DETECCIÓN DE FRAUDE BY PASS SOBRE VOZ IP CON PRUEBAS DE LOOP AUTOMATIZADAS

JUAN SEBASTIÁN CORTÉS MOTTA

UNIVERSIDAD SANTO TOMÁS
FACULTAD DE INGENIERÍA DE TELECOMUNICACIONES
BOGOTÁ D.C.
2012

DETECCIÓN DE FRAUDE BY PASS SOBRE VOZ IP CON PRUEBAS DE LOOP AUTOMATIZADAS

Presentado por:

JUAN SEBASTIÁN CORTÉS MOTTA
2081741

Proyecto de Pasantía para optar por el título de Ingeniero de Telecomunicaciones
(Monografía)

Dirigido por:

ING. MSc. ELVIS EDUARDO GAONA GARCÍA

UNIVERSIDAD SANTO TOMÁS
FACULTAD DE INGENIERÍA DE TELECOMUNICACIONES
BOGOTÁ D.C.
2012

Nota de Aceptación

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Director

Bogotá D.C. (16, Enero, 2012)

Agradecimientos

Brindo mis agradecimientos a las siguientes personas por su valiosa contribución al desarrollo y elaboración del proyecto planteado mediante este documento.

- Gaona Elvis, Director de la monografía. por su constante colaboración en la tarea de revisar y corregir el correcto desarrollo y elaboración de este proyecto.
- La Universidad Santo Tomás de Bogotá D.C., por brindarme los conocimientos teóricos en comunicaciones necesarios para el entendimiento de la problemática existente planteada en esta monografía.
- Bornachera Cesar, Ingeniero del área de protección y aseguramiento de ingresos quien me brindó su conocimiento en el tema de fraudes en redes móviles, especialmente en fraude *By Pass*.
- Velásquez Javier, Ingeniero del área de protección y aseguramiento de ingresos por su constante ayuda en la búsqueda de tecnologías y soluciones que pudieran ser aplicadas al sistema anti fraude desarrollado.
- Hover Juan, Ingeniero del área de protección y aseguramiento de ingresos por brindarme la oportunidad de desarrollar este proyecto haciéndome cargo de una problemática la cual en estos momentos es de gran importancia para el operador móvil.
- Riveros Carolina, Ingeniera del área de protección y aseguramiento de ingresos por sus aportes respecto a dudas puntuales en temas de funcionamiento y tarifas de servicios.
- López Jesús, Estudiante de Ingeniería de Telecomunicaciones de la Universidad Santo Tomás por su paciencia y dedicación para colaborarme en la elaboración del Anexo de instalación y configuración de una IP-PBX en Linux.

Resumen

Desde la aparición de las redes de telefonía móvil celular se han desarrollado tecnologías y servicios a través de estas que permiten a los usuarios de la red interactuar de formas variadas no solo entre estos, también con entidades como bancos y empresas prestadoras de otros servicios. Por tal motivo ciertas personas han ideado y desarrollado métodos y técnicas destinadas a la realización de fraude con el fin de obtener un beneficio para sí mismos o para terceros y perjudicar a quien es víctima de este acto, es decir los usuarios de la red o la red como tal. Debido a las graves consecuencias que puede generar el fraude sobre quien recae esta acción, se deben implementar medidas de prevención, detección y corrección que permitan mitigar el daño causado y a su vez disminuir los casos que se presentan en la red y en sus usuarios. Es por esto que la generación de ideas que permitan el desarrollo e implementación de nuevos procesos de detección más eficientes y que se adapten a las nuevas formas de fraude que surgen con el tiempo toma un rol importante dentro de las empresas prestadoras de servicios de comunicaciones, por lo cual se propone una solución en base a un nuevo sistema de detección de fraude enfocado al tráfico de llamadas internacionales a equipos móviles mediante la tecnología Voz IP.

Palabras Clave

Fraude, detección, prevención, corrección, sistema, información, servicio, red, comunicaciones, Voz IP.

Abstract

Since the occurrence of mobile phone networks have developed technologies and services through these that allow network users to interact in many different ways not only between these, also with entities such as banks and other service companies. For this reason some people have devised and developed methods and techniques for conducting fraud in order to obtain a benefit for themselves or others and prejudice who is victim of this act, users of the network or the network as such. Because of the serious consequences that can generate fraud who falls on this action, should implement measures for prevention, detection and correction to mitigate the damage and decrease the cases that occur in the network and its users. That is why the generation of ideas to the development and implementation of new screening processes more efficient and to adapt to new forms of fraud that emerge over time takes an important role within the companies providing communications services, therefore proposes a solution based on a new fraud detection system focused international call traffic to mobile devices using VoIP technology.

Keywords

Fraud, detection, prevention, correction, system, information, service, network, communications, VoIP.

Contenido

Pág.

Lista de figuras

Pág.

Índice de Tablas

Pág.

Glosario

CDR: *(Call Detail Record). Es el registro de llamadas, mensajería y navegación en Internet realizado por un terminal móvil dentro de la red del operador. En este registro se encuentra información como el tiempo de navegación, la duración y el destinatario de una llamada. Estos registros se encuentran en el HLR del operador y permiten mantener un registro completo de todos los acontecimientos de los terminales en la red.*

CI: *(Carrier Internacional). En español se refiere a Servicio Portador Internacional y corresponde a aquellas empresas que tienen la facultad de proporcionar la capacidad necesaria para el transporte de señales de telecomunicaciones, originadas y terminadas en un país, hacia o desde el ámbito internacional.*

HLR: *(Home Location Register). Base de datos en la cual se encuentran todos los registros acerca de las actividades realizadas por un terminal móvil dentro de la red en cuanto a mensajería, llamadas y navegación en Internet.*

IP: *(Internet Protocol). Protocolo no orientado a conexión diseñado para su uso en sistemas interconectados por redes de comunicaciones de ordenadores, permitiendo el encaminamiento de paquetes (datagramas) a través de la red, lo cual asegura el intercambio de información entre sí.*

LDI: *(Larga Distancia Internacional). Servicio de telefonía pública básica conmutada que brinda el operador a un usuario para que este se pueda comunicar hacia un país extranjero.*

PC: *(Personal Computer). Microcomputadora diseñada para el uso de una sola persona a la vez la cual permite realizar actividades como navegar en Internet, realizar trabajos de texto y escuchar música entre muchas otras actividades.*

PSTN: *(Public Switched Telephone Network). Conocido en español como Red de Telefonía Publica Conmutada, es el conjunto de elementos que hacen posible la transmisión conmutada de voz, con acceso generalizado al público y que puede funcionar como red de transito en interconexión con otras redes.*

ROAMING INTERNACIONAL: *Servicio de comunicaciones mediante el cual un dispositivo móvil puede enviar y recibir llamadas, mensajes cortos y todos los demás servicios que ofrece un operador móvil sin que este se encuentre dentro de*

la zona de cobertura de dicho operador, para esto el usuario debe estar dentro de la zona de cobertura de red de un operador extranjero con el cual el operador local tiene convenio de Roaming Internacional.

SIM CARD: (*Subscriber Identity Module Card). Tarjeta inteligente que permite al usuario conectarse a la red del operador móvil gracias una clave contenida en esta, la cual permite identificar al usuario dentro de la red.*

SMARTPHONE: *Teléfono inteligente que integra las funciones de un teléfono celular y una Personal Digital Assistant el cual puede comunicarse a través de Wi-fi, Bluetooth, envío de mensajería y llamadas convencionales haciendo uso ya sea de una red de telefonía móvil o de Internet.*

SMS: *(Short Messages Service). Servicio que permite el envío de mensajes cortos (texto) entre teléfonos móviles o fijos, estos mensajes tienen un máximo de 160 caracteres.*

SO: *(Sistema Operativo). Conjunto de software que se encargan de controlar los distintos recursos de un ordenador.*

SOFTPHONE: *(Acrónimo entre Software y Telephone). Programa de software que permite generar y recibir llamadas desde un PC conectado a Internet haciendo uso de la tecnología Voz IP.*

SOFTSWITCH: *(Acrónimo entre Software y Switch). Es el principal dispositivo en la capa de control dentro de una arquitectura NGN (Next Generation Network), encargado de proporcionar el control de llamada (señalización y gestión de servicios), procesamiento de llamadas y otros servicios.*

SQL: *(Structured Query Languaje) Lenguaje de programación para el acceso a bases de datos relacionales que permite consultar la información contenida en estas por medio de sentencias declarativas las cuales indican cual es el resultado esperado sin necesidad de especificar el proceso necesario para realizar la consulta deseada.*

TCP: *(Transmission Control Protocol). Protocolo de Internet que forma un circuito completo de comunicaciones, de forma que el flujo de datos entre origen y destino sea continuo, consiguiendo que los paquetes recibidos en el destino se ordenen de forma correcta sin que exista perdida de información debido al viaje de los datos en la red.*

UT: *(User Terminal). Equipo de comunicaciones de propiedad del usuario que permite a este conectarse a la red del operador y hacer uso de los servicios que este ofrece.*

VOZ IP: *(Voice over Internet Protocol). Tecnología que aplica un conjunto de protocolos y aplicaciones que permiten establecer una comunicación para el intercambio de información, principalmente voz y video, en tiempo real a través de la red de Internet.*

PARTE I

Introducción a la Monografía

Capítulo 1

1.Introducción

La interconexión e interoperabilidad de las redes que prestan servicios de comunicaciones, sin importar que estas brinden distintos servicios, ha favorecido el desarrollo y continuo mejoramiento de las redes de telefonía móvil y la inclusión de la transmisión de datos a través de estas. Se han desarrollado servicios de comunicaciones como las llamadas móvil-móvil, móvil-fijo, móvil-PC, uso de datos para navegación en Internet, Roaming Internacional y llamadas de larga distancia internacional (LDI). Todos estos son servicios que permiten a los usuarios interactuar de formas variadas, por llamadas de voz tradicional, por mensajes cortos (SMS), a través de las famosas redes sociales, por mensajería instantánea o hasta haciendo uso de Voz IP.

Todas estas formas de interactuar han generado que cada vez sea mayor el número de usuarios que hacen uso de los servicios móviles. Usuarios que pueden ser personas del común o empresas en general. Así mismo, también existe gran cantidad de utilidades que le dan estos usuarios a los servicios móviles, entre los más comunes se encuentran la comunicación entre personas, la navegación en la web, la navegación satelital, el envío de información acerca del pago de servicios con entidades bancarias y de servicios públicos, entre otros.

A su vez se han encontrado formas de realizar fraude por medio de estos servicios que ofrecen las redes móviles, de las cuales existen variadas modalidades. El envío de mensajes informando al usuario que "ha sido el ganador de premios", las llamadas notificando que "un familiar ha sufrido un accidente", y otros como el uso de líneas móviles de forma indebida tanto el llamadas nacionales como internacionales son modalidades cada vez más comunes debido a su alta efectividad para conseguir un beneficio en favor de quien comete estas actividades, en la mayoría de los casos un beneficio económico.

Por este motivo los operadores móviles que prestan estos servicios deben idear e implementar medidas que permitan disminuir las actividades fraudulentas que se presentan en su red, las cuales afectan de manera adversa sus ingresos económicos. Para el caso de esta monografía, la misma será enfocada en la evaluación y proposición de un proceso de detección de fraude, específicamente del llamado "By Pass" el cual se presenta en llamadas internacionales tanto a redes fijas como móviles

1.1. Planteamiento del problema

Con la evolución de las redes TCP/IP se han generado nuevas formas de comunicarse, un claro ejemplo de esto es la Voz IP. Gracias a la implementación de esta tecnología es posible comunicarse con una persona que se encuentra en cualquier lugar del mundo con una conexión a Internet por medio de una llamada IP, lo único que se necesita es ser usuario de un proveedor de este servicio el cual le permite al usuario elegir un identificador que lo distingue de los demás usuarios del servicio y un Softphone que básicamente se encarga de cumplir las mismas funciones de un teléfono tradicional pero desde un PC o un Smartphone permitiendo generar y recibir llamadas.

La cantidad de usuarios que hacen uso de esta tecnología crece rápidamente, esto se debe principalmente a las facilidades que brinda con respecto a la telefonía fija y móvil tradicional, permitiendo generar y recibir llamadas e inclusive video llamadas entre usuarios que se encuentran conectados a Internet de forma gratuita, lo cual por supuesto genera gran interés en las personas. Además, permite generar y recibir llamadas desde y hacia el Softphone del usuario a cualquier terminal móvil o fijo de otra persona sin importar el país en que ambos se encuentren, para este caso la llamada si tiene un costo el cual corresponde a aquel que se genera por el convenio de interconexión entre la red del proveedor del servicio de Voz IP y el proveedor del servicio de telefonía.

La problemática en la cual se centra esta monografía nace a partir del uso indebido que ciertas personas han decidido dar a esos beneficios que brinda la tecnología Voz IP. Este uso indebido no es más que una modalidad de fraude que perjudica económicamente a operadores tanto de telefonía móvil como fija y operadores de LDI que brindan sus servicios de interconexión de estos operadores hacia los CI. A nivel mundial el fraude en el tráfico de llamadas internacionales se conoce como *By Pass*, el cual se encuentra definido por la empresa Movistar en su anexo de conductas no autorizadas para el cliente (s/f) como: "*Procedimiento que consiste en recibir trafico de larga distancia internacional, sin hacer uso de los operadores de telecomunicaciones habilitados legalmente para prestar este servicio*" (pág. 1).

El *By Pass* es utilizado con el fin de obtener un beneficio económico a favor de la persona que realiza esta actividad ilegal en la gran mayoría de países en el mundo. Este fraude se presenta cuando la llamada es generada desde un Softphone perteneciente a una empresa prestadora del servicio de Voz IP o un terminal móvil o fijo como se realiza normalmente pero en este caso de forma ilegal o indebida se cursan llamada sin necesidad de ingresar al país de destino

por una central de tráfico internacional para finalmente ser recibida en un terminal móvil o fijo, en este caso el prestador del servicio de telefonía Voz IP no tiene conocimiento de que sus llamadas son cursadas haciendo uso de un sistema *By Pass.* La segunda modalidad se presenta cuando el prestador del servicio de telefonía Voz IP tiene complicidad con el sistema fraudulento por tanto enruta sus llamadas directamente desde internet hacia el sistema *By Pass*.

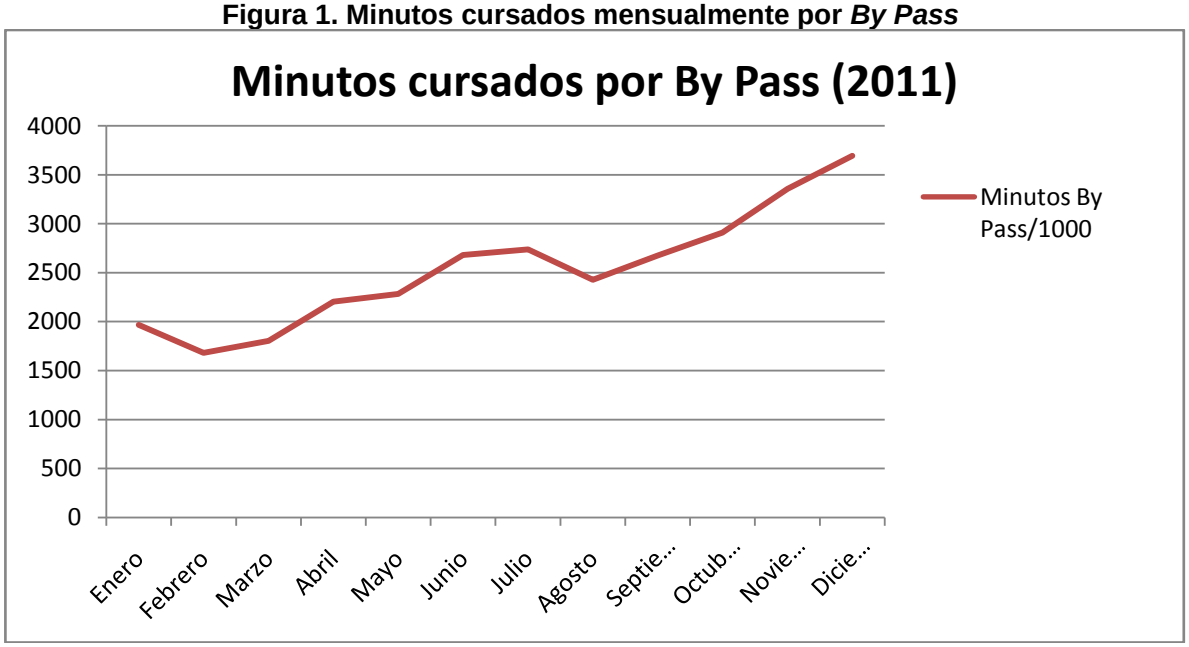
Esta modalidad de fraude genera pérdidas económicas para las empresas prestadoras de los servicios de telefonía para larga distancia internacional. Estas pérdidas económicas se presentan entre muchos otros factores, debido a que el tráfico internacional que es cursado haciendo uso de *By Pass* no es ingresado por las troncales internacionales con las cuales se tiene convenio y por las que además se paga un dinero para permitir que los operadores se conecten. Un ejemplo de este tipo de casos se presentó en el año 2002 cuando la empresa de comunicaciones EPM ganó una demanda a la empresa Overseas CATV Ltda. por la prestación del servicio de LDI haciendo uso de *By Pass* sobre líneas telefónicas del demandante con una indemnización a favor de EPM por $1.200 millones de pesos colombianos, valor que se estimó como aquel que había perdido EPM debido a las actividades realizadas por la empresa demandada[i].

En la actualidad no existen cifras oficiales acerca de la cantidad de minutos que son cursados haciendo uso de *By Pass* en Colombia, sin embargo, en la figura 1 se observa de forma aproximada la cantidad de minutos en llamadas entrantes de larga distancia internacional con destino en la red del operador móvil Claro Soluciones Móviles S.A. cursados haciendo uso de *By Pass*, cifras que permiten dar una idea de la dimensión del problema en términos de dinero que está dejando de percibir este operador debido a este fraude.

