El fraude en roaming: estrategias de ataque y de defensa

Gabriel Maciá-Fernández*, Universidad de Granada (España)

***Resumen*— El fraude es uno de los aspectos que más preocupan en el sector de las telecomunicaciones. Genera cantidades importantes de pérdidas financieras en dicho sector cada año. Para las operadoras de telefonía móvil, una de las grandes contribuciones a las pérdidas por fraude viene dada por aquél que se produce en escenarios de roaming. En este artículo se pretende realizar un análisis de las causas que generan estos tipos de fraude y de las estrategias y medidas encaminadas a defender a las operadoras contra el mismo. A modo de metodología de estudio se propone, además, una serie de cuestiones a debatir entre los principales agentes implicados en la prevención del fraude en roaming, con el fin de elaborar una agenda de trabajo para la mejora de las perspectivas en este sector.**

I. INTRODUCCIÓN

La mayor causa de pérdida de ingresos en el área de la industria de telecomunicaciones es el fraude [1]. En el campo de las telecomunicaciones móviles, uno de los aspectos de negocio que más contribuye a la pérdida de ingresos debidos al fraude es el roaming [2]. El servicio de roaming permite a abonados de una red móvil, denominada red propietaria (en adelante HPMN, del inglés *Home Public Mobile Network*), utilizar los servicios ofertados por dicha red mediante el acceso a través de una red diferente, denominada red visitada (en adelante VPMN, del inglés *Visited Public Mobile Network*).

Debido a la evolución de los servicios que se ofertan por los operadores de telecomunicación, las redes internacionales de fraude han ido desarrollando técnicas complejas de fraude que permiten generar pérdidas considerables en los ingresos de una compañía. Estas pérdidas son posteriormente repercutidas, posiblemente, en las tarifas que dichas compañías cobran a sus abonados, produciendo un incremento de los precios.

Es preciso, por consiguiente, tanto para los operadores como para los gobiernos y usuarios, establecer y facilitar medidas de tipo técnico, político, económico y social que dificulten la existencia de fraude en este campo. El éxito en esta empresa repercute en el beneficio de todos los agentes implicados excepto en el de los estafadores.

En esta línea, este artículo trata de aportar una visión sobre el problema del fraude en entornos de roaming y las diferentes estrategias o técnicas para abordar su solución. Para ello, se realiza una clasificación y descripción tanto de las técnicas de fraude como de los métodos de defensa asociados, analizando las ventajas e inconvenientes de cada uno de ellos. Finalmente, también se pretende definir una serie de cuestiones por resolver para continuar en la lucha contra este tipo de fraudes.

La estructura de este artículo es la siguiente: en el Apartado II se realiza un repaso de las principales nociones sobre el funcionamiento del servicio de roaming. En el Apartado III se realiza una clasificación de las diferentes estrategias de fraude más comunes. Las técnicas de defensa contra el fraude en roaming están descritas y analizadas en el Apartado IV. El apartado V propone una metodología para la revisión y planificación del futuro en la lucha contra el fraude en roaming. Finalmente, se concluye con el Apartado VI.

II. NOCIONES SOBRE ROAMING

El roaming es la capacidad de los abonados de una red inalámbrica para realizar o recibir llamadas de voz, enviar o recibir datos, o acceder a otros servicios cuando se encuentran fuera de la zona geográfica de cobertura de su red propietaria, por medio del uso de los recursos de una red visitada.

Se puede, por tanto, concluir, que en el roaming intervienen tres principales agentes: el abonado, que es quien utiliza los servicios, la red propietaria o HPMN, que es la que posee la suscripción del abonado, y la red visitada o VPMN, en cuya zona geográfica de cobertura el abonado accede a los servicios contratados con la HPMN.

Para posibilitar que los abonados de una operadora puedan hacer roaming en otra VPMN es necesario establecer previamente un acuerdo entre ambas operadoras. Los procedimientos para la realización de estos acuerdos suelen estar normalizados, como por ejemplo los propuestos por parte de la asociación de operadoras GSM (GSMA) [3] y, básicamente, consisten en la firma de unos contratos que establecen las condiciones del acuerdo, y en la realización de unos protocolos de pruebas de tipo técnico para permitir la gestión del servicio entre ambas operadoras.

El roaming se puede hacer tanto para los servicios de voz como los de datos. En el caso de los servicios de voz, la VPMN, previamente a permitir que el abonado se asocie a su

* Gabriel Maciá Fernández es profesor ayudante doctor en la Universidad de Granada (España).
Dirección postal: 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
Tfno: +34-958-241000 (ext: 20048)

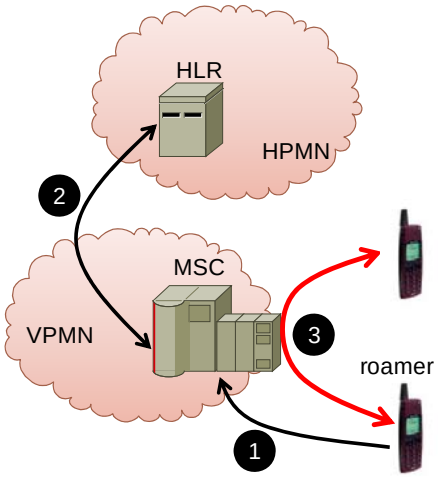

Fig. 1. Escenario de llamada de voz en roaming: 1- solicitud de conexión a la red (MSC), 2- consulta de la MSC sobre la suscripción a la HPMN (HLR), y 3- establecimiento de la conexión de voz.

red (a través de la central de conmutación (MSC) que da cobertura al abonado), realiza una consulta a la HPMN sobre los servicios a los que el abonado está suscrito (información que reside en la base de datos HLR de la que es propietaria la HPMN). Posteriormente, si la suscripción es correcta, permite al abonado el acceso a los servicios que correspondan, por ejemplo, el establecimiento de una llamada de voz. En la Fig. 1 se puede observar un diagrama de este escenario.

