Fraudulent Call Detection For Mobile Networks

Sameer Qayyum, Shaheer Mansoor, Adeel Khalid, Khushbakht, Zahid Halim and A.Rauf Baig
Department of Computer Science
National University of Computer and Emerging Science, FAST-NU
H11/4 Islamabad, Pakistan.
{i060028,i060231,i060017,i060292, zahid.halim,rauf.baig}@nu.edu.pk
http://www.nu.edu.pk, http://www.ming.org.pk/

Abstract—Telecommunication industry has witnessed an enormous growth in terms of number of subscribers and revenue over the past few years. Still there are certain trends in the revenue of the telecommunication that show an instant fall, reason being change in customer behavior. Telecom operators are subjected to fraud in various forms, among the leading are subscription and superimposition fraud. In the U.S the sum of losses caused by fraudulent activity for the telecom industry is over 650 million dollars a year. The aim in this work is to cater the subscription fraud and bring the figures well within the desired range. In this work we use machine learning techniques to address the issue. Our solution uses a neural network to detect fraudulent behavior for subscription fraud. The neural network takes as input time series data of individual customers to predict their normal behavior. The crucial aspects of the network's predictions being accurate are the fraud profiles; some test cases are created which are used to make the neural network learn a fraudulent behavior.

Keywords: Telecom data, Fraudulent behavior prediction, Artificial Neural Network.

I. INTRODUCTION

Telecom industry in Pakistan has witnessed an enormous growth in terms of number of subscribers and revenue. In 2004 the number of total cell phone subscribers in Pakistan was 5,022,908 and rose up to 96,709,585 by November 2009[1]. During this time many different operators entered the market and enjoyed the growing markets, but between 2004 and 2009 the rate at which the telecom sector was expanding fell. Between 2004 to 2007 it was around 100% each year and between 2008 and 2009 it had fallen below 20%[2]. Now companies face the inevitable challenge of retaining old customers and reduce operational costs to retain their market share. This means companies can no longer disregard aspects like fraud and need to utilize intelligent techniques to minimize fraud losses. Neural networks can be developed, and previously have been developed to serve such purposes, and trained in a certain way to detect a class of frauds, Telecom fraud can be detected by constructing profiles of fraudulent behavior based on previous frauds.

Our application uses a neural network to detect fraudulent behavior for subscription fraud. The network uses time series data of individual customers to predict their natural behavior. The crucial aspects of the network's predictions being accurate are the fraud profiles. For this purpose we create test cases which are used to make the network learn a fraudulent behavior. Companies usually target a certain market segment and have different customer classes. This means that one set of standard profiles cannot be created that represent all types of fraud within the telecom sector. Depending on the previous fraud that has occurred, these profiles can be created that best represent the fraud at hand. However there are aspects of fraudulent activities that are common for all cases, thus there is a need for the application to be amendable enough to learn and predict slightly different kinds of fraud.

We are using a neural network that is supervised and uses a test dataset for learning. The network is designed such that it can be improvised to train and detect different frauds within datasets. Purpose being is to aid telecommunication operators to optimize the network according to their respective class of fraud.

The paper is organized as follows: section II covers the previous work, section III list the fraud detection model that covers the profiling, ANN architecture and training, section IV covers the experimentation and results and section V concludes the paper.

II. PREVIOUS WORK

Neural networks have previously been used in many fraud detection applications, among the well known examples are credit card and call card. Banks often use neural networks to monitor their transactions.

Visa international experienced a loss of 655million dollars in revenue due to fraud in 1993 [4]. They developed a neural network that is based on deviation detection in customers purchasing patterns, the interesting aspect of their neural network is that it lets the customers evolve overtime and doesn't generate fake alarms caused by deviations not due to fraudulent activity. Recently many leading telecommunication companies worldwide have incorporated neural network based applications to detect fraudulent behavior, these applications have adequate detection rate and a lot fraud is stopped.

Sen Wu in [9] identifies the common characteristics of fraudulent behavior of customers in telecom industry systematically. They use clustering techniques of data mining to identify outliers in data. The work in [9] gives definition of target customers who are maliciously based on these specific methods are proposed to build, evaluate, and apply the model for identifying fraudulent behavior. The outliers are identified using Kohonen neural network clustering algorithm.

