ELSEVIER

Expert Systems with Applications 31 (2006) 337–344

Expert Systems with Applications

www.elsevier.com/locate/eswa

Subscription fraud prevention in telecommunications using fuzzy rules and neural networks

Pablo A. Estévez *, Claudio M. Held, Claudio A. Perez

Department of Electrical Engineering, University of Chile, Casilla 412-3, Santiago, Chile

Abstract

A system to prevent subscription fraud in fixed telecommunications with high impact on long-distance carriers is proposed. The system consists of a classification module and a prediction module. The classification module classifies subscribers according to their previous historical behavior into four different categories: subscription fraudulent, otherwise fraudulent, insolvent and normal. The prediction module allows us to identify potential fraudulent customers at the time of subscription. The classification module was implemented using fuzzy rules. It was applied to a database containing information of over 10,000 real subscribers of a major telecom company in Chile. In this database, a subscription fraud prevalence of 2.2% was found. The prediction module was implemented as a multilayer perceptron neural network. It was able to identify 56.2% of the true fraudsters, screening only 3.5% of all the subscribers in the test set. This study shows the feasibility of significantly preventing subscription fraud in telecommunications by analyzing the application information and the customer antecedents at the time of application.

Keywords: Fraud prevention; Fraud detection; Subscription fraud; Neural networks; Fuzzy rules

1. Introduction

The biggest revenue leakage area in the telecom industry is fraud (Wieland, 2004). Global telecommunications fraud losses are estimated in the tens of billions of dollars every year (FML, 2003; Hoath, 1998). The history of telecommunications crime, including several types of fraudulent activities, was reviewed by Collins (1999a,b, 2000). Some authors have emphasized the importance of distinguishing between fraud prevention and fraud detection (Bolton & Hand, 2002). Fraud prevention describes measures to avoid fraud to occur in the first place. In contrast, fraud detection involves identifying fraud as quickly as possible once it has been committed.

Shawe-Taylor, Howker, Gosset, Hyland, Verrelst and Moreau (2000) distinguished six different fraud scenarios: subscription fraud, the manipulation of Private Branch Exchange (PBX) facilities or dial through fraud, freephone fraud, premium rate service fraud, handset theft and roaming fraud. Subscription fraud, which is defined as the use of telephone services with no intention of paying, is probably the most significant and prevalent worldwide telecom fraud (FML, 2003; Hoath, 1998). Subscription fraud can be subdivided into two categories: (a) for profit, i.e. mainly for selling long distance calls and (b) for personal usage. Subscription fraud can be committed upon fixed and mobile telephones, and it is usually difficult to distinguish from bad debt, particularly if the fraud is for personal usage. Both subscription fraud and bad debt are major problems to telecom in developing and third world countries (Hoath, 1999). Two strategies have been proposed for detecting subscription fraud: examining account applications and tracking customer behavior (Fawcett & Provost, 2002b). Other efforts have focused on formalizing and predicting the deceiving intention of fraudsters (Barghava, Zhong, & Lu, 2003).

The detection of fraud in mobile telecommunications was investigated in the European project Advance Security for Personal Communications Technologies (ASPeCT) (Burge & Shawe-Taylor, 2001; Shawe-Taylor, Howker, & Burge, 1999; Shawe-Taylor et al., 2000). The ASPeCT fraud detection tool is based on investigating sequences of call detail records (CDRs), which contain the details of each mobile phone call attempt for billing purposes. The information produced for billing also contains usage behavior information valuable for fraud detection. A differential analysis is performed to identify a fraudster through profiling the behavior of a user. The analysis of user profiles are based on comparison of recent and longer-term behavior histories derived from the toll ticket data. Alarms are activated when the usage pattern of a mobile phone changes significantly over a short period of time. The ASPeCT

* Corresponding author. Tel. +56 2 9784207; fax: +56 2 6720162.
E-mail address: pestevez@cec.uchile.cl (P.A. Estévez).

0957-4174/$ - see front matter © 2005 Elsevier Ltd. All rights reserved.
doi:10.1016/j.eswa.2005.09.028

fraud detection tool utilizes a rule-based system for identifying certain frauds, and neural networks (NNs) to deal with novel or abnormal instances or scenarios. Rosset, Murad, Neumann, Idan, and Pinkas (1999) used customer data, in addition to CDRs, to discover rules for identifying subscription fraud.

