Enhancing Fraud Detection in Credit Card Transactions Using Graph Neural Networks

Abstract

This proposal outlines a research project focused on enhancing fraud detection in credit card transactions through Graph Neural Networks (GNNs). Utilizing the IBM credit card transaction dataset, which comprises 24 million transactions, including 30,000 labelled fraudulent cases, this project aims to leverage GNNs to identify complex patterns indicative of fraud. The objective is to modify existing models and establish a structured experimental plan to evaluate the effectiveness of GNNs compared to traditional Machine Learning methods.

Introduction

Fraudulent transactions pose a significant threat to financial institutions, leading to considerable financial losses. Traditional detection methods, such as logistic regression and decision trees, often struggle to identify complex relationships within transaction data. This project proposes the application of GNNs to model interactions among transactions, merchants, and credit cards, improving detection accuracy.

Literature Review

Research on fraud detection has primarily focused on traditional machine learning techniques, but recent studies highlight the potential of GNNs in this domain. Wu et al. (2020) demonstrated that GNNs outperform conventional methods by leveraging relational data. Additionally, Zhang et al. (2021) emphasized the effectiveness of graph-based approaches for anomaly detection. This project builds on these findings, applying GNNs specifically to credit card transactions.

Methods

Research Design and Modeling Methods:

1. **Data Preparation:**
    - Utilize the IBM credit card transaction dataset, containing 24 million transactions, to construct a graph representation where nodes represent transactions, merchants, and credit cards. Edges will indicate relationships between these entities, allowing for the modeling of interactions.

2. **Data Exploration and Visualization:**
   - Conduct exploratory data analysis (EDA) to understand the distribution of fraudulent and non-fraudulent transactions, examining factors such as transaction amounts and merchant types.
   - Visualize the graph structure to identify patterns and anomalies.
3. **Implementation and Programming:**
   - Develop GNN models using frameworks such as PyTorch Geometric or DGL (Deep Graph Library). The model will be designed to learn from the graph structure and predict fraudulent transactions.
   - Compare the GNN model's performance against traditional ML models, such as logistic regression and random forests, to establish a benchmark.
4. **Experimental Plan:**
   - Utilize cross-validation to evaluate model performance, focusing on metrics such as precision, recall, and F1-score to assess the fraudulent transactions.
   - Implement techniques to address class imbalance, such as oversampling the minority class or using cost-sensitive learning.

Results

The outcome is an improved fraud detection model that outperforms traditional methods in both accuracy and efficiency. The GNN's ability to capture complex relationships among transactions and merchants is expected to reveal hidden patterns indicative of fraud, enhancing the overall predictive power of the model. Results will be documented and analyzed, comparing the performance of the GNN model with established baselines.

Conclusions

The research will demonstrate that GNNs can significantly enhance fraud detection in credit card transactions by modeling complex relationships within the data. This study aims to provide actionable insights for financial institutions, recommending the integration of GNN-based models into their fraud detection systems. The findings will contribute to the field of fraud detection and open avenues for future research in leveraging graph-based methods for complex anomaly detection tasks.