XÂY DỰNG HỆ THỐNG HỌC PHÂN TÁN TRÊN MẠNG ĐỒ THỊ CHO PHÁT HIỆN RỬA TIỀN

Trần Lê Minh Nhật
[1] Trường ĐH Công Nghệ Thông Tin

Hoàng Minh Thái
[1] Trường ĐH Công Nghệ Thông Tin

Summary

- **Vấn đề:** Rửa tiền ngày càng tinh vi, gây rủi ro tài chính lớn.
- **Giải pháp:** Kết hợp **Graph Neural Network (GNN)** và **Federated Learning (Học liên kết)**.
- **Thực nghiệm:** Trên 3 bộ dữ liệu (IBM AML, SAML-D, Elliptic2).
- **Mục tiêu:** Giảm tỷ lệ bỏ sót tội phạm(đo qua AUC, F1), đảm bảo tính riêng tư.

Purpose

Mục tiêu tổng quát:
Xây dựng hệ thống phát hiện rửa tiền hiệu quả dựa trên GNN, đồng thời giải quyết hai thách thức chính: Data silos (phân mảnh dữ liệu) và Neighborhood camouflage (ngụy trang láng giềng).

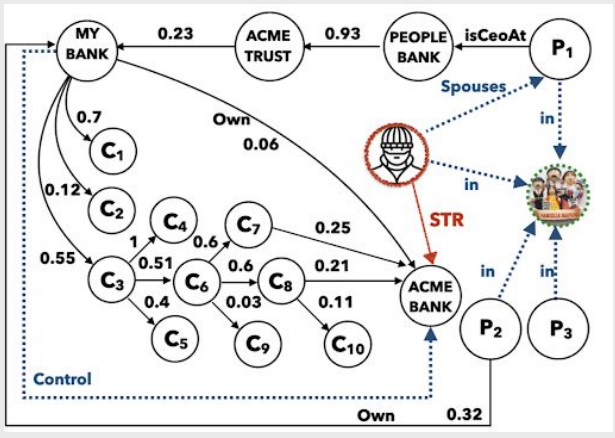
Mục tiêu cụ thể:
- (1) Thiết kế & huấn luyện các kiến trúc GNN (GCN/GAT/GIN) tích hợp federated learning trên bộ dữ liệu chuẩn
- (2) Triển khai chiến lược federated (FedProx) để xử lý non-IID giữa các ngân hàng
- (3) Đề xuất cơ chế Node Representation Residual để bảo toàn đặc trưng node và chống giả dạng

Overview

- **Dữ liệu**: Xây dựng đồ thị giao dịch từ logs tài chính, trong đó mỗi node biểu diễn một tài khoản và mỗi edge biểu diễn một giao dịch kèm theo các thuộc tính (số tiền, thời gian, loại giao dịch). Nghiên cứu sử dụng ba bộ dữ liệu chuẩn trong lĩnh vực AML gồm IBM AML, SAML-D và Elliptic2, phản ánh các kịch bản rửa tiền với mức độ phức tạp khác nhau. Dữ liệu được tiền xử lý bằng các kỹ thuật chuẩn hoá đặc trưng, xử lý mất cân bằng lớp (do giao dịch gian lận chiếm tỷ lệ rất nhỏ) nhằm cải thiện khả năng học của mô hình.
- **Mô hình**: Thử nghiệm và so sánh các kiến trúc Graph Neural Network tiêu biểu gồm GINe, GATe và RGCN, cho phép khai thác cả đặc trưng node và edge thông qua cơ chế message passing. Để giải quyết hiện tượng *Neighborhood Camouflage*, mô hình được tích hợp Node Representation Residual tại mỗi lớp GNN, giúp bảo toàn và tăng cường vai trò của đặc trưng gốc (ego-features) của node, hạn chế việc node gian lận bị "đồng hoá" bởi các láng giềng hợp pháp.
- **Federated setup**: Thiết lập môi trường Federated Learning mô phỏng từ 5–10 client đại diện cho các ngân hàng hoặc tổ chức tài chính khác nhau. Mỗi client huấn luyện mô hình cục bộ trên dữ liệu riêng và chỉ chia sẻ tham số mô hình (weights/gradients) thay vì dữ liệu thô, đảm bảo tính riêng tư. Thuật toán FedProx được sử dụng thay cho FedAvg nhằm xử lý hiệu quả dữ liệu non-IID giữa các client và cải thiện độ ổn định hội tụ.
- **Thử nghiệm & đánh giá**: Tiến hành so sánh toàn diện giữa Centralized Learning và Federated Learning, cũng như giữa GNN truyền thống và GNN tích hợp Residual thông qua các thí nghiệm ablation. Hiệu năng mô hình được đánh giá bằng các chỉ số tiêu chuẩn trong bài toán AML gồm Accuracy, F1-score và AUC-ROC, nhằm kiểm chứng hiệu quả của phương pháp đề xuất trong môi trường dữ liệu phân tán và nhiễu.

