ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

ESTUDIO DE LA FACTIBILIDAD DE LA CONEXIÓN DE DOS EQUIPOS DE RADIOGONIOMETRÍA PARA LA DETERMINACIÓN DE UNA SEÑAL DE TELEFONÍA MÓVIL CELULAR TECNOLOGÍA GSM

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

PAULINA ADRIANA MORILLO ALCÍVAR
pymo2504@gmail.com

DIRECTOR: MSc. MIGUEL HINOJOSA
mhinojosar@yahoo.com

Quito, Marzo 2011

DECLARACIÓN

Yo Paulina Adriana Morillo Alcívar declaro bajo juramento 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.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____

Paulina Adriana Morillo Alcívar

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Paulina Adriana Morillo Alcívar, bajo mi supervisión.

_____

MSc. Miguel Hinojosa
DIRECTOR DEL PROYECTO

DEDICATORIA

A mi madre Elizabeth quien ha sido el mejor ejemplo de lucha, constancia y trabajo así como el impulso para no rendirme y llevar a buen fin todo lo que emprendo,

A mi padre Fernando quien inculcó en mí, la convicción de que no hay mejor herencia para los hijos que la educación,

A mi novio Diego, quien ha sido un verdadero amigo y me ha orientado siempre a ser la mejor,

Y por último a mis hermanas y hermanos, motivo por el cual me esfuerzo cada día para que con este pequeño ejemplo no se rindan y siempre luchen por lograr sus objetivos, con todo mi amor para ell@s: Estefanía, Julieth, Ma. Fernanda, Patricia, Diego, Abel y Daniela.

AGRADECIMIENTO

En primer lugar quiero agradecer a Dios, por haber puesto en mi corazón el valor de realizar todas las cosas con AMOR, valor que me ha llevado a superar los obstáculos para poder culminar con éxito mis estudios universitarios.

Quiero agradecer también a mi familia por ser el pilar fundamental en todos los proyectos que he emprendido en la vida.

A mis maestros que han dado un aporte importante en mi formación no solo como profesional sino también como ser humano.

A mi novio quien ha sido el compañero y amigo en los buenos y malos momentos.

Y para terminar a mis amigos y compañeros de trabajo que han influenciado positivamente cada iniciativa para la realización de este proyecto.

Cabe mencionar que he preferido no escribir los nombres de todos a quienes tengo una profunda gratitud, ya que considero que cada persona que he conocido a lo largo de mi vida ha aportado un granito de arena para llegar a ser lo que ahora soy, por esta razón al no poder agradecerles de forma directa a través de un papel, elevo una oración a Dios por cada uno de ellos para que Él sepa reconocer cada obra de sus manos.

ÍNDICE DE CONTENIDOS

CAPÍTULO 3

ESTUDIO DE LA FACTIBILIDAD DEL USO DEL SISTEMA DE RADIOGOIOMETRÍA, PARA DETECCIÓN DE SEÑALES DE TELEFONÍA MOVIL CELULAR

CAPÍTULO 4

PRUEBAS REALIZADAS, Y RESULTADOS

ANEXOS:

ANEXO A.- Manual de Usuario de los Equipos de Radiogoniometría ALMOS 3000 (Operación Directa)

ANEXO B.- Manual de Usuario de los Equipos de Radiogoniometría ALMOS 3000 (Operación Remota)

ANEXO C.- Data sheet programa de emulador de puertos virtuales VSPE

ANEXO D.- Procedimientos para la instalación de los módems 3.5G modelo ZTE y configuración de la VPN asignada para pruebas.

ANEXO E.- Configuración de Puertos Virtuales a través de software VSPE.

ANEXO F.- Manual de Ensamblaje y Mantenimiento de los Equipos de Radiogoniometría ALMOS 3000.

ANEXO G.- Trazas independientes de las pruebas realizadas en Ferroviaria.

ÍNDICE DE FIGURAS

CAPÍTULO 1

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

ÍNDICE DE TABLAS

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

RESUMEN

El desarrollo de la tecnología trae consigo además de notorios beneficios, una serie de nuevas formas de fraude, uno de estos y la más perjudicial para el estado en términos económicos es el By-pass telefónico o Sistemas de telefonía internacional no autorizados.

Anteriormente cuando los sistemas By-pass eran implementados a través de líneas de telefonía fija combatir este tipo de fraude era un poco más sencillo, pues si bien se necesitaban de una serie de análisis e investigaciones, el sistema dejaba rastros que permitían encontrarlo, es decir con solo rastrear la línea detectada y seguir el par de cobre se podía encontrar la instalación.

Sin embargo el desarrollo de la telefonía móvil ha traído consigo nuevas implementaciones de los sistemas de By-pass telefónico, que son mucho más complicadas de detectar, y requieren un análisis investigativo bastante amplio. La dificultad recae en el hecho de que no hay huella que seguir, el rastro que deja el dispositivo móvil en una celda podría darnos un área de algunos kilómetros, lo que nos impide tener precisión en la detección de la ubicación de la instalación.

Al ser la radiogoniometría una de las técnicas más antiguas para la detección de señales electromagnéticas, se ha analizado la posibilidad de crear un sistema que permita utilizar equipos de radiogoniometría para ubicar los sistemas de By-pass.

Esta solución podría funcionar de forma directa y eficaz siempre y cuando la frecuencia se mantenga fija, pero como los sistemas implementados a través de líneas móviles celulares utilizan actualmente la tecnología GSM, se dificulta su utilización, puesto que la tecnología de salto de frecuencia no mantiene portadoras en frecuencias fijas.

Por tal motivo se presentan, describen y analizan la factibilidad de dos posibles soluciones para poder aplicar un sistema de radiogoniometría en la detección de este tipo de instalaciones.

PRESENTACIÓN

Con desarrollo y avance de la tecnología, es necesario crear herramientas que permitan combatir de forma efectiva a los fraudes que se cometen en el sector de las Telecomunicaciones, el presente proyecto denominado: Estudio de la Factibilidad de la Conexión de dos Equipos de radiogoniometría para la determinación de una Señal de Telefonía Móvil Celular tecnología GSM, pretende analizar y presentar posibles soluciones para contrarrestar el fraude por sistemas de telefonía internacional no autorizados. El desarrollo de este proyecto se presenta en cinco capítulos, como se explica a continuación:

En el Capítulo 1 se presenta una breve descripción de los conceptos y definiciones de radiogoniometría, y se describe la funcionalidad de los equipos de radiogoniometría ALMOS 3000, utilizados en el presente proyecto.

En el Capítulo 2 se describe como se realizó la conexión de los equipos de radiogoniometría ALMOS 3000, además de analiza e investiga herramientas de hardware y software que permitieron la integración del sistema.

En el Capítulo 3, se estudia la factibilidad de dos posibles soluciones, para utilizar el sistema de radiogoniometría en la detección de señales de telefonía móvil celular. Para esto se realiza un análisis de la tecnología GSM, puesto que es la base para desarrollar la herramienta que permita mitigar este tipo de fraude.

En el Capítulo 4, se presentan los resultados de las pruebas realizadas con el sistema en la detección de señales en la banda de UHF y pruebas en las que se ha utilizado el sistema para la detección de señales de telefonía móvil celular.

En el Capítulo 5 se plantean conclusiones y recomendaciones desarrolladas y obtenidas a lo largo del proceso investigativo y de análisis del presente proyecto.
Por último se provee una serie de documentos técnicos como anexos, con información adicional que fortalece la comprensión de algunos temas desarrollados en el proyecto.

CAPÍTULO 1

MARCO TEÓRICO

1.1 INTRODUCCIÓN

Las ondas de radio desde su aparición han sido un medio de comunicación muy explotado y se han convertido en un aliado importante en temas de localización y orientación. Desde la búsqueda de transmisores clandestinos, el rastreo de radiobalizas de salvamento o la localización de fuentes de interferencia. Hasta el posicionamiento por GPS (sistema de posicionamiento global) o incluso en radioastronomía con estrellas pulsantes a modo de faros espaciales. Este hecho ha contribuido al desarrollo de métodos de detección de señales, aplicando razonamientos sencillos, fáciles de entender y usar.[1]

1.2 RADIOGONIOMETRÍA

1.2.1 DEFINICIÓN

Del latín radius (rayo, radio) y del griego gonía (ángulo) y metría (medida), significa la medida de ángulos por radio. La Unión Internacional de las Telecomunicaciones, en su Reglamento de Radiocomunicaciones, la define como "radiodeterminación que utiliza la recepción de ondas radioeléctricas para determinar la dirección de una estación o de un objeto" [2]

La radiogoniometría es una ciencia que permite determinar la dirección en que se reciben las señales del emisor que se tenga sintonizado. Actualmente, el radiogoniómetro ha pasado a ser una rama de una técnica más amplia: la Radiodeterminación, definida según el citado Reglamento como "la determinación

[1] FUENTE: http://www.qsl.net/eb1hbk/taller/radiogonio.html
[2] FUENTE: http://www.canalsocial.net/GER/

de una posición u obtención de información relativa a una posición mediante las propiedades de propagación de las ondas radioeléctricas". Según se aplique o no para fines de navegación, la radiodeterminación recibe el nombre de Radionavegación o Radiolocalización.

1.2.2 MÉTODO DE TRIANGULACIÓN

La triangulación es una forma de determinar la ubicación de algo usando la ubicación de otras cosas. En geometría, es el uso de triángulos para determinar posiciones de puntos, medidas de distancias o áreas de figuras. Esta definición se aplica regularmente en la localización y ubicación de puntos remotos.

1.2.2.1 Triangulación de una Señal

Este método se utiliza para localizar o rastrear en un lugar una antena de radio desde donde se origina, por ejemplo, una transmisión clandestina.

Para esto sólo será necesario desplazarse con el radiogoniómetro y determinar desde dos o tres posiciones diferentes la dirección de procedencia de la señal y a continuación trasladarla a una carta o mapa de una ciudad o un descampado. El punto donde se cortan las líneas que se trazan en el mapa será el lugar exacto desde el cual se origina la transmisión. En la actualidad existen receptores, que contienen el software necesario para procesar toda la información y realizar la triangulación directamente.

1.3 RADIOGONIÓMETRO

1.3.1 DEFINICIÓN

El radiogoniómetro es un receptor especial, que permite determinar la dirección y sentido con que llega la emisión de un transmisor distante, lo cual implica la medida del ángulo formado por el círculo máximo terrestre que pasa por

transmisor y receptor con una dirección de referencia, generalmente el norte magnético (N) o el eje popa-proa de una nave.

En las estaciones radiogoniométricas de tierra la referencia suele ser el N, y el ángulo medido es, por tanto, el azimut. En los radiogoniómetros de avión o barco, el origen de ángulos, llamados marcaciones, es el eje popa proa. El azimut es por tanto la suma de la marcación más el rumbo, existen radiogoniómetros cuyo círculo indicador, recorrido por una aguja o puntero, tiene dos escalas concéntricas de 0 a 360°; sobre una fija se leen las marcaciones, mientras la otra, movida por un repetidor de la aguja (giroscópica o giro magnética), proporciona el azimut del emisor a cuya frecuencia se sintonice el radiogoniómetro.

A diferencia de un receptor regular de radio, un receptor radiogoniométrico, con el equipo asociado, indica la dirección aproximada a lo largo de una línea imaginaria en la que se encuentra un transmisor distante. Aún cuando la información que se obtenga por la radiogoniometría puede que no sea siempre lo suficientemente exacta, puede determinar la dirección de un transmisor distante, en la mayoría de los casos, a una exactitud en el orden de más o menos 2 grados.

Una posición radiogoniométrica puede determinar tan solo la dirección aproximada de un transmisor distante. No obstante, por medio del uso de dos sitios radiogoniométricos se puede encontrar la ubicación aproximada de una antena transmisora. Mediante el uso de dos o tres sitios de radiogoniometría, se puede encontrar una posición fija.

El equipo de radiogoniometría puede funcionar desde cualquier transporte móvil, autos, aviones, helicópteros. Las plataformas transportadas por aire elevan la antena receptora y aumentan las posibilidades de interceptar las señales de radio a mayores distancias. En caso de mucha lluvia o un tiempo demasiado nublado, el resultado podría variar mucho. Por esta razón los sistemas aéreos necesitan de equipo complementario montado en tierra.

1.3.2 PRINCIPIO DE FUNCIONAMIENTO

El radiogoniómetro se basa en una antena directiva que explora el horizonte buscando una cierta señal. La radiogoniometría clásica utiliza antenas de cuadro, que vienen a ser una o varias espiras en un plano, combinadas con sendos dipolos, muchas veces unidos mecánicamente al cuadro.

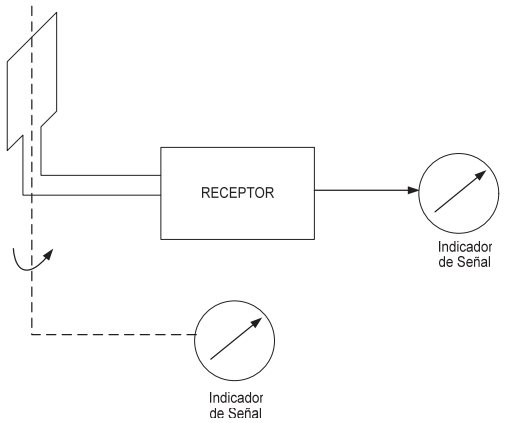


Figura 1.1. Diagrama de Bloques de un radiogoniómetro[3]

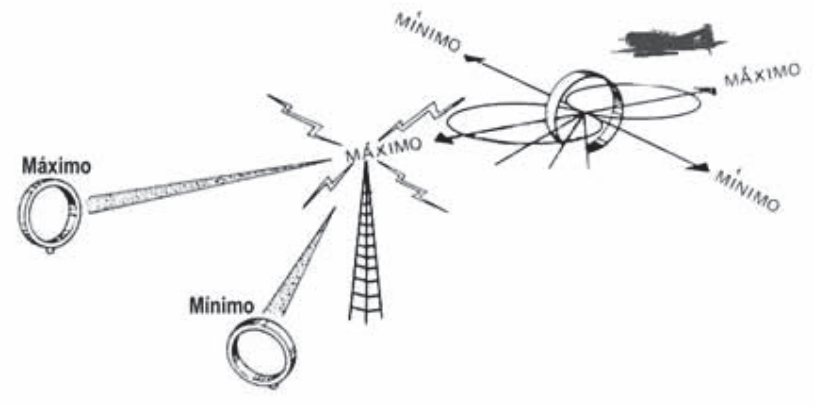


Figura 1.2. Funcionamiento del radiogoniómetro[4]

La combinación de un dipolo y una antena de cuadro producen un diagrama de radiación en forma de cardioide (1+cos θ), que gira al girar el cuadro sobre su eje vertical. Como el nulo del cardiode es abrupto, mientras que su máximo es muy

[3] FUENTE: http://nacc.upc.es/adf/adf.radiogoniometro.html
[4] FUENTE: http://www.exordio.com/1939-1945/civilis/telecom/hf-df.html

suave, la antena se gira hasta que la señal incidente desaparece. En este momento se sabe que ésta proviene de la dirección hacia la que apunta el nulo de la antena.

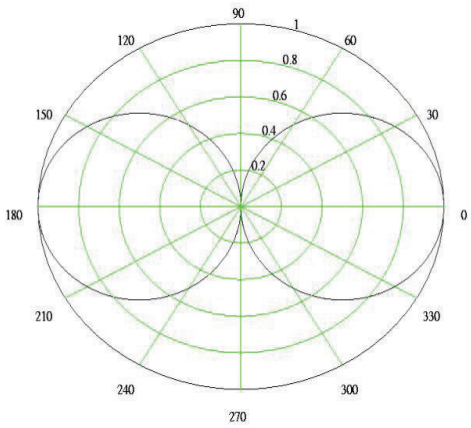


Figura 1.3 Diagrama de Recepción de la Antena de Cuadro[5]

Generalmente, las antenas utilizadas por los Radiogoniómetros son del tipo de cuadro o del tipo circular. La característica de esas antenas hace que las señales se reciban con mayor intensidad cuando uno de los bordes está dirigido hacia la estación transmisora.

Debido a su forma, las antenas reciben con mayor intensidad desde dos direcciones opuestas y para evitar esa ambigüedad se utiliza una segunda antena que en el receptor refuerza las señales en la dirección verdadera. Si bien los puntos de máxima intensidad no son fáciles de determinar, los de mínima si lo son, es decir que una antena bien diseñada es capaz de hacer desaparecer la señal al orientarla de manera apropiada.

Muchos diseños de antena presentan esta propiedad, sin embargo, para establecer con gran precisión la orientación se requiere de técnicas mucho más sofisticadas.

[5] FUENTE: http://nacc.upc.es/adf/adf.radiogoniometro.html

Figura 1.4 Antena típica de Radiogoniómetro[6]

Las técnicas más sofisticadas, tales como matrices por etapas se utilizan generalmente para encontrar con alta precisión la dirección con sistemas llamados goniómetros como se utilizan en la inteligencia de señales.

Los receptores usados en radiogoniometría tienen un instrumento de medición para poder leer la intensidad de la señal, pero un operador experto puede determinar la dirección por medios auditivos. En la práctica, las antenas se rotan alrededor de una escala graduada en 360 grados de azimut, donde el operador lee la dirección relativa de la ubicación de la estación recibida.

1.3.3 TIPOS DE RADIOGONIÓMETRO

1.3.3.1 Radiogoniómetro de cuadro giratorio

Propuesto por A. Blondel (1863-1938) en 1902, utiliza las propiedades directivas de una antena en forma de cuadro. En el caso de polarización normal de la onda recibida (campo eléctrico E vertical, campo magnético H horizontal, vector P de propagación horizontal y perpendicular a E y a H), la tensión captada por el cuadro es máxima cuando su plano coincide con P, y se anula con el cuadro perpendicular a la dirección de propagación. El diagrama ofrece, así, una forma bicircular o de 8. En la versión más sencilla, el cuadro, conectado a un receptor

[6] FUENTE: http://www.exordio.com/1939-1945/civilis/telecom/hf-df.html

con auriculares, se gira a mano hasta dejar de escuchar la emisión, cuya marcación aparecerá entonces en un limbo graduado, cuya aguja gira con el cuadro. La lectura así obtenida tiene una ambigüedad de 180°. Para resolverla, es decir, para determinar el sentido, se acciona un conmutador que asocia al cuadro una antena vertical, de forma que su señal anule un máximo del 8 y duplique el otro. El 8 queda transformado en una cardiode, cuyo nulo da la dirección y sentido del emisor. Por ser este nulo menos agudo y preciso que los nulos del 8, sólo se usa el cardiode para el sentido.

1.3.3.2 Radiogoniómetro de cuadros fijos

Desarrollado por E. Bellini (1876-1943) y Tosi en 1907, tiene dos cuadros fijos verticales, cruzados ortogonalmente, cuyas salidas se conectan a sendas bobinas fijas, también ortogonales, que rodean a una bobina giratoria exploradora. La salida de esta bobina, conectada al receptor, obedece al mismo diagrama en 8 que un cuadro giratorio. El conjunto de bobinas, convenientemente apantallado, recibe el nombre de goniómetro. En VHF y UHF, en vez de bobinas, se usan armaduras de condensador formando un goniómetro capacitivo, en vez del inductivo constituido por las bobinas. En ambos casos, el acoplamiento con una antena vertical, realizado con la debida relación de amplitudes y fases, proporciona el diagrama en cardiode determinador del sentido. El sistema Bellini-Tosí elimina las dificultades de mover, desde el local del receptor, un cuadro exterior. Estas dificultades son más apreciables en los radiogoniómetros de onda media, cuyos cuadros son necesariamente grandes.[7]

Cuando la onda recibida no está polarizada normalmente los cuadros producen un error debido a la captación por sus lados horizontales; el diagrama sigue siendo en 8, pero los nulos ya no coinciden con la dirección del emisor. El efecto de noche, producido por interferencia del rayo reflejado en la ionosfera con el rayo directo, así como el efecto aeroplano, motivado por inclinación de viraje o de gran altitud, consisten en errores por recepción de ondas polarizadas anormalmente.

[7] FUENTE: J.A. Biyd, D.B. Harris, D.D. King & H.W. Welch, Jr. Electronic Countermeasures," Direction Finding". 1979 Los Altos, CA: Peninsula Publishing. ISBN 0-932146-00-7.

No debe confundirse el mencionado efecto avión con el debido a la distorsión del campo electromagnético por reflexiones en el fuselaje. Para suprimir estos efectos, Adcock patentó un sistema en Inglaterra (1919), consistente en suprimir los lados horizontales del cuadro, que queda reducido a dos antenas verticales conectadas en su punto medio (antenas en H de VHF y UHF) o en su base (antena en U). Las conexiones deben blindarse.

1.3.3.3 Radiogoniómetro con un solo canal

Se refiere a la utilización de una matriz multi-antena con un solo receptor de canal de radio. Este enfoque del DF*, obviamente ofrece algunas ventajas y desventajas. Ya que sólo utiliza un receptor, la movilidad y menor consumo de energía ofrece claras ventajas, pero sin la capacidad de mirar a cada antena simultáneamente (lo que sería el caso si hubiera que utilizar varios receptores) para las operaciones más complejas tienen que ocurrir en la antena con el fin de presentar la señal al receptor.

1.3.3.4 Radiogoniómetro de exploración azimutal

La bobina central del radiogoniómetro de Bellini y Tossi gira con velocidad constante. Esto modula en doble banda lateral la señal incidente, estando su dirección de incidencia codificada en la fase. Un comparador de fase entre la señal de doble banda lateral (DBL) detectada y la frecuencia de giro de la antena produce la indicación de dirección.[8]

1.3.3.5 Radiogoniómetro de Watson - Watt

Dispone tres canales idénticos: uno para el dipolo y los otros para dos cuadros perpendiculares. Los canales producen una señal detectada que se aplica a un tubo de rayos catódicos, de la siguiente forma: los canales de las bobinas se conectan a las placas de deflexión, una bobina a las horizontales y la otra a las

---

[8] FUENTE: ROUTLEDGE y KEGAN Paul, Marine Electronic Navigation, 2da Edición.
* DF: son las siglas en ingles de Direction Finder que significa Radiogoniómetro

verticales. Esto produce, ante una señal incidente, una traza en la pantalla de consola de rastreo del radar TRC (Tracker Radar Console) orientada en la dirección de incidencia de la señal. El canal del dipolo se conecta al eje Z, de modo que borra media traza, dejando solamente la parte que apunta al emisor de la señal.[9]

1.3.3.6 Radiogoniómetro Doppler

Se basa en una antena omnidireccional que gira sobre una circunferencia horizontal. La señal incidente aparece modulada en frecuencia por el efecto Doppler, por tanto la dirección de incidencia aparece codificada en la fase de la señal modulada.

Si un elemento de antena gira (círculo de radio R), la señal recibida con una frecuencia ω_o es modulada en frecuencia con la frecuencia de rotación ω_r de la antena debido al efecto Doopler:

Si la fuente se mueve hacia la fuente de radiación, la frecuencia aumenta; si la antena se aleja de la fuente de radiación, la frecuencia recibida se reduce.

De la amplitud instantánea U(t):

$$U(t) = \text{acos}\,(\omega_0 t + \frac{2\pi R}{\lambda_0}\cos(\omega_0 t - \alpha) + \phi)$$

Se deriva la frecuencia instantánea ω(t):

$$\omega(t) = \frac{d\phi(t)}{dt} = \omega_0 - \frac{2\pi R}{\lambda_0}\omega_r \text{sen}(\omega_r t - \alpha)$$

Luego de filtrar la componente DC de ω_0, la señal Doppler demodulada S_D se obtiene como:

$$S_D = \frac{2\pi R}{\lambda_0}\omega_r \text{sen}(\omega_r t - \alpha)$$

La fase de la señal demodulada, comparada con la referencia S_r

$$S_r = -sin\omega_r t$$

Igual a la frecuencia central, derivada de la rotación de la antena, permite obtener el rumbo α que se está buscando.

[9] FUENTE: KEEN R, Wireless Direction Finding, 8va. Edición, 1947, Iliffe, Londres

La rotación mecánica de un elemento de antena es la práctica no es posible ni recomendable. Varios elementos (dipolos, monopolos, lazos cruzados) se ponen en un círculo y se escanean con la ayuda de conmutadores electrónicos.

Para obtener resultados con el radiogoniómetro sin ambigüedades, el espaciamiento entre los elementos de antena individuales debe ser más pequeño que media longitud de onda λ de operación; en la práctica una distancia de alrededor de la tercera parte de la mínima λ de operación puede seleccionarse.
Si esta regla es agregada a las antenas de los radiogoniómetros Doppler, es posible tener cualquier tamaño de apertura que permita:

- Alta inmunidad a la recepción multitrayectoria.
- Alta sensibilidad que puede ser implementada de manera sencilla.

Una desventaja del Método Doppler es el tiempo requerido, ya que para poder obtener el rumbo es necesario que se de al menos un ciclo de escaneo. Con una frecuencia de rotación del orden de los 170 Hz en las bandas de VHF/UHF un ciclo toma alrededor de 6ms.

El radiogoniómetro con el método de Doppler por tanto obtiene la línea de rumbo basado en la fase de la señal recibida, además considera la medida de la variación de la fase, efecto Doppler inducido en la señal, por la conmutación del arreglo de antenas. La fase de la señal a la salida del detector de cruce cero es directamente proporcional al ángulo de la dirección del arribo de la señal.

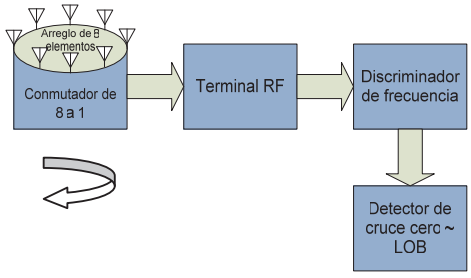


Figura 1.5 Diagrama de bloques del Radiogoniómetro con el método de Doppler[10]

[10] FUENTE: http://www.exordio.com/1939-1945/civilis/telecom/hf-df.html

1.3.3.7 Radiogoniómetros automáticos

Un ADF* es un instrumento marino o aéreo de radionavegación, es un instrumento de navegación automático y continuo, que muestra la posición relativa de la nave o aeronave a una estación de radio adecuada. Los receptores ADF son normalmente sintonizados a las bases de aviación o balizas no direccionales NDB (Non-Directional Beacon) marinos que operan en la banda LW entre 190 a 535 kHz. [11]

1.4 APLICACIONES DE LA RADIOGONIOMETRÍA EN LA DETERMINACIÓN DE LA UBICACIÓN DE SISTEMAS DE COMUNICACIONES

1.4.1 APORTE EN LA NAVEGACIÓN Y AVIACIÓN

El radiogoniómetro se usa como ayuda a la navegación aérea y marítima, en un inicio se utilizaban estaciones terrestres desde las cuales se informaba al piloto su marcación, esto resultaba un proceso muy lento para velocidad actual de los aviones, por lo que el empleo del radiogoniómetro de tierra en aviación quedó relegado a ciertos aeropuertos que, en las bandas de VHF o UHF, lo utilizan en el control de aproximación o como auxiliar del radar en la identificación de aviones.

Por el contrario, el radiogoniómetro a bordo permite al piloto tomar sus marcaciones propias de emisores cuya situación conoce, que pueden ser especiales para radionavegación (radiofaros) o comunes de radiodifusión, disponiendo así de una valiosa ayuda en zonas no cubiertas por otros sistemas de radionavegación. Sobre todos se emplea el radiogoniómetro automático, llamado radiocompás, que permite seguir rutas jalonadas por radiofaros no direccionales de onda media o aproximarse a aeropuertos.[12]

---

[11] FUENTE: http://nacc.upc.es/adf/index.html
*ADF: son las siglas en inglés del Radiogoniómetro Automático (Automatic Direction Finder)

[12] FUENTE: ROUTLEDGE y KEGAN Paul, Marine Electronic Navigation, 2da. Edición, pág. 68–69.

1.4.2 BÚSQUEDA DE TRANSMISORES CLANDESTINOS

Uno de los mayores usos, durante la guerra fue para el espionaje y contraespionaje entre países enemigos, pues a través de radiogoniómetros podían detectar emisiones enemigas y contraatacar, en la actualidad el uso de radiogoniometría para buscar emisiones clandestinas se sigue dando especialmente en entidades gubernamentales para controlar tanto a estaciones autorizadas como no autorizadas, monitoreando en ambos casos su ubicación.

1.4.3 SEGUIMIENTO DE VIDA SILVESTRE

La ubicación de radio-etiquetado de animales mediante la triangulación es una técnica de investigación aplicada ampliamente para estudiar el movimiento de los animales. La técnica fue utilizada por primera vez en la década de 1960, cuando la tecnología utilizada en los transmisores de radio y las baterías se hicieron lo suficientemente pequeñas como para insertarse en los animales salvajes, y ahora es ampliamente desplegada para una variedad de estudios de la fauna silvestre.

La mayoría del rastreo de animales salvajes que se han colocado con los equipos de radio transmisor se lleva a cabo por un investigador de campo con una dirección de radio específica que permita encontrar el dispositivo. Cuando el investigador quiere localizar a un animal en particular, la ubicación de los animales puede ser triangulada por la determinación de la dirección de transmisores de varias localidades.

1.4.4 RECONOCIMIENTO

Matrices graduales y otras técnicas avanzadas de antena son utilizadas para rastrear los lanzamientos de los sistemas de cohetes y sus trayectorias resultantes. Estos sistemas pueden ser utilizados para fines de defensa y también para obtener información de inteligencia sobre el funcionamiento de los misiles

pertenecientes a otras naciones. Estas mismas técnicas se utilizan para la detección y el seguimiento de los aviones convencionales.

1.4.5 DEPORTE

Actividades auspiciadas por grupos y organizaciones que involucran el uso de las habilidades para encontrar la dirección de radio, para localizar los transmisores en lugares desconocidos han sido populares desde el final de la Segunda Guerra Mundial. Muchos de estos eventos fueron promovidos con el fin de la práctica de la utilización de técnicas de dirección de radio para encontrar respuesta a los desastres y los propósitos de defensa civil, o para practicar la localización de la fuente de interferencia de radio frecuencia. La forma más popular de este deporte, en todo el mundo, es conocida como "la caza del transmisor", o "la caza del zorro" tiene lugar en un área geográfica más grande, como el área metropolitana de una gran ciudad, y la mayoría de los participantes viajan en vehículos de motor mientras tratan de localizar uno o más transmisores de radio con el fin de encontrar nuevas y efectivas técnicas de localización.

1.5 DESCRIPCIÓN DE LOS RADIOGONIÓMETROS ALMOS 3000

El radiogoniómetro ALMOS 3000 está basado en el radiogoniómetro de Doopler y permite el establecimiento de la dirección desde la cual se recibe una señal transmitida.

Esta dirección puede referirse a un transmisor de radio u otras formas de comunicación inalámbrica.

Al combinar la información de dos o más receptores de radiogoniometría, ubicado en diferentes sitios, la fuente de transmisión puede ser localizada en el espacio mediante un proceso de triangulación, a esto se conoce como el cruce de líneas de rumbo “croos-cut” o fijación del punto de transmisión “fix”.

Las unidades automáticas de búsqueda de rumbo en el radiogoniómetro ALMOS 3000 permite la detección, el monitoreo y la localización de fuentes transmisoras de radio en el rango VHF y UHF desde 20 Hz a 3000MHz.

Donde es aplicable los radiogoniómetro barre las frecuencia en un modo de detección. La información del rumbo o línea de rumbo LOB (Line off bearing) debe ser capturada, a pesar de tratarse de pulsos de pequeña duración.

El LOB obtenido a través del ALMOS 3000 tiene una precisión de 1.5° RMS (máx 2.5°), cubriendo un rango completo de 0 a 360°.

1.5.1 DESCRIPCIÓN DEL HARDWARE

El DFSR-3000 con antena procesadora de señal SDP-3000 utiliza la técnica de Doppler para medir y mostrar la dirección relativa entre las antenas y la fuente de transmisión de radio.

