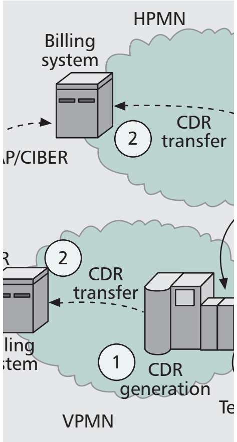
ACCEPTED FROM OPEN CALL

FRAUD IN ROAMING SCENARIOS: AN OVERVIEW

GABRIEL MACIA-FERNANDEZ, PEDRO GARCIA-TEODORO, AND JESUS DIAZ-VERDEJO,
UNIVERSITY OF GRANADA



In the mobile telecom sector fraud can lead to large financial losses. The authors present the major concerns regarding such security threats, and then propose a classification for this type of attack.

ABSTRACT

In the mobile telecommunications sector in general, and in the roaming scenario in particular, fraud can lead to large financial losses. This article first presents the major concerns regarding such security threats, and then proposes a classification for this type of attack, highlighting the necessity for the different players involved to take joint action.

INTRODUCTION

The mobile telecommunications sector is severely affected by security threats, with fraud attacks in roaming contexts one of the greatest causes of financial losses in the industry every year [1]. Because of the evolution of the services provided by telecommunications operators, more and more elaborate attack techniques are being developed by international fraudsters. These activities impact directly on the companies involved and have repercussions regarding potential increases in tariffs. Therefore, it is necessary for providers, governments, and users to establish and facilitate technical, political, economic, and social measures to prevent fraud in roaming. Success in this undertaking will benefit all parties except the wrongdoers. To illustrate the incidence and relevance of the issues dealt with in this article, some global statistics regarding current worldwide mobile communications are provided in Table 1. It should also be noticed that the progressive deployment and integration of new broadband technologies (3G/4G) in the near future could help reduce fraud in the field of mobile communications.

With these considerations in mind, this article presents an overview of the problem of fraud in roaming environments for mobile communications, as well as various strategies or techniques to tackle it. Two main contributions are made. First, fraud techniques and related protection methods are described and classified, and the advantages and drawbacks of each are reviewed. Second, because the visibility of fraud incidents influences customers' perception of the reputations of the companies affected, the latter are reluctant to publicize details of such occurrences. Little research has been carried out in this field, partly due to the low perception of the problem and also because of the lack of data available for analyzing the algorithms and techniques applied. Consequently, we seek to stimulate research in this area by highlighting the main problems, which to some extent overlap with those encountered in intrusion detection in the area of data networks.

MOBILITY AND ROAMING BASICS IN COMMUNICATIONS

Roaming is the ability of the subscribers of a mobile network, referred to as the proprietary network (hereinafter HPMN, i.e., home public mobile network), to use remotely the services of such a network by accessing it through a different network, referred to as the visited network (hereinafter VPMN, i.e., visited public mobile network). Three major actors intervene in roaming scenarios: the subscriber, who makes use of the telecommunications services provided; the HPMN, which handles the user's subscription and services; and the VPMN, in whose geographical coverage area users gain access to the services contracted with the HPMN. To enable the operator's subscribers to engage roaming facilities in a given VPMN, a roaming agreement must previously be negotiated between the two telecommunications operators. The procedures for drafting this business aspect are usually standardized, as in the case of Global System for Mobile Communications (GSM) service through the GSM Association (GSMA; www.gsmworld.com) procedures.

Roaming can be triggered for both voice and data services. In the former case, the VPMN, before providing access to the visiting users (through the mobile switching center/visited location register [MSC/VLR], which provides geographical coverage to requesting subscribers), queries the HPMN about the services to which these users are subscribed (information held in the home location register [HLR] database owned by the HPMN). Then, if the subscriptions are correct, the subscribers will be enabled to gain access to the corresponding services (e.g., voice call establishment). Figure 1a shows the steps followed in this scenario.

Data roaming is similar, although some features differentiate it from the voice call case. Here, the subscriber is associated (after querying the HLR) with a node called the serving General Packet Radio Service (GPRS) support node

	Total	Roaming
Number of subscribers (millions)	2000 (>80% GSM)	700
Revenues ($ in billions)	800	120
Financial losses due to fraud ($ in billions)	40	6 ~ 0.002 per incident (large operators) ~ 0.015 per incident (the highest one)

Table 1. *Worldwide data on current mobile communications, where the percentage of roaming is around 15% (Source: GSMA and MACH, 2007).*

To enable the operator's subscribers to engage roaming facilities in a given VPMN, a roaming agreement must previously be negotiated between the two telecommunications operators. The procedures for drafting this business aspect are usually standardized.