In [10] the author presents the use of neural networks for the detection of telecommunication fraud using a concept of profiling. Author clamed successfully trained using simulated data resulting in a 98% detection rate when tested for call-sell fraud. In [11] Wei Xu uses rough fuzzy set based approach to detect fraud in 3G mobile telecommunication network. They design a rule based system called Citi FMS to detect abnormities and alarm.

III. FRAUD DETECTION MODEL

A. Supervised Neural Network

The network we have developed is a multilayer perceptron. It is based on three layers, input, a hidden and an output, and it associates a fraud rating to a customer based on his calling profile. The learning rate determines the rate at which the values for weights change and converge to a deterministic network. Changing the number of neurons (hidden layer) produces different results, thus all architectures have to be analyzed and tested in order to find the optimal network, for this purpose we tested the results of networks with varying number of neurons and reached an optimal solution, which is the selected architecture in this case. Once this was established the network was ready to consider real data inputs and predict fraudulent behavior [5].

B. Behavioral Profiling

As mentioned earlier the fraud profile constructed to detect fraud plays a very key role. Capturing the generic profile based on fraud known to be committed previously can't serve as a solution. The aim here is to provide the telecom operators with a generic model of the fraud profile which they should be able to improvise according to their own collected stats on fraud (model of fraud). For this purpose we developed two techniques, one was to let the users select their own combination of fraud features which they think best represent fraud they are dealing with, and the other was to associate weight priorities based on user's input to give more priority to one fraud aspect with respect to others, this again helps in better establishing a fraud profile [6].

Apart from the capturing the features of the fraudulent behavior we are interested in capturing the change in a customer's calling behavior, the change here represents one of the two: the customer is deviating from his normal calling behavior and might commit or the customer's calling behavior is changing and it is an effect of a socio-economic change in that person's life e.g. promotion, student to employee etc. This type of change in customers calling behavior occurs over time and is natural, but if the detection application doesn't understand this, then it can result in false alarms being raised and such events damage customer relations. We developed a technique to capture the evolution in a customer's calling behavior which helps solve this problem. First we calculate the deviations in the customers calling behavior for the most recent past 4 months, i.e. deviations from month 1, 2, 3 and 4. These would make up the historical behavioral profile of the customer, besides this we set a 2-3 weeks (depending on customer class segment) time window for the current activity period that would be a representation of the customer's current calling behavior. Now we can analyze the change in customer's calling behavior with

respect to their change in behavior and calculate their behavioral evolution. Certain changes like a promotion or change in economic status would die down as the event enters the historical profile from the current behavior window, this happens because we only capture the deviation a person has made form his normal behavior, and in case of an event like a promotion (or any other form of behavioral evolution) the future deviations would be low as the future behavior would conform to the current one, in this case deviations would drop and averages in general will rise for that customer. Figure 1 explains how a normal customer evolves with time as compared to fraudulent customer in figure 2.

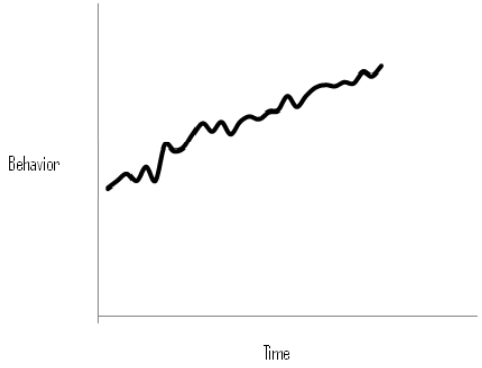

Figure 1: Non-Fraudulent Customer Evolution.

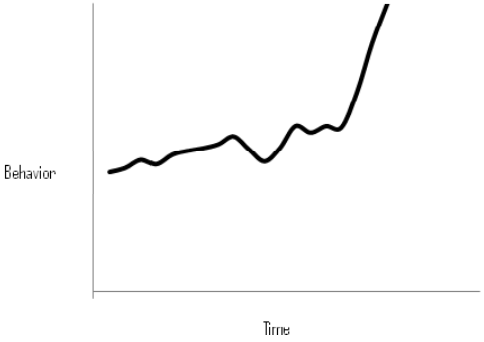

Figure 2: Fraudulent Customer Evolution.

