Roaming fraud: assault and defense strategies

Gabriel Maciá-Fernández,* University of Granada, Spain

***Abstract*— Fraud is one of the major concerns of the telecommunication sector. It leads to high amounts of financial losses in this sector every year. For mobile telephony operators, one of the largest contributing factors to losses due to fraud is the one coming from roaming scenarios. The present article intends to examine the causes generating these types of fraud and the strategies and measures aimed at protecting operators from them. The methodology to study this matter raises a series of questions to be discussed among the main players involved in preventing roaming fraud for the purpose of drawing up a working agenda to improve the outlook for this sector.**

I. INTRODUCTION

The greatest cause of income losses in the telecommunication industry is fraud [1]. In the area of mobile telecommunications, one of the business aspects that most contributes to income loss due to fraud is roaming [2]. Roaming service enables the subscribers of a mobile network, referred to as the home network (hereinafter HPMN, that is, Home Public Mobile Network), to use the services provided by this network by means of access through a different network, referred to as the visited network (hereinafter VPMN, that is, Visited Public Mobile Network).

Because of the evolution of the services that are supplied by telecommunication operators, international fraud organized networks have been developing complex fraud techniques that make it possible to generate substantial losses in a company's earnings. These losses may later have repercussions for the rates that these companies charge to their subscribers, which leads to a rise in prices.

It is therefore necessary, not only for operators but also for governments and users, to establish and facilitate technical, political, economic, and social measures that hamper roaming fraud. Success in this undertaking shall bring benefits to all the players involved except the fraudsters.

Along this line, the present article attempts to provide an overview of the problem of fraud in roaming environments, as well as the various strategies or techniques to tackle it. To do this, it classifies and describes both fraud techniques and related protection methods and reviews the advantages and drawbacks of each. Finally, it also intends to raise a series of questions that need to be answered to continue combating this type of fraud.

The present article is structured as follows: Section II reviews the most important notions about how roaming service functions. Section III classifies the various most common fraud strategies. Defense techniques against roaming fraud are described and examined in Section IV. Section V proposes a methodology to revise and plan for the future in the fight against roaming fraud. Finally, conclusions are drawn in Section VI.

II. NOTIONS ABOUT ROAMING

Roaming is the capacity of subscribers to a wireless network to make or receive voice calls, send or receive data or gain access to other services when they are outside the geographical area covered by their home network by using the resources of a visited network.

It can therefore be concluded that three major players intervene in roaming: the subscriber, who is the one using the services; the proprietary network, or HPMN, which is the one that holds the user's subscription; and the visited network, or VPMN, in whose geographical area of coverage the subscriber gains access to the services hired with the HPMN.

To enable an operator's subscribers to engage in roaming in another VPMN, an agreement between both operators must be previously drawn up. The procedures for drafting these agreements are usually standardized, such as those proposed by the GSM Association (GSMA) [3], and they basically consist of signing contracts that set forth the conditions of the agreement and running technical testing protocols to facilitate service management between both operators.

Roaming can be done for both voice and data services. In the case of voice services, the VPMN, prior to allowing the subscriber to be associated to its network (through the mobile switching center (MSC) that provides coverage to the subscriber), queries the HPMN about the services that the users subscribes to (information that is housed in the HLR database owned by the HPMN). Afterwards, if the subscription is correct, it enables the subscriber to gain access to the corresponding services, for example, the establishment of a voice call. Fig. 1 provides a diagram of this scenario.

Data roaming is similar, but it has some important features that differentiate it. In this case, the subscriber is associated (after querying the HLR) to a node called the SGSN (Serving

THIS PAPER IS A TRANSLATION FROM ITS ORIGINAL VERSION IN SPANISH. THE AUTHOR IS NOT RESPONSIBLE FOR POSSIBLE TRANSLATION ERRORS.

* Gabriel Maciá Fernández is an assistant doctoral professor at the University of Granada in Spain.

Mailing address: ETS. Ingenierías Informática y de Telecomunicación. Dpto. Teoría de la Señal, Telemática y Comunicaciones, Universidad de Granada. c/ Daniel Saucedo Aranda, s/n. 18071 Granada (España).

