الجمهورية الجزائرية الديمقراطية الشعبية
Republic of Algeria Democratic and Popular
وزارة التعليم العالي والبحث العلمي
Ministry of Higher Education and Scientific Research
المدرسة العليا للإعلام الآلي - 8 ماي 1945 - سيدي بلعباس
Higher School of Computer Science - 08 May 1945 - Sidi Bel Abbès

Thesis

To obtain the diploma of **Master**

Field: **Computer Science**

Specialization: **Artificial Intelligence and Data Science (AIDS)**

Theme

Hybrid Graph Neural Network for Anomaly Detection in Complex Systems: Case of Advanced Persistent Threats Attacks

---

Presented by: **LEBGA HANANE**

Submitted on: 08/10/2025

In front of the jury composed of:

President:	Dr.Nassima Dif
Supervisor:	Dr. Sidahmed Benabderrahmane
Co-supervisor:	Pr. Sidi Mohamed Benslimane
Examiner:	Dr.Khaldi Miloud

الملخص

تمثل التهديدات المستمرة المتقدمة (APTs) تحديًا محوريًا للأمن السيبراني الحديث، حيث تُدار على شكل حملات هجومية متطورة ومتعددة المراحل يقف خلفها خصوم ذوو مهارات عالية، مستغلين التعقيد الكامن في لبنى التحتية السيبرانية الفيزيائية المعاصرة. تُمكّن هذه التهديدات من تسريب كميات هائلة من البيانات أو اختراق النظام بشكل مستدام، مما يجعلها من أخطر أنماط الهجمات الإلكترونية المعاصرة.

تقدم هذه الأطروحة مراجعة شاملة وحديثة لمنهجيات الكشف عن التهديدات المستمرة المتقدمة (APT) من منظور نظرية الأنظمة المعقدة، مؤسسةً لإطار نظري موحد يفسر طبيعة هذه التهديدات والتحديات الأساسية في كشفها. يستعرض العمل التطور المنهجي بدءًا من الأساليب التقليدية القائمة على التوقيع والقواعد، مرورًا بخوارزميات التعلم الآلي الكلاسيكي، ووصولاً إلى بنى الشبكات العصبية الرسومية (GNN) المعاصرة. كما يتضمن التقييم النقدي تحليلاً لأكثر من ٣٥ إطارًا للكشف عبر ثلاثة أجيال منهجية، مع التركيز على قدراتها في استيعاب التعقيد الهيكلي، والديناميكيات الزمنية، والسلوكيات الناشئة التي تميز حملات APT .

يسهم هذا العمل في صياغة تصنيف منهجي دقيق وإرساء مقاييس أداء شاملة، إلى جانب تحديد فجوات بحثية ملحة تشكل عوائق أمام النشر التشغيلي الفعال. وعليه، يُوفّر البحث أساسًا معرفيًا بالغ الأهمية لفهم القدرات الحالية، كما يرسم خريطة طريق لتطوير أنظمة كشف من الجيل التالي قادرة على مواجهة خصوم سيبرانيين متزايدي التطور.

الكلمات المفتاحية: التهديدات المستمرة المتقدمة، الأنظمة المعقدة، الشبكات العصبية الرسومية، اكتشاف الشذوذ، الأمن السيبراني، التعلم الآلي، التعلم العميق.

Abstract

Advanced Persistent Threats (APTs) represent a critical challenge to modern cybersecurity, characterized by sophisticated, multi-stage attack campaigns orchestrated by highly skilled adversaries who exploit the inherent complexity of contemporary cyber-physical infrastructures. These threats enable massive data exfiltration and sustained system compromise. This thesis presents a comprehensive state-of-the-art review of APT detection methodologies through the conceptual lens of complex systems theory, establishing a unified theoretical framework that explains both the nature of APTs and the fundamental challenges in detecting them.

We systematically analyze the paradigmatic evolution from traditional signature-based and rule-based approaches through classical machine learning to contemporary graph neural network (GNN) architectures. Our critical evaluation examines 35+ detection frameworks across three methodological generations, assessing their capabilities to capture the structural complexity, temporal dynamics, and emergent behaviors characteristic of APT campaigns.

This work contributes a rigorous methodological taxonomy, comprehensive performance benchmarking, and systematic identification of research gaps that constitute barriers to effective operational deployment. This research provides both a critical foundation for understanding current capabilities and a roadmap for developing next-generation APT detection systems capable of countering increasingly sophisticated cyber adversaries.

Key words : Advanced Persistent Threats, Complex Systems, Graph Neural Networks, Anomaly Detection, Cybersecurity, Machine learning, Deep Learning.

Résumé

Les menaces persistantes avancées (APT) représentent un défi majeur pour la cybersécurité moderne. Elles se caractérisent par des campagnes d'attaques sophistiquées en plusieurs étapes, orchestrées par des adversaires hautement qualifiés qui exploitent la complexité inhérente des infrastructures cyberphysiques contemporaines. Ces menaces permettent l'exfiltration massive de données et la compromission durable des systèmes. Cette thèse présente un état des lieux complet des méthodologies de détection des APT à travers le prisme conceptuel de la théorie des systèmes complexes, établissant un cadre théorique unifié expliquant à la fois la nature des APT et les défis fondamentaux de leur détection

La recherche transforme les données tabulaires de cybersécurité en Nous analysons systématiquement l'évolution paradigmatique des approches traditionnelles basées sur les signatures et les règles, en passant par l'apprentissage automatique classique, jusqu'aux architectures contemporaines de réseaux de neurones graphes (GNN). Notre évaluation critique examine plus de 35 cadres de détection répartis sur trois générations méthodologiques, évaluant leur capacité à saisir la complexité structurelle, la dynamique temporelle et les comportements émergents caractéristiques des campagnes APT.

Ce travail contribue à une taxonomie méthodologique rigoureuse, à une analyse comparative complète des performances et à une identification systématique des lacunes de la recherche qui constituent des obstacles à un déploiement opérationnel efficace. Cette recherche fournit à la fois une base essentielle pour comprendre les capacités actuelles et une feuille de route pour le développement de systèmes de détection APT de nouvelle génération capables de contrer des cyber-adversaires de plus en plus sophistiqués.

Mots-clés : Menaces persistantes avancées, systèmes complexes, réseaux neuronaux graphiques, détection d'anomalies, cybersécurité, apprentissage automatique, apprentissage profond.