El roaming de datos es similar, pero tiene algunas características diferenciadoras importantes. En este caso, el abonado se asocia (previa consulta al HLR) a un nodo denominado SGSN (*Serving GPRS Support Node*). Posteriormente indica a la red móvil el tipo de red de datos a la que se quiere conectar, y se establece un contexto con dicha red de datos a través de un nodo denominado GGSN (*Gateway GPRS Support Node*). La Fig. 2 muestra gráficamente este proceso.

Es importante indicar que, mientras el SGSN pertenece a la VPMN, el GGSN siempre es propiedad de la HPMN, por lo que los datos que se emiten o reciben por el abonado deben transitar necesariamente por la HPMN. Esto no sucede con el tráfico de voz, para el que la interacción entre VPMN y HPMN es, en muchos casos, solamente la consulta inicial al HLR. Esto exige que, para poder tarificar los servicios, tanto de voz como de datos, la VPMN deba enviar la información recopilada sobre las llamadas realizadas y los datos transmitidos por el abonado a la HPMN. Estos datos vienen recogidos en unos registros de tarificación denominados CDR (*Call Detail Record)* o más genéricamente UDR (*Usage Detail Record*). La VPMN, que debe cobrar según los servicios prestados, envía esta información a la HPMN agrupando los CDRs en unos ficheros con una estructura definida. El estándar más utilizado en las redes GSM para estos ficheros ha sido definido por la GSMA y se denomina TAP (*Transfer Account Procedure*) [4], mientras que en las redes CDMA se utiliza CIBER (*Cellular Intercarrier Billing Exchange Roamer record)*.

Una vez recibidos los ficheros TAP/CIBER, la HPMN debe liquidar la deuda con la VPMN según las tarifas establecidas en los acuerdos de roaming (IOT, *Inter-Operator Tariff*) [5].

Para ahorrar a las operadoras que tienen un alto número de acuerdos de roaming la tarea de gestionar el envío y recepción de los ficheros TAP/CIBER a cada uno de los operadores con acuerdo, se hace uso de ciertas compañías que hacen de centro de intercambio para estos datos (se las denomina DCH, del inglés *Data Clearing House*). De este modo, el DCH es la única interfaz para el operador y se encarga de gestionar todos los aspectos relativos a la transmisión y recepción de los ficheros TAP/CIBER con la operadora que contrata este servicio.

III. El Fraude en Roaming

Cuando una VPMN cursa llamadas o servicios de un abonado de la HPMN, genera los CDR correspondientes y los envía a la HPMN según los procedimientos y plazos establecidos [6]. Posteriormente deberá cobrar de la HPMN las cantidades que se adeudan. Por su parte, la HPMN repercutirá la cantidad que corresponda al abonado. Ahora bien, cuando el abonado accede al servicio de forma fraudulenta, la HPMN no podrá cobrar a dicho abonado la cantidad que corresponde, por lo que la operadora incurre en pérdidas.

Se puede decir que el fraude en escenarios de roaming no es más que la extensión de las técnicas de fraude en escenarios convencionales. Sin embargo, estos tipos de fraude poseen unas características propias que los hacen más perjudiciales desde el punto de vista de las pérdidas que ocasionan [7] [8]. Estas características son:

- *Mayor tiempo de detección:* dado que el fraude se produce desde una red diferente a la del abonado, el tiempo en detectar

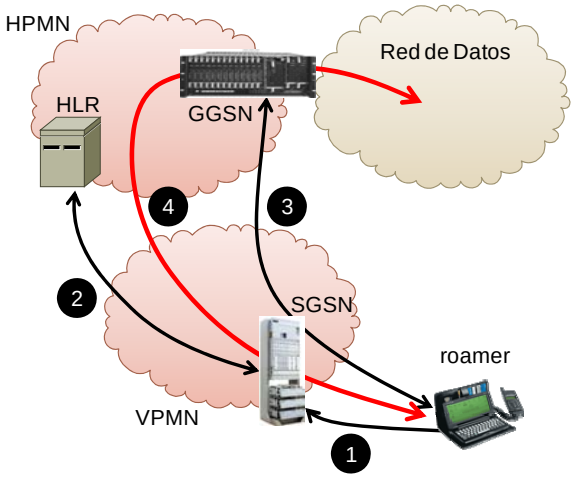

Fig. 2. Escenario de llamada de datos en roaming: (1) solicitud de conexión a la red (SGSN), (2) consulta del SGSN sobre la suscripción a la HPMN (HLR), (3) petición de establecimiento del contexto al GGSN, y (4) establecimiento de la conexión de datos.

la situación de fraude es mayor, debido principalmente a que deben existir protocolos de comunicación entre ambas redes que no siempre son suficientemente ágiles.

- *Mayor tiempo de reacción:* una vez se ha detectado el fraude, las dificultades de tipo técnico y administrativo para evitar que continúe generándose son mayores que si el operador estafado tuviera el control de todos los sistemas a su alcance.

- *Más dificultades técnicas en la solución:* los sistemas de prevención, detección y respuesta automática contra el fraude tienen mayor complejidad, debido principalmente a la heterogeneidad de las redes VPMN y HPMN involucradas, lo que hace que, en muchos casos, los protocolos de actuación fallen y, por consiguiente, el fraude sea mayor.

