Fuzzy Logic Application for Fraud Management System

Muhammad Daud Nurdin[1] **Hendrawan**[2] **Andriyan Bayu Suksmono**[3]
School of Electrical Engineering and Informatics, Institut Teknologi Bandung
E-mail: 1) syechdaud@yahoo.com 2) hend@telecom.ee.itb.ac.id 3) suksmono@yahoo.com

Abstract – **Telecommunications fraud has been one of the big problems in telecommunication services. Therefore, various of methods are used to detect it, such as using neural network to detect fraud with analyzing customer's usage profile. However, usage profile does not always represent the fraud absolutely. On this paper, authors offer the fuzzy logic for further analysis against indications of fraud which is produced by neural network, with refer to administration profile, payment history, usage data, and others special records. The experiments show satisfaction results.**

Keywords*: cellular communications, telecommunications fraud, fraud management, fraud detection, neural network, fuzzy logic.*

I. INTRODUCTION

One of the problems in telecommunication services which is crucial is the fraud. There are as many definitions of telecommunications fraud as there are fraud managers employed in the industry. However, there does seem to be a general consensus that telecom fraud, as the term is generally applied, involves the theft of services or deliberate abuse of voice and data networks. Furthermore, it is accepted that in these cases the perpetrator's intention is to completely avoid or at least reduce the charges that would legitimately have been charged for the services used. On occasion, this avoidance of call charges will be achieved through the use of deception in order to fool billing and customer care systems into invoicing the wrong party.[6]

Telecommunications fraud has been identified as the single biggest cause of revenue loss for telecommunications providers, with figures averaging between 3 and 5 percent of an operator's annual revenue. Current statistics point to a global loss of USD 55 billion per year, making telecommunications fraud a bigger business than international drug trafficking.[6]

Authors have done a research while analyze the data that was gotten from a operator of cellular communication in Indonesia. Data which was gotten and analyzed is postpaid GSM only. Therefore, the researches of fraud on this paper are focus on that communications cellular.

One of the methods which are used to detect fraud is implementation of neural network, which is analysis of usage profile which is gotten or built from CDR (call detail record). However, usage profile does not always represent the fraud absolutely. Sometime, there is customer who has usage profile which is indicated fraud, but he did not do a fraud. On other hand, there is customer has common usage profile but he was not intent to pay early. He was included in backlist instead.

Authors designed the system using fuzzy logic to analyze further against the indications of fraud which is produced by neural network in order that is fraud or not fraud can be decided decisively. In this case, authors do not explain about detection using neural network.

II. TYPES OF TELECOMMUNICATIONS FRAUD

Usually, the user's aim to do the fraud can be classified into two categories. The first, *revenue based* that is fraud action with purpose to get the financial advantages. The example for this type of fraud is *call selling*, i.e. fraudster provides service for others people with low tariff.

The second, *non-revenue based* that is fraud action without purpose to get the financial advantages. Some of this fraudster's motivation are getting prestige among fraudsters, looking for satisfactions and challenges to find weakness of a system and procedure, and revenging a corporation with manner breaking it financially or making its reputation to be bad.

Generally, telecommunications fraud (especially which often occur in Indonesia) based on when it occurs, can be classified into three groups. The first group is fraud which occur when the user register to be a customer. This group includes *subscription fraud*. The second group is fraud which occur when the user using the telecommunication services. These groups include *call selling*, *SIM cloning*, *ghosting*, and *surfing*. And the third group is frauds which occur after the user using the telecommunication services and when he will be asked to pay the billing. This group includes *payment evasion*.

II.1. SUBSCRIPTION

Perpetrators of this fraud apply for a service and once activated, immediately use it for national and international calls with no intention to pay for the calls made. Usually, fraudsters begin their action by applying to be a customer with using false identity and manipulate administration data at an application form.

II.2. CALL SELLING

The perpetrators sell service to others. Services are usually sold cheaper than the legal telecommunications shop. But, the perpetrators never pay the bill to provider. They will runaway from responsibility for paying. In action, they sometime make Call Forwarding mechanism to do.

II.3. GHOSTING

The fraudsters make the usage data on provider disappear. It can be they do with help of a person in a certain capacity. Also they can do it by using technology to make calls across network by deceiving the record system (e.g. billing system). Therefore, there are several calls that are disappearing from CDR or the usage of

service to be low. Sometime the fraudster also involve insider to erase data.

II.4. SURFING

Surfing is basically a service stealing. Service stealing usually happens when someone's handset or SIM card was stolen, or used without being known by the owner.

II.5. SIM CLONING

Cloning is the process of replicating an existing customer's hardware or firmware, allowing calls to be made on their account. The legitimate customer will not become aware of the deception until they receive an inflated bill at the end of the month and so cloned phones are often sold with a 30 day guarantee.

II.6. PAYMENT EVASION

Customer avoids from obligation of bill. This type of fraud might be difficultly differed to *bad debt* – customer can not pay the bill because bankrupt.

