ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE INGENIERÍA

ESTUDIO DEL FRAUDE TECNOLÓGICO EN EL SISTEMA DE TELEFONÍA MÓVIL CELULAR

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

ESTUARDO BLADIMIR VACA GUAICHA

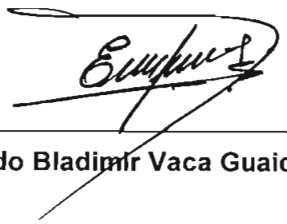
DIRECTOR: ING. HUGO CARRIÓN ROBALINO

QUITO, OCTUBRE, 2000

DECLARACIÓN

Yo Estuardo Bladimir Vaca Guaicha, declaro que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

La Escuela Politécnica Nacional, puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la Ley, Reglamento de Propiedad Intelectual y por la normatividad institucional vigente.



Estuardo Bladimir Vaca Guaicha

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Estuardo Bladimir Vaca Guaicha, bajo mi supervisión.

Ing. Hugo Carrión Robalino
DIRECTOR DE TESIS

AGRADECIMIENTOS

Quiero dejar constancia el reconocimiento a mis padres y hermanos, quienes han colaborado enormemente en la elaboración del presente trabajo, y especial gratitud a Guadalupe por su apoyo incondicional.

DEDICATORIA

A mis padres, hermanos y amigos; quienes me apoyaron con abnegación y constancia para el feliz término del presente trabajo.

PRÓLOGO

En la realización de la presente tesis sobre el tema: *Estudio del Fraude Tecnológico en el Sistema de Telefonía Móvil Celular,* el estudiante se ha propuesto analizar los principales parámetros que influyen en la formación del fraude, sus tipos; medidas de prevención y técnicas de detección, así como también las dificultades que se tiene en el control del mismo.

El desarrollo del tema se fundamenta en un análisis de ideas y conceptos de los problemas de fraude que presentan las operadoras celulares de todo el mundo, básicamente extractadas de fuentes legales, especialmente de *BellSouth*, *PortaCelular*, *Ericsson*, Internet y otros. Sobre esta base se estructuran todos los elementos de juicio del tema propuesto para presentarlo como un todo orgánico y articulado; tomando en cuenta que por propia seguridad de las operadoras celulares, la información es muy confidencial.

Para su lógica ejecución y fácil comprensión, el presente trabajo pone a consideración las siguientes partes esenciales: inicia con un *estudio* básico del sistema de telefonía móvil celular; sigue luego con un *bosquejo del fraude tecnológico* en el sistema móvil celular, continúa con un *análisis descriptivo* de los servicios de detección/prevención del fraude, nuevas tecnologías para combatir los futuros desarrollos en fraudes y *concluye* con un *análisis* de los distintos factores de la administración de fraude que hay que considerar para la aplicación de una solución antifraude en particular.

La tarea realizada por el Sr. Estuardo Vaca Guaicha responde al interés, seriedad y dedicación requeridas para la elaboración de un proyecto de titulación, acentuando también el agradecimiento que se les da a las empresas antes mencionadas por colaborar con la ayuda intelectual y material para la elaboración de dicho trabajo.

Es de esperar que el presente proyecto de titulación sea enfocado para los profesores y estudiantes en la rama de Telecomunicaciones.

Quito, 6 de octubre del 2000

CONTENIDO

PRESENTACIÓN

Cuando un operador introduce por primera vez la telefonía celular en una zona, su objetivo primario es organizar capacidad y cobertura, y reclutar clientes. Sin embargo, al madurar sus redes y al aumentar la competencia, los financiadores esperan una ganancia razonable sobre sus inversiones; no pueden tolerarse por ejemplo pérdidas no recuperables como resultado del fraude.

Es posible que en algunos países las pérdidas representen el 20 % de la facturación mensual, por ejemplo, en los Estados Unidos el perjuicio contabilizado en 1997 sobrepasó los dos billones de dólares y en todo el mundo un estimativo indica que los fraudes puedan ocasionar pérdidas de hasta 4 billones de dólares. Y aún más, estas cifras no tienen los costes indirectos del fraude, el coste del equipo antifraude, y el impacto negativo que el fraude ejerce sobre el uso y sobre el aumento de abonados cuando éstos se sienten incomodados.

Capítulo 1. Se estudia la arquitectura del Sistema de Telefonía Móvil Celular, con el propósito de revisar básicamente los principales elementos que pueden ser afectados por el fraude.

Capítulo 2. El análisis comienza con la categorización del fraude en el sistema celular: principales tipos de fraude que atacan a las operadoras celulares, su tendencia y crecimiento; para continuar con los esquemas más comunes para detectar o prevenir este problema; para terminar se realiza una breve descripción de los servicios antifraude.

Capítulo 3. Descripción completa de los servicios de detección/prevención del fraude, diferentes métodos, técnicas de detección y herramientas preventivas para combatirlo; desde los sistemas más básicos hasta los más complejos, que están siendo utilizados actualmente.

Capítulo 4. Las nuevas tendencias tecnológicas para combatir los futuros desarrollos en fraude: biométrica en las huellas digitales de los suscriptores, mejoras CDMA para la aplicación de sistemas de tercera generación y un vistazo a los sistemas de comunicación personal y global para comunicaciones móviles.

Capítulo 5. La administración de fraude en la aplicación de las principales soluciones antifraude combinada con los mejoramientos tecnológicos, avanzados teléfonos digitales, crecimiento de las defensas contra el fraude y su co-relación con los otros departamentos de la operadora celular, permitirá reducir las pérdidas de ingresos, mejoramiento del servicio celular y cortará las actividades criminales junto con el uso ilegal de los teléfonos.

CAPÍTULO I

SISTEMA DE TELEFONÍA MÓVIL CELULAR

1.1 ARQUITECTURA DEL SISTEMA CELULAR

Los Laboratorios *Bell AT&T, Murray Hill, N.J.*, propusieron el concepto celular bajo la arquitectura del Sistema de Telefonía Móvil Avanzado (*AMPS: Advanced Mobile Phone System*) en 1971.

El concepto celular añade una dimensión espacial al modelo troncalizado básico. El bajo perfil, los sitios de celda de baja potencia fueron enlazados a través de una central de conmutación y funciones de control. Reduciendo cada área de celda de cobertura se invitaba a la reutilización de frecuencias. Las celdas usando el mismo conjunto de canales de radio podrían evitar interferencia mutua si ellas estuvieren separadas la suficiente distancia. La interferencia entre las celdas es proporcional no a la distancia entre ellas, pero sí a la relación de esa distancia a sus radios. Por esta razón los diseñadores tienen la libertad en determinar el número de canales de radio disponibles para los suscriptores. Más canales de radio pueden ser agregados a un sistema, simplemente reduciendo la potencia de transmisión por celda, haciendo las celdas más pequeñas, y llenando las áreas de coberturas desocupadas con nuevas celdas.

Los sistemas celulares empezaron a aparecer repentinamente sobre todo el mundo en los inicios de los 80's, sobre un conjunto de esquemas de señalización incompatibles desplegados en diferentes bandas de frecuencias.

Cada una de ellos era una variación del modelo AMPS que apareció en el hemisferio occidental, Australia y partes de Asia. Algunos de los sistemas FM fueron NMT-450 y NMT-900 en Escandinavia, Europa oriental y partes de Asia; C-Netz en Alemania, Portugal y Sud-Africa; RMTS en Italia; RC-2000 en Francia; TACS en el Reino Unido; y los sistemas MCSL1 y JTACS en Japón.

1.1.1 DEFINICIÓN DE CELDA

El Sistema de Telefonía Móvil Celular utiliza un número considerable de transmisores de baja potencia para crear celdas, que son las áreas geográficas básicas de estos sistemas de comunicaciones inalámbricas y desde las cuales se pueden efectuar llamadas, usando un único canal de radio. Las variaciones de los niveles de potencia permiten manejar el tamaño de las celdas de acuerdo con la densidad de abonados y la demanda en una región en particular.

Como los usuarios móviles se desplazan entre varias celdas, sus conversaciones son transferidas entre las celdas a fin de mantener un servicio continuo. Los canales (frecuencias) usadas en una celda pueden ser reutilizadas en otra celda que esté ubicada una cierta distancia de la primera. Cada celda tiene una estación base que consiste de una torre y una pequeña edificación que contiene el equipo de radio.

El área de cobertura ideal de una estación base sobre terreno plano puede llegar a ser circular. En la práctica el terreno provoca que las áreas de cobertura sean irregulares. Para realizar la división de un área geográfica de acuerdo a la cobertura, es posible representarlo en una forma hexagonal, la cual es una idealización que supone lo siguiente:

- Todos los sitios tienen el mismo sistema de antena.
- El terreno es plano.
- Todas las alturas de las antenas son idénticas.

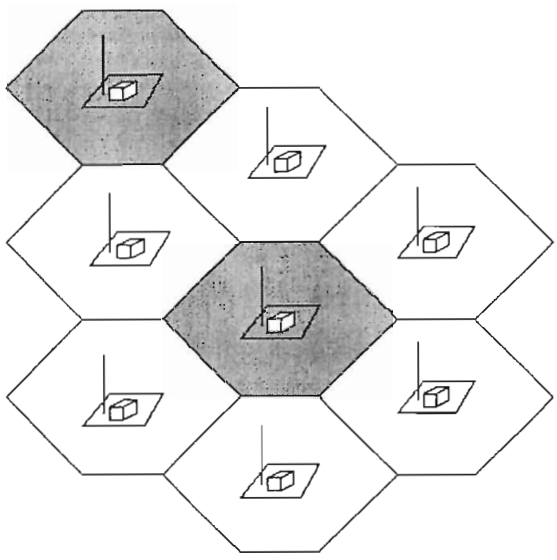


Figura 1.1 Representación hexagonal de las celdas y sus respectivas estaciones base

El sistema está diseñado para suministrar el servicio usando un plan de cobertura de radio celular. Este plan divide un área metropolitana en un número de áreas de cobertura o celdas, en las cuales se asigna una cierta cantidad de canales de radio disponibles.

El tamaño de las celdas depende de las características de tráfico que demande el área de cobertura. Grandes capacidades son requeridas en zonas urbanas o comerciales y en otros sitios de alto tráfico (ej. Autopistas con gran tráfico), por lo cual pequeñas celdas son implementadas en estas áreas. En los casos en los cuales la estación base está localizada en la parte central dentro de una celda y utiliza antenas omnidireccionales, estas celdas son conocidas como omnidireccionales.

Es posible implementar un número de celdas desde un solo sitio mediante el uso de antenas direccionales. Típicamente las antenas utilizadas para dar cobertura a los sectores tienen una apertura de 120°, 90°, o 60°, dando como resultado 3, 4 o 6 sectores respectivamente. Esto se muestra a continuación:

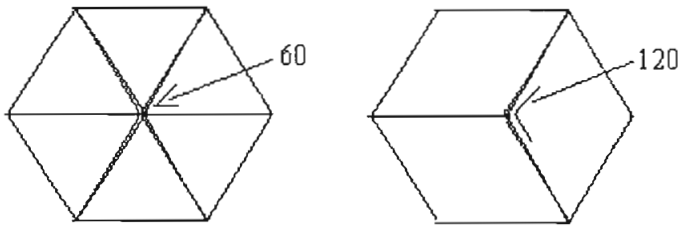


Figura 1.2 Celdas sectorizadas para una apertura de 60° y 120° respectivamente

A este tipo de celdas se las denomina celdas sectorizadas o sectoriales.

La cobertura de las celdas puede ser reducida mediante los siguientes procedimientos:

- Reduciendo la potencia de transmisión.
- Reduciendo la posición de altura de las antenas.
- Utilizando un ángulo de elevación negativo en antenas direccionales o sectorizadas.

1.1.2 REUTILIZACIÓN DE FRECUENCIAS

La cantidad de espectro disponible para los sistemas móviles es muy limitado, por lo que los sistemas de telefonía celular deben usar el espectro asignado en forma eficiente, que permita proveer un adecuado servicio para un gran número de usuarios.

El uso eficiente de las frecuencias disponibles es posible realizarlo mediante una sistemática reutilización de los canales. Un ejemplo se muestra en la figura siguiente. El identificativo mostrado en cada celda representa un conjunto de canales usados dentro de cada una de las celdas.

En los modelos en los cuales este patrón se repite regularmente, en particular el caso mostrado en la figura 1.3, el proceso puede ser descrito como un "Patrón de repetición de 7 celdas" o que se tiene un "tamaño de grupo" (*cluster size*) de 7, los patrones de reutilización de frecuencias más utilizados son de 3, 4 y 7. Debe notarse que debe existir una separación coherente entre celdas que utilizan un conjunto de canales determinados. Esta separación es conocida como la distancia de reutilización de frecuencias.

Patrones de reutilización de frecuencias con un gran tamaño de agrupación tienen a su vez una mayor distancia de reutilización y por supuesto menores niveles de interferencia. Sin embargo estos tienen un número pequeño de canales disponibles en cada celda, por lo que debe existir una correlación entre niveles de interferencia y el número de canales disponibles en cada celda.

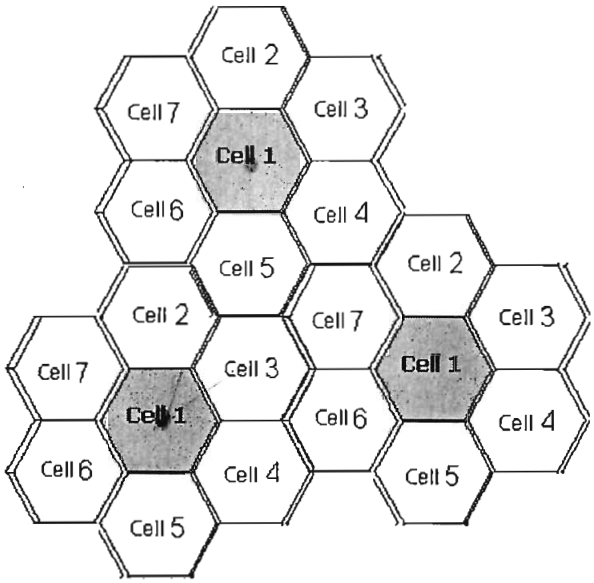


Figura 1.3 Patrón de repetición de 7 celdas (cluster size)

En áreas rurales donde el tráfico es menor, la cobertura está determinada por el transmisor y la sensibilidad del receptor (el cual está determinado por el ruido térmico que se introduce). Entonces se dice que el sistema está limitado por el ruido. En áreas urbanas las celdas son pequeñas y su tráfico es alto.

La cobertura tiende a ser determinada por la interferencia cocanal, y el sistema se dice que está limitado por interferencia. Si la distancia de reutilización de frecuencias es suficiente, el nivel de la interferencia cocanal será menor. Las señales interferentes dan como resultado ciertas relaciones de portadora a interferencia dentro del área de cobertura requerida. A modo de ejemplo los niveles de C/I típicos, que son requeridos por los sistemas móviles celulares a fin de dar un funcionamiento satisfactorio a los usuarios, son los siguientes:

- AMPS/TACS 18dB (correspondiente a una S/N del canal = 38dB).
- GSM 10dB.

Se ha determinado que el efecto de las señales interferentes está asociado con una distribución de desvanecimiento de Rayleigh (desvanecimiento de trayectoria múltiple), en la que por efecto de clima y de frecuencia, las ondas pueden refractarse en las capas atmosféricas más bajas y tardar un poco más en llegar que las ondas directas. Las ondas diferidas pueden llegar fuera de fase con la onda directa y cancelar así la señal. La relación portadora a interferencia (C/I) tendrá entonces una distribución de Rayleigh, desvanecimientos de señal más profundos son menos frecuentes que los desvanecimientos menos profundos. Es usual en los diseños de los sistemas móviles celulares conseguir una C/I determinada, sobre el 90% de la zona de cobertura planeada.

En la figura 1.4, está considerando el caso del receptor del sector A, el caso más crítico de interferencia puede provocarse debido a un móvil en la celda más cercana que utilice la misma frecuencia, posicionado cerca de la estación base de las celdas, para este caso en la posición M. La distancia entre el móvil y la estación base de la celda es D, es decir la separación de los sitios de celda (*cell sites*).

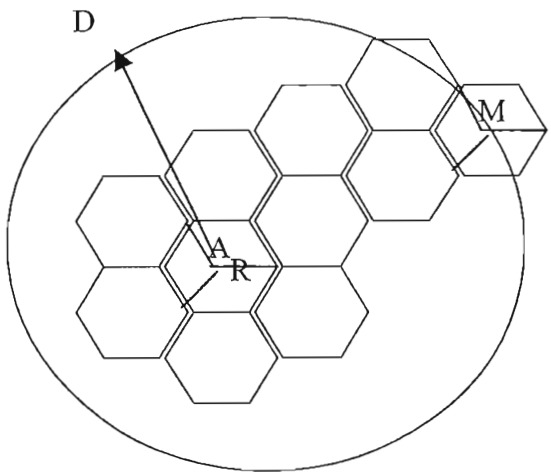


Figura 1.4 Distancia de Reutilización

Si R es el radio de la celda y D es la separación entre sitios de celda, entones la relación D/R es conocida como la relación de reutilización. Para determinar la distancia de reutilización de frecuencia en un patrón celular regular se debe aplicar la siguiente fórmula empírica:

$$i^2 + ij + j^2 = N$$

Donde N es el número de celdas totales de un patrón celular, por ejemplo en un patrón 7/21, N=21; i e j son enteros positivos. Para utilizar la celda más cercana donde la frecuencia es reutilizada se debe considerar que: i representa el desplazamiento en diámetros desde el centro de la celda por cualquier lado del hexágono, y j representa el desplazamiento en diámetros a partir de donde termina i con una dirección de 60° antihorario, con respecto a la dirección de i como se puede ver en la figura 1.5. Por ejemplo si N=21 entonces los valores de i e j que cumplen con la ecuación serán 4 y 1 respectivamente.

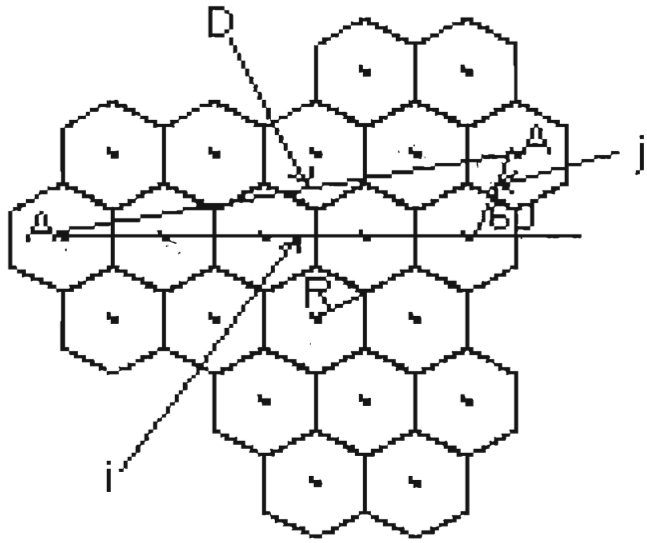


Figura 1.5 Ubicación de las celdas por reutilización de frecuencias

Aplicando la geometría de los hexágonos se demuestra que la distancia de reutilización de frecuencia, en función al patrón utilizado y al radio de la celda es:

$$D=R\sqrt{(3N)}$$

Para diferentes tamaños de "cluster", se tienen diferentes valores de D/R, así por ejemplo con celdas sectorizadas:

Tamaño del Cluster (N)	D/R
9	5.2
12	6
21	7.93

Tabla 1.1 Relación del tamaño del cluster con respecto al D/R

Es posible realizar estimaciones teóricas de relaciones de portadora a interferencia (C/I) sobre los bordes de celda en términos de la relación D/R.

En este caso se debería asumir que la tierra es plana, a menos que las alturas de las antenas, ganancia y potencias de transmisión fueron asumidas constantes, cuyo resultado podría ser no tan real.

Debe notarse que si se asume que estos parámetros son constantes, el nivel de la operadora estará determinado por el radio de acción de la estación base elegida y el nivel de interferencia dependerá de los radios de acción de las señales interferentes, entonces la relación C/I dependerá de la atenuación del trayecto y se asume propagación por tierra plana.

Para sistemas móviles celulares analógicos una relación de C/I de 18dB es requerida sobre el 90% del área de cobertura. En la práctica en zonas urbanas esto se puede conseguir con:

- K= 12 para celdas omnidireccionales.
- K= 21 para sectores con 120°.

Donde K es el número de celdas dentro del patrón de reutilización. Para pequeñas celdas sectorizadas (1km de separación) en un ambiente urbano, se tiene:

K	C/I (90%)
21	18.5
12	14
9	12

Tabla 1.2 C/I para diferentes patrones de reutilización K.

La dispersión y el efecto de la tierra significa que hay un límite al tamaño mínimo de la celda que puede ser usado mientras se siga manteniendo adecuadas distancias de reutilización.

Esto es probablemente alrededor de 1 km de separación a 900 MHz. La correcta localización del sitio de base (por ejemplo en el centro del hexágono) llega a ser crítica cuando se utilizan celdas de pequeño tamaño. La reducción de interferencias puede lograrse con los siguientes métodos:

- Control de potencia.
- Transmisión discontinua.

Control de potencia

En este caso la potencia de los transmisores se reduce al mínimo para obtener resultados satisfactorios en el enlace. Esto es dado bajo el control de la red, la cual monitorea y ajusta los niveles de potencia tanto del móvil como de las estaciones base. Los niveles de interferencia se reducen significativamente. Esta técnica también permite ahorros de batería en los móviles, lo cual es importante en equipos portátiles y transportables debido a su tamaño.

Transmisión discontinua

Este es un mecanismo que permite a los transmisores de radio ser apagados durante las pausas en las conversaciones. El nivel de la interferencia global se reduce, y la batería de la estación móvil es conservada. Inicialmente muchos sistemas móviles celulares son configurados con celdas omnidireccionales para minimizar costos iniciales. A medida que el tráfico generado por los usuarios se incrementa, es necesario incrementar capacidad, lo cual es posible con la sectorización ya sea a 120° o 60°.

Además la compartición de frecuencias permite incrementar la capacidad del sistema. Un plan de agrupación de 7 celdas permite la expansión para conseguir una sectorización de 120°.

1.1.3 BANDA DE FRECUENCIAS

La Comisión Federal de Comunicaciones (*FCC: Federal Communications Commission*), es la principal agencia gubernamental de los Estados Unidos.

La FCC ha regulado sobre cualquier área metropolitana, que allí pueden haber como dos proveedores de servicio celular, llamadas portadoras. Portadora de sin línea (Banda A) y portadora de línea o local (Banda B).

La mitad de los canales disponibles están distribuidos por la operadora de banda A, y la otra mitad está distribuida por la operadora de banda B. Originalmente, cuando los primeros celulares aparecieron, había 666 canales, 333 por portadora siguiendo el protocolo de señalización AMPS. En 1987 la FCC, aumentó el espectro celular a los 832 canales, 416 por portadora. El uso de los 832 canales celulares es a veces referido como AMPS Extendido (E-AMPS). La distribución espectral se muestra a continuación:

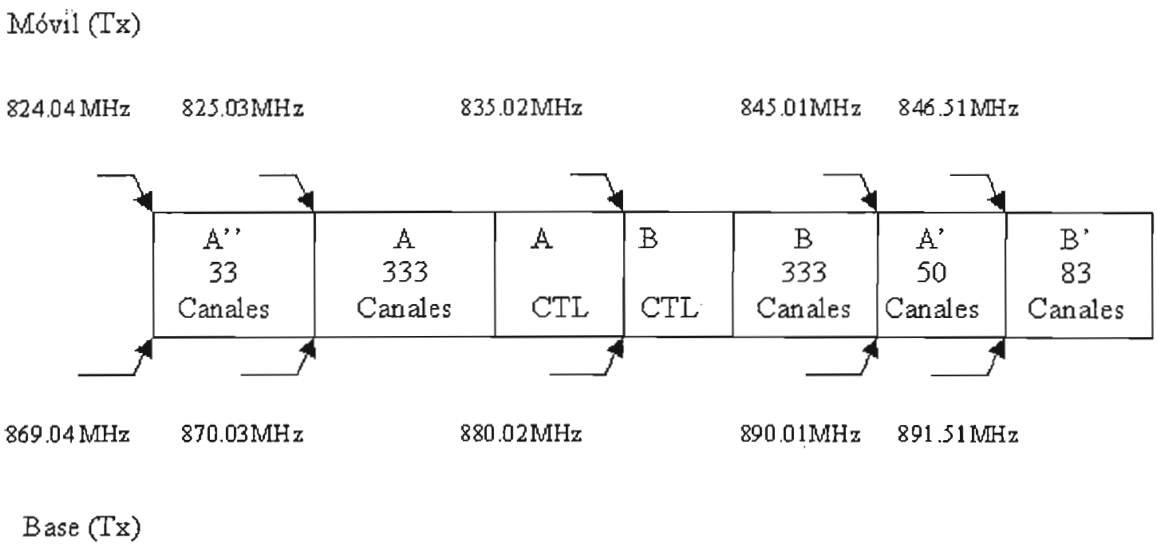


Figura 1.6 Espectro de la frecuencia del Sistema de Telefonía Móvil Avanzado (AMPS)

La banda A, asignada para el operador de telefonía inalámbrica (non-wireline) se divide en tres grupos:

- Banda A normal que va desde el canal 1 al canal 333.
- Banda A extendida (A') que va desde el canal 667 al 716.
- Banda A doble extendida (A") que va desde el canal 991 al 1023. Esta banda se asigna al canal digital.

Cada canal de comunicación dispone de dos frecuencias, la de transmisión de móvil a estación base y de transmisión de estación base a móvil, cuya separación de frecuencias es de 45 MHz. La separación de canales es de 30 kHz.

Las frecuencias más bajas son asignadas a las unidades (teléfonos), mientras que las más altas son asignadas a los sitios de celda. De los 416 canales, 21 son canales de control de datos digital, o canales de *set up* y los 395 restantes son canales de voz. Los canales están numerados de 1 a 1023 y hay un vacío de 800 a 990.

La banda B, asignada al operador alámbrico (wireline), se divide en dos grupos:

- Banda B normal, que va desde el canal 334 al canal 666.
- Banda B extendida, que va desde el canal 717 al 799.

La frecuencia de transmisión del móvil a estación base se determina a partir de la siguiente fórmula:

N = # del canal celular; F = frecuencia celular
Para N entre 1 y 866: F = 825 + 0.03 * N
Para N entre 990 a 1023: F = 794.31 + 0.03 * N

La frecuencia de transnmisión de la estación base al móvil resulta al sumar las frecuencias calculadas con las fórmulas anteriores, 45 MHz.

Los canales consisten de dos frecuencias: (1) una frecuencia de transmisión, y (2) una frecuencia de recepción. Las frecuencias son asignadas a las estaciones base y a los clientes. Cuando un cliente transmite, llamamos transmisión en el sentido de regreso o a veces llamado sentido inverso (*reverse*), cuando la estación base transmite, llamamos transmisión en el sentido de adelanto o a veces llamado sentido directo (*forward*).

La transmisión en el sentido de regreso es la recepción en el sentido de adelanto y viceversa. Hay dos tipos de canales: los canales de control y los canales de voz. A cada sitio de celda se le asigna un canal de control y varios canales de voz. Las conversaciones entre teléfonos celulares pueden ocurrir sobre los canales de voz, los canales de control son usados para enviar y recibir solamente datos digitales entre los teléfonos celulares y la estación base de la celda. La señalización sobre los canales de control estrictamente está gobernada por el protocolo de señalización AMPS. Este protocolo se usa a través del hemisferio occidental y en muchos países alrededor del mundo.

En la banda A, los canales 313 al 333 son diseñados para ser usados como canales de control. En ciertas instancias donde se necesita un canal de control adicional, el canal 312 puede ser usado. Este podría ser realizado mediante la configuración del número de canales de acceso (NAC) y el número de canales de búsqueda (NPC) usando este canal de control extra, 22 (este es a menudo el tradicional N =21).

Debe notarse que este canal de control extra no debe ser usado en el borde de las áreas de servicio de cualquier sistema. Esto es porque los móviles deben estar dirigidos en el Sistema de Mensajes de Parámetros de Cabecera (SPOM) dependiendo de cuantos canales de control deben ser explorados (21 ó 22). Si el móvil acaba de ingresar al sistema (desde otro sistema), no puede ser notificada la exploración de los 22 canales de control.

De esta manera el móvil no tomará las señales de *paging* sobre los 312 canales. Si el móvil fue voceado o si un intento de llamada fue originado, él no puede responder a esa búsqueda o puede iniciarla sobre una celda equivocada.

En la banda B, los canales de control típicamente usan los canales 334 al 354. En instancias donde se necesita un canal de control extra, el canal 355 puede ser usado. Esto podría ser realizado usando un método similar al mencionado anteriormente.

Los 21 canales de control de cada banda pueden estar dedicados a dos aplicaciones diferentes: canales de acceso y canales de búsqueda (*paging*).

Los datos sobre los canales de control en el sentido de adelanto proveen información tal como el número de identificación del sistema (SID) y el rango de los canales a explorar para encontrar los canales de acceso y de *paging*. Los canales de acceso son usados para responder a una búsqueda o a una llamada originada. El sistema y el teléfono celular usarán los canales de acceso donde la transferencia de datos en dos vías, ocurre para determinar el canal de voz inicial. Los canales de búsqueda si son usados, fijan el mantenimiento para un teléfono celular desocupado.

Cuando el controlador central recibe una llamada por parte de teléfono celular, la señalización de búsqueda empezará sobre un canal de *paging*. En muchos sistemas, las funciones de ambos canales de control estarán suministradas por el mismo canal de acceso para una celda particular. Múltiples canales de búsqueda son usados solamente en áreas de gran densidad.

1.2 ELEMENTOS DE RED

La Red de Servicio Móvil Terrestre Público (PLMN), consiste de Centros de Conmutación de Servicio Móviles (MSC), Registros de Ubicaciones Local (HLR), Estaciones Base (BS) y Estaciones Móviles (MS).

Como se muestra en la figura 1.7, una red AMPS hace uso de la PSTN a través de la MSC, el equipo de la estación base y la interconexión entre estos módulos.

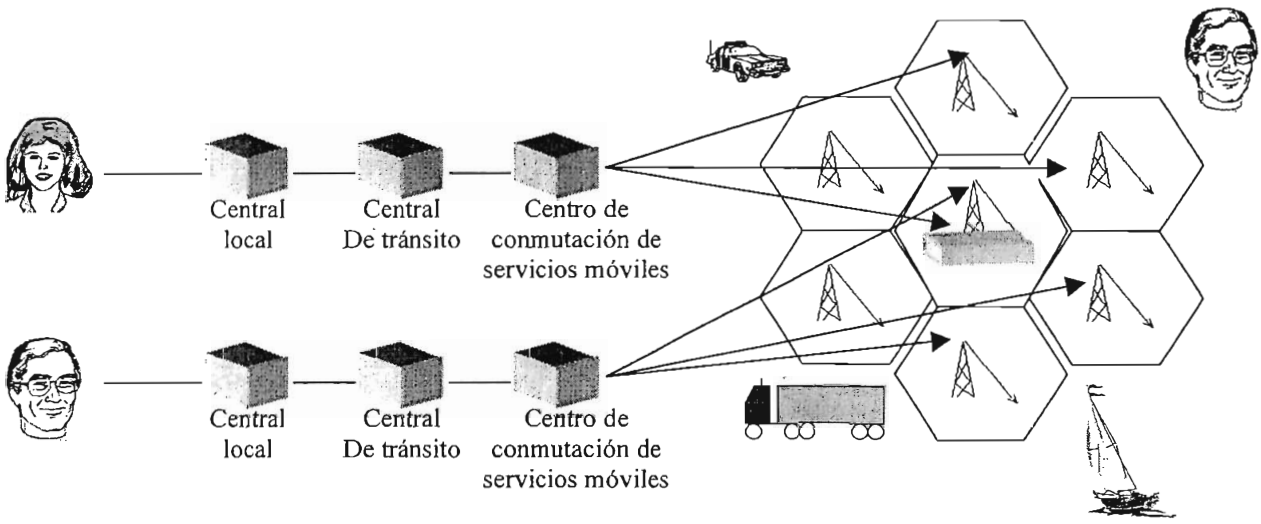


Figura 1.7 Sistema de telefonía móvil celular simplificado

El diseño modular de la red permite adaptarla a diversos requisitos de capacidad añadiendo mas MSCs, HLRs, estaciones base, canales de radio y equipos de transmisión.

1.2.1 CENTRO DE CONMUTACIÓN MÓVIL

A veces también se denomina Oficina de Conmutación de Teléfonos Móviles (MTSO). Su función principal es la de proveer un camino de voz para la conexión entre una estación móvil y un abonado fijo, o entre dos estaciones móviles. Un MSC está compuesto por un número de procesadores que controlan las funciones de conmutación, control de llamadas, interfaces de datos y el manejo de bases de datos de usuarios. Además la MSC se constituye como la interface a la PSTN. Esta conexión puede hacerse en el ámbito local, de tránsito nacional o de tránsito internacional.

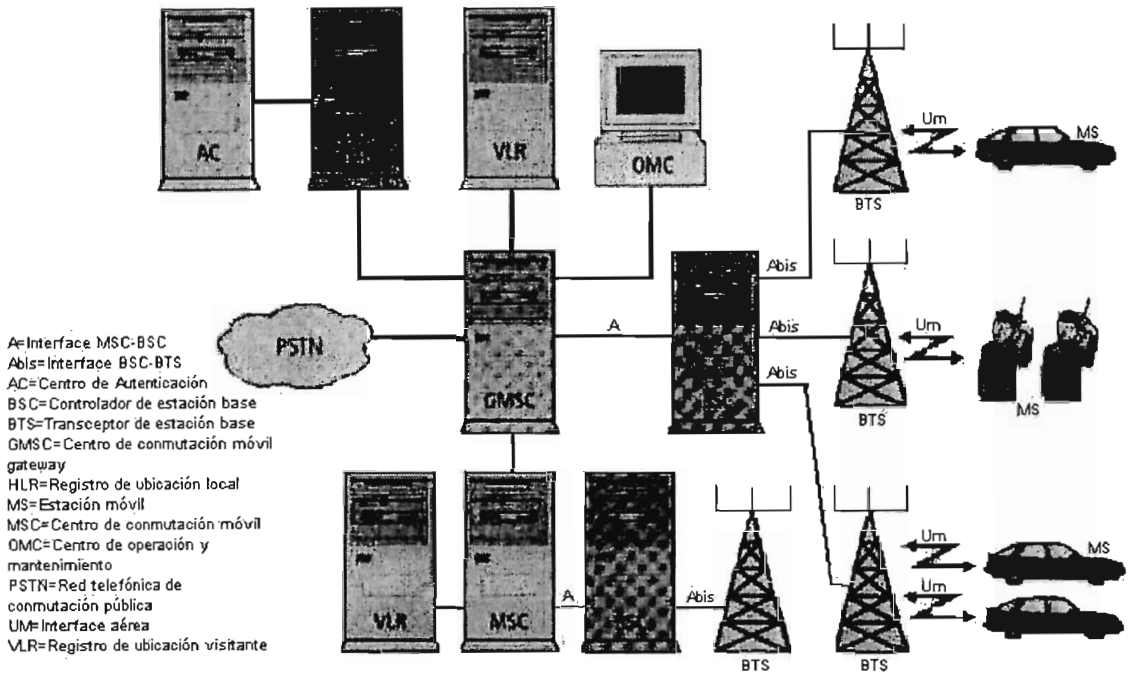


Figura 1.8 Esquema simplificado de un Centro de Conmutación Móvil[1]

Entre las funciones del MSC, se tienen las siguientes:

- Conmutación de audio.
- Control de radio frecuencia y de estación base.
- Evaluación de operación y facturación.

1.2.1.1 Conmutación de audio

El conmutador digital desempeña la función de conmutación de circuitos de voz entre la PSTN y las estaciones base, para llamadas entre usuarios fijos-móviles y móviles- móviles.

[1] Malcom W. Oliphant, (1999), p.21.

Para llamadas entre usuarios de la red fija hacia estaciones móviles, el MSC traduce los dígitos marcados del indicativo del número de abonado e inicia la búsqueda en las áreas donde se espere que la estación móvil se encuentre y causa que el móvil correspondiente sea informado a través del equipo de radio de cada estación base. Para llamadas desde estaciones móviles hacia abonados de la red fija o hacia usuarios móviles, el MSC debe codificar los dígitos marcados por el móvil e iniciar la llamada a través de las líneas troncales hacia la PSTN o da aviso a la unidad de teléfono móvil a través del equipo de radio de la estación base de la celda apropiada.

En el proceso de transferencia de llamadas, el MSC puede ser responsable de la determinación de mediciones requeridas en celdas adyacentes y la implementación de un algoritmo para la determinación de la mejor celda como destinataria de esta transferencia. El MSC entonces inicia y maneja la secuencia de eventos que dan como resultado que la estación móvil llegue en forma exitosa a la celda de destino.

1.2.1.2 Control de radio frecuencia y de estación base

El conmutador digital procesa los datos recibidos desde las estaciones base y adicionalmente cualquier otro dato relativo a las condiciones de alarma y mal funcionamiento de las mismas. Igualmente, envía datos a las unidades móviles a través de las estaciones base, instruyendo a las unidades a cambiar de canal o nivel de potencia y ordena a las unidades base la ejecución de pruebas de diagnóstico propio en forma automática y periódica o cuando sean solicitadas debido a los informes de mal funcionamiento de las estaciones base.

1.2.1.3 Evaluación de operación y facturación

El conmutador digital recopila y registra todos los eventos necesarios para la facturación y para la evaluación de operación del sistema.

Estos datos pueden ser transferidos de una cinta magnética a discos de un sistema centralizado de facturación y procesamiento de datos. El HLR es una base de datos que contiene, en forma permanente, información sobre todos los abonados, sus servicios, su localización y el estado de su actividad.

El HLR proveerá de información para validarla inmediatamente después de que el perfil del cliente haya alcanzado rasgos importantes, como por ejemplo, correo de voz. En las grandes redes con alta densidad de abonados, los HLRs son nodos separados, mientras que en las redes pequeñas pueden ser integrados en el MSC. El Registro de Localización de Visitantes (VLR) es una base de datos que contiene toda la información temporal necesaria para el MSC, que permite brindar servicio a los abonados visitantes a la red.

El Centro de Mensajes (MC) soporta varios tipos de servicios de mensajería, por ejemplo casillero de voz (*voice mail*), fax y correo electrónico (*e-mail*). Dentro del sistema se puede introducir un Sistema de Soporte de Operación (OSS) para el manejo de MSC, BS, HLR, y redes celulares.

1.2.2 ESTACIONES BASE

Las estaciones base manejan y supervisan la conexión radioeléctrica entre ella y la estación móvil, así como la comunicación con la MSC. El término equipo de estación base es usualmente reservado para radios y componentes electrónicos asociados, sin embargo el equipo de estación base puede ser extendido para describir antenas, mástiles de antenas, cables, duplexores, equipos auxiliares, baterías de respaldo, generadores eléctricos de emergencia, equipos de pruebas y otros equipos requeridos. Los sitios en los cuales se ubican las estaciones base pueden ser en montañas o en los sitios en los cuales el proveedor del servicio considere apropiado. Una estación base incluye las siguientes funciones principales:

- Grupo de radiocanales.
- Interface central/equipo de radio.
- Alimentación.
- Sistema de antenas.

1.2.2.1 Grupo de radiocanales

El Grupo de Radiocanales (*RCG: Radio Channels Group*)es común a los canales de voz analógicos y digitales. La filosofía básica de diseño es la compatibilidad. Es fácil introducir una interface digital de radio en las estaciones de base analógicas existentes. El RCG comprende los siguientes módulos principales:

- Módulos de canal.
- Sistema de combinador de transmisor.
- Sistema de multiacoplador de receptor.

Módulos de canal

Hay tres tipos de módulos de canal para el servicio analógico: Módulos de Transceptor Analógico (TRM), Módulos de Receptor de Intensidad de la Señal (SRM) y Módulos de Probador de Canal (CTM). Para el servicio digital hay Módulos de Transceptor Digital (DTRM) y Módulos de Verificación de Localización (LVM)

El TRM puede configurarse como canal de voz o canal de control o receptor de intensidad de la señal (SR), mientras que el SRM está diseñado específicamente para la función de receptor de intensidad de la señal y el CTM para la función de probador de canal.

Combinador de transmisor

El combinador de transmisor proporciona la posibilidad de combinar hasta 24 transmisores con una antena común. Se puede elegir entre dos tipos diferentes de sistema de combinador, unos de sincronización manual y el otro de sincronización automática.

El combinador de sincronización automática sintoniza automáticamente a las mismas frecuencias que los transceptores relacionados en presencia de potencia RF, es decir, que no es necesario ir a los lugares para cambiar las frecuencias.

Multiacoplador de receptor

El multiacoplador de recepción permite la conexión de hasta 48 receptores en diversidad, a una antena común e incluye:

- Canales de control.
- Canales de localización.
- Canales de Voz.

1.2.2.2 Canal de control

El canal de control provee una información global del sistema a los móviles en una celda dada. También efectúa la búsqueda (*paging*) de móviles individuales para determinar su disponibilidad para recibir llamadas. Los canales de control configuran las llamadas originadas y terminadas en los móviles, además controlan el registro del móvil.

El canal de control principal reporta al MSC la respuesta de un móvil a la búsqueda (*page response*) o la información de un intento de llamada desde un móvil. El MSC entonces utiliza al canal de control para asignar al móvil un canal de voz apropiado.

1.2.2.3 Canal de localización

El canal de localización monitorea los niveles de potencia de la señal de los canales en la banda del receptor, además reporta los niveles de potencia y la tendencia de cualquier canal que haya sido requerido por el MSC, en un proceso de *hand-off*. El MSC debe determinar en que celda el móvil está ubicado, lo cual es posible con el receptor de localización de todas las celdas adyacentes a la celda que maneja la llamada. El receptor de localización provee información de la señal más fuerte recibida (RSSI) y un tono de supervisión de audio (SAT) que fuera requerida desde el MSC.

La velocidad del proceso de *hand-off* está sujeta a la velocidad con la cual la información de localización puede ser procesada por el MSC y el receptor de localización. En sistemas de alta capacidad, la velocidad de localización depende del tiempo requerido para que el receptor de localización se sintonice al canal deseado y efectúe las mediciones de RSSI y SAT.

1.2.2.4 Canales de voz

Los canales de voz proveen el camino de voz y la conversión de la señal requerida, para mantener llamadas en los móviles. Además, supervisan las llamadas y monitorean al móvil para el acceso de servicios especiales, tales como conferencias tripartitas, también monitorean los niveles de intensidad de la señal y establecen las tendencias para determinar si se requiere un *hand-off*.

El canal de voz además de ser utilizado para comunicación de voz, supervisión de la calidad de transmisión de la voz, se lo utiliza en la transmisión de datos, por ejemplo, durante las transferencias, y para control de potencia de salida

1.2.3 ESTACIONES MÓVILES

La unidad móvil de suscriptor consiste en una unidad de control y un transceptor de radio que transmite y recibe señales de radio desde y hacia una estación base o sitio de celda (*cell site*), además de una unidad lógica y una antena móvil. La unidad de control es la interface entre el suscriptor y el sistema. La estación móvil requiere de un teclado, un parlante, una unidad de control de un suscriptor e indicadores.

El transceptor proporciona la transmisión y recepción de la voz en modo dúplex. La banda RF, está dividida en dos segmentos separados en 20 MHz de ancho de banda, cada uno con 666 canales. El primer segmento de 825 a 845 MHz, contiene los canales de transmisión de la unidad suscriptora. El segundo segmento de 870 a 890 MHz, contiene los canales de recepción de la unidad suscriptora. Cada frecuencia de transmisión de la unidad suscriptora está separado de su frecuencia recepción dúplex por 45 MHz.

La diferencia de una unidad móvil de una portátil no es tan grande, las unidades portátiles tienen una potencia de salida más baja y una antena menos eficiente. De acuerdo con la potencia radiada efectiva nominal (ERP) transmitida, se definen los tres tipos de terminales de suscriptor, así:

- Móvil: 3watts. Denominado de Clase I.
- Transportable: 1.6watts. Denominado de Clase II.
- Portátil: 0.6watts. Denominado de Clase III.

La identificación de la edad de un teléfono celular se la hace por medio de la Marca de Clase de la Estación (*SCM: Station Class Mark*). Este número tiene una longitud de 4 bits que están desglosados como sigue:

Bit 1: 0 para los 666 canales en uso (antiguo).
1 para los 832 canales en uso (nuevo).
Bit 2: 0 para una unidad móvil (en vehículos).
1 para transmitir voz (para portátiles).
Bit 3 y 4: Identifica la clase de potencia de la unidad.

Bajo el comando de señales enviadas por las estaciones base, el ERP puede ser reducido bajo el valor nominal en pasos de 4dB hasta 28dB debajo de los 3 watts. La portadora del transmisor se modulada en frecuencia con información de audio y señalización codificada en binario.

Tanto la señal de audio y la información de señalización pueden ser representadas al mismo tiempo, dependiendo del estado (*status*) de la estación suscriptora. La operadora es entonces enviada a la unidad de antena para la radiación hacia una estación base localizada.

Las señales que entran por la antena desde una estación base localizada, arriban al receptor, donde son amplificadas y demoduladas. Las señales pueden ser de voz (la cual es enviada a la unidad de control) o información de señalización codificada (la cual es enviada a la circuitería lógica para ser decodificada).

La circuitería lógica para la unidad transceptora funciona como el control *master* de la unidad suscriptora. La circuitería lógica codifica y decodifica la información de señalización codificada en binario de 10 kbps, la cual es usada para la comunicación entre una estación base localizada y la unidad suscriptora. Algunas de las mayores funciones lógicas incluyen lo siguiente:

- Decodificar órdenes recibidas de una celda localizada, tales como órdenes para re - sintonizar el transceptor a un nuevo canal de frecuencia.

- Codificar la información de señalización para transmisión hacia la estación base localizada. Esta información incluye dígitos marcados para originar llamadas, tonos, DTMF, para señalización total durante la conversación, respuesta rápida, desconexión de la señal al completar una llamada e identificación del suscriptor ante el sistema.
- Realizar las funciones de control del transceptor, tales como sintonizar el receptor, detectar las pérdidas de la señal desde la base y desconectar la comunicación automáticamente.
- Proveer al suscriptor la información correspondiente al *status*, como por ejemplo, una indicación de que se encuentra en un área que no hay servicio, visitante (*roamer*), etc.

1.3 PARÁMETROS DE LOS SISTEMAS MÓVILES CELULARES

En este punto se analizarán algunos parámetros que deben ser configurados a nivel de MSCs y de estaciones base para asegurar un correcto funcionamiento del sistema, que permita que los procesos de llamada sean adecuados.

1.3.1 IDENTIFICACIÓN DEL SISTEMA

Identificación del Sistema (*SID: System IDentification*), define el sistema local de la estación móvil en FCC, y consiste de un número de 15 bits de longitud, los cuales definen el identificativo internacional y un número de sistema.

1.3.2 TONO DE SUPERVISIÓN DE AUDIO

En los sistemas móviles celulares, la interferencia más significativa es la de una unidad de móvil a una celda distante, que utilice la misma frecuencia de trabajo.

En AMPS las celdas adyacentes definen un tono denominado Tono de Supervisión de Audio (*SAT: Supervision Audio Tone*), para identificar portadoras externas, lo cual minimiza la probabilidad de tomar decisiones erróneas de control, debido a interferencias, ya sea cocanal o de canal adyacente.

Para prevenir una interferencia, la detección de un código ajeno de SAT, bloquea temporalmente el canal (si es que está desocupado) y si el canal se encuentra ocupado, entonces ocurre una transferencia de la llamada a otro canal de voz. En los dos casos este canal se vuelve no disponible para tráfico y la capacidad del sistema se ve reducida.

Hay tres posibles SATs, y el SAT correcto debe ser transmitido más o menos continuamente tanto sobre en canal de control en adelanto, en sentido directo; como sobre el canal de control de retraso, sentido inverso; si una conversación esta siendo sostenida.

El SAT también sirve como un código de tono de *squelch*, para eliminar ruidos no deseados cuando una portadora no está presente. Cuando al teléfono celular se le asigna un canal de voz, éste escucha para el SAT apropiado, y si este no escucha el SAT correcto deja caer la llamada. Si el SAT correcto es escuchado, el teléfono celular transmite el SAT correcto sobre el canal de control en el sentido inverso.

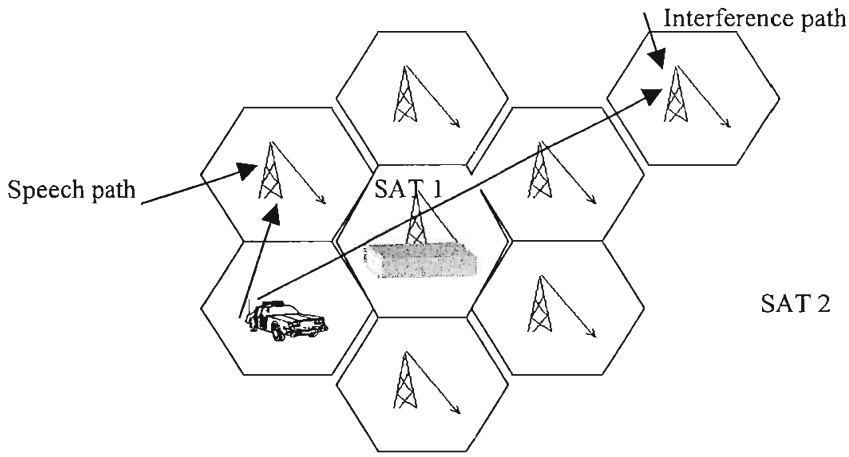


Figura 1.9 Establecimiento de un Tono de Supervisión de Audio para evitar interferencia

Los tres tonos SAT tienen diferentes valores de frecuencias únicas:

- 5970 Hz SAT 0.
- 6000 Hz SAT 1.
- 6030 Hz SAT 2.

Se los utiliza para identificar el tráfico local de la celda, del tráfico inherente de las celdas locales. El SAT se genera en la estación base y regresa por medio de la estación móvil.

1.3.3 CÓDIGO DE COLOR DIGITAL

El Código de Color Digital (*DCC: Digital Color Code*) es similar al SAT, pero su aplicación está en los canales de control (0,1,2,3). El código de color está constituido por 2 bits codificados en 7 bits, utilizando un código de *Hamming* (7:4) y se los utiliza para identificar la estación base a la cual se dirige el mensaje.

Además de estas señales de supervisión, se utiliza un tono de 10 kHz (excursión: ± 8 kHz) denominado tono de señalización (*ST: Signaling Tone*), que es generado por el móvil cuando el terminal se encuentra en condición de reposo, además este tono es enviado por el canal de conversación hasta que el móvil sé

encuentre en la condición de descolgado (*off-hook*). Este tono no es generado cuando el móvil se encuentra en la condición de descolgado y finalmente este tono es enviado durante un período de 1.8 segundos a la liberación de una llamada y por un período de 0.4 segundos si se solicita una conferencia tripartita. En canales NAMPS, el ST es reemplazado por su equivalente digital, llamado Digital ST (DST), cuya frecuencia es de 10 kHz y enviada por 50 milisegundos.

Existen ciertos parámetros definidos para el usuario que determinan el comportamiento de una estación base. Tales parámetros se los define en tablas en los MSCs identificando los niveles de referencia, así:

a) SSD (*Signal Strenght Decrease*).- Este parámetro especifica el nivel umbral de la intensidad de la señal de radiofrecuencia (RF), requerido para inicializar el decremento de la potencia de transmisión de la estación móvil. El rango del parámetro SSD está entre –118dBm y –55dBm. Este parámetro es utilizado para que el móvil trabaje con la potencia necesaria para la comunicación y así no desgaste su batería más de lo debido cuando se encuentra cerca de la estación base.

b) SSI (*Signal Strenght Increase*).- Este parámetro especifica el nivel umbral de la intensidad de la señal de RF, bajo el cual se inicia un incremento de la potencia de transmisión de la estación móvil. El rango del parámetro SSI está entre –118dBm y –55dBm. Este parámetro es utilizado para cuando el móvil se está alejando de la estación base y el nivel de la señal comienza a disminuir.

c) SSH (*Signal Strenght Hand-off*).- Este parámetro especifica el nivel umbral de la intensidad de la señal de RF, bajo el cual un requerimiento de *hand-off* es iniciado. El rango del parámetro SSH está entre –118dBm y –55dBm. Este parámetro interviene cuando se tienen celdas vecinas y un móvil se encuentra en movimiento en la dirección de una a otra celda.

d) SSB (*Signal Strenght Blocking*).- Este parámetro especifica el nivel umbral de la intensidad de la señal de RF, por encima del cual se ordena bloquear a un canal de voz libre (encapsulándole). Cuando el receptor en el canal de voz detecta una señal portadora "no deseada" por encima del parámetro establecido SSB, el canal de voz permanecerá bloqueado. El rango del parámetro SSB está entre –118dBm y –55dBm. En otras palabras este parámetro da la sensibilidad de los canales, es decir mientras disminuye aproximándose a –118dBm, el canal es más sensible a interferencias.

e) SSHY (*Signal Strenght Hysteresis*).- Este parámetro especifica la diferencia de intensidad de la señal en dB entre la celda vecina y la celda en uso, requerida para escoger una celda vecina como candidata para realizar el *hand-off*. El rango del parámetro SSHY está entre +63 a –63 dBm.

f) SNH (*Signal to Noise Hand-off*).- Este parámetro representa el nivel umbral de la relación señal a ruido, bajo el cual se iniciará un requerimiento de *hand-off*. Un SAT es incluido en la transmisión del canal de voz, el mismo que es recibido y enviado por la estación móvil. El canal de voz evalúa la relación señal a ruido (S/N) del SAT retornado. Si la relación está debajo del valor SNH asignado, un requerimiento de *hand-off* será iniciado, aunque la medición del nivel de señal sea mejor que SSH. El rango del parámetro SNH está entre 0 y 63dBm.

g) SNR (*Signal to Noise Release*).- Este parámetro representa el nivel umbral de la relación señal a ruido, bajo el cual se inicia una liberación de llamada. El sistema dará una oportunidad a la llamada en proceso, para continuar en otra celda por medio de un requerimiento de *hand-off*. En caso que el *hand-off* no tenga éxito, la llamada es liberada. El rango del parámetro SNR está entre 0 y 63dB. Este parámetro da la sensibilidad con respecto al ruido, mientras el canal es más grande, el canal es más sensible.

h) SUH (*Supress Hand-off*).- Este parámetro representa el intervalo de tiempo en el cual será suprimida la iniciación de una nueva solicitud de *hand-off*. Las solicitudes de *hand-off* serán iniciadas con el intervalo especificado por SUH, mientras que la intensidad de señal de RF sea menor que SSH y/o S/N en el SAT sea menor que SNH. El rango del parámetro SUH es de 1-20 segundos.

i) Cell ID.- Representa la identificación de una celda. Es recomendable que este parámetro este formado por el nombre de la ubicación más una letra o dígito.

j) Ncell (*Neighbouring Cell*).- Es definida como una celda, a la cual un *hand-off* puede ser realizado, cuando las dos celdas están conectadas al mismo MSC. Sobre las 16 N celdas pueden ser definidas para cada una.