En el año 2011 el valor de un minuto real (tarificado en segundos) de larga distancia internacional cobrado por Claro Soluciones Móviles S.A. al operador de LDI Infracel era de COP$83[1] aproximadamente para permitir el ingreso del tráfico internacional a su red. Gracias a esta información se puede estimar que en promedio, mensualmente este operador registró pérdidas entre COP$145.130.000 y COP$307.100.000, aunque se debe tener en cuenta que a pesar de que estas llamadas fueron cursadas por *By Pass* el operador móvil percibió económicamente el valor de estas llamadas como si fueran nacionales, las cuales en plan postpago tienen un valor aproximado de COP$41.97, por tanto las pérdidas reales del operador son aproximadamente un 50.56% menos que los valores mencionados para unas pérdidas entre COP$71.752.272 y COP$151.830.240.

[1] Bornachera, Cesar (comunicación personal, 18 de Septiembre de 2012)

Figura 1. Minutos cursados mensualmente por *By Pass*



Fuente: Claro Soluciones Móviles S.A.

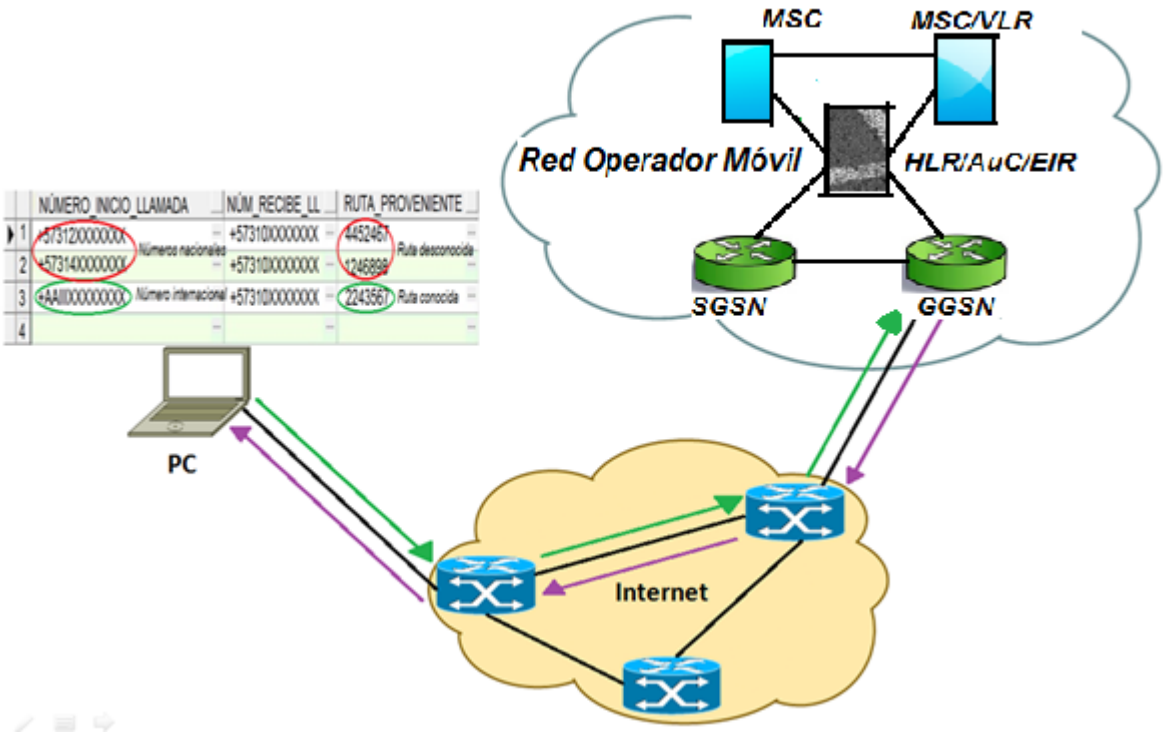
Debido a lo anterior los operadores de telefonía dedican sus esfuerzos a la implementación de sistemas y procesos de detección de fraude que permitan reducir el número de casos de *By Pass* que se presentan dentro de su red de comunicaciones. El constante incremento de usuarios de Voz IP y de llamadas cursadas haciendo uso de *By Pass*, ha generado que con el tiempo estos procesos se vuelvan menos eficientes debido al gran volumen de casos que se presentan diariamente lo cual hace más complejo tomar medidas correctivas que contrarresten el efecto negativo producido por esta práctica, generando una inversión mayor de tiempo por parte del encargado de supervisar el proceso de detección e inclusive, una mayor cantidad de empleados destinados a esta tarea.

En la actualidad este proceso se realiza de forma manual en la mayoría de operadores móviles, realizándose un sistema de detección y corrección de *By Pass* que requiere de una gran cantidad de tiempo por parte de la persona encargada de realizar este proceso con las limitaciones que este conlleva.

Este proceso se lleva a cabo en la actualidad con pruebas de “Lazo” o “Loop” consistentes en generar manualmente una llamada internacional mediante un Softphone o un terminal móvil con saldo para llamadas internacionales (saldo obtenido via Web para el primer caso y mediante la compra de una tarjeta de recarga perteneciente al prestador del servicio ilegal para el ultimo caso), llamada que tiene como destinatario un terminal móvil predeterminado cuya línea es propiedad del operador móvil y que se encuentra en el área donde se realizan las pruebas para que de forma manual la misma persona que inició la llamada sea

quien rechace la misma con el fin de no generar un costo debido al establecimiento de la comunicación. Luego de finalizar la llamada se procede a verificar mediante la ejecución de determinadas secuencias de SQL desde un PC, con conexión a la red del operador móvil, los CDR's (registros con información específica de la llamada) registrados en el HLR del operador y que previamente fueron generados debido a las llamadas realizadas mediante el proceso descrito anteriormente. Estos CDR's contienen información acerca del número de línea perteneciente al terminal que generó la llamada, el número de la línea hacia donde se dirige la llamada, la hora en que se realiza y el identificador de la ruta por donde se cursa la misma. La figura 2 ilustra de forma básica el proceso de consulta de los registros en el HLR y el resultado obtenido.

Figura 2. Consulta de CDR's en la red del operador móvil.



Fuente: Autor. Figuras: Cisco Systems Inc.

Luego de obtener los registros tal y como se observa en la figura 2. Estos registros son organizados y filtrados para que únicamente sean tenidos en cuenta aquellos que son de interés, este filtrado es indispensable para el proceso de detección debido a que en el HLR se encuentran los registros de todos los sucesos que ocurren en la red en cuanto a llamadas y mensajería.

Posteriormente se comparan los CDR's de interés con una tabla predeterminada en la cual se encuentra la información correspondiente a aquellas troncales de telefonía internacional con las cuales tiene convenio de interconexión el operador móvil, es decir, las rutas establecidas para las llamadas provenientes de otros países. Luego de realizar la comparación, se identifica cuales llamadas fueron cursadas haciendo uso de *By Pass*, estas siempre provienen de una ruta no identificada y dejan como registro un número móvil perteneciente a un operador de telefonía del mismo país al cual se dirige la llamada.

Finalmente se reportan aquellas Sim Card´s que están siendo utilizadas para *By Pass* con el fin de poder tomar medidas preventivas y correctivas debido a su uso fraudulento. Estas medidas van desde bloqueo del tráfico entrante y saliente a la línea detectada hasta la culminación unilateral del contrato pactado entre el operador y el dueño de la misma, quien en la gran mayoría de veces, consigue estas líneas mediante documentación falsa, robada o adulterada.

Luego de describir el proceso de detección actual que maneja el operador móvil respecto a este tipo de fraude, se evidencia que la necesidad de marcar de forma manual al móvil predeterminado por el área para la recepción de las llamadas y que además estas sean rechazadas para que no se genere ningún costo debido al establecimiento de la comunicación, implica: el uso de un terminal móvil, dos en el caso de que la llamada se genere desde un móvil y no desde un Softphone, y también la constante atención por parte del empleado encargado del proceso para rechazar la llamada en el momento adecuado. Posteriormente el encargado del proceso debe realizar un filtrado de los CDR's que se encuentran en el HLR, tarea que implica un acceso a la red del operador móvil desde la Intranet de la compañía, lo cual se presta para la aparición de los denominados delitos informáticos, como la captura de datos que viajan en la red, la suplantación de identidad del equipo que está extrayendo los CDR's o cualquier otro inherente al uso de redes informáticas.

En cuanto a la eficacia del proceso actual no se han encontrado falencias ya que no cabe posibilidad de que un número nacional funcione para ingreso de tráfico internacional por medios diferentes al *By Pass*. Para el caso de la eficiencia, la falencia más grave que se ha encontrado es la gran cantidad de tiempo que toma llevar a cabo todo el proceso como tal, puesto que se realiza de forma manual en su gran mayoría, lo cual implica que mientras se están generando y rechazando las llamadas, el mismo empleado no puede estar realizando las consultas de CDR's en el HLR, tampoco puede estar realizando la comparación con las tablas predeterminadas con la información acerca de las rutas entrantes ni tampoco generando el reporte con las líneas detectadas como fraudulentas. El tiempo real de funcionamiento del proceso actual se reduce únicamente a aquellas horas en las que el empleado se dedica exclusivamente a la generación y rechazo de llamadas, esto implica que durante las horas que este se dedica a las demás tareas del proceso o se encuentra fuera de su horario

laboral el proceso de detección se detiene en su totalidad. Lo anterior implica que durante fines de semana y horas de la noche no se detecten las líneas que están siendo usadas para *By Pass*. Limitante que han aprovechado los sistemas fraudulentos para brindar sus servicios de llamadas por *By Pass* en fines de semana y horas nocturnas sin ser detectados por el operador móvil.

Este es sin duda alguna el mayor aliciente para la búsqueda de un nuevo sistema de detección de fraude por parte del operador móvil. Se debe implementar un sistema de detección de fraude que permita realizar pruebas de *By Pass* de una forma rápida y sencilla, que sea independiente de la cantidad de horas que se invierte por parte del empleado para este proceso y que tenga la suficiente autonomía para realizar pruebas de forma continua durante horas o días enteros sin las necesidad de ser supervisado por una persona.

A partir de lo anterior surge la siguiente pregunta problemica:

¿Es posible implementar nuevos procesos y sistemas anti fraude que permitan aumentar la eficiencia en la detección de aquellas actividades fraudulentas que se presentan en la red del operador de telefonía móvil?

1.2. Justificación del trabajo

En los servicios de comunicaciones móviles existen dos partes involucradas, el operador y el usuario. El operador se puede considerar como aquel que le brinda al usuario el acceso y uso de los servicios que este ofrece, el usuario se puede considerar como aquel quien hace uso de estos servicios a cambio de una retribución económica en favor del operador. Cuando en estos servicios se presenta el fraude en cualquiera de sus modalidades, se ve involucrada una tercera parte y es quien comete el fraude (defraudador). Desde cualquiera de estas tres partes la implementación de un sistema de detección de fraude puede ser justificado.

Como ya se explicó anteriormente el *By Pass* es el fraude que se presenta en el trafico de llamadas internacionales tanto móviles como fijas que son cursadas a través de Internet gracias a la tecnología Voz IP sin pasar por las centrales de tráfico internacional, lo cual implica que una llamada internacional sea tarificada como si fuera una llamada nacional la cual tiene un costo inferior, generando así mayores beneficios económicos para el sistema fraudulento.

A partir de lo anterior se entiende que, por parte del operador móvil se están presentando pérdidas económicas debido a que su servicio de llamadas internacionales no está siendo utilizado correctamente y en cambio las llamadas entrantes a su red son tarificadas con el precio de una llamada local. Por otra parte este está pagando a los operadores internacionales por permitir la interconexión entre sí para que su servicio de llamada internacional funcione correctamente, pero debido al *By Pass* la cantidad de usuarios que hace uso de este servicio se hace menor por lo cual el operador está pagando por una interconexión que no se está usando en la cantidad esperada.

Por otra parte, quien ofrece el servicio fraudulento está infringiendo la ley puesto que presta un servicio ilegal de comunicaciones, aunque esto no implica que la empresa sea ilegal, el cual le está generando un beneficio económico ya que cobra al usuario un valor determinado por cursar su llamada el cual es inferior al de una llamada internacional pero superior al de una local, siendo este ultimo el valor real que paga el actor fraudulento al operador móvil por hacer uso de su red.

Finalmente se encuentra el usuario quien es participe de forma inconsciente en el fraude, suponiendo que este no conoce el funcionamiento del servicio que está utilizando, quien motivado por el precio inferior que le ofrece el actor fraudulento, prefiere hacer uso del servicio de llamada internacional por *By Pass* que pagar la tarifa que le ofrece el operador.

Esta modalidad de fraude se considera una conducta desleal hacía el operador por parte tanto de quien ofrece el servicio ilegal como de quien hace uso del servicio tal y como lo indica el artículo 18 de la Ley 256 de 1996[ii] el cual trata acerca de la competencia desleal.

Además, genera un desequilibrio económico en el mercado, ya que los operadores prestadores del servicio de llamada de larga distancia internacional no pueden ofrecer una tarifa que sea capaz de competir con aquella que ofrecen quienes brindan el servicio haciendo uso de *By Pass* tal y como lo estableció la Comisión de Regulación de Telecomunicaciones en su proyecto de fraude en los servicios de telecomunicaciones, regulación y asesoría en reoriginamiento de tráfico entrante de larga distancia internacional, "*en definitiva, el enrutador ilegal puede proporcionar a un segmento de mercado sensible al precio, una oferta mucho más atractiva que los operadores legalmente establecidos que si tienen todas las cargas ya mencionadas*".

Ante estas situaciones se evidencia la necesidad por parte del operador de implementar medidas que permitan disminuir el número de casos de *By Pass* que se presentan en su red, razón por la cual se justifica la proposición de un sistema de detección de fraude en tráfico de llamadas internacionales.

1.3. Objetivos

1.3.1. Objetivo General

Diseñar un proceso eficiente de detección de fraude tipo *By Pass* para el tráfico de llamadas internacionales que hacen uso de la tecnología Voz IP con destino en la red de un operador de telefonía móvil.

1.3.2. Objetivos Específicos

- Evaluar el proceso actual de detección de fraude para llamadas internacionales mediante Voz IP que se maneja en la empresa, identificando sus falencias y limitaciones.
- Identificar las oportunidades de mejora que se presentan en los procesos de detección actuales y realizar un estudio acerca de las herramientas tecnológicas actuales en el mercado que puedan ser utilizadas para la detección de fraude *By Pass*.
- Analizar las alternativas existentes con el fin de idear y desarrollar un nuevo proceso que brinde mayores beneficios en la detección de fraude frente al proceso que maneja el operador móvil.
- Plantear a la empresa prestadora de servicios móviles una alternativa para la realización de su proceso de detección que permita aumentar la eficiencia actual contra este tipo de fraude de forma económica.
- Cumplir con la misión de la Universidad Santo Tomás, aportando una solución a una problemática actual en el área de las comunicaciones que afecta la sociedad, lo anterior de forma ética, creativa y critica.

1.4. Alcances y limitaciones

1.4.1. Alcances

Entregar una metodología documentada que permita la detección del fraude tipo *By Pass* en una empresa de telefonía móvil celular.

1.4.2. Limitaciones

Las limitaciones encontradas en el desarrollo de esta monografía y de la temática que se aborda por medio de esta son:

- Solamente se analizará el fraude tipo *By Pass* debido a que en la actualidad es el que representa la mayor cantidad de pérdidas económicas para el operador.
- La restricción parcial para el uso de cualquier información perteneciente al operador móvil en el cual se desarrolla la monografía.
- No se cuenta con todos los dispositivos o elementos físicos necesarios para la implementación del sistema de detección de *By Pass* propuesto.
- No se puede implementar el nuevo proceso de detección debido a que en el operador móvil no se tiene presupuestado ningún recurso económico que permita invertir en la compra de los elementos necesarios.
- Para la implementación de un nuevo sistema de detección de fraude se debe obtener el aval del gerente encargado de la gerencia de protección y aseguramiento de ingresos y del coordinador del área de protección tecnológica, este último cargo se encuentra de momento vacante y en espera de un nuevo encargado.
- El proceso a desarrollar aplica únicamente para la detección de fraude *By Pass* mediante la tecnología Voz IP y no para el caso de la telefonía móvil tradicional, caso que también está siendo desarrollado en el operador mediante otro proceso de detección el cual hace uso del software SISPRIN.

1.5. Delimitación

1.5.1. Espacial

Este proyecto es desarrollado en el área de protección tecnológica perteneciente la gerencia de protección y aseguramiento de ingresos de un operador móvil con funcionamiento en Colombia, siendo la ciudad de Bogotá D.C. el lugar de ubicación del área en mención. Por otra parte, el proceso de detección de fraude planteado puede ser aplicado en cualquier operador de prestador del servicio de telefonía móvil independientemente de las características de su red, su ubicación física o la cantidad de usuarios que este maneje entre muchos otros factores.

1.5.2. Cronológica

Este proyecto abarca en su totalidad un periodo de 5 meses y contempla un total de 8 actividades a desarrollar las cuales se manejan de la siguiente forma.

Tabla 1. Cronograma

Actividad \ Mes	*Agosto*	*Septiembre*	*Octubre*	*Noviembre*	*Diciembre*
Búsqueda y elección de tema					
Introducción a la monografía					
Marco Teórico					
Desarrollo del proceso de detección de fraude.					
Conclusiones					
Revisión por parte del Director					
Revisión por parte de humanidades					
Revisión por parte de Comité de Grado					

Fuente: Autor

Como se observa en la Tabla 1. Durante el mes de Agosto se realiza la búsqueda de varios temas tecnológicos que estén siendo tratados por el área de protección tecnológica del operador móvil y que requieran de alguna mejora sustancial en su funcionamiento, además se hace la elección del tema a desarrollar, lo anterior en base a los resultados obtenidos en la búsqueda de

información acerca de las posibilidades de mejora del proceso actual existentes en el mercado.

Durante el mes de Septiembre se realiza la introducción de la monografía y el marco teórico en su totalidad y adicionalmente también se trabaja en el desarrollo de un nuevo proceso de detección de fraude.