Email: gmacia @ ugr.es

Phone: +34-958-241000 (ext: 20048)

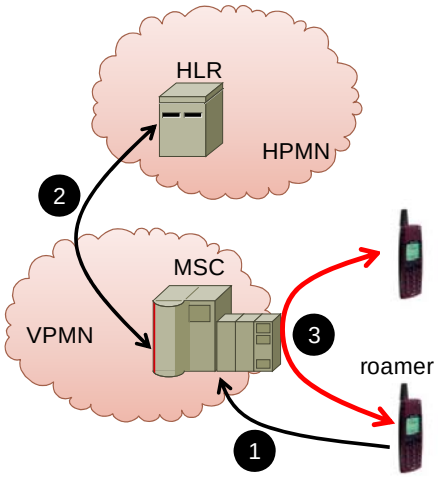

Fig. 1. Scenario of voice call in roaming: 1) network connection request (MSC), 2) query by the MSC about the subscription to the HPMN (HLR), and 3) voice connection.

GPRS Support Node). Afterwards the user indicates to the mobile network the type of data network to which it wishes to establish a connection, and a context is established with this data network through a node called GGSN (Gateway GPRS Support Node). Fig. 2 provides a graphic overview of this process.

It is important to indicate that, whereas the SGSN belongs to the VPMN, the GGSN is always the property of the HPMN, and therefore the data that are transmitted or received by the subscriber must necessarily pass by way of the HPMN. This does not happen with voice traffic, for which the interaction between VPMN and HPMN is oftentimes only the initial query to the HLR. Therefore, to be able to set the rates for both voice and data services, the VPMN must send information gathered about the calls made and the data transmitted by the subscriber to the HPMN. These data are collected in billing records referred to as CDRs (Call Detail Records), or generically UDRs (Usage Detail Records). The VPMN, who must charge on the basis of the services that are provided, sends this information to the HPMN, compiling the CDRs together in files that have a well-defined structure. The most widely used standard for these files in the GSM network has been defined by the GSMA and is called TAP (Transfer Account Procedure) [4], whereas the CDMA networks use CIBER (Cellular Intercarrier Billing Exchange Roamer record).

Once the TAP/CIBER files have been received, the HPMN must pay the debt incurred with VPMN on the basis of the rates set in the roaming agreements (IOT, Inter-Operator Tariff) [5].

To save the operators that have a large number of roaming agreements from the chore of managing the sending and receiving of the TAP/CIBER files to each and every operator with an agreement, certain companies are used to act as a clearinghouse for these data (they are called DCH, that is, Data Clearing Houses). Thus, the DCH is the only interface for the operator and is in charge of managing all the aspects involved in transmitting and receiving the TAP/CIBER files with the operator that hires this service.

III. Roaming Fraud

When a VPMN processes a HPMN user's calls or services, it generates the corresponding CDRs and sends them to the HPMN according to the procedures and time-limits that have been set [6]. Afterwards, it will have to charge the HPMN for the amounts owed. As for the HPMN, it shall deduct the amount pertaining to the subscriber. Now, when the user gains access to the service by fraudulent means, the HPMN is unable to charge said user for the corresponding amount and as a result the operator incurs a loss.

It can be said that fraud in roaming scenarios is nothing more than the extension of fraud techniques in conventional scenarios. Nevertheless, these kinds of fraud have their own characteristics that make them even more harmful because of the losses they trigger [7] [8]. These characteristics are indicated below:

- *Longer time for detection:* 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 there must be communication protocols between both networks and these protocols are not always sufficiently efficient.

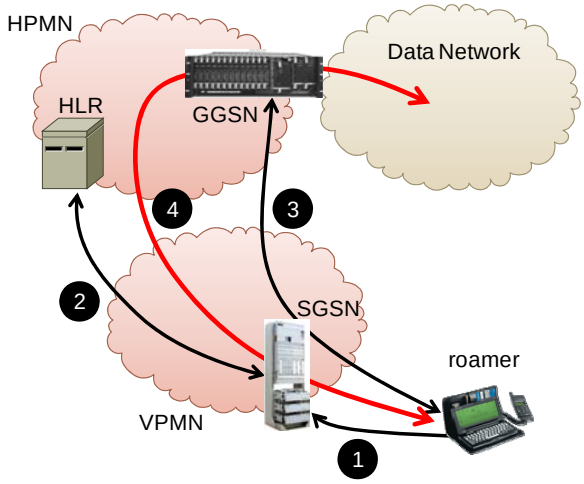

Fig. 2. Scenario for data call in roaming: (1) network connection request (SGSN), (2) SGSN query about the subscription to HPMN (HLR), (3) context establishment request to GGSN, and (4) data connection establishment.

- *Greater time of response:* Once the fraud has been detected, the technical and administrative difficulties to prevent it from continuing are greater than if the operator that is the victim of the fraud had control over all the systems within its reach.

- *More technical difficulties in resolving the fraud:* The prevention, detection and automatic response systems to combat fraud are more complex mainly because of the diversity of the VPMN and HPMN networks involved, which in many cases leads to failure of the performance protocols, which in turn makes the fraud even greater.