INTENSIDAD DE LA SEÑAL	PARÁMETRO
-72dBm	SSD: mobile power decrease
-82dBm	SSI: mobile power increase
-95dBm	SSH: mobile hand off level
-110dBm	SSB: block channel level

Tabla 1.3 Niveles de Intensidad de Señal utilizados como referencia

1.4 INTERFACE DE RADIO

1.4.1 DESCRIPCIÓN DE LA INTERFACE DE RADIO

La señalización aérea se establece a través del canal de control en el sentido hacia adelante, es decir en el sentido de estación base a móvil, como en el sentido reverso, de móvil a estación base. La señalización se da al enviar trenes de bits codificados en unidades denominadas palabras. En AMPS, una palabra enviada al móvil contiene 28 bits, una palabra desde el móvil contiene 36 bits.

Un código adicional de 12 bits de corrección de error es añadido, resultando en longitudes de llamada de palabra de 40 y 48 bits respectivamente. Por seguridad cada palabra es repetida un cierto número de veces. En la figura se puede observar que el formato del mensaje del móvil solicitando un número de la red es de dos palabras de 48 bits cada uno, describiendo un número de 16 dígitos. La información es repetida 5 veces.

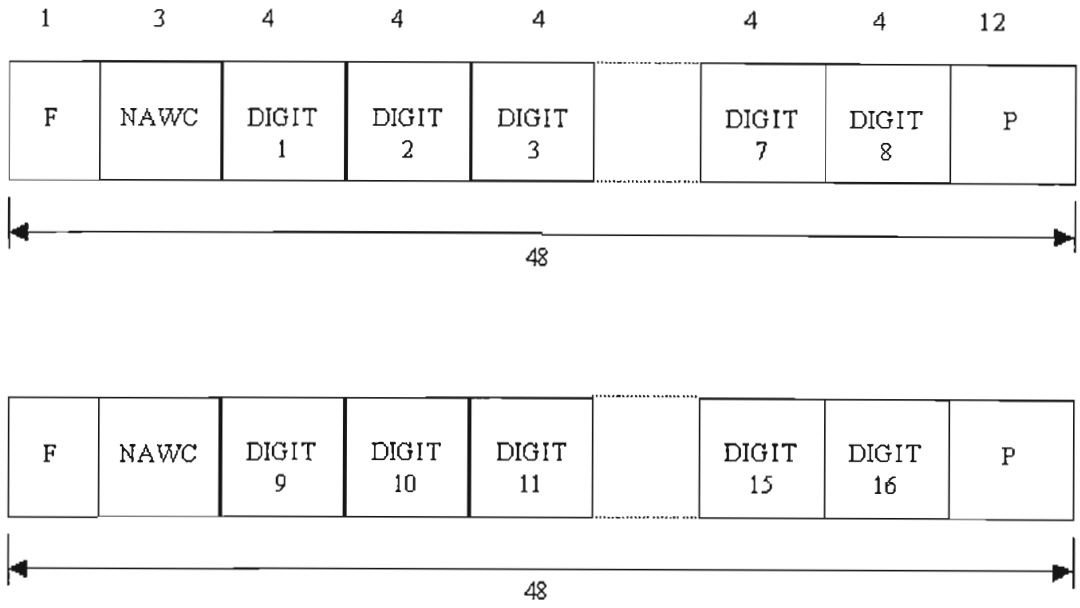


Figura 1.10 Trenes de bits codificados en palabras

1.4.2 CANAL DE CONTROL EN ADELANTO

El Canal de Control de Adelanto (*FOCC: Forward Control Channel*) consiste de tres corrientes discretas de información, la corriente A, la corriente B y la corriente ocupado-libre (*busy-idle*), las cuales son multiplexadas. Los mensajes para las estaciones móviles con el bit menos significativo de su número MIN igual a "0", son enviados sobre la corriente A, y esos mensajes con un "1" en su bit menos significativo son enviados sobre la corriente B.

La corriente *busy- idle* contiene bits ociosos y ocupados, los cuales indican si el canal de control reverso esta ocupado u ocioso, por ejemplo si este bit es igual a "0" ésta ocupado, y si es 1, está desocupado u ocioso.

El tren de palabras comienza con *DOTTING* que es un término usado para describir la señal enviada para sincronismo de los móviles.

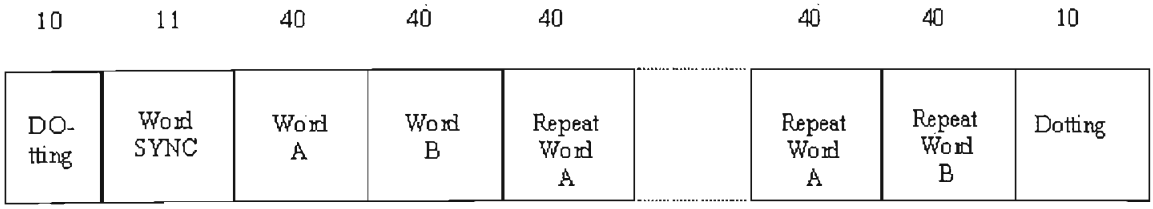


Figura 1.11 Formato general de un mensaje en el canal de control en adelanto

El *dotting* consiste de una secuencia de 10 bits a saber, 1010101010 seguido por un código de palabra de 11 bits 11100010010. Cada palabra contiene 40 bits incluyendo paridad, y se repite 5 veces (un bloque) para asegurar la correcta transferencia de información. Para un mensaje multipalabra, el segundo bloque de palabra y los subsecuentes bloques están formados de la misma manera que el primer bloque incluyendo el *dotting* y el código de sincronismo.

Cada mensaje consiste de una o más palabras. Los mensajes transmitidos sobre este canal son:

- Mensaje de control de la estación móvil.
- Mensaje de cabecera.
- Mensaje control – *filler*.

1.4.3 CANAL DE VOZ EN ADELANTO

El Canal de Voz de Adelanto (*FVC: Forward Voice Channel*) es una corriente de datos de banda ancha que se envía por la estación terrena de la estación móvil. Esta corriente de datos debe ser generada a una velocidad de 10kbps.

Una secuencia de 37 bits del campo *dotting* y un código de sincronización de 11 bits son enviados para permitir a las estaciones móviles sincronizarse con los datos que están ingresando, excepto en la primera repetición, en donde se usan los 101 bits de la secuencia *dotting*.

1.4.4 CANAL DE CONTROL REVERSO

El Canal de Control Reverso (*RECC: Reverse Control Channel*) es una corriente de datos de banda ancha que se envía desde la estación móvil a la estación terrena. Esta corriente de datos correrá a una velocidad de 10kbps ± 1bps.

Todos los mensajes comienzan con una secuencia de 30 bits del campo de *dotting* 01010101....010101 y un código de sincronismo de 11 bits 11100010010 y la codificación del código de color digital.

Cada palabra contiene 48 bits, incluyendo paridad y se repite 5 veces con el propósito de formar un bloque. Una palabra está formada por 36 bits codificados por un código de línea BCH y con una distancia de 5 (48, 36; 5).

Cada mensaje del RECC puede estar constituido por una de las cinco palabras. Los tipos de mensaje que pueden ser transmitidos sobre el canal de control reverso son los siguientes:

- Mensaje de respuesta de búsqueda.
- Creación del mensaje.
- Mensaje de confirmación de la orden.
- Mensaje ordenado.

1.4.5 CANAL DE VOZ REVERSO

El Canal de Voz Reverso (*RVC: Reverse Voice Channel*) es una corriente de datos de banda ancha que se envían desde la estación móvil a la estación terrena. Esta corriente de datos debe ser generada a una velocidad de 10kbps.

Una secuencia de 37 bits del campo dotting y un código de sincronización de 11 bits son enviados para permitir a las estaciones móviles sincronizarse con los datos que están ingresando, excepto en la primera repetición, en donde se usan los 101 bits de la secuencia *dotting*. Cada palabra contiene 48 bits, incluyendo paridad y se repite 5 veces junto con el campo *dotting* y el código de sincronismo, todo esto constituye un bloque de palabra.

Cada mensaje puede consistir de una o dos palabras. Los tipos de mensajes que pueden ser transmitidos sobre el canal de voz reversa son:

- Mensaje de conformación de la orden.
- Mensaje de llamada – dirección.

1.4.6 MENSAJE DE CABECERA

- Sistema de los parámetros del mensaje de cabecera.
- Acción global del mensaje de cabecera.
- Mensaje de registro de la identificación.
- Mensaje control – filler.

Los mensajes de cabecera son enviados en un grupo llamado tren del mensaje de cabecera. El primer mensaje del tren debe ser el sistema de parámetros, el mensaje de acción global y/o el mensaje del registro ID son enviados seguidamente al final del primer mensaje.

El número total de palabras en el tren es una más que el valor del campo NAWC contenido en la primera palabra del sistema de parámetros. La última palabra del tren debe fijarse en "0".

1.4.7 ESTÁNDARES

La familia de estándares inalámbricos AMPS fueron introducidos como otro estándar para radiotelefonía analógica, ya que AMPS siguió al IMTS. Sin embargo, debido a la alta capacidad permitida en el concepto celular, la baja potencia con la cual el sistema opera, y el diseño robusto de AMPS por AT&T, AMPS ha sido todo un suceso.

Más de la mitad de los teléfonos celulares en el mundo operan de acuerdo al estándar AMPS, el cual desde 1988 ha sido mantenido y desarrollado por la Asociación de Industrias de Telecomunicaciones (TIA). Desde este comienzo exitoso, AMPS se ha expandido para introducir tecnologías digitales como TDMA, CDMA, operación en banda angosta (NAMPS), modificaciones residenciales y empresariales.

Algunos de los principales estándares del interface de radio AMPS, son los siguientes:

- **IS – 3: Celular Analógico**

Este es el estándar original del celular analógico, que fuera reemplazado por el estándar ANSI EIA/TIA – 553 y por el estándar interino TIA IS – 91.

- **EIA/TIA – 553: Celular Analógico**

La versión ANSI del estándar celular analógico. Generalmente un paso atrás del IS – 91, sin soporte para NAMPS.

- **IS – 54: TDMA Celular Digital**

Un sistema celular digital que comprime tres conversaciones en un canal analógico, utilizando la tecnología de Acceso Múltiple por División de Tiempo. Planes futuros permitirán establecer seis conversaciones en un solo canal y utilizando una interpolación digital en las conversaciones, una capacidad incrementada al doble.

- **IS – 88: Celular analógico de banda estrecha (NAMPS)**

Un sistema desarrollado por MOTOROLA que comprime tres conversaciones en un solo canal, utilizando Multiplexación por división de frecuencia. Inicialmente estandarizado en un estándar interino TIA IS – 88, y ahora incorporado en IS-91.

- **IS – 91: Celular analógico y PCS**

La versión TIA del estándar celular analógico, en el que se incorpora la funcionalidad de IS – 88 e IS – 94 operando en la banda PCS (sobre los 2GHz).

- **IS – 94: Celular para lugares interiores**

Un estándar para la operación del sistema celular en lugares interiores, utilizando extremadas bajas potencias. Ahora incorporado en IS – 91.

- **IS – 95: CDMA Celular digital**

Un sistema celular digital que permite la compresión de entre 10 a 20 conversaciones en un canal celular por la combinación de canales de 30kHz en un solo canal de 1.25MHz, utilizando tecnología de Acceso Múltiple por división de código para combinar y recuperar las conversaciones individuales.

- **IS – 136: TDMA Celular Digital con la introducción del canal de control digital**

Una extensión al IS – 54 TDMA, que incluye un canal de control más avanzado, conocido como el canal de control digital (DCCH), para distinguirlo del canal de control analógico, que es menos sofisticado, y que aún sigue siendo digital.

1.5 PROCESAMIENTO DE LLAMADAS

La conclusión de una llamada dentro de un sistema de rádio celular es muy similar a la red de telefonía pública conmutada. Cuando una unidad móvil se enciende, realiza una serie de procedimientos de arranque y después prueba la intensidad de la señal recibida en todos los canales del usuario prescritos. La unidad automáticamente se sintoniza al canal con la intensidad de la señal de recepción más fuerte y se sincroniza para controlar la información transmitida por el controlador de sitio de célula. La unidad móvil interpreta la información y continúa monitoreando él(los) canal(es) de control. La unidad móvil automáticamente rastrea periódicamente para asegurarse que está utilizando el mejor canal de control.

Dentro de un sistema móvil celular, las llamadas se pueden realizar entre una línea compartida y un teléfono móvil o entre dos teléfonos móviles.

1.5.1 LLAMADAS DE LÍNEA A MÓVIL

El centro de conmutación de un sistema celular recibe una llamada de una línea compartida a través de una línea interconectada dedicada, desde la PSTN. El conmutador traslada los dígitos marcados recibidos y determina si la unidad móvil, a la cual la llamada está destinada, está colgada o descolgada (ocupada). Si la unidad móvil está disponible, el conmutador vocea al suscriptor móvil. Siguiendo una respuesta de voceo de la unidad móvil, el conmutador asigna un canal desocupado e instruye a la unidad móvil que se sintonice a ese canal.

La unidad móvil envía una verificación de la sintonización del canal por medio del controlador en el sitio de la celda, y después envía un tono de progreso de llamada al teléfono móvil del suscriptor, causando que éste suene. El conmutador termina los tonos de progreso, cuando recibe la indicación positiva que el suscriptor ha contestado el teléfono y la conversación entre las dos personas ha comenzado.

1.5.2 LLAMADAS DE MÓVIL A LÍNEA

Un suscriptor móvil que desea llamar a una línea compartida, primero introduce el número llamado en la memoria de la unidad, usando los botones de tono o de pulso en la unidad de teléfono. El suscriptor, oprime la tecla para enviar, la cual transmite el número marcado, así como el número de identificación del suscriptor móvil al conmutador (MIN1, MIN2). Si el número de identificación es válido, el conmutador enruta la llamada sobre una interconexión de línea compartida. Usando el controlador de sitio de celda, el conmutador asigna a la unidad móvil un canal de usuario desocupado e instruye a la unidad móvil que sintonice ese canal.

Después de que el conmutador recibe la verificación, que la unidad móvil está sintonizada al canal asignado, el suscriptor móvil recibe un tono de llamada progresiva, audible, del conmutador. Después de que la persona a la que se llamó levanta el teléfono, el conmutador termina los tonos de llamada progresiva y la conversación puede conversar.

1.5.3 LLAMADAS DE MÓVIL A MÓVIL

Para originar una llamada a otra unidad móvil, el que llama introduce el número marcado en la memoria de la unidad, por medio del teclado en el dispositivo de teléfono y después oprime la tecla de enviar. El conmutador recibe el número de identificación del que llama y el número marcado y después determina si la unidad llamada está libre para recibir la llamada. El conmutador envía un comando de voceo a todos los controladores de sitio de celda y el que es llamado (el cual puede estar en cualquier parte del servicio) recibe un llamado.

Después de un voceo positivo del que fue llamado, el conmutador asigna a cada uno, un canal de usuario desocupado y les instruye para que se sintonicen a su canal respectivo. Entonces el teléfono del que está llamando suena.

Cuando el sistema recibe una noticia que el que fue llamado ha contestado el teléfono, el conmutador termina el tono de llamada progresiva y la conversación puede comenzar entre las dos unidades móviles.

Si un suscriptor móvil desea iniciar una llamada y los canales de usuario están ocupados, el conmutador envía un comando de reintento dirigido instruyendo al suscriptor que vuelva a intentar la llamada por una celda vecina. Si el sistema no puede distribuir un canal por medio de la celda vecina, el conmutador transmite un mensaje de interrupción a la unidad móvil que está llamando por medio del canal de control. Cada vez que está llamando a un suscriptor móvil que está descolgado, el que llama recibe una señal de ocupado.

1.5.4 LOCALIZACIÓN Y TRANSFERENCIA DE LLAMADAS

1.5.4.1 Localización

La función de localización efectúa la supervisión de la calidad de transmisión del radio trayecto. Esta función permite mantener una buena calidad de transmisión durante una llamada analógica en curso, independientemente del desplazamiento del abonado dentro de la zona de servicio.

El equipo de canal de voz en la estación de base evalúa continuamente la relación señal a ruido del tono audible de supervisión (SAT) y la intensidad de la señal de la onda portadora en una llamada en curso. Cuando el equipo del canal de voz ha determinado que la calidad de transmisión es inferior a un nivel especificado (fijado por celda mediante comandos en el MSC), notificará al MSC que es necesario localizar un mejor canal de voz.

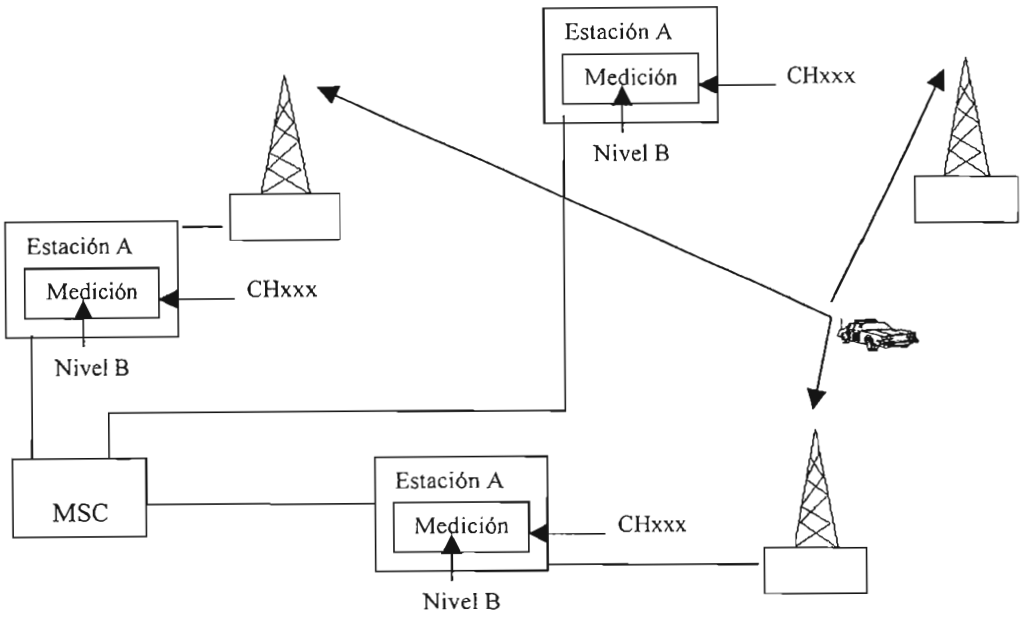


Figura 1.12 Las estaciones vecinas miden el nivel de señal del canal en uso, la MSC hace el cambio a la estación con mejor señal.

El MSC solicita entonces al equipo receptor de intensidad de la señal en las celdas adyacentes que informe sobre los resultados de medición de la intensidad de la señal de onda portadora de la frecuencia particular usada.

Los resultados se evalúan (según parámetros establecidos por celda mediante comandos) y clasifican jerárquicamente en el MSC. Si se encuentra un canal de voz libre en la mejor celda y el canal de voz reconoce el SAT usado para la llamada en curso, se inicia una transferencia. Si no se cumplen ambos criterios, la búsqueda de un canal libre continuará en la segunda celda mejor, y así sucesivamente.

La función de localización digital supervisa continuamente la calidad del canal para llamadas digitales. El equipo del canal digital de voz usa un proceso de transferencia con asistencia móvil para facilitar la recolección efectiva de las mediciones necesarias para el análisis de localización.

El equipo del canal digital de voz evalúa la intensidad de la señal portadora de RF y la tasa de errores de bits (BER). Una vez que el equipo del canal digital de voz ha determinado que podría mejorarse la calidad de la llamada si esta fuera manejada por otro canal de voz, se iniciará una petición de transferencia al MSC. La petición de transferencia incluye una lista de candidatos posibles para la transferencia.

1.5.4.2 Transferencia de llamadas

Cuando una llamada ha sido establecida, el canal de voz asignado, realiza mediciones de la intensidad de la señal recibida de la unidad móvil. Si el nivel de RSSI se encuentra bajo un valor umbral, la unidad móvil requerirá al MSC una transferencia de llamada (*Hand-off*) a un canal que presente una mejor calidad. El algoritmo de decisión del *Hand-off* está basado en mediciones de RSSI, disponibilidad de canales, niveles de potencia del móvil y un balance de carga.

Los parámetros medios se comparan con los de la estación base y si existe una mejora mínima de 3dB, el MSC transmite una orden a la estación móvil para que cambie la frecuencia al nuevo canal de voz elegido en la nueva celda. La estación móvil confirma la orden y se hace una conmutación en el MSC al mismo tiempo que la estación móvil cambia su frecuencia.

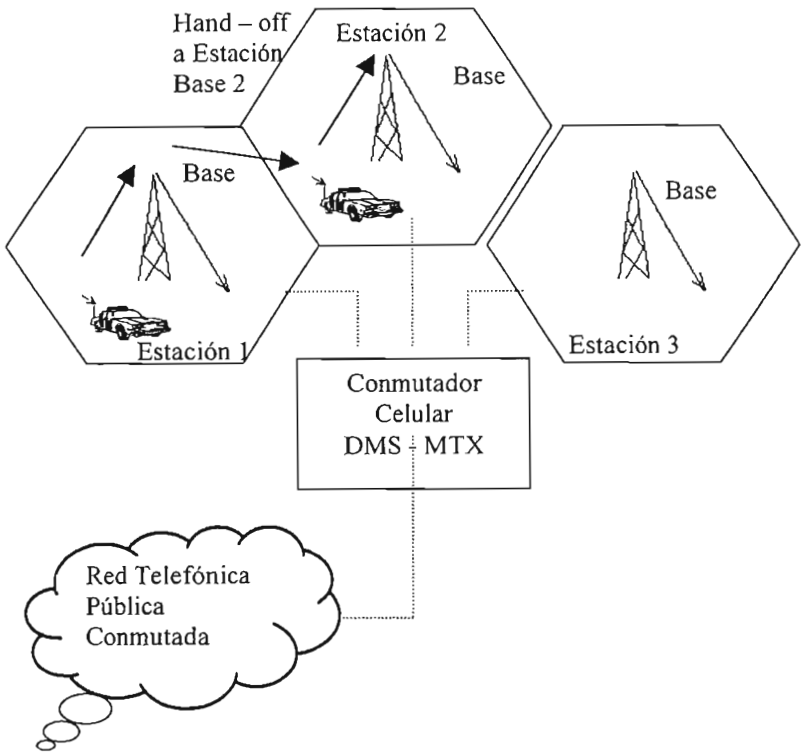


Figura 1.13 Establecimiento de llamada (hand-off) entre dos celdas adyacentes

1.5.4.3 Transferencia entre centros de conmutación

Esta es una extensión de la función de transferencia que permite conmutar también las llamadas en curso a celdas controladas por otros MSC. También gestiona la transferencia de información para servicios de abonado al MSC visitado.

Conjuntamente con la función de indicación automática de la posición del móvil, la trasferencia entre centros de conmutación permite independizar al abonado de las fronteras entre MSC. La señalización requerida se basa, como en el caso de la indicación automática de la posición del móvil, en CCITT No.7 y una parte de usuario de telefonía móvil (MTUP) específica.

También es posible la transferencia entre centros de conmutación de distintos fabricantes. Esto se hace según la norma IS-41, que también soporta el principio de minimización de trayectoria, es decir que, una vez que una llamada anteriormente transferida, es transferida a un tercer MSC, solo intervendrán en la llamada el primero y el último MSC.

1.5.5 MANTENIMIENTO DE LLAMADA

El mantenimiento de llamada consiste de órdenes, supervisión, requerimientos de llamada y transferencias, siguiendo la asignación de un canal de voz, se efectúa a través de una transmisión periódica de órdenes a las unidades móviles a fin de controlar la secuencia de transferencia, requerimientos de servicios en una llamada establecida, control de potencia, y desconexión de llamadas. Estas órdenes son originadas desde el MSC o desde la unidad de control transmitida por la unidad móvil.

La supervisión de llamada es mantenida una vez que a la unidad móvil se le ha asignado un canal de voz. La frecuencia correspondiente al canal de voz está asociada a un tono SAT, mediante el cual el transceptor monitorea la continuidad del canal de voz y hace un muestreo, revisando la presencia de tonos SAT extraños.

Los requerimientos de servicio, se consiguen mediante el uso del tono de señalización ST, el cual es utilizado para activar ciertas facilidades y funciones de señalización. Cuando un móvil requiere un servicio adicional en una llamada cursada, tal como conferencia o transferencia de llamada, esta genera una señal intermitente utilizando este tono. El transceptor del canal de voz monitorea este tono y envía un mensaje al MSC cuando esto ocurre, con lo cual el servicio requerido es entonces procesado.

1.5.6 LIBERACIÓN DE LLAMADA

Cuando el móvil que tiene una llamada en proceso, da por finalizado, envía un tono de señalización ST de 1.8 segundos. Este tono es detectado en la estación base, el canal de transmisión es desconectado y el MSC libera la llamada.

1.5.7 SISTEMA DE TASACIÓN

1.5.7.1 Principios de tasación

Normalmente, se suelen usar los principios de tasación en la PSTN también en la PLMN. Esto significa que el costo de la llamada se basa en el origen, la categoría del abonado que origina el número marcado y la categoría del abonado de destino. La tasación del abonado que llama se aplica en las llamadas hacia y desde estaciones móviles. Por ello, se puede usar la tasación normal de la PSTN sin modificación cuando se introduce el servicio de telefonía móvil.

La tasación de las llamadas móviles originadas que algunos sistemas utilizan se hace mediante *toll ticketing*. La salida de datos de *toll ticketing* la efectúa la MSC donde se ha originado la llamada. No obstante, se puede también tasar las llamadas entrantes a los abonados móviles. En tales casos, la salida de datos de *toll ticketing* será producida en el MSC donde termina la llamada.

1.5.7.2 Análisis de tasación

El análisis de tasación proporciona la base para tasar las llamadas y servicios. Uno de los datos incluidos es, en qué lugar de la red tiene que efectuarse la tasación de la llamada en cuestión. Normalmente el punto de tasación para el tráfico local es la central de origen.

En el análisis de tasación se incluye la clase de tarifa para la llamada. Un ejemplo de clase de tarifa para la llamada, es llamada dentro de la zona de tasación propia. Diferentes juegos de parámetros de entrada pueden tener por resultado la misma clase de tarifa.

Un programa de conmutación de tarifas calcula las diferentes tarifas que se han de utilizar a diferentes horas. Esto significa que cada clase de tarifa puede incluir diferentes tarifas según la hora del día y el tipo de día.

1.5.7.3 Registro de datos de tasación

Este registro incluye funciones para *toll ticketing* (TT). Tiene una lista de individuos, y se asigna uno de tales individuos a cada llamada tasada por el TT. En el CDR individual listado, se recopilan todos los datos de interés para la tasación de la llamada y se envían al bloque de TT para su salida cuando se desconecta la llamada. Los datos incluidos en los registros de TT son también suficientes para la contabilidad internacional.

1.5.7.4 Toll ticketing

El *Toll ticketing* comprende funciones para edición y salida de datos. Recibe los datos del CDR, edita los datos al formato requerido y los envía al subsistema de gestión de archivos para su salida. La salida estándar de datos TT está codificada en ISO (ASCII). A continuación se dan unos ejemplos de la información incluida en el registro de TT:

- Número del abonado que llama.
- Número del abonado llamado.
- Categoría del abonado llamado.
- Fecha y hora del comienzo de la tasación.
- Duración tasable.

- Rutas entrante-saliente
- Clase de tarifa

El subsistema de tasación ha sido especialmente adaptado a las necesidades particulares de la telefonía móvil celular, esto significa que se pueden usar diferentes formatos de registro para llamadas entrantes y salientes, pudiéndose incluir la indicación de desconexión de llamadas anormales.

CAPÍTULO II

FRAUDE TECNOLÓGICO EN EL SISTEMA DE TELEFONÍA MÓVIL CELULAR

2.1 CATEGORIZANDO EL FRAUDE EN EL SISTEMA DE TELEFONÍA MÓVIL CELULAR

El fraude constituye un serio problema para los operadores de todo el mundo, dado que las pérdidas que ocasiona ascienden a miles de millones de dólares por año. El fraude puede ser simplemente definido como "la deshonestidad de personas que causan pérdidas económicas a otros". En el caso de las telecomunicaciones, el fraude incluye la obtención y uso de productos o servicios con el intento de evadir pagos o mensualidades.

Todos los distribuidores de telecomunicaciones y los consumidores de estos servicios están expuestos al fraude de una forma u otra. El incremento del alcance y complejidad de los productos de comunicación, servicios y características, proveen nuevas oportunidades de fraude al hampa internacional.

La industria celular está trabajando para terminar este abuso, porque muchos de los abusadores son criminales fuertes, tales como la guerrilla y los traficantes de droga; el 80 por ciento de los narcotraficantes arrestados en 1998 en los Estados Unidos fueron encontrados con la posesión de teléfonos clonados,

de acuerdo al testimonio de la Administración de Esfuerzos Antidroga[1] de ese país.

La identificación consistente y la clasificación del fraude son esenciales para establecer efectivas medidas de seguridad. La siguiente estructura de clasificación ayudará a los operadores a identificar los casos de fraude, y facilitará enlaces entre ellos. La estructura define los tipos de fraude por un número de factores, esos factores son combinados por cada fraude para producir una clasificación definida. Los elementos de clasificación son los siguientes:

- Motivo.
- Maneras.
- Modo.
- Método.
- Extensión del Método.

Motivo

El motivo es el objetivo fundamental del fraude. Los motivos incluyen:

- Hacer dinero.
- Ahorrar dinero.
- Anonimato.
- Causar pérdidas o daños.
- Provisión de un servicio público.

Maneras

El fraude es usado para satisfacer los motivos o un determinado fin, y consiste de:

[1] Michael J. Riezenman (2000), p.42.

- Vender llamadas.
- Facilidad, por diseminación o suministro de productos de fraude, tener métodos y/o códigos de acceso.

Los tipos de fraude pueden generalmente considerarse como fraudes de ingreso; son los que intentan hacer dinero mediante un abuso directo de los productos y servicios de telecomunicaciones. Los fraudes de ingreso pueden estar bien organizados y vistos como un gran negocio. Los fraudes de no ingresos envuelven el uso de un servicio telefónico con el propósito de no tener ingresos, solamente con el propósito de perjudicar a los proveedores del servicio.

Modo

El modo del fraude es el método genérico de él, e incluye:

- **Suscripción.-** Obteniendo una cuenta para facilitar el fraude.
- ***Surfing*.-** El uso de servicios existentes sin autorización.
- ***Ghosting*.-** La manipulación o engaño de la red o soportando sistemas para mantener el fraude.
- **Facturación (*accounting*).-** Manipulación de los procesos o sistemas de facturación, directa o indirectamente.
- **Abuso de información.-** Obteniendo información, métodos de acceso y/o códigos, por un número de maneras diferentes, para vender o usar.

Métodos

Los métodos del fraude son la manera detallada de cometer el fraude. Estos métodos varían por producto, por servicio y por red, por lo general son los siguientes:

- Suscripción.
  - Aplicación fraudulenta (uso de detalles falsos).

  - Evasión de pagos o mensualidades (uso de nuestros detalles legítimos con intento de evadir pagos).
- *Surfing.*
  - Clonación (*Cloning*).
  - Duplicación de claves de cuenta.
  - Tarjetas de llamadas por *surfing.*
  - Abuso indirecto de los números de acceso.
- *Ghosting.*
  - Cuentas no facturadas.
  - Abuso de mantenimiento de los sistemas.
  - Supresión del CDR.
- Facturación.
  - Reclamo de clientes falsos.
  - Extensión incorrecta de una factura de por vida, estado o características específicas.
  - Reducir responsabilidades a personas involucradas.
  - Obteniendo un retorno de efectivo (emitiendo cheques falsos).
- Abuso de información.
  - Venta directa de los detalles del VIP del cliente.
  - Revelación de negocios vulnerables.

Métodos de extensión

El método puede incluir técnicas o herramientas que son usadas para extender la vida o el valor del fraude. Los más comunes incluyen:

- Rasgos amigables del abusador (*friendly fraud*)
- Vagando (*Roaming*).

2.1.1 TIPOS DE FRAUDE TECNOLÓGICO EN EL SISTEMA DE TELEFONÍA MÓVIL CELULAR

La tecnología celular, en virtud de los hechos, transmite la información a través del aire, abriéndose a las actividades fraudulentas. El fraude, en los Estados Unidos, a los proveedores (operadoras) y a sus consumidores les cuesta anualmente ya billones de dólares y, con un aumento del delito de un 50% por año.

La seguridad celular ha sido un negocio que va incrementándose en un esfuerzo para combatir el crecimiento del fraude. Los sistemas móviles celulares son vulnerables al fraude en varios puntos de la red.

Hasta ahora los elementos más frecuentemente atacados son el microteléfono, la interface de radio, y la red de señalización. Internet es un foro popular para los falseadores que en cuestión de minutos pueden comunicar a una audiencia global instrucciones detalladas sobre la forma de cometer el fraude telefónico. Desdichadamente los criminales han manejado sin problemas los métodos de detección que utilizan las operadoras y puede ser que los teléfonos celulares son más vulnerables que antes.

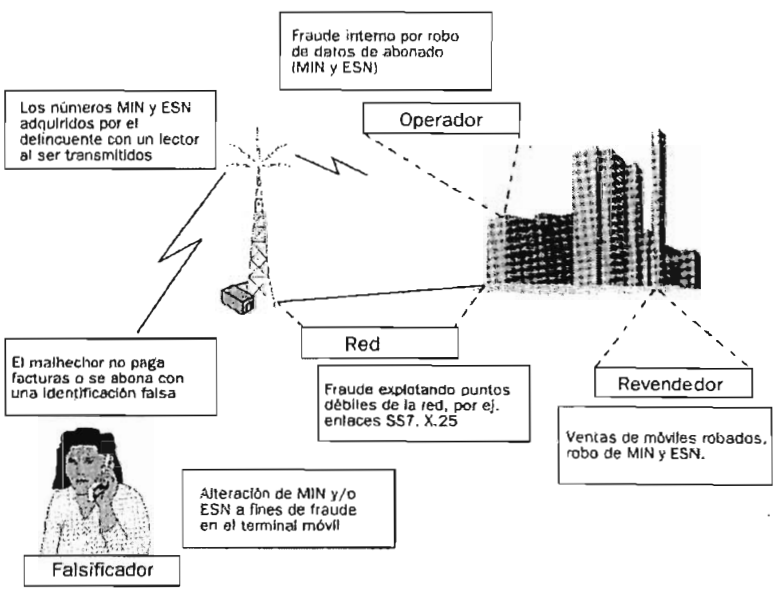


Figura 2.1 Algunos puntos vulnerables en el Sistema Móvil Celular

Caso comercial simple

Este caso comercial simple se brinda a fin de que el lector tenga una idea sencilla de las enormes pérdidas monetarias que el fraude puede ocasionar a un sistema. Para estimar esas pérdidas habrá que tener en cuenta algunos parámetros básicos, a saber:

- Cantidad de abonados: a efectos de simplificar, supongamos 100.000.
- Porcentaje de fraude en el sistema: el 10% no es una estimación excesiva en muchos sistemas.
- Tarifa fija mensual: lo normal es 40 US$/mes.
- Tarifa por llamada: lo normal es 0.20 US$/minuto.
- Tiempo de llamada por abonado: el tiempo promedio normal es de 200 minutos/mes.

Con estos datos se obtiene:

- Pérdidas sobre la tarifa mensual = 100.000*0.10*40 = 40.000 US$/mes.
- Pérdidas sobre las llamadas=100.000*0.10*0.20*200 = 400.000 US$/mes,

Esto hace un total de 440.000 US$/mes!!!

Adviértase que el cálculo anterior es para un sistema con 100.000 abonados. En el caso de operadores con 1.000.000 de abonados esa cifra será 10 veces mayor, lo que significa una pérdida por fraude de 4.400.000 US$/mes.

A este costo debe sumarse la pérdida de capacidad de la red provocada por el usuario fraudulento.

Fraude analógico

Las señales que se intercambian en teléfonos analógicos son fáciles de detectar debido al tipo de modulación que ellos utilizan, el ESN por ejemplo al marcar un número telefónico se transmite como un código multifrecuencial. De esta manera, el par ESN/MIN pueden ser interceptados por equipos detectores de señales de radio frecuencia, denominados *scanners*.

Así el impostor realiza la clonación de teléfonos celulares, con el uso de los pares de números robados.

Fraude digital

Las nuevas tendencias tecnológicas, están utilizando estándares, técnicas mucho más avanzadas con el propósito de que las señales interceptadas sean más difíciles de recuperar, como son: encripción, codificación, y actualmente dispersión espectral.

Pero, aunque estas técnicas reduzcan considerablemente el fraude, este puede ser realizado mediante el fraude interno dentro de la empresa, o tener acceso a la empresa manufacturera y obtener los ESNs, es decir alguna persona que trabaja ahí logra robar el par de números MIN/ESN.

2.1.1.1 Surfing

Un tipo de fraude que afecta en gran medida a las empresas operadoras del servicio celular es el denominado *surfing*. El *surfing*, trabaja primordialmente en zonas densamente concurridas, como por ejemplo aeropuertos y terminales de buses. Las personas que realizan esta actividad merodean a las posibles víctimas que por ejemplo están llamando con número de tarjeta, número de identificación personal, o escuchan el número que le dijo a un operador.

Los más ambiciosos surfeadores utilizan cámaras de televisión y filman los números de identificación personal cuando un usuario está pagando su factura de teléfono en lugares destinados para este fin. Como este tipo de fraude utiliza servicios existentes sin autorización, deriva dos técnicas de fraude más comunes en la industria celular, como son la suscripción fraudulenta, y la clonación (*cloning*).

2.1.1.2 Suscripción fraudulenta

El negocio más grande y más rápido que hace crecer al fraude, es la suscripción; la cual afecta tanto a las operadoras alámbricas como a las inalámbricas.

El proceso de suscripción o de registro de un usuario es el procedimiento por el cual el sistema celular sabe la situación exacta del móvil y subsecuentemente el Registro de Ubicaciones Local (HLR) con el propósito de originar o terminar una llamada.

La suscripción fraudulenta, es el fraude por identidad falsa en el momento de la subscripción del servicio. Se da por que quien hace el fraude se vale de una identidad falsa y aprovecha el teléfono celular durante el tiempo en que la operadora demora en cortar el servicio (uno o dos meses) por falta de pago.

El fraude de suscripción se puede llevar a cabo de muchos modos diferentes. La idea general consiste en engañar al sistema administrativo del operador. Los ejemplos típicos de este tipo de fraude son suscripciones contratadas con datos personales erróneos o clientes que realizan una gran cantidad de llamadas el primer mes y luego desaparecen sin pagar la factura.

Una vez que la suscripción fraudulenta ha sido obtenida, los perpetradores generarán llamadas de alto costo, antes que sean desconectados y evitar pagar la factura.

En un número de casos, esto ocurre en el servicio de *roaming* internacional, donde los perpetradores toman o envían el nuevo teléfono al extranjero y luego hacen llamadas.

2.1.1.3 Fraude administrativo

Se accede a datos de centrales y abonados y se les modifica sin autorización. Esto puede ser realizado por el propio personal del operador (fraude interno) o bien por alguien que se conecte con las líneas que entran al HLR y el MSC.

Las redes analógicas han introducido sistemas de detección como *RF Fingerprint* de posibles actividades de clonación. Mientras que las redes digitales (GSM, D – AMPS) han sofisticado los procesos de autenticación, y en el caso de GSM, la tarjeta de seguridad SIM está a disposición.

2.1.1.4 Clonación

En orden de función, un móvil debe ser registrado por la red. En redes análogas (TACS, AMPS y NMT) cada teléfono es programado con dos números de identificación. Esos son, el Número de Serie Electrónico (*ESN: Electronic Serial Number*) y el Número de Identificación del Móvil (*MIN: Mobile Identification number*). El ESN normalmente es programado en la fábrica manufacturera, identifica el equipo actual. El MIN es ingresado por el proveedor del servicio, identifica al cliente. El MIN es también el número telefónico del suscriptor. La red mantiene una tabla de validación del par ESN/MIN.

Cuando un teléfono celular intenta registrarse, este transmite el par ESN/MIN a través de la interface aérea a la estación base más cercana. Este es

retransmitido a la base de datos y si estos son marcados como válidos, se mantienen en la base de datos y el teléfono puede hacer la llamada.

Cada llamada hecha será facturada a la cuenta del cliente poseedor del par ESN/MIN utilizado fraudulentamente.

El fraude celular, en este caso, consiste en la obtención de una copia del sistema de funcionamiento de un aparato celular que opera legalmente, para transferirla a otro que se convierte en un "clon" del primero, pero que opera ilegalmente y sin control alguno, causando un grave perjuicio económico al primer usuario y a las operadoras del servicio.

En este tipo de fraude, los parámetros de identificación del teléfono celular, perteneciente a un usuario legítimo como se mencionó antes, son capturados y copiados vía *hardware* y/o *software* a otro teléfono, el cual podrá recibir y realizar llamadas sin que el usuario y la operadora lo perciban, algo así como una extensión invisible, siendo el valor de las llamadas atribuidas al teléfono legítimo.

Un teléfono celular clon es vendido en el mercado negro y generalmente usado para propósitos de crimen como narcotráfico, terrorismo, contrabando, secuestro, etc.

El fraude por clonación es el más común y que más pérdidas está causando, y esto debido a la relativa facilidad con que puede ser cometido, pues la mayoría de las operadoras en el mundo usan sistemas de telefonía celular basados en tecnologías analógicas, como AMPS, bastante usado en USA y en Latinoamérica, en el cual la transmisión de informaciones es hecha en espacio abierto sin ninguna protección.

El capturar y el copiar el par ESN/MIN del teléfono original puede hacerse de varias maneras:

- El MIN y el ESN son interceptados al transmitirse a través de la interface aérea
- Un empleado del operador celular "roba" del sistema el MIN y el ESN

Cada par ESN/MIN representa una combinación única que puede ser usada para validar una suscripción legítima. Cuando una suscripción es activada por primera vez, el par ESN/MIN quedan aparejados y almacenados en la base de datos del operador, es decir en el HLR. Desde este momento, cada vez que el terminal móvil solicita acceso al MSC, éste verifica que los números que se le han transmitido desde el terminal móvil concuerdan con los números recibidos desde el HLR. Si en efecto concuerdan, el MSC cursa la petición de servicio.

Inevitablemente, cada vez que el sistema recibe una petición de acceso, ambos números MIN y ESN son transmitidos por la interface de radio y ello sin protección. Por lo tanto, cualquiera que tenga un tipo esencial de explorador (*scanner*) de frecuencias puede interceptar las combinaciones MIN/ESN, digitalizarlas y usarlas fraudulentamente.

Figura 2.2 Un malhechor capturando combinaciones MIN/ESN al ser transmitidos por radio[1]

[1] Catharina Lundin, Binh Nguyen y Ben Ewart, (1996), p.146.

Hay dos tipos de clonación, el primero es la reprogramación de los teléfonos celulares, y el segundo es el denominado *Tumbling*.

a) Reprogramación de los teléfonos celulares

Reprogramando el par ESN/MIN de los teléfonos celulares con los números interceptados es la forma más extendida de fraude. Para capturar el par, se necesita de dispositivos tanto en *hardware* como en *software* que pueden fácilmente ser comprados en el mercado.

Típicamente en teléfonos celulares antiguos, la técnica que se utilizaba era la extracción del ESN de la memoria PROM o de la EPROM, copiándolo e insertándolo en el nuevo teléfono o clon. En los teléfonos más nuevos, los datos son removidos vía puerto serial por medio de una computadora.

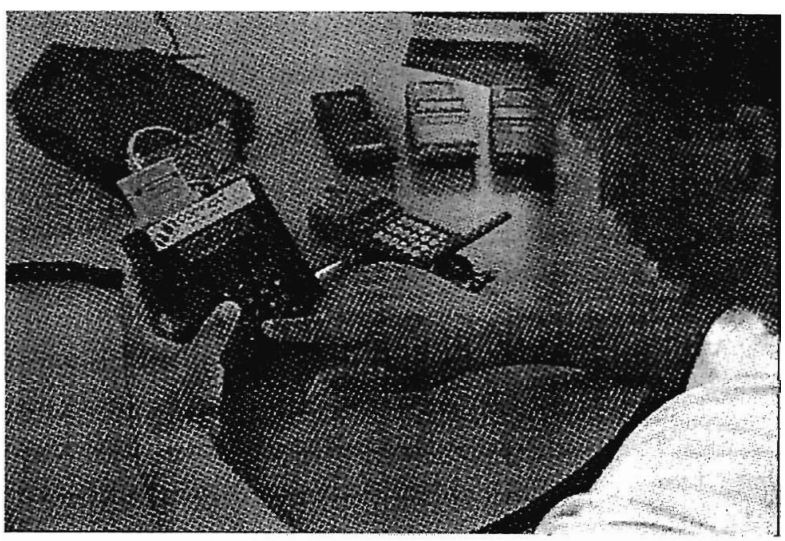


Figura 2.3 El falsificador altera el número MIN y/o ESN en el terminal móvil, para su uso indebido[1]

[1] Catharina Lundin, Binh Nguyen y Ben Ewart, (1996), p.147.

Módulo de asignación del número

El Módulo de Asignación del Número (*NAM: Number Assignment Module*) es un componente de memoria (usualmente una PROM o EPROM) que contiene el número del suscriptor, el sistema de identificación local, MIN/SCM, bloqueo, códigos, y otros datos requeridos por el sistema. Algunos teléfonos pueden ser reprogramados vía *handset*, con lo que se puede cambiar el MIN varias veces (usualmente el *software* del teléfono se bloquea después de 3 a 20 cambios). La NAM es el corazón de la factura de información.

La suma de todas las palabras en la NAM más las dos últimas deben igualar al número de ceros en los últimos dos dígitos. El radio chequea esta suma y si esta no es correcta, el radio asume que la NAM está dañada o falsificada.

Esta característica fue usada por las personas que realizan fraude (*fraudsters*) en teléfonos antiguos para engañar a los sitios de celda cuando estos realizan *roaming*. El software de los sitios de celda más nuevos está haciendo más rápidamente obsoleto este truco, pero ahora los bandidos modifican el *software* de la EPROM.

Número de identificación del móvil

El Número de Identificación del Móvil (*MIN: Mobile Identification Number*) está constituido de 34 bits divididos en dos partes. Estos son originados del número del teléfono celular de la siguiente manera:

MIN2: un número de 10 bits que se obtiene del indicativo de país, para nuestro ejemplo elegimos el 234 que es de Nigeria.

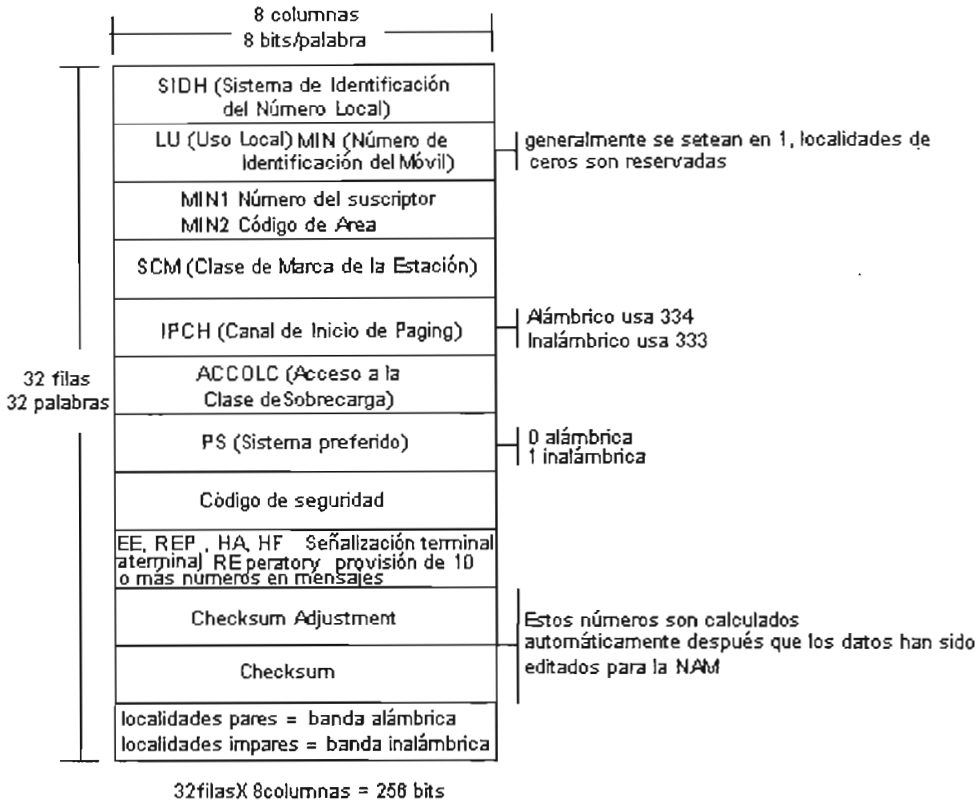


Figura 2.4 Elementos de una NAM

Tomando cada dígito en orden desde la izquierda y sumándole 9 se obtiene:

2+9=11 = 1

3+9=12 = 2

4+9=13 = 3

Así, el número 234 se convirtió en 123, a este número lo convertimos a binario y obtenemos: 0001111011

MIN1: un número de 24 bits representando por FIRST + 6 dígitos del número telefónico, dando 7 dígitos en total.

Los primeros 4 bits del MIN, llamado MIN1 es el número FIRST (indicativo interurbano). Los siguientes 10 bits son convertidos de la misma manera del MIN2, solamente los primeros 3 dígitos del número telefónico son usados.

Los 10 bits del MIN1 son codificados usando los 3 dígitos del número telefónico y convertidos de la misma manera que el MIN2. Así en MIN1 de 2-763112 podría ser:

FIRST	2		
(número telefónico)	2	763	112
(modificación de los dígitos)	(2)	652	001
(convertir cada bloque a binario)	0010	1010001100	0000000001

Así el número completo del MIN de 34 bits para (234-2)763112 es:

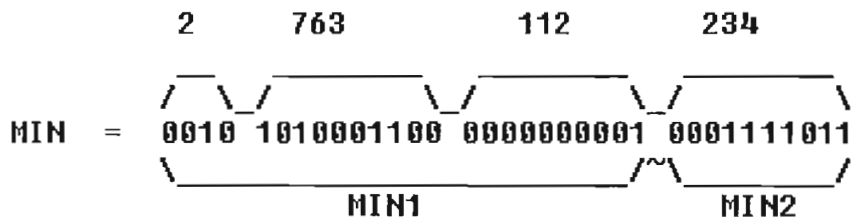


Figura 2.5 MIN completo correspondiente al número telefónico (234-2)763112

Número de serie electrónico

Dependiendo del modelo que usted tenga, el Número de Serie Electrónico (*ESN: Electronic Serial Number*) estará localizado en una memoria PROM. La PROM es programada en la fábrica manufacturera donde fue construida. El código de la memoria debería posiblemente ser obtenido desoldándola de la tarjeta del teléfono celular, poniéndola luego en un lector de PROM, y luego obteniendo un mapa de memoria del chip.

El número de serie para cada teléfono es codificado en un número binario de 32 bits. El ESN consta de tres partes: un código del fabricante, un área reservada y un número de serie asignado por el fabricante. Es un número hexadecimal de 8 bits, el cual es codificado directamente a binario, por ejemplo:

Número de serie: 821A056F

Dígitos:	8	2	1	A	0	5	6	F
ESN =	1000	0010	0001	1010	0000	0101	0110	1111

Cuando el teléfono (234-2)763112 se envía a través de la red, los datos se envían de la siguiente manera:

10101010101010101010101010101111100010010xxxxxx	dotting.word.sync.dcc
10101110xxxx00101010001100000000001xxxxxxxxxxxxx	min1
10101110xxxx00101010001100000000001xxxxxxxxxxxxx	min1
10101110xxxx00101010001100000000001xxxxxxxxxxxxx	min1
10101110xxxx00101010001100000000001xxxxxxxxxxxxx	min1
10101110xxxx00101010001100000000001xxxxxxxxxxxxx	min1
0001xxxxxxxxxxxxx0000000000011110111xxxxxxxxxxxxx	min2
0001xxxxxxxxxxxxx0000000000011110111xxxxxxxxxxxxx	min2
0001xxxxxxxxxxxxx0000000000011110111xxxxxxxxxxxxx	min2
0001xxxxxxxxxxxxx0000000000011110111xxxxxxxxxxxxx	min2
0001xxxxxxxxxxxxx0000000000011110111xxxxxxxxxxxxx	min2
0000100000100001101000000101011011111xxxxxxxxxxx	esn
0000100000100001101000000101011011111xxxxxxxxxxx	esn
0000100000100001101000000101011011111xxxxxxxxxxx	esn
0000100000100001101000000101011011111xxxxxxxxxxx	esn
0000100000100001101000000101011011111xxxxxxxxxxx	esn
etc. etc. etc. etc. etc. etc.	
xxxxx variable items, parity, SCM etc.	

Figura 2.6 Envío del número (234-2)763112 a través de la red

Este es el bloque mínimo necesario para recobrar el par de números.

Todos los bloques son de una longitud de 48 bits, y se repiten cinco veces, la información requerida está en los primeros 36 bits y en los 12 bits sobrantes donde están crc/paridad. La información más relevante o importante, esn/min1/min2, están en las primeras 3 palabras, los bloques 4 y 5 contienen los dígitos del número marcado si el teléfono está tratando de hacer una llamada.

