Hybrid Strategy of Analysis and Control of Telecommunications Frauds

Longbing Cao, Chao Luo, Dan Luo, Chengqi Zhang

Abstract—**The problem of telecommunications frauds has been getting more and more serous for many years, and is even getting more and more worse not only in western countries but also in some developing countries. Detection, Analysis and prevention mechanisms are emerging both from telecommunications operators and academia. In this paper, we present a hybrid strategy of analysis and control of telecommunications frauds from engineering viewpoint. Our first task is to identify the complexity of telecommunications frauds, we discuss possible fraud scenarios and their evolution. Furthermore, in order to build an information system to deal with realistic telecommunications frauds, we summarize and propose a hybrid strategy, which includes a solution package, five models and four types of analyses, to construct a loop-closed system for analysis and control of frauds. We further discuss a system framework for analysis and control of telecommunications frauds.**

***Index Terms*—telecommunications frauds, hybrid strategy, analysis and control**

I. INTRODUCTION

It is estimated that telecommunications industry loses several billion dollars per year due to a wide variety of frauds. In China, it is reported that the losses amounted to 20 billion RMB YUAN in 2001 for telecommunications frauds [1]. As for the situation in western countries, it is estimated that the revenue losses total 3% to 6% annually depending on specific services and varying in time [2]. Therefore, prevention, early detection, analysis and control of various fraudulent activities are some important steps and activities used by telecommunications operators and administrative organizations.

Currently, administrative actions and human intervention have been taken in fraud detection and management, many possible solutions are being proposed or under discussion for controlling telecommunications frauds, such as legislative rules, customer information-gathering, customer credit certification and assessment, additional security measures taken in telecommunications system. All of these methods make telecommunications networks and services less vulnerable to frauds than before. Nevertheless, certain types of commercial frauds are very hard to preclude by technical means. It is also anticipated that the introduction of new services can lead to the development of new ways to defraud the system.

The use of sophisticated and systematic fraud analysis and control techniques can assist in early prevention and detection of commercial frauds, and will also reduce the effectiveness of technical frauds. On the other hand, these technical means will assist in analyzing, monitoring and controlling fraud pre-, during and post-trade.

In this paper, in respect of our practical and fruitful work experiences both in industrial and experimental sides in telecommunications frauds treatment in China, based on a commerce-funded TFAC project (Telecommunications Fraud Analysis and Control) [3] targeted at development of hybrid intelligent system combining new techniques and concepts for detection, prediction, prevention, analysis, monitoring, and control of frauds in telecommunication industries, we intends to report on the progress made during our first phase. We mainly focus on our proposed hybrid strategies and a package solution for implementing fraud analysis and control in telecommunications.

The remainder of this paper is organised as follows: Section 2 discusses possible fraud scenarios and their evolution; Section 3 introduces a hybrid intelligent infrastructure for analyzing and control of telecommunications frauds. We propose a package solution, five models, and four types of analyses for building telecommunications frauds treatment system. A framework of hybrid intelligent analysis and control of telecommunications frauds is presented in section four. Section 5 summarizes and gives our future works.

II. COMPLEXITY OF TELECOMMUNICATIONS FRAUDS

The first stage of telecommunications fraud analysis and control consists of the identification of possible fraud scenarios in telecommunications networks and services.

Telecommunications fraudsters are organised criminals who deliberately plan to defraud or steal the telecommunications services, many techniques have been identified, subscription fraud, PBX fraud, calling card fraud, PRS fraud, accounting fraud, content sells, pre-paid fraud, call sells, m-commerce fraud, slamming fraud, technical fraud, internal fraud, ghosting fraud, surfing fraud, payphone fraud, virus attacks, eavesdropping, etc. These scenarios have been classified mainly by the technical manner.

In the IP arena, the business model is quite different from traditional telephony services. The Internet and IP bring new business models involving several different actors. However, the business models imposed by this Internet-enabled environment indicate that roles and actors will be dynamic in nature. These actors include content providers, service

Longbing Cao and Chengqi Zhang are with the Faculty of Information Technology, University of Technology, Sydney, Australia. Longbing Cao is CTO of Beijing Guoxin Intelligent System Technology Co., which focuses on services providing for telecommunications industry. (lbcao@it.uts.edu.au, chengqi@it.uts.edu.au).