Tradicionalmente, la principal técnica utilizada para cometer fraude en las redes de telecomunicación ha sido la conocida como fraude de suscripción, esto es, un abonado se da de alta con información personal errónea o con una cuenta bancaria falsa, y utiliza el teléfono para hacer llamadas, normalmente de alto coste. Sin embargo, la evolución de las redes de telecomunicación (desarrollo del 3G) y la aparición de nuevos y más complejos servicios ha provocado que las redes criminales organizadas internacionalmente hayan desarrollado nuevas estrategias y plataformas tecnológicas para el fraude que permiten provocar considerables pérdidas a los operadores.

Según el método que se sigue para cometer un fraude, se puede presentar una clasificación de los fraudes en roaming según el esquema mostrado en la Fig. 3.

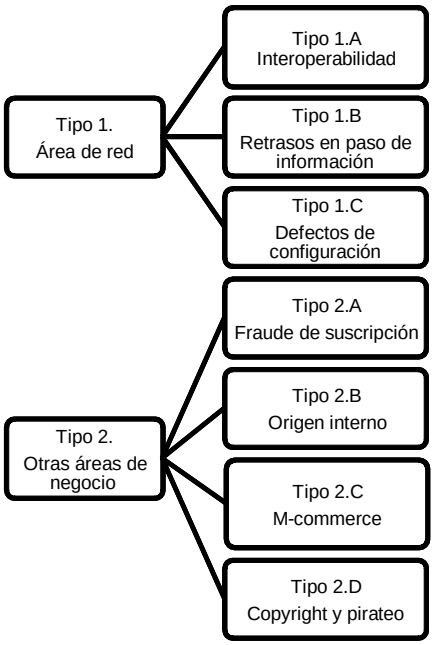

Fig. 3. Clasificación de los métodos de fraude en entornos de roaming.

Tipo 1. Fraudes por causas técnicas en la red: tratan de aprovechar fallos de tipo técnico en la configuración, diseño o arquitectura de las redes de comunicación de las operadoras. Las causas más comunes que permiten la aparición de estos fraudes son:

***Tipo 1.A. Fallos de interoperabilidad**:* son errores en el funcionamiento esperado entre los equipos de red de los operadores. Estos fallos vienen comúnmente provocados por la existencia de tecnologías diferentes y/o por la existencia de equipos de varios proveedores (entornos *multivendor*). Veamos algún ejemplo:

- Abonado de tipo prepago en roaming GSM que se queda sin saldo, o de tipo postpago con control de consumo que llega al tope. Si no existe algún mecanismo que permita controlar la llamada cuando ésta se encuentra activa (mediante un tipo de señalización estándar denominada CAMEL en GSM y WIN en CDMA), para evitar que se siga generando gasto con nuevas llamadas, la HPMN modifica la suscripción del abonado desactivando el servicio TS22 (SMS originante), cambiando su perfil GPRS (prohibiendo ciertos APNs – *Access Point Name*) y/o prohibiendo las llamadas. Una vez modificada la suscripción, se notifica a la VPMN para que ésta actualice la información del abonado. Sin embargo, si la operadora destino no acepta los mensajes con los que se notifica o la versión de los mismos, no va a actualizar la suscripción del abonado. El problema sucede cuando no sólo no la actualiza sino que, además, no notifica el error. Entonces la HPMN considera que se ha actualizado y el abonado sigue generando gasto que posteriormente no se podrá cobrar.
- Un fallo muy frecuente debido a la interoperabilidad es relativo a las restricciones en las centrales (*barrings*), sobretodo en VPMN multivendor, ya que las pruebas de funcionamiento que se hacen antes de completar el acuerdo de roaming se realizan en una única central. Si el fabricante de dicha es distinto del de aquella en la que el abonado en roaming se encuentra, ambas pueden comportarse de forma distinta, lo que puede dar problemas. Un ejemplo frecuente sucede cuando un abonado tiene una restricción de llamadas salientes (debido posiblemente a que no paga, o bien a que es prepago y no hay acuerdo de CAMEL/WIN, etc.) y se localiza en una central de la VPMN con este fallo. Al recibir notificación de la HPMN sobre una restricción de llamadas salientes (BAOC) de la red HPMN, la central en la VPMN no interpreta bien esta información, por lo que el abonado podrá seguir llamando.

Tipo 1.B. Retrasos en el paso de información: estos fraudes aprovechan la ventana temporal que existe desde el instante en que comienzan a cometerse hasta que son detectados y se ejecutan medidas de reacción contra los mismos. Esta ventana temporal viene determinada, fundamentalmente, por el tiempo que tarda la información de tarificación en ser enviada desde la VPMN hasta la HPMN, y el empleado en investigar la posible existencia de fraude (ver Apartado IV). El estafador utiliza alguna técnica de fraude de las aquí relacionadas o alguna nueva, y como lugar de

ejecución para el fraude elige aquellas redes cuyos tiempos de paso de información sean mayores, aumentando así la cuantía de las pérdidas.

