Análisis de Protocolos de Señalización para la detección de comportamientos irregulares en líneas de telefonía fija, utilizando sondas de señalización

Orquera E.*; Herrera C.; Estévez L.***

**Escuela Politécnica Nacional, Facultad de Ingeniería Eléctrica y Electrónica,tano_1821@hotmail.com),*
**Corporación Nacional de Telecomunicaciones, e-mail: luis.estevez@cnt.gob.ec*

***Escuela Politécnica Nacional, Facultad de Ingeniería Eléctrica y Electrónica*
Quito, Ecuador (Tel: 593-2-507144; e-mail: carlos.herrera@epn.edu.ec)

Resumen: *En el sector de las telecomunicaciones, es necesario tratar y gestionar al fraude con la debida importancia, puesto que este hecho produce pérdidas de alrededor del 4.8% del total de ingresos económicos obtenidos por las empresas que brindan estos servicios. Dichas empresas continuamente buscan implementar a sus procesos de gestión diferentes métodos para detectar conductas inusuales por parte de los suscriptores que puedan reflejar potenciales usos indebidos de los servicios o casos de fraude dentro de las telecomunicaciones y que posteriormente se traducen en pérdidas económicas para las empresas.*

A consecuencia de lo expuesto surge el presente trabajo con el fin de realizar un control de fraude en telefonía fija a bajo nivel, mediante el análisis y establecimiento de valores umbrales de varios campos de los registros de llamadas conocidos como CDRs, los cuales son obtenidos al sondear protocolos de señalización, específicamente para el caso, SIP y SIGTRAN.

Palabras clave: *Fraude en telefonía fija, protocolos de señalización, telefonía sobre IP, SIP, SIGTRAN.*

Abstract: *In the telecommunications sector, it is necessary to treat and manage fraud with due weight since this fact produces losses of about 4.8% of the total income obtained by the companies that provide these services. These companies continuously seek to implement different methods to detect unusual behavior by subscribers that may reflect potential misuse of the services or fraud within the telecommunications and subsequently translated in economic losses for enterprises to their management processes.*

As a result of the above comes this work in order to perform a fraud control in fixed telephony at low level through the analysis and value thresholds for various fields of call logs known as CDRs, which are obtained to probing signaling protocols, specifically for the case, SIP, SIGTRAN.

Keywords: *Fraud fixed telephony signaling protocols, IP telephony, SIP, SIGTRAN.*

1. INTRODUCCIÓN

Durante los últimos años, el avance tecnológico ha sido el pilar fundamental para proporcionar servicios de telecomunicaciones de alta calidad; en contraste, en el área correspondiente a la telefonía, este avance tecnológico desempeña un papel antagónico ya que permite desarrollar en mayor número y con mayor eficiencia, sistemas de fraude que ocasionan cuantiosas pérdidas a las empresas que prestan dichos servicios.

El objetivo del presente artículo se basa en la descripción de la implementación de un control de fraudes para telefonía fija mediante el análisis de protocolos de señalización.

Actualmente ha tenido una gran acogida la telefonía IP; la cual se basa en comunicaciones telefónicas realizadas a través de redes TCP/IP. La información que se transmite a través de la red se divide en paquetes de datos, los cuales tienen un encabezado que identifica el origen y el destino, un número de secuencia, un bloque de datos y un código de comprobación de errores. Los enrutadores envían estos paquetes a través de la red hasta que llegan a su destino, en donde se utiliza el número de secuencia para volver a ensamblar en su orden original. Los paquetes de datos comparten un circuito con otras transmisiones a diferencia de la telefonía tradicional, que utiliza un circuito por cada llamada telefónica.

La importancia de la Telefonía IP radica en la reducción los costos de las llamadas (hasta en un 74%), cuyo precio no depende del tiempo de conexión; por lo cual la reducción en costos puede ser considerable, especialmente para las empresas que tienen sucursales en distintas ciudades o países. En la Fig. 1 se puede observar el proceso requeridopara el establecimiento de una llamada telefónica IP.

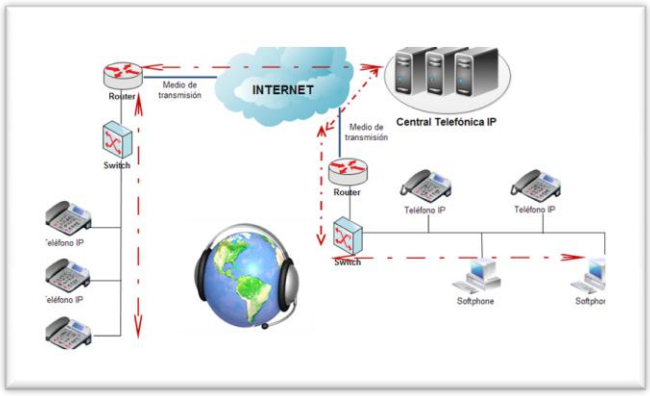

Figura 1.Proceso de llamada IP

2. SEÑALIZACIÓN EN TELEFONÍA.

La señalización es el proceso por el cual se realiza la localización de usuarios, establecimiento y negociación de sesiones y la gestión de la red. Las principales funciones de la señalización son: [1]

- Control de tráfico.
- Gestión de la red.
- Acceso a base de datos.

Existen dos diferentes tipos de señalización:

a) Señalización de abonado.

Es el intercambio de un conjunto de señales entre el usuario y el centro de conmutación. Estas señales son las siguientes:

- Supervisión o estado: permite iniciar el establecimiento, mantenimiento y terminación de la comunicación.
- Dirección:contiene información del destino.
- Tarifación: provee información sobre el costo de la llamada.
- Información al usuario: indica el estado de la llamada

b) Señalización entre centrales.

Se refiere al intercambio de un conjunto de señales entre centrales. Existen dos diferentes maneras de enviar la señalización:

Señalización asociada al canal.

La información de señalización se transmite por el mismo canal por donde se transmite el tráfico de voz. La señalización se transmitemediante un enlace PCM de 32 intervalos de tiempo para el estándar europeo, en donde la señal de línea se envía por el intervalo 16 y las señales de registro se envían por los canales de tráfico de voz.

Señalización por canal común.