Chao Luo is a master student in Department of Electronics and Information, Liaoning Technical University (chao.luo@ mail.ia.ac.cn).

Dan Luo is a master student and works at China Science and Technology Exchange Center, Ministry of Science and Technology, China (dan.luo@ mail.ia.ac.cn).

ICITA2004 ISBN 0-646-42313-4

providers, network operators, customers, but also fraudsters. A telecommunications operator may take on several roles at a single time point, e.g., act as both network operator and service provider. Unfortunately, this also opens for a plethora of possible frauds, such as illegal redistribution, excess download and subscription fraud.

Other characteristics that have been studied are whether frauds are technical fraud operated for financial gain, or they are fraud related to personal use - hence not employed for profiteering, or abuse authorities and manipulating services for relative use from inside of telecommunications institutions. This above classification is achieved by considering whether the network abuse is the result of administrative fraud, procurement fraud, or application fraud [4].

Furthermore, types of telecommunications frauds, in both wireless and wireline networks, can be divided into following three types: (1) technical frauds: such as pay phone or prepaid, tumbling and magic phones, PBX feature abuse, stolen credit cards or numbers, stolen or counterfeit handsets, clip-on, cloning or home and roaming, PRS fraud; (2) subscription frauds: e.g., accounting fraud, content sells, pre-paid fraud, call sells, eavesdropping, identity theft, SIM card cloning, IP fraud, bad debt, call forward, roaming; and (3) internal frauds: for instance, ghosting, telecommunications data theft, security breach of systems, commissions on fraudulent sales, unauthorized provisioning of services.

As for the detection and control of telecommunications frauds, with the advancement of telecommunications customers from the perspectives of technologies and services, fraudsters are getting more and more familiar with drawbacks and rips both at telecommunications technical side and administrative side. In other words, the fraudulent techniques and behaviors of telecommunications fraudsters are also dynamic changing with the evolution of telecommunications industry.

III. HYBRID INTELLIGENT ANALYSIS AND CONTROL

With the emergence of large amount of new services, those traditional methods for incident detection are imperfect for efficiency, tool management, and complexities of new services; a package solution is expected by telecommunications operators for treating varying frauds beforehand and afterward.

As mentioned in section 2, the continuously evolutionary fraudulent activities have presented more and more rigorous criterions over telecommunications fraud treatment. New methodology and technical means, such as data mining and knowledge discovery, self-learning and adaptive tools, emergent pattern detection and recognition, data stream mining, are in expectation of from multiple disciplines respectively for dealing with the complexities of telecommunications frauds. However, what makes the above researchers and application providers unsure include whether their proposed solutions are valid for practical fraud monitoring and control.

In this section, we'd like to present our package solutions for coping with telecommunications frauds based on the idea of hybrid intelligent systems. We first discuss the infrastructure of our package solutions, and then, in order to implement this package solution, we argue that five models and four-type analysis are needed for a total and complete treatment of frauds in practice.

A. Package solutions for fraud treatment

Most of telecommunications frauds, which have been studied or are currently in studies, mainly focus on theoretical research of fraud detection and analysis involving different disciplines and algorithms. However, the requirements proposed by telecommunications operators, whether wireless or wireline, expect a total solution to fight back fraudsters, commencing from pre-trade to post-trade, feasibly and efficiently.

In addition, functionalities from telecommunications fraud detection and/or management systems presently available, either abuliding or in use, mainly focus on operational reports' representation by predefined, OLAP and ad hoc means, which to some degree have satisfied basic requirements of operational analysis based on related data fields gathered from telecommunications business operational support systems and other information technology systems. As for data mining technology, even though it is being professed as a passkey to mining gold from TB-level data, an irritant to upgrade productivity and customer relationship from hidden intelligence, and a financial guards to avoid revenue losses, there are still many drawbacks displaying when they are used for practical fraud analysis, in despite of functionalities limitations for a total solution, such as system integration of data mining with data presentation tools in an active knowledge portal, visualization and explanation of mining results, which block it to its alleged destinations.

Moreover, as a telecommunications fraud decision support system, how does it feed back those analysis results from reports and data mining to decision-makers? How does it adapt, update or control the operational systems and network switches to step into a well-ordered and fraud-avoidable situation after testing or modifying the configurations of the related BOSS systems and fraud management system automatically or human-involved?

