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 de **Master**
Filière: **Informatique**
Spécialité: **Intelligence Artificielle et Science de Données (IASD)**

Thème

Internet of Vehicles DDoS Attacks Detection Based on Artificial Intelligence

---

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 comprehensive study of IoV applications and their network security issues, particularly focusing on DDoS attacks and their dangerous impacts. It details state-of-the-art AI-based approaches for detecting misbehavior in IoV, addressing a critical aspect of cybersecurity in ITS.

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 دراسة شاملة لتطبيقات VoI ومشاكل الأمان الشبكي الخاصة بها، مع التركيز بشكل خاص على هجمات SoDD وتأثيراتها الخطيرة. وتفصل النهج الحديثة المعتمدة على الذكاء الاصطناعي لاكتشاف السلوكيات الضارة في VoI، مما يعالج جانبًا حاسمًا من الأمن السيبراني في أنظمة النقل الذكية.

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 étude complète des applications IoV et de leurs problèmes de sécurité réseau, en se concentrant particulièrement sur les attaques DDoS et leurs impacts dangereux. Elle détaille les approches basées sur l'IA de pointe pour détecter les comportements malveillants dans l'IoV, abordant un aspect critique de la cybersécurité dans les ITS.

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