Cada sitio de celda usa un máximo de 16 canales, de los cuales hasta 4 son canales de control, donde siempre el canal de control número 1 está disponible en cada celda.

Las torres celulares son fácilmente identificables por la plataforma triangular que usan en la parte más alta del mástil y con antenas cortas dispuestas verticalmente en cada esquina de la plataforma. Los teléfonos celulares usan una velocidad de transmisión de 10 kbps, modulación de frecuencia y se usan tanto para voz como también para datos.

b) Generación aleatoria del ESN (*TUMBLING*)

Explota la falta de autenticación en tiempo real durante el *roaming*. Ejecutando un algoritmo con una computadora conectada a una unidad móvil, se transmiten a la red celular, códigos ESN aleatorios. Cuando el ESN y el MIN enviados coinciden con el ESN y el MIN almacenados en el HLR, el sistema acepta a la unidad móvil y se establece una conexión con la central. Los teléfonos *tumbler* utilizan constantemente números de identificación diferentes, estos son difíciles de monitorear.

El uso de códigos falsos revela un punto débil dentro de la red celular. Esto permite, realizar la primera llamada desde un nuevo par ESN/MIN para pasar a través del sistema antes de verificar la validación de ese par. Esos teléfonos engañan al sistema haciéndole pensar que cada llamada hecha con los números de identificación falsos es la primera llamada sobre ese par específico.

Si la Clase de Marca de la Estación (SCM) no está fijado adecuadamente durante la programación de la EPROM, este tendrá efectos adversos en la operación del teléfono. Esto podría además reducir la seguridad del *software* para un teléfono "*tumbling*".

La dificultad en detectar las imitaciones o clones, con frecuencia se combina con el **fraude por *roaming***, o de seguimiento en las comunicaciones celulares, cuando las combinaciones MIN/ESN se roban de un área celular determinada y se utilizan en otra.

2.1.1.5 Fraude de las tarjetas de llamada

El atractivo de las tarjetas de llamada (*calling cards*) para los *fraudsters* es su movilidad; ellas pueden ser usadas desde cualquier teléfono y en cualquier lugar. Esto le provee al *fraudster* un nivel más alto de anonimato que un clon y claramente es menos riesgoso que estar caminando dentro de tu trabajo y tratar de obtener un teléfono GSM fraudulentamente.

Como el par ESN/MIN es analógico, los números de la tarjeta y sus PINs (*Personal Identification Numbers*) asociados deben ser suministrados a la red para validar al visitante antes de que la tarjeta de llamada sea procesada. El número de la tarjeta de llamada, es usado para identificarla, el emisor de la tarjeta y el portador, se imprimen en la parte frontal de la tarjeta.

El PIN es normalmente secreto y no se imprime donde quiera, pero debe ser memorizado por el portador. El portador marca un número de acceso para la tarjeta del servicio que él está usando. Luego a él se le pregunta por el ingreso del número al que desea llamar (el número de la tarjeta) y finalmente el PIN. Todo esto es hecho normalmente vía clave telefónica y con la tarjeta que sirve como referencia al visitante.

Esto significa que el portador puede fijar una llamada sin tener la tarjeta en su posesión, siempre y cuando él recuerde su número de tarjeta. Las implicaciones de la configuración de este servicio son que cualquiera quien conozca los números del portador y el PIN, puede realizar llamadas a expensas del portador.

De hecho, docenas de personas pueden hacer cientos de llamadas simultáneamente desde muchos teléfonos. Los *fraudsters* pueden obtener los números de la tarjeta y del PIN de varias maneras, incluyendo el personal junto con el servicio de administración. Sin embargo, uno de los métodos más comunes de robar los números es también el más básico; ellos miran sobre los hombros del visitante cuando él ingresa su número, o utilizando binoculares.

Esto se da generalmente en lugares muy concurridos, como son los aeropuertos y estaciones de bus, donde comúnmente existe un teléfono de pago (*payphone*) que usa estas tarjetas. Este modo peculiar de robar ha sido nombrado "*shoulder surfing*".

2.1.1.6 Robo

El celular es aprovechado para realizar llamadas antes de que sea reportado el robo físico.

Hay muchas maneras de obtener el número ESN. La primera, es extraer el ESN del teléfono original como ya lo habíamos descrito anteriormente, segundo, vía *software* introducirlo en el teléfono clon, y por último el paso más difícil, robar. Los dos primeros son obvios, pero el último es ilegal. Para capturar el par ESN/MIN de las ondas de aire, los piratas utilizan dispositivos destinados para este fin, como son:

- *Tone Scanners*.

- Demoduladores (*Black box*, *Blue box*).
- *Software* para reprogramación de los números.
- Computadoras, instaladas sobre sitios clandestinos cercanos a los teléfonos celulares o a los sitios de celda.

Figura 2.7 Equipo típico usado por los malhechores[1]

Por lo general los dispositivos anteriormente mencionados son vendidos por las empresas operadoras de servicios de telefonía móvil celular para propósitos de monitoreo y reparación y/o para las agencias que hacen cumplir las leyes, lo cual es legal. La ilegalidad se da cuando ciertas personas consiguen y utilizan estos aparatos para realizar fraude.

Los *scanners* hoy en día son capaces de recibir las bandas de frecuencia usadas por los teléfonos celulares (824-849MHz, 869-894MHz, 1.85-1.91GHz, y 1.93-1.99GHz), las unidades más antiguas pueden recibir estas frecuencias con facilidad. Además, los *scanners* más nuevos (digitales) pueden modificarse, conforme el receptor añada las bandas extras, pero estos son demasiado costos.

[1] Catharina Lundin, Binh Nguyen y Ben Ewart, (1996), p.148.

Una forma tecnológica de robar se da al aumentar la potencia de salida de una unidad móvil a fin de ocupar el canal vocal de un abonado legítimo. Una vez establecido el contacto con el sistema puede utilizarse el servicio de segundo número, que permite que la unidad móvil se conecte con un abonado al tiempo que se marca otro número. Cuando se establece la conexión con el segundo número, se desconecta el primero.

2.1.1.7 Estación base falsa

Un delincuente simula el sistema móvil celular en cuestión, con una "estación base" que obliga activamente a los terminales móviles de sus cercanías a transmitir combinaciones MIN/ESN, junto con otra información quizá secreta.

2.1.1.8 Venta de llamadas

Si bien, este se ha escuchado como un tipo de fraude, *call selling* es de hecho un término que acostumbra describir una manera en la cual cualquier técnica de fraude es explotada para generar ingresos ó ganancias.

Una ilustración de esta diferencia podría ser que probablemente un día se tropiece con un teléfono móvil clonado. Descubriendo que este trabaja de una manera en la que no va a ser facturado por las llamadas que haga, se podrá en un momento de debilidad, llamar a un poco de amigos y a lugares distantes. En este punto la persona se convertirá en un "s*ervice fraudster*".

Esta rutina envuelve a la persona, quien realiza poco a poco venta de llamadas, a vecinos, empieza a obtener dinero extra y llega a tal punto en que él ha formado su propia sociedad llamada " *revenue fraudsters*".

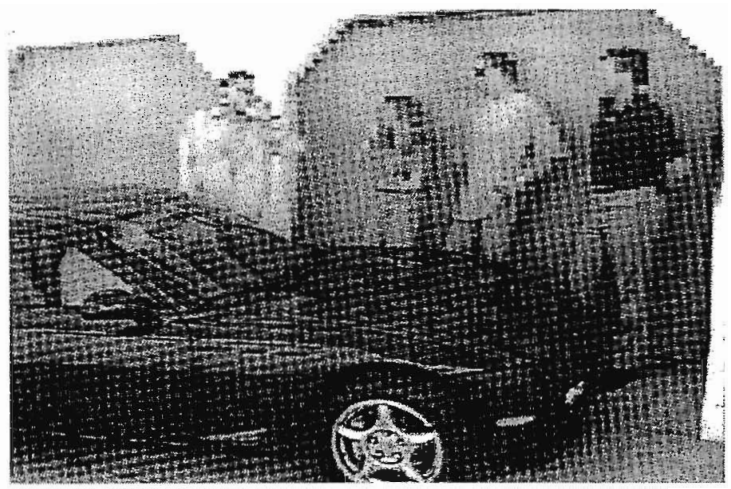


Figura 2.8 Venta de servicios celulares a precios reducidos por parte de " operadores" ambulantes, " vendedores de llamadas" [1].

2.1.1.9 Fraude subsidiado

Algunas proveedoras del servicio celular subsidian teléfonos con la condición de que los suscriptores mantengan con la compañía su contrato, por un período específico, típicamente un año. Pero lo que sucede a veces es que los teléfonos son activados en otras redes de la operadora. Un distribuidor, por ejemplo, quien ha comprado un lote de teléfonos a bajo precio de alguna operadora, él puede venderlos a alguna persona que no es afiliada a esa operadora.

En Latinoamérica, esa persona, que puede ser un vendedor no necesariamente puede estar en el mismo país del distribuidor. El resultado, la operadora pierde el dinero invertido por el subsidio de esos teléfonos.

[1] Catharina Lundin, Binh Nguyen y Ben Ewart, (1996), p.149.

2.2 ESQUEMAS PARA PREVENIR/DETECTAR EL FRAUDE

Algunas de las maneras que los proveedores del servicio celular utilizan para combatir el fraude son:

- Encripción.
- Bloqueo.
- Verificación del usuario.
- Análisis de los parámetros de tráfico.

2.2.1 ENCRIPCIÓN

Una de las maneras más eficaces para prevenir el fraude, es la encripción. La encripción tiene dos beneficios claves:

- Imposibilita a las personas que hacen fraude, robar el par ESN/MIN y
- Previene escuchar a escondidas (*eavesdropping*) las llamadas celulares.

La encripción es muy utilizada en teléfonos celulares digitales, porque ellos usan números binarios 1s y 0s que pueden ser codificados y decodificados sin dificultad. Con la encripción se pueden desarrollar claves, es decir algoritmos de *software* o unos dispositivos de *hardware* que codifican y bloquean el acceso de información. Solo si la misma clave o una clave asociada puede descifrar la información.

Las señales analógicas, sin embargo son extremadamente difíciles y caras para ser encriptadas. Puesto que muchos teléfonos celulares son típicamente analógicos, la encripción no es ampliamente usada en este tiempo. La industria celular y sus consumidores están gradualmente emigrando hacia la aplicación digital, de tal forma que la encripción se incrementará rápidamente.

Otro obstáculo para la encripción ha sido la oposición del FBI y la Agencia de Seguridad Nacional en los Estados Unidos, por cuanto los criminales podrían codificar sus comunicaciones. Esto podría impedir a estas organizaciones estar en la capacidad de conducir seguimientos satisfactorios en las conversaciones sobre teléfonos celulares.

De acuerdo a esto, se ha creado un chip específico denominado "*Clipper Chip*", sobre el cual se puede encriptar la información con una cierta combinación (como una combinación de caja fuerte), de esta manera la comunicación solo puede ser decodificada con la clave respectiva. El chip *Clipper* utiliza una clave de 80 bits para cifrar tanto datos como voz digitalizada y se instalará en los equipos de comunicación de datos propiedad del gobierno de los Estados Unidos, tales como computadoras, módem, fax y teléfonos.

El chip de cifrado de datos, *Clipper,* permitirá que las agencias federales y las empresas, se protejan de los intrusos que intenten violentar los sistemas informáticos y de los criminales.

Este es un coprocesador de cifrado de 12Mbits/seg diseñado por Mykotronix y fabricado con técnicas VLSI. El chip está protegido para evitar que pueda ser abierto, de forma que no se puede estudiar su diseño (ingeniería inversa). Lo desarrollaron conjuntamente la Agencia Nacional de Seguridad (*NSA: National Security Agency*) y el Instituto Nacional de Normalización y Tecnología.

El propósito de utilizar esta manera de encripción es que las organizaciones gubernamentales y otras afines puedan decodificar esas comunicaciones conociendo la combinación. Esto mejora su capacidad de escuchar las conversaciones encriptadas sobre teléfonos celulares cuando sea necesario.

El uso de este chip, es muy controvertido. A pesar de que se ha utilizado un algoritmo secreto, se plantean dudas acerca de sí su implementación ha sido la correcta, y si el algoritmo de cifrado tiene una puerta-falsa para descifrar los mensajes que sólo conocen las personas que lo han diseñado.

2.2.2 BLOQUEO

Las operadoras para protegerse, bloquean a los visitantes de alto riesgo de ciertos tipos de llamadas. Por ejemplo, ellos permitirán hacer llamadas internacionales solamente con las principales tarjetas de crédito que permite el operador. Otro tipo de bloqueo es permitir hacer llamadas de larga distancia solamente a las personas que tienen buenos estados de cuenta.

2.2.3 VERIFICACIÓN DE USUARIOS

Varias compañías han desarrollado el método de verificación de usuarios. Por lo general esta medida de prevención contra el fraude dispone de tres características para la identificación del usuario:

- El usuario debe ingresar o decir su clave (*password*)
- Luego el sistema utiliza el método de verificación de voz, el cual requiere que el usuario diga su clave, con el propósito de compararla con una previamente registrada.
- Acceso prepago (*prepaid*), donde los usuarios pagan en adelanto para cargas de larga distancia.

2.2.4 ANÁLISIS DE TRÁFICO

En la actualidad, el método más ampliamente usado para detectar el fraude celular es el análisis de tráfico.

En muchos casos una inteligencia artificial, *software,* se usa para detectar patrones de llamadas sospechosas, tales como crecimientos repentinos de las longitudes típicas de llamadas, o un incremento repentino de las llamadas internacionales. El *software*, determinará si esto es posible físicamente, cuando el suscriptor está haciendo una llamada desde un sitio típico, basado en la localización y en el tiempo desde que la llamada previa se produjo. Si ocurre cualquier conducta sospechosa, el software hará producir un sonido de alarma, y los investigadores podrán utilizar esta información como una evidencia de fraude.

Los nuevos servicios de *hardware* ayudan constantemente a rastrear el estado de los teléfonos celulares, tal que los parámetros sospechosos pueden ser detectados. El proceso de detección, también puede darse, introduciendo un sofisticado sistema que analiza variaciones de parámetros típicos en tiempo real.

Si los nuevos parámetros, no coinciden con los que se utilizan como referencia, la llamada será bloqueada y otras operaciones adicionales del sistema. Algunas de las compañías que han desarrollado (o están desarrollando) el software para detectar patrones de tráfico sospechosos son:

- GTE una empresa conjunta entre *Pacific Telesis y Electronic Data Systems y Coral Systems Inc.*
- AT&T junto con *Coral Systems Inc.*

2.3 BREVE DESCRIPCIÓN DE LOS SERVICIOS DE DETECCIÓN/ PREVENCIÓN DEL FRAUDE

La principal meta de las medidas de seguridad sobre sistemas móviles celulares es asegurar la privacidad de las transmisiones y metadatos, de intercepciones que permitan usos no autorizados del sistema.

Capacidades limitadas de las tecnologías más antiguas como las analógicas, abren sitios o lugares más vulnerables y ofrecen menos armas para combatir el fraude celular. Al mismo tiempo, las nuevas tendencias tecnológicas, como la digital, incrementan la complejidad de las redes al manejarlas y en sus costos de mantenimiento, pero en un futuro cercano ofrecerán evitar grandes pérdidas y lo más importante, evitar el fraude.

2.3.1 MEDIDAS DE PREVENCIÓN DEL FRAUDE ANALÓGICO/DIGITAL

Debido a las dificultades tecnológicas en la encripción de señales y sistemas analógicos, todas las comunicaciones son transmitidas en "claro". Esto no es tan importante para los aficionados de la radio que interceptan las conversaciones de los teléfonos celulares con un *scanner.*

Debido a las limitaciones inherentes de la tecnología analógica hay técnicas de prevención para redes analógicas sumadas a las medidas generales listadas anteriormente. En contraste las nuevas redes digitales ofrecen abundantes capacidades de seguridad.

Muchas técnicas para combatir el fraude están siendo recomendadas, y es así como algunas compañías ya están usando algunos de estos sistemas.

2.3.2 RECOMENDACIONES SOBRE LOS SERVICIOS DE PREVENCIÓN DE FRAUDE DEPENDIENTES DEL SISTEMA DEL OPERADOR

El objetivo de esta sección es brindar al lector una idea sencilla acerca de los Servicios de Prevención de Fraude que pueden recomendarse en distintas situaciones. Tal como se indicó anteriormente, es difícil generalizar, siendo fundamental realizar una cuidadosa investigación en cada caso. Aquí se mencionan las características típicas de distintos sistemas y las recomendaciones para cada uno de ellos.

Es importante observar que no es el sistema el que limita los servicios preferibles y disponibles, sino las normas de las estaciones móviles del sistema.

Estaciones móviles de modo doble = normas IS-54B e IS-136
Estaciones con capacidad de autenticación = normas IS-54B, IS-91 e IS-136
Estaciones móviles analógicas antiguas = norma EIA/TIA 553

Sistema D-AMPS y AMPS fundamentalmente con estaciones móviles de modo doble o capaces de Autenticación

Servicios de prevención de fraude recomendados para sistemas que utilizan *roaming* automático:

- Autenticación.
- *RF Fingerprint*.
- Sistema de Detección de Fraude Celular (*CFDS: Cellular Fraud Detection System*).

Servicios de prevención de fraude para sistemas que solo utilizan *roaming* manual:

- Verificación y Validación.
- Notificación automática de no coincidencia del ESN.
- Bloqueo de llamadas ante la detección de fraude.
- Detección de actividad fraudulenta.
- Desconexión de llamadas.
- Inhabilitación de llamadas por celda individual (solo en caso de muy alto porcentaje de fraude en emplazamientos de celdas especiales).
- Protección contra el uso indebido del puerto de roamer.

- Verificación del número de serie y el número de estación móvil.
- *RF Fingerprint.*
- CFDS.

Sistemas D-AMPS y AMPS fundamentalmente con estaciones móviles analógicas antiguas

Servicios de prevención de fraude recomendados para sistemas que utilizan *roaming* automático:

- Autenticación.
- *RF Fingerprint.*
- Bloqueo Automático de Llamadas (*ACB: Automatic Call Blocking*).
- CFDS.

Servicios de prevención de fraude para sistemas que solo utilizan *roaming* manual:

- Verificación y Validación.
- Notificación automática de no coincidencia del ESN.
- Bloqueo de llamadas ante la detección de fraude.
- Detección de actividad fraudulenta.
- Desconexión de llamadas.
- Inhabilitación de llamadas por celda individual (solo en caso de muy alto porcentaje de fraude en emplazamientos de celdas especiales).
- Protección contra el uso indebido del puerto de roamer.
- Verificación del número de serie y el número de estación móvil.
- *RF Fingerprint.*
- CFDS.

Sistemas AMPS solamente, fundamentalmente con estaciones móviles analógicas antiguas.

Servicios de prevención de fraude recomendados para sistemas que utilizan *roaming* automático:

- Autenticación (es importante la rápida implementación de la autenticación, de modo que el sistema pueda migrar hacia la prestación de autenticación total con las nuevas estaciones móviles ofrecidas actualmente).
- *RF Fingerprint.*
- ACB.
- CFDS.

Servicios de prevención de fraude para sistemas que solo utilizan *roaming* manual:

- Verificación y Validación.
- Notificación automática de no coincidencia del ESN.
- Bloqueo de llamadas ante la detección de fraude.
- Detección de actividad fraudulenta.
- Desconexión de llamadas.
- Inhabilitación de llamadas por celda individual (solo en caso de muy alto porcentaje de fraude en emplazamientos de celdas especiales).
- Protección contra el uso indebido del puerto de roamer.
- Verificación del número de serie y el número de estación móvil.
- *RF Fingerprint.*
- CFDS.

2.3.2.1 Lista de servicios de prevención de fraude

En la tabla 2.1 se indican los sistemas y Servicios de Prevención de Fraude disponibles en la mayoría de productos de las distintas empresas proveedoras, al tiempo que se describe para qué tipo de fraude resultan efectivos los distintos servicios.

Es difícil medir exactamente la eficiencia de un determinado servicio en comparación con otro en lo que respecta a un tipo específico de fraude, dado que eso se basa en distintos factores y depende en gran medida del operador y del mercado.

Tipos de fraude Servicios de Prevención/Detección de Fraude	Clonación	Generación Aleatoria del ESN/MIN	Robo	Fraude de suscripción y administrativo
Verificación	Sí	Sí	No	No
Validación	Sí	Sí	No	Fraude Suscripción
Sistemas de perfil de usuario	Sí	Sí	No	Fraude Suscripción
Autenticación	Sí	Sí	Sí	Fraude Administrativo
Bloqueo automático de llamadas	Sí	Sí	No	No
Notificación automática de no coincidencia del ESN	Sí	Sí	No	No
Detección de actividad fraudulenta	Sí	Sí	Sí	No
Bloqueo de llamadas ante la detección de fraude	Sí	Sí	Sí	No
Desconexión de llamadas	Sí, si se detecta	Sí, si se detecta	Sí, si se detecta	No
Inhabilitación de llamadas por celdas individuales	Sí, si se detecta	Sí, si se detecta	Sí, si se detecta	No
Protección contra el uso indebido del puerto de roamer	Sí, para sistemas de *roaming* manual	Sí, para sistemas de *roaming* manual	No	No
Verificación del número de serie y el número de estación móvil	Sí, para sistemas de *roaming* manual	Sí, para sistemas de *roaming* manual	No	No
Sistema de detección de fraude celular (CFDS)	Sí	Sí	Sí	Sí, para ambos
Huella digital de RF	Sí	Sí	Sí	Sí, para ambos

Tabla 2.1 Lista de Servicios de Prevención de Fraude disponibles en varios productos

2.3.2.2 Descripción de los servicios

Verificación

Verificación es un servicio que permite a las operadoras locales poder escoger dos opciones, bloquear o restringir vagantes (*roamers*) en mercados de alto tráfico, automáticamente verificando a un visitante (*caller*) a través de un número de identificación personal (PIN) o por un experimentado servicio.

Para determinar la autenticidad de los *roamers*, verificación utiliza una Respuesta de Voz Integrada (IVR). El IVR acepta estándares de entrada de tono doble multifrecuencia (DTMF) de los teléfonos de *roamers*, y puede apuntar a un *roamer* para un PIN. El IVR apuntará rápidamente al *roamer* para sus MINs a menos que este sea automáticamente capturado cuando el mercado de servicio pase el número de identificación automático (ANI).

Validación de llamadas

Validación bloquea las llamadas fraudulentas usando *roaming* antes de que ellas sean conectadas. La función de registro de llamadas proporcionada por estos servicios facilita la entrega automática de llamadas, permitiendo a sus clientes recibir llamadas mientras realizan *roaming*. Validación maximiza la rentabilidad proveyendo y registrando sin interrupciones el servicio para validar roamers. Además ofrece protección contra fraudes debido a *tumbling*, desactivando las llamadas.

Validación ha desarrollado un algoritmo exclusivo que ha eliminado prácticamente el problema de alteración numérica (*tumbling*) de los números MIN o ESN. El administrador de fraude bloquea las llamadas fraudulentas basándose en ciertos umbrales específicos que admiten usuarios con multi-NAM.

Sistema de perfil de usuario

Cada usuario individualmente tiene un perfil de llamadas particular, para estar en la capacidad de reconocer el comportamiento de ese particular cliente. Esto es importante porque mediante este procedimiento el sistema puede saber si el usuario es legítimo o no, analizando los cambios en el comportamiento de su perfil. Cada perfil es multi-dimensional, los cuales incluyen los siguientes atributos de llamada: destinos diferentes, duraciones de llamada diferentes, agregado de duración de llamadas, hora del día, fecha de la semana, etc.

Autenticación

Los orígenes de la autenticación se remontan a los primeros años 1990, en que se creó él IS-54 (es estándar de la interface de radio TDMA de EE.UU.). Cuando se práctica el método de autenticación, la identidad de un terminal móvil no es aceptada automáticamente por el simple hecho de ser correctos sus números MIN, ESN o PIN.

El terminal móvil debe ser en cambio autentificado antes de que sus llamadas sean procesadas. El procedimiento de autenticación, que permite que el terminal móvil sea aprobado sin transmitir ningunos datos secretos, se consigue pidiendo el centro de autenticación (AC), o el centro MSC, al terminal móvil que emita una contraseña numérica para la cual este último debe llevar a cabo cálculos avanzados cuyos resultados son exactos solamente si el terminal móvil ha sido programado con la información secreta correcta.

Esta moderna tecnología utiliza el algoritmo CAVE avanzado para validar la identidad de las estaciones móviles. La función de autenticación (*authentication*) se basa en números secretos de 6 a 26 dígitos (claves A: *A-Key*) almacenados en la estación móvil y en el HLR/AC. La autenticación evita los tipos de fraude por clonación, robo, y generación aleatoria del ESN, así como el fraude de suscripción interno cometido por personal del operador. La autenticación es exitosamente utilizada por muchos de los operadores más importantes del mundo, y su evolución la ha conducido a ser la norma mundial para evitar el fraude celular en los sistemas AMPS y D - AMPS.

La clave A, junto con otros parámetros, se ingresa al algoritmo CAVE que calcula una respuesta (AUTHR) tanto en la estación móvil como en el HLR. Luego la red verifica que los dos resultados sean iguales. Si no hay coincidencia la estación móvil no se conecta con el sistema. La clave A nunca se envía a través de la interface aérea.

El servicio brinda total soporte al *roaming* entre sistemas móviles, si ambos tienen implementada la autenticación. Aunque el servicio de autenticación requiere estaciones móviles que cumplan con la norma provisoria 54, revisión B (IS-54 Rev. B) o posterior (IS-91 o IS-136), no exige canales de tráfico digitales, de modo que una red analógica (con canales vocales analógicos solamente) también brindará soporte a la autenticación.

La función de autenticación comprende varios procedimientos, tal como se describe a continuación:

- **Conminación global a ejecutar algoritmo.** Durante la fase de acceso al sistema, éste exige al terminal móvil que ejecute el algoritmo CAVE usando su clave A y la información obtenida del sistema a través de la interface de radio. El resultado se devuelve al sistema para su validación.
- **Conminación única.** Una conminación única a elaborar una contraseña, que es iniciada por el AC o por el MSC, valida un terminal móvil individual usando un conjunto de datos que es único para dicho terminal. La petición se lleva a cabo al establecerse la llamada o al recibirse una petición en cualquier momento.
- **Conminación a estación base.** Conminando a la estación a elaborar la contraseña, el terminal móvil puede validar dicha estación base protegiéndose con ello contra intentos de fraude por parte de estaciones base falsas.
- **Actualización de Datos Secretos Compartidos.** La actualización de Datos Secretos Compartidos, SSD, puede hacerse como cuestión de rutina, o cuando hay razones para sospechar que dichos datos han sido penetrados.
- **Secreto de voz.** El Secreto de Voz, es una función que complementa los procedimientos de autenticación. Esta función cifra la conversación de la comunicación en su trayecto por la interface de radio entre un terminal móvil digital y una estación base. Un secreto de voz eficiente y conveniente es posible por medio del acceso TDMA y utilizando el algoritmo CAVE.

- **Cifrado de mensajes de señalización.** El Cifrado de Mensajes de Señalización, SME, que es otro complemento de los procedimientos de autenticación, protege la información del abonado cifrando un subconjunto seleccionado de mensajes de señalización entre la estación base y el terminal móvil.

Con el despliegue de la autenticación el fraude quedará limitado a dos categorías: fraude de suscripción y robo físico del teléfono. Estos dos tipos de fraude no pueden probablemente eliminarse nunca, pero en cambio puede tratarse y prevenirse más fácilmente que el fraude de clonación. Está seguro que su operadora inalámbrica tiene las seguridades adecuadas contra la clonación. Use un teléfono capaz de usar autenticación (*authentication capable phone*). Si no sabe si su teléfono es autentificable puede revisar la siguiente lista en el ANEXO A.

Bloqueo automático de llamadas

El servicio de bloqueo automático de llamadas (ACB) impide, a un usuario fraudulento que no cuente con el número PIN del abonado, originar llamadas desde una estación móvil robada o clonada. Esto ha demostrado ser sumamente eficaz contra los tipos de fraude por clonación y generación aleatoria de ESN/MIN.

El servicio de ACB puede utilizarse para todo tipo de estaciones móviles y se basa en un código de número de identificación personal (PIN) de 4 dígitos que debe ingresar el abonado al efectuar la primera llamada después de haber apagado la estación móvil. Si se marca un número PIN erróneo el abonado no podrá efectuar la llamada telefónica. El servicio se vuelve a activar automáticamente tan pronto como el abonado apaga la estación móvil.

Notificación automática de no coincidencia del ESN

El principal beneficio de este servicio es que informa al operador acerca de la no coincidencia del ESN, permitiéndole tomar medidas inmediatas a fin de encontrar la causa de ella, lo que conducirá a una mayor satisfacción del cliente. De lo contrario, los clientes legítimos se quejarán al operador porque no reciben servicio.

Esta notificación advierte al operador de que se ha producido una no coincidencia, para que pueda solucionar la situación más rápidamente. El servicio de notificación automática del ESN permitirá que todos los eventos de no coincidencia del ESN detectados por el sistema sean enviados a un dispositivo de Entrada/Salida (especificado por el operador) exclusivamente dedicado a la notificación de esos eventos. Este servicio es aplicable a los eventos de no coincidencia del ESN detectados en el HLR y el MSC.

Bloqueo de llamadas ante la detección de fraude, y detección de actividad fraudulenta

Los servicios de detección de actividad fraudulenta y bloqueo de llamadas ante la detección de fraude son herramientas efectivas para detectar y combatir el fraude celular. Estos servicios detectan en un rango muy amplio de actividades fraudulentas que pueden causar los tipos de fraude por clonación, generación aleatoria de ESN/MIN y robo.

El servicio de Detección de Actividad Fraudulenta (FAD) es una función de vigilancia on line que reporta posibles eventos fraudulentos relacionados tanto con las llamadas como con las actividades de suscripción. Dicho servicio identifica llamadas específicas y otras actividades que podrían indicar el uso fraudulento del sistema.

Cuando se detectan estos eventos se registran los elementos que probablemente pudieran interpretarse como fraude. Esos eventos pueden enviarse a un dispositivo de Entrada/Salida (E/S), donde una función de reporte genera un listado que contiene el número de la estación móvil y un código de motivo para cada evento. La otra posibilidad es que cuando se detecte y verifique un fraude se active automáticamente el bloqueo de llamadas ante la detección de fraude. Los futuros intentos de acceso por parte del abonado bloqueado se enrutarán automáticamente hacia un anuncio o hacia el personal de atención al cliente, a efectos de tomar las medidas pertinentes.

Desconexión de llamadas

El servicio de desconexión de llamadas proporciona a los operadores comandos para desconectar las llamadas que se consideran fraudulentas y les posibilita supervisar las llamadas prolongadas, que tienen mucha mayor probabilidad de ser fraudulentas.

Si ese es el caso, el operador puede terminar la llamada inmediatamente, así como todas las derivaciones de la misma, minimizando de este modo cualquier pérdida adicional asociada con la llamada. Este servicio también incluye la supervisión de llamadas prolongadas, lo que permitirá a los operadores monitorear y reaccionar ante llamadas que se extiendan durante un período anormalmente extenso. Las llamadas prolongadas detectadas pueden desconectarse en forma manual, utilizando comandos, o automáticamente mediante el servicio de desconexión de llamadas.

Inhabilitación de llamadas por celda individual

El servicio de inhabilitación de llamadas por celda individual permite a los operadores evitar la iniciación de llamadas en una celda, según el Troncal Móvil de Líneas Bidireccionales (MBLT) entrante.

La mayor ventaja de este servicio es que posibilita al operador evitar rápidamente la iniciación de llamadas desde un emplazamiento de celda en que muchas estaciones móviles se comportan de modo fraudulento. También puede utilizarse, por ejemplo, en emplazamientos de celdas especiales, durante la noche, en áreas en que el fraude es un problema muy común.

Protección contra el uso indebido del puerto de roamer

Un MSC brinda soporte a las llamadas realizadas a los abonados móviles que están efectuando *roaming* en su área o áreas de servicio, designando en el sistema uno o más puertos para que sirvan como puertos de roamer. El servicio de protección contra el uso indebido del puerto de roamer evita el uso fraudulento de dicho puerto, asegurando que las llamadas se cursen hasta su destino solo si el abonado móvil está en el área atendida por el mismo.

Verificación del número de serie y el número de estación móvil

El servicio de verificación del número de serie y el número de estación móvil reduce la cantidad de número de llamadas fraudulentas, así como la cantidad de solicitudes de actualizaciones de localización y validación innecesarias procesadas por el sistema local del abonado, es decir, el HLR.

Dado que cada estación móvil es única, puede utilizarse un proceso de verificación para determinar si se le permite acceder a los servicios prestados por el sistema celular.

Huella digital de radio frecuencia

PhonePrint ha cambiado la manera de aproximarse al fraude de la industria celular. Así con solo un sistema disponible como, *PhonePrint* autentifica a los usuarios legítimos y desconecta a los clonados. Este sistema es fácil de instalar y fácil de implementar. *PhonePrint* protege la base de entrada de los suscriptores de la operadora desde los equipos más antiguos hasta los últimos teléfonos de hoy en día.

Corsair Communications patentó este servicio, mediante la gran experiencia en el diseño de sistemas distribuidos, infraestructura de redes celulares y la ingeniería de radio frecuencia. Dos huellas digitales (*fingerprints*) no son semejantes, dos señales de radio no son iguales, tampoco. *PhonePrint* usa una tecnología de señal inteligente conocida como huella digital de radio frecuencia (*RF Fingerprint*) para detectar y desconectar llamadas fraudulentas desde teléfonos clonados dentro de pocos segundos. A través de técnicas de procesamiento de señales, originalmente desarrolladas por el gobierno de los EE.UU. para aplicaciones de inteligencia, los ingenieros de *Corsair* han alcanzado la más alta resolución de datos con los mejores algoritmos de análisis de señales que los expertos nunca han pensado como una solución que entregue una seguridad y solución viable para el fraude de clonación celular.

Este análisis genera un único patrón de señal asociada con cada teléfono, llamada *RF Fingerprint*. *PhonePrint* captura la señal del clon, lo compara con la huella digital de un usuario legítimo, y desconecta la llamada. El resultado: los teléfonos de los usuarios son seguros, y la red celular, también. *PhonePrint* para aproximarse al fraude de una manera satisfactoria utiliza los siguientes requerimientos:

- Uso de la huella digital alta – exacta para distinguir usuarios legítimos de clonadores.

  - RF es rápido y confiable.
- Aplicado en dondequiera, todo el tiempo
  - Huella digital (*fingerprint*) para cada suscriptor
  - Revisión o chequeo de cada llamada
- Esta aproximación requiere una arquitectura distribuida intensiva de datos.

Este sistema es transparente para los usuarios celulares, sin requerir PINs, sin retrasos en la iniciación de la llamada, o cambios en el aparato celular.

La validación de resultados comerciales, son eficaces:

- > 90% efectivo contra clones con <1% de impacto negativo sobre buenos clientes
- > 100 millones de intentos de llamadas fraudulentas terminadas hasta la fecha
- Desplegado en los Estados Unidos e Internacionalmente sobre 40 mercados

2.4 MEDIDAS DE PREVENCIÓN PARA EDUCAR A LOS CONSUMIDORES

Todos los usuarios de los teléfonos celulares deberían saber, que el fraude puede ser evitado tanto en términos de prevención como en la detección. Los consumidores pueden detectar el fraude mediante:

- Mirando una actividad no usual en su factura de llamadas mensual.
- Reportando recibos frecuentes de números erróneos o desconexiones, los cuales pueden indicar que alguien más está usando sus números del móvil.
- Preguntando al proveedor inalámbrico o alámbrico, si puede eliminar los servicios de larga distancia nacional e internacional previo acuerdo.

- Si se sabe de algún suscriptor sospechoso, repórtelo inmediatamente al proveedor del servicio o a su agencia contra el fraude.

Los consumidores pueden ayudar a prevenir el fraude mediante:

- Bloqueando sus teléfonos o retirando las antenas del *handset* (para evitar llamar la atención del vehículo).
- Protegiendo documentos muy importantes, como acuerdos de suscripción, los cuales incluyen números de serie electrónico. No deje estos contratos en lugares inseguros tales como la guantera en el compartimiento del carro, y en especial en lugares peligrosos durante mucho tiempo.
- Reportar inmediatamente un teléfono robado, a la operadora del servicio móvil celular.
- No dejar su teléfono dentro de su auto. Destruya todas las etiquetas de las cajas de sus teléfonos. Ciertos números de esas cajas pueden ser usados para ser clones.

CAPÍTULO III

DESCRIPCIÓN DE LOS SERVICIOS DE DETECCIÓN, PREVENCIÓN DEL FRAUDE TECNOLÓGICO

La dirección para la estrategia de prevención del fraude en la industria celular, es especificada dentro del programa de Administración Total del Fraude de la Asociación de Industrias de Telecomunicaciones Celulares (*CTIA: Cellular Telecommunications Industry Asociation*), la cual estimula a las operadoras a:

1. Reforzar a la empresa mediante el despliegue IS-41 para validación pre-llamada, implementar cambios y operaciones revisadas para mitigar los ataques *hackers*, y practicar estrictos procedimientos en la activación de suscriptores.
2. Activar la seguridad de los teléfonos, los cuales son autenticables y proveer seguridad contra el ataque de los ESNs, como es reconocido por el Programa de Certificación de la CTIA.
3. Instalar sistemas de perfiles de usuario (*customer profiling system*) para detectar clonación.
4. Desplegar sistemas de prevención como huellas digitales de radio frecuencia (*RF Fingerprint*) y verificación de procesos de *roaming*; y
5. Facilitar el despliegue de Autenticación, la última herramienta contra el fraude en la industria celular.

En la tabla 3.1, se describen las dos principales opciones para erradicar el fraude, detección y prevención, además de los servicios básicos que utilizan.

Servicios de Prevención/Detección de Fraude	Tipos de Medida	Servicios Básicos
1. – Verificación de *roamers*	Previene	5, 9
2. – Validación de *roamers*	Previene	5, 9
3. – Sistemas de perfil de usuario	Detecta	6, 8, 12,13
4. – Autenticación	Previene	
5. –Bloqueo automático de llamadas	Previene	
6. - Notificación automática de no coincidencia del ESN	Previene	
6. – Detección de actividad fraudulenta	Previene/Detecta	
8. – Bloqueo de llamadas antela detección de fraude	Previene/Detecta	
9. – Desconexión de llamadas	Previene	
10. – Inhabilitación de llamadas por celdas individuales	Previene	
11. – Protección contra el uso indebido del puerto de *roamer*	Previene	
12. – Verificación del número de serie y el número de estación móvil	Previene	
13. – Sistema de detección defraude celular (CFDS)	Previene/Detecta	
14. – Huella digital de RF	Previene/Detecta	1, 2,5, 6, 8

Tabla 3.1 Lista de Servicios de Prevención/Detección de Fraude

3.1 VERIFICACIÓN Y VALIDACIÓN DE ROAMERS

3.1.1 VERIFICACIÓN

Verificación es un servicio que permite a los operadores locales poder escoger dos opciones: bloquear o restringir *roamers* en mercados de alto tráfico, automáticamente verificando a un visitante a través de un Número de Identificación Personal (*PIN: Personal Identification Number*) que se requerirá cada vez que se realice una llamada de larga distancia, ya sea nacional o internacional, desde la ciudad de origen o desde cualquier otra.

El servicio de verificación le proporciona flexibilidad y control sin precedentes al sistema, así se puede evitar la manipulación de números marcados de alto tráfico.

3.1.1.1 Beneficios

Las soluciones de fraude deberían permitir a los suscriptores vagar sin interrupciones en el servicio. Verificación, escoge independientemente cuándo, dónde y cómo interviene para implementar la protección.

- El servicio puede ser autorizado por un periodo de tiempo definido: minutos, horas, días o semanas.
- El servicio puede ser limitado en un mercado dado basado en la hora del día para todos los usuarios, grupo de usuarios, o un cliente dado.
- El servicio puede ser bloqueado en un mercado dado para todos los usuarios, un grupo de usuarios, o un usuario específico.
- La frecuencia o alcance puede ser controlada.
- Puede aceptar número de identificación automático o tono doble multi-frecuencia.

3.1.1.2 Descripción

Su simplicidad define al cliente las restricciones de acuerdo, a dónde y cuándo él siente mayor vulnerabilidad: por mercado, grupos de *roamers* o periodos de tiempo. El servicio impone sus niveles de bloqueo, definidos aún cuando un móvil posea un PIN válido.

Validación también permite automáticamente controlar las señalizaciones IS-41 para enrutar *roamers* localizados en mercados de alto tráfico, mediante la legitimidad del *roamer*.

Número de identificación personal

El PIN es un código usado por un número telefónico móvil en conjunto con una tarjeta del suscriptor para completar una llamada. Después de completar las llamadas, el usuario re-ingresa el código, bloqueando el teléfono. Un clonador puede tener robados el par de números ESN/MIN pero no podría realizar llamadas usando esos números a menos que el suscriptor haya desbloqueado el teléfono. Para los usuarios que están vagando, las operadoras pueden mejorar la protección del método PIN por la conjunción de información de PINs con otros mercados quienes usan esos parámetros de *roaming*.

Beneficios de emplear el PIN

- Protección para evitar llamadas de larga distancia no autorizadas.
- Su uso es muy sencillo y sólo requiere el PIN para llamadas de Larga Distancia; es decir, las llamadas locales, asteriscos o servicios de emergencia continúan con su marcación original (sin PIN).
- Reduce la posibilidad de cargos indebidos por fraude, evitando molestias en el servicio.

El uso de *roaming* no se verá afectado por el empleo del PIN, el cual funcionará en cualquier lugar con cobertura celular, tanto en el país de origen, como del extranjero. Si se olvida o extravía el PIN, puede comunicarse inmediatamente al servicio de atención al cliente, por ejemplo Otecel; para que el antiguo PIN sea desactivado y se le proporcione uno nuevo, que estará vigente únicamente durante una hora, puede personalizar un nuevo PIN en la forma aquí señalada.

¿Cómo se debe personalizar el PIN?

Marca *57 + PIN anterior (4 dígitos) + # + PIN nuevo (4 dígitos) + SND y espera tono de confirmación.

¿Cómo activar la transferencia de llamadas con el PIN?

Para transferir:

1. Abra el acceso a larga distancia con:
   *560 + PIN (4 dígitos) + SND y espera tono de confirmación.
2. Efectúa la transferencia deseada con *71, *73 o *74 (Ej. : *71 + número telefónico + SND) y espera tono de confirmación.
3. Cierra el acceso a larga distancia, con:
   *56 + PIN (4 dígitos) + SND y espera tono de confirmación

Para desactivar la transferencia:

1. Repite el paso 1.
2. Desactive la transferencia marcando *710, *730 o *740 + SND, según la transferencia que haya utilizado, y espere el tono de confirmación.
3. No olvide repetir el paso 3 para activar el bloqueo nuevamente.

¿Y si olvidas cerrar el acceso a larga distancia?

Si esto ocurre, durante el tiempo en que olvide cerrarlo, quedará desprotegido ante un clon, con las molestias e inconvenientes que ello implica.

¿Si migra de paquete o esta en baja temporal y vuelve a activarse, requiere de otro PIN?

No. El PIN de cada usuario se mantiene siempre igual, a menos que decida personalizarlo y puede hacerlo cuantas veces lo desee a cualquier hora del día o de la noche.

¿Qué medidas de seguridad se debe adoptar para evitar el fraude celular?

- Cerrar siempre con su PIN el acceso a larga distancia después de efectuar una llamada de larga distancia.
- Memorizar el PIN y no proporcionarlo a persona alguna.

- Si se equivoca al marcar los códigos de apertura y cierre del acceso a larga distancia, escuchará un mensaje de error. Vuelve a intentarlo nuevamente. Si vuelve a escuchar el mensaje, llame al servicio al cliente.
- Guardar en un lugar seguro el contrato, para evitar que la información personal reciba un mal uso.
- No olvidar el celular en el automóvil o en estacionamientos públicos.
- En caso de robo, repórtelo inmediatamente al teléfono de atención a clientes de la localidad.

Recuerde:

- El uso del PIN no tiene costo alguno y es indispensable para realizar llamadas de larga distancia desde la ciudad de origen ó cuando se encuentre de viaje.
- No es necesario utilizarlo sí se hace llamadas locales o a los servicios de emergencia o asteriscos.
- Es recomendable que al recibir el PIN lo personalice como aquí se indica, eligiendo una combinación de cuatro dígitos que se pueda recordar fácilmente.
- Si tiene contratada la transferencia de llamadas, se debe usar el PIN para abrir el acceso, realizar la transferencia y volver a cerrarlo. Para desactivar la transferencia, debe volver a abrir el acceso, realizar la desactivación y volver a cerrarlo para su seguridad.

Respuesta de voz integrada

Para determinar la autenticidad de los *roamer*s, verificación utiliza una Respuesta de Voz Integrada (*IVR: Interactive Voice Response*). El IVR es un elemento de suma importancia al momento de automatizar procesos de consulta, toma de pedidos, envíos de reportes vía fax y cualquier consulta de productos y/o servicios de la empresa. El IVR disminuye tremendamente la labor de servicio del operador, en virtud de su capacidad de ofrecer un servicio 7 días x 24 horas, los 365 días del año.

El operador autómata está en capacidad de reconocer el abonado que le llama a través de la identificación automática.

Una vez identificado el cliente, el sistema puede localizar toda la información respectiva en la base de datos y ofrecer una primera línea de servicio de alta calidad. Si el usuario aún desea hablar con un operador, la llamada es transferida en conjunción con los datos del cliente, lo que minimiza el tiempo de preguntas y respuesta y permite ofrecer la solución requerida. El IVR acepta estándares de entrada DTMF de los teléfonos de *roamer*s, y puede apuntar a un *roamer* para un PIN. El IVR apuntará rápidamente al *roamer* para sus MINs a menos que éste sea automáticamente capturado cuando el mercado de servicio pase el ANI.

Tono dual multi-frecuencia

El Tono doble Multi-frecuencia (*DTMF: Dual Tone Multi-frecuency*) codifica el ingreso de las teclas presionadas del teléfono, definiendo 16 diferentes patrones de tonos. Cada botón emite un tono que es la combinación de dos frecuencias en orden para minimizar la posibilidad de que una señal incorrecta sea recibida por el dispositivo en el momento de presionar los botones. El DTMF o interface *touchtone* originalmente fue desarrollado para simplificar las actividades de mensajería, tal como "para tomar su mensaje, presione 1".

Número de identificación automático

El Número de Identificación Automático (*ANI: Automatic Number Identification*) usa un equipo que automáticamente identifica y registra el número desde el cual usted llama. Muchas veces se puede averiguar el nombre y la dirección de la persona que llama simplemente revisando la base de datos del sistema.

Un sistema IVR responde a los visitantes siguiendo un registro secuencial. Responde verbalmente o después de producir un *touchtone*, es decir cuando se presiona un botón del *dialpad* del teléfono, números del 0-9 y las teclas * y #. Al presionar un botón del *dialpad* habilitamos la señalización DTMF suministrando la información requerida al sistema.

El IVR tiene las siguientes aplicaciones:

- El **Localizador ramal** ayuda a los clientes a encontrar el ramal o la localización más cercana, para luego transferir al visitante.
- **Problemas de llamadas sirven** para reparar y da a los visitantes un status basado en un número de pase.
- **Chequeo de garantía** pregunta a un visitante por un número ID, explora la base de datos para mirar si el cliente está bajo garantía y dice al visitante que acción tomar.
- **Status de cuenta,** chequeando y cargando balances permite a los clientes acceder directamente a la información de cuentas, pago automatizado de facturas, y otros servicios avanzados. IVR reduce el costo de transacciones e incrementa la disponibilidad del servicio.
- Los fabricantes permiten hacer **transacción de tarjetas de crédito,** para vender productos/servicios sobre los teléfonos 24 horas al día, 7 días a la semana.
- **Requerimiento de registro-visitante:** las transacciones IVR son guardadas en una base de datos tal que las compañías conocen las áreas en las cuales el visitante requiere ayuda.
- **Interoperabilidad** con el centro de autenticación local para proveer el más efectivo sistema de protección de fraude.

3.1.2 VALIDACIÓN DE ROAMERS

Validación bloquea las llamadas fraudulentas antes de que ellas sean conectadas. La función de registro de llamadas proporcionada por estos servicios facilita la entrega automática de llamadas, permitiendo a sus clientes recibir llamadas mientras realizan *roaming*.

3.1.2.1 Beneficios

- Maximiza la rentabilidad registrando y prestando un servicio automático a los *roamers* válidos.
- Reduce las pérdidas por fraude al denegar servicio cuando detecta alteración numérica (*tumbling*) y desconectar llamadas.
- Reduce las deudas incobrables y la insatisfacción de los clientes ocasionada por la activación de unidades robadas.
- Proporciona interoperabilidad entre mercados sin IS-41, IS-41, SS7 y mercados con GSM para servicios de validación.
- Obtiene validación pre-llamada con IS-41 para abonados locales sin incurrir en el gasto de actualizar la central.
- Actualización automática del Archivo de Aplicación Negativa.

3.1.2.2 Descripción

Existen dos tipos de validación:

- Validación pre-llamada
- Validación post-llamada

Validación pre-llamada

El servicio de validación pre-llamada es el de mayor aceptación en la industria. Su principal función es la de bloquear las llamadas fraudulentas antes de procesarlas, además cuando la central local y la central servidora utilizan este servicio, es posible validar a los *roamers* desconocidos desde su central local, lo que significa que los usuarios no autorizados no pueden completar sus llamadas.

Validación post-llamada

Cuando el entorno de la central local tiene el Servicio de Validación Post-llamada (*PVS: Post-call roamer Validation Service*), el administrador de fraude puede seguir protegiendo el uso fraudulento de la llamada, mediante la desconexión (*tearing down*) de las mismas, cuando están en curso.

Validación ha desarrollado un algoritmo exclusivo que ha eliminado prácticamente el problema de alteración numérica (*tumbling*) de los números MIN o ESN. El administrador de fraude bloquea las llamadas fraudulentas basándose en ciertos umbrales específicos que admiten usuarios con múltiples NAM.

Cuando la central servidora realiza la validación usando el servicio de validación post-llamada, las unidades fraudulentas se consignan en el Archivo de Aplicación Negativa, y se genera una actualización de archivo negativo para la central servidora. Se elimina el tiempo de espera de la central local, acelerando la entrada al Archivo de Aplicación Negativa.

Como se sabe, para cada operador celular, puede resultar difícil seguirle la pista a los usuarios fraudulentos sin comprometer el servicio transparente e ininterrumpido que esperan los clientes, los servicios de validación, incluyen información de *roaming* en línea más completa, que incluye la actividad de registro y validación mediante el servicio administración de fraude, y a través de redes SS7.

Los eventos a los que se da seguimiento pueden incluir cada registro e intento de llamada. Como parte de la opción de identificación de fraude, el servicio indica automáticamente a la central servidora que realice la validación "por llamada". Esto no afecta la frecuencia con que el servicio verifica la validación con la central local, que se determina en la central local.

En términos de la norma IS-41, se da seguimiento a todas las notificaciones de registro y pedidos de calificación, como por ejemplo desconexión de llamadas, cuyo seguimiento se efectúa como un tipo de evento separado. Actualmente, el seguimiento de las notificaciones de registro se realiza solamente en el sistema SS7, dado que son los únicos mensajes que indican una presencia física en el mercado. Esto es obligatorio para detectar el fraude por clonación. Validación puede usar otro tipo de mensajes, ya que emplea su propia base de datos para efectuar el seguimiento de la ubicación de los abonados que hacen *roaming*.

3.2 SISTEMA DE PERFIL DE USUARIO

El Sistema de Perfil de Usuario (*Custumer Profiling System*) es un sistema que hace notar actividades inusuales en los parámetros de llamada de los usuarios. Así por ejemplo *profiling* recibe y actualiza la información de los suscriptores en tiempo real, intentos de llamada o completadas para actividades de inscripción y características de activación, extensas cuentas de llamada y listas muy grandes de llamadas de larga distancia.

El sistema (*software*) genera perfiles de llamadas, de acuerdo con el historial de uso de cada suscriptor y los compara automáticamente con las llamadas que no se ajustan a estos parámetros. Por ejemplo, un usuario particular, usualmente llama a un círculo de familiares, amigos, compañeros de oficina, y otros números (que pocas veces utiliza). Pero un día el sistema detecta que desde su teléfono empieza a hacer llamadas frecuentes a números que no están dentro de su patrón histórico.

En este instante se activa una alarma y el titular del teléfono es contactado por el operador para informarle del hecho y comprobar la legitimidad de la llamada sospechosa.

Adicionalmente, los programas también son capaces de identificar intentos de fraude cuando se presenta la denominada colisión de llamada (*collision checking*), que se produce cuando el usuario legal y el clonador realizan una comunicación simultáneamente.

De la misma forma, detecta llamadas fuera de secuencia, es decir, el usuario hace una llamada desde el norte de la ciudad y a los pocos minutos registra otras desde el sur. Allí, el sistema deduce que es imposible que el abonado haya recorrido esa distancia en tan corto tiempo, y por consiguiente, la alarma de posible clonación se activa.

Para la mayoría de proveedores, *Profiling* opera tanto en redes analógicas (AMPS, ETACS) como en redes digitales (GSM, CDMA, TDMA) expandiendo su capacidad y funcionalidad, mejorando desempeño e integración con otros sistemas de control de fraude.

Basado en una poderosa tecnología para identificar, y alertar automáticamente actividades fraudulentas sospechosas en la red. Este sistema de detección reduce las pérdidas tanto por fraude de clonación local como de *roaming*, como también suscripción fraudulenta.

Profiling usa técnicas de detección de fraude estandarizadas por la CTIA, tales como colisión y chequeo de velocidad (*velocity checking*). En suma, provee mejoras en los patrones de análisis en todos los datos que ingresan incluyendo desde distintos lugares, hora del día, dígitos marcados y duración de las llamadas para identificar comportamientos inusuales y potencialmente fraudulentos.

Podemos con este sistema, identificar un suscriptor típico durante un período de comprobación y contra parámetros que el operador defina. *Profiling* usa avanzados análisis estadísticos para evaluar y aprender progresivamente el comportamiento de los patrones individuales de los usuarios. Ese perfil individual del usuario está continuamente actualizado para asegurar niveles de casos confidenciales.

