Analysing Similarity Graphs for Credit Card Fraud Detection

Vahid Shahrivari, Ioana Karnstedt-Hulpus
Utrecht University, The Netherlands
{v.shahrivarijoghan, i.r.karnstedt-hulpus}@uu.nl

1 Introduction

In this paper, we investigate the use of similarity graphs to solve problems of detection of rare events such as financial fraud or internet attacks. Two main classes of methods are generally used for rare event detection. The first class consists of the unsupervised methods for anomaly detection. In this case, the system is agnostic of previous examples of the rare events it tries to detect, and looks for events that differ significantly from the majority. Similarity graphs lend themselves straightforwardly to the detection of anomalous items as they are by definition able to find those entities that are particularly dissimilar to the rest. The second class of systems contains those that implement supervised classification methods. In this case, the similarity graphs can be used to compute features that capture complex patterns of similarity between the positive class (e.g. rare event) and the rest. Furthermore, in domains where the assumption can be made that rare events bear some similarity to one another, the similarity graph can reveal new rare events by similarity to known past rare events - this can be seen as a generalization over the kNN model.

2 Similarity Graphs and Features

When representing items as nodes in similarity graphs, there is an edge between a pair of nodes if their similarity is considered substantial. Theoretically, there is a certain similarity between any two items, however, materializing all these similarities as edges leads to a completely connected graph, which brings a lot of computational overhead, while representing a lot of insignificant similarities. Thus, a similarity graph is usually built either by limiting for each node the set of outgoing edges to the top-k most similar other nodes, or by deciding a similarity threshold such that all the pairs with a lower score would not be linked. We experiment with both settings.

In this paper, we propose two types of similarity graph based features: (i) similarity to known previous rare events, and (ii) divergence from the majority. The first type of features relies on the assumption that rare events have something in common. This might or might not apply to a domain. The second type of features assumes that rare events stand out by being dissimilar to the others.

3 Experiments and Conclusion

We conduct our experiments on a dataset of credit card fraud detection[1][1]. It contains 284,807 transactions that occurred in two days. Among them, 492 (0.172%) are labelled as fraud. The dataset is anonymised such that each transaction has 28 features computed with PCA. To create the similarity graph, we import all the transactions into a Milvus vector database [3], and run top-k a-NN queries. As a model for classification, we use random forest because of its very good performance on the same task in the past [2]. We show that the use of the similarity graph features significantly improves the detection of credit card fraud transactions, with the most impact on Recall.

To sum up, our experiments show that similarity graphs can be used to uncover complex patterns of similarity between events that can then be used to single out the rare events.

[1] https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud

References

[1] A. Dal Pozzolo, O. Caelen, Y.-A. Le Borgne, S. Waterschoot, and G. Bontempi. Learned lessons in credit card fraud detection from a practitioner perspective. *Expert Systems with Applications*, 41:4915–4928, 08 2014.

[2] Y.-A. Le Borgne, W. Siblini, B. Lebichot, and G. Bontempi. *Reproducible Machine Learning for Credit Card Fraud Detection - Practical Handbook*. Université Libre de Bruxelles, 2022.

[3] J. Wang, X. Yi, R. Guo, H. Jin, P. Xu, S. Li, X. Wang, X. Guo, C. Li, X. Xu, et al. Milvus: A purpose-built vector data management system. In *Proceedings of the 2021 International Conference on Management of Data*, pages 2614–2627, 2021.