En el mes de Octubre se continúa con el desarrollo del nuevo proceso de detección de fraude hasta finalizarlo en su totalidad junto con las conclusiones obtenidas a través del trabajo realizado. Durante los meses de Septiembre y Octubre todas las actividades ya mencionadas son revisadas periódicamente por el Director de la monografía de acuerdo a lo convenido con el estudiante.

En el mes de Noviembre la monografía es presentada ante la división de Humanidades para su corrección y posterior aprobación, durante el mes de Diciembre se presenta la monografía ante el Comité de Grado de la facultad de Ingeniería de Telecomunicaciones de la Universidad Santo Tomás con el fin de obtener la aprobación que permita obtener el título de Ingeniero de Telecomunicaciones de la Universidad en mención.

1.5.3. Metodológica

El proceso metodológico que se emplea para el desarrollo de este proyecto se basa en la identificación de una problemática de actualidad que esté afectando a los operadores de servicios de comunicaciones móviles y que su detección sea responsabilidad del área de protección tecnológica del operador en el cual trabaja el estudiante.

A partir de la problemática identificada, por medio de la practica se detectan las limitaciones que presenta el sistema de detección que se maneja actualmente en el área contra esta problemática para que en conjunto con una posterior investigación que permita dar conocimiento acerca de las opciones tecnológicas existentes en el mercado, se pueda idear un nuevo proceso que brinde mejoras y beneficios frente al proceso de detección actual para fraude en tráfico de llamadas internacionales.

Luego de conocer las alternativas existentes para implementar un nuevo sistema de detección del fraude específico que trata la monografía, se procede a realizar el análisis de la alternativa que más se ajuste a las necesidades y limitaciones del operador móvil.

Finalmente se brinda al operador móvil una alternativa económica frente al proceso de detección de fraude, que refleje tanto el conocimiento adquirido durante la pasantía de grado desarrollada en la empresa acerca de los tipos de

fraude existentes en la actualidad y las técnicas que se utilizan para contrarrestar los efectos que estos producen, como del conocimiento adquirido a través de los cuatro años y medio cursados en la facultad de Ingeniería de Telecomunicaciones de la Universidad Santo Tomas.

1.5.4. Financiera

Si bien el propósito de este proyecto es el de plantear una propuesta al proveedor de servicios de comunicaciones móviles para realizar su proceso de detección de fraude *By Pass* y no el de implementar el proceso desarrollado, un objetivo especifico de este trabajo es el del proponer una propuesta que sea económica para el operador, razón por la cual es importante establecer los elementos necesarios para el correcto funcionamiento del proceso y el costo aproximado de cada uno de estos para conformar un valor consolidado o total, que es en el que se supone tendría que incurrir el operador móvil en caso de decidir, cuando las limitaciones descritas lo permitan, implementar el proceso que se ha decidido proponer.

Se debe aclarar que hay elementos que no se necesita sean de una referencia, marca o modelo especifico, debido a que no requieren de ninguna característica particular como es el caso de un PC. Por esta razón se proponen elementos con un costo promedio en el rango de valores actuales que se encuentra disponible en el mercado. En la tabla 2 se observa el valor de los elementos necesarios para la implementación del proceso de detección de fraude *By Pass* planteado.

Tabla 2. Costo elementos del proceso de detección

Elemento	***Proveedor-Fabricante***	***No. Unidades***	***Valor Unidad***	***Valor total***
PC (CPU+Monitor+Mouse+ Keyboard) *	Hewlett-Packard / Compac /Sony / Samsung	1	COP$1.200.000	COP$1.200.000
Softphone (Proveedor Voz IP)	Skype / VoIPBuster / Adiptel	NA	Gratis	Gratis
Conexión a Internet**	Conexión ya existente con servicio funcionando	1	COP$55.000	Ya pago
Software Asterisk+Free PBX	Digium	1	Gratis	Gratis
Saldo de proveedores Voz IP ***	Skype / VoIPBuster / Adiptel	No definido	Mínimo COP$5.000	No definido
Sim Card	Movistar / Claro / Tigo / Uff	1	COP$8.000	COP$8.000
Switch 5 puertos	TP-Link	1	COP$25.000	COP$25.000
Cable UTP/RJ-45 (1 metro)	NA	3	COP$12.000	COP$36.000
GSM-IP Gateway 1 modulo Sim	Dinstar	1	COP$350.000	COP$350.000
Total				COP$1.619.000

Fuente: Autor

Nota: *Los valores representados en la Tabla 2 se manejan en pesos Colombianos y están sujetos a modificaciones dependiendo del movimiento del mercado y de la elección exacta de cada elemento necesario para la implementación del nuevo proceso en caso de que el operador decida implementar el proyecto. *Se propone un PC con características de Hardware de: 4.0 GB de RAM, Procesador AMD Athlon X2 3GHz, Monitor de 12 pulgadas. Lo anterior con el fin de que tenga características similares a los PC que tiene el operador actualmente, características que además permiten el correcto funcionamiento del sistema propuesto. ** La conexión a Internet necesaria para el PC ya se encuentra habilitada, en funcionamiento y disponible para su utilización, el costo de este servicio ya se encuentra pago por parte del operador. ***El saldo para la generación de llamadas a destinos móviles desde los servidores de Voz IP tienen generalmente el costo mínimo descrito en la Tabla 2, no se define el número de saldos que se deben adquirir ya que la cantidad de softphone a utilizar puede variar con el tiempo dependiendo de los nuevos proveedores de Voz IP que surjan y que puedan ser sospechosos de hacer uso de sistemas By Pass, por tal motivo el costo asociado de estas recargas asociado a la propuesta no se ha estipulado como un costo fijo sino como un ocasional.*

1.6. Enfoque Humanístico

En este proyecto existe un factor humanístico y ético generado por conductas indebidas que en un principio se pueden pensar como negativas y dirigidas únicamente al operador de telefonía móvil celular, pero existen consecuencias que van más allá afectando además al estado del país en el cual funcionan estos operadores y por tanto a su población.

Aquellas personas que realizan actividades fraudulentas con el fin de lucrarse económicamente, en la mayoría de los casos con resultados millonarios a su favor, están reduciendo los ingresos económicos percibidos por los operadores móviles victimas de estas conductas, por consiguiente el estado del país al cual pertenecen estos operadores también se ve afectado, se debe recordar que los impuestos que cobra el estado a las empresas varía en función de los ingresos generados percibidos, lo cual conlleva a un menor capital para la inversión en obras, proyectos y demás actividades que buscan brindar solución a problemáticas existentes en la población. Lo anterior hablando por el lado del estado pero este no es el único que colabora con la destinación de recursos al cubrimiento de necesidades o problemáticas del pueblo, los operadores móviles también apoyan directamente a la gente con obras sociales que ayudan principalmente a las personas de recursos mínimos de barrios marginales de las ciudades o en pueblos donde la tecnología aún no es parte integral de la vida de sus habitantes. Un ejemplo de estas actividades, tema conocido como responsabilidad social, se evidencia en el operador de servicios de comunicaciones Colombia Telecomunicaciones S.A. ESP. (Movistar) quien regala juguetes y ropa a niños de escasos recursos o equipos como PC’s en colegios pobres para colaborar en la educación de niños y jóvenes o el operador Claro S.A. con su copa de futbol Claro destinada a la participación de jóvenes de todo el país, brindándoles la oportunidad de desenvolverse en ambientes sanos y competitivos que despiertan en estos valores como la honestidad, la responsabilidad y la amistad.

Es cierto que en la actualidad la responsabilidad social es llevada a cabo por la gran mayoría de empresas así como también lo es el hecho de que la cantidad de recursos que se destinan a este tema es muy bajo en comparación con los ingresos percibidos, pero de cierta forma una pequeña parte de estos recursos terminan beneficiando a la sociedad, brindando apoyo a los más necesitados y retribuyendo de una u otra manera a las personas, caso que no sucede cuando se realizan actividades fraudulentas, no solo en la red de un operador móvil sino en cualquier actividad que se realice en la vida, donde todo el beneficio económico se

destina a una o un grupo de personas inescrupulosas, faltas de ética y sentido humanístico.

Para el caso del fraude que se trata en este proyecto, es seguro que quienes realizan estas conductas fraudulentas son personas con conocimientos avanzados en el área de las comunicaciones, que han invertido tiempo de estudio en el entendimiento de las debilidades y funcionamiento de redes de telefonía móvil celular e IP, quienes probablemente sean profesionales en esta área o en afines como la electrónica o sistemas. Profesionales que han aprovechado su saber para beneficiarse económicamente sin importar que sus actividades sean ilegales o ilícitas en algunos países y que además afecten a toda la sociedad. Son entonces estas personas profesionales sin ética que han abandonado sus principios, olvidando que estos como personas privilegiadas con acceso a educación y conocimientos avanzados deben enfocar sus esfuerzos en la contribución al desarrollo social y económico del país en lugar de entorpecerlo con su avaricia.

PARTE II

Marco Teórico

Capítulo 2

2. Fraude en Redes Móviles

Las redes móviles son sin duda alguna uno de los desarrollos tecnológicos más importantes de las últimas décadas, desde su aparición cambiaron la forma en que se comunican las personas, dejando a un lado la necesidad de encontrarse en un punto establecido conectado a la red como en el caso de la telefonía fija, permitiendo a los usuarios generar y recibir llamadas en cualquier lugar que estos se encuentren siempre y cuando se tenga cobertura de la red móvil, sin necesidad de una conexión física. Lo anterior en conjunto con desarrollos posteriores en este tipo de redes ha generado que el uso de terminales móviles sea una necesidad de las personas para el desarrollo de sus actividades cotidianas y laborales, y de las empresas para sus actividades comerciales.

Por tal motivo, se han desarrollado formas de realizar fraude a través de estas redes. Fraudes que han variado con el tiempo en función de las características técnicas de la red, de los terminales móviles, y de los servicios y aplicaciones que la red brinda. Uno de los primeros tipos de fraude existentes en las redes móviles fue la interceptación de la señal transmitida desde la Radio Base hasta el terminal móvil o viceversa con el fin de obtener información confidencial, este tipo de fraude solo pudo ser realizado en las redes de 1ra. Generación, cuya aparición se dio en los años 70 en Estados Unidos[iii]*, debido al poco nivel de seguridad manejado por estas redes.*

Posteriormente el desarrollo de las redes 2G en los años 90, permitió que solucionar el problema de la interceptación de la señal debido a nuevos sistemas de seguridad, razón por la cual se idearon nuevas formas de realizar fraude, robo de terminales y Sim Card's, clonación de tarjetas prepago y fraudes de suscripción, son solo algunos de los más comunes para este tipo de redes, aunque en la actualidad algunos de estos siguen presentes en redes 3G.

En los años 2000 surgieron las redes de 3ra. Generación, las cuales ya no solo tenían el fin de transmitir voz y mensajería a los usuarios, está vez el usuario tenía la capacidad mediante su terminal móvil de estar conectado a Internet en todo momento y navegar a través de esta de forma similar a lo que se realizaba desde un PC. Si bien este adelanto tecnológico ha generado un cambio total en la forma de comunicarse permitiendo la aparición de Smartphones, redes sociales, mensajería instantánea y demás, también ha permitido que a través de estas

redes se puedan realizar todas las actividades fraudulentas que se presentan en las redes de Internet convencionales lo cual ha implicado un gran esfuerzo por parte de los operadores móviles para poder implementar sistemas y procesos que permitan detectar e identificar los fraudes presentes en su red y reducir el impacto negativo que estos causan al usuario o al operador.

A medida que se desarrolla este capítulo se mencionan y explican de forma sencilla algunos de los tipos de fraude más comunes en las redes móviles con el fin de brindar una perspectiva más amplia acerca de la necesidad de implementar medidas de seguridad que permitan la detección, identificación y corrección de fraude.

2.1. Definición de fraude

El fraude se define como toda acción contraria a la verdad y a la rectitud, que perjudica a la persona contra quien se comete. Acto tendiente a eludir una disposición legal en perjuicio del Estado o de terceros. Engaño que se realiza eludiendo obligaciones legales o usurpando derechos con el fin de obtener un beneficio.[iv]

Para el área de las telecomunicaciones en general, según la CANTV[2] en la presentación elaborada por la gerencia de seguridad de la operación (2008) el fraude es: *"El uso o adquisición de los servicios de telecomunicaciones a través de medios ilegales y sin la intención de pagar por ellos."*.(Pág. 3) También se encuentra definido por el Gobierno de Honduras en el anteproyecto de medidas contra el fraude *By Pass (2012)* como: *"La prestación, comercialización, mercadeo y uso de los servicios de comunicaciones, por medio de prácticas no autorizadas y que son realizadas contraponiendo las disposiciones del régimen regulatorio y que van en detrimentos de los intereses de los proveedores…"* (Art. 5, Pág. 6).

Es importante mencionar que el fraude en comunicaciones en cualquiera de sus modalidades está generando pérdidas multimillonarias a los operadores de comunicaciones por tanto también a los estados y a las personas. A continuación algunos datos entregados por la CFCA[3] acerca del fraude en comunicaciones:

- *Anualmente las pérdidas por fraude en telecomunicaciones ascienden entre $35 a $40 Billones de Dólares Estadounidenses.*
- *80% de las compañías de Telecomunicaciones indican que el fraude continúa en ascenso.*
- *45% de las compañías indican que el fraude se ha incrementado dentro de su compañía.*
- *El fraude evoluciona con la tecnología y su entorno.*

[2] Compañía Anónima Nacional de Teléfonos de Venezuela.
[3] Communications Fraud Control Association

2.2. Clasificación de fraude en redes móviles

Sin importar la gran variedad de modalidades de fraude que pueden presentarse en una red de comunicaciones móviles todas pueden clasificarse en dos categorías, están todas aquellas que son realizadas desde fuera del operador, es decir, fraude externo o todas aquellas que son realizadas por empleados del operador móvil o con complicidad de estos aprovechando su posición privilegiada al ser parte de la organización, es decir, fraude interno. Cabe resaltar que aunque la gran mayoría de las actividades fraudulentas son realizadas con el fin de obtener un beneficio económico a favor de quien comete la actividad fraudulenta, existen casos en el que estas actividades se realizan por placer, siendo el caso más común la intrusión a la red del operador violando sus sistemas de seguridad con el fin de probarse así mismo que se tiene la capacidad de superar las medidas implementadas, siendo la conducta descrita anteriormente aquella que realizan los denominados Hackers.

2.2.1. Fraude interno

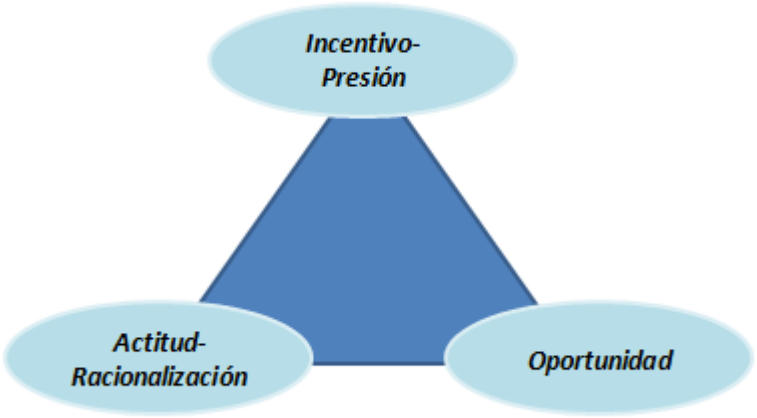
Este tipo de fraude es aquel se presenta cuando un empleado del operador móvil comete una actividad fraudulenta o es cómplice de una actividad que permite la realización de fraude en los sistemas del operador aprovechando el conocimiento que tiene acerca del funcionamiento de estos y de las medidas y sistemas de seguridad implementados, conocimiento que ha sido adquirido debido al desarrollo de su labor dentro de la compañía.

Según el “Estudio Global sobre delitos económicos” y el “informe sobre delitos económicos y fraude empresarial en España”, ambos realizados por la PWC[4] el fraude se puede caracterizar mediante el “triangulo del fraude” el cual se observa en la figura 3. En esta se evidencia que los tres factores fundamentales que alientan al fraude interno son: El incentivo o la presión, la actitud o racionalización y la oportunidad.

Se puede pensar que toda actividad fraudulenta implica un incentivo, ya sea económico o personal en el caso de los hackers como ya se mencionó anteriormente, pero lo cierto es que existen aquellos casos en que un empleado de la empresa es forzado a través del uso de la violencia o intimidación para que realice la actividad fraudulenta u omita una actividad determinada por parte de personas externas a la organización, es decir sea extorsionado.

[4] Price Waterhouse Cooper

Figura 3. Triangulo del fraude



Fuente: Price Waterhouse Cooper

Respecto a la actitud y racionalización del empleado, todo parte de la base ética de la persona como tal ya que una persona con principios éticos no sucumbirá a un incentivo económico si sabe que esta conducta fraudulenta genera una afectación negativa sobre el operador móvil o alguno de sus empleados o usuarios. Aunque es innegable que ante un acto de extorsión en el cual está en juego la integridad física de una persona, mantener una postura ética es complicado por no decir que imposible.

El tercer factor determinante según el triangulo del fraude es la oportunidad. Si bien la palabra oportunidad tiene gran variedad de definiciones dependiendo del ámbito en el cual se desee usar, todas estas definiciones tienen algo en común, la oportunidad es una circunstancia favorable que se da en función de un determinado momento y lugar. En el caso del operador móvil, existen oportunidades de realizar fraude interno que pueden variar dependiendo por ejemplo del cargo y funciones del empleado. Por tal motivo existen auditorías y controles internos, el análisis de riesgos o la dirección de seguridad informática. Estas medidas aseguran en cierta forma que las oportunidades de que se realicen actividades fraudulentas desde el interior del operador puedan ser evitadas, detectadas y/o corregidas. Pero lo cierto es que la gran mayoría de veces estas medidas no son suficientes, de acuerdo al estudio realizado por la dirección general de investigación especial en telecomunicaciones de ecuador descrito en su libro de fraude en comunicaciones (s/f) esto se debe a que: *"Los esfuerzos y recursos de los departamentos de fraude dentro de la industria de telecomunicaciones, están fuertemente concentradas en combatir los ataques desde fuentes externas, y el fraude interno raramente recibe la atención que se merece."* (Pág. 8).