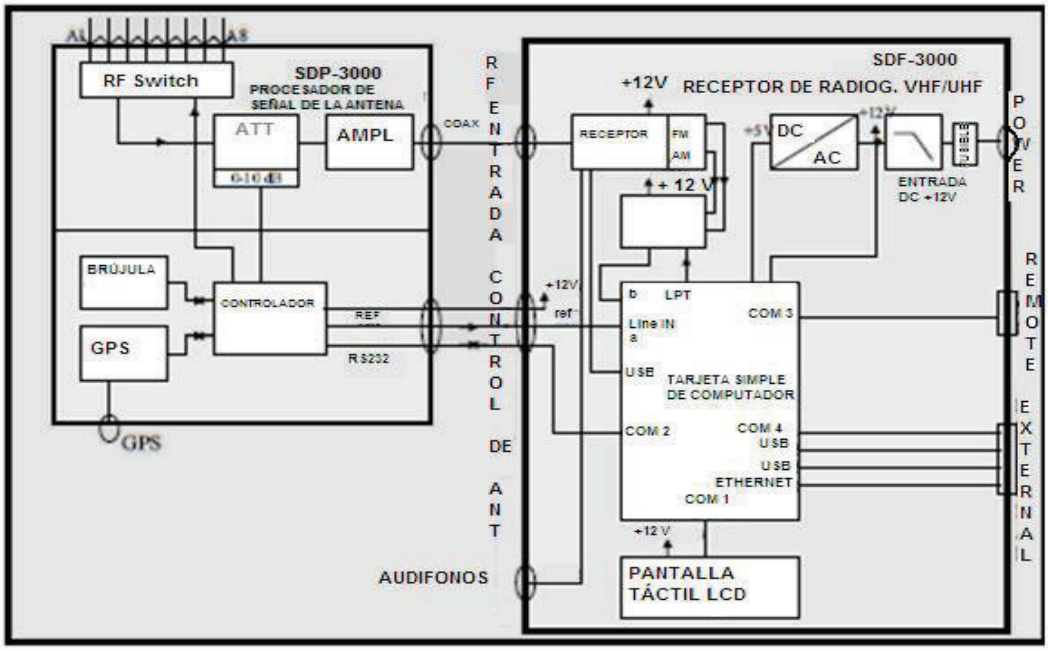


Figura 1.6 Diagrama de bloques del Equipo Antena[13]

[13] FUENTE: http://www.exordio.com/1939-1945/civilis/telecom/hf-df.html

1.5.1.1 Partes del Equipo de Radiogoniometría

El Equipo de Radiogoniometría consta de los siguientes elementos:

- Receptor DF VHF/UHF DFSR-3000, Cable de control.
- Un procesador de Señal antena SDP-3000, cable coaxial de Radiofrecuencia.
- 8 brazos de antena VHF de 35 cm con 16 Elementos de extensión de antena VHF de 29 cm.
- 8 antenas dipolo UHF.
- Antena de GPS.
- Fuente de alimentación, cable de alimentación.

1.5.1.1.1 Antena con procesador de señal SDP-3000

La antena con procesador de señal SDP-3000 contiene los elementos del equipo de radiogoniometría para encontrar las funciones del DFSR-3000. Los ocho conectores tipo N para la conexión mecánica y eléctrica de los brazos de la antena están ubicadas a los lados de la cabeza de la antena. Estas son las entradas del conmutador de RF. El conector de control y de alimentación, el conector de salida de RF (TNC), conector de entrada a la antena GPS (SMA) y en el acondicionamiento mecánico para la fijación de la antena de la cabeza en el mástil se encuentran en la parte inferior de la cabeza de la antena. La cabeza de la antena contiene dos placas de circuito impreso (PCB).

El panel de RF es un multiplexor de alta frecuencia que cambia las señales de entrada de antena a la señales RF de salida, periódicamente. El multiplexado de la señal de RF va a la entrada de un amplificador de bajo ruido (LNA low noise amplifier) a través de un atenuador. La atenuación de 0 a 10 dB es seleccionable desde la pantalla táctil LCD de la DFSR-3000. La salida del LNA alimenta la entrada del receptor a través de un cable coaxial de diez metros. La unidad de navegación es un PCB dentro de la cabeza del DF, que tiene varias tareas una de ellas es el proceso de localización de la dirección. La unidad contiene los módulos

individuales para propósitos especiales, por ejemplo la determinación de correcciones de posición GPS y la orientación magnética de la cabeza.[14]

La comunicación entre estos módulos y la unidad principal del procesador de rumbo se resuelve con dos microcontroladores independientes, que son responsables de la adquisición de datos desde el GPS, y del módulo de brújula para la conmutación de la antena.

Los módulos se pueden comunicar entre sí a través de un bus SPI (interfaz periférico serial) y se puede controlar la una a la otra (como un acuerdo de master-esclavo) con comandos externos. La unidad de navegación recibe la tensión de alimentación de CC (corriente continua) de 12 V de la principal unidad de DF (DFSR-3000), a través del cable de control. El suministro se alimenta a través de un filtro para eliminar ruido y alguna señal de corriente alterna no deseada de las líneas de alimentación. El cable de control también contiene las dos señales RS232 para el microcontrolador y las comunicaciones con la unidad principal. El rango de frecuencias del equipo de radiogoniometría, depende del rango de operación de la cabeza, la longitud de los brazos de la antena y la longitud de las antenas dipolo en los brazos.

- La antena, configurada con intervalo de 80 cm de base, los brazos y los dipolos UHF_DIP_V40 en posición vertical opera en la banda de frecuencias 100-450 MHz.

- La antena, con el intervalo de 42 cm de base, con los brazos y con los dipolos de VHF_DIP_V40 en posición vertical opera en rango de frecuencia de 350-1200 MHz.

[14] FUENTE: Manual de Radiogoniómetro ALMOS 3000, Montaje e instalación ; pág. 10

1.5.1.1.2 Receptor DF VHF/UHF DFSR-3000

Figura 1.7 Parte Frontal del Equipo de Radiogoniometría ALMOS 3000[15]

La señal de alta frecuencia multiplexada de la unidad principal de la antena, alimenta la entrada del receptor incorporado en el SDF-3000. El receptor realiza una demodulación FM. El receptor es controlado a través de un puerto USB del ordenador de una sola placa (SBC) que también figuran en DFSR-3000. La señal de referencia proviene del SDP-3000 y va a una entrada de audio " a " del SBC. La señal desmodulada FM va a la entrada de un filtro de banda base, de ancho de banda angosto. La salida del filtro de banda base se alimenta a la entrada " b" del SBC. Un programa se ejecuta en el SBC realizando el proceso de la transformada rápida de fourier (TRF) y evaluando el rumbo.

En la parte frontal del DFSR-3000 están el conector de los audífonos y la pantalla LCD con el panel táctil para ingresar los datos. La configuración de los parámetros del equipo y sus funcionalidades, se presentan en el Anexo A.

1.5.2 DESCRIPCIÓN DEL SOFTWARE DE CONTROL

El radiogoniómetro ALMOS 3000 puede ser usado vía remota a través del software de control remoto el mismo que proporciona una interfaz gráfica de usuario la cual que permite manejar el equipo de forma sencilla.

El esquema del software de control remoto se visualiza en la figura 1.7 siguiente:

[15] FUENTE: Manual de Radiogoniómetro ALMOS 3000, Montaje e instalación ; pág. 1

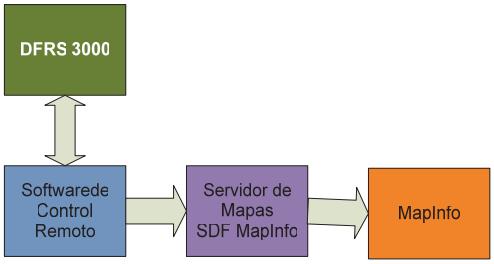


Figura 1.8 Esquema del funcionamiento del software de control remoto[16]

El software de control remoto del equipo de radiogoniometría almos 3000, tiene las mismas opciones del equipo operando en forma directa, y además nos permite visualizar a través de un software de mapas, en este caso el MAP INFO, la ubicación de la medición y las líneas de triangulación, de esta manera podemos procesar los datos con mayor precisión el interfaz entre el software de control remoto y el MAP INFO la realiza un programa propietario denominado SDF MAP INFO. Entre el DFSR-3000 y el software remoto pueden usarse los siguientes modos de transmisión de datos: Serial, TCP/IP, AT Modem, GSM Modem and Radio, para esto es necesario los puertos utilizados en los diferentes tipos de conexión sean correctamente configurados.

La conexión serial a través de la interfaz RS232, es uno de los tipos de conexión más usados.

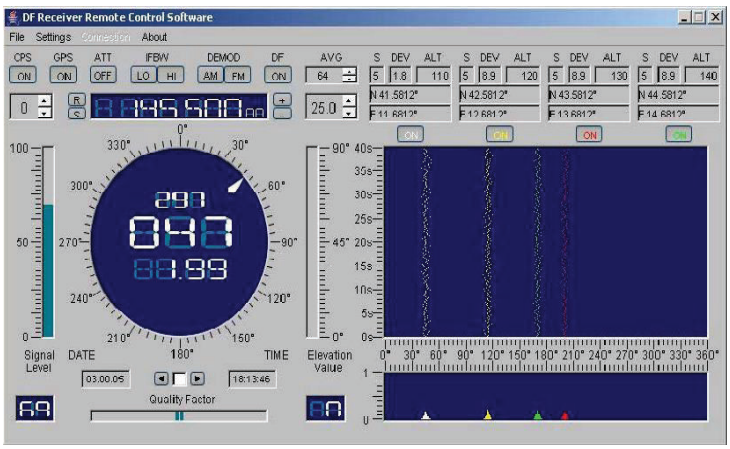


Figura 1.9 Interfaz Gráfica de Usuario del Software de Control Remoto del DF[17]

[16] FUENTE: Manual de Radiogoniómetro ALMOS 3000, Acceso Remoto ; pág. 2
[17] FUENTE: Manual de Radiogoniómetro ALMOS 3000, Acceso Remoto ; pág. 2

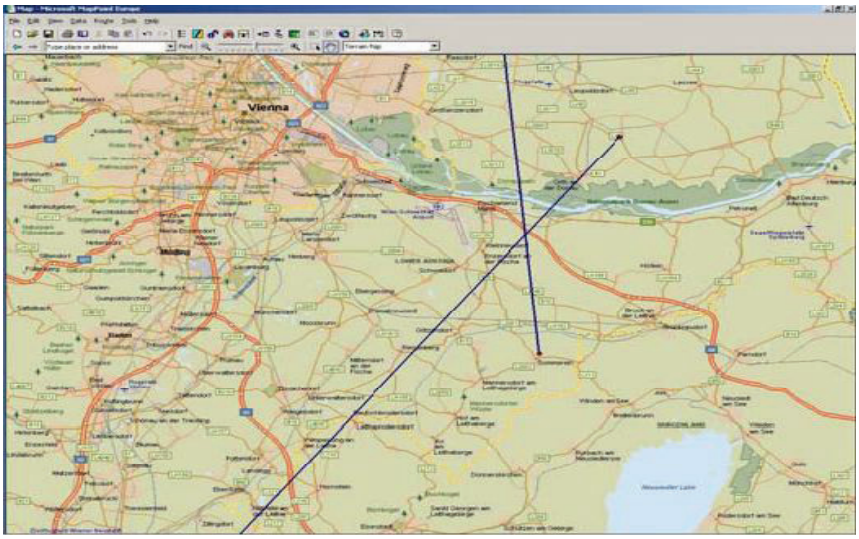


Figura 1.10 Presentación de la triangulación en un Mapa Digital[18]

La descripción de la configuración, opciones y funcionalidades del software de control remoto del DF Almos 3000 se presentan en el Anexo B.

[18] FUENTE: Manual de Radiogoniómetro ALMOS 3000, Acceso Remoto ; pág. 9

CAPÍTULO 2

CONEXIÓN DE DOS EQUIPOS DE RADIOGONIOMETRÍA, PARA DETECCIONES EN TIEMPO REAL

2.1 TECNOLOGÍA GPRS/EDGE

Con los servicios de datos ofrecidos en GSM, se detectaron ciertas carencias que impidieron su despegue sobre la red 2G como: baja velocidad de transmisión (9.6 Kbps),[19] alto tiempo de establecimiento de la conexión, facturación basada en tiempo de conexión, independientemente del tráfico generado.

Bajo estas circunstancias nació la Red GPRS, que se fundamenta en una red de conmutación de paquetes superpuesta a la actual red GSM, que permite las mejoras como: conexión y transporte de alta velocidad, conexión permanente, movilidad, tiempo bajo de establecimiento, número de ranura de tiempo asignados según servicio, facturación basada en cantidad de tráfico transmitido no a tiempo de llamada, calidad de servicio, etc.

Para los operadores, se consigue un mejor aprovechamiento del espectro radioeléctrico, pues el enlace radio, solo se utiliza cuando se están recibiendo o transmitiendo datos. Esto implica que varios usuarios pueden compartir el mismo radiocanal, con el consiguiente aumento de eficiencia, y con un bajo costo en implantación de Red a nivel Radio, es decir ya no es necesario tener un canal dedicado para cada usuario ya que cada canal es compartido por varios usuarios. Se puede recibir voz y datos simultáneamente, la conexión se realiza en el mismo momento que el usuario lo solicita pudiendo ocupar varios canales cuando el flujo de información así lo exija. [20]

---

[19] FUENTE: http://knol.google.com/k/sistema-de-control-via-gprs-y-sms#
[20] FUENTE: http://www2.udec.cl/~eduamoli/gprs.htm

2.1.1 SERVICIO DE RADIO POR PAQUETES (GPRS)

Es una tecnología digital de telefonía móvil la cual proporciona velocidades de transferencia de datos superiores a las generadas por la tecnología GSM. El GPRS es especialmente útil para conectarse a Internet. [21]

2.1.2 EVOLUCIÓN DE GSM CON VELOCIDADES DE TRASMISIÓN MEJORADAS (EDGE)

Es una tecnología de la telefonía celular móvil que actúa como puente entre las redes 2G (segunda generación) y 3G (tercera generación), se considera una evolución de GPRS que tiene como principal fortaleza la aceleración en la transmisión de datos o navegación.

2.2 TECNOLOGÍA UMTS/HSDPA (3.5G)

2.2.1 INTRODUCCIÓN

3G es una abreviatura para tercera-generación de telefonía móvil. Los servicios asociados con la tercera generación proporcionan la posibilidad para transferir tanto voz y datos. Esta evolución vista desde el lado de GSM pasa por GPRS-EDGE, también conocido como 2.5G y caracterizadas por llegar a velocidades de hasta 384Kbps. La evolución inicial a tercera generación también es conocida como UMTS (Sistema Universal de Telefonía Móvil), permite alcanzar velocidades superiores a EDGE de hasta 2 MBps.

Actualmente, la tecnología conocida como HSDPA (Acceso por paquetes de alta velocidad de bajada) está caracterizada por alcanzar velocidades máximas de hasta 14MBps manteniéndose asociados los servicios de voz y datos. En ese sentido, el HSDPA ofrece mejor velocidad en el Downlink (bajada de datos) mas no en el Uplink (subida de datos) que se mantiene en 384Kbps máximo. Cabe aclarar que el concepto UMTS engloba a los conceptos WCDMA (3G) y

[21] FUENTE: http://www.mundov.com/gprs_edge.php

HSDPA/HSUPA (3.5G). Con esta tecnología se pueden desarrollar nuevos servicios de valor agregado a las llamadas o servicios actuales para el beneficio de los usuarios de las operadoras que cuentan con este tipo de tecnologías.

2.2.2 MULTIPLE ACCESO POR DIVISIÓN DE CÓDIGO DE BANDA ANCHA (W-CDMA)

Múltiple acceso por División de código de banda ancha es el sistema de acceso de radio utilizados por los sistemas celulares de tercera generación implementados en diversas partes del mundo, para soportar servicios de banda ancha, como acceso a Internet de alta velocidad, video y transmisión de imágenes de alta calidad con la misma calidad que las redes fijas. [22]

En sistemas de WCDMA la interfaz CDMA se combina con la base de las redes GSM. El estándar de WCDMA fue desarrollado a través del proyecto 3GPP (Asociación de proyectos de tercera Generación) que apunta a garantizar la interoperabilidad entre diferentes redes 3G. El estándar que ha surgido a través de este proyecto de asociación se basa en el Sistema Universal de ETSI de Telecomunicaciones Móviles UMTS y es comúnmente conocida como UTRA Acceso de Radio Terrestre UMTS. El método de acceso para UTRA es de secuencia directa (DS-CDMA). La información se extiende sobre una franja de aproximadamente 5 MHz. Este ancho de banda ha dado lugar al nombre CDMA de ancho de banda o WCDMA.

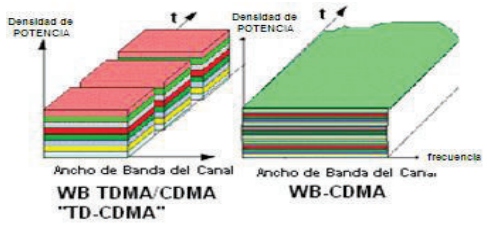


Figura 2.1 Ocupación del Canal[23]

En WCDMA, existen dos modos diferentes de operación posibles: TDD o FDD.

[22] FUENTE: http://www.tech-faq.com/wcdma.html
[23] FUENTE: http://www.umtsworld.com/technology/wcdma.htm

2.2.2.1 Duplexación por división de tiempo (TDD)

Es un método de transmisión duplex, donde el enlace ascendente y descendente se realiza en la misma banda de frecuencia mediante el uso de intervalos de tiempo sincronizados. Por lo tanto intervalos de tiempo en un canal físico se dividen en componentes de transmisión y recepción.

2.2.2.2 Duplexación por división de frecuencia (FDD)

Es un método a doble cara, las transmisiones de enlace ascendente y descendente emplean dos bandas de frecuencia separadas. Un par de bandas de frecuencias con una separación especificada se asigna para la conexión. Desde las diferentes regiones tienen diferentes regímenes de atribución de frecuencias, la capacidad de operar en modo FDD o TDD permite la utilización eficiente del espectro disponible.

2.2.3 ACCESO POR PAQUETES DE ALTA VELOCIDAD DE BAJADA (HSDPA)

HSDPA, Acceso por paquetes de alta velocidad de bajada, es un nuevo protocolo para transmisión de datos de telefonía. Este es conocido como 3.5G esencialmente, el estándar preverá velocidades de bajada en un teléfono móvil equivalente a una línea ADLS (Asymmetric Digital Subscriber Line), eliminando las limitaciones impuestas al uso del teléfono por una conexión lenta. Se trata de una evolución y mejora en W-CDMA.

HSDPA mejora la velocidad de transferencia de datos por un factor de al menos cinco veces más que W-CDMA. HSDPA puede alcanzar velocidades teóricas de transmisión de datos de 10.8 Mbps (megabits por segundo). Uno de los principales servicios es la transmisión de video y archivos de música.

2.2.4 SISTEMA UNIVERSAL DE TELECOMUNICACIONES MÓVILES (UMTS)

UMTS, (Sistema Universal de Telecomunicaciones Móviles), es la evolución lógica de la comunidad GSM a la tercera generación, la transmisión de paquetes basada en texto, voz digitalizada, vídeo y multimedia puede llegar a velocidades de hasta 2 megabits por segundo (Mbps). UMTS ofrece un conjunto consistente de servicios en dispositivos móviles y para los usuarios de teléfonos, sin importar dónde se encuentren en el mundo. UMTS se basa en el Sistema Global para el estándar de comunicaciones móviles (GSM). También es respaldada por los principales organismos de normalización y los fabricantes como el estándar previsto para los usuarios móviles de todo el mundo.

Una vez que UMTS está totalmente disponible, la informática y los usuarios de teléfonos pueden estar constantemente conectados a Internet. Los usuarios tendrán acceso a través de una combinación de las transmisiones inalámbricas terrestre y por satélite. Hasta que UMTS se aplique plenamente, los usuarios pueden utilizar los dispositivos multi-modo que cambiaran a la tecnología actualmente disponibles (tales como el GSM 900 y 1800), donde UMTS no está actualmente disponible[24]

UMTS tiene una estructura jerárquica, es decir, está compuesta por tres tipos de Celdas: Macro Celda, Micro Celda y Pico celda con un mínimo de 5 MHz de ancho de banda por Celda.

2.2.4.1 Macro Celda

Macro Celda tiene radios desde 1km hasta 35km y se destinan para ofrecer cobertura rural y carreteras para vehículos u otros objetos que se mueven a alta velocidad (transmisión de datos de 144kbit/s.).

[24]FUENTE: http://searchmobilecomputing.techtarget.com/definition/UMTS

2.2.4.2 Micro Celda

La Micro Celda tiene radios desde 50km hasta 1km. Ofrece servicio a usuarios fijos o que se muevan lentamente con elevada densidad de tráfico (urbana) con velocidades de 384kbit/s, usando UTRAFDD.

2.2.4.3 Pico Celda

Las Pico Celdas tienen radios hasta 50m. Ofrecen coberturas localizadas en interiores, usando ULTRA-TDD, con velocidades del orden de los 3Mbit/s.[25]

2.3 RED VIRTUAL PRIVADA VPN

Una VPN, es una red privada que se desarrolla, mediante un proceso de encapsulación y en su caso de encriptación, de los paquetes de datos a distintos puntos remotos mediante el uso de la infraestructura de una red pública. Los paquetes de datos de la red privada van de forma segura a través de un "túnel" definido en la red pública.

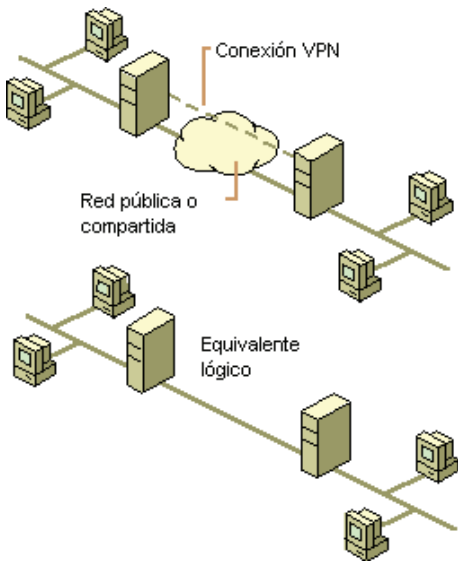


Figura 2.2 Descripción Gráfica de una VPN[26]

[25] FUENTE: http://www.cypsela.es/especiales/pdf199/umts.pdf
[26] FUENTE: http://www.uv.es/siuv/cas/zxarxa/vpn.htm

2.3.1 REQUERIMIENTOS DE UNA VPN

2.3.1.1 Identificación de usuario

Las VPN deben verificar la identidad de los usuarios y restringir su acceso a aquellos que no se encuentren autorizados.

2.3.1.2 Codificación de datos

Los datos que se van a transmitir a través de la red pública (Internet), antes deben ser cifrados, para que así no puedan ser leídos. Esta tarea se realiza con algoritmos de cifrado como DES o 3DES que solo pueden ser leídos por el emisor y receptor.

2.3.1.3 Administración de claves

Uno de los requisitos de las VPN, es la actualización de las claves de cifrado para los usuarios, necesaria para la comunicación entre los nodos y puntos remotos.

2.3.2 ACCIONES DE SEGURIDAD

Para hacer posible que la VPN trabaje de forma segura es necesario proporcionar los medios para garantizar la autentificación, integridad y confidencialidad de toda la comunicación:

2.3.2.1 Autentificación y autorización

Este es el primer paso para establecer la comunicación, en el cual se verifica quién está del otro lado, tanto el usuario/equipo y qué nivel de acceso debe tener.

2.3.2.2 Integridad de Datos

Esta medida comprueba que los datos enviados no han sido alterados. Para ello se utiliza funciones de resumen o Hash.

La función hash es una suma de comprobación criptográfica o un código de integridad de mensaje (MIC) que ambos interlocutores deben calcular para comprobar el mensaje. Por ejemplo, el equipo remitente utiliza una función hash y una clave compartida para calcular la suma de comprobación del mensaje, y la incluye en el paquete. El equipo receptor debe calcular la misma función hash sobre el mensaje recibido con la clave compartida y comparar el resultado con el original (que se incluye en el paquete del remitente). Si el mensaje ha cambiado durante el trayecto, los valores de hash serán diferentes y se descartará el paquete. [27]

2.3.2.3 Confidencialidad

Dado que los datos viajan a través de un medio tan hostil como Internet, dichos datos son susceptibles de intercepción, por lo que resulta fundamental el cifrado de los mismos. De este modo, la información no debe poder ser interpretada por nadie más que los destinatarios de la misma, para esto de usa algoritmos de cifrado.

2.3.2.4 No repudio

Esta acción significa que un mensaje debe ser firmado antes de ser enviado, de esta manera el que lo firma no puede negar que el mensaje fue enviado por él.

Las ventajas de una red virtual privada son: Integridad, confidencialidad y seguridad de datos además de que se reducen los costos, son sencillas de usar, y facilitan la comunicación entre dos usuarios en lugares distantes.

---

[27] FUENTE: http://technet.microsoft.com/es-es/library/cc736330(WS.10).aspx

2.3.3 TIPOS DE VPN

Básicamente existen tres arquitecturas de conexión VPN, que son de acceso remoto, punto a punto y VLAN.[28]

2.3.3.1 VPN de acceso remoto

Es quizás el modelo más usado actualmente, y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones preparados, etc.) utilizando Internet como vínculo de acceso. Una vez autentificados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa. Muchas empresas han reemplazado con esta tecnología su infraestructura dial-up (módems y líneas telefónicas).

2.3.3.2 VPN punto a punto

Este esquema se utiliza para conectar oficinas remotas con la sede central de la organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos enlaces punto a punto tradicionales, sobre todo en las comunicaciones internacionales. Es más común el siguiente punto, también llamado tecnología de túnel o tunneling.

2.3.3.2.1 Técnica de túnel (Tunneling)

La técnica de tunneling consiste en encapsular un protocolo de red sobre otro (protocolo de red encapsulador) creando un túnel dentro de una red de computadoras. El establecimiento de dicho túnel se implementa incluyendo una PDU determinada dentro de otra PDU con el objetivo de transmitirla desde un

[28] FUENTE: http://blackspiral.org/docs/pfc/itis

extremo al otro del túnel sin que sea necesaria una interpretación intermedia de la PDU encapsulada. El protocolo del paquete que vuelve a encapsular solo es entendido por el emisor y por el receptor, en concreto, por el gateway que lo envía y por el gateway que lo recibe.[29] Para los usuarios que utilizan esos routers el proceso es transparente ya que el empaquetamiento y el des-empaquetamiento se realiza en el Gateway y no, normalmente en el PC. De esta manera se encaminan los paquetes de datos sobre nodos intermedios que son incapaces de ver en claro el contenido de dichos paquetes. El túnel queda definido por los puntos extremos y el protocolo de comunicación empleado, que entre otros, podría ser SSH (Secure SHell, en español: intérprete de órdenes segura).

Básicamente se usan tres protocolos, el protocolo del carrier, el protocolo de encapsulamiento y protocolo pasajero.

- **El protocolo del portador**

Es el protocolo usado por la red, para transforma la información de un punto a otro.

- **En protocolo del encapsulamiento**

Es el protocolo que aplica el encapsulamiento del paquete enviado, y según el tipo será más o menos seguro, pudiendo ser GRE encapsulamiento general de Ruteo (Generic Routing Encapsulation), IPSec, entre otros, siendo el IPSec el más seguro entre los populares.

- **El protocolo pasajero**

Es el protocolo del paquete de información que se envía dentro del envoltorio, es decir, el paquete original de información. Los "protocolos pasajero" habituales son IP.

[29] FUENTE: http://www.34t.com/box-docs.asp?doc=649

El uso de la técnica de túnel persigue diferentes objetivos, dependiendo del problema que se esté tratando, como por ejemplo la comunicación de islas en escenarios multicast, la redirección de tráfico, etc. Uno de los ejemplos más claros de utilización de esta técnica consiste en la redirección de tráfico en escenarios IP Móvil. En escenarios de IP móvil, cuando un nodo-móvil no se encuentra en su red base, necesita que su home-agent realice ciertas funciones en su puesto, entre las que se encuentra la de capturar el tráfico dirigido al nodo-móvil y redirigirlo hacia él. Esa redirección del tráfico se realiza usando un mecanismo de tunneling, ya que es necesario que los paquetes conserven su estructura y contenido originales (dirección IP de origen y destino, puertos, etc.) cuando sean recibidos por el nodo-móvil.

Además la técnica de túnel tiene implicaciones muy importantes para las VPNs. por ejemplo, se pueden enviar paquetes que utilizan cualquier protocolo no soportado por Internet encapsulado por un paquete IP que si puede ser enviado por Internet. También puede enviar un paquete destinado a una IP de una red privada (no perteneciente a Internet y por tanto no localizable) encapsulado por un paquete IP con una dirección pública que si encontrará su destino en Internet.[30]

En un túnel de una VPN de punto-a-punto, el protocolo de encapsulamiento que generalmente se utiliza es el GRE este permite poder pasar un paquete de cualquier protocolo nativo encapsulado en un paquete IP que puede ser enviado por Internet, este paquete incluye información de que tipo de paquete se está encapsulando además de la información de la conexión entre el cliente y el servidor.

Para tener una VPN con mayor seguridad, el protocolo que se utiliza es IPSec en modo túnel, este es protocolo de encapsulamiento seguro tanto en conexiones que unen oficinas como en conexiones de un usuario a una oficina porque además de encriptar las información es eficiente autentificando los usuarios.

[30] FUENTE: http://www.34t.com/box-docs.asp?doc=649

2.3.3.3 VPN interna VLAN

Este esquema es el menos difundido pero uno de los más poderosos para utilizar dentro de la empresa. Es una variante del tipo "acceso remoto" pero, en vez de utilizar Internet como medio de conexión, emplea la misma red de área local (LAN) de la empresa. Sirve para aislar zonas y servicios de la red interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas (WiFi).

Un ejemplo clásico es un servidor con información sensible, como las nóminas de sueldos, ubicado detrás de un equipo VPN, el cual provee autenticación adicional más el agregado del cifrado, haciendo posible que sólo el personal de recursos humanos habilitado pueda acceder a la información.

2.3.4 TIPOS DE CONEXIÓN

2.3.4.1 Conexión de acceso remoto

Una conexión de acceso remoto es realizada por un cliente o un usuario de una computadora que se conecta a una red privada, los paquetes enviados a través de la conexión VPN son originados al cliente de acceso remoto, y éste se autentifica al servidor de acceso remoto, y el servidor se autentifica ante el cliente.

2.3.4.2 Conexión VPN Ruteador a Ruteador

Una conexión VPN ruteador a ruteador es realizada por un ruteador, y este a su vez se conecta a una red privada. En este tipo de conexión, los paquetes enviados desde cualquier ruteador no se originan en los ruteadores. El ruteador que realiza la llamada se autentifica ante el ruteador que responde y este a su vez se autentica ante el ruteador que realiza la llamada y también sirve para la intranet.

2.3.4.3 Conexión VPN firewall a firewall

Una conexión VPN firewall a firewall es realizada por uno de ellos, y éste a su vez se conecta a una red privada. En este tipo de conexión, los paquetes son enviados desde cualquier usuario en Internet. El firewall que realiza la llamada se autentifica ante el que responde y éste a su vez se autentifica ante el llamante.

2.4 CONEXIÓN DE DOS EQUIPOS DE RADIOGONIOMETRÍA A TRAVÉS DE UNA VPN.

2.4.1 DESCRIPCIÓN

Los equipos de radiogoniometría utilizados en la aplicación, cuentan con un software de control remoto que nos permite conectarnos a través de algunos medios, entre los más usados están: Conexión serial, o conexión TCP-IP.

Para que el sistema sea móvil es necesario realizar la conexión a través de una red pública inalámbrica. Por esta razón se asigna una VPN en una red pública de telefonía móvil. Con lo que logramos que la conexión sea independiente de la distancia de los equipos, y del lugar donde se encuentren, dependiendo únicamente de la cobertura que tenga la red, que al ser de una operadora de servicios de telefonía móvil celular en el país, brinda un campo muy amplio de operación.

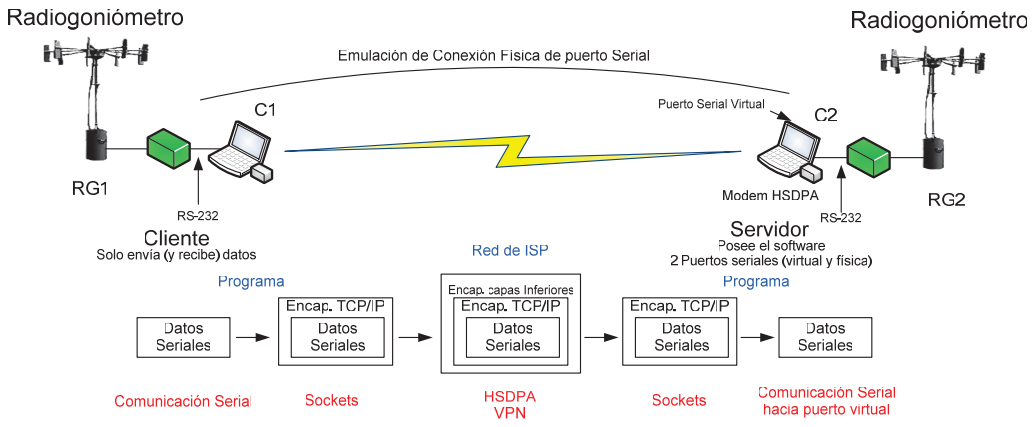


Figura 2.3 Diagrama de Conexión del sistema de Radiogoniometría

El receptor del radiogoniómetro permite su conexión física a un dispositivo remoto a través de un puerto serial, esto se convierte en un inconveniente al utilizar módems HSDPA, ya que estos módems no poseen un interfaz RS232 por lo que se hace necesario algún tipo de mecanismo adicional que permita el transporte de datos seriales por la red.

En el diagrama de conexión de la figura 2.3 se puede visualizar la conexión, los dos radiogoniómetros RG1 y RG2 se conectan directamente al computador cliente C1 y al computador servidor C2 respectivamente, por medio del puerto serial. El RG2 se conecta con el computador C2 a través del software de control remoto, con el Modo de conexión serial, por medio del puerto serial físico COM1.