3.2.1 BENEFICIOS

No todas las actividades sospechosas requieren inmediata investigación humana. Eso es porque el sistema *profiling* da prioridad a los casos de fraude de alta probabilidad que pueden hacer mucho mayor daño que los casos con menos impacto.

También, expande su capacidad para iniciar acciones automáticas de acuerdo a las políticas y procedimientos de la compañía. Por ejemplo, se puede interactuar con otros sistemas para enrutar a un visitante al servicio al cliente *online* o cortar un servicio de suscripción.

- **Reducción de pérdidas de ingresos.** Reducción de pérdidas incurridas por fraude
- **Mejoramiento en la exactitud y eficiencia.** Motores basados en parámetros de detección y poderosas herramientas de manejo de alarmas para identificar exacta y eficientemente el fraude por clonación y por suscripción fraudulenta.
- **Mejoramiento de productividad.** Extensas herramientas de análisis fáciles de usar en la investigación y análisis de la actividad fraudulenta.
- **Administración del cliente mejorado.** Integrando e intercambiando datos con la facturación y sistemas de cuidado del cliente, mejorará el proceso de administración del mismo.
- **Migración hacia nuevas tecnologías.** Para usos futuros, tiene la capacidad de trabajar con sistemas de segunda y tercera generación, como por ejemplo

Autenticación, *RF Fingerprint* para mejorar su total solución en la administración del fraude.

3.2.2 DESCRIPCIÓN

La tecnología de perfiles de usuario, mantiene registradas e identificadas las llamadas de los suscriptores y los patrones de *roaming*. Si hay un comportamiento fuera de lo normal en los patrones, una alarma aparecerá, y la operadora contactará al suscriptor para confirmar si las llamadas son válidas o no.

3.2.2.1 Acceso de datos de llamada y normalización

Los datos de llamadas son accedidos desde múltiples fuentes, incluyendo CDRs, switches, dispositivos de mediación, etc., la recopilación de los datos se realiza a través de un centro de intercambio de información, el cual barre las llamadas y las envía a la operadora de telefonía móvil, estos datos son normalizados en preparación para subsecuentes análisis por el tipo de tasación y motores basados en parámetros de detección para la generación de alarmas.

La tasación de llamadas o tarifación aplica un valor monetario a cada llamada, basada en tarifas fijas por el usuario a través de una Interface de Usuario Gráfico (GUI). Por la aplicación de tarifas los operadores pueden fijar niveles basados en el valor de la llamada, como también del monitoreo de la suma de pérdidas ocasionadas por el fraude que pueden ser incurridas por un tipo de servicio en particular o en segmentos de mercado.

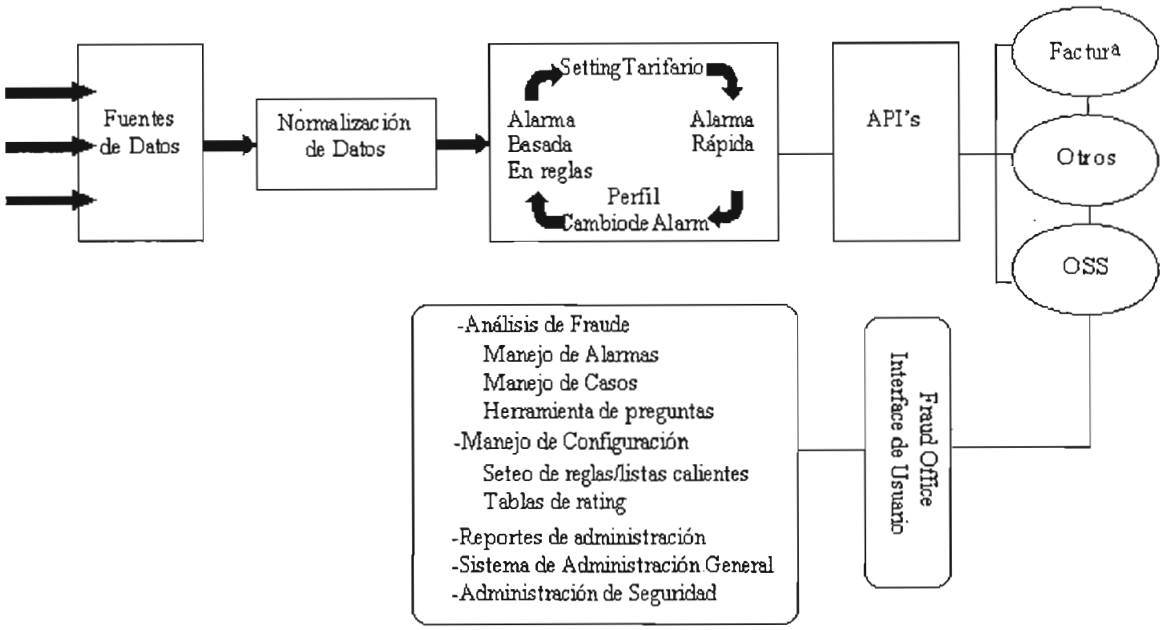


Figura 3.1 Servidor de Perfil de Usuario

3.2.2.2 Generación de alarma

Los CDRs normalizados son transferidos a través de los motores basados en parámetros de detección donde ellos son chequeados por reglas definidas por el usuario. Un análisis del perfil del cliente es también iniciado al ingresar los datos. Este análisis puede indicar cambios en los parámetros de llamada del suscriptor. Las alarmas generadas son escritas y seguidamente leídas desde su almacenaje e inteligentemente presentadas al usuario a través del GUI.

Todos los nuevos suscriptores estarán separadamente identificados y registrados por el sistema. Ellos son identificados como nuevos cuando sus registros CDR son identificados por primera vez. Después de un cierto período son designados como "recientes" para un nuevo período. Los filtros del sistema permiten a usuarios nuevos/recientes ser segregados y examinados separadamente de las cuentas más maduras.

Los nuevos suscriptores son identificados en el momento en que ellos activan un perfil inicial para estas cuentas. La naturaleza del perfil del nuevo suscriptor será determinada en el foco de la base de datos del suscriptor en conjunto con el proveedor del sistema. La intención es identificar suscriptores fraudulentos desde el principio. Esta característica permite al analista monitorear el uso actual de los nuevos suscriptores desde el momento en que ellos se han activado, además le permite al sistema poder continuamente y automáticamente actualizar la información de cada usuario.

3.2.2.3 Características de diseño

Profiling es un sistema abierto que utiliza la arquitectura cliente/servidor, puede usar diferentes plataformas, tales como diseño orientado a objetos, Unix y C++, el servidor corre bajo ambiente UNIX, mientras que el cliente corre sobre Windows NT o Windos 95/98. El cliente y el servidor se comunican sobre una red LAN o WAN usando TCP/IP.

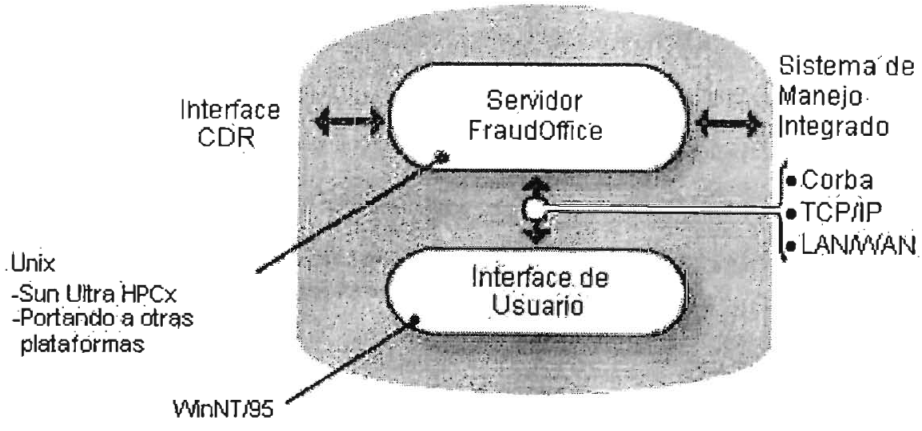


Figura 3.2 Sistema de Administración Integrado[1]

[1] www.Ericsson.se/fraudoffice.com/what's fraudoffice?

Este sistema permite interoperabilidad con los sistemas del operador, tales como switches, dispositivos de mediación, nodos, cuentas y servicios de provisión y pueden ser configurados para reunir las necesidades y procesos del operador.

Características

- Detecta el fraude en redes fijas, móviles e inteligentes
- Incrementa la exactitud en la detección de cambios en el comportamiento de llamadas del usuario, mediante sus motores basados en parámetros de detección.
- Con el GUI, asegura un alto nivel de productividad permitiendo a los usuarios hacer un uso completo del sistema con mínimo soporte y formación.
- Soportes a través de portabilidad a través de un rango de plataformas de hardware, incluyen SUN, HP, Digital e IBM.
- Escalabilidad, abastecimiento para redes de grandes volúmenes y tamaños
- Arquitectura modular y abierta, permite flexibilidad y fácil integración, suministrando a las operadoras un servicio más personalizado.

Hardware y software del sistema

- Servidor y estación de trabajo UNIX.
- Base de Datos Informix.
- La red dependiente de la opción de despliegue.
- Diseñado para una operación individual.
- Interface de Usuario Gráfico que incluye nuevas pantallas, respuestas más rápidas y poderosas herramientas para navegar fácilmente.
- Es transparente al usuario en el manejo de casos sospechosos de fraude.
- Mejora la productividad de los usuarios, reduce sus costos e incrementa la eficiencia de sus análisis.

Interface de usuario gráfico (GUI)

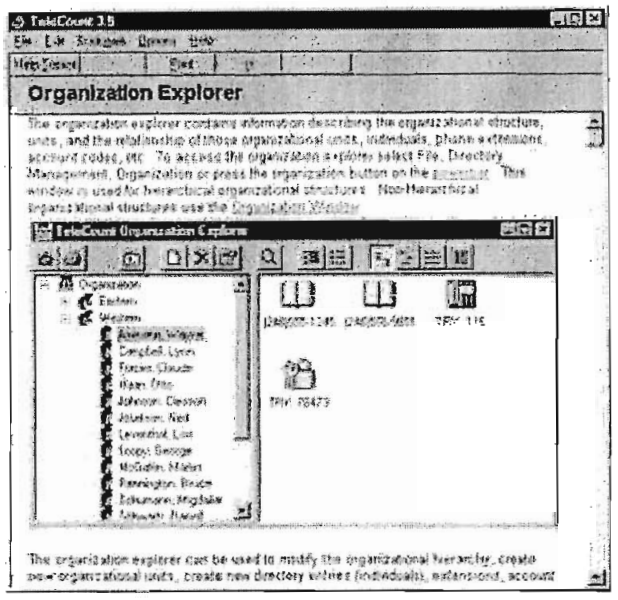


Figura 3.3 GUI Fácil de aprender, mediante herramientas de ayuda interactivas[1]

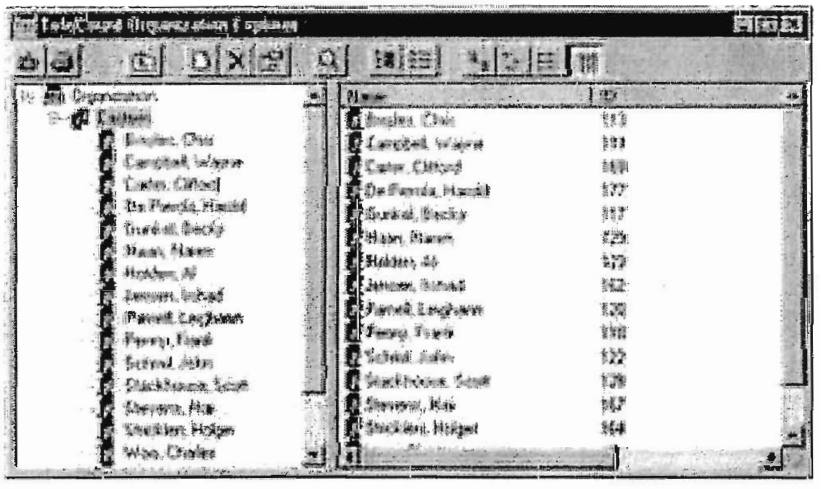


Figura 3.4 GUI. Fácil de usar, en ambiente windows[2]

[1] www.Ericsson.se/fraudoffice.com/fraudoffice software?
[2] www.Ericsson.se/fraudoffice.com/fraudoffice software?

La interface de usuario gráfico presenta las siguientes características:

- Capacidad de comprimir y archivar todos los registros.
- Soporta la entrada de visitantes ID/ANI.
- Edita a registros existentes y a nuevos.
- Importa datos de llamada desde otros programas, utilizando ODBC.
- Actualizaciones de los servicios de tarifación.
- Sobre los 160 reportes con criterio de selección flexible.
- Crea reportes personalizados o modifica los existentes.
- Soporta e-mail y exporta reportes en una variedad de formatos incluyendo: HTML, RTF, ASCII&PDF.
- Esquematiza los datos de llamada, con el propósito de imprimir, importar, exportar sobre bases regulares.
- Trabajo completamente en red.
- Seguridad, utiliza contraseñas para accesos a reportes y registros confidenciales.

3.3 AUTENTICACIÓN

Autenticación hace uso de números secretos que son almacenados en el teléfono celular y conocidos por la red, pero nunca pasando por el aire. El servicio de Autenticación requiere que la estación móvil y el Centro de Conmutación Móvil Visitado (*VMSC: Visited Mobile Switching Center*) intercambien y comparen datos. Usando esos datos y un número generado aleatoriamente, ambos ejecutan en forma independiente el algoritmo de Encriptado Vocal y Autenticación Celular (*CAVE: Cellular Authentication Voice Encode*). Si los resultados coinciden, la identidad del móvil se autentica. El servicio se basa en la categoría de abonado.

Esto permitirá autenticar cualquier estación móvil capaz de brindar soporte a ese servicio, por ejemplo IS-91, IS-54B o IS-136. Los móviles analógicos producidos a partir de 1996, así como los móviles TDMA, brindan soporte a la Autenticación. Este servicio no es aplicable a los teléfonos analógicos EIA/TIA 553. En algunos casos, los teléfonos EIA/TIA 553 pueden adaptarse a la norma IS-91, pero ello depende totalmente del fabricante del teléfono y el modelo de la estación móvil.

3.3.1 BENEFICIOS

Este moderno servicio, que utiliza el algoritmo CAVE avanzado para validar la identidad de las estaciones móviles, constituye la tecnología de prevención de fraude más avanzada y eficaz de que se dispone. La autenticación impide todos los tipos de fraude por clonación, robo y generación aleatoria de ESN, y también evita el fraude de suscripción interno cometido por el personal del operador. La autenticación es utilizada con éxito por muchos de los operadores más importantes del mundo, y su evolución la ha conducido a ser la norma mundial para evitar el fraude celular en los sistemas AMPS y D - AMPS.

Este algoritmo está diseñado por avalancha, muy rápido, para aplicar un análisis de la relación demanda-respuesta, que es una técnica que requiere que la estación base emita un pedido de código de autenticación a la unidad móvil, la que, a su vez, responde con el código de secuencia correspondiente.

Ya que un número aleatorio diferente es usado para cada intercambio, un escuchador a escondidas (*eavesdropper*) podría tener un trabajo muy duro tratando de obtener los números secretos del teléfono. Esto no sugiere que sofisticados crackeadores de códigos no lo puedan hacer (los expertos en la Agencia de Seguridad Nacional podrían probablemente considerar esto como ejercicios de calentamiento), pero aún criminales de alto nivel raramente tienen acceso a la pericia requerida o equipamiento.

3.3.2 DESCRIPCIÓN

La implementación de la funcionalidad de autenticación en la red, se basa en el TSB sobre autenticación, encriptado de mensajes de señalización y privacidad vocal publicado en la TR45.2 de la TIA. Este documento define las directivas de la industria celular respecto de cómo utilizar las transacciones de autenticación de IS-54, Rev. B, desde el punto de vista de la red. También define las modificaciones de IS-41 requeridas para brindar soporte a la autenticación.

Aunque el servicio de autenticación requiere estaciones móviles que cumplan con la norma provisoria 54, revisión B (IS-54 Rev.B) o posterior, no exige canales de tráfico digitales, de modo que una red analógica (con canales vocales analógicos solamente) también brindará soporte a la autenticación.

La norma IS-41C requiere una nueva categoría de abonado, la que cuenta con capacidad de autenticación (AuthCap), a la que ha de brindarse soporte en el HLR y MSC. El parámetro forma parte del perfil del abonado y define si se puede efectuar o no la autenticación cuando del abonado accede a la red. Las operaciones de autenticación se inician solo después que el MSC recibe la indicación de que el abonado cuenta con la capacidad de autenticación.

El registro de ubicaciones local/centro de autenticación (HLR/AC) de algunos sistemas no podrán detectar clones totales en esta primera implementación de la autenticación con sistemas más antiguos, ya que el proveedor no brindará soporte al mecanismo de actualización COUNT definido en el TSB 51 de la TIA.

La función de autenticación se basa en claves secretas, que nunca se envían o muestran abiertamente, y se ingresan (junto con otros parámetros) a un algoritmo que calcula una respuesta. Tanto la red como la estación móvil ejecutan el algoritmo y calculan la respuesta y, posteriormente, la red verifica que los resultados sean iguales.

En caso de no coincidir, el operador es alertado por un listado, y en tal caso puede tomar manualmente las medidas adecuadas. El uso de este servicio exige que el terminal móvil cuente con la capacidad de autenticación.

Nota: Este servicio no incluye el soporte para la gestión de la clave A. A este respecto se recomienda la utilización de un Sistema de Gestión de Autenticación (AMS). El algoritmo CAVE utilizado para este servicio exige una licencia de exportación, por lo que la funcionalidad no se cargará automáticamente en la central. Una vez aprobada la licencia, el *software* se cargará por separado.

3.3.3 IMPLEMENTACIÓN

Las operaciones de autenticación se inician solo después que el MSC recibe la indicación de que el abonado cuenta con la capacidad de autenticación. La función de Centro de Autenticación (AC) se implementa en el MSC/HLR, a fin de facilitar el servicio de autenticación. Una interface de señalización patentada permite que el AC y el HLR cooperen en el proceso de conexión/desconexión del abonado. El AC es la única entidad del MSC/HLR en la que se almacenan los datos de autenticación (es decir, los datos de la clave A) para un abonado.

Una clave A es un número único (de 6 a 26 dígitos) asignado a cada abonado por el HLR. La distribución del número de la clave A al abonado es realizada por el operador. La clave A reside en la memoria permanente de la estación móvil, así como en el AC del MSC/HLR del abonado.

Estrictos procedimientos de control garantizan que la clave A nunca se transmita a través de ninguno de los protocolos de señalización a los que se brinda soporte en un entorno de conmutación de red, es decir la norma provisoria 41 (IS-41) o la Parte de Usuario de Telefonía Móvil (MTUP), ni se muestre abiertamente.

En cambio, cuando se transmite información de autenticación entre nodos de la red, la clave A se utiliza para generar Datos Secretos Compartidos (*SSD: Shared Secret Data*), que son los que se envían.

La clave A se utiliza como parámetro de entrada al algoritmo CAVE para crear la respuesta, es decir los SSD. Esos SSD se transmiten en el sistema y se utilizan como parámetro de entrada al algoritmo CAVE para calcular la respuesta de autenticación.

El algoritmo CAVE se almacena en los AC, HLR y VMSC de la red y en la estación móvil. Todos los cálculos de este algoritmo, tanto en el AC como en el MSC, se realizan utilizando el Dispositivo Procesador Regional (RPD). El nuevo RPD es un procesador MC 68020. El RPD del HLR/AC se utiliza para la validación de la clave A y la generación de los SSD. Los SSD solo se generan en el AC. Para limitar la carga sobre el HLR/AC, los RPDs pueden ubicarse en el MSC para la generación de los SSD. La cantidad de RPDs necesarios depende de la cantidad de abonados que se deben autenticar.

En la tabla 3.2 se indica la cantidad de *magazines* necesaria en el HLR/AC, considerando cuatro dispositivos por *magazine* y el agregado de un dispositivo adicional para redundancia.

Cantidad de Abonados que Utilizan Autenticación	**Cantidad de Magazines**
100.000 o menos	1
100.001 a 200.000	1
200.001 a 300.000	2
300.001 a 400.000	2
400.001 a 500.000	2
500.001 a 600.000	3

Tabla 3.2 Magazines por abonado

A efectos de limitar la cantidad de señalización requerida en los MSCs se recomienda la utilización de un magazine (con cuatro RPDs) para cada uno de ellos.

3.3.3.1 Solicitud de autenticación

Al recibir desde la estación móvil una llamada originada o una respuesta al paging, el VMSC valida a esa estación enviando al AC un mensaje de Solicitud de Autenticación. Si los SSD no se comparten con el VMSC, éste envía un mensaje de solicitud de autenticación cada vez que la estación móvil requiere autenticación.

> Nota: Los SSD se comparten si el VMSC puede ejecutar el algoritmo CAVE, y la clave A y los SSD son idénticos tanto en el AC como en la estación móvil.

Si el AC recibe un mensaje de solicitud de autenticación que contiene una Respuesta de Autorización (AUTHR), el AC lo valida. Si no se envía AUTHR, el AC envía los SSD si el VMSC puede aceptarlos (el algoritmo CAVE reside en el MSC). Si el MSC no puede aceptar los SSD, el AC efectúa un cálculo de Autorización Única (AUTHU) y lo envía al VMSC, de modo que éste pueda enviar una Demanda Única a la estación móvil.

3.3.4 FUNCIONES

Este ofrecimiento específico del servicio de autenticación comprende las siguientes funciones:

- Actualización de datos secretos compartidos (SSD)
- Procedimiento de respuesta a la demanda única

3.3.4.1 Actualización de los datos secretos compartidos

Siempre que una estación móvil capaz de autenticación accede al VMSC, éste envía al AC del abonado un mensaje de Solicitud de Autenticación.

El AC utiliza el algoritmo CAVE para generar (SSD). Cuando se actualiza los SSD, el AC envía al VMSC los nuevos SSD y el número aleatorio (RANDSSD) utilizado para generarlos, en un mensaje de Orden de Actualización de SSD.

Con esta implementación, no se envían nuevos SSD del HLR/AC al MSC hasta que la actualización de los SSD sea exitosa. La estación móvil utiliza el algoritmo CAVE a fin de generar sus SSD, utilizando el RANDSSD recibido, el ESN almacenado de la misma y la clave A. Para validar los nuevos SSD, la estación móvil procede del siguiente modo:

- La estación móvil genera un número aleatorio (RANDBS) y lo envía al VMSC (o al AC sí los SSD no se comparten con el VMSC) en un mensaje de Orden de Demanda a la Estación Base.
- La estación móvil y el VMSC calculan independientemente la palabra de resultado (AUTHBS) utilizando los nuevos SSD y el RANDBS.
- El VMSC envía el resultado de su cálculo a la estación móvil.
- La estación móvil compara el resultado enviado por el VMSC con el de su propio cálculo, para determinar la validez de los nuevos SSD.
- La estación móvil retorna al VMSC un mensaje de Confirmación de Actualización de SSD, en el que se especifica la validez o no de los SSD.
- La estación móvil puede utilizar los nuevos SSD cuando recibe del VMSC una Respuesta a la Demanda Única.

3.3.4.2 Directiva de autenticación

El AC puede enviar una orden ó Directiva de Autenticación cuando determina que debe efectuarse una actualización de SSD para un abonado específico. El AC puede ordenar una actualización por los siguientes motivos:

- Administrativo
- Tráfico

El AC inicia una orden ó Directiva de Autenticación por los siguientes motivos administrativos:

- Actualización periódica de SSD
- Actualización de SSD iniciada por comando

3.3.4.3 Procedimiento de respuesta a la demanda única

A fin de determinar la legitimidad de las actividades de llamadas de la estación móvil, el VMSC (o el AC en un sistema con SSD no compartidos) puede iniciar una Respuesta a la Demanda Única. El VMSC genera una Respuesta a la Demanda Única en las siguientes circunstancias:

- Al establecer la llamada
- Después de la actualización de SSD en el VMSC
- Luego de un mensaje de solicitud de integración desde la estación móvil

El procedimiento se inicia del siguiente modo:

- El VMSC genera un número aleatorio exclusivo (RANDU) y lo envía a la estación móvil a través del canal vocal o el canal de tráfico digital.
- La estación móvil aplica el algoritmo CAVE a RANDU para calcular un resultado de autenticación (AUTHU) y lo envía al MSC.

- El VMSC también ha generado AUTHU y lo compara con el recibido de la estación móvil.

Si se detecta una no-coincidencia, se informa este resultado al MSC/HLR del abonado. El AC utiliza temporizadores internos para generar la Respuesta a la Demanda Única, que envía al VMSC. Si ocurriera que la estación móvil está inactiva cuando se recibe la respuesta a la demanda, el VMSC la almacena hasta que la estación móvil se ubica en un canal de tráfico.

3.3.4.4 Acciones

Cuando un procedimiento de actualización de SSD o Respuesta a la Demanda Única produce una no-coincidencia, el MSC/HLR del abonado determina las medidas a ser tomadas por el VMSC. El MSC/HLR puede especificar una de las acciones siguientes:

- Denegar el acceso a la estación móvil
- Iniciar otro procedimiento de autenticación
- No efectuar procedimientos de autenticación adicionales.

Cuando el MSC/HLR ordena al VMSC denegar acceso a la estación móvil, el VMSC determina el tipo de acceso de llamada y procede en base al mismo del siguiente modo:

- Si el acceso de llamada es una llamada originada que se cursa a una operadora o número de emergencias, el VMSC permite que la misma continúe. De lo contrario, el VMSC enruta la llamada hacia un código de fin de selección.
- Si el acceso de llamada es un establecimiento de llamada con pre-enrutamiento, el VMSC cancela el pre-enrutamiento y notifica al MSC/HLR de que no se recibió ninguna respuesta al paging.

- Si el acceso de llamada es una llamada destinada a un abonado móvil, el VMSC determina si continuarla o no, o desconectarla.
- Si el acceso de llamada es una llamada de interrogación, el VMSC la desconecta.

Cuando el MSC/HLR deniega el acceso, los datos de tasación de la llamada se actualizan a efectos de incluir una indicación de acceso denegado.

3.3.5 ADMINISTRACIÓN

El operador asigna el servicio de Autenticación a un abonado móvil utilizando la clase AUH disponible en los procedimientos administrativos del HLR. Una vez asignada la clase, se definen los datos del abonado y se activa la misma.

3.3.5.1 Creación de la clave A

El operador puede especificar la longitud de la clave A utilizando un comando. Al ser emitido, el comando genera automáticamente una clave A para un abonado. Dicha clave puede ser nueva o reemplazar a una existente. Una vez generada la clave A, la misma se enruta hacia una impresora o un terminal, pero, por motivos de seguridad, sólo puede mostrarse en formato codificado. En este punto, la clave A puede enviarse al abonado móvil. Cuando una estación móvil accede por primera vez al sistema utilizando datos de clave A nuevos, el AC ordenará una actualización de SSD.

El abonado móvil tiene un tiempo limitado para instalar la clave A nueva o de reemplazo. Si el límite de tiempo vence sin que se instale dicha clave se generará una alarma para informar al operador que el límite de tiempo ha expirado. El abonado será eliminado de la lista de alarma cuando se instale la clave A.

3.3.6 PRESTACIONES

El servicio de autenticación brinda soporte a las siguientes prestaciones:

- Algoritmo sofisticado para generar datos de comparación.
- Procedimientos seguros para almacenamiento, transmisión y recuperación de datos.
- Interface aérea según la Norma Provisoria 54 Revisión B (o posterior).
- Protocolos de señalización MTUP y Norma Provisoria 41 (incluyendo IS-41C).

3.3.7 AUTENTICACIÓN IS-91

3.3.7.1 Introducción

La autenticación es un proceso IS-54B en el cual se intercambia información entre una estación base y un móvil, para confirmar la identidad del móvil. Este proceso impide el uso de móviles restringidos o robados y de abonados no autorizados (radio pirata). Los móviles fabricados antes de incorporar la especificación IS-54B en la producción no se ven afectados.

Se asigna una Clave A de 64 bits (o más) a cada móvil. Los 64 bits de información se almacenan en la memoria de identificación y seguridad permanente del móvil y también en el registro de ubicación local/centro de autenticación (HLR/AC).

Con fines de seguridad, la clave A nunca se envía por interface aérea, más bien se usa en el algoritmo CAVE para generar SSD. Figura 3.5.

Los Datos Secretos Compartidos (SSD) constituyen un patrón de 128 bits almacenados en la memoria semipermanente del móvil. Constan de dos cantidades de 64 bits, SSD_A y SSD_B. El SSD_A se utiliza para fines de autenticación y el SSD_B se utiliza para la privacidad de voz y la confidencialidad de mensajes.

Se puede generar un nuevo valor de cantidades de SSD en el móvil cuando se envía una Orden de Actualización de SSD.

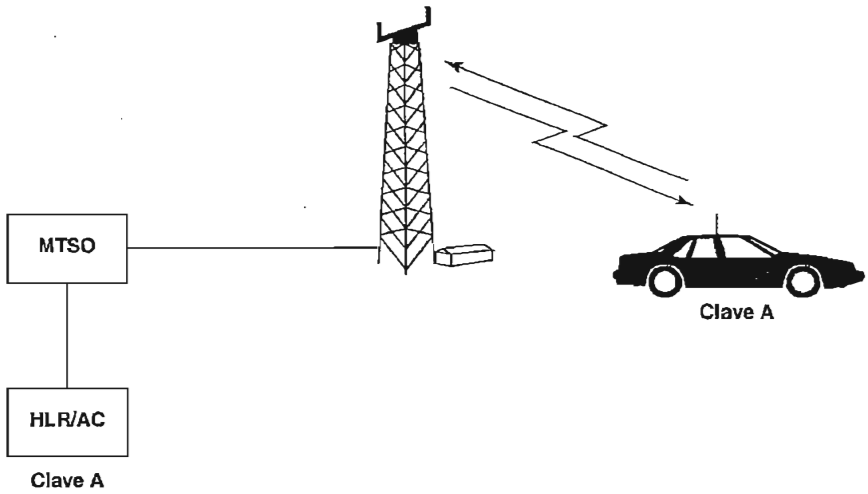


Figura 3.5 Procedimiento de establecimiento de Autenticación

3.3.7.2 Autenticación durante el registro móvil

Cuando el móvil intenta registrarse y el elemento de información AUTH en el Sistema de Parámetros de Mensajes de Cabecera (*SPOM: System Parameter Overhead Message*) del FOCC se fija en 1, se ejecutan los siguientes pasos de autenticación (Figura 3.6):

1. El móvil inicializa el algoritmo CAVE.
2. El algoritmo se ejecuta y AUTHR se fija en la salida de 18 bits.
3. El móvil envía la **Palabra de Autenticación** (que contiene AUTHR, RANDC y COUNT) en el RECC a la estación base.
4. La estación base calcula AUTHR utilizando el SSD_A generado por la HLR/AC.

5. Se comparan los valores recibidos. Si corresponden, el registro tiene éxito. Si falta alguna de las comparaciones, la estación base puede iniciar la **Respuesta de Prueba Unica** o el procedimiento de **Actualización de SSD.**

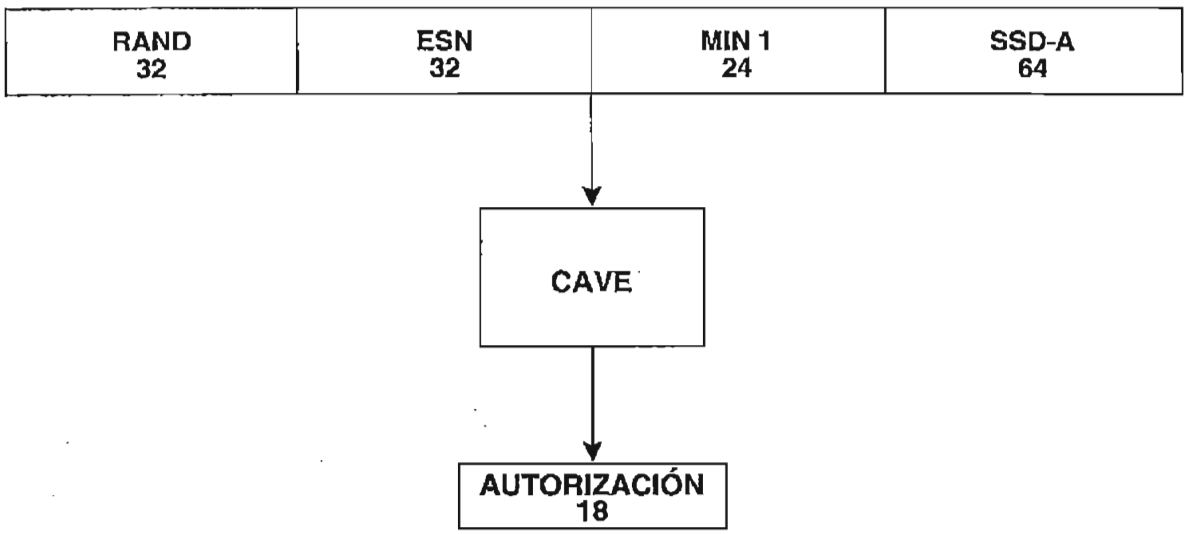


Figura 3.6 Cálculo de AUTHR para el registro móvil

3.3.7.3 Autenticación durante la originación móvil

Cuando el móvil intenta originar una llamada y el elemento de información AUTH en el SPOM está establecido en 1, se ejecutan los siguientes pasos de autenticación (Figura 3.7):

1. El móvil inicializa el algoritmo CAVE
2. Se ejecuta el algoritmo y AUTHR se fija en la salida de 18 bits.
3. El móvil envía la Palabra de Autenticación (que contiene AUTHR, RANDC y COUNT) en RECC a la estación base.
4. La estación base calcula AUTHR utilizando SSD_A generado por la HLR/AC.
5. Se comparan los valores recibidos; si corresponden, se inicia el establecimiento de llamada. Una vez asignado a un DTC o a un VC, la estación base puede emitir un **Mensaje de actualización de parámetros** para actualizar el parámetro de historial de las llamadas en el móvil.

Si falla alguna de las comparaciones, la estación base puede negar el servicio, iniciar la **Respuesta de prueba única** o el procedimiento de **Actualización de SSD.**

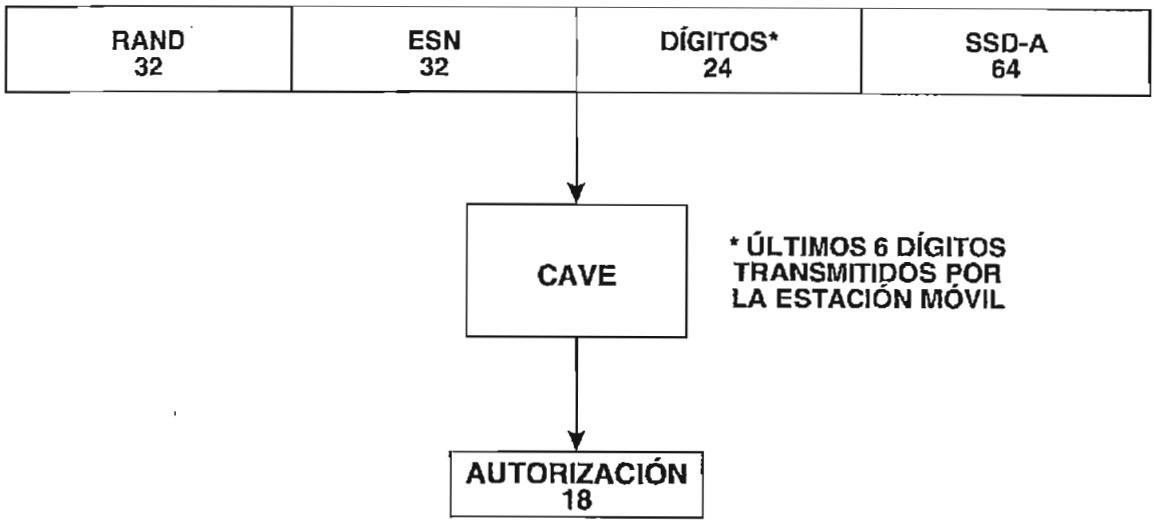


Figura 3.7 Cálculo de AUTHR para la Originación móvil

3.3.7.4 Autenticación durante la terminación de llamada

Cuando se produce una correspondencia de aviso y el elemento de información AUTH en el SPOM se fija en 1, se ejecutan los siguientes pasos de autenticación (Figura 3.8):

1. El móvil inicializa el algoritmo CAVE.
2. El algoritmo se ejecuta y AUTHR se fija en la salida de 18 bits.
3. El móvil envía la **Palabra de autenticación** (que contiene AUTHR, RANDC y COUNT) en el RECC a la estación base.
4. La estación base calcula AUTHR utilizando el SSD_A generado por el HLR/AC.

5. Se comparan los valores recibidos; si corresponden, se inicia el establecimiento de llamada. Una vez asignados a un DTC o a un VC, la estación base puede emitir un **Mensaje de actualización de parámetros** para actualizar el parámetro de historial de las llamadas en el móvil. Si falla alguna de las comparaciones, la estación base puede negar el servicio, iniciar la **Respuesta de Prueba Única** o el procedimiento de **Actualización de SSD.**

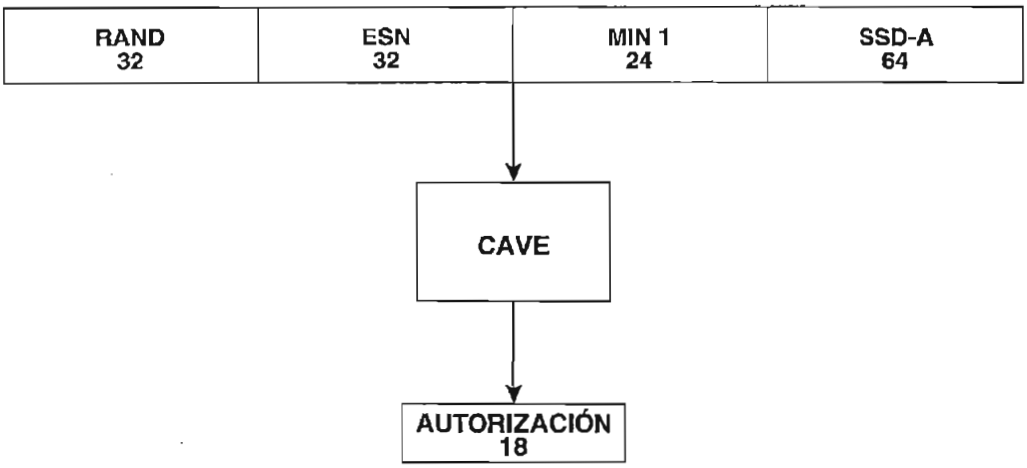


Figura 3.8 Cálculo de AUTHR para la Terminación móvil

3.3.7.5 Respuesta de prueba única

La estación base inicia este procedimiento que se puede procesar en cualquier combinación de canal de control, tráfico y/o voz. Figura 3.9.

1. La estación base envía una **Orden de Prueba Única** al móvil por el FOCC, el FDTC o el FVC. La orden contiene un patrón aleatorio de 24 bits, generado por la estación base, denominado RANDU.
2. El móvil recibe la orden e inicializa al algoritmo CAVE.
3. El algoritmo se ejecuta y AUTHU se fija en la salida de 18 bits.
4. El móvil envía la **Confirmación de orden de prueba única** a la estación base en el RECC, RDTC o RVC.
5. La estación base calcula AUTHU utilizando el SSD_A generado por el HLR/AC.

6. Los valores recibidos se comparan entre sí y si falla la comparación, la estación base puede negar nuevos intentos de acceso, desconectar la llamada en curso o iniciar la **Actualización de SSD.**

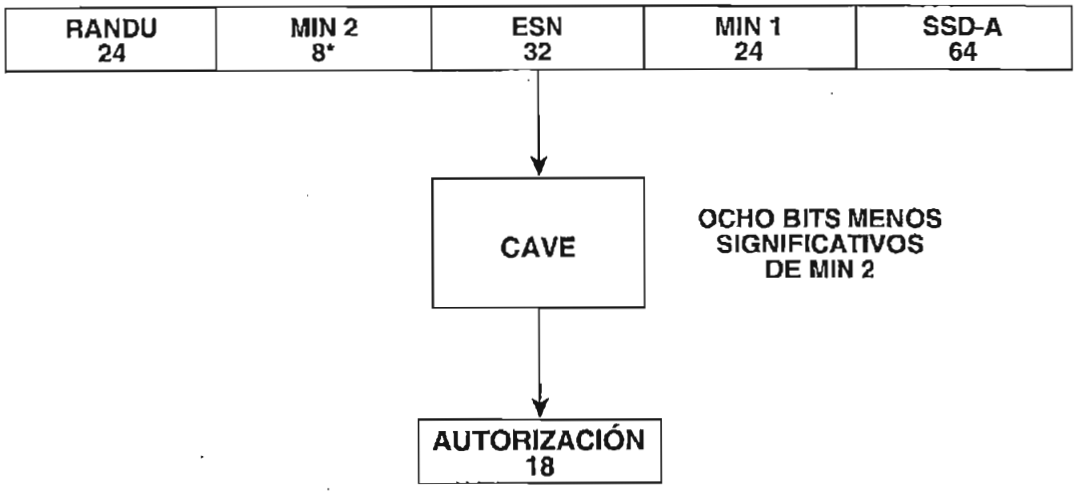


Figura 3.9 Cálculo de AUTHU

3.3.7.6 Actualización de datos secretos compartidos

La actualización de Datos Secretos Compartidos implica la aplicación del algoritmo CAVE, inicializado con información específica del móvil, datos aleatorios y la clave A del móvil. Figura 3.10.

1. La estación base envía una **Orden de Actualización de SSD** al móvil en el FOCC, FDTC o FVC. La orden contiene RANDSSD, un número aleatorio de 56 bits que también utiliza la HLR/AC para hacer cálculos.
2. Luego de recibir la orden, el móvil inicializa el algoritmo CAVE.
3. El algoritmo se ejecuta teniendo como resultado SSD_A_NEW y SSD_B_NEW. SSD_A_NEW contiene los 64 bits más significativos y SSD_B_NEW contiene los 64 bits menos significativos del algoritmo.
4. El móvil envía una **Orden de Prueba de Estación Base** a la estación base en el RECC, el RTDC o el RVC. La orden contiene RANDBS, un número aleatorio de 32 bits seleccionado por el móvil.

5. Luego de recibir la orden, la estación base inicializa el algoritmo CAVE. Para el cálculo se utiliza SSD_A_NEW de la HLR/AC y RANDBS del móvil.
6. Se ejecuta el algoritmo teniendo como resultado AUTHBS, la salida de 18 bits.
7. La estación base incluye AUTHBS en el mensaje de **Confirmación de Orden de Prueba de Estación Base** enviado al móvil en el FOCC, FDTC o FVC.
8. El móvil también reinicia al algoritmo CAVE, teniendo como resultado AUTHBS. Figura 3.11.
9. Luego de recibir la confirmación de la estación base, el móvil compara los valores.
10. El móvil envía un mensaje de Confirmación de Orden de Actualización de los SSD a la estación base en el RECC, RTDC o RVC. El mensaje señala el éxito o el fracaso de la actualización. Si hay éxito, SSD_A y SSD_B se fijan en SSD_A_NEW y SSD_B_NEW. De lo contrario, se descartan los valores NEW.

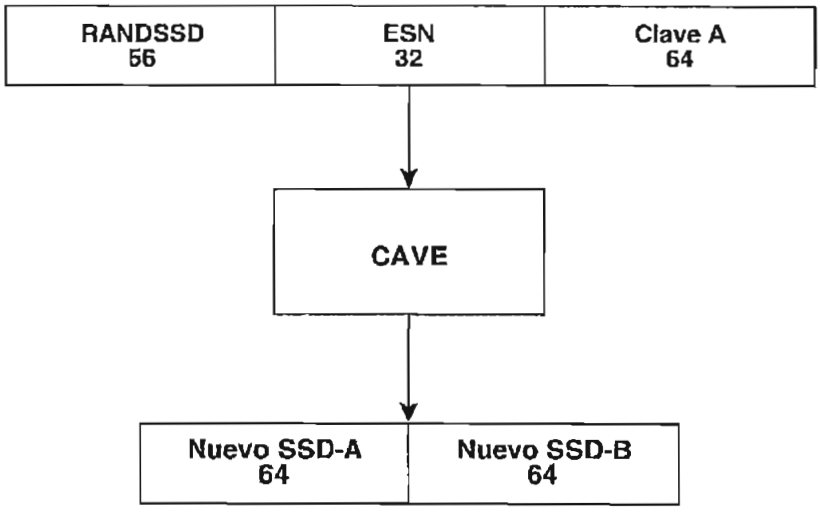


Figura 3.10 Nuevo cálculo de SSD

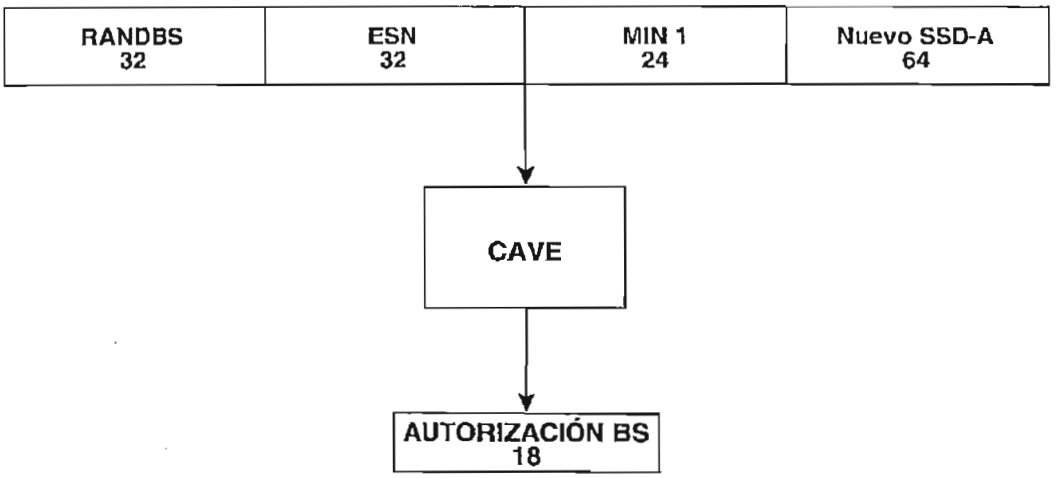


Figura 3.11 Cálculo de AUTHBS

3.4 BLOQUEO AUTOMÁTICO DE LLAMADAS

El servicio de Bloqueo Automático de Llamadas (*ACB: Automatic Call Blocking*) es una extensión de la funcionalidad del Bloqueo Controlado por Código (*CCB: Code Control Blocking*) en origen. El nuevo servicio ACB también incluye la funcionalidad de inhibición del número PIN en el HLR, descrito a continuación.

3.4.1 BENEFICIOS

El servicio ACB imposibilita, a un usuario fraudulento que no cuente con el número PIN del abonado, originar llamadas desde una estación móvil robada o clonada. Esto ha demostrado ser sumamente efectivo contra los tipos de fraude por clonación y generación aleatoria de ESN/MIN. El servicio también podría ser muy eficaz si, por ejemplo, el usuario prestara el teléfono a los hijos pero no quisiera que pudieran realizar llamadas de larga distancia.

3.4.2 DESCRIPCIÓN

Cuando un abonado tiene ACB, después de una liberación por tiempo (dependiente de la central) debida al apagado del teléfono móvil, la clase de

bloqueo se activa automáticamente para el abonado sin necesidad de que éste tome ningún tipo de medida.

El servicio CCB existente permite a un abonado bloquear todos o determinados tipos de llamadas salientes. Con el CCB se asigna al abonado un Número de Identificación Personal (PIN) para la activación y desactivación del bloqueo. El servicio CCB puede ser utilizado, por ejemplo, por un abonado que desee limitar la cantidad de llamadas internacionales o de larga distancia realizadas desde el móvil.

Una vez activado el CCB deberá ingresarse el código PIN para desactivarlo a fin de permitir al abonado realizar una llamada. Sin embargo, con el CCB el abonado debe recordar reactivar dicho servicio, mediante el uso de un PIN, si desea restablecer el bloqueo de esas llamadas.

Con el ACB, en cambio, el bloqueo se restablece automáticamente después de que la estación móvil se torna inactiva en la red, sin necesidad de que el abonado tome ningún tipo de medida. Si el abonado tiene tanto CCB como ACB y se envía un mensaje de inactividad al HLR, se implementa el nivel de bloqueo más restrictivo. Por ejemplo, si un abonado tiene CCB-2 (bloqueo de todas las llamadas internacionales) y ACB-3 (bloqueo de todas las llamadas salientes), cuando se reciba un mensaje de inactividad se bloquearán todas las llamadas salientes provenientes del móvil.

3.4.3 FUNCIONALIDAD DE INHIBICIÓN DEL CÓDIGO PIN EN EL HLR

La Inhibición del código PIN en el HLR es una mejora del servicio ACB existente. Esta mejora brinda al operador la opción de enmascarar la contraseña del procedimiento del abonado a fin de evitar que los distribuidores celulares con acceso al HLR descubran dicha contraseña.

El comando HSSDP inicia un listado de los datos del abonado en el HLR. Si el abonado tiene ACB, ese listado puede contener la contraseña del procedimiento (código PIN).

El beneficio brindado por esta mejora consiste en proporcionar a los operadores la capacidad de restringir la posibilidad de descubrir el Código PIN del abonado, lo cual evita el posible fraude y uso indebido por parte de aquellos que tienen acceso al HLR.

3.5 NOTIFICACIÓN AUTOMÁTICA DE NO-COINCIDENCIA DEL ESN

Este servicio permitirá que todos los eventos de no-coincidencia del ESN detectados por el sistema sean enviados a un dispositivo de entrada/salida (especificado por el operador) exclusivamente dedicado a la notificación automática de esos eventos. Este servicio es aplicable a los eventos de no-coincidencia del ESN detectados en el HLR y el MSC.

3.5.1 BENEFICIOS

La notificación automática de no coincidencia del ESN informa al operador acerca de la no-coincidencia del ESN permitiéndole tomar medidas inmediatas a fin de encontrar la causa de ella, lo que conducirá a una mayor satisfacción del cliente. De lo contrario, los clientes legítimos se quejarían al operador porque no reciben servicio. Esta Notificación advierte al operador de que se ha producido una no-coincidencia, de modo que pueda solucionar la situación más rápidamente.

3.5.2 DESCRIPCIÓN

Un evento de no-coincidencia del ESN se produce cuando el ESN que se envía a través del aire no coincide con el ESN del abonado que está almacenado en su registro.

La no coincidencia del ESN puede producirse tanto en el MSC como en el HLR. Distintas situaciones pueden conducir a eventos de no-coincidencia del ESN detectados por el sistema, por ejemplo:

- Un móvil fraudulento que intenta un acceso ilegal al sistema
- ESN de un abonado ingresado en forma incorrecta en el registro de abonado del HLR. En consecuencia, un evento de no-coincidencia del ESN será detectado en el HLR cuando el abonado intente acceder al sistema.
- Respuestas al paging provenientes de móviles fraudulentos que pueden estar intentando "robar" un canal vocal.

Sin la notificación automática de no-coincidencia del ESN el operador no sabrá cuándo al abonado se le ha negado el servicio debido a la no-coincidencia de un número ESN. El solo hecho de la no-coincidencia de números ESN no necesariamente significa que se esté cometiendo fraude.

Simplemente podría ser un caso de ingreso incorrecto del ESN en el registro de abonado del HLR, como se indicó anteriormente.

3.6 BLOQUEO DE LLAMADAS ANTE LA DETECCIÓN DE FRAUDE, Y DETECCIÓN DE ACTIVIDAD FRAUDULENTA

El servicio de Detección de Actividad Fraudulenta (*FAD: Fraud Activity Detection*) es una función de vigilancia *online* que reporta posibles eventos fraudulentos relacionados tanto con las llamadas como con las actividades de subscripción.

El servicio FAD identifica llamadas específicas y otras actividades que podrían indicar el uso fraudulento del sistema. Dicho servicio detecta el fraude en una red monitoreando la actividad de las estaciones móviles en el centro de conmutación móvil/registro de ubicaciones visitante (MSC/VLR) y el HLR.

Cuando se detectan estos eventos se registran los elementos que probablemente pudieran interpretarse como fraude.

Los eventos pueden enviarse a un dispositivo de Entrada/Salida (E/S), donde una función de reporte genera un listado que contiene el número de la estación móvil y un código de motivo para cada evento. La otra posibilidad es que cuando se detecte y verifique un fraude se active automáticamente el bloqueo de llamadas ante la detección de fraude. Los futuros intentos de acceso por parte del abonado bloqueado se enrutarán automáticamente hacia un anuncio o al personal de atención al cliente, a efectos de tomar las medidas pertinentes.

3.6.1 BENEFICIOS

Los servicios de detección de actividad fraudulenta y bloqueo de llamadas ante la detección de fraude son herramientas efectivas para descubrir y combatir el fraude celular. Estos servicios detectan en muy amplio rango de actividades fraudulentas que pueden causar los tipos de fraude por clonación, generación aleatoria de ESN/MIN y "robo".

3.6.2 DESCRIPCIÓN

Los siguientes eventos activan el bloqueo de llamadas ante la detección de fraude:

- Intento de llamada detectado en el caso de un abonado marcado como ocupado.
- Acceso de registro de un abonado marcado como ocupado.
- Mensaje de cancelación de localización recibido de un abonado marcado como ocupado.
- Respuesta o respuestas desconocidas al paging en el caso de un abonado marcado como ocupado.

- Múltiples respuestas desconocidas al paging intercentrales en el caso de un abonado marcado como ocupado.
- Registro prematuro.
- Violación co-DCCH y co-canal detectada para las respuestas al paging.
- No-coincidencia entre Capacidad/Modo del Canal de Control detectada para acceso de originación.
- No-coincidencia entre Capacidad/Modo del Canal de Control detectada para acceso de registro.
- Llamada de servicio recibida de un abonado marcado como ocupado.

