intelligent Transportation Systems.

Résumé

Les systèmes de transport intelligents modernes reposent sur des réseaux véhiculaires intelligents afin de permettre une communication fluide entre véhicules (V2V) et entre véhicules et infrastructures (V2I), améliorant ainsi la sécurité routière et l'efficacité du trafic. Cependant, cette connectivité accrue expose ces réseaux à un large éventail de cybermenaces, présentant des risques importants pour la sécurité publique et l'intégrité des données.

Pour répondre à ces défis, ce travail propose un cadre complet de détection des cybermenaces pour les réseaux véhiculaires intelligents, basé sur une architecture robuste exploitant XGBoost. Le système proposé utilise une chaîne d'optimisation en plusieurs étapes : sélection de caractéristiques par métaheuristique (via Battle Royale Optimization), ingénierie avancée des caractéristiques et réglage global des hyperparamètres par Differential Evolution. Cette approche permet de réduire systématiquement la dimensionnalité, d'améliorer l'interprétabilité du modèle et de maximiser les performances de détection.

Un protocole de validation tenant compte de l'expéditeur est mis en œuvre afin d'assurer une véritable généralisation à de nouveaux véhicules, évitant efficacement la fuite de données et le surapprentissage. Le modèle XGBoost optimisé affiche une précision robuste et un score F1 macro-moyenné réaliste sur le jeu de données VeReMi Extension. Le système intègre également des stratégies de pondération des classes pour traiter le déséquilibre sévère des classes et est conçu pour un déploiement en temps réel, facilitant l'intégration avec les infrastructures de sécurité véhiculaires existantes.

Ce mémoire présente brièvement les technologies, la méthodologie et les stratégies d'optimisation utilisées, ainsi qu'une évaluation des résultats et de leurs implications pour la sécurité des transports intelligents. Les résultats confirment que la combinaison de l'optimisation métaheuristique et de l'apprentissage automatique avancé offre une solution évolutive et efficace pour la détection des cybermenaces dans les réseaux véhiculaires intelligents.

Mots-clés : Réseaux véhiculaires intelligents, Détection des cybermenaces, Apprentissage automatique, Optimisation métaheuristique, Validation tenant compte de l'expéditeur, Systèmes de transport intelligents.