Tipo 1.C. Defectos en la configuración de la red: estos fallos son provocados por procedimientos de operación y mantenimiento con insuficiente nivel de calidad, o bien por la existencia de personal sin un entrenamiento o capacitación adecuados. En este sentido también se pueden citar algunos ejemplos:

- Operadoras que no protegen sus SMSC (centros servidores de mensajes cortos). Al recibir dichos SMSCs mensajes cortos de abonados que no son suyos los cursan, no pudiendo posteriormente cobrarlos.
- Abonados en roaming que marcan números *premium rate* (llamadas de entretenimiento o de adultos) de un operador distinto al visitado. Esto normalmente no está permitido en el acuerdo de interconexión y hay problemas para determinar qué operadora paga qué al tercer país (al cual pertenecen los números premium rate). La VPMN debería impedir estas llamadas, pero una configuración defectuosa permitiría la existencia de estos escenarios. Por otro lado, en caso de que exista acuerdo para el uso de CAMEL/WIN, es la HPMN la que debería configurar los números de destino, para evitar lo más posible este fraude.

Tipo 2. Fraudes causados por defectos en otras áreas del negocio: este tipo de fraudes tienen como causa la existencia de procesos ineficientes o mal diseñados en el negocio, o bien por algunos aspectos técnicos no relacionados directamente con la red de telecomunicaciones. Algunos ejemplos de fraudes de este tipo se relacionan a continuación:

Tipo 2.A. Fraudes de suscripción: anteriormente mencionados, en estos fraudes un abonado impostor obtiene tarjetas para hacer llamadas usando para ello diversas técnicas fraudulentas, que varían desde dar una identidad falsa (normalmente a la operadora telefónica que gestiona la contratación), hasta cuentas corrientes o tarjetas de crédito inexistentes, o bien con insuficiente saldo. Las tarjetas son posteriormente enviadas al extranjero y pueden ser utilizadas para obtener beneficio de alguna forma. Los usos más comunes para este tipo de tarjetas son:

- *Venta de llamadas:* variantes desde el alquiler del teléfono, hasta la existencia de locutorios que permiten realizar llamadas.

- *Desvío de llamadas / multiconferencia:* se pueden ofrecer servicios de llamadas locales al número fraudulento, que será desviado a un número internacional o simplemente a un número más caro. También se puede usar como variante la de conectar dos abonados en multiconferencia mediante la tarjeta fraudulenta.

- *Fraude en micropagos:* el micropago es una variante de pago que permite la realización de pagos de pequeña cantidad a través del móvil. El precio de la compra, usualmente de baja cuantía, es cargado directamente en la factura del teléfono. Evidentemente, la existencia de este tipo de tarjetas fraudulentas generará pérdidas que pueden ser significativas al operador.

- *Llamadas a números premium rate:* el estafador puede utilizar las tarjetas para realizar llamadas a números premium rate de su propiedad, obteniendo de este modo el beneficio. Cada tarjeta se puede utilizar para realizar incluso varias llamadas simultáneas, con el fin obtener un mayor beneficio en el menor tiempo.

- *Fraudes IRSF (International Revenue Share Fraud):* este tipo de fraudes es similar al anterior (premium rate) en ciertos aspectos. En este caso, tras el fraude de suscripción, se realizan llamadas de larga duración destinos internacionales con alto coste (p.ej. típicamente de naciones que se corresponden con pequeñas islas o rangos de numeración de servicios satélite). Las llamadas no alcanzan, generalmente, los destinos geográficos que les corresponderían, sino que son encaminadas por una operadora intermedia hacia un tercer proveedor que posee un servicio de pago compartido (p.ej. audiotexto). A veces, este encaminamiento se realiza incluso sin el consentimiento del propietario del rango de numeración. De esta forma, el proveedor del servicio de pago compartido obtiene el beneficio de estas llamadas, a la vez que no pagará a la operadora con la que posee la suscripción fraudulenta. Este tipo de fraudes ha sido ampliamente documentado por GSMA [9], habiéndose elaborado listas negras de numeraciones fraudulentas o sospechosas.

Tipo 2.B. Fraudes de origen interno: este tipo de fraudes son generados por personal perteneciente a las propias compañías, debido a sistemas de seguridad internos deficientes o protocolos de actuación demasiado permisivos. Algunas variantes consisten en el robo de tarjetas SIM y en su posterior activación, en caso de que se tenga acceso a los sistemas de provisión de la compañía. También es muy frecuente la comisión de este tipo de fraudes mediante el robo de tarjetas de prueba para los escenarios de roaming, y su posterior utilización.

Tipo 2.C. Fraude en M-commerce: el M-commerce o comercio móvil es la variante móvil del e-commerce o comercio en Internet. La existencia de redes 3G permite al terminal móvil realizar la gestión de compras en Internet mediante la compra con tarjetas de crédito. Estas tarjetas de crédito falsas o robadas, cuando se usan para comprar productos ofrecidos por el propio operador, hacen incurrir a éste en costes de fraude. Hay que indicar que este tipo de fraudes es igual al que se produce en entornos e-commerce. En este caso, la plataforma móvil permite el acceso a los abonados en movilidad para la ejecución del fraude.

Tipo 2.D. Fraudes de copyright y pirateo: los nuevos servicios de descarga de contenidos (música, video, logos, etc.) implican la existencia de unos costes de copyright para los operadores. Ello implica que la posible existencia de pirateo que permita copiar dichos contenidos sin previo pago hace también incurrir en costes de fraude.

Hay que notar que, de todos los tipos de fraude mostrados, solamente en los dos últimos no tendrá una especial repercusión el hecho de que sucedan en escenarios de roaming, dado que los costes serán realmente iguales si suceden en otros escenarios. El resto de fraudes será especialmente crítico cuando sucede en entornos de roaming, principalmente debido a las tres causas ya señaladas: mayor tiempo de detección, mayor tiempo de reacción y más dificultades técnicas en la solución del problema.