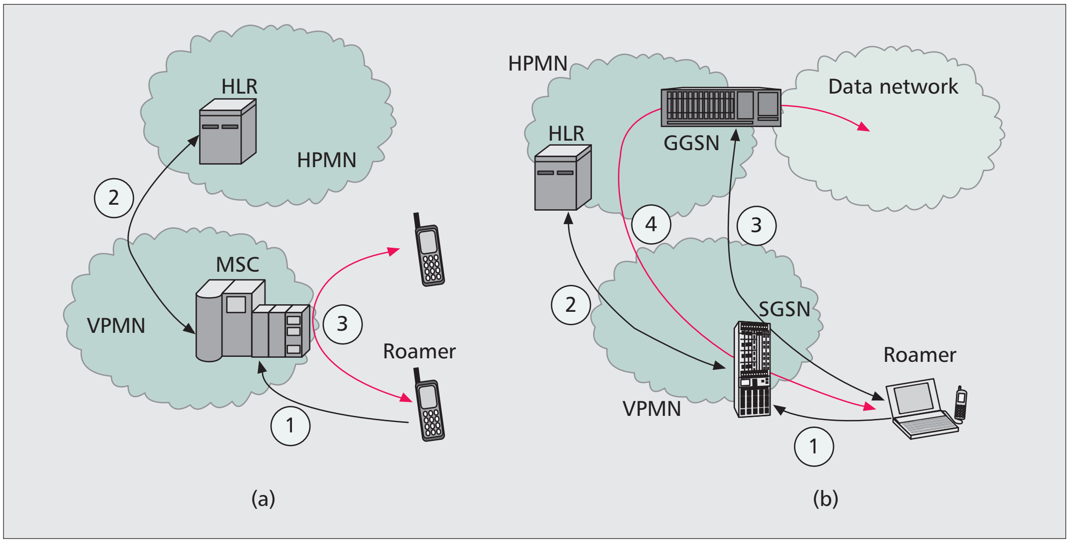


Figure 1. *Scenarios for voice and data calls in roaming: a) voice call, 1: network connection request (to MSC/VLR), 2: query by the MSC to the HPMN (HLR) about the subscription, 3: voice connection (VLR); b) data call, 1: network connection request (to SGSN), 2: SGSN query to HPMN about the subscription (HLR), 3: context establishment request to GGSN, 4: data connection establishment.*

(SGSN). Then the roamer indicates the data network to which a connection should be made, and a context is established between them through a node called the gateway GPRS support node (GGSN). The steps for this process are shown in Fig. 1b. Note that the SGSN belongs to the VPMN, whereas the GGSN is located in the HPMN. Therefore, both the data transmitted and those received by the mobile subscriber necessarily go through the HPMN. On the contrary, this does not happen in the voice traffic case, for which the VPMN-HPMN interaction is often reduced to just the initial query to the HLR.

Figure 2 shows a scenario in which a subscriber in an HPMN calls a roamer in a VPMN. The call is established in three parts or legs:

- An originating leg (OL) between the subscriber and MSC1
- A roaming leg (RL) between MSC1 and MSC2
- A terminating leg (TL) between MSC2 and the roamer

The subscriber in this scenario will be charged for the OL, while the roamer will pay for the RL and TL. The process to charge both the subscriber and roamer is as follows. Data related to the call (duration, time, origin, destination, etc.) is collected by MSCs (or SGSN and GGSN) in call data files referred to as call detail records (CDRs) (step 1 in Fig. 2). Next, these CDRs are sent to the billing systems in their respective networks (step 2 in Fig. 2). These systems are in charge of the processing of CDRs and the generation of invoices to subscribers. As the HPMN is responsible for generating invoices for both subscriber and roamer, the VPMN sends CDR information to the HPMN (step 3 in Fig. 2) compiled in a well established data structure. For this compilation process, the GSMA has defined the standard transfer account procedure (TAP) [2], whereas code-division multiple access (CDMA) networks use the cellular intercarrier billing exchange roamer (CIBER) record. There are well established timescales for the transfer of these files [3]. To relieve operators with a large number of roaming agreements of the onerous task of managing the TAP/CIBER files for every operator under the agreement, certain companies act as a clearinghouse for these data. Such companies are called data clearing houses (DCHs). A DCH is a single interface for an operator, and is in charge of managing all aspects of transmitting, receiving, and converting the TAP/CIBER files on behalf of the operator hiring the service. Finally, once the TAP/CIBER files are received, the HPMN must pay the debt incurred with the VPMN in accordance with the corresponding roaming agreement tariffs, termed interoperator tariffs (IOTs) [2].