Consiste en utilizar un mismo canal para enviar la señalización de varias comunicaciones separado del canal de voz. La señalización de canal común es más eficaz y flexible que la que se realiza dentro del canal de voz, dando mayor soporte a los requerimientos de las redes digitales de comunicación.

3. PROTOCOLOS DE SEÑALIZACIÓN SIP Y SIGTRAN.

Protocolo SIGTRAN

SIGTRAN está definido por la IETF en el RFC 2719 publicado en octubre de 1999. Es un conjunto de protocolos que se encargan de transportar señalización de telefonía SS7 sobre redes IP. SIGTRAN describe la manera de presentar la información de SS7 sobre una red de transporte IP, permitiendo una interoperabilidad entre redes IP de nueva generación y redes SS7 ya existentes. [2]

Los protocolos SIGTRAN determinan los medios por los cuales se pueden transportar los mensajes de SS7 de una forma confiable sobre las redes IP. Existen tres componentes de la arquitectura SIGTRAN:

- Capa de red: IP estándar como protocolo de red.
- Capa de transporte: Protocolo de transporte común para la capa protocolar de SS7. Soporta un conjunto común de funciones para el transporte confiable de la señalización.
- Módulo de adaptación: para emular las capas más bajas del protocolo. Existen varios protocolos de aplicación de señalización, tales como: M2PA, M2UA, M3UA, SUA e IUA.

En la Fig. 2 se puede observar las capas correspondientes de la Arquitectura SIGTRAN.

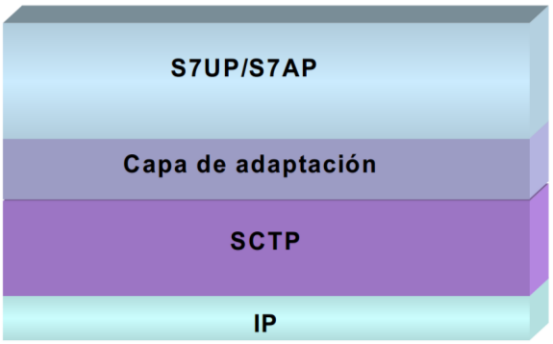

Figura 2. Arquitectura de SIGTRAN

Para obtener los registros de llamadas conocidas como CDRs, se debe analizar cada una de las capas de esta arquitectura. Estos datos son utilizados para posteriormente poder evaluarlos, con el objetivo de identificar posibles fraudes en telefonía.

Protocolo SIP

SIP es el acrónimo de Protocolo de Inicio de Sesiones; definido en el RFC 3261. Es un protocolo de señalización usado en telefonía y videoconferencia a través de Internet o para comunicaciones que implican datos en tiempo real. SIP fue creado por IETF MMUSIC WorkingGroup para establecer, modificar y finalizar sesiones entre dos participantes, así como también sesiones multicast. Este protocolo está basado en el Protocolo de Transporte simple de correo (SMTP) y en el Protocolo de Transferencia Hipertexto (HTTP).SIP es un protocolo basado en el modelo cliente servidor y ubicado en la capa de aplicación de la arquitectura TCP/IP, se usa para comunicaciones multimedia con otros protocolos como RSVP, RTP, SDP, entre otros.

El protocolo de Inicio de Sesiones es independiente de los protocolos de las capas inferiores, puede soportarse sobre TCP o UDP; además sobre IP, ATM, FrameRelay o X.25.

Los mensajes SIP están en formato de texto plano y utilizan una sintaxis muy similar a la del protocolo HTTP. Estos mensajes pueden ser solicitudes o respuestas y su formato se detalla a continuación para cada uno de estos tipos.[3]

La estructura general que presenta un mensaje SIP contiene las siguientes partes, tal como se indica en la Fig 3.

Figura 3. Formato mensajes SIP

Línea de inicio.

Es el comienzo de cualquier mensaje SIP. Esta línea está definida para mensajes de solicitud (línea de solicitud) y para mensajes de respuesta (línea de estado).

Mensajes de solicitud.

Línea de solicitud: Contiene los siguientes campos como se indica en la Fig. 4.

Método	SP	Request – URL	SP	Versión del protocolo	CRLF

Figura 4. Estructura de línea de solicitud de mensajes SIP

Mensaje de respuesta.

Línea de estado: Contiene los siguientes campos como se indica en la Fig. 5.

Versión del protocolo	SP	Status code	SP	Reason-Phrase	CRLF

Figura 5. Estructura de línea de estado de mensajes SIP.

Cabeceras de mensajes SIP.

Dentro de los campos de cabecera se encuentra información relacionada con la sesión como es: origen de la llamada, tipo de mensaje, trayectoria del mensaje entre otras características.

Cuerpo del mensaje SIP.

El cuerpo del mensaje SIP se usa para describir la sesión que va a comenzar; también se lo llama carga útil y puntualiza algunas características específicas como son: versión del códec (normalmente el estructurado en SDP) de video y audio, así como también las frecuencias de muestreo.

En esta estructura de los mensajes SIP, se puede extraer los campos que conforman los detalles de llamada conocidos como CDRs, con el fin de evaluar y detectar fraudes en telefonía fija.

4. FRAUDES EN TELEFONÍA Y MÉTODOS DE CONTROL.

En telecomunicaciones, el fraude se determina por conductas ilegítimas que perjudican intereses de abonados y usuarios como cobertura y calidad de servicio. El fraude es el uso deshonesto de servicios de telecomunicaciones donde la persona que lo comete no tiene la intención de pagar por los servicios utilizados.

Existen varios factores que impulsan el cometer fraude en las telecomunicaciones como son: gran avance tecnológico, movilidad de los servicios, convergencia tecnológica determinada por la interconexión de redes mediante la utilización del Internet entre otros.

En la actualidad es de gran importancia el uso de herramientas que permitan controlar el tráfico telefónico para poder identificar conductas inusuales por parte de los suscriptores, que puedan reflejar potenciales usos indebidos de los servicios o casos de fraude dentro de las telecomunicaciones que posteriormente se traducen en pérdidas económicas para las empresas.

Existen diferentes tipos de fraude en telefonía, entre los cuales se pueden describir los siguientes:

FRAUDE POR SUSCRIPCIÓN.