Entre una gran variedad de actividades fraudulentas que se pueden realizar al interior del operador se encuentran la apropiación indebida de activos, el soborno y corrupción, la omisión de un deber, la modificación de información, el espionaje a favor de la competencia, entre otros.

Sin embargo, en cuanto al fraude que se realiza sobre la red y sistemas del operador móvil, la manipulación de la información y la apropiación o comercialización de activos del operador son los dos tipos de fraude interno más comunes y que tienen mayor afectación negativa sobre este.

2.2.1.1. Manipulación de la información

La manipulación de información dentro de una organización, sin importar cuál sea la actividad comercial de esta, es una problemática que puede suceder al interior de la misma en una gran variedad de situaciones, todo depende del cargo y funciones del empleado, de que información desea manipular y del proceso que se ha detectado previamente como vulnerable para cometer una conducta fraudulenta. En el caso de un operador móvil que cuenta con millones de usuarios la gran cantidad de herramientas y aplicaciones necesarias para brindar los servicios del operador en conjunto con la cantidad de empleados y funciones a realizar genera incontables posibilidades o situaciones propicias para realizar fraude.

Un ejemplo de manipulación de la información se presenta cuando un empleado del operador móvil, el cual tiene acceso a las plataformas de suscripción de usuarios, introduce datos erróneos o altera los registros existentes para el uso de los servicios que presta el operador con el fin de que el consumo realizado por la línea registrada no pueda ser facturado a algún usuario.

2.2.1.2. Apropiación y comercialización de activos

La apropiación de activos abarca gran cantidad de actividades, estas van desde el robo de papelería hasta el de elementos de la red como terminales móviles, Sim Card’s, computadores, cables, routers u otros similares. Dentro de la apropiación de activos también se incluye el robo de activos de información, por ejemplo el robo de archivos con información confidencial acerca de las líneas que deben ser reportadas como sospechosas de *By Pass*, permitiendo que estas sigan operando durante más tiempo hasta que vuelvan a ser detectadas, lo cual implica pérdidas económicas para el operador.

Respecto a la comercialización de activos que como ya se explicó pueden ser físicos o de información, se abarcan situaciones como la venta de información confidencial del operador móvil para que sea usada por la competencia o cualquier

otra entidad que pueda hacer uso de esta información para sacar provecho a favor del mismo o para afectar las actividades comerciales del operador. También se encuentra la comercialización de terminales móviles los cuales son vendidos al empleado del operador con descuentos elevados y posteriormente este vende el equipo por un valor superior. Otro ejemplo de comercialización de activos se presenta cuando un empleado el cual tiene asignada una línea entregada por el operador para que este desarrolle sus actividades laborales, es decir una línea "in-house", comercializa minutos a destinos internacionales por medio de conferencia y todo el costo de estas comunicaciones son asumidos por el operador.

2.2.2. Fraude Externo

Como su nombre lo indica este tipo de fraude corresponde a todas aquellas actividades fraudulentas en las cuales intervienen personas ajenas al operador móvil, aunque como se explica más adelante cuando se mencionan otros fraudes en redes móviles puede haber complicidad con un empleado del operador el cual facilita el desarrollo del fraude.

Aun cuando se cuenta con departamentos especializados como el de detección y control de fraude o el de seguridad informática los cuales implementan procesos con el fin de evitar que aquellas personas que realizan estas actividades no puedan cumplir con su objetivo de obtener un beneficio a costas de las vulnerabilidades de la red o del desconocimiento del los usuarios estas medidas no son suficientes para evitar que se presenten fraudes en su red. Lo anterior se debe a varios factores entre los cuales se encuentran la falta de una legislación homogénea en todos los países que penalice estas actividades lo cual brinda a quienes realizan fraude un refugio para continuar afectando a cualquiera que sea la victima de sus actividades, la falta de controles modernos que se ajusten a las nuevas modalidades de fraude que surgen día a día, o la gran habilidad que tienen quienes realizan fraude para sobrepasar las medidas existentes por parte del operador.

Debido a que en la actualidad las redes móviles ya no brindan únicamente el servicio de voz y mensajería, sino que también integran los servicios de transmisión de datos, estas redes pueden sufrir todos los ataques ya conocidos en las redes de Internet, entre los más comunes se encuentran el Phishing, los virus informáticos y el Spam. Pero además de estos también existen aquellos fraudes que se presentan desde hace varias décadas en las redes de telefonía convencional y que han sido adaptados de cierta forma para poder sacar provecho igualmente en las redes móviles. Entre los más conocidos se encuentran el Call Back, el fraude de suscripción, el fraude en Roaming Internacional y *By Pass*, siendo este último el que más pérdidas económicas genera a los operadores que brindan el servicio de larga distancia internacional.

2.3. Fraude *By Pass* en redes móviles

Como ya se mencionó, este tipo de fraude se presenta tanto en telefonía fija como móvil y consiste en recibir trafico de larga distancia internacional haciendo uso de un sistema *By Pass* el cual permite redirigir este tráfico para que sea directamente recibido por las centrales nacionales sin ingresar por las centrales de tráfico internacional pertenecientes a los operadores de telecomunicaciones habilitados legalmente en el país para prestar este servicio, operadores de LDI que además tienen un convenio establecido con el operador móvil para mantener la interconexión entre sí. De esta forma la tarificación de la llamada proveniente desde un país en el exterior hacia la red del operador móvil es realizada con el valor de una llamada nacional la cual tiene un valor inferior al de una llamada nacional[v], diferencia que en algunos casos llega a ser hasta 8 veces el de una llamada nacional lo cual genera grandes beneficios económicos a favor de quienes hacen uso de sistemas *By Pass* y así mismo grandes pérdidas al operador móvil.

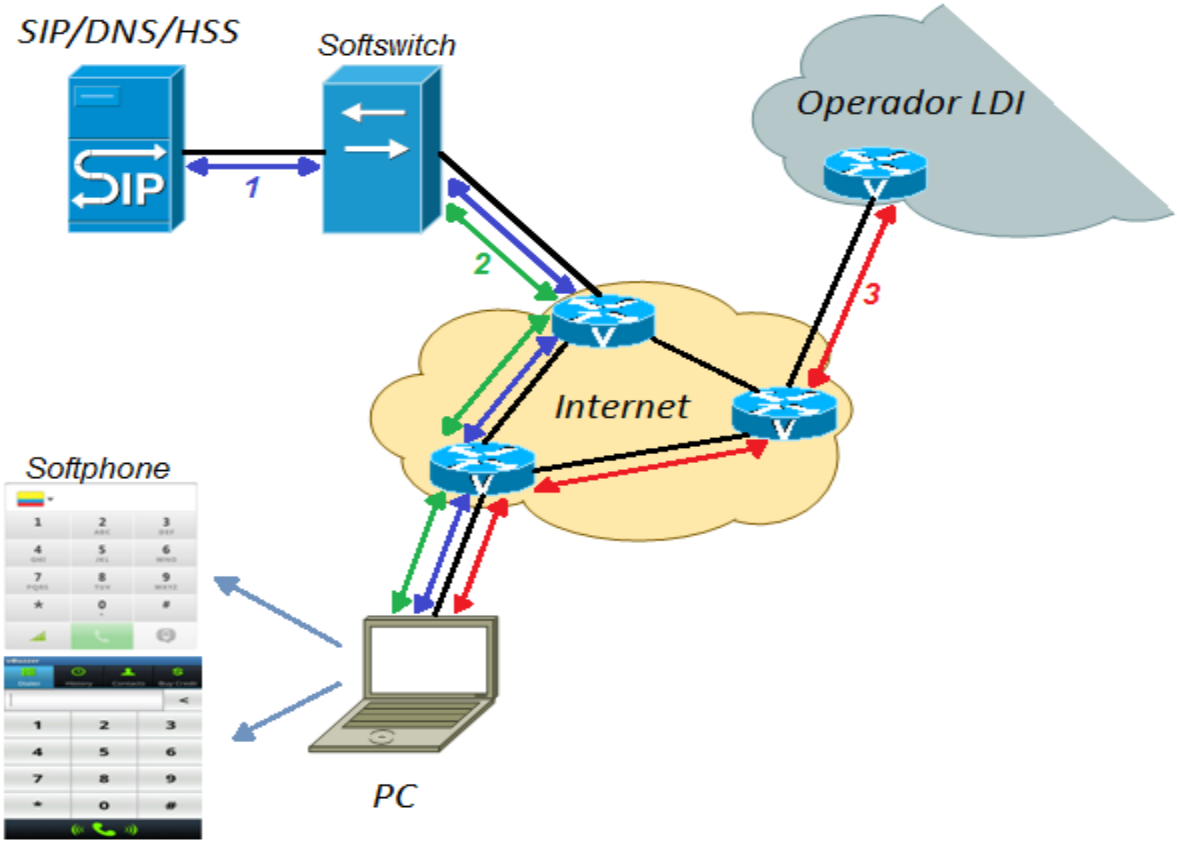
2.3.1. Funcionamiento de un sistema By Pass

Un sistema *By Pass* se encuentra conformado en el caso de la Voz IP por un Softphone que ha sido desarrollado por el operador del Servicio Voz IP, que puede ser legal o ilegal, el cual le permite al usuario registrarse en su servidor o por un conjunto de terminales móviles en el caso de la telefonía móvil tradicional. Entre los operadores de Voz IP más conocidos se encuentran SkypeOut, VoIPBuster o Vbuzzer, aunque en la actualidad se encuentran más de 2000 proveedores de Voz IP en el mundo.[vi] Posteriormente por medio de una recarga de salgo vía Internet para el caso de Voz IP o comprando una tarjeta con saldo para el caso de la telefonía móvil tradicional el usuario tiene la posibilidad de llamar desde su Softphone o terminal móvil a un numero ya sea fijo o móvil que se encuentra en otro país con una tarifa inferior a la que ofrecen los operadores móviles o fijos de dicho país, tarifas que varían dependiendo del país de destino.

En la figura 4 se muestra el proceso realizado para generar una llamada Voz IP a un equipo móvil o fijo en otro país. Primero el usuario se registra a través de su Softphone en el servidor del proveedor de Voz IP, posteriormente este hace login (inicia sesión) en el servidor para poder empezar a usar los servicios que brinda el proveedor. En el momento en que el usuario marca a un número móvil o fijo que se encuentra ya sea en su propio país o en el exterior el Softphone envía los datos de destino al Softswitch y este se encarga de establecer, entre muchas otras funciones, la ruta por donde debe ser cursada la llamada para que esta se

dirija al operador LDI indicado. Finalmente cuando ya se ha establecido la ruta que debe tomar el tráfico generado por la comunicación, se procede a iniciar la llamada.

Figura 4. Generación de una llamada Voz IP



Fuente: Autor. Figuras: Cisco Systems Inc.

Este operador de Voz IP tiene convenios de interconexión con operadores de LDI los cuales se encargan de recibir la llamada entrante que ha sido generada por el usuario, de igual forma en que lo harían tanto los operadores de telefonía móvil como fija, y dependiendo del país de destino de la llamada esta es direccionada hacia un CI el cual tiene un convenio ya establecido tanto con el operador de LDI del país que genera la llamada como con un operador LDI del país al cual se dirige la llamada de esta forma el Carrier se encarga de transportar todo el trafico proveniente desde el operador LDI y lo entrega en el país de destino mientras que el operador LDI le permite al CI recibir en el país todo el trafico proveniente del exterior.

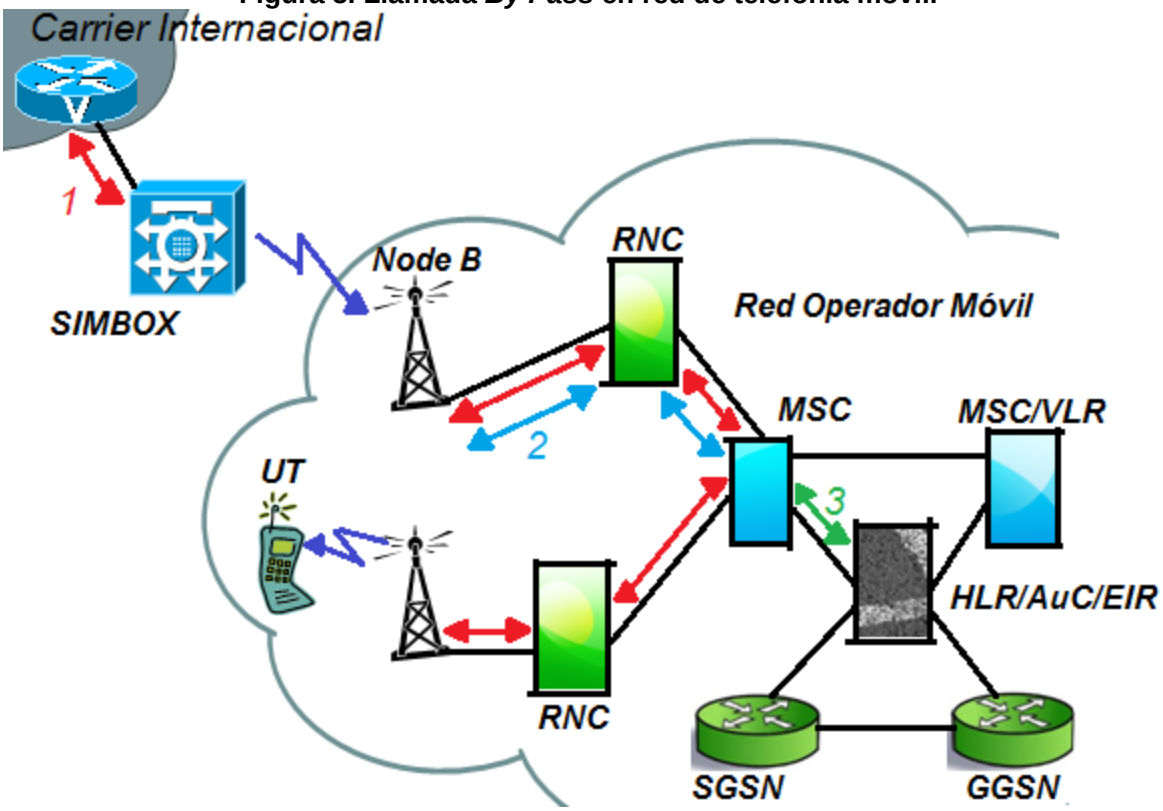
Luego de que la llamada es transportada hasta el país de destino esta llamada únicamente puede ser ingresada a través de los operadores LDI de aquel

país los cuales a su vez tienen convenios de interconexión con los operadores tanto de telefonía móvil como fija. Hasta este punto del proceso no existe ninguna diferencia entre una llamada de LDI convencional y una llamada por *By Pass*, el problema surge al momento de recibir el tráfico entrante al país de destino, es aquí cuando este es ingresado a través de un operador *By Pass* el cual se hace pasar por operador de LDI sin encontrarse habilitado legalmente para brindar este servicio, para el caso de Colombia los operadores legales más conocidos son Telmex, Orbitel, Infracel, UNE.

Finalmente, luego de que el tráfico proveniente del extranjero es recibido por el Operador de LDI este le entrega el tráfico al operador de telefonía móvil o fija del país de destino a través de una ruta preestablecida para que este se encargue de realizar la conmutación de la llamada y pueda ser recibida por el usuario final, estableciendo así la comunicación entre ambos usuarios. Para el caso de *By Pass* la llamada es recibida directamente desde el CI por el falso operador de LDI el cual, por ser ilegal, no cuenta con una ruta establecida con los operadores de telefonía del país de destino para poder ingresar su tráfico y realizar el establecimiento de la llamada, es en este punto donde se genera el fraude *By Pass*. Estos operadores ilegales ingresan su tráfico por medio de un equipo de comunicaciones conocido como Simbox el cual se encarga de conmutar el trafico proveniente desde Internet para que mediante un grupo de Sim Card’s conectadas al Simbox se pueda generar la marcación de la llamada en el caso de que la llamada se dirija a un operador móvil o de un IP-PBX conectado mediante un Signaling and Media GateWay a una línea telefónica fija en el caso de que la llamada se dirija a un operador fijo, siendo esta última la opción menos utilizada debido a permite una fácil detección no solo del fraude sino de los responsables del fraude puesto que para estas líneas tienen una ubicación física determinada que ya conoce el operador del telefonía fija desde el momento que se realizó la instalación de la línea. De esta forma se logra que una llamada internacional sea vista como una llamada local en la red del operador local como Claro, Movistar, Tigo, ETB o Telmex entre muchos otros, generando así un beneficio económico para el falso operador de LDI. En la figura 5 se ilustra gráficamente como se encuentra conectado el sistema *By Pass* al CI como a la red del operador local móvil. Para el caso de *By Pass* en telefonía fija la ilustración es similar excepto por el equipo utilizado para realizar la interconexión entre el CI y la red PSTN.

Cuando el usuario que se encuentra en un país extranjero genera una llamada la cual es cursada por *By Pass*, el trafico de la llamada es ingresado desde el CI al Simbox el cual por medio de Sim Card’s genera una llamada local por lo cual se hace una solicitud a la red móvil para generar la llamada local y posteriormente la red busca en su HLR toda la información necesaria para que se pueda establecer la llamada de forma correcta, posteriormente mediante Paging (técnica que permite ubicar el UT dentro de la red) se determina la ubicación del terminal móvil de destino, finalmente se establece la ruta que debe tomar el trafico para que se pueda establecer la comunicaciones entre los usuarios.

Figura 5. Llamada *By Pass* en red de telefonía móvil.