According to Cahill, Lambert, Pinheiro, and Sun (2002), a fraud detection algorithm has two components: (a) a summary of the activity on an account that can be kept current and (b) rules that are applied to account summaries to identify accounts with fraudulent activity. A popular approach is to reduce the CDRs for an account to several statistics that are computed for each period, e.g. average call duration, and compare them to thresholds. Fawcett and Provost (1997a,b) and Fawcett (2002a) developed a method for choosing account-specific thresholds rather than universal thresholds. Their procedure takes daily traffic summaries for a set of accounts that experienced at least 30 days of fraud-free traffic activity followed by a period of fraud. This method was applied to cellular cloning, in which fraudulent usage is superimposed upon the legitimate usage of an account. For each account a set of rules that distinguish fraud from non-fraud was developed. The superset of the rules for all accounts was then pruned by keeping only those that cover many accounts, with possibly different thresholds for different accounts. Cahill et al. (2002) defined account signatures to track legitimate call behaviors in real time. An account signature describes which call variables (e.g. call duration) are likely and which are unlikely for the account. Signatures evolve with each new call that is not considered fraudulent, so each established customer eventually has its own signature. Likewise, fraud signatures are defined for each kind of fraud using the same structure as an account signature. A call is scored by comparing its probability to belong to the account signature and to a fraud signature. For new accounts the first calls are used to assign signature components, associating them with calling patterns of a given segment of customers with similar initial information.

Cortes, Pregibon, and Volinsky (2001, 2003) applied large dynamic graphs, represented as the union of small sub-graphs called communities of interest, to the area of telecommunications fraud detection. The nodes in the graphs are network IDs and the edges represent communications between pairs of network IDs. In one application, the 'guilt by association' argument was used to detect new cases of fraud in the network, one week after the new accounts were activated. It was found that the probability of an account to be fraudulent is an increasing function of the number of fraudulent nodes in its community of interest. A second example used a distance metric between communities of interest to suggest when an individual whose account had recently been disconnected for fraud had assumed a new network identity. This assumed that the calling patterns of the new account had not changed very much from the previous account.

In the last decade, modern intelligent systems have been applied to fraud detection. Bolton and Hand (2002) reviewed the statistical and machine learning technologies for fraud detection, including their application to detect activities in money laundering, e-commerce, credit card fraud, telecommunication fraud and computer intrusion. Weatherford (2002) presented several real-world applications of intelligent fraud detection technologies. Kou, Lu, Sirwongwattana, and Huang (2004) made a survey of fraud detection techniques used in telecommunication, as well as in credit card fraud and computer intrusion. Phua, Lee, Smith, and Gayler (2005) made a comprehensive survey of data mining techniques applied to fraud detection. Hong and Weiss (2001) presented several predictive models for data mining applied to fraud detection and insurance risk assessment. Some authors have provided comprehensive surveys of NNs (Vellido, Lisboa, & Vaughan, 1999; Wong, Bodnovich, & Selvi, 1997) and Expert Systems (ES) (Liao, 2005; Wong & Monaco, 1995) applications in business. Vellido et al. (1999) found that published applications of NNs in real-world scale are scant. One difficulty for publishing results is the need for confidentiality of private companies operating in a tough competitive environment. The main advantages of NNs are: (a) their suitability to handle incomplete, missing or noisy data; (b) being a non-parametric method, it does not require any a-priori assumptions about the distribution and/or mapping of the data; and (c) their demonstrated capability to approximate any continuous function. The lack of explanatory capabilities is considered as the main shortcoming of the application of NNs. Hence, several attempts have been made to integrate NNs and ES; a synergistic effect between them is expected, as ES are characterized by their capability of explaining their own reasoning process.

Other authors have used data mining techniques to develop a decision support system for predicting customer insolvency in telecommunications (Daskalaki, Kopanas, Goudara, & Avouris, 2003). In their approach, it is assumed that insolvent customers behave differently on the average from the rest of the customers, especially during a critical period preceding the due-date for payment. The prediction of customer insolvency for a telecommunications company as a problem was found to be similar to the fraud detection problems in mobile and conventional telecommunications as well as in credit or calling card operations. Among the common characteristics found are the following: significant loss of revenue, unpredictability of human behavior, information retrieval involves processing huge amounts of data from several different sources; fraudulent cases are rare compared to legitimate ones. Ezawa and Norton (1996) constructed Bayesian networks to predict uncollectible telecommunications accounts.

The related problem of subscriber churning in mobile telecommunications, i.e. the movement of subscribers from one provider to another, has been investigated using NNs (Mozer, Wolniewicz, Grimes, Johnson, & Kaushansky, 2000) and data mining (Wei & Chiu, 2002). Mozer et al. (2000) used techniques from statistical machine learning to evaluate the benefits of predicting churn. Experiments were carried out using a database of 47,000 subscribers that included information about their usage (CDRs, quality of service), billing, credit, application for service (contract details, rate plan, and credit report), and complaint history. The outcome was expressed using a lift curve which plots the fraction of all