Los datos enviados por el RG1 deben pasar por un simulador de puertos, que será el encargado de encapsular los datos seriales y convertirlos en paquetes TCP/IP, para que viajen por la VPN por medio del módem HSDPA, conectado a uno de los puertos USB del computador C1. Los datos se reciben en el computador C2 donde se realiza el proceso inverso, de esta forma el radiogoniómetro remoto RG1 se conecta al software de control remoto en modo serial a través de un puerto COM virtual.

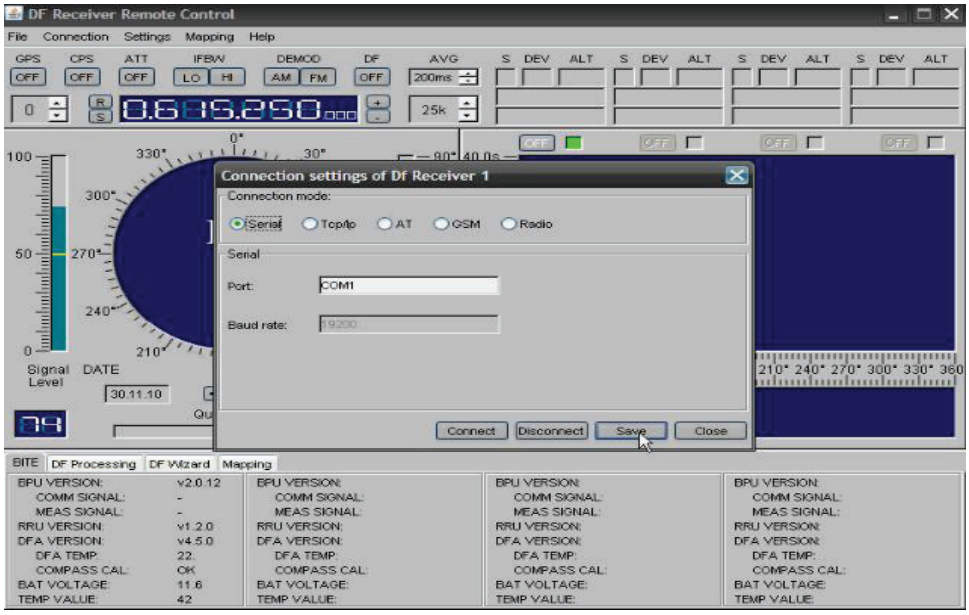


Figura 2.4 Ventana para realizar la conexión a través del puerto físico COM 1

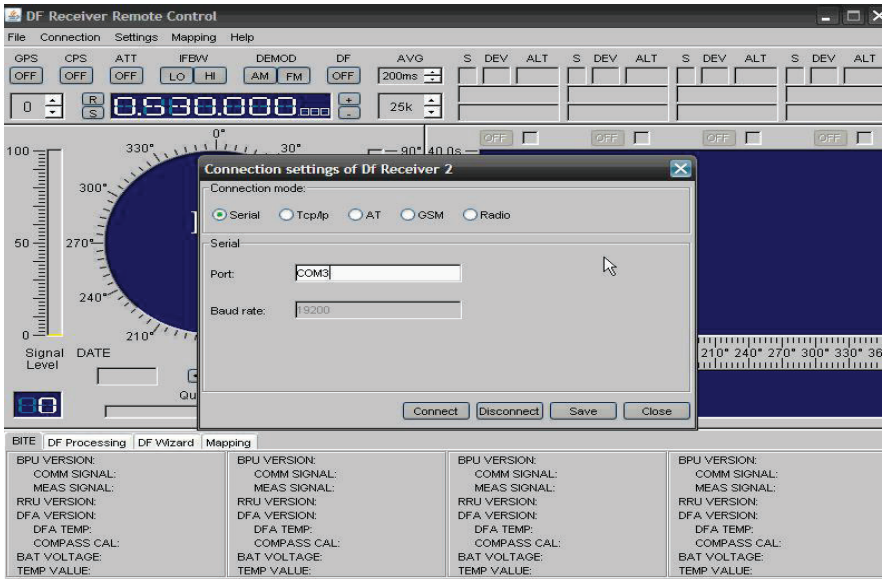


Figura 2.5 Ventana para realizar la conexión a través del puerto virtual COM 3

2.4.2 REQUERIMIENTOS DE HARDWARE

Las herramientas de hardware utilizadas para esta aplicación son:

Cantidad	Descripción de Hardware
2	Radiogoniómetros Almos 3000, con puerto serial.
2	Computadoras Laptop HP: 1 puerto serial físico COM1 4 puertos USB
2	Módems HSDPA Modelo ZTE.
2	Cables RS232 hembra-hembra

Tabla 2.1 Requerimientos de Hardware

2.4.3 REQUERIMIENTOS DE SOFTWARE

Para poder realizar la simulación de puertos necesaria para conectar los equipos de radiogoniometría utilizando los módems HSDPA, se usa el programa VSP (Virtual Serial Port) ver Anexo C.

El programa VSP, es un software libre que permite la creación de puertos virtuales, y la comunicación de estos con puertos físicos existentes en el computador.

Por medio de este programa, el computador se convierte en un puente entre el puerto serial físico del receptor y el puerto USB por el cual se conecta el modem HSDPA, es decir se encapsulan los datos seriales del receptor de radiogoniometría para que puedan ser enviados a través de TCP/IP, por la VPN del computador cliente al computador servidor.

El encendido de la conexión se realiza por medio del software de control remoto del radiogoniómetro ver Anexo B. Los datos se pueden visualizar a través de un mapa digital por medio del programa MAPINFO, este programa permite cargar mapas elaborados en formatos como Auto-CAD entre otros.

2.4.4 CONFIGURACIÓN DE LA VPN

La configuración de la VPN, es relativamente sencilla, para esto es necesario que el servicio sea levantado por una operadora de telefonía móvil y que a su vez se proporcionen los chips para cada módem con sus respectivos parámetros de configuración, los mismos que son:

Número Telefónico	IMSI	APN	Dirección IP
95834247	740000105156919	sva18.operador.com.ec	10.117.18.34
95835068	740000105156921	sva18.operador.com.ec	10.117.18.35

Tabla 2.2 Parámetros de configuración de la VPN

Un APN o Access Point Name es el nombre de un punto de acceso para GPRS/HSDPA que en algunos casos viene predeterminado en el dispositivo móvil y sino es así se debe configurar para que pueda acceder a Internet, está puede ser una dirección IP a la cual un móvil se puede conectar, un punto de

configuración que es usado para esa conexión, una opción particular que se configura en un dispositivo móvil, etc.[31]

Los APN pueden ser variados. Son usados en redes tanto públicas como privadas. Por ejemplo: grancompania.mnc012.mcc345.gprs, tuwap.com, internet.compania.com, etc.

Una vez que el dispositivo se ha conectado, usa el servidor de nombres de dominios DNS para hacer el proceso llamado Resolución de APN, que finalmente da la IP real de la APN.

Con la obtención de los parámetros de configuración se instalan los módems en el computador a través de un interfaz de usuario amigable, que nos permite crear la conexión entre los dos dispositivos, ver Anexo D.

Para comprobar la conexión entre los módems y verificar que la VPN, ha sido activada realizamos pruebas de ping.

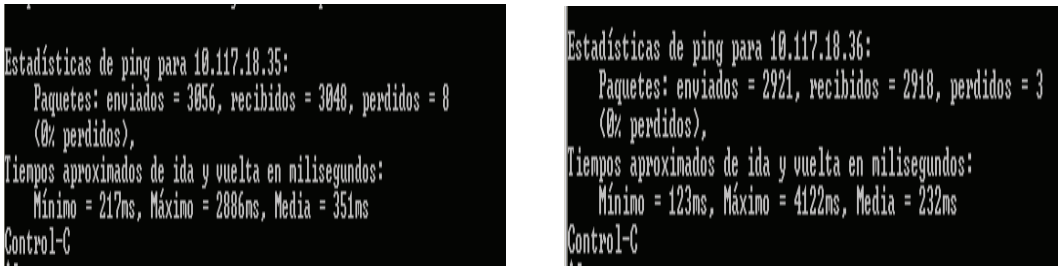


Figura 2.6 Pruebas de Ping Realizadas entre los módems

Una vez que la VPN está activa, y con los respectivos requerimientos de hardware y software se procede a configurar los parámetros para llevar a cabo la conexión, ver Anexo E.

[31] FUENTE: http://mibam.entel.cl/posts/que-es-una-apn

CAPÍTULO 3

ESTUDIO DE LA FACTIBILIDAD DEL USO DEL SISTEMA DE RADIOGOIOMETRÍA, PARA DETECCIÓN DE SEÑALES DE TELEFONÍA MOVIL CELULAR

3.1 FRAUDE EN TELECOMUNICACIONES

Las modalidades de fraude que afectan hoy en día, tanto a las empresas de telecomunicaciones como a sus usuarios, son diversas.

Teniendo en cuenta que el fraude ocasiona pérdidas millonarias, es de vital importancia contar con una estrategia de prevención, detección e investigación del fraude.

3.1.1 DEFINICIÓN

3.1.1.1 Fraude según la RAE

Acción contraria a la verdad y a la rectitud32, que perjudica a la persona u organización contra quien se comete.

3.1.1.2 Fraude en Telecomunicaciones

Es el uso o adquisición de los servicios de telecomunicaciones a través de medios ilegales y sin la intención de pagar por ellos.[33]

Este tipo de fraudes afecta cada año tanto a operadoras de servicios como al estado, es por esta razón que se ahondan esfuerzos para su detección y combate.

---

[32] FUENTE: http://definicion.de/fraude/
[33] FUENTE: canTV, Presentación fraude en telecomunicaciones

3.1.2 TIPO Y MODALIDADES DE FRAUDE EN TELECOMUNICACIONES

Existen tres grupos de fraudes, de donde se derivan una serie de ilícitos, estos son: fraude por suscripción, fraude Interno, fraude técnico.

3.1.2.1 Fraude por suscripción

Se caracteriza por la presentación de información y documentación imprecisa, incorrecta o de un tercero, (obtenida con fraude) para suscribir un servicio y no cumplir con las obligaciones de pago. En otros casos compran servicios a nombre de indigentes, a quienes les pagan sumas ridículas para que les "presten" sus documentos de identificación y luego nadie paga tales cuentas.[34] Involucran dos ilícitos: documentación falsa y robo de identidad.

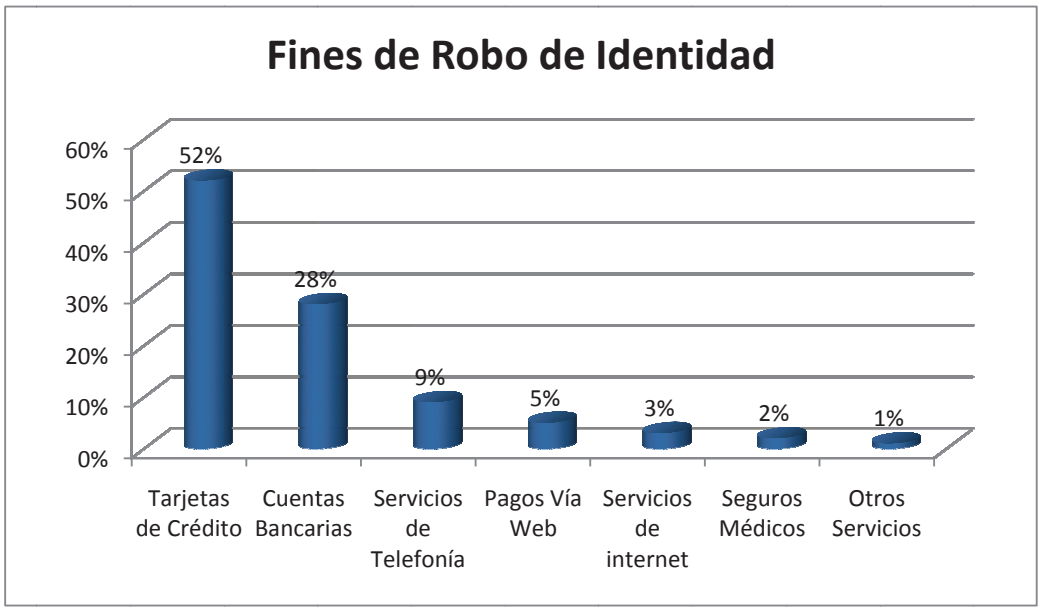


Figura 3.1 Estadística de los delitos que se cometen por medio del robo de identidad

Aproximadamente en el mundo diariamente son víctimas de robo de identidad de 8.000 a 12.000 personas. [35]

[34] FUENTE: SUPERTEL, Libro Fraude en Telecomunicaciones, pág. 13
[35] FUENTE: canTV, Presentación fraude en telecomunicaciones

3.1.2.2 Fraude Interno

Fraude que se origina desde el propio equipo de la compañía de Telecomunicaciones o en sus aliados de negocio. Probablemente es la fuente más importante de pérdidas en compañías de Telecomunicaciones. Requiere el claro conocimiento de los procesos del negocio y las tecnologías. Requiere acceso a las aplicaciones, facilidades de red e información. El principal objetivo es obtener dinero a través del ilícito. La detección se basa en la experiencia del equipo de fraude. Este deriva en otros dos ilícitos que son: manipulación de Sistemas y la usurpación de usuarios y claves.

3.1.2.3 Fraude Técnico

Este tipo de fraude requiere, un conocimiento técnico del funcionamiento y manejo de equipos de telecomunicaciones, estos tiene la particularidad que evolucionan de acuerdo a al desarrollo de la tecnología, entre los más sonados e importantes tenemos, robo de líneas, el clonning, call back, refilling,by-pass, entre otros.

3.1.2.3.1 Clonación (Cloning)

Es la "copia" ilegal de los datos que identifican un terminal móvil, para hacer que las llamadas sean cobradas a un cliente válido. En este caso los datos del cliente válido son obtenidos de la red de telefonía celular, a través de equipo especial. Esto solo es posible cuando los equipos móviles no están autenticados, cosa que no pasa con las redes TDMA y GSM.[36]

[36] FUENTE: canTV, Presentación fraude en telecomunicaciones

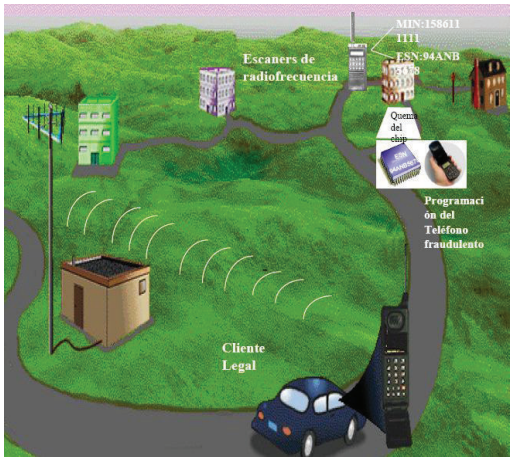


Figura 3.2 Esquema General de la modalidad de fraude cloning

3.1.2.3.2 Retorno de Llamada (Call back)

Es el procedimiento mediante el cual se revierte el origen del tráfico internacional, haciendo una llamada "disparo" que no es contestada (y por tanto no cobrada), para que un equipo en el otro extremo obtenga la información del llamante y devuelva la llamada, con tono de ese otro país. Fue uno de los primeros fraudes importantes que se detectaron en el país.[37]

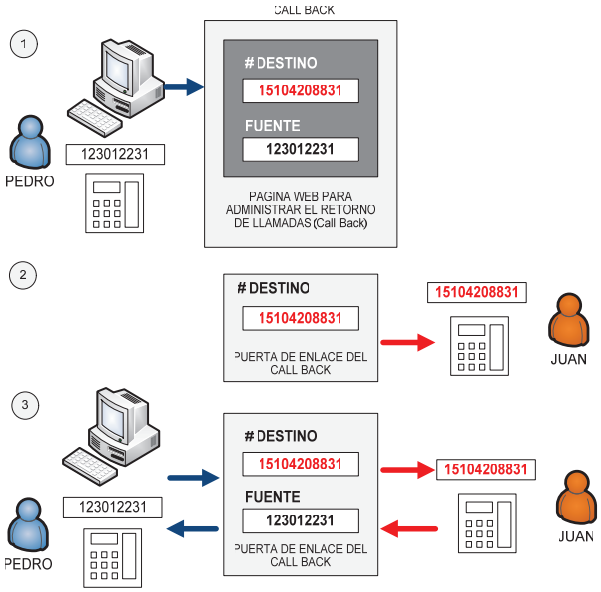


Figura 3.3 Esquema de call-back ofrecido en internet

[37] FUENTE: http://www.global4you.net/nn_callback.htm

3.1.2.3.3 Re-direccionamiento de Llamadas (Refilling)

Procedimiento mediante el cual el país que origina el tráfico lo enruta al destino final, a través de un tercero, que utiliza como tránsito. Debido a las diferencias tarifarias entre los países involucrados, el país que origina el tráfico paga una tarifa de terminación más baja al país destino, y al quien sirve de tránsito generalmente no se le paga nada, pues dicho tráfico se introduce mediante bypass.

3.1.2.3.4 Sistema de tráfico Internacional no autorizado (Bypass)

De los tipos de fraude existentes, el que más perjuicio origina a las operadoras de telefonía y al estado ecuatoriano, lo constituye el By pass, que en los últimos años ha causado pérdidas millonarias a nuestro país.[38]

Se denomina comúnmente bypass, a la importación o exportación de tráfico telefónico, realizado por una persona física o jurídica que no es concesionaria, para lo cual utiliza redes alternas o paralelas (ilegales), a las establecidas por el operador concesionado, con el objeto de evadir las tasas contables entre operadores establecidos (es decir, se evita la tarifación de la llamada internacional, y se la convierte en una llamada local).

El tráfico de llamadas entrantes es aproximadamente 8 veces mayor que el de las llamadas salientes y en este mismo sentido se comete el ilícito del By-pass. El By-pass se muestra como una ruta alternativa para los portadores internacionales, la cual presenta un costo sumamente menor que el exigido por las compañías telefónicas locales; por este motivo deciden: ingresar sus volúmenes de tráfico mediante esta vía alternativa; o, fomentar la implementación de sistemas de By-pass para ingresar su tráfico a un menor costo. El tráfico telefónico internacional se enruta por telepuertos privados (sean estos autorizados o no autorizados) y no por telepuertos internacionales de las empresas telefónicas. Del telepuerto

[38] FUENTE: Instituto Costarricense de Electricidad Telecomunicaciones presentación Fraude en Telecomunicaciones

privado, acceden a un local clandestino mediante enlaces de última milla: fibra óptica, spread spectrum, líneas dedicadas de cobre o microondas.

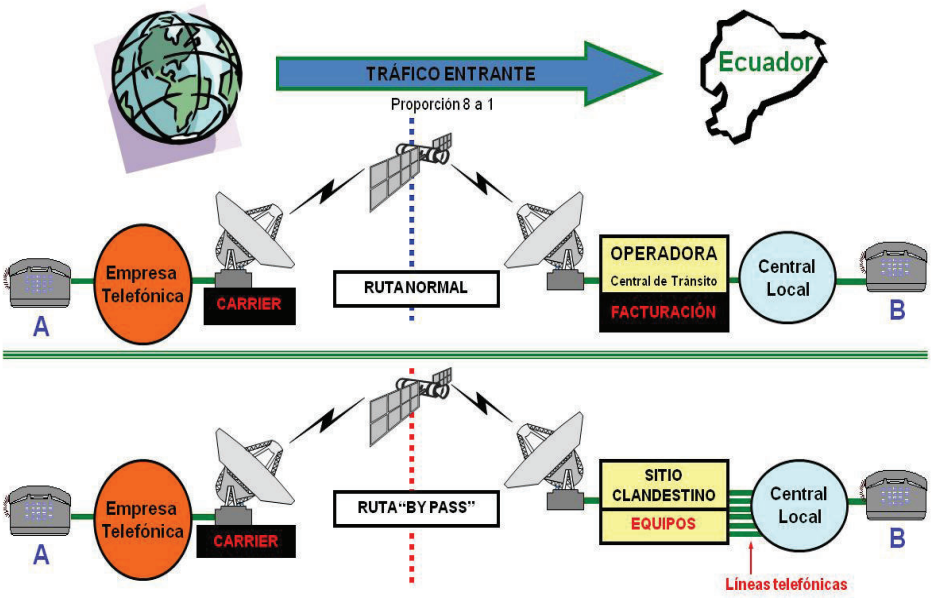


Figura 3.4 Modalidad de Fraude By-Pass

Inicialmente este ilícito se realizaba a través de líneas telefónicas fijas, esto hacía mucho más fácil su detección, en la actualidad la mayoría de sistemas by pass, son implementados por líneas móviles celulares, y la tecnología GSM ha sido una herramienta que facilita mucho el trabajo de los delincuentes, sin mucho esfuerzo una persona puede adquirir líneas telefónicas celulares que pueden ser utilizadas para cometer este tipo de fraude, a esto se suma la movilidad de los equipos que en conjunto obstaculiza el proceso de detección de este tipo de sistemas. Si bien existen mecanismos que amedrentan al delincuente una vez que se detecta el mismo; como el bloqueo de las tarjetas SIM, interrupción de llamadas, etc, este vuelve a reincidir porque no existe una detección in fraganti en el lugar mismo de la infracción.[39]

[39] FUENTE: SUPERTEL, Artículo Fraude en Telecomunicaciones en el Ecuador, 20 de marzo 2010

3.1.3 SISTEMAS BY-PASS A TRAVÉS DE LÍNEAS MÓVILES CELULARES, TECNOLOGÍA GSM

Este tipo de fraude aparece en nuestro país, en el año 2003, donde se marca una nueva etapa en la historia de fraude a través de by-pass.

En este tipo de fraude se utilizan equipos SIMbox, es decir equipos especiales que permiten, a través de una "batería" o grupo de tarjetas SIM de teléfonos celulares, exportar o importar tráfico internacional, haciendo bypass. Las tarjetas SIM son obtenidas mediante fraudes de suscripción.

Los equipos de telecomunicaciones son cada vez más avanzados de tal manera que los "gateways" utilizados permiten fácilmente la convergencia de una red de datos con una red telefónica móvil celular; y, los enlaces internacionales se implementan utilizando las ventajas de la red de Internet y la tecnología de voz sobre IP (VoIP), proporcionando una mejor calidad en la comunicación telefónica, casi de manera similar a la de una red convencional.[40]

El tráfico telefónico internacional detectado que cursa por un sistema "By pass", tiene su origen incluso en portales IP, así también, dichos sistemas no autorizados se implementan para cursar tráfico ilegal a una determinada red en nuestro país, esto debido a la diferencia por cargos de interconexión existente entre las diversas redes de nuestro país.

3.1.3.1 Acciones realizadas para combatir y erradicar el By-pass a través de líneas móviles celulares

El organismo técnico de control cuyo objetivo es controlar los servicios de telecomunicaciones y combatir los fraudes que se producen dentro del sector, tiene interés en el desarrollo de una herramienta que permita mitigar este tipo de fraude a través de la detección de los sistemas de tráfico telefónico internacional

[40] FUENTE: Instituto Costarricense de Electricidad Telecomunicaciones, presentación Fraude en Telecomunicaciones.

no autorizados implementados a través de líneas celulares móviles, como se ha mencionado el principal inconveniente para combatir este tipo de fraude, a sido la movilidad que brinda está tecnología a los nuevos sistemas by-pass, lo que dificulta su localización.

Con la cooperación de los operadores del servicio móvil celular y a través de un drive test (prueba de conducción), se puede determinar la zona de operación del by-pass, sin embargo esta zona resulta demasiado grande para determinar la ubicación de un dispositivo.

Con este antecedente el organismo técnico de control adquirió dos equipos de radiogoniometría que permiten localizar señales en un frecuencia fija dentro de la banda de UHF. Las frecuencias que utiliza GSM para su operación se encuentran dentro de esta banda por lo que una aplicación específica que se quiere dar a los equipos, luego de determinar una zona más pequeña de operación, es que puedan ser usados para localizar señales de telefonía móvil celular, para ubicar el dispositivo móvil que genera esta señal y de esta manera encontrar la instalación fraudulenta.

Esta idea suena muy ambiciosa y podría significar una herramienta poderosa en el combate de sistemas by-pass, sin embargo el segundo inconveniente que se presenta es que GSM utiliza una tecnología llamada *frequency hopping* (saltos de frecuencia, canales), es decir la frecuencia que usa en su comunicación no es constante en el tiempo, por este motivo una ubicación tradicional con el uso del sistema de radiogoniometría no sería posible.

En un trabajo en conjunto con todos los involucrados en este tema se propone dos posibles soluciones que permitirán al menos en teoría aplicar el sistema de radiogoniometría para localizar dispositivos móviles. Las mismas que son: La implementación de una radiobase insertada para el establecimiento de una llamada ciega y la realización de Pruebas Nocturnas para determinar la ubicación más probable del dispositivo móvil.

3.2 FACTIBILIDAD DE LA IMPLEMENTACIÓN DE UNA RADIO BASE INSERTADA, PARA EL ESTABLECIMIENTO DE LA LLAMADA CIEGA

3.2.1 OBJETIVO

El objetivo principal que persigue la implementación de una radiobase insertada para el establecimiento de una llamada ciega es determinar la localización de un dispositivo móvil a través del sistema de radiogoniometría implementado por el organismo técnico de control. Esto con el fin de combatir efectivamente el fraude de los sistemas de tráfico telefónico internacional no autorizados (by-pass), implementado a través de líneas móviles celulares.

3.2.2 IMPORTANCIA

Este proyecto es de vital importancia para el combate a los sistemas by-pass implementados a través de líneas móviles celulares, ya que se pretende encontrar la ubicación de la instalación fraudulenta para determinar los responsables del delito y obtener las pruebas necesarias que incriminen al o (os) proscrito(s), con lo que se logra frenar este tipo de fraude causante de un gran perjuicio económico para el estado.

3.2.3 INTRODUCCIÓN

Para poder establecer un procedimiento o buscar una herramienta efectiva que permita encontrar la ubicación de un dispositivo móvil que está siendo usado en sistemas de tráfico internacional no autorizado By-pass, es necesario conocer y entender el funcionamiento y operación de la tecnología GSM, ya que existen parámetros que determinarán la factibilidad o no de una acción, por lo que en las siguientes secciones, se explica las definiciones y conceptos propios de GSM que deben ser considerados en el análisis.

3.2.4 TECNOLOGÍA MOVIL CELULAR GSM

GSM, Sistema Global para Comunicaciones Móviles, es una de las tecnologías de telefonía móvil celular más utilizada del mundo, especialmente en Europa.

Los servicios móviles basados en la tecnología GSM se lanzaron por primera vez en Finlandia en 1991. Hoy en día, existen más de 690 redes de telefonía móvil GSM, alrededor de 213 países y según la Asociación de GSM, la tecnología GSM representa el 82,4% de todas las conexiones móviles mundiales, lo que significa aproximadamente dos mil millones de usuarios de telefonía móvil GSM en todo el mundo.

Las redes de telefonía móvil, se basan en el concepto de celdas, es decir zonas circulares que se superponen para cubrir un área geográfica. Las redes celulares hacen uso de un transmisor-receptor central en cada celda, denominado Estación base o Estación base transceptora, BTS.

Cuanto menor sea el radio de una celda, mayor será el ancho de banda disponible. Por lo tanto, en zonas urbanas muy pobladas, hay celdas con un radio de unos cientos de metros mientras que en zonas rurales hay celdas enormes de hasta 30 kilómetros que proporcionan cobertura.

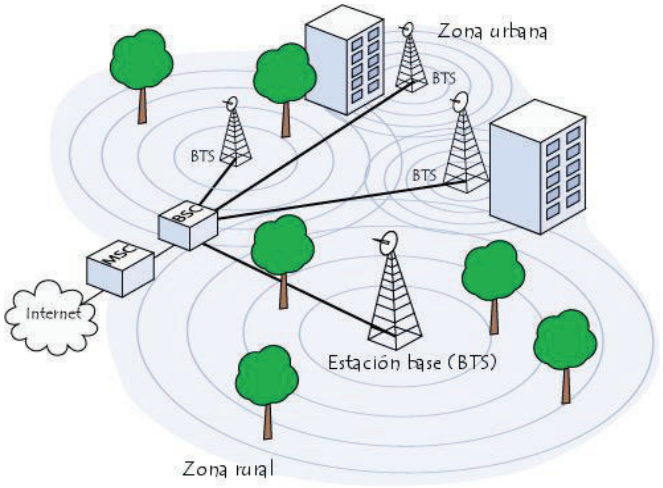


Figura 3.5 Área de Cobertura de las diferentes celdas en GSM[41]

[41] FUENTE: http://es.kioskea.net/contents/telephonie-mobile/gsm.php3

En una red celular, cada celda está rodeada por 6 celdas contiguas por esto las celdas generalmente se dibujan como un hexágono. Para evitar interferencia, las celdas adyacentes no pueden usar la misma frecuencia. En la práctica, dos celdas que usan el mismo rango de frecuencia deben estar separadas por una distancia equivalente a dos o tres veces el diámetro de la celda. Usa portadoras de 200kHz con 8 canales en TDMA (ranuras de tiempo).

3.2.4.1 Arquitectura de la red GSM

La arquitectura de una red GSM, está compuesta por tres elementos estos son:

- Estación Móvil
- Subsistema Estación Base
- Subsistema de red

En una red GSM, la terminal del usuario se llama estación móvil. Una estación móvil está constituida por una tarjeta SIM (Módulo de identificación de abonado), que permite identificar de manera única al usuario y a la terminal móvil, o sea, al dispositivo del usuario.

Las terminales se identifican por medio de un número único de identificación de 15 dígitos denominado IMEI (Identificador internacional de equipos móviles). Cada tarjeta SIM posee un número de identificación único y secreto denominado IMSI (Identificador internacional de abonados móviles). Este código se puede proteger con una clave de 4 dígitos llamada código *PIN*. [42]

Por lo tanto, la tarjeta SIM permite identificar a cada usuario independientemente de la terminal utilizada durante la comunicación con la estación base. Las comunicaciones entre una estación móvil y una estación base se producen a través de un vínculo de radio, por lo general denominado interfaz de aire (o en raras ocasiones, interfaz Um). Todas las estaciones base de una red celular están conectadas a un controlador de estaciones base (o BSC), que administra la

[42] FUENTE: http://es.kioskea.net/contents/telephonie-mobile/gsm.php3

distribución de los recursos. El sistema compuesto del controlador de estaciones base y sus estaciones base conectadas es el Subsistema de estaciones base (o BSS).

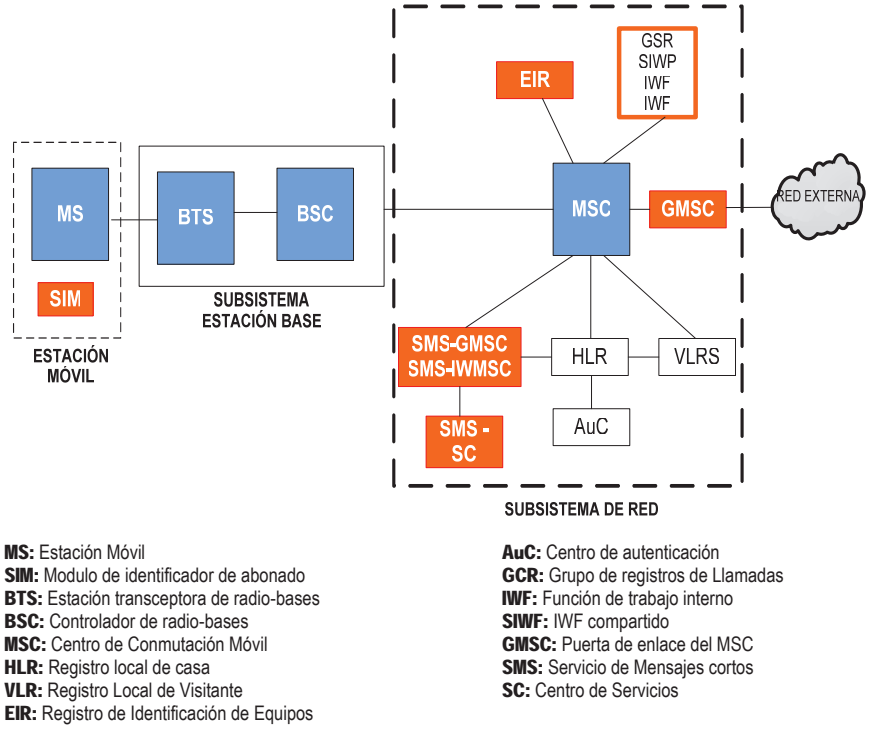


Figura 3.6 Esquema de Red Celular GSM[43]

Por último, los controladores de estaciones base están físicamente conectados al Centro de conmutación móvil (MSC) que los conecta con la red de telefonía pública y con Internet; lo administra el operador de la red telefónica. El MSC pertenece a un Subsistema de conmutación de red (NSS) que gestiona las identidades de los usuarios, su ubicación y el establecimiento de comunicaciones con otros usuarios. Generalmente, el MSC se conecta a bases de datos que proporcionan funciones adicionales como HLR, VLR, EIR.

Las zonas de cobertura de cada celda dependerá de las condiciones del lugar (número de viviendas, número de habitantes, obstrucciones, etc., donde se va a dar la comunicación, en general el alcanza de las celdas celulares en zonas urbanas es más pequeña que la de una zona rural.

