Comparing Graph Features for Automated Credit Card Fraud Detection

Michael Holtz

October 15, 2023

1 Abstract

In 2022, the Federal Trade Commission received over 440,000 reports of credit card fraud, an increase of over 50,000 over the previous year [1, 2]. The annual cost of credit card fraud in the United States has been estimated at XXXXXXX. These factors have lead researchers and institutions to develop novel techniques to detect credit card fraud. Using machine learning techniques to identify fraudulent transactions has been an area of research since at least 1994 and has been a hot topic as of late as the number of credit card transactions continues to rise year over year [3, 4]. Specifically, Prusti, Das, and Rath found that the inclusion of three graph features increased the effectiveness of five supervised and two unsupervised machine learning algorithms [5]. In this paper we seek to evaluate many different graph features and feature selection algorithms to judge the best subset of features for each of the seven machine learning algorithms.

2 Introduction

Credit card data is some of the most regulated data in the world. Finding quality datasets, even for academic use, is nearly impossible. In an attempt to solve this, some have turned to simulations such as BankSim[6]. These simulations start with real anonymized transaction data and simulate a market of buyers, sellers, and fraudsters such that the resulting transactions contain the same fraud indicators as the real world data. The resulting dataset can be freely used and shared as it does not contain any private information.

Prusti, Das, and Rath used the BankSim simulation dataset to train several machine learning models, first on features derived directly from the transactions, and secondly on features derived from a graph model of the transactions. They found that the graph features, degree centrality, PageRank, and label propagation algorithm (LPA) community improved the performance of the models significantly. They measured each model on several well known classification metrics, accuracy, precision, recall, Mathews corelation coefficient, ROC-AUC, and AUPRC.

While replicating their study, we found a similar increase for each feature and each metric. It is worth noting that we did not use a graph database, as the dataset is small enough to fit easily in memory, allowing for much quicker calculation.

We also included a measure specifically designed for credit card fraud models [7]. While most metrics treat false positives and false negatives in the same way, this cost sensitive measure seeks to more closely represent the cost that a credit card company must pay for each resulting. True negatives or legitimate transactions that are classified as legitimate transactions result in no cost to the company. False positives, or normal transactions that are flagged as fraudulent, incur some flat cost C_a, associated with the cost of investigating the transaction manually and contacting the cardholder. True positives, fraudulent transactions correctly identified as such, incur the same cost C_a. False negatives are fraudulent transactions that were mistakenly identified as legitimate. In this case the company looses the amount of the transaction. We can visualize these costs in a cost matrix, with C_a being the administrative cost associated with handling a suspected fraud and Amt_i being the amount transaction in the i-th transaction classified.

$$\begin{array}{r c} & \begin{array}{cc} \text{True Fraud} & \text{True Legitimate} \end{array} \\ \begin{array}{r} \text{Predicted Fraud} \\ \text{Predicted Legitimate} \end{array} & \begin{bmatrix} C_a & C_a \\ Amt_i & 0 \end{bmatrix} \end{array}$$

References

[1] C. S. Network, *Data Book 2021.* Federal Trade Commission, 2021.

[2] ——, *Data Book 2022.* Federal Trade Commission, 2022.

[3] Ghosh and Reilly, “Credit card fraud detection with a neural-network,” in *1994 Proceedings of the Twenty-Seventh Hawaii International Conference on System Sciences*, vol. 3, 1994, pp. 621–630.

[4] F. Reserve, “Federal reserve payments study (frps),” Jul 2023. [Online]. Available: https://www.federalreserve.gov/paymentsystems/fr-payments-study.htm

[5] D. Prusti, D. Das, and S. K. Rath, “Credit card fraud detection technique by applying graph database model.” *Arabian Journal for Science and Engineering*, vol. 46, no. 1-20, 2021.

[6] E. A. Lopez-Rojas and S. Axelsson, “Banksim: A bank payment simulation for fraud detection research,” in *26th European Modeling and Simulation Symposium, EMSS 2014*, 09 2014.

[7] A. C. Bahnsen, A. Stojanovic, D. Aouada, and B. Ottersten, "Cost sensitive credit card fraud detection using bayes minimum risk," in *2013 12th International Conference on Machine Learning and Applications*, vol. 1, 2013, pp. 333–338.