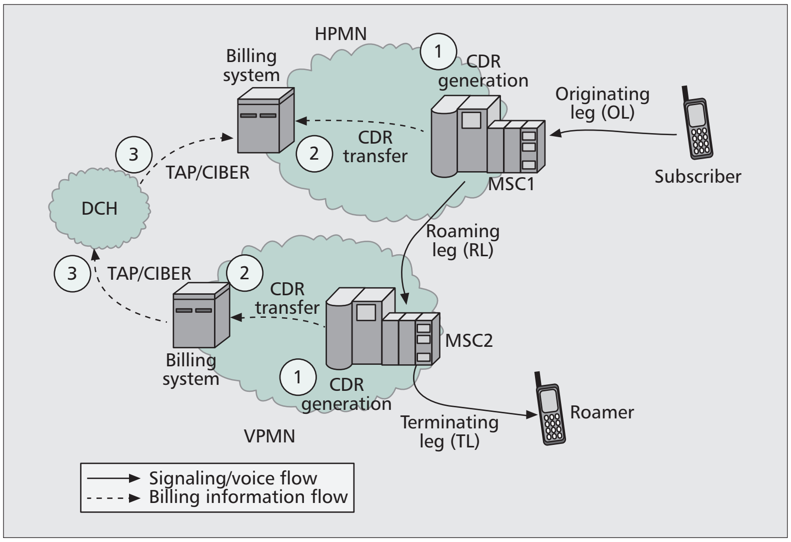


Figure 2. *Billing information flow process in a call from HPMN to a roamer in a VPMN. Step 1: generation of CDRs in MSCs. Step 2: transfer of CDRs from MSCs to billing systems. Step 3: transfer of CDRs from VPMN to HPMN by using TAP/CIBER.*

Fraud Attacks in Roaming Environments

Fraud in a roaming scenario consists of access by the subscriber to the resources of the HPMN via the VPNM in such a way that the operator of the HPMN is unable to charge the subscriber for the services provided and is obliged to pay the operator of the VPNM for the facilities provided in the roaming scenario.

Fraud in roaming may be considered an extension of the fraud techniques used in conventional environments. Nevertheless, the roaming fraud case has some particular characteristics that make it even more harmful, because of the losses incurred [4, 5].

Longer detection time: Since the fraud is perpetrated from a network other than that of the subscriber, the time required to detect the fraud is longer, mainly because of the existence of delays in the communication of the information between VPMN and HPMN.

Longer response time: Once the fraud has been detected, the technical and administrative difficulties to prevent it from persisting are greater than when the victim operator has direct control over all the systems affected.

More technical difficulties in resolving the fraud: Prevention, detection, and automatic response systems to combat fraud are more complex in roaming scenarios, mainly because of the diversity of the VPMNs and HPMNs involved. In many cases this leads to a decrease in the speed of the global process, which makes the fraud even greater.

Higher financial losses: Fraud in traditional communication scenarios implies financial losses for service providers. This loss can be much greater in roaming environments due to the charges payable to the VPMN under the roaming situation.

Depending on the method used to perpetrate fraud actions and the business area of the telecommunications operator that is affected by it, roaming fraud can be classified as shown in Fig. 3. This classification is not intended to be exhaustive, but only to give an idea of different means used by fraudsters in order to illegally obtain benefits. These are discussed in greater detail below.

Type 1. Fraud Based on Technical Network Factors

In this case fraudsters take advantage of technical faults in the configuration, design, or architecture of the operator network. The most common causes in this respect are the following.

Interoperability faults (type 1A): Errors in the expected interfunctioning between the operators' network equipment frequently arise, due to the presence of different technologies and/or equipment from various suppliers (multivendor environments). Malfunctions are frequently associated with incorrect implementation of standards. Consequently, certain items of equipment fail to correctly parse the information coming from others. This, together with the lack of exhaustive roaming tests, can give rise to faults.

Consider the case of a prepaid roaming GSM subscriber with a null credit balance, or a postpaid subscriber who has reached his/her limit. Improper communication between the VPMN and the HPMN might enable the user to continue using the service while the HPMN will be impeded from charging for it.

Another common interoperability fault concerns barrings (restrictions in telephone exchanges), especially in multivendor VPMNs, mainly because conformance testing sets are conducted in only one exchange before roaming agreements are completed. If the manufacturer of such an MSC is different from that of the MSC where the roamer is located, severe problems may appear. A particular case is that of a subscriber who is subject to barring on outgoing calls and is located in a VPMN MSC with the described fault. When the MSC receives notification from the HPMN about the barring of all outgoing calls from the HPMN network, it does not process this information properly, and hence the subscriber may continue using the service.