[43]FUENTE: http://www.ieee802.org/21/archived_docs/Documents/Handoff_Freedman.pdf

3.2.4.1.1 Estación Móvil (MS)

La estación móvil está conformada por el equipo móvil y la tarjeta SIM.
El equipo móvil este debe tener la capacidad operar bajo las condiciones descritas en la tabla 3.1

	DESCRIPCIÓN
BANDA DUAL	Capaz de operar a: GSM 900 (SISTEMA EUROPEO) DSC 800/PCS (SISTEMA AMERICANO)
MODO DUAL	Capaz de conectarse a: GSM DECT

Tabla 3.1 Descripción de Operación de un Dispositivo Móvil GSM

El modulo de identidad suscriptor, proporciona la información contenida en la tabla 3.2:

ASIGNACIÓN	DESCRIPCIÓN
MSISDN	El número telefónico del abonado
IMSI	Identificación internacional de abonados móviles
ACTIVA, INACTIVA	El estado de la tarjeta SIM
COD. SERV.	El código de servicio (asignado por el operador)
PIN	Código de identificación personal
PUNK	Código personal de desbloqueo

Tabla 3.2 Descripción de la Información de una tarjeta SIM

3.2.4.1.2 Subsistema Estación Base (BSS)

El subsistema de Estación Bases es el encargado de controlar la interfaz de radio y está conformado por la estación base de transceptora (BTS) y estación base de control (BSC).

- **Estación Base Transceptora (BTS)**

En el subsistema de estación base pueden haber una o varias BTS, estas contienen los transmisores/receptores que sirven a una celda, se encargan de la

interfaz física entre el dispositivo móvil y la BSC, realiza la gestión de Diversidad de la Antena, Esta efectúa la técnica de *Frecuency Hopping* (salto de frecuencia), el control dinámico de potencia, gestiona los algoritmos de clave, y monitoriza la conexión.

- **Estación Base de Control (BSC)**

Gobierna los recursos de radio para las BTS a él conectadas. Se encarga de la gestión y configuración del canal de radio y la elección de la celda y el canal, además realiza la gestión del handover, y hace la transcodificación de canales de radio (16 ó 8kbps) a canales a 64kbps.

3.3.4.1.3 Subsistema de Red (NSS)

El subsistema de red es el que permite la interconexión entre el BSS con otras redes públicas (PSTN, ISDN, PSPDN, CSPDN). Implementa las funciones de base de datos necesarias para identificar a los usuarios y localizar terminales, además realiza la conducción de las llamadas, y permite la facturación.

Está conformado por: MSC (Centro de Conmutación Móvil), HLR (Registro de Datos local), VLR (Registro Local de Visitante), EIR (Registro Identificador de Equipo), AuC(Centro de Autenticación), OMC (centro de Operación y Mantenimiento).

- **Centro de Conmutación Móvil (MSC)**

El MSC es el elemento central del subsistema de red, este se ocupa de la gestión del tráfico de una o más, actuado como un ruteador. Además se encarga de interconectar los demás elementos del NSS. Dentro de la gestión de llamadas, realiza la autenticación de la llamada localización e identificación del MS, efectúa la conmutación entre el BSS del mismo NSS o con otros MSC de otras redes, hace las funciones de Gateway con otras redes (PLMN, ISDN, PRTN, etc).

En cuanto al proceso del handover realiza el handover Intra-MSC, y el handover Inter MSC. El MSC asocia el IMSI con el TMSI, para mantener la confidencialidad de la identidad de usuario en el momento de la transmisión.

- **El Registro de ubicación de origen (HLR)**

HLR es una base de datos que contiene información como posición geográfica, información administrativa, IMSI, MSISDN, etc., de los abonados registrados dentro de la zona del conmutador (MSC).

Es la encargada de la seguridad del diálogo con el AuC y el VLR, de registrar la posición geográfica de los terminales para actualizar los VLR´s. realizar el coste de la llamada en base a la información del MSC y gestionar los datos de usuario y datos estadísticos.

- **El Registro de ubicación de visitante (VLR)**

El VLR es una base de datos temporal que contiene información de usuarios que no son abonados locales. El VLR recupera los datos de un usuario nuevo del HLR de la zona de abonado del usuario. Los datos se conservan mientras el usuario está dentro de la zona y se eliminan en cuanto abandona la zona o después de un período de inactividad prolongado cuando el terminal está apagado.

El VLR se suele implementar en el MSC para simplificar la señalización así el área geográfica del MSC es la del VLR. Este registro almacena: EL TMSI, el estado de la estación móvil, tipo de servicios suscritos por el abonado, y la zona de área local del dispositivo móvil.

- **Registro de identificación del equipo (EIR)**

El EIR es una base de datos que contiene la lista de terminales móviles, verifica si una estación móvil está autorizada para acceder al sistema. Cada vez que un MS

intenta acceder a la red la MSC verifica mediante el EIR la lista a la que pertenece, tomando las acciones correspondientes.

Existen tres listas que identifican al equipo, la lista blanca, contiene los IMEI que pueden ingresar al sistema, la lista gris contiene IMEI marcados y no homologados, y la lista negra, que contiene los IMEI que han sido bloqueados por motivos de robo, pérdida, etc.

- **Centro de Autenticación (AuC)**

Es el punto de la red que verifica las identidades de los usuarios. La red celular compuesta de esta manera está diseñada para admitir movilidad a través de la gestión de traspasos que son movimientos que se realizan de una celda a otra. El AuC verifica si el servicio es solicitado por un abonado legítimo.

La autenticación se produce cada vez que el MS se conecta a la red, cada vez que el MS efectúa o recibe una llamada, cada vez que se actualiza la posición del dispositivo móvil, o cada vez que se realiza el acceso a algunos de los servicios suplementarios.

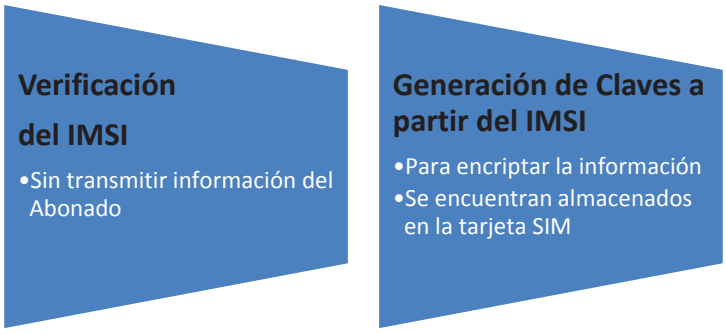


Figura 3.7 Proceso de Autenticación de un móvil

- **Centro de operación y mantenimiento (OMC)**

El OMC es utilizado para la monitorización y mantenimiento de la red por parte del operador. El OMC puede acceder remotamente a todos los elementos del PLMN,

gestiona las alarmas y estado del sistema recopila la información de los usuarios para la facturación, supervisa el flujo del tráfico para posibles cambios en la arquitectura de red y en general realiza la administración de los abonados.

3.2.4.1.4 Interfaz de Radio (Um)

Es la interfaz entre la estación móvil y la BTS, utiliza TDMA/FDMA combinado paa la transmisión de los datos.

- **Acceso Múltiple por División de Tiempo (TDMA)**

TDMA (acceso múltiple por división de tiempo) es una tecnología utilizada en la comunicación digital de un teléfono celular, este tipo de tecnología divide cada canal un número de ranuras de tiempo con el fin de aumentar la cantidad de datos que se pueden transmitir o recibir.

TDMA es usado por algunos estándares como el Servicio Telefónico móvil americano digital (D-AMPS), Sistema Global de Comunicaciones Móviles (GSM), y Celular digital personal (PDC). Sin embargo, cada uno de estos sistemas aplica TDMA de una manera algo diferente e incompatible.

Un esquema alternativo para la multiplexación con FDMA TDMA es CDMA (acceso múltiple por división de código), que tiene toda la gama de frecuencias asignadas para un servicio determinado y la información de multiplexación para todos los usuarios en toda la gama del espectro, al mismo tiempo.[44]

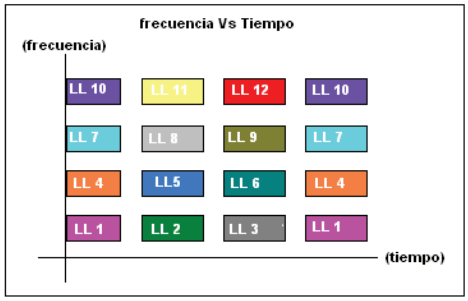


Figura 3.8 Múltiple Acceso por División de Tiempo

[44]FUENTE: www.pangolinsms.com/.../tdma-large.gif

- **Acceso Múltiple por División de Frecuencia (FDMA)**

FDMA (acceso múltiple por división de frecuencia) es la división de la banda de frecuencias atribuidas para la comunicación inalámbrica de telefonía celular en 30 canales, cada uno de los cuales pueden llevar a una conversación de voz, un servicio digital o transportar datos digitales. FDMA es una tecnología base en el analógico Avanzado de Teléfono Móvil (AMPS), el sistema de telefonía celular más ampliamente usado en América del Norte. Con FDMA, cada canal puede ser asignado a un solo usuario a la vez. FDMA también se utiliza en el total del sistema de comunicaciones de acceso (TAC).[45]

En GSM también se utiliza FDMA, pero agrega un acceso múltiple por división de tiempo (TDMA) para obtener más canales por cada canal FDMA, aumentado el número de llamadas que pueden ser manejados en un canal.

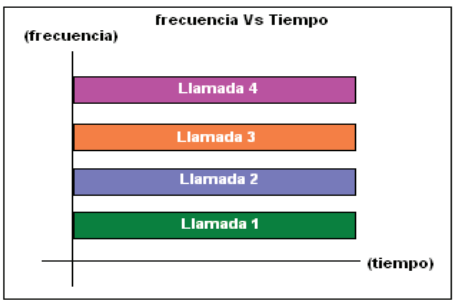


Figura 3.9 Múltiple Acceso por División de Frecuencia

3.2.4.2 Consideraciones Adicionales

Como el ancho de banda es limitado, GSM utiliza técnicas de acceso para rehusar las frecuencias, estás son SDMA (Acceso Múltiple por División de Espacio y FHMA (Múltiple Acceso por Salto de Frecuencia).

[45] FUENTE: http://searchmobilecomputing.techtarget.com/definition/FDMA

- **SDMA, Múltiple Acceso por División de Espacio**

Esta técnica utiliza celdas adyacentes a distintas frecuencias para repartir de mejor manera el uso de las frecuencias, de esta manera se logra su reutilización en celdas no contiguas.

SDMA es un MIMO (múltiples entradas y múltiple salidas, una arquitectura de antena esquema múltiple) basados en la arquitectura de red inalámbrica de comunicación, sobre todo conveniente para las redes móviles ad-hoc, que permite el acceso a un canal de comunicación mediante la identificación de la ubicación del usuario y estableciendo una asignación uno a uno entre la división de ancho de banda de red y la ubicación espacial del móvil.[46] SDMA combinadas con las otras técnicas de acceso juegan un papel muy importante dentro de las comunicaciones móviles.

- **FHMA, Múltiple Acceso por Salto de Frecuencia**

Variación seudo aleatoria de la frecuencia portadora de envío del dispositivo móvil a la red, se basa la transmisión de señales de espectro ensanchado en el que la señal se emite sobre una serie de radiofrecuencias aparentemente aleatorias, saltando de frecuencia en frecuencia sincrónicamente con el transmisor.

Las señales en espectro ensanchado son altamente resistentes al ruido y a la interferencia, además son difíciles de interceptar. Una transmisión de este tipo suena como un ruido de corta duración, o como un incremento en el ruido en cualquier receptor, excepto para el que esté usando la secuencia que fue usada por el transmisor. Las transmisiones en espectro ensanchado pueden compartir una banda de frecuencia con muchos tipos de transmisiones convencionales con mínima interferencia. Sin embargo su principal desventaja es su bajo ancho de banda.

[46] FUENTE: http://it.toolbox.com/wiki/index.php/SDMA

3.2.4.3 Señalización

Además del uso de espectro para la realización de llamadas, GSM prevé que el terminal envíe y reciba datos para una serie de usos de señalización, como por ejemplo el registro inicial en la red al encender el terminal, la salida de la red al apagarlo, el canal en que va a establecerse la comunicación si entra o sale una llamada, la información del número de la llamada entrante, etc., además dispone que cada cierto tiempo el terminal avise a la red de que se encuentra encendido para optimizar el uso del espectro y no reservar capacidad para terminales apagados o fuera de cobertura.

Este uso del transmisor, se conoce como ráfagas de señalización, este ocupa muy poca capacidad de red y se utiliza también para enviar y recibir los mensajes cortos SMS sin necesidad de asignar un canal de radio. En ocasiones es sencillo escuchar una ráfaga de señalización si el teléfono se encuentra cerca de un aparato susceptible de captar interferencias, como un aparato de radio o televisión. [47] Los canales utilizados se encuentran detallados en la figura 3.10, siguiente:

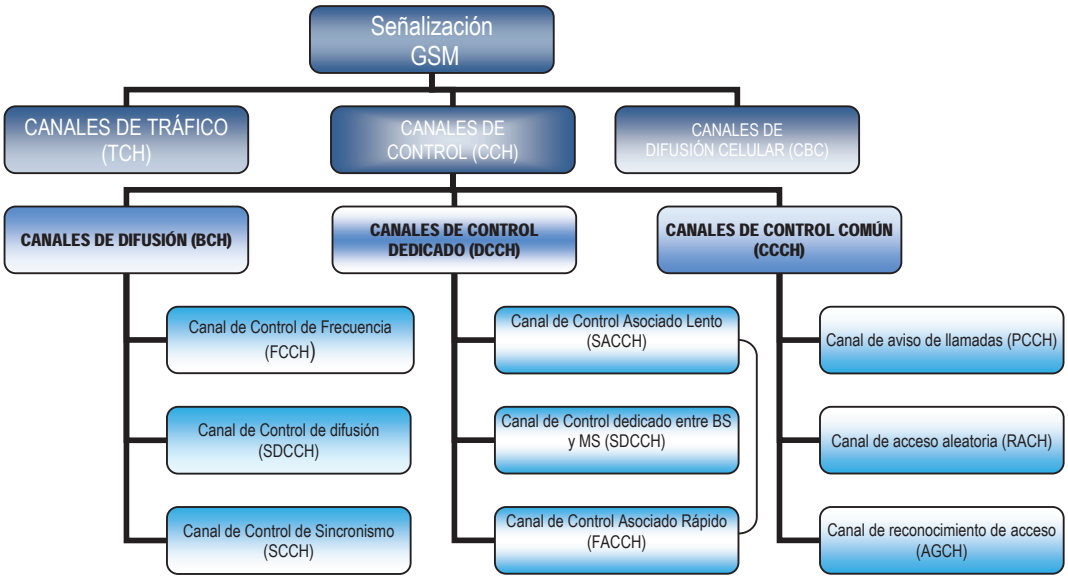


Figura 3.10 Canales de Señalización en GSM

[47] FUENTE: http://www.scribd.com/doc/39399415/SENALIZACION-GSM

* Los Canales de Control Asociados Lentos y Rápidos (SACCH y FACCH) se usan para supervisar las transmisiones de datos entre la estación móvil y la estación base durante una llamada.

3.2.4.4 Proceso para establecer una llamada

Cuando se enciende un teléfono celular, éste se engancha con una celda mediante un canal de control que envía sus datos a un VLR o un HLR, etc. Los canales monitores de control del teléfono, buscan a la señal más fuerte (aún cuando no se haga ninguna llamada). El teléfono celular (MS) se engancha al canal de control más fuerte. El número telefónico es ingresado. El teléfono se contacta con la MSC, a través de la red (BTS, BSC, etc.) la cual le asigna un canal para la conversación.

Después de la Inicialización, el teléfono entra en el modo de espera (idle). EL móvil responde al mensaje de búsqueda *(page)* enviado por el MSC. El MSC informa al teléfono del canal a ser usado para la conversación. EL teléfono se sintoniza a sí mismo a ese canal y completa la llamada.

3.2.5 HANDOVER EN GSM

Uno de los elementos clave de un teléfono móvil o un sistema móvil de telecomunicaciones, es que el sistema se divide en muchas celdas pequeñas para proporcionar una buena frecuencia de re-uso y cobertura. Sin embargo, como el dispositivo móvil se mueve fuera de una celda a otra, debe ser posible mantener la conexión. El handover es por lo tanto la transición de la transmisión de la señal de una estación base a una estación base geográficamente adyacente para cualquier usuario dado que se mueva alrededor.

En una red de telefonía celular ideal, se debería fijar siempre a cada usuario de un teléfono o un módem dentro del alcance de una estación base, es decir dentro de la región cubierta por cada estación base que se conoce como celda. El tamaño y la forma de cada célula en una red depende de la naturaleza del terreno en la región, el número de estaciones base, y la serie de transmisión / recepción de cada estación base. En teoría, las celdas en una red se superponen, porque la mayor parte del tiempo, el hardware de un abonado está dentro del alcance de

más de una estación base. La red debe decidir, de momento a momento, de que usuario se encargará cada estación base.

Cada vez que un abonado de telefonía móvil celular pasa de una celda a otra, la red cambia automáticamente la responsabilidad de cobertura de una estación base a otra. Cada transición de estación base, así como la secuencia de procesador de la conmutación en sí, se llama handover. En una red que funcione adecuadamente, los handover cambian suavemente, sin lagunas en las comunicaciones y sin confusión acerca de qué estación base debe tratar con el abonado. Para los usuarios de una red el proceso de handover es transparente.

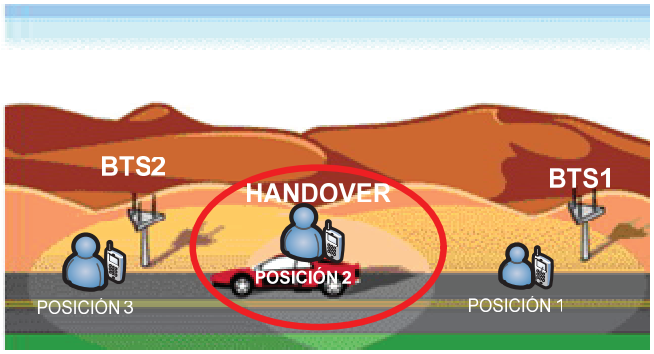


Figura 3.11 Proceso de Handover entre BTSs

El tipo de handover que se utiliza en GSM es del tipos duro, esto es que la entidad receptora deja de demodular y descodificar la información transmitida en un enlace y comienza a demodular y descodificar la información transmitida en otro enlace con posible pérdida de información. Se caracteriza por una desconexión temporal del canal de tráfico al cambiar el terminal de usuario de frecuencia. [48]

3.2.5.1 Tipos de Handover en GSM

Existen cuatro tipos de handover que se pueden realizar exclusivamente para el sistema GSM:

[48] FUENTE: http://www.upv.es/satelite/trabajos/pracGrupo3/handoff.htm

3.2.5.1.1 Handover Intra-BTS

Esta forma de Handover de GSM se produce cuando se requiere cambiar la frecuencia o la ranura que está utilizando un teléfono móvil debido a la interferencia, o por otras razones. En esta forma de handover, el dispositivo móvil permanece unida al receptor bajo la misma estación, pero cambia el canal o ranura.

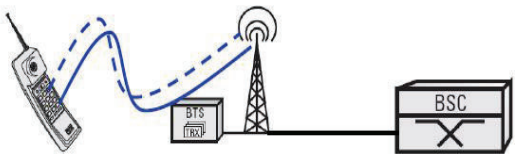


Figura 3.12 Handover Intra-BTS[49]

3.2.5.1.2 Handover Intra-BTS Inter BSC

Este tipo de handover se produce cuando el dispositivo móvil se mueve fuera del área de cobertura de una BTS, es decir pasa a otra BTS pero que está controlada por el mismo BSC. En este caso, el BSC es capaz de realizar el handover y le asigna un nuevo canal y la ranura para el móvil, antes de soltar la BTS antigua a la que estaba enganchada el dispositivo móvil.

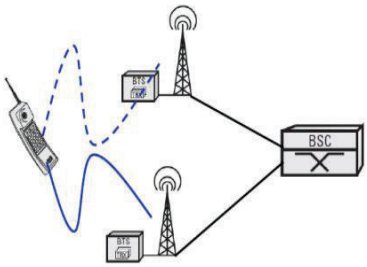


Figura 3.13 Handover Intra-BTS[50]

3.2.5.1.3 Handover Inter BSC

Cuando el dispositivo móvil se mueve fuera del rango de celdas controladas por una BSC, el handover que se debe realizar no es solamente de una BTS a otra sino de una BSC a otra, este proceso es controlado por el MSC.

---

[49] FUENTE: www.rohde-schwarz.com/WWW/Publicat.nsf/article/.../n180_cmu200.pdf
[50] FUENTE: www.rohde-schwarz.com/WWW/Publicat.nsf/article/.../n180_cmu200.pdf

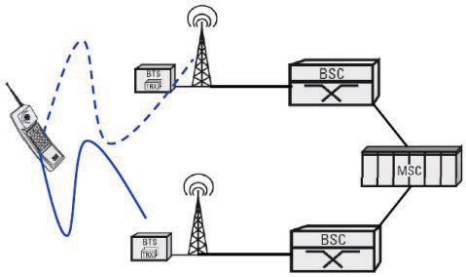


Figura 3.14 Handover Inter BSC [51]

3.2.5.1.4 Handover Inter MSC

Esta forma de handover cuando ocurre existe un cambio entre MSC´s (entre redes), en este caso las dos MSCs tienen que negociar quien controla el handover.

3.2.5.2 Proceso de handover en GSM

Aunque existen varias formas de handover en GSM, como se detalló anteriormente, respecto al dispositivo móvil son vistos de manera muy similar.

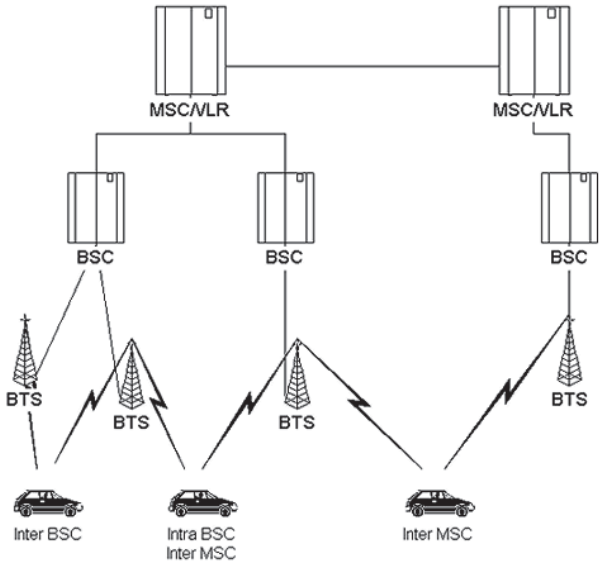


Figura 3.15 Ejemplo Típico de los Casos de handover[52]

[51] FUENTE: www.rohde-schwarz.com/WWW/Publicat.nsf/article/.../n180_cmu200.pdf
[52] FUENTE: http://server-die.alc.upv.es/asignaturas/LSED/2002-03/Redes_GSM/roaming.htm

Hay una serie de etapas involucradas en la realización de un handover de una celda a otra, o de una estación base a otra.

En GSM, que utiliza técnicas TDMA el transmisor sólo transmite por una ranura de ocho, y así mismo el receptor sólo recibe por una ranura en ocho. Como resultado de esto, la sección de radio frecuencia del dispositivo móvil podría estar inactiva durante 6 ranuras de un total de ocho, esto no sucede debido a que durante las ranuras de tiempo en las que no se está comunicando con la BTS, analiza los canales de radiofrecuencia para encontrar frecuencias de faro que podrían ser más fuerte o más apropiadas. Además de esto, cuando el dispositivo móvil se comunica con una BTS particular, una de las respuestas que hace es enviar una lista de los canales de radio, y las frecuencias de faro de la BTS vecinas a través de los canales de difusión (BCCH). El móvil analiza estos canales y emite informes de la calidad del nuevo enlace con la BTS. De esta manera el dispositivo móvil ayuda a la decisión de handover y, en consecuencia esta forma de entrega de GSM se conoce como asistencia del dispositivo móvil al handover (MAHO). [53]

La red sabe la calidad de la relación entre el dispositivo móvil y la BTS, así como la fuerza de la BTS local, de la que informó el dispositivo móvil. También se conoce la disponibilidad de canales en las celdas cercanas, con todo esto se obtiene toda la información que se necesita para poder tomar una decisión sobre si un dispositivo móvil requiere el handover de una BTS a otra. Si la red decide que es necesario para el dispositivo móvil un handover, le asigna una ranura de tiempo en un nuevo canal. Se informa a la BTS y al dispositivo móvil del cambio, y a continuación se sintonizan durante el período no está transmitiendo o recibiendo, es decir, en un período de inactividad.

Un elemento clave de la entrega GSM es el tiempo y la sincronización. Existe una serie de escenarios posibles que pueden ocurrir dependiendo del nivel de la sincronización.

[53] FUENTE: http://www.radio-electronics.com/info/cellulartelecomms/gsm_technical/handover-handoff.php

3.2.5.2.1 Sincronización de la anterior BTS a la nueva BTS

En este caso, la BTS obtiene detalles del nuevo canal físico en la celda vecina y se la entrega directamente sobre el móvil. El móvil, opcionalmente, puede transmitir cuatro ráfagas de acceso. Estos son ráfagas más cortas que las ráfagas estándar y por lo tanto efectos de sincronización pobre no causan superposición con otras ráfagas. Sin embargo, en este caso ya que la sincronización es buena, estas ráfagas sólo se utilizan para proporcionar un ajuste fino.

3.2.5.2.2 Desfase de tiempo entre la Sincronización de la anterior BTS a la nueva BTS

En algunos casos puede haber un desfase de tiempo entre la BTS anterior y la BTS nueva. En este caso, el tiempo de desplazamiento es proporcionado al móvil para que pueda realizar el ajuste. El tipo de handover que se realiza en este proceso es un handover estándar de sincronización.[54]

3.2.5.2.3 Handover no sincronizado

Cuando se lleva a cabo un traspaso de celdas no sincronizado, el móvil transmite 64 ráfagas de acceso al nuevo canal. Esto permite que la estación base pueda determinar y ajustar la sincronización para que el móvil puede acceder a la nueva BTS adecuadamente. Esto además permite que el móvil pueda volver a establecer la conexión a través de la nueva BTS con la sincronización correcta. [55]

3.2.5.3 Handover Inter-sistema

Con la evolución de las normas y la migración de GSM a otras tecnologías de 2G a 3G como UMTS / WCDMA, HSPA, entre otros, existe la necesidad de transferencia de una tecnología a otra. A menudo la cobertura GSM de 2G será mejor que la de los demás sistemas, y se utiliza como reserva. Cuando se requiere handover de esta naturaleza, es mucho más complicado que un simple

[54] FUENTE: http://www.radio-electronics.com/info/cellulartelecomms/gsm_technical/handover-handoff.php
[55] FUENTE: http://www.radio-electronics.com/info/cellulartelecomms/gsm_technical/handover-handoff.php

handover de GSM, ya que se pretende que dos sistemas técnicamente diferentes puedan manejar un handover.

Estos handover se pueden llamar handover Inter-sistemas o handover Inter-RAT ya que ocurre entre diferentes tecnologías de acceso de radio. La forma más común handovers Inter-sistemas se produce entre redes GSM y redes UMTS/WCDMA.

3.2.5.3.1 Handover de UMTS / WCDMA a GSM

Hay dos nuevas divisiones de esta categoría de handover:

- **Handover Blindado**

Esta forma de handover se produce cuando handover de la estación base a la que pertenece el móvil, pasa los detalles de la nueva celda para vincular el móvil a la misma y establecer la sincronización entre el móvil y la nueva celda.

En este modo la red selecciona la estación base de GSM que considera óptima. El móvil primero localiza el canal de difusión de la nueva celda, ganado tiempo de sincronización y a continuación lleva a cavo el handover entre celdas no sincronizado.[56]

- **Handover Comprimido**

Utilizando esta forma de handover, el móvil usa las lagunas de transmisión que se producen para analizar la recepción de las radio-bases locales de GSM, recurriendo a la lista de las radio bases vecinas para seleccionar a la estación base adecuada. Después de haber seleccionado una estación base adecuada el handover se lleva a cabo nuevamente sin que se haya producido ningún tipo de sincronización de tiempo.

[56] FUENTE: http://www.radio-electronics.com/info/cellulartelecomms/gsm_technical/handover-handoff.php

3.2.5.3.2 Handover de GSM a UMTS / WCDMA

Esta forma de handover es soportada por GSM, gracias a una lista de BS vecinas, está lista se creó para que sea mucho más sencilla esta operación. Como la red de GSM/2G es habitualmente mas extensa que la red 3G, este tipo de handover no ocurre cuando el móvil deja un área de cobertura y debe encontrar rápidamente una nueva estación base para mantener la comunicación, más bien el handover de GSM a UMTS ocurre para proporcionar una mejora en el rendimiento y, normalmente, sólo puede tener lugar cuando las condiciones son adecuadas. La lista de BS vecinas informará al móvil cuando esto puede ocurrir.[57]

3.2.6 DESCRIPCIÓN TEÓRICA DE LA SOLUCIÓN

Uno de los principales inconvenientes en la detección del by-pass a través de telefonía móvil GSM, es además de la movilidad que ofrece la tecnología, la variación de la frecuencia, lo que impide que se use de forma directa el sistema de radiogoniometría, por está razón para la ubicación de los dispositivos móviles utilizados en sistemas by-pass es necesario aplicar un método previo para fijar al dispositivo a una frecuencia conocida sin que el dispositivo lo note para no causar ningún tipo de alerta. Si esto se logra la detección de la ubicación de este dispositivo se puede realizar con el uso del sistema de radiogoniometría.

En los métodos convencionales, es muy común el establecer una llamada para obtener datos del dispositivo móvil que queremos encontrar, sin embargo el problema radica en que esta llamada podría alertar al usuario del dispositivo. Por lo que el primer aspecto de esta metodología proporciona un método de establecimiento de una llamada con un dispositivo de comunicación móvil, que comprende la transmisión de una petición de llamada al MS buscado sobre un lazo inalámbrico, en donde la petición de llamada es adaptada para que el MS transmita una señal de localización mientras se bloquea un proceso de gestión de conexión, que de otro modo haría que en el MS active una alerta de llamada visual o audible para el usuario.

---

[57] FUENTE: http://www.radio-electronics.com/info/cellulartelecomms/gsm_technical/handover-handoff.php

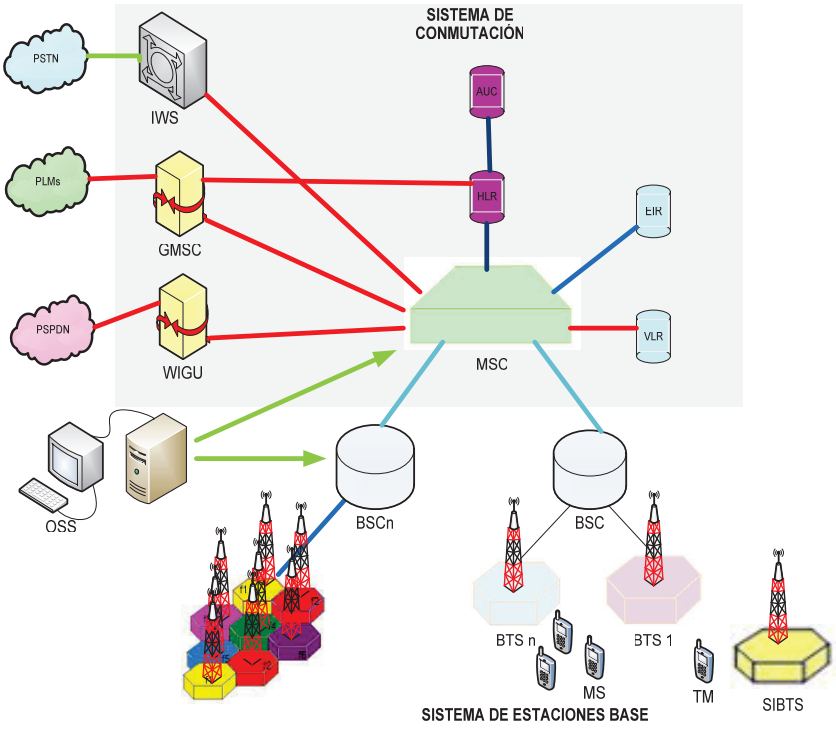


Figura 3.16 Diagrama General de introducción de SIBTS

Este primer paso permite establecer una "llamada ciega", es decir, una conexión de señalización con o sin el cambio de datos de usuario (ID), que no proporciona una alerta de llamada visual o audible al usuario del MS. Tal "llamada ciega" entonces puede ser utilizada para hallar la dirección o cualquier otro propósito deseado. En GSM, se aplica únicamente la autenticación del equipo de usuario con la red, permitiendo la posibilidad de evadir esa seguridad a través de una radiobase falsa agregada. La autenticación incompleta del MS inhibe el mecanismo convencional, permitiendo que se pueda convertir a un celular en una baliza de RF y que el equipo DF determine el LOB (Linea de Rumbo) de la baliza simulada en una frecuencia conocida. Esto se facilita porque el MS ignorará los mensajes, que no son de un terminal bien autenticado en la red que transporta sus transmisiones, y que son terminadas por las centrales del protocolo. El MS determina que la red que lo habla tiene los datos inexactos o perdidos de su protección de "Integridad", cuando es sometido por las especificaciones del protocolo.