Este tipo de fraude consiste en la falsificación o alteración de documentos, suplantando la identidad de terceras personas con el fin de que los cargos se registren a nombre de ellas. El defraudador realiza el máximo uso posible de la línea telefónica hasta que es suspendida por falta de pago, afectando la imagen de las personas suplantadas, las cuales son registradas como usuarios morosos; aunque la empresa prestadora del servicio es la más afectada por no poder cobrar por el consumo realizado en la línea telefónica.

En una empresa de telecomunicaciones, es importante contar con un departamento que se encargue de la verificación de la veracidad de los datos del suscriptor, previo a la firma del contrato de servicio. Se debe tener un proceso minucioso de validación de información del suscriptor para evitar el fraude por suscripción. En la Fig. 6 se indica el proceso de fraude por suscripción.

Figura 6. Fraude por suscripción.

FRAUDE CLIP-ON.

Esta modalidad de fraude ocurre cuando el defraudador sustrae una línea telefónica activa desde la acometida de la red externa o desde el armario para llevarla hacia su domicilio y realizar llamadas, cuyo consumo será cobrado al suscriptor de la línea.

El principal afectado por este tipo de fraude es el suscriptor de la línea telefónica, puesto que debe pagar el consumo realizado por el infractor en el caso de que no se compruebe el fraude. Además la empresa prestadora del servicio se ve afectada en la imagen y en daños provocados en su infraestructura.

Este tipo de fraude se detecta generalmente mediante reclamos realizados por los propietarios de líneas telefónicas robadas, quienes se ven afectados en un incremento considerado de sus facturas. El fraude clip on también es detectado por los especialistas de fraude de las empresas, quienes analizan el tráfico telefónico con el objetivo de encontrar comportamientos atípicos que puedan reflejar un posible fraude por robo de líneas o clip on. [5]

FRAUDE DE TERCER PAÍS.

Se lo denomina así porque interviene un tercer país como defraudador, para la comunicación entre los otros dos países. En este tipo de fraude, el defraudador utiliza varias líneas telefónicas para comunicar a dos usuarios de diferentes países mediante un conmutador o una llamada en conferencia. En este proceso, el defraudador en un país Z llama a un destino en un país X, el cual solicita comunicarse con un destino en un país Y, la persona en el país Z marca hacia el destino del país Y yestablece la comunicación. El defraudador realiza todas las llamadas posibles hasta que las líneas sean suspendidas por falta de pago, afectando directamente a las empresas proveedoras del servicio. En la Fig. 7 se ilustra el fraude de Tercer País.

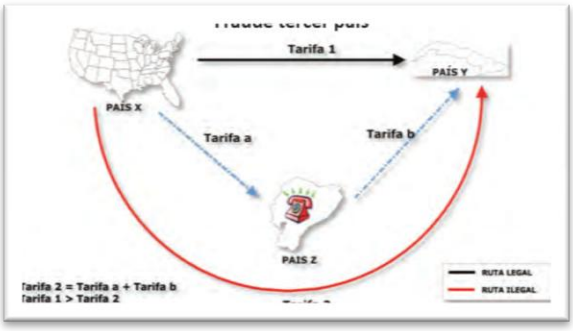

Figura 7. Fraude de Tercer País [5]

Este tipo de fraude se detecta por la presencia de llamadas hacia destinos internacionales atípicos. Cuando se identifica este tipo de llamadas el analista de fraude debe consultar la facturación de la línea que realiza la llamada, así como también analizar el tráfico telefónico que presenta la misma con el fin de determinar un perfil de comportamiento.

FRAUDE DE PBX.

Las Centrales Secundarias Privadas conocidas como PBX, son usadas por las empresas para conectarse a la red telefónica pública conmutada. Estas centrales son vulnerables a sufrir ataques por parte de defraudadores que obtienen beneficios económicos al cobrar por llamadas de tráfico nacional, internacional, llamadas a teléfonos móviles entre otras; siendo perjudicadas las empresas propietarias de las PBX que tienen que pagar por las llamadas fraudulentas realizadas. [6]

Este tipo de fraude es factible, ya que las PBX disponen de puertos de acceso remoto conocidos como DISA, estos puertos son usados para que empleados que se encuentran fuera de la empresa puedan realizar llamadas que son cargadas al número del PBX. Los defraudadores conocen las claves para poder acceder a la configuración de la PBX y poder lucrar mediante el uso ilícito de la misma.

En una PBX existe un puerto destinado al mantenimiento remoto, el defraudador logra acceder a este puerto mediante un módem y de esta forma realiza llamadas normalmente registradas en las noches y los fines de semana ocasionando un perjuicio económico directo a la empresa propietaria de la PBX. En la Fig. 8 se indica un ejemplo de este tipo de fraude.

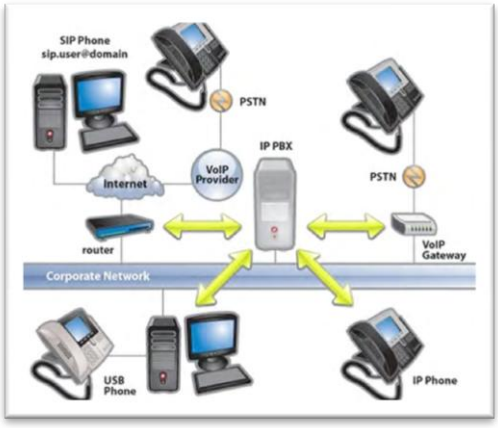

Figura 8. Fraude de PBX

El principal responsable para evitar este tipo de fraude es la empresa propietaria de la PBX, la cual debe tener un control completo de las personas y de las claves de acceso para la configuración de su PBX. Cuando existe un incremento considerable de las llamadas realizadas desde la central de la empresa, es muy importante realizar un análisis de los destinos llamados así como también de los horarios de las llamadas realizadas para lograr detectar el origen de la actividad fraudulenta. Si la empresa no cuenta con personal especializado para la configuración de la PBX, es necesario contratar terceras personas (empresas) para garantizar el correcto funcionamiento y mantenimiento de la central privada.

BY PASS

Este tipo de fraude consiste en cursar tráfico internacional de un país A hacia un país B; impidiendo que el mismo pase por las centrales de tráfico internacional y de esta forma registrar en la tarifación una llamada internacional como llamada local. [4] Los sistemas By-Pass son posibles ya que cuenta en su estructura con tres componentes: un enlace internacional, equipos que procesen la voz y un lugar encubierto con un gran número de líneas telefónicas para llevar cada llamada internacional a la central de una red local.

