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 80٠5491. بسيدي بلعباس

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

THESIS

To obtain the diploma of **Masters**
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 is a cornerstone of cybersecurity, particularly in the identification of Advanced Persistent Threats (APTs), which are stealthy, long-lasting, and highly adaptive attacks. Traditional signature-based methods often fall short in capturing novel or evolving attack patterns, leading to the rise of diverse anomaly detection approaches. This thesis provides a comprehensive review of the state of the art in anomaly detection techniques for APTs, encompassing statistical models, machine learning, deep learning, graph-based methods, and reinforcement learning. Each approach is analyzed with respect to its underlying principles, strengths, limitations, and applicability to real-world scenarios. Special attention is given to key challenges such as data imbalance, feature complexity, adversarial behavior, and detection latency. The study also highlights evaluation metrics and datasets commonly used in the literature, offering insights into their impact on benchmarking results. By synthesizing current advances, this work aims to guide future research directions and support the design of more resilient and adaptive APT detection systems.

Keywords: Anomaly Detection, Cybersecurity, Advanced Persistent Threats, Machine Learning, Deep Learning, Reinforcement Learning, Graph-based Methods

---

Résumé

La détection d'anomalies constitue un pilier fondamental de la cybersécurité, notamment face aux menaces persistantes avancées (APTs), qui sont furtives, durables et adaptatives. Les approches traditionnelles basées sur les signatures montrent leurs limites face aux attaques nouvelles ou en évolution, ce qui a conduit au développement de multiples techniques de détection d'anomalies. Ce mémoire propose une analyse approfondie de l'état de l'art des méthodes de détection appliquées aux APTs, couvrant les modèles statistiques, l'apprentissage automatique, l'apprentissage profond, les approches basées sur les graphes et l'apprentissage par renforcement. Chaque catégorie est étudiée en termes de principes, d'avantages, de limites et de pertinence pour les environnements réels. Une attention particulière est portée aux défis majeurs tels que le déséquilibre des données, la complexité des caractéristiques, les comportements adversariaux et la latence de détection. L'étude met également en évidence les jeux de données et les métriques d'évaluation utilisés dans la littérature, afin de mieux comprendre leur influence sur la comparaison des résultats. En synthétisant ces avancées, ce travail vise à orienter les recherches futures et à contribuer à la conception de systèmes de détection des APTs plus résilients et adaptatifs.

Mots-clés : Détection d'anomalies, Cybersécurité, Menaces persistantes avancées, Apprentissage automatique, Apprentissage profond, Apprentissage par renforcement, Méthodes basées sur les graphes

---

ملخص

تُعدّ كشف الحالات الشاذة ركيزة أساسية في مجال الأمن السيبراني، خصوصًا في مواجهة الهجمات المتقدمة المستمرة (sTPA) التي تتميز بالخفاء والاستمرارية والقدرة العالية على التكيّف. غالبًا ما تفشل الطرق التقليدية المعتمدة على التواقيع في اكتشاف الأنماط الجديدة أو المتطورة للهجمات، مما أدى إلى ظهور العديد من تقنيات كشف الشذوذ. يقدّم هذا العمل مراجعة شاملة لأحدث الأساليب في كشف الشذوذ المطبّقة على الـ sTPA، بما في ذلك النماذج الإحصائية، وتعلم الآلة، والتعلم العميق، والأساليب القائمة على الرسوم البيانية، والتعلم المعزز. تم تحليل كل فئة من حيث المبادئ الأساسية، ونقاط القوة، والقيود، ومدى ملاءمتها للتطبيقات الواقعية. كما يسلط البحث الضوء على التحديات الرئيسة مثل عدم توازن البيانات، وتعقيد السمات، والسلوكيات الخصامية، وزمن الاستجابة. إضافة إلى ذلك، يستعرض هذا العمل مجموعات البيانات ومقاييس التقييم الأكثر استخدامًا في الأدبيات، ويوضح أثرها على نتائج المقارنة. ومن خلال هذا الاستعراض، يسعى البحث إلى توجيه الدراسات المستقبلية والمساهمة في تطوير أنظمة كشف أكثر مرونة وقدرة على التكيف مع التهديدات السيبرانية الديناميكية.

الكلمات المفتاحية: كشف الشذوذ، الأمن السيبراني، الهجمات المتقدمة المستمرة، تعلم الآلة، التعلم العميق، التعلم المعزز، الأساليب القائمة على الرسوم البيانية