C. Fraud Profile

There are many candidates that could add up to the fraud profile being constructed, in general average international calls deviation and average number of text messages deviation are good indicators of fraudulent behavior. Telecom operators are subjected to different types of fraud, those offering unrestricted calling packages are often subjected to fraud that occurs in a relatively longer period of time then those offering restricted packages in terms of credit limit. Different features of the fraud profile can be calculated to represent averages, distinct event counts, deviations and means etc. A combination of these then serves as a model for the appropriate fraud to be detected. Omitting a feature is a delicate choice and should be made after thorough analysis of the test dataset. Supervised neural networks have the weakness of only identifying fraud they have been seen and making predictions on new types of fraud is not trivial for supervised networks.

A central repository of CDRs (Call Detail Records) can be constructed. CDRs contain information about all the calls made by subscribers, their duration, location etc. The repository can then be used to calculate certain summarized features for individual callers; the summarization is done so a feature represents a certain behavior over a period of time. Once these features have been calculated they can be used to construct a fraudulent profile. The fraud profiles we constructed consisted of two parts, current and historical. These together were used to calculate the individual customer evolution and were allotted evolution points based on the analysis.

D. Training

For training the neural network, 107,050 call detail records from 300 unique callers was used. Among the 300 callers 75 were established as fraudsters. The test data used contained historical data of customers for up to 4 months, and deviation in customers calling behavior was calculated for each month along with the current behavior, the evolution points served as a distinction between normal evolution and anomalies. All the fraud cases were associated a fraud rating depending on the evolution points, anomalies were associated higher fraud rating than those with normal evolution.

The dataset of 107,050 call records was used to set up a data repository from which summarized features for individual callers were calculated. These summarized features consisted of values like standard deviation of average call duration per day etc, along with this historical profiles were constructed which contained features such as standard deviation of international calls for month 1, similarly for month 2, 3 and 4 [7].

E. ANN Architecture

The neural network we have developed consists of 14 input neurons, 5 hidden layer neuron and 1 output layer neuron, after regressive testing and analysis we established the fact that 5 served as the optimum number of neurons in the hidden layer, figure 4 elaborates on the results of the tests we conducted. To accommodate the facility to chose a different set of features to represent fraud, the input layer was designed such so that each neuron could be associated with a feature and then the number of features could determine the number of neurons in the input layer. Here the user was given privilege to give priorities to certain features over other, in the application backend the respective weight of the neuron was given more weight age and that neuron followed a slightly different weight adjustment mechanism. The weight adjustment function used is given in equation (1)

$$Wnew = Wold + JJ * \partial * dfi(e)/de * Xi \quad (1)$$

Where JJ represents the learning rate, & the error generated at the output neuron, f(e) the activation function and xi is the current input. The activation function used was sigmoid function

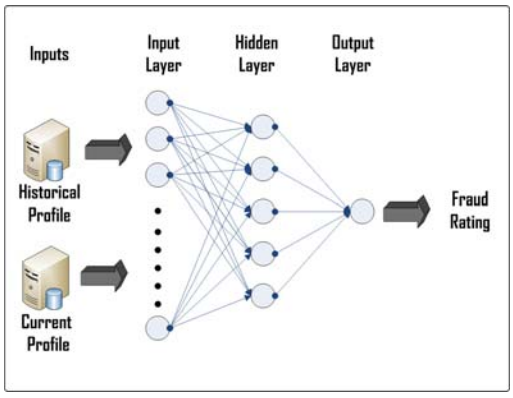

Figure 3: ANN architecture

To increase the confidence in the network's prediction, we analyzed the fraud ratings predicted by the network against the customer evolution points. The relation suggested that subtracting the value of the fraud rating from the evolution points gave the confidence in prediction. Each record was assigned a fraud flag, records with a high confidence in prediction (very likely to commit fraud) had their fraud flag raised, these were the most likely to commit fraud [8].