IV. Sistemas de Protección Contra el Fraude en Roaming

Un sistema de protección contra el fraude es un sistema que utiliza la HPMN con el objetivo de, tal y como su nombre indica, reducir el máximo posible tanto la posibilidad de sufrir un fraude como el impacto de los mismos en caso de que estos sucedan. Un sistema de protección contra el fraude debe constar de las etapas representadas en la Fig. 4. En primer lugar, existe una etapa de prevención en la que se establecen medidas encaminadas a prevenir y, por tanto, a dificultar la comisión de los fraudes. De forma paralela a esta etapa de prevención se suceden en el tiempo, secuencialmente, el resto de etapas. En la etapa de recogida de datos se reciben los datos de tarificación y también los posibles avisos de uso fraudulento por parte de las VPMN. A continuación se produce una etapa de detección, en la que se analizan los datos recibidos para localizar patrones de comportamiento fraudulentos. El resultado de esta etapa será una lista de abonados con posible comportamiento anómalo, que será enviada a la etapa de supervisión. En ella se analizan, por parte de los departamentos especializados en fraude o de una empresa subcontratada, estos casos de alto riesgo para decidir si se actúa sobre ellos. Finalmente, en caso de que sea necesaria una actuación, en la etapa de respuesta se activan los mecanismos necesarios para cortar la evolución del fraude.

Un parámetro clave para la evaluación de un sistema de prevención del fraude es el tiempo medio de resolución, T_R, es decir, el tiempo que pasa desde que se produce la primera llamada o acción fraudulenta hasta que la medida de respuesta asociada resuelve el problema. Además, también debe tenerse en cuenta la complejidad y el coste asociado a la implantación y mantenimiento del sistema.

En este sentido, se puede decir que, al igual que en cualquier sistema de seguridad, el nivel de seguridad que aporta un sistema de protección contra el fraude vendrá determinado por el menor de los niveles de seguridad aportados por cada una de sus etapas.

Puede decirse que, en los últimos años, se han realizado esfuerzos muy valiosos en la mejora de los sistemas de protección contra el fraude. Sin embargo, parece ser que la mayoría de estos esfuerzos se han focalizado en la mejora de la etapa de recogida de datos. Aún queda mucho trabajo por completar en el resto de etapas para que el sistema completo quede completamente desarrollado.

Fig. 4. Etapas constitutivas de un sistema de protección contra el fraude.

A continuación se analizan un poco más detalladamente cada una de las etapas constitutivas de un sistema de protección contra el fraude.

A. *Etapa de prevención del fraude*

Esta etapa está constituida por ciertas medidas preventivas que tratan de dificultar la comisión de fraudes. En este sentido, son numerosas las medidas que se han propuesto y aplicado para esta etapa. Entre ellas se pueden destacar las siguientes:

- Restricción de los servicios cuando el abonado está en roaming: esta medida pretende aplicar una estrategia consistente en activar gradualmente los servicios al abonado cuando se va comprobando que éste es de confianza. Existen varias posibilidades [10]: desde la activación gradual del roaming a los clientes, hasta ofrecer roaming selectivo a desde determinados operadores solamente, restringir las llamadas a números premium rate cuando se está en roaming, impedir el desvío de llamadas internacionales en roaming, limitar la duración de las llamadas, etc. Hay que indicar que este tipo de medidas, aunque ayudan en la prevención del fraude, inciden directamente en la calidad del servicio dado al cliente, ya que éste deberá preocuparse de la activación de los mismos previa justificación a la operadora.

- Optimización de los acuerdos de roaming: es importante considerar, en los acuerdos de roaming, todos los aspectos que puedan surgir en la prestación del servicio, a fin de eliminar problemáticas posteriores. En este sentido, es importante el uso de las recomendaciones de ciertos organismos, como GSMA o CDG (*CDMA Development Group)* respecto a dichos acuerdos [3].

- Realización de pruebas de roaming exhaustivas: este tipo de pruebas reducen la posibilidad de sufrir fraudes de tipo 1.A y 1.C (ver Apartado III). Son pruebas relativas no solamente a la prestación de servicios de roaming, sino también al envío de ficheros de tarificación, interoperabilidad, etc. Para la realización de estas pruebas es muy recomendable utilizar equipos de los diferentes proveedores existentes en cada red (HPMN y VPMN). Por otro lado, existen recomendaciones propuestas por GSMA y CDG acerca de los protocolos de pruebas a realizar [3] [11].

- Prevención de fraudes de suscripción (tipo 2.A): para evitar este tipo de fraudes, existen una serie de recomendaciones

[11] orientadas fundamentalmente a la optimización de los procesos de negocio relativos a la gestión de clientes y a la distribución. Algunas de las medidas que se proponen en este sentido son la validación de la información aportada por los suscriptores contra ciertas bases de datos, como registros electorales o listas negras de fraude, solicitar garantías de pago, incrementar la capacitación del personal de distribución en temas de fraude, auditar con frecuencia los procedimientos aplicados, realizar un control del crédito de los clientes, establecer un régimen sancionador contra el fraude, etc. También son recomendables ciertos procedimientos post-venta, como los encaminados a verificar los datos de los clientes, mediante el envío de cartas postales a la dirección dada, llamadas a los datos de contacto, solicitar la respuesta a un e-mail, etc.

B. Etapa de recogida de datos

La optimización de esta etapa es clave para la reducción del tiempo medio de resolución, T_R. Es deseable reducir al máximo dicho tiempo debido a que, de este modo, se elimina la causa 1.B de generación de fraude, los retrasos en el paso de información (ver Apartado III).

