Katholieke Universiteit Leuven

Departement Elektrotechniek ESAT-SISTA/TR 1997-44

Detection of Mobile Phone Fraud using Supervised Neural Networks: A First Prototype [1]

Yves Moreau and Joos Vandewalle[2]

April 1997
Submitted to ICANN 97

[1] This report is available by anonymous ftp from *ftp.esat.kuleuven.ac.be* in the file *pub/SISTA/moreau/reports/icann97_TR97-44.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/* .

Detection of Mobile Phone Fraud using Supervised Neural Networks: A First Prototype

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 first prototype of a tool based on a supervised neural network for the detection of fraud in mobile communications. This prototype is being developed 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.

1 Introduction

The mobile communication industry suffers major losses to fraud. In the U.S. alone, the industry estimates its loss of revenue to over 650 million dollars a year. Because of the direct impact of fraud on the bottom-line of mobile phone providers, the prevention and detection of fraud has become a priority. The main target of fraudsters remains the first-generation analogue mobile phones, 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 a knowledge based systems and on unsupervised learning [4]

[1] More information about this project and a demonstration of the prototype are available from http://www.esat.kuleuven.ac.be/cosic/aspect.

have been developed by our partners. We also present the result of a preliminary evaluation of our tool.

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 typical example would be subscription fraud, where a fraudster acquires a subscription to the mobile network under a false identity; and starts reselling the use of his phone to unscrupulous customers (typically for international calls to distant foreign countries) at a rate lower than the regular tariff. 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. The information we use is

1. the International Mobile Subscriber Identity (the IMSI, which identifies a user uniquely)
2. the starting date of the call
3. the starting time of the call
4. the duration of the call
5. the number that was called
6. the type of call (national or international)

More information is available from the toll ticket, but only these six characteristics are considered at this point. The limited complexity of the system will come from the constraint that massive amounts of information need to be processed: A network operator can have over a million subscribers, placing a few million calls a day. A major requirement was that the system had to analyze up to 50 calls per second.

3 User Profiling

A first approach to fraud detection is to detect excessive activity. For example, we might want to raise an alarm if a user is making more than two hours of calls from Europe to South America on any single day. This is called absolute analysis, because the alarm will be raised on the basis of the activity, independently of whom the user is. With this approach users with a high level of activity will raise alarms, since high activity is characteristic of fraud; however, if these users happen not to be fraudsters but legitimate users, they will in fact be the very best customers; hence, those who need to be treated most carefully. Therefore, to avoid troubling legitimate high-end users, it is necessary to know what the normal activity of the user is; and to raise alarms on the basis of 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 (Current User Profile) and a long-term (User Profile History) representation of the behavior of the user; and by basing the analysis on a comparison of the two. This is depicted in Figure 1. 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.

