الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي و البحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
المدرسة العليا للاعلام الالي 8 ماي 5491
École Supérieure en Informatique
8 Mai 1945 Sidi Bel Abbès

THESIS

To obtain the diploma of **Engineer**
Field: **Computer Science**
Specialty: **Artificial Intelligence and Data Science (IASD)**

Theme

Artificial Intelligence-based intrusion detection and cyber threats mitigation system within smart vehicular network (VANETs)

Presented by:
AYAD Amani

Submission Date: **01/10/2025**
In front of the jury composed of:

Dr. ANANI Djihed	President
Dr. BABA-AHMED Manel	Supervisor
Dr. BOUSMAHA Rabab	Co-Supervisor
Dr. NAOUM Hanae	Examiner

Academic Year : 2024-2025

Abstract

Road safety is crucial as it directly impacts citizens' quality of life. To achieve safer and more efficient transport networks, Intelligent Transportation Systems (ITS) leverage vehicle-to-everything (V2X) communications, enabling seamless interaction between vehicles and infrastructure for improved traffic flow and safety.

However, the high mobility and dynamic topology of vehicular networks make them vulnerable to cyber attacks. Conventional intrusion detection systems (IDS) struggle to detect novel or sophisticated threats in real time. Attacks such as Denial-of-Service (DoS), replay, and Sybil attacks can disrupt communication and compromise road safety, underscoring the need for advanced detection methods suited to such environments.

This research introduces a hierarchical IDS for VANETs, combining a lightweight CatBoost classifier at Roadside Units (RSUs) for fast anomaly detection with a centralized deep learning model—integrating Bi-LSTM, CNN, and attention mechanisms—for precise multi-class attack classification. The system was trained on an extended VeReMi dataset and fine-tuned with data generated using NS-3 and SUMO.

Evaluated in a real-time VANET simulation, the proposed two-tier IDS achieved high detection accuracy with low latency. Compared to state-of-the-art methods, it outperforms standalone machine and deep learning IDS, demonstrating the effectiveness of combining multiple techniques to strengthen cybersecurity in ITS and mitigate diverse cyber threats.

Keywords——— Intelligent Transportation Systems, VANETs, Cybersecurity, Intrusion Detection System, Artificial Intelligence, Machine Learning, Deep Learning.

Résumé

La sécurité routière est cruciale car elle impacte directement la qualité de vie des citoyens. Pour rendre les réseaux de transport plus sûrs et plus efficaces, les Systèmes de Transport Intelligents (ITS) s'appuient sur les communications véhicule-à-tout (V2X), permettant une interaction fluide entre les véhicules et les infrastructures afin d'améliorer la circulation et la sécurité routière.

Cependant, la forte mobilité et la topologie dynamique des réseaux véhiculaires les rendent vulnérables aux cyberattaques. Les systèmes classiques de détection d'intrusion (IDS) peinent à identifier en temps réel des menaces nouvelles ou sophistiquées. Des attaques telles que le Déni de Service (DoS), la relecture et l'attaque Sybil peuvent perturber les communications et compromettre la sécurité routière, soulignant la nécessité de méthodes de détection avancées adaptées à ces environnements.

Cette recherche propose un IDS hiérarchique pour les VANETs, combinant un classifieur CatBoost léger déployé dans les unités routières (RSU) pour une détection rapide des anomalies, et un modèle centralisé de deep learning intégrant Bi-LSTM, CNN et des mécanismes d'attention pour une classification précise des attaques multi-classes. Le système a été entraîné sur une version étendue du jeu de données VeReMi et affiné avec des données générées via NS-3 et SUMO.

Évalué dans une simulation VANET en temps réel, l'IDS proposé à deux niveaux a atteint une grande précision de détection avec une faible latence. Comparé aux méthodes de pointe existantes, il surpasse les IDS basés uniquement sur l'apprentissage automatique ou profond, démontrant l'efficacité de la combinaison de plusieurs techniques pour renforcer la cybersécurité des ITS et contrer une large gamme de menaces.

Mots-clés ——— Systèmes de Transport Intelligents, VANETs, Cybersécurité, Système de Détection d'Intrusion, Intelligence Artificielle, Apprentissage Automatique, Apprentissage Profond.

الملخص

تُعد السلامة المرورية أمرًا بالغ الأهمية لما لها من تأثير مباشر على جودة حياة المواطنين. ومن أجل تحقيق شبكات نقل أكثر أمانًا وكفاءة، تستفيد أنظمة النقل الذكية (ITS) من تقنيات الاتصال بين المركبات وكل شيء ،(V2X) مما يتيح تفاعلاً سلسًا بين المركبات والبنية التحتية بهدف تحسين انسيابية حركة المرور وتعزيز السلامة.

إلا أن الارتفاع الكبير في سرعة المركبات والطبيعة الديناميكية لطوبولوجيا الشبكات في بيئات VANETs يجعلانها عرضة لهجمات إلكترونية متعددة. وتواجه أنظمة كشف التسلل التقليدية (IDS) صعوبة في اكتشاف الهجمات الجديدة أو المتقدمة في الزمن الحقيقي. إذ يمكن لهجمات مثل الحرمان من الخدمة ،(DoS) وإعادة الإرسال ،(Replay) وهجمات سيبيل (Sybil) أن تعرقل الاتصال وتُعرّض السلامة المرورية للخطر، مما يبرز الحاجة إلى آليات كشف أكثر تطورًا تتناسب مع هذه البيئات.

يُقدِّم هذا البحث نظام كشف تسلل هرمي مخصص لشبكات ،VANET يجمع بين مصنف خفيف الوزن يعتمد على خوارزمية CatBoost عند وحدات الطرق الجانبية (RSUs) للكشف السريع عن الشذوذ، ونموذج تعلم عميق مركزي يدمج بين الشبكات العصبونية ثنائية الاتجاه طويلة الذاكرة ،(Bi-LSTM) والشبكات الالتفافية ،(CNN) وآليات الانتباه (Attention) لتحقيق تصنيف دقيق متعدد الفئات للهجمات. وقد جرى تدريب النظام باستخدام نسخة موسعة من مجموعة بيانات ،VeReMi مع تحسينها ببيانات مولدة عبر المحاكيات NS-3 وSUMO.

أُجري تقييم النظام المقترح ضمن محاكاة آنية لشبكات ،VANET وأظهرت النتائج أنه يحقق دقة كشف عالية بزمن استجابة منخفض. وبالمقارنة مع أحدث الأساليب في المجال، فقد تفوق النظام على أنظمة كشف التسلل المعتمدة فقط على التعلم الآلي أو العميق، مما يثبت فعالية الجمع بين تقنيات متعددة لتعزيز أمن أنظمة النقل الذكية (ITS) والحد من التهديدات السيبرانية المتنوعة.

الكلمات المفتاحية——— أنظمة النقل الذكية، ،VANETs الأمن السيبراني، نظام كشف التسلل، الذكاء الاصطناعي، التعلم الآلي، التعلم العميق.