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 **Master**
Field: **Computer Science**
Specialty: **Artificial Intelligence and Data Science (IASD)**

Theme

Artificial Intelligence-based intrusion detection methods for smart vehicular network (VANETs): A Comparative Study

---

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

The rapid growth of vehicular networks has introduced new opportunities for safer and more efficient transportation systems. Smart Vehicular Networks (VANETs) play a central role in Intelligent Transportation Systems (ITS), enabling real-time communication between vehicles and infrastructure to enhance road safety, reduce congestion, and improve overall traffic management. However, the open and dynamic nature of VANETs makes them highly vulnerable to a wide range of cyber threats, such as Denial of Service (DoS/DDoS), spoofing, Sybil attacks, and message tampering. These threats can compromise communication reliability, disrupt traffic flow, or even lead to severe accidents.

To address these challenges, Intrusion Detection Systems (IDS) have become essential components of VANET security. While traditional IDS approaches rely on predefined attack signatures or static rules, they often fail to detect novel or evolving attack patterns in complex vehicular environments. Artificial Intelligence (AI), particularly Machine Learning (ML) and Deep Learning (DL), offers adaptive and data-driven solutions capable of learning hidden patterns from network traffic and identifying anomalies in real time. These techniques enhance detection accuracy, scalability, and resilience against diverse and sophisticated cyberattacks.

This thesis provides a comprehensive study of VANETs and their security challenges, with a particular focus on intrusion detection and cyber threat mitigation. It reviews the architecture and applications of VANETs, analyzes common attack vectors, and examines existing IDS techniques. Furthermore, it surveys state-of-the-art AI-driven approaches for intrusion detection in VANETs, highlighting their strengths and limitations. The work concludes with a comparative analysis of offline and real-time detection methods.

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

Résumé

La croissance rapide des réseaux véhiculaires a introduit de nouvelles opportunités pour des systèmes de transport plus sûrs et plus efficaces. Les réseaux véhiculaires intelligents (VANETs) jouent un rôle central dans les systèmes de transport intelligents (ITS), en permettant une communication en temps réel entre les véhicules et les infrastructures afin d'améliorer la sécurité routière, de réduire la congestion et d'optimiser la gestion globale du trafic. Cependant, la nature ouverte et dynamique des VANETs les rend particulièrement vulnérables à un large éventail de menaces informatiques, telles que les attaques par déni de service (DoS/DDoS), l'usurpation d'identité, les attaques de type Sybil et la falsification de messages. Ces menaces peuvent compromettre la fiabilité des communications, perturber la circulation ou même provoquer de graves accidents.

Pour relever ces défis, les systèmes de détection d'intrusion (IDS) sont devenus des composants essentiels de la sécurité des VANETs. Alors que les approches traditionnelles d'IDS reposent sur des signatures d'attaque prédéfinies ou des règles statiques, elles échouent souvent à détecter des modèles d'attaques nouveaux ou évolutifs dans des environnements véhiculaires complexes. L'intelligence artificielle (IA), en particulier l'apprentissage automatique (ML) et l'apprentissage profond (DL), propose des solutions adaptatives et basées sur les données, capables d'apprendre des schémas cachés à partir du trafic réseau et d'identifier les anomalies en temps réel. Ces techniques renforcent la précision de la détection, l'évolutivité et la résilience face à des cyberattaques diverses et sophistiquées.

Ce mémoire propose une étude approfondie des VANETs et de leurs défis en matière de sécurité, avec un accent particulier sur la détection d'intrusion et l'atténuation des menaces informatiques. Il présente l'architecture et les applications des VANETs, analyse les vecteurs d'attaque les plus courants et examine les techniques d'IDS existantes. De plus, il passe en revue les approches récentes basées sur l'IA pour la détection d'intrusion dans les VANETs, en soulignant leurs forces et leurs limites. Le travail se conclut par une analyse comparative des méthodes de détection hors ligne et en temps réel.

Mots clés——— Systèmes de transport intelligents, VANETs, Cybersécurité, Système de détection d'intrusion, Intelligence artificielle, Apprentissage automatique, Apprentissage profond.

الملخص

إن النمو السريع للشبكات الخاصة بالمركبات قد أدّى إلى ظهور فرص جديدة من أجل أنظمة نقل أكثر أماناً وكفاءة. تلعب الشبكات الذكية للمركبات (VANETs) دوراً محورياً في أنظمة النقل الذكية ،(ITS) حيث تُمكّن من التواصل في الوقت الحقيقي بين المركبات والبنية التحتية بهدف تعزيز السلامة المرورية، تقليل الازدحام، وتحسين إدارة حركة المرور بشكل عام. ومع ذلك، فإن الطبيعة المفتوحة والديناميكية لهذه الشبكات تجعلها شديدة التعرض لمجموعة واسعة من التهديدات السيبرانية، مثل هجمات حجب الخدمة ،(DoS/DDoS) انتحال الهوية، هجمات ،Sybil وتزوير الرسائل. هذه التهديدات قد تُضعف موثوقية الاتصالات، تُعطل حركة المرور، أو حتى تتسبب في حوادث خطيرة.

لمواجهة هذه التحديات، أصبحت أنظمة كشف التسلل (IDS) عنصراً أساسياً في أمن شبكات .VANET وعلى الرغم من أن الأنظمة التقليدية تعتمد على أنماط هجوم معرفة مسبقاً أو قواعد ثابتة، إلا أنها غالباً ما تفشل في اكتشاف أنماط هجمات جديدة أو متطورة في بيئات المركبات المعقدة. توفر تقنيات الذكاء الاصطناعي ،(AI) وخاصة التعلم الآلي (ML) والتعلم العميق ،(DL) حلولاً تكيفية قائمة على البيانات، قادرة على تعلم الأنماط الخفية من حركة المرور الشبكية واكتشاف الشذوذات في الوقت الحقيقي. هذه التقنيات تُعزز دقة الاكتشاف، وقابلية التوسع، والقدرة على الصمود أمام الهجمات السيبرانية المتنوعة والمعقدة.

يقدم هذا العمل دراسة شاملة لشبكات VANET وتحدياتها الأمنية، مع التركيز بشكل خاص على كشف التسلل والتخفيف من التهديدات السيبرانية. كما يستعرض هيكلية VANET وتطبيقاتها، ويحلل أكثر متجهات الهجوم شيوعاً، ويفحص تقنيات IDS الحالية. علاوة على ذلك، يستعرض أحدث المقاربات المعتمدة على الذكاء الاصطناعي للكشف عن التسلل في شبكات ،VANET مسلطاً الضوء على نقاط القوة والقصور فيها. ويُختتم العمل بتحليل مقارن بين طرق الكشف غير المتزامنة (offline) والكشف في الوقت الحقيقي.

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