To this end, according to the requirements we got from China telecommunications industries, we proposed a package solution for fraud treatment beforehand, in process, and afterward. Fig. 1 illustrates the functionalities of our proposed telecommunications fraud analysis and control system. Furthermore, we depict it in Fig. 2 for more architectural details of the telecommunications fraud analysis and control. By this solution, we want to build up (1) an integrated and waterstream-like workflow system from prevention to resolution, (2) a hybrid intelligent platform which synthesizes a variety of artificial intelligent technologies on demand, from symbolism to connectionism, from top-down to bottom-up, and (3) a (possibly intelligent) component-based network engineering encapsulating customized or legacy components.

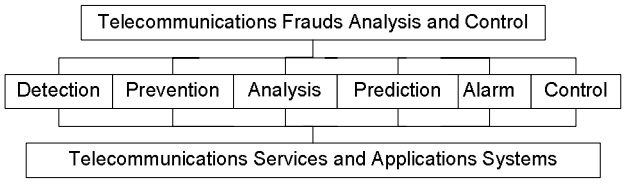

Fig.1 System structure of telecomm fraud analysis and control

This system is shown to be a loop-closed one which enclosed feedbacks of reports, events, and actions regarding decision-support, prevention, alarms and control mechanism of frauds. As for frauds, detected, analyzed and/or predicted in either case of events or thresholds, alarms and actions will be issued to control or prevent irregular telecommunications operations and/or fraudulent activities. New fraudulent behaviors will be fed back to fraudulent behaviors database in fraud control system for future alerts under similar conditions. Thus, the fraud control system will get more and more intelligent and smart with time proceeding, and to some degree have adaptive and self-learning abilities.

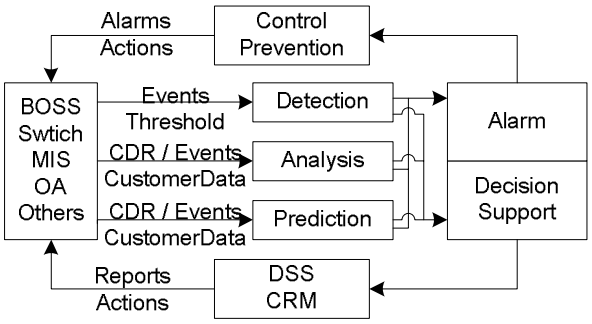

Fig.2 Solution architecture

B. Five Models

According to what we got and used in building telecommunications fraud solutions, successful planning and implementation of telecommunications fraud analysis and control should be based on five kinds of hardcore models related to the whole processes and workflow of telecommunications industry: domain specific operation model and customer model, telecommunications fraud system model, data model for fraud data warehouse and data marts, and algorithm models for fraud analysis and mining. Among all above five models, the domain specific operation model and customer model serves for foundation of implementing telecommunications fraud analysis and control.

Before startup of analysis and design of telecommunications fraud analysis and control, a collection of domain operation and its customer models matching with reality of telecommunications operations and customers should be clarified and testified by cross disciplinary domain experts. In the second place, based on the above groundwork of operation and customer models, a system model can be set up as the framework of designing and implementing telecommunications fraud analysis and control. With this blueprint of telecommunications fraud analysis and control constructed on top of operation and system models, it is time to customize data models for fraud data warehouse and data marts now, which may be arranged regarding subjects and special topics. Furthermore, algorithm models for fraud data analysis and mining, with regard to statistics analysis and mining, should be specified in respect of problem domain and algorithm selection.

It is worthy of noting that the hypothesis, assessment and modification of modeling are based on methodology of metasynthetic engineering [5], which was proposed for building hybrid intelligent systems targeted at dealing with very complex problems.

Up to now, with all these five models securing most key points of problem requirements and problem-solving, it is relatively easier to start up telecommunications fraud analysis and control. Fig. 3 shows the relationships among these models.

