

الجمهورية الشعبية الديمقراطية الجزائرية
People's Democratic Republic of Algeria
وزارة التعليم العالي والبحث العلمي
Ministry of Higher Education and Scientific Research
المدرسة العليا للإعلام الآلي 08 ماي 1945. بسيدي بلعباس
Higher School of Computer Science
8 Mai 1945 - Sidi Bel Abbès



THESIS

To obtain the diploma of **Engineering Degree**
Field: **Computer Science**
Specialty: **Ingénierie des Systèmes Informatiques (ISI)**
Theme

Federated Graph Neural Network for DDoS Detection in IoT Network

Presented by:
Fellahi Achref Ghanem

Submission Date: **June, 2026**
Defended before the jury composed of:

Dr. Belalia Amina

Dr. Bensenane Hamdane

Dr. Brahmia Mohamed El Amine

Dr. Ghalmane Zakariya

Dr. Anani Djihed

President

Supervisor

Co-Supervisor

Co-Supervisor

Examiner

Academic Year : 2025/2026

Abstract

The rapid expansion of Internet of Things (IoT) networks across critical infrastructure domains has created vast, heterogeneous, and distributed ecosystems that are increasingly vulnerable to sophisticated cyberattacks, particularly Distributed Denial of Service (DDoS) campaigns that exploit the scale and connectivity of IoT deployments to overwhelm network resources and disrupt essential services. Traditional Intrusion Detection Systems (IDS), whether centralized or signature-based, are structurally inadequate for IoT environments: they cannot scale to billions of distributed devices, fail to capture the graph-structural signatures of coordinated attacks, and require the centralization of sensitive traffic data that privacy regulations and operational constraints prohibit.

This master’s thesis presents a structured bibliographic review of the evolution of intrusion detection systems for IoT networks, systematically surveying and critically analyzing the state of the art from classical signature-based and anomaly-based approaches, through machine learning and deep learning techniques, to the most recent graph neural network and federated learning frameworks. The review is organized along a clear architectural progression: from centralized graph-based IDS methods that leverage topological features such as centrality measures to enrich detection models, to privacy-preserving federated architectures that distribute model training across heterogeneous IoT clients without sharing raw traffic data.

In addition to the bibliographic contribution, this thesis includes a reproduction and adaptation of a federated graph neural network framework for DDoS detection in IoT networks, serving as a practical validation of the concepts identified through the literature review. This work establishes a comprehensive analytical foundation for understanding the current landscape and open challenges of IDS in IoT, and identifies promising research directions at the intersection of graph-structural learning, federated privacy preservation, and real-time deployment in resource-constrained environments.

Keywords: Internet of Things (IoT), Intrusion Detection Systems (IDS), Distributed Denial of Service (DDoS), Federated Learning, Graph Neural Networks (GNN), Graph
--

Attention Networks (GAT), GraphSAGE, Centrality Measures, Complex Networks, Privacy-Preserving Security.

ملخص

أسفر التوسع السريع لشبكات إنترنت الأشياء عبر قطاعات البنية التحتية الحيوية عن نشوء أنظمة بيئية واسعة وغير متجانسة وموزعة، باتت أكثر عرضةً للهجمات الإلكترونية المتطورة، ولا سيما هجمات الحرمان من الخدمة الموزعة التي تستغل حجم منظومات إنترنت الأشياء وتربطها لإغراق موارد الشبكة وتعطيل الخدمات الأساسية. وتُعدّ أنظمة كشف التسلل التقليدية، سواء أكانت مركزية أم قائمة على التوقعات، غير ملائمة هيكلياً لبيئات إنترنت الأشياء؛ إذ لا تستطيع التوسع لاستيعاب مليارات الأجهزة الموزعة، وتعجز عن رصد البصمات البنوية للرسوم البيانية الخاصة بالهجمات المنسقة، فضلاً عن اشتراطها مركزة بيانات حركة المرور الحساسة التي تحظرها أنظمة حماية الخصوصية والقيود التشغيلية.

