# Telecommunication Fraud and Detection Techniques: A Review

Neha Bhullar
Assistant Professor, ECE
PEC University of Technology
Chandigarh, India
*neha_bhardwaj20@yahoo.com, neha.bhullar@pec.ac.in*

***Abstract***— Fraud is one of the major concerns in Telecommunication industry. Due to dramatic increase in number of frauds which accounts for high revenue loss to the government, many fraud detection techniques have evolved recently. The intent of the paper is to review different kinds of frauds and corresponding detection techniques.

***Keywords-*** *Fraud, Genetic Algorithm, Neural Network, Fraud Detection*

*****

## I. INTRODUCTION

The unscrupulous use of telecommunication facilities or services provided by the telecom operators is termed as telecommunication fraud.

Detecting a fraud is important as the operator and government has to face a huge revenue loss .Due to the increase in the fraud now days, special security features has to be incorporated to overcome this situation.

Various techniques have been devised to identify and then to rectify the frauds in this paper, various kinds of frauds have been discusses and the proposed way to rectify them has been given.

## II. LITERATURE SURVEY

Telecom operators are prone to various kinds of frauds. A fraud is costly to the network carrier as network capacity is wasted and also revenue loss occurs [8] some of the frauds are listed below:

### 1. Subscription Fraud

Sameer Qayyum et al. has described subscription fraud as the most common fraud encountered by GSM [1].In this, fraudster misuses the services by changing some of his personal information and has no intent to pay the bill[2].

The author has deployed machine learning techniques to overcome this issue.

### 2. Cloning

Cloning Fraud facilitates making calls and other services using other person's subscription .Cloning facilitates the fraudster in a way that he does not have to pay the bill [2][9].A smart card reader connected to a computer is used to read the information on SIM card to be cloned to an empty SIM card. RJ Frank et al. [7] stated that even sometimes the software deployed to depict fraud can also have a colon so intelligent methods have to be incorporated to overcome this threat.

Ogundile O.O. [2] has proposed the registration of SIM card as an intuitive way to overcome this kind of fraud.

### 3. Roaming Fraud

Gabriel Macia et al. [3] has described Roaming Fraud as the ability of the subscribers of a mobile network (HPMN-Home Public Mobile Network) to use remotely the services of such a network by accessing it through a different network (VPMN, i.e., visited public mobile network).

This kind of fraud can be overcome at an earlier stage if operators exchange roaming CDRs more often

### 4. Tumbling

Anita B.Desai et al. [4] described tumbling as use of fake serial numbers on cloned handsets so that the successive calls are attributed to different legitimate phones

This kind of fraud can be overcome by use of data mining techniques in neural nets.

### 5. Superimposed Fraud

Constantionos S.Hilas et al. [5] described superimposed fraud as a fraud in which the fraudster uses a legitimate user account in parallel with the authorized user. Such kind of frauds come into knowledge when the authorized users complaint about the excessive billing.

This fraud can be overcome by building a robust system to check the authenticity of users.

### 6. Call and SMS Spamming

Dr. Ian Howells et al. [6] has described call and SMS spamming as receiving fraudulent calls and messages like email spam. It is illegal to send messages or calls to the users who have not subscribed for that facility.

This fraud can be overcome by reporting the matter immediately to the operator.

### 7. Phishing

In this the fraudster simply tries to acquire the personal information like username, password and other sensitive information by posing as a legitimate company [6]

### 8. Surfing

Xerandy et al. [9] described Surfing as stealing of service. It usually occurs when someone's handset is stolen or is used by fraudster without the knowledge of the authorized user. Surfing is basically of two types:

Permanent Surfing: It can be defined as stealing of someone's mobile equipment or SIM card. The user is generally aware of this kind of Surfing.

Incident surfing: This type of surfing is generally not known by the user and is comparatively difficult to detect as the user himself is not aware of this fraud. Basically, it is a temporary feature in which fraudster is using the mobile phone for some malicious activities and is returning back to the subscriber.

### 9. Behavioural Fraud

Linda Delamaine et al. [10] described behavioral fraud as a fraud in which details of the legitimate SIM cards have been fraudulently obtained and sales are made of the same. Such kind of fraud can be overcome by proper verification of Number of SIM Card purchased from the operator company.

### 10. Application Fraud

Linda Delamaine et al. [10] described Application Fraud as a fraud in which a user applies for a mobile SIM Card with wrong or false information. To overcome such kinds of frauds, a management based system should be incorporated which can easily detect a fraudster and fake applications.

## III. Detection Techniques

Due to the rapid increase in frauds in telecommunication sector in recent years which results in heavy loss to the operators and government [4], several detection techniques to detect the fraud has evolved.

Fraud detection involves monitoring the behavior of subscribers to depict any variations from the behavior and to depict if any fraudulent activity has occurred. Few detection techniques are listed hereby:

### 1. Data Processing and Analysis Technique:

Xerandy et al. [9][12] stated that for this fraud detection technique, first of all the information will be collected depending on what kind of fraud is being monitored eg CDR Patterns of the subscribers will be taken from the operator ,location of the user in some cases [16][17]and the call patterns, location from where call is made, frequency of calling etc parameters would be studied and any deviation from such patterns can be termed as fraud. CDR details can be further described as:

a. MSISDN- SIM Card Number
b. B number-Mobile number of the called person
c. IMIE-International Mobile Equipment Identity
d. Duration of the call

### 2. User Profiling Techniques:

Xerandy [9] stated that to detect frauds using neural networks, supervised neural network is to be trained before it is assigned. In the training process, the neural net is trained with certain set of input parameters and then profiling will be done. There are two kinds of user profiling: Profiling to be analyzed and the reference profiling.

