الجمهورية الشعبية الديمقراطية الجزائرية
**République Algérienne Démocratique et Populaire**
وزارة التعليم العالي و البحث العلمي
**Ministère de l'Enseignement Supérieur et de la Recherche Scientifique**
**المدرسة العليا للإعلام الآلي 08٠ ماي 5491٠ بسيدي بلعباس**
**École Supérieure en Informatique**
**-08 Mai 1945- Sidi Bel Abbès**


# MEMOIRE

En Vue de l'obtention du dimplôme d' **Ingénieur d'État**
Filière: **Informatique**
Spécialité: **Intelligence Artificielle et Science de Données (IASD)**

## Thème

---

# Deep Multimodal Learning for Real-Time DDoS Attacks Detection in Internet of Vehicles

---

Présenté par:
**Mohamed ABABSA**

Soutenu le: **15, Sept, 2024**
Devant le jury composé de:

| | |
|---|---|
| **Mr. Fayssal BENDAOUAD** | President |
| **Mr. Miloud KHALDI** | Examinateur |
| **Mr. Abdelhamid MALKI** | Encadrant |
| **Mr. Soheyb RIBOUH** | Co-encadrant |

*Année Universitaire : 2023/2024*

# Abstract

The number of road traffic accidents has increased significantly and it is therefore urgent to improve road safety and control. Road safety is a priority for societies because it affects the quality of life of citizens. As a result, the progress and integration of intelligent transportation systems (ITS) has therefore been central to creating safer and more efficient transport networks.

The Internet of Vehicles (IoV) has the potential to improve road safety and provide comforts to travellers. However, this technology is vulnerable to a variety of security vulnerabilities that malicious actors could exploit. One of the most serious threats to IoV is a Distributed Denial of Service (DDoS) attack that could disrupt traffic flow, stop communications between vehicles, or cause accidents.

In order to protect communications, the implementation of the Misbehavior Detection System (MDS) is essential. Traditional MDSs systems rely on database attack patterns, but struggles with new attack patterns. For this reason, adaptive technology is needed. Deep Learning (DL) techniques offers solutions for detecting misbehaved activities in real-time within complex and dynamic network environments. These methods can analyze large network data to identify DDoS attacks and other malicious activity patterns.

Thus, our research proposes a security method bydeveloping a new Deep Multimodal Learning (DML) approach as the basis for an MDS to detect and mitigate DDoS attacks in IoV. The proposed approach has been evaluated in real-time, showing very encouraging results and outperforming state-of-the-art methods, demonstrating significant efficacy and reliability in protecting vehicular networks from cyber-attacks.

***Keywords***— Intelligent Transport Systems, Internet of Vehicles, DDoS Attacks, MisBehavior Detection System, Deep Learning

# الملخص

ازداد عدد حوادث المرور بشكل كبير، وبالتالي أصبح من الملح تحسين السلامة المرورية والسيطرة عليها. تعتبر السلامة المرورية أولوية للمجتمعات لأنها تؤثر على جودة حياة المواطنين. وبالتالي، فإن تقدم واندماج أنظمة النقل الذكية (STI) كان مركزيًا لإنشاء شبكات نقل أكثر أمانًا وكفاءة.

يمتلك إنترنت المركبات (VoI)القدرة على تحسين السلامة المرورية وتوفير الراحة للمسافرين. ومع ذلك، فإن هذه التكنولوجيا عرضة لمجموعة متنوعة من الثغرات الأمنية التي يمكن أن يستغلها الفاعلون الضارون. واحدة من أخطر التهديدات لـ VoIهي هجوم الحرمان من الخدمة الموزع (SoDD)الذي يمكن أن يعطل تدفق المرور، ويوقف الاتصالات بين المركبات، أو يسبب حوادث.

لحماية الاتصالات، فإن تنفيذ نظام كشف السلوك غير الصحيح (SDM)ضروري. تعتمد أنظمة SDMالتقليدية على أنماط الهجوم الموجودة في قواعد البيانات، لكنها تواجه صعوبة مع الأنماط الجديدة للهجوم. لهذا السبب، هناك حاجة إلى تكنولوجيا تكيفية. تقدم تقنيات التعلم العميق (LD)حلولًا للكشف عن الأنشطة غير السليمة في الوقت الحقيقي في بيئات الشبكات المعقدة والديناميكية. يمكن لهذه الأساليب تحليل بيانات الشبكة الكبيرة لتحديد هجمات SoDD وأنماط الأنشطة الضارة الأخرى.

لذلك، تقترح أبحاثنا طريقة أمان من خلال تطوير نهج جديد للتعلم العميق المتعدد الوسائط (LMD) كأساس لنظام كشف وتخفيف (SDM) للهجمات من نوع SoDD في إنترنت المركبات (VoI). تم تقييم النهج المقترح في الوقت الفعلي، حيث أظهرت النتائج تشجيعًا كبيرًا وتفوقًا على الأساليب الحديثة، مما يثبت فعالية كبيرة وموثوقية في حماية الشبكات المتعلقة بالمركبات من الهجمات الإلكترونية.

**الكلمات المفتاحية:** أنظمة النقل الذكية، إنترنت المركبات، هجمات SoDD، نظام كشف السلوك السيئ، التعلم العميق

# Résumé

Le nombre d'accidents de la route a considérablement augmenté et il est donc urgent d'améliorer la sécurité et le contrôle routiers. La sécurité routière est une priorité pour les sociétés car elle affecte la qualité de vie des citoyens. En conséquence, les progrès et l'intégration des systèmes de transport intelligents (ITS) ont été essentiels pour créer des réseaux de transport plus sûrs et plus efficaces.

L'Internet des Véhicules (IoV) a le potentiel d'améliorer la sécurité routière et d'offrir des commodités aux voyageurs. Cependant, cette technologie est vulnérable à diverses failles de sécurité que des acteurs malveillants pourraient exploiter. L'une des menaces les plus graves pour l'IoV est une attaque par déni de service distribué (DDoS) qui pourrait perturber le flux de trafic, interrompre les communications entre les véhicules ou provoquer des accidents.

Afin de protéger les communications, la mise en œuvre d'un Système de Détection de Comportements Malveillants (MDS) est essentielle. Les MDS traditionnels reposent sur des modèles d'attaques de base de données, mais ont du mal à détecter de nouveaux modèles d'attaques. Pour cette raison, une technologie adaptative est nécessaire. Les techniques d'apprentissage profond (DL) offrent des solutions pour détecter les activités malveillantes en temps réel dans des environnements de réseau complexes et dynamiques. Ces méthodes peuvent analyser de grandes quantités de données réseau pour identifier les attaques DDoS et d'autres modèles d'activités malveillantes.

Ainsi, notre recherche propose une méthode de sécurité en développant une nouvelle approche d'apprentissage profond multimodal (DML) comme base pour un système de détection et de mitigation (MDS) des attaques DDoS dans l'IoV. L'approche proposée a été évaluée en temps réel, montrant des résultats très encourageants et surpassant les méthodes de pointe, démontrant une efficacité et une fiabilité significatives dans la protection des réseaux de véhicules contre les cyberattaques.

***Mots clés***— Systèmes de Transport Intelligents, Internet des Véhicules, Attaques DDoS, Système de Détection de Comportements Anormaux, Apprentissage Profond