Time delay in data exchange (type 1B): This type of fraud takes advantage of the exposure time interval, that is, the elapsed time between when the fraud starts being perpetrated and the instant at which it is detected and measures to combat it are deployed. This interval is determined by the time involved in sending the CDR-related information from the VPMN to the HPMN, and the time employed to investigate the potential existence of a fraud attack.

Network configuration flaws (type 1C): These flaws are triggered by inefficient operation and maintenance procedures, and also by inadequately trained technical staff. Two illustrative examples can be cited. First, when unprotected short message service centers (SMSCs) receive short messages from subscribers other than their own subscribers, they carry out the processing but are unable to charge for them afterward. Another interesting example of this kind of fraud occurs when roaming subscribers dial *pre-*

mium rate numbers (entertainment or adult calls) in a VPMN. Generally, this is not allowed in the VPMN-HPMN interconnection agreements. Although the VPMN may prevent this service from being provided, a faulty configuration could make such scenarios possible.

Type 2. Fraud Enabled by Flaws in Other Business Areas

This type of fraud stems from inefficient/poorly designed business processes, or because of technical aspects not directly related to the telecommunications network. Some examples of this kind of fraud are described below.

Subscription fraud (type 2A): This type of fraud involves an impostor subscriber who uses false accounts or cards with insufficient credit balance to gain fraudulent access to services. Some of the most common actions in this respect are as follows. *Call sale* ranges from phone rentals to the setting up of telephone booths to make calls. *Call forwarding* consists of fraudulently providing local calls, and then forwarding them to more expensive international remote services. The use of *micro-payments* and calls to *premium rate numbers* with fraudulent cards may also generate substantial losses for operators. Similar to the premium rate case, the international revenue share fraud (IRSF) [6] claims, after the subscription attack, for high-cost international calls. As a rule, the calls do not reach the geographical destinations, but are routed by an intermediate operator to a third provider with a shared payment service, which obtains the benefit.

Internal frauds (type 2B): These frauds are committed by personnel belonging to the telecommunications companies themselves, enabled by defective internal security systems or protocols. Two variants consist of the theft of SIM cards and their subsequent activation, and the use of test cards for roaming scenarios.

Fraud in M-commerce (type 2C): The use of stolen or false credit cards for mobile commerce services entails fraud costs for the providers. This type of fraud is identical to that perpetrated in e-commerce environments, the mobility of the subscribers being the only difference in committing the fraud.

Copyright fraud (type 2D): The new content download services (music, video, logos, etc.) incur copyright costs for the operators.

Fraud types 2C and 2D are not specific for roaming scenarios, but are general to all environments. Types 2A and 2B are, however, critical in roaming circumstances, mainly due to longer detection times and the existence of greater technical difficulties and higher financial losses, as discussed earlier.

Protection Systems Against Roaming Fraud

A fraud protection system is used in the HPMN for the purpose of reducing as much as possible both the possibility of being the victim of fraud and the impact of a fraud attack if one does take place. A system to protect against fraud should consist of the stages indicated in Fig. 4. First of all, a *prevention stage* should exist, in which measures aimed at preventing or hampering the perpetration of fraud are established. Alongside this first stage, the remaining stages are sequentially carried out. In the *data collection* stage VPMNs generate CDR data as well as possible notifications about fraudulent actions. Subsequently, there is a *detection stage* during which the data received by the HPMN are reviewed to search for fraudulent behavior patterns. The result of this stage will consist of a list of subscribers with possibly anomalous behavior, which is passed on to the *supervision stage* for the analysis of high-risk events by specialized staff. Finally, if response actions are required, the mechanisms needed to counter the evolution of the fraud are activated in the *response stage*.