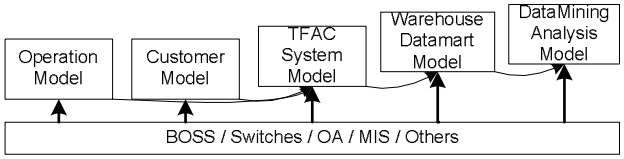

Fig.3 Modelling of telecommunications fraud analysis and control

C. Four-type Analysis

In terms of practical functionality and promotion to telecommunications enterprises healthy operations and management far away from fraudulent corrasion, data analyses act as a key and leading actor. In order to deal with different levels and aspects of requirements from telecommunications fraud analysis and control, for each data warehouse subject or data mart special, four types of analysis can be served, i.e. predefined analysis, ad hoc analysis, OLAP analysis and data mining analysis, based on data from telecommunications business operational support systems, switches system, office automation systems, management information systems and other external systems and resources, we show them in Fig. 4.

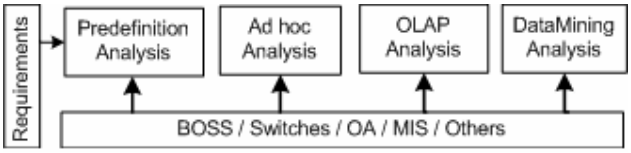

Fig.4 Four types of analysis

Predefined analysis is carried out mainly based on predefined requirements using historical data, aggregate of historical data, and middle-granularity data in terms of statistics preparation or other principles., which serve as most of the daily services and the largest part of fixed reports for operational analyses for finding abnormal actions or fraudulent behaviors. However, as a flexible and dynamic application for monitoring dynamic frauds, ad hoc analyses present runtime reports' generation mechanism for producing online reports based on sub-subjects or sub-specials under one subject or special, or multiple subjects or specials. Moreover, OLAP analyses denote online multidimensional and/or relational types of analysis processing for exhibiting a multi-level picture of fraudulent behaviors.

As an in-depth analysis and decision support tool, data mining [6] takes on significant roles in finding unusual fraudulent activities or patterns from large scale, historical and dynamic telecommunications services data. Due to system complexities and colorful potentials in decision support, a hybrid data mining system integrating multiple mining algorithms on basis of different computing principles is acceptable and to the point for mining multifarious fraudulent patterns from fundamental information produced from BOSS,

switches, customer relationship management system, and administrative systems, etc.

Furthermore, new attention has been drawn from data mining to stream data mining [7] and process for preventing, predicting, detecting, analyzing and controlling fraudulent behaviors and impairment based on large amount of online, continuous telecommunications data streams entering telecommunications information systems in real time. This research will enhance our ability of online and dynamic fraud detection, prevention, prediction, analysis, alarm and control.

IV. Framework of hybrid intelligent analysis and control of telecommunications frauds

On the basis of what we have discussed before, in this section, in order to give a more concrete and practical impression of our proposed package solutions for telecommunications frauds treatment, we further present a type of system framework we used for constructing telecommunications frauds management based on the methodology and infrastructure shown above.

Being built on top of the five predefined models, i.e. operation model, customer model, system model, data model and algorithm model, hybrid intelligent telecommunications fraud analysis and control platform extracts data needed by operational requirements through a kind of incrementally fast backup technology in compressed format. After the cleaning of the raw materials, it is sent to a temporary operational data store for usage of operational analysis and backup. Currently, six subjects of data warehouse and another six specials of data marts [8] have testified and established in the data warehouse center after the transformation of data preparation.

With the fraud data warehouse and data marts, three main types of data processing, including detection, analysis and prediction, are conducted on the top of the preset data subjects and specials in the warehouse and marts. For each subject or special, there are generally four kinds of analysis mechanisms available, namely predefined analysis, ad hoc analysis, OLAP analysis and data mining analysis, in terms of specific problem requirements on demand. The analytic results can be used for alarm and prevention or for decision support according to which have been activated in the preset specification.

In order to support decision making, a technical report builder and a decision report builder are used for generating technical reports (mainly for technical analysts and operation analysts), decision-making reports (mainly for department or middle level managers) and final decision support reports (mainly submitted to general manager for some significant decision or permission). All these report builders provide dynamic convenience and tools for generating user-friendly reports visualizing and explaining the analysis results of all above four kinds of analysis mechanisms in a plain style based on report templates. Respective users, in terms of their specific responsibilities, use these analysis results for production dispatching, customer relationship management, operation control or prevention. It is worthy of mentioning here that the above operations are conducted by ways of automatically or human-computer cooperated for different environment or policy limitations. In some case, we can only implement control, prevention and production dispatching by humans through the human computer interaction interface.