3.2.6.1 Establecimiento de la llamada ciega

En la red GSM hay "n" radio bases BTS n que forman parte de la red GSM para comunicarse con un equipo móvil MS buscado. La radio-base insertada SIBTS obtiene los parámetros GSM desde un terminal de Prueba TM (Test Mobile), y realiza un subconjunto de funciones de una red GSM completa, como los protocolos de conmutación de la interfase inalámbrica en la central móvil de conmutación (MSC) y las funciones de seguridad y autenticación de los Registros Local y de Visitante HLR/VLR y del centro de Autenticación AUC.

La radio base insertada SIBTS tiene una memoria que almacena los datos de la identidad del abonado IMSI, la identidad temporal del abonado TMSI, y la identificación del equipo IMEI del móvil MS y de algunos otros MSs que la radio-base agregada SIBTS está por monitorear.

La IMSI se obtiene removiendo la tarjeta SIM del MS e insertándola en un lector comercial de tarjetas SIM; y la IMEI se obtiene marcando *#06# en el teclado de la MS. La IMSI y/o la IMEI pueden también ser obtenidas directamente del operador de la red móvil.

O también, con la radio-base agregada SIBTS, se puede interrogar al MS para adquirir sus datos (IMSI e IMEI), siguiendo el método de la Aplicación de Patente EP-A-1051043. El procedimiento se basa en los pasos de la tabla 3.3:

#	Procedimientos
1	La MS objetivo selecciona una radiobase (BTS 1).
2	La radiobase agregada SIBTS que está lo más cerca posible a dicho MS obtiene la lista BA (Broadcast Allocation) desde la BTS 1.
3	Se selecciona una radiobase (BTS n) de la lista BA, adyacente a la BTS 1.
4	La emite un código de área local (LAC) que difiere de los códigos LACs próximos a la MS. Así la MS transmite sus códigos IMSI e IMEI a la radiobase agregada SIBTS.
5	Y se opera la radiobase agregada SIBTS en la frecuencia del canal de control de broadcast (BCCH) de la BTS n a una potencia mayor que la de la BTS 1. Esto hace que el MS sea atendido por la radiobase SIBTS.

Tabla 3.3 Proceso para Introducir Una SIBTS

La radiobase SIBTS es típicamente un dispositivo móvil (simulador de radiobase) que puede ser instalado en un vehículo. Para su uso, la radiobase insertada SIBTS se puede mover en un área de interés, y sirve para adquirir parámetros de identidad de un conjunto de terminales MSs registrados en la red GSM de esa área. De forma alternativa la radiobase agregada SIBTS puede ser situada permanentemente en un área de interés. En ambos casos, la radiobase insertada SIBTS hace una transmisión falsa en celda que proporciona el alcance de la radiobase insertada que no está bajo el control de la red de GSM. Obteniendo el IMSI y el IMEI, es posible hacer que la MS transmita en una frecuencia específica de GSM como lo haría en una llamada normal de voz. Esto puede ser logrado usando los protocolos estándar de GSM, como en la infraestructura convencional de GSM. Transmitiendo la señal, puede utilizarse el sistema de radiogoniometría para determinar la dirección relativa de la MS. El sistema de radiogoniometría puede detectar la radiación emitida por el MS con un arreglo doppler de 8 antenas, y obtener la Dirección del móvil MS.

La radiobase agregada SIBTS hace que el MS inicie la transmisión sin que el usuario pueda percatarse de eso. Esto se conoce como una "llamada ciega". Una vez que la llamada ciega se ha establecido, el sistema de radiogoniometría puede determinar el LOB sin que el usuario conozca que está siendo localizado.

El establecimiento de una llamada ciega es ilustrado por el mecanismo mostrado en la Tabla 3.4. Está especificado en teoría con los mensajes de capa 2 y 3 de GSM intercambiados entre el BSS y la MS. Estos son mensajes convencionales como se menciona en la norma GSM 04.08: "Especificación de Capa 3 de la Interfase de Radio Móvil". Los mensajes vienen con un número variable de parámetros que son significativos, que podrían significar el primer inconveniente en este método.

#	Procedimientos	#	Procedimientos
1	RR Solicitud del canal (MS)	12	RR Reporte de Medición (MS)
2	RR Asignación Inmediata (BSS)	13	Información del Sistema Tipo [5 o 6]
3	RR Respuesta de Paginación (MS)	14	MM Solicitud de Identificación (BSS)
4	MM Solicitud de Autenticación (BSS)	15	MM Respuesta de Identificación (MS)
5	RR Reporte de Medición (MS)	16	MM Respuesta de Identificación (BSS)
6	Información del Sistema Tipo [5 o 6] (BSS)	17	MM Respuesta de Identificación (MS)
7	MM Respuesta de Autenticación (MS)	18	Información del sistema Tipo [5 o 6] (BSS)
8	RR Comando modo Cifrado (BSS)	19	RR Comando de Asignación (BSS)
9	RR Modo completo de Cifrado (MS)	20	RR Asignación Completa (MS)
10	MM Solicitud de Identificación (BSS)	21	Información del Sistema Tipo [5 o 6]
11	MM Respuesta de Identificación (MS)	22	Se repite la información del sistema y RR Medida de Soporte de Mensajes. Acción de la llamada ciega y establecimiento de un canal de liberación RR de la BSSS.

Tabla 3.4 Manipulación de Mensajes para realizar la llamada Ciega

3.2.6.2 Análisis de Involucrados

Los principales involucrados para la implementación de la radio-base insertada y el establecimiento de la llamada ciega con el objeto de ubicar un dispositivo móvil celular de tecnología GSM a través del sistema de radiogoniometría son: el Organismo técnico de Control, operadoras de telefonía móvil celular y el proveedor de los equipos de radiogoniometría.

3.2.6.2.1 Organismo de Control

Intereses	Problemas	Objetivos	Recursos y mandatos
Ubicar geográficamente un dispositivo móvil en una red GSM, para poder localizar sistemas de tráfico internacional no autorizados. Tener más y mejores herramientas que permitan combatir el by-pass implementado en líneas móviles celulares (tecnología GSM) Mejorar la gestión en cuanto al combate del fraude en telecomunicaciones. Poder hacer frente a ilícitos que han evolucionado junto con la tecnología como es el caso del by-pass a través de líneas móviles celulares (tecnología GSM)	Dificultar en el combate de sistemas by-pass implementados a través de líneas celulares móviles, tecnología GSM. Dificultad del sistema de radiogoniometría para detectar una frecuencia no constante en el tiempo. Dificultad en la identificación del canal de operación de un equipo móvil en una llamada en GSM. Poca cooperación e iniciativa dentro de algunos técnicos en las operadoras del servicio de telefonía móvil celular. Poca utilización de software libre y protocolos abiertos, en las operadoras y sus equipos. Exceso de confidencialidad técnica de las operadoras con el Organismo Técnico de Control. Dependencia de la estabilidad de la red de la operadora en la conexión del sistema de radiogoniometría.	Utilizar el sistema de radiogoniometría para la ubicación de un dispositivo móvil, tecnología GSM. Obtener un procedimiento para fijar la frecuencia de un dispositivo móvil para que pueda se ubicado por el sistema de radiogoniometría. Utilizar una SBITS para controlar el canal en el que opera una MS y evitar *frequency hopping*. Realizar charlas sobre la importancia de la cooperación y el trabajo coordinado en estas iniciativas. Desarrollar los protocolos y paquetes de software que sean necesarios para aplicar el sistema de radiogoniometría. Firmar un acuerdo de confidencialidad con las operadoras, en el manejo de su información.	R1: Técnicos capacitados. R2: Recursos económicos. R3: Instalaciones y equipos de mediciones. R4: Sistema de radiogoniometría. M1: Velar por la calidad de los servicios en las empresas de telecomunicaciones. M2: Cuidar los intereses de la ciudadanía.

Tabla 3.5 Análisis de Involucrado (Organismo Técnico de Control)

3.2.6.2.2 Operadora de Telefonía Móvil

Intereses	Problemas	Objetivos	Recursos y mandatos
Localización de un dispositivo móvil dentro de su red celular con fines investigativos. Tener más y mejores herramientas de control dentro de su sistema. Colaborar con l Organismo Técnico de Control en procedimientos de control y gestión del servicio.	Dificultad en la identificación del canal de operación de un equipo móvil en una llamada en GSM. Dificultad en la implementación de cambios dentro de su red de servicios. Pocos técnicos para que trabajen de forma directa y permanente con la Organismo Técnico de Control. Inviabilidad de alterar sus niveles de calidad y servicio según las normas y controles que establece la Organismo Técnico de Control. Escaso presupuesto para proyectos de manipulación de protocolos. Pocas de técnicas para controlar el orden de los mensajes GSM en las BSC.	Utilizar una SBITS para controlar el canal en el que opera una MS y evitar frequency hopping. Tener una planificación para realizar cambios en el sistema de la operadora (en una ventana de operación). Asignar un técnico que sea responsable de esta solución y que trabaje en una de las Operadoras de Telefonía Móvil. Acordar con el organismo técnico de Control, horarios determinados para pruebas para que los índices de calidad no se vean afectados. Cofinanciar la solución con las Operadoras de telefonía móvil. Desarrollar una técnica propietaria para el control de mensajes de GSM basada en software libre.	R1: Infraestructura de red celular. R2: Técnicos capacitados. R3: Núcleo de red celular con tecnología propietaria. M1: Brindar servicio celular de calidad y precio justo. M2: Apoyar a al Organismo Técnico de Control en las gestiones que sean necesarias para investigaciones y controles de calidad.

Tabla 3.6 Análisis de Involucrado (Operadora de Telefonía Móvil)

3.2.6.2.3 Proveedor del Equipo de Radiogoniometría

Intereses	Problemas	Objetivos	Recursos y mandatos
• Afianzar las relaciones entre el Organismo técnico de Control y el Proveedor de los equipos de radiogoniometría • Brindar asesoría técnica. • Dar soporte técnico en sus equipos.	• Dificultad para contactar a los fabricantes de los dispositivos. • Insuficiente experiencia en la implementación de la solución.	• Coordinar con las operadoras de telefonía móvil y los fabricantes de los dispositivos de red para proponer el acceso a sus protocolos. • Conseguir asesoría técnica de un ingeniero que conozca la forma de implementar una SIBTS sencilla.	• R1: R1: Personal técnico que conoce el funcionamiento y características de equipos de medición. • R2: Personal técnico que conoce y domina el manejo el radiogoniómetro. • M1: Cumplir las

Tabla 3.7 Análisis de Involucrado (Proveedor del Equipo de Radiogoniometría)

3.2.6.3 Marco Lógico de la Solución

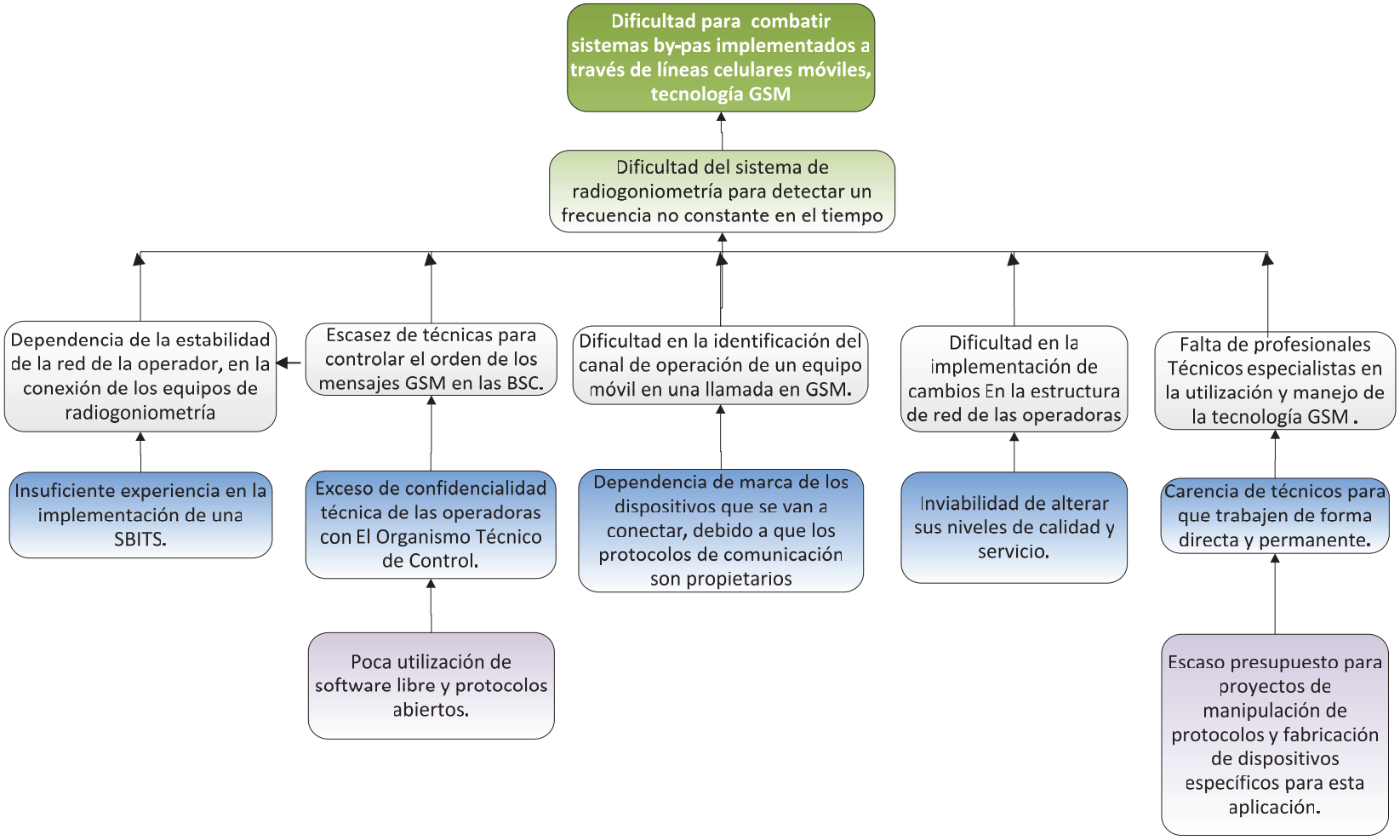


Figura 3.17 Árbol de Problemas de la Solución Planteada

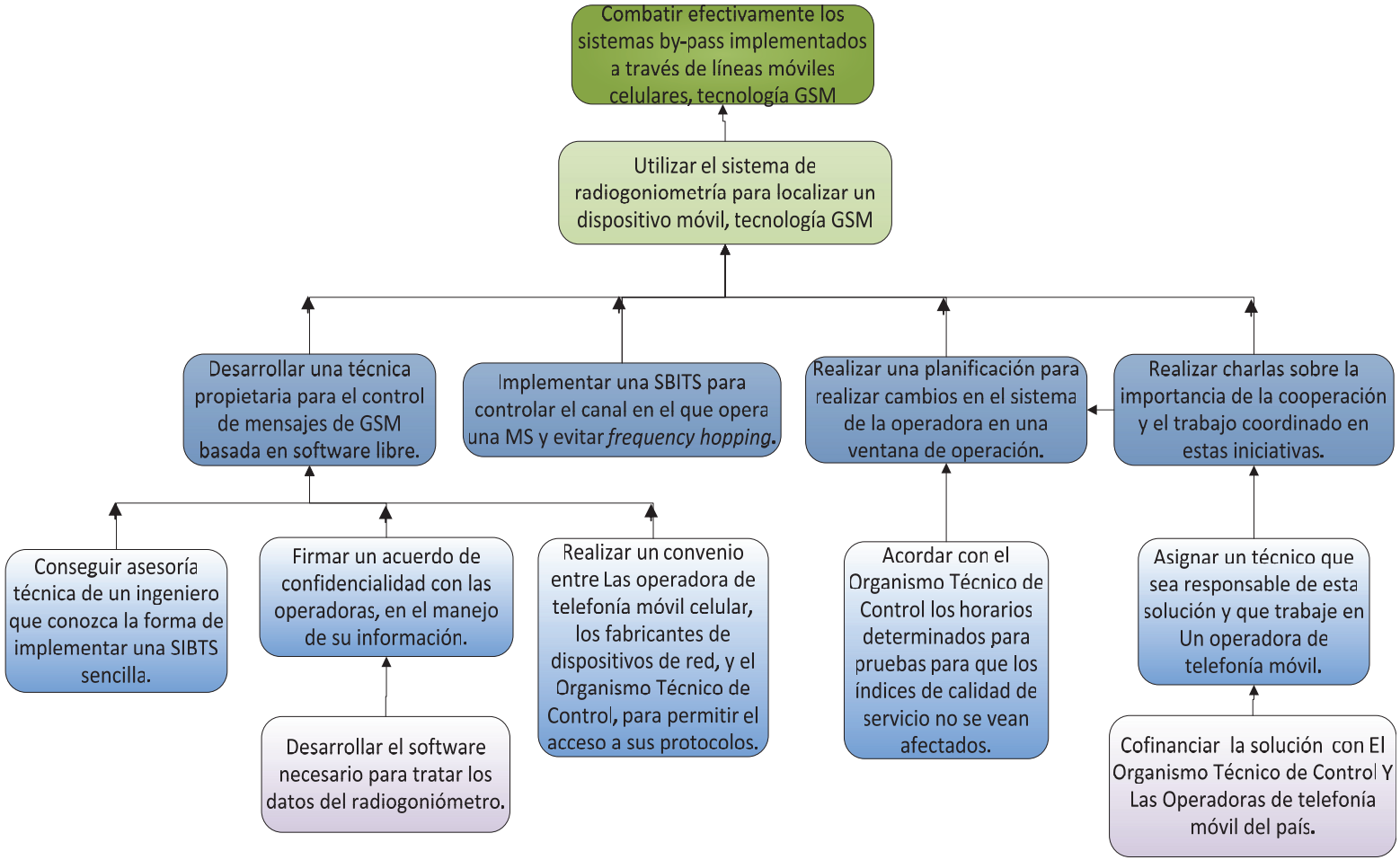


Figura 3.18 Árbol de Objetivos de la Solución Planteada

3.2.6.4 Mapa Conceptual

	Detalles	Indicadores	Verificadores	Supuestos
Fin	Combatir efectivamente los sistemas by-pass implementados a través de líneas móviles celulares.			
Propósito	Utilizar el sistema de radiogoniometría en la detección de dispositivos móviles celulares tecnología GSM	Con 3 pruebas de corta duración se determina la zona más probable donde se encuentra la MS buscada, aproximadamente en 30 minutos.	Mapa de la ciudad con la posible ubicación de la MS buscada.	Existe cooperación de las operadoras para realizar las pruebas.
Componentes	a) Desarrollar una técnica propietaria para el control de mensajes de GSM y operación de una SIBTS basada en software libre. b) Implementar una SBITS para manipular el funcionamiento de una MS en GSM y controlar en lo posible *frequency hopping*. c) Realizar una planificación para realizar cambios en el sistema de la operadora en una ventana de operación. d) Realizar charlas sobre la importancia de la cooperación y el trabajo coordinado en estas iniciativas.			c) Las operadoras se han preparado para realizar los ajustes necesarios en la ventana de operación. d) Los directivos de las operadoras participan en la capacitación del personal.

Continua ⟶

Actividades	a.1) Conseguir asesoría técnica de un especialista que conozca los protocolos y la forma de implementar una SIBTS sencilla. a.2) Firmar un acuerdo de confidencialidad con las operadoras, en el manejo de su información. **a.2.1) Desarrollar el software y hardware necesario para la implementación de la solución.** a.3) Realizar un convenio entre las operadoras de telefonía móvil, los fabricantes de dispositivos de red y el Organismo técnico de Control para permitir la cooperación en el acceso a protocolos, e infraestructura. c.1) Acordar con el Organismo Técnico de Control horarios determinados para pruebas, y evitar sanciones por los posibles bajos niveles de calidad que se puedan generar durante dichas pruebas. d.1) Asignar un técnico de Telefónica que sea responsable de esta solución y que trabaje en coordinación con el Organismo Técnico de Control. d.1.1) Cofinanciar la solución con el Organismo técnico de Control y las operadoras de telefonía móvil.	**a.1)** **a.2)** **a.2.1)** **a.3)** **c.1)** **d.1)** **d.1.1)**	a.1) Los fabricantes colaboran a través de asesoría con los técnicos. a.3) Las operadoras y las casas fabricantes acceden a compartir información y coordinar acciones. a.4) Los pagos y el financiamiento se realizan según lo acordado.

Tabla 3.8 Mapa Conceptual de la Implementación de la Solución

3.2.7 FACTIBILIDAD TÉCNICA

La solución tecnológica descrita teóricamente acoge el funcionamiento en GSM de una Radio Base Insertada Móvil (SIBTS), que tendrá la capacidad de registrar, al menos, un equipo terminal móvil y mantenerlo en una frecuencia determinada para proceder a utilizar el radiogoniómetro e identificar su ubicación.

Es necesario tener en cuenta que para el uso de este método de ubicación es indispensable la ejecución de una llamada ciega, que solo puede ser realizada si el equipo terminal se conecta a la red de la operadora a la que está asociado, por esto se requiere de un trabajo coordinado entre las operadoras y el Organismo Técnico de Control.

Existen tres posibles formas con las que se podría desarrollar la solución las cuales son: la implementación únicamente de la SIBTS, implementación de la SIBTS y la BSC, e implementación de una pequeña red celular independiente.

3.2.7.1 Formas de Implementación

3.2.7.1.1 Implementación de la SIBTS

La adquisición de una SIBTS (radio base insertada) que se conecte a una BSC de la operadora donde se realice la investigación.

En este caso la radio-base insertada necesita ser reconocida tanto por el dispositivo móvil así como por la BS que controla esa área de cobertura. Además deberá obtener los datos de los registros de la MSC, para poder encontrar al dispositivo móvil buscado.

Una vez que se logre la inserción de la radio base a la red de la operadora a la que pertenece el dispositivo móvil buscado, se realiza el proceso de la llamada, está implementación es básicamente la solución original planteada, sin embargo

debe superar algunas consideraciones prácticas observadas más adelante para poder ser llevada a la práctica.

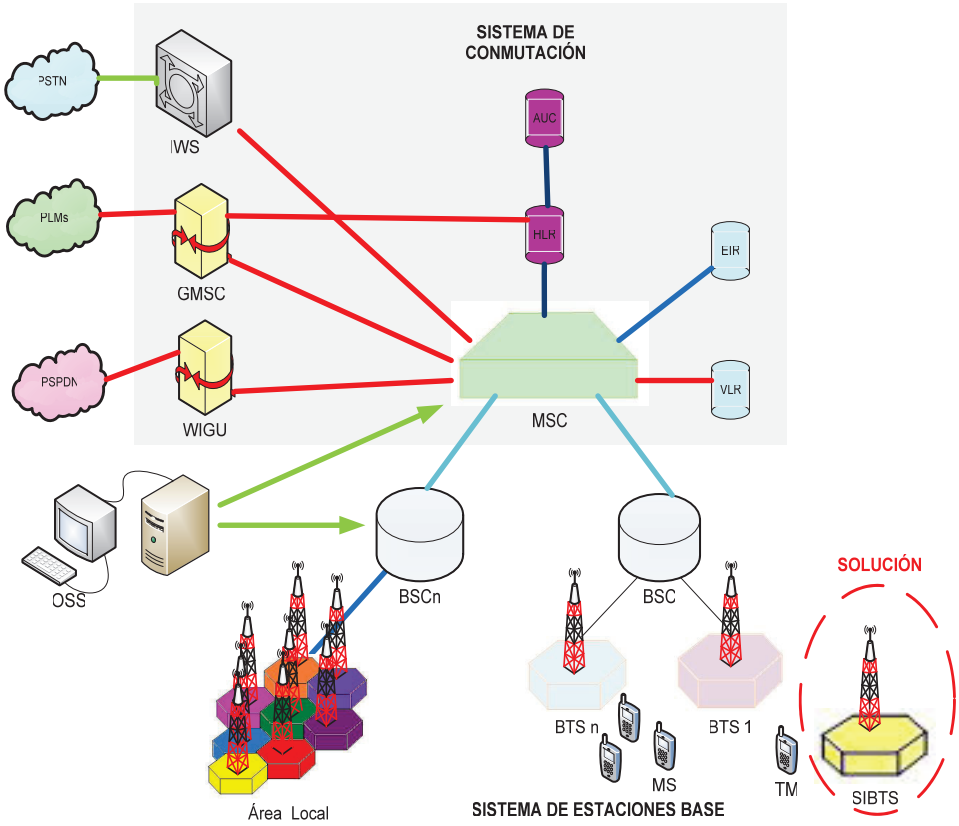


Figura 3.19 Implementación de la SIBTS

3.2.7.1.2 Implementación de la SIBTS y la BSC

La implementación de sistema que se conecte directamente a la MSC de la operadora (sin pasar por las BSC's) donde se realice la investigación. Esto significa que este pequeño sistema también tendrá una BSC independiente además de la SIBTS.

La inserción de la BSC a más de SIBTS, se realiza para evitar la configuración que se requiere al tratar de conseguir que la SIBTS sea reconocida por la BSC de la red de la operadora que controla las BTS de la zona donde se encuentra el dispositivo móvil en investigación, de está manera la BSC implementada se

conecta directamente a la MSC de la red, y se tiene un control directo del sistema sin depender de los elementos de red propios de la operadora.

Al igual que la primera propuesta este método de implementación debe superar algunos inconvenientes técnicos que ocurren en la práctica, y en caso de que esto suceda el procedimiento de la llamada ciega será muy similar a la anterior propuesta.

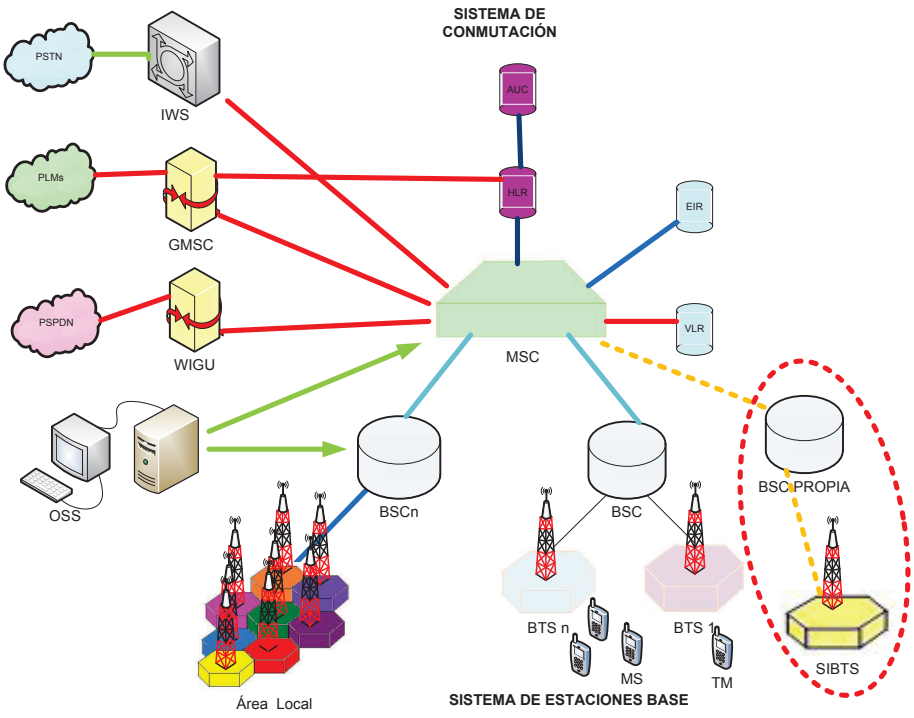


Figura 3.20 Implementación de la SIBTS + BSC

3.2.7.1.3 Implementación de una pequeña red celular independiente

Implementación de una pequeña red celular conformada por su propia MSC, su propia BSC y la SIBTS. Esta propuesta de implementación tiene por objeto evitar la dependencia técnica y administrativa con la Operadora de telefonía móvil puesto que los parámetros de configuración se manejarían de forma independiente y directa por parte del organismo técnico de control. Sin embargo para lograr que el dispositivo móvil se enganche a la SIBTS es necesario que la operadora proporcione la información de los registros del dispositivo móvil

además de que debe aparentar ser la red de la operadora a la que pertenece el MS, ya que en el proceso de autenticación el dispositivo móvil va a reconocer a la red de la operadora que le da originalmente el servicio.

Como ya se ha mencionado en los casos anteriores de implementación de la solución, el objetivo final es lograr que el dispositivo reconozca a la SIBTS y se puedan manipular los parámetros de comunicación para realizar el procedimiento de la llamada ciega y fijar al MS a una frecuencia que se podrá determinar a través del sistema de radiogoniometría.

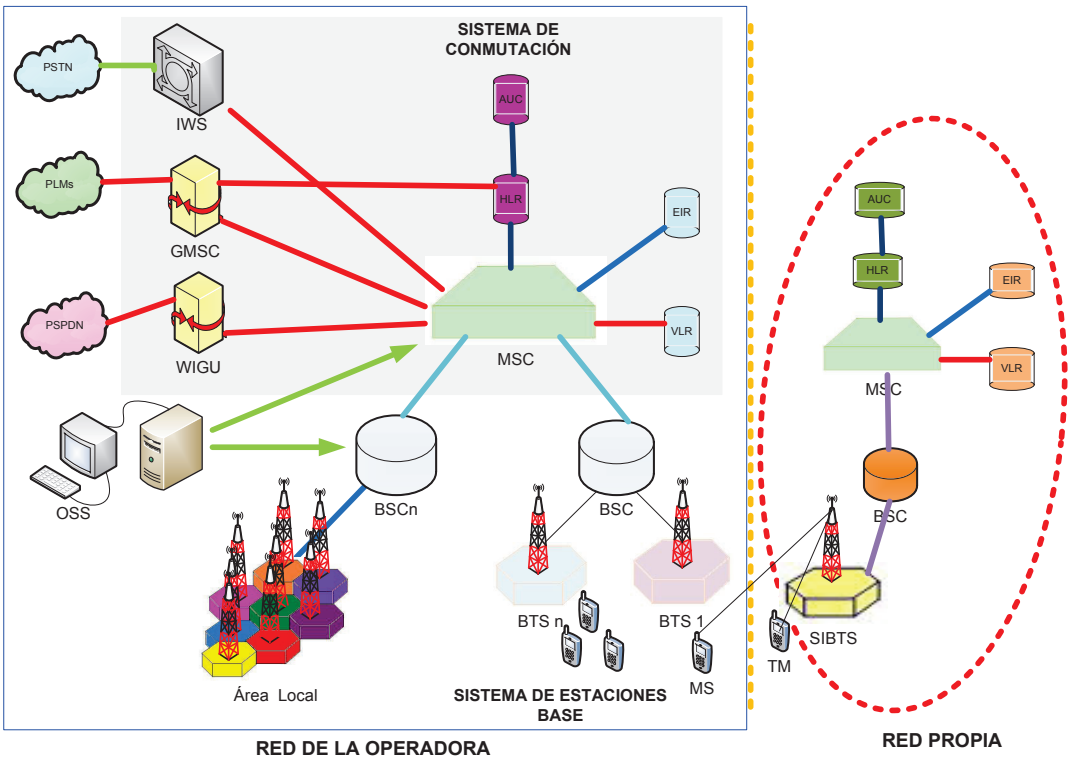


Figura 3.21 Implementación de una mini red Propia

3.2.7.1 Inconvenientes Técnicos

Las tres formas de implementación de la radio base insertada, para el establecimiento de la llamada ciega, deben superar algunos inconvenientes técnicos generales así como específicos para cada calos mismos que son:

- Dificultad para enganchar al equipo móvil buscado a las SIBTS, ya que estos se manejan a través de mensajes de señalización y Registro de Autentificación AuC, que permite que el dispositivo reconozca la operadora que le brinda el servicio y a su vez la operadora identifica si el dispositivo es el legítimo, cada prueba implicaría por tanto la utilización de estos registros para cargarlos al sistema en el caso de la mini red. Para el caso de la implementación de las SIBTS, o la implementación de la SIBTS más la BTS, se requiere que exista este vínculo entre los registros mencionados y los elementos implementos, estas configuraciones y parámetros se realizan a nivel de núcleo de red de la operadora, y afectan por tanto a todos los usuarios asignados a la Estación Base de la zona de prueba.

- Para lograr el enganche del dispositivo móvil a nuestra SIBTS en cualquiera de las tres formas posibles, es necesario que la operadora baje la potencia de las radio bases cercanas a la SIBTS, esto afecta a la calidad del servicio que deben cumplir las operadoras, es decir el resto de dispositivos móviles que se encuentren dentro de la cobertura de la SIBTS no contarían con servicio, por lo que se perturba no a un dispositivo móvil sino a todos los que se encuentren dentro del sector de la investigación.