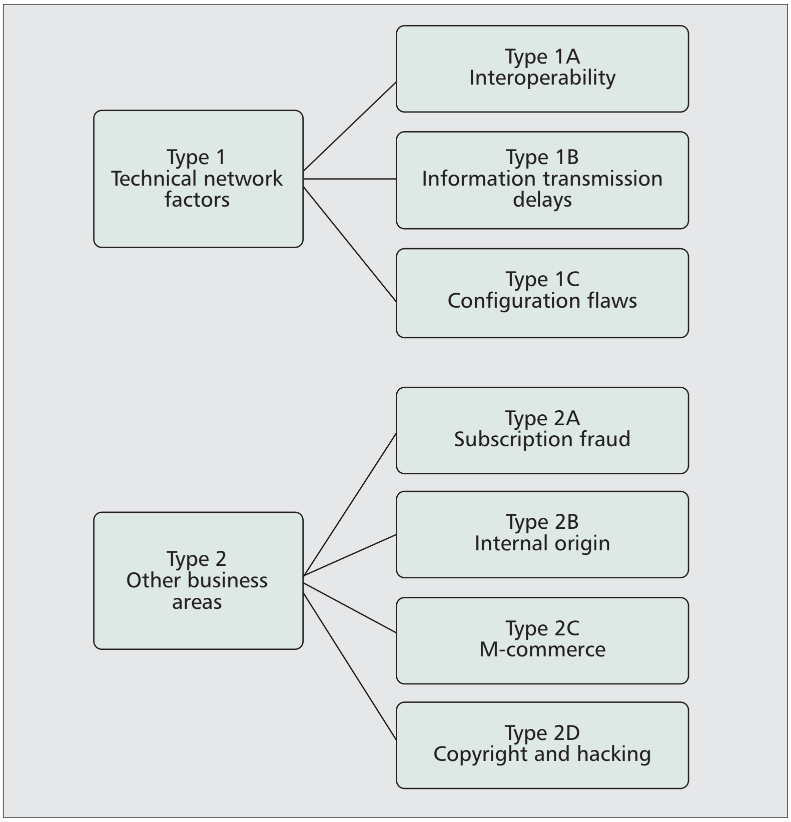


Figure 3. *Classification for fraudulent methods in roaming environments.*

Two key parameters in evaluating the efficiency of a fraud protection system are the *average resolution time*, T_R, that is, the time elapsed between the occurrence of a fraudulent action and the execution of the necessary response measures, and the accuracy of the results given by the system. As a first approach, the value of T_R can be expressed as

$$T_R = T_{CDR}^{VPMN \rightarrow HPMN} + T_{CDR}^{HPMN1} + T_{CDR}^{HPMN2},$$

where the latter three terms are the time spent in receiving the CDR data collected by the VPMN, the delay in the HPMN in initiating the handling of the information, and the time involved in raising a fraud alarm and resolving the corresponding problem, ($T_{CDR}^{HPMN2} = T_{detection} + T_{supervision} + T_{response}$), respectively.

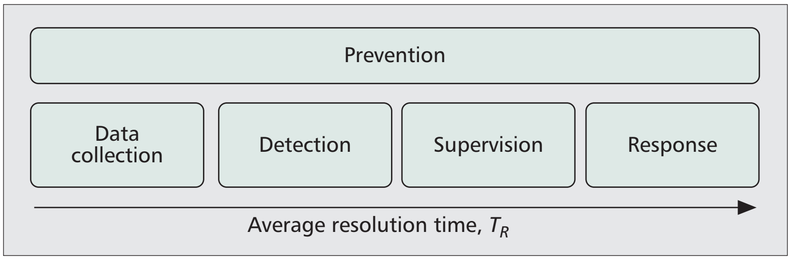


Figure 4. *Stages comprising a fraud protection system.*

As in any other security system, the level of security provided by a fraud protection system is determined by the lowest security level provided by each of its components. Below, each of the stages comprising a fraud protection system is examined in greater detail.

Fraud Prevention Stage

In this stage preventive measures are taken to hamper the perpetration of fraud. Among others, the following have been proposed and applied:

Service restrictions when the subscriber is in roaming mode: A strategy consisting of the gradual activation of services as the subscriber proves to be trustworthy. This may be achieved in various ways: the gradual activation of the roaming mode for customers, selective roaming to/from only certain operators, restrictions on calls to premium rate numbers in roaming, prevention of international calls forwarding in roaming, limitation of the duration for phone calls, and so on. This type of measure, although helping prevent fraud, has a direct impact on the quality of the service provided to the customer, who must provide the operator with prior justification in order for services to be provided.

Optimization of roaming agreements: In roaming agreements it is important to consider all the aspects that might arise during the service provision, in order to forestall potential problems. Thus, it is important to apply the recommendations made by certain organizations (e.g., GSMA), as discussed in the previous sections.

Exhaustive roaming testing sets: These kinds of tests curtail the possibility of suffering from fraud types 1A and 1C. They involve not only roaming related services but also CDR files, interoperator interoperability, and so on. To carry out these tests, it is advisable to use equipment from various providers in the HPMN and VPMN. The GSMA, among other organizations, has made recommendations about the testing protocols to be considered.

Prevention of subscription fraud: Specific recommendations have been made to prevent this kind of fraud (type 2A), essentially aimed at optimizing business processes for client management and distribution. Some of the main measures proposed regard validating the information provided by subscribers, enhancing staff training to combat fraud, auditing customer credits, drawing up a structure to punish fraud, and so on. Certain after-sale procedures are also advisable, such as those aimed at checking customers' personal information and requesting email replies.

