Detecting SIM Box Fraud Using Neural Network

Chapter · January 2013

DOI: 10.1007/978-94-007-5860-5_69

10 authors, including:

Hussein Abdikarim

2 PUBLICATIONS **21** CITATIONS

SEE PROFILE

Haashi Elmi

BPP University College

3 PUBLICATIONS **38** CITATIONS

SEE PROFILE

Subariah Ibrahim

Universiti Teknologi Malaysia

52 PUBLICATIONS **718** CITATIONS

SEE PROFILE

Roselina Sallehuddin

Universiti Teknologi Malaysia

126 PUBLICATIONS **991** CITATIONS

SEE PROFILE

Detecting SIM Box Fraud Using Neural Network

Abdikarim Hussein Elmi, Subariah Ibrahim and Roselina Sallehuddin

Abstract One of the most severe threats to revenue and quality of service in telecom providers is fraud. The advent of new technologies has provided fraudsters new techniques to commit fraud. SIM box fraud is one of such fraud that has emerged with the use of VOIP technologies. In this work, a total of nine features found to be useful in identifying SIM box fraud subscriber are derived from the attributes of the Customer Database Record (CDR). Artificial Neural Networks (ANN) has shown promising solutions in classification problems due to their generalization capabilities. Therefore, supervised learning method was applied using Multi layer perceptron (MLP) as a classifier. Dataset obtained from real mobile communication company was used for the experiments. ANN had shown classification accuracy of 98.71 %.

Keywords Multi layer perceptron · SIM box fraud · Classification · Telecom fraud

A. H. Elmi (✉) · S. Ibrahim · R. Sallehuddin
Faculty of Computer Science and Information System, Universiti Teknologi Malaysia, 81300 Skudai, Johor, Malaysia
e-mail: sirabdikarim@yahoo.com

S. Ibrahim
e-mail: subariah@utm.my

R. Sallehuddin
e-mail: roselina@utm.my

K. J. Kim and K.-Y. Chung (eds.), *IT Convergence and Security 2012*,
Lecture Notes in Electrical Engineering 215, DOI: 10.1007/978-94-007-5860-5_69,

1 Introduction

The theft of service and misuse of voice as well as data networks of telecom providers is considered as fraud. The perpetrator's intention could be to avoid the service charges completely or reduce the charges that would have been charged for the service used. The intention could also be deeper than that and the fraudster's aim might be to gain profit by misusing the network of the provider [1]. Losses due to fraud in telecom industry are highly significant.

Even though telecommunication industry suffers major losses due to fraud there is no comprehensive published research on this area mainly due to lack of publicly available data to perform experiments on. The data to be used for the experiments contains confidential information of customers and in most cases law and enforcement authorities prohibit exposing the confidential information of customers [2]. On the other hand, any broad research published publicly about fraud detection methods will be utilized by fraudsters to evade from detection [1, 3]. Existing research work is mainly focusing on subscription and superimposed types of fraud which are the dominant types of fraud in telecom industries worldwide. However, another type of fraud called SIM box bypass fraud has become a challenging threat to telecom companies in some parts of Africa and Asia. The success of this fraud depends on obtaining SIM cards. Therefore the effects of SIM box bypass fraud vary across countries. In countries where unregistered SIM cards are not allowed and the government laws recognize the SIM box devices as illegal equipment, the effect is less compared to countries where obtaining of SIM cards by customers is very cheap or even free and government laws do not prohibit unregistered subscribers. The fact that this type of fraud is not a problem for all telecom companies worldwide might justify the reason why the publicly available research on this type of fraud is very limited.

SIM box' fraud takes place when individuals or organizations buy thousands of SIM cards offering free or low cost calls to mobile numbers. The SIM cards are used to channel national or international calls away from mobile network operators and deliver them as local calls, costing operators' millions in revenue loss [4, 5]. A SIM box is VoIP gateway device that maps the call from VoIP to a SIM card (in the SIM box) of the same mobile operator of the destination mobile [5].

In this paper we present a study on which set of descriptors that can be used to detect SIM cards originating from SIM box devices have been identified. Neural Networks are promising solutions to this type of problem as they can learn complex patterns and trends within a noisy data. Neural networks have particularly shown better performance results than other techniques in the domain of telecom fraud. Therefore, supervised learning method was applied using Multi layer perceptron (MLP) as a classifier. The dataset that was used for this study is obtained from a real mobile communication network and contains subscribers/SIM cards that have been tested and approved by the operator to be SIM box fraud SIM cards and normal SIM cards. The next section describes the dataset and descriptors used.