La mayoría de los operadores CDMA en América afrontan esta tarea mediante el intercambio de CDRs en casi tiempo real. Los CDRs sin procesar son recogidos por la VPMN y enviados directamente (sin pasar incluso por los centros de intercambio de datos) hacia la HPMN correspondiente. Esto implica que la reducción del riesgo de fraude debida a esta etapa es grande [12].

En el mundo GSM, sin embargo, se han planteado, analizado e implementado varias técnicas diferentes. Las principales propuestas que se han realizado hasta el momento para la implementación de esta etapa son las siguientes:

- ***HUR*** **(High Usage Report):** definido por el GSMA en [13], consiste en la monitorización, por parte de la VPMN, de los tickets de tarificación asociados a los diferentes abonados en roaming. En caso de que algún abonado supere una cantidad umbral determinada de gasto se envía notificación a la HPMN, la cual investigará mediante un gestor de fraude si éste existe o no. El umbral de gasto se establece en el contrato bilateral entre los operadores. Este sistema, propuesto como obligatorio por el GSMA hasta el 30 de septiembre de 2008 tiene dos desventajas fundamentalmente. En primer lugar, el tiempo que se tarda en recibir los informes es alto, debido a que dependen de los ciclos de facturación (se puede tardar hasta 36 horas en enviar un fichero TAP de facturación). Además, presentan una información limitada sobre el escenario del fraude y posiblemente hay que esperar a la llegada de los ficheros de tarificación completos para tener una percepción global del problema.

- ***FIGS*** **(Fraud Information Gathering System):** definido por el 3GPP [15], es una solución basada en el intercambio de señalización CAMEL entre los operadores, de modo que la VPMN puede enviar a la HPMN los CDR's correspondientes a un número determinado de abonados. Este sistema presenta algunas desventajas. Primero, debido a que existe un número límite en la cantidad de abonados a monitorizar, no está claro cómo elegir los abonados concretos a supervisar. Además, supone el despliegue de CAMEL en los operadores, lo que no siempre existe. Finalmente, en caso de que exista señalización CAMEL, se requiere un entrenamiento específico en dichos procedimientos por parte del personal técnico.

- **Monitorización de enlaces de señalización:** la monitorización de la señalización aporta una información que permite, bajo ciertas circunstancias, facilitar la tarea de encontrar patrones de comportamiento fraudulentos. La información se suele obtener de la comunicación entre el VLR visitado y el HLR. De este modo, se puede realizar la observación del comportamiento de ciertos IMSIs, obteniendo ciertos datos, como el nivel o carga de peticiones realizadas o como la identidad de las redes que emiten dichas peticiones. Aunque este sistema es una fuente posible de información, solamente se puede considerar como complementaria a otras, debido a que la información aportada no permite resolver como fraude un determinado comportamiento, y también a que la propia información puede estar sesgada por comportamientos como llamadas de muy larga duración, que generan poca carga, o malas configuraciones de la gestión de tripletas de autenticación en la VPMN, que generan mucha carga sin que por ello existan muchas llamadas.

- ***NRTRDE*** **(Near Real Time Roaming Data Exchange):** Desarrollado por el GSMA, el objetivo de este esquema es la transmisión en tiempo casi real de los CDRs hacia la HPMN. Concretamente, se establece un tiempo límite de 4 horas para la transmisión de los mismos [6]. Este esquema ha sido recomendado en los últimos años por el GSMA para su implantación, estableciéndose como obligatorio a partir de octubre de 2008. Presenta, además de la considerable reducción de retardos en los tiempos de traspaso de información, otras ventajas. El hecho de que se envíe la tarificación mediante otro flujo de información separado de los ficheros TAP permite la comparación de los CDRs para detectar inconsistencias y comprobar la integridad de uno u otro sistema. Aunque supone una mejora considerable con respecto a los anteriores, existen también algunas desventajas que hay que señalar. Primero, las VPMN tienen pocos incentivos para su despliegue, ya que la principal beneficiada es la HPMN. Adicionalmente, la recepción de un flujo de CDRs de tarificación adicional a los ficheros TAP implica la inversión en sistemas de proceso y almacenamiento adicionales. Finalmente, con respecto a esquemas como HUR, en el que la información viene previamente filtrada, en el caso de NRTRDE será necesario un procesado adicional de la información para inferir las alarmas de fraude. Esto último también puede considerarse como una ventaja, dado que NRTRDE proporciona más información y, por tanto, los sistemas de detección basados en dicha información pueden ajustarse mejor, reduciendo la tasa de falsos positivos.

- ***Monitorización del tráfico de datos:*** dado que el tráfico de datos del abonado en roaming fluye entre el SGSN de la VPMN y el GGSN de la HPMN, es posible para la HPMN monitorizar dicho tráfico como si se generara en la propia red. Para ello, se recomienda la utilización de unos sistemas denominados RTC (*Real Time Charging* en prepago o *Roaming Traffic Control* en postpago), ubicados en el trayecto de los datos entre el SGSN y el GGSN. Estos sistemas monitorizan el tráfico de datos en tiempo real, proporcionando dicha información a la etapa de detección.

Finalmente, para esta etapa hay que indicar que, aunque una operadora utilice sistemas de intercambio de información en tiempo real con otra (como sucede habitualmente entre operadoras con tecnología CDMA), desde el momento en que ésta realice un acuerdo de roaming con otra operadora que no lo implemente está expuesta a toda la problemática que aparece en las técnicas anteriormente expuestas.