Data Collection Stage

Optimizing this second stage is crucial to reduce the average resolution time, T_R. It is advisable to decrease this interval to the utmost to eliminate the perpetration of fraud type 1B, which exploits time delay in data exchange.

Most CDMA operators in America tackle this matter by exchanging CDRs in almost real time. The unprocessed CDRs are picked up by the VPMN and sent directly (without even passing through the data exchange centers) to the corresponding HPMN. This greatly decreases fraud risks [7]. In the GSM world, however, various other techniques have been proposed, examined, and implemented. The main proposals made to date for the implementation of the data collection stage are:

High Usage Report: Defined by the GSMA [8], HUR consists of VPMN monitoring of the call data tickets related to the subscribers in roaming. If a subscriber exceeds a given threshold, a notification is sent to the HPMN. The procedure, proposed as mandatory by the GSMA until September 30, 2008, has two fundamental drawbacks. First, the time lag involved in receiving the reports is broad, because they depend on the billing cycles (it can take up to 36 hours to send a TAP billing file). In addition, the reports provide limited information about the fraud scenario, and it is advisable to wait for the complete call data files in order to obtain an overall view of the problem.

Fraud Information Gathering System: Defined by 3GPP [9], FIGS is a solution based on the CAMEL signaling exchange system between operators [10], by which the VPMN can send, in real time, the CDRs pertaining to a given number of subscribers to the HPMN. This scheme, too, presents certain drawbacks. First, because there is a ceiling on the number of subscribers to be monitored, it is not clear how to choose the specific subscribers that require surveillance. In addition, the deployment of CAMEL by the operators is assumed, which is not always the case. Finally, if CAMEL signaling exists, technical staff is required for specific training in these procedures.

Monitoring of signaling information: Signaling monitoring obtains information that makes it possible, under certain circumstances, to facilitate the task of identifying patterns of fraudulent behavior. The information is usually obtained from the VLR (VPMN)-HLR (HPMN) communication. Thus, the behavior of certain subscribers can be observed to obtain data such as the load level for requests, or the identity of the networks that issue the requests. This scheme can only be considered as complementary to others, because the information provided does not allow a given behavior pattern to be classified as certain fraud.

Near Real Time Roaming Data Exchange: Developed by GSMA, the purpose of this scheme is the transmission of CDRs in almost real time. Specifically, there is a 4-hour time-limit for this transmission [3]. Implementation of NRTRDE is mandatory since October 2008. In addition to the substantial decrease achieved in lags with respect to the time required for information transfer, the present technique has other advantages. The fact that the call data are sent into an information flow that is separate from the TAP files makes it possible to compare the CDRs and thus detect inconsistencies, and also to check the integrity of the systems. Moreover, detection systems can be better adjusted, thus reducing their "false positive rate" (level of events erroneously detected as fraudulent). However, although NRTRDE constitutes a considerable improvement over previous systems, it also has some drawbacks that should be pointed out. First, there are few incentives for the VPMN to put it into practice, because the principal beneficiary is the HPMN. Additionally, receiving an extra flow for CDRs requires investment in additional processing and storage infrastructure.

Data traffic monitoring: Since the subscriber's data traffic in roaming flows between the SGSN of the VPMN and the GGSN of the HPMN, it is possible for the latter to monitor such traffic as if it were generated by the network itself. To do this, the use of systems known as RTC ("Real Time Charging," in pre-pay, or "Roaming Traffic Control," in post-pay), located in the SGSN-GGSN data route, is recommended. These systems monitor data traffic in real time, providing this information for the detection stage.

It should be noted that considerable effort is currently being made towards deploying online charging systems [11], especially in IMS ("IP multimedia system") frameworks, which aim at providing a standard interface to integrate the charging of heterogeneous network equipment on a real time basis. These systems will reduce to a minimum the value of T_R, as they monitor and transfer per flow and obtain service charging information in real time, thus making the networks less vulnerable to frauds caused by delays in data exchange (fraud type 1B).

Detection Stage

The detection module uses all the information generated during the data collection stage, and it must decide whether a behavior is anomalous or not. In this stage, the FMS ("Fraud Management System") plays a crucial role, as it is an automatic (or semi-automatic) system that processes the CDR information and searches for fraud patterns.

The detection of fraudulent activities is a pattern classification problem, quite similar to others like intrusion detection in the network security field. Current available techniques that tackle these problems range from statistical approaches to more complex methods, i.e., data mining, machine learning and neural networks [7, 12, 13].