En la Fig. 9 se ilustra un sistema Bypass con sus respectivos componentes.

Figura 9. Componentes Sistema ByPass

Existen dos tipos de sistemas By Pass:

- **Entrante:** Es el tráfico internacional que ingresa desde otros países, sin pasar por la central de tráfico internacional.

- **Saliente:** Es el tráfico internacional que sale de un país hacia el exterior. Se lo realiza generalmente mediante la venta de tarjetas de telefonía ilícitas, reventa de minutos, etc.

Para poder detectar un sistema de fraude tipo By Pass, es necesario contar con un departamento de control especializado que se encargue de efectuar un procedimiento llamado "pruebas de lazo". En este tipo de pruebas, se realiza llamadas (manualmente o automáticamente) desde el país en donde se quiere identificar el fraude, usando para ello tarjetas de telefonía internacional. El objetivo principal de las pruebas de lazo es obtener información acerca del portador (carrier), si la llamada se la realizó legalmente el número identificado será un carrier legalmente establecido; caso contrario se identificará un número local, lo cual es una alarma de un posible sistema By Pass.

5. MÉTODOS DE CONTROL DE FRAUDE EN TELECOMUNICACIONES.

Actualmente los fraudes en telecomunicaciones perjudican económicamente a las empresas prestadoras de servicios limitando su capacidad de brindar más y mejores servicios a los usuarios o suscriptores. Es por ello que dichas empresas están conscientes de la importancia de mejorar la detección y la prevención del fraude en telecomunicaciones, ya que finalmente, al tener menos pérdidas ocasionadas por actos fraudulentos, se dispondrá de más recursos económicos que se puedan invertir en beneficio de la sociedad. Ahí radica la necesidad de contar con adecuados mecanismos de control que permitan una efectiva prevención, detección, análisis y disuasión de eventos de prestación de servicios de forma no legal, que puedan generarse en la red de comunicaciones de una empresa.

Dentro de los principales métodos de control de fraude en telefonía se describe los siguientes:

LLAMADAS DE PRUEBA DE TRÁFICO TELEFÓNICO INTERNACIONAL.

Este tipo de método de control de fraude se basa en la realización de llamadas internacionales con el fin de encontrar irregularidades en éstas, que generen señales de alerta sobre la presencia de posibles actividades fraudulentas. El propósito de estas pruebas es monitorear los canales y rutas que se están utilizando para comunicarse con el país a través de una red de telefonía. Existen diferentes mecanismos de llamadas de prueba como son:

Pruebas de lazo telefónico internacional (loop).

Su funcionamiento se basa en la generación manual o automática de llamadas internacionales desde el país donde se requiere identificar el fraude, usando para ello tarjetas de telefonía internacional. Todas estas llamadas se ejecutan hacia líneas terminales que son de propiedad de quien realiza la prueba, con el objetivo de obtener información acerca del número telefónico origen y real por el cual ingresó la llamada [6]. Cuando una llamada internacional ingresa a través de una ruta normal, el teléfono de prueba identifica un número asignado al carrier internacional que procesó la llamada; sin embargo, cuando la llamada fue recibida a través de un sistema ilegal, el identificador de llamadas registra un número local, del cual posteriormente se obtiene la localización exacta y la información de la persona a la cual pertenece la línea telefónica. En la Fig. 10 se ilustra una prueba de lazo telefónico internacional.

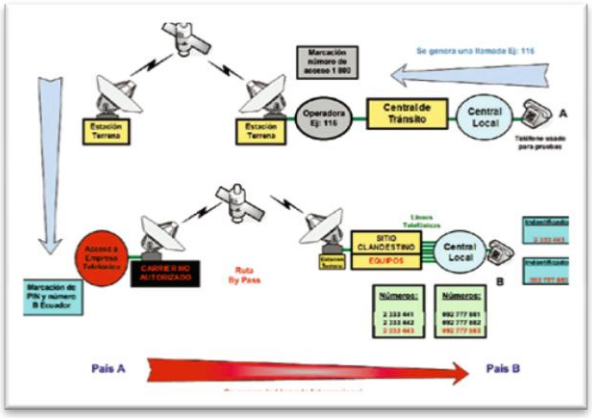

Figura 10. Prueba de lazo telefónico internacional.

El principal objetivo de este método de control es el de detectar en forma técnica los números de las líneas telefónicas que presuntamente están siendo utilizadas para cursar de manera no autorizada llamadas de origen internacional hacia las redes de operadoras telefónicas autorizadas en un determinado país. Permite detectar líneas que estén cursando tráfico telefónico internacional entrante no autorizado a través de operadores de Voz sobre IP (VoIP) y tarjetas prepago de telefonía internacional.

Bombardeo de llamadas.

Consiste en realizar llamadas desde distintos países a varios números telefónicos previamente seleccionados pertenecientes a una red de telecomunicaciones, con el objetivo de detectar líneas que cursen tráfico telefónico internacional entrante no autorizado. Es decir que verifica el correcto ingreso de llamadas internacionales entrantes desde las redes de telefonía hacia la red de una empresa de telecomunicaciones que realiza el control a través de rutas tipo "carrier" autorizados. Este tipo de mecanismo se indica en la Fig. 11.

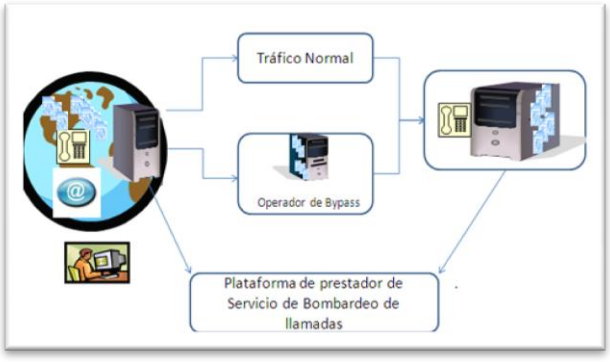

Figura 11. Bombardeo de llamadas

PERFILAMIENTO DE TRÁFICO TELEFÓNICO

Este método analiza el tráfico cursado por las líneas telefónicas que conforman una red, con el fin de identificar aquellas que presentan un comportamiento atípico, indicador de un potencial escenario de fraude. Este método implica la determinación y cuantificación de parámetros que alertan el uso de una línea telefónica en actividades irregulares de telecomunicaciones. El establecimiento de valores umbrales de dichos parámetros que integran una llamada telefónica

constituyen verdaderos filtros, que permiten identificar aquellos números telefónicos que están siendo utilizados en una presunta práctica ilícita de telecomunicaciones.

