Katholieke Universiteit Leuven

Departement Elektrotechniek ESAT-SISTA/TR 1997-42

Fraud Detection in Mobile Communications using Supervised Neural Networks [1]

Yves Moreau and Joos Vandewalle[2]

April 1997
to appear in Proceedings of SNN'97:
Europe's Best Neural Networks Practice,
World Scientific

[1] This report is available by anonymous ftp from *ftp.esat.kuleuven.ac.be* in the file *pub/SISTA/moreau/reports/icann97_tr97-42.ps*

[2] ESAT - Katholieke Universiteit Leuven, Kardinaal Mercierlaan 94, 3001 Leuven (Heverlee), Belgium, tel +32/16/32 18 06, fax +32/16/32 19 86, email: *yves.moreau@esat.kuleuven.ac.be*, www: *http://www.esat.kuleuven.ac.be/~moreau/* .

Fraud Detection in Mobile Communications using Supervised Neural Networks

Yves Moreau, Herman Verrelst, and Joos Vandewalle

Elektrotechniek - ESAT, Katholieke Universiteit Leuven,
Kardinaal Mercierlaan 94, B-3001 Leuven, Belgium,
yves.moreau@esat.kuleuven.ac.be,
http://www.esat.kuleuven.ac.be/~moreau/.

Abstract. We present the results of the development of the first prototype of a supervised neural network for the detection of fraud in mobile communications. We have developed this prototype in the framework of a project of the European Commission on Advanced Security for Personal Communications (ASPeCT)[1], together with two other prototypes based on unsupervised neural networks and knowledge-based systems, respectively. If technology permits, we will present a demonstration of our prototype at the SNN'97 conference.

1 Introduction

The mobile communication industry suffers major losses to fraud. In the U.S. alone, it estimates its loss of revenue to over 650 million dollars a year. Therefore, the prevention and detection of fraud has become a top priority. The first-generation analogue mobile phones remain the main target of fraudsters since the second-generation digital phones, like GSM (Global System for Mobile communications), provide enhanced security features. However, as the industry migrates further into second-generation and future third-generation systems (high-bandwidth digital systems, like the Universal Mobile Telephony System UMTS), fraud is expected to follow this migration. The European Community is focusing its research effort to accelerate the deployment of advanced communications infrastructures and services through its Advanced Communications Technologies and Services (ACTS) program. In the framework of this program, the ASPeCT project addresses the issues of security in mobile communications in the future UMTS, and during the migration from GSM to UMTS. Within this project, a workpackage is dedicated to the detection and management of fraud in mobile communication networks using advanced ("intelligent") decision tools. The result of the first part of the work of this workpackage has been the development of three first prototypes of fraud detection tools [1, 2, 3]. We present here the fraud detection tool based on supervised learning, while two others prototypes based on unsupervised learning, and knowledge-based systems have been developed by our partners.

[1] More information about this project is available from http://www.esat.kuleuven.ac.be/cosic/aspect

2 Fraud Scenarios and Fraud Indicators

The operation of a mobile network is complex, and fraudsters invest a lot of energy to find and exploit every weakness of the system. The first step of the project was thus to analyze the operation of the network, and identify and categorize the vast range of possible scenarios of fraud. A common example would be subscription fraud, where a fraudster acquires a subscription to the mobile network under a fake identity, and starts reselling the use of his phone (typically for international calls to distant foreign countries) at a rate lower than the regular tariff to unscrupulous customers. The fraudster accumulates a large number of expensive calls, but disappears before the bill can be collected.
After identifying the possible fraud scenarios, we have identified the possible indicators that could be extracted from the information available on the network to detect fraud. An example could be an excessive number of international calls. The information about the activity on the network is encoded in the toll tickets of all the calls placed on the network. A toll ticket is a bill issued by the network after each call, which contains all relevant information about the call. Among others are the International Mobile Subscriber Identity (IMSI) - which identifies a user uniquely -, the starting date of the call, its starting time, its duration, the number that was called and whether this call was international or not. More information is available from the toll ticket, but only these six characteristics are considered at this point. The main constraint comes from the massive amount of information that needs to be processed. A network operator can have over a million subscribers, placing a few million calls a day. The system needs to be able to analyze up to 50 calls per second.

3 User Profiling

A first approach to fraud detection is to detect excessive activity. For example, if a user is making more than two hours of calls from Europe to South America a day, we might want to raise an alarm. This is called absolute analysis, because the alarm will be raised on the basis of the activity, independently of the user who is being monitored. The disadvantage with this approach is that users with a high level of activity will raise alarms; but if these users are not fraudsters but well legitimate users, they will happen to be the very best customers; hence, those who in fact need to be treated most carefully. Therefore, it is necessary to know what the normal activity of the user is, and we will want to detect sudden changes in the behavior of a user. This is called differential analysis.
The analysis is implemented as follows. A large database is built where a set of relevant parameters (called user profile) is stored for each user. When a toll ticket is produced on the telephone network, the profile of the user who made the call is retrieved from the database; the profile is updated with the data contained in the toll ticket; and it is passed on to the fraud detection engine that checks if the activity of the user warrants the raise of an alarm. The differential part of the analysis is implemented by splitting the user profile into a short-term and a

long-term representation of the behavior of the user; and by basing the analysis on a comparison of the two. A list of the users who are producing alarms is kept, and the list of the toll tickets produced by the suspicious users is recorded. This information forms the basis of an audit trail that can be later used for prosecution, if necessary.