The main technique traditionally used to perpetrate fraud in telecommunication networks has been the one known as subscription fraud, that is, a subscriber opens an account providing wrong personal information or a false bank account number and uses the phone to make calls, usually high-cost calls. The evolution of telecommunication networks (development of 3G) and the emergence of new and more complex services, however, have led international organized criminal networks to develop new technological strategies and platforms for fraud that can trigger substantial losses for operators.

Depending on the method used to perpetrate the fraud, roaming fraud can be classified as indicated in the diagram of Fig. 3.

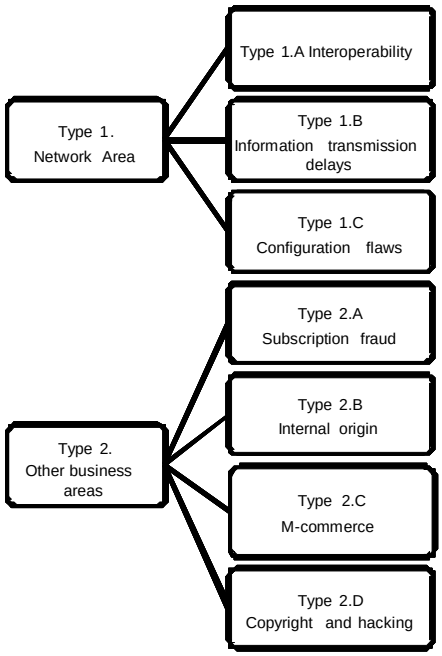

Fig. 3. Classification of methods of fraud in roaming environments.

Type 1. Fraud for technical causes in the network: They try to take advantage of technical breakdowns in the configuration, design or architecture of the communication networks of the operators. The most common causes that make it possible for this fraud to work are indicated below:

Type 1.A. Interoperability breakdowns*:* They consist of errors in the expected functioning between the operators' network equipment. These breakdowns are commonly triggered by the presence of different technologies and/or the presence of equipment from various suppliers (multivendor environments). Let us examine one example:

- Prepaid subscriber in GSM roaming who is left without any credit or a postpaid subscriber whose use is monitored and who reaches his maximum limit. If there is no mechanism that makes it possible to control the call when it is active (by some type of standard signalling called CAMEL in GSM and WIN in CDMA), to prevent generating further spending on new calls, the HPMN changes the subscriber's subscription by deactivating the TS22 service (originating SMS), changing his GPRS profile (forbidding certain APNs, that is, Access Point Names) and/or forbidding the calls. Once the subscription has been modified, the VPMN is notified so that it can update the subscriber's information. Nevertheless, if the destination operator does not accept the messages used to notify it or the version of the messages, it will not update the subscriber's subscription. The problem occurs not only when the update is not made but also when the error is not notified. Then the HPMN considers that the update has been made and the subscribers keep on generating expenses that will not be possible to collect afterwards.
- One very frequent breakdown stemming from interoperability involves barrings, especially in multivendor VPMN, because the functioning tests that are conducted before completing the roaming agreement take place in one single switching center. If the manufacturer of this center is different from the manufacturer of the center where the roaming subscriber is located, both may behave differently, which could lead to problems. A frequent example involves a subscriber who has a barring on outgoing calls (possibly because he does not pay or because he is a prepaid subscriber and there is no CAMEL/WIN agreement, etc.) and who is located in a switching center of the VPMN with this breakdown. When receiving notification from the HPMN about a barring of all outgoing calls (BAOC) of the HPMN network, the switching center in the VPMN does not process this information well, and therefore the subscriber can keep on calling.

Type 1.B. Delays in the information transmission: This type of fraud takes advantage of the window of opportunity, that is, the time between the instant at which the fraud starts being perpetrated and that at which it is detected and certain measures to combat it are implemented. This exposure is essentially determined by the time it takes to send the tariff-setting information from the VPMN to the HPMN and the time it takes the employee to investigate the possible existence of fraud (see Section IV). The fraudster uses one of the fraud techniques described herein or some other new technique, and chooses for its application those networks whose information transmission times are greater, thus increasing the amount of the losses.

Type 1.C. Network configuration flaws: These flaws are triggered by operation and maintenance procedures whose quality is insufficient or else by staff without adequate training. In this regard, some examples can be cited:

- Operators that do not protect their Short Message Service Centers (SMSC). When these SMSCs receive short messages from subscribers other than their own subscribers, they process them but then are unable to charge for them afterwards.
- Roaming subscribers that dial premium rate numbers (entertainment or adult calls) of an operator that is different from the visited operator. Normally this is not allowed in the interconnection agreement, and there are problems to determine which operator pays what to the third country (to which the premium rate numbers belong). The VPMN should prevent these calls from being made, but a faulty configuration could make these scenarios possible. Furthermore, if there is an agreement for the use of CAMEL/WIN, it is the HPMN that should configure the destination numbers to prevent this fraud to the greatest extent possible.