En la Fig. 12, se detalla los pasos para establecer un control de fraude mediante perfilamiento del tráfico telefónico.

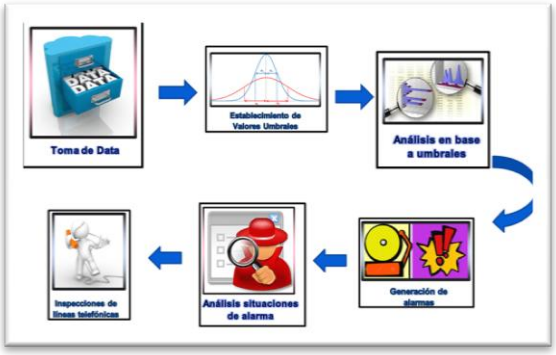

Figura 12. Perfilamiento de tráfico telefónico

El método de perfilamiento de tráfico telefónico se basa en analizar la información de una llamada creando perfiles de comportamiento de las líneas de telefonía y estableciendo valores máximos de ciertos parámetros de esta información, dentro de los cuales se puede considerar que se presenta un comportamiento regular. Este tipo de control se basa en un método llamado análisis delArchivo de detalle de Llamadas CDRs(Call Detail Record), el cual se indica a continuación.

Análisis de CDRs.

Los CDRs son registros que contienen información muy importante sobre una llamada telefónica, tales como el número de origen, número de destino, duración de llamada, número de llamadas entre otros. Todos estos parámetros son analizados para determinar el comportamiento que tiene cada una de las llamadas que generan una señal de alerta con el fin de garantizar que no exista actividades fraudulentas.

Cada uno de los campos que conforman un CDR es analizado en función de detectar diferentes tipos de fraude. Por ejemplo cuando un número de origen realiza muchas llamadas con destinos internacionales y recibe pocas llamadas, se presenta una alarma de que ese número llamante este siendo parte de un sistema By Pass. Cuando un número realiza llamadas con un destino atípico, se presume la existencia de un fraude de tercer país,

En la Fig. 13 se muestran los principales campos de los CDRs y se relaciona a cada uno de ellos con los diferentes tipos de fraude que se pueden identificar mediante su análisis.

Número de origen	Número de destino	Hora de inicio de llamada	Hora de Fin de llamada	Duración de llamada	Fecha de inicio de llamada	Fecha de fin de llamada
022852XXX	0013219457XXX	23:45	04:45	300	01/06/2014	02/06/2014

Figura 13. Campos de CDR.

- **Fraude Clip On:** Este tipo de fraude se lo identifica estableciendo valores umbrales para los parámetros de los campos: número de destino, hora de inicio de llamada, hora de fin de llamada y duración de llamada. Además es muy importante determinar el número de llamadas que se ha realizado desde la línea. Valores inusuales en estos campos indican la posible presencia de fraude.
- **Fraude Tercer País:** Para lograr identificar Fraude de Tercer País, es necesario evaluar el campo de destino de llamadas acompañado con el número de llamadas realizadas. Varias llamadas a destinos atípicos dan la alerta de la existencia de este tipo de fraude. También se analiza el campo de duración de llamada.
- **Fraude de PBX:** En una empresa que cuenta con una PBX, es común el tipo de fraude por llamadas de terceros. Este tipo de fraude se puede identificar analizando principalmente los campos: número de destino, hora de inicio llamada, hora de fin de llamada y fecha de inicio y fin de llamada. Llamadas hechas en horarios fuera de oficina, en horas inusuales y a destinos internacionales o celulares, indican la sospecha de actividad fraudulenta.
- **Bypass:** Este tipo de fraude se lo detecta en forma similar al de relleno (refilling). Se debe analizar dentro de los CDRs los campos de origen de llamada, destino de llamada y duración con el fin de determinar el comportamiento de las líneas telefónicas. Cabe mencionar que resulta muy complejo identificar este tipo de fraude con el método de análisis de CDRs, por lo cual se utiliza el método de pruebas de lazo telefónico internacional descrito anteriormente.

6. DETECCIÓN DE POSIBLES FRAUDES EN TELEFONÍA FIJA MEDIANTE EL ANÁLISIS DE LOS CDRS.

Dentro de los servicios de telefonía fija que prestan las empresas de Telecomunicaciones, es de gran importancia realizar un control del tráfico telefónico para lograr identificar posibles usos indebidos del servicio que pueden representar potenciales escenarios de fraude. El método que se utilizó para lograr detectar comportamientos atípicos en las líneas de telefonía, se basa en el análisis de los registros de llamada conocidos como CDRs, los cuales contienen diferentes campos de información como son: origen, destino, fecha de la llamada, hora de inicio de la llamada, hora de finalización de llamada, duración, tipo de llamada entre otros [7]. En función de detectar posibles fraudes, se establecieron valores umbrales para varios de estos campos. Si al analizar los CDRs, se observan valores superiores a los umbrales, se genera una alarma, que debe ser tomada en cuenta para confirmar si existe una actividad fraudulenta. Cuando surge una alarma se realiza un análisis diferencial, en el cual se monitorean patrones de comportamiento de la línea telefónica comparando sus más recientes actividades con el historial de uso de la misma; un cambio en el patrón de comportamiento permitirá detectar escenarios fraudulentos.

CONTROL DE TRÁFICO TELEFÓNICO PARA FRAUDE CLIP ON.

Existe un patrón de comportamiento habitual en las líneas de telefonía fija mediante las cuales se realiza el denominado fraude Clip On o Robo de Líneas. Este comportamiento se basa en la realización de llamadas, generalmente a destinos celulares e internacionales; las llamadas son de larga duración efectuadas en altas horas de la noche con la finalidad de que el defraudador no sea descubierto por el dueño de la línea telefónica al coincidir en la utilización de la misma. Otro indicador importante es la presencia de llamadas hacia destinos nunca antes realizados bajo las condiciones

anteriormente descritas.En la Fig. 14 se indica el comportamiento de una línea telefónica con fraude Clip On.