III. FRAUD MANAGEMENT

Fraud management is a very general issue, which we can define as including the following: [4]

- *Fraud prevention*: the enforcement of strict access and usage controls to ensure that fraud cannot take place.
- *Fraud detection*: real-time or non-real-time observation of indicators (mainly service usage metrics) and determination of whether fraud is taking place or has taken place. This usually triggers some action, such as blocking access to the service or generation of a notification.
- *Fraud reduction*: recognizing that fraud prevention is almost impossible in practice, ensuring that it happens rarely and that its effects are minimized. This usually requires real-time detection.

Among of them, fraud detection is a popular issue and interesting many researchers. Commonly, fraud detection system is designed based on artificial intelligence such as: Genetic Algorithms, Neural Networks, Rule Induction, Fuzzy Logic, Expert Systems, and Regression Analysis.

Fraud Management System which is offered by our research is shown by Figure 1 below.

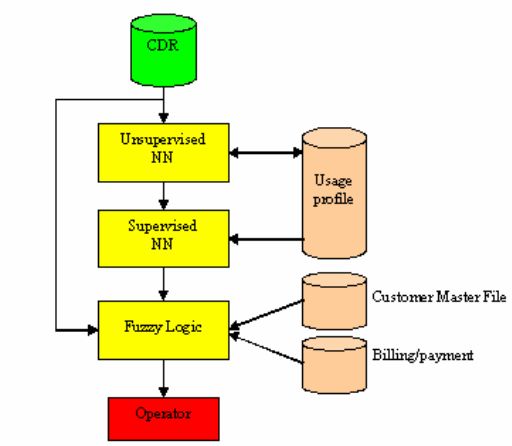

Figure 1. Design of Fraud Management System

System uses two types of artificial intelligence that are neural network (NN) and fuzzy logic. It consists of three parts that are *Unsupervised NN*, *Supervised NN*, and *Fuzzy Logic*. Unsupervised NN makes the usage profiles of users; Supervised NN uses the profile for detecting user which is indicated to do fraud. Than, Fuzzy Logic makes decision whether fraud based on rules which are applied to it by considering other aspects. Those aspects consist of administration data, history payment, white list, hot list, etc.

IV. FRAUD DETECTION USING FUZZY LOGIC

Fuzzy logic which is used here is of fuzzy inference system (FIS) with Mamdani method. Overall system was designed while consider to characteristics of fraud that was described above. System was intended to detect five types of frauds that are subscription, call selling, ghosting, surfing, dan SIM cloning.

IV.1. MEMBERSHIP FUNCTIONS OF INPUTS AND OUTPUTS

System was built using 12 input variables and 5 output variables. The input variables and its membership functions respectively are Indication of Call Selling (HIGH, MEDIUM, LOW), Indication of Ghosting (HIGH, MEDIUM, LOW), Indication of SIM Cloning (HIGH, MEDIUM, LOW), Indication of Surfing (HIGH, MEDIUM, LOW), Value Ratio (UP, CONSTANT, DOWN), Class of Economy (LOW, MEDIUM, HIGH), Customer Status (NO, INPROCESS, YES), Customer Risk (LOW, MEDIUM, HIGH), Black List (YES/NO), Validation of ID (VALID/NOT), White List (YES/NO), and Payment History (BAD, ENOUGH, GOOD).

The output variables and its membership functions respectively are Call Selling (FRAUD/NOT), Ghosting (FRAUD/NOT), SIM Cloning (FRAUD/NOT), Surfing (FRAUD/NOT), and Subscription (FRAUD/NOT).

Some of curves of the membership functions are shown in figures below.

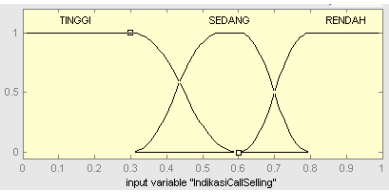

Figure 2. One of input variable: Indication of Call Selling

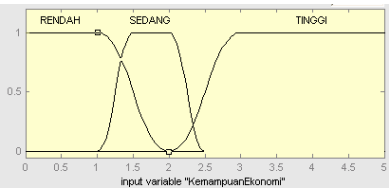

Figure 3. One of input variable: Class of Economy

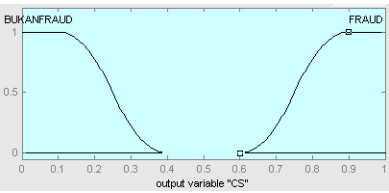

Figure 4. One of output variable: Call Selling

IV.2. PRE-PROCESSING

Input data for fuzzy logic must be numerical format and in a typical range. Therefore, it is required pre-processing to many of types of data, such as CDR, customers master file, and payment history.

Some of the pre-processing are introduced below. Customer Status was changed to numeric (0 for no data, 0.5 for in process, 1 for data OK). The list of customers in blocked (Black List) was changed to numeric (0 for NO, 1 for YES). The list of customers with good track record (White List) was changed to numeric (0 for NO, 1 for YES). Class of Economy field of CMF was prepared to be processed. Customer Risk was made numeric based on customer data (age, education, occupation, etc.).