El operador puede especificar tres parámetros para el bloqueo de llamadas ante la detección de fraude:

- El tipo de abonado
  - Con o sin ACB o CCB
  - Todos los abonados
  - Ningún abonado (servicio desactivado)
- Los eventos utilizados para activar el bloqueo de llamadas ante la detección de fraude
- El nivel de bloqueo de llamadas asignado para los abonados sin las clases ACB o CCB

Por ejemplo, existe la posibilidad de los siguientes casos mutuamente excluyentes:

a. El abonado tiene ACB. Si no está activo, el bloqueo de llamadas ante la detección de fraude lo activará. Para volver a obtener acceso total el ACB debe desactivarse con el código (PIN). Este bloqueo de llamadas ante la detección de fraude puede ser transparente para el abonado (ya que él puede no saber por qué se ha implementado el bloqueo).

b. El abonado tiene CCB. Si no está activo, se activa automáticamente. Para volver a obtener acceso total el CCB debe desactivarse con el código PIN.

c. Si el abonado no tiene CCB o ACB, se modifica la clase de Bloqueo de Llamadas (CBA) de su perfil a fin de posibilitar la realización de determinadas llamadas originadas. En este caso, el abonado puede ser informado de que el móvil está bloqueado y deberá contactarse con el operador para volver a obtener acceso total.

3.6.3 ADMINISTRACIÓN

Se proporcionan comandos para iniciar (MTFDI), detener (MTFDE) e imprimir (MTFDP) el status del servicio FAD. Existe un dispositivo de E/S dedicado para reportar los eventos que pudieran interpretarse como fraudulentos. El reporte incluye el Número de Estación Móvil (MSNB) y un código de motivo.

Se ha asignado una categoría de impresión exclusiva a los datos de eventos de colisión de llamadas para posibilitar su fácil clasificación a fin de distinguirlos de los demás datos de E/S. Antes de ser enviados al dispositivo de E/S los eventos sospechados de fraudulentos se almacenan en un buffer.

Cuando el espacio ocupado en el buffer excede un nivel específico el sistema genera una alarma. Se especifica un parámetro dependiente de la aplicación a fin de determinar el porcentaje de ocupación del buffer. La alarma se desactiva cuando la cantidad de eventos del buffer disminuye a menos del cinco por ciento del nivel de ocupación especificado.

La ocupación del buffer también depende de la velocidad a la que puede enviar los eventos al dispositivo de E/S. La cantidad máxima de eventos que se pueden enviar al dispositivo de E/S está limitada por la velocidad (en baudios) de dicho dispositivo.

3.6.4 PRESTACIONES

El servicio FAD ofrece al operador una herramienta poderosa para detectar el uso fraudulento del sistema celular. No obstante, al utilizar este servicio se debe tener en cuenta que en algunos casos las colisiones de llamadas reportadas son ocasionadas por accesos de abonados legítimos. Estos accesos podrían producirse cuando el sistema no detecta la liberación de la llamada y el abonado intenta posteriormente un acceso de originación, o cuando el sistema no elimina una localización temporaria del abonado como resultado de fallas de señalización y recibe posteriormente otro acceso.

3.7 DESCONEXIÓN DE LLAMADAS

La desconexión de llamadas es un servicio que permite al operador terminar todas las derivaciones de llamadas asociadas con una llamada que se considera fraudulenta, incluyendo cualquier llamada en espera. Este servicio también incluye la supervisión de llamadas prolongadas, lo que permitirá a los operadores monitorear y reaccionar ante llamadas que se extiendan durante un período anormalmente extenso. Las llamadas prolongadas detectadas pueden desconectarse en forma manual, utilizando comandos, o automáticamente mediante el servicio de desconexión de llamadas.

3.7.1 BENEFICIOS

El servicio de desconexión de llamadas proporciona a los operadores comandos que desconectan las llamadas que se consideran fraudulentas y les permite supervisar las llamadas prolongadas, que tienen mucha mayor probabilidad de ser fraudulentas. Si se determina que una llamada es fraudulenta, o si el operador desea limitar esas llamadas de sus clientes, puede terminarla inmediatamente, así como todas las derivaciones de la misma, minimizando de ese modo cualquier pérdida adicional asociada con la llamada.

3.7.2 DESCRIPCIÓN

La supervisión de llamadas prolongadas permitirá a los operadores monitorear llamadas y tomar medidas ante las que se prolonguen durante un período anormalmente extenso. Una llamada prolongada es aquella que excede un límite de tiempo especificado por comandos. La duración monitoreada de una llamada comienza a partir de la recepción de la respuesta del abonado B. La duración incluye todos los estados de la llamada (por ejemplo, llamada retenida) hasta la desconexión.

Si la duración de una llamada excede el límite de tiempo se emite un listado. Las llamadas prolongadas detectadas pueden desconectarse en forma manual, utilizando comandos, o automáticamente mediante este servicio.

El servicio de desconexión de llamadas también permite al operador terminar todas las derivaciones de llamadas asociadas con una llamada considerada fraudulenta, incluyendo todas las llamadas en espera. Un nuevo grupo de comandos activa o desactiva la función. Uno de esos comandos permite al operador especificar el MIN del abonado, el Número de Abonado (SNB) asociado con la llamada que ha de desconectarse. Las llamadas de emergencia no se desconectarán.

La desconexión se produce dentro de los 3 a 5 segundos después de emitido el comando. El mismo operará sobre las llamadas tanto originadas por abonados móviles como destinadas a ellos. Se dispondrá de un contador para registrar la cantidad de llamadas desconectadas. Los registros TT incluirán el motivo de la desconexión de la llamada.

3.8 INHABILITACIÓN DE LLAMADAS POR CELDA INDIVIDUAL

3.8.1 BENEFICIOS

El servicio de inhabilitación de llamadas por celda individual posibilita al operador evitar rápidamente la iniciación de llamadas desde un emplazamiento de celda en que muchas estaciones móviles se comportan de modo fraudulento. También pude utilizarse, por ejemplo, en emplazamientos de celdas especiales, durante la noche, en áreas en que el fraude es un problema muy común.

3.8.2 DESCRIPCIÓN

Esto significa que puede elegirse un emplazamiento de celda especial y todas las estaciones móviles de esa celda tendrán bloqueadas la iniciación de llamadas, aunque no obstante podrán efectuar llamadas a las estaciones móviles dentro de la celda.

La inhabilitación de llamadas se realiza utilizando comandos MML para especificar la ruta MBLT que ha de inhabilitarse. El servicio de inhabilitación de llamadas por celda individual permite a los operadores evitar la iniciación de una llamada en una celda, dependiendo de la troncal móvil de líneas bidireccionales (MBLT) entrante.

3.9 PROTECCIÓN CONTRA EL USO INDEBIDO DEL PUERTO DE ROAMER

Un MSC brinda soporte a las llamadas realizadas a los abonados móviles que están efectuando *roaming* en su área o áreas de servicio, designando en el sistema uno o más puertos para que sirvan como puertos de *roamer*. El servicio de protección contra el uso indebido del puerto de *roamer* tiene como ventaja principal, evitar el uso fraudulento del mismo, asegurando que las llamadas se cursen hasta su destino sólo si el abonado móvil está en el área atendida por ese puerto.

3.9.1 DESCRIPCIÓN

3.9.1.1 Selección de llamadas entrantes en dos etapas

En una red, un MSC puede atender una o más áreas. Cuando existe esta configuración, se asignará un puerto de *roamer* a cada área y un número piloto a cada puerto (ver Figura 3.12). La configuración mostrada en la figura representa un MSC que presta servicio a tres ciudades, cada una de las cuales es atendida por un puerto de *roamer*.

La función de selección de llamadas entrantes en dos etapas permite a quién efectúa una llamada comunicarse con abonados que efectúan *roaming*, utilizando un procedimiento de marcación en dos etapas. Primero, quien efectúa la llamada marca el número de abonado móvil, como de costumbre, después de lo cual escuchará un anuncio grabado indicándole que marque el número piloto del puerto de *roamer* donde esta registrado dicho abonado.

Una vez marcado el número piloto, el receptor de códigos de teclado le proporciona un segundo tono de discado. Al recibirlo desarrolla la segunda etapa del procedimiento, marcando el número del abonado móvil. Finalmente, el MSC convierte el número marcado en el número temporariamente asignado al abonado móvil que efectúa *roaming*.

Cuando el MSC recibe una llamada vía el puerto del *roamer* se produce el paging. Al recibir una respuesta al paging de la estación móvil, el MSC efectúa una verificación a fin de asegurarse de que la respuesta se haya originado en una celda atendida por ese puerto de llamada se curse hasta su destino. En caso contrario, quien efectúa la llamada entrante será enrutado según las instrucciones de los datos de la central.

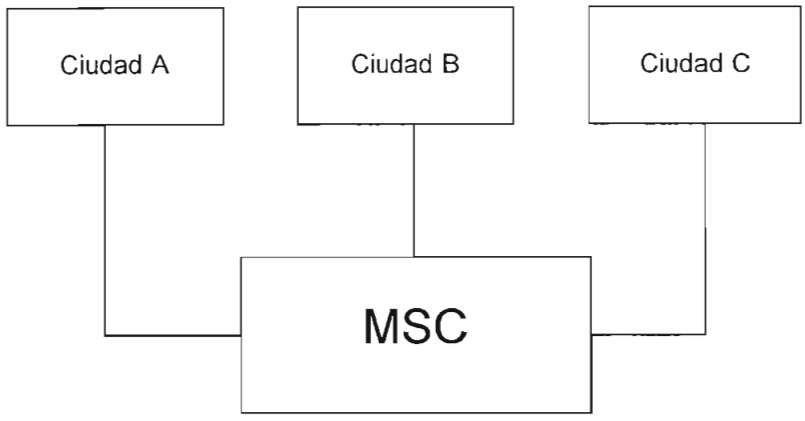


Figura 3.12 MSC que Atiende a Tres Ciudades

Ciudad A: Número Piloto del Puerto de *Roamer* NPA NXA ROAM
Ciudad B: Número Piloto del Puerto de *Roamer* NPA NXB ROAM
Ciudad C: Número Piloto del Puerto de *Roamer* NPA NXC ROAM

3.9.1.2 Protección contra el uso indebido del puerto de roamer

En la configuración presentada en la Figura 3.12, un MSC atiende a tres ciudades. El servicio de protección contra el uso indebido del puerto de *roamer* limita el paging a las celdas atendidas por el puerto de *roamer* cuyo número piloto se marcó.

Este servicio evita que un cliente complete llamadas de larga distancia pero se le facturen como llamadas locales. Por ejemplo, a un cliente de la ciudad A no se le permite cursar una llamada a un abonado móvil que ha efectuado *roaming* a la ciudad C utilizando el número piloto del puerto de *roamer* reservado para la ciudad A (NPA NXA ROAM).

3.9.1.3 Mejoras a las llamadas a puertos de roamer y al acceso local

Las mejoras a las Llamadas a Puertos de *Roamer* y al Acceso Local son mejoras realizadas al servicio existente, Protección Contra el Uso Indebido del Puerto de *Roamer.* Se brindan dos mejoras clave.

La primera solo afecta al MSC y no al HLR, mientras que la segunda afecta al VMSC como al HLR y requiere que ambos nodos tengan el mismo procesador para que la misma funcione.

La primera mejora provoca una reducción importante de los datos de central necesarios para establecer la funcionalidad de acceso local a través de un puerto de *roamer*. En los datos de central se define solo una ruta, en vez de definir una ruta para cada HLR de la red celular. La segunda requiere la transferencia de un indicador de puerto de *roamer* en varios mensajes IS-41, como elemento de datos privado, a fin de brindar soporte a las transferencias provenientes tanto del GMSC (*Gateway Mobile Switching Center*) como del VMSC.

El beneficio de esta mejora es la simplificación de la Configuración del Puerto de *Roamer*, lo que permite un mayor aprovechamiento de la red.

3.9.2 ADMINISTRACIÓN

La base de datos del MSC proporciona comandos para agregar y eliminar celdas a ser atendidas por un puerto de *roamer*. Adicionalmente, mediante comandos pueden obtenerse listados que especifican todas las celdas atendidas por un puerto de *roamer*.

3.10 VERIFICACIÓN DEL NÚMERO DE SERIE Y DEL NÚMERO DE ESTACIÓN MÓVIL

3.10.1 Beneficios

El servicio de verificación del número de serie y el número de estación móvil reduce la cantidad de llamadas fraudulentas, así como la cantidad de solicitudes de actualizaciones de localización y validación innecesarias procesadas por el sistema local del abonado, es decir el HLR.

3.10.2 Descripción

El servicio opera del siguiente modo en los nodos de la red:

1. En el primer acceso al sistema en una central visitada, el MSC verifica el formato y rango del ESN y el Número de Estación Móvil (MSNB) recibidos. Durante los accesos posteriores, se verifican el ESN y el MSNB comparándolos con los almacenados en los datos de abonado del abonado móvil.
2. El HLR bloqueará a los abonados cuyos ESNs no hayan sido previamente almacenados en un HLR por el operador del sistema. Esta función particular requiere que el operador ingrese manualmente a los datos del HLR todos los ESNs válidos.
3. Si no se ha ingresado ningún ESN, el HLR almacena automáticamente en el registro del abonado el ESN recibido durante un acceso al sistema.

El segundo y tercer ítem no son aplicables a los *roamer*s manuales y son mutuamente excluyentes. Por lo tanto, no pueden estar simultáneamente activos en un sistema celular.

Los párrafos siguientes tratan sobre la capacidad del servicio de verificar el número de serie electrónico y el número de estación móvil.

3.10.2.1 Verificación del número de serie electrónico

El proceso de verificación se compone de dos pasos:

- Verificación de formato del ESN
- Verificación del ESN

Verificación de formato del ESN

La primera vez que un abonado móvil visitante (*roamer*) accede al sistema, o sea que se le asigna un registro de visitantes por primera vez, el MSC visitado valida el formato del ESN de la estación móvil antes de enviar al HLR una solicitud de validación de número de serie y un mensaje de actualización de localización. Esa verificación de formato asegura que el código del fabricante y el área reservada del número de serie se ajusten a los límites previamente establecidos por el operador.

Verificación del ESN

La verificación del ESN recibe soporte para *roamer*s del sistema tanto automáticos como manuales. Un *roamer* automático es el que utiliza los servicios de un sistema celular que emplea los protocolos de la Parte de Usuario de Telefonía Móvil (MTUP) patentada por la Norma Provisoria 41 (IS-41) de la Asociación de Industrias Electrónicas. Estos protocolos facilitan la señalización entre centrales hasta el punto en que los servicios de comunicaciones están uniformemente disponibles a través de la red, prescindiendo del tipo de central que presta los servicios o de la localización física del abonado. Un *roamer* manual es el que ingresa desde otro sistema que no forma parte de la red de *roaming* automático.

Cuando un *roamer* automático se registra en un MSC y accede al sistema, o sea que se han recuperado los datos del abonado del sistema local y se han almacenado en un registro del MSC visitado, éste último verifica que el ESN recibido de la estación móvil durante el acceso y el ESN almacenado en los datos de abonado sean idénticos. Cuando un *roamer* manual intenta el acceso al sistema por primera vez, el ESN incluido en ese acceso se almacena en el registro de visitantes del MSC visitado. El número de serie se verifica comparándolo con una lista de bloqueo en el MSC visitado y se envía a una oficina de *clearing* para su comprobación.

Casos de tráfico

El MSC visitado responde de modo diferente cuando detecta un ESN no válido, según el tipo de *roamer* y tipo de acceso al sistema recibido, como se detalla a continuación:

- Al recibir una respuesta al paging de un *roamer* manual que no tiene ningún ESN previamente almacenado en el registro de visitantes, el MSC verifica el formato del ESN recibido en dicha respuesta. Si el ESN no aprueba la verificación, el MSC cancela la llamada.
- Al recibir una respuesta al paging de un *roamer* registrado, el MSC lleva a cabo la verificación del ESN. Si el ESN recibido no aprueba la verificación, el MSC ignora la respuesta al paging.
- Al recibir un acceso de originación, el MSC verifica el formato del ESN y se asegura que los ESNs recibidos y almacenados coincidan. Si cualquiera de esas verificaciones da por resultado un ESN no válido, el MSC vuelve a enrutar la llamada de acuerdo con los datos de la central.
- Al recibir un acceso de registro, el MSC verifica el formato del ESN y se asegura que los ESNs recibidos y almacenados coincidan. Si cualquiera de esas verificaciones da por resultado un ESN no válido, el MSC visitado envía un reconocimiento de registro a la estación móvil, al tiempo que ignora el acceso de registro. El reconocimiento se transmite a fin de evitar que la estación móvil realice accesos de registro repetidos.

3.11 HUELLA DIGITAL DE RADIO FRECUENCIA

El servicio de inteligencia de los EE.UU. desarrolló una técnica que permite mantener registrados e identificados los movimientos de los grupos enemigos, denominada huella digital de radio frecuencia (*RF Fingerprint*). *Corsair Communications Inc., Palo Alto, California*, es actualmente la única compañía activa en el campo.

PhonePrint patentado por *Corsair* es un sistema de control de fraude, diseñado para prevenir servicios de robo usando teléfonos clonados. El sistema consiste de una serie de unidades de red localizadas en los sitios de celda de la operadora celular. Cada unidad en el sitio de celda revisa o chequea todas las llamadas fijadas por teléfonos celulares en esta área para detectar llamadas originadas de clones.

La tecnología *RF Fingerprint* identifica y desconecta las llamadas realizadas desde teléfonos clonados sin rastro de interferencia para el suscriptor celular. *PhonePrint* es una combinación de hardware y software que las operadoras celulares instalan en las estaciones base en áreas de alto fraude.

Una vez instalado, este caracteriza todos los teléfonos que requieren por el servicio (por monitoreo del canal de control reverso) y crea una base de datos de sus huellas de RF, o huellas digitales. La base de datos adquiere pronto los accesos para casi todos los usuarios activos en el área. En los siguientes requerimientos del servicio, este compara las huellas almacenadas con las entrantes. Si ellas no coinciden, la llamada es desconectada, eliminada antes de que sea completada.

De hecho, un usuario legítimo no notará cualquier cambio en el servicio, no ingresará códigos PIN, no habrá retrasos en la conexión. Los clonadores sin embargo escucharán el *setup* de la llamada y luego un silencio, producto de la desconexión.

PhonePrint trabaja sobre redes analógicas (AMPS y ETACS) como también sobre redes digitales (TDMA) para las operadoras inalámbricas que tratan de mejorar su tecnología. *PhonePrint* también suministra un nivel ideal de protección para redes donde la autenticación ya ha sido desplegada.

3.11.1 BENEFICIOS

PhonePrint es fácil para instalar, llena los espacios vacíos de la infraestructura celular existente, y opera en forma paralela con el procesamiento de llamadas. *PhonePrint* tuvo sus orígenes en el *TRW Inc.*, de la cual Corsair la convirtió en 1994. La compañía Cleveland, Ohio, desarrolló similares sistemas para usos militares. Tales sistemas, pueden decir que una unidad enemiga que se supone permanece en la posición X que de hecho se mueve hacia una posición Y, tiene una huella de RF asociada al radio de la unidad. Obviamente, este paso implica, que la huella digital de RF trabajará con cualquier teléfono, y de hecho, con cualquier transmisor. Esto es por lo tanto particularmente conveniente para los teléfonos celulares analógicos legales, los cuales no tienen defensas antifraude. Hasta ahora este sistema ha sido muy efectivo, según datos actuales, se han desconectado mas de 300 millones de llamadas en los EE.UU.

El sistema *PhonePrint* consiste de 5 componentes:

- Unidades de Radio Frecuencia (*RFU: Radio Frecuency Unit*).
- Sistema Central de Control (*SCC: System Control Center*).
- Servidor de Aplicación en Tiempo-Real (*RTAS: Real-Time Application Server*).
- Interface de Usuario *PhonePrint.*
- La Red *PhonePrint.*

Esos componentes son descritos en la figura 3.13

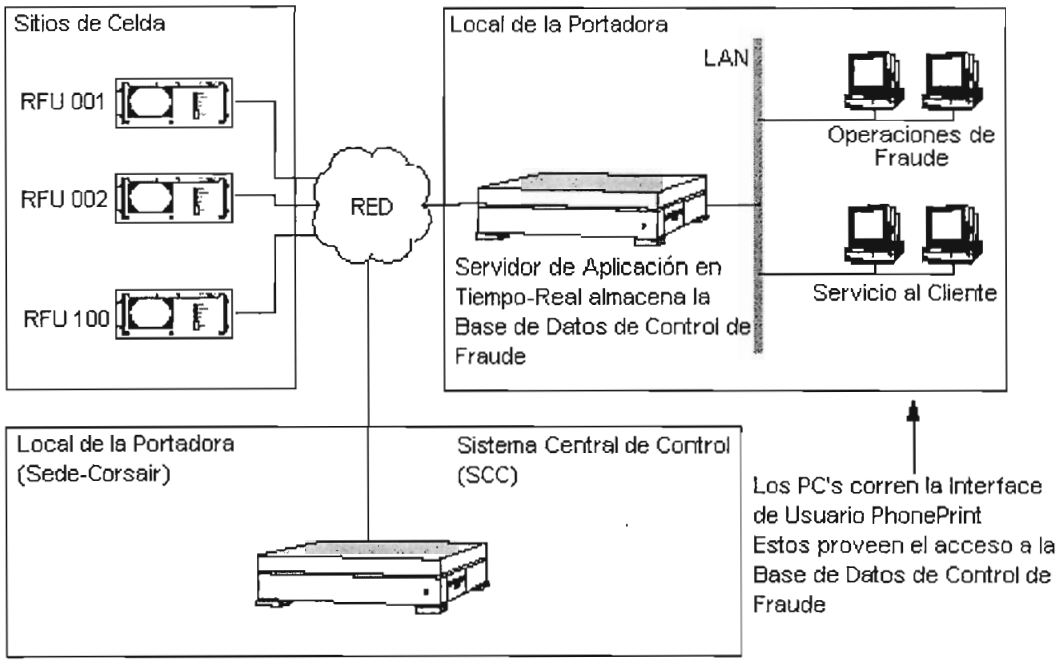


Figura 3.13 Componentes de un sistema PhonePrint

3.11.2 DESCRIPCIÓN

RF Fingerprint hace uso de las señales de RF emitidas por los teléfonos celulares. Los patrones exactos de la señal varían de un teléfono a otro, esta técnica analiza las señales para distinguirlas entre los teléfonos.

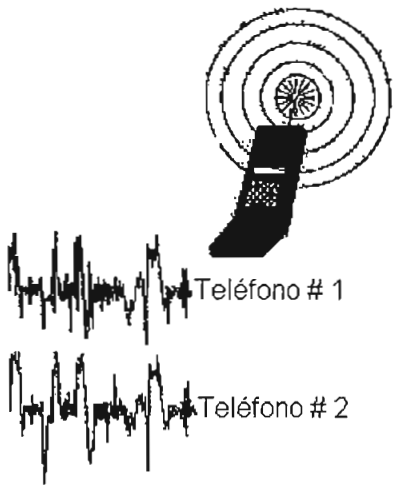


Figura 3.14 Señales de Radio Frecuencia (RF) de dos teléfonos celulares

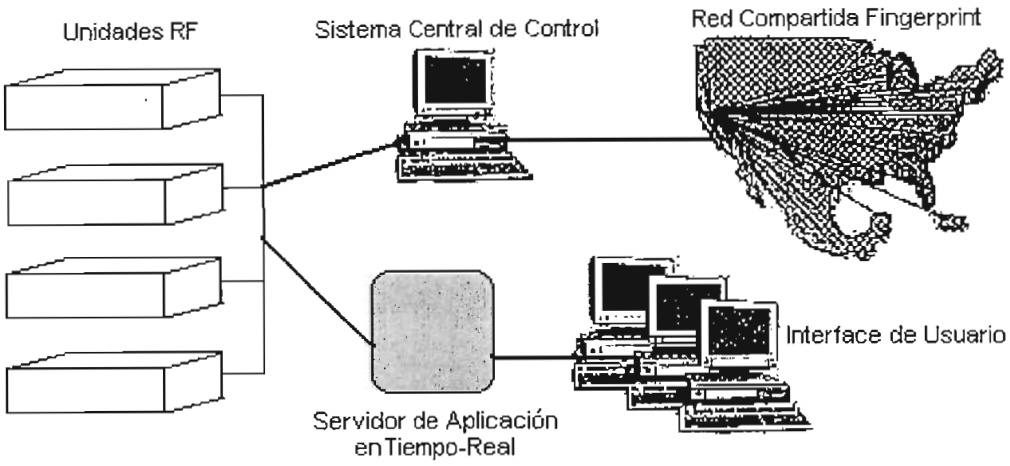


Figura 3.15 Arquitectura PhonePrint

3.11.2.1 Unidades de radio frecuencia

Una RFU captura las características de radio frecuencia de los teléfonos celulares midiendo su huella digital para cada evento, y decide cuales llamadas son fraudulentas. Los RFUs son instalados en los sitios de celda de la operadora celular y se comunican con el SCC y RTAS vía Red *PhonePrint*. Para configurar apropiadamente los RFUs, tanto el código de color digital como el canal de control son necesarios.

Características del RFU

- Colecta la señal de RF sobre el canal de control reverso.
- Procesa la señal y forma la huella digital de RF.
- Compara las huellas digitales con las de la base de datos.
- Desconecta las llamadas fraudulentas en segundos.

El RFU es una unidad montable de 7 pulgadas de altura y se puede montar en un rack de 19 o 21 pulgadas.

Proceso de desconexión de llamada

PhonePrint ofrece dos métodos para desconectar las llamadas fraudulentas: desconexión distribuida de llamadas y desconexión de llamadas conmutador bajado (*switch-based*). En instalaciones con desconexión distribuida de llamadas, los RFUs desconectan las llamadas fraudulentas en la estación base. El RFU monitorea el canal de control de adelanto, sentido directo (FOCC) para determinar la asignación del canal de voz (VCA) de las llamadas fraudulentas.

Después de la asignación VCA, el RFU sintoniza a ese VCA y transmite una señal de desconexión en el receptor de la estación base, desconectando la llamada del teléfono fraudulento. En instalaciones con desconexión de llamadas conmutador bajado, el RFU envía una petición de desconexión de llamada a la Aplicación de Desconexión (TDA) en el Servidor de Aplicación en Tiempo-Real (RTAS). El TDA envía una petición de desconexión al conmutador central, el cual desconecta la llamada fraudulenta.

3.11.2.2 Sistema central de control

El Sistema Central de Control carga nuevas huellas digitales desde los RFUs y usa estos datos para actualizar la base de datos master *RF Fingerprint*. Este también provee control administrativo sobre el sistema de entrada.

Enlazado al SCC, la red de *Roaming PhonePrint* conecta mercados con sus patrones de *roaming* para protegerlos contra el fraude.

Figura 3.16 Sistema Central de Control (SCC)

El SCC maneja la base de datos *PhonePrint* del mercado celular. Estos componentes del software central desempeñan tareas claves en la base diariamente:

- Características de procesos RF acerca de cada teléfono observado por los RFUs y desarrolla huellas digitales RF.
- Actualiza la base de datos RF fingerprint de cada RFU.
- Genera reportes.
- Envía datos al RTAS – estos datos acceden a través de la interface de usuario *PhonePrint*.
- Intercambia huellas digitales RF fingerprint con los SCCs de otros mercados celulares para desconectar llamadas en tiempo real cuando haya fraude por *roaming*.

El SCC reside en una estación de trabajo Sun (*Sun workstation*). El SCC puede estar localizado en la sede de la operadora celular. El SCC se comunica con los RFUs, RTASs y otros SCCs vía Red *PhonePrint*.

3.11.2.3 Servidor de aplicación en tiempo-real

El RTAS recibe información y peticiones de desconexión y almacena los datos acerca de todos los números MINs en el mercado. Dos aplicaciones soportan las funciones del RTAS: la Aplicación de Desconexión (TDA) ubicada en el servidor y la Aplicación de Interface de Usuario (UIA) ubicada en la estación de trabajo.

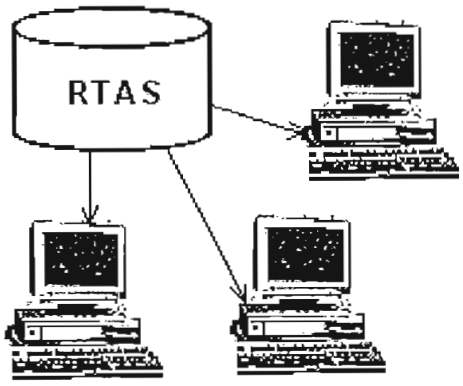


Figura 3.17 Servidor de Aplicación en Tiempo Real (RTAS)

Aplicación de desconexión

La Aplicación de Desconexión (*TDA: Tear-down Application*) recibe peticiones de desconexión de llamadas desde los RFUs. En instalaciones con desconexión de llamadas conmutador bajado, la aplicación de desconexión envía un mensaje al conmutador celular en un centro de conmutación móvil (MSC) requiriendo que el conmutador desconecte la llamada. Tanto con sistemas de desconexión distribuida como de desconexión conmutador bajado, el TDA adelanta la desconexión de llamada a la aplicación de interface de usuario.

Aplicación de interface de usuario

La Aplicación de Interface de Usuario (*UIA: User Interface Application*) almacena la base de datos de control de fraude, la base de datos es un sistema de administración que contiene los datos de los teléfonos que *PhonePrint* ha observado en el mercado celular. Por ejemplo, la base de datos de control de fraude contiene una tabla mostrando el *status* de todos los MINs y una tabla que muestra los MINs que la operadora celular especifica como MINs "siempre permitidos", para los cuales *PhonePrint* nunca desconectará las llamadas. La operadora celular empleada puede acceder a la base de datos de control de fraude mediante la interface de usuario.

El RTAS reside en una estación de trabajo en el sitio físico de la operadora celular. En pocas palabras el RTAS entrega en tiempo real información a la interface de usuario de la operadora para monitorear la información de *PhonePrint*, analizar los datos fraudulentos y generar reportes.

El RTAS se comunica con los RFUs y con los SCCs vía Red *PhonePrint* y con la interface de usuario *PhonePrint* vía red de área local (LAN).

3.11.2.4 Interface de usuario PhonePrint

La interface de usuario *PhonePrint* permite a las operadoras celulares acceder a la base de datos de control de fraude. La interface de usuario *PhonePrint* corre en cualquier computador personal compatible con Microsoft Windows 3.1, 3.11, Windows 95 o Windows NT. La interface de usuario ayuda a cumplir con las siguientes tareas:

- Explorar información de desconexión de llamadas por un tiempo muy lejano atrás, por ejemplo 45 días, como también de sucesos recientes, como de 3 minutos.
- Explorar la base de datos por fecha, hora, sitio ID, MIN y dígitos marcados, como también por otros criterios.
- Usar la Interface de Usuario para observar la historia de desconexión de llamadas de un MIN dado para responder a inquietudes de los usuarios.
- Generar varios reporten que incluyen:
    - Reporte Sumario del Sitio: El reporte puede ser esquematizado para lotes de salida.
    - Reporte de Desconexión (Local/*Roaming*).
    - Reporte de validación del status del MIN.
    - Reporte de status "siempre permitido" (MINs y Logs): El reporte puede ser esquematizado para lotes de salida.

- MINs sospechosos (Probable fraude).
- Red *PhonePrint.*
- Datos de *Roaming* (en Tiempo Real).

Tipos de usuario

La interface de usuario *PhonePrint* está diseñada para alojar una variedad de usuarios, quienes requieren acceso a diferentes datos. Por ejemplo, algunos clientes requieren acceso a datos ESN y la capacidad de añadir o remover MINs de la lista "siempre permitidos", mientras otros usuarios requieren no acceder a los datos ESN, sino simplemente revisar la lista "siempre permitidos".

Para alojar esos usuarios diferentes, *PhonePrint* define un rango de tipos de usuario, cada uno con diferentes privilegios de acceso.

El control de acceso presenta en su operación:

- Dos modos de Operación:
  - Normal.
  - Restringida.
- Niveles de Acceso "Estándar":
  - Solicitud del Cliente.
  - Administración de la Solicitud del Cliente.
  - Operaciones de Fraude.

Figura 3.18 Interface de Usuario -Control de Acceso

Cada posición del usuario soporta un modo normal y restringido los cuales ocultan ciertos campos de archivos confidenciales.

Reportes

La interface de usuario permite crear y organizar 4 reportes:

Reporte del sumario del sitio. Este reporte es un sumario de llamadas que *PhonePrint* observa y desconecta en el mercado celular por día. Este reporte incluye tanto la información del sumario como la información sitio por sitio.

Reporte de desconexión. Este reporte muestra los detalles de cada llamada desconectada en el mercado celular por día. Este incluye el MIN, ESN, códigos de desconexión, modos de desconexión, dígitos marcados y el sitio donde la llamada fue desconectada, así como la fecha y la hora de desconexión. Para desconectar los MINs de otros mercados, este reporte identifica el mercado donde la desconexión ocurrió.

Reporte del status del MIN. Este reporte contiene información acerca de la validación y el índice de fraude de todos los MINs en el mercado celular local.

El *status* de validación indica si *PhonePrint* ha observado un adecuado número de intercepciones (en otras palabras, si el MIN es válido). El índice de fraude indica la probabilidad que el fraude ha ocurrido en un MIN particular.

Reporte del status siempre permitido. Este reporte provee información acerca de los MINs listados en la lista "siempre permitidos". Especialmente, puedes ver la fecha que el MIN fue añadido a la lista, el nombre del usuario que añadió el número MIN y el *status* del procedimiento.

Los niveles de acceso "Estándar":

- **Solicitud del cliente**
  - Reporte sumario de desconexión (ESN y ID del sitio de celda restringidos)
  - Control de acceso a la interface: puede solamente chequear el status de los MINs (ID del sitio de celda restringido)
- **Manejo de la solicitud del cliente**
  - Reporte sumario de desconexión (ESN y ID del sitio de celda restringidos)
  - Control de acceso a la interface: puede chequear el status de los MINs, como también editar la lista de acceso MIN (ID del sitio de celda restringido)
- **Operaciones de fraude**
  - Reporte sumario del sitio de celda
  - Reporte sumario de desconexión (ESN restringido)
  - Respuestas del status del MIN (ESN restringido)
  - Control de acceso a la interface: puede chequear el status del MIN, como también editar la lista de acceso MIN (ID del sitio de celda restringido)
  - Edita la lista "siempre permitidos"(MINs y Logs)

Características de operación clave

- **Alarmas en tiempo real recibidas en el SCC desde el RTAS y RFUs**
  - Detecta los enlaces de la red caídos (*downed*), el RFU no recibe intercepciones, y cambios del código de color

- Visualización de un sumario de alarma con la capacidad para penetrar en cada subsistema para más detalles

- **Configuración del RFU, herramientas de control y status**
  - Capacidad para instalar o verificar la configuración de uno, algunos, o todos los RFUs (cargar o descargar datos, etc.)
- **Centro de control Corsair**
  - Servidor localizado en Palo Alto, CA, y usado por operaciones Corsair para administrar todos los SCCs en la red de *roaming*
  - Difusión de los archivos de control para los SCCs
    - Actualiza de la lista NPA/NXX
    - Automáticamente configura los SCCs para añadir nuevos mercados para la red *roaming*
  - Recupera reportes y logs desde todos los SCCs para monitorear su desempeño

3.11.2.5 Red PhonePrint

La red *PhonePrint* consiste de la red de la operadora celular y de la red de *roaming* en tiempo-real. Usando la red de la operadora, la red *PhonePrint*, conecta todos los RFUs del mercado al SCC y al RTAS.

Usando la red de *roaming* en tiempo-real, la red *PhonePrint* conecta los SCC de diferentes mercados unos con otros. La Figura 3.19 muestra como los componentes *PhonePrint* son conectados a través de una Red *PhonePrint*.

Para mantener la seguridad de todos los datos, el sistema *PhonePrint* requiere de contraseñas (*passwords*) para el acceso de usuarios a cualquiera de sus componentes, así se definen niveles de acceso, suma/cambio de los perfiles del usuario por parte del administrador, y los usuarios del sistema pueden cambiar su propio *password*.

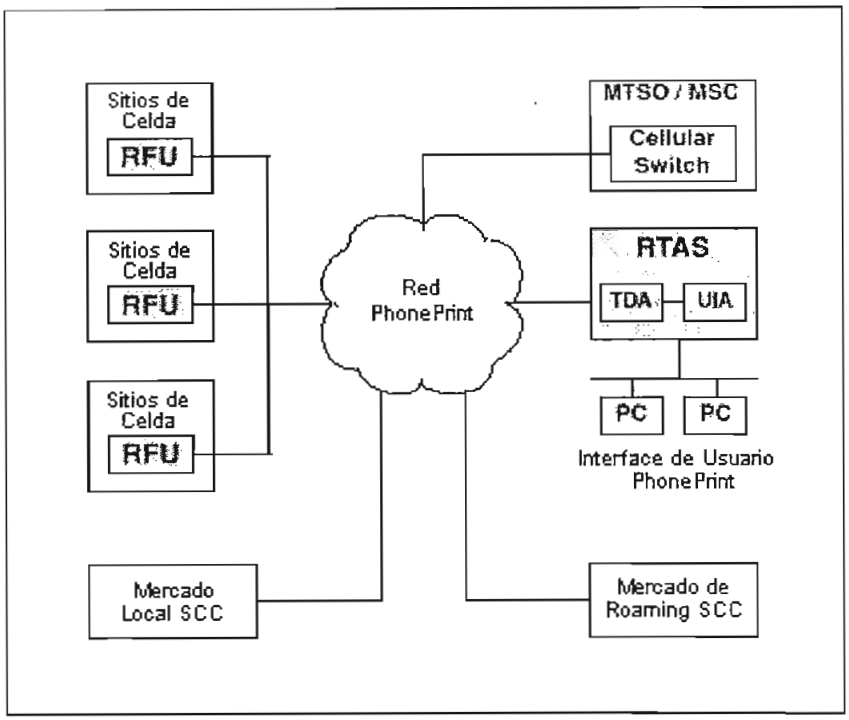


Figura 3.19 Red PhonePrint

En suma, el sistema puede ser configurado tal que los archivos transferidos entre el SCC y los RFUs son encriptados. La seguridad protege al tráfico de la red entre un SCC y un RTAS por transmisión de datos encriptados automáticamente. La información que no sea confidencial ni de contraseña es transmitida abiertamente.

La operación del sistema *PhonePrint* está conducida por cuatro funciones principales:

- Coleccionando y analizando señales de RF.
- Eliminando llamadas fraudulentas.
- Manejando la base de datos *RF fingerprint*.
- Proveyendo salida por las operadoras celulares y recibiendo entrada desde operadoras celulares.

3.11.2.6 Coleccionando y analizando señales de RF

Los RFUs *PhonePrint* coleccionan y analizan las señales de RF desde los teléfonos celulares. Un receptor de RFUs colecciona la señal y la tarjeta de procesamiento digital de los RFUs analizan la señal.

a. **Colección:** Los receptores en los RFUs monitorean la actividad del canal de control reverso (RECC) en un sitio de celda. En particular, los RFUs monitorean y coleccionan la señal de datos RF para iniciación, respuestas de *paging* y registración. Cada evento, cada tiempo, el RFU captura una señal del teléfono móvil, esta acción es llamada intercepción. Por colección de intercepciones en el RECC, *PhonePrint* es capaz de construir la base de datos de huella digital rápida y exactamente. Después de capturar la señal el receptor la digitaliza y las envía a una tarjeta de procesamiento digital de señales (DSP). Digitalizando la señal permite al RF construir huellas digitales RF altamente confiables.
b. **Análisis:** La tarjeta de procesamiento digital de señales analiza una intercepción examinando las características específicas de la señal capturada. Porque de hecho en la fabricación y diseño de teléfonos celulares, esas características de la señal difieren de un teléfono a otro. La tarjeta DSP crea una representación digital única de la señal capturada. Esta representación digital es la huella digital RF (*RF fingerprint*).

- **Paso 1: Colección de señales para construir marcas**
  - Desplegar en sitios de alto tráfico para colectar la mayor cantidad de huellas digitales de los suscriptores.
  - Usar todos los eventos del RECC para madurar marcas rápidamente.
  - La Marca es considerada "madura" cuando 10 o más RECC interceptados han sido recibidos.
- La colección de la señal puede empezar inmediatamente.

- **Paso 2: Validación de las marcas**
  - Fase I- La operadora provee datos.
    - Números contactados, Dígitos Marcados Frecuentemente (FDD), etc.
  - Fase II- Validación de un solo grupo.
  - Fase III- Validación en Masa, etc.
- El acceso a la validación es fluido.
- En general, la base de datos puede contener > 90% validado, se puede tener MINs maduros dentro de 4 meses.

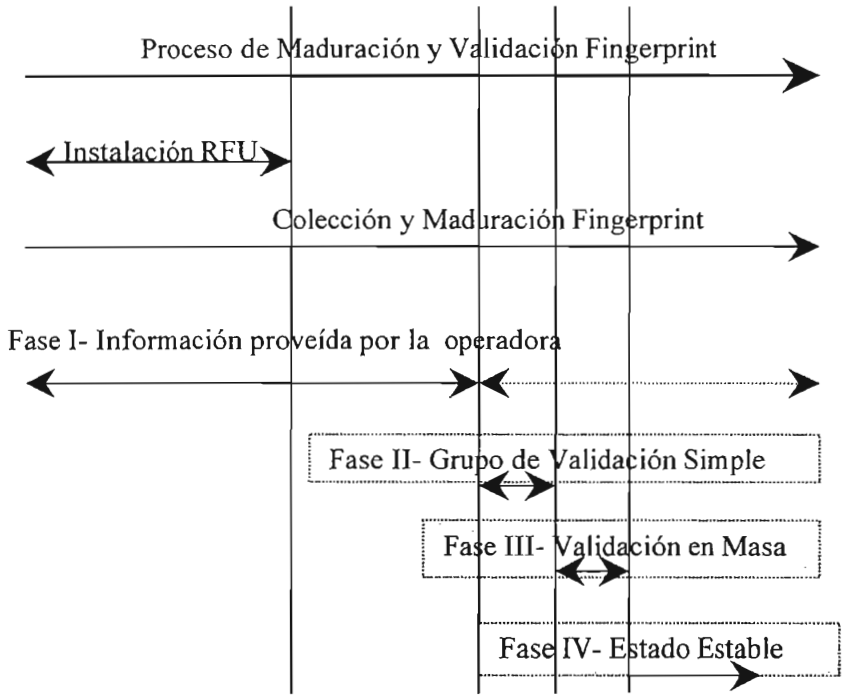


Figura 3.20 Proceso de Validación en el Tiempo

El RFU almacena las huellas digitales de RF interceptadas a lo largo de la información recopilada, tal como la hora, sitio de celda, MIN, ESN, número marcado e información de desconexión. Al final de cada día el RFU compila estos datos y los envía al SCC, donde este es incorporado en la base de datos fingerprint.

3.11.2.7 Desconexión de las llamadas fraudulentas

Después de colectar y analizar la señal de una llamada específica, el RFU decide si la llamada debería ser desconectada. Cada operadora celular puede especificar los MINs y los dígitos marcados que son siempre o nunca permitidos, ahí creando una unidad lógica para el RFU a seguir. Cuando el set lógico no dicta que una llamada está automáticamente conectada o automáticamente desconecta, compara la huella digital de la llamada interceptada con la huella del MIN de la llamada en la base de datos fingerprint.

Si la huella interceptada coincide con la huella digital del teléfono legítimo, el RFU registra la llamada y no toma acciones drásticas. Si la huella interceptada no coincide con la huella digital del teléfono legítimo, el RFU inicia el proceso de desconexión de llamada.

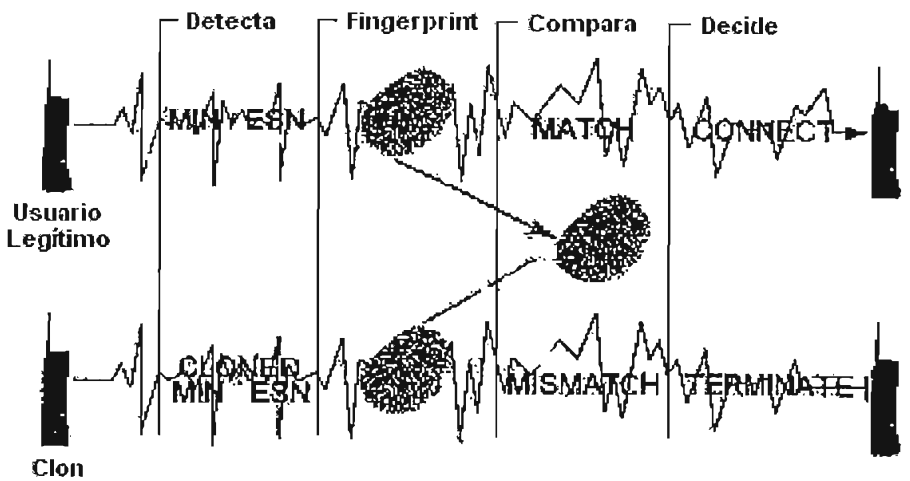


Figura 3.21 Como PhonePrint detecta el fraude? (Pasos)

La base de datos fingerprint contiene las huellas RF maduras y validadas del mercado. Después de hacer una huella madura, *PhonePrint* debe colectar 10 intercepciones, después de validar una huella, *PhonePrint* asegura que la huella pertenezca a un suscriptor legítimo.

En algunas instancias la base de datos puede no contener una huella digital madura y válida para un determinado MIN. En este caso el RFU puede utilizar métodos alternativos, tales como errores de fabricación para determinar si una llamada es legítima o no.

La huella digital de un teléfono hecho por un fabricante particular siempre fallará dentro de cierto rango. Si la marca interceptada no coincide con el rango asociado con el fabricante (determinado por el ESN interceptado) pero coincide con el rango asociado a otro fabricante, el RFU puede iniciar la desconexión de la llamada.

1. ***Roaming***: *PhonePrint* puede identificar y desconectar clones vagantes. En particular *PhonePrint* puede compartir huellas digitales con otros mercados protegidos por *PhonePrint*. Cuando el RFU detecta un MIN vagante, este determina el mercado del *roamer*. Para mercados con huellas digitales compartidas, el RFU envía una petición al SCC para la huella digital del *roamer*. El SCC enviará esta petición al SCC del *roamer*. Cuando la huella es recibida, tanto el SCC como el RFU guardarán la huella digital del *roamer* para configurar y eliminar la necesidad de requerimientos futuros. Peticiones para huellas digitales desde SCC de un *roamer* son tomadas en tiempo real, permitiendo el requerimiento del RFU para desconectar llamadas fraudulentas. Cuando el *roamer* está en frente de un mercado sin el servicio de huellas digitales compartidas, el RFU puede aplicar errores lógicos de fabricación.

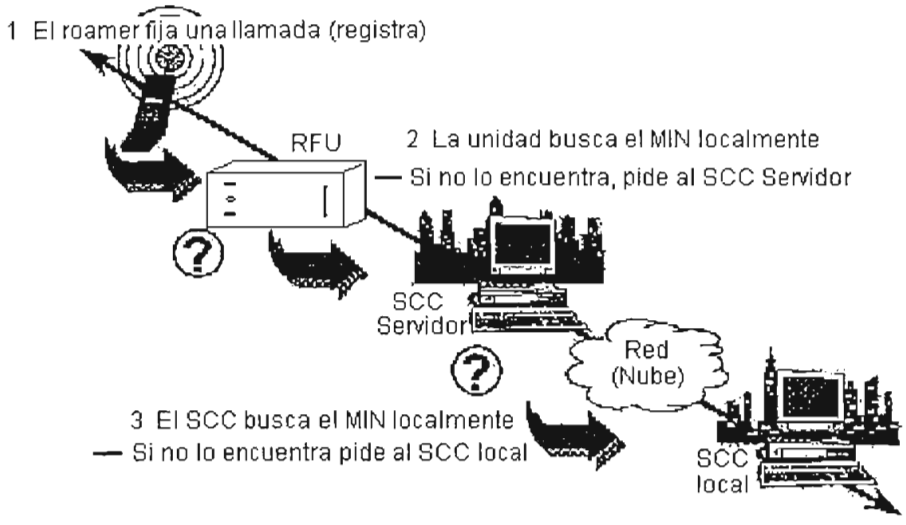


Figura 3.22 Fingerprint Compartida: "La pregunta"

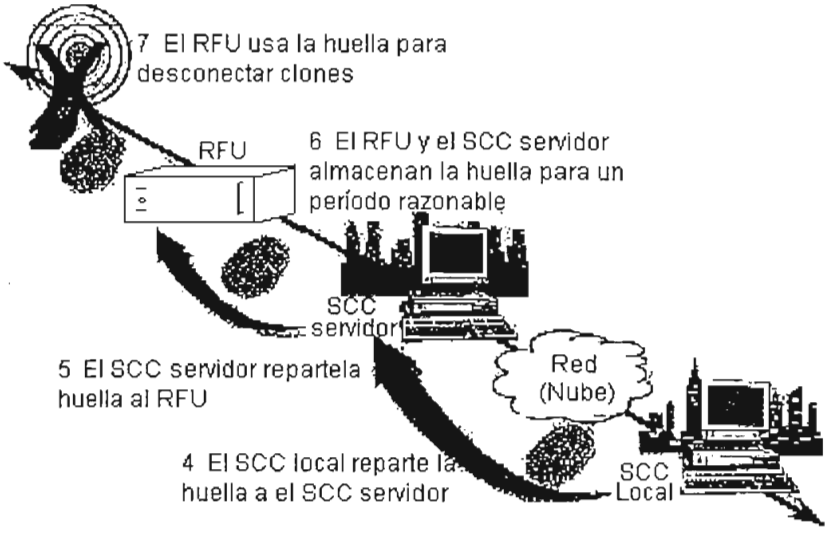


Figura 3.23 Fingerprint Compartida: "La respuesta"

2. **Proceso de desconexión:** Después de que el RFU identifica una llamada fraudulenta, éste inicia el proceso de desconexión. Dos tipos de desconexión son posibles en un RFU: desconexión de llamada por conmutador bajado y por desconexión distribuida. En la primera el RFU envía una petición de desconexión de llamada al TDA (localizado en el RTAS). El TDA transfiere este requerimiento directamente al conmutador y repetirá el mensaje hasta que el conmutador responda que la llamada ha sido desconectada o hasta que un tiempo especificado haya transcurrido.

El TDA también transfiere la información al UIA, permitiendo a la operadora celular que sucedió con la llamada, a través del Interface de Usuario. La figura 3.31 describe el proceso de desconexión conmutador bajado.

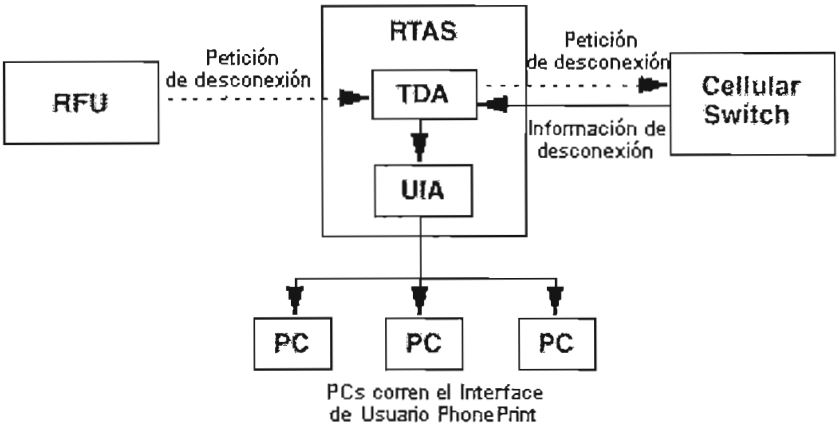


Figura 3.24 Desconexión de llamada switch-based

La desconexión de llamadas conmutador bajado tiene varias ventajas. Por ejemplo este servicio elimina los residuos de facturación asociados con llamadas desconectadas. Las llamadas pueden ser desconectadas aún después del *hand-off* a otros sitios de celda. Finalmente este servicio puede desconectar teléfonos digitales que usan canales de control analógicos.

En la desconexión distribuida, los RFUs desconectan las llamadas fraudulentas en la estación base. En esas instalaciones el RFU monitorea el canal de control de adelanto, sentido directo (FOCC) para determinar la asignación del canal de voz de llamadas fraudulentas. El RFU sintoniza el canal de voz asignado a la llamada y transmite una señal de desconexión en el receptor de la estación base, desconectando la llamada. Las llamadas son terminadas dentro de 3 a 5 segundos después de que el sistema celular emite la asignación del canal de voz en el canal de control de adelanto.

Arquitectura distribuida

- Características en tiempo real.
  - Huellas digitales en *roaming* compartido.
  - Interface del cliente.
- Características del lote.
  - Datos de alta resolución.
  - Edificación de huellas digitales sobre todas las señales en el RECC.
  - Colección de todos los datos.

Beneficios de la arquitectura distribuida

- Inteligencia de mercado completa.
  - Extensa base de datos sobre todos los MINs.
  - Edificación rápida de la base de datos por monitoreo de todas las actividades en el RECC.
  - Todas las llamadas son examinadas, así al primer intento de llamada fraudulenta sobre cualquier MIN es detectada inmediatamente.
- Colección de un conjunto de datos, es el corazón del requerimiento de diseño.

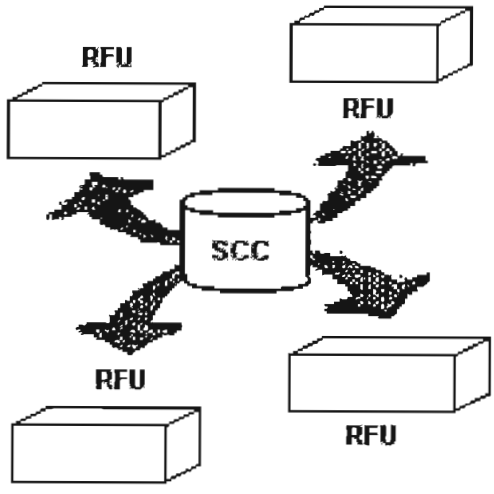


Figura 3.25 Arquitectura Distribuida

El sistema *PhonePrint* usa receptores en los RFUs para monitorear todas las actividades sobre el RECC en un sitio de celda. Las actividades que son monitoreadas incluyen originación de llamadas, respuestas de paging, activaciones, y orden de confirmaciones. Monitoreando todas las actividades sobre el RECC permite al sistema construir una base de datos fingerprint rápida y exactamente.