Figura 14. Comportamiento Fraude Clip On.

Valores umbrales de los campos a ser considerados.

Para algunos de estos campos fue factible establecer valores umbrales después de realizar varias pruebas del control para este tipo de fraude. En otros campos del CDR, únicamente se estableció algún tipo de restricción que permita optimizar las cadenas de consultas. En la tabla 1 se detalla estos valores y restricciones con la respectiva justificación.

Tabla 1 Umbrales - Restricciones de campos para Fraude Clip On.

CAMPO	VALOR UMBRAL	RESTRICCIÓN	JUSTIFICACIÓN / OBSERVACIÓN
Número de origen	Ninguno	Números de Pichincha.	Se restringe el número origen solo a la provincia de Pichincha.
Número de destino	Ninguno	Destinos internacionales y celulares	En el fraude Clip On, el defraudador generalmente trata de sacar el mayor provecho de la línea telefónica a la cual está estafando; por ello es muy común que realice llamadas hacia destinos celulares e internacionales que tiene una tarifa más alta en el mercado de la telefonía.
Fecha inicio	Ninguno	Ninguno	Parámetro modificable.
Fecha Fin	Ninguno	Ninguno	Parámetro modificable.
Hora de inicio	23h00 a 04h00	Ninguno	El defraudador prefiere realizar llamadas dentro del horario indicado para evitar ser descubierto por el dueño de la línea telefónica al coincidir en el uso de la misma.
Hora de fin	23h00 a 04h00	Ninguno	El defraudador prefiere realizar llamadas dentro del horario indicado para evitar ser descubierto por el dueño de la línea telefónica al coincidir en el uso de la misma.
Duración	Llamadas con duración mayor a 1 hora	Ninguno	Generalmente en este tipo de fraude, las llamadas realizadas son de larga duración. Después de varias pruebas y en base al monitoreo de patrones de uso de la línea telefónica; se estableció como valor umbral para la duración de las llamadas una hora.

CONTROL DE TRÁFICO TELEFÓNICO PARA FRAUDE PBX.

Las centrales secundarias privadas conocidas como PBX pertenecientes generalmente a empresas, deben tener un alto grado de seguridad en su configuración para evitar la presencia de fraude. En la práctica, existen diferentes mecanismos por los cuales los defraudadores pueden hacer mal uso de estas centrales con el objetivo de lucrar de forma ilícita. Todos estos métodos reflejan patrones de comportamientos definidos en los cuales existe la presencia de llamadas generalmente hacia destinos internacionales (países inusuales con tarifas telefónicas altas).

Los defraudadores hacen uso de estas líneas telefónicas en horarios fuera de oficina; es decir en horas de la noche y en días no laborables con el fin de realizar el máximo consumo de llamadas sin la posibilidad de ser descubiertos o interrumpidos por el personal administrativo y técnico de la empresa de ser el caso.

Es muy importante aclarar que este tipo de fraude representa un gran impacto en la economía de pequeñas empresas o de suscriptores residenciales; los cuales deben asumir el pago de las llamadas fraudulentas realizadas desde su central privada. Un incremento de tan solo centenas o miles de dólares en la planilla telefónica mensual, puede resultar catastrófico para este tipo de suscriptores; es decir que en estas líneas se debe realizar un control minucioso del tráfico telefónico generado por la central PBX con el fin de detectar la presencia de fraude.

En una gran mayoría, los fraudes realizados en las PBX, son efectuados generalmente en aquellas líneas en las cuales existe la presencia de llamadas hacia destinos internacionales muy poco usuales y con tarifas de telefonía altas; con el objetivo de tener un mayor beneficio económico. En la Fig. 15, se puede observar de forma detallada el comportamiento de las líneas telefónicas para este tipo de fraude.

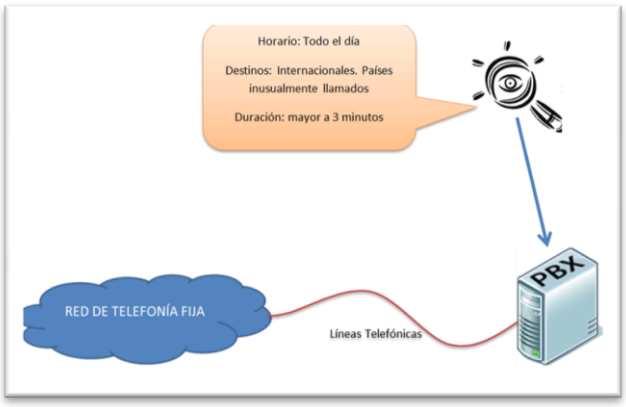

Figura 15. Comportamiento Fraude PBX

Valores umbrales de los campos a ser considerados.

Según el patrón de comportamiento descrito anteriormente, los campos de los CDRs a ser considerados para este tipo de fraude, se detalla en la Tabla 2

Tabla 2. Umbrales - Restricciones de campos para Fraude PBX.

CAMPO	VALOR UMBRAL	RESTRICCIÓN	JUSTIFICACIÓN / OBSERVACIÓN
Número de origen	Ninguno	Números correspondientes solo a líneas de Pichincha.	Este tipo de fraude se lo analiza únicamente en los números correspondientes a PBX de empresas o personas particulares.
CAMPO	**VALOR UMBRAL**	**RESTRICCIÓN**	**JUSTIFICACIÓN / OBSERVACIÓN**
Número de destino	Ninguno	Destinos internacionales	En este tipo de fraude el principal objetivo es obtener el mayor provecho de las centrales PBX; por ello las llamadas son hechas hacia destinos internacionales poco usuales que tienen una tarifa más alta en el mercado de la telefonía.
Hora de inicio	Todo el día	Ninguno	En fraude de PBX de empresas grandes, solo se necesita tener una llamada hacia destinos internacionales inusuales para tener una señal de alarma.
Hora de fin	Todo el día	Ninguno	En fraude de PBX de empresas grandes, solo se necesita tener una llamada hacia destinos internacionales inusuales para tener una señal de alarma.
Duración	Mayor a 3 minutos	Ninguno	Una llamada con pocos minutos de duración hacia destinos internacionales atípicos es motivo suficiente para un análisis de tráfico telefónico con el propósito de detectar un posible fraude.