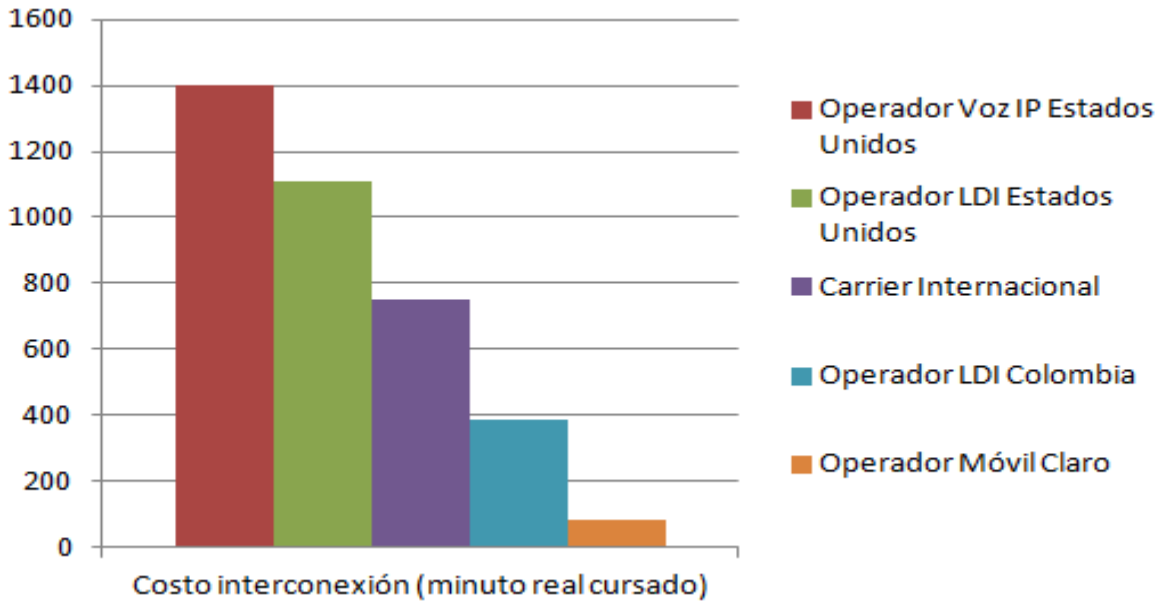
Fuente: Autor. Figuras Cisco Systems Inc.

Es así como se realiza el fraude *By Pass*, pero además es importante dar una explicación acerca de la forma en que se maneja el tema costos de interconexión existentes en la actualidad por parte tanto de los operadores móviles o fijos, los operadores de LDI como de los CI con el fin de poder establecer exactamente donde se presenta el beneficio económico a favor de quienes realizan fraude puesto que aunque se le tarifique como una llamada local, también existen otros costos que no se han tenido en cuenta.

En las figuras 6 y 7. se muestran todos los operadores involucrados en el establecimiento de una llamada de larga distancia internacional y una por *By Pass* respectivamente. La interconexión entre cada uno de estos operadores tiene un costo por minuto real cursado a través de la conexión establecida, estos costos pueden variar fuertemente dependiendo del país de origen y de destino. En algunos casos como el del país Cuba, el valor de establecimiento de una llamada dirigida a aquel país puede llegar a ser hasta 5 veces superior al de una llamada que se dirige a Estados Unidos, la variación de las tarifas de LDI en el mundo pueden ser tan variadas que en algunos casos, como se explica más adelante en

el denominado fraude de tercer país, es más económico cursar una llamada que se dirige desde el país A con destino al país B a través del país C que directamente desde el A al B. En este caso para poder dar un ejemplo de los beneficios y costos existentes en el proceso *By Pass* se propone como ejemplo una llamada que se dirige a Colombia hacia un móvil del operador Claro Soluciones Móviles S.A. proveniente desde Estados Unidos, el usuario que genera la llamada es un usuario prepago sin plan especial para LDI. Estos valores no son reales pero son aproximados que permiten dar una idea de las ganancias aproximadas que este fraude genera. Los valores son manejados en pesos colombianos.

Figura 6. Costos de interconexión de una llamada LDI.

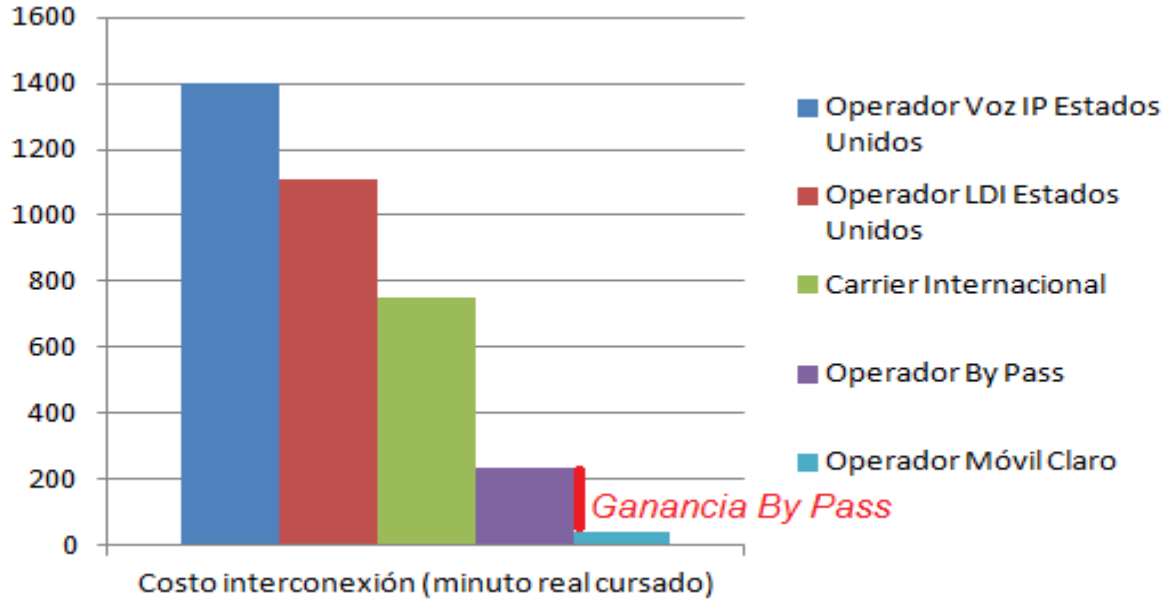


Fuente: Bornachera Cesar, (comunicación personal, 26 de Septiembre de 2012).

En la grafica 7 se evidencia que debido al tráfico *By Pass* ya no existe la necesidad que cursar la llamada a través del operador LDI del país de destino en el caso de que el operador Voz IP haga uso de los operadores LDI del país de origen, lo anterior se conoce como trafico entrante. Pero también se puede dar el caso en que el operador Voz IP, el cual es ilegal, tiene complicidad con el sistema *By Pass* evitando el uso de un operador LDI del país de origen para enviar su tráfico hacia el extranjero, esta modalidad se denomina trafico saliente. Además se observa que el sistema *By Pass* reemplaza en la cadena de interconexión al operador de LDI obteniendo así una gran cantidad de ingresos económicos puesto que al ofrecer una tarifa inferior al CI para recibir su trafico este ingresa la mayor cantidad posible por el sistema *By Pass* y este incrementa aun mas sus ganancias debido a que el precio que paga por el establecimiento de la llamada local es de

aproximadamente COP$41.97[5], valor inferior en más de un 50% al valor que percibe el operador por permitir a los operadores de LDI ingresar el trafico proveniente del extranjero a su red.

Figura 7. Costos de interconexión de una llamada por *By Pass*



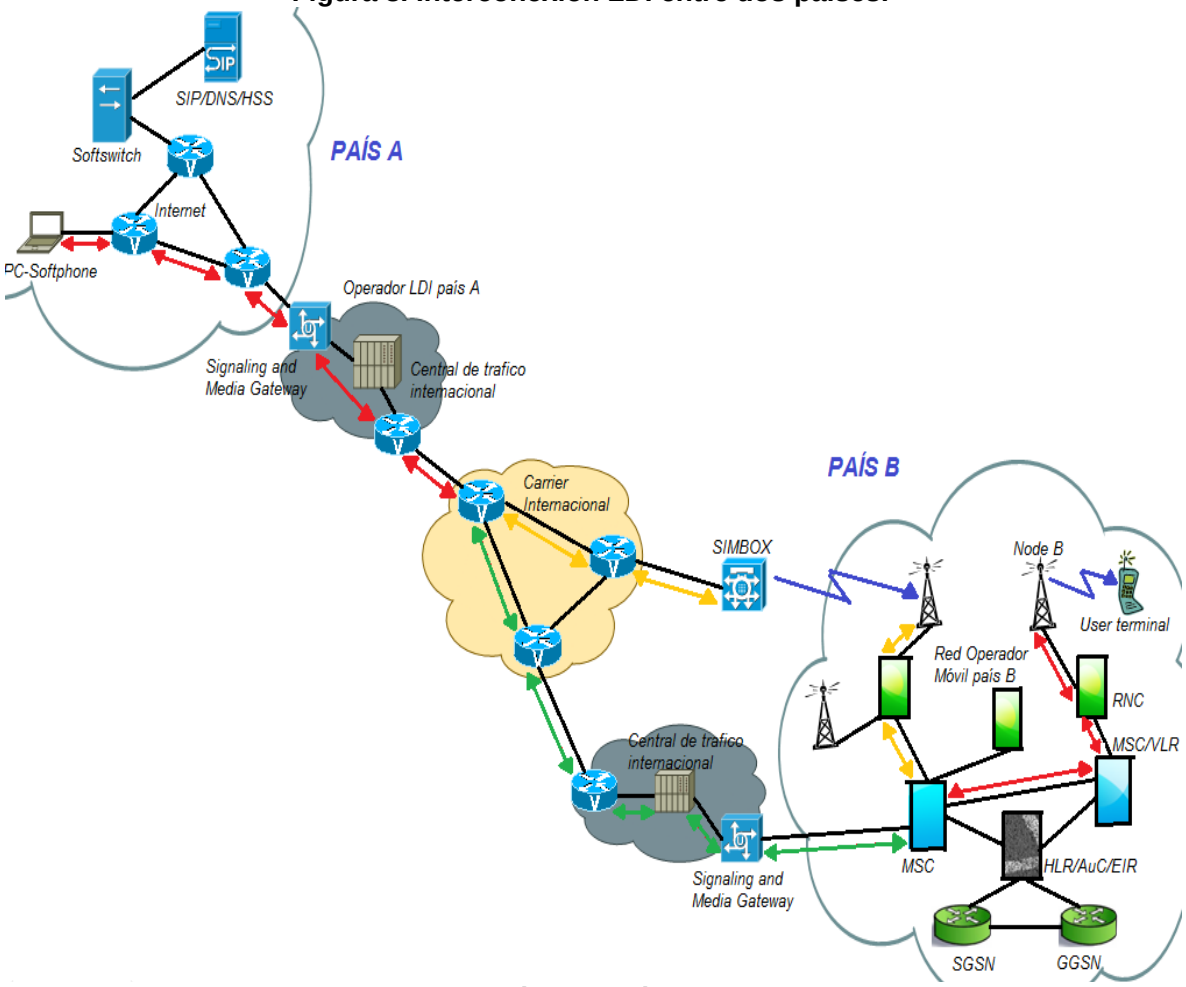
Fuente: Bornachera Cesar, (comunicación personal, 26 de Septiembre de 2012).

Estas graficas permiten suponer que del costo total que se cobra al usuario por cada minuto cursado el operador *By Pass* percibe aproximadamente el 12.8%. Pero en aquellos casos en que la llamada es generada desde un operador de Voz IP que además es ilegal y es parte del mismo sistema *By Pass* estas ganancias son del 97% aproximadamente puesto que tampoco se hace uso de un operador LDI del país que genera la llamada ni de un CI.

Con el fin de obtener una idea global acerca de todas las parte involucradas en el proceso de una llamada *By Pass* y una de larga distancia internacional mediante un Softphone perteneciente a un operador Voz IP legal, el cual no tiene conocimiento de que sus llamadas hacen uso de un sistema *By Pass*, se ha realizado la figura 8 la cual ilustra una ruta cualquiera existente entre dos países. En color rojo se describe la ruta que toma el tráfico generado por una llamada desde un Softphone hasta un móvil que se encuentra en la red de un operador en un país extranjero. Los colores verde y naranja muestran la ruta que toma el tráfico cuando es cursado como una llamada de LDI y cuando es una cursada por *By Pass* respectivamente.

[5] www.claro.com.co

Figura 8. Interconexión LDI entre dos países.



Fuente: Autor. Figuras: Cisco Systems Inc.

Se puede pensar que el problema del fraude *By Pass* podría ser solucionado fácilmente si los CI no brindaran a los falsos operadores de LDI una conexión a su red pero debido a que no existe una normativa internacional que regule este tema y al no poder aplicar las normas existentes en los distintos países a estos Carriers debido a que no pertenecen a ningún país como tal, estos no realizan las debidas inspecciones para verificar qué operador LDI es legal y cual no, además en países como Estados Unidos no es ilegal el tráfico internacional de llamadas sin hacer uso de una central de tráfico internacional a diferencia de países como Colombia.

2.3.2. Características de un sistema By Pass

Los sistemas *By Pass* en telefonía móvil debido a los elementos que lo conforman según la dirección general de investigación especial en telecomunicaciones de ecuador descrito en su libro de fraude en comunicaciones (s/f), se caracterizan por:

- Hacer uso grandes grupos de Sim Card’s asociados a un mismo usuario, casi siempre obteniendo estas líneas mediante fraude se suscripción o rodo de identidad (Surfing).
- Necesitar un enlace internacional que permita recibir el tráfico proveniente de los CI el cual a diferencia de un enlace tradicional cuenta con un espectro simétrico para transmisión y recepción de tráfico, lo anterior con el fin de mantener la misma calidad de la comunicación en ambos sentidos.
- Las líneas utilizadas generan grandes cantidades de tráfico pero no reciben llamadas, tampoco generan ni reciben mensajería.
- Registrar mayor actividad en horas de la noche y fines de semana, esto se debe a que en la mayoría de casos los sistemas de detección únicamente funcionan en horas laborales no nocturnas de lunes a viernes, lo cual ya tienen identificado quienes realizan este fraude.
- Generar un gran consumo de los recursos radioeléctricos de una misma radio base, esto se debe a que el Simbox se encuentra en una misma ubicación.
- Ofrecer tarifas ligeramente inferiores a las ofrecidas en el mercado tanto para recibir el tráfico proveniente de un CI como para el establecimiento de la llamada del usuario en caso de que también hagan uso de portales electrónicos (Softphone).
- Las líneas utilizadas cuentan con planes postpago de grandes cantidades de minutos para llamadas nacionales puesto que tienen un costo hasta 8 veces inferior que el aplicado por el operador para una línea prepago.

Debido a las características de estos sistemas fraudulentos es posible detectar y ubicar físicamente el lugar donde se está realizando el fraude, más adelante en la sección 2.3.3 se muestra la relación entre las características del sistema y su detección y ubicación.

2.3.3. Detección y ubicación de un sistema By Pass

Un sistema *By Pass* puede ser detectado mediante la consulta de los CDR's registrados en el HLR del operador móvil pertenecientes a cada llamada generada por cada una de las líneas fraudulentas. En estos registros siempre se encuentra la información acerca del número que inicia la llamada, el número a donde se destina la llamada, la hora y duración de la llamada, entre otros datos.

La diferencia que permite identificar un sistema *By Pass* es que al verificar los CDR's el número registrado como aquel que inicia la llamada es un número nacional perteneciente a alguno de los operadores móviles del país de destino, casi siempre del mismo operador que la línea utilizada por el terminal de destino puesto que el costo de la llamada es más barato. Mientras que para el caso de una llamada Internacional que ha sido cursada haciendo uso de los Operadores de LDI establecidos legalmente el número registrado como aquel que inicia la llamada es un número Internacional asociado al Carrier que transportó el trafico generado por la llamada.

De esta forma, mediante la constante generación de llamadas de Voz IP por parte de la gerencia de control de fraude del operador móvil con destino a un terminal móvil con línea perteneciente al mismo operador se van creado CDR's que posteriormente pueden ser analizados para identificar las líneas utilizadas para fraude *By Pass*, lo que posteriormente permite suspender el servicio permanentemente para estas líneas y tomar medidas legales contra el usuario o grupo de usuarios asociados o registrados como propietarios de estas líneas. Un ejemplo de estas medidas se encuentra en el anexo de conductas no autorizadas para el cliente perteneciente al operador móvil Movistar en la clausula tercera que habla acerca de las sanciones al usuario entre las cuales se encuentran: *"Terminación unilateral del contrato y suspensión inmediata del servicio, pago al operador por la cantidad de minutos cursados por las líneas implicadas con un valor por minuto igual al establecido entre el operador móvil y los operadores de LDI con los cuales este tiene acuerdos."* (Pág. 8).

En cuanto a la ubicación de un sistema *By Pass* el nivel de complejidad es elevado pero no imposible, la primera información a verificar cuando ya se tienen identificadas las líneas usadas para fraude y por consiguiente el usuario propietario de estas líneas es la dirección de residencia indicada por el usuario al momento de firmar contrato con el operador, pero esta medida resulta ser ineficiente debido a que generalmente el contrato fue firmado con datos falsos o documentación robada. Una medida más efectiva aunque de mayor complejidad es mediante la información registrada por la red del operador acerca de las celdas en las cuales se generan llamadas de las líneas fraudulentas aunque la ubicación se reduce a un área que puede tener un tamaño de cientos de metros debido al

alcance de la celda. Pero este problema puede ser resuelto mediante la trilateración entre celdas, técnica utilizada para la radionavegación de terminales móviles. En este caso la ventaja existente es que a pesar de que se utilizan móviles para realizar fraude el equipo Simbox en el cual se encuentran conectadas las Sim Card’s precisa de un lugar fijo para su funcionamiento.

En el caso de que el operador detecte y ubique un sistema *By Pass* este puede acudir a medidas aun más fuertes que las establecidas en las clausulas sancionarías, medidas que pueden llegar incluso al punto de verificar mediante una orden legal la propiedad (vivienda) en la cual se detectó el sistema. Esta información se puede corroborar en la clausula cuarta del anexo de conductas no permitidas al usuario del operador Movistar clausula que lleva el nombre de Derecho de Inspección.

2.4. Otros fraudes en redes móviles

Todos los fraudes que son descritos a continuación corresponden a fraude de tipo externo excepto el fraude de suscripción y el Gosthing que pueden presentar complicidad de un empleado del operador lo cual los convierte en fraudes tanto externos como internos. Cada uno de estos fraudes genera una pérdida económica al operador móvil, por esta razón existe la gerencia de protección tecnológica y aseguramiento de ingresos quien se encarga de disminuir los efectos negativos producidos por estas conductas ilícitas. Para cada uno de estos fraudes existen medidas de detección y control tan complejas como las medidas de detección de *By Pass* o inclusive aun más. En todo caso, únicamente se menciona en qué consiste el fraude con el fin de brindar una idea más amplia acerca de la gran cantidad de conductas fraudulentas que pueden presentarse en la red del operador móvil pero no se describe el proceso de detección utilizado para cada uno.