- Cada BTS tiene un ID único, en base a este número ID único la MSC controla toda la actividad y tráfico en las BTS, para realizar el handoff o handover, como se explicó en los numerales anteriores el handover tiene diferentes escenarios y es un proceso fundamental para que la comunicación de los equipos no se vea afectada, este depende en la mayoría de ocasiones de la BS y de la MSC.

- Como el sistema debe permitir movilidad, ya que se requiere su uso en diferentes lugares del país, donde se realiza la investigación, esto implicaría una configuración del handover y los registros HLR, VLR para cada ocasión que se realicen las pruebas. La manipulación de la información de los registros que maneja la operación de los dispositivos móviles conectados a

la red, se maneja en la MSC esto conlleva a la alteración de una gran parte de la red.

- La comunicación entre la SIBTS y los demás elementos de la red GSM, se complica debido a que los equipos se comunican con protocolos propietarios que dependen del fabricante, estos protocolos no son manejados por la operadora, y se manejan de manera muy cuidadosa por el fabricante, lo que dificulta la modificación de los mismos. Además es importante menciona que existe incompatibilidad entre los protocolos de comunicación de elementos de red de diferentes fabricantes.

- El querer alterar el orden de los mensajes que maneja el protocolo GSM con el fin de realizar la llamada ciega, no resulta muy sencillo ya que estos mensajes son manejados a nivel de núcleo de red (MSC), y cambiar la configuración afectaría a todos los usuarios que se encuentran bajo esa parte de la red (MSC), en general las operadoras cuentan con 2 o 3 núcleos que controlan los usuarios de todo un país dependiendo el tamaño del mismo, esto implica que una configuración en la MSC para un dispositivo móvil específico afectan del 33% al 50% de usuarios de la red. Los mensajes de señalización que deben efectuarse para realizar la llamada ciega y no alarmar al implicado en el delito, no afecta solamente al dispositivo que está siendo usado por él, sino a todos los dispositivos manejados por la MSC.

- Es importante mencionar que para que el proceso de conexión del sistema de radiogoniometría no se vea afectado para esto se requiere que se trabaje con al menos con dos operadoras de telefonía móvil celular, la una para que soporte la conexión del sistema de radiogoniometría y la segunda será la operadora involucrada en caso de investigación.

3.2.8 FACTIBILIDAD ECONÓMICA

En función a los beneficios que conlleva el combate a los sistemas de telefonía internacional no autorizados, es posible considerar que la inversión económica que demanda este tipo de solución sean plenamente compasados por la disminución del perjuicio económico que estos sistemas causan tanto al estado como al operador autorizado del servicio, por tanto a pesar de las dificultades técnicas mencionadas en el numeral anterior, el siguiente análisis pretende recalcar la gestión y los esfuerzos por combatir este tipo de fraude.

3.2.8.1 Beneficios Económicos por el Combate al By-pass

En los últimos cinco años se ha realizado un combate fuerte a los sistemas de telefonía móvil no autorizados, esto ha contribuido a la disminución de las pérdidas económicas producidas por el mismo, lo que implica un beneficio económico bastante fuerte para el país.

De los datos obtenidos por la Superintendencia de Telecomunicaciones tenemos los montos estimados que se han dejado de perder en los últimos años por causa del combate a este tipo de delitos, estos datos se encuentran detallados en la tabla 3.9 a continuación:

INTERVENCIONES A SISTEMAS DE TELEFONÍA INTERNACIONA TIPO BY-PASS		
AÑO	CANTIDAD DE INTERVENCIONES REALIZADAS	MONTO ESTIMADO QUE SE EVITÓ PERDER POR ACCIONES REALIZADAS POR LA SUPERTEL
2005	13	3.486.033
2006	18	17.609.200
2007	15	8.801.691
2008	17	11.508.109
2009	26	11.646.597
2010	40	15.599.168

Tabla 3.9 Montos Estimados de lo que se evitó perder por el combate a los sistemas de telefonía Internacional tipo BY-PASS[58]

[58] FUENTE: Datos Confidenciales SUPERTEL

El beneficio económico no ocurre solamente para el país sino como es obvio para las diferentes operadoras de telefonía fija o móvil que cuentan con la autorización respectiva para dar el servicio de telefonía internacional.

La Superintendencia de Telecomunicaciones trabaja en conjunto con las operadoras de telefonía existentes en el país, para mitigar el fraude en telecomunicaciones producidos por sistemas de telefonía internacional no autorizado by-pass.

3.2.8.2 Costos de Implementación

En cualquiera de los casos, las soluciones propuestas tendrían que ser realizadas por un fabricante de infraestructura de redes de telefonía tecnología GSM, los principales fabricantes que brindan este tipo de soluciones tecnológicas son: Nokia, Siemens y Ericson.

Estas empresas coinciden en que cualquiera de las formas propuestas para la implementación de la solución sería muy costosa, además de tener un sin número de limitaciones técnicas que escapan de sus manos y que impiden cumplir el objetivo propuesto. Sin embargo se expusieron verbalmente valores estimados de la solución en caso de que esta supere los inconvenientes técnicos antes mencionados. [59]

Desarrollo e Implementación	*Costo Aproximado (USD)* *Fabricantes: Ericsson, Siemens, Nokia*
SIBTS (técnicamente descartada)	*400.000*
SIBTS + BSC (técnicamente descartada)	*900.000*
SIBTS + BSC + MSC	*1´200.000*

Tabla 3.10 Montos estimados proporcionados por los fabricantes[60]

[59] FUENTE: Datos técnicos obtenidos en reuniones con los principales fabricantes de elementos de telefonía móvil.
[60] FUENTE: Valores Estimados Fabricante Ericsson

3.2.8.3 Beneficios del Sistema

Los beneficios que presenta el sistema de detección son:

- Optimización del proceso de detección de un dispositivo móvil celular, logrando un combate efectivo contra el fraude por sistemas de tráfico internacional no autorizados (by-pass) implementados a través de líneas móviles celulares.

- Mayor flexibilidad y movilidad del sistema, características indispensables para poder encontrar la ubicación de una emisión clandestina.

- Mayor y mejor aprovechamiento de recursos tecnológicos, y disminución del tiempo de detección, ya que se podría determinar la posición de un dispositivo móvil en tiempo real

- Promover la coordinación y participación de todas las partes afectadas por los sistemas de tráfico internacional no autorizados (by-pass) implementados a través de líneas móviles celulares, es decir operadores, proveedores, organismo técnico de control.

3.2.8.4 Consideraciones

A pesar de los notables beneficios que brinda una herramienta que permita la detección de un dispositivo móvil para combatir los sistemas de telefonía internacional no autorizados es importante considerar que el costo del sistema correrá por cuenta del Organismo técnico de Control, por lo tanto al ser una inversión pública el sistema debe cumplir las especificaciones técnicas mencionadas para lograr el objetico final del mismo, estas especificaciones son dependientes de una serie de escenarios y factores que no se encuentran en manos de los fabricantes ni en manos del organismo técnico de control, por tanto aunque se pueda contar con el financiamientos es de vital importancia verificar la viabilidad de la solución.

Por tanto se debe mencionar que el uso del sistema queda supeditado a la tecnología GSM, ya que está basado en el funcionamiento de la red 2G y no es escalable a otras tecnologías de comunicación. Con el desarrollo de las tecnologías de comunicación móviles es substancial considerar la obtención de una herramienta que si bien esté orientada al combate de sistemas de telefonía internacional no autorizados implementados a través de líneas móviles celulares (tecnología GSM), permita la escalabilidad a otras tecnologías que van apareciendo ya que de no ser así esta herramienta tendría utilidad por un par de años, y este hecho no justifica la compra de la solución.

3.2.9 FACTIBILIDAD OPERATIVA

La operación de la implementación de la radio base insertada y establecimiento de la llamada ciega, depende como se ha visto en numerales anteriores de la colaboración directa de la operadora de telefonía móvil involucrada en el caso, así como la asistencia técnica permanente de lo fabricantes que realicen la solución, y de los proveedores de los equipos de radiogoniometría, esto quiere decir que el funcionamiento del sistema en cuestión está íntimamente ligado con la capacidad técnica del personal profesional encargado en la operación del sistema. La falta de profesional técnico especializado en el área de GSM, podría ser uno de los principales problemas al momento de utilizar el sistema.

La colaboración efectiva y oportuna de la operadora (operadora involucrada en el caso por sus líneas detectadas en un by-pass) al momento de entregar la información requerida para la configuración del sistema juega un papel muy importante, ya que el tiempo disponible para realizar las pruebas es muy corto (cuestión de minutos), y cada segundo que se pierda podría significar pérdidas económicas para la operadora además de el fallo de la prueba.

La conectividad de los equipos a través de la VPN, es un factor importante al momento de realizar las pruebas, ya que de esta depende que se puedan tomar las trazas y los puntos de triangulación para localizar al dispositivo móvil, es necesario por lo tanto que se cuente con el apoyo de otra operadora de telefonía

móvil celular a través de la cual se levante la VPN, de esta manera garantizamos que la conexión de los equipos no se vea afectada por la manipulación de los parámetros de red de la Operadora e involucrada en el caso. Por lo tanto es necesario que se trabaje simultáneamente con dos operadoras de telefonía móvil que cumplan los dos papeles en forma dual, es decir cuando una esté involucrada en un caso, la otra presta su red para levantar la VPN, y viceversa.

Si se consigue solucionar oportunamente los puntos mencionados anteriormente, la operación del sistema queda supeditada a la capacidad técnica del personal profesional encargado en la operación del sistema.

3.3 PRUEBAS NOCTURNAS PARA DETERMINAR LA UBICACIÓN DE MAYOR PROBABILIDAD DONDE SE ENCUENTRA EL DISPOSITIVO

3.3.1 OBJETIVO

El objetivo principal que persigue la realización de pruebas nocturnas es tener el menor número de interferencias de otros dispositivos móviles para poder utilizar el sistema de radiogoniometría y localizar la señal de telefonía móvil, tecnología GSM del dispositivo buscado.

3.3.2 IMPORTANCIA

Esta forma de determinar la ubicación de un dispositivo móvil es muy importante, ya que en el caso que no se pueda implementar las radiobase insertada y el establecimiento de la llamada ciega para poder fijar a una frecuencia al dispositivo buscado, esta metodología puede ser una alternativa que si bien sería bastante probabilística podría arrojar resultados válidos si tomamos en cuenta algunas consideraciones.

3.3.3 DESCRIPCIÓN

El método se ejecuta después de haber reducido la zona del by-pass a través de un drive test, descrito en la solución anterior.

La prueba consiste en realizar pruebas a altas horas de la noche, con el fin de evitar el tráfico telefónico que se produce por el uso normal del teléfono celular. Si el tráfico normal disminuye, la Operadora puede identificar el tráfico producido por el sistema by-pass que generalmente se encuentra en plena operación, además se puede conocer los canales de tráfico de voz (TCH) y los canales de difusión de control BCCH por los que se están realizando las llamadas. Conociendo estos datos también se pueden identificar las frecuencias que se están utilizando en la comunicación, al determinar las frecuencias de los canales podemos establecer una frecuencia de búsqueda en el sistema de radiogoniometría y empezar a monitorear el canal.

Las trazas que toman los equipos de radiogoniometría de la posición de la frecuencia, van a variar de un ángulo a otro debido a los saltos de frecuencia, pero van a empezar a coincidir en un área determinada, lo que nos ayuda a establecer una zona donde probablemente se encuentra el sistema de telefonía internacional no autorizado By-pass.

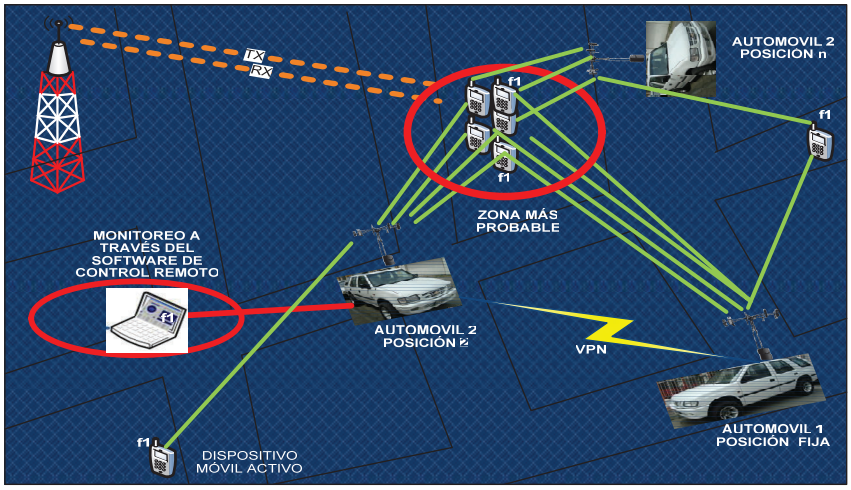


Figura 3.22 Ejemplo de realización de Pruebas Nocturnas

3.3.4 FACTIBILIDAD TÉCNICA

En cuanto a la parte técnica este procedimiento es totalmente realizable puesto que el sistema de radiogoniometría cuenta con la capacidad de monitorear la frecuencia en tiempo real, y situar las trazas en un mapa digital.

Esto permite hacer una valoración de las posiciones de la frecuencia que está detectando el sistema de radiogoniometría, además permite un post procesamiento para determinar la posición de mayor coincidencia en el mapa.
Para este procedimiento debemos contar con la colaboración únicamente de la operadora involucrada en la investigación, ya que está proporciona la información de las frecuencias y canales utilizados en la zona de investigación.

Para la realización de la prueba, se requiere que el sistema By-pass se encuentre en plena operación, por tal razón se escogen horas de la noche donde la demanda del el tráfico internacional aumenta considerablemente.

Los requerimientos de hardware para realizar el procedimiento, están detallados en la tabla 3.11.

Requerimientos de Hardware	
Cantidad	Equipos
2	Equipos de Radiogoniometría
2	Computadores
2	Módems ZTE

Tabla 3.11 Requerimientos de Hardware

Se debe indicar que los equipos mencionados en la tabla 3.11, han sido adquiridos por la SUPERTEL, para el mismo propósito.

Adicionalmente se debe tomar en cuenta los requerimientos de software detallados en la tabla 3.12.

Requerimientos de Software
Programa Emulador de Puertos Virtuales
Software de control Remoto del Radiogoniómetro

Tabla 3.12 Requerimientos de Software

A través de la conexión de los equipos de radiogoniometría que se describió en el Capítulo 2, se puede realizar este procedimiento.

La efectividad de este procedimiento está íntimamente ligada a las coincidencias de posición que se sitúen en el mapa el momento de la prueba, por esta razón las medidas deben tomarse en tiempo real, además la zona probable se obtiene luego de un post procesamiento.

3.3.5 FACTIBILIDAD ECONÓMICA

Debido a que el Organismo Técnico de Control cuenta con los recursos técnicos necesarios, para la ejecución de este tipo de procedimientos, no se requiere inversión adicional en hardware o software. Por tanto no existe un impedimento económico para aplicar esta herramienta.

Además se cuenta con el personal técnico capacitado para la operación del sistema lo que permite aprovechar y optimizar los recursos con los que cuenta la Institución, dándoles un uso adecuado y pertinente en beneficio del estado.

Esta herramienta además de no involucrar más recursos, permite combatir de manera más efectiva el fraude tipo By-pass implementados a través de líneas móviles celulares, ya que si bien no determina la posición de un dispositivo de manera exacta, se obtiene un área mucho más pequeña, con la que se puede realizar un análisis y encontrar la ubicación de la instalación.

3.3.6 FACTIBILIDAD OPERATIVA

La operatividad del sistema viene dado por dos factores importantes estos son:

- La coordinación entre el Organismo Técnico de Control y la operadora involucrada en la investigación.

- La capacidad técnica para operar y calibrar los equipos de radiogoniometría así como la conexión del sistema.

El primer punto, es manejable debido a que el Organismo Técnico de Control mantiene un Convenio de Cooperación Único con nueve operadoras de Telefonía en el país el mismo fue firmado el 25 de Noviembre del 2009[61], y su fin es poder gestionar acciones en contra del fraude en telecomunicaciones tipo By-pass, mejorar herramientas para el combate, y mantener una relación de cooperación constante entre todos los afectados por este tipo de delito.

En cuanto al segundo punto, la Superintendencia de Telecomunicaciones cuenta con un grupo de profesionales, con capacidades técnicas muy altas, esto permite que el proceso de realización de este tipo de pruebas pueda ser operado de manera correcta y efectiva.

[61] FUENTE: Superintendencia de Telecomunicaciones (DIE)

CAPÍTULO 4

PRUEBAS REALIZADAS, Y RESULTADOS

4.1 ERRORES EN EL RADIOGONIÓMETRO

4.1.1 ERRORES POR FACTORES EXTERNOS

Durante las operaciones de rutina del radiogoniómetro, el equipo DF proporcionará un rendimiento fiable en condiciones variables.

Hay varios factores que degradan el buscador de dirección del RG, como la capacidad de determinar con precisión la línea de rumbo (LOB) de la antena del DF a la antena del emisor. Es importante saber que estos factores degradarán el rendimiento del sistema de cualquier RG, algunos sistemas más que otros, algunos de los factores más que otros. Algunos de estos errores se encuentran en la tabla 4.1., la descripción de estos se errores se encuentra en el Anexo F.

ERRORES POR FACTORES EXTERNOS
Debidos a la polarización de la señal.
Debidos a la ruta de la señal.
Debidos a la ubicación del sitio.
Debidos a error de procesamiento instrumento DF.
Debidos a la fuente emisora.
Debidos a las plataformas móviles.
Debidos al mástil de montaje
Otras fuentes de error.

Tabla 4.1 Errores por Factores Externos

Hay que tener en cuenta que en la mayoría de los casos, rara vez hay sólo un error producido por un factor. Por otra parte, el error total es una combinación de cada uno de los factores de error individual.

4.1.2 ERRORES CALCULABLES DE LOS RESULTADOS

4.1.2.1 Error Pico

El Error Pico se encuentra tomando un número específico (n) de medidas de intervalos de azimut a una frecuencia específica y luego usando la medida de error más grande como la precisión de rumbo de la antena a esa frecuencia. Si este procedimiento se repite a otras frecuencias de interés el peor caso del error máximo se usa como el total.

El Error máximo se considera como una medida que afecta la precisión del rumbo medido, este tiene la desventaja de que a medida que el número de muestras de medición se incremente (es decir, aumento del el número de azimut de prueba y frecuencias de pruebas), el error máximo también se incrementa.

Esto es estadísticamente desde la perspectiva convergente, es decir que con una técnica de muestreo adecuado, un observador experimentado esperaría que un número mayor de muestras debiera traducirse en una convergencia de estimación de precisión de rumbo. Puesto que el error máximo es una estimación de los resultados divergentes, no es ampliamente utilizado.

4.1.2.2 Error Promedio

El error promedio se encuentra tomando un número de intervalos de azimut y frecuencias particulares, se suman las magnitudes (valores absolutos) de cada error y la suma se divide por el número de intervalos tomados.

Si este procedimiento se repite con otras frecuencias de interés, un promedio compuesto se podría calcular simplemente sumando el error medio para cada frecuencia y luego dividiendo este número por el número total de frecuencias de prueba. El Error Promedio no puede exceder nunca de error máximo y casi siempre es mucho menor en magnitud.

Aunque el error promedio es convergente (a diferencia de error pico como se se vio anteriormente) no es ampliamente usado como un error que tenga gran afectación a la precisión de rumbo.

4.1.2.3 Error RMS

Error RMS (error cuadrático medio) es el error de mayor consideración para la precisión del rumbo, por lo tanto el que más se utiliza en la industria de radiogoniometría.

Computacionalmente, se calcula por medio de la fórmula $\sqrt{(\Sigma\,\mathbf{E2/n})}$, como este proceso es menos directo que el cálculo de los errores pico o medio, en la Tabla 4.2 se muestra una comparación y cálculo de los errores, pico, promedio, RMS, realizados con unas muestras de una medición.

Azimut Medido	Azimut Conocido	Error del Rumbo (E)	E^2
000.0	000.0	0	0
022.5	020.5	-2	4
045.0	042.0	-3	9
067.5	065.5	-2	4
090.0	091.0	+1	1
112.5	113.5	+1	1
135.0	138.0	+3	9
157.5	159.5	+2	4
180.0	180.0	0	0
202.5	203.5	+1	1
225.0	224.0	-1	1
247.5	244.5	-3	9
270.0	268.0	-2	4
292.5	293.5	+1	1
315.0	317.0	+4	16
337.5	339.5	+4	16

Tabla 4.2 Ejemplo de tabulación de Mediciones

Con los datos tabulados procedemos a realizar el cálculo de errores; los valores de los mismos se encuentran en la tabla 4.3.

Cálculo	Valor
ΣE^2	80
Media ($\Sigma E^2/n$)	80/16 = 5.0
Error RMS $\sqrt{(\Sigma \mathbf{E2/n}}$	2.24°
Error pico	4° (determinados por inspección)
Error Promedio	$\|E\| / n$ = 1.88°
Error BIAS	$\Sigma_i^n{}_{=1} E /n$= 0.25°

Tabla 4.3 Ejemplo de Errores Calculables

Aunque el error RMS puede ser tan bajo como el error medio (cuando todas las magnitudes de error son los mismos), en el caso general, es mayor que el error medio. En el ejemplo anterior, el error promedio es de 1,88° en comparación con el error RMS de 2,24°. Debido a su amplia aceptación como un estándar de la industria y su corrección estadística, casi todos los equipos de radiogoniometría llevan la exactitud de rumbo expresada en términos del error RMS.

4.1.2.4 Error BIAS y recepción multi trayectoria

4.1.2.4.1 Definición

Aunque el error BIAS no puede catalogarse como un error de afectación de precisión de rumbo independiente, este es un concepto de medida de rumbo que es extremadamente importante, relevante e independiente de la técnica de medición seleccionada.

El Error BIAS puede ser pensado como un error por compensación (offset) que puede eliminarse (en principio) simplemente por la rotación física de la antena DF. Por ejemplo, si una antena de radiogoniometría presenta un error BIAS de 1 grado a una frecuencia de prueba determinada, este error puede ser eliminado por simple inspección de forma adecuada rotando 1 grado a la antena a fin de compensar el error BIAS. Una vez que esta nueva alineación mecánica se ha

logrado, una nueva prueba se realiza para confirmar que el error BIAS se ha eliminado (a pesar de que otros errores todavía se encuentran presentes).

4.1.2.4.2 Causas

Los errores BIAS en general pueden estar relacionados con el instrumento o inducidos por la recepción multi-trayectoria. El error BIAS relacionado con el instrumento se da por la insensibilidad a la frecuencia, mientras que el error BIAS inducido por las reflexiones tienden a ser altamente sensibles con recepción de la frecuencia. Fundamentalmente, los errores de rumbo en una antena de radiogoniometría se producen por la fase y aumento de desequilibrios causados por el circuito que subsecuentemente procesa el receptor de señales de la antena. A pesar del post-procesamiento, la señal de la antena en el receptor radiogoniómetro y el procesador de rumbo pueden así mismo inducir errores de rumbo.

Para propósitos analíticos y sin perder la generalidad se han agrupado los errores del receptor DF y el procesador de rumbo dentro de la antena de radiogoniometría y se asume que esta es ideal (libre de error) en un receptor y un procesador de rumbo. Las implicaciones de este resultado son extremadamente importantes. En concreto, la aparente ausencia de cualquier mecanismo por el cual se puede producir errores BIAS implica que cualquier error BIAS aparente que resulta en el transcurso de las pruebas de la antena del DF deben ser causadas por defectos del procedimiento o de recepción multi-trayectoria.

En efecto, computacionalmente puede "girar" la antena del radiogoniómetro ligeramente como se indicó anteriormente para compensar los efectos de la recepción multi-trayectoria, lo que permite una estimación de la precisión de rumbo que está virtualmente no contaminada por efectos multi-trayectoria. Se debe tener en cuenta que en general, en cada frecuencia será necesario un desplazamiento diferente de prueba, ya que hay varias rutas de errores de rumbo q tienden a ser altamente sensibles a la frecuencia.

4.2 PRUEBAS DEL SISTEMA

4.2.1 PRUEBAS DE HARDWARE

El sistema de radiogoniometría se conecta a través de una VPN, implementada en una red de telefonía móvil celular, por tanto su estabilidad está sujeta a una serie de parámetros de calidad propios de la red, sin embargo es necesario que se efectúen pruebas que verifiquen que esa estabilidad permite que los radiogoniómetros funcionen de forma correcta y que cumplan su objetivo final.

Estas pruebas consisten en su primera fase, en verificar la parte física de las conexiones, es decir que los cables seriales que conectan al computador con el radiogoniómetro no presente ninguna falla (tanto en el computador local, como el computador remoto), así mismo que los módems este colocados correctamente en los puertos USB habilitados del computador.

Figura 4.1 Conexiones en el Computador

Es importante verificar que el cable que transporta la señal de radiofrecuencia desde la antena al receptor radiogoniómetro se encuentre bien ajustado, y adicionalmente no se encuentre demasiado torcido, esto con el fin de evitar interferencias. De la misma manera se procede con el cable utilizado para las señales de control del procesador de señales.

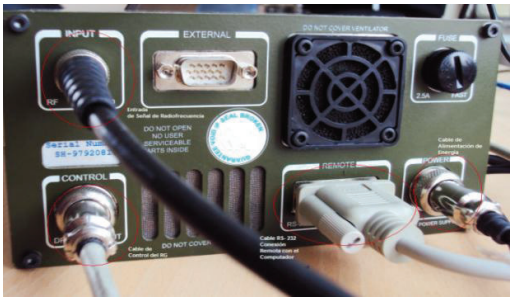


Figura 4.2 Conexiones en el Receptor Radiogoniometro

Es necesario, confirmar la posición correcta de los elementos de la antena así como su disposición y calibración.

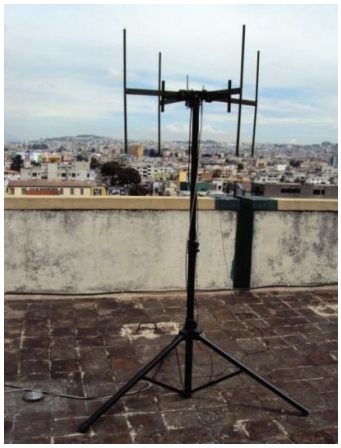


Figura 4.3 Instalación de la Antena y procesador de RG.

Además de verificar el estado de la conexión física es necesario también que se efectúe la calibración de equipo con mucha precisión, pues de este procedimiento dependerá la efectividad de la prueba.

El proceso de calibración del equipo de radiogoniometría se encuentra detallado en el Anexo F

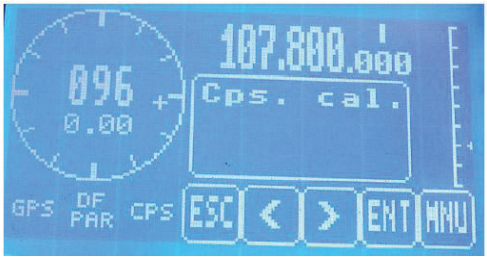


Figura 4.4 Modo Calibración[62]

[62] Fuente: Manual de Instalación y Mantenimiento de Equipo de Radiogoniometría ALMOS 3000

Luego debe comprobar que la VPN asignada está activada y se pueden transmitir datos de un computador a otro, esto se realiza mediante pruebas de ping entre los módems conectados a los computadores, después se requieren habilitar los puertos virtuales tantos de TCP/IP como seriales que se utilizan para interactuar con los equipos de radiogoniometría a través del software de control remoto. Si los puertos virtuales están correctamente configurados estamos listos para probar la conectividad de todo el sistema a través del encendido remoto de los equipos de radiogoniometría.

4.2.2 PRUEBAS DE CONECTIVIDAD

Como se indicó anteriormente la primera prueba que se debe realizar es de conectividad, es decir se debe verificar que los módems estén conectados a través de la VPN asignada por la Operadora de Telefonía Móvil. Esto se verifica a través de las pruebas de ping desde el computador local al computador remoto y viceversa.

Hay ocasiones en que solo responde el ping el computador local o solo el computador remoto, esto sucede generalmente por la configuración de los firewall y antivirus instalados en el computador, es necesario por tanto verificar que respondan los dos equipos a las pruebas de ping, ya que mientras esto no suceda, los demás elementos del sistema no se pueden comunicar.

Los chips de los módems con sus respectivas direcciones IP, se pueden colocar de forma indistinta ya sea en el computador local o en el computador remoto, es decir no deben permanecer de forma definitiva en uno u otro computador, sin embargo es necesario identificar qué dirección IP corresponde al radiogoniómetro local y que dirección IP corresponde al computador remoto, en el momento de la prueba, ya que la configuración de los puertos virtuales se la realiza en base a esta información. Una dirección IP, será asignada al servidor TCP, configurado en el computador local y otra IP se asignará al cliente TCP, configurado en el

computador remoto. La descripción de los procedimientos para configurar los puertos virtuales se encuentra detallada en el Anexo E.

A modo de ejemplo se realizan las pruebas indicando la asignación de direcciones IP utilizadas, para este caso.

EQUIPO	DIRECCIÓN IP
REMOTO	10.117.18.35
LOCAL	10.117.18.36

Tabla 4.4 Asignación de Direcciones IP

Si el equipo remoto se encuentra muy distante de la persona que va a realizar las pruebas, toda la configuración que puede ejecutar de forma remota habilitando la opción de escritorio remoto. El escritorio remoto es una herramienta que nos permite tener acceso al computador e interactúar con él como si estuviéramos manejandolo de forma directa cuando en realidad se encuentra físicamente en otro sitio, con lo que logramos disminución de personal técnico y optimización del tiempo.

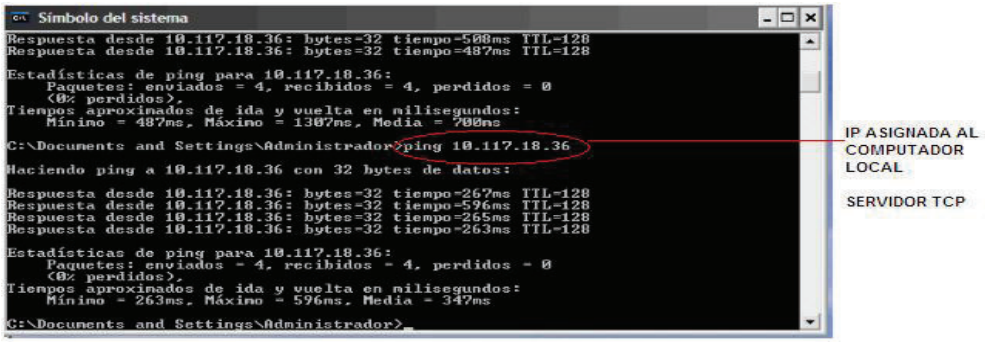


Figura 4.5 Prueba de ping desde el computador remoto al computador local

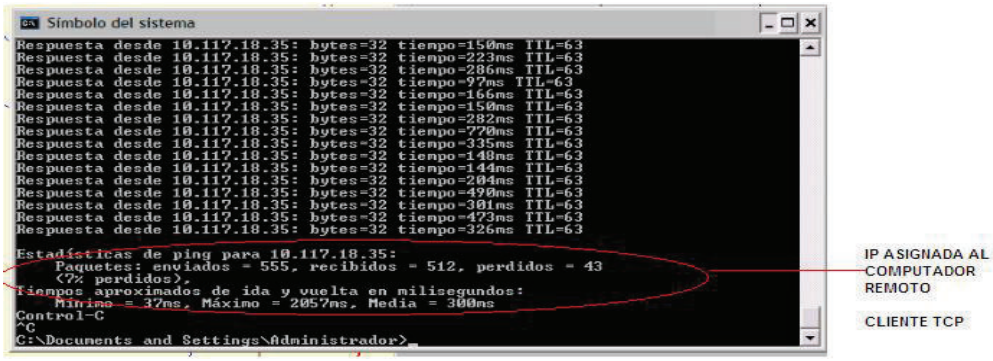


Figura 4.6 Prueba de ping desde el computador local al computador remoto

Una vez realizada las pruebas de ping, se procede a configurar los puertos virtuales y verificar que efectivamente estén habilitados, de no ser así aparecerá en pantalla un mensaje de error, que indicará el estado de la conexión.

Cuando la conexión es estable y se puede transmitir y recibir datos a través de los puertos virtuales creados, aparece en la pantalla del Emulador de puertos virtuales un mensaje de OK, esto indica que los puertos están habilitados y comunicados a través de la VPN. Para que no ocurran errores en la inicialización de puertos, es preferible configurar y habilitar el servidor TCP en el computador local y luego configurar y habilitar el cliente TCP en el computador remoto.

Si la conexión entre los módems se interrumpe por alguna razón, los puertos quedan inhabilitados y se activarán una vez que se restablezca la conexión. Sin embargo en ocasiones es necesario refrescar la configuración de los puertos apagando y encendiendo la simulación.