Type 2. Fraud caused by flaws in other areas of the business: This type of fraud stems from inefficient or poorly designed processes in the business or else because of technical aspects not directly related to the telecommunication network. Some examples of fraud of this kind are described below:

Type 2.A. Subscription fraud: Mentioned earlier, this type of fraud involves an impostor subscriber who obtains cards to make calls using various fraudulents techniques, ranging from giving a false identity (normally to the phone operator who handles the hiring) to current accounts or credit cards that do not exist or do not have a sufficient balance. The cards are later sent abroad and can be used to obtain some kind of benefits. The most common uses for this type of card are indicated below:

- *Call selling:* Variants ranging from phone rentals to phone shops that make it possible to make phone calls.

- *Call forwarding / multiconference call:* Local call services can be supplied to the fraudulent number, which shall be forwarded to an international number of simply to a more expensive number. One of the variants that can also be used is connecting two subscribers in a multiconference call using the fraudulent card.

- *Micropayment fraud:* Micropayment is a payment variant that makes it possible to make small payment amounts through a mobile phone. The price of the purchase, which usually involves a low amount, is charged directly to the phone bill. It is obvious that this type of fraudulent card will generate losses that could end up by being quite substantial for the operator.

- *Calls to premium rate numbers:* The fraudster may use the cards to make calls to premium rate numbers that he owns, thus obtaining benefits. Each card can be used to make even various calls at the same time, for the purpose of getting the most benefit in the least amount of time.

- *International Revenue Share Fraud* (IRSF): In certain aspects, this type of fraud is similar to the preceding one (premium rate). In this case, after the subscription fraud, long calls are made to high-cost international destinations (for example, typically from nations that correspond with small islands or number ranges of satellite service). As a rule, the calls do not reach the geographical destinations that would pertain to them but rather are routed by an intermediate operator to a third provider that has a shared payment service (for example, audiotext). Sometimes, this routing takes place even without the consent of the owner of the numbering range. Thus, the shared payment service provider obtains the benefit of these calls while not paying the operator with which it owns the fraudulent subscription. This type of fraud has been widely documented by GSMA [9], and black lists of fraudulent or suspicious numbering have been drawn up.

Type 2.B. Frauds of internal origin: This type of fraud is carried out by the staff belonging to the companies themselves because of defective internal security systems or performance protocols that are too permissive. Some variants consist of the theft of SIM cards and their subsequent activation, when access is gained to the company's supply systems. This type of fraud is very frequent when it involves the theft of roaming scenario test cards and their subsequent use.

Type 2.C. Fraud in M-commerce: M-commerce or mobile commerce is the mobile phone variant of e-commerce or online purchases via Internet. The presence of 3G networks makes it possible for the mobile terminal to handle purchases on Internet by buying credit cards. These false or stolen credit cards, when they are used to purchase products offered by the operator itself, entail fraud costs for the latter. It must be pointed out that this type of fraud is identical to the fraud perpetrated in e-commerce environments. In this case, the mobile platform makes it possible to gain access to mobile phone subscribers to commit the fraud.

Type 2.D. Copyright and hacking fraud: New downloading services (music, video, logos, etc.) involve copyright costs for operators. This means that possible hacking that enables these contents to be copied without any prior payment also incurs fraud costs.

It should be noted that, of all the fraud types described, only in the last two will the fact that they take place in roaming scenarios not have any special repercussions, because the costs shall actually be identical to those that would occur if the fraud took place in other scenarios. The remaining fraud types shall be especially critical when they take place in roaming environments, mainly because of the three causes that have already been pointed out: longer time to detect, greater response time, and greater technical difficulties in tackling the problem.

IV. ROAMING FRAUD PROTECTION SYSTEMS

A fraud protection system is a system that uses the HPMN for the purpose, as it names indicates, of reducing to the greatest possible extent both the possibility of being the victim of fraud and the impact of fraud if it ever does take place. A system to protect against fraud must consist of the stages indicated in Fig. 4. First of all, there is a prevention stage, in which the measures aimed at preventing and therefore hampering the perpetration of fraud are established. Alongside this prevention stage, the remaining stages are implemented in sequence. In the data collection stage, the billing data and also possible notifications of fraudulent use by the VPMNs are received. Subsequently, there is a detection stage, during which the data that have been received are reviewed to locate fraudulent behavior patterns. The result of this stage shall consist of a list of subscribers with possibly anomalous behavior, which shall be sent to the surveillance stage, at which time the departments specializing in fraud or an outsourced company shall examine these high-risk cases to decide whether they should act upon the information or not. Finally, if action is required, in the response stage the mechanisms that are needed to put a stop to the evolution of the fraud are activated.