Section 2 discusses the method applied and Sect. 3 presents the results obtained from the experiments. Last section concludes the work.

1.1 Dataset and Descriptors

The huge volumes of data stored by telecommunication companies include Customer Data Record (CDR) which is the database that stores the call information of each subscriber. Whenever a subscriber makes a call over the operator's network a toll ticket is prepared which contains complete information of the call made including the subscriber id, the called number, duration of the call, time, destination location etc. In this fraud scenario the CDR database serves a suitable source of information where useful knowledge about callers can be extracted to identify fraudulent calls made by subscribers.

This study is based on Global Systems for mobile communications (GSM) network and specifically the Customer Data Record (CDR) database of prepaid subscribers. The dataset used for the experiments contained 234,324 calls made by 6415 subscribers from one Cell-ID. The dataset consisted of 2126 fraud subscribers and 4289 normal subscribers which is equivalent to 66.86 % of legitimate subscribers and 33.14 % of SIM box fraud subscribers. The total duration of these call transactions was two months.

A Total of 9 features have been identified to be useful in detecting SIM box fraud. Table 1 shows the list of these features and their description.

Table 1 Selected descriptors

Field Name	Description
Call sub	This is the subscriber identity module (SIM) number which was used as the identity field
Total calls	This feature is derived from counting the **total calls** made by each subscriber on a single day
Total numbers called	This feature is the total different unique subscribers called by the customer (subscriber) on a single day
Total minutes	Total duration of all calls made by the subscriber in minutes on a single day
Total night calls	The total calls made by the subscriber during the midnight (12:00 to 5:00 am) on a single day
Total numbers called at night	The total different unique subscribers called during the midnight (12:00 to 5:00 am) on a single day
Total minutes at night	The total duration of all calls made by the subscriber in minutes at midnight (12:00 to 5:00 am)
Total incoming	Total number of calls received by the subscriber on a single day
Called numbers to total calls ratio	This is the ratio of the **total numbers called/total calls**
Average minutes	The is the average call duration of each subscriber

2 Materials and Methods

Neural Network is a group of simulated neurons interconnected to represent a computation mathematical model that can take one or more inputs to produce an output by learning the complex relationships between the inputs and outputs [6]. Supervised learning requires an input pattern along with the associated output values which is given by an external supervisor [7, 8].

2.1 Multi Layer Perceptron

Feed Forward Neural Network contains neurons and edges that form a network. The neurons are set of nodes and are of three types: input, hidden and output. Each node is a unit of processing. The edges are the links between two nodes and they have associated weights [8]. In Multi layer perceptron the network consists of multiple layers of computational units, usually connected in a feed-forward way. Each neuron in one layer has direct connections to the neurons of the subsequent layer although not to other nodes in the same layer. There might be more than one hidden layer [9, 10].

A neuron has a number of inputs and one output. It combines all the input values (Combination), does certain calculations, and then triggers an output value (activation) [8, 11]. There are different ways to combine inputs. One of the most popular methods is the weighted sum, meaning that the sum of each input value is multiplied by its associated weight. Therefore, for a given node g we have:

$$Net_g = \sum w_{ij} x_{ij_1} = w_{0j} x_{0j} + w_{1j} x_{1j} + \cdots . w_{ij} x_{ij} \tag{1}$$

where x_{ij} represents the i'th input to node j, w_{ij} represents the weight associated with the i'th input to node j and there are $I + 1$ inputs to node j.

The value obtained from the combination function is passed to non-linear activation function as input. One of the most common activation functions used by Neural Network is the sigmoid function. This is a nonlinear functions and result in nonlinear behaviour. Sigmoid function is used in this study. Following is definitions of sigmoid function:

$$\text{Sigmoid} = \frac{1}{1 + e^{-x}} \tag{2}$$

where x is the input value and **e** is base of natural logarithms, equal to about 2.718281828. The output value from this activation function is then passed along the connection to the connected nodes in the next layer.

Back-propagation algorithm is a commonly used supervised algorithm to train feed-forward networks. The whole purpose of neural network training is to minimize the training errors.