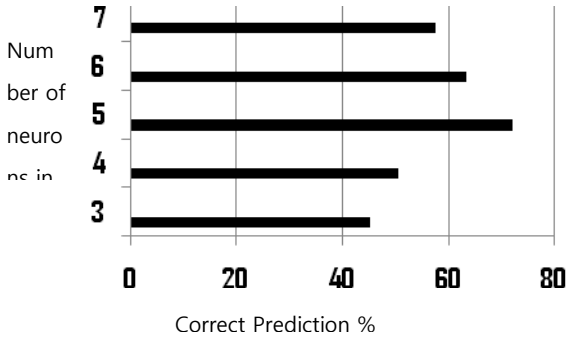

Figure 3: Performance comparison of different number of neurons in ANN architecture

IV. EXPERIMENTATION

Currently the neural network developed consists of a multilayer perceptron with one output neuron, however we are working on a prototype that consists of two output neurons and has a slightly different network architecture. The current neural network uses a single threshold value and adjusts the weights of the network based on the error in the prediction, what we think can add up to the network's prediction success is the fact that the neural network trains itself on fraud and non fraud cases in a slightly different way, that is, two output neurons can be used in place of one. One to detect fraud and the other to detect non fraud, both have different threshold values and the error generated by one test case can be different at both the output neurons, to reduce the impact of weight adjustment of one output neuron on the other can be catered by holding a different weight set for each output neuron and adjusting the respective weights according to the error at that output neuron in case the output produces an error. The idea here is not to completely isolate the weights of one neuron from the other, then the basic advantage of using two output neurons is completely lost, thus the input layer contains only a single layer of weights that serves both the output neurons.

V. CONCLUSION & FUTURE WORK

Neural networks are fast becoming a reliable way to detect fraud. Pakistan Telecom industry needs to accommodate these applications to optimize their costs and profits, though every operator needs to develop their own detection model and framework, generic applications can be developed that conceptualize fraud

in a broader sense. We are currently working on such problems and hope to come up with realistic solutions.

REFERENCES

[1] PTA, Telecom Indicators- Mobile Cellular Services, (Wednesday, 23 December 2009), <http://www.pta.gov.pk>, (visited Friday, 1 January 2010).

[2] M. Arif, M. Rab, A. Rehman, W. Hassan, M. Riaz, " Pakistan Telecommunication Annual Report 2008-2009" Chapter 4 - Mobile Cellular Services. Pakistan Telecommunication Authority: Ministry Of Information, Government of Pakistan.

[3] Y. Moreau, E. Lerouge, H. Verrelst, J. Vandewalle, C. Stormann, P. Burge, "A hybrid system for fraud detection in mobile communications", ESANN'1999 proceedings, pp. 447-454.

[4] P. Barson, S. Field, N. Davey, G. McAskie, and
R. Frank. The detection of fraud in mobile phone networks. Neural Network World, 6(4):477–484, 1996.

[5] Y. Moreau, H. Verrelst, and J. Vandewalle. Detection of mobile phone fraud using supervised neural networks: A first prototype. In International Conference on Artificial Neural Networks Proceedings (ICANN'97), pages 1065–1070, October 1997.

[6] C.Hilas and J.Sahalos , 'User profiling for fraud detection in telecommunication networks', 5th International Conference on Technology and Automation, Thessaloniki, Greece, 2005.

[7] P. Ferreira, O. Belo, R. Alves, and L. Cortesao. Establishing fraud detection patterns based on signatures. In Proceedings of the 7th Industrial Conference on Data Mining, Leipzig - Germany, 2006.

[8] S. Wu, N. Kang, L. Yang, "Fraudulent Behavior Forecast in Telecom Industry Based on Data Mining Technology" Communications of the IIMA 2007, Volume 7 Issue 4, pp. 201-6.

[9] S. Wu, N. Kang, L. Yang, "Fraudulent Behavior Forecast in Telecom Industry Based on Data Mining Technology" , Communications of the IIMA, 2007

[10] A.J. Hussain and E. Chew, "Data Mining and Telecommunication Fraud Detection Using Artificial Neural Networks," 9th International Workshop on Systems, Signals and Image Processing, IWSSIP'02, Manchester, UK

[11] W. Xu, Y. Pang, J. Ma, S. Wang, G. Hao, S. Zeng, Y. Qain, " Fraud detection in telecommunication: a rough fuzzy set based approach", International Conference of Machine Learning and Cybernetics, 1249 - 1253, 2008.