A key parameter to evaluate a fraud prevention system is the average time of resolution, T_R, that is, the time that elapses between the first call or fraudulent action until the related response measures actually resolve the problem. In addition, the complexity and cost of the system's implementation and maintenance must be taken into account.

In this regard, it can be said that, just as in any other security system, the level of security that is provided by a fraud protection system shall be determined by the lowest security levels provided by each of its stages.

It can be said that, over the past years, highly valuable efforts have been made to improve fraud protection systems. Nevertheless, it seems that most of these efforts have focused on improving data collection. There is still much work that needs to be finished in the remaining stages before the complete system can become fully developed.

Each one of the stages comprising a fraud protection system is examined in greater detail below.

A. *Fraud prevention stage*

This stage is comprised of certain preventive measures that try to hamper the perpetration of fraud. In this regard, there are many measures that have been proposed and applied for this stage, among which the following are noteworthy:

- Service restrictions when the subscriber is in roaming: this measure intends to implement a strategy that consists of gradually activating the services to the subscriber as the subscriber proves to be trustworthy. There are various possibilities [10]: from the gradual activation of the roaming for customers to offering selective roaming to and from given operators only, restricting calls to premium rate numbers when it is in roaming, preventing the forwarding of international calls in roaming, limiting the duration of the phone calls, etc. It should be pointed out that this type of measure, although helping fraud prevention, has a direct impact on the quality of the service provided to the customer since the latter will have to be concerned about the activation of these services after prior justification to the operator.

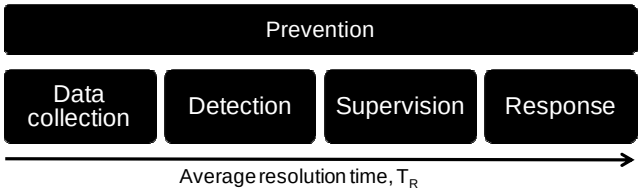

Fig. 4. Stages comprising a fraud protection system.

- Optimization of roaming agreements: It is important to consider, in roaming agreements, all aspects that might arise in service delivery, in order to eliminate subsequent problems. In this regard, it is important to apply the recommendations made by certain organizations such as GSMA or CDG (CDMA Development Group) regarding these agreements [3].

- Conducting thorough roaming tests: This kind of test curtails the possibility of suffering from fraud types 1.A and 1.C (see Section III). They are tests involving not only the delivery of roaming services but also the processing of the billing files, interoperability, etc. To conduct these tests, it is advisable to use the equipment of various providers in each network (HPMN and VPMN). Furthermore, there are recommendations proposed by GSMA and CDG about the test protocols to be run [3] [11].

- Prevention of subscription fraud (type 2.A): To avoid this kind of fraud, there is a series of recommendations [11] essentially aimed at optimizing the business processes related to customers and distribution. Some of the measures that are being proposed in this regard are the validation of the information provided by the subscribers from certain databases, such as electoral registers or black lists on fraud, requesting payment collateral, enhancing distribution staff training regarding fraud issues, monitoring customer credit, drawing up a structure to punish fraud, etc. Certain after-sale procedures are also advisable, such as those aimed at checking the data of customers, by sending postcards to the addresses that are given, making phone calls to the contact information, requesting an e-mail reply, etc.

B. *Data collection stage*

Optimization of this stage is crucial to reduce the average time for resolving problems, T_R. It is advisable to reduce to the utmost this lapse of time because that is how it may be possible to eliminate cause 1.B of the perpetration of fraud, that is, delays in transmitting information (see Section III).

Most CDMA operators in the Americas 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 implies that reducing fraud risk because of this stage is great [12].

In the GSM world, however, various techniques have been proposed, examined, and implemented. The main proposals made to date for the implementation of this stage are as follows:

- **HUR (High Usage Report):** Defined by the GSMA in [13], it consists of VPMN monitoring of the billing records related to the many subscribers in roaming. If a subscriber goes over a given spending threshold, a notification is sent to the HPMN, which shall do the investigation using a fraud manager to determine if there is any fraud or not. The spending threshold is set in the bilateral contract between the operators. This system, which is proposed as mandatory by the GSMA until September 30, 2008, has two fundamental drawbacks. First of all, the time lag involved to receive the reports is long, because the reports depend on the billing cycles (it can take up to 36 hours to send a TAP billing file). In addition, they provide limited information on the fraud scenario and you may have to wait for the complete billing information before obtaining an overall perception of the problem.