In our system, a universal human computer interaction interface, referred as active knowledge portal, is in study, which lodges many centers, like certificate center, security center, control center, model center, warehouse center, decision center, and knowledge center, etc. These centers serve as the human computer interfaces, more importantly, they are digital nerve center of the business intelligence platform. For example, the four above mentioned underlying models are finally arranged in the model center; however, the customer credit evaluation system and operational specification assessment are done in the knowledge center.

V. Conclusions and Future Work

Telecommunications fraud has been a more and more attention-drawing problems, crossing all most all countries, developed and developing, eastern and western, in both industries and academia. Solutions for implementing telecommunications fraud detection and management are proposed by more and more vendors from database fields, telecommunications services providers, statistics software providers and some emergent telecommunications application providers.

However, according to our research and comparison, most of them just consider something as it stands, for instance, mainly focus on fraud detection or pure analysis. As a matter of fact, what the telecommunications operators needed is a practical package solution, which can help them solve problems emerged beforehand, during the events and afterward. Hybrid intelligent technology makes it possible for us to provide a flexible and loop-closed mechanism, and a package solution for total and complete treatment of telecommunications frauds and control, which supports user-friendly, intelligent and well-ordered fraud detection, prevention, analysis, alarm and control. It may also provide multi-level mechanisms and tactics regarding data mining, data analysis, and data presentation available for different purposes.

For fraudulent activities are quite often and mostly complicated, another key issue for implementing practical fraud treatment system is to construct a collection of domain-specific models. Since the generic emphasis of data model doesn't tackle other significant issues relevant to operational mechanism, customer relationship, system infrastructure, etc. Therefore, in our minds, these domain models should include all four types of models mentioned above.

This platform combines some knowledge development tools and models' builders based on multidisciplinary intelligent technologies. For instance, knowledge development platform is used for managing system parameters, domain experts' knowledge, customer relationship, customer credit management and evaluation system; a technical report builder for generating analysis report is built for technicians and analysts; a decision support report builder mainly serve for building decision support reports for middle level and high level decision makers; data model builder and predefined report builder predefines reports; human computer cooperation center provides human computer-cooperated control mechanism to fulfill feedback of analysis results to operational systems. With these tools, this platform presents much stronger power for

dealing with complex fraud analysis and control flexibly, intelligently and systematically.

Our future works include but are not limited to the following aspects:

(1) implementing package solution of analysis and control of telecommunications frauds from both theoretical and industrial sides;

(2) as an automatic and flexible paradigm for building complex software system, multi-agent technology provide some unique and strong support for designing hybrid intelligent system. Our next step is to build an agent-based experimental fraud analysis and control system integrated hybrid intelligent technologies.

(3) the idea of building a loop-closed system to deal with frauds from detection, analysis to prevention and control has attracted strong interests from industrial partners, we'll study how to build such kind of analysis and control system.

REFERENCES

[1] Reasons and countermeasures for telecommunications owe fee upgrading, *Aisa-pacific Economy*, 2002, No 6 (in Chinese).

[2] Paul de Jager, "Introduction to using intelligent techniques for telecommunications fraud detection", http://www.eurescom.de/~pub/seminars/past/2001/SecurityFraud/12-Jager/.

[3] L.B. Cao, Y. Zhao, D. Wang, "System Design of Intelligent Telecommunications Fraud Analysis and Control", Technical Report, GX005-04-04, Beijing Guoxin Intelligent System Technology, Co., Ltd, 31 October, 2002 (in Chinese).

[4] P Burge, J Shawe-Taylor, C Cooke, Y Moreau, B Preneel, C Stoermann, "Fraud Detection and Management in Mobile Telecommunications Networks".

[5] R.W. Dai, J Wang, and J Tian, *Metasynthesis of intelligent systems*, Zhejiang Science and Technology Publishing House, China, 1995 (in Chinese).

[6] Jiawei Han and Micheline Kamber, *Data Mining: Concepts and Techniques*, Morgan Kaufmann Publishers, August 2000.

[7] B. Babcock, S. Babu, M. Datar, R. Motawani, and J. Widom, "Models and issues in data stream systems", PODS'02 (tutorial).

[8] L.B. Cao, Y. Zhao, "Overall Plan of Telecommunication Business Intelligence", Technical Report, GX001-01-01, Beijing Guoxin Intelligent System Technology, Co., Ltd, 28 August, 2002 (in Chinese).