C. Etapa de detección

La etapa de detección recibe toda la información generada en la etapa de recogida de datos y debe decidir si un comportamiento es anómalo o no. En esta etapa juegan un papel determinante los denominados sistemas de gestión de fraude (FMS, *Fraud Management Systems*). Estos son sistemas automáticos que analizan la información de tarificación en búsqueda de patrones de fraude. El método más sencillo que aplican está basado en la detección basada en reglas o firmas (ej. cuando una llamada supera una duración de 30 minutos se envía una alarma). Algunos también permiten la utilización de perfiles para grupos diferentes de abonados, o incluso para abonados individuales, y las reglas aplicadas se adaptan según el perfil considerado. Además, ciertos FMSs más complejos hacen uso de algoritmos de aprendizaje tales como redes neuronales para inferir, a partir del comportamiento observado de los abonados, las reglas a aplicar para la detección.

Existen numerosos sistemas comerciales que, en este campo, tratan de abrirse mercado o se encuentran consolidados. Entre ellos se pueden citar algunas soluciones aportadas por compañías como Mach [17], Syniverse [18], FairIsaac [19], Agilent [20], Starhome [21], ecTel [22], gmv [23], etc.

Finalmente, hay que indicar que los sistemas de monitorización en tiempo real del tráfico de datos (RTC) también incorporan capacidades de detección y, de este modo, permiten generar ante la observación de posibles comportamientos de fraude.

D. Etapa de supervisión

Los presuntos incidentes de fraude cuyos datos notifica el sistema de detección deben ser analizados exhaustivamente antes de concluir definitivamente que el evento observado se trata de un fraude. Este análisis se lleva a cabo, fundamentalmente, por el departamento de fraude de la compañía, o por una compañía especializada que es subcontratada.

Las principales dificultades que surgen en esta etapa son debidas a los retardos que se producen en la realización de la propia investigación del fraude. Estos retardos se incrementan considerablemente cuando las notificaciones del sistema de detección son en horario no laboral. En muchos de estos casos, las compañías no tienen previsto un plan de actuación. Esta falta de previsión hace inútiles los esfuerzos e inversiones realizadas en otras etapas del sistema de protección para reducir el tiempo medio de respuesta. De hecho, este escenario es más frecuente de lo que se podría esperar a primera vista, dado que las redes internacionales de fraude son conscientes de las limitaciones de las compañías en este aspecto, y cometen sus fraudes aprovechando estas ventanas temporales.

E. Etapa de respuesta

Si en la etapa de supervisión se concluye que el fraude está siendo efectuado, es necesaria una actuación que aborte la acción fraudulenta. Para ello, es deseable que la HPMN, en primer lugar, corte las llamadas o servicios que se están utilizando en dicho instante y, en segundo lugar, evite que se pueda continuar cometiendo el fraude. También se puede optar por otro tipo de soluciones menos intrusivas, como una notificación previa al cliente, para evitar afectar al servicio en aquellos casos en los que realmente no existe el fraude (falsos positivos).

Para evitar que se sigan pudiendo utilizar los servicios se modifica la suscripción del abonado fraudulento para al menos evitar la generación de SMS (modificación del TS22), prohibir todas las llamadas originantes (BAOC) y las terminantes en roaming (BAIC roam), e impedir la conexión a APNs de datos.

Respecto al corte de las llamadas y servicios, en caso de que exista un acuerdo CAMEL con la VPMN, se puede hacer en tiempo real mediante el uso de la funcionalidad IST (*Inmediate Service Termination*) [24]. Otra alternativa que no implica el corte en tiempo real de los servicios consiste en la notificación a la VPMN mediante algún medio preestablecido (email, llamada telefónica, etc.) y la gestión del corte por parte de ésta.

V. REVISIÓN Y PLANIFICACIÓN DEL FUTURO DE LA PROTECCIÓN CONTRA EL FRAUDE EN ROAMING

En este apartado se pretende proponer determinadas cuestiones que permiten situar la posición actual en la lucha contra el fraude en roaming y que, además, motivan la planificación futura en este campo. Son preguntas que deben ser abordadas por los principales agentes implicados en el campo de la prevención de fraudes en roaming, esto es, operadores de telefonía móvil, proveedores, entidades gubernamentales y financiadoras, analistas, etc., y que tratan de motivar un debate para la elaboración de una agenda de trabajo.

Situación de partida:

Magnitud del problema

- ¿Cuál es la magnitud e impacto actual de las pérdidas por fraude en general? ¿Y por los fraudes en roaming?
- ¿Qué frecuencia tienen estos fraudes y qué porcentaje de abonados son fraudulentos?
- ¿Qué porcentaje de fraude en roaming se produce en su operadora por los abonados entrantes? ¿Y por los salientes?

Sistemas de protección contra fraude

- ¿Existen implantados sistemas de protección de fraude funcionales?
- ¿Cuáles son las principales deficiencias de estos sistemas implantados?
- ¿Qué etapa es la que presenta más problemas?
- ¿Cuáles son los costes (OPEX y CAPEX) asociados al establecimiento de sistemas de protección de fraudes?
- ¿Qué impacto tienen las medidas de restricción de servicios en roaming para el desarrollo del negocio?
- ¿En qué estado se encuentran las inversiones para el despliegue de NRTRDE? ¿Qué dificultades se encuentran para realizar este tipo de inversiones?