- **FIGS (Fraud Information Gathering System):** Defined by the 3GPP [15], it is a solution based on the exchange of CAMEL signalling between the operators, so that the VPMN can send to the HPMN the CDRs pertaining to a given number of subscribers. This system does have 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, it assumes the rollout of CAMEL in the operators, which is not always the case. Finally, if there is a CAMEL signalling, specific training in these procedures is required for the technical staff.

- **Monitoring signalling connections:** Monitoring of the signalling provides information that makes it possible, under certain circumstances, to facilitate the task of finding patterns of fraudulent behavior. The information is usually obtained from communication between the visited VLR and the HLR. Thus, the behavior of certain IMSIs can be observed to obtain certain data such as the level or charge of requests made or the identity of the networks that issues these requests. Although this system is a possible source of information, it can only be considered as complementary to others, because the information provided does not make it possible to qualify a certain behavior as fraud and also because the information itself can be biased by behaviors such as very long calls that generate little charges or bad configurations of the management of authentification triplets in the VPMN, which generate a high charges although there many not be many calls.

- **NRTRDE (Near Real Time Roaming Data Exchange):** Developed by GSMA, the purpose of this scheme is the transmittal of CDRs to the HPMN in almost real time. Concretely, there is a 4-hour time-limit for the transmittal of the CDRs [6]. This scheme has been recommended over the past years by GSMA for implementation and shall be mandatory as of October 2008. In addition to the substantial decline in lags with respect to the time for transferring information, it also has other advantages. The fact that billing information is sent by another information stream that is separate from the TAP files makes it possible to compare the CDRs to detect inconsistences and to check the integrity of one system or another. Although it is a considerable improvement over the previous systems, it also has some drawbacks that must be pointed out. First, there are few incentives for the VPMN to roll it out because the principal beneficiary is the HPMN. In addition, receiving an extra stream of CDRs to the TAP files requires investment in additional processing and storing systems. Finally, with regard to schemes such as HUR, in which the information is previously filtered, in the case of NRTRDE, additional processing of information shall be needed to infer alarms of fraud. The latter can also be considered an advantage, since NRTRDE provides more information and, therefore, the detection systems based on this information can be better adjusted, thus reducing the rate of positive falses.

- ***Monitoring data traffic:*** Since the subscriber's roaming data traffic flows between the SGSN of the VPMN and the GGSN of the HPMN, it is possible for the HPMN to monitor this traffic as if it were generated in the network itself. To do this, the use of systems called RTC (Real Time Charging in prepay or Roaming Traffic Control in postpay), which are located on the data route between the SGSN and GGSN, is recommended. These systems monitor data traffic in real time, providing this information in the detection stage.

Finally, for this stage, it must be indicated that, although an operator uses systems for the exchange of information in real time with another operator (as customarily occurs between operators with CDMA technology), from the time it draws up a roaming agreement with another operator that does not implement it, it is vulnerable to all the problems that appear in the previously described techniques.

C. Detection stage

The detection stage receives all the information generated in the data collection stage and must decide whether a behavior is anomalous or not. In this stage, the so-called Fraud Management Systems (FSM) performs a crucial role. They are automatic systems that process the billing information to find patterns of fraud. The simplest method they apply relies on detection based on rules or signatures (for example, when a call is over 30 minutes, an alarm signal is transmitted). Some of them also make it possible to use profiles for different groups of subscribers or even for individual subscribers, and

the rules that are applied are adapted on the basis of the profile considered. In addition, certain more complex FMSs use learning algorithms such as neural networks to infer, on the basis of subscribers' observed behavior, the rules to be applied for the detection.

There are many commercial systems, in this field, that are trying to open up the market or that are consolidated. Among them can be cited some solutions provided by companies such as Mach [17], Syniverse [18], FairIsaac [19], Agilent [20], Starhome [21], ecTel [22], gmv [23], etc.

Finally, it must be indicated that the systems for data traffic monitoring in real time (RTC) also incorporate detection capabilities and thus make it possible to observe possible behaviors of fraud.

D. Surveillance stage

Alleged incidents of fraud whose data are notified by the detection system must be thoroughly reviewed before concluding definitively that the event that has been observed is indeed a fraud. This review is conducted essentially by the company's fraud department or by an outsourced specialized company.