Equation 3 gives one of the common methods for calculating the error for neurons at the output layer using the derivative of the logistic function:

$$Err = O_1(1 - O_1)(T_i - O_1) \tag{3}$$

In this case, Oi is the output of the output neuron unit i, and T_i is the actual value for this output neuron based on the training sample. The error calculation of the hidden neurons is based on the errors of the neurons in the subsequent layers and the associated weights as shown in Eq. 4.

$$Err_i = O_i(1 - O_i)\sum_j Err_i W_{ij} \tag{4}$$

O_i is the output of the hidden neuron unit I, which has j outputs to the subsequent layer. Err_j is the error of neuron unit j, and W_{ij} is the weight between these two neurons. After the error of each neuron is calculated, the next step is to adjust the weights in the network accordingly using Eq. 5.

$$W_{ij,new} = W_{ij} + l * Err_j * O_i \tag{5}$$

Here l, is value ranging from 0 to 1. The variable $\boldsymbol{l}$ is called learning rate. If the value of $\boldsymbol{l}$ is smaller, the changes on the weights get smaller after each iteration, signifying slower learning rates.

To obtain the best Neural Network architecture for this research, four parameters settings were considered. The number of hidden layers in the network architecture as well as the number of neurons in each hidden layer is considered. The learning rate and momentum parameters which have significant effect on the performance of any neural network architecture are also considered.

Three architectures of neural network were considered in this research; one, two and three hidden layers and 5, 9 and 18 hidden nodes in each hidden layer. The learning rate is a constant chosen to help the network weights move toward a global minimum of Sum Square Error (SSE). Therefore, in this research four values of learning rate are considered: 0.1, 0.3, 0.6 and 0.9. The back-propagation algorithm is made more powerful through the addition of a momentum term. Momentum helps in the early stages of the algorithms, by increasing the rate at which the weights approach the neighbourhood of optimality. Therefore, four values of momentum term are used in this study: 0.1, 0.3, 0.6 and 0.9.

3 Results and Discussions

This section discusses the results obtained in comparing the ANN models created to find the neural network architecture which provides the most reliable and accurate predictions. All possible combination of the parameter settings was experimented and as a result, 240 neural network models were created. The models were evaluated based on their prediction accuracy, generalization error, time taken

to build the model, precision and recall. 10—Fold cross-validation results of the models were compared.

Classification accuracy ranged from 56.1 to 98.71 %. It has been observed that the models show the worst performance results when both momentum and learning rate are increased to range of 0.6–0.9. The highest classification accuracy that could be achieved in these values was 86.16 % and the root mean square error was as high as 0.66. In all network layers; 3, 4, and 5, the overall accuracy degraded significantly when this range was used. This could be explained by the fact that higher values of learning rate and momentum could lead the algorithm to overshoot the optimal configuration.

Figure 1 compares the best classification accuracy of the three hidden layers experimented with respect to the learning rate parameter. When one and two hidden layers are used, the accuracy degrades as the learning rate is increased from 0.1 to 0.3. But accuracy again increases until the learning rate is 0.6 where it starts to decline dramatically if further increased. However, when three hidden layers are used, the accuracy increases as the learning rate is increased from 0.1 to 0.6 and then the accuracy declines if the learning rate is increased from this point.

The highest accuracy was achieved when two hidden layers were used at a learning rate of 0.6. Another observation shown by the graph is that the classification accuracy for all hidden layers decreases as the learning rate is increased from 0.6 to 0.9.

Figure 1 also compares the classification accuracy of all hidden layers with respect to momentum term. From the figure, it can be clearly seen that hidden layer 2 at a momentum of 0.3 shows the best performance. The performance also degrades after the momentum of 0.3 for two and three hidden layers. The classification accuracy degrades significantly for all hidden layers at a momentum of 0.9.