2.4.1. Fraude de suscriptor

Consiste en la adquisición de líneas telefónicas asociadas a servicios de comunicaciones que ofrece el operador móvil haciendo uso de una identidad inventada la cual no existe o mediante el robo o suplantación de identidad de otra persona con el fin de que la facturación por estos servicios no pueda ser cobrada a alguien o sea cobrada a la persona a quien se le robó la identidad. En este tipo de fraude existe la posibilidad de que haya complicidad de un empleado del operador móvil el cual ingresa adrede los datos falsos.

2.4.2. Gosthing

Fraude en el cual se modifican los CDR’s de las bases de datos del operador móvil con el fin de afectar datos como tarificación por el uso de servicios, servicios asociados a una línea, dirección de cobro de las facturas, etc.

2.4.3. Spoofing

Consiste en el uso de técnicas de suplantación de identidad a través de alguno de los servicios que brinda el operador. Un ejemplo de Spoofing es el Spam y el Phishing mediante SMS, donde se envían cientos o miles de mensajes no solicitados a distintos usuarios de la red informando que es el ganador del

algún premio pero para poder reclamarlo debe informar algún dato o enviar un mensaje a otro destino, obteniendo la confianza del usuario en la información enviada suplantando la identidad de entidades públicas o privadas reconocidas, recolectando así tanto información confidencial de los usuarios como su dinero.

2.4.4. Spyware

Programas de software que se alojan clandestinamente en el dispositivo móvil del usuario, proveniente desde la red de Internet o desde otro terminal, con el fin de capturar información de las actividades realizadas por el usuario, especialmente los datos digitados como cuentas y contraseñas sin que este sepa de la existencia del software espía en su equipo.

2.4.5. Robo de líneas y terminales móviles

Este fraude generalmente se produce mediante un atraco al usuario con el fin de realizar la posterior venta del terminal móvil o la comercialización de sus partes para ser utilizadas como repuestos, también con el objetivo de aprovechar el tiempo que transcurre desde el momento en que se roba al usuario hasta que este reporta ante el operador móvil la situación para hacer el máximo uso de todos los servicios que se encuentran asociados a la línea del usuario como minutos, navegación y mensajería puesto que a pesar de ser víctima de esta situación, el usuario tiene que pagar por el consumo realizado por el victimario.

2.4.6. Fraude de tercer país

Este fraude consiste en la adquisición mediante fraude de suscripción de una o varias líneas ya sean fijas o móviles por parte del defraudador el cual se encuentra en el país A, este recibe la información de un usuario que se encuentra en el país B el cual desea comunicarse con un usuario del país C, cuando ya se tienen los datos del usuario de origen y de destino, el defraudador genera una llamada internacional con destino al usuario en el país B y otra al usuario en el país C y mediante el uso de conferencia permite que estos se puedan comunicar. Finalmente el defraudador del país A se retira para que el consumo producido no pueda ser cobrado por el operador.

2.4.7. Fraude en Roaming Internacional

Mediante la adquisición de una o varias líneas, mediante fraude de subscrición, pertenecientes a un operador móvil las cuales tienen activadas el servicio de Roaming Internacional el defraudador comercializa los beneficios del

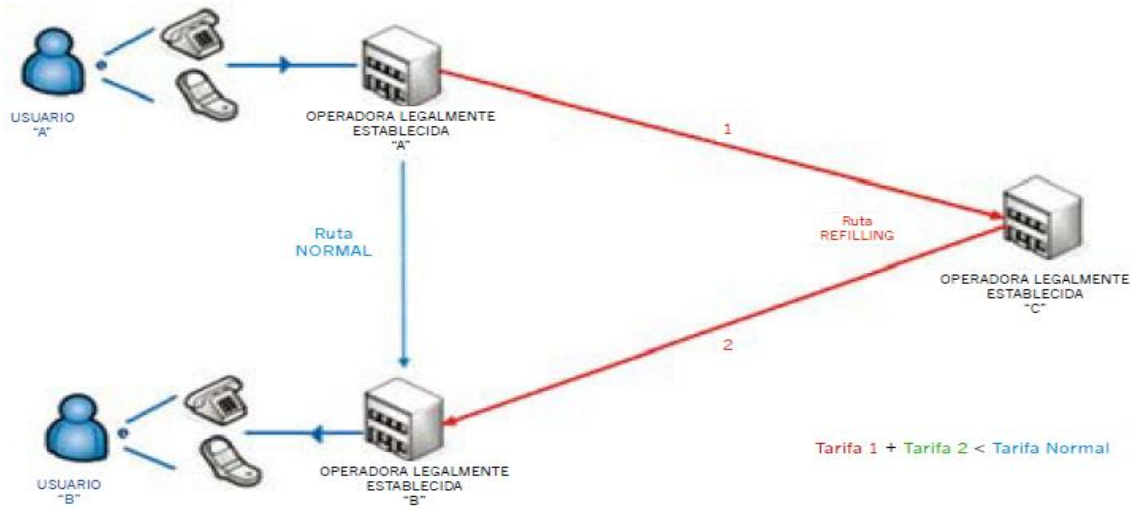
servicio en mención generando elevados consumos de servicio, los cuales tienen un costo elevado, antes de que el operador se percate de la situación y suspenda el servicio a las líneas implicadas. Se debe mencionar que el operador que brinda el servicio de Roaming se percata de la situación cuando recibe el reporte de consumo del defraudador enviado por el operador móvil del país extranjero donde este se encuentra, dependiendo del país extranjero estos reportes pueden ser enviados cada 4 horas pero en algunos casos este tiempo aumenta hasta 36 horas, lo anterior genera una gran cantidad de tiempo para que el defraudador haga provecho de este fraude hasta que sea detectado.

Con el fin de reducir las pérdidas producidas en Roaming Internacional la GSMA[6] ha establecido como norma a nivel global que todos los operadores móviles deben enviar el reporte de estos consumos cada 4 horas como máximo.

2.4.8. Refilling

Este fraude presenta una particularidad, es realizado por operadores legalmente establecidos con el fin de reducir los costos de tráfico internacional. El fraude consiste en enviar el tráfico saliente desde el país A con destino al país B mediante una ruta alterna la cual involucra a un país C. Esto se debe a que en algunos casos la interconexión entre países llega a ser demasiado costosa. La figura 9 ilustra el proceso de fraude Refilling.

Figura 9. Fraude Refilling



Fuente: Dirección General de Investigación Especial en Telecomunicaciones de Ecuador.

[6] Groupe Speciale Mobile Association

PARTE III

Desarrollo de un sistema de detección de fraude en tráfico de llamadas internacionales por Voz IP

Capítulo 3

3. Desarrollo del sistema de detección de fraude para tráfico por *By Pass*

En este capítulo se describen los elementos y procesos que conforman el sistema antifraude propuesto el cual busca que se automatice la detección de By Pass en la red de un operador móvil. Esta propuesta surge a partir de la necesidad de implementar nuevas medidas que aumenten la eficiencia actual en la detección de este tipo de fraude con el fin de conseguir la disminución de casos exitosos de fraude dentro de la red del operador, con lo cual se espera también la baja de pérdidas económicas por parte del mismo.

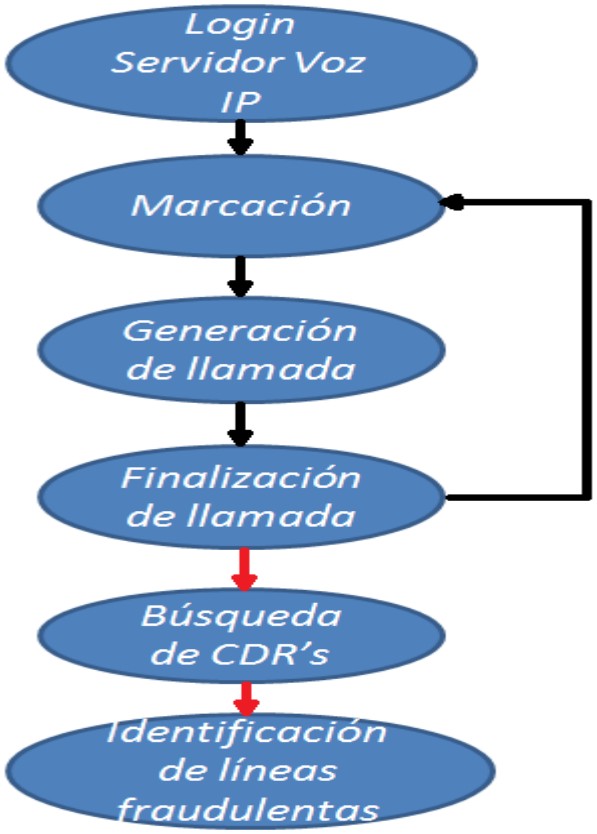
A partir del estudio acerca del funcionamiento de este tipo de fraude, sus características y formas de detección, estudio descrito en el marco teórico desarrollado en el capítulo 2, se generan ideas acerca de como mitigar en gran medida la necesidad ya mencionada existente por parte del operador, ideas que en conjunto con el análisis del funcionamiento del sistema actual el cual permitió evidenciar sus falencias y limitaciones, factores cuya existencia permite a quienes realizan el fraude By Pass continuar con sus actividades fraudulentas sin ser detectados por el operador, logrando de esta forma desarrollar un sistema de detección que brinda grandes ventajas en la detección de fraude By Pass frente al sistema actual de forma relativamente económica en comparación con las pérdidas económicas producidas por este fraude, perdidas que han sido estimadas en el planteamiento del problema del capítulo 1.

De esta forma se plantea una propuesta efectiva al operador móvil para la realización del proceso de detección de fraude, propuesta que se espera pueda ser implementada en un futuro cercano no solo dentro de este operador sino en otros operadores móviles debido a la vigencia de este tipo de fraude, con beneficios además del operador móvil para el estado quien recibe un porcentaje de las ganancias económicas de este, las cuales como ya se evidenció se reducen debido a los distintos tipos de fraude existentes en redes móviles.

3.1. Arquitectura y funcionamiento del sistema

El sistema de detección propuesto tiene el mismo principio de funcionamiento del proceso actual, por medio de la marcación a un teléfono determinado se generan registros de llamada que posteriormente son analizados para determinar aquellas líneas que están siendo utilizadas para fraude *By Pass*. El proceso de funcionamiento del sistema es ilustrado en la figura 10.

Figura 10. Proceso de detección *By Pass* para Voz IP



Fuente: Autor

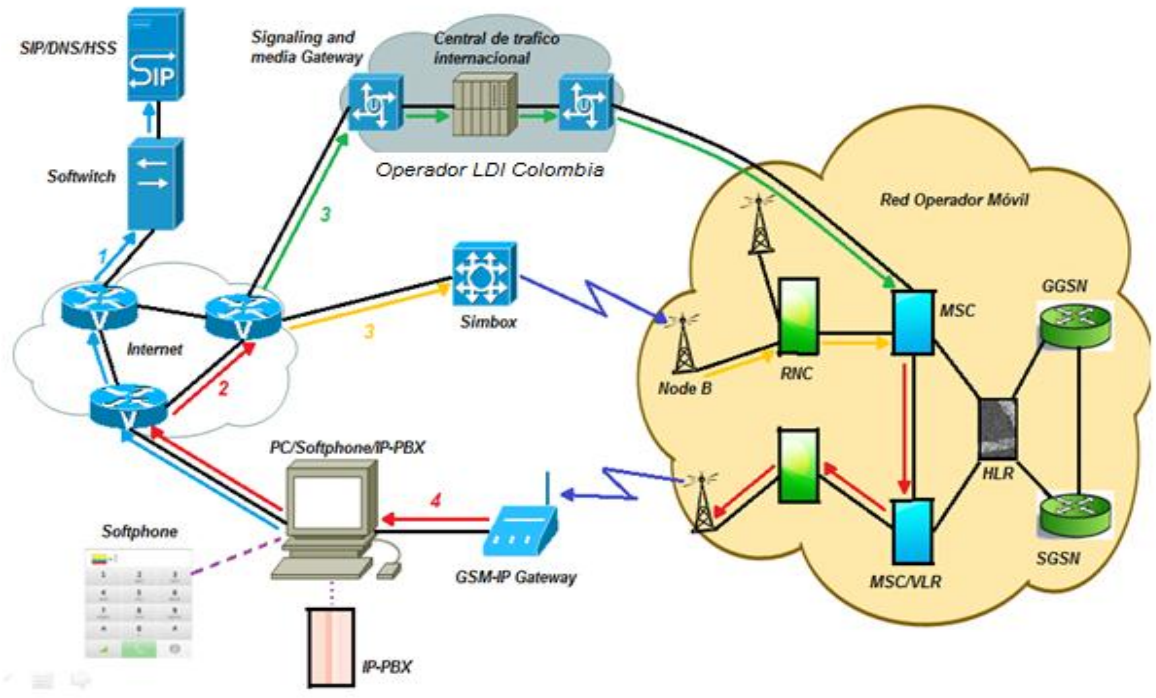
3.1.1. Arquitectura

El sistema desarrollado busca aumentar la eficiencia en la detección del fraude ya mencionado, para esto se debe reducir al mínimo la cantidad de trabajo en que se ve involucrado el encargado de las funciones de detección dentro del

proceso puesto que su incidencia en el desarrollo del mismo puede generar limitaciones en la capacidad de detección del sistema tal y como sucede con el sistema actual que como ya se mencionó únicamente funciona durante el corto periodo de tiempo en el cual el encargado del proceso está realizando la marcación, generación de llamadas y finalización de la misma, para los demás procesos como el de consulta de CDR's en el HLR, tarea que puede llegar a tomar hasta 30 minutos, e identificación de líneas fraudulentas e inclusive para todo el tiempo en que este no se encuentra en su jornada laboral, el proceso de detección se detiene en su totalidad.

La arquitectura planteada para este nuevo proceso reduce en gran medida la participación del encargado del proceso permitiendo a este trabajar en otras funciones y únicamente enfocarse en la búsqueda de los CDR's y generación de reportes de líneas fraudulentas cuando este lo desee, tareas que ahora serán más rápidas y sencillas, para las demás tareas no es necesario la supervisión de este, esto implica que el funcionamiento del sistema de detección abarca también las horas nocturnas y fines de semana, es decir, funciona en todo momento siempre y cuando se encuentren encendidos los elementos que conforman el sistema, ya que factores externos como una interrupción .eléctrica, un fallo de software u otros pueden alterar el correcto funcionamiento del sistema. La arquitectura planteada se ilustra en la figura 11.

Figura 11. Arquitectura del sistema propuesto



Fuente: Autor. Figuras: Cisco Systems Inc.

3.1.2. Funcionamiento

Los siguientes pasos describen de forma básica el funcionamiento del sistema propuesto y permiten conocer los dispositivos y programas que hacen parte del nuevo sistema anti fraude. En la sección 3.3. se menciona el funcionamiento de cada uno de los elementos que conforman el sistema y su contribución al proceso de detección.

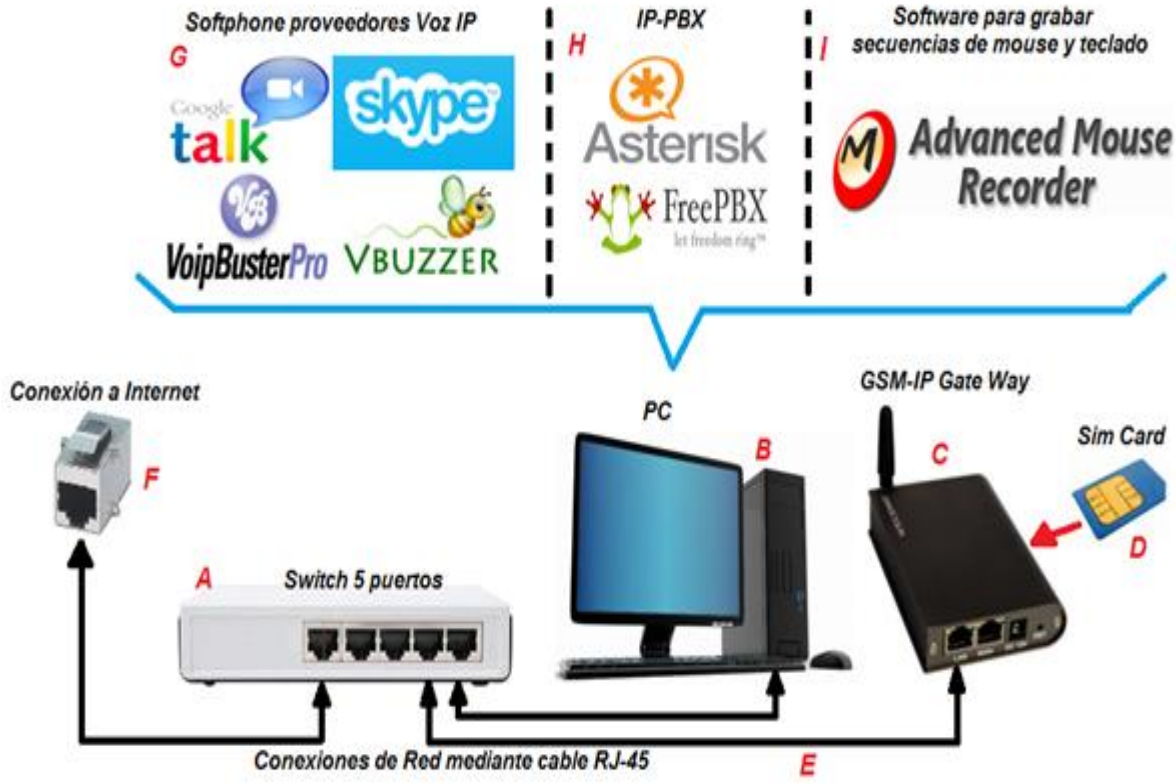
- Desde un PC con conexión a la red de internet se inicia sesión en el servidor de un proveedor Voz IP.
- Haciendo uso del Softphone que este proveedor ha desarrollado se hace una recarga de saldo para que se puedan generar llamadas.
- Se realiza la marcación a un número determinado, generando así una llamada Voz IP la cual tiene como destino la red de un operador móvil.
- El tráfico producido por esta llamada puede ser cursado haciendo uso de un operador de LDI en Colombia o de un sistema *By Pass.*
- El operador LDI o el sistema By Pass se encargan de entregar el tráfico a la red del operador móvil para que este finalmente lleve esta llamada hasta la línea de destino, en ambos casos la llamada se dirige a la línea predeterminada para el sistema de detección.
- Esta línea se encuentra asociada a una Sim Card que ya no se encontrará dentro de un terminal móvil como se hace en el sistema de detección actual, ahora estará instalada en un equipo que cumple las funciones de Media Gateway entre la red de telefonía móvil celular y una red IP.
- Gracias a este dispositivo el cual permite por medio de una conexión de red transmitir la información recibida por la Sim Card, debido a la llamada entrante, a un PC.
- En este PC en el cual mediante la instalación de un Software, que permite a este funcionar como un IP-PBX, se registra toda la información proveniente de la Sim Card, así todos los CDR´s generados por el proceso de marcación y generación de llamada no solo se encontrarán en el HLR del operador móvil, también estarán en el PC destinado al proceso de detección de fraude.
- Mediante la instalación y configuración de un Software que registra el movimiento y demás acciones del cursor, se mantiene la constante marcación, generación y finalización de llamadas desde el Softphone a la línea predeterminada.
- Se realiza la consulta de los registros, esta tarea se convierte en un proceso rápido y sencillo ya que no es necesario realizar una larga búsqueda de registros hasta encontrar los que son de interés.
- Se identifican aquellas líneas que han sido detectadas como fraudulentas para tomar medidas correctivas.

