Decision Support Systems 75 (2015) 38–48

Contents lists available at ScienceDirect

Decision Support Systems

journal homepage: www.elsevier.com/locate/dss

APATE: A novel approach for automated credit card transaction fraud detection using network-based extensions

Véronique Van Vlasselaer [a], Cristián Bravo [b,*], Olivier Caelen [c], Tina Eliassi-Rad [d], Leman Akoglu [e], Monique Snoeck [a], Bart Baesens [a,f]

[a] Department of Decision Sciences and Information Management, KU Leuven, Naamsestraat 69, B-3000 Leuven, Belgium
[b] Departamento de Ingeniería Industrial, Universidad de Talca, Curicó, Chile
[c] Fraud Risk Management Analytics, Worldline, Brussels, Belgium
[d] Department of Computer Science, Rutgers University, Piscataway, NJ, USA
[e] Department of Computer Science, Stony Brook University, Stony Brook, NY, USA
[f] School of Management, University of Southampton, Southampton, United Kingdom

ARTICLE INFO

Article history:
Received 11 September 2014
Received in revised form 11 February 2015
Accepted 30 April 2015
Available online 8 May 2015

Keywords:
Credit card transaction fraud
Network analysis
Bipartite graphs
Supervised learning

ABSTRACT

In the last decade, the ease of online payment has opened up many new opportunities for e-commerce, lowering the geographical boundaries for retail. While e-commerce is still gaining popularity, it is also the playground of fraudsters who try to misuse the transparency of online purchases and the transfer of credit card records. This paper proposes *APATE*, a novel approach to detect fraudulent credit card transactions conducted in online stores. Our approach combines (1) intrinsic features derived from the characteristics of incoming transactions and the customer spending history using the fundamentals of RFM (Recency–Frequency–Monetary); and (2) network-based features by exploiting the network of credit card holders and merchants and deriving a time-dependent suspiciousness score for each network object. Our results show that both intrinsic and network-based features are two strongly intertwined sides of the same picture. The combination of these two types of features leads to the best performing models which reach AUC-scores higher than 0.98.

1. Introduction

In recent years, e-commerce has gained a lot in popularity mainly due to the ease of cross-border purchases and online credit card transactions. Customers are no longer bound by the offers and conditions of local retailers, but can choose between a multitude of retailers all over the world and are able to compare their products, offered quality, price, services, etc. in just a few clicks. While e-commerce is already a mature business with many players, security for online payment lags behind. Recently, the European Central Bank (ECB) reported that the value of card fraud increased in 2012 by 14.8% compared to the year before [21]. The main reason is the strong growth in online sales, resulting in many "card-not-present" transactions (CNP), a means of payment that catches the attention of illicit people who try to mislead the system by pretending to be someone else. As a consequence, credit card issuers need an automated system that prevents the pursue of an incoming transaction if that transaction is highly sensitive to fraud, i.e. the transaction does not correspond to normal customer behavior.

This work focuses on *automatically* detecting online fraudulent transactions. Data mining offers a plethora of techniques to find patterns in data, distinguishing normal from suspicious transactions. A key challenge in fraud is to appropriately deal with the atypical character of fraud. That is, there are many legitimate transactions and only few evidence of fraudulent transactions to learn from, which complicates the detection process. Carefully thinking about and creating significant characteristics that are able to capture irregular behavior, is an essential step in an efficient fraud detection process. In this paper, we combine both intrinsic and network-related features. Intrinsic features analyze the transaction as if it is an isolated entity, and compare whether the transaction fits in the normal customer profile. We create those features by deriving RFM attributes – Recency, Frequency and Monetary Value – of the credit card holder's past transactions. Network-based features, on the other hand, characterize each transaction by creating and analyzing a network consisting of credit card holders and merchants which are related by means of transactions. A sample network is given in Fig. 1.

We use a collective inference algorithm to spread fraudulent influence through the network by using a limited set of confirmed fraudulent transactions and decide upon the suspiciousness of each network object

* Corresponding author at: Km. 1 Camino a Los Niches, 3344158 Curicó, Chile. Tel.: +56 75 220 1756.