CONTROL DE TRÁFICO TELEFÓNICO PARA FRAUDE BYPASS.

Para la ejecución de fraude By Pass, los defraudadores generalmente deben contar con varias líneas telefónicas para finalizar las llamadas internacionales en la red de telefonía de una operadora. Estas líneas telefónicas tienen un patrón de comportamiento en el cual presentan volúmenes de tráfico altos; a su vez no tienen muchas llamadas recibidas.

Un potencial indicativo, de un fraude By Pass, en el comportamiento de las líneas telefónicas, es la diversidad y variedad existente de los números telefónicos de destino los cuales son únicamente números locales y nacionales. El tiempo de duración de las llamadas es media. Todo el comportamiento descrito anteriormente se presenta con una mayor intensidad los fines de semana y días festivos.

En la Fig. 16, se detalla el comportamiento de líneas telefónicas utilizadas en un fraude By Pass.

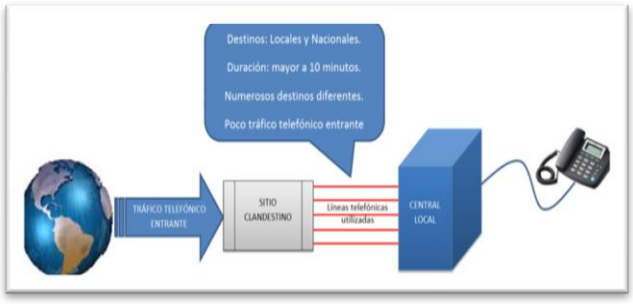

Figura 16. Comportamiento de líneas telefónicas usadas en fraude By Pass Entrante

Valores umbrales de los campos a ser considerados.

Una vez descrito el patrón de comportamiento de las líneas telefónicas utilizadas para realizar fraude By Pass, en la tabla 3, se indican los diferentes campos con los respectivos valores umbrales o restricciones.

Tabla 3. Umbrales - Restricciones de campos para Fraude By Pass Entrante.

CAMPO	VALOR	RESTRICCIÓN	JUSTIFICACIÓN /

	UMBRAL		OBSERVACIÓN
Número de origen	Ninguno	Números correspondientes solo a líneas de Pichincha.	Solo se analizará líneas telefónicas fijas de la provincia de Pichincha.
Número de destino	Ninguno	Destinos locales y nacionales	En este tipo de fraude se introduce el tráfico telefónico internacional por líneas telefónicas locales y nacionales.
Hora de inicio	Todo el día	Ninguno	Se analizará el tráfico telefónico generado durante todo el día.
Hora de fin	Todo el día	Ninguno	Se analizará el tráfico telefónico generado durante todo el día.
Duración	Mayor a 10 minutos	Ninguno	Las llamadas hacia destinos internacionales tienen una duración media aproximada de diez minutos.

CONTROL DE TRÁFICO TELEFÓNICO PARA FRAUDE DE TERCER PAÍS.

Para el fraude de Tercer País, el defraudador usa una o varias líneas telefónicas para realizar llamadas hacia destinos internacionales, en especial hacia países de África, Medio Oriente y Cuba, ya que en esos países se registra antecedentes históricos para este tipo de fraude. El fraude de Tercer País generalmente viene acompañado de un fraude por suscripción, puesto que el estafador adquiere líneas telefónicas con identidades falsas, mediante las cuales realiza la mayor cantidad de llamadas posibles las 24 horas del día, hasta que estas líneas son suspendidas por falta de pago. También es muy común encontrar este tipo de fraude basado en sistemas By Pass. En la Fig. 17 se indica el comportamiento de líneas telefónicas implicadas en fraude Tercer País.

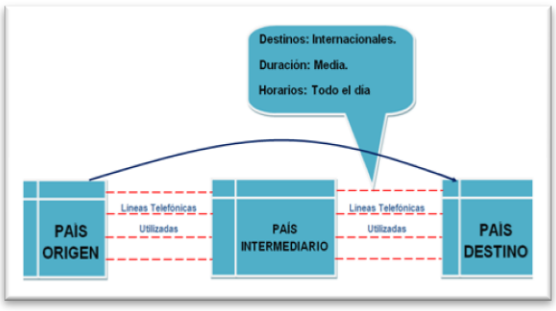

Figura 17. Comportamiento Fraude Tercer País

Valores umbrales de los campos a ser considerados.

En la tabla 4, se detalla los diferentes campos a ser considerados con los respectivos valores umbrales o restricciones.

Tabla 4. Umbrales - Restricciones de campos para Fraude de Tercer País.

CAMPO	VALOR UMBRAL	RESTRICCIÓN	JUSTIFICACIÓN / OBSERVACIÓN
Número de origen	Ninguno	Números correspondientes solo a líneas telefónicas de Pichincha.	El presente proyecto está destinado a analizar fraudes realizados en telefonía fija en la provincia de Pichincha.
Número de destino	Ninguno	Destinos Internacionales	En el fraude de Tercer País, el defraudador generalmente realiza llamadas a destinos internacionales (en especial a Medio Oriente, África y Cuba), para de esta forma sacar el mayor beneficio posible a las líneas telefónicas utilizadas.
Hora de inicio	Todo el día	Ninguno	Se analizará el tráfico telefónico generado durante todo el día.
Hora de fin	Todo el día	Ninguno	Se analizará el tráfico telefónico generado durante todo el día.
Duración	Mayor a 5 minutos	Ninguno	Las llamadas hacia destinos internacionales tienen una duración media aproximada de cinco minutos.

7. RESULTADOS FINALES

Después de implementar y ejecutar el control de fraude en telefonía fija surgieron diversas alarmas en el análisis de cada uno de los tipos de fraude. Cuando surge una alarma se realiza un análisis diferencial, en el cual se monitorean patrones de comportamiento de la línea telefónica comparando sus más recientes actividades con la historia de uso de la misma; un cambio en el patrón de comportamiento permitirá detectar escenarios fraudulentos. De esta forma se obtuvieron los siguientes resultados.

a) FRAUDE CLIP ON.