### 3. Prediction Techniques

The objective of fraud detection is to maximize the correct predictions and minimize the incorrect predictions to an acceptable level [11]. A Fault tolerant system based on neural net need to be designed to depict a particular kind of fraud correctly keeping into account the false alarm rate, fraud catching rate, false negative rate [8].

### 4. Data Mining Clustering Technique with Genetic Algorithm

V.Umayaparvathi et al. [13][4] stated that fraudster or malpractices can be effectively minimized by collecting the relevant data and by applying pattern clustering and genetic Algorithms on it.

### 5. Probalistic Methods

Michiaki et al.[14] in his work described Gaussian Mixture Model to model the probability density of users' past behavior so that the current behavior can be studied or monitored. Any deviations can help in guessing a fraud
.

## IV. CONCLUSION

The telecommunication fraud can clearly be seen as a major issue in terms of loss of service, revenue and is a major challenge to different operators and the government nowadays. This paper has reviewed different kinds of frauds available and discussed the measures to detect them eg Probabilistic Methods, data mining techniques etc.

## V. FUTURE WORK

Any of the major prevalent frauds can be studied in detail and corresponding detection technique can be employed. Depending on the type of fraud under study, the database related to the same can be collected, studied and can be used to train a neural network using any kind of existing neural network algorithms (eg Back Propagation Network, RBFN etc).The future inputs can be given to the trained neural net to check the deviations from the set standards and remedial procedures can be applied to overcome the same.

## REFERENCES:

[1] Sameer Qayyum, Shaheer Mansoor, Adeel Khalid, Zahid Halim and A.Rauf Baig, "Fraudulent Call Detection for Mobile Networks", IEEE 2010.

[2] Ogundile O.O, "Fraud Analysis in Nigeria's Mobile Telecommunication Industry", International Journal of Scientifica and Research Publications Volume 3, Issue 2, February 2013

[3] Gabriel Macia-Fernandez, Pedro Garcia-Teodoro and Jesus Diaz-Verdejo, "Fraud in Roaming Scenarios: An Overview", IEEE Wireless Communications, 2010.

[4] Anita B.Desai, Dr.Ravindra Deshmukh, "Data Mining Techniques for Fraud Detection", International Journal of Computer Science and Information Technologies, Vol. 4 (1), 2013.

[5] Constantionos S.Hilas, "Designing an expert system for fraud detection in private telecommunications networks", Elsevier Volume 36, Issue 9, November 2009.

[6] Dr. Ian Howells, Dr.Volkmar and Padraig ,"Telecom fraud 101:Fraud types, Fraud methods & Fraud Technology"

[7] RJ Frank, SP Hunt and N Davey, "Applications of Neural Networks to Telecommunication Systems", Hatfield, Herts, UK.AL 10 9 AB

[8] Yufeng Kou, Chang Tien Lu, Sirirat Sirwongwattana, "Survey of Fraud Detection Techniques", IEEE 2004.

[9] Xerandy, Hendrawan, Andriyan B Suksmono, "A Research on Usage Pattern and Analysis Techniques for Communication Fraud: SIM Cloning and Surfing" IEEE 2006.

[10] Linda Delamine (UK), Hussein Abdou (UK), John Pointon (UK), "Credit Card Fraud and Detection Techniques: A Review", Banks and Bank Systems, Volume4, Issue2, 2009.

[11] SAS Institute, Using Data Mining Techniques for fraud detection: A Best Practice Approach to Government Technology Solutions, Whitepapers. http:/www.sas.com, 1996.

[12] M.R. Arahal, M. Berenguel, F. Pavon,E.F. Camacho, "Comparing the performance of some Neural Fraud Detectors in Telecommunications", European Control Conference, 2003, Cambridge, UK

[13] V.Umayaparvathi, Dr.K.Iyakutti, "A Fraud Detection Approach in Telecommunication using Cluster GA", International Journal of Computer Trends and Technology, 2011

[14] Michiaki Taniguchi, Michael Haft, Jaako Hollmen, Volker Tresp, "Fraud Detection in Communication Networks using Neural and Probabilistic Methods", IEEE 1998

[15] Syed Ahsan Shabbir,Kannadasan R, "An Effective Fraud Detection System using Mining Technique", IJSR, Volume3, Issue5, May2013

[16] Cistian-Liviu Leca, Ioan Nicolaescu, "Significant Location Detecton & Prediction in Cellular Networks using Artificial Neural Networks", http://www.hrpub.org, 2015

[17] Smita Parija,Santosh Kumar Nanda, Prasanna Kumar Sahu, Sudhansu Sekhar Singh, "Location Prediction of Mobility Management using Soft Computing Techniques in Cellular Network", I.J. Computer Network and Information Security, 2013.

[18] Antonio Manuel Rubio , Joao Paulo, Carlos Henrique, Rafael Timoteo, "Neural Network Predictor for Fraud Detection: A Study Case for the Federal Patrimony Department", www.icofcs.org, 2012