3.2. Dispositivos y programas del sistema

Todos los dispositivos y programas descritos a continuación cumplen una función específica dentro del proceso de detección de fraude *By Pass*, por tal motivo se explica su funcionamiento y en algunos casos se ha elaborado un manual en el cual se expone como se instalan y configuran estos elementos del sistema. Este manual se encuentra al final de este documento en la sección de anexos.

La arquitectura del sistema ya fue descrita pero no se ha hecho mención de todos y cada uno de los elementos que conforman el sistema propuesto, los cuales son tanto de Hardware como de Software, es por esto que en la figura 12 se muestra la interconexión entre cada uno de ellos.

Figura 12. Interconexión de los elementos del sistema



Fuente: Autor

3.2.1. Elementos de hardware

A. Switch

Este dispositivo cumple la función de interconectar los demás elementos de hardware del sistema, su función es de vital importancia ya que para poder interconectar tanto la red móvil como la red de internet al computador del sistema se debe realizar un arreglo que permita a este conectarse simultáneamente a más de un puerto de red lo cual es posible mediante un switch o mediante un adaptador IP-USB, para esta caso se ha elegido usar la primera opción.

B. PC

Este es el dispositivo principal del sistema, en el se encuentran todos los elementos de Software del sistema, desde este se generan las llamadas de Voz IP, se maneja el registro de las llamadas gracias a los CDR's almacenados en la base de datos SQL que se encuentra dentro de este y se realizan otras funciones por medio de los programas instalados en este. El sistema operativo para este PC es el de licencia gratuita Linux Ubuntu en cualquiera de sus versiones, esto se debe a que Asterisk & Free PBX, programas que permiten funcionar al PC como una IP-PBX, han sido desarrollados para funcionar sobre este SO, aunque en la actualidad ya se ha desarrollado para otros como Windows o MAC, y los dispositivos como el IP-GSM Gateway han sido desarrollados para funcionar como una extensión más de Asterisk lo cual implica que para el tema de configuración y correcto funcionamiento de todos estos dispositivos se cuenta con un mejor soporte del desarrollador y en internet si se trabajan en Linux.

C. GSM-IP Gateway

Este es un nombre genérico utilizado para todos aquellos dispositivos que permiten recibir y enviar trafico ya sea desde una red IP a una red de telefonía móvil celular o viceversa, su nombre no implica que su funcionamiento se encuentre limitado a la tecnología GSM y su tecnología de acceso al medio FDMA, en la actualidad estos dispositivos funcionar para otras tecnologías de acceso a la red como CDMA el cual es utilizado en redes UMTS o HSPA+. Este cuenta con uno o varios módulos que permiten insertar tarjetas Sim Card por tanto se puede tener más de una línea de telefonía móvil en el mismo dispositivo, la mayoría vienen con la antena para la transmisión y recepción de información ya integrada y pueden llegar a tener uno o varios puertos de Internet. Para el caso del sistema propuesto solo es necesario que este Gateway tenga módulo para una Sim Card, un puerto de Internet y la antena ya integrada tal y como se observa en la figura 12.

D. Sim Card

Esta tarjeta, la cual se ingresa en el GSM-IP Gateway, permite conectarse a la red de un determinado operador móvil por medio de cierta información contenida en su interior. Esta información permite saber a la red celular que la Sim Card pertenece a su operador y además que la línea sea distinguida de las demás líneas que se encuentran en la red, desde el punto de vista del usuario esta distinción se realiza mediante un número telefónico, en el caso del sistema propuesto es el número al cual siempre se dirigen las llamadas generadas desde los Softphone.

E. Cable de Red UTP con puerto RJ-45

Este cable se encarga de interconectar los puertos de red de distintos elementos de hardware. Para el sistema de detección propuesto no es necesario que se haga uso de un cable con características especiales en cuanto a velocidad de transmisión o inmunidad al ruido electromagnético por tanto se sugiere hacer uso de cable UTP categoría 5 el cual tiene un costo bajo y es el que se utiliza comúnmente en redes LAN.

F. Conexión a Internet

Por medio de esta conexión se puede hacer uso de los servicios que brindan los operadores de telefonía Voz IP, generación de llamadas IP a la red móvil por medio del inicio de sesión en sus servidores. Esta conexión también es importante para el proceso de instalación y configuración de los elementos de software del sistema anti fraude ya que todos estos deben ser descargados desde internet.

3.2.2. Elementos de software

G. Softphone proveedores de Voz IP

Gracias a estos se pueden generar las llamadas hacia la línea móvil predeterminada. Se aconseja hacer uso de Softphones que pertenezcan a varios operadores de telefonía Voz IP ya que cada uno de estos enruta su tráfico por diferentes caminos dentro de la red internet, distintos operadores de LDI, por tanto probablemente distintos CI por lo que en caso de que se haga uso de un sistema *By Pass*, esta práctica fraudulenta tenga más probabilidades de ser detectada. Así mismo se deben instalar Softphone de operadores de telefonía Voz IP sospechosos de ser ilegales y que tengan complicidad con sistemas *By Pass.*

H. IP-PBX

Este elemento de software se encuentra conformado por varios programas que cumplen una determinada función pero que en conjunto permiten al PC funcionar como una central de conmutación telefónica convencional sobre una red IP, programas como Asterisk que se encarga de la conmutación y señalización del trafico, Free PBX que se encarga de la administración de las funciones y servicios que brinda Asterisk, SQL el cual aporta la base de datos en la cual se aloja toda la información de planes de marcación, configuración de extensiones y almacenamiento de CDR's con la información de los sucesos acontecidos en la IP-PBX, y el Apache2 el cual es un servidor web que permite alojar la pagina de configuración de Free PBX para poder administrar el Asterisk a través de una interfaz sencilla sin necesidad de recurrir al terminal de Linux para realizar la configuración por medio de comandos y códigos.

Al hablar acerca de la instalación de una IP-PBX Asterisk es común pensar en utilizar la compilación de CentOS puesto que esta ya tiene configurada todos los paquetes, servicios y funciones ya mencionados. Pero para el caso del sistema de detección propuesto el cual busca ser eficiente en la detección y aprovechamiento máximo de los elementos que lo conforman, la opción de hacer uso de la compilación CentOS va en contra de la eficiencia que se busca conseguir, lo anterior se debe a que esta compilación inhabilita totalmente el PC para otras tareas ya que CentOS es en sí mismo un SO que funciona mediante comandos de consola o terminal y no permite la instalación ni ejecución de programas distintos al del IP-PBX lo cual implica que los Softphone, la configuración vía Web y demás elementos de Software del sistema deben ser instalados en un PC adicional por lo tanto se necesitaría de dos PC y no de uno para el sistema de detección. La solución a este problema se da mediante la instalación y configuración de todos los programas ya mencionados como necesarios para el correcto funcionamiento de la IP-PBX sobre el SO Linux, este proceso es mucho más complicado que haciendo uso del CentOS pero en la sección de Anexos se explica la forma correcta de realizar este procedimiento de instalación y configuración.

I. Software para grabar y reproducir secuencias de mouse y teclado

Este software tiene la función de reproducir determinadas secuencias del mouse y del teclado que permiten realizar la marcación, generación y finalización de la llamada desde los Softphone de forma completamente automatizada.

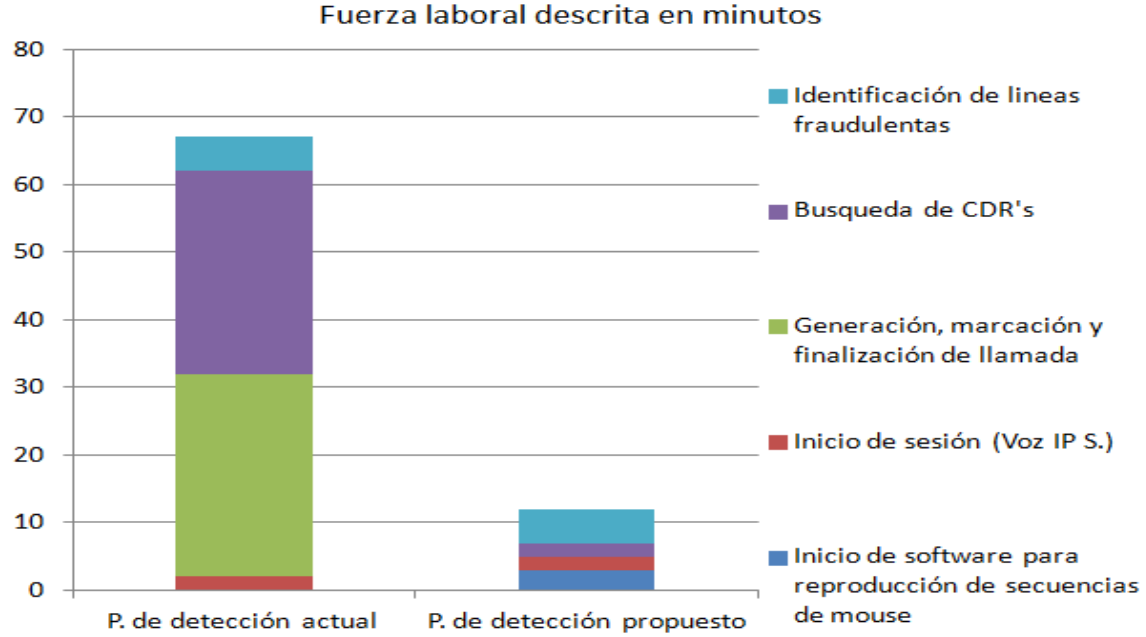
3.3. Mejoras en el funcionamiento

Las ventajas en el funcionamiento del sistema propuesto son expresadas en términos de fuerza laboral invertida diariamente y tiempo real de pruebas semanalmente en comparación con el proceso actual. Estas ventajas resaltan la mejoría únicamente términos de eficiencia en el funcionamiento del proceso de detección y no es términos de eficacia. Para ambos sistemas de detección la eficacia es la misma y es de un 100% ya que cuando una llamada es cursada por *By Pass* siempre y sin lugar a excepciones el número registrado es nacional, para el caso de una llamada cursada haciendo uso de un operador de LDI el número registrado es internacional sin lugar a excepciones.

3.3.1. Mejora en términos de fuerza laboral invertida

Por confidencialidad de la información no se revela la fuente de la siguiente información puesto que esto implica directamente al operador móvil en el cual se realizan estas prácticas y procedimientos de detección de fraude y por tanto donde se ha realizado este proyecto. La figura 13 muestra la fuerza laboral invertida en minutos para el desarrollo del proceso de detección de fraude.

Figura 13. Fuerza laboral invertida diariamente.



Fuente: Confidencial

En la anterior figura se observa que existe una disminución de la fuerza laboral invertida en el proceso de detección de un 80% aproximadamente. Esto se debe principalmente al tiempo que se invierte en la marcación, generación y finalización de las llamadas puesto que en el sistema propuesto estas tareas se realizan de forma automatizada y al tiempo invertido en la consulta de CDR's en base de datos, como ya se mencionó esto se debe a que en el sistema actual se debe realizar una extensa búsqueda en el HLR del operador, en el cual ocurre una gran cantidad de sucesos, mientras que en el sistema propuesto en la base de datos únicamente se encuentran los registros que son de interés para el proceso de detección. Respecto a la identificación de líneas fraudulentas y el inicio de sesión en el servidor de los proveedores de Voz IP el tiempo invertido es el mismo en ambos procesos ya que el proceso propuesto no brinda ninguna mejoría en la realización de estas tareas. Finalmente se debe adicionar un tiempo al proceso de detección propuesto el cual corresponde a la puesta en marcha del software que reproduce secuencias de mouse y teclado, este tiempo se ha estimado de 3 minutos.

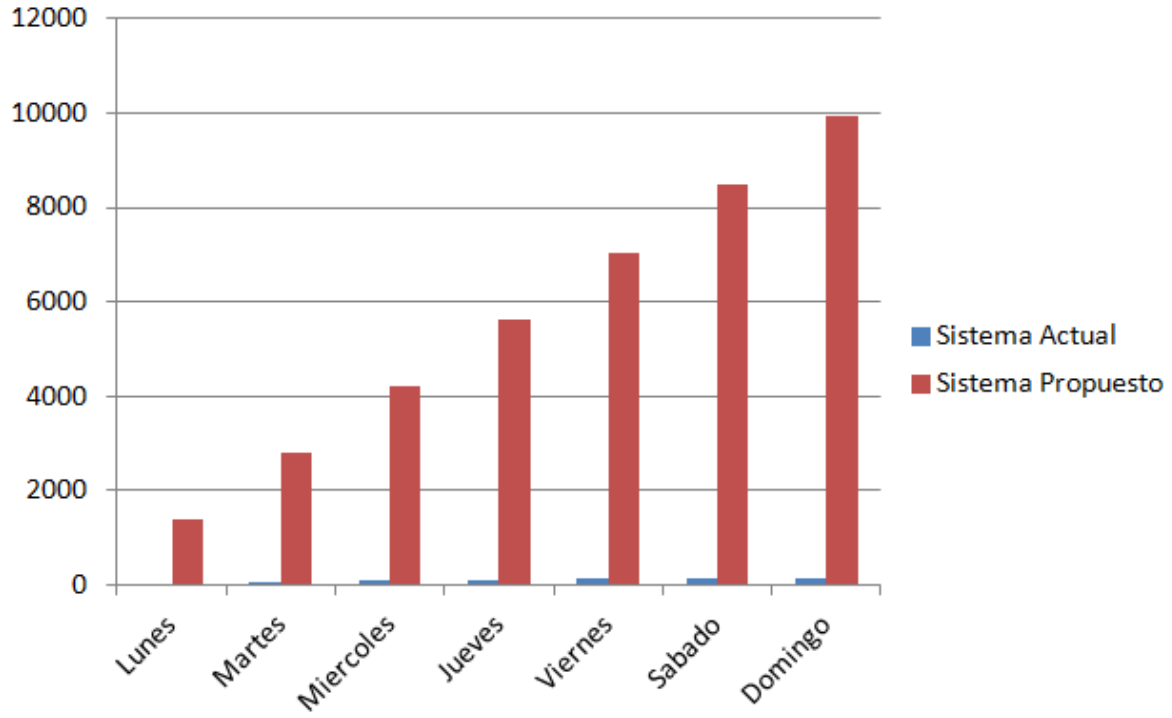
3.3.2. Mejora en términos de tiempo real de pruebas

Para el caso del tiempo real de pruebas en la detección de fraude *By Pass* en llamadas internacionales mediante Voz IP es necesario establecer como tiempo real de pruebas aquel tiempo en el cual se están realizando las tareas de marcación, generación y finalización de las llamadas puesto que es en el resultado de estas 3 tareas es que quedan registradas en la base datos aquellas líneas fraudulentas. Cuando el encargado del proceso se encuentra realizando la búsqueda de CDR's o la identificación de líneas fraudulentas se detiene en la totalidad la posibilidad de detectar nuevas líneas fraudulentas ya que no se está cursando tráfico internacional.

A partir de la información planteada en la figura 13 se entiende que el tiempo real de pruebas es de 30 minutos diarios aproximadamente, y que además al ser esta una tarea manual, esta es realizada únicamente en aquellos días que el encargado de realizar el proceso de detección se encuentra laborando en el operador, por tal motivo el tiempo real de pruebas es de 30 minutos multiplicados por 5 que es el número de días que este asiste al trabajo para un total de 150 minutos semanales. Para el caso del sistema de detección propuesto el tiempo real de funcionamiento es todo aquel en el cual no se están realizando ninguna de las otras actividades del proceso como la ejecución del software que reproduce las secuencias del mouse y teclado, búsqueda de CDR's e identificación de líneas fraudulentas. Dado que el sistema es completamente autónomo durante el proceso de marcación, generación y finalización de llamadas, estas tareas se repiten durante todo el día o tiempo que se establezca para que se realicen las demás tareas del proceso, la repetición de estas tareas también se da durante el fin de semana completo las 24 horas del día, lo anterior en el caso ideal en el cual

ningún factor externo afecta el correcto funcionamiento del sistema. La figura 14 muestra la cantidad de minutos reales de pruebas acumuladas durante una semana. En esta imagen se observa que diariamente la cantidad de minutos reales de pruebas es aproximadamente 47 veces mayor con el sistema de detección propuesto con respecto al sistema de detección actual entre semana, esta diferencia se acumula para establecer un total semanal el cual es aproximadamente 66.2 veces superior ya que en los fines de semana el sistema actual se detiene en su totalidad mientras el sistema propuesto funciona las 24 horas del día acentuando la diferencia entre ambos sistemas.