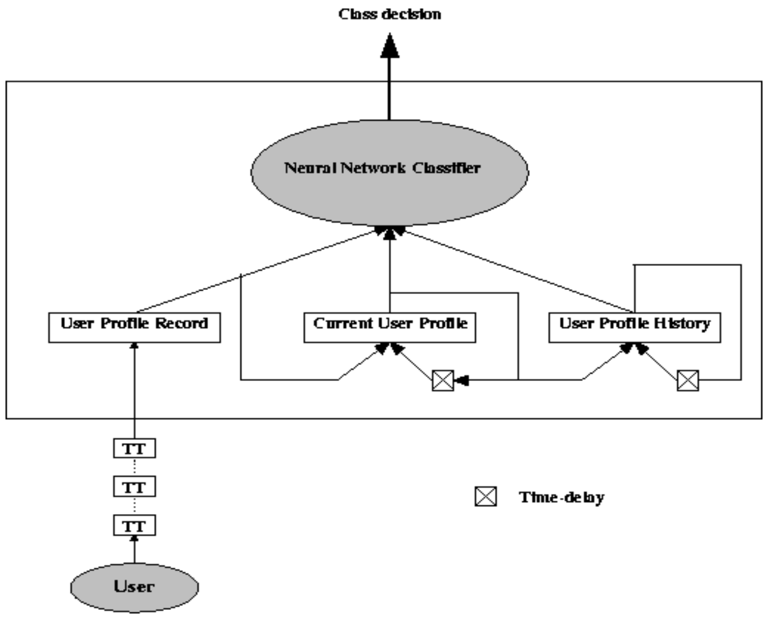

Fig. 1. Architecture of the fraud detection tool

4 Supervised Neural Networks for Fraud Detection

Fraud detection systems using neural networks are currently being developed worldwide for a variety of applications [5, 6], among which fraud detection in mobile communications [7, 8], though litterature on the subject in scarce.
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 constraints 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. The training and evaluation of the prototype are difficult tasks because of the messy nature of the data. The problem with the data are numerous. Different users make vastly different number of calls; their call history also covers different periods of time. There is no guarantee that none of the new users are not fraudsters, nor that the call history of fraudsters contains enough information for detection using an analysis of call duration and call frequency patterns, or that the whole call history of a fraudster is associated to fraud. For these reasons, the user profiles are labeled manually into suspicious and non-suspicious (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.

4.1 Evaluation of the prototype

For testing, we used data consisting of the activity of 1974 new users during over a two-month period, and of the call history of 208 fraudsters. The testing data was collected so as to minimize the problems mentioned above, but they are far from completely alleviated. Squared error criteria on the test set consisting of both fraudulent and new users are essentially meaningless because the proportion of fraudulent cases to normal cases is not representative of the true proportion. This proportion is in fact unknown. We therefore settled for criteria based on percentage of “correct” classification (fraudsters classified as suspicious and new users classified as non-suspicious) on the two classes separately. Further, if we want the system to be used in practice, the operator needs to be able to control the number of alarms generated by the system. Another constraint is that the ratio of correct detections to false alarm needs to be high enough, so that the alarms are taken seriously. The first constraint is dealt with by using a variable alarm threshold. We then compute the percentage of fraudsters who are detected, and the percentage of new users who raise an alarm. This is represented in a diagram called a receiver-operating characteristic, which is depicted in Figure 2. To give an idea of the performance, it is possible to correctly classify 90% of the fraudsters, while misclassifying 10% of the new users. Such a performance, while being of interest, is unusable in practice because it would generate a flood of false alarms. This is because a network contains hundreds of thousands of users. However, if we accept to detect only 50% of the fraudsters, we will misclassify only 0.3% of the new users. Although we cannot answer the question of what the ratio between correct detection and false alarms is, since we do not know the exact proportion of fraud on the network, such a percentage of misclassification is expected to keep the number of alarms under control. In fact, the overall performance is close to the performance expected from a pre-competitive product. Moreover, a large proportion of the alarms generated for the new users are known to be "abnormal legitimate usage", such as lines used for test purposes, where the traffic is extremely high because of the special nature of the number. This will be dealt with in the next stage of the project.

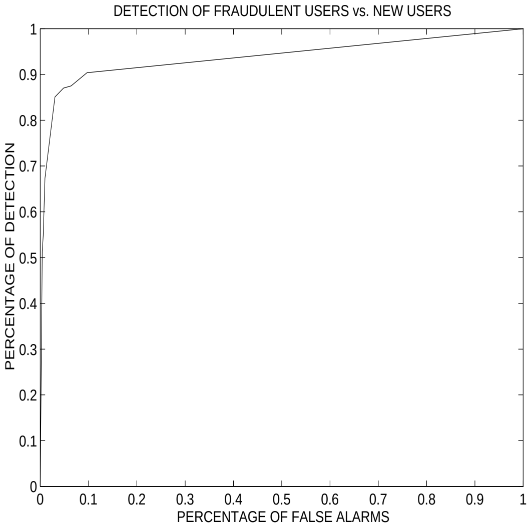

Fig. 2. Receiver-operating characteristic of the fraud detection tool

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 high 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, Spain (1996)
4. Burge P., Shawe-Taylor J.: Detecting Cellular Fraud Using Adaptive Prototypes. To appear in Proceedings of AAAI-97 Workshop on AI Approaches to Fraud Detection and Risk Management, Providence, RI (1997)
5. 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
6. 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
7. 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
8. 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