3.11.2.8 Manejando la base de datos PhonePrint

Para hacer decisiones de desconexión oportunas, todo RFU en un mercado requiere una actualización de la base de datos fingerprint. El SCC maneja la base de datos *PhonePrint*: colecta los datos desde los RFUs, procesa e integra esos datos para crear actualizaciones de las huellas digitales y distribuye la base de datos a los RFUs.

Colección de datos

PhonePrint usa los datos de señal RF coleccionados y analizados por los RFUs para crear la base de datos fingerprint. Todas las noches el SCC recobra los datos coleccionados por cada RFU del mercado. Las comunicaciones entre el RFU y el SCC no interfieren con la operación normal del RFU, porque el RFU usa un sistema de operación multi-tarea.

Integración de datos

El SCC procesa e integra todas las llamadas interceptadas coleccionadas en cada RFU para crear huellas digitales RF altamente definidas. El SCC agrupa intercepciones y las define como huellas digitales RF de usuarios legítimos o como huellas digitales RF de clonadores. A medida que el número de intercepciones colectadas se incrementa, la definición de la huella digital se incrementa.

Después de colectar 10 intercepciones, *PhonePrint* designa una marca como madura. Una huella digital RF madura tiene la definición requerida para hacer decisiones de desconexión de llamadas. Durante la integración de datos el SCC valida las huellas digitales RF. Cuando el SCC valida una huella, este la identifica como una huella perteneciente a un usuario legítimo. Solamente después de que una huella digital RF es madura y válida, *PhonePrint* usa la marca para hacer una decisión de desconexión de llamada. El proceso de integración de datos también incorpora otra información en la base de datos, tales como números críticos que nunca deberían desconectarse, y números marcados asociados con actividades fraudulentas.

El RFU puede usar esta información con set lógicos suplementarios de la operadora para desconectar llamadas y para identificar suscriptores legítimos o clonados.

Distribución de datos

Después de integrar los datos colectados, el SCC crea una base de datos *fingerprint* única y distribuye una copia actualizada de la madurez y validez de las huellas a cada RFU en el mercado. Así, cada RFU tiene una base de datos de las distintas huellas que existen en el mercado.

Por estar la base de datos distribuida a través del mercado celular, ningún punto de la misma puede hacer fracasar a la base de datos y al sistema, si existe alguna falla. De esta manera si el SCC experimenta falla total, los RFUs continúan identificando y bloqueando llamadas fraudulentas, las consecuencias de este fallo solamente pueden retrasar un ciclo de actualización en la base de datos.

3.11.2.9 Operadora celular de entrada y salida

El sistema *PhonePrint* está diseñado para brindar a las operadoras celulares acceso a un conjunto de salidas que permita a la operadora valorar el desempeño del sistema. En suma, *PhonePrint* requiere muchos tipos de entradas de la operadora celular. La salida es accesible al Interface de Usuario *PhonePrint*. La mayoría de entradas deberían estar sujetas a un operador SCC.

Entrada de la operadora celular

PhonePrint requiere de la operadora celular una entrada específica. Las operadoras respaldadas por los diferentes fabricantes (*Ericsson, Alcatel, Corsair, etc.*) o el operador SCC con archivos que contienen los datos requeridos.

- **NPA-NXX lista 1(Requerido).** Este archivo lista el código de área y prefija los primeros 6 dígitos de todos los MINs en el mercado de la operadora. *PhonePrint* usa este archivo para determinar si una llamada pertenece a un MIN local o a un MIN de *roaming*.
- **Dígitos marcados frecuentemente (Requerido).** Para cada suscriptor legítimo en el mercado, este archivo lista el MIN y un conjunto de números telefónicos que el suscriptor a menudo marca, tales como de un negocio ó como el número de voice mail. *PhonePrint* usa el archivo de dígitos marcados frecuentemente para validar las huellas digitales RF con el propósito de asegurar que una determinada huella pertenezca a un usuario legítimo.
- **Archivo contacto (Requerido).** Para cada suscriptor en el mercado, este archivo lista el MIN y los números telefónicos que la operadora celular utiliza para contactar al suscriptor. *PhonePrint* también usa este archivo para validar la huella digital RF.
- **MINs siempre permitidos.** Este archivo lista los MINs que *PhonePrint* nunca desconectará.
- **MINs nunca permitidos.** Este archivo lista los MINs que *PhonePrint* siempre desconectará.

- **Dígitos marcados siempre permitidos.** Este archivo lista los números de teléfono que *PhonePrint* permite llamar (aún teléfonos clonados).
- **Dígitos marcados bloqueados.** Este archivo lista los números de teléfono que *PhonePrint* no permite llamar (aún teléfonos legítimos).
  - En lugar de una lista NPA-NXX. El sistema ETACS requiere un bloque de lista MIN. Este archivo lista los bloques de MINs, definidos por los primeros 6 a 10 dígitos.

PhonePrint usa el bloque de lista MIN para determinar si una llamada pertenece a un MIN local o a un MIN *roamer*.

3.11.3 Responsabilidades de la operadora

3.11.3.1 Selección del sitio de celda

Típicamente hay dos categorías de sitios que necesitan ser considerados cuando seleccionamos el sitio para desplegar:

a. **Alto tráfico/bajo fraude.-** Las unidades (RFUs) en estos sitios serán usadas para rápidamente construir una base de datos de huellas digitales maduras y válidas. Los sitios de celda en áreas tales como arterias de tráfico, centros de negocio y aeropuertos son buenos candidatos para desplegar RFUs en esta categoría.

b. **Gran fraude.-** Estos sitios han experimentado grandes tasas de fraude y serán excelentes candidatos para desarrollar RFUs. Los RFUs en estos sitios serán usados para terminar las llamadas realizadas por teléfonos clonados.

3.11.3.2 Acceso al sitio de celda

El acceso se requiere durante la instalación de las unidades. El operador permitirá el acceso a los distintos equipos de los sitios de celda (claves, combinaciones, etc.), a los proveedores del sistema *PhonePrint,* por ejemplo: Ericsson, Coirsair, AT&T, etc. Además el operador proveerá un local central para el reparto de los RFUs y organizar su envío hacia los distintos de celda.

CAPÍTULO IV

TENDENCIAS TECNOLÓGICAS PARA LA REDUCCIÓN DEL FRAUDE

Los sistemas de perfil de usuario (*profiling*) y los PINs están en su vía de salida, algunos operadores y expertos en prevención de fraude así lo creen. Los PINs han sido derrotados por los clonadores; para los bandidos celulares, los números PIN son a menudo de un mayor valor e incrementan el precio que ellos pueden dar por un teléfono clonado.

La tendencia toma una dirección en el sentido de los Servicios de Comunicación Personal (*PCS: Personal Communication Services*), Sistemas Globales para Comunicaciones Móviles (*GSM: Global System for Mobile communications*), registros de datos de tasación más inteligentes, huella digital de radio frecuencia y autenticación.

4.1 NUEVOS PROCESOS Y TÉCNICAS EN LA PREVENCIÓN Y DETECCIÓN DEL FRAUDE CELULAR

Muchos alcances se enfocan en la identificación de los usuarios. El problema, de hecho, es no encontrar las soluciones, es decir todos los componentes que forman junto al sistema celular; tales como la banca, el proveedor del servicio celular, y el teléfono deberían acordar sobre la misma solución, terminal a terminal.

Y la industria celular, debería estandarizar esa solución para manejar la masa del mercado bajo la norma terminal-accesibilidad del usuario[1].

La Biométrica puede jugar un rol importante aquí. De hecho, una compañía, *AuthenTec Inc. , Melbourne, Filadelfia.* , está desarrollando un sensor de huellas digitales que puede ser integrado dentro del teléfono celular sin añadir notablemente el peso del teléfono, precio, o consumo de energía.

4.1.1 ¿CÓMO UN TELÉFONO PUEDE CHEQUEAR LAS HUELLAS DIGITALES?

Como todos sabemos, el tiempo ha demostrado que la forma de verificar la identidad de una persona es a través de su huella digital. Para la presente aplicación, la pregunta es, ¿puede ser esto hecho rápidamente, sin la asistencia de algún experto, cuando la persona está usando el teléfono celular en las afueras de la ciudad?

La respuesta, de acuerdo a los expertos de la *AuthenTec Inc*, es sí. Todo esto se reúne en el sensor de huella digital Fingerloc de la compañía. Este está acompañado de un *software*, y un microprocesador con el cual el programa puede arrancar. El problema, no es encontrar el microprocesador. Los teléfonos digitales modernos, contienen poderosos procesadores permanentes que nada tiene que hacer cuando una llamada celular no está en progreso. El sensor Fingerloc (ver la figura 4.1) es un chip de silicón monolítico que realiza un sensado, asociado a una circuitería, todo cubierto apropiadamente por una delgada capa (75μm). Este puede ser fácilmente empotrado en la superficie de un teléfono celular, donde la robusta capa lo protegerá de los rigores del uso normal.

[1] Michael J. Riezenman, (2000), p.40.

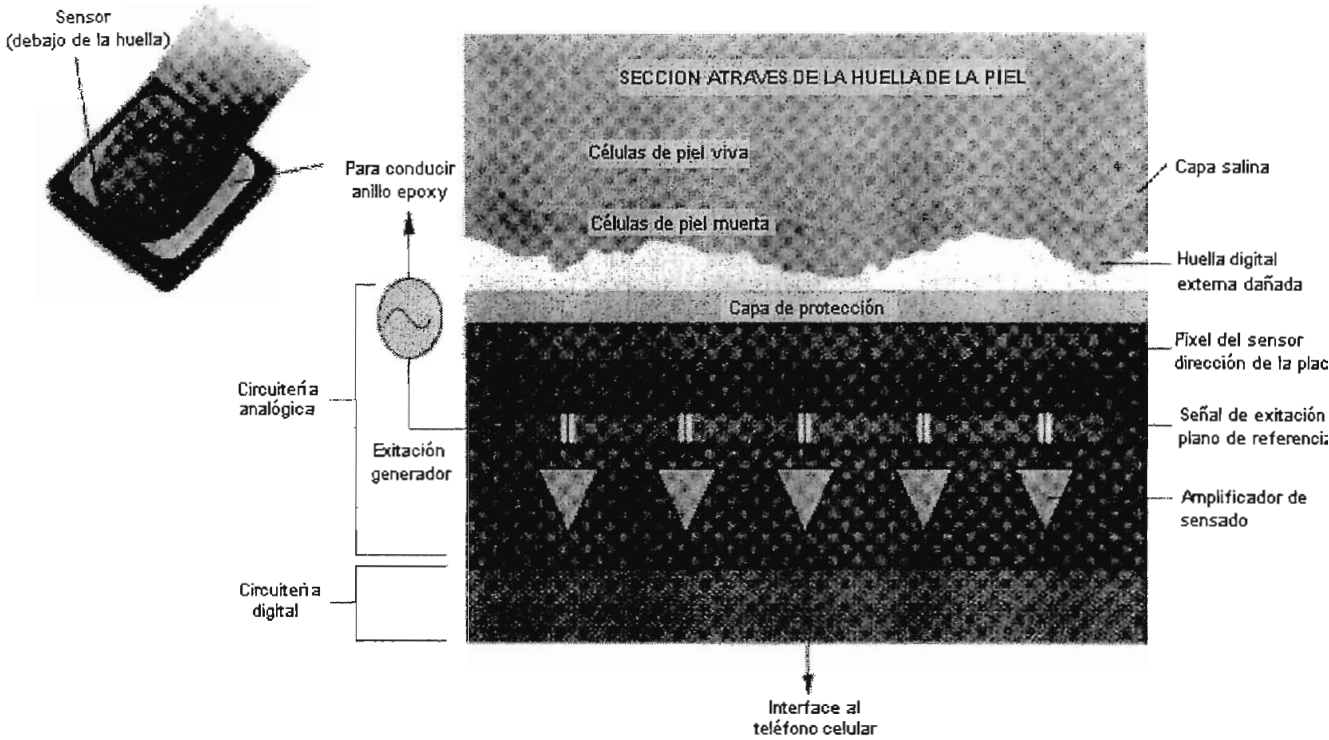


Figura 4.1 Sensor Fingerloc[1]

La ventaja clave del Fingerloc sobre otros sensores de huellas digitales (ópticos), es que éste ignora la huella digital externa, la cual es a menudo sucia o dañada o que tiende a desaparecer.

Por otra parte, este sensa la huella digital en un nivel soterrado de la vida de las células, donde las huellas digitales son creadas, y donde ellas son encontradas en condiciones no definidas. Lo que hace es aplicar una señal AC de bajo voltaje a la yema del dedo y luego mide la variación en amplitud del campo eléctrico sobre la superficie de la yema.

[1] Michael J. Riezenman, (2000), p.41.

La señal es aplicada por medio de un anillo conductivo circundante al área del sensor (ver la figura 4.1, nuevamente). El campo eléctrico es producido entre el plano de referencia y una fina capa de líquido salino altamente conductivo que reside en la interface del tejido vivo y del muerto de la piel. La capa salina tiene la misma forma que el tejido vivo—la forma de la huella digital.

Siendo altamente conductivo, las formas de la huella son impuestas como una condición límite sobre el campo, modulado analógicamente por la huella digital. Un arreglo de minúsculas antenas en una matriz de 96 filas y columnas hace el sensado actual. Localizado por encima del plano de referencia, el arreglo mide cerca de 6.5 mm de lado, dando al sensor una resolución lineal de cerca de 15 pixels por milímetro.

Los campos eléctricos (valorados) analógicos sensados son explorados desde la matriz del sensor, una columna a la vez, digitalizado, y enviado desde el chip Fingerloc hacia el microprocesador del teléfono celular para nuevos procesamientos.

En el teléfono celular, un módulo de *software* del *AuthenTec* analiza el patrón de la huella digital y extrae información de él, el cual lo convierte en una única representación de la huella digital propietaria. Un usuario, tiene una única representación, llamada plantilla, que es almacenada en una memoria no volátil para usos futuros. Para autenticar un usuario, este es comparado con todas las plantillas almacenadas en una base de datos para determinar la identidad del suscriptor. Lo que pase luego, depende de como el fabricante del teléfono celular y el proveedor del servicio tengan fijado. Si el teléfono no reconoce al solicitante, el servicio probablemente será denegado. Esto resulta más interesante cuando el sistema no reconoce la huella digital, en este caso se pueden crear bases de datos siguiendo patrones de comportamiento para cada usuario identificando las posibles causas de este suceso.

Por ejemplo, un suscriptor puede tener un teléfono encendido, pero no puede realizar llamadas locales, no importa que botón él presione. Los usuarios más antiguos pueden tener sus características personales automáticamente almacenadas en el teléfono, ciertos privilegios pueden ser activados o bloqueados. Y, de acuerdo, con los estándares correctos, el sensor puede ser parte de un sistema de verificación y autenticación.

4.1.2 CONTEO DE LLAMADAS

El conteo de llamadas (*call counting*) es otra técnica que puede ser usada en vez de las más usuales, junto con el servicio de autenticación. Como autenticación, este requiere que el teléfono sea capaz de desempeñar esta parte del proceso. Con *call counting*, ambos, el teléfono y la red identifican y registran el número de llamadas hechas por el teléfono. Esos números son comparados siempre que una llamada sea hecha. Si ellas no coinciden o si ellas no concuerdan por más de una cantidad específica (generalmente una), la llamada no es permitida.

Obviamente, si alguien ha clonado un teléfono, tanto él como el usuario legítimo estarán haciendo llamadas, así la red tendrá identificados esos números, y podrá seguir diferentes procesos para determinar si esta ocurriendo fraude .

4.2 DESARROLLO DE NUEVOS ESTÁNDARES EN LOS SISTEMAS DIGITALES, SEGUNDA Y TERCERA GENERACIÓN

Hace cincuenta años, los teléfonos celulares fueron una extravagancia. Hoy en día, están a menudo dando diferentes alternativas tanto en soporte como en proyectos de mercadeo y promociones de nuevos productos. Teniendo como corriente principal, las comunicaciones de voz, ellos han tomado nuevos desafíos, transmitiendo (equitativamente) datos a gran velocidad, vídeo, y multimedia.

Esos desafíos tecnológicos son conocidos como la telefonía celular de tercera generación. Desde este punto de vista, los primeros teléfonos analógicos son etiquetados como de la primera generación, mientras que los sistemas con tecnologías de radio digital son conocidos como de la segunda generación.

Para que no se piense que los teléfonos celulares analógicos están obsoletos, o que son una tecnología obsoleta, en junio de 1999, sobre el 70% de los suscriptores en los Estados Unidos permanecen usando teléfonos analógicos[1]. Y muchos quienes tienen teléfonos celulares que trabajan en modo doble vuelven al modo analógico cuando vagan, especialmente en áreas rurales.

La última cifra de la CTIA, menciona que la penetración digital, actualmente excede el 50%. Pero la CTIA cuenta con teléfonos duales como también con digitales, así que este número no puede diferir demasiado con el dato anterior. Cualquiera que sea el número exacto, el mensaje es claro: los que escuchan a escondidas (*eavesdroppers*) no solo lo hacen por interés histórico.

4.2.1 CDMAONE

4.2.1.1 ¿Qué es cdmaOne?

Es un nombre comercial de marca registrada, reservado para uso exclusivo de las empresas que son miembros del Grupo de Desarrollo CDMA (*CDG: CDMA Development Group*) y que describe un sistema inalámbrico completo que incorpora la interface aérea IS-95 CDMA, la norma de la red ANSI-41 para la interconexión por conmutación, además de muchas otras normas que integran el sistema inalámbrico completo.

El nombre *cdmaOne* nos permite comunicar un número de mensajes importantes.

[1] Michael J. Riezenman, (2000), p.40.

Primero *cdmaOne* representa el sistema inalámbrico terminal a terminal y las especificaciones necesarias (IS-95, IS-96, IS-41, etc.) que gobiernan sus operaciones. Esto es, por lo tanto, un término mucho más exclusivo que el CDMA IS-95, el cual solo se refiere a las especificaciones de la interface aérea. El denominador *One*, refiere el hecho de esta tecnología proveerá una familia de servicios relacionados sobre un único estándar, incluyendo: celulares, PCS, WLL, y comunicaciones satelitales.

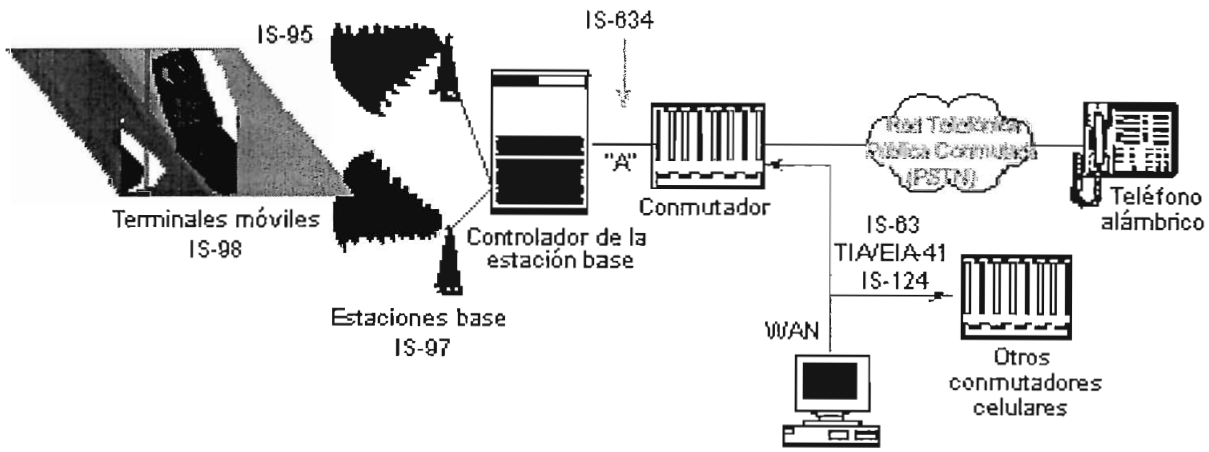


Figura 4.2 Componentes de un sistema cdmaOne[1]

4.2.1.2 Iniciativas de roaming

Roaming internacional

El grupo reúne operadores, fabricantes, y proveedores de sistemas de *roaming* con el propósito de:

- Discutir y superar dificultades en el establecimiento de *roaming* internacional.
- Desarrollar un sistema de *roaming* internacional automático utilizando interfaces y normas abiertas.

[1] www.cdg.org/what's cdmone.

- *Roaming* internacional es altamente prioritario para el CDG.
- Movilidad es un índice (*benchmark*) de globalización.

4.2.1.3 CdmaConnect

CDG desarrolló el *cdmaConnect* en febrero de 1998 para desarrollar los siguientes puntos claves:

- Proveer una plataforma de *roaming* punto a punto basado en IS-54 con *GTE TSI y Cibernet*.
  - Conectividad.
  - Administración del fraude.
  - Casa Transparente (*Clearinghouse*).
  - Servicios financieros.
  - *Roaming* entre diferentes estándares.
- Generar documentos para operadores CDMA.
  - Tablas de configuraciones de *switch* probadas.
  - Listado de proveedores de sistemas de cobro calificados.
  - Listado de operadores y administradores de *roaming*.
  - Formulario para el acuerdo de *roaming*.
  - Planilla de datos técnicos requeridos.
- Procedimiento de pruebas terminal a terminal.

¿Cómo opera cdmaConnect?

CdmaConnect provee la estructura necesaria para establecer *roaming*.

- Acuerdo.
  - ¿ Con quién voy a prestar el servicio?.
- Conectividad.

- ¿ Cómo obtienen mis suscriptores el servicio?.

- Intercambio de datos.
  - ¿Cómo intercambiamos información sobre nuestras cuentas?.
- Detección de fraude.
  - ¿ Cómo me protejo de pérdidas?.
- Contabilidad.
  - ¿ Cómo intercambiamos los fondos para los pagos?.

Conectividad

CDG recomienda el uso de redes privadas X.25 para lograr conectividad para la señalización IS-41.

- Aplicable para redes y datos.
- Más efectivo desde el punto de vista de costo para altos volúmenes de tráfico.

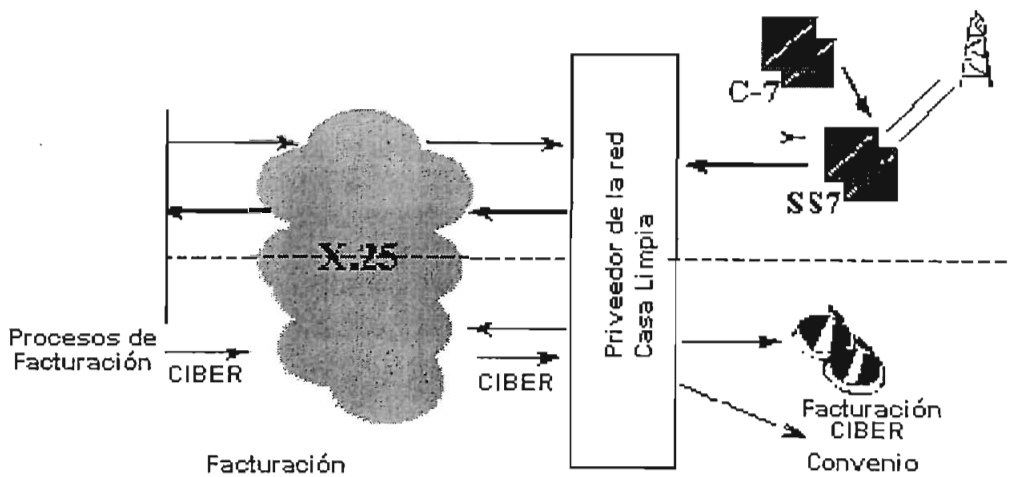


Figura 4.3 Conectividad[1]

[1] www.cdg.org/what's cdmone.

Detección de fraude

- Minimizar el fraude de *roaming*.
  - Herramientas para prevención de fraude.
    - Generación de perfiles de cliente.
    - Recolección de CDR en tiempo real.
  - Estas herramientas permiten identificar a los clientes de *roaming*.

  Los operadores de América del Norte requieren que todos los socios de *roaming* utilicen todas estas herramientas.
- Acuerdo Contable.
  - Transacciones financieras para hacer y recibir pagos periódicamente.
  - Aspectos del acuerdo.
    - Auditoría y control.
    - Uso del sistema bancario.
    - Aspectos legales y créditos.
    - Recolección de deudas.
    - Cambios de divisas.

  Varios operadores de América del Norte requieren la participación de programas financieros para evitar dificultades con sus socios en *roaming*.

4.2.1.4 Numeración MIN – IMSI

Numeración MIN

El CDG ha advertido las limitaciones del MIN utilizado en sistemas ANSI-41 para aplicaciones de *roaming* internacional y portabilidad de número. Reconoce los esfuerzos realizados por IFAST para resolver el problema mediante la asignación de bloques de IRM con el formato:

(0/1) (-- -- --) (-- -- -- -- -- --)

Prefijo asignado por IFAST 4 dígitos	Número asignado por el operador local 6 dígitos

Numeración IMSI

CDG apoya el uso de IMSI de 15 dígitos en las estaciones base y terminales móviles y su adopción como solución de largo plazo para facilitar el *roaming* internacional y evita incompatibilidades entre sistemas en el futuro. La estructura del IMSI responde a la recomendación UIT-TE.212

(-- -- --) (-- --) (-- -- -- -- -- -- -- -- -- --)

Móvil País Código 3 dígitos	Móvil Red Código 3dígitos	Móvil Estación Número de Identificación Código 10 dígitos

4.2.1.5 Seguridad y fraude

- Acceso no autorizado (cloning, falsificación MIN/ESN, etc.).
  - Solución: autenticación.
- Escuchas telefónicas (*eavesdropping*).
  - Solución: privacidad de voz y datos encriptados.
- Integridad del sistema.
  - Solución: señalización encriptada.

Seguridad en CDMA

Cada teléfono celular tiene una única clave secreta y genera parámetros de seguridad para cada llamada utilizando algoritmos CAVE. El sistema de claves funciona de la siguiente manera:

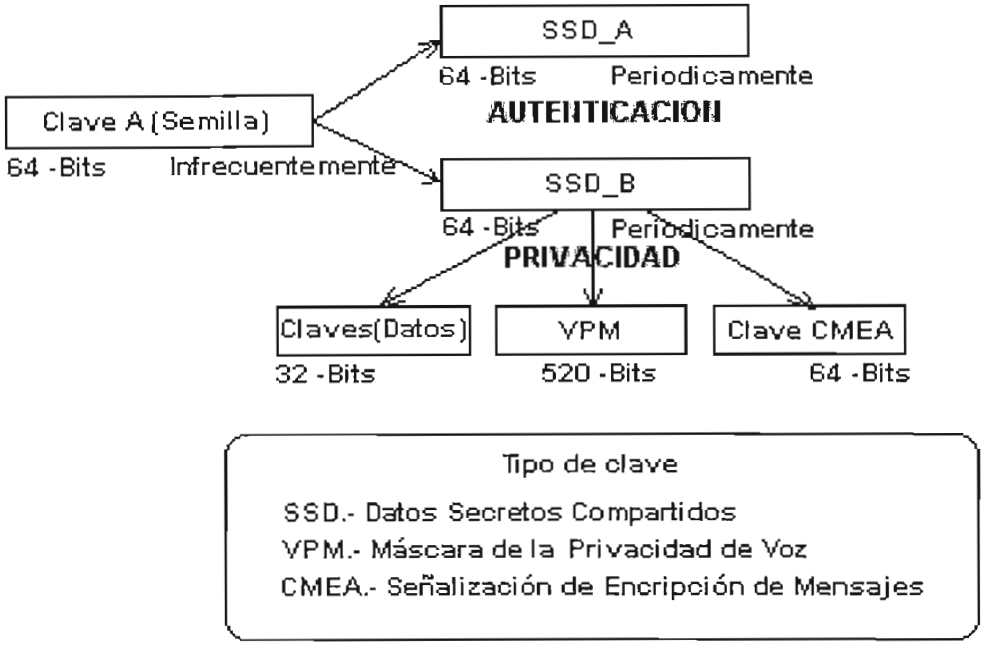


Figura 4.4 Algoritmo de Autenticación-CAVE

Prevención del fraude en CDMA

Incluso sin encripción, CDMA provee privacidad intrínseca de toda la información transmitida por sus canales (datos, voz, señalización) debido al proceso de dispersión espectral. La combinación de encripción, codificación y dispersión espectral otorga a CDMA extremadamente altos niveles de seguridad.

La tecnología digital es no clonable, si la autenticación no está activada, es posible clonar un teléfono CDMA, mucho más complejo y más costoso que clonar un teléfono analógico, pero ciertamente posible.

En el caso de CDMA, los perpetradores tienen un problema demasiado complicado—una revoltijo de docenas de conversaciones, cada una modulada por un código pseudoaleatorio diferente, todos ocupando la misma banda. Así la señal tiene que ser decodificada con el mismo código, lo que puede obtenerse mediante un gran esfuerzo.

Más aún, en sistemas digitales, la voz es vocodificada. El sonido no solamente es digitalizado, sino también comprimido. Así, quien esté interesado en descomprimirlo necesita saber el algoritmo de compresión usado.

De esta manera, los *eavesdroppers* necesitan saber, qué cantidad de la información recibida de un teléfono celular en la estación base es necesaria para tener la oportunidad de decodificar ó descifrar códigos y datos importantes, para cometer sus fechorías. Sin embargo, el equipo de prueba usado legítimamente por los técnicos también puede ser usado para clonar teléfonos. Ya que los microprocesadores en los teléfonos conocen los códigos de dispersión, un *hacker* ingenioso podría desensamblar un teléfono CDMA e interconectarlo a un computador personal, convirtiéndolo en un *scanner* CDMA.

4.2.1.6 Evolución a la tercera generación

Requisitos de los operadores para sistemas 3G

- Mayores prestaciones para información y multimedia.
- Control y flexibilidad para el suscriptor.
- Mayor capacidad para atender nuevas demandas.
- Simplicidad de operación y mantenimiento.
- Preservación de las inversiones para sistemas de 2da. Generación.

4.2.2 LA IMPORTANCIA DEL UWC-136

El subcomité TR-45.3 de la TIA, el cual formula el estándar TIA/EIA-136, reconoce completamente la enorme base instalada de los teléfonos y redes GSM, y las posibilidades de *roaming* internacional que ellos ofrecen. Por consiguiente, el subcomité está trabajando en algunos escenarios de convergencia con las formas desarrolladas de GSM bajo el título UWC-136. Este proyecto es uno de los pocos que utiliza un estándar puro TDMA sin elementos CDMA en todo—una propiedad que abre la posibilidad de desplegar las características avanzadas dentro de las bandas de frecuencias tan estrechas de 1MHz.

El UWC-136 es importante porque éste representa un camino de evolución para tecnologías antiguas como AMPS y para las de segunda generación--TIA/EIA-136, las cuales fueron diseñadas especialmente para compatibilidad con AMPS.

Hay más teléfonos AMPS en el mundo que cualquier otro tipo, excepto por el GSM. En 1990 el Consorcio Universal de las Comunicaciones Inalámbricas (*UWCC: Universal Wireless Communications Consorcium*) anunció un plan de convergencia con GSM. Este anuncio estimuló la visibilidad de la tecnología de transmisión de radio UWC-136, la cual propone un despliegue a bajo costo, evolucionar el camino de AMPS y de los operadores TIA/EIA-136. La tecnología es tolerante de la banda de frecuencia en la cual éste es desplegado: 500 MHz a 2,5 GHz.

Los sistemas de acceso, sean de tiempo o de código están generalmente confinados a regulaciones forzadas para incrementar la capacidad del canal sin incrementar el ancho de banda. Este es alcanzado en GSM y en el UWC-136 con el que ha sido llamada tecnología EDGE (para velocidad de datos mejorada para la evolución GSM).

Los sistemas celulares de hoy en día han emergido de una evolución larga interrumpida por avances significativos en técnicas de radio (modulación de frecuencia, por ejemplo) y dispositivos electrónicos de alta integración (microprocesadores y procesadores digitales de señal).

Algunos Sistemas Celulares Digitales de Segunda Generación				
	GSM (Sistema Global para Comunicaciones Móviles)	TIA/EIA-136 (Asociación de Industrias de Telecomunicaciones/ Alianza de Industrias Electrónicas)	IS-95 (Estándar Interino 95)	PDC (Comunicaciones Digitales Personal/Pacífico)
Rango de Frecuencias, MHz				
Banda	GSM-900	Celular		--
Uplink	935-960	869-894		940-956
Downlink	890-915	824-849		810-826
Banda	GSM-1800			
Uplink	1805-1880			
Downlink	1710-1785			
Banda	GSM-1900	PCS		--
Uplink	1930-1990	1930-1990		1429-1453
Downlink	1850-1910	1850-1910		1477-1501
Espaciamiento de canal, kHz	200	1250		25
Canales (Mínimo)	125	832	20	1600
Usuarios por canal	8	3	<63	3
Técnicas de acceso múltiple	FDMA/TDMA		FDMA/CDMA	FDMA/TDMA

Tabla 4.1 Sistemas Celulares de Segunda Generación

La primera generación de celulares analógicos apareció en la década de los 80's. La segunda generación de sistemas celulares, apareció una década más tarde, exitosamente sobre las deficiencias de los sistemas analógicos:

la carencia de seguridad y privacidad, características limitadas de la red, y altos costos. Con el arribo del milenio, 10 años después del arribo del celular digital, las iniciativas de la tercera generación que están emergiendo están diseñadas para mejorar – no reparar – la interface aérea, así esos sistemas móviles pueden brindar nuevos servicios para más suscriptores.

El radio digital también ha alterado el camino de la evolución de radio analógico. La práctica analógica siempre trabajó en la dirección de los canales más estrechos, mejorada planificación de frecuencia y mejores relaciones portadora a interferencia. El radio digital sustituye aplicaciones de banda ancha por las estrechas, planificación de potencia para planificación de frecuencia, y administración del ruido para relaciones portadora a interferencia altas.

Pero, un estándar único emergerá para la tercera generación. Sin embargo el equivalente, las tecnologías de transmisión de radio estarán en la mirada de más suscriptores, ellos difieren lo suficiente en los detalles para cada una, para ser atractivas para diferentes operadoras, teniendo sus propias metas operacionales, aplicaciones, realidades del mercado, clientes y lo concerniente a la legalidad en la interoperabilidad de las redes. Por otro lado, habrá una familia de estándares, cada uno con sus propias ventajas.

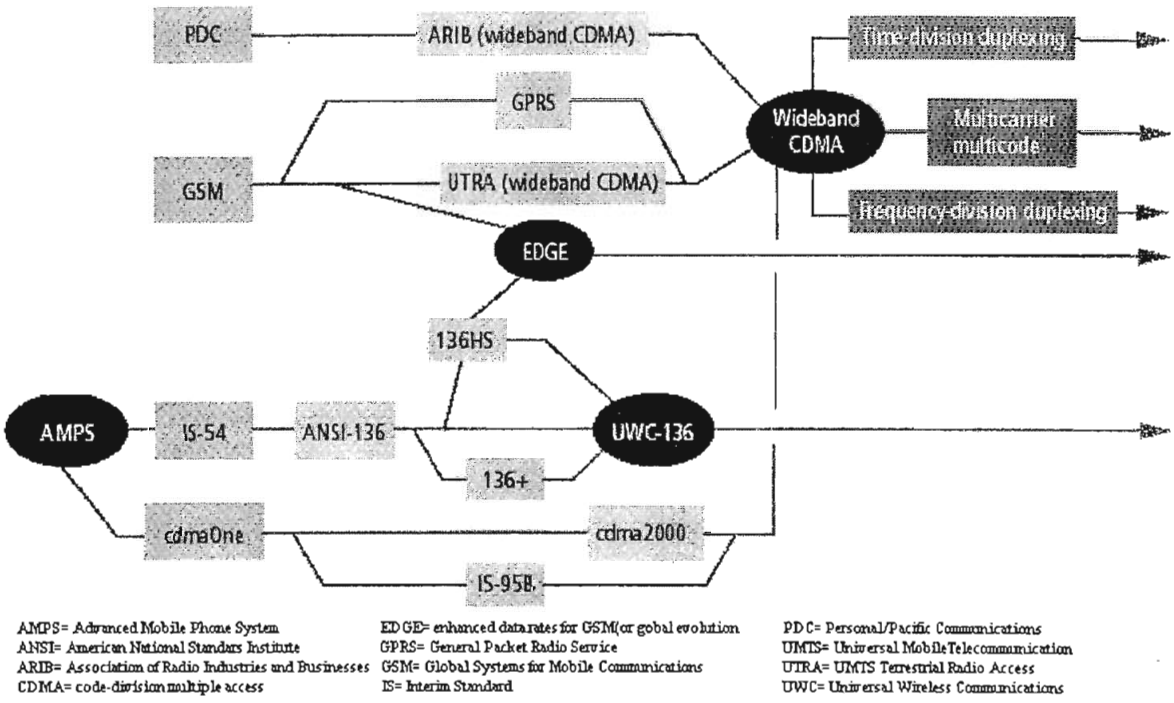


Figura 4.5 Familia de estándares. Evolución[1]

4.2.3 W-CDMA

W-CDMA es un nombre que identifica las normas ETSI y NTT DoCoMo para tecnología de tercera generación sometida ante la ITU como parte del proceso IMT-2000 3G.

Esta norma incorpora una interfaz aérea que utiliza la técnica CDMA, pero que no es compatible en la forma en que está definida para la interface aérea y de red con *cdmaOne*, *cdma2000* o IS-136. La especificación de interface aérea no es compatible con GSM y, por lo tanto, no apoya la migración evolutiva.

[1] Malcom W. Oliphant, (1999), p.28.

4.2.4 CDMA2000

CDG ha estado trabajando para definir el próximo paso en la tecnología *cdmaOne*, con esfuerzos que aceleran rápidamente el despliegue del estándar *cdma2000.* El subcomité TR-45.5 de la TIA sometió una tecnología de transmisión de radio llamada *cdma2000.* Esta Tecnología de Transmisión de Radio (*RTT: Radio Transmission Technology*) protege las inversiones en equipos y sistemas IS-95, de las cuales hay una buena cantidad en Norte América y Korea.

Cdma2000 es un nombre que identifica la norma TIA para tecnología de tercera generación que es un resultado evolutivo de *cdmaOne* y que ofrece a los operadores que han desplegado un sistema *cdmaOne* de segunda generación una trayectoria de migración transparente que respalda económicamente la actualización a las características y servicios 3G dentro de las asignaciones del espectro actual tanto para los operadores celulares como los de PCS. La interface de red definida para *cdma2000* apoya la red de segunda generación de todos los operadores actuales, independientemente de la tecnología (*cdmaOne*, IS-136 TDMA o GSM). La TIA ha presentado esta norma ante la ITU como parte del proceso IMT-2000 3G.

A fin de facilitar la migración de *cdmaOne* a las capacidades de *cdma2000* ofreciendo características avanzadas en el mercado de una manera flexible y oportuna, su implementación se ha dividido en fases evolutivas. Las capacidades de la primera fase se han definido en una norma conocida como 1XRTT. La fecha de publicación de la 1XRTT se ha fijado para el primer trimestre de 1999. Esta norma introduce datos en paquete a 144 kbps en un entorno móvil y a mayor velocidad en un entorno fijo.

Diez tecnologías de transmisión de radio terrestre				
Technology	Acronym	Supporter	Acronym	Nationality
Cdma2000 (code division multiple-access)		TIA Wideband Spread-spectrum Digital Technology Committe (TR-45.5)		United States
Digital enhanced cordless telecomunications	DECT	European Telecommunications Standars Institute	ETSI	Europe
Global multiband synchronous direct-sequence CDMA	CDMA I			Korea
Global asynchronousdirect-sequence CDMA	CDMA II			Korea
Time-division synchronous CDMA	TD-SCDMA	China Academy of Telecommunication Technology	CATT	China
UMTS (Universal Mobile Telecommunication System) terrestrial radio access	UTRA	ETSI Special Mobile Group	ETSISMG	Europe
Universal Wireless Communications 136	UWC-136	TIA Digital Cellular Commitee (TR-45.3)		United States
Wideband-CDMA/NA	W-CDMA/NA	Alliance for Telecommunications Industry Solutions --T1P1 Commitee	ATIS	United States
Wideband-CDMA	W-CDMA	Association of Radio Industries and Businesses	ARIB	Japan
Wireless integrated-services digital-network multi-media services W-CDMA	WINS W-CDMA	TIA Mobile & Personal Communications 1800 Commitee (TR-46)		United States

Tabla 4.2 Diez Tecnologías de Transmisión de Radio Terrestre[1]

Las características disponibles con 1XRTT representan un incremento doble, tanto en la capacidad para voz como en el tiempo de operación en espera, una capacidad de datos de más de 300 kbps, servicios avanzados de datos en paquete, además de que se extiende considerablemente la duración de la batería y contiene tecnología mejorada en el modo inactivo. Se ofrecerán todas estas capacidades en un canal existente de 1.25 MHz de *cdmaOne*.

La evolución de *cdmaOne* hasta llegar a las capacidades completas de *cdma2000* continuará en la fase dos e incorporará las capacidades de 1XRTT, apoyará canales de todos los tamaños (5 MHz, 10 MHz, etc.), proporcionará velocidad de circuitos y datos en paquete de hasta 2 Mbps, incorporará capacidades avanzadas de multimedia e incluirá una estructura para los servicios

[1] Malcom W. Oliphant, (1999), p.23.

de voz y codificadores de voz 3G, entre los que figuran los datos de paquetes de "*voice over*" y de circuitos.

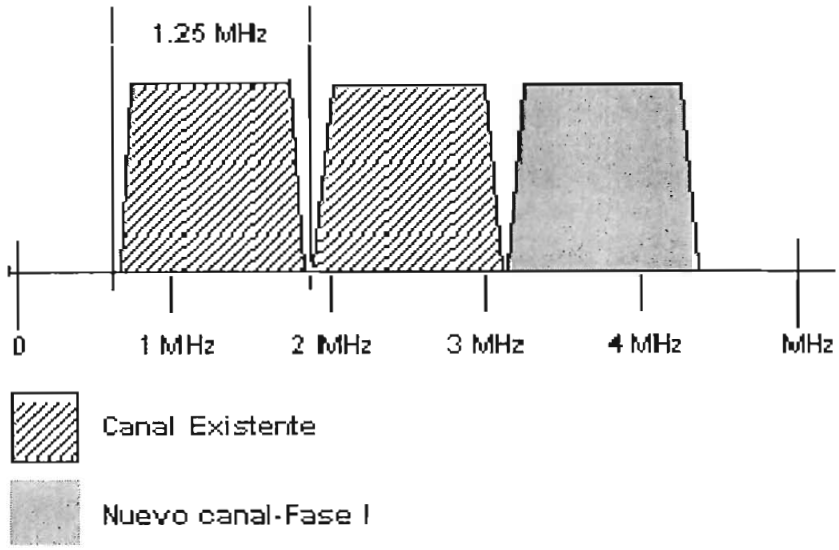


Figura 4.6 cdma2000 (Fase I)

La tecnología TR-45.5 soporta *handoffs* entre la segunda generación (*cdmaOne*) y sistemas de tercera generación (*cdma2000*). Un sistema *cdmaOne* puede desplegar algunas características más nuevas sin incrementar el ancho de banda del canal, proveyendo que ciertos detalles de señalización y recursos lógicos dentro del canal de 1.25 MHz sean modificados para reunir las necesidades de los paquetes de radio y de los servicios asimétricos.

4.3 EN EL SERVICIO DE COMUNICACIONES PERSONAL

Los Servicios de Comunicación Personal (*PCS: Personal Communication Services*) son servicios que ofrecen alguna combinación de movilidad del terminal, movilidad personal y gestión del perfil del servicio de telecomunicación. La movilidad personal se relaciona con la asignación de un único número personal a nivel mundial, la gestión del perfil del servicio se relaciona con la aptitud de ubicar al servicio en cualquier lugar, y la movilidad o portabilidad, se relaciona con las diferentes tecnologías de acceso.

PCS fue diseñado para ser un servicio personal, esforzado para proveer servicio en muchos de los lugares donde las personas permanecen en contacto. PCS es un servicio digital, por lo tanto los servicios de autenticación y privacidad se complementan mucho mejor, garantizando un mejor servicio a los usuarios.

La mayor ventaja es la calidad de voz y seguridad, no solamente porque usa tecnología digital, sino por la tecnología digital específica que él usa. Esa tecnología es el Sistema Global para Comunicaciones Móviles (GSM), TDMA (IS-136), DCS 1900, OMNIPOINT, Q-CDMA, y trabaja en la banda desde los 1850-2200 MHz asignada por la FCC.

El estándar GSM provee el cerebro de un teléfono móvil PCS. Este contiene la identificación del usuario y la información de las cuentas que pueden ser intercambiadas entre los teléfonos, así que las llamadas pueden ser hechas o recibidas aún cuando el usuario no esté usando su propio teléfono.

4.4 EN EL SISTEMA GLOBAL PARA COMUNICACIONES MÓVILES

4.4.1 EL PROPÓSITO DE SEGURIDAD

El resultado de todos los fraudes ocasiona una pérdida al operador. Es importante reconocer que esta pérdida puede estar en términos de:

- Pérdidas financieras no directas, donde el resultado es la pérdida de clientes y un incremento en el uso del sistema sin percibir ganancias.
- Pérdidas financieras directas, donde el dinero es repartido a otros, tales como otras redes, proveedores, y operadores.
- Desconcierto potencial, donde los clientes pueden moverse a otros servicios por la carencia de seguridad.

- Fracaso para reunir los requerimientos legales y regulatorios, como las condiciones de licencia, Actas de la compañía o la legislación de protección de datos.

El objetivo de seguridad para el sistema GSM es hacer al sistema tan seguro como la red conmutada de telefonía pública. El uso del radio en la transmisión media permite un número de amenazas potenciales para los escuchas a escondidas de las transmisiones.

El Grupo Memorándum de Acuerdos GSM (*GSM MoU: GSM Memorandum of Understanding Group*) produce la dirección sobre estas áreas en la interacción del operador con los miembros. Las características técnicas para seguridad son solo una pequeña parte de los requerimientos de seguridad, la más grande amenaza proviene del ataque más simple tal como la revelación de las claves de seguridad, sistemas de facturación inseguros o corrupción. Se requiere de un balance efectivo para asegurar que estos procesos de seguridad reúnan estos requerimientos.

4.4.2 LIMITACIONES DE SEGURIDAD

Los sistemas celulares existentes tienen un número de debilidades que fueron consideradas en los requerimientos de seguridad para GSM. La seguridad para GSM tiene que ser apropiada para el sistema del operador y del cliente.

- Los operadores del sistema desean asegurar que la emisión de las facturas sea para la gente apropiada, y que los servicios no puedan ser comprometidos
- El cliente requiere algo de privacidad sobre el tráfico que es escuchado por los escuchadores a escondidas

Las contra medidas son diseñadas:

- Para hacer el camino de radio tan seguro como las redes fijas, lo cual implica anonimato y confidencialidad para proteger contra el eavesdropping.
- Para tener una fuerte autenticación, para proteger al operador contra el fraude de facturación.

Los procesos de seguridad no deben:

- Añadir significantemente al retraso de la llamada inicial o la comunicación subsecuente.
- Incrementar el ancho de banda del canal.
- Permitir incrementar la tasa de errores, o errores de propagación.
- Añadir excesiva complejidad para el resto del sistema.
- Incrementar el costo eficiencia.

El diseño de un sistema GSM del operador debe tomar en cuenta el ambiente y los procesos de seguridad tales como:

- La generación y distribución de claves.
- Intercambio de información entre operadores.
- La confidencialidad de los algoritmos.

4.4.3 DESCRIPCIÓN DE LAS FUNCIONES DE LOS SERVICIOS

GSM provee tres niveles de seguridad.

Primer sistema de seguridad:

- La suscripción GSM es registrada en el Módulo de la Interface del Suscriptor (*SIM: Suscriber Interface Module*).

- La tarjeta SIM puede ser insertada en cualquier terminal GSM.
- El propietario de la tarjeta SIM es facturado.
- El GSM chequea la validez del suscriptor.

Segundo sistema de seguridad:

- El sistema GSM identifica la localización del visitante.
- Los teléfonos robados no pueden ser fácilmente usados, así ellos pueden ser rastreados.
- El equipo receptor de llamadas sobre una estación base puede identificar al visitante después de aceptar la llamada.

Tercer sistema de seguridad:

- Se usa encripción totalmente digital para hacer imposible el fraude por clonación y el *eavesdropping.*

  Los servicios de seguridad proveídos por GSM son:

- **Anonimato.** No es fácil identificar al usuario del sistema.
- **Autenticación.** El operador sabe quien está usando el sistema para propósitos de facturación.
- **Protección en la señalización.** La información más sensible en el canal de señalización, como los números telefónicos son protegidos sobre el camino de radio.
- **Protección de los datos de usuario.** Los datos del usuario, están protegidos al pasar través de la interface aérea.

4.4.3.1 Anonimato

Para asegurar la confidencialidad del suscriptor, se usa el Módulo Temporal de la Identidad del Suscriptor (*TMSI: Temporary Module Suscriber Identity*). El TMSI se envía a la estación móvil después de que los procedimientos de autenticación y encripción han tomado lugar. La estación base responde al recibir el TMSI. El TMSI es válido en el área local donde fue emitido. Para las comunicaciones fuera del área local, la Identificación del Area Local (*LAI: Local Area Identification*) es necesaria junto con el TMSI.

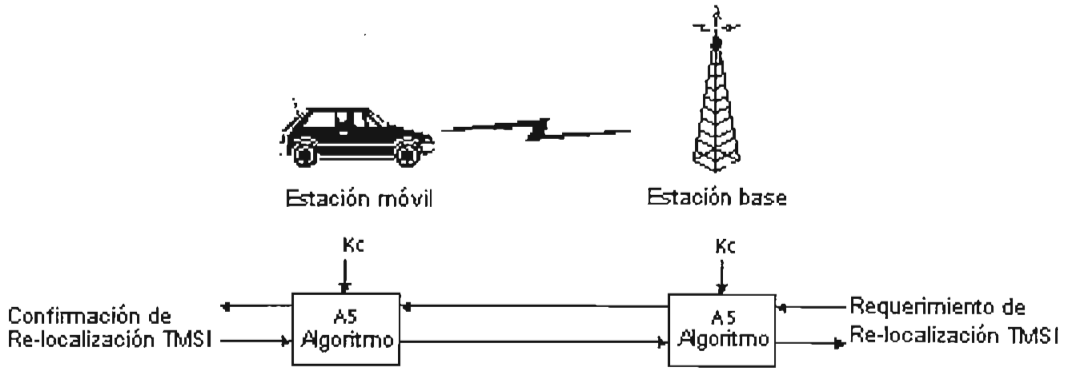


Figura 4.7 Proceso de anonimato

El anonimato se provee mediante identificadores temporales. Cuando al principio un usuario origina una llamada, se usa su identidad real, y un identificador personal, se emite sobre él. Solamente para registrar al usuario es posible esto, para determinar que se ha usado la identidad temporal.

4.4.3.2 Autenticación

La red GSM autentica la identidad del suscriptor a través del uso de un mecanismo de demanda-respuesta. Un número aleatorio de 128 bits (RAND) se envía al MS.

El MS computa la respuesta señalizada de 32 bits (SRES) basada en la encripción del número aleatorio (RAND) con el algoritmo de autenticación A3 usando la clave de autenticación individual del suscriptor Ki. Sobre la señal recibida SRES del suscriptor, la red GSM repite el cálculo para verificar su identidad. Note que la clave de autenticación individual del suscriptor nunca es transmitida sobre el canal de radio. Este está presente en el SIM del suscriptor, como también sobre las bases de datos del sistema.

Si el SRES recibido concuerda con el valor calculado, el MS ha sido exitosamente autenticado y puede continuar. Si el valor no coincide, la conexión es terminada y un fracaso de la autenticación se muestra en el MS.

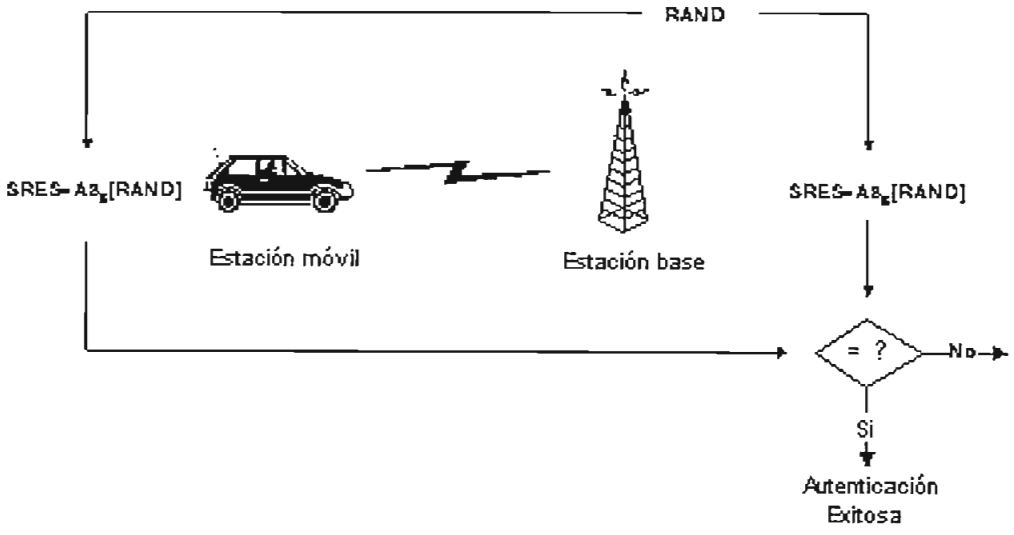


Figura 4.8 Proceso de autenticación en GSM

El cálculo de la respuesta de la señal se procesa dentro de la SIM. Este provee una seguridad mejorada, porque la información confidencial como la Identidad del Suscriptor del Móvil Internacional (*IMSI: International Mobile Subscriber Identity*), Ki, nunca son liberadas de la tarjeta en este proceso.