يقدم هذا المذكرة مراجعةً بليوغرافيةً منهجيةً لتطور أنظمة كشف التسلل في شبكات إنترنت الأشياء، من خلال مسح نقدي ومنظم لحالة الفن، بدءاً من الأساليب الكلاسيكية القائمة على التوقعات والشذوذ، مروراً بتقنيات التعلم الآلي والتعلم العميق، وصولاً إلى أحدث أطر الشبكات العصبية البيانية والتعلم الاتحادي. وتسير المراجعة وفق تسلسل معماري واضح، من أساليب كشف التسلل المركزية القائمة على الرسوم البيانية التي تستثمر الخصائص الطوبولوجية كمقاييس المركزية لإثراء نماذج الكشف، نحو بنيات اتحادية حافظة للخصوصية توزع تدريب النماذج بين عملاء إنترنت الأشياء غير المتجانسين دون مشاركة بيانات حركة المرور الخام.

إضافةً إلى الإسهام البليوغرافي، يتضمن هذا العمل إعادة إنتاج وتكييفاً لإطار شبكة عصبية بيانية اتحادية للكشف عن هجمات الحرمان من الخدمة الموزعة في شبكات إنترنت الأشياء، بوصفه تحقيقاً عملياً من المفاهيم المستخلصة عبر مراجعة الأدبيات. ويرسي هذا العمل أساساً تحليلياً شاملاً لفهم المشهد الراهن والتحديات المفتوحة لأنظمة كشف التسلل في إنترنت الأشياء، ويرسم آفاقاً بحثية واعدة عند تقاطع التعلم البنوي بالرسوم البيانية، والحفاظ على الخصوصية عبر الاتحاد، والنشر الفوري في البيئات محدودة الموارد.

الكلمات المفتاحية: إنترنت الأشياء، أنظمة كشف التسلل، الحرمان من الخدمة الموزعة، التعلم الاتحادي، الشبكات العصبية
البيانية، شبكات الانتباه البياني، EGAShparG، مقاييس المركزية، الشبكات المعقدة، الأمن الحافظ للخصوصية.

Résumé

L’expansion rapide des réseaux de l’Internet des Objets (IoT) dans les domaines des infrastructures critiques a engendré des écosystèmes vastes, hétérogènes et distribués, de plus en plus exposés à des cyberattaques sophistiquées, notamment les attaques par Dénis de Service Distribué (DDoS) qui exploitent l’échelle et la connectivité des déploiements IoT pour saturer les ressources réseau et perturber les services essentiels. Les Systèmes de Détection d’Intrusion (IDS) traditionnels, qu’ils soient centralisés ou basés sur des signatures, s’avèrent structurellement inadaptés aux environnements IoT : ils ne peuvent pas s’étendre à des milliards d’appareils distribués, échouent à capturer les signatures structurelles en graphe des attaques coordonnées, et imposent la centralisation de données de trafic sensibles que les réglementations sur la vie privée et les contraintes opérationnelles interdisent.

Ce mémoire de master présente une revue bibliographique structurée de l’évolution des systèmes de détection d’intrusion pour les réseaux IoT, en analysant de manière systématique et critique l’état de l’art, depuis les approches classiques basées sur les signatures et les anomalies, en passant par les techniques d’apprentissage automatique et d’apprentissage profond, jusqu’aux cadres les plus récents fondés sur les réseaux de neurones en graphe et l’apprentissage fédéré. La revue est organisée selon une progression architecturale claire : des méthodes IDS centralisées basées sur les graphes, qui exploitent des caractéristiques topologiques telles que les mesures de centralité pour enrichir les modèles de détection, vers des architectures fédérées préservant la confidentialité, qui distribuent l’entraînement des modèles entre des clients IoT hétérogènes sans partage des données de trafic brutes.

En complément de la contribution bibliographique, ce mémoire inclut une reproduction et une adaptation d’un cadre de réseau de neurones en graphe fédéré pour la détection des attaques DDoS dans les réseaux IoT, constituant une validation pratique des concepts identifiés lors de la revue de littérature. Ce travail établit une base analytique exhaustive pour comprendre le paysage actuel et les défis ouverts des IDS dans l’IoT, et identifie des pistes de recherche prometteuses à l’intersection de l’apprentissage structurel en graphe, de la préservation de la confidentialité par fédération, et du déploiement en temps réel dans des environnements à ressources limitées.

Mots-clés : Internet des Objets (IoT), Systèmes de Détection d’Intrusion (IDS), Déni de Service Distribué (DDoS), Apprentissage Fédéré, Réseaux de Neurones en Graphe (GNN), Réseaux d’Attention en Graphe (GAT), GraphSAGE, Mesures de Centralité, Réseaux Complexes, Sécurité Préservant la Vie Privée.