En la realización del presente Proyecto, existieron 11 líneas telefónicas identificadas como probables escenarios de fraude. Finalmente se realizó las inspecciones, encontrando fraude por robo de líneas telefónicas en cuatro de ellas; por lo que se procedió a informar a los abonados y tomar las medidas correctivas en estos casos.

b) FRAUDE PBX.

Dentro de varias fechas en las cuales se ejecutó el presente control, se obtuvo seis números telefónicos asociados a PBX de los cuales se analizó el tráfico cursado resultando una sola línea telefónica perjudicada por este tipo de fraude, la cual registró pérdidas económicas sobre los $2800 durante dos meses.

c) FRAUDE BYPASS.

Inicialmente se encontraron 25 líneas telefónicas potencialmente usadas para fraude Bypass Entrante. Se determinó que en este caso la gran mayoría de líneas telefónicas estaban definidas como líneas comerciales, lo cual justifica la existencia de tarifas altas de facturación y de altos volúmenes de tráfico generadas por las mismas. Finalmente quedó como señal de alarma una línea telefónica residencial en la cual el abonado propietario estaba haciendo un mal uso del servicio; ya que se utilizaba la línea telefónica residencial ubicada en un local de negocio. El abonado obtenía beneficios económicos al alquilar dicha línea residencial. Es por ello que este caso se cerró al no encontrar la presencia de

fraude ByPass, existiendo únicamente una recategorización de la línea telefónica.

d) FRAUDE TERCER PAÍS.

Después de ejecutar la consulta de acuerdo a los parámetros establecidos para la misma, se pudo observar que durante todas las fechas en las cuales se tomó los datos con el analizador de protocolos, únicamente se generaron como alarmas 3 líneas telefónicas para ser examinadas. Se contactó con los propietarios de las líneas telefónicas, quienes confirmaron que las llamadas fueron realizadas desde sus instalaciones de forma legítima, por lo cual se cerraron estos tres casos de análisis de fraude.

8. CONCLUSIONES

Para la implementación del control de fraude, en este Proyecto se utilizó el método de perfilamiento de una línea telefónica, en el cual se analiza la información de las llamadas realizadas por las líneas telefónicas con el objetivo de identificar aquellas que presentan un comportamiento atípico, indicador de un potencial escenario de fraude. Este método crea perfiles de comportamiento de las líneas de telefonía y establece valores umbrales para los campos de los CDRs como son: número de origen, número de destino, duración de llamada, fecha de inicio y fin de llamada, hora de inicio y fin de llamada. Si existen valores mayores a los umbrales establecidos, se genera una señal de alerta que debe ser considerada por el analista de fraude para examinar las líneas telefónicas más detalladamente.

Una vez finalizados la implementación y ejecución del control elaborado en este Proyecto, se puede concluir que los fraudes realizados en telefonía fija pueden llegar a ser causales de pérdidas económicas muy elevadas tanto en líneas comerciales como residenciales; es por esta razón que es muy importante realizar el monitoreo de la red de telefonía en tiempo real y analizar los casos de fraude con la brevedad posible, para evitar que las repercusiones económicas sean demasiado altas para los abonados perjudicados.

Después de aplicar el control de fraude implementado en este proyecto, se puede concluir que es común encontrar fraude Clip On en líneas telefónicas debido a que es uno de los fraudes más fáciles de realizarlos y no demandan una adquisición previa de infraestructura determinada para realizarlo. Generalmente este tipo de fraude se lo comete vulnerando la acometida externa del servicio, aunque también se puede conectar un cable secundario al cable troncal y llevándolo hacia la ubicación del defraudador siendo este último proceder más complejo.

El fraude hacia una PBX también está presente debido fundamentalmente a las vulnerabilidades existentes al configurar una PBX sin las debidas normas de seguridad, De acuerdo a la experiencia, este tipo de fraude se lo comete realizando llamadas hacia países de destino inusualmente llamados por los abonados de Ecuador; es por esta razón que el control de fraude PBX implementado se basa en encontrar específicamente llamadas realizadas desde una PBX hacia países que tienen antecedentes históricos en este tipo de fraude.

Mediante la aplicación del control de fraude, se puede concluir que actualmente, las redes de telefonía fija de la de las empresas de telecomunicaciones se encuentran libres de fraudes como By Pass entrante y Tercer País debido a controles más específicos que se realizan para estos tipos de fraude como es la prueba de lazo cerrado en la cual se genera llamadas internacionales desde el país donde se quiere identificar el fraude hacia líneas terminales que son de propiedad de quien realiza la prueba identificando si la llamada pasó por un carrier autorizado o por un sistema ilegal.

AGRADECIMIENTOS

Este trabajo fue auspiciado y asesorado por la Escuela Politécnica Nacional y la Corporación Nacional de Telecomunicaciones.

REFERENCIAS

[1] RENDÓN, Álvaro. SEÑALIZACIÓN EN REDES TELEFÓNICAS. *h*ttp://dtm.unicauca.edu.com/ pregrado/conmutacion/transp/2.4-Senalizacion.pdf.2013

[2] PEREIRA, Javier. SISTEMA DE SEÑALIZACIÓN SIGTRAN. https://eva.fing.edu.uy/pluginfile.php /67122/mod_resource/content/1/20110619_sigtran.pdf. 2011.

[3] Request for Comments 3261. Internet Engineering Task Force (IETF). Network Working Group. SIP: Session Initiation Protocol. https://www.ietf.org/rfc/rfc3261.txt. 2002

[4] Universidad Distrital Francisco José Francisco de Caldas.. TÉCNICAS DE DETECCIÓN, PREVENCIÓN Y CONTROL DE FRAUDE EN TELECOMUNICACIONES. Colombia. 2004.

[5] MEZA, María. Dirección General de Investigación Especial en Telecomunicaciones (SUPERTEL). FRAUDE EN TELECOMUNICACIONES. Primera edición. Quito. 2008.

[6] SUPERTEL. Delitos en Telecomunicaciones. http://www.supertel.gob.ec/pdf/publicaciones/delitos%20telecomunicaciones%20revista_supertel.pdf. Quito. 2011.

[7] 1) MEJÍA, David; GARZÓN Carlos. IMPLEMENTACIÓN DE UN PROTOTIPO DE SISTEMA DE REPORTES WEB PARA TELEFONÍA IP. Revista Politécnica. Vol. 33. Año 2014.