4.4.3.3 Protección de los datos de usuario y señalización

El SIM contiene la clave cifrada por el algoritmo A8 el cual es usado para producir la clave cifrada de 64 bits (*Kc: ciphering key*). La clave cifrada es computada por la aplicación del mismo número aleatorio (RAND) usado en el proceso de autenticación junto con la clave de autenticación (*Ki: authentication key*). La clave Kc se usa para encriptar y desencriptar los datos entre el MS y BS. Un nivel adicional de seguridad se provee al tener varias maneras de cambiar la clave de cifrado, haciendo al sistema más resistente a las escuchas a escondidas.

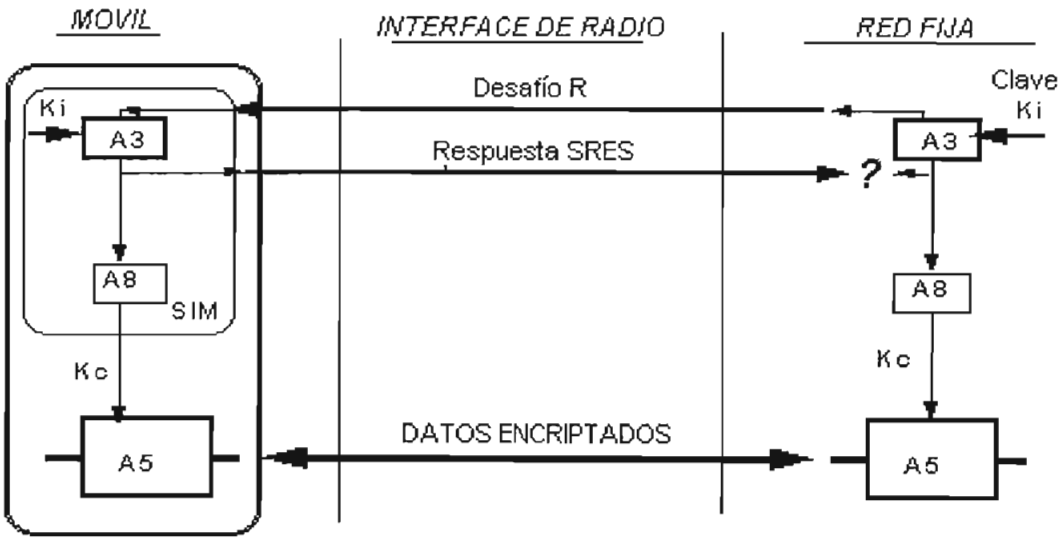


Figura 4.9 Encripción para GSM

De manera similar al proceso de autenticación, el cómputo de la clave cifrada toma lugar internamente dentro de la SIM. El encriptado de voz y las comunicaciones de datos entre el MS y la red se obtienen a través del uso del algoritmo de cifrado A5.

Las comunicaciones encriptadas mediante una petición de cifrado desde la red GSM. Sobre el recibo de este comando, la estación base comienza la encripción y desencripción de datos usando el algoritmo de cifrado (A5) y la clave de cifrado (Kc).

4.4.3.4 Implementación y roaming

TIA/EIA-136 y IS-95 usa el modelo de referencia TIA/EIA-41 para *roaming*, mientras GSM emplea un modelo similar de su propiedad. Sus arquitecturas de red son ciertamente similares, pero hay cuatro diferencias entre las dos.

El algoritmo de autenticación A3 es una opción del operador, y es implementado dentro de la tarjeta inteligente (*smart card*). Así que los operadores pueden inter-trabajar sin revelar los algoritmos de autenticación y las claves del móvil (Ki) del uno al otro, GSM permite demandas tripartitas (R), respuestas (SRES) y claves de comunicación (Kc) para ser enviadas entre los operadores sobre las redes conectadas.

Los algoritmos de la serie A5 están contenidos dentro del equipo móvil, así ellos tienen que ser lo suficientemente rápidos y con un *hardware* eficiente. Hay dos algoritmos definidos que se usan en GSM, conocidos como A5/1 y A5/2. Las especificaciones mejoradas de la fase 1 desplegadas por el ETSI permiten trabajar entre los móviles que contienen A5/1 y A5/2 y redes no encriptadas. Estos algoritmos pueden ser todos construidos con unos pocos miles de transistores y usualmente cubren un área pequeña de un chip dentro del teléfono.

4.4.4 USO MUNDIAL DE LOS ALGORITMOS

Ahora hay tres posibilidades diferentes para GSM, no encriptado, y el uso del algoritmo A5/1 o el algoritmo A5/2 para la seguridad de los datos.

Esto surgió porque el estándar GSM fue diseñado por la Europa Occidental y las regulaciones no permitieron el uso esta tecnología original fuera de Europa. Los usos de los algoritmos en la infraestructura de la red del operador son controlados por el Grupo GSM MoU de acuerdo a la fórmula siguiente:

- El algoritmo A5/1 puede usarse por los países que son miembros del CEPT.
- El algoritmo A5/2 se usará por los operadores en los países que no caen dentro de la categoría anterior.

El control de exportación en los móviles es mínimo, y la próxima generación de móviles soportará A5/1, A5/2, y sin encripción. Los protocolos para soportar las distintas formas de A5 (más de 7) están disponibles en GSM.

4.4.5 OTROS MECANISMOS DE SEGURIDAD PARA GSM

4.4.5.1 Tarjeta SIM

La tarjeta SIM está dentro de cada teléfono, y funciona como un cerebro digital. Esta tarjeta previene que el par ESN/MIN sea robado y que las llamadas sean escuchadas a escondidas.

La memoria digital de la SIM, almacena información, como planes de velocidad, características de servicio, así como también permite personalizarlos fácilmente. La tarjeta inteligente viene en dos formatos, una versión parecida a un pequeño chip semi-permanente dentro del teléfono. La segunda versión es similar a una tarjeta de crédito y puede ser usada en teléfonos equipados con un *slot* para la misma.

Hay siempre la posibilidad (no tenemos el conocimiento) que la tarjeta SIM pueda ser alterada. Esto es considerado menos probable, especialmente si algunos operadores usan sus propias versiones de A3.

Las claves Ki y la numeración IMSI podrían ser altaradas por alguien que vende la información por dinero. En las redes GSM, un algoritmo de encripción aleatoriza las transmisiones de voz digitalizadas entre el teléfono y el sitio de transmisión GSM. La información que se requiere para decodificar la encripción se oculta dentro de la tarjeta inteligente, de esta manera se previene de manera efectiva el *eavesdropping* y el fraude por clonación.

Si la tarjeta es robada, el operador de la red simplemente desactiva la tarjeta. Las comunicaciones inalámbricas encriptadas digitalmente garantizan la confidencialidad completa de todas las llamadas de voz y datos.

4.4.5.2 Identificador internacional del equipo móvil

En GSM la suscripción de los usuarios y la capacidad de autenticación está contenida dentro de la tarjeta inteligente (SIM). Cualquier móvil tomará la identidad de un suscriptor, mediante la inserción de una tarjeta inteligente. Ahora los *fraudsters* tratan de robar las tarjetas SIM para realizar fraude.

Para prevenir esto, GSM ha especificado un Identificador Internacional del Equipo Móvil (*IMEI: International Mobile Equipment Identifier*). Si bien, para el operador, en la primera evaluación, esto hace parecer que el robo de los teléfonos no tenga efecto, así ellos no afectarán una suscripción, pero incrementarán los problemas que encierra el personal.

Un Registro de Identidad del Equipo (*EIR*: *Equipment Identity Register*) existe en cada red, con listas Negras, Blancas y Grises para los móviles robados, móviles válidos y móviles que necesitan ser registrados, respectivamente.

Las listas son para identificar los móviles locales dentro de la red.

GSM ha definido un procedimiento en el que un móvil aprobado, perdido o un móvil robado pueden ser comunicados a todos los otros operadores. Un Registro Central de la Identidad del Equipo (*CEIR: Central Equipment Identity Register*) ha sido propuesto. Las autoridades de aprobación norman la lista de números blancos (rango aleatorio de IMEIs válidos) para los fabricantes móviles, y los fabricantes le informan al CEIR cuando los móviles están liberados en el mercado. Todos los operadores están en la capacidad de echar las listas negras al CEIR, y al mismo tiempo colectan una lista consolidada de todos las listas blancas y negras de los operadores. Por este método, móviles inválidos o robados puede ser rápidamente desplegados a través de todo el mundo. Los problemas de *roaming* internacional son minimizados por el uso de dos procedimientos:

- Intercambio rápido de la información de cuentas.
- Notificación de la red local del visitante cuando él ha excedido un cierto límite de facturación.

4.4.5.3 Medidas y detección del fraude

Un diseño apropiado de un sistema de facturación puede ser usado para detectar los patrones de fraude de mayor uso. Los diferentes tipos de fraude a menudo producen un distinto patrón que puede ser detectado, pero este a veces no es obvio desde la inspección de los registros de llamada. Sin embargo, los que necesitan ser detectados son:

- Llamadas múltiples en el mismo tiempo.
- Variaciones grandes en los ingresos que han sido pagados para otras partes.

- Variaciones grandes en la duración de las llamadas, como llamadas muy cortas o largas.
- Cambios en el uso del usuario, tal vez indica que un móvil ha sido robado o está siendo abusado.
- Monitorear el uso de un cliente fiel durante un período de prueba.

Con la capacidad de detección del fraude, y los procedimientos de seguridad fijados, es posible minimizar los efectos del fraude sobre el sistema de facturación.

CAPÍTULO V

ADMINISTRACIÓN DEL FRAUDE Y SEGURIDAD EN EL SISTEMA DE TELEFONÍA MÓVIL CELULAR

No hay una simple panacea para afrontar los distintos problemas dentro de la operadora, sin embargo una fusión planificada de personas, destrezas, organizaciones, equipo y procesos en el tiempo correcto, en el lugar correcto y con el suficiente compromiso, desarrollará una posición en el mercado mucho más fuerte y con una base de rentabilidad más grande.

Espero que lo que sigue será de uso para la operadora celular, sea esta pequeña, mediana o grande, nueva o establecida y para que las personas que la lean, profesores o estudiantes entiendan lo que realmente pasa en un gran negocio, como son las telecomunicaciones.

5.1 FRAUDE Y SEGURIDAD

5.1.1 CONSIDERACIONES ESTRATÉGICAS PARA LA RED CELULAR

¿Dónde hay que empezar?

Las decisiones fundamentales deben ser tomadas por, o con la elección de alguien con una gran experiencia en el conocimiento de normas de fraude y seguridad (*F&S: Fraud and Security)*.

Hay muchas preguntas cruciales que tienen que ser contestadas cuando se decidan las políticas y las aproximaciones en este campo.

La inexperiencia dará como resultado no solo planes o soluciones erróneas, sino un incorrecto o incompleto proceso de solución. Un experto debería tomar inmediatamente la decisión de adoptar una estrategia de F&S (o examinar una existente). Cualquiera que sea el experto debería desarrollar las siguientes recomendaciones para el Consejo Directivo.

5.1.2 ¿QUÉ ES UN ATAQUE FRAUDULENTO?

Esta pregunta es normalmente formulada por el inexperto director o por el principal administrador; ¿el fraude y la deuda mala no son las mismas cosas?. La respuesta, es un rotundo NO!. En todo fraude hay un componente de deshonestidad, fabricación o falsificación, la distinción entre el fraude y una deuda mala es a menudo difícil. Por esta razón, muchas organizaciones luchan para separarlas.

La diferencia está, en que el fraude es de intento y la deuda mala es de deshonestidad. El perpetrador no intenta pagar por el servicio que usa, el deudor (moroso) intenta pagar, pero cuando la cuente llegue, ellos simplemente son incapaces de pagar. La confusión aumenta porque ambos problemas hacen perder dinero y engañan, lo último es obligatorio para el fraude, y puede a menudo ser difícil de encontrar, el engaño puede encontrarse:

- En cualquier elemento de la identidad del suscriptor.
- En el modo de pago.
- En lo que causa la persona que engaña en los elementos de tu servicio, como evitar el sistema de facturación, ocultar los accesos de la red o alteración y abuso del equipo terminal.

En algunos casos el engaño puede no ser detectado por la persona que está aplicando el servicio.

Esto es común para los perpetradores que inducen a las personas a completar aplicaciones exactamente con sus propias identidades pero con la intención de robar y malversar ese servicio y el acceso al tiempo-aire que provee. La morosidad (débito en contra) para un cierto suscriptor, refleja la incapacidad para pagar el servicio utilizado sin tener la intención de engañar, es decir, el suscriptor usa su propia identidad. Lo difícil es la inhibición de la capacidad para engañar y la vigilancia para ese engaño.

Fundamental en esta etapa es reconocer que las dos emisiones son diferentes y requieren diferentes destrezas y recursos. Una buena manera para medir las consecuencias de la suscripción fraudulenta, históricamente, es hacer un muestreo de las cuentas de morosidad y chequear cada una, basándose en un conjunto definido de criterios de identificación del fraude (por ejemplo, detalles de contactos falsos, pagos no realizados, etc). Cada deuda puede ser clasificada como fraude o como morosidad. Este ejercicio a menudo ayuda a identificar los puntos débiles de la empresa que pueden ser luego soportadas por el análisis.

Definiendo una apropiada clasificación y mecanismos de medida de fraude, es importante para estar en la capacidad de identificar el origen de los casos, monitorear las tendencias y dirigir los recursos para optimizar los efectos. Usando el mismo tratamiento para ambos desórdenes será ineficaz contra uno de ellos.

En un operador de gran trayectoria, cerca de la mitad de ingresos de pérdidas por fraude fueron servicios de tipos de fraude de bajo nivel, deudores repetidos, etc. Considerando el número de cuentas, probablemente caen dentro de esta categoría, el costo de este fraude puede a menudo exceder el costo del más visible fraude de ingreso, como es la venta de llamadas (*Call Selling*).

5.1.3 ¿CUÁLES EQUIPOS, HERRAMIENTAS Y SERVICIOS DEBERÍAN SER CONSIDERADOS?

Esto cae bajo las siguientes cabezas:

- Sistemas de administración (detección) de fraude .
- Herramientas analíticas.
- Servicios de consultoría.
- Misceláneas técnicas y equipo de investigación.

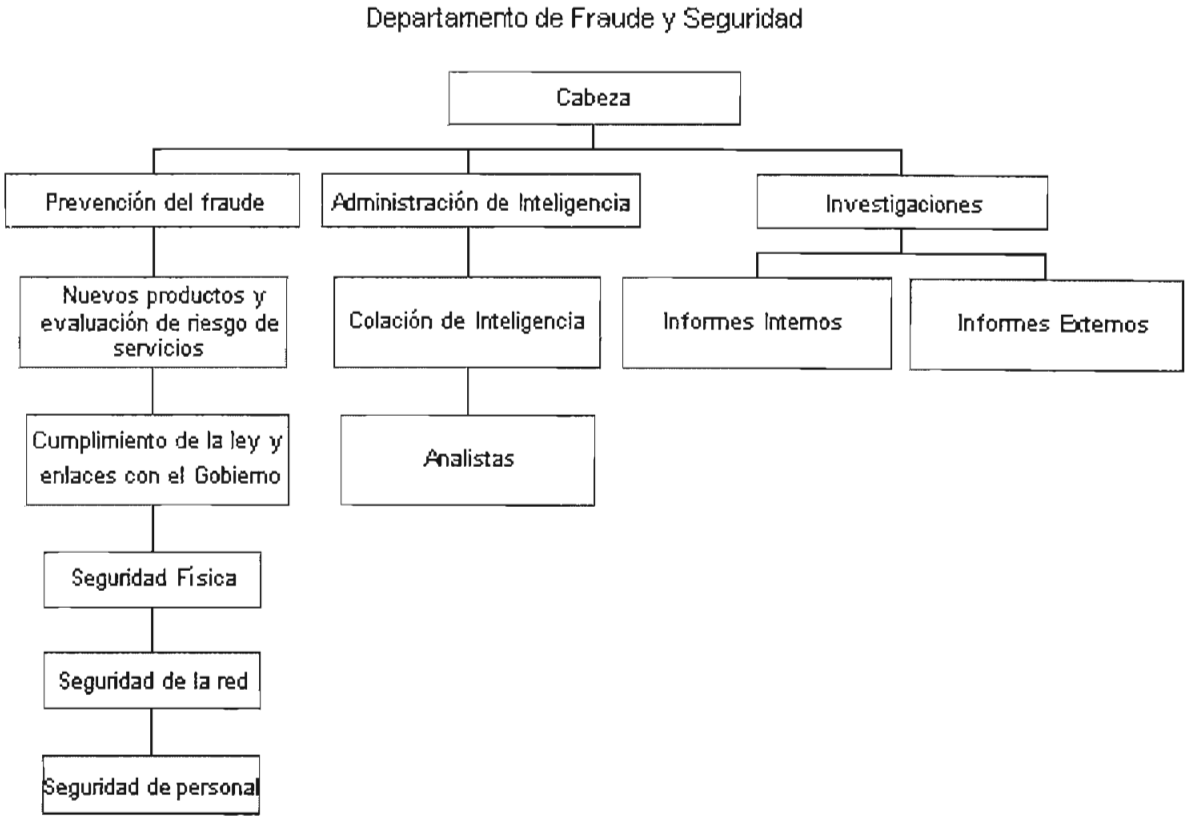


Figura 5.1 Organigrama jerárquico de un departamento de fraude y seguridad

5.1.3.1 Sistemas de administración de fraude

Un documento de esta longitud no puede adecuadamente describir el rango y habilidad de los productos disponibles (sobre 30). Los proveedores serán más que complacientes para ilustrar, describir y demostrar sus capacidades. Consultores independientes son conocedores de este proceso, su asistencia es necesaria. Teniendo la competencia y la capacidad de recursos para obtener el mejor de los productos, es tan esencial como el mismo sistema de administración de fraude. Esto no es una panacea para el fraude. En términos entablados hay sistemas que están basados en:

- Reglas.
- Eventos o perfiles.
- Lógica neural o compleja.

Las principales características de estos sistemas engloban un conjunto de servicios, tales como tipos de alerta: colisión, velocidad; alto uso, no uso, números calientes, destinos calientes, variación de uso, etc., como también la consolidación de uno o más de ellos.

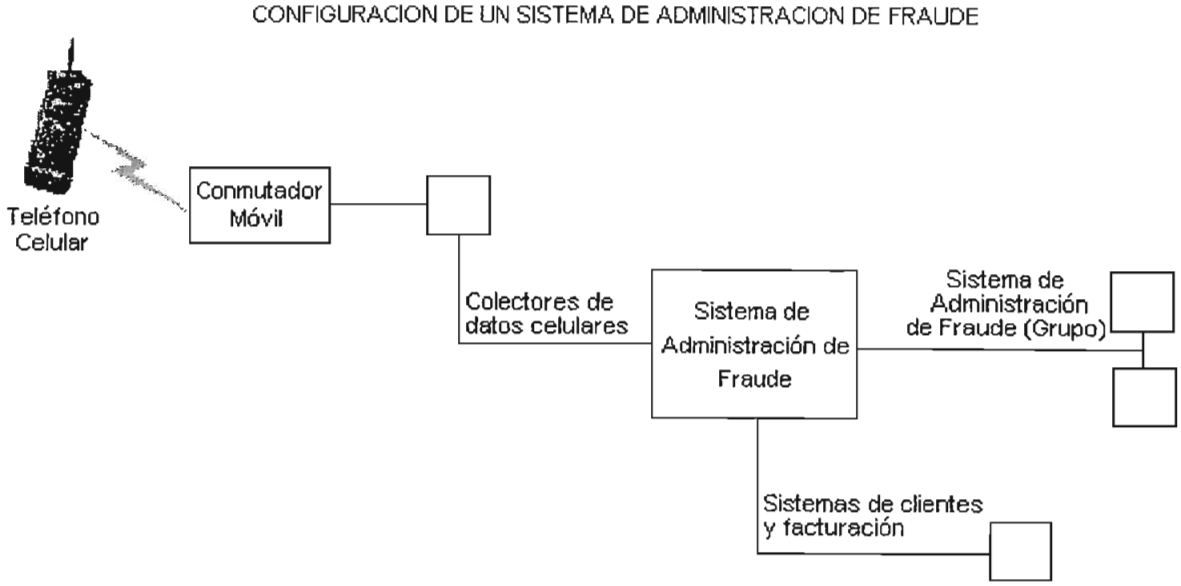


Figura 5.2 Configuración de un Sistema de Administración de Fraude

Algunos de los criterios clave que se debería tener en la lista deseada de tales sistemas son:

- Flexibilidad.
- Facilidad de uso.
- Número manejable de alertas.
- Efectivo manejo y capacidad de demostración.
- Habilidad para aceptar datos completos o parciales.
- Capacidad.
- Soporte, formación e implementación.
- Capacidad de interacción con otras fuentes de datos y herramientas analíticas.
- Tiempo-real (o cierre).

Dado el rango de tecnologías, opciones de configuración de red, diferentes estrategias internas y la variedad de procesos predominantes en la empresa, no existe un sistema de fraude que pueda desplegar todos los requerimientos para cada red. Un sistema de fraude es una significante inversión para cualquier organización. Al escoger un sistema que no trabaje bien o no detecte específicos tipos de fraude que se puede tener, el costo es muy alto a largo plazo. En algunos casos, en un despliegue local, el uso de funcionalidades de uno u otro sistema, puede reunir a corto plazo las urgentes necesidades y puede evitar el apresuramiento en decisiones.

Cuidadosamente siguiendo un riguroso proceso de selección, se asegurará tiempo y dinero, sobre todo, se mejorará que el sistema despliegue las necesidades requeridas.

Si bien el diseño de la seguridad en los nuevos productos al principio es normalmente más fácil y tiene un mayor costo-eficiencia que al añadirlos a los existentes, no todos los productos han sido desarrollados de esta manera. Debemos trabajar en una plataforma de seguridad de productos, examinando los productos establecidos, considerando la tecnología, personas, procesos y sistemas.

Mientras los procesos de seguridad de los productos son universalmente aplicables, hay particulares deficiencias en algunos de los tipos de servicio. Hay que trabajar constantemente con los operadores y proveedores desplegando las últimas tecnologías y servicios.

5.1.3.2 Herramientas analíticas

Un rango mucho más pequeño de productos, es esencial, que represente relativamente una fracción del costo de un sistema de administración de fraude. Sin embargo, esto no es un sustituto. Estas herramientas toman una gran cantidad de datos, incluyendo registro de datos de tasación (CDR), analiza su significado contra ciertas instrucciones (por el analista), y demuestra los resultados ilustradamente o geográficamente. Esto puede ser basado en el tiempo, evento, secuencia o comportamiento. Esto significa dirigir y enfocar las fuentes de investigación por revisión de un cuadro historial y predecir patrones de fraude futuro.

Por otra parte, este análisis asistirá en la demostración de eventos y evidencia para el administrador, Policía y Juzgados. Ellos pueden tomar datos de cualquier fuente en cualquier formato, aún video.

5.1.3.3 Servicios de consultoría

Hay, sin duda, una falta de ganas disponibles por parte de los expertos del F&S particularmente dentro del campo de las telecomunicaciones.

El consultor puede ser sensible a usarlos para establecer una conexión entre huecos vulnerables del operador, capacidad casa dentro, tanto en una base conservada o asignado por las tareas. Ellos ofrecerán:

- Formación – por el personal del Departamento de Fraude (FSD).
- Conocimiento – por otro personal.
- Valoración del riesgo.
- Auditores de F&S.
- Investigaciones.
- Análisis.
- Políticas y Procedimientos.

Los costos pueden parecer altos, pero si los requerimientos son adecuadamente identificados y la consultoría fielmente manejada, los beneficios pesarán más que los gastos y a menudo proveerán soluciones que son difíciles de encontrar.

5.1.3.4 Miscelánea técnica y equipos de investigación

El uso de algunos aparatos es restringido en ciertos países. Dependiendo de la extensión del FSD remitido, los siguientes pueden ser considerados:

- Pruebas terminales y examinación del equipo.
- Cámaras permanentes y video.
- Registradores de audio (para entrevistas sospechosas en ciertos países).
- Dispositivos electrónicos para vigilancia.
- Equipos de Interrogación (PC).

Precaución: Todos los anteriores pueden ser usados solamente donde hay acuerdos con la ley.

5.2 PROCESOS DE ADMINISTRACIÓN DEL FRAUDE

Nuevas tecnologías, productos y procesos proveen nuevas oportunidades de fraude. El manejo del fraude debería ser considerado como un ciclo cerrado girando alrededor de los diferentes tipos de fraude, descritos en capítulos anteriores.

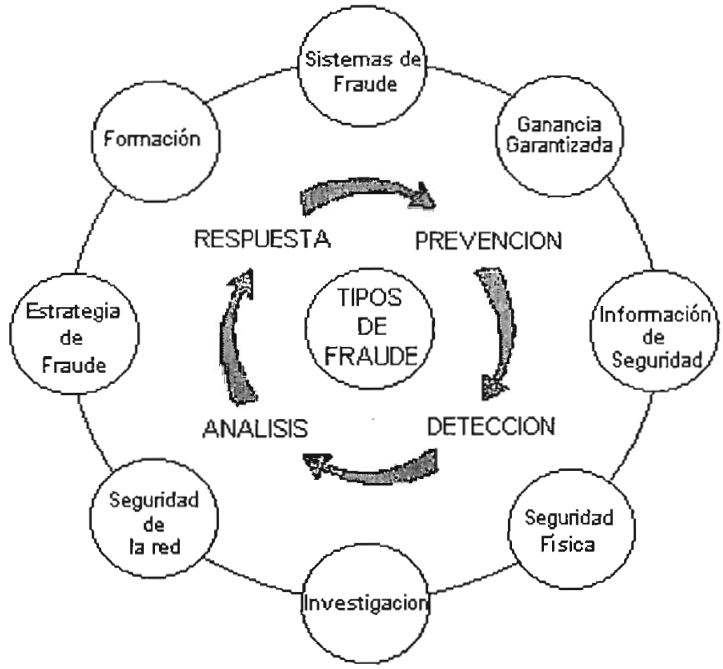


Figura 5.3 Procesos en la Administración del Fraude

- Podemos asegurar que el riesgo se minimice construyendo medidas de prevención apropiadas. Sin embargo, tenemos que tener en claro que no podemos prevenir todos los tipos de fraude.
- Debemos detectar, dónde la prevención fracasa. Detectar lo más pronto posible, ayudará a limitar las ganancias de los perpetradores y minimizar las pérdidas en el sistema de telefonía móvil celular.
- Una vez que el fraude ha sido detectado es importante entenderlo a través de análisis. Los resultados de los análisis pueden ser realimentados para mejorar los procesos de detección y manejar las demás estrategias del ciclo.

- Las respuestas variarán dependiendo del origen del problema y pueden incluir: desconexión, controles de llamada, mejoramiento de los productos de seguridad o detección.
- Las medidas ayudarán a determinar la eficiencia de los procesos de entrada y asegurará el uso efectivo de los recursos disponibles.

Valoración del riesgo de fraude

Solo entendiendo profundamente el fraude de la organización y los riesgos de seguridad, podemos aplicar los apropiados niveles de recursos, costo-eficiencia.

Con una examinación de la empresa, sabemos cómo ésta opera, su posición actual y sus planes futuros. Se identificará áreas de riesgo existente y futuras, luego se proveerá un conjunto de recomendaciones claras, priorizando y accediendo a un despliegue fácil. El resultado de la valoración será un aporte, pero no nos dejará libre de problemas.

5.2.1 SOPORTE DEL SISTEMA DE FRAUDE

Los sistemas de fraude son a menudo un componente clave en la estrategia de la administración del fraude. Ellos pueden representar una inversión significante.

Recuperar esa inversión es crítica, porque depende de muchos factores que pueden afectarla. Si un sistema es configurado inapropiadamente u operado, los beneficios potenciales pueden ser severamente reducidos--algunos operadores han sustituido sistemas, cuando lo necesario era fijar ciertos parámetros y procesos de operación. Se debe enfocar en:

- Seleccionar un nuevo sistema.
  - Definir el mercado y los requerimientos del sistema.

- Alternativas en la construcción y en la decisión de compra.
- Manejar un proceso de selección imparcial y auditable.
- Ayudar a obtener el mejor sistema posible que satisfaga las necesidades y ganancias de la compañía.

- Implementar el sistema y la infraestructura de soporte.
  - Instalar el equipo de fraude y las interfaces críticas de la empresa.
  - Proveer una formación especializada al grupo de fraude y a los recursos de la empresa.
  - Inventariar y documentar todos los procesos de administración de fraude.
  - Establecer sistemas de configuración efectivos para optimizar la detección y los recursos propios.
  - Definir las pérdidas de fraude y las medidas de economía y mecanismos de reporte.
  - Definir y comprobar el soporte del sistema para asegurar su completa funcionalidad.
  - Implementación de un proyecto de administración.
- Examinar y mejorar el sistema existente.
  - Examinar el equipo de fraude y su desempeño operacional.
  - Configurar el sistema para optimizar la detección del fraude.
  - Especificar los cambios en la configuración de los sistemas existentes, nuevos y de los productos.
  - Inventariar y documentar la configuración del sistema y los procesos de administración.

Escogiendo el sistema de fraude correcto y haciéndolo trabajar bien en la operadora, ayudaremos a optimizar la recuperación de su inversión en el sistema y en la infraestructura asociada. Todos los puntos mencionados anteriormente en los procesos de administración de fraude están enfocados en el siguiente análisis, para las dos propuestas de solución que tenemos actualmente, como son, autenticación y *RF Fingerprint*:

Autenticación y *RF Fingerprint* juegan un invalorable rol en la reducción de los niveles de fraude, tales como la clonación, generación aleatoria ESN/MIN, suscripción fraudulenta, robo. Mientras muchos consideran que *RF Fingerprint* es una solución interina, autenticación está creciendo como uno de los estándares dentro de la industria celular.

Estas dos soluciones técnicas garantizarán la seguridad en los teléfonos celulares y en la red, pero no garantizan nada acerca de las personas que los usan.

5.2.2 ANÁLISIS DE APLICACIÓN PARA LOS SISTEMAS DE AUTENTICACIÓN Y RF FINGERPRINT

5.2.2.1 Consideraciones del fraude por clonación en un mundo digital

Hay algunas equivocaciones en el mercado, en cuanto a la seguridad inherente contra el fraude en los mercados digitales. En los Estados Unidos y en América Latina, la tecnología digital TDMA está siendo desplegada rápidamente, pero ¿cuán segura es ésta?.

En la tecnología TDMA se provee un poco más de protección del fraude por clonación que en los mercados analógicos existentes. Tal es así, que las soluciones de protección del fraude deberían continuar para ser desplegadas hacia los mercados digitales. Sobre los últimos pocos años, los operadores inalámbricos han desplegado numerosas soluciones de protección contra el fraude en los mercados celulares, incluyendo sistemas de *profiling*, sistemas de autenticación de claves, aplicaciones de facturación, y sistemas *RF Fingerprint*.

Esto favorece aparentemente a que una solución no tan simple o sola, pueda proveer una solución completa para cualquier especie de fraude. Más bien un conjunto complementario de sistemas de prevención y detección pueden proveer una solución más completa de protección.

5.2.2.2 Soluciones

Históricamente la principal solución deseada por los operadores para proveer protección contra el fraude de clonación en los mercados digitales TDMA ha sido autenticación. Sin embargo, en los últimos años, la primera solución para mercados digitales TDMA estará disponible con *RF Fingerprint.* Esto dará a las operadoras celulares nuevas opciones para la protección y detección, y así dar otra opción en la comparación de estas dos tecnologías.

Ambas, autenticación y *RF Fingerprint* pueden ser usadas tan bien en ambientes analógicos como en digitales, y ambas soluciones proveen significativa protección contra el fraude por clonación. Pero es importante notar que cada una de ellas despliega características y operación únicas.

Idealmente, los operadores podrían desplegar ambas soluciones para asegurar máxima protección. Sin embargo, si consideramos separadamente, la próxima generación de soluciones *RF Fingerprint* podrán tener algunas ventajas sobre las soluciones de autenticación.

5.2.2.3 La longevidad de autenticación

El escepticismo acerca de la eficacia de cualquier solución de fraude continúa envolviendo códigos artificiales que han incrementado sin parar en recientes años. Y sin duda han estado carburando por instancias altamente hechas públicas de los esquemas de encripción y autenticación incluyendo procesos de seguridad alterados; tales como seguridad en Netscape y en el algoritmo de encripción de mensajes celulares (CMEA). El principal algoritmo anti-clonación, CAVE, no ha tenido los suficientes efectos expuestos hasta la fecha, ha sido criticado, a tal punto que lo consideran anticuado y potencialmente vulnerable para los rompedores de códigos. Así los algoritmos están constantemente mejorándose para hacer frente a estos malhechores.

RF Fingerprint, por otra parte, analiza las características de la señal de cada teléfono individualmente y toma una decisión de validación basada sobre métricas únicas e incopiables. Por lo tanto no hay que romper códigos.

5.2.2.4 El desafío administrativo en el despliegue de la autenticación

La seguridad proporcionada por los algoritmos criptográficos en los sistemas de autenticación puede ser irrelevante, así existe una gran vulnerabilidad expuesta en los procedimientos de implementación de autenticación usadas por las operadoras.

Hay un número de desafíos que necesitan ser implementados en un sistema de autenticación durante su despliegue:

- Compatibilidad entre los tipos de switches .
- Estándares incompatibles para cargar las claves A en los teléfonos.
- Compartir los datos secretos compartidos (SSD) para *roaming*.
- Provisionar autenticación fuera de los mercados grandes.
- Los gastos de configuración y las estrategias administrativas.

Los operadores buscan estrategias de implementación simples, aún teniendo que adoptar procedimientos que reduzcan significativamente la eficiencia de solución de autenticación, tal como tener la clave A universalmente fijada para una configuración por *default* de todos los ceros. En mercados, donde el servicio ya ha sido desplegado sin autenticación, el despliegue logístico de la autenticación puede ser arrollador.

Alternativamente, *RF Fingerprint* tiene una arquitectura escalable, es decir, es ofrecida como una solución buró o como un sistema completo (incluyendo convenios internacionales). La implementación y la operación se realizan por el proveedor del servicio, causando interrupciones mínimas para la organización.

5.2.2.5 Protección de roaming

Las operadoras están ahora confrontando el hecho de que, como *RF Fingerprint*, la autenticación deber ser desplegada dondequiera para proveer una protección completa de roaming. En Norte América, por ejemplo, el área de presión de autenticación es muy grande, sin embargo, hay falta de cobertura en el desarrollo de mercados. *RF Fingerprint* tiene un extenso y muy bien establecido mercado de roaming analógico en todas partes de Norte América, Latino América y partes de Asia. Esta ha sido desplegada en cientos de sitios de celda en cientos de mercados, y ha tenido éxito dondequiera.

5.2.2.6 Implicación organizacional

Una cantidad significante de fraude inalámbrico viene internamente de la organización de la operadora. La mayor amenaza para la autenticación (las redes protegidas) es el compromiso ético por parte de los empleados de la operadora. En la otra mano, RF Fingerprint no puede ser copiado, así no hay amenaza de generar internamente fraude por clonación. *RF Fingerprint* es también altamente automatizado, lo cual reduce los gastos operacionales y de personal comparado con autenticación, la cual puede ser compleja e incómoda.

5.2.2.7 Compatibilidad con teléfonos existentes

Es importante notar que los teléfonos más antiguos no pueden ser autenticables. Particularmente en economías altamente desarrolladas, esto puede favorecer un mayor marketing. El despliegue de los sistemas de claves de autenticación puede por lo tanto dejar a los operadores en riesgo con los teléfonos más viejos o sujetarlos a incrementar los programas de los teléfonos. Aún en los mercados donde existen teléfonos que son autenticables, los operadores enfrentan tales desafíos. Como la autenticación es inicialmente desplegada, los teléfonos necesitan ser programados directamente, afectando de todas formas al usuario.

En contraste *RF Fingerprint* es compatible con cualquier teléfono, sea digital TDMA o analógico, y así, protege el ingreso a la base del mercado, incluyendo teléfonos analógicos y TDMA más antiguos. Es decir, es transparente al usuario.

RF Fingerprint podría ser impedida por una falta de estandarización, *Corsair y CTS*, por ejemplo, actualmente no son compatibles, pero ambas, han estado agresivamente pactando con *Bellcore* acerca del desarrollo de un estándar de interoperabilidad. Hasta que tal estándar exista, sin embargo, las operadoras probablemente escogerán la tecnología que cubra sus necesidades.

5.2.2.8 Asunto de costo

Desde que las primeras soluciones anti-clonación fueron introducidas, la industria celular ha medido los sucesos de estas soluciones por la cantidad de fraude activo que ha sido detenido.

La métrica tradicional de éste, ha sido el número de "desconexiones," o llamadas fraudulentas denegadas. Es decir, por la naturaleza de una efectiva solución contra el fraude por clonación, el número total de intentos fraudulentos disminuye en un mercado dramáticamente, a través del tiempo. Esto guía a algunos operadores a creer que el fraude emitido ha sido solucionado y cuestionar el valor del costo continuo de protección.

Sin embargo, esto favorece aparentemente a que la métrica se transfiere ineficazmente en la medida real del riesgo del fraude. Hay fraudes latentes no medibles, que existen en el mercado. Los perpetradores atacan el camino de menos resistencia, y debería la protección anti-clonación ser reducida, el fraude por clonación retornará en el manejo.

Por otro lado la medida del valor de una solución de fraude, se examinará por el costo por desconexión, un modelo seguro podría ser una solución más apropiada. Tal modelo podría medir la protección costo por llamada o la protección costo por suscriptor.

Si bien los mercados pueden usar una aproximación organizada para desplegar autenticación, eventualmente la estación base, el MSC, el HLR tendrán que ser revalorizados para ser autenticables. Adicionalmente una base de datos/traductor de clave A debe ser comprado e instalado paralelamente a través de una formación y seguridad. Mientras los costos de los sistemas de autenticación se han disminuido en algo desde su introducción, la implementación de plataformas múltiples asociadas con la proliferación de estos sistemas por todas partes de una red introduce sucesivos incrementos en los costos, que, combinados con delicadas implementaciones logísticas, puede resultar en una solución muy costosa.

Así, empleados, ingenieros, solicitudes de clientes, activaciones, y ventas, deberían ser formados en autenticación. Los operadores con tecnologías basadas en *RF Fingerprint* pueden disfrutar las ventajas en costo a través de la conjunción de la infraestructura con sus despliegues TDMA mediante la adición de receptores con capacidad de TDMA en las estaciones base seleccionadas, lo cual significativamente reduce el costo de despliegue y el costo de operación por llamada protegida.

5.2.2.9 ¿El fraude por clonación en las redes de modo dual, como en las analógicas?

Con la aceptación ampliamente dispersa y con el despliegue que la tecnología digital ha disfrutado por todas partes de los U.S., Canadá, y Latino América, las redes analógicas para la mayoría de partes, ha estado olvidada y el riesgo del fraude por clonación está latente. *RF Fingerprint* en las redes analógicas virtualmente ha eliminado la existencia del fraude por clonación.

En casos extremos, las operadoras ingenuas han mirado el despliegue de la infraestructura digital combinada con la reducción de los eventos de llamadas analógicas clonadas como justificación para reducir el despliegue de la cobertura de sus *RF Fingerprint* analógicos. Como los perpetradores continúan con sus siempre creativas e ingeniosas luchas para liberar el tiempo aire, tales mercados desprotegidos encontrarán pérdidas incrementándose nuevamente.

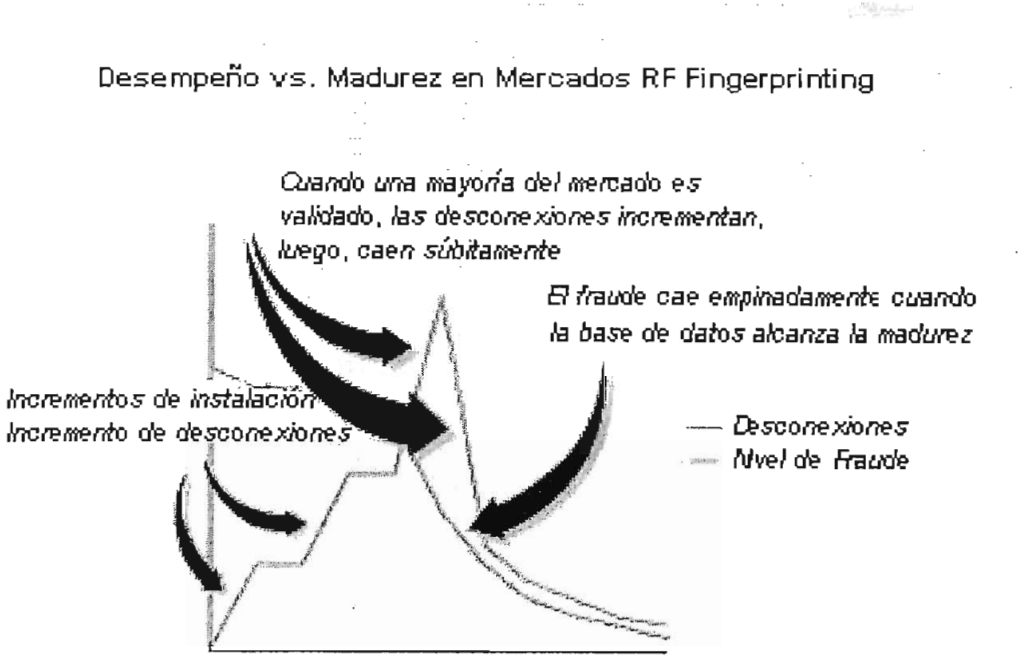


Figura 5.4 Desempeño versus maduración en mercados RF Fingerprint[1]

5.2.2.10 ¿Mantenimiento de las redes analógicas?

Mientras nadie puede discutir de la importancia y las economías proporcionadas por el despliegue de la tecnología digital, la tecnología analógica esta lejos de la muerte. Más allá de las redes de roaming, la tecnología analógica complementa la infraestructura digital proveyendo cobertura en los agujeros que esta tecnología puede dejar, capacidad de sobreflujo y los profundos costos económicos.

[1] www.corsair.com/search/rffingerprint

En Norte América y en América Latina, los suscriptores AMPS exceden en número a los suscriptores TDMA por un factor estimado de tres.

Protección de la infraestructura analógica

La industria puede estar viendo una reducción en el número de suscriptores AMPS dedicados, sin embargo, la tecnología analógica mantiene al roaming como el denominador común entre las bondades de los mercados digitales. Sin un estándar digital único, para favorecer la tecnología escogida de entre la mayoría de portadoras (CDMA, TDMA, PCS), los vacíos que en cobertura mantendrán en el cercano mediano plazo requiere infraestructura AMPS para proveer inconfundibles servicios a los suscriptores. La autenticación analógica está disponible, pero muchas portadoras no la han visto completa, para desplegar esta complicada tecnología en sus mercados analógicos, apoyando en cambio el mantenimiento de la tecnología *RF Fingerprint* comprobada.

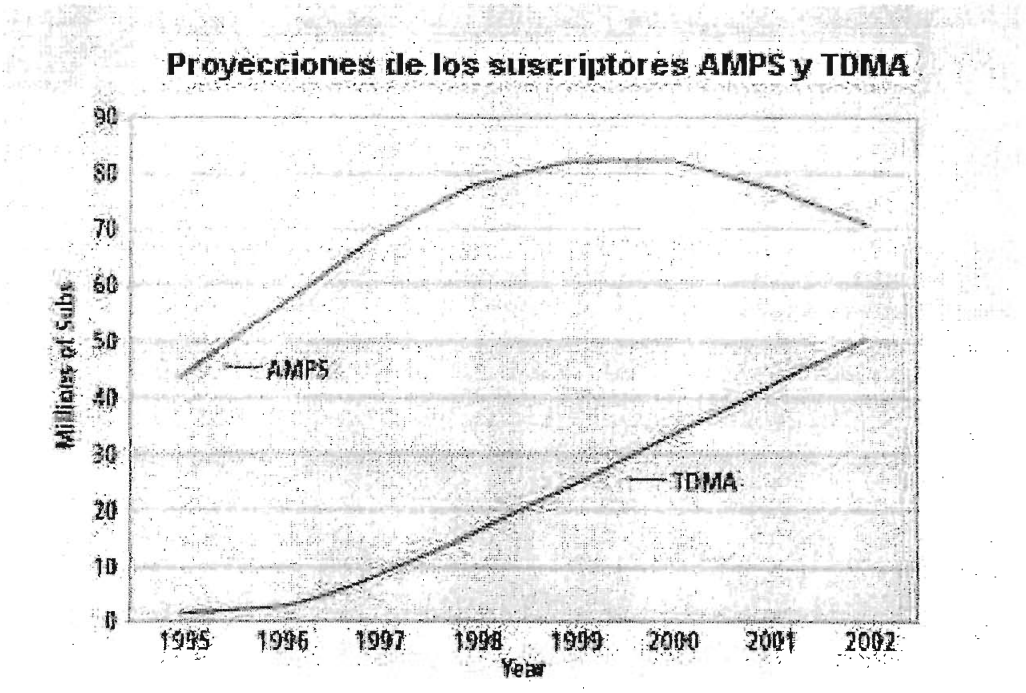


Figura 5.5 Proyecciones de los suscriptores AMPS y TDMA[1]

[1] www.corsair.com/search/rffingerprint

5.2.3 GANANCIA GARANTIZADA

Las Telecomunicaciones es uno de los ambientes más difíciles en el cual se garantiza ganancias porque el gran número de transacciones procesadas es de bajo valor. Un proceso de ganancia garantizada busca asegurar que todas las ganancias que deben ser acumuladas de activaciones, suscripciones y uso de redes es exactamente facturada de una manera oportuna. Los mecanismos que son requeridos para asegurar ganancias, son:

- Auditando el paso de los datos del conmutador a la factura, asegurando que esos registros no desaparezcan, o se modifiquen.
- Verificando que todas las llamadas produzcan reportes precisos.
- Analizando anomalías o tendencias que puedan indicar problemas.
- Controlando cambios hechos a las plataformas de soporte (conmutadores, aprovisionando y facturando sistemas) para asegurar que esos cambios sean apropiadamente autorizados y correctamente implementados.
- Analizando diferencias entre ganancias facturadas y colectadas.

5.2.4 SEGURIDAD DE LA INFORMACIÓN

La información es una de las ventajas más grandes de la organización. Hechos y figuras acerca de los usuarios, redes, productos y procedimientos son esenciales para la operación de la empresa. Cada edificio, computadora, escritorio y empleados contienen información que debe ser protegida.

Sin la apropiada protección, los requerimientos de protección de datos locales podrían fallar, hacer titulares en la prensa nacional, o ayudar a otros operadores ganar una competitiva ventaja. Afortunadamente, hay muchas maneras para proteger la información, podemos identificar la información en riesgo, determinar niveles apropiados y planear implementarlos.

5.2.5 SEGURIDAD FÍSICA

El riesgo asociado, variará con cada uno por toda la empresa y los controles aplicados deben ser balanceados cuando el riesgo se presente. Debemos enfocarnos en los siguientes aspectos:

- Examinar las operaciones de la empresa de extremo a extremo.
- Examinar el enfoque desplegado de elementos específicos de su operación, sitios o edificios.
- Despliegue de políticas, estrategias y estándares para reunir las necesidades más exactas.
- Introduciendo procesos de administración y controles para mantener la eficiencia de la infraestructura de seguridad mientras la compañía crece y cambia.

5.2.6 INVESTIGACIÓN

Usada apropiadamente, la investigación, puede ser una herramienta efectiva en el combate contra el fraude. Sin embargo, un inapropiado uso de recursos, puede aumentar el costo de operación y un incompleto proceso de administración del fraude. Investigaciones eficaces deberían enfocar en claves emitidas y/o elementos particulares de los casos de fraude para optimizar el impacto. Los administradores de la investigación tienen conocimientos en las agencias que hacen cumplir las leyes y en las más grandes empresas de telecomunicaciones y están bien versados en prácticas comerciales y técnicas de investigación. Sus destrezas pueden ser aplicadas para ayudar en:

- Reunir y analizar la información.
- Planear y manejar la investigación de casos específicos.

- Reunir y preservar la evidencia para soportar los casos.
- Hacer a menudo complejas decisiones.
- Fijar las políticas de investigación.
- Desplegar tus propias destrezas de investigación a través de la formación, preparando y transfiriendo esos conocimientos.
- Establecer un análisis efectivo y manejo de los sistemas para soportar las investigaciones dentro de la empresa.

Los criminales, como los electrones, tienden a tomar el camino de menos resistencia. En el caso del sistema de telefonía móvil celular, las defensas fijadas contra la clonación han motivado a los criminales a adoptar las varias técnicas usadas por robos internos de información confidencial, tanto del sistema como de los usuarios, las cuales están reunidas bajo la rúbrica, suscripción fraudulenta. Así como la clonación, las principales defensas industriales han persuadido al Congreso a fortalecer los estatutos (en este caso, el Título 18, Sección 1028 del Código de los Estados Unidos, "Fraude y actividad relacionada en conexión con la identificación de documentos e información")[1].

De acuerdo a como ahora las leyes permanecen, este es un Crimen Federal meramente por el robo de la información de identidad de alguna persona, con el intento de defraudar. Adicionalmente, las normas y regulaciones de la FCC prohíben el engaño con y/o la alteración de ESNs en el interior de un teléfono inalámbrico. Cada móvil debe tener un único ESN y dos teléfonos no pueden emitir el mismo número, de acuerdo a las normas de la FCC.

La industria se ha hecho particularmente susceptible a la suscripción fraudulenta, cuando ésta empezó a seguir nuevos usuarios a través de canales no tradicionales como son el telemarketing y el Internet.

[1] Michael J. Riezenman, (2000), p.40.

De igual manera las operadoras han estado trabajando junto con el Servicio Secreto de los Estados Unidos, para que el Congreso mejore la ley relacionada con "Fraude y actividad relacionada en conexión con accesos a dispositivos" (Título 18, Sección 1029, del Código de los Estados Unidos)[1], en el que se establece como Crimen Federal el apropiarse de scanners o programar teléfonos celulares con el intento de hacer fraude.

Esa misma ley también establece crímenes hechos maliciosamente, y con el intento para defraudar, para usar un teléfono falsificado, para traficar en tales teléfonos o para poseer 15 o más de ellos. La ley es seria, especifica una prisión máxima de 10 o 15 años (por primera vez), dependiendo de la naturaleza exacta del crimen.

5.2.7 SEGURIDAD DE LA RED

Mejorando la confidencialidad, integridad y disponibilidad de la información, sistemas y redes, junto con las acciones de los usuarios; se puede reducir la oportunidad de fraude:

- La confidencialidad de datos es crítica para prevenir su abuso por parte de los perpetradores dentro y fuera de la organización
- Los mecanismos para mejorar la integridad de los datos minimizarán la oportunidad de fraude y hace que la detección sea más fácil y más rápida

5.2.8 ESTRATEGIA DE FRAUDE, PÓLITICAS Y PROCEDIMIENTOS

Resolver el problema del fraude en el sistema de telefonía móvil celular es una tarea difícil. A menudo, la importancia de enfocar el problema, no es reconocido por toda la organización, principalmente por los conflictos con otras partes de la empresa.

---

[1] Michael J. Riezenman, (2000), p.40.

En tal ambiente, esta meta a menudo es difícil de alcanzar. Aplicando una estructura coherente para la administración del fraude es esencial para el éxito. Para aplicar esa estructura:

- Trabajarán representantes de diferentes partes de la empresa para desplegar políticas configuradas sobre todas las direcciones para la administración del fraude.
- La estrategia de la administración del fraude fija una visión para la organización y un aprovechamiento para alcanzar esa meta. Se trabajará siguiendo una examinación del mercado, trabajar conjuntamente para desplegar una estrategia para transportarla hacia el futuro.

5.2.9 FORMACIÓN

Los perpetradores están desplegando sus usos, o abusos de los servicios y productos, de los operadores más rápido como nunca antes.

Un efectivo administrador de fraude requiere una combinación de destrezas operacionales y una apropiada estructura de sus roles y responsabilidades. Similarmente, un énfasis inapropiado en una solución de fraude dejará vulnerabilidades donde quiera. Hay diferentes cursos de formación que desarrollan en el profesional un nivel de entendimiento y destrezas requeridas para combatir el fraude eficientemente.

La formación provee un aprendizaje estructurado mediante cursos los cuales reparten los conceptos claves durante todo el día y sobre todo el evento. Una mezcla de sesiones de aprendizaje, grupos de discusión y prácticas de ejercicios proveen el beneficio real de esta formación.

5.3 EXPERIENCIA DE LAS OPERADORAS LOCALES EN EL ECUADOR

En nuestro país, el fraude celular no ha alcanzado aún los niveles de pérdidas tan altas como en otros, pero eso no quiere decir que las operadoras locales no deban preocuparse por este problema. Tanto *BellSouth* como *PortaCelular* han registrado fraude, en particular por suscripción fraudulenta, pero estimativamente sin afectar a sus ingresos ni a sus usuarios. Según declaraciones de estas dos operadoras, para evitar el crecimiento del fraude, han mejorado sus sistemas de prevención, utilizando tecnología avanzada, ya que no hay organismo estatal que los proteja ni sentencie a los malhechores.

Los sistemas utilizados por las dos empresas de telefonía celular más grandes del país para detectar fraudes por clonación son: la plataforma Ericsson, en el caso de Otecel (*BellSouth*) y la plataforma Compaq en el caso de Conecell (*Portacelular*).

Tanto Otecel como Conecell han hecho inversiones para prevenir el auge de la clonación de celulares, ofreciendo ambos un conjunto de servicios que aseguren este propósito. Estas dos empresas siguen un esquema de administración de fraude similar, basándose en toda la información analizada previamente es este capítulo.

En la parte de Administración de Fraude y Seguridad, se han creado Departamentos de Fraude, a la cabeza de estos, se encuentran sus respectivos Gerentes de Fraude, con unos pocos años de experiencia, pero con la suficiente preparación para conseguir los objetivos que persiguen estos departamentos.

Sus principales funciones son las de mantener pistados los problemas de fraude mediante la aplicación de políticas o protocolos para investigar estos incidentes. Formando tales equipos también ha mejorado la comunicación entre las operadoras y sus usuarios honestos en los resultados del fraude.

Los dos gerentes de estas dos empresas, concuerdan en decir que haciendo esfuerzos para ganar más conocimientos, se puede colectar y analizar los datos de fraude más rápidamente, de esta manera se pueden hacer decisiones más rápidas acerca de que hacer. Tienen claro que golpear el fraude será un proceso a largo plazo.