Description

Input/Output của đề tài:
- **Input (Đầu vào):** Dữ liệu lịch sử giao dịch của ngân hàng, tổ chức tiền tệ.
- **Output (Đầu ra):** Phân loại từng giao dịch hoặc tài khoản là: **Hợp pháp (Licit)** hoặc **Bất hợp pháp (Illicit/Money Laundering)**.



Rule-based antimoney laundering system (Rule-based Anti-Money Laundering in Financial Intelligence Units: Experience and Vision)

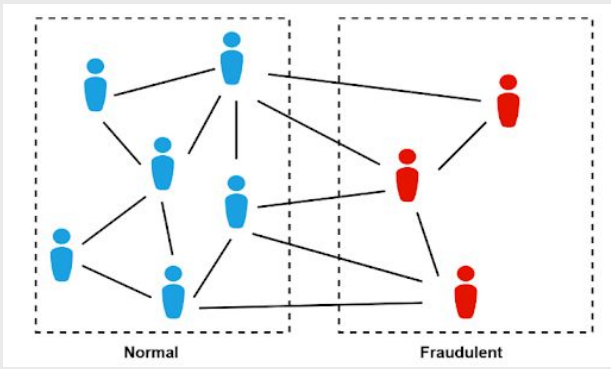
Nội dung 1: Tìm hiểu tổng quan đề tài
- Tìm hiểu tổng quan các phương pháp để giải quyết từng nhiệm vụ Anti money laundering và 2 vấn đề **Sự phân mảnh dữ liệu** và **Giả dạng**.

Nội dung 2: Nghiên cứu và Thu thập dữ liệu
- Sử dụng 3 bộ dataset nghiên cứu phổ biến: **IBM AML** (phức tạp, mô phỏng thực tế), **SAML-D**, và **Elliptic2**.
- Tiền xử lý dữ liệu: Xây dựng đồ thị từ logs giao dịch, chuẩn hóa đặc trưng (feature normalization), xử lý mất cân bằng dữ liệu (imbalance data).

Nội dung 3: Thiết kế và Cài đặt Mô hình GNN
- Thử nghiệm các kiến trúc: **GINe** (Graph Isomorphism Network with edge features), **GATe** (Graph Attention Network with edge features), **RGCN** (Relational GCN).

Nội dung 4: Kiến trúc Mô hình & Kỹ thuật cốt lõi (Core Techniques)
- **Federated Strategy:** Sử dụng thuật toán **FedProx** thay FedAvg truyền thống để xử lý vấn đề **Non-IID Dat**.

Nội dung 5: Quy trình Thực nghiệm
- Thiết lập môi trường giả lập Federated với 5-10 clients.
- So sánh hiệu năng (Ablation Study) giữa: GNN thường vs. GNN + Residual; Centralized vs. Federated.



The illustration of neighborhood camouflage (FLAG : Fraud Detection with LLM-enhanced Graph Neural Network)

Trần Lê Minh Nhật - Trường Đại học Công Nghệ Thông Tin
Email : 23521098@gm.uit.edu.vn