Figura 14. Tiempo real de pruebas acumulado en minutos semanalmente



Fuente: Confidencial

Es importante aclarar que aunque el tiempo real de pruebas sea muy superior por medio del sistema de detección propuesto esto no implica que la relación de líneas fraudulentas detectadas sea igual, lo más probable es que la cantidad de líneas detectadas aumente en gran medida, especialmente en horas de la noche y fines de semana pero no en una relación tan elevada.

3.4. Comparación entre los sistemas

Mediante la tabla 3 se realiza un comparativo entre el sistema de detección actual y el sistema de detección propuesto, esta comparación no solo abarca temas de funcionamiento los cuales ya fueron tratados en la sección 3.3, en este caso también se comparan temas de escalabilidad y flexibilidad del sistema, además permite evidenciar las ventajas y desventajas que brinda cada sistema.

Tabla 3. Comparación entre los sistemas

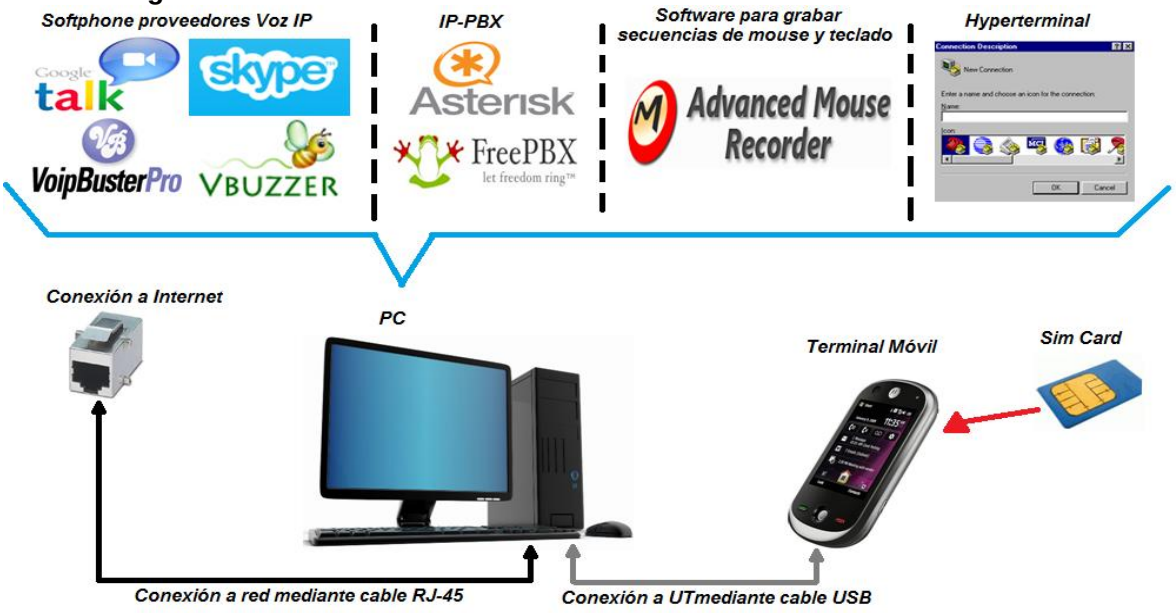
	Sistema actual	***Sistema propuesto***
Requiere constante supervisión	SI	NO
Generación de trafico automatizado	NO	SI
Tiempo real de funcionamiento diario	30 minutos (aprox.)	1410 minutos (aprox.)
Fuerza laboral invertida diariamente	68 minutos (aprox.)	12 minutos (aprox.)
Funcionamiento en fines de semana y horas nocturnas	NO	SI
Permite agregar líneas al sistema	SI	SI
Requiere de nuevos dispositivos para agregar líneas (excepto Sim Card)	SI	NO, hasta 16 líneas
Requiere filtrado de CDR's	SI	NO
Aumento de fuerza laboral en caso de aumentar el número de líneas	SI	NO
Generación de reporte automático	NO	SI
Aplicable a redes de telefonía fija	SI	SI
Eficacia	100%	100%
Requiere de configuración del sistema para agregar nuevas líneas	NO	SI
Capacidad para utilizar líneas de forma simultanea	NO	NO

Fuente: Autor

3.5. Variación del sistema propuesto

Frente al sistema de detección propuesto se ha planteado una variación al mismo que aunque no altera el principio fundamental de su funcionamiento si tiene una ligera diferencia en algunos de los elementos tanto de software como de hardware que lo conforman. Esto se debe principalmente al equipo que permite conectar el PC a la red de operador móvil. Para esta variación se propone recibir el tráfico generado desde los Softphone a una línea móvil que, al igual que en el sistema actual, se encuentra en un terminal móvil y no en un GSM-IP Gateway. Cuando el trafico es recibido por la Sim Card la información del caller ya no se envía a la base de datos de la IP-PBX configurada en el PC mediante un puerto de internet, ahora la información es enviada y almacenada en la base de datos mediante el establecimiento de una comunicación entre el terminal móvil y el PC haciendo uso de un puerto USB gracias a un determinado conjunto de comandos los cuales se encargan de enviar instrucciones al terminal para que este informe ciertos datos al PC, en este caso se necesitan los datos del número que ha generado la llamada hacia la línea, los comandos que permiten esta comunicación son los AT o comandos de Hayes los cuales según Hernández, Jiménez, Medina y Montero (Noviembre, 2009) son: "*Instrucciones codificadas que conforman un lenguaje de comunicación entre el hombre y un terminal modem*" (Pág. 18), siendo estos controlados desde la herramienta Hyperterminal.

Figura 15. Variación en la interconexión de los elementos del sistema.



Fuente: Autor

Debido a que ya no existe la necesidad de utilizar dos interfaces de red como si ocurre en el caso del sistema propuesto, no se hace necesaria la utilización del switch planteado ni del GSM-IP Gateway, quedando la interconexión de los elementos del sistema alterada. Esta nueva interconexión se ilustra en la figura 15.

Es esta variación del sistema una propuesta más económica debido a que el costo de un terminal móvil que permita funcionar de la forma ya descrita puede tener un costo de COP$150.000, valor inferior al del GSM-IP Gateway y el switch 5 puertos juntos. El inconveniente principal que se observa para esta propuesta es que en caso de decidir aumentar el número de líneas con las que cuenta el sistema la única variación a realizar en el sistema propuesto solo se necesita que el GSM-IP Gateway cuente con mas módulos para la inserción de Sim Card’s pero se seguirá necesitando únicamente una interfaz de red, mientras que para esta variación del sistema si se desean instalar mas líneas al sistema se deben adquirir más terminales móviles y por consiguiente se hace necesario el uso de mas puertos USB, lo cual implica la compra de un multi puerto USB ya que la cantidad de estos puertos en el PC es bastante limitada.

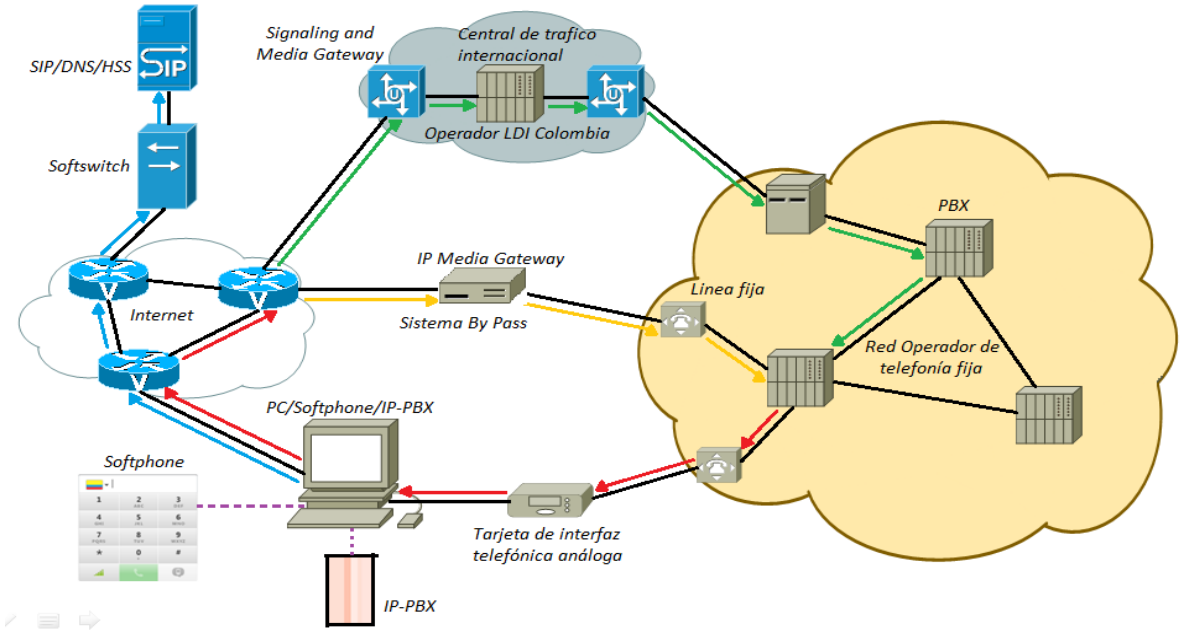
3.6. Aplicación del sistema en redes de telefonía fija

El sistema planteado puede ser aplicado tanto a redes de telefonía móvil celular como a redes de telefonía fija tradicional, por tal motivo se ha decidido explicar de forma resumida la aplicación de este sistema a dichas redes partiendo del entendimiento acerca del funcionamiento de los sistemas *By Pass* y del sistema propuesto.

Para el caso de los sistemas *By Pass* sobre redes de telefonía fija tradicional, estos hacen uso de IP Media Gateway, equipo que se encarga de conmutar el tráfico proveniente desde una red IP hacia una red tradicional de conmutación de circuitos, cumpliendo la misma función de un Simbox en redes móviles. En estos sistemas se hace uso de líneas de telefonía fija, por tal motivo no es muy común la utilización de estos sistemas ya que la ubicación de una línea fija es fácil de realizar ya que al momento de la instalación ya es de conocimiento de la empresa prestadora del servicio la dirección del inmueble donde esta es instalada, caso que no sucede con el uso de Sim Card's.

La arquitectura del sistema propuesto aplicado a redes de telefonía fija se encuentra en la figura 16.

Figura 16. Sistema de detección aplicado a una red de telefonía fija.



Fuente: Autor. Figuras: Cisco Systems Inc.

En estos sistemas la detección del fraude se evidencia debido a que el número que proviene desde el exterior hace uso de un Carrier conocido, el cual tiene su propio número de identificación, con el cual tiene convenio el operador fijo mientras que aquellas llamadas cursadas mediante un sistemas *By Pass* tienen asociados un número de identificación diferente al de los Carriers ya conocidos.

Respecto a los equipos que se deben utilizar para la correcta aplicación de este sistema de detección a una red de telefonía fija la única variación importante es el equipo que se encarga de interconectar el sistema con dicha red y la línea que se debe usar. Lo anterior se consigue mediante una línea fija, la misma que se usa para conectar un teléfono tradicional, a esta se debe conectar una tarjeta de interfaz telefónica análoga y a su vez este debe ser conectado al switch de 5 puertos, de manera idéntica como se ilustra en la figura 12 con las respectivas variaciones ya mencionadas.

PARTE IV

Conclusiones

Capítulo 4

4. Conclusiones de la monografía

Mediante este ultimo capitulo se da a conocer las conclusiones obtenidas gracias al desarrollo de este proyecto y la metodología utilizada para este, relacionando las tareas de evaluación del proceso actual, identificación de las oportunidades de mejora y análisis de las alternativas existentes para mejorar el proceso dando cumplimiento a los objetivos planteados para este proyecto y brindando al operador móvil una alternativa para la mitigación de una problemática que se presenta dentro de su red.

4.1. Conclusiones en el desarrollo

La implementación de sistemas anti fraude no debe tener como única finalidad la prevención, detección y corrección de actividades indebidas sobre las redes y servicios de un operador móvil, estas también deben buscar la manera de desalentar a los defraudadores a cometer reiteradamente estas conductas.

Cualquier solución tecnológica existente ante algún tipo de fraude nunca puede considerarse como 100% exitosa en la consecución del objetivo para el cual fue diseñada ni la solución definitiva a los problemas que el fraude conlleva, constantemente se idearán formas de vulnerarla o evitarla por medio de nuevas técnicas y tipos de fraude, razón por la cual se debe mantener un continuo mejoramiento de estos sistemas para mantener los efectos negativos del fraude en un nivel tolerable para el operador.

El sistema de detección propuesto tiene una cantidad de horas de funcionamiento hasta 65 veces superior al del sistema actual por tanto el número de pruebas que se realizan aumenta en una relación similar, lo anterior implica que la cantidad de líneas fraudulentas detectadas también aumenta aunque no se puede determinar en que porcentaje, en todo caso con un aumento del 2.5% de líneas detectadas en un solo mes el operador móvil habrá recuperado la inversión realizada en la implementación del sistema propuesto en caso de decidir su implementación, esto indica que la propuesta planteada no solo es eficiente sino que además es económica y significa una pequeña cantidad de dinero con respecto al total monetario que ahorrará el operador móvil gracias a esta propuesta.

Se han detectado limitación y falencias en el proceso de detección actual, factores que han mermado con el paso del tiempo la eficiencia del sistema lo cual ha permitido que exista una cantidad de recursos económicos perdidos por el operador bastante elevada, siendo esta la razón principal por la cual el operador móvil ha decidido implementar dos nuevos sistemas de detección de fraude *By Pass*, uno para llamadas mediante Voz IP y otro mediante telefonía móvil tradicional.

4.2. Conclusiones humanísticas

En toda actividad que el hombre realiza este siempre intenta ir mas allá, inventar e intentar algo nuevo, llegar más lejos de lo que alguien ha llegado, siempre impulsado por su curiosidad y fuerte deseo de entender lo desconocido y dar respuesta a todas las preguntas que este se plantea, lo anterior ha permitido a la sociedad en que este se desenvuelve desarrollarse constantemente. Pero este no es el único deseo del hombre, el tener más poder, dinero o cosas que los demás ha llevado a que en algunos casos este se corrompa causando perjuicios a los demás, para el caso del tema tratado en este proyecto, habiéndose convertido en el arma mas poderosa para zacear su ambición el fraude.

Entendiendo que las personas que realizan el tipo de fraude *By Pass* tienen un alto grado de conocimiento en el área de las comunicaciones, especialmente de redes tanto IP como móviles y también de algunos de los servicios que estás brindan, por tanto probablemente sean personas con educación universitaria, existe un problema de formación ética y humanística en estos profesionales proveniente desde las entidades universitarias y de educación superior quienes no inculcan valores en los futuros profesionales para aportar con su conocimiento al desarrollo social.

Referencias electrónicas

- ***Tribulinux.*** Como instalar Asterisk 10 en Ubuntu 12.04 (s/f). Tomado de <http://www.tribulinux.com/como-instalar-asterisk-10-en-ubuntu-12-04.html>

- ***Peves Alberto, (2011, 9 de Enero*).** Manipulando un celular vía comandos AT. Tomado de <http://www.vidainformatico.com/2011/01/manipulando-un-celular-via-comandos-at.html>

- ***Bluehack.*** Comandos AT (s/f). Tomado de <http://bluehack.elhacker.net/proyectos/comandosat/comandosat.html>

- ***Instalación de Asterisk*.** Freepbx en Ubuntu server 11.04 (s/f). Tomado de <http://www.taringa.net/posts/linux/12153191/Instalacion-de-Asterisk_-Freepbx--en-ubuntu-server-11_04.html>

- ***Gonzalez Pineda Cesar, (2009).*** Telefonía IP Asterisk. Tomado de <http://www.slideshare.net/ces1227/manual-de-instalacion-de-asterisk>

- ***Ares Roberto. (s/f).*** Telefonía-IP. Tomado de <http://www.monografias.com/trabajos16/telefonia-senalizacion/telefonia-senalizacion.shtml>

- ***Sistemas By Pass en el Ecuador. (s/f).*** Tomado de <http://es.scribd.com/doc/56090204/2/SERVICIOS-DE-LLAMADAS-INTERNACIONALES-Y-EL-By-Pass>

- ***Glosario utilizado en el documento.*** Tomado de <http://www.mintic.gov.co/index.php/glosario>, <http://www.gsmspain.com/glosario> y <http://www.telefoniavozip.com/glosario-voip/h/h.htm>

- ***Ministerio de transporte y comunicaciones del Perú***. Servicios portadores. Tomado de: <http://www.mtc.gob.pe/portal/comunicacion/concesion/publicos/portador.htm>

- ***Cárdenas Espinosa Rubén Darío (2010, 9 de Septiembre)*** Explicación normas APA para trabajos escritos. Tomado de <http://www.slideshare.net/rdcardenas75/explicacion-normas-apa-para-trabajos-escritos>

Lista de citas

[i] ***UNE***, sala de prensa. Recuperado el 18 de Septiembre de 2012 de: <http://saladeprensa.une.com.co/index.php?option=com_content&view=article&id=340%3Aune-gana-demanda-contra-competidor-desleal-de-telefonia-larga-distancia&Itemid=166>

[ii] ***Senado de la Republica de Colombia***, secretaría. Recuperado el 19 de Septiembre de 2012 de: <http://www.secretariasenado.gov.co/senado/basedoc/ley/1996/ley_0256_1996.html>

[iii] ***Comes Agustí Ramón. (2010, 22 de Junio)*** Las comunicaciones móviles como motor de progreso. Recuperado el 19 de Septiembre de 2012 de: <http://www.real-academia-de-ingenieria.org/docs/2011/01/10/18260001_4_8_0.pdf>

[iv] ***Real Academia española***. <http://www.rae.es/rae.html>

[v] ***Colombia Móvil S.A E.S.P***. Planes y paquetigos, Internacional. Recuperado el 4 de Octubre de 2012 de: <http://www.tigo.com.co/personas/planes>

[vi] ***Lista de proveedores Voz IP***. Recuperado el 4 de Octubre de 2012 de <http://www.voipproviderslist.com/>