IV.3. RULES

Making the rules for fuzzy inference system is an important session of this system. This is for getting sense of system which is sensitive and appropriate. Thus, decision making of fraud or not can be done accurately.

There are 29 rules in this system. Some of them are written below. If (CustomerStatus is NO) then (Subscription is FRAUD). If (IndicationOfCallSelling is HIGH) and (ClassOfEconomy is LOW) then (CallSelling is FRAUD). If (IndicationOfCallSelling is LOW) and (BlackList is YES) then (CallSelling is FRAUD). If (IndicationOfSurfing is MEDIUM) and (ValidationOfID is not VALID) then (Subscription is FRAUD). If (IndicationOfSIMCloning is LOW) and (ValueRatio is HIGH) then (SIMCloning is FRAUD).

V. RESULT OF SIMULATION

Fuzzy logic require many of type and complicated data, that are CDR, CMF, White List, Black List, and Payment History. Also, these data require pre-processing to be input for fuzzy logic. Some of the data have been gotten authors from operator. Because of others data are not available and pre-processing program is in making process; authors use dummy data for running system.

Experiments show using fuzzy logic has made positive change in analysis of indication of fraud which is given by neural network. A typical data record which was tested is given below.

Table 1. A typical record of data for FIS input

No.	Input Variable	Value	Note
1.	IndicationOfCallSelling	0.5	MEDIUM
2.	IndicationOfGhosting	0.9	LOW
3.	IndicationOfSIMCloning	0.8	LOW
4.	IndicationOfSurfing	0.85	LOW
5.	ValueRatio	3.5	HIGH
6.	ClassOfEconomy	1 million	LOW
7.	CustomerStatus	1	YES
8.	CustomerRisk	0.5	MEDIUM
9.	BlackList	0	NO
10.	ValidationOfID	1	VALID
11.	PaymentHistory	0.5	MEDIUM
12.	WhiteList	0	NOT

Table 2. A typical record of data for FIS output

No.	Output Variable	Value	Note
1.	CallSelling	0.7	FRAUD
2.	Ghosting	0	Not FRAUD
3.	SIMCloning	0	Not FRAUD
4.	Shurfing	0	Not FRAUD
5.	Subscription	0	Not FRAUD

VI. CONCLUSION AND FUTURE WORK

One of the problems in telecommunication services which is crucial is the fraud. Fraud has caused big loss of operator's revenue and others to its stakeholder. Therefore, it is required a system to detect fraud, such as avoid bigger disadvantage. The system is called fraud management system. The frauds which are researched by authors are *call selling*, *surfing*, *ghosting*, *SIM cloning*, and *subscription*.

Based on research, authors design a comprehensive fraud management system considering aspects: usage profile, administration profile, payment history, and others special records. System consists of three main blocks that are *unsupervised neural network, supervised neural network*, and *fuzzy logic*. Here, authors were only to describe and design *fuzzy logic* subsystem. Fuzzy logic

was effective to consider several of aspect related to fraud. Thus, decision making of fraud or not can be done accurately.

There are some works for the future, such as making the user interface for running system and making the pre-processing program which can read all data from others devices. In the real application, we need system can run faster. Hence, we need the lower language to apply the system.

ACKNOWLEDGEMENT

This research is funded by ITB Research Grant no. 0076/K01.03/PL2.1.5/UI/2005. The authors would like to thank them.

REFERENCES

[1] David Lloyd. 2003. *International Roaming Fraud Trends & Prevention Techniques.* Fair Isaac Corporation.

[2] Jaakko Hollm´en. 2000. *User profiling and classification for fraud detection in mobile communications networks*. Dissertation. Helsinki University of Technology.

[3] Jyh-Shing Roger Jang, Chuen-Tsai Sun, dan Eiji Mizumi. 1997. *Neuro-Fuzzy and Soft Computing.* Prentice-Hall International, Inc.

[4] Jimmy McGibney & Seán Hearne. 2003. *An Approach to Rules based Fraud Management in Emerging Converged Networks.* Waterford Institute of Technology, Ireland.

[5] Longbing Cao, Chao Luo, Dan Luo, Chengqi Zhang. 2004. *Hybrid Strategy of Analysis and Control of Telecommunications Frauds.* Proceedings of the 2nd International Conference on Information Technology for Application (ICITA 2004).

[6] Riaan Jacobs. 2003. *Telecommunications Fraud, The Single Biggest Cause of Revenue Loss for Telecommunications Providers.* Dimension Data Service Provider Solutions (SPS).

[7] Richard Derrig. 2002. *The Merging of Neural Networks, Fuzzy Logic, and Genetic Algorithms*. Insurance Fraud Bureau of Massachusetts.

[8] Richard J. Bolton and David J. Hand. 2002. *Statistical Fraud Detection: A Review.* Imperial College.

[9] Sri Kusumadewi. 2002. *Analisis & Desain Sistem Fuzzy Menggunakan Toolbox Matlab.* Yogyakarta: Graha Ilmu.

[10] The MathWorks. *Fuzzy Logic Toolbox For Use with MATLAB®*. User Guide's. Version 2.