4 Supervised Neural Networks for Fraud Detection

Applications of neural networks to fraud detection are currently being developed worldwide for a variety of applications [4, 5], among which fraud detection in mobile communications [6, 7].

The main part of the work went into designing a set of features that would adequately capture the behavior of a user, especially its dynamics. The features are based on short-term and long-term averages and standard deviations of duration and frequency of national and international calls. This resulted in a set of 16 features, which are updated for each user after he makes a call. It is of importance to be able to update and manage these feature profiles for all the users in real-time. This imposed severe constrained on the speed of the database and on the design of the features. The features are therefore computed using a simple and efficient filtering strategy. The available data consists of a list of the toll tickets produced by 300 new users of the network over a six-week period, and of 300 cases of fraud over a period of six months. For all 600 users, all the toll tickets are processed to produce sequences of user profiles. These user profiles are labeled manually into fraudulent and non-fraudulent (it is necessary to determine when fraud begins in a sequence of toll tickets associated to a case of fraud). The architecture used is a multilayer perceptron; and the training is performed on part of the data using a conjugate-gradient procedure. The rest of the data is used for testing. The architecture of the multilayer perceptron is adapted to obtain optimal performance. The problem with testing is that classification error is a misleading index of performance because of the heterogeneity of the data (no guarantee that new users are not fraudsters, different time spans for the "new users" data and the fraud "data", different proportions of fraud in the training data and on the actual network...). The investigation of the performance of the system is a problem in its own right and is currently being investigated. As an indicator, on the testing data, this prototype achieved a correct classification of fraud cases in the 80-90% range, for a misclassification of the new users in the 2-5% range; the other prototypes achieved comparable performance.

5 Conclusions and Future Work

We have briefly introduced our work on the detection of fraud in mobile telecommunication networks. We have presented a first prototype developed in the framework of the ASPeCT project, which uses a multilayer perceptron trained on normal and fraudulent data of the network. We have demonstrated the feasibility and potential of this approach. We are currently thoroughly evaluating the prototype before we develop it further. The next developments will be the extension of the number of features to characterize behaviors that cannot be described within the current system, and the integration of our prototype together with the other prototypes into a meta-tool.

6 Acknowledgments

Joos Vandewalle is a full Professor at the K.U. Leuven. Yves Moreau is a research assistant of the F.W.O. - Vlaanderen. This work is supported by several institutions:

1. the Flemish Government: Concerted Research Action GOA-MIPS (Model-based Information Processing Systems)
2. the Belgian State, Prime Minister's Office - Federal Office for Scientific, Technical and Cultural Affairs - Interuniversity Poles of Attraction Programme: (IUAP P4-02): Modeling, Identication, Simulation and Control of Complex Systems
3. the European Commission: ACTS ASPECT: Advanced Security for Personal Communications Technology

References

1. ACTS AC095, project ASPeCT: Definition of Fraud Detection Concepts. ACTS ASPeCT, AC095/ATEA/W22/DS/P/06/A (1996)
2. ACTS AC095, project ASPeCT: Fraud Management Tools: First Prototypes. ACTS ASPeCT, AC095/DOC/RUL/072/WP22/A (1997)
3. Moreau Y., Preneel B., Burge P., Shawe-Taylor J., Stoermann C., Cooke C.: Novel Techniques for Fraud Detection in Mobile Telecommunications. ACTS Mobile Summit, Grenada (1996)
4. Ghosh S., Reilly D.: Credit Card Fraud Detection with a Neural-Network. Proceedings of the 27th Annual Hawaii International Conference on System Science, IEEE Computer Society Press **3** (1994) 621–630
5. Fanning K., Cogger K., Srivasta R.: Detection of Management Fraud: a Neural Network Approach. International Journal of Intelligent Systems in Accounting, Finance, and Management **4** (1995) 113–126
6. Connor L., Brothers L., Alspector J.: Neural Network Detection of Fraudulent Calling Card Patterns. Proceedings of the International Workshop on Applications of Neural Networks to Telecommunications, Lawrence Erlbaum Associates (1995) 362–370
7. Barson P., Field S., Davey N. McAskie G., Frank R.: The Detection of Fraud in Mobile Phone Networks. Neural Network World **6** 4 (1996) 477–484

This article was processed using the LaTeX macro package with LLNCS style