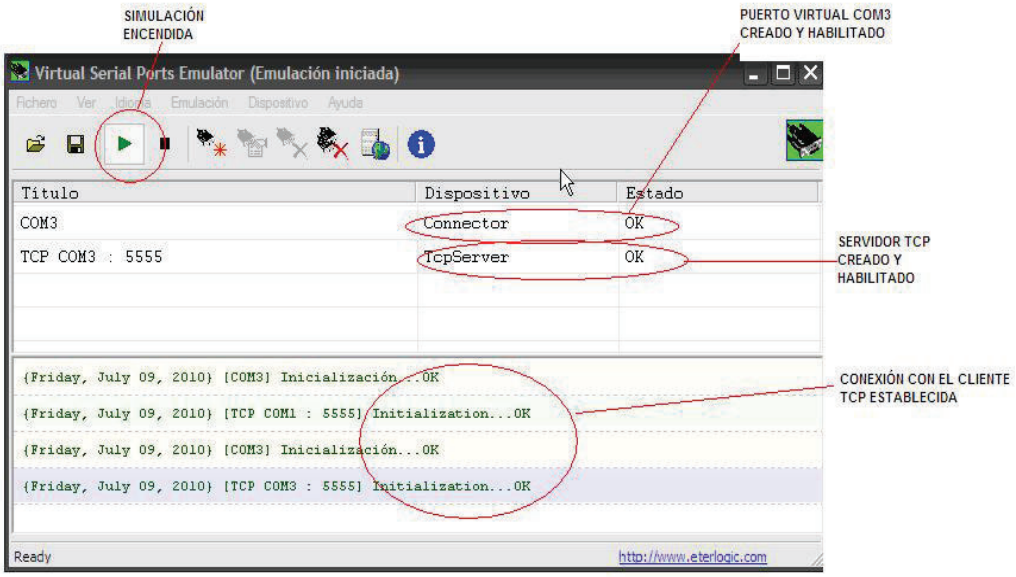


Figura 4.7 Configuración Puertos Virtuales Computador Local

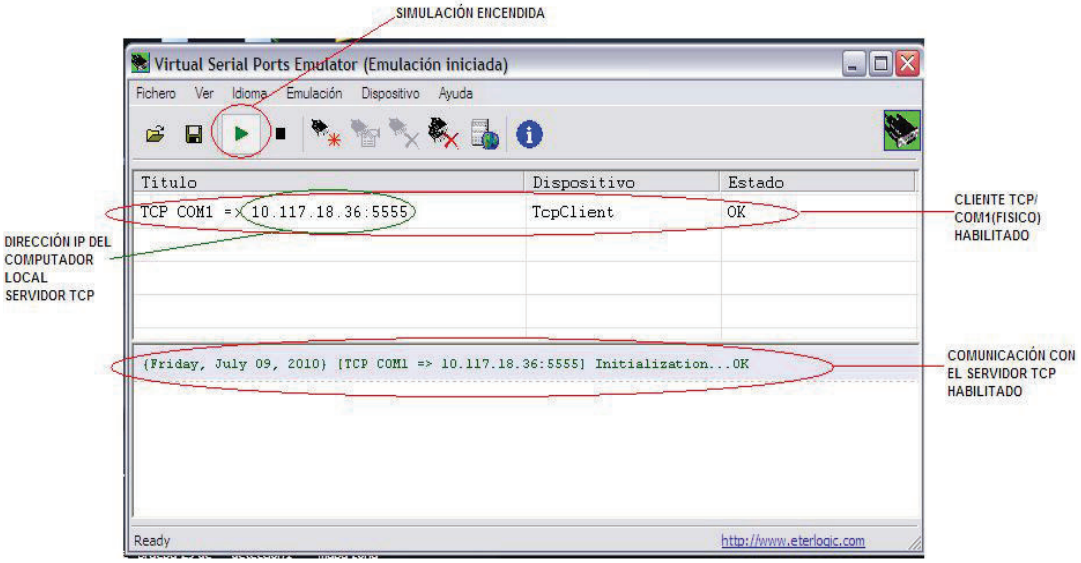


Figura 4.8 Configuración Puertos Virtuales Computador Remoto

Si los pasos anteriormente mencionados han sido realizados de forma correcta, los equipos de radiogoniometría van a estar en la capacidad de poder ser controlados remotamente desde un computador a través del software de control remoto. Para esto el equipo de radiogoniometría debe estar en el modo de conexión remota a través del puerto serial. El procedimiento para colocar al radiogoniómetro en modo conexión remota serial se detalla en el Anexo A[63].

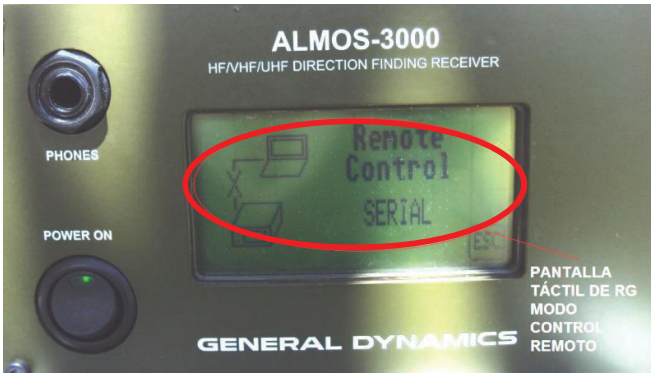


Figura 4.9 Radiogoniómetro en Modo control Remoto por puerto serial

Cuando los radiogoniómetros se encuentran en el modo remoto de conexión serial, se deshabilitan las opciones de la pantalla táctil para que el equipo se control a través de software.

[63] FUENTE: Manual de Usuario DF- ALMOS 3000, pág. 17

El software de control remoto nos da todas las opciones de manejo del radiogoniómetro como si estuviera de forma local, pero además permiten almacenar los datos obtenidos para realizar un pos procesamiento y poder tener mayor afinación en los resultados. Todos los parámetros configurables se encuentran descritos en el Anexo B.

Adicionalmente y lo más importante es que estas mediciones se pueden visualizar a través de un programa de mapas, que en este caso es MAPINFO, donde se trazan las líneas de rumbo medidas por cada radiogoniómetro y se efectúa la triangulación que determina la posición de la frecuencia buscada. Este proceso es de mucha utilidad en la búsqueda de emisores clandestinos ya que también proporciona la información de los puntos de intersección en latitud y longitud.

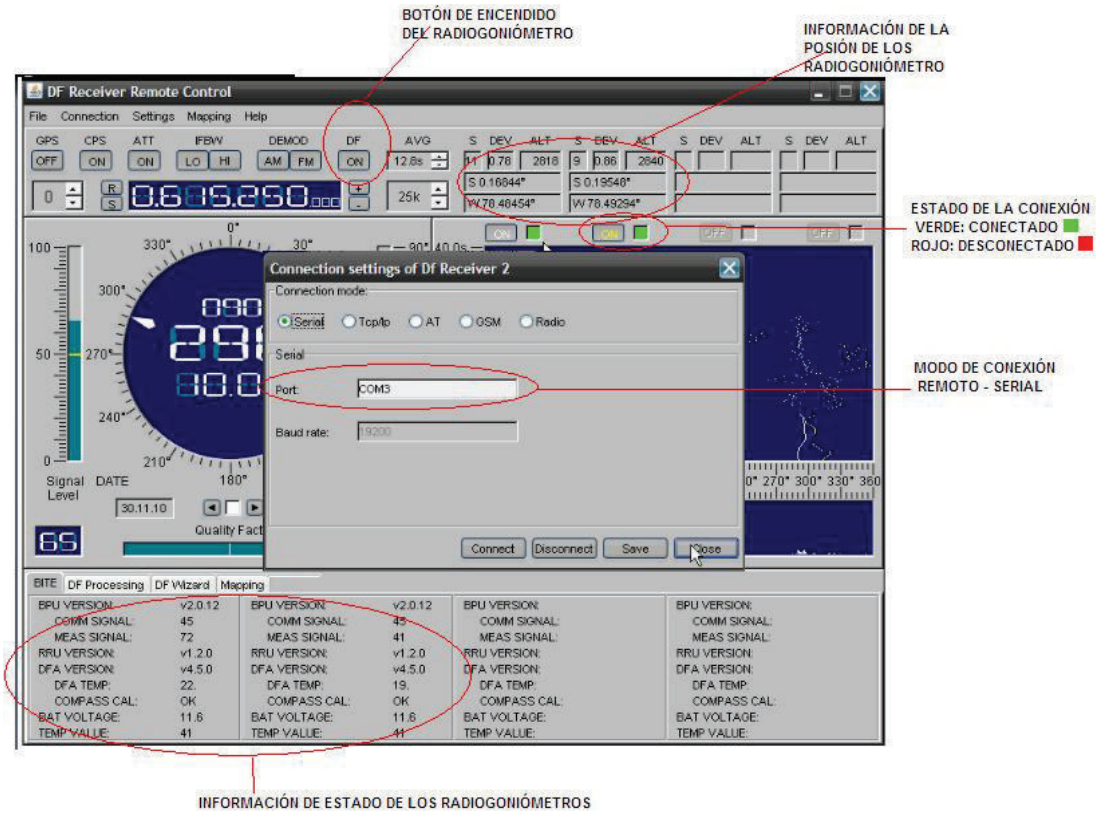


Figura 4.10 Encendido de los Radiogoniómetros en forma remota

4.2.3 PRUEBAS PARA DETERMINAR LA UBICACIÓN DE UN EMISOR A UNA FRECUENCIA FIJA EN BANDA UHF

Para localizar una frecuencia fija el uso del sistema de radiogoniometría es mucho más efectivo, puesto que la frecuencia se mantiene constante en el tiempo y la precisión de la medición está sujeta a dos factores: la potencia de la señal buscada y la calibración de los equipos. Además los equipos pueden ubicarse físicamente en una posición fija, en este caso las posiciones indicadas en la tabla 4.5, a continuación.

RADIOGONIOMETROS	POSICIÓN		
	DIRECCION	UBICACIÓN GEOGRÁFICA	
		LATITUD	LONGITUD
RG1	Edificio Intendencia Norte, Av. Amazonas N40-71 y Gaspar de Villaroel	S 0,16845	W 78,48452
RG2	Edificio Matriz SUPERTEL, Av. 9 de Octubre N70-25 y Berlín	S 0,19549	W 78,49292

Tabla 4.5 Posición de los Radiogoniómetros en las Pruebas

Para las pruebas presentadas se han escogido tres canales de televisión de la banda de UHF, el detalle de los canales de televisión escogidos se encuentran en la tabla 4.6 descrita a continuación.

			UBICACIÓN GEOGRÁFICA TX		
NOMBRE ESTACION	CANAL	FECRUENCIA (Mhz)	LONGITUD	LATITUD	POTENCIA VIDEO
TV+ (TEVEMAS)	33	585,25	78°30'59"W	00°10'08"S	5000
CANAL 42-UHF	42	639,25	78°31'11"W	00°09'52"S	5000
ECUADOR TV	48	675,25	78°31'28.4"W	00°10'07.4"S	80000

Tabla 4.6 Frecuencia y Ubicación de los transmisores buscados en las pruebas[64]

Con los datos proporcionados por la tabla 4.6, se realizan las pruebas, monitoreando en cada caso la frecuencia que queremos encontrar, cada

[64] FUENTE: Registro SUPERTEL, Dirección de Radio y TV.

frecuencia representa 1 prueba, y las mediciones que se obtengan serán comparadas con el dato real de la posición, para verificar la precisión de los equipos y calcular el valor del error.

4.2.3.1 Medición de Azimut

El azimut es es el ángulo horizontal medido en el sentido de las manecillas del reloj a partir de un meridiano de referencia[65], en nuestro caso el norte magnético. Como la medición del azimut depende del punto de referencia de donde se mida, en cada prueba se obtienen dos valores de azimut uno por cada radiogoniómetro, por tanto el cálculo de errores se realiza de forma independiente, comparando los valores medidos con valores de azimut de referencia. Los valores de azimut de referencia se presentan en la tabla 4.7 siguiente:

	AZIMUT	
CANAL	RG1 (°)	RG2 (°)
33	270,38	319,82
42	276,49	310,8
48	269,21	318,58

Tabla 4.7 Valores de Azimut (referencia)

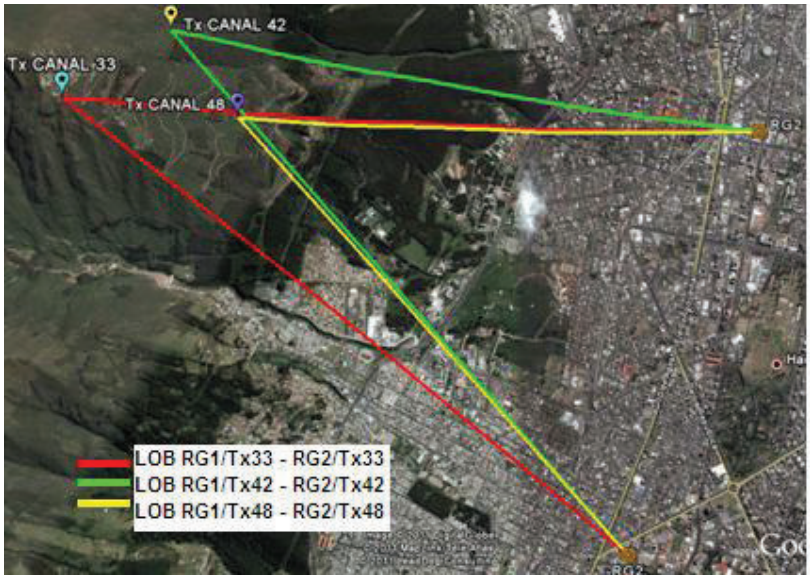


Figura 4.11 Presentación de la Ubicación de Tx y los RG en el Mapa

[65] FUENTE: http://doblevia.wordpress.com/2007/03/19/rumbo-y-azimut/

4.2.3.1.2 Resultados de las Pruebas efectuadas y Calculo de Errores

- Prueba 1: Canal 33/frec. 585,25 MHz

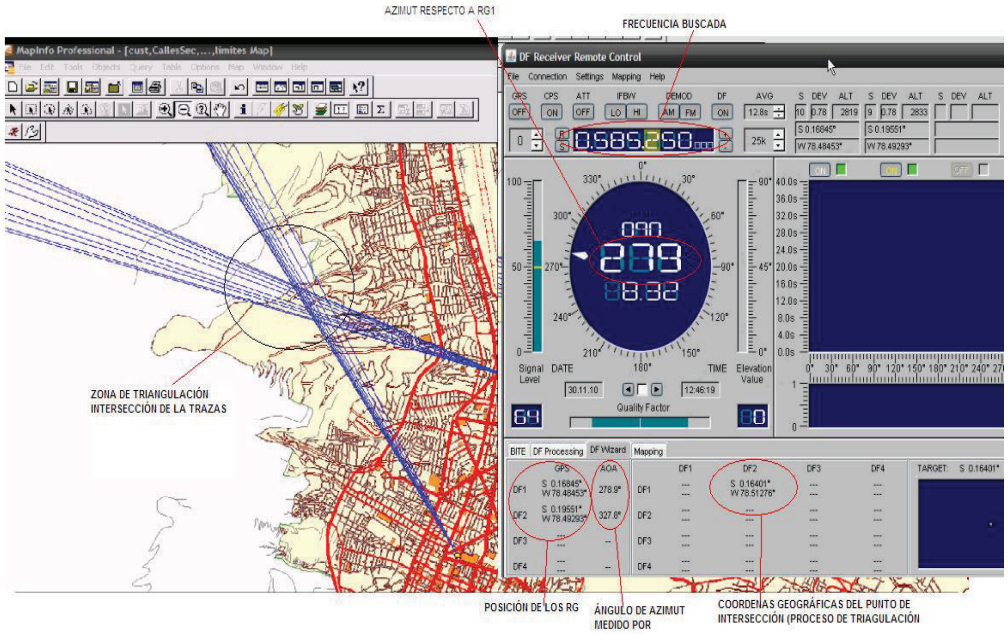


Figura 4.12 Proceso de Triangulación gráfico prueba 1 (Medición de la ubicación)

#	RADIOGONIÓMETRO 1				RADIOGONIÓMETRO 2			
	Azimut medido	Azimut Real	Error de Rumbo	E^2	Azimut medido	Azimut Real	Error de Rumbo	E^2
1	270,6	270,4	0,2	0,05	319,9	319,8	0,1	0,01
2	271,8	270,4	1,4	2,02	318,4	319,8	-1,4	2,02
3	278,9	270,4	8,5	72,59	327,8	319,8	8,0	63,68
4	269,1	270,4	-1,3	1,64	318,7	319,8	-1,1	1,25
5	269,9	270,4	-0,5	0,23	320,1	319,8	0,3	0,08
6	269,5	270,4	-0,9	0,77	320,3	319,8	0,5	0,23
7	271,3	270,4	0,9	0,85	321,4	319,8	1,6	2,50
8	270,8	270,4	0,4	0,18	319,6	319,8	-0,2	0,05
9	270,6	270,4	0,2	0,05	318,9	319,8	-0,9	0,85
10	272,4	270,4	2,0	4,08	319,3	319,8	-0,5	0,27
11	274,4	270,4	4,0	16,16	318,7	319,8	-1,1	1,25
12	267,7	270,4	-2,7	7,18	320,5	319,8	0,7	0,46
13	269,8	270,4	-0,6	0,34	317,8	319,8	-2,0	4,08
14	270,2	270,4	-0,2	0,03	319,7	319,8	-0,1	0,01
15	271,9	270,4	1,5	2,31	319,5	319,8	-0,3	0,10
16	270,3	270,4	-0,1	0,01	319,3	319,8	-0,5	0,27
17	269,8	270,4	-0,6	0,34	320,1	319,8	0,3	0,08
18	271,4	270,4	1,0	1,04	319,8	319,8	0,0	0,00
19	271,2	270,4	0,8	0,67	319,9	319,8	0,1	0,01
20	270,7	270,4	0,3	0,10	318,7	319,8	-1,1	1,25
	SUMATORIO		3,6	110,63			-4,2	78,45

Tabla 4.8 Medidas de Azimut respecto a RG1 y RG2

Una vez tabulados las mediciones se procede a realizar el cálculo de errores, para determinar la precisión del sistema.

	ERRORES CALCULADOS	
	RG1	RG2
MEDIA	5,53°	3,92°
RMS	2,35°	1,98°
ERROR PICO	8,5°	8°
ERROR PROMEDIO	1,4%	1,042%
ERROR BIAS	0,18%	-0,21%

Tabla 4.9 Errores de la medición del Azimut del RG1y RG2

El procesamiento de las dos pruebas restantes, tienen un tratamiento muy similar los resultados se presentan a continuación:

- Prueba 2: Canal 42/frec. 639,25 MHz

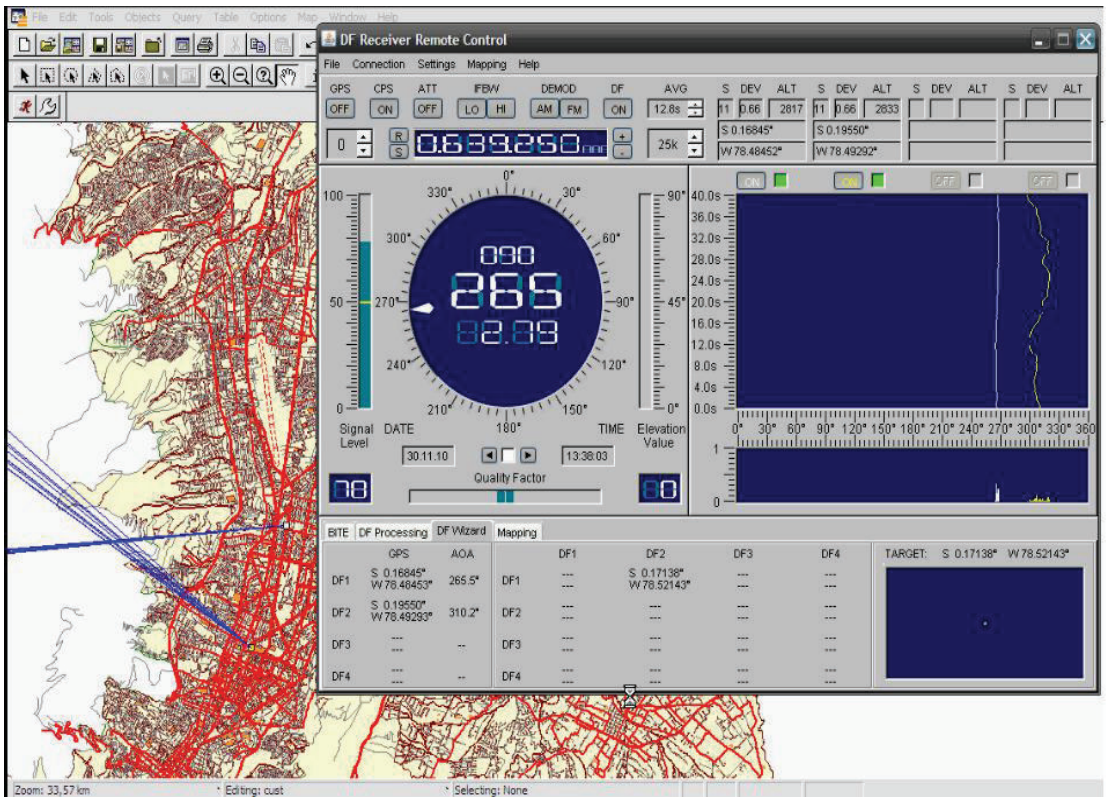


Figura 4.13 Proceso de Triangulación gráfico prueba 2 (Medición de la ubicación)

	RADIOGONIÓMETRO 1				RADIOGONIÓMETRO 2			
#	Azimut medido	Azimut Real	Error de Rumbo	E^2	Azimut medido	Azimut Real	Error de Rumbo	E^2
1	275,9	276,4	-0,5	0,25	311,3	310,8	0,5	0,25
2	277,1	276,4	0,7	0,49	310,9	310,8	0,1	0,01
3	276,3	276,4	-0,1	0,01	309,8	310,8	-1,0	1,00
4	276,2	276,4	-0,2	0,04	308,8	310,8	-2,0	4,00
5	265,5	276,4	-10,9	118,81	310,2	310,8	-0,6	0,36
6	276,9	276,4	0,5	0,25	310,5	310,8	-0,3	0,09
7	276,2	276,4	-0,2	0,04	310,9	310,8	0,1	0,01
8	280,1	276,4	3,7	13,69	310,8	310,8	0,0	0,00
9	270,6	276,4	-5,8	33,64	310,3	310,8	-0,5	0,25
10	276,5	276,4	0,1	0,01	310,1	310,8	-0,7	0,49
11	274,4	276,4	-2,0	4,00	312,3	310,8	1,5	2,25
12	277,7	276,4	1,3	1,69	311,8	310,8	1,0	1,00
13	279,8	276,4	3,4	11,56	311,1	310,8	0,3	0,09
14	277,2	276,4	0,8	0,64	309,7	310,8	-1,1	1,21
15	275,9	276,4	-0,5	0,25	310,4	310,8	-0,4	0,16
16	276,3	276,4	-0,1	0,01	310,7	310,8	-0,1	0,01
17	279,8	276,4	3,4	11,56	309,8	310,8	-1,0	1,00
18	276,4	276,4	0,0	0,00	310,8	310,8	0,0	0,00
19	276,2	276,4	-0,2	0,04	310,4	310,8	-0,4	0,16
20	276,7	276,4	0,3	0,09	310,3	310,8	-0,5	0,25
		SUMATORIO	6,4	197,07			-0,7	12,59

Tabla 4.10 Medidas de Azimut respecto a RG1 y RG2

	ERRORES CALCULADOS	
	RG1	RG2
MEDIA	9,85°	0,6295°
RMS	3,1390285°	0,7934104°
ERROR PICO	-10,9°	-2°
ERROR PROMEDIO	1,7%	0,605%
ERROR BIAS	0,32%	-0,035%

Tabla 4.11 Errores de la medición del Azimut del RG1y RG2

- Prueba 3: Canal 48/frec. 675,25 MHz

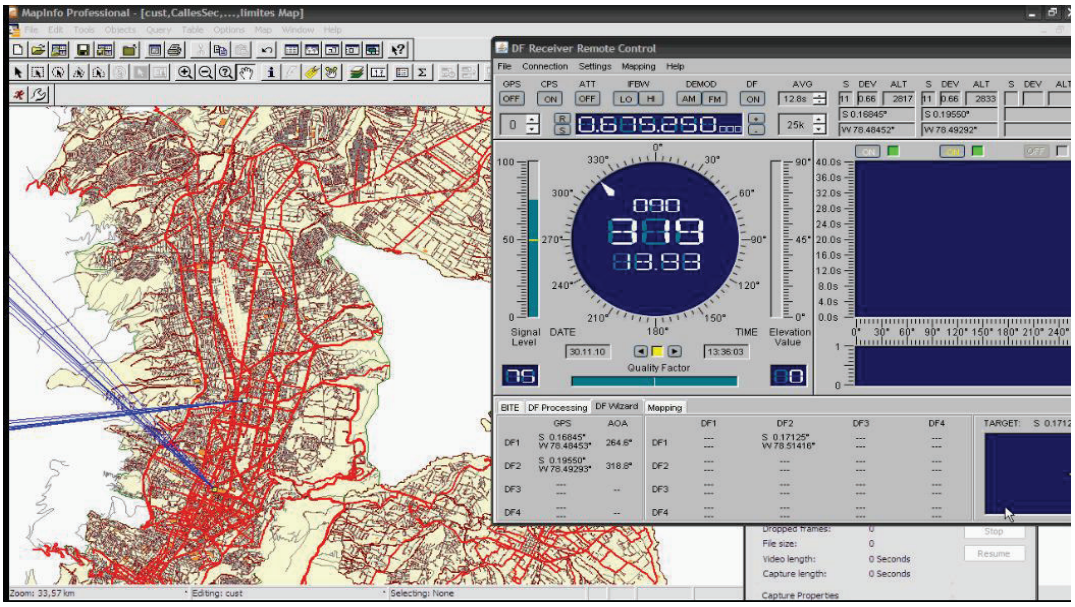


Figura 4.14 Proceso de Triangulación gráfico prueba 3 (Medición de la ubicación)

	RADIOGONIOMETRO 1				RADIOGONIOMETRO 2			
#	Azimut medido	Azimut Real	Error de Rumbo	E^2	Azimut medido	Azimut Real	Error de Rumbo	E^2
1	270,1	269,2	0,9	0,79	320,3	318,6	1,7	2,89
2	269,9	269,2	0,7	0,48	319,9	318,6	1,3	1,69
3	268,1	269,2	-1,1	1,23	319,8	318,6	1,2	1,44
4	269,3	269,2	0,1	0,01	318,8	318,6	0,2	0,04
5	269,2	269,2	0,0	0,00	320,2	318,6	1,6	2,56
6	270,3	269,2	1,1	1,19	318,5	318,6	-0,1	0,01
7	271,2	269,2	2,0	3,96	319,9	318,6	1,3	1,69
8	268,9	269,2	-0,3	0,10	318,8	318,6	0,2	0,04
9	268,6	269,2	-0,6	0,37	320,3	318,6	1,7	2,89
10	267,4	269,2	-1,8	3,28	318,1	318,6	-0,5	0,25
11	271,2	269,2	2,0	3,96	317,3	318,6	-1,3	1,69
12	270,8	269,2	1,6	2,53	321,8	318,6	3,2	10,24
13	270,3	269,2	1,1	1,19	318,1	318,6	-0,5	0,25
14	269,1	269,2	-0,1	0,01	319,7	318,6	1,1	1,21
15	264,6	269,2	-4,6	21,25	318,8	318,6	0,2	0,04
16	269,7	269,2	0,5	0,24	318,7	318,6	0,1	0,01
17	269,2	269,2	0,0	0,00	318,8	318,6	0,2	0,04
18	268,8	269,2	-0,4	0,17	319,8	318,6	1,2	1,44
19	269,7	269,2	0,5	0,24	320,4	318,6	1,8	3,24
20	270,1	269,2	0,9	0,79	319,3	318,6	0,7	0,49
		SUMATORIO	1,4	41,78			6,7	32,15

Tabla 4.12 Medidas de Azimut respecto a RG1 y RG2

	ERRORES CALCULADOS	
	RG1	RG2
MEDIA	2,09°	1,6075°
RMS	1,4453719°	1,26787223°
ERROR PICO	-4,6°	3,2°
ERROR PROMEDIO	1,0%	-0,055%
ERROR BIAS	0,07%	1,005%

Tabla 4.13 Errores de la mediciones del Azimut por RG1 y RG2

4.2.3.2 Proceso de triangulación

Las pruebas del sistema de radiogoniometría convergen en la ubicación del punto de intersección de las trazas de LOB (línea de rumbo) de cada radiogoniómetro, este proceso se conoce como triangulación de señales, se puede realizar de forma manual ubicando en un mapa las coordenadas de la posición de cada radiogoniómetro y la medida del ángulo azimut que cada uno ha determinado.

Al igual que el ángulo de azimut, este proceso se puede ejecutar mediante la triangulación de las dos señales en tiempo real por medio del software de control remoto. Los datos obtenidos en este proceso se pueden tabular y considerar en el cálculo de errores.

	UBICACIÓN GEOGRÁFICA			
CANAL	LATITUD (°)		LONGITUD (°)	
33	S	0,1688889	W	78,516389
42	S	0,1644444	W	78,519722
48	S	0,1687222	W	78,524556

Tabla 4.14 Posición de los Canales de TV buscados

4.2.3.2.1 Resultados

Los resultados se encuentran expresados en tablas con los datos de las mediciones realizadas en diferentes pruebas.