Entorno político – social

- ¿Qué porcentaje de población o qué sectores se podrían estar beneficiando potencialmente de los efectos del fraude en roaming (venta de llamadas, etc.)?
- ¿Qué nivel de permisividad social existe con el fraude en roaming?
- Además de la repercusión en las cuentas de resultados de las compañías operadoras, ¿a qué sectores económicos está afectando indirectamente el fraude en roaming?
- ¿Qué establecen las legislaciones nacionales respecto a los beneficios obtenidos del fraude en roaming?
- ¿Existen oportunidades de negocio o nichos de mercado que no se están explotando debido a los temores generados por la existencia del fraude en roaming?

Planificación futura:

- ¿Son necesarias legislaciones más restrictivas para evitar el fraude en roaming?
- ¿En qué áreas hay que situar la inversión para evitar el fraude en roaming?
- ¿Son necearias nuevas técnicas que mejoren el tiempo medio de resolución de los incidentes de fraude?
- ¿Serían adecuadas determinadas políticas de subvención a operadores para la mejora de sistemas de prevención del fraude?
- Dada la evolución de los sistemas 3G, ¿son válidas en las compañías las estructuras funcionales o departamentales de análisis unidisciplinar? Por ejemplo, ¿tiene sentido tener un departamento de seguridad de red separado del departamento de gestión de fraude?
- ¿Considera que el fraude en roaming es más perjudicial para el desarrollo del negocio en pequeños operadores?
- ¿Qué tipo de acciones colectivas considera que se pueden abordar para reducir el fraude en roaming? Ej. Fortalecer GSMA en Latinoamérica, apoyar a las operadoras más débiles para evitar problemas de tipo técnico (fraudes de tipo 1) procedentes de ellas, etc.

VI. Conclusión

Este artículo ha realizado una discusión de las metodologías empleadas para la comisión de fraudes en entornos de roaming y de las posibles estrategias de protección contra el fraude propuestas hasta el momento.

Adicionalmente, se ha propuesto una metodología para el análisis de la situación actual del problema del fraude en roaming, y para el desarrollo de una agenda de trabajo en este campo.

Este documento es adecuado para su análisis en talleres de trabajo sobre el fraude en roaming en los que participen agentes principales del sector, esto es, compañías operadoras de telefonía móvil, proveedores y fabricantes, analistas, legisladores gubernamentales, y sector financiero. En esta línea tienen gran relevancia ciertas iniciativas como la desarrollada por IIRSA/CITEL para estudiar el escenario actual de los servicios de roaming en el contexto sudamericano.

Referencias

[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, Disponible en: 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, Inmediate Service Termination (IST), Service Description, Aug. 1998.

GLOSARIO

APN: Access Point Name. En una red GPRS, define cada una de las posibles configuraciones que un usuario tiene para conectarse a distintas redes de datos.

BAOC: Barring of All Outgoing Calls. Restricción de llamadas salientes para un abonado. Esta restricción se realiza en el HLR de la HPMN.

CAMEL: Customized Applications for Mobile Networks Enhanced Logic. Tipo de señalización de red inteligente que permite ofrecer en roaming los mismos servicios que cuando el abonado está en su red origen. Utilizado en redes GSM.

CDR: Call Detail Record. Registro de tarificación con la información de una llamada de voz.

CIBER: Cellular Intercarrier Billing Exchange Roamer record. Estándar usado en redes CDMA consistente en la compilación de CDRs en ficheros para su envío desde la VPMN hacia la HPMN.

DCH: Data Clearing House. Servicio ofrecido a operadores en roaming consistente en gestionar el envío y recepción de ficheros TAP como una única interfaz para el operador que lo contrata.

FIGS: Fraud Information Gathering System. Sistema de recogida de datos basado en CAMEL.

GSM: Global System Mobile. Sistema de comunicaciones móviles estandarizado por ETSI.

GSMA: GSM Association. Asociación de operadoras GSM.

GGSN: Gateway GPRS Support Node. Nodo de la red de datos.

HLR: Home Location Register. Base de datos con las suscripciones de los abonados y sus características.

HPMN: Home Public Mobile Network. Red propietaria de la suscripción de un abonado en roaming.

HUR: High Usage Report. Informe que las VPMN envían a las HPMN cuando se detectan posibles situaciones de fraude. Reflejan solamente información acerca de los abonados potencialmente fraudulentos.

IOT: Inter-Operator Tariff. Tarifas acordadas entre operadores para los servicios de roaming.

IST: Inmediate Service Termination. Funcionalidad de red inteligente que permite finalizar una llamada cuando ésta se encuentra activa.

MSC: Mobile Switching Center. Central de conmutación de la red voz.

NRTRDE: Near Real Time Roaming Data Exchange. Sistema de recogida de datos en cuasi-tiempo real. Especificado por GSMA.

RTC: Real Time Charging / Roaming Traffic Control. Sistema de monitorización en tiempo real del tráfico de datos en roaming.

SGSN: Serving GPRS Support Node. Nodo de la red de datos que controla el acceso del móvil a la red. Es el equivalente a la MSC en una red de datos. En un escenario de roaming se encuentra ubicado en la VPMN.

SMSC: Short Message Service Center. Centro servidor de mensajes cortos, encargado de la recepción de los mensajes cortos de los abonados propios y el envío a sus destinos.

TAP: Transfer Account Procedure. Estándar de GSMA que consiste en un fichero compilado con la información de registros de tarificación en roaming.

UDR: Usage Detail Record. Registro de tarificación con la información de uso de un servicio.

VPMN: Visited Public Mobile Network. Red visitada por un operador en roaming.

WIN: Wireless Intelligent Network. Tipo de señalización de red inteligente que permite ofrecer en roaming los mismos servicios que cuando el abonado está en su red origen. Utilizado en redes CDMA.