Los vendedores de productos antifraude usualmente establecen estrechas relaciones con las operadoras, con el propósito de combatir de mejor manera específicos tipos de fraude y trabajar continuamente con estos productos.

En el soporte del sistema, estas portadoras siguen un formato de implementación, basado en la combinación de distintos servicios que incluyen:

- Sistemas PIN.
- Autenticación.
- Tecnología de Perfiles de Usuarios.
- Equipos de Investigación de Fraude.

En la primera línea de defensa, el sistema PIN, requiere la clave de un usuario particular para poder desbloquear su teléfono y poder realizar llamadas de larga distancia. Después de completar la llamada, el cliente reingresa el código, bloqueando el teléfono. Para clientes que usan el servicio de roaming, pueden mejorar la protección del método PIN por compartición de la información del PIN con otras portadoras que tienen los mismos patrones.

Como segunda defensa, ambas portadoras utilizan sistemas de autenticación para prevenir y detectar el fraude. Otecel, manifestó que quisieron implementar la tecnología PhonePrint, pero a largo plazo resulta muy costosa debido a que hay que instalar una RFU en cada estación base, pero no la desechan tampoco.

Con el sistema que ellos tienen implementado, a largo plazo, primero han recuperado su inversión y protegerán a su compañía por muchos años más. Conecell por su parte, no ha querido hacer reemplazos a su sistema y van a seguir utilizando la autenticación como principal servicio de protección.

Otecel, admite que tienen pérdidas debido a fraude por clonación y por suscripción fraudulenta, pero que su peso no afecta ni a la compañía, ni a los usuarios. El departamento de fraude ha identificado a las personas que comenten fraude por clonación, pero por no haber un organismo que intermedie con la justicia, no han seguido con las disposiciones legales. Conecel no reveló esos datos y prefirió olvidar el asunto.

Otra línea de defensa, es la tecnología de perfil de usuario, la cual permite pistar las llamadas de los suscriptores y patrones de roaming. Si hay un comportamiento inusual, el sistema alertará al operador y este reportará el hecho, para que luego la operadora contacte al suscriptor para confirmar si las llamadas fueron o no válidas.

De esta manera, la protección que ofrecen estas empresas a sus clientes les garantizará mayor competitividad y sobre todo les permitirá elegir a la que satisfaga la mayor parte de sus necesidades.

5.4 CONCLUSIONES Y RECOMENDACIONES

- Las operadoras están continuamente elevando la tecnología de sus redes para maximizar sus líneas inferiores. Las soluciones de fraude han evolucionado con la tecnología de redes y proveen protección a las bases de ingreso de los suscriptores de la operadora, pero no hay soluciones efectivas que puedan eliminar todos los tipos de fraude.

- El fraude puede presentarse de varias maneras. Así, hay diferentes tipos de fraude, allí estarán diferentes efectos observados en diferentes partes de la empresa. Algunos de estos efectos aparecerán para ser negocios o normas de calidad más que normas de fraude y pueden por lo tanto ser tratados inapropiadamente.
- El fraude es una seria preocupación para todos los miembros de la industria de comunicaciones inalámbricas. Los abonados se sienten maltratados cuando sus teléfonos cesan de funcionar, o cuando reciben grandes facturas por servicios que una persona ajena ha usado a sus expensas. Los operadores pueden ofrecer cambiar el número MIN de un abonado pero esto es una solución inconveniente. Los departamentos de servicio a los clientes deben estar bien preparados para tratar con los clientes infelices que han sido objetos del fraude, ya que los clientes pueden cambiar fácilmente su proveedor de servicios (lo cual resulta en mayor agitación). Las operadoras se sienten así mismo frustradas por tener que acarrear los costes de un tráfico no autorizado. Estas pérdidas indican sin embargo claramente cualquier proveedor de servicios antifraude está en posesión de una oportunidad inapreciable, con su cartera de medidas combativas del fraude, para ejercer un impacto directo y positivo en la hoja de balance de los operadores, al minimizar o eliminar totalmente el fraude.
- Una solución no tan simple o sola, no necesariamente proveerá una solución completa para cualquier tipo de fraude, soluciones conjuntas a través de carteras antifraude que ataquen en diferentes frentes del sistema celular, proveerán una solución mucho más completa de protección, en especial cuando usen diversas formas de detección. Es así que las pérdidas por clonación disminuyeron de un 4% en 1995 a ½% en 1997 debido al uso de sistemas de perfiles, huella digital RF, y autenticación (60% a nivel mundial).

- El fraude por clonación se ha reducido dramáticamente en los recientes años, pero el fraude permanece latente, en postura de serias amenazas a la rentabilidad de las operadoras. Mientras la autenticación ha sido rápidamente adoptada como una solución al fraude por clonación en mercados TDMA, carece de desarrollo en mercados de *roaming* (debido a que los SSD no tienen interoperabilidad entre mercados). Soluciones *RF Fingerprint* que emergen pueden proveer significantes ventajas para segmentos específicos del mercado (analógico y digital).
- Las redes de modo dual complican el despliegue eficaz de las soluciones de fraude por clonación. La infraestructura analógica y los teléfonos más antiguos no dudarán en mantener su operación para los años que vienen, y por consiguiente, las operadoras deben considerar una estrategia de protección completa que es eficaz para las dos tecnologías, nuevas y establecidas.
- En este momento, tanto Autenticación como *RF Fingerprint* proveen protección en mercados digitales. Desplegar las dos soluciones paralelamente no es recomendable, debido a la incompatibilidad tanto con teléfonos como con la red; así autenticación puede dejar mercados analógicos desprotegidos por no ser autenticables (no solo en teléfonos sino también en conmutadores, estaciones base, AC, etc.) aún en mercados donde se dispone de teléfonos autenticables tiene problemas, no dispone de un suficiente despliegue de mercados. *RF Fingerprint* carece de estandarización y no presenta compatibilidad entre proveedoras del servicio, la diferencia está en que esta solución es compatible con cualquier teléfono, digital o analógico; y lo más importante es transparente al usuario.
- Autenticación no es un sistema muy automatizado, debido a que algunas de sus operaciones básicas pueden ser realizadas por parte del operador, mientras tanto *RF Fingerprint* es mucho más automatizada, de esta manera se reducen gastos operacionales y de formación del personal en el manejo de dicho sistema.

- Con el aparecimiento de rompedores de códigos, la vulnerabilidad de los seguros digitales ha aumentado, de hecho las constantes mejoras sobre dichos seguros ha frenado a dichos malhechores, no en su totalidad; autenticación presenta claves A inseguras en el momento de grabarse y por *default* todos los bits son ceros, además que en los recientes años el algoritmo CAVE ha sido objeto de manipulación, entonces por qué no considerar nuevas tecnologías que involucran análisis de señales con métricas únicas e incopiables, como *RF Fingerprint*, otra alternativa que puede surgir tal como autenticación, y con más fuerza.
- A nivel de costo-eficiencia, a largo plazo, autenticación podrá ser desplegada en la mayor parte de mercados, pero tomando en cuenta los recientes avances de la tecnología de radio frecuencia, *RF Fingerprint* no es una solución descabellada, cabe notar que en costos de implementación, esta última es más elevada, debido a que hay que instalar unidades de radio frecuencia en cada estación base.
- Autenticación posee ciertas deficiencias en el proceso de demanda y respuesta, por ejemplo, la respuesta de prueba única puede ser interceptada por *scanners* digitales, todavía no usados por su alto costo; y además algunas redes no soportan demandas periódicas en el momento de producirse una registración u originación.
- *RF Fingerprint* trabaja paralelamente con su propia base de datos de huellas digitales de RF, permitiéndolo bajo una gran cantidad de parámetros construir dichas hullas mediante una maduración eficaz, de esta manera puede diferenciar los distintas llamadas e intentos de llamadas como sucesos de fraude o caso contrario de no fraude.
- Idealmente, la tercera generación debería proveer los servicios de comunicaciones personales en cualquier tiempo y en cualquier lugar. Mientras las transiciones de sistemas analógicos a los primeros digitales fueron diseñadas para arreglar los problemas que ellos acarrean, como seguridad, bloqueo, e incompatibilidades regionales; la migración a la tercera generación abre una vista en su totalidad hacia nuevos servicios. El precio es un esfuerzo

grande, para cada fase de migración, con cada fase demandando su propio plan de negocios.

- El desarrollo apropiado de eficaces fuentes de Fraude y Seguridad es una contribución principal a la fortaleza comercial y competencia para cualquier organización.
- Las métricas de la cantidad de fraude que ha sido detenido, desconexión de llamadas versus tiempo, no garantizan totalmente que el fraude está perdiendo la batalla, la razón, existen fraudes no medibles y que están ocultos dentro de la empresa. Estos nos determinan el costo de una solución de fraude mediante el costo por desconexión, pero esto es parte de los parámetros técnicos, mas no los relacionados con el personal interno.
- La mayor amenaza para las operadoras celulares en la actualidad, es la suscripción fraudulenta, en los Estados Unidos hay 40 millones de teléfonos analógicos a ser clonados, pero 250 millones de identidades para robar. Si una solución antifraude no puede manejar el comportamiento ético por parte de los empleados; no sirven de nada los esfuerzos técnicos que se han implementado. Por esta razón, una adecuada administración del fraude, junto con los equipos de personal afines, garantizará la máxima seguridad y será una arma poderosa en el combate contra el fraude
- Es importante la creación de controles de producción y la necesidad de una empresa en línea, para de esta manera detectar actividades fraudulentas desde los registros de datos de tasación. Empresa en línea en el sentido de fomentar herramientas de gestión para medir productividad por análisis de fraude y costo contable por fraude recibido.
- Se debe incentivar la creación de acuerdos internacionales entre grupos detectores de fraude, especialmente en el caso de *roaming*.

- Dos de los procesos de administración de fraude que hace falta explotarlo, especialmente en Latinoamérica y en especial el Ecuador, son la investigación y la falta de legislación. En nuestro medio, las operadoras celulares no tienen organismo alguno que las proteja contra los criminales, y por lo tanto ni pena carcelaria por los engaños que les han causado, por esta razón, a futuro; el Congreso Nacional debería regular estas actividades, basándose en leyes, las penas correspondientes por abuso de información y utilización de equipos con el propósito de cometer fraude.
- Se recomienda a cualquier estudiante de telecomunicaciones, interesado en este proyecto de titulación, continuar con esta investigación, llenando algunos espacios que quedaron sin hacerlo; la administración de fraude y todo lo que ésta engloba junto con todos los nexos con los distintos departamentos dentro de una operadora celular, es un campo demasiado extenso y complicado, en el sentido de que toda la información que se requiere para realizarlo es demasiada confidencial, pero como yo lo experimenté, imposible. El reto está en continuar este estudio para todos los demás sistemas móviles que se tienen actualmente, la aplicación de la biométrica a las huellas digitales de los suscriptores, también los beneficios prácticos de la aplicación de tecnologías de redes neurales y lógica difusa en su interoperabilidad con las redes convencionales para mejorar la efectividad del análisis sobre los departamentos de manejo de fraude, la actualización que se hace a los registros de datos de tasación y los beneficios de las innovaciones sobre sus bases de datos.

REFERENCIAS BIBLIOGRÁFICAS

- HTTP://TEASER.IEEE.ORG/PUBS/SPECTRUM/9908/CELL.HTML
- HTTP://WWW.WOW-COM.COM/CONSUMER/FAQS/FAQ_FRAUD.CFM
- WWW.ALCATEL.COM
- WWW.ATTWS.COM
- WWW.BELLSOUTH.COM
- WWW.CDG.ORG
- WWW.CELLULARONEPR.COM
- WWW.CINECOM.COM
- WWW.COMMISION-JUNTION.COM
- WWW.COMPAQ.COM
- WWW.CORSAIR.COM
- WWW.ERICSSON.COM
- WWW.ERICSSON.SE/FRAUDOFFICE.COM
- WWW.ETSI.FR
- WWW.FRAUDMANAGEMENT.COM
- WWW.GSM-PCS.ORG
- WWW.GSMWORLD.COM
- WWW.IDENTIX.COM
- WWW.IMTA.ORG
- WWW.ITU.INT

- WWW.LUCENT.COM/WIRELESSNET/VRITUAL
- WWW.MOTOROLA.COM
- WWW.NOKIA.COM/DISCOVERY
- WWW.QUALCOMM.COM
- WWW.TELECOUNT.COM
- WWW.TIAONLINE.ORG
- WWW.TSI.GTE.COM
- WWW.UWCC.ORG
- WWW.WIRELESSWEEK.COM
- WWW.WOW-COM.COM/TECHOPS/SECURITY
- FML Securing Business, Segundo Congreso Latinoamericano sobre: Revenue Assurance &Fraud Management en Telecomunicaciones, 17-19 Mayo 2000.
- J. Riezenman Michael, Cellular Security: better, but foes still lurk, Vol.37, No.6, IEEE Spectrum, Junio 2000.
- Lundin Catharina, Nguyen Binh y Ewart Ben ,Tratamiento y Prevención del Fraude en el Sistema Amps/D-amps, Ericsson, 1996.
- Rivas Castro Yeliza, Combatiendo el delito en telefonía móvil, Mobile LatinoAmérica, Enero-Marzo 2000.
- Tomasi Wayne, Sistemas de Comunicaciones Electrónicas, Prentice-Hall, Segunda Edición, 1996.
- W. Oliphant Malcom, The Mobile Phone Meets the Internet, Vol.36, No.8, IEEE Spectrum, Agosto 1999.
- Zambonino Franklin, Telefonía Celular y Sistemas Inalámbricos, SUPTEL, Diciembre 1998.

ANEXO A

LISTA DE TELÉFONOS ANALÓGICOS QUE SOPORTAN Y NO SOPORTAN AUTENTICACIÓN

MARCA	MODELO	MODO	AUTENTICACION
ERICSSON	AF738	ANALÓGICO	SÍ
ERICSSON	AF778	ANALÓGICO	SÍ
ERICSSON	AH210	ANALÓGICO	NO
ERICSSON	AH220	ANALÓGICO	NO
ERICSSON	AH230	ANALÓGICO	NO
ERICSSON	AH237	ANALÓGICO	NO
ERICSSON	AH238	ANALÓGICO	NO
ERICSSON	AH300	ANALÓGICO	NO
ERICSSON	AH310	ANALÓGICO	NO
ERICSSON	AH320	ANALÓGICO	NO
ERICSSON	AH600	ANALÓGICO	SÍ
ERICSSON	AH618	ANALÓGICO	SÍ
ERICSSON	AH620	ANALÓGICO	SÍ
ERICSSON	AH628	ANALÓGICO	SÍ
ERICSSON	AH630	ANALÓGICO	SÍ
ERICSSON	AH97	ANALÓGICO	NO
GENERAL ELECTRIC	CT500	ANALÓGICO	NO
GENERAL ELECTRIC	CT550	ANALÓGICO	NO
GENERAL ELECTRIC	CT700	ANALÓGICO	NO
GENERAL ELECTRIC	CT750	ANALÓGICO	NO
GENERAL ELECTRIC	CT800	ANALÓGICO	NO
ERICSSON	DF338	ANALÓGICO/DIGITAL	SÍ
ERICSSON	DF338vi	ANALÓGICO/DIGITAL	SÍ
ERICSSON	DF688	ANALÓGICO/DIGITAL	SÍ
ERICSSON	DH318	ANALÓGICO/DIGITAL	SÍ
ERICSSON	DH318vi	ANALÓGICO/DIGITAL	SÍ
ERICSSON	DH336	ANALÓGICO/DIGITAL	SÍ
ERICSSON	DH338	ANALÓGICO/DIGITAL	SÍ
ERICSSON	DH343	ANALÓGICO/DIGITAL	SÍ
ERICSSON	DH353	ANALÓGICO/DIGITAL	SÍ
ERICSSON	DH368	ANALÓGICO/DIGITAL	SÍ

ERICSSON	DH368vi	ANALÓGICO/DIGITAL	SÍ
ERICSSON	DH618	ANALÓGICO/DIGITAL	SÍ
ERICSSON	DH668	ANALÓGICO/DIGITAL	SÍ
GENERAL ELECTRIC	DT3325	ANALÓGICO/DIGITAL	SÍ
GENERAL ELECTRIC	DT3500	ANALÓGICO/DIGITAL	SÍ
ERICSSON	KF688	ANALÓGICO/DIGITAL	SÍ
ERICSSON	KF788	ANALÓGICO/DIGITAL	SÍ
ERICSSON	KH618	ANALÓGICO/DIGITAL	SÍ
ERICSSON	KH668	ANALÓGICO/DIGITAL	SÍ
ERICSSON	PD328	ANALÓGICO/DIGITAL	SÍ
ERICSSON	PD398	ANALÓGICO/DIGITAL	SÍ

ANEXO B

ARQUITECTURA DE UN SISTEMA DE AUTENTICACIÓN PARA UN PROVEEDOR ESPECIFICO (SYNACOM)

Basados en la aceptación de este sistema a nivel, mundial la mayoría de proveedores de este servicio han adoptado un esquema general en la arquitectura de red para adaptarse a los distintos mercados en que puede desarrollarse, por esta razón a manera de ejemplo se muestra una breve descripción de cada uno de los elementos que pueden participar en la formación de un sistema de autenticación. Para el caso específico se presenta el Sistema de Prevención Antifraude que suministra *Synacom Corporation*.

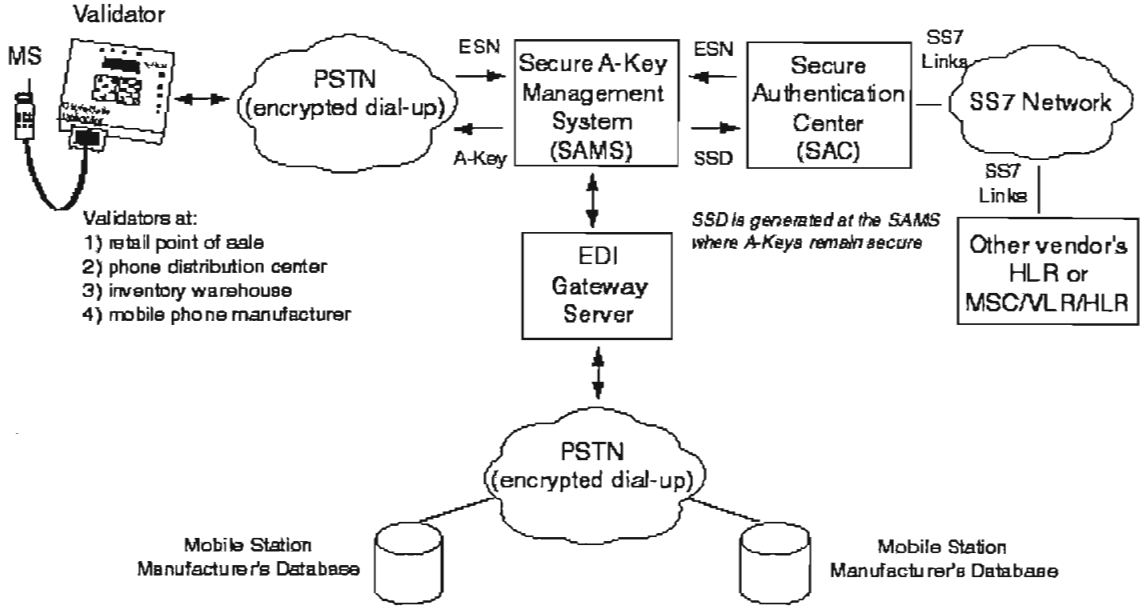


Figura B.1 Interconexión de los principales elementos que permiten el mejor desempeño de Autenticación

Elemento de validación

Es la interface entre el Sistema de Administración de Seguridades Clave A (SAMS) y la estación móvil, el validador distribuye claves A sin revelarlos a las personas, una situación consistente con la primera ley de seguridad: La Clave A debe ser manejada por un número mínimo de personas; ninguna es mejor.

Este elemento también puede ser configurado para automáticamente programar la mayoría de los parámetros del servicio de activación NAM, entre ellos cuentan el MIN, el sistema ID, etc., disminuyendo el tiempo que toma en activar un nuevo suscriptor y eliminando errores que pueden ocurrir cuando los parámetros son programados manualmente.

Figura B.2 Equipo de Validación

La interface de usuario del validador consiste de un display LCD y dos teclados para el ingreso de datos administrativos. Los teclados permiten al usuario interactuar con el equipo durante los procesos de programación. El validador tiene dos interfaces físicas:

- Un módem interno para conectarse con el SAMS.
- Un Pórtico DB-25 para conectarse con los teléfonos móviles.

El validador provee las siguientes funciones básicas en la programación de las claves A:

- El validador lee y comunica al SAMS el identificador único del teléfono. El SAMS le responde con la Clave A y otros datos, la cual es luego programada en el teléfono por el validador.
- Los datos de marcado, ID guardados, y datos del agente, son todos almacenados en el validador para auxiliar en casos en que la programación del teléfono móvil lo necesite. Los datos guardados en el validador están protegidos por contraseñas de seguridad multinivel.

Sistema de administración de seguridades clave A (SAMS)

El SAMS es una caja de herramientas que provee una variedad de utilidades para la manipulación de Claves A. Este es un sistema versátil y flexible, diseñado para reunir las distintas necesidades de los Ejecutivos y métodos de operación para portadoras individuales.

SAMS ofrece las siguientes características y funciones, las cuales permiten fácil integración en un sistema ya existente:

- El AC puede estar solo o integrado con un HLR o con un *switch*.
- Las claves A son generadas y guardadas en el SAMS, o preprogramadas. Las claves A pueden ser obtenidas aún usando Intercambio de Datos Electrónicos (EDI) para las portadoras con una base instalada capaz de autentificar estaciones móviles (en operación o en inventario).
- El SAMS transfiere las claves A directamente al AC o através del Sistema de Aprovisionamiento de la Portadora.
- Generación del SSD por el Centro Seguro de Autenticación (SAC)
- Interface para los sistemas de aprovisionamiento para la distribución de la Clave A y del MIN.

- Interface de Usuario Gráfica (GUI).
- Reportes y loggs

Los siguientes requerimientos de hardware y software son indispensables:

- Usa un sistema de computadoras *Sun Microsystem* el cual soporta una plataforma o un Sistema de Operación *Sun Solaris* UNIX y el Sistema de Manejo de Base de Datos Oracle.
- Plataforma *Enterprise* 2 y *Enterprise* 3500 para aplicaciones más grandes y con el propósito de ofrecer mayor soporte en situaciones de fallas.

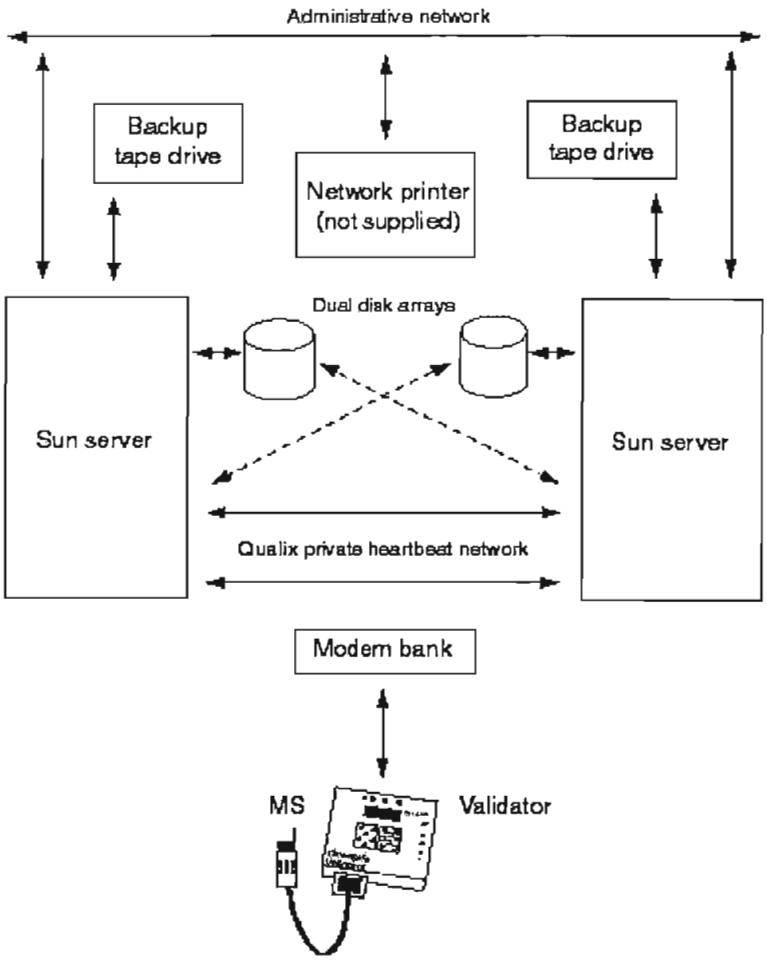


Figura B.3 Esquematización del hardware del sistema SAMS

Centro seguro de autenticación (SAC)

SAC provee el Centro de Autenticación funcionalmente para sistemas de telefonía móvil celular y para sistemas PCS. Los procesos de autenticación se realizan en tiempo- real y pueden soportar sistemas AMPS, D-AMPS, TDMA y CDMA. El SAC interactúa tanto con el SAMS como con el validador para crear una efectiva solución de autenticación terminal a terminal en toda la red.

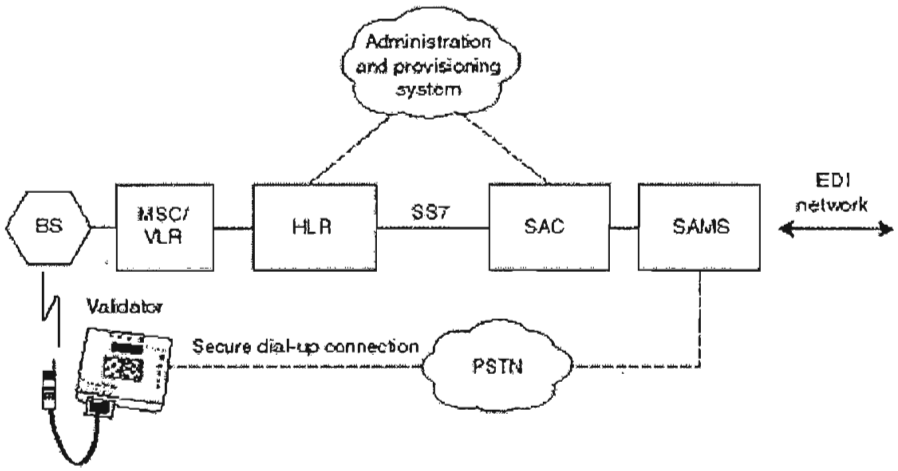


Figura B.4 Interconexión del SAC-SAMS-Validador para formar un eficaz sistema de Autenticación

El SAC posee las siguientes características:

- Procedimientos estándares de autenticación.
- Sistema de Administración de Clave A de Roaming (RKMS).
- Configuración de las políticas de autenticación.
- Interface de Usuario Gráfico.
- Control de Acceso del Usuario, impresión y configuración del software, respaldos, restauración y recuperación.
- Documentación y cursos de enseñanza.

- Utiliza un sistema AlphaCompaq *Server* como plataforma de hardware, utiliza una configuración escalable, de sistema abierto y un alto desempeño en un precio razonable.
- Sistema de Operación Digital UNIX.
- Sistema de Administración de Base de Datos Oracle.

Interoperabilidad entre redes GSM y redes IS-41

Para eliminar los problemas presentados por la incompatibilidad de estándares, el sistema RoamFree provee esta solución, al interconectar redes GSM con las basadas en estándares AMPS, D-AMPS, TDMA, y CDMA. La familia RoamFree consiste de dos sistemas:

- RoamFree Gateway 100 para portadoras GSM que desean suministrar servicio de roaming en sistemas IS-41, IS-91y IS-136.
- RoamFree Gateway 200 para portadoras que desean proveer servicio de roaming en sistemas GSM.

RoamFree Gateway 100

RoamFree Gateway 100 implementa soluciones de conversión de protocolos, mapeo de la base de datos, y administración de todas las funciones soportadas entre las redes como un todo o separadas como se muestra en la figura.

RoamFree Gateway aparece como el HLR para la red IS-41 sirviendo al suscriptor de roaming, y como VLR para servir a la red GSM local del suscriptor.

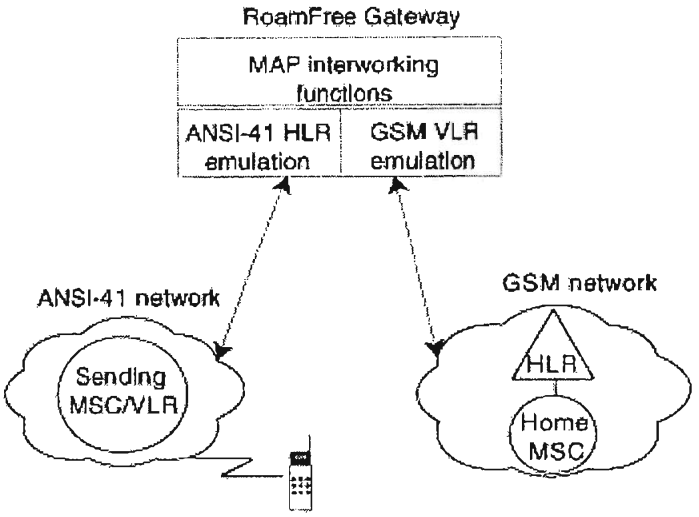


Figura B.5 RoamFree Gateway 100

Para reunir las necesidades especiales de GSM para el mercado IS-41, el RKMS ahora soporta la red GSM y la integra en la plataforma del SAC.

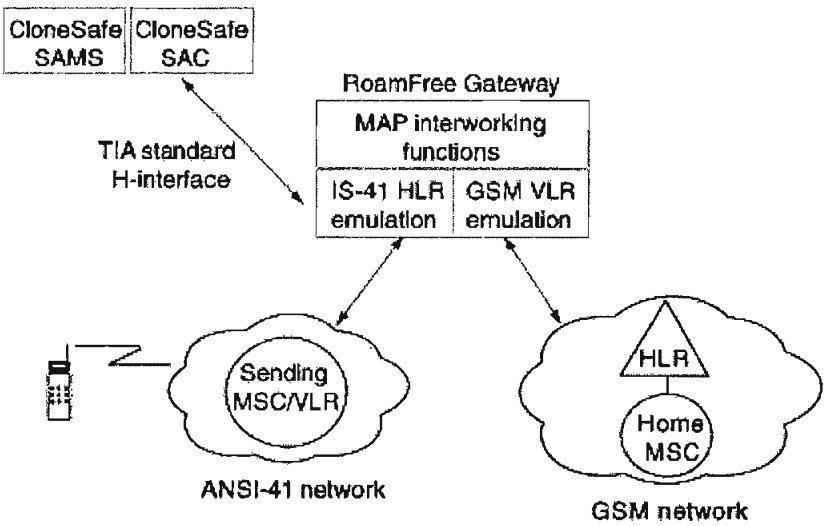


Figura B.6 RoamFree Gateway-SAC para crear una solución de interworking y autenticación

RoamFree Gateway 200

RoamFree Gateway 200 implementa soluciones de conversión de protocolos, mapeo de la base de datos, y administración de todas las funciones soportadas entre las redes como un todo o separadas como se muestra en la figura.

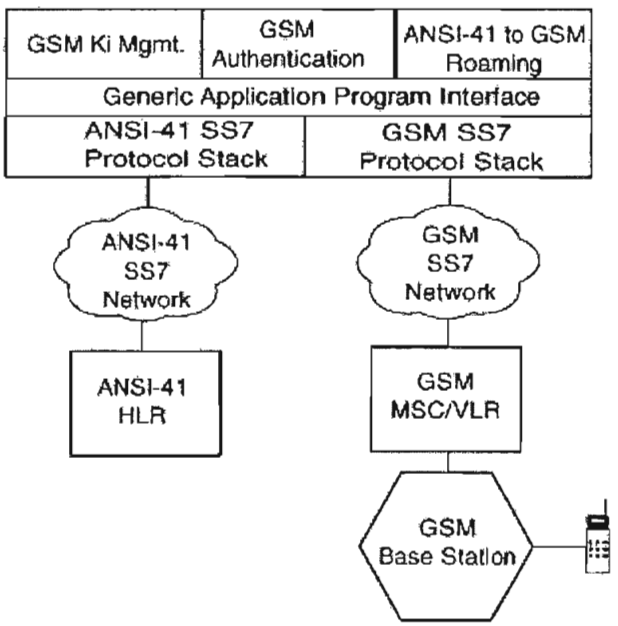


Figura B.7 RoamFree Gateway 200

RoamFree Gateway aparece como HLR para la red GSM sirviendo al suscriptor de roaming y como el VLR para la red local IS-41 del suscriptor. RoamFree Gateway 200 consolida el estándar GSM de autenticación sobre la plataforma RoamFree Gateway. Las funciones del AC RoamFree Gateway son invocadas en el HLR cuando el VLR requiere autenticación para un suscriptor.

GLOSARIO

A

Acceso fraudulento: Cualquier uso no autorizado de servicios inalámbricos de una manera intencionada o no intencionada, manipulación o programando los números ESN/MIN de un teléfono inalámbrico.

Activación de un teléfono celular: La activación es un proceso que se realiza en presencia de cada cliente, ya que una vez incluida toda la información en la base de datos de la central celular, el usuario efectúa inmediatamente una llamada que da por habilitado su teléfono. Para que la comunicación telefónica se lleve a cabo, el cliente debe visualizar en su aparato la señal de reconocimiento proveniente de la estación celular base.

Activación de teléfonos fantasmas (*ghosting*): O servicios no tasados en la red sin autorización.

Activación de voz: Una característica que permite a un suscriptor marcar un número telefónico por comandos hablados.

Administración de fraude: Es una de esas expresiones que intenta colocar la mejor faceta sobre una situación mala. Engloba un ciclo completo de actividades que pretenden reducir las actividades fraudulentas dentro de una operadora inalámbrica.

AMPS (*Advanced Mobile Phone System*): Sistema de Telefonía Móvil Avanzado, el estándar celular analógico, adoptado primero en los Estados Unidos y después en más de 55 países.

ANSI (*American National Standars Institute*): Instituto Nacional de Estandarización Norte Americano.

Área de Cobertura: Extensión territorial atendida por las señales de una estación base. Coincide con el área de una celda.

Área de registro: Región en la que el celular fue registrado.

Área de servicio: Área en la que la estación móvil tiene acceso al servicio móvil celular originando o recibiendo llamadas, inclusive a la red pública de telefonía.

Autenticación: Una tecnología de prevención de fraude que toma un número de valores, incluyendo un identificador del teléfono de 26 caracteres o clave A, no se envía a través del aire para crear un valor secreto compartido usado para verificar la autenticidad de un usuario.

B

Banda doble: Describe un teléfono que trabaja sobre las frecuencias de 800 MHz celular y 1900 MHz PCS.

Biométrica: Tecnología basada sobre un sistema que verifica la identidad de una persona a través del sensado de su huella digital por medio de sensores ópticos que exploran tridimensionalmente las características de ella, tales como, ondulaciones de la piel, crestas y valles; para crear un único patrón el cual está sosegado dentro de una plantilla en una base de datos.

C

CDR (*call detail record*): Registro de datos de tasación. Es una clave indispensable en los sistemas de análisis de una red. Los CDRs contienen información acerca de una llamada específica o intento de llamada, números telefónicos marcados, duración de llamadas (mantenimiento y tiempo de conversación) para cursar una llamada o para desconectarla.

Canal de control: Un canal lógico que lleva la información de la red como voz ó mensajes de datos y los transmite sobre la red.

Canal: Dos frecuencias de radio, la una usada para enviar y la otra para recibir.

CAVE (*Cellular authentication and voice encryption*): Algoritmo definido por la IS-54B (TR45.3). Un algoritmo criptográfico que es usado para generar datos que se intercambian entre la red y el teléfono celular.

CDMA (*Code Division Multiple Access*): Acceso Múltiple por División de Código. Tecnología de la interface aire de espectro disperso usada en algunos teléfonos celulares digitales, servicios de comunicación personal y otras redes inalámbricas.

Cdma2000: Tecnología inalámbrica de tercera generación, propuesta sometida a la Unión Internacional de Telecomunicaciones, el cual está basado en el estándar cdmaone o IS-95.

Cdmaone: Estándar CDMA IS-95 desarrollada por Qualcomm Inc.; una palabra ideada por el grupo de desarrollo CDMA.

Celda sectorizada: El proceso de crear más cobertura y capacidad en un área geográfica haciendo que más de una celda cubra la misma área que la celda originalmente lo hacía. Cada celda cubre un área más pequeña, con menos potencia, y así ofrece la capacidad de reutilización de frecuencias más veces en un área de cobertura geográfica más grande como una ciudad o una metrópoli.

Celda: Un área geográfica dentro del sistema inalámbrico que es cubierta por la señal enviada y recibida por el equipo transmisor y receptor localizado dentro de esa área. Típicamente referida como un sitio de celda, estás son representadas por formas hexagonales cuando los ingenieros planifican sistemas. Esas formas fueron al inicio derivadas de los panales de las abejas, dentro de la cual cada unidad básica está referida como una celda.

Celular prepago: Un sistema que permite a los suscriptores ingresar a un servicio inalámbrico avanzado. El prepago es generalmente usado para clientes de crédito perjudicado ó a esos quienes desean adherirse a un presupuesto.

Celular: Nombre dado al concepto original de dividir un área geográfica grande en áreas de cobertura más pequeña llamadas celdas. Cada celda mantiene las llamadas sobre diferentes canales y se comunica con la unidad central de proceso, llamada conmutador, para facilitar las transferencias de llamadas desde una celda a otra cuando un usuario se traslada a través del sistema.

Centro de autenticación: Una base de datos protegida que almacena y procesa claves secretas requeridas para autenticar teléfonos inalámbricos.

Clave A: Un número secreto emitido para un teléfono celular que es usado junto con la información de datos secretos compartidos de un suscriptor para autenticación.

Clon: Un teléfono inalámbrico programado con números de identificación del móvil o electrónico serial robados o duplicados.

Codificación: Función realizada por un dispositivo que convierte señales analógicas a códigos digitales, tal que cualquier conjunto de datos se puede alterar siguiendo las reglas de dicho código. La función opuesta se denomina decodificación, en la cual los códigos digitales se convierten a señales analógicas.

Colisión de llamadas: Este evento describe la ocurrencia de dos llamadas del mismo móvil (dos móviles con el mismo número) en localidades separadas ampliamente dentro de un período de tiempo que hace imposible este suceso.

Controlador de estación base: La parte de la infraestructura del sistema inalámbrico que controla una o múltiples señales de radio del sitio de celda, así reduce la carga sobre el conmutador. Esto puede ser visto como una forma de procesamiento distribuido.

Correo de voz (*voice mail*): (También llamada mensajería de voz). Un servicio de respuesta computarizada, que responde una llamada, manifiesta un salido y graba un mensaje.

Costo-eficiencia: Este término tiene implicaciones acerca del costo de las herramientas usadas en la operación y mantenimiento de un sistema, por ejemplo, el costo de contratar y formar las destrezas técnicas del personal como también el costo de mantenimiento y actualizaciones de *software* para el monitoreo de cierto equipo con la finalidad de obtener ganancias.

Cracker: Argot para alguien quien rompe código encriptados ó circuitería de una computadora.

CTIA (*Cellular Telecommunications Industry Association*): Asociación de Industrias de Telecomunicaciones Celulares, un grupo de empresas de representación celular, PCS y portadoras de radio móvil especializadas.

D

Demanda única: Un intento especial de autenticación inicialmente usada por el AC como resultado de un intento previo que falló o una indicación que la estación móvil es posiblemente fraudulenta (o alguna otra anormalidad).

D-AMPS (*digital AMPS*): Usado por *Ericsson Inc.* Para describir la tecnología de acceso por división de tiempo IS-136.

Dispersión espectral: Técnica utilizada sobre el acceso múltiple por división de código (CDMA), el cual establece que no hay restricciones de tiempo o de ancho de banda en las transmisiones. Por ejemplo, cada transmisor de estación terrena puede transmitir, cada vez que lo desea, y puede utilizar cualquier ancho de banda o todos los anchos de banda asignados a un sistema o canal de satélite en particular. Debido a que no hay limitaciones en el ancho de banda, al CDMA a veces se le conoce como acceso múltiple del espectro disperso; las transmisiones se pueden extender por todo el ancho de la banda designado.

DSP (*digital signal processor*): Un microprocesador especializado que desempeña operaciones matemáticas sobre una corriente de datos en tiempo real para producir una segunda corriente de datos (modificada).

E

Encripción: El proceso de aleatorizar un mensaje tal como la señal de un teléfono digital para prevenirlo de ser leído por personas no autorizadas.

Escuchas a escondidas (*eavesdropping*): Intervención de llamadas telefónicas provenientes de una red fija ó móvil por parte de perpetradores, con el propósito de obtener información confidencial del propio sistema como también del usuario.

ESN (*electronic serial number*): Número serial electrónico. El número de identificación único empotrado en un teléfono inalámbrico por el fabricante. Cada vez que una llamada es fijada, el ESN es automáticamente transmitido a la estación base tal que el centro de conmutación móvil de la operadora inalámbrica puede chequear la validez de la llamada.

Espectro disperso (*spread spectrum*): Esta tecnología de transmisión de radio, dispersa la información sobre un gran ancho de banda que es necesario para reducir significativamente el nivel de interferencia en el sistema e incrementar su capacidad.

Estación base transmisora (BTS): La porción de la infraestructura del sistema inalámbrico que es responsable de enviar y recibir las señales de radio sobre las ondas de aire. Este dispositivo toma las señales de radio de los teléfonos de los suscriptores y las envía sobre líneas telefónicas dedicadas o señales de microondas hacia el conmutador.

F

FCC (*Federal Communications Commission*): Comisión Federal de Comunicaciones. La agencia federal responsable de la administración reservada y comercial del espectro.

Fraude de teléfonos robados: El uso no autorizado de un teléfono robado de un cliente legítimo antes de que él reporte el robo.

Fraude tecnológico: Deshonestidad de personas que causan pérdidas económicas mediante la obtención y uso de productos o servicios con el intento de evadir pagos o mensualidades dentro de una operadora inalámbrica.

Full-Duplex: Término de radio aplicado a transmisiones tales como llamadas telefónicas que permiten hablar y escuchar al mismo tiempo usando dos frecuencias para crear un canal. Cada frecuencia es usada separadamente, es decir una para transmitir y otra para recibir.

G

Generación aleatoria de ESNs (*tumbling*): El proceso de cambiar el ESN en un teléfono cada vez que una llamada telefónica es hecha, así le permite al usuario hacer llamadas y tener cargados ilegalmente los números de alguien más.

GSM (*global system for mobile communications*): Sistema global para comunicaciones móviles. Un celular digital o una red PCS usada en todas partes del mundo.

GUI (*graphical user interface*): Un término de computación referido a un sistema de operación ó ambiente que despliega opciones sobre una pantalla, como símbolos gráficos, íconos o fotografías.

H

Hackers: Una persona o grupo de personas que ganan acceso a seguridades de una red de computadoras por placer o desafío, algunas veces para robar información o para sabotear el sistema.

HLR (*home location register*): Registro de ubicación local. Una base de datos que reside dentro de una red inalámbrica local que chequea la identidad de un suscriptor local.

Huella digital madura: Una huella digital de radio frecuencia es madura por lo menos cuando se haya validado 10 veces, por este método una huella alcanza cierta definición requerida para hacer decisiones de desconexión de llamadas.

Huella digital de radio frecuencia: Un proceso que identifica un teléfono celular por medio de una huella digital única que caracteriza estas señales de transmisión. La huella digital de radio frecuencia es un proceso usado para prevenir el fraude por clonación, ya que un teléfono clonado no tendrá la misma huella digital de un teléfono legal con los mismos números de identificación electrónicos.

I

IMSI (*internacional mobile suscriber identity*): Es una cadena de cifras decimales, hasta un máximo de 15 cifras, que identifica internacionalmente un solo terminal o abonado del servicio móvil.

IMT-2000: El nombre de la Unión Internacional de Telecomunicaciones para el estándar global de la tercera generación para telecomunicaciones móviles.

Ingreso asegurado: Una empresa básica, la cual puede tener sustancial impacto sobre el desempeño de la empresa es ingreso o ganancia asegurada.

Interface aire: El estándar de operación de un sistema de una red inalámbrica; tecnologías que la incluyen: AMPS, TDMA, CDMA y GSM.

Interferencia de canal adyacente: Señal perjudicial a una frecuencia debido a la presencia de otra señal en una frecuencia cercana.

Interoperabilidad: La capacidad de una red para operar con otras redes, tal como dos redes basadas sobre diferentes protocolos o tecnologías.

IS (*Interim Estándar*): Una designación del Instituto Nacional de Estandarización Norte Americano, usualmente seguido por un número que refiere a un protocolo aceptado por la industria; por ejemplo, IS-95, IS-136, IS-41,etc.

IS-41: El estándar de red que permite a todos los MSCs intercambiar información de los suscriptores.

ITU (*International Telecommunicatios Union*): Unión Internacional de Telecomunicaciones. Una agencia de las Naciones Unidas, sede en Ginebra que promueve los desarrollos de los servicios de telecomunicaciones a nivel mundial y la distribución intercontinental del espectro para futuros usos.

L

Lista negra: Esta denota las llamadas de quien la suscripción a la red ha sido negada por alguna razón (posiblemente por participar en uno de los esquemas de fraude listados en esta tesis.

M

MIN (*mobile identification number*): Número de identificación móvil. Únicamente identifica una unidad móvil dentro de una operadora de una red inalámbrica. El MIN a menudo puede ser marcado desde otras redes, alámbricas o inalámbricas.

Modo doble: Describe un teléfono que trabaja sobre redes analógicas y digitales.

Móvil, o teléfono de automóvil: Un tipo de teléfono celular que está permanentemente instalado en un automóvil o en uno más pesado. Estos transmiten a tres watts de potencia, funcionan con la batería del vehículo y usan una antena externa.

MSC (*mobile switching center*): Centro de conmutación móvil. El intermediario electrónico entre los sitios de celda y la red telefónica pública conmutada, procesa el tráfico de acá para allá.

N

NAM (*number assigment module*): La NAM es la memoria electrónica en el teléfono celular que almacena el número de identificación móvil y el número electrónico serial y otros más.

O

Operaciones de venta de llamadas: Estos servicios de reventa sin licencia son instalados para proveer comunicaciones internacionales fraudulentas, combinando teléfonos fraudulentos con números de tarjetas de larga distancia robadas, el revendedor puede ofrecer una llamada a bajo costo a personas quienes desean contactar a sus familiares, amigos, negocios en cualquier parte del mundo.

Originación: El proceso por el cual un suscriptor móvil inicia una llamada accediendo al MSC por medio de la marcación de dígitos.

P

PCS (*personal communications services*): Servicios de comunicaciones personal. Uno de dos vías, opera en la banda de los 1900 MHz proyectado como la segunda generación de celulares.

Perfil de usuario: El proceso de compilar la información de uso de un suscriptor (tal como frecuencia de llamadas, localización de llamadas a o desde y usos de tiempo aire mensualmente), típicamente para identificar el uso fraudulento o para identificar usuarios que probablemente terminen el servicio.

PIN (*personal identification number*): Número de identificación personal. Un código usado por un número telefónico móvil junto con una tarjeta SIM para completar una llamada.

Portable: Un teléfono más liviano que entra en un bolsillo o bolsa y posee una potencia de transmisión de 0.6 watts suministrada por una batería recargable de poco tamaño y peso.

Portadora A: Compañía celular no alámbrica (inalámbrica).

Portadora B: Compañía celular alámbrica.

R

Reconocimiento de voz: La capacidad de teléfonos celulares, PCs y otros dispositivos de comunicaciones para ser activados o controlados mediante comandos de voz.

Red visitada: Red que presta servicio a un usuario cuando éste transita fuera de la red propia.

Registración: El proceso por el cual un suscriptor móvil hece su localización conocida para el MSC y, subsecuentemente para el HLR, habilitando la originación o terminación de una llamada.

Reutilización de frecuencia: La capacidad de la asignación de canales específicos a una celda básica para ser usados nuevamente en otra celda, cuando hay la suficiente distancia entre las dos a fin de prevenir la interferencia co-canal que afecta a la calidad de servicio. Esta técnica asegura a un sistema celular incrementar capacidad con un número limitado de canales.

Roaming automático: Es el que utiliza los servicios de un sistema celular que emplea los protocolos de la parte de usuario de telefonía móvil patentada de Ericsson o la norma provisoria IS-41 de la TIA. Estos protocolos facilitan la señalización entre centrales hasta el punto en que los servicios de comunicaciones están uniformemente disponibles a través de la red, prescindiendo del tipo de central que presta los servicios o de la localización física del abonado.

Roaming manual: Es el que ingresa desde otro sistema que no forma parte de la red de roaming automático.

S

Seguridad celular: Actividad que permite minimizar pérdidas de fraude y previene el uso ilícito de una red tan rápido como sea posible.

Servicio de movilidad: Servicio de telecomunicación de admite la movilidad para terminales o usuarios mediante el acceso desde y hacia la red pública a través de una red propia y/o red(es) visitada(s).

Servicio de suscripción fraudulenta: Una característica disponible en el HLR, por el cual el estado de una unidad suscrita puede ser marcada como fraudulenta en la base de datos del HLR. El servicio para un suscriptor marcado como fraudulento puede ser denegado o limitado de algunas maneras. El sistema puede fijar este estado como resultado de una operación de autenticación o puede ser fijado manualmente por el operador.

Servidor de aplicación en tiempo real (RTAS): Es instalado y operado en un sitio dentro de la edificación de la operadora. Contiene una base de datos de la información completa de la información de todos los eventos, la cual permite un número de reportes estandarizados para ser generados en tiempo real

SID (*system identification number*): Número de identificación del sistema: Un número único asignado a cualquier operador inalámbrico, que es luego programado en los teléfonos que los suscriptores compran para recibir servicio.

SIM (*subscriber identity mobile*): Identidad del suscriptor móvil. Sinónimo con la tarjeta inteligente.

Sistema Central de Control (SCC): Recibe los datos de huellas digitales diariamente de las RFUs a la cual está enlazado y usa estos datos para actualizar la base de datos *master* SCC.

Sitio de celda: El espacio donde las antenas y equipos de comunicaciones de red están localizados.

SS7 (*signaling system 7*): Una señalización de alta velocidad en la columna vertebral de una red de telefonía pública conmutada.

T

Tarjeta inteligente: Una tarjeta de plástico que contiene datos importantes acerca de la identidad de una persona que le permite acceso a una red. También contiene información del suscriptor, a menudo insertada dentro de teléfonos GSM para vagar sobre diferentes países.

TDMA (*time division multiple access*): Una tecnología de interface aire digital usada en celulares, PCS y redes móviles de radio mejoradas.

Teléfonos clones falsificados: Con el ESN clonado, el criminal no pretende ser un vagante fuera de la ciudad mas bien un usuario legítimo. Con este tipo de fraude, el criminal coloca dentro de un teléfono un chip que puede ser programado con los números MIN/ESN del usuario legítimo. El criminal obtiene combinaciones de números válidos a través del uso de equipos de prueba usados ilegalmente ó a través de un empleo inescrupuloso de un agente que vende al por menor u operador.

Teléfonos tumbler falsificados: Este tipo de fraude alteraría un teléfono inalámbrico tal que este generaría una serie de números ESNs y hace a la persona que está hablando ser un nuevo cliente cada vez que una llamada es realizada. Esta técnica se realiza por sustitución de la NAM, un componente electrónico en el teléfono inalámbrico que empareja el ESN con el MIN.

Tercera generación (3G): Un nuevo estándar que promete ofrecer incremento de capacidad y aplicaciones de datos de alta velocidad sobre los 2 Mbps. Este también integrará tecnología pico, micro y macro celular y permitirá roaming global.

Terminal móvil (*handset*): Cualquier terminal portátil, transportable o manual que admite servicios de movilidad.

TIA (*Telecommunications Industry Assotiation*): Asociación de Industrias de Telecomunicaciones. Grupo comercial que representa a fabricantes y suministradores de productos de comunicaciones y tecnologías de información.

Tiempo aire: Tiempo que se gasta por el uso de un teléfono celular.

Tono doble multi frecuencia (DTMF): Los sonidos hechos por el teclado de un teléfono cuando los botones son presionados. Cada botón emite un sonido que es la combinación específica de dos de ellos con el propósito de minimizar la posibilidad de recibir una señal no deseada por el equipo, cuando este intenta originar una llamada.

Transferencia de llamada (handoff): El proceso que ocurre cuando una red inalámbrica automáticamente conmuta una llamada de un móvil a un sitio de celda adyacente.

Trasportable: Un teléfono móvil estándar de 3 watts que puede ser retirado de un automóvil y usado con un paquete de baterías adjunto. Aunque técnicamente portable, el transportable no debe ser confundido con el de mano, una pieza de teléfono inalámbrico.

Tumbler: Teléfono al que se le programa para que genere aleatoriamente números ESNs con el propósito de obtener combinaciones de tales números con sus respectivos MINs previamente obtenidos de las ondas de aire o por robo de teléfonos celulares.

U

Unidades de radio frecuencia (RFUs): Son instaladas en las estaciones de radio base de la operadora. Las RFUs monitorean el canal de control en el sentido de regreso y extraen los datos de las huellas digitales únicas emitidas de cada móvil dentro del área de cobertura en la cual ellas están instaladas.

Usuario de servicio móvil: Usuario que se abona a un servicio de movilidad para acceder al mismo.

UWC-136: Un estándar inalámbrico de tercera generación basado en tecnología TDMA que fue desarrollado por el Consorcio Universal de Comunicaciones Inalámbricas y es uno de los candidatos 3G sometido a la ITU por los Estados Unidos.

UWCC (*Universal Wireless Communications Consortium*): Consorcio Universal de Comunicaciones Inalámbricas. Un grupo de industrias que soportan el estándar IS-136 y tecnología de redes inalámbricas inteligentes IS-41.

V

Vagando (*roaming*): Viajando a las afueras del área local de la operadora.

VLR (*visitor location register*): Registro de ubicaciones del visitante. Una base de datos de la red, que hospeda información acerca de usuarios bajo roaming.

W

W-CDMA (*wideband code division multiply access*): Acceso múltiple por división de código de banda ancha. El estándar de tercera generación ofrecido a la ITU por parte de propulsores GSM.