Although pattern classification is a very active research area, there exist few works related to fraud detection in telecommunications and even fewer are focused on the peculiarities of fraud in roaming. This fact is mainly due to privacy, brand image, and economic concerns from the major operators [14]. These are usually reluctant to make data available for research purposes.

A good overview on methods for fraud detection in telecommunications is presented in [14]. Some of them are based on the use of signatures or rules, e.g., when a call is over 30 minutes, an alarm signal is raised. Other approaches rely on statistical characterization of the behavior of a given subscriber or group of subscribers, i.e., usage profiles are extracted and used as normality models. Some authors use neural networks, expert systems or data mining, among other techniques, to derive these profiles and extract the relevant parameters from CDRs. A representative example of this approach is the ASPeCT project [15]. On the other hand, machine learning methods have also been tested in order to establish a general normality (or abnormality) model for the whole system. In this case, not only CDRs, but also voice or signaling traffic, and other related events might be considered [14].

Although some of these techniques seem promising for the detection of fraud in roaming, their main problem is related to the so called false positives rate [12, 13]. In order to reduce them, detection modules in current solutions use to work in a supervised manner. However, this leads to an increase in the average resolution time, T_R.

There exist many current commercial systems from companies in this field, some of which are still incipient, while others are consolidated (e.g., Mach, Syniverse Technologies, FairIsaac, Agilent, StarHome, ECtel, gmv).

Finally, let us note that systems for data traffic monitoring in real time (RTC) also incorporate detection capabilities, and thus make it possible to observe possibly fraudulent behavior.

Supervision Stage

The fraud alarms triggered by the detection system must be thoroughly reviewed before it is definitively concluded that the observed event is indeed a fraud attack. This review is normally conducted by the company's fraud department or by an outsourced specialized company.

The fraud alarms triggered by the detection system must be thoroughly reviewed before it is definitively concluded that the observed event is indeed a fraud attack. This review is normally conducted by the company's fraud department or by an outsourced specialized company.

The principal difficulties arising during this stage are those due to the lags that arise as the fraud investigation takes place. These lags increase considerably when the notifications of the detection system take place during off hours. In many such cases, the companies involved have not envisaged any kind of action plan. This lack of planning nullifies the effort and investment made in other stages of the protection system to reduce the average resolution time. This scenario is more frequent than might be expected at first sight; international fraud networks are aware of the limitations of companies in this respect, and take advantage of exposure timings to perpetrate their fraud.

Note that, by means of this stage, the accuracy of the system is maximized, assuming that a manual inspection of the data is more reliable. However, manual inspection involves greater values of T_R. This fact highlights the necessity for the development of improved automatic detection algorithms that provide acceptable accuracy. With the use of these algorithms, the supervision and the detection stages could be merged into a single phase.

Response Stage

If a fraud alarm is raised during the supervision stage, it is necessary to act in some way to abort the fraudulent action. To do this, it is advisable for the HPMN, first, to suspend the calls or services currently in use, and, second, to prevent the fraud from continuing. Another less intrusive type of solution can also be opted for, such as that of a prior notification to the customer to avoid affecting the service when fraud does not really occur (false positive case).

The know-how gained in this field should help us win the battle against fraudsters. Finally, social and political aspects are relevant to the fight against fraud. Thus, there is a need to analyze the social impact of fraud and the political and regulatory measures that should be deployed.

To prevent further provision of the service, the fraudulent user's subscription is altered to at least prevent the generation of SMS, barring all outgoing and incoming calls in roaming, and preventing the connection to data access points.

Suspension of calls and services can be effected in real time by using the IST ("Immediate Service Termination") functionality, if a CAMEL signaling agreement with the VPMN exists [10]. Another alternative which does not involve the suspension of the services in real time is to notify the VPMN (by e-mail, phone call, etc.), which will then carry out the interruption.

Challenges in Fighting Fraud in Roaming

Up to now, few private companies have focused on helping operators to fight fraud in roaming, mainly because of the poor perception of this problem and also due to the lack of data provided by the operators for analysis and research.

In order to plan a roadmap for fighting fraud in roaming, the first step is to clarify the magnitude of the problem, in terms of the current losses, dimension, operators and subscribers affected, etc. Second, a key research area involves systems to protect against fraud. The problems in this area are similar to those facing the IDSs in data networks. Thus, the know-how gained in this field should help us win the battle against fraudsters. Finally, social and political aspects are relevant to the fight against fraud. Thus, there is a need to analyze the social impact of fraud and the political and regulatory measures that should be deployed.

