# Détection d'anomalies dans les flux de graphes et attaques d'empoisonnement

Fatma Zohra Khaoula Saadi*, Abd Errahmane Kiouche*,**
Karima Amrouche* Hamida Seba** Mohamed-Lamine Messai***

*Ecole nationale Supérieure d'Informatique (ESI) Oued Smar Alger Algérie
{gf_saadi, k_amrouche}@esi.dz,
https://www.esi.dz/
**Université de Lyon, Université Lyon 1, LIRIS UMR 5205 F-69622 France
{abd-errahmane.kiouche, hamida.seba}@univ-lyon1.fr
***Université de Lyon, Lyon 2, ERIC UR 3083, France
mohamed-lamine.messai@univ-lyon2.fr

**Résumé.** Le problème de détection d'anomalies dans les flux de graphes se pose dans de nombreuses applications comme la cyber-sécurité et la finance. Plusieurs méthodes sont proposées dans la littérature pour répondre à cette problématique. Cependant, la plupart de ces méthodes sont vulnérables aux attaques par empoisonnement qui consistent à compromettre le processus d'apprentissage en injectant des données corrompues lors de la phase d'initialisation ou d'entraînement afin d'altérer le modèle représentant le comportement normal du système. Dans ce travail, nous étendons une des méthodes, les plus récentes et les plus effectives, de détection d'anomalies pour résister à cette attaque. Nous procédons par hybridation en considérant une autre méthode de détection d'anomalies comme un filtre qui élimine les données empoisonnées.

## 1 Introduction

Les graphes dynamiques, ou en flux, représentent l'une des solutions les plus utilisées dans la modélisation des données produites par des systèmes qui évoluent dans le temps. Ce sont généralement des données volumineuses et inter-connectées que l'on retrouve dans plusieurs applications parmi lesquelles on peut citer : les réseaux sociaux, les systèmes informatiques, le Web et la biologie. Un graphe dynamique est un graphe dont la structure change avec le temps (i.e., à un instant $t$, on n'aura qu'une vision partielle sur le graphe). A chaque instant $t$, un évènement de suppression ou d'ajout d'un élément (nœud, arête, étiquette ou poids) du graphe pourrait avoir lieu.

Nous nous sommes intéressés, dans ce travail, à l'étude des détecteurs d'anomalies dans les flux de graphes. D'une manière générale, un détecteur d'anomalies identifie les éléments du système qui sont considérablement différents des autres éléments. L'existence de ces éléments peut être due à une activité anormale comme une cyber-attaque, comme elle peut représenter simplement un évènement intéressant pour le système étudié. Dans un flux de graphes, une