	FRECUENCIA DE BÚSQUEDA 585,25 MHz							
	Posición Medida		Posición de Referencia		Error		Error2	
#	Latitud	Longitud	Latitud	Longitud	Latitud	Longitud	Latitud	Longitud
1	S 0,16884	W 78,51654	S 0,16889	W 78,51639	S 0,000049	W -0,000150	S 0,000000002401	W 0,0000000225
2	S 0,16798	W 78,51432	S 0,16889	W 78,51639	S 0,000909	W 0,002070	S 0,000000826281	W 0,0000042849
3	S 0,16988	W 78,51437	S 0,16889	W 78,51639	S -0,000991	W 0,002020	S 0,000000982081	W 0,0000040804
4	S 0,16823	W 78,51789	S 0,16889	W 78,51639	S 0,000659	W -0,001500	S 0,000000434281	W 0,0000022500
5	S 0,16972	W 78,51987	S 0,16889	W 78,51639	S -0,000831	W -0,003480	S 0,000000690561	W 0,0000121104
6	S 0,16885	W 78,51498	S 0,16889	W 78,51639	S 0,000039	W 0,001410	S 0,000000001521	W 0,0000019881
7	S 0,16887	W 78,51633	S 0,16889	W 78,51639	S 0,000019	W 0,000060	S 0,000000000361	W 0,0000000036
8	S 0,16965	W 78,51637	S 0,16889	W 78,51639	S -0,000761	W 0,000020	S 0,000000579121	W 0,0000000004
9	S 0,16865	W 78,51641	S 0,16889	W 78,51639	S 0,000239	W -0,000020	S 0,000000057121	W 0,0000000004
10	S 0,16401	W 78,51276	S 0,16889	W 78,51639	S 0,004879	W 0,003630	S 0,000023804641	W 0,0000131769
11	S 0,16883	W 78,51639	S 0,16889	W 78,51639	S 0,000059	W 0,000000	S 0,000000003481	W 0,0000000000
12	S 0,16987	W 78,51678	S 0,16889	W 78,51639	S -0,000981	W -0,000390	S 0,000000962361	W 0,0000001521
13	S 0,16884	W 78,51965	S 0,16889	W 78,51639	S 0,000049	W -0,003260	S 0,000000002401	W 0,0000106276
14	S 0,16886	W 78,51876	S 0,16889	W 78,51639	S 0,000029	W -0,002370	S 0,000000000841	W 0,0000056169
15	S 0,16868	W 78,51976	S 0,16889	W 78,51639	S 0,000209	W -0,003370	S 0,000000043681	W 0,0000113569
16	S 0,16785	W 78,51864	S 0,16889	W 78,51639	S 0,001039	W -0,002250	S 0,000001079521	W 0,0000050625
17	S 0,16978	W 78,51439	S 0,16889	W 78,51639	S -0,000891	W 0,002000	S 0,000000793881	W 0,0000040000
18	S 0,16885	W 78,51869	S 0,16889	W 78,51639	S 0,000039	W -0,002300	S 0,000000001521	W 0,0000052900
19	S 0,16887	W 78,51636	S 0,16889	W 78,51639	S 0,000019	W 0,000030	S 0,000000000361	W 0,0000000009
20	S 0,16884	W 78,51693	S 0,16889	W 78,51639	S 0,000049	W -0,000540	S 0,000000002401	W 0,0000002916
				SUMATORIO	S 0,003830	W -0,008390	S 2,89045E-06	W 4,23985E-05

Tabla 4.15 Medición de la Ubicación de la frecuencia (PRUEBA 1)

	FRECUENCIA DE BÚSQUEDA 639,25 MHz															
	Posición Medida				Posición de Referencia				Error				Error2			
#	Latitud		Longitud		Latitud		Longitud		Latitud		Longitud		Latitud		Longitud	
1	S	0,16456	W	78,51876	S	0,16444	W	78,51972	S	-0,000116	W	0,000962	S	0,000000013353	W	0,0000009259
2	S	0,16475	W	78,51487	S	0,16444	W	78,51972	S	-0,000306	W	0,004852	S	0,000000093364	W	0,0000235441
3	S	0,16854	W	78,51974	S	0,16444	W	78,51972	S	-0,004096	W	-0,000018	S	0,000016773575	W	0,0000000003
4	S	0,16456	W	78,51661	S	0,16444	W	78,51972	S	-0,000116	W	0,003112	S	0,000000013353	W	0,0000096859
5	S	0,17009	W	78,51276	S	0,16444	W	78,51972	S	-0,005646	W	0,006962	S	0,000031872298	W	0,0000484725
6	S	0,17138	W	78,51143	S	0,16444	W	78,51972	S	-0,006936	W	0,008292	S	0,000048101931	W	0,0000687609
7	S	0,16432	W	78,5141	S	0,16444	W	78,51972	S	0,000124	W	0,005622	S	0,000000015486	W	0,0000316094
8	S	0,16449	W	78,5184	S	0,16444	W	78,51972	S	-0,000046	W	0,001322	S	0,000000002075	W	0,0000017483
9	S	0,16582	W	78,51975	S	0,16444	W	78,51972	S	-0,001376	W	-0,000028	S	0,000001892153	W	0,0000000008
10	S	0,16537	W	78,51972	S	0,16444	W	78,51972	S	-0,000926	W	0,000002	S	0,000000856653	W	0,0000000000
11	S	0,16466	W	78,51986	S	0,16444	W	78,51972	S	-0,000216	W	-0,000138	S	0,000000046464	W	0,0000000190
12	S	0,16448	W	78,51463	S	0,16444	W	78,51972	S	-0,000036	W	0,005092	S	0,000000001264	W	0,0000259307
13	S	0,16432	W	78,51912	S	0,16444	W	78,51972	S	0,000124	W	0,000602	S	0,000000015486	W	0,0000003627
14	S	0,17021	W	78,51923	S	0,16444	W	78,51972	S	-0,005766	W	0,000492	S	0,000033241631	W	0,0000002423
15	S	0,16446	W	78,51944	S	0,16444	W	78,51972	S	-0,000016	W	0,000282	S	0,000000000242	W	0,0000000796
16	S	0,16437	W	78,519899	S	0,16444	W	78,51972	S	0,000074	W	-0,000177	S	0,000000005542	W	0,0000000313
17	S	0,16531	W	78,51239	S	0,16444	W	78,51972	S	-0,000866	W	0,007332	S	0,000000749186	W	0,0000537615
18	S	0,16486	W	78,51984	S	0,16444	W	78,51972	S	-0,000416	W	-0,000118	S	0,000000172686	W	0,0000000139
19	S	0,16481	W	78,51977	S	0,16444	W	78,51972	S	-0,000366	W	-0,000048	S	0,000000133631	W	0,0000000023
20	S	0,16445	W	78,51872	S	0,16444	W	78,51972	S	-0,000006	W	0,001002	S	0,000000000031	W	0,0000010044
							SUMATORIO		S	-0,026921	W	0,04541	S	3,43662E-05	W	8,14477E-05

Tabla 4.16 Medición de la Ubicación de la frecuencia. (PRUEBA 2)

	FRECUENCIA DE BÚSQUEDA 675,25 MHz															
	Posición Medida				Posición de Referencia				Error				Error2			
#	Latitud		Longitud		Latitud		Longitud		Latitud		Longitud		Latitud		Longitud	
1	S	0,16877	W	78,52674	S	0,16872	W	78,52456	S	-0,000050	W	-0,002184	S	0,000000002500	W	0,0000047718
2	S	0,17023	W	78,51993	S	0,16872	W	78,52456	S	-0,001510	W	0,004626	S	0,000002280100	W	0,0000213958
3	S	0,16946	W	78,52643	S	0,16872	W	78,52456	S	-0,000740	W	-0,001874	S	0,000000547600	W	0,0000035135
4	S	0,16933	W	78,51986	S	0,16872	W	78,52456	S	-0,000610	W	0,004696	S	0,000000372100	W	0,0000220482
5	S	0,16971	W	78,52438	S	0,16872	W	78,52456	S	-0,000990	W	0,000176	S	0,000000980100	W	0,0000000308
6	S	0,16836	W	78,52753	S	0,16872	W	78,52456	S	0,000360	W	-0,002974	S	0,000000129600	W	0,0000088473
7	S	0,17102	W	78,52699	S	0,16872	W	78,52456	S	-0,002300	W	-0,002434	S	0,000005290000	W	0,0000059265
8	S	0,16834	W	78,52462	S	0,16872	W	78,52456	S	0,000380	W	-0,000064	S	0,000000144400	W	0,0000000042
9	S	0,16999	W	78,52371	S	0,16872	W	78,52456	S	-0,001270	W	0,000846	S	0,000001612900	W	0,0000007150
10	S	0,16253	W	78,52981	S	0,16872	W	78,52456	S	0,006190	W	-0,005254	S	0,000038316100	W	0,0000276092
11	S	0,16954	W	78,51989	S	0,16872	W	78,52456	S	-0,000820	W	0,004666	S	0,000000672400	W	0,0000217674
12	S	0,16432	W	78,52654	S	0,16872	W	78,52456	S	0,004400	W	-0,001984	S	0,000019360000	W	0,0000039380
13	S	0,17001	W	78,51327	S	0,16872	W	78,52456	S	-0,001290	W	0,011286	S	0,000001664100	W	0,0001273638
14	S	0,16977	W	78,52976	S	0,16872	W	78,52456	S	-0,001050	W	-0,005204	S	0,000001102500	W	0,0000270862
15	S	0,16622	W	78,52397	S	0,16872	W	78,52456	S	0,002500	W	0,000586	S	0,000006250000	W	0,0000003429
16	S	0,16983	W	78,52831	S	0,16872	W	78,52456	S	-0,001110	W	-0,003754	S	0,000001232100	W	0,0000140959
17	S	0,17125	W	78,51416	S	0,16872	W	78,52456	S	-0,002530	W	0,010396	S	0,000006400900	W	0,0001080676
18	S	0,16588	W	78,51987	S	0,16872	W	78,52456	S	0,002840	W	0,004686	S	0,000008065600	W	0,0000219544
19	S	0,16743	W	78,52761	S	0,16872	W	78,52456	S	0,001290	W	-0,003054	S	0,000001664100	W	0,0000093296
20	S	0,16932	W	78,51984	S	0,16872	W	78,52456	S	-0,000600	W	0,004716	S	0,000000360000	W	0,0000222365
							SUMATORIO		S	0,003090	W	0,01789	S	4,67717E-05	W	0,000356182

Tabla 4.17 Medición de la Ubicación de la frecuencia (PRUEBA 3)

4.2.3.2.2 Caculo de Errores

	frecuencia = 585,25 MHz				frecuencia = 639,25 MHz				frecuencia = 675,25 MHz			
	Latitud		Longitud		Latitud		Longitud		Latitud		Longitud	
MEDIA	S	0,0000001	W	0,00000212	S	0,0000017	W	0,00000407	S	0,0000023	W	0,00001781
RMS	S	0,0003802	W	0,00145600	S	0,0013108	W	0,00201801	S	0,0015292	W	0,00422008
ERROR PICO	S	-0,0048790	W	0,00001318	S	-0,0057656	W	0,00049222	S	0,0025000	W	0,00058556
ERROR	S	0,0006370	W	0,00154350	S	0,0013784	W	0,00232284	S	0,0016415	W	0,00377300
ERROR BIAS	S	0,0001915	W	-0,00041950	S	-0,0013461	W	0,00227027	S	0,0001545	W	0,00089456

Tabla 4.18 Errores de la Medición de la ubicación de la señal de RG1 y RG2

En la localización de un trasmisor se debe considerar la precisión del equipo utilizado para la medición, ya que la variación de milésimas de grado en latitud y longitud son muy significativas, pues podrían cambiar totalmente la ubicación del emisor, así por ejemplo cuando hablamos de un grado en latitud o longitud, en distancia eso se traduce aproximadamente a 111Km[66], esto significa que una milésima de grado equivale a 111m, este es un gran error y podría hacer variar notablemente los resultado, por lo que se prefiere que el error se produzca en el quinto o sexto digito decimal, este consideración proporciona un error aceptable.

4.3 PRUEBAS EN DETECCIÓN DE SEÑALES DE TELEFONÍA MÓVIL CELULAR, TECNOLOGÍA GSM

4.3.1 CONSIDERACIONES MÓVILES

En pruebas de detección de señales de telefonía móvil celular, tecnología GSM, el sistema debe ser totalmente móvil, es por esto que las antenas de radiogoniometría pueden montarse en un vehículo para su movilización durante las pruebas, este mecanismo de movilidad puede producir algunos errores en la precisión de la medición por esta razón es necesario tomar en cuenta algunas consideraciones que eviten estos errores.

[66] FUENTE: http://www.manualvuelo.com/NAV/NAV72.html

Estas consideraciones tienen que ver con el modo correcto de instalar una antena, eliminar obstrucciones, excesos de cable, etc., y se encuentran detallados en el Anexo F.[67]

4.3.2 CASO FERROVIARIA

Para realizar un operativo, con el fin de ubicar un dispositivo móvil usado en sistemas de telefonía internacional no autorizados se requiere el apoyo conjunto tanto del Organismo técnico de Control como de la Operadora involucrada en el caso. Es la Operadora del servicio quien facilita información sustancial para el desarrollo y ejecución de las pruebas.

A través del análisis de tráfico que genera el dispositivo móvil se puede conocer la radio base que utiliza el sistema By-pass, esto nos permite hacer pruebas previas de drive test que conllevan a limitar una zona más pequeña en la que podemos aplicar el sistema de radiogoniometría.

Las condiciones del lugar juegan un papel muy importante puesto que si es una zona muy concurrida el tráfico producido por By-pass se camufla tras el tráfico telefónico normal, por lo que se dificulta la realización de este tipo de pruebas. Sin embargo si las pruebas se ejecutan a horas de la madrugada se reduce las llamadas normales, quedando como único generador de tráfico el sistema By-pass buscado.

4.3.2.1 Procedimientos y Resultados

El operativo del caso Ferroviaria se realizó a las 12 pm hasta las 3 am, al ser una zona residencial, el número de llamadas normales era muy reducido por tanto se tenía la certeza de que el tráfico telefónico cursado era producido por el sistema By-pass.

---

[67] FUENTE: Manual de Instalación y mantenimiento del Equipo de Radiogoniometría ALMOS 3000, pág. 19.

Una vez identificada la zona y el tráfico cursado se precisa conocer los canales utilizados al igual que las frecuencias para empezar el monitoreo. Los datos requeridos para estas pruebas se encuentran en la tabla 4.19, mostrada a continuación.

DATOS TÉCNICOS DE LAS LÍNEAS DETECTADAS							
	Nombre	Sector	BCCH	Canales de Tráfico (TCH)	Cell ID	BSIC	LAC
RADIO BASE PRINCIPAL	FERROVIARIA	B	224	188,223, 237, 251	21093	7-0	24301

Tabla 4.19 Datos Técnicos de las líneas detectadas[68]

	TCCH	
Canal	Frec. Tx (MHz)	Frec. Rx (MHz)
186	880,8	835,8
223	888,2	843,2
237	891	846
251	893,8	848,8

Tabla 4.20 Frecuencias de los canales TCCH[69]

Por facilidad en la operación de los equipos se colocó un radiogoniómetro en una posición fija, mientras que el segundo radiogoniómetro se movía alrededor de la zona de investigación. Los dos radiogoniómetros eran controlados a través del software de control remoto, de donde se monitoreó los diferentes canales de tráfico, buscando la frecuencia utilizada en la transmisión de voz.

Con la ejecución de esta prueba se puede tomar los datos de la posición tanto del RG móvil como del cruce de las trazas del LOB del RG1 y RG2. Estos datos se presentan en pantalla y se van guardando en un archivo de registros dentro de la carpeta asignada para el programa del RG. Los archivos guardados de la prueba permiten realizar un post procesamiento para determinar los cruces de mayor coincidencia, con lo que se puede encontrar la ubicación más probable del sistema By-pass.

[68] FUENTE: Datos proporcionados por la Operadora, depende de los condiciones del lugar.
[69] FUENTE: Datos proporcionados por la Operadora. Asignación de frecuencias para cada canal.

Posición RG1 (Móvil)				Posición RG2 (Fijo)				Punto de Intersección RG1-RG2			
Latitud		Longitud		Latitud		Longitud		Latitud		Longitud	
S	0,25466	W	78,51617	S	0,25501	W	78,51515	S	0,25521	W	78,51634
S	0,25466	W	78,51617	S	0,25501	W	78,51515	S	0,25521	W	78,51636
S	0,25414	W	78,51539	S	0,25501	W	78,51516	S	0,25523	W	78,51607
S	0,25414	W	78,51539	S	0,25501	W	78,51516	S	0,25507	W	78,51544
S	0,25414	W	78,51539	S	0,25501	W	78,51516	S	0,25602	W	78,51932
S	0,25414	W	78,51539	S	0,25501	W	78,51516	S	0,25644	W	78,51717
S	0,25414	W	78,51539	S	0,25501	W	78,51516	S	0,25500	W	78,51523
S	0,25373	W	78,51522	S	0,25501	W	78,51515	S	0,25395	W	78,51538
S	0,25366	W	78,51522	S	0,25501	W	78,51515	S	0,25339	W	78,51612
S	0,25366	W	78,51522	S	0,25501	W	78,51515	S	0,25393	W	78,51580
S	0,25354	W	78,51524	S	0,25501	W	78,51515	S	0,25413	W	78,51538
S	0,25354	W	78,51524	S	0,25501	W	78,51515	S	0,25381	W	78,51547
S	0,25346	W	78,51526	S	0,25501	W	78,51515	S	0,25341	W	78,51534
S	0,25341	W	78,51527	S	0,25501	W	78,51515	S	0,25333	W	78,51535
S	0,25341	W	78,51527	S	0,25501	W	78,51515	S	0,25330	W	78,51535
S	0,25325	W	78,5153	S	0,25501	W	78,51515	S	0,25506	W	78,51541
S	0,25322	W	78,5153	S	0,25501	W	78,51515	S	0,25517	W	78,51599
S	0,2532	W	78,5153	S	0,25501	W	78,51515	S	0,25424	W	78,51545
S	0,25282	W	78,51519	S	0,25501	W	78,51515	S	0,25529	W	78,51610
S	0,25279	W	78,51515	S	0,25501	W	78,51515	S	0,25576	W	78,51766
S	0,25245	W	78,51564	S	0,25501	W	78,51515	S	0,25548	W	78,51652
S	0,25245	W	78,51564	S	0,25501	W	78,51515	S	0,25531	W	78,51601
S	0,25263	W	78,51567	S	0,25501	W	78,51514	S	0,25509	W	78,51527
S	0,25317	W	78,5153	S	0,25501	W	78,51515	S	0,25311	W	78,51589
S	0,25279	W	78,51558	S	0,25501	W	78,51515	S	0,25523	W	78,51542
S	0,25323	W	78,51534	S	0,25501	W	78,51516	S	0,25472	W	78,51637
S	0,25325	W	78,51533	S	0,25501	W	78,51516	S	0,25495	W	78,51541
S	0,2533	W	78,51533	S	0,25501	W	78,51516	S	0,25484	W	78,51587
S	0,25332	W	78,51533	S	0,25501	W	78,51516	S	0,25505	W	78,51589
S	0,25345	W	78,51431	S	0,25501	W	78,51516	S	0,25511	W	78,51533
S	0,25386	W	78,51529	S	0,25501	W	78,51516	S	0,25545	W	78,51695
S	0,25408	W	78,51543	S	0,25501	W	78,51516	S	0,25474	W	78,51610
S	0,25416	W	78,51533	S	0,25501	W	78,51516	S	0,25479	W	78,51612
S	0,25416	W	78,51533	S	0,25501	W	78,51516	S	0,25488	W	78,51574
S	0,25416	W	78,51553	S	0,25501	W	78,51516	S	0,25501	W	78,51520
S	0,25416	W	78,51553	S	0,25501	W	78,51516	S	0,25481	W	78,51579
S	0,25416	W	78,51553	S	0,25501	W	78,51516	S	0,25541	W	78,51566

Tabla 4.21 Mediciones de la posición de la señal celular en la Banda de UHF

Los resultados se pueden tabular en tablas de Excel, lo cual facilita el análisis.

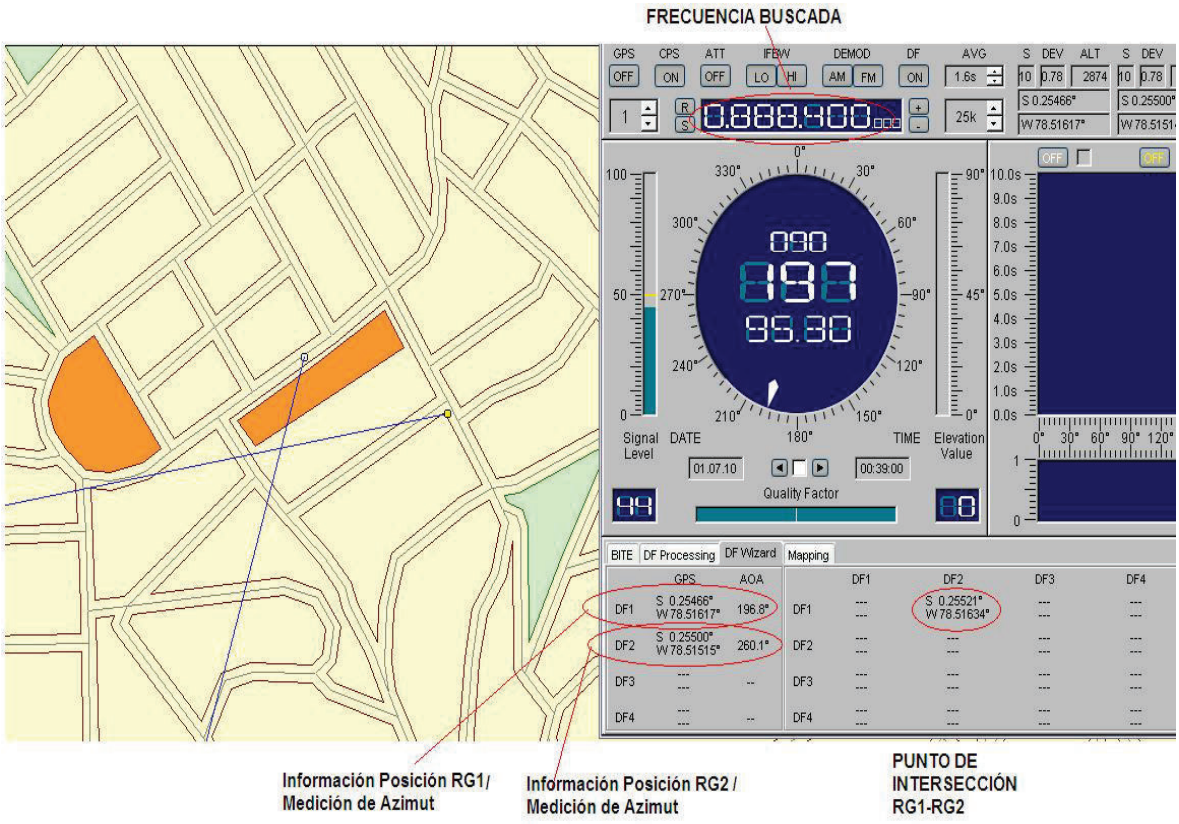
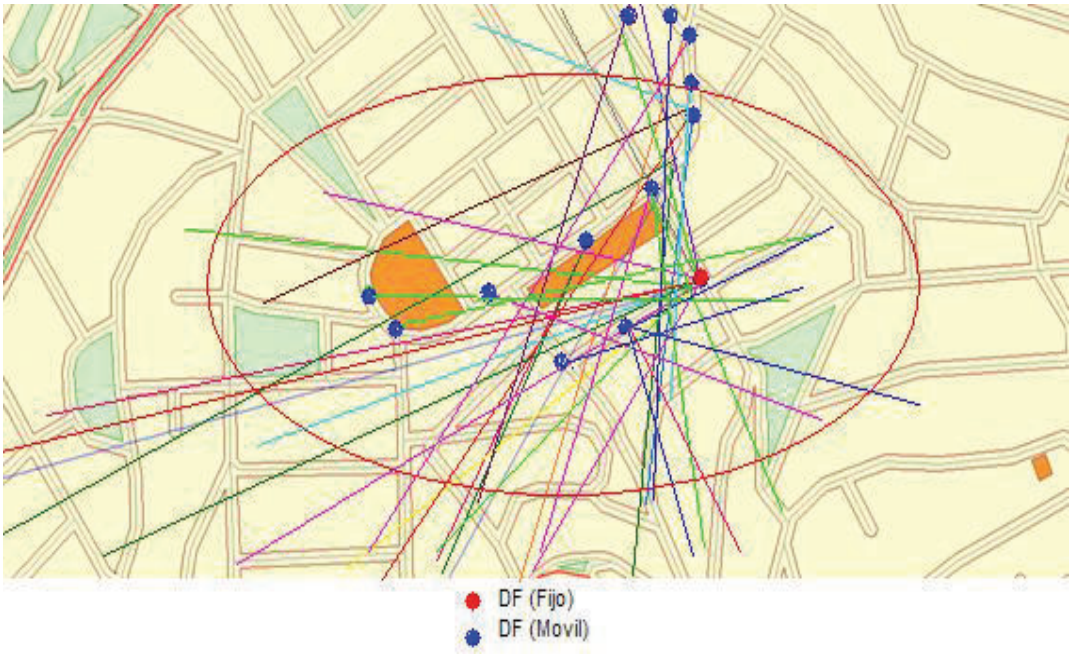


Figura 4.15 Proceso de detección, presentación Gráfica

Cuando el sistema de telefonía By-pass se encuentra en plena actividad, el número de coincidencias va a ser mayor, por tanto la precisión de la prueba estará sujeta al número de trazas que se puedan tomar, de ahí la importancia de que las mediciones se registren en tiempo real ya que cuando esto ocurre se puede saber con certeza que el punto de intersección presentado en pantalla es el punto de donde se emitió la señal en ese instante de tiempo.

Una vez terminada la prueba se toman todas las trazas individuales y se trasladan a un solo mapa para poder visualizar los resultados de manera global. Las trazas individuales se encuentran en el Anexo G.



.

Figura 4.16 Traslado de las trazas individuales en un solo mapa (MAPINFO)

Figura 4.17 Traslado de la zona probable a GOOGLE EARTH

Al encontrar una zona más reducida se deben efectuar una serie de inspecciones del lugar para identificar elementos del sistema By-pass, que delaten la instalación, además se buscan los enlaces digitales contratados en la zona que

pueden estar siendo utilizados por el sistema bypass, estos datos nos permiten finalmente dar con la ubicación de la instalación.

La efectividad del sistema se reflejo a través de la obtención de la ubicación de la instalación del Bypass, en la zona donde se realizaron las pruebas.

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

Del desarrollo del presente proyecto de titulación se concluye que:

- El perjuicio causado por los sistemas de telefonía internacional no autorizados, en términos económicos representan para el país pérdidas millonarias, de ahí la importancia de buscar nuevas herramientas que permitan mitigar este tipo de fraude.

- Los equipos de radiogoniometría obtenidos por la SUPERTEL, son equipos de alta tecnología sin embargo su utilidad es mayor y logra su propósito cuando se consigue la integración de ambos en un solo sistema, con el que se puedan desarrollar pruebas que efectúen el proceso de triangulación de señales de forma directa, el sistema implementado permite la integración de los dos equipos de radiogoniometría esto permite obtener mediciones en tiempo real.

- Las mediciones en tiempo real juegan un papel vital en las detecciones de señales de telefonía móvil celular, pues de las mediciones instantáneas que se tomen se podrá obtener los puntos probables de ubicación del dispositivo móvil que queremos encontrar.

- La utilización de puertos virtuales, optimiza el uso de puertos físicos en un computador, además permite la compatibilidad de diferente protocolos utilizados en la transporte de los datos.

- En pruebas de búsqueda de instalaciones de sistemas de telefonía móvil internacional implementado a través de líneas móviles celulares

(Tecnología GSM), la movilidad del sistema es un factor determinante pues debe estar en la capacidad de funcionar en cualquier sitio del país donde se desarrolle la investigación, por tal motivo el sistema fue implementado de tal manera que cumpla con esta condición.

- La estabilidad del sistema está supeditado a la estabilidad de la red, puesto que la VPN ha sido implementada en una red de telefonía celular, en el Ecuador se presentan dos tecnologías de red para este tipo de servicio, estas son tecnología GPRS y tecnología 3G, la primera es bastante inestable en la transmisión de datos, por lo que no brinda un soporte adecuado para la conexión de los equipos de radiogoniometría, sin embargo en lugares no muy congestionados podría servir como una alternativa de conexión, en el caso de la tecnología 3G esta es mucho más robusta pero su principal inconveniente es la cobertura mínima existente en el país, por tal motivo los módems utilizados tienen una funcionalidad dual, esto es; que pueden funcionar en las dos tecnologías dependiendo de la zona en la que se realice la investigación.

- La implementación de la solución SIBTS propuesta no es viable debido a que tiene un gran componente teórico que no ha sido ampliamente probado en forma práctica.

- El mayor inconveniente práctico que presenta la solución de la SIBTS se da por el manejo propietario de los protocolos utilizados en la comunicación de los diferentes componentes de la red.

- La configuración de los parámetros que se necesitan para realizar la llamada ciega, presenta un alto grado de complejidad debido a que estos parámetros se modifican en su mayoría en el núcleo de la red, afectando no solo al dispositivo buscado, sino a todos los usuarios que se controlen a través de ese MSC

- Al utilizar este tipo de solución, los parámetros de planeación de Red deben ser coordinados con los Operadores móviles, lo que podría retrasar la ejecución de los operativos y se tendría un alto riesgo de fuga de información.

- El constante cambio y dinamismo que existe sobre la información de parámetros de Red de Operadores Móviles, necesitaría una permanente actualización de parámetros sobre la SIBTS, de no ser así se podría incurrir en errores de ejecución en operativos.

- La ejecución de operativos basados en la SIBTS, involucraría no solo variar los parámetros de la red sino también disminuir la calidad del servicio dado por los operadores, este hecho va en contra de los derechos usuarios y de los estatutos legales presentes en los contratos de concesión de cada operador.

- La solución SIBTS puede alcanzar un alto costo, debido a que no es una Solución probada en forma Global y al no ser escalable a otras tecnologías, el tiempo de utilidad del mismo estaría sujeto a la permanecía de la telefonía GSM. Con el rápido desarrollo de las redes móviles, el costo de la solución versus su tiempo de vida útil no justificaría su adquisición.

- El procedimiento propuesto para utilizar el sistema de radiogoniometría para determinar la ubicación de un dispositivo móvil celular sin el uso de la SIBTS es totalmente viable, ya que se cuenta con todas las herramientas técnicas para su ejecución. Sin embargo se requiere de un trabajo conjunto entre la SUPERTEL y las operadoras móviles involucradas.

- La probabilidad de encontrar el dispositivo móvil buscado aumenta cuando el sistema bypass se encuentra en plena actividad al momento de ejecutar las pruebas, sin embargo las condiciones del sitio son determinantes para obtener resultados positivos.

- La reducción de la zona, donde podría estar instalado el sistema Bypass, facilita la búsqueda de su ubicación, ya que complementada con la inspección del lugar y la búsqueda de enlaces, se pueden obtener resultados acertados, como fue el caso Ferroviaria.

- El sistema de radiogoniometría es una herramienta muy poderosa que permite combatir de forma efectiva las actividades ilícitas que se producen en el campo de las telecomunicaciones, como es el caso de los sistemas de telefonía internacional no autorizados (Bypass) implementados a través de líneas móviles celulares tecnología GSM.

RECOMENDACIONES

- Con el rápido desarrollo de las tecnologías, la implementación de nuevas técnicas de fraude también avanza a pasos agigantados, por tanto es recomendable contar con herramientas tecnológicas que permitan mitigarlas.

- Se recomienda investigar nuevas formas de combate al fraude en telecomunicaciones, puesto que el uso del internet y la convergencia de tecnologías han dejado una puerta abierta para que se susciten innumerables tipos de fraudes.

- La precisión de las mediciones, dependen de la calibración de los equipos de radiogoniometría, por tanto este proceso se debe realizar con mucho cuidado y tomando en cuenta todas las indicaciones dadas por el fabricante.

BIBLIOGRAFÍA:

LIBROS:

- CHANDRAN Sathish, Advances in Direction-of-Arrival Estimation, Editorial Artech House Publisher, 30 de Diciembre del 2005.

- JENKINS Herndon H., Small-Aperture Radio Direction-Finding, Editorial Artech House Publishers, 1 de Abril de 1991.

- GETHING P. J. D. , Radio Direction Finding and Superresolution, Editorial The Institution of Engineering and Technology; 2da. Edición, 1 de Octubre de 1991.

- FORSSELL Börje, Radionavigation systems, Editorial Prentice Hall, 1991.

- PÉREZ Jaime; Radionavegación, Edición UPC, 1995.

- J.A. Biyd, D.B. Harris, D.D. King & H.W. Welch, Jr. Electronic Countermeasures," Direction Finding". 1979 Los Altos, CA: Peninsula Publishing. ISBN 0-932146-00-7.

- ROUTLEDGE y KEGAN Paul, Marine Electronic Navigation, 2da Edición.

- KEEN R, Wireless Direction Finding, 8va. Edición, 1947, Iliffe, Londres.

- MESA María Jose, Fraude en Telecomunicaciones, SUPERTEL 2007

REVISTAS:

- MOELL Joseph D., CURLEE Thomas N.; Transmitter Hunting; Paperback , 1987

- LIPSKY Stephen E.; Microwave Passive Direction Finding; Paperback, Junio 2004

- MILLER Frederic P., VANDOME Agnes F., MCBREWSTE John; Amateur Radio Direction Finding; Paperback, 2009

- MANUAL de Usuario de los Equipos de Radiogoniometría ALOMOS 3000

- MANUAL de Software de Control Remoto de los Equipos de Radiogoniometría ALMOS 3000

- MANUAL de instalación y mantenimiento de Los Equipos de Radiogoniometría ALMOS 3000

- Instituto Costarricense de Electricidad Telecomunicaciones/ presentación Fraude en Telecomunicaciones.

PÁGINAS WEB:

- http://www.tele.ucl.ac.be/EDU/ELEC2796/elec2796_5.pdf
- http://www.cypsela.es/especiales/pdf199/umts.pdf
- http://www.freebookcentre.net/mobile-technology/Free-UMTS-Books-Download.html
- http://www.radio-electronics.com/info/cellulartelecomms/gsm_technical/handover-handoff.php
- http://searchmobilecomputing.techtarget.com/definition/handoff
- http://www.ieee802.org/21/archived_docs/Documents/OtherDocuments/Handoff_Freedman.pdf
- http://www.upv.es/satelite/trabajos/pracGrupo3/handoff.htm
- http://searchmobilecomputing.techtarget.com/news/919011/Definitions-CDMA-TDMA-and-GSM
- http://www.bandaancha.es/Informacion/Tecnologias/TecnologiasInalambricas/Paginas/UMTS.aspx
- http://www.slideshare.net/durango0395/diapositivas-de-tecnologia-35-g
- http://www.qsl.net/eb1hbk/taller/radiogonio.html

- http://www.canalsocial.net/GER/
- http://nacc.upc.es/adf/adf.radiogoniometro.html
- http://www.exordio.com/1939-1945/civilis/telecom/hf-df.html
- http://knol.google.com/k/sistema-de-control-via-gprs-y-sms
- http://www2.udec.cl/~eduamoli/gprs.htm
- http://www.mundov.com/gprs_edge.php
- http://searchmobilecomputing.techtarget.com/definition/UMTS
- http://www.tech-faq.com/wcdma.html
- http://www.umtsworld.com/technology/wcdma.htm
- http://www.uv.es/siuv/cas/zxarxa/vpn.htm
- http://www.cypsela.es/especiales/pdf199/umts.pdf
- http://technet.microsoft.com/es-es/library/cc736330(WS.10).aspx
- http://blackspiral.org/docs/pfc/itis
- http://www.34t.com/box-docs.asp?doc=649
- http://definicion.de/fraude/
- canTV, Presentación fraude en telecomunicaciones
- http://es.kioskea.net/contents/telephonie-mobile/gsm.php3
- http://www.ieee802.org/21/archived_docs/Documents/Handoff_Freedman.pdf
- www.pangolinsms.com/.../tdma-large.gif
- http://searchmobilecomputing.techtarget.com/definition/FDMA
- http://it.toolbox.com/wiki/index.php/SDMA
- http://www.scribd.com/doc/39399415/SENALIZACION-GSM
- http://www.upv.es/satelite/trabajos/pracGrupo3/handoff.htm
- http://it.toolbox.com/wiki/index.php/SDMA
- www.rohde-schwarz.com/WWW/Publicat.nsf/article/.../n180_cmu200.pdf
- http://server-die.alc.upv.es/asignaturas/LSED/2002-03/Redes_GSM/roaming.htm
- http://www.radio-electronics.com/info/cellulartelecomms/gsm_technical/handover-handoff.php
- http://doblevia.wordpress.com/2007/03/19/rumbo-y-azimut/
- http://www.manualvuelo.com/NAV/NAV72.html