Conclusion

Roaming fraud is an important problem that has attracted the attention of many important companies and operators. We have analyzed this problem in order to highlight two main concerns: first, the sensitive nature of the problem has made the industry reluctant to reveal information, and hence little research has been carried out in this field. The present article seeks to encourage the research community to investigate these issues. Second, we survey fraud techniques and protection policies, with the purpose of clarifying and identifying the main questions. We show how the technologies in this field are not mature, possibly because most work has been aimed towards data collection mechanisms, leaving other aspects unconsidered.

Acknowledgements

We wish to thank the Inter-American Development Bank (IDB) and, specially, Jose Maria Díaz Batanero for motivating and supporting this work through the IIRSA initiative program. This article has been partially supported by the Spanish Government through MEC (Project TSI2005-08145-C02-02, FEDER funds 70 percent). Finally, we thank the anonymous reviewers for their comments, which have enabled us to significantly improve the quality of this article.

References

[1] Mach, "White Paper on Fraud Protection," Nov. 2007; http://www.mach.com

[2] S. K. Siddiqui, *Roaming in Wireless Networks*, McGraw Hill, 2006.

[3] GSMA, "PRD BA.08, v19.0, Timescales for Data Transfer," May 2007.

[4] M. Johnson, "Revenue Assurance, Fraud & Security in 3G Telecom Services," *J. Economic Crime Mgmt.*, vol. 1, no. 2, 2002.

[5] J. Hynninen, "Experiences in Mobile Phone Fraud"; http://citeseer.ist.psu.edu /hynninen00experiences.html

[6] GSMA, "PRD FF.17, v2.0, International Revenue Share Fraud," Oct. 2007.

[7] T. Fawcett and F. Provost, "Fraud Detection," W. Klösgen and J. Zytkow, Eds., *Handbook of Data Mining and Knowledge Discovery* (Sec. F2), Oxford Univ. Press, 2002.

[8] GSMA, "PRD FF.04, v2.3, High Usage Report Format and Contents," Oct. 2007.

[9] 3GPP, "ETSI TS 101 107, v8.0.1, Fraud Information Gathering System (FIGS), Service Description," June 2001.

[10] R. Noldus, *CAMEL, Intelligent Networks for the GSM, GPRS and UMTS Network*, Wiley & Sons, 2006. ISBN: 0-470-01694-9.

[11] K. Ahmavaara, H. Haverinen, and R. Pichna, "Interworking Architecture between 3GPP and WLAN Systems," *IEEE Commun. Mag.*, vol. 41, no. 11, 2003, pp. 74–81.

[12] R. Bolton and D. Hand, "Statistical Fraud Detection: A Review," *Statistical Sci.*, vol. 17, n. 3, 2002, pp. 235–55.

[13] Y. Kou *et al.*, "Survey of Fraud Detection Techniques," *Proc. 2004 IEEE Int'l. Conf. Networking, Sensing and Control*, 2004, pp. 749–54.

[14] P. Estévez, C. Held, and C. Pérez, "Subscription Fraud Prevention in Telecommunications Using Fuzzy Rules and Neural Networks," *Expert Sys. with Apps.*, vol. 31, 2006, pp. 337–44.

[15] P. Burge and J. Shawe-Taylor, "An Unsupervised Neural Network Approach to Profiling the Behavior of Mobile Phone Users for Use in Fraud Detection," *J. Parallel and Distrib. Comp.*, vol. 61, 2001, pp. 915–25.

Biographies

GABRIEL MACIA-FERNANDEZ (gmacia@ugr.es) is an assistant professor in the Department of Signal Theory, Telematics and Communications of the University of Granada. He received an M.S. in telecommunications engineering from the University of Seville and got a Ph.D. in 2007 from the University of Granada. From 1999 to 2005 he worked as a specialist consultant with Vodafone Spain. His research was initially focused on multicasting technologies, but he is currently working on computer and network security.

PEDRO GARCIA-TEODORO (pgteodor@ugr.es) is an associate professor in the Department of Signal Theory, Telematics and Communications of the University of Granada, Spain. He received his B.Sc. in physics from the University of Granada in 1989 and a Ph.D. degree in physics in 1996. His initial research interest was concerned with speech technologies. Since then, his professional profile has derived to the field of computer and network security, specially focused on intrusion detection and denial of service attacks.

JESUS E. DIAZ-VERDEJO (jedv@ugr.es) is an associate professor in the Department of Signal Theory, Telematics and Communications of the University of Granada. He received his B.Sc. in physics in 1989 and a Ph.D. degree in physics in 1995 from the University of Granada. His initial research interest was related to speech technologies, especially automatic speech recognition. He is currently working on computer and network security, although he has developed some work in telematics applications and e-learning systems.