The principal difficulties arising from this stage are those due to the lags that occur in conducting the investigation itself of fraud. These lags become considerably longer when the notifications of the detection system take place during offhours. In many of these cases, the companies have not envisaged any plan of action. This lack of planning renders useless the efforts and investments that have been made in other stages of the protection system to reduce the average time of response. In fact, this scenario is more frequent than might be expected at first sight, because international fraud networks are aware of the limitations of companies in this respect and take advantage of these timings of exposure to perpetrate their fraud.

E. Response stage

If in the surveillance stage it is concluded that the fraud is taking place, it is necessary to act and abort the fraudulent action. To do this, it is advisable, first of all, to have the HPMN suspend the calls or services that are being used at that time, and, second, to prevent the fraud from continuing. Another less intrusive type of solution can also be opted for, such as a prior notification to the customer to avoid affecting the service in those cases where there really is no fraud (false positives).

To prevent any further use of services, the fraudulent subscriber's subscription is altered to at least prevent the generation of SMS (modification of the TS22), barring all outgoing calls (BAOC) and all incoming calls in roaming (BAIC roam), and preventing connection to data APNs.

Regarding the suspension of calls and services, if there is a CAMEL agreement with the VPMN, it can be done in real time by using the ISR (Immediate Service Termination) functionality [24]. Another alternative that does not involve the suspension in real time of the services consists of notifying the VPMN by some established means (e-mail, phone call, etc.) and the management of the suspension by the VPMN.

V. Reviewing and Planning the Future of Roaming Fraud Protection

This section intends to raise certain questions that would make it possible to determine the current status of the fight against roaming fraud and motivate future planning in this field. They are questions that should be tackled by the principal stakeholders involved in roaming fraud prevention, that is, mobile telephony operators, providers, government and financing entities, analysts, etc., and that try to encourage debate to draw up a working agenda.

Starting point:

Magnitude of the problem

- What is the current magnitude or impact of losses stemming from fraud in general? And from roaming fraud?
- How frequent are these frauds and what percentage share of subscribers are fraudulent?
- What percentage of roaming fraud is produced in your operator by incoming subscribers? And by outgoing subscribers?

Fraud protection systems

- Have functional fraud protection systems been installed?
- What are the principal deficiencies in the systems that have been installed?
- What stage involves the most problems?
- What are the costs (OPEX and CAPEX) associated to the establishment of fraud protection systems?
- What impact do the roaming service barring measures have on business development?
- What is the status of investments for the rollout of NRTRDE? What difficulties prevent this type of investment from being made?

Political-social environment

- What percentage share of the population or what sectors could potentially benefit from the impacts of roaming fraud (sale of calls, etc.)?
- What level of social permissiveness is there with respect to roaming fraud?
- In addition to the repercussions for the performance accounts of operator companies, what economic sectors is roaming fraud affecting indirectly?
- What do national legislatures prescribe with regard to the benefits obtained from roaming fraud?
- Are there business opportunities or market niches that are not being tapped because of the fears about roaming fraud?

Future planning:

- Is more restrictive lawmaking needed to prevent roaming fraud?
- In what areas does investment have to be made to prevent roaming fraud?
- Are new techniques needed to improve the average time for resolving incidents of fraud?
- Would certain policies for subsidizing operators be suitable to improve fraud prevention systems?
- In view of the evolution of 3G systems, are functional or departmental structures of unidisciplinary review in companies valid? For example, would it make sense to have a network security department separate from the fraud management department?
- Is roaming fraud considered to be more deleterious for business development among small operators?
- What type of collective action do you believe might be tackled to reduce roaming fraud? For example, building up GSMA in Latin America, supporting the weaker operators to prevent technical problems (type 1 frauds), stemming from them, etc.

VI. Conclusion

The present article has discussed the methodologies used to perpetrate fraud in roaming environments and possible fraud protection strategies that have been proposed to date.

Furthermore, a methodology has been proposed to examine the current status of the roaming fraud problem and to draw up a working agenda in this area.

The present paper is suitable for review at workshops on roaming fraud attended by the sector's principal stakeholders, that is, mobile telephony operator companies, suppliers and manufacturers, analysts, government lawmakers, and the financial sector. Along this line, certain initiatives are of the utmost important such as the one drawn up by IIRSA/CITEL to study the current roaming services scenario in South America.

