الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
المدرسة العليا للإعلام الآلي ماي 0805491. بسيدي بلعباس

École Supérieure en Informatique
-08 Mai 1945- Sidi Bel Abbès

THESIS

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

Theme

Deep Reinforcement Learning for Anomaly Detection in Cybersecurity

---

Presented by:
Ayat BOUAZZA

Submission Date: **Sept, 2025**
In front of the jury composed of:

Dr.BENDAOUD Fayssal	President
Dr.BENABDERRAHMANE Sid Ahmed	Supervisor
Pr.BENSLIMANE Sidi Mohamed	CO-Supervisor
Dr.BENDELLA Mohammed Salih	Examiner

Academic Year : 2024/2025

Abstract

Anomaly detection plays a vital role in cybersecurity, where identifying rare and stealthy threats is essential for protecting critical systems. Traditional detection approaches often struggle with label scarcity, evolving behaviors, and high-dimensional data. This thesis investigates the use of Deep Reinforcement Learning (DRL), with a focus on the Deep Q-Network (DQN), to address these challenges. A custom anomaly detection environment was designed by integrating latent representations and reconstruction errors from an autoencoder, enabling the DQN agent to sequentially identify anomalous samples. The reward function was tailored to promote accurate and early detection, even under sparse supervision. Experiments conducted across diverse datasets, including both static and streaming scenarios, demonstrate that the proposed framework can adaptively learn effective detection policies and achieve competitive results in ranking anomalies. These findings highlight the potential of DRL, and specifically DQN, as a promising direction for advancing anomaly detection in dynamic cybersecurity environments.

Keywords: Deep Reinforcement Learning, Anomaly Detection, Cybersecurity, Autoencoder, Streaming Data

---

Résumé

La détection d'anomalies joue un rôle essentiel en cybersécurité, où l'identification des menaces rares et furtives est cruciale pour protéger les systèmes critiques. Les approches traditionnelles rencontrent souvent des limites liées au manque d'étiquettes, à l'évolution des comportements et à la complexité des données. Ce mémoire explore l'utilisation de l'Apprentissage par Renforcement Profond (DRL), en mettant l'accent sur le Deep Q-Network (DQN), pour relever ces défis. Un environnement de détection d'anomalies a été conçu en intégrant des représentations latentes et des erreurs de reconstruction issues d'un autoencodeur, permettant à l'agent DQN d'identifier séquentiellement les échantillons anormaux. La fonction de récompense a été adaptée afin de favoriser une détection précise et précoce, même en présence d'une supervision limitée. Les expériences menées sur divers jeux de données, incluant des scénarios statiques et en flux, montrent que le cadre proposé peut apprendre de manière adaptative des politiques de détection efficaces et obtenir des résultats compétitifs dans le classement des anomalies.

Mots-clés : Apprentissage par Renforcement Profond, Détection d'anomalies, Cybersécurité, Autoencodeur, Données en flux

---

ملخص

يلعب اكتشاف الحالات الشاذة دورًا حيويًا في الأمن السيبراني، حيث يعد تحديد التهديدات النادرة والخفية أمرًا أساسيًا لحماية الأنظمة الحيوية. غالبًا ما تواجه الأساليب التقليدية للكشف صعوبة في ندرة التسميات، والسلوكيات المتطورة، والبيانات عالية الأبعاد. تبحث هذه الأطروحة في استخدام التعلم العميق المعزز ، مع التركيز على شبكة Q العميقة ، لمعالجة هذه التحديات. تم تصميم بيئة مخصصة لاكتشاف الشذوذ من خلال دمج التمثيلات الكامنة وأخطاء إعادة البناء من جهاز التشفير التلقائي، مما يمكّن وكيل من تحديد العينات الشاذة بشكل متسلسل. تم تصميم دالة المكافأة لتعزيز الكشف الدقيق والمبكر، حتى في ظل الإشراف النادر. التجارب التي أجريت على مجموعات بيانات متنوعة، بما في ذلك السيناريوهات الثابتة والبث المباشر، تُظهر أن الإطار المقترح يمكنه تعلم سياسات كشف فعالة بشكل تكيفي وتحقيق نتائج تنافسية في تصنيف الحالات الشاذة. تُبرز هذه النتائج إمكانيات التعلم المعزز العميق، وبشكل خاص شبكة ، كاتجاه واعد لتطوير كشف الحالات الشاذة في بيئات الأمن السيبراني الديناميكية.

الكلمات المفتاحية: التعلم العميق بالتعزيز، كشف الحالات الشاذة، الأمن السيبراني، المشفر التلقائي، البيانات المتدفقة