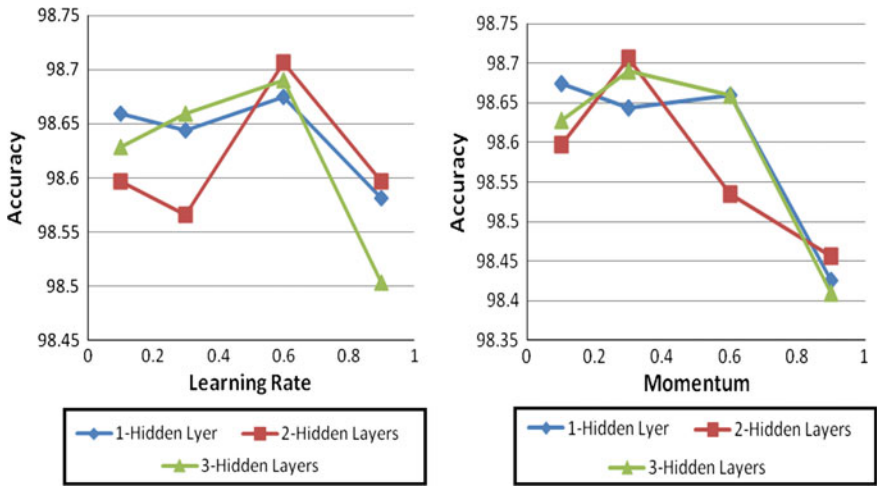

Fig. 1 Accuracy against learning rate and momentum for all hidden layers

Table 2 Confusion matrix of Selected ANN model

	Normal	Fraud
Normal	4269	20
Fraud	63	2063

Table 3 Results of the best ANN

	Best model
RMSE	0.10380
Accuracy	98.7061 %
Time	17.17
ROC area	0.997
Precision	0.987
Recall	0.987

Table 4 Parameter values of best ANN model

	Best model
Input layer nodes	9
Hidden layer 1 nodes	5
Hidden layer 2 nodes	5
Hidden layer 3 nodes	N
Output nodes	2
Learning rate	0.6
Momentum	0.3

The conclusion that can be made from these figures is that, very high learning and momentum rates significantly degrade the classification accuracy of the models. The best results are obtained when lower value of momentum is used with relatively higher value of learning rate.

From the analysis discussed in this section, the best results were obtained when two hidden layers each having five hidden neurons was used with learning rate of 0.6 and a momentum term of 0.3.

In the confusion matrix shown in Table 2, the columns represent the predicted values and rows represent the actual cases. The model was able to correctly classify 2063 out of the 2125 fraud subscribers and 4269 out of the 4289 normal subscribers. Fraud is the negative target value, false negative count is 63 and false positive count is only 20. Table 3 shows performance results of the best model and Table 4 shows the parameter values used in this model.

4 Conclusions

The focus of this work was to come up with a set of features that can be used to effectively identify SIM cards originating from SIM box devices and an algorithm that can classify subscribers with high accuracy. The learning potentials of neural

network for the detection of SIM box fraud subscribers were investigated. The experimental results revealed that ANN has high classification accuracy. SVM has recently found considerable attention in classification problems due to its generalization capabilities and less computational power. In future work SVM will also be investigated and compared with ANN.

Acknowledgments The authors first thank the anonymous reviewers for their valuable comments and to Universiti Teknologi Malaysia (UTM) for the FRGS Grant Vote number 4F086 that is sponsored by Ministry of Higher Education (MOHE) and Research Management Centre, Universiti Teknologi Malaysia, Skudai, Johor.

References

1. Taniguchi M, Haft M, Hollmen J, Tresp V (1998) Fraud detection in communications networks using neural and probabilistic methods. In: Proceedings of the 1998 IEEE international conference on acoustics speech and signal processing, vol 2. IEEE, Los Alamitos, pp 1241–1244
2. Hilas C, Mastorocostas P (2008) An application of supervised and unsupervised learning approaches to telecommunications fraud detection. Knowl Based Syst 21(7):721–726
3. Azgomi NL (2009) A taxonomy of frauds and fraud detection techniques. In: Proceedings of CISTM 2009, Ghaziabad, India, pp 256–267
4. Telenor GS (2010) Global SIM box detection
5. Nokia Siemens Neworks Corporation (2008). Battling illegal call operations with fraud management systems
6. Larose DT (2005) Discovering knowledge in data. John Wiley and Sons, Inc., Hoboken
7. Ghosh M (2010) Telecoms fraud. Comput Fraud Secur 2010(7):14–17
8. MacLennan J (2009) Data mining with Microsoft SQL Server 2008. Wiley Publishing Inc, Indianapolis
9. Mark EM, Venkayala S (2007) Java data mining strategy, standard, and practice. Diane Cerra, San Francisco
10. Cortesao L, Martins F, Rosa A, Carvalho P (2005) Fraud management systems in telecommunications: a practical approach. In: Proceeding of ICT, 2005
11. Pablo A, Este′vez CM, Claudio AP (2005) Subscription fraud prevention in telecommunications using fuzzy rules and neural networks. In: Proceedings of the expert systems with applications. Santiago, Chile, 2005
12. Hilas C, Mastorocostas P (2008) An application of supervised and unsupervised learning approaches to telecommunications fraud detection. Knowl Based Syst 21(7):721–726