References

[1] K. Wieland, The last taboo? Revenue leakage continues to hamper the telecom industry, *Telecommunications (International Edition)* 38 (2004), pp. 10–11.
[2] Mach, White Paper on Fraud Protection, Nov. 2007, Available at: www.mach.com
[3] GSMA, PRD BA.40, v4.1, Roaming guide, Sept. 2006.
[4] GSMA, PRD TD.58, v1.6, TAP3 Implementation Handbook, Dec. 2007.
[5] GSMA, PRD BA.41, v4.0, IOT Handbook, Aug. 2007.
[6] GSMA, PRD BA.08, v19.0, Timescales for Data Transfer, May 2007.
[7] M. Johnson, Revenue Assurance, Fraud & Security in 3G Telecom Services, Journal of Economic Crime Management, 1(2), 2002.
[8] J. Hynninen, Experiences in Mobile Phone Fraud, Available at: citeseer.ist.psu.edu/hynninen00experiences.html
[9] GSMA, PRD FF.17, v2.0, International Revenue Share Fraud, Oct. 2007.
[10] GSMA, PRD FF.06, v3.0, Advice on Roaming Services, Oct. 2000.
[11] CDG #52, IS-41 Interworking Test Specification, Ver. 1.0, April 12, 2004.
[12] GSMA, PRD FF.01, v2.0, GSM Subscription Fraud Management Guidelines, Aug. 2006.
[13] CDG #117, Inter-standard Roaming White Paper, Ver. 2.0, Dec. 5, 2005.
[14] GSMA, PRD FF.04, v2.3, High Usage Report Format and Contents, Oct. 2007.
[15] 3GPP, ETSI TS 101 107, v8.0.1, Fraud Information Gathering System (FIGS), Service Description, June 2001.
[16] GSMA, PRD FF.02, v3.0, Fraud Management Systems – Guidelines to GSM operators, June 1996.
[17] http://www.mach.com
[18] htpp://www.syniverse.com
[19] http://www.fairisaac.com/fic/en
[20] http://www.agilent.com
[21] http://www.starhome.com
[22] http://www.ectel.com
[23] http://www.gmv.es
[24] 3GPP, ETSI TS 101 749, v7.1.1, Immediate Service Termination (IST), Service Description, Aug. 1998.

Glossary

APN: Access Point Name. In a GPRS network, it defines each one of the possible configurations that a user has to connect with different data networks.
BAOC: Barring of All Outgoing Calls. Restriction of outgoing calls for a subscriber. This restriction takes place in the HLR of the HPMN.
CAMEL: Customized Applications for Mobile Networks Enhanced Logic. Type of intelligent network signalling that makes it possible to offer in roaming the same services as those offered when the subscriber is in his source network. Used in GSM networks.
CDR: Call Detail Record. Tariff-setting record with the information of a voice call.
CIBER: Cellular Intercarrier Billing Exchange Roamer record. Standard used in CDMA networks consisting of the compilation of CDRs in files for sending from the VPMN to the HPMN.
DCH: Data Clearing House. Service provided to operators in roaming, comprised of handling the sending and receiving of TAP files as the only interface for the operator that hires it.
FIGS: Fraud Information Gathering System. CAMEL-based data-gathering system.
GSM: Global System Mobile. Mobile communication system standardized by ETSI.
GSMA: GSM Association. Association of GSM operators.
GGSN: Gateway GPRS Support Node. Data network node.
HLR: Home Location Register. Database with the subscriptions of the subscribers and their characteristics.
HPMN: Home Public Mobile Network. Proprietary network of the subscription of a subscriber in roaming.
HUR: High Usage Report. Report that the VPMN sends to the HPMN when possible fraud situations are detected. They only reflect information about potentially fraudulent subscribers.
IOT: Inter-Operator Tariff. Tariffs agreed upon between operators for roaming services.
IST: Immediate Service Termination. Functionality of the intelligent network that makes it possible to finalize a call when it is active.
MSC: Mobile Switching Center. Voice network switching center.
NRTRDE: Near Real Time Roaming Data Exchange. Systems for gathering data in almost real time. Specified by GSMA.
RTC: Real Time Charging / Roaming Traffic Control. System for roaming data traffic monitoring in real time.
SGSN: Serving GPRS Support Node. Data network node controling the mobile's access to the network. It is equivalent to MSC in a data network. In a roaming scenario it is located in the VPMN.
SMSC: Short Message Service Center. It is in charge of receiving short messages from its own subscribers and sending them to their destinations.
TAP: Transfer Account Procedure. GSMA standard, which consists of a file compiled with information on roaming tariff-setting records.
UDR: Usage Detail Record. Record of tariff-setting with information on the use of a service.
VPMN: Visited Public Mobile Network. Network visited by a roaming operator.
WIN: Wireless Intelligent Network. Type of intelligent network signalling that makes it possible to offer in roaming the same services as those when the subscriber is in his source network. Used in CDMA networks.