http://dx.doi.org/10.1016/j.dss.2015.04.013
0167-9236/

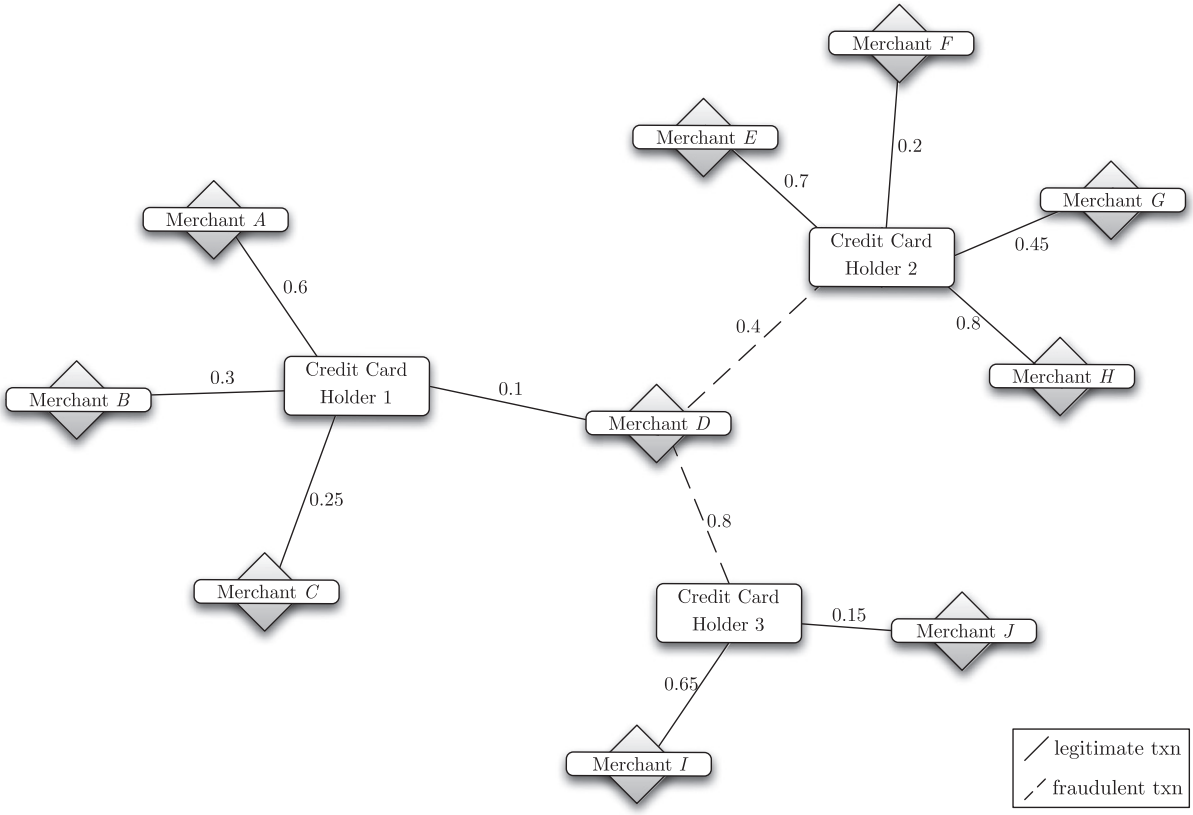

Fig. 1. Toy example of a credit card fraud network. Weights depict the recency of the transaction between the merchant and credit card holder.

by deriving an exposure score — i.e. the extent to which the transaction, the associated account holder and the merchant are exposed to past fraudulent influences.

In this work, we will answer the following questions: (1) Is a new incoming transaction in line with normal customer behavior, i.e. does it correspond to regular spending patterns of that customer in terms of (a) *frequency* or the average number of transactions over a certain time window, (b) *recency* or the average time in between the current and previous transaction and (c) *monetary value* or the amount spent on that transaction? (2) Which merchants, credit cards and transactions are sensitive to fraud? Given past network-based information between merchants and credit card holders through the transactions made, how do we derive a suspiciousness score for (a) merchants indicating which merchants are often related to fraud, and as a consequence, form a risk of pursuing future fraudulent transactions; (b) credit card holders who act irregularly or whose credit card is stolen and (c) transactions by combining evidence of the associated credit card holder and merchant; (3) does our detection approach which combines both intrinsic and network-based features, significantly boost the performance over traditional intrinsic-only models, and if so, which specific set of features contribute in detecting efficiently fraud?

We propose *APATE* (short for: Anomaly Prevention using Advanced Transaction Exploration), a novel, automated and real-time approach to tackle credit card transaction fraud by mapping past purchasing patterns and customer behavior into meaningful features and compare those features with the characteristics of a new, incoming transaction. We apply supervised data mining techniques to uncover fraudulent patterns from a real-life credit card transaction data set obtained from a large credit card issuer in Belgium. Our approach complies with the six-second rule, i.e. within six seconds the *APATE* algorithm needs to decide whether the transaction should or should not be pursued. We contribute by proposing a new propagation algorithm to propagate fraud from the network edges (i.e., the transactions) towards all the network components (i.e., the credit card holders and merchants) and derive for each transaction network-based features. Those features are combined with a set of intrinsic features to feed the learning algorithms. Our fraud detection model is able to *dynamically* adapt to a changing environment and continues to operate under the condition that fraudsters invent new ways to perpetrate their illegal activities.

The remainder of the paper is organized as follows. We introduce the credit card fraud domain in Section 2. Section 3 discusses the proposed methodology, and focuses on intrinsic and network-based feature extraction (Sections 3.1 and 3.2). In Section 4, we summarize the results. Section 5 concludes this paper.

2. Credit card transaction fraud

2.1. Background

Credit card fraud detection is a widely studied research domain. Bhatla et al. [9] and Delamaire et al. [18] distinguishes between various types of fraud like application fraud (i.e., acquiring a credit card with false information), stolen or lost card, counterfeit card (i.e., card copying or using a card which does not belong to the owner) and card-not-present (CNP) fraud (i.e., using credit card details to make distance purchases). Our paper focuses on CNP fraud perpetrated through online credit card transactions.

As manually processing credit card transactions is a time-consuming and resource-demanding task, credit card issuers search for high-performing and efficient algorithms that *automatically* look for anomalies in the set of incoming transactions. Data mining is a well-known and often suitable solution to big data problems involving risk such as credit risk modeling [6], churn prediction [34] and survival analysis [5]. Nevertheless, fraud detection in general is an atypical prediction task which requires a tailored approach to address and